

H. E. Rose

# A COURSE ON FINITE GROUPS

Web Sections, Web Chapters and  
Solution Appendix

Springer



## TABLE OF Web Sections

The material presented in this **Web Site** is additional to that given in the main text – **A Course on Finite Groups**. It consists of extra sections to some of the chapters with in most cases a set of supplementary problems, two extra chapters providing an introduction to group representation theory, and a long Appendix giving solutions, ranging from brief hints to complete answers, to all of the problems listed in the main text. Chapter, section, definition, theorem, problem and equation numbers all follow on from those given in the main text. In fact these **Web Sections** could be printed, and then slotted into the main text at the appropriate places allowing for the non-consecutive page numbers. Again it is a pleasure to thank Ben Fairbairn for commenting on and improving the text.

Web Section 3.6	Representations of $A_5$ .....	325
3.7	Problems 3W .....	327
Web Section 4.6	The Transfer .....	331
4.7	Group Presentation, Part 2 .....	335
4.8	Problems 4W .....	347
Web Section 5.4	Transitive and Primitive Permutation Groups, Iwasawa's Lemma .....	351
5.5	Problems 5W .....	358
Web Section 6.5	Further Applications. Burnside's Normal Complement Theorem, Groups with Cyclic Sylow Subgroups .....	361
6.6	Problems 6W .....	369
Web Section 7.5	Infinite Abelian Groups. A Brief Introduction .....	371
Web Section 9.4	Schur-Zassenhaus Theorem .....	377
9.5	Problems 9W .....	384

<b>Web Section 12.6</b>	Simple Groups of Order less than 1000000, a second proof of the Simplicity of the Groups $L_n(q)$ , and a method for generating Steiner Systems for some Mathieu Groups .....	387
12.7	Problem 12W .....	399
<b>Web Chapter 13</b>	<b>Representation and Character Theory</b> .....	401
13.1	Representations and Modules .....	402
13.2	Theorems of Schur and Maschke .....	408
13.3	Characters and Orthogonality Relations .....	412
13.4	Lifts and Normal Subgroups .....	422
13.5	Problems 13 .....	427
<b>Web Chapter 14</b>	<b>Character Tables and Theorems of Burnside and Frobenius</b> .....	433
14.1	Character Tables .....	434
14.2	Burnside's $p^r q^s$ -theorem .....	440
14.3	Frobenius Groups .....	444
14.4	Problems 14 .....	455
14.5	Appendix on Algebraic Integers .....	459
<b>Web Solution Appendix</b>	<b>Answers and Solutions, Problems 2</b> .....	461
	Problems 3 .....	472
	Problems 4 .....	481
	Problems 5 .....	489
	Problems 6 .....	497
	Problems 7 .....	508
	Problems 8 .....	515
	Problems 9 .....	521
	Problems 10 .....	524
	Problems 11 .....	532
	Problems 12 .....	538
	Problems A .....	544
	Problems B .....	545
	Subgroup lattice diagrams for Groups of Order 8, 12 or 16 .....	547
	Addendum .....	559

## 3.6 Representations of $A_5$

At the beginning of this chapter we noted that most groups have several distinct *representations*; to illustrate this fact we discuss here some representations of  $A_5$ . In Section 3.2 we introduced  $A_5$  as the group of all even permutations on a five element set. It can also be (indirectly) specified as the only non-Abelian simple group up to isomorphism of order less than 100,<sup>1</sup> see Problem 6.15.

The group  $A_5$  has a number of presentations, three are as follows:

$$\mathcal{P}_1 : \langle a, b \mid a^3 = b^5 = (ab)^2 = e \rangle,$$

$$\mathcal{P}_2 : \langle a, b \mid a^5 = b^5 = (ab)^2 = (a^4b)^3 = e \rangle,$$

$$\mathcal{P}_3 : \langle a, b, c \mid a^3 = b^3 = c^3 = (ab)^2 = (bc)^2 = (ca)^2 = e \rangle.$$

To show that each of these presentations do in fact define  $A_5$  we can argue as follows. Consider  $\mathcal{P}_1$ . We associate permutations in  $A_5$  (treating  $A_5$  as a permutation group) with each generator and then show that the corresponding relations hold. This shows that a copy of  $A_5$  is a factor of  $\mathcal{P}_1$ . Secondly, we show that  $\mathcal{P}_1$  has 60 elements and this will be done in Problem 3.26. Similar arguments are required for  $\mathcal{P}_2$  and  $\mathcal{P}_3$ . For  $\mathcal{P}_1$  set

$$a \mapsto (1, 4, 2) \quad \text{and} \quad b \mapsto (1, 2, 3, 4, 5), \quad \text{then} \quad ab = (1, 5)(3, 4).$$

It is immediately clear that the relations of  $\mathcal{P}_1$  are satisfied. For  $\mathcal{P}_2$  we set

$$a \mapsto (2, 1, 3, 4, 5) \quad \text{and} \quad b \mapsto (1, 2, 3, 4, 5), \quad \text{then}$$

$$ab = (1, 4)(3, 5) \quad \text{and} \quad a^4b = (1, 3, 2),$$

and for  $\mathcal{P}_3$  we set

$$a \mapsto (1, 2, 3), \quad b \mapsto (1, 2, 4) \quad \text{and} \quad c \mapsto (1, 2, 5),$$

note that  $(1, 2, j)(1, 2, k) = (1, k)(2, j)$  if  $j, k > 2$  and  $j \neq k$ .

The group  $A_5$  also has a number of matrix representations, we give two here and one more in Problem 3.27, further representation examples can be found in the ATLAS (1985). First we show that  $SL_2(4)$  is one such representation. This group is defined as the set of all  $2 \times 2$  matrices  $A$  with  $\det A = 1$  defined over the 4-element field  $\mathbb{F}_4$ , see Section 3.3. Let the elements of  $\mathbb{F}_4$  be

$$0, 1, c \text{ and } c + 1, \quad \text{where} \quad 1 + c + c^2 = 0,$$

and we work ‘modulo 2’, that is  $1 + 1 = c + c = 0$  and  $c^2 = c + 1$ ; see Section 12.2. Using the presentation  $\mathcal{P}_3$ , we set

$$a \mapsto \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad b \mapsto \begin{pmatrix} 1 & c+1 \\ c & 0 \end{pmatrix} \quad \text{and} \quad c \mapsto \begin{pmatrix} 1 & c \\ c+1 & 0 \end{pmatrix},$$

---

<sup>1</sup> In fact, it is the only non-Abelian simple group of order less than 168, see Chapter 12.

then

$$ab = \begin{pmatrix} c+1 & c+1 \\ 1 & c+1 \end{pmatrix}, \quad bc = \begin{pmatrix} c+1 & c \\ c & c+1 \end{pmatrix} \quad \text{and} \quad ca = \begin{pmatrix} c+1 & 1 \\ c+1 & c+1 \end{pmatrix}.$$

We leave it as an exercise for the reader to show that these matrices satisfy the relations in  $\mathcal{P}_3$ , and that this system contains 60 matrices.

Our second matrix representation is  $L_2(5)$  which is defined as follows. Working over the 5-element field (that is working ‘modulo 5’), we take  $SL_2(5)$  and factor out its centre. The process of forming a factor group is defined Chapter 4. The centre of  $SL_2(5)$  is  $\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$ , see Problem 3.19; hence we work in  $SL_2(5)$  and treat  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$  and  $\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$  as the ‘same’ matrix. Formally, the elements of  $L_2(5)$  are the cosets of  $Z(SL_2(5))$  in the group  $SL_2(5)$ . Note that  $-1 \equiv 4 \pmod{5}$  *et cetera*. Using the presentation  $\mathcal{P}_2$  above, we set

$$a \mapsto \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix} \quad \text{and} \quad b \mapsto \begin{pmatrix} 4 & 1 \\ 1 & 3 \end{pmatrix},$$

then

$$ab \mapsto \begin{pmatrix} 4 & 1 \\ 3 & 1 \end{pmatrix} \quad \text{and} \quad a^4b \mapsto \begin{pmatrix} 4 & 1 \\ 4 & 0 \end{pmatrix},$$

and it is a simple matter to show that the relations of  $\mathcal{P}_2$  are satisfied. The choice of matrices and permutations above do satisfy the required conditions but are definitely not unique; as an exercise the reader should find some other examples.

Another representation of  $A_5$  is as the rotational symmetry group of a dodecahedron. A dodecahedron is a regular solid structure with twelve regular equal-sized plane pentagonal faces with edges of equal length. This structure has three types of rotational symmetry: (i) rotation about a line drawn through the centres of opposite faces, this has order 5 as the faces are regular and have five edges; (ii) rotation about opposite vertices, in this structure three pentagonal faces meet at a vertex, and so this symmetry has order 3; and (iii) rotation about the centres of opposite edges, this has order 2. Now using the presentation  $\mathcal{P}_1$  above, if we associate a symmetry of type (ii) with  $a$  and a symmetry of type (i) with  $b$ , then a symmetry of type (iii) is associated with  $ab$ . To see this the reader should obtain a model of an dodecahedron and try it! It is now easily seen that the relations of  $\mathcal{P}_1$  are satisfied, and (with some patience) that there are 60 symmetries in all. An excellent film, made by the Open University for their second year course in pure mathematics, illustrates this isomorphism clearly.

The group  $A_5$  can also be treated as the rotational symmetry group of a icosahedron. An icosahedron  $I$  is a regular solid with 20 identical equilateral triangular faces and it can be inscribed in a dodecahedron  $D$  by taking the vertices of  $I$  as the centres of the faces of  $D$ . This process is self-inverse for we can also inscribe a dodecahedron inside an icosahedron using the same method. This latter representation of  $A_5$  is the one that has been used by

some chemists to describe the structure of the carbon molecule Carbon60, see page 24.

The ATLAS (1985) gives some more representations of  $A_5$ , for example as unitary groups defined over the fields  $\mathbb{F}_{16}$  or  $\mathbb{F}_{25}$ . Also this group occurs as maximal subgroups of a number of simple groups, for example  $A_6$ ,  $L_2(k)$  where  $k = 11, 16, 19, 29$  and  $31$ , and the Janko group  $J_2$  (sometimes called the Hall-Janko group). Further details are given in Chapter 12, the ATLAS (1985), and the 'online' Atlas.

### 3.7 Problems 3W

**Problem 3.25** (An Example of a Free Group) A linear fractional transformation  $f$  of the complex plane  $\mathbb{C}$  to itself is a map of the form

$$f_{a,b,c,d}(z) = \frac{az+b}{cz+d} \quad \text{where} \quad ad-bc \neq 0 \quad \text{for} \quad a, b, c, d \in \mathbb{C}.$$

(i) Show that the mapping

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto f_{a,b,c,d}$$

is a homomorphism (see Section 4.1) from  $GL_2(\mathbb{C})$  to the group of all linear fractional transformations.

(ii) Show that the matrices  $A = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$  and  $B = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$  generate a free subgroup in the group of all linear fractional transformations. (Hint. Consider the effect on points inside and outside the unit circle in the complex plane.)

**Problem 3.26\*** Let  $G = \langle a, b \mid a^3 = b^5 = (ab)^2 = e \rangle$ ; see page 325. Show that  $G$  has at most 60 elements using the following method, see Passman (1968, page 120). Clearly if  $H = \langle b \rangle$ , then  $o(H) = 5$  and  $H \leq G$ . Consider the following set of twelve cosets of  $H$  in  $G$  (we are not assuming that they are distinct, but in fact they are).

$$\begin{array}{cccccc} H & Ha^2 & Ha^2ba & Ha^2b^2 & Ha^2b^2a^2 & Ha^2b^2a^2ba \\ Ha & Ha^2b & Ha^2ba^2 & Ha^2b^2a & Ha^2b^2a^2b & Ha^2b^2a^2ba^2 \end{array}.$$

Further, let  $H^*$  denote the union of these twelve cosets. Now if  $H_1 \in H^*$ , then  $H_1a \in H^*$  as  $a^3 = e$ . By considering each coset in turn, show that if  $H_1 \in H^*$  then  $H_1b \in H^*$ . Deduce  $H^*G = H^*$ , and so prove the result.

**Problem 3.27** Working over the complex field  $\mathbb{C}$ , let  $z$  be a primitive fifth-root of unity, that is  $z^5 = 1$  and  $z \neq 1$ . Note that

$$2(z+z^4) = -1 + \sqrt{5} \quad \text{and} \quad 2(z^2+z^3) = -1 - \sqrt{5}.$$

Further let

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & z & 0 \\ 0 & 0 & z^4 \end{pmatrix}, \quad B = \frac{1}{2\sqrt{5}} \begin{pmatrix} 2 & 4 & 4 \\ 2 & -1 - \sqrt{5} & -1 + \sqrt{5} \\ 2 & -1 + \sqrt{5} & -1 - \sqrt{5} \end{pmatrix}.$$

(i) Show that  $A^5 = B^2 = (AB)^3 = I_3$ , and so using Problem 3.26 show that  $\langle A, B \rangle \simeq A_5$ . Note that the presentation suggested here is closely related to the presentation  $\mathcal{P}_1$  given on page 325.

(ii) Give representatives of the conjugacy classes.

We shall return to this example in **Web Section 14.1**.

**Problem 3.28** (Properties of  $A_6$ ) (i) Our first representation of  $A_6$  is as the group of even permutations on the set  $X = \{1, 2, 3, 4, 5, 6\}$ . It also has the following two presentations:

$$\langle a, b \mid a^5 = b^5 = (ab)^2 = (a^4b)^4 = e \rangle,$$

and

$$\langle c, d \mid c^5 = d^3 = (cd)^4 = [c, d] = e \rangle,$$

where the square brackets denotes the commutator. Note the similarity of the first of these presentations with the presentation  $\mathcal{P}_2$  for  $A_5$  given on page 325. Show that each of these presentations is valid for  $A_6$  using the following method. Begin by showing that if we set

$$a \mapsto (1, 2, 3, 4, 5) \quad \text{and} \quad b \mapsto (1, 4, 6, 3, 2)$$

then  $a$  and  $b$  satisfy the first set of relations, and if we set

$$c \mapsto (1, 2, 3, 4, 5) \quad \text{and} \quad d \mapsto (4, 5, 6)$$

then  $c$  and  $d$  satisfy the second set. Now show that  $b$  can be expressed in terms of  $c$  and  $d$ , and also  $d$  can be expressed in terms of  $a$  and  $b$ , and use these facts to establish these presentations.

(ii) Show that the group  $G = \langle (1, 2)(3, 4), (1, 2, 3)(4, 5, 6) \rangle$  is a subgroup of  $A_6$  using one of the presentations of  $A_5$  given in this section.

(iii) By trial show that the group  $G$  given in (ii) is doubly transitive on  $\{1, 2, 3, 4, 5, 6\}$ , that is for every pair of two-element subsets of  $X$ :  $X_i = \{x_{i1}, x_{i2}\} \subseteq X$ , there exists  $\sigma \in G$  with the properties  $x_{11}\sigma = x_{21}$  and  $x_{12}\sigma = x_{22}$ .

(iv) How many copies of  $A_5$  occur as subgroups in  $A_6$ ?

See also Problems 4.20 and 12.4(ii).

**Problem 3.29** (i) Show that if  $n > 2$ , then every index  $n$  subgroup in  $A_n$  is isomorphic to  $A_{n-1}$ . (Hint. Use Theorem 5.15 and the example on page 192.)



(ii) Use (i) to show that if  $G$  is a non-Abelian simple group with order 60, then  $G \simeq A_5$ . The method is as follows. Using Theorem 5.15 and the Sylow theory (for the prime 5) to show that  $G$  can be embedded in  $S_6$ , then use (i) and Problem 3.7(ii).

**Problem 3.30** Suppose  $\sigma \in S_n$  has the cyclic decomposition

$$\sigma = (a_1, \dots, a_{i_1})(b_1, \dots, b_{i_2}) \dots (c_1, \dots, c_{i_n}).$$

Let  $\xi_\sigma$ , a product of 2-cycles, be defined by

$$\xi_\sigma = (a_2, a_{i_1})(a_3, a_{i_1-1}) \dots (a_{j_1}, a_{k_1})(b_2, b_{i_2})(b_3, b_{i_2-1}) \dots (c_{j_n}, c_{k_n}),$$

where no 2-cycle is present if  $i_r = 2$  (that is if the  $r$ th cycle in  $\sigma$  is a 2-cycle), and

$$\begin{aligned} j_r &= [i_r/2] \quad \text{and} \quad k_r = j_r + 2 \quad \text{if } i_r \text{ is even} \\ j_r &= [i_r/2] + 1 \quad \text{and} \quad k_r = j_r + 1 \quad \text{if } i_r \text{ is odd,} \end{aligned}$$

where the square brackets denote integer part. The term  $\xi_\sigma$  is called the *standard conjugator* for  $\sigma$ .

(i) Show that  $\xi_\sigma^{-1} \sigma \xi_\sigma = \sigma^{-1}$ .

(ii) A group  $G$  is called *ambivalent* if each element of  $G$  is a conjugate of its inverse. Prove that

(a)  $S_n$  is ambivalent for all  $n$ ,

(b)  $A_n$  is ambivalent if, and only if,  $n = 1, 2, 5, 6, 10$  or  $14$ .

(Hint. See Theorem 3.12 and Problems 3.3 and 5.25, and for (b) consider the following cases where  $\tau \in S_n$

if  $n = 4r$ , then  $\tau$  is a  $(4r - 1)$ -cycle  $\times$  1-cycle;

if  $n = 4r + 1$  and  $r > 1$ , then  $\tau$  is a  $(4r - 3)$ -cycle  $\times$  3-cycle;

if  $n = 4r + 2$  and  $r > 3$ , then  $\tau$  is a  $(4r - 7)$ -cycle  $\times$  5-cycle  $\times$  3-cycle  $\times$  1-cycle;

if  $n = 4r + 3$ , then  $\tau$  is an  $n$ -cycle.)

One application of ambivalence is related to the character theory of the group in question, for if  $G$  is ambivalent then all of the irreducible characters of  $G$  are entirely real-valued; a stronger result holds for symmetric groups, see **Web Chapter 13**.

**Problem 3.31** (An Infinite Simple Group) Let  $S_{\mathbb{N}}$  denote the group of all permutations of the positive integers  $\mathbb{N}$ . If  $\sigma \in S_{\mathbb{N}}$  let

$$z(\sigma) = \{n \in \mathbb{N} : n\sigma \neq n\},$$

so  $z(\sigma)$  equals the set of integers moved by  $\sigma$ , note that this set may be finite or infinite.

(i) For  $\sigma, \tau \in S_{\mathbb{N}}$  show that (a)  $z(\sigma^{-1}) = z(\sigma)$ , (b)  $z(\sigma\tau) \subseteq z(\sigma) \cup z(\tau)$ , (c)  $z(\sigma^{-1}\tau\sigma) = \{n\sigma : n \in z(\tau)\}$ , and (d) if  $z(\sigma) \cap z(\tau) = \emptyset$  then  $\sigma$  and  $\tau$  commute.

Now define

$$S_{(\mathbb{N})} = \{\sigma \in S_{\mathbb{N}} : o(z(\sigma)) < \infty\},$$

it is called the *restricted symmetric group on  $\mathbb{N}$* , and it contains those permutations that move only a finite number of elements of  $\mathbb{N}$ .

(ii) Show that (a)  $S_{(\mathbb{N})} \triangleleft S_{\mathbb{N}}$ , (b) every element of  $S_{(\mathbb{N})}$  has finite order, and (c)  $S_{(\mathbb{N})}$  has infinitely many cosets in  $S_{\mathbb{N}}$ . In the notation of Chapter 4, the factor group  $S_{\mathbb{N}}/S_{(\mathbb{N})}$  is infinite.

Further, for  $k = 1, 2, \dots$ , define

$$S_{(\mathbb{N})}^k = \{\sigma \in S_{(\mathbb{N})} : n\sigma = n \text{ for all } n > k\}.$$

(iii) Show that, for all  $k$ , (a)  $S_{(\mathbb{N})}^k < S_{(\mathbb{N})}$ , (b)  $S_{(\mathbb{N})}^k \simeq S_k$ , (c)  $S_{(\mathbb{N})}^1 < S_{(\mathbb{N})}^2 < \dots < S_{(\mathbb{N})}$ , and (d)  $\bigcup_{k=1}^{\infty} S_{(\mathbb{N})}^k = S_{(\mathbb{N})}$ .

Lastly define  $A_{(\mathbb{N})}^1 = A_{(\mathbb{N})}^2 = \langle e \rangle$ , for  $k > 1$  let  $A_{(\mathbb{N})}^k$  denote the unique subgroup of index 2 in  $S_{(\mathbb{N})}^k$  (note we need to prove uniqueness), and let

$$A_{(\mathbb{N})} = \bigcup_{k=1}^{\infty} A_{(\mathbb{N})}^k.$$

(iv) Prove that  $A_{(\mathbb{N})}^k \simeq A_k$ ,  $A_{(\mathbb{N})}^1 < A_{(\mathbb{N})}^2 < \dots < A_{(\mathbb{N})}$ , and so deduce, using Problem 2.30,  $A_{(\mathbb{N})}$  is simple.

(v) As a corollary show that  $A_{(\mathbb{N})}$  contains a subgroup isomorphic to the infinite cyclic group  $\mathbb{Z}$ .

## 4.6 The Transfer

In this section we define a new homomorphism called the *transfer* first introduced by Issai Schur to prove the result quoted in Problem 4.29. It provides an example of the construction of an actual homomorphism, and we shall use it in **Web Section 6.5** to prove Burnside's Normal Complement Theorem (Theorem 6.23). We shall only consider the Abelian subgroup case; in the general non-Abelian case, the subgroup  $H$  in the definition below is replaced by  $H/H'$ ; see for example Rose (1978) or Rotman (1994). Either case provides a useful exercise in the methods discussed in this chapter.

We begin with

**Definition 4.24** For a group  $G$  and a subgroup  $H$  of finite index  $n$ , a set  $T$  containing exactly one representative from each left coset of  $H$  in  $G$  is called a *transversal* of  $H$  in  $G$ .

*Notes.* (a) If  $T = \{a_1, \dots, a_n\}$  and  $T$  is a transversal of  $H$  in  $G$ , then

$$G = \dot{\bigcup}_{i=1}^n a_i H,$$

where the dot denotes disjoint union. The transversal given by this definition is, strictly speaking, a *left* transversal. Right transversals can also be defined but we shall not need them, see Problem 4.24.

(b) By Lemma 2.22 an element  $a_i \in T$  cannot belong to two distinct cosets of  $H$ .

(c) In Chapter 9 we define a similar entity called the *section* which is a type of transversal with an extra condition concerning the neutral element.

Before defining the transfer we need to establish some basic facts about transversals. See also Problem 4.23.

**Lemma 4.25** Suppose  $H \leq G$ ,  $H$  is Abelian,  $[G : H] = n$ ,  $g \in G$ , and  $T = \{a_1, \dots, a_n\}$  is a transversal of  $H$  in  $G$ .

(i) There exists  $h_r \in H$  and  $\sigma \in S_n$  that depend on  $g$  and satisfy

$$ga_r = a_{r\sigma} h_r \quad \text{for } r = 1, \dots, n.$$

(ii) If  $\{b_1, \dots, b_n\}$  is another transversal of  $H$  in  $G$ , and so by (i)  $gb_r = b_{r\nu} k_r$  for some  $k_r \in H$  and  $\nu \in S_n$ , then

$$\prod_{r=1}^n h_r = \prod_{r=1}^n k_r.$$

*Proof.* (i) As  $ga_r$  belongs to some left coset of  $H$  in  $G$ , we can find  $h_r \in H$  and an integer  $s_r$  to satisfy

$$ga_r = a_{s_r} h_r \quad \text{where } 1 \leq s_r \leq n \quad \text{and } 1 \leq r \leq n.$$

To prove (i) we need to show that  $s_r$  defines a permutation in  $S_n$ . It is sufficient to show that  $s_r$  is injective because an injection of a finite set to itself is also surjective (Problem A5 in Appendix A).

Suppose  $ga_{r'} = a_{s_{r'}}h_{r'}$ , for  $h_{r'} \in H$ , and  $s_r = s_{r'}$ . Then we have

$$a_r^{-1}a_{r'} = (ga_r)^{-1}(ga_{r'}) = (a_{s_r}h_r)^{-1}(a_{s_{r'}}h_{r'}) = h_r^{-1}h_{r'} \in H,$$

by assumption. Hence by Lemma 2.22,  $a_rH = a_{r'}H$  which shows that  $r = r'$  because  $T$  is a transversal. Therefore the function  $s$  is injective, and so it is a bijection on  $\{1, \dots, n\}$ , that is a permutation belonging to  $S_n$ .

(ii) Set  $s = \sigma \in S_n$ . By (i) with  $g = e$ , there exist  $j_r \in H$  and  $\varphi \in S_n$  satisfying  $b_r = a_{r\varphi}j_r$ , for  $1 \leq r \leq n$ . So using (i) again, and the identity  $a_{r\varphi\sigma} = a_{r\varphi\sigma\varphi^{-1}}\varphi$ , we have

$$gb_r = g(a_{r\varphi}j_r) = (a_{r\varphi\sigma}h_{r\varphi})j_r = b_{r\varphi\sigma\varphi^{-1}}(j_{r\varphi\sigma\varphi^{-1}})^{-1}h_{r\varphi}j_r.$$

As  $\varphi\sigma\varphi^{-1} \in S_n$  and  $(j_{r\varphi\sigma\varphi^{-1}})^{-1}h_{r\varphi}j_r \in H$ , we can set  $\nu = \varphi\sigma\varphi^{-1}$  and

$$k_r = (j_{r\varphi\sigma\varphi^{-1}})^{-1}h_{r\varphi}j_r,$$

which gives  $gb_r = b_{r\nu}k_r$  as required. Hence, as  $H$  is Abelian, we obtain

$$\prod_r k_r = \prod_r (j_{r\varphi\sigma\varphi^{-1}})^{-1}h_{r\varphi}j_r = \prod_r j_r^{-1} \prod_r h_r \prod_r j_r = \prod_r h_r,$$

as  $\varphi, \sigma \in S_n$ , where the parameter  $r$  ranges from 1 to  $n$  in each product. The result follows.  $\square$

Now using Lemma 4.25(ii) we can define the transfer which we shall see is a homomorphism from  $G$  to  $H$ .

**Definition 4.26** Let  $H$  be an Abelian subgroup of  $G$  with index  $n$ . Using the notation set up in Lemma 4.25, the function  $\xi : G \rightarrow H$  given by

$$g\xi = \prod_{r=1}^n h_r \quad \text{for all } g \in G,$$

is called the *transfer* of  $H$  in  $G$ .

By Lemma 4.25(ii), this expression is independent of the coset representatives  $h_r$ , and so it is a well-defined function.

**Theorem 4.27** The transfer  $\xi : G \rightarrow H$  is a homomorphism.

*Proof.* Suppose  $g, h \in G$ ,  $ga_r = a_{r\sigma}j_r$  and  $ha_r = a_{r\nu}k_r$  where  $\{a_1, \dots, a_n\}$  is a transversal and  $\sigma, \nu \in S_n$ ; see above. Then

$$gha_r = ga_{r\nu}k_r = a_{r\nu\sigma}j_{r\nu}k_r,$$

and so, as  $H$  is Abelian,

$$gh\xi = \prod_r j_r \nu k_r = \prod_r j_r \cdot \prod_r k_r = g\xi \cdot h\xi,$$

which proves the theorem.  $\square$

*Example.* Let  $G = D_4 = \langle a, b \mid a^4 = b^2 = e, bab = a^3 \rangle$  and let  $H = \langle ab \rangle \leq G$ . The cosets of  $H$  in  $G$  are  $\{e, ab\}$ ,  $\{a, a^2b\}$ ,  $\{a^2, a^3b\}$  and  $\{a^3, b\}$ , and we can take  $T = \{e, a, a^2, a^3\}$  as a transversal. Putting  $g = b$  in Lemma 4.25 we obtain

$$\begin{aligned} b \cdot \underline{e} &= a^4b = \underline{a^3} \cdot (ab) \\ b \cdot \underline{a} &= a^3b = \underline{a^2} \cdot (ab) \\ b \cdot \underline{a^2} &= a^2b = \underline{a} \cdot (ab) \\ b \cdot \underline{a^3} &= ab = \underline{e} \cdot (ab), \end{aligned}$$

where on each side of these equations the elements of  $T$  are underlined. The permutation  $\sigma$ , see (i) of Lemma 4.25, in this case has the form  $\sigma = (1, 4)(2, 3)$  as  $e$  and  $a^3$ , and  $a$  and  $a^2$  are interchanged, and  $b\xi = (ab)^4 = e$ . A similar calculation shows that  $a\xi = e$ , and so the transfer in this example is the trivial homomorphism. We obtain the same result if we take a different transversal. For example let  $T' = \{ab, a, a^2, b\}$  be a second transversal, then repeating the above calculations we obtain

$$\begin{aligned} b \cdot \underline{ab} &= \underline{b} \cdot (ab) \\ b \cdot \underline{a} &= a^3b = \underline{a^2} \cdot (ab) \\ b \cdot \underline{a^2} &= a^2b = \underline{a} \cdot (ab) \\ b \cdot \underline{b} &= e = \underline{ab} \cdot (ab), \end{aligned}$$

and again we have  $b\xi = (ab)^4 = e$ .

The following corollaries are useful in the evaluation of the transfer.

**Corollary 4.28** *Using the notation set out above where  $T = \{a_1, \dots, a_n\}$  is a transversal of  $H$  in  $G$  and  $g \in G$ , we can write  $T$  as a disjoint union of subsets*

$$T = \{a_{1,1}, \dots, a_{1,m_1}\} \dot{\cup} \dots \dot{\cup} \{a_{t,1}, \dots, a_{t,m_t}\}$$

where

- (i)  $g\xi = \prod_{r=1}^t a_{r,1}^{-1} g^{m_r} a_{r,1}$ ,
- (ii)  $\sum_{r=1}^t m_r = [G : H]$ , and
- (iii)  $m_r$  is the smallest positive  $s$  such that  $a_{r,1}^{-1} g^s a_{r,1} \in H$ .

*Proof.* As above we have  $\sigma \in S_n$  and, for  $r = 1, \dots, n$ ,  $ga_r = a_{r\sigma} h_r$  where  $h_r \in H$ . Let  $(r_1, \dots, r_{m_1})$  be a cycle of length  $m_1$  in  $\sigma$ , see Definition 3.3, and let  $a_{r_1} = a_{1,1}, \dots, a_{r_{m_1}} = a_{1,m_1}$ , then

$$ga_{1,1} = a_{1,2} h_{r_1}, ga_{1,2} = a_{1,3} h_{r_2}, \dots, ga_{1,m_1} = a_{1,1} h_{r_{m_1}},$$

and combining these we obtain

$$a_{1,1}^{-1}g^{m_1}a_{1,1} = h_{r_{m_1}} \cdots h_{r_1} \in H.$$

Also if  $s < m$ ,

$$a_{1,1}^{-1}g^s a_{1,1} = a_{1,1}^{-1}a_{r_{s+1}} h_{r_s} \cdots h_{r_1} \notin H$$

because the set  $T$  is a transversal. This shows that  $m_1$  is minimal, and a similar argument can be applied to the remaining cycles  $(a_{2,1}, \dots, a_{2,m_2}), \dots$ . The main part of the result now follows using the definition of  $\xi$ .  $\square$

We return to the example on page 333. The permutation  $\sigma$  equals  $(1, 4)(2, 3)$ , and so in this case  $m_1 = m_2 = 2$ ,  $a_{1,1} = e$ ,  $a_{1,2} = a^3$ ,  $a_{2,1} = a$  and  $a_{2,2} = a^2$ . Now using the corollary above we have

$$b\xi = \prod_{r=1}^2 a_{r,1}^{-1}b^2a_{r,1} = (eb^2e)(a^3b^2a) = e$$

as in the example on page 333.

**Corollary 4.29** *Again using the notation set out above, if  $H \leq Z(G)$  then, for all  $g \in G$ ,  $g\xi = g^n$  where  $n = [G : H]$ .*

*Proof.* As  $H \leq Z(G)$ , we have  $H \triangleleft G$ , see Problem 2.14. So if  $g \in G$  and  $a^{-1}g^{m_r}a \in H$ , then  $g^{m_r} = a(a^{-1}g^{m_r}a)a^{-1} \in H$ . But  $H \leq Z(G)$ , and so  $a^{-1}g^{m_r}a = g^{m_r}$ . The result now follows by Corollary 4.28(i) and (ii).  $\square$

Returning again to the example on page 333, we have  $Z(G) = Z(D_4) = \langle a^2 \rangle$ , and a transversal is  $\{e, a, b, ab\}$ . The reader should now check that  $g\xi = e$  for all  $g \in G$ , and also  $g^4 = e$ , again for all  $g \in G$ , confirming the corollary in this case.

As noted above an important application of the transfer is in the proof of Burnside's Normal Complement Theorem given in Web Section 6.5. Another is the following

**Theorem 4.30** *For a group  $G$ , if  $p \mid o(G' \cap Z(G))$ , then a Sylow  $p$ -subgroup of  $G$  is not Abelian.*

A proof of this result is given in Problem 4.30. The result itself has connections with the so-called *Schur multiplier* of a group, see Web Section 12.6 and Issacs [2008], page 151.

Some more problems relating to the work of this section are given at the end of the next section.

## 4.7 Group Presentation, Part 2

The main purpose of this section is to show that the group presentation construction described on page 58 is valid. We claimed that given a set (alphabet)  $A$  and a set of relations  $R$  on  $A$  (words on  $A \cup A'$ ), then the system

$$H = \langle A \mid R \rangle$$

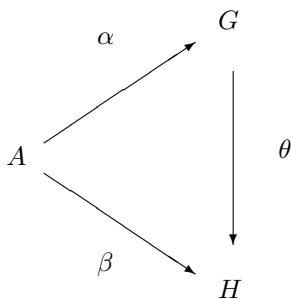
always forms a group. We do this by first constructing the ‘free’ group  $G$  on  $A$ , and then showing that  $H$  can be treated as a factor group of  $G$ , the implied normal subgroup being defined in terms of the words in  $R$ . Although we know that  $H$  forms a group, it can be quite difficult (and in some cases impossible) to determine its properties. In the second part of this section we describe a method mainly due to Todd and Coxeter which in many cases will help with this determination; it gives a description of the coset product once a suitable subgroup is known.

First we need to give a new definition of the term ‘free’.

**Definition 4.31** Given a set  $A$ , the group  $G$  is called *free on  $A$*  if the conditions (i) and (ii) given below are satisfied.

- (i) There exists a map  $\alpha$  from  $A$  to  $G$ .
- (ii) Given a group  $H$  and a map  $\beta$  from  $A$  to  $H$  there exists a unique homomorphism  $\theta : G \rightarrow H$  which satisfies  $\alpha\theta = \beta$ .

The diagram below illustrates the maps given by this definition. In many applications the set  $A$  is an alphabet (page 55),  $G$  is defined by a presentation on  $A$ , and the map  $\alpha$  is the inclusion map of  $A$  into  $G$ .



If  $G$  was not free, then there would exist at least one group  $H$  for which no homomorphism from  $G$  to  $H$  was possible because some relation would hold in  $G$  but not in  $H$ . So in this sense the ‘free’ group  $G$  is the most ‘general’ possible on the set (alphabet)  $A$ . This definition of ‘free’ is an extension of the notion of a ‘free Abelian group’. A *free Abelian group*  $G$  is defined as a direct product (Web page 371) of copies of the infinite cyclic group  $\mathbb{Z}$ ; that is if  $I = \{\dots, i, \dots\}$  is an index set, and  $a_i$  is a generator of the  $i$ th copy of  $\mathbb{Z}$ , then a free Abelian group  $G$  has the form

$$G = \prod_I \mathbb{Z} = \prod_{i \in I} \langle a_i \rangle,$$

with a typical element of the form

$$\dots a_i^{s_i} \dots$$

where  $s_i$  is some integer. In this case the group is Abelian, and so the order of the elements is immaterial. Let  $\alpha : I \rightarrow G$  be given by  $i\alpha = a_i$ , and let  $\beta$  be a map from  $I$  into some group  $H$ , then it is easy to see that there exists a unique homomorphism  $\theta$  from the free Abelian group  $G$  to  $H$  given by

$$(\dots a_i^{s_i} \dots)\theta = (\dots (i\beta)^{s_i} \dots).$$

The definition of the term ‘free’ given in the main text for a general group was an informal one, so secondly we give a formal version of our original definition. We shall then show that the two definitions agree.

**Definition 4.32** Let  $G$  be a group.

(i) A subset  $C$  of  $G \setminus \{e\}$  *freely generates*  $G$  if, and only if, each  $g \in G \setminus \{e\}$  can be uniquely expressed in the form

$$g = c_1^{r_1} \dots c_j^{r_j}, \quad (4.5)$$

where  $c_i \in C$ ,  $c_{i+1} \neq c_i$  for all  $i$ , and  $r_i$  is a nonzero integer.

(ii)  $G$  is called *free* if, and only if, it is freely generated by some subset  $C$  of  $G \setminus \{e\}$ .

*Notes.* (a) The elements  $c_i$  are not necessarily distinct, only adjacent ones are. For example  $c_1 c_2 c_1 c_2 c_1 \in G$ . (b) The most important word in the definition is ‘uniquely’: if  $c_1^{r_1} \dots c_j^{r_j} = d_1^{s_1} \dots d_k^{s_k}$  where  $c_i, d_i \in C$ , and  $r_i$  and  $s_i$  are nonzero integers, then  $j = k$ ,  $c_i = d_i$  and  $r_i = s_i$  for  $i = 1, \dots, j$  — there are no relations amongst the elements of  $G$  apart from those that make  $G$  into a group.

We show now that our two definitions of *free* agree.

**Theorem 4.33** *If  $G$  is freely generated by  $C$  (Definition 4.32),  $H$  is a group, and  $\alpha$  is a map from  $C$  into  $H$ , then there exists a unique homomorphism  $\theta : G \rightarrow H$  with the property  $\theta|_C = \alpha$ .*

*Proof.* We establish uniqueness first. Suppose  $\theta$  exists and  $g$  is given by (4.5), then

$$\begin{aligned} e_G \theta &= e_H \quad \text{and} \\ g\theta &= (c_1 \theta)^{r_1} \dots (c_j \theta)^{r_j} \\ &= (c_i \alpha)^{r_1} \dots (c_j \alpha)^{r_j} \end{aligned} \quad (4.6)$$

This shows that  $\theta$  is unique. Also  $c_i \theta = c_i \alpha$ , and so  $\theta|_C = \alpha$ . For the main homomorphism equation we proceed as follows. First we have, if  $g \neq e$ ,



$$\begin{aligned}
(eg)\theta &= g\theta = e\theta g\theta, \\
(ge)\theta &= g\theta e\theta \quad \text{and} \\
(ee)\theta &= e\theta = e\theta e\theta.
\end{aligned}$$

Secondly, suppose  $h = b^s$  where  $b \in C$  and  $s$  is a non-zero integer. There are three cases to consider.

*Case 1.*  $b \neq c_j$ . We have

$$\begin{aligned}
gh &= c_1^{r_1} \dots c_j^{r_j} b^s \quad \text{and} \\
(gh)\theta &= (c_1\alpha)^{r_1} \dots (c_j\alpha)^{r_j} (b\alpha)^s = g\theta h\theta.
\end{aligned}$$

*Case 2.*  $b = c_j$  and  $r_j + s \neq 0$ . We have

$$\begin{aligned}
gh &= c_1^{r_1} \dots c_j^{r_j+s} \quad \text{and} \\
(gh)\theta &= (c_1\alpha)^{r_1} \dots (c_j\alpha)^{r_j+s} = g\theta h\theta.
\end{aligned}$$

*Case 3.*  $b = c_j$  and  $r_j + s = 0$ . We have

$$\begin{aligned}
gh &= c_1^{r_1} \dots c_{j-1}^{r_{j-1}} \quad \text{and} \\
(gh)\theta &= (c_1\alpha)^{r_1} \dots (c_{j-1}\alpha)^{r_{j-1}} (c_j\alpha)^{r_j+s} \\
&= (c_1\alpha)^{r_1} \dots (c_j\alpha)^{r_j} (b\alpha)^s = g\theta h\theta.
\end{aligned}$$

Hence we have  $gh\theta = g\theta h\theta$  for all  $g$  and  $h$  of the form  $b^s$ . Lastly we proceed by induction (on  $k$ ). Suppose  $h = h_1 h_2$  where  $h_1 = b_1^{s_1} \dots b_{k-1}^{s_{k-1}}$  and  $h_2 = b_k^{s_k}$ . Then using the inductive hypothesis we have

$$\begin{aligned}
(gh)\theta &= (gh_1 h_2)\theta = (gh_1)\theta h_2\theta = g\theta h_1\theta h_2\theta \\
&= g\theta(h_1 h_2)\theta = g\theta h\theta.
\end{aligned}$$

This completes the proof of Theorem 4.33.  $\square$

For the converse of the theorem see Problem 4.32.

Next we consider the formation a free group on a set, first we need to establish the uniqueness property of reduced words. On page 57 we described the process of forming the reduced word  $w^{[*]}$  of a word  $w$ . This process always gives a unique result as the next theorem shows.

**Theorem 4.34** *For each word  $w$  on an alphabet  $A$  the reduction process described on page 57 gives a unique reduced word  $w^{[*]}$ .*

*Proof.* First note that every word  $w$  does reduce to a reduced word. Reduction proceeds by deleting pairs of letters from  $w$  step by step to form a reduced word and, as  $w$  only has a finite number of letters, this procedure must stop after a finite number of steps.

We prove the result by induction on  $n$ , the length (number of symbols) of  $w$ , that is on the number of letters from  $A \cup A'$  that make up  $w$ . If  $n = 0$  there is nothing to prove as  $w$  is then the empty word which is

clearly reduced. Note that words of length 1 are also reduced. Suppose the result holds for all words of length less than or equal to  $n$  where  $n > 1$ . Let  $w$  is a word of length  $n + 1$ , and suppose we have two reductions (deletions) labelled (a) and (b). In (a), suppose the deletion removes the consecutive pair of letters  $a_i a_{i+1}$ , and in (b), suppose the deletion removes the consecutive pair  $a_j a_{j+1}$ . There are a number of cases to consider.

*Case 1.*  $j = i$  In this case the two reductions each give the same word  $w'$ , say, of length  $n - 1$ . By the inductive hypothesis,  $w'$  reduces to a unique reduced word, and so this is also true for  $w$ .

We may now assume that  $j > i$ .

*Case 2.*  $j = i + 1$  In this case we may suppose the  $i$ th,  $(i + 1)$ st and  $(i + 2)$ nd letters take the form

$$aa'a \quad \text{or} \quad a'aa',$$

for some letter  $a \in A$ . This follows because we have consecutive deletions in this case. Consider  $aa'a$ . Deletion (a) will reduce this term to  $a$  (by the removal of  $aa'$  as  $a_i = a$ ,  $a_{i+1} = a'$  and  $a_{i+2} = a$  in this case), and deletion (b) will again reduce this term to  $a$  (this time by the removal of  $a'a$  where  $a_j = a'$  and  $a_{j+1} = a$ ). In each case the deletions give the same result, a word of length  $n - 1$  with  $a$  in the  $i$ th place, and as in Case 1 we can apply the inductive hypothesis. An exactly similar argument applies to subword  $a'aa'$  which reduces to  $a'$ . Hence the induction step is complete in this case.

*Case 3.*  $j > i + 1$ . In this case we suppose  $a_i a_{i+1}$  is removed by Deletion (a), and  $a_j a_{j+1}$  is removed by Deletion (b); note there is no overlap. Let  $w'$  denote the result of Deletion (a) on  $w$ , and let  $w''$  the result of Deletion (b) on  $w$ . Further, we can remove  $a_j a_{j+1}$  from  $w'$  to form a new word  $x$  (of length  $n - 3$ ). We can also remove  $a_i a_{i+1}$  from  $w''$ , and then we obtain the *same* word  $x$  (as  $j > i + 1$ ). By the inductive hypothesis  $w'$ ,  $w''$  and  $x$  all reduce to the same reduced word. This follows because  $x$  has a unique reduction  $x^{[*]}$  (by the inductive hypothesis),  $w'$  and  $w''$  both reduce to  $x$ , and so both  $(w')^{[*]}$  and  $(w'')^{[*]}$  equal  $x^{[*]}$ . But Deletion (a) (of  $w$ ) gives  $w'$ , and Deletion (b) (also of  $w$ ) gives  $w''$ . Hence the induction step is complete in this final case and the theorem follows.  $\square$

We can now prove our main existence theorem.

**Theorem 4.35** *For all sets of letters  $A$  there exists a free group on  $A$ .*

*Proof.* An element of the group that we are about to construct is a reduced word on the set  $A$ . Suppose  $w_1$  and  $w_2$  are reduced words on  $A$ . (Note that by definition we have a second disjoint set  $A'$  having the same cardinality as  $A$ , and a bijective map  $'$  between  $A$  and  $A'$ . Also the symbols that make up  $w_1$  and  $w_2$  belong to  $A \cup A'$ .) Using Definition 3.17 we can form the reduced product

$$(w_1 w_2)^*$$

of  $w_1$  and  $w_2$ ; that is we can form the concatenation  $w_1w_2$  and then we apply the reduction process to form  $(w_1w_2)^*$ . By Theorem 4.34 this gives a well-defined product on  $A \cup A'$ . This product is associative, for if  $w_1, w_2$  and  $w_3$  are words on  $A$ , then both  $((w_1w_2)^*w_3)^*$  and  $(w_1^*(w_2w_3)^*)^*$  are equal to the unique reduction of  $w_1w_2w_3$  given by Theorem 4.34. The neutral element is the empty word which we denote by  $e$  (Note that  $e$  does not belong to  $A \cup A'$ ; see page 57). The inverse of the reduced word

$$c_1c_2 \dots c_n \quad \text{is the word} \quad c_n c_{n-1} \dots c_1,$$

where each  $c_i \in A \cup A'$ . As the first of these words is reduced, it follows immediately that the second word is also reduced. (Note that the reduction process is symmetrical as there is a bijection  $'$  between  $A$  and  $A'$ .) Hence we see that the set of reduced words on  $A$  forms a group which we denote by  $\langle G \rangle$ . We need to show that it is free.

Let  $\alpha$  be the inclusion map from  $A$  into  $G$ , clearly  $a\alpha = a$  for all  $a \in A$ . This gives the first part of Definition 4.31. For the second part suppose  $H$  is a group and  $\beta : A \rightarrow H$ . First we extend the domain of  $\beta$  to  $A \cup A'$  by defining

$$a'\beta = (a\beta)^{-1} \quad \text{for } a \in A. \quad (4.7)$$

This is valid because we are using the inverse operation in the group  $H$ . Further, if  $w = a_1a_2 \dots a_n$  where each  $a_i \in A \cup A'$ , we define the map  $\psi$  from the set of words on  $A$  into  $H$  by

$$w\psi = a_1\beta \cdot \dots \cdot a_n\beta.$$

Note that by (4.7) if we reduce the word  $w$  by deleting  $a_i a'_i$  or  $a'_i a_i$  the value of  $\psi$  is unaltered. Let  $\theta$  be  $\psi$  with its domain restricted to  $G$ , and so  $\theta : G \rightarrow H$ . We claim that  $\theta$  is a homomorphism. If  $w_1$  and  $w_2$  are reduced words on  $A$  (that is elements of  $G$ ), then

$$\begin{aligned} w_1\theta w_2\theta &= w_1w_2\theta && \text{by definition} \\ &= ((w_1w_2)^*)\theta && \text{by note above,} \end{aligned}$$

so  $\theta$  is the homomorphism required by Definition 4.31. Also clearly we have  $\alpha\theta = \beta$  by definition. This completes the proof.  $\square$

An immediate consequence of this result is the following characterisation of all groups.

**Theorem 4.36** *Every group is a homomorphic image of a free group.*

*Proof.* Let  $H$  be a group and let  $B$  be a generating set for  $H$  (page 25). Further, let  $\alpha$  be the inclusion map from  $B$  into  $H$ . By Theorem 4.35 there exists a free group  $G$  on the set  $B$ . Applying Condition (ii) in Definition 4.31 there exists a homomorphism  $\theta$  from  $G$  to  $H$  with the property

$$(a\alpha)\theta = a \quad \text{for } a \in B.$$

But  $\langle B \rangle = H$  by definition of  $B$ , and so  $\theta$  is surjective. Hence

$$H = \{g\theta : g \in G\} = G\theta$$

which gives the result.  $\square$

A famous theorem due Nielsen and Schreier states that every subgroup of a free group is also free; see the references quoted at the end of this subsection. Our next corollary shows how normal subgroups come into the picture. Remember that a *relation* of an alphabet  $A$  is an equation of the form  $x = e$  where  $x$  is a word on  $A \cup A'$  (page 58).

**Corollary 4.37** *Using the notation set out above where  $G$  is the free group on  $A$ ,  $\theta$  is a homomorphism from  $G$  to  $H$ , and  $\alpha$  is the inclusion map from  $A$  to  $G$ , then  $x = e$  is a relation in  $H$  if, and only if,  $x\alpha$  belongs to the kernel of the homomorphism  $\theta$ .*

*Proof.* Let

$$x = c_1 \dots c_r \quad \text{where} \quad c_i \in A \cap A' \quad \text{for} \quad i = 1, \dots, r.$$

The map  $\alpha$  has domain  $A$ , we can extend its domain to  $A \cup A'$  by defining

$$(a')\alpha = (a\alpha)^{-1} \quad \text{for} \quad a \in A.$$

This is valid as we are working in the group  $G$ . We have  $(a\alpha)\theta = a$  and using this definition we also have  $(a'\alpha)\theta = a^{-1}$ . As  $\theta$  is a homomorphism this further gives

$$(x\alpha)\theta = (c_1\alpha)\theta \dots (c_r\alpha)\theta = c_1 \dots c_r = x = e,$$

and so  $x \in \ker \theta$ .

Conversely, suppose  $y \in \ker \theta$  and  $y = d_1 \alpha \dots d_s \alpha$ . As we are working inside  $G$  we may assume that  $d_1 \dots d_s$  is a reduced word on the alphabet  $A$ . Now  $y\theta = e$  by supposition, and

$$y\theta = d_1 \dots d_s = e.$$

By Theorem 4.34 the  $d_i$  are unique, hence  $d_1 \dots d_s = e$  is a valid relation in  $H$ .  $\square$

We can now prove our main result: Theorem 3.19. We begin by restating this result. We have alphabets  $A = \{a_1, \dots, a_n\}$  and  $A' = \{a'_1, \dots, a'_n\}$ , a bijection  $'$  mapping  $A$  onto  $A'$ , and a collection of words  $R = \{x_1, \dots, x_m\}$  where each  $x_i$  is a concatenation of letters from  $A \cup A'$ . The system  $\langle A \mid R \rangle$  is a subset of the free group on  $A$  with the added relations

$$x_1 = \dots = x_m = e.$$

Theorem 3.19 claims that this system forms a group, we prove this by showing that it can be defined as the factor group  $G/K$  where  $G$  is the free group on  $A$ , and  $K$  is the smallest normal subgroup given by Corollary 4.37 using the relations in  $R$ . We let  $\alpha$  be the inclusion map of  $A$  into  $G$  which as before we extend to  $A'$  by letting  $a'\alpha = (a\alpha)^{-1}$  and, if  $x = c_1 \dots c_r$  is a word on  $A \cup A'$ , then we let

$$x\alpha = c_1\alpha \dots c_r\alpha.$$

Further, let  $\beta : A \rightarrow G/K$  be given by

$$a\beta = (a\alpha)K \quad \text{for } a \in A.$$

As above we extend the domain of the function  $\beta$  to  $A \cup A'$  by defining  $a'\beta = (a\beta)^{-1}$  for  $a' \in A'$ , and if  $x = c_1 \dots c_r$  where  $c_i \in A \cup A', i = 1, \dots, r$ , we let  $x\beta = c_1\beta \dots c_r\beta$ . Lastly we define

$$\begin{aligned} A\beta &= \{a\beta : a \in A\}, \\ (A\beta)^{-1} &= \{a'\beta : a' \in A'\}, \quad \text{and} \\ R\beta &= \{x_i\beta : i = 1, \dots, m\}. \end{aligned}$$

**Theorem 4.38 (3.19)** *Using the notation set out above, the set  $R\beta$  is a collection of relations on the generating set  $A\beta$ , and*

$$G/K = \langle A\beta \mid R\beta \rangle.$$

*Proof.* In this proof  $\alpha, \beta$  and  $\gamma$  are maps from sets of letters to groups, and  $\theta$  and  $\phi$  are homomorphisms. As  $G = \langle A\alpha \rangle$  by definition, we see that  $G/K = \langle A\beta \rangle$ . Also if  $x_i \in R$ , then  $(x_i\alpha)K = K$ , and so  $x_i\beta = e$  in  $G/K$ ; that is  $x_i\beta = e$  is a relation of  $G/K$  for all  $i$ . This shows that

$$G/K \supseteq \langle A\beta \mid R\beta \rangle.$$

Let  $J$  be a group and let  $\gamma$  be a map from  $A\beta$  to  $J$  which preserves the relations in  $R\beta$ . We now apply the definition of a free group to the map  $\beta\gamma$  from  $A$  to  $J$ . Hence there exists a unique homomorphism  $\theta : G \rightarrow J$  with the property

$$(a\alpha)\theta = (a\beta)\gamma \quad \text{for } a \in A.$$

The map  $\theta$  is a homomorphism, hence  $((a\alpha)^{-1})\theta = ((a\alpha)\theta)^{-1}$ . Also we can extend the domain of  $\gamma$  to  $A \cup A'$  by defining

$$(a'\beta)\gamma = ((a\beta)\gamma)^{-1},$$

which gives

$$(a'\alpha)\theta = ((a\beta)\gamma)^{-1} = (a'\beta)\gamma \quad \text{and} \quad (x_i\alpha)\theta = (x_i\beta)\gamma$$

for all  $i$ . But by definition  $\gamma$  preserves the relations in  $R\beta$ , and so

$$(x_i\beta)\gamma = e \quad \text{which shows that } x_i\beta \in \ker \theta,$$

and as  $K$  is minimal this further shows that

$$K \leq \ker \theta.$$

Therefore  $\theta$  induces a homomorphism  $\phi$  from  $H(= G/K)$  to  $J$  which satisfies

$$(a\beta)\phi = (a\alpha)\theta = (a\beta)\gamma.$$

Now using Problem 4.13(iv) [see Addendum]  $\phi$  can be extended to a homomorphism from  $H$  to  $J$ . This shows that  $G = \langle A\beta \mid R\beta \rangle$ . We using the same idea here at that given in Definition 4.31, see the note below the diagram on page 335.  $\square$

**Corollary 4.39** *If  $A$  is a set of generators for a group  $G$ , then there exists a set  $R$  of relations defined on the elements of  $A \cup A'$  with the property  $G = \langle A \mid R \rangle$ .*

*Proof.* The First Isomorphism Theorem applied to the homomorphism  $\theta$  defined in the above proof gives an isomorphism from  $G/\ker \theta$  onto  $H$  which maps  $(a\alpha)\ker \theta$  to  $a$ . Now suppose  $R = \{x_i\alpha : i = 1, \dots, s\}$  is a set of generators for  $\ker \theta$ , then  $\ker \theta$  is identical to the smallest normal subgroup  $K$  containing all elements of the form  $x_i\alpha$  for  $i = 1, \dots, s$ , and so by Theorem 4.38 we have  $G = \langle A \mid R \rangle$  because  $a\theta$  is mapped to  $a$  and  $x_i\theta$  is mapped to  $x_i$  by this isomorphism.  $\square$

We have now completed our stated aim which was to prove Theorem 3.18, that is to justify the use of presentations in the theory. Further developments have been considered many of which relate infinite groups. One of these involves the extension of free group theory to so-called *free products* and *free products with amalgamated subgroups*; for details the reader should consult Scott [1964], Suzuki [1982], or Robinson [1982] amongst other texts. Another development concerns the *Word Problem for Groups*, an important result proved independently by P. S. Novikov, W. W. Boone, and J. L. Britten which extends a similar result for semigroups proved by A. A. Markov and E. L. Post, and which makes extensive use of ideas from mathematical logic. A group with a presentation  $G = \langle A \mid R \rangle$  is said to have a *solvable word problem* if there exists a computer algorithm which will determine in a finite time whether the equation  $x = e$  holds in  $G$  where  $x$  is an arbitrary word on the alphabet  $A$ . Novikov, Boone and Britten showed that there exists a finitely presented group (that is one with a finite alphabet and a finite number of relations) for which the word problem is unsolvable — there is at least one word in this group for which we cannot determine whether, or not, it equals the neutral element. A good account of this topic is given in Rotman [1994].

## ***Coset Enumeration***

As we have noted before, given a presentation of a group it can be difficult, and in some cases impossible, to determine the group's properties including its order or even if it is finite. Todd and Coxeter developed a method which will give some of these properties provided we know in advance that the group is finite. It is 'mechanical' and so is easily computerised; the computer program GAP makes extensive use of this procedure in several contexts. We shall describe the basic method by giving a series of examples.

Suppose we have a group with a presentation  $G$  and a subgroup  $H$ , the method of Todd and Coxeter will determine the coset product. We label the cosets with the numerals  $1, 2, \dots$ , where the subgroup  $H$  has the label 1. If  $a$  is a generator of the group  $G$  then, given a numeral (coset)  $m$ , the method will solve the equation  $ma = n$ , that is it will determine the coset  $ma$ ; remember throughout that the numerals  $m$  and  $n$  are labels for cosets. We do this by constructing a table of coset multiplications; once this is complete we can describe the basic structure of the group in question.

**Example 1. Dihedral Group  $D_3$  with a Subgroup of Order 2**

For our first example we consider the group

$$D_3 = \langle a, b \mid a^2 = b^3 = (ab)^2 = e \rangle,$$

and take  $H = \langle a \rangle$ . (We often take  $H$  cyclic but this is not essential.) The first row of the table lists the letters which make up the relations with asterisks between the relation words, and so has the form:

$$* a \ a \ * \ b \ b \ b \ * \ a \ b \ a \ b \ *$$

We begin the second row by placing '1' below each asterisk (this corresponds to the fact that each relation word equals the neutral element) and *between* each pair of relation letters  $a$  (as  $Ha = H$  (or  $1a = 1$ ) for all  $a \in H (= 1)$ )

$$\begin{array}{cccccccccccc} * & a & & a & * & b & & b & & b & * & a & & b & & a & & b & * \\ 1 & & 1 & & 1 & & & & 1 & & & & & & & & & & 1 \end{array}$$

This reads as  $1a = 1$  *et cetera*; in general if  $m$  and  $n$  are consecutive numerals in a row and  $c$  is the group letter at the head of the columns containing  $m$  and  $n$ , then  $mc = n$  is the coset product. At each stage we use the information to hand to try to complete the row, if we cannot do this we introduce a new coset (numeral). In our example we can put '1' in the seventh place copying the first two entries (that is,  $1a = 1$ ). As we have no information on  $b$  yet we place '2' and '3' in the fourth and fifth columns, respectively, as shown below (so  $1b = 2$  and  $2b = 3$ ). This gives our first 'new fact':  $3b = 1$  (note  $b$  is an element of order 3) and enables us to complete the row. We can place '2' in the eighth column and '3' in the ninth (as  $1b = 2$ , and  $3b = 1$ ). This provides a new fact:  $2a = 3$  which we will use later.

$$\begin{array}{cccccccccccc} * & a & & a & * & b & & b & & b & * & a & & b & & a & & b & * \\ 1 & & 1 & & 1 & & 2 & & 3 & & 1 & & 1 & & 2 & & 3 & & 1 \end{array}$$

We have introduced two new cosets (numerals) 2 and 3, and so we need at least two new rows in the table. In some cases a few of these rows will not be necessary because we can find one or more identities between the cosets under consideration and those already introduced, but this is not so here. We begin by placing '2' below each asterisk in Row 3 and '3' below each asterisk in Row 4, and then we try to complete these rows using the information tabulated so far. So we can place '3' in the second entry of the third row using the fact noted above ( $2a = 3$ ). This gives a new fact:  $3a = 2$  (note that

$a$  is an element of order 2). We now have sufficient information to complete the table as shown below.

*	$a$	$a$	*	$b$	$b$	$b$	*	$a$	$b$	$a$	$b$	*
1	1	1	2	3	1	1	2	3	1	3	1	
2	3	2	3	1	2	3	1	1	2	3	2	
3	2	3	1	2	3	2	3	2	3	2	3	

By definition the table is finished because we have the same number of completed rows as numerals (cosets). It gives the following description of the coset product:

$$1a = 1, 2a = 3, 3a = 2, 1b = 2, 2b = 3, 3b = 1. \quad (4.8)$$

This incidentally reproves the fact that  $o(D_3) = 6$ , that is the order of  $H$  ( $o(\langle a \rangle)$ ) times the number of coset rows in the table (which also equals the number of numerals used). The reader should check that the data given in (4.8) is exactly mirrored in the table above.

**Example 2. Symmetric Group  $S_4$  with a Subgroup of Order 4**

For our second example we consider the symmetric group  $S_4$ , using the presentation

$$S_4 = \langle a, b \mid a^4 = b^3 = (ab)^2 = e \rangle,$$

and the subgroup  $H = \langle a \rangle$ . We introduce two extra symbols. Each time a new numeral (coset) is defined (reading the tables from left to right, and then by columns) we place a bar over it, and each time a new fact is discovered (of the form  $mc = n$ ) we place the symbol  $\asymp$  between  $m$  and  $n$ . So, following the same procedure as above, the first two rows of our coset enumeration table for  $S_4$  and  $H$  are as follows:

*	$a$	$a$	$a$	$a$	*	$b$	$b$	$b$	*	$a$	$b$	$a$	$b$	*
$\bar{1}$	1	1	1	1	1	$\bar{2}$	$\bar{3}$	$\asymp$	1	1	2	$\asymp$	3	1

We have  $3b = 1$  (as  $b^3 = e$ ) and  $2a = 3$  (as  $1b = 2$ ), but we do not have a value for  $3a$  which we set as 4, or for  $4a$  which we set as 5. On the other hand we do have  $5a = 2$  applying the relation  $a^4 = e$ . Using this information we can write down the next two rows of the coset table as follows:

*	$a$	$a$	$a$	$a$	*	$b$	$b$	$b$	*	$a$	$b$	$a$	$b$	*
$\bar{1}$	1	1	1	1	1	$\bar{2}$	$\bar{3}$	$\asymp$	1	1	2	$\asymp$	3	1
2	3	$\bar{4}$	$\bar{5}$	$\asymp$	2	3	1	2	2	3	1	1	2	
3	4	5	2		3	1	2	3	4	$\asymp$	5	2	3	

At this stage the table is not complete because we have more numerals (cosets) than numeral rows. So we need to start again placing '4' below each asterisk in Row 5 and '5' below each asterisk in Row 6. During this process we will need to introduce the sixth coset (numeral) '6' by defining  $5b = 6$ . Constructing this row (Row 5) shows that  $6a = 6$  and  $6b = 4$ . Hence we can complete the table now.



*	$a$	$a$	$a$	$a$	*	$b$	$b$	$b$	*	$a$	$b$	$a$	$b$	*
$\bar{1}$	1	1	1	1	1	$\bar{2}$	$\bar{3}$	$\asymp$	1	1	2	$\asymp$	3	1
2	3	$\bar{4}$	$\bar{5}$	$\asymp$	2	3	1	2	3	1	1	2		
3	4	5	2	3	1	2	3	4	$\asymp$	5	2	3		
4	5	2	3	4	5	$\bar{6}$	4	5	6	$\asymp$	6	$\asymp$	4	
5	2	3	4	5	6	4	5	2	3	4	5			
6	6	6	6	6	4	5	6	6	4	5	6			

The table is now finished, we have six cosets  $1, 2, \dots, 6$  and six rows; and so the coset product is given by

$$\begin{aligned} 1a &= 1, \quad 2a = 3, \quad 3a = 4, \quad 4a = 5, \quad 5a = 2, \quad 6a = 6, \\ 1b &= 2, \quad 2b = 3, \quad 3b = 1, \quad 4b = 5, \quad 5b = 6, \quad 6b = 4. \end{aligned}$$

This can be used to give a permutation representation for  $S_4$  with  $a \rightarrow (2, 3, 4, 5)$  and  $b \rightarrow (1, 2, 3)(4, 5, 6)$ . Note also that each column in this table is a permutation of the set  $\{1, 2, \dots, 6\}$ , similar properties hold for all coset enumeration tables (use Lemma 2.22) and this can be used as a check on the calculations.

**Example 3. Special Linear Group  $SL_2(3)$  with a Cyclic Subgroup of Order 3**

Our remaining two examples will again use groups from Chapter 8, and they will illustrate some further simple adaptations of the method. Let  $SL_2(3)$  be presented by

$$SL_2(3) = \langle a, b \mid a^3 = abab^{-1}a^{-1}b^{-1} = e \rangle,$$

with subgroup  $H = \langle a \rangle$ ; see page 176. We fill in the first three lines of the coset enumeration table using similar arguments to those applied in the example above by letting  $1b = 2$ ,  $3b^{-1} = 2$ ,  $2a = 4$ ,  $4a = 5$  and  $5b^{-1} = 6$ . Using inverses these also show that  $2b^{-1} = 1$ ,  $2b = 3$ ,  $5a^{-1} = 4$  and  $6a^{-1} = 3$  (as  $5b^{-1} = 6$  and  $3b^{-1} = 2$ ). Secondly we can deduce the identities:  $4b^{-1} = 4$  (and so  $4b = 4$ ) and  $5a = 2$  (as  $a^3 = e$ ). Hence the first three rows of the table are:

*	$a$	$a$	$a$	*	$a$	$b$	$a$	$b^{-1}$	$a^{-1}$	$b^{-1}$	*
$\bar{1}$	1	1		1	1	$\bar{2}$	$\bar{4}$	$\asymp$	4	2	1
2	4	$\bar{5}$	$\asymp$	2	4	$\asymp$	4	5	$\bar{6}$	$\asymp$	$\bar{3}$

We can now proceed much as before. We let  $6a = 7$  and  $5b = 8$ , this gives  $7a = 3$  and  $8a = 8$ . Hence the next three lines of the table are:

3	6	$\bar{7}$	$\asymp$	3	6	5	2	1	1	3
4	5	2	4	5	$\bar{8}$	$\asymp$	8	5	4	4
5	2	4	5	2	3	6	8	8	8	5

We have used eight cosets (numerals) and so we need at least three further rows in the table. This is sufficient because we do not need to introduce any more cosets; hence the complete table is as follows:

*	$a$	$a$	$a$	*	$a$	$b$	$a$	$b^{-1}$	$a^{-1}$	$b^{-1}$	*
$\bar{1}$	1	1		1	1	$\bar{2}$	$\bar{4}$	$\asymp$	4	2	1
2	4	$\bar{5}$	$\asymp$	2	4	$\asymp$	4	5	$\bar{6}$	$\asymp$	$\bar{3}$
3	6	$\bar{7}$	$\asymp$	3	6	5	2	1	1	1	3
4	5	2		4	5	$\bar{8}$	$\asymp$	8	5	4	4
5	2	4		5	2	3	6	8	8	5	5
6	7	3		6	7	$\asymp$	7	3	2	5	6
7	3	6		7	3	1	1	3	7	7	7
8	8	8		8	8	6	7	7	6	8	8

The information in this table can be summarised as follows:

$$\begin{aligned} 1a &= 1, 2a = 4, 3a = 6, 4a = 5, 5a = 2, 6a = 7, 7a = 3, 8a = 8, \\ 1b &= 2, 2b = 3, 3b = 1, 4b = 4, 5b = 8, 6b = 5, 7b = 7, 8b = 6. \end{aligned}$$

This reproves the fact that  $o(SL_2(3)) = o(A) \cdot 8 = 24$ .

**Example 4. Group  $E$  with its Subgroup of Order 3**

For our last example we consider the group  $E$  with its presentation (page 182)

$$E = \langle a, b \mid a^4 = d^6 = (ad)^2 = (a^3d)^2 = e \rangle,$$

and its unique subgroup of order 3 given by  $H = \langle d^2 \rangle$ . Here  $H$  is not generated by one of the group generators  $a$  or  $d$ , so we proceed as follows. We define

$$1a = 2, 2a = 3, 3a = 4, \text{ and } 1d = 5.$$

As we are considering cosets of  $H$  we have  $5d = 1$  ( $d^2, d^4$  and  $d^6 = e$  all lie in  $H$ ). Also as  $a^4 = e$ , we have  $4a = 1$ . This gives the first half of Row 2 in the table on the next page. To complete this row we define

$$2d = 6, \text{ and } 4d = 7.$$

As  $5d = 1$  these equations give

$$6a = 5, \text{ and } 7a^{-1} = 5 \text{ or } 5a = 7,$$

see the completed row in the table below. The information in this row also gives  $2a^{-1} = 1$  and  $5a^{-1} = 6$ . Applying this to the latter part of Row 3 we obtain  $6d = 2$  as this row ends in '2' (that is  $(ad)^2 = e$ ). If we set  $3d = 8$  we obtain  $8a = 6$  (check between the third and fourth asterisks in Row 3). This completes the third row and we can construct the fourth row using similar methods which gives the facts:  $7a = 8$  and  $8d = 3$ . No new cosets are needed for we can complete the remaining rows using the information to hand.

$*$	$a$	$a$	$a$	$a$	$*$	$d$	$d$	$d$	$d$	$d$	$d$	$d$	$*$	$a$	$d$	$a$	$d$	$a^{-1}$	$d$	$a^{-1}$	$d$	$*$
$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\asymp$	1	$\bar{5}$	1	5	1	5	1	2	$\bar{6}$	$\asymp$	5	1	4	$\bar{7}$	$\asymp$	5	1	
2	3	4	1	2	6	2	6	2	6	2	3	$\bar{8}$	$\asymp$	6	2	1	5	6	$\asymp$	2		
3	4	1	2	3	8	3	8	3	8	3	4	7	$\asymp$	8	3	2	6	8	$\asymp$	3		
4	1	2	3	4	7	4	7	4	7	4	1	5	7	4	3	8	7	4				
5	7	8	6	5	1	5	1	5	1	5	7	4	1	5	6	2	1	5				
6	5	7	8	6	2	6	2	6	2	6	5	1	2	6	8	3	2	6				
7	8	6	5	7	4	7	4	7	4	7	8	3	4	7	5	1	4	7				
8	6	5	7	8	3	8	3	8	3	8	6	2	3	8	7	4	3	8				

$$1a = 2, 2a = 3, 3a = 4, 4a = 1, 5a = 7, 6a = 5, 7a = 8, 8a = 6,$$

$$1d = 5, 2d = 6, 3d = 8, 4d = 7, 5d = 1, 6d = 2, 7d = 4, 8d = 3.$$

## 4.8 Problems 4W

(iv) If  $K \triangleleft G$  and  $T$  is a transversal of  $K$  in  $G$ , show that the set  $T^{-1} = \{t^{-1} : t \in T\}$  is also a transversal of  $K$  in  $G$ .

**Problem 4.24** For this problem we use the term *left transversal* for the transversal given in Definition 4.24. First you are asked to define a *right transversal*.

Now suppose  $H \leq G$ .

(i) Show that if  $H \triangleleft G$ , then every left transversal is a right transversal, and vice versa.

(ii) Prove that if every left transversal of  $H$  in  $G$  is also a right transversal, then  $H \triangleleft G$ .

(iii) Give an example using one of the groups discussed in Chapter 8.

**Problem 4.25** Suppose  $K \triangleleft J \leq G$ ,  $[G : J] = n < \infty$ ,  $o(J/K) = m < \infty$  and  $J/K$  is Abelian. Prove that if  $(m, n) = 1$ , then

$$J \cap G' \cap Z(G) \leq K.$$

**Problem 4.26** Suppose  $G$  is a finite group.

(i) Show that if  $G$  has a Abelian Sylow  $p$ -subgroup, then  $p \nmid o(G' \cap Z(G))$ . Hence deduce  $G' \cap Z(G) = \langle e \rangle$  if all of the Sylow subgroups of  $G$  are Abelian. Theorem 10.18 is also relevant here.

(ii) Prove that if  $G/Z(G)$  is a  $p$ -group, then  $G'$  is also a  $p$ -group.

(iii) Give an example to show that the converse of (ii) is false.

(iv) Lastly, suppose  $G$  is a non-Abelian  $p$ -group, show that

$$G' \cap Z(G) > \langle e \rangle.$$

**Problem 4.27** Suppose  $n > 2$  and  $G = S_n$ . Using the natural action (Chapter 5) of  $G$  on the set  $\{1, 2, \dots, n\}$ , let  $H = \text{stab}_G(1)$  and  $J = A_n \cap H$ . Show that the transfer of  $G$  into  $H/J$  is non-trivial if, and only if,  $n$  is odd. (Hint. Note that  $\{e, (1, 2), \dots, (1, n)\}$  is a transversal of  $H$  in  $G$ .)

For the next two problems suppose the groups  $G$  are infinite.

**Problem 4.28** Show that if  $G$  has a finite generating set and  $H$  is a subgroup of  $G$  with the property  $[G : H] < \infty$ , then  $H$  also has a finite generating set. Note that this result can fail if the index  $[G : H]$  is infinite.

**Problem 4.29** Prove the following important result which is due to Schur:

$$\text{If } [G : Z(G)] < \infty \text{ then } G' \text{ is finite.}$$

(Hint. Begin by showing that  $G'$  has a finite generating set, then use the previous problem to deduce  $G' \cap Z(G)$  also has a finite generating set. Now consider the transfer of  $G$  into  $Z(G)$ , and use Corollary 4.29.) We noted earlier that an Abelian group with a finite generating set and finite exponent is finite; this is not true in general, see page 26.

**Problem 4.30** Prove Theorem 4.30. (Hint. Assume the contrary, choose  $a \in P \cap G' \cap Z(G)$  and, using the transfer  $\xi$  of  $G$  to  $P$ , show that  $a\xi = a^{[G:P]}$ . Then, noting that  $\xi$  is a homomorphism, obtain a contradiction. For the second part see Chapter 8.)

**Problem 4.31** Suppose  $G$  is a free group. Prove the following statements.

- (i)  $G$  is torsion-free (except for  $e$  it has no elements of finite order).
- (ii) If  $G$  has at least two generators (its rank is larger than 1), then it is centreless.
- (iii)  $G$  is Abelian if, and only if, it is cyclic.

**Problem 4.32** Prove the converse of Theorem 4.33, and so complete the result relating our two definitions of ‘free’. (Hint. Consider the homomorphism property given in Definition 4.31.)

**Problem 4.33** Suppose  $\langle A \mid R \rangle$  is a presentation of a group  $G$ . Show that if  $S$  is another set of relations on  $A$ , then the group  $H = \langle A \mid R \cup S \rangle$  is a homomorphic image of  $G$ . Hence if we add more relations to the presentation of  $G$  we obtain a presentation of some factor group of  $G$ .

**Problem 4.34** Let  $a, b, c$  and  $d$  be elements of a finite group which satisfy:

$$a^{-1}ba = b^2, \quad b^{-1}cb = c^2, \quad c^{-1}dc = d^2, \quad d^{-1}ad = a^2.$$

Using the following method show that  $a = b = c = d = e$ . Suppose  $o(a) = r$  and  $o(b) = s$  with  $r, s > 1$ . Show that

$$2^r \equiv 1 \pmod{s}.$$

Deduce the least prime divisor of  $r$  is smaller than the least prime divisor of  $s$ . Further, if  $q$  is a prime divisor of  $s$ , then there exists divisors  $t$  and  $p$  (prime) of  $r$  which satisfy

$$2^t \not\equiv 1 \pmod{q} \quad \text{and} \quad 2^{tp} \equiv 1 \pmod{q}.$$

Now use Fermat’s Theorem to obtain a contradiction.

In 1951 Higman<sup>2</sup> showed that if we remove the requirement that  $G$  is finite, then  $G$  is not the neutral group, and it has a maximal normal subgroup  $K$  with the property that  $G/K$  is a finitely generated infinite simple group — one of the first known examples of such a group.

**Problem 4.35** Investigate the proposition: Suppose  $G$  is a group with  $n$  generators and  $m$  relations where  $m < n$ , then  $G$  is infinite.

**Problem 4.36** Write out the coset enumeration tables for the group  $A_5$  and subgroups isomorphic to (a)  $C_5$ , (b)  $C_3$ , and (c)  $C_2 \times C_2$ .

**Problem 4.37** Explain why the coset enumeration method fails for the group

$$H = \langle a, b \mid a^3 = b^3 = (ab)^3 = e \rangle$$

and the subgroup  $\langle a \rangle$ . (Hint. Try to construct the coset enumeration table.) Note that the method will succeed if the exponents 3, 3, 3 are replaced by

<sup>2</sup> A finitely generated infinite simple group. J. London Math. Soc., **26**, pp. 61-64.

either (a)  $2, 2, m$  where  $m \geq 2$  (Problem 3.22), or (b)  $2, 3, n$  where  $3 \leq n \leq 5$ ; see Coxeter and Moser [1984].

**Problem 4.38** Consider the group  $J$  with presentation

$$J = \langle a, b \mid a^5 = b^3 = (ab)^4 = e, R \rangle$$

where  $R$  stands for the relation:  $(ab)^2 \in Z(J)$ . First construct the coset enumeration table for this group and the subgroup generated by  $a$  and  $(ab)^2$ . Secondly, try to simplify this table by introducing a new ‘variable’  $c = ab$  (for more details see Suzuki [1982], page 176). Incidentally  $J$  is isomorphic to the special linear group  $SL_2(5)$  (page 451).

## 5.4W Transitive and Primitive Permutation Groups

Here we return to the study of permutation groups begun in Chapter 3 and introduce *transitivity* and *primitivity*. This work is more ‘specialised’ than that given in the earlier sections of the chapter; some applications will be given in Chapter 12 and **Web Section** 12.6. The development is based in part on Robinson [1982], Chapter 7.

### *Transitivity*

We begin with

**Definition 5.28** (i) Given a set  $X$ , a group of permutations  $G$  on  $X$ , that is a subgroup of  $S_X$ , is called a *permutation group* on  $X$ .

(ii) The *degree* of  $G$  is  $o(X)$ .

(iii)  $G$  is called *transitive* on  $X$  if, for each pair  $x, y \in X$ , there exists an element  $\sigma \in G$  with the property

$$y = x\sigma.$$

If this property fails then  $G$  is called *intransitive* on  $X$ .

(iv) If  $G$  acts on  $X$  and  $\nu : G \mapsto S_X$  is the permutation representation given in Definition 5.9, then the action of  $G$  on  $X$  is called *faithful* if the homomorphism  $\nu$  is injective.

By Theorem 5.11, we see that if  $\nu$  is injective, then the intersection of the stabilisers  $\text{stab}_G(x)$  for  $x \in X$  is the neutral subgroup.

In Example (d) on page 93 we defined a *permutation action*. For each permutation group  $G$  on  $X$  we see that  $G$  acts on  $X$  using this permutation action, and  $G$  is transitive if, and only if, the corresponding action is transitive.

*Examples.* Clearly both the groups  $A_n$  and  $S_n$  are transitive on their underlying sets  $\{1, \dots, n\}$ , but note there are both intransitive on the set  $\{1, \dots, n+1\}$ . Some further examples are given in Chapter 12.

A stronger transitivity property holds for the group  $S_n$  (Problem 5.29 gives a similar property for  $A_n$ ): if we take two subsets of  $X = \{1, \dots, n\}$ , each with  $k$  elements where  $k \leq n$ , there is an element of  $S_n$  which provides a bijection of the first set onto the second; we say  $S_n$  is *k-transitive*, see definition below. For large  $k$  not many  $k$ -transitive groups exist<sup>3</sup>, but those that do have a number of special properties.

<sup>3</sup> The following result holds (see the reference quoted above)

- (i) The only 4-transitive groups are  $S_n$  ( $n > 3$ ),  $A_n$  ( $n > 5$ ),  $M_{11}$  and  $M_{23}$ ,
- (ii) The only 5-transitive groups are  $S_n$  ( $n > 4$ ),  $A_n$  ( $n > 6$ ),  $M_{12}$  and  $M_{24}$ , and
- (iii) If  $n > 5$ , then the only  $n$ -transitive groups are  $S_n$  and  $A_{n+2}$ .

The current proof of this theorem relies on CFSG, but it is generally believed that a CFSG-free proof is possible — a hard open problem!

Given a finite set  $X$  and positive integer  $k$  which is not greater than  $o(X)$  we let  $\{X; k\}$  denote the set of all ordered  $k$ -element subsets of  $X$  with no repetition. If  $o(X) = n$  and  $k \leq n$ , then clearly

$$o(\{X; k\}) = n(n-1) \dots (n-(k-1)). \quad (5.10)$$

If  $G$  is a permutation group on  $X$ , we define a new action of  $G$  on  $\{X; k\}$  by

$$(a_1, \dots, a_k) \cdot \sigma = (a_1 \sigma, \dots, a_k \sigma), \quad (5.11)$$

where  $(a_1, \dots, a_k) \in \{X; k\}$ ,  $\sigma \in G$ , and  $k \leq n$ , the reader should check that the action axioms hold.

**Definition 5.29** (i) Using the notation set out above, we say that  $G$  is  $k$ -transitive if the action of  $G$  on  $\{X; k\}$  is transitive.

(ii)  $G$  is called *sharply  $k$ -transitive* if it is  $k$ -transitive, and for every pair of  $k$ -tuples in  $\{X; k\}$  there is a *unique*  $\sigma \in G$  which provides a bijection of the first member of the pair to the second.

Note that 1-transitivity is the same as transitivity. Once we have proved the following two results we shall give some examples of sharply 2- and 3-transitive groups, and in Chapter 12 we shall discuss some sharply 4- and 5-transitive examples – the *Mathieu groups*  $M_{11}$  and  $M_{12}$ .

The following straightforward theorem is basic.

**Theorem 5.30** *If  $G$  is a transitive permutation group on a finite set  $X$ ,  $x \in X$ , and  $k > 1$ , then  $G$  is  $k$ -transitive on  $X$  if, and only if,  $\text{stab}_G(x)$  is  $(k-1)$ -transitive on  $X \setminus \{x\}$ .*

*Proof.* First suppose  $G$  is  $k$ -transitive on  $X$ . If

$$(x_1, \dots, x_{k-1}), (y_1, \dots, y_{k-1}) \in \{X \setminus \{x\}; k-1\},$$

then  $x_i \neq x \neq y_i$  for  $i = 1, \dots, k-1$ , and by hypothesis ( $k$ -transitivity), there exists  $\sigma \in G$  which maps

$$(x_1, \dots, x_{k-1}, x) \quad \text{to} \quad (y_1, \dots, y_{k-1}, x).$$

But then  $\sigma$  maps  $x$  to  $x$ , and  $(x_1, \dots, x_{k-1})$  to  $(y_1, \dots, y_{k-1})$ , and as this applies to all pairs of distinct  $(k-1)$ -tuples of elements of  $G$ , the result follows in this case by the definitions of stability and  $(k-1)$ -transitivity.

Conversely, suppose  $\text{stab}_G(x)$  is  $(k-1)$ -transitive on  $\{X \setminus \{x\}; k-1\}$ , and let  $(x_1, \dots, x_k), (y_1, \dots, y_k) \in \{X; k\}$ . The group  $G$  is transitive by hypothesis, and so there exists  $\tau_1, \tau_2 \in G$  to satisfy

$$x_k \tau_1 = x \quad \text{and} \quad x \tau_2 = y_k.$$

By hypothesis we can find  $\sigma \in \text{stab}_G(x)$  which maps  $(x_1 \tau_1, \dots, x_{k-1} \tau_1)$  to  $(y_1 \tau_2^{-1}, \dots, y_{k-1} \tau_2^{-1})$ . That is



$$x_i \tau_1 \sigma = y_i \tau_2^{-1} \quad \text{or} \quad x_i \tau_1 \sigma \tau_2 = y_i,$$

for  $i = 1, \dots, k-1$ . Further, as  $\sigma \in \text{stab}_G(x)$  we have  $x_k \tau_1 \sigma \tau_2 = x \sigma \tau_2 = x \tau_2 = y_k$ . Combining these two statements we see that  $\tau_1 \sigma \tau_2$  belongs to  $G$  and maps  $(x_1, \dots, x_k)$  to  $(y_1, \dots, y_k)$ . As above this applies to all subsets of  $G$  with  $k$  elements, and so the result follows.  $\square$

Note that by treating each  $x$  in turn this result shows that if a group  $G$  is  $(k+1)$ -transitive, then it is also  $k$ -transitive as  $\text{stab}_G(x) \leq G$ .

**Corollary 5.31** *Suppose  $o(X) = n$ ,  $k \leq n$ , and  $G$  is  $k$ -transitive on  $X$ .*

- (i)  *$o(G)$  is divisible by  $n(n-1)\dots(n-(k-1))$ .*
- (ii)  *$G$  is sharply  $k$ -transitive if, and only if,  $o(G) = n(n-1)\dots(n-(k-1))$ .*

*Proof.* (i) This is an immediate consequence of (5.10) and the Orbit-stabiliser Theorem (Theorem 5.7).

(ii) This also follows from (5.10) and Theorem 5.7, for in this case the stabiliser has order 1.  $\square$

We give some examples of sharply 2- and 3-transitive groups.

*Example.* Let

$$X = \mathbb{F}_p \cup \{\infty\}.$$

Reader: think of  $X$  as a ‘line’ in a ‘geometry’ defined over the finite field  $\mathbb{F}_p$  with  $p+1$  elements where  $\{\infty\}$  is the ‘point at infinity’ on this line.<sup>4</sup> We work with the symbol  $\infty$  in the usual naive way, that is:  $1/0 = \infty$ ,  $a + \infty = \infty = a - \infty$ ,  $\infty/\infty = 1$  *et cetera*. Further, let  $LF(p)$  denote the set of *linear fractional transformations* on  $\mathcal{P}$ ; that is the set of functions  $\alpha : \mathcal{P} \rightarrow \mathcal{P}$  where, for  $x \in \mathcal{P} \setminus \{\infty\}$ ,

$$x\alpha = \frac{ax+b}{cx+d} \quad \text{and} \quad \infty\alpha = \frac{a}{c},$$

$a, b, c, d \in \mathbb{F}_p$ , and  $ad - bc \neq 0$  (that is  $ad - bc \not\equiv 0 \pmod{p}$ ). It can be shown that  $LF(p)$  is a group with the operation of composition of functions, and it is isomorphic to  $GL_2(p)$  factored by its centre ( $PGL_2(p)$ ; page 170). Using the natural action of  $LF(p)$  on  $\mathcal{P}$ , where  $x\backslash\alpha = x\alpha$ , we define

$$LP(p) = \text{stab}_{LF(p)}(\infty),$$

and we obtain the group of all linear polynomial functions, that is maps of the type  $x \rightarrow ax + b$  where  $x \in \mathcal{P}$  and  $a \neq 0$ . We have

**Theorem 5.32** (i) *The group  $LP(p)$  is sharply 2-transitive on  $\mathbb{F}_p$ , and it has order  $p(p-1)$ .*

(ii) *The group  $LF(p)$  is sharply 3-transitive on  $\mathbb{F}_p \cup \{\infty\}$ , and it has order  $p(p^2-1)$ .*

<sup>4</sup> We can use any finite field as the base field in this example. Also  $\mathcal{P}$  is called the *projective line*, see Chapter 12 for a further discussion of this type of geometry.

*Proof.* We show first that  $LP(p)$  is 2-transitive on  $\mathbb{F}_p$ . As  $\mathbb{F}_p$  is a field, given  $x_1, y_1, x_2, y_2 \in \mathbb{F}_p$  where  $x_i \neq y_i, i = 1, 2$ , we can find  $a, b \in \mathbb{F}_p$  to satisfy:

$$x_2 = ax_1 + b, \quad y_2 = ay_1 + b \quad \text{where} \quad a \neq 0.$$

Hence there exists an element of  $LP(p)$  which maps  $(x_1, y_1)$  to  $(x_2, y_2)$ , and so  $LP(p)$  is 2-transitive. This further shows that  $LF(p)$  is transitive on  $X = \mathbb{F}_p \cup \{\infty\}$  because  $LP(p)$  is transitive on  $\mathbb{F}_p$ , and the linear fractional function which maps  $x$  to  $1/x$  also maps  $\infty = 1/0$  to 0, and vice versa. Using Theorem 5.30 this shows that  $LF(p)$  is 3-transitive on the set  $X$ .

Further, the order of  $LP(p)$  is  $p(p-1)$ . In the definition above,  $a$  and  $b$  are arbitrary elements of  $\mathbb{F}_p$  except that  $a \neq 0$ . Hence by Corollary 5.31(ii),  $LP(p)$  is sharply 2-transitive on  $\mathbb{F}_p$ . Also  $o(LF(p)) = (p+1)p(p-1)$  because  $[LF(p) : LP(p)] = o(X) = p+1$ , and so  $LF(p)$  is sharply 3-transitive, again by Corollary 5.31(ii); the theorem follows.  $\square$

Zassenhaus has shown that every sharply 2-transitive group is either of the same general type as  $LP(p)$ , or has one of the following orders:  $5^2, 7^2, 11^2, 23^2, 29^2$  or  $59^2$ ; see Passman [1968], and Huppert and Blackburn III (1982b). We shall return to this topic in Web Section 14.3 where we discuss *Frobenius groups*.

## Primitive Permutation Groups

We come now to *primitive permutation groups*, they have a somewhat technical definition but as we shall see below they are a useful tool in the further development of the theory of transitive groups.

**Definition 5.33** Let  $G$  be a transitive permutation group on a set  $X$ . A proper subset  $Y$  of  $X$  is called an *imprimitive subset*, or sometimes a *block*, for  $G$  if

- (i)  $o(Y) \geq 2$ , and
- (ii) for each  $\sigma$  in  $G$ , the sets  $Y$  and  $Y\sigma$  are either identical or disjoint.

The group  $G$  is called *imprimitive* if it possesses an imprimitive subset, and it is called *primitive* if no such subset exists. To be more precise it is the action that is (im)primitive: A permutation group is (im)primitive if the corresponding action has this property.

It is easy to see that the symmetric group  $S_n$  is primitive provided  $n > 2$ . The group  $D_4$  is an example of an imprimitive group. This group has the presentation  $\langle a, b \mid a^4 = b^2 = (ab)^2 = e \rangle$ , and we can treat it as a permutation group on a 4-element set if, for example, we let  $a \mapsto (1, 2, 3, 4)$  and  $b \mapsto (1, 3)$ . It is a straightforward exercise to show that  $Y = \{a, ab\} = \{(1, 2, 3, 4), (1, 2)(3, 4)\}$  is an imprimitive subset for  $D_4$ . For instance  $Y(1, 3) = Y$ , and  $Y(13)(24) = \{(1, 4, 3, 2), (1, 3)\}$  which has no element in common with  $Y$ .

The imprimitive subsets of an imprimitive group behave rather like cosets for we have<sup>5</sup> imprimitive subsets

**Theorem 5.34** *Suppose  $G$  is a transitive permutation group on  $X$ ,  $Y$  is an imprimitive subset for  $G$ , and  $H = \{\sigma \in G : Y\sigma = Y\}$ .*

(i)  $H \leq G$ .

(ii) *If  $Z$  is a transversal of  $H$  in  $G$  (Web Section 4.6), then the collection of subsets*

$$Y\sigma = \{y\sigma : y \in Y\},$$

*one for each  $\sigma \in Z$ , forms a partition of  $X$ .*

(iii)  $o(X) = o(Y) \cdot o(Z)$ .

(iv) *In the natural action, defined by right multiplication, the subsets  $Y\sigma$  are permuted by the elements of  $G$ .*

*Proof.* (i) This is a straightforward exercise for the reader.

(ii) and (iii) Suppose  $x \in X$  and  $y \in Y$ . We can find  $\tau \in G$  to satisfy  $x = y\tau$  because  $G$  is transitive. Also, as  $Z$  is a transversal of  $H$  in  $G$ , we can find  $\alpha \in H$  and  $\nu \in Z$  to satisfy  $\tau = \alpha\nu$ . Combining these equations we have, for  $x \in X$ ,

$$x = y\tau = (y\alpha)\nu \in Y\nu,$$

hence  $X$  equals the union of  $Y\nu$  for  $\nu \in Z$ . Further, if  $Y\nu \cap Y\nu' \neq \emptyset$ , then  $Y \cap Y\nu'\nu^{-1} \neq \emptyset$ , and so  $Y = Y\nu'\nu^{-1}$  and  $\nu'\nu^{-1} \in H$  as  $Y$  is an imprimitive subset. But  $\nu$  and  $\nu'$  are members of the same transversal, therefore  $\nu = \nu'$ . This proves (ii), and (iii) follows immediately because  $o(Y\nu) = o(Y)$ .

(iv) If  $\nu \in Z$  and  $\sigma \in G$ , then  $H\nu\sigma = H\nu_1$ , say, is a permutation of the set of right cosets of  $H$  in  $G$ . Therefore  $(Y\nu)\sigma = Y\nu_1$ , that is (iv) follows.  $\square$

**Corollary 5.35** *If  $G$  is a transitive permutation group on  $X$  and  $o(X)$  is prime, then  $G$  is primitive.*

*Proof.* This follows immediately from Theorem 5.34(iii).  $\square$

For example this shows that  $S_3$  acts primitively on  $\{1, 2, 3\}$ . The reader should check that the argument we used for  $D_4$  in the example on page 354 does not work in this case.

**Theorem 5.36** *If  $G$  is a transitive permutation group on  $X$ , then  $G$  is primitive if, and only if,  $\text{stab}_G(x)$  is a maximal subgroup of  $G$ , and this applies for all  $x \in X$ .*

*Proof.* Suppose we have  $\text{stab}_G(x) < H < G$ , that is the stabiliser of  $x$  in  $G$  is not maximal. Let

<sup>5</sup> Note that the imprimitive subsets, the blocks, are subsets of the underlying set  $X$  and not of the group  $G$ .

$$Y = \{x\sigma : \sigma \in H\}.$$

Now  $o(Y) \geq 2$  because  $\text{stab}_G(x)$  is a proper subgroup of  $H$ . Also  $Y \neq X$ . For if  $Y = X$  and  $\sigma \in G$ , we can find  $\tau \in H$  to satisfy  $x\sigma = x\tau$ , that is  $\sigma\tau^{-1} \in \text{stab}_G(x)$  which in turn shows that  $\sigma \in H$  and, as this holds for all  $\sigma \in G$ , we have  $H = G$  contradicting our hypothesis. Is  $Y$  an imprimitive subset? Yes, for if  $Y \cap Y\sigma \neq \emptyset$  we can find  $\tau_1, \tau_2 \in H$  with the property  $x\tau_1 = x\tau_2\sigma$ . This gives in turn  $\tau_2\sigma\tau_1^{-1} \in \text{stab}_G(x)$ ,  $\sigma \in H$ , and  $Y = Y\sigma$ . By definition it follows that  $G$  is imprimitive.

For the converse, suppose  $Y$  is an imprimitive subset of  $X$ . By the transitivity of  $G$  we may suppose  $x \in Y$ . Let

$$J = \{\sigma \in G : Y = Y\sigma\} \quad \text{so} \quad J \leq G,$$

as the reader can easily check. Now let  $y, z \in Y$ . As  $G$  is transitive, we can find  $\sigma \in G$  to satisfy  $y\sigma = z$ , then  $z \in Y \cap Y\sigma$  and  $\sigma \in J$ . By the Orbit-stabiliser Theorem (Theorem 5.7) this shows that

$$o(Y) = [J : \text{stab}_J(x)].$$

If  $\sigma \in \text{stab}_G(x)$ , then  $x = x\sigma \in Y \cap Y\sigma$  which shows that  $Y = Y\sigma$  as  $Y$  is imprimitive, and  $\sigma \in J$  (by definition of  $J$ ). Hence  $\text{stab}_G(x) \leq J$  and  $\text{stab}_G(x) = \text{stab}_J(x)$ . Combining these we have

$$o(X) = [G : \text{stab}_G(x)] \quad \text{and} \quad o(Y) = [J : \text{stab}_J(x)] = [J : \text{stab}_G(x)].$$

Therefore  $\text{stab}_G(x) < J$  as  $o(Y) > 1$ , and  $J < G$  as  $o(Y) < o(X)$ , that is  $\text{stab}_G(x)$  is not maximal in  $G$ .  $\square$

The following corollary gives a number of examples of primitive groups, remember that a  $k$ -transitive group is 2-transitive if  $k \geq 2$ .

**Corollary 5.37** *A 2-transitive permutation group is primitive.*

*Proof.* Suppose  $G$  is 2-transitive on  $X$ , and  $Y \subseteq X$  is an imprimitive set for  $G$ , then we can find  $x, y \in Y$ ,  $x \neq y$  and  $z \in X \setminus Y$  (set difference). By the 2-transitivity of  $G$ , there is an element  $\sigma \in G$  satisfying  $x\sigma = x$  and  $y\sigma = z$ . Hence  $x \in Y \cap Y\sigma$  which in turn shows that  $Y = Y\sigma$ . This is a contradiction because it also implies that  $z = y\sigma \in Y$ .  $\square$

The last basic result in this section provides a connection between primitive groups and transitivity.

**Theorem 5.38** *If  $K$  is a non-neutral normal subgroup of a primitive permutation group  $G$  on  $X$ , then  $K$  is transitive on  $X$ .*

*Proof.* Let  $x \in X$  and let  $Y = \{x\sigma : \sigma \in K\}$ , so  $Y$  is an orbit of the natural action of  $K$  on  $X$  which contains  $x$ . If  $\alpha \in G$  and  $\sigma \in K$ , then  $(x\sigma)\alpha = x\alpha\alpha^{-1}\sigma\alpha$  where  $\alpha^{-1}\sigma\alpha \in K$  by hypothesis. This shows that  $Y\alpha$  is another orbit of  $K$  on  $X$ , one which contains  $x\alpha$ . As orbits are either disjoint or identical, see Lemma 5.2, we have  $Y = Y\alpha$  or

$Y \cap Y\alpha = \emptyset$ , that is  $Y$  is an imprimitive set if it contains more than one element. But by hypothesis no such set exists, and so either  $Y = X$ , and then  $K$  is transitive, or every orbit has order 1 in which case  $K = \langle e \rangle$  — the kernel of the action of a permutation group is  $\langle e \rangle$  by definition.

□

We shall illustrate these results with three applications, more are given in Chapter 12. First we give another proof of the simplicity of  $A_5$ . This proof uses Cauchy's Theorem (Theorem 6.2) whose proof only requires some basic action properties, and so is independent of the work presented in this section.

**Theorem 5.39** *The group  $A_5$  is simple.*

*Proof.* Suppose  $K \triangleleft A_5$  and  $K \neq \langle e \rangle$ . By Problem 5.29(ii),  $A_5$  is 3-transitive, and so 2-transitive; see comment on page 356. Hence by Corollary 5.37 it is primitive, and by Theorem 5.38 the normal subgroup  $K$  is transitive on  $\{1, 2, 3, 4, 5\}$ . Further by Corollary 5.31 we have  $5 \mid o(K)$ , and so by Cauchy's Theorem (Theorem 6.2), it follows that  $K$  contains a 5-cycle which we can take to be  $(1, 2, 3, 4, 5)$ . But  $K \triangleleft A_5$ , and so  $K$  contains the twelve 5-cycles which are conjugate to  $(1, 2, 3, 4, 5)$ , see Problem 3.3. The subgroup  $K$  also contains  $e$ , that is  $K$  contains at least 13 elements, but we have seen (page 101) that  $A_5$  has no proper subgroup of order greater than 12. Therefore  $K = A_5$ , and the result follows. □

Using some further permutation group properties which we have not developed (they involve so-called *regular normal subgroups*), the above proof can be extended to show that  $A_n$  is simple for all  $n \geq 5$ ; see Robinson [1982], page 195.

For our second illustration the reader will need to read Section 11.1 first, it deals with the notion of solubility. It can be shown that if  $G$  is a soluble primitive permutation group then it has prime-power degree. This in turn can be used to show that  $G$  can be interpreted as a affine group (that is a linear group which includes translations) over a field of prime-power degree. As with most of the material in this section further details can be found in Chapter 7 of Robinson [1982].

Lastly we use this work to give a group simplicity criterion which has wide applicability. It can be used to establish the simplicity several classes of classical groups including the linear groups  $L_n(q)$ , and some Mathieu groups; see Chapter 12.

**Theorem 5.40** (Iwasawa's Lemma) *Suppose*

- (a)  $G$  is a perfect group (that is  $G' = G$ ), and
- (b)  $G$  acts faithfully (Definition 5.28) and primitively on a set  $X$ .

*If there exists an Abelian subgroup  $J$  of  $G$ , which is normal in  $\text{stab}_G(x)$  where  $x \in X$ , whose normal closure  $J^*$  in  $G$  is  $G$  itself, then  $G$  is simple.*

The normal closure of a group was introduced in Problem 2.25, this problem gives

$$J^* = \langle g^{-1}Jg : g \in G \rangle.$$

*Proof.* Suppose the subgroup  $K$  satisfies  $\langle e \rangle < K \triangleleft G$ , we prove the theorem by showing that  $K = G$ . By Problem 5.27,  $K$  acts transitively on  $X$ , and so by Problem 5.28

$$G = K \operatorname{stab}_G(x). \quad (5.12)$$

Also by Supposition (b), if  $g \in G$ , then for all  $i$  there exist  $g_i \in G$  and  $j_i \in J$  with

$$g = \prod_i g_i^{-1} j_i g_i. \quad (5.13)$$

By (5.12) we can write  $g_i = k_i a_i$  where  $k_i \in K$  and  $a_i \in \operatorname{stab}_G(x)$ . Hence as  $J \triangleleft \operatorname{stab}_G(x)$ , equation (5.13) gives

$$g = \prod_i k_i^{-1} a_i^{-1} j_i a_i k_i \in KJK \leq KJ$$

as  $K \leq JK$ . This holds for all  $g \in G$  hence

$$G = KJ. \quad (5.14)$$

Applying the Second Isomorphism Theorem (Theorem 4.15) to (5.14) we obtain

$$J/(J \cap K) \simeq KJ/K = G/K.$$

Now  $J$  is Abelian by supposition and, as a factor group of an Abelian group is itself Abelian, we also have  $G/K$  is Abelian. By Problem 4.6 this shows that  $G' \leq K$ . But by (a)  $G' = G$ , so  $K = G$  as required.  $\square$

This result can be strengthened by replacing the condition ‘ $J$  is Abelian’ by the condition ‘ $J$  is soluble’; see Issacs (2008), page 252. In **Web Section 12.6** we shall use this lemma to reprove the simplicity of the linear groups  $L_n(q)$  in all cases except  $n = 2$  and  $q < 4$ .

## 5.5 Problems 5W

**Problem 5.27** Suppose  $G$  acts on the set  $X$  which has more than one element, and  $H \leq G$ . For  $x \in X$ , let  $x \setminus H = \{x \setminus h : h \in H\}$ .

(i) If  $x, y \in X$  and  $x \setminus H \cap y \setminus H \neq \emptyset$ , show that  $x \setminus H = y \setminus H$ .

(ii) If  $H \triangleleft G$  show that  $x \setminus H$  is a block in  $X$  for each  $x \in X$ . For the definition of a block see Definition 5.33.

(iii) Now suppose  $\langle e \rangle < H \triangleleft G$ . Show that the action of  $H$  on  $X$  is transitive if the action of  $G$  on  $X$  is both faithful and primitive. Secondly, show that  $o(X) \mid o(H)$ . (Hint. Use (ii) to show that, for  $x \in X$ ,  $x \setminus H$  equals either  $\emptyset$ ,  $\{x\}$  or  $X$ , and use the given conditions to show that the first two cases are impossible.)

**Problem 5.28** (i) Suppose  $K \triangleleft G$ ,  $G$  acts on the set  $X$ , and  $K$  acts transitively on  $X$ , show that for all  $x \in X$

$$G = K\text{stab}_G(x).$$

(Hint. Note that as  $K$  acts transitively on  $X$ , given  $x \in X$  and  $g \in G$ , there exists  $k \in K$  with the property  $x \setminus g = x \setminus k$ .)

(ii) Use (i) to reprove Lemma 6.14 – the Frattini Argument.

**Problem 5.29** (i) Show that  $S_n$  is sharply  $n$ -transitive and  $(n-1)$ -transitive on the set  $\{1, \dots, n\}$ . Is this second transitivity property sharp? The symmetric groups are in fact the only groups with this property.

(ii) Secondly, show that  $A_n$  is sharply  $(n-2)$ -transitive, provided  $n > 2$ .

(iii) Prove that  $S_n$  is primitive.

**Problem 5.30** (i) Suppose  $G$  acts on  $X$ ,  $K \triangleleft G$  and  $O$  is the set of orbits of  $K$  on  $X$  (that is we can naturally extend the action of  $G$  on  $X$  to an action of  $G$  onto the set of all subsets  $X$ ). Show that  $G$  acts transitively on  $O$ .

(ii) Suppose the permutation group  $G$  acts primitively on  $X$  and it contains a 2-cycle. Show that  $G \simeq S_X$ .

**Problem 5.31** (i) Using Theorem 5.22, prove that if  $G$  is a primitive permutation group of degree  $m$  where  $2 \mid m$  and  $m > 2$ , then  $4 \mid o(G)$ .

(ii) Suppose  $G$  is a permutation group,  $K$  is a minimum normal subgroup of  $G$  (page 235), and  $K$  is both transitive and Abelian, prove that  $G$  is primitive.

**Problem 5.32\*** Suppose  $G$  is a sharply 2-transitive group on  $X$ . Show that its degree, that is  $o(X)$ , is a power of some prime  $p$  using the following method. Let  $o(X) = n$ . Apart from the neutral permutation, elements of  $G$  either have no fixed points, or have exactly one fixed point. Let  $G_{(0)}$  denote the first of these sets and  $G_{(1)}$  the second, so by hypothesis

$$G = \{e\} \cup G_{(0)} \cup G_{(1)}.$$

Finally let  $p \mid n$  where  $p$  is prime.

(i) Show that if  $\alpha$  is an element of order  $p$  in  $G$ , then  $\alpha \in G_{(0)}$ .

(ii) By considering  $G_{(1)}$  and the stabilisers of the elements of  $G$ , deduce  $o(G_{(0)}) = n - 1$ .

(iii) Using Theorem 5.19, prove the result.

**Problem 5.33** (i) Show that if the group  $G$  acts faithfully and primitively on a set  $X$ , then  $\Phi(G) = \langle e \rangle$ . For details concerning the Frattini subgroup  $\Phi(G)$  see Section 10.2.

(ii) Suppose  $G$  is a  $p$ -group which is not elementary Abelian. Show that it cannot act both faithfully and primitively on a set  $X$ .

**Problem 5.34** Suppose  $G$  is a nilpotent permutation group of order larger than 1. (For a definition of nilpotency see Chapter 10.) Prove that  $G$  is primitive if, and only if, the order of the set on which  $G$  is acting equals  $o(G)$  and this integer is prime.

**Problem 5.35** Let  $G$  act on the set  $X$  where  $o(X) > 1$ . If this action is both faithful and primitive, and if  $\langle e \rangle < H \triangleleft G$ , show that  $H$  acts transitively in  $X$ , and deduce

$$o(X) \mid o(H).$$

(Hint. See Problem 5.27.)



## 6.5 Further Applications

Three further aspects of Sylow theory will be discussed in this section: (a) Intersections of Sylow subgroups, the radical, and Brodkey's Theorem; (b) Burnside's Normal Complement Theorem with some applications; and (c) a theorem of Hölder, Burnside and Zassenhaus which classifies amongst others all groups of square-free order.

### *Intersections of Sylow Subgroups, the Radical and Brodkey's Theorem*

For a fixed prime  $p$ , the  $p$ -radical  $O_p(G)$  of a finite group  $G$  is defined as the intersection of all Sylow  $p$ -subgroups  $P_i$  of  $G$ , it is an important example of a normal subgroup of  $G$ ; see pages 87, 133 and 222. The question arises: In this definition do we need to use all of the subgroups  $P_i$  to obtain the  $p$ -radical, or is a subset sufficient? Brodkey<sup>6</sup> showed that if  $P_i$  is Abelian, then the intersection of just two is sufficient to define the  $p$ -radical provided the 'right' two are chosen. The Abelianness condition is essential, see Problem 6.24, also there are a number of applications.

We shall prove Brodkey's result now. It is a corollary of the following lemma which applies to all Sylow subgroups of a finite group.

**Lemma 6.19** *Suppose  $Q$  and  $R$  are Sylow  $p$ -subgroups of  $G$  with the following property: If  $T = Q \cap R$ , then  $o(T)$  is minimal as  $Q$  and  $R$  range over all pairs of Sylow  $p$ -subgroups  $P_i$  of  $G$ . The  $p$ -radical  $O_p(G)$  is the unique largest subgroup of  $T$  which is normal in both  $Q$  and  $R$ .*

*Proof.* Suppose  $K \leq T$ ,  $K \triangleleft Q$  and  $K \triangleleft R$ . If we can show that

$$K \leq P_i \quad \text{for all Sylow } p\text{-subgroups } P_i \text{ of } G, \quad (6.8)$$

then  $K \leq O_p(G)$  and the result follows.

By definition of the normaliser we have  $Q \leq N_G(K)$ . Also  $P_i \cap N_G(K)$  is a  $p$ -subgroup of  $N_G(K)$ , and so it is contained in some Sylow  $p$ -subgroup of  $N_G(K)$ . Combining these propositions and using Sylow 2 (Theorem 6.9) we can find  $a \in N_G(K)$  to satisfy

$$P_i \cap N_G(K) \leq a^{-1}Qa.$$

We also have  $R \leq N_G(K)$ , and so  $a^{-1}Ra \leq N_G(K)$ . Hence

$$P_i \cap a^{-1}Ra = P_i \cap N_G(K) \cap a^{-1}Ra \leq a^{-1}Qa \cap a^{-1}Ra = a^{-1}Ta.$$

This gives

---

<sup>6</sup> Brodkey, J. S. (1963), A note on finite groups with an Abelian Sylow subgroup. Proc. Amer. Math. Soc., **14**, 132-3.

$$T = a(a^{-1}Ta)a^{-1} \geq a(P_i \cap a^{-1}Ra)a^{-1} = aP_ia^{-1} \cap R. \quad (6.9)$$

Now both  $aP_ia^{-1}$  and  $R$  are Sylow  $p$ -subgroups of  $G$ , and by (6.9) their intersection is contained in  $T$ . But by definition,  $T$  is minimal for this property, hence

$$aP_ia^{-1} \cap R = T, \quad \text{and so} \quad K \leq T \leq aP_ia^{-1}.$$

This shows that  $a^{-1}Ka \leq P_i$ , but by assumption  $g^{-1}Kg = K$  for all  $g \in G$ , hence (6.8) follows and the proof is complete.  $\square$

We can now derive

**Theorem 6.20** (Brodkey's Theorem) *If  $G$  has Abelian Sylow  $p$ -subgroups  $P_i$ , then  $i$  and  $j$  can be chosen so that*

$$P_i \cap P_j = O_p(G).$$

*Proof.* If in Lemma 6.19 the Sylow  $p$ -subgroups  $Q$  and  $R$  are Abelian, then automatically the intersection  $T$  chosen there is normal in both of them, and so the result follows.  $\square$

**Corollary 6.21** *Suppose  $P$  is an Abelian Sylow  $p$ -subgroup of  $G$ .*

- (i)  $o(O_p(G)) \geq o(P)^2/o(G)$ .
- (ii) *If  $o(P) > [G : P]$ , then  $G$  is not simple provided  $o(G) \neq p$ .*

*Proof.* (i) By Brodkey's Theorem there exist Abelian Sylow  $p$ -subgroups  $Q$  and  $R$  of  $G$  satisfying  $Q \cap R = O_p(G)$ . Hence by Theorem 5.8 we have

$$o(G) \geq o(QR) = \frac{o(Q)o(R)}{o(Q \cap R)} = \frac{o(P)^2}{o(O_p(G))},$$

and (i) follows.

(ii) By Problem 6.19(vi) and (i),  $O_p(G)$  is a proper non-neutral normal subgroup of  $G$ . Hence  $G$  is not simple.  $\square$

For example if  $o(G) = 4p$  and  $p > 3$ , then  $G$  is not simple as  $p^2 > 4p$  in this case. Some further examples are given in Problem 6.25.

In the printed text we also considered intersections of Sylow subgroups in part of the proof of Theorem 6.13, and in Problems 6.8 and 6.17.

### ***Burnside's Normal Complement Theorem***

We begin with

**Definition 6.22** (i) Let  $H, J \leq G$ ,  $HJ = G$  and  $H \cap J = \langle e \rangle$ . The subgroup  $J$  is called a *complement* of  $H$  in  $G$ , and  $H$  is a complement of  $J$  in  $G$ .

(ii) If  $K \triangleleft G$ , then  $G$  is called an *extension* of  $K$  by  $H$  if  $G/K \simeq H$ .

*Notes.* In (i), if  $H \triangleleft G$ , then  $G/H \simeq J$  by the Second Isomorphism Theorem (Theorem 4.15), and so  $G$  is an extension of  $H$  by  $J$ ; and in (ii),  $K$  does not necessarily have a complement. One possible reason is that  $G$  may not contain a subgroup isomorphic to  $H$ .

Some of the most important results in the theory concern the existence of complements. These include the Schur-Zassenhaus Theorem to be proved in **Web Section 9.4**, results about semi-direct products given in Chapter 7, and Burnside's theorem to be proved now. This result gives a condition under which a Sylow subgroup has a (normal) complement, it has a number of useful applications, an example is given after the proof.

**Theorem 6.23(17)** (Burnside's Normal Complement Theorem) *If  $G$  is a finite group and  $P$  is a Sylow subgroup of  $G$  which satisfies the condition*

$$P \leq Z(N_G(P)), \quad (6.10)$$

*then  $P$  has a normal complement in  $G$ .*

The condition (6.10) is equivalent to the statement:  $C_G(P) = N_G(P)$ ; see Problem 5.17(ii). The proof below uses the *transfer*, before proceeding the reader should review **Web Section 4.6** which introduces this entity.

*Proof.* Note first that as  $P$  is a subgroup of a centre, it is Abelian. Let  $[G : P] = m$  and let  $\xi$  denote the transfer of  $G$  to  $P$ , see Definition 4.26 in **Web Section 4.6**. The map  $\xi$  is a homomorphism and we shall prove the theorem by showing that its kernel is a (normal) complement of  $P$ . Let  $a \in P$ . By Corollary 4.28, the value of  $a\xi$  is given by

$$a\xi = \prod_r h_r^{-1} a^{m_r} h_r,$$

where  $\{h_1, \dots, h_n\}$  is a subset of a transversal, and  $1 \leq m_r \leq m$ . For each  $r$  both  $a^{m_r}$  and  $h_r^{-1} a^{m_r} h_r$  belong to  $P$  by definition and Corollary 4.28, and they are conjugate in  $C_G(P)$ , for as  $P$  is Abelian it is a subgroup of  $C_G(P)$ . Using Problem 6.10(ii) we see that, as these elements belong to  $C_G(P)$  and are conjugate in  $G$ , they are also conjugate in  $N_G(P)$ , and so there exist  $j_r \in N_G(P)$  with the property

$$h_r^{-1} a^{m_r} h_r = j_r^{-1} a^{m_r} j_r = a^{m_r}.$$

This last equality follows by (6.10). Hence by Corollary 4.29

$$a\xi = a^m \quad \text{for all } a \in P \quad \text{where } m = \sum_r m_r = [G : P].$$

Suppose  $o(P) = p^t$ , then  $(m, p^t) = 1$  as  $P$  is a Sylow  $p$ -subgroup. Using the Euclidean Algorithm (Theorem B2), integers  $r$  and  $s$  can be found to satisfy  $rm + sp^t = 1$ , and so as  $a \in P$

$$a = a^{rm} a^{sp^t} = (a^m)^r.$$

Rewriting this we have  $a^r \xi = a^{rm} = a$ ; that is  $\xi$  is surjective. Let  $K = \ker \xi$ , then the First Isomorphism Theorem (Theorem 4.11) shows that  $G/K \simeq P$ . So  $G = KP$ , and  $K \cap P = \langle e \rangle$ , because we have  $o(K) = [G : P] = m$  and  $(m, p^t) = 1$ . The theorem follows because a kernel of a homomorphism,  $\xi$  in this case, is always normal.  $\square$

*Example.* Let  $G$  be a non-Abelian group of order  $pq$  with  $p < q$ , and let  $P_1, P_2 \leq G$  with  $o(P_i) = p$ ,  $i = 1, 2$ , that is  $G$  has distinct Sylow  $p$ -subgroups. We have  $P_1 = N_G(P_1)$  as  $P_1$  is non-normal, and so  $P_1 = Z(N_G(P_1))$  as  $P_1$  is Abelian. Hence the condition of Burnside's theorem applies, and therefore  $P_1$  has a normal complement of order  $q$ . This provides a second derivation of Theorem 6.11.

Some consequences of Burnside's theorem are given now, more will follow in the problem section. The first is concerned with the smallest prime dividing the order of a group.

**Theorem 6.24** *Suppose  $G$  is a group,  $p_0$  is the smallest prime dividing  $o(G)$ , and  $P$  is a cyclic Sylow  $p_0$ -subgroup of  $G$ , then  $P$  has a normal complement in  $G$ .*

*Proof.* We have

- (a) by the  $N/C$ -theorem (Theorem 5.26),  $N_G(P)/C_G(P)$  is isomorphic to a subgroup of  $\text{Aut } P$ ;
- (b) by Theorem 4.23 and later comments,  $o(\text{Aut } P) = p_0^{n-1}(p_0 - 1)$  as  $P$  is cyclic; and
- (c)  $C_G(P) \geq P$  as  $P$  is Abelian (cyclic).

Now as  $P$  is a Sylow  $p_0$ -subgroup, (c) implies

$$p_0 \nmid o(N_G(P)/C_G(P)), \quad \text{and so} \quad o(N_G(P)/C_G(P)) \mid p_0 - 1$$

by (b). But  $p_0$  is the smallest prime dividing  $o(G)$ , hence

$$o(N_G(P)/C_G(P)) = 1.$$

Therefore  $N_G(P) = C_G(P)$ , and by Problem 5.17, this shows that the condition for Burnside's theorem (Theorem 6.23) applies, hence  $P$  has a normal complement.  $\square$

In Problem 2.19 we showed that if  $G$  has a subgroup  $H$  with index 2, then  $H \triangleleft G$ . The theorem above shows that  $H$  always exists if its order is odd. Reader: What happens if  $o(H)$  is even?

**Corollary 6.25** *If  $o(G) = 2m$  where  $m$  is odd, then  $G$  has a normal subgroup  $K$  with  $o(K) = m$ .*

*Proof.* This follows immediately from Theorem 6.24, as the Sylow 2-subgroup of  $G$  is necessarily cyclic.  $\square$

This result can be extended to show that if  $G$  is simple and non-Abelian, then either 8 or 12 divides  $o(G)$  as we show now.

**Theorem 6.26** *If  $G$  is a non-Abelian simple group and  $p_0$  is the smallest prime dividing  $o(G)$ , then either  $p_0^3 \mid o(G)$ , or  $12 \mid o(G)$ .*

*Proof.* Let  $P$  be a Sylow  $p_0$ -subgroup of  $G$ . By Theorem 6.24, it is not cyclic, and so

(a) either  $p_0^3 \mid o(G)$ , or

(b)  $P$  is a non-cyclic group of order  $p_0^2$ , that is  $P \simeq C_{p_0} \times C_{p_0}$ , see Section 7.2.

If (a) holds the result follows, and if (b) holds  $P$  is an elementary Abelian  $p_0$ -group (Problem 4.18(i)). In this case, by Problem 4.18(iii) we have

$$o(\text{Aut } P) = p_0(p_0 + 1)(p_0 - 1)^2 = t,$$

say. By the  $N/C$ -theorem (Theorem 5.26),  $o(N_G(P)/C_G(P))$  is a divisor of  $t$  which is larger than 1 (by Burnside's theorem and the hypothesis). Also  $p_0 \nmid o(N_G(P)/C_G(P))$  as  $P \leq C_G(P)$  and  $P$  is a Sylow subgroup. Hence, as  $p_0$  is the smallest prime divisor of  $o(G)$ , it follows that  $p_0 + 1 \mid t$ . If  $p_0$  is odd this gives a contradiction because the smallest prime divisor of  $t$  is at least  $p_0 + 2$ . Hence  $p_0 = 2$ , then  $t = o(\text{Aut } P) = 6$ , which shows finally that  $12 \mid o(G)$  as required.  $\square$

The Feit-Thompson Odd Order Theorem states that every group of composite odd order contains a proper non-neutral normal subgroup. This together with Theorem 6.26 shows that the order of every non-Abelian simple group is divisible by 8 or 12. In fact, this can be improved to: The order of every such group is divisible by 12, 16 or 56. There exists one class of simple groups, the so-called *Suzuki groups*  $Sz(2^{2n+1})$  with  $n > 0$  (Web Chapter 14), whose orders are divisible by 8 but not by 3.

Our next application provides another method for proving that groups of certain orders cannot be simple.

**Theorem 6.27** *If  $G$  is simple,  $o(G) = pm > p$ ,  $p \nmid m$ , and  $P$  is a Sylow  $p$ -subgroup of  $G$ , then  $C_G(P) < N_G(P) < G$  and  $[N_G(P) : C_G(P)] \mid p - 1$ .*

*Proof.* By Burnside's and the  $N/C$  theorems (Theorems 6.23 and 5.26) we have  $C_G(P) < N_G(P)$  and, by Sylow 3,  $N_G(P) < G$ , both as  $G$  is simple. Further  $P \leq C_G(P)$  because  $P$  is Abelian, and  $o(\text{Aut } P) = p - 1$  as  $o(P) = p$ . Hence the  $N/C$ -theorem gives the second result.  $\square$

*Example.* There are no simple groups of order 396.

We have  $396 = 2^2 \cdot 3^2 \cdot 11$ , and so a group of order 396 will have a Sylow 11-subgroup  $P_1$ , say. If  $G$  is simple, then  $n_{11} = 12$  and  $o(N_G(P_1)) = 33$  by Sylow 3 and 4. But by Theorem 6.27,  $o(C_G(P_1)) = 11$ , as  $o(C_G(P_1))$  is at least 11 because  $P_1 \leq C_G(P_1)$ , and so  $[N_G(P_1) : C_G(P_1)] = 3$  which clearly does not divide 10. This contradiction shows that a group of order 396 must have a normal subgroup of order 11, and therefore cannot be simple. Some further examples are given in Problem 6.28.

### *Groups with Cyclic Sylow Subgroups*

As a further application of Burnside's theorem (Theorem 6.23) we prove the following *Classification Theorem*. Classification theorems are important in the quest to describe all groups, amongst other consequences this particular result will determine (that is, give representations of) all groups with square-free order. There is a unique Abelian group for each fixed square-free order, that is the cyclic group with this order; see Section 7.2. This uniqueness does not carry over to the non-Abelian case as will be seen in the example at the end of this section. Although this classification result is a consequence of Burnside's theorem, it also relies on results proved in Chapter 11; there is no circularity here because these (solubility) results follow directly from the work presented in Chapters 2 and 4.

We begin with

**Definition 6.28** A group is called *metacyclic*, or sometimes *Frobenius* (Web section 14.3), if it can be represented as an extension (Definition 6.19) of one cyclic group by another cyclic group.

The cyclic and dihedral groups are examples of metacyclic groups. Reader: Give the cyclic subgroups in the dihedral case.

Let  $G$  be a finite group all of whose Sylow subgroups are cyclic; note that all subgroups and all factor groups of finite cyclic groups are themselves finite and cyclic by Theorem 4.20. We also have in this case:

- (a) If  $G$  is Abelian, then  $G$  is cyclic, this follows from the Sylow theory and Problem 4.15(ii), this also follows from the direct product theory.
- (b) All Sylow subgroups of subgroups of  $G$  are cyclic; by Sylow 5, every  $p$ -subgroup of  $G$  is contained in a Sylow  $p$ -subgroup of  $G$ .
- (c) All Sylow subgroups of factor groups of  $G$  are cyclic. For if  $K \triangleleft G$ , a Sylow subgroup of  $G/K$  has the form  $PK/K$  where  $P$  is a Sylow subgroup of  $G$  (Problem 6.10(iii)), and by the Second Isomorphism Theorem (Theorem 4.15),  $PK/K \simeq P/(P \cap K)$ , but  $P$  is cyclic and so  $PK/K$  is also cyclic.

The last preliminary fact we need is

**Lemma 6.29** *If  $G$  is finite and all of its Sylow subgroups are cyclic, then both  $G'$  and  $G/G'$  are cyclic, where  $G'$  denotes the derived subgroup of  $G$ .*

This result, which is due to Zassenhaus, implies that  $G$  is metacyclic if it satisfies the conditions of the lemma. The proof relies on Theorem 6.23 and some basic work given in Problems 11.12 and 11.13. For a different proof see Issacs [2008], page 160. As noted above there is no circularity here because all of the facts concerning solubility used in these proofs are elementary consequences of the isomorphism theorems given in Chapter 4. But it should be noted that the main result used in the proof of Lemma 6.29 is Burnside's Normal Complement Theorem (Theorem 6.23).

Using these preliminary facts we can now show that a finite group with cyclic Sylow subgroups is metacyclic. In fact we have the following stronger result due to Hölder, Burnside and Zassenhaus which involves four number-theoretic conditions.

**Theorem 6.30(18)** *If  $G$  is a finite group all of whose Sylow subgroups are cyclic, then  $G$  has the presentation*

$$G \simeq \langle a, b \mid a^m = b^n = e, b^{-1}ab = a^r \rangle,$$

where

- (i)  $(m, n(r-1)) = 1$ ,    (ii)  $r^n \equiv 1 \pmod{m}$ ,
- (iii)  $0 \leq r < m$ ,    (iv)  $m$  is odd.

If  $G$  is a  $p$ -group, or if it is Abelian, then  $m = r = 1$  and  $a = e$  in the representation above, and  $G$  is cyclic. Also the converse of this theorem clearly follows from the preliminary results (b) and (c) given on the previous page. The condition is necessary. For example the order of  $A_5$ , that is  $2^2 \cdot 3 \cdot 5$ , satisfies the conditions (i) to (iv) above with  $m = 5$ , but the theorem does not apply because  $A_5$  has a non-cyclic Sylow subgroup.

*Proof.* By Lemma 6.29 we may suppose

$$G' = \langle a \rangle \triangleleft G \quad \text{and} \quad G/G' = \langle bG' \rangle, \quad (6.11)$$

for suitably chosen  $a, b \in G$ . Let  $o(G') = m$  and  $o(G/G') = n$ , and so by Lagrange's Theorem (Theorem 2.27),  $o(G) = mn$  and  $o(a) = m$ . We will show below that  $(m, n) = 1$ . By (6.11) we have

$$G = \langle a, b \rangle \quad \text{and} \quad b^{-1}ab = a^r, \quad (6.12)$$

for some  $r$  satisfying  $0 \leq r < m$  as  $o(a) = m$ . The second equation in (6.12) gives  $[a, b] = a^{-1}b^{-1}ab = a^{r-1}$ . Let

$$J = \langle a^{r-1} \rangle.$$

We show next that  $J = G'$ . By Problem 4.22(v),  $J \text{ char } G'$ , and so as  $G' \triangleleft G$  (Problem 2.16) we have  $J \triangleleft G$  by Problem 4.22(iv). By (6.12) this shows that  $G/J = \langle aJ, bJ \rangle$ , and

$$[aJ, bJ] = (aJ)^{-1}(bJ)^{-1}(aJ)(bJ) = [a, b]J = J,$$

as  $[a, b] \in J$ . This proves that  $G/J$  is generated by two elements which commute, hence it is Abelian. Therefore, by Problem 4.6(ii), we have  $G' \leq J$  and so  $J = G'$  because  $J \leq G'$  by definition. Therefore as  $o(a) = m$  we have

$$\langle a^{r-1} \rangle = J = G' = \langle a \rangle \quad \text{which gives} \quad (r-1, m) = 1. \quad (6.13)$$

Next we show that  $\langle b \rangle$  is a complement of  $G'$  in  $G$ . As  $o(G/G') = n$  we have  $b^n \in G'$  and so  $b^n = a^s$  for some integer  $s$ . Therefore, as  $b^{-1}ab = a^r$ ,

$$a^s = b^n = b^{-1}(b^n)b = b^{-1}(a^s)b = a^{rs} \quad \text{which gives} \quad a^{(r-1)s} = e.$$

Now  $o(a) = m$ , and so  $m \mid (r-1)s$ ; applying (6.13) this gives  $m \mid s$  and

$$b^n = e \quad \text{with} \quad o(b) = n,$$

as  $G/G' = \langle bG' \rangle$  and  $o(G/G') = n$ . Further, as  $G = \langle b \rangle G'$  we have using the Second Isomorphism Theorem (Theorem 4.15)

$$G/G' = \langle b \rangle G' / G' \simeq \langle b \rangle / (\langle b \rangle \cap G')$$

and, as  $o(G/G') = o(\langle b \rangle)$ , this shows that

$$\langle b \rangle \cap G' = \langle e \rangle.$$

Therefore  $\langle b \rangle$  is a complement of  $G'$  in  $G$ .

Lastly we prove that  $(m, n) = 1$ . Suppose not, so there exists a prime  $q$  dividing both  $m$  and  $n$ , and

$$o(a^{m/q}) = q = o(b^{n/q}).$$

Now  $\langle a^{m/q} \rangle \triangleleft G$  because  $J = \langle a \rangle \triangleleft G$ , so if we let

$$L = \langle a^{m/q} \rangle \langle b^{n/q} \rangle, \quad \text{then} \quad L \leq G \quad \text{and} \quad o(L) = q^2.$$

By Sylow 5,  $L \leq Q$  where  $Q$  is a Sylow  $q$ -subgroup of  $G$ . By hypothesis  $Q$  is cyclic, and so it has a *unique* subgroup of order  $q$  by Theorem 4.20. This is impossible because both  $\langle a^{m/q} \rangle$  and  $\langle b^{n/q} \rangle$  are subgroups of  $Q$  of order  $q$ . Hence  $(m, n) = 1$ . The reader should now check that the conditions (i) to (iv) are satisfied.  $\square$

As noted above an important special case of this result is:

Every group with square-free order is metacyclic,

for in this case all Sylow subgroups are necessarily cyclic. But note that several non-isomorphic groups may be involved; that is there may be several distinct solutions to the number-theoretic conditions (i) to (iv) in Theorem 6.30 for a group of given order. Let

$$F_{m,n,r} = \langle a, b \mid a^m = b^n = e, b^{-1}ab = a^r \rangle.$$

We usually drop the suffix ' $r$ ' when there is only one value, so we have  $F_{1,n,1} = F_{1,n} \simeq C_n$  and  $F_{m,2,m-1} = F_{m,2} \simeq D_m$ . Consider for example groups of order  $42 = 2 \cdot 3 \cdot 7$ , and let  $m, n$  and  $r$  satisfy conditions (i) to (iv) in Theorem 6.30. In this case  $m = 1, 3, 7$  or  $21$ ; so as just noted we only need to consider the cases



$m = 3$  or  $7$ . If  $m = 3$ , then  $n = 14$ , and  $2$  is the only possible value for  $r$ ; hence we obtain the group  $F_{3,14}$ . If  $m = 7$ , then  $n = 6$  and by Fermat's Theorem (Theorem B10)  $r = (1), 2, 3, 4, 5$  or  $6$ , suggesting possibly five new groups. But only three are non-isomorphic, they are  $F_{7,6,2} \simeq F_{7,6,4}$ ,  $F_{7,6,3} \simeq F_{7,6,5}$  and  $F_{7,6,6}$ ; the reader should check these facts by looking at their centres. Therefore there are six non-isomorphic groups of order  $42$ , they are  $C_{42}$ ,  $D_{21}$  and the four Frobenius groups listed above, all of which are metacyclic. Some further examples are given in Problem 6.31.

## 6.6 Problems 6W

**Problem 6.24** The Abelianness condition in Brodkey's Theorem (Theorem 6.20) is essential, prove this using the following example. Let  $J = C_3 \times C_3$ . The automorphism group  $\text{Aut } J$  of  $J$  is isomorphic to  $GL_3(2)$  with order  $48$ , and this group has a Sylow  $2$ -subgroup  $A$ , say, of order  $16$ . Form the semi-direct product of  $J$  by  $A$ , show that its  $2$ -radical is neutral, and so complete the proof.

**Problem 6.25** (i) Use Corollary 6.22 to prove that the following groups are not simple.

- (a) A group of order  $12p$  where  $p > 12$ .
- (b) A group of order  $p^2q^2$  where  $q > p$ .
- (c) All groups of order  $1764$ ,  $2205$  and  $2352$ .

(ii) Prove that if  $O_p(G) = \langle e \rangle$ , then Sylow  $p$ -subgroups  $P_1$  and  $P_2$  of  $G$  exist satisfying  $Z(P_1) \cap Z(P_2) = \langle e \rangle$ .

**Problem 6.26** (i) Suppose  $p$  is odd and it is the smallest prime dividing  $o(G)$ . Show that if  $p^3 \nmid o(G)$ , then  $G$  has a normal  $p$ -complement.

(ii) Suppose  $G$  is simple and it has an Abelian Sylow  $2$ -subgroup of order  $8$ , prove that  $7 \mid o(G)$ . The groups  $L_2(8)$  and  $J_1$  are examples (Chapter 12 including its Web section).

**Problem 6.27** (i) Show that the normal complement of the Sylow  $p$ -subgroup  $P$  given by Burnside's Theorem can be taken as  $O_{p'}(G)$  where  $p'$  denotes the set of primes dividing  $o(G)$  except  $p$  itself.

(ii) Prove that a Sylow  $2$ -subgroup of a finite simple group cannot be cyclic.

**Problem 6.28** Show that there are no simple groups with orders  $264$ ,  $945$  or  $3864$ .

**Problem 6.29** Prove that a group of order  $p^3q$  is not simple using the following method. First show that  $p < q$ , then use the Sylow theory and Burnside's Theorem (Theorem 6.23) to obtain  $n_q = p^2$ , and lastly deduce  $p = 2$  and  $q = 3$ . Note that  $n_p$  need not equal  $1$ , give an example.

**Problem 6.30** Suppose  $o(G) = p^2qr$  where  $p, q$  and  $r$  are distinct primes. Show that if  $G$  is simple, then  $G \simeq A_5$ . One method is as follows.

First show we may assume that  $p < q < r$ ;

If  $P$  is a Sylow  $p$ -subgroup, show that  $P \simeq C_p \times C_p$ , and  $[N_G(P) : C_G(P)]$  equals  $q$  or  $r$ ;

Deduce  $p = 2$  and  $q = 3$ , and so prove that  $G \simeq A_5$ .

**Problem 6.31** Find all groups of order 105, 210 and 474, see the table on page 294.

**Problem 6.32** Prove that no group of composite square-free order can be simple. Use this to show that if  $o(G)$  is square-free, and  $p^*$  is the largest prime factor of this order, then  $G$  has a normal Sylow  $p^*$ -subgroup.

**Problem 6.33** (i) Let  $p$  be the smallest prime dividing  $o(G)$ . Suppose  $P$  is a cyclic Sylow  $p$ -subgroup of  $G$ , show that  $G$  has a normal complement.

(ii) Use (i) to prove that if all of the Sylow  $p$ -subgroups of  $G$  are cyclic, then  $G$  is soluble (Chapter 11). Further show that if  $n \mid o(G)$ , then  $G$  has a subgroup of order  $n$ , and any two such subgroups are conjugate in  $G$ .

**Problem 6.34** Suppose  $G$  is a finite group with the property that for all of its Abelian subgroups  $J$  we have  $N_G(J) = C_G(J)$ . Show that  $G$  is Abelian.

**Problem 6.35** Suppose  $G$  is simple,  $2^r \mid o(G)$  and  $2^{r+1} \nmid o(G)$ . Show that if  $r = 1$  or  $2$ , then  $3 \mid o(G)$ . Note that for the only simple groups where  $3 \nmid o(G)$ , the Suzuki groups  $Sz(2^{2n+1})$ , we have  $r \geq 6$ .

**Problem 6.36** Let  $p$  be a prime. If  $p^2 \mid o(G)$ , show that  $p \mid o(\text{Aut } G)$ . (Hint. Use Corollary 5.27, Burnside's Theorem, and Theorems 7.12, 4.23 and 3.15.)

**Problem 6.37** Classify all groups of order  $pqr$  where  $p, q$  and  $r$  are primes and  $p < q < r$ . (Hint. Use Problem 6.32.)

**Problem 6.38** Suppose  $H$  be a Hall subgroup of  $G$  (Chapter 11) with the property

$$H \leq Z(N_G(H)).$$

Prove that  $G$  has normal  $p$ -complements for all primes  $p$  dividing  $o(H)$ . (Hint. Use induction. Prove first that if  $P$  is a Sylow subgroup of  $H$  and  $N_G(P) < G$ , then  $P \leq Z(N_G(P))$ . Secondly prove that if  $P \triangleleft G$  and  $Q$  is a Sylow subgroup of  $H$  which satisfies  $N_G(Q) < G$ , then  $P \leq Z(N_G(Q))$ .

## 7.5 — Infinite Abelian Groups

The printed text is mainly concerned with finite groups. Infinite groups like the rational numbers  $\mathbb{Q}$  have many important properties, and so some mention of them is needed. This **Web Section** lists the basic facts in the Abelian case, no proofs will be given; the reader who wishes to discover more should consult Kaplansky (1969), Fuchs (1970, 1973), Chapter 8 of Rose (1978), or Chapter 10 of Rotman (1994).

We begin by extending the notion of direct product to the case where an infinite number of factors is involved. There are two types which we call the *cartesian product* and the *direct product*. Suppose  $I = \{\dots, i_0, i_1, \dots\}$  is an index set and for each  $i_n \in I$  we are given a group  $G_{i_n}$ . As in the finite case we first form the set-theoretic cartesian product of the underlying sets of the groups  $G_{i_n}$ :

$$\mathbf{G} = \dots \times G_{i_0} \times G_{i_1} \times \dots,$$

we call the elements of  $\mathbf{G}$  ‘vectors’. Secondly we introduce an operation  $\odot$  on  $\mathbf{G}$  using the same procedure as in Definition 7.1.

**Definition 7.19** (i) If  $\mathbf{a} = (\dots, a_{i_0}, a_{i_1}, \dots)$  and  $\mathbf{b} = (\dots, b_{i_0}, b_{i_1}, \dots)$  are vectors in  $\mathbf{G}$ , then we define

$$\mathbf{a} \odot \mathbf{b} = (\dots, a_{i_0} b_{i_0}, a_{i_1} b_{i_1}, \dots), \quad (7.13)$$

where  $a_{i_n}, b_{i_n} \in G_{i_n}$  for all  $n$ . The collection of all vectors of  $\mathbf{G}$  with this operation  $\odot$  forms a group called the *cartesian product* which is denoted by

$$\bigotimes_{i_n \in I} G_{i_n}.$$

(ii) Let  $\mathbf{H}$  be the subset of  $\mathbf{G}$  of those vectors that have only a finite number of non-neutral entries. The set  $\mathbf{H}$  with the operation (7.13) forms a group called the *direct product* which is denoted by

$$\prod_{i_n \in I} G_{i_n}.$$

Note that

$$\prod_{i_n \in I} G_{i_n} \triangleleft \bigotimes_{i_n \in I} G_{i_n},$$

as the reader can easily check. The properties listed in Lemma 7.5 for finite direct products also apply to both the cartesian and the (infinite) direct product.

From now on all groups discussed in this section are Abelian.

Our first result concerns the extension of the Fundamental Theorem of Abelian Groups (Theorem 7.12) to the infinite case. A group is said to be *finitely generated* if it has a presentation (Section 3.4 and **Web Section 4.7**) with a finite number of generating elements. The Fundamental Theorem extends to this case for we have

**Theorem 7.20** *A finitely generated Abelian group can be expressed as a direct product of cyclic groups of prime power and/or infinite order.*

The proof of this result is similar to the second proof of the finite case given in Section 7.2.

### ***Divisibility***

Many infinite Abelian groups are not finitely generated, for instance the rational numbers  $\mathbb{Q}$  (Problem 3.17). But this group has another important property – it is *divisible*; that is for each positive integer  $m$  and each rational number  $a/b \in \mathbb{Q}$ , there exists another rational number  $c/d \in \mathbb{Q}$  with the property  $m(c/d) = a/b$  (put  $c = a$  and  $d = mb$ ). In the standard ‘multiplicative’ notation:

For all positive integers  $m$ , every element in  $\mathbb{Q}$  has an ‘ $m$ -th (additive) root’ in  $\mathbb{Q}$ .

With *torsion* to be defined below, divisibility plays a major role in the Abelian theory.

**Definition 7.21** An Abelian group  $G$ , with as usual its operation expressed multiplicatively using concatenation, is called *divisible* if for all  $g \in G$  and all positive integers  $m$ , there exists another element  $h \in G$  satisfying

$$h^m = g.$$

*Examples.* The following are divisible groups:  $\langle e \rangle$ ,  $\mathbb{Q}$  (as above),  $\mathbb{R}$ ,  $\mathbb{C}$  (in these two cases it is the additive group that is divisible), the multiplicative group of the non-zero complex numbers,<sup>7</sup> and  $C_{p^\infty}$  (Problem 6.7). A factor group of a divisible group is divisible, and if  $G_n, n = \dots, 0, 1, \dots$  is a collection of divisible groups, then both the cartesian and the direct products of the  $G_n$  are divisible. A subgroup of a divisible group need not be divisible; for example  $\mathbb{Z} \leq \mathbb{Q}$ , and  $\mathbb{Z}$  is not divisible.

Further we set

**Definition 7.22** (i) Given a group  $G$ , the subgroup generated by all elements of all divisible subgroups of  $G$  is denoted by  $dG$ , it is called the *divisible subgroup* of  $G$ .

(ii) A group  $G$  is called *reduced* if, and only if,  $dG = \langle e \rangle$ .

Clearly  $G$  is divisible if, and only if,  $dG = G$ . It is not difficult to prove that

**Theorem 7.23** *Every Abelian group  $G$  has the direct product decomposition*

$$G = dG \times R$$

where  $R$  is reduced.

---

<sup>7</sup> This follows because  $\mathbb{C}$  is an algebraically closed field.

**Corollary 7.24** *Every group is isomorphic to a subgroup of a divisible group.*

It is possible to give a characterisation of divisible groups as follows.

**Theorem 7.25** *Every divisible group can be expressed as a direct product of copies of  $\mathbb{Q}$ , and copies of  $C_{p^\infty}$  for suitably chosen primes  $p$ .*

The groups  $C_{p^\infty}$  for  $p = 2, 3, \dots$  were defined in Problem 6.7. One consequence of this theorem implies that the real numbers  $\mathbb{R}$  can be expressed as a direct product of copies of  $\mathbb{Q}$ , but uncountably many copies are needed. This is related to a topic in real analysis called the *Hamel Basis*; see for example *Introductory Real Analysis* by Kolmogorov and Fomin (Dover, New York, 1970). No similar characterisation of reduced groups exists, some are direct products of cyclic groups but many others are not. The next topic will provide some more information on this question.

## Torsion

The second major distinction in the Abelian theory is between *torsion* and *torsion-free* or; in our previous terminology, between finite and infinite order.

**Definition 7.26** (i) The *torsion subgroup*  $tG$  of a group  $G$  (with operation expressed multiplicatively using concatenation) is given by

$$tG = \{g \in G : g^m = e \text{ for some positive integer } m\}.$$

(ii) A group  $G$  is called *torsion* if  $tG = G$ , and *torsion-free* if  $tG = \langle e \rangle$ .

It is easy to prove that  $tG \leq G$  for all  $G$ . Every finite group is torsion,  $\mathbb{Q}$  is an example of a torsion-free group, whilst  $\mathbb{R}^*$ , the non-zero reals with multiplication, is neither torsion nor torsion-free; reader, why?

The following result is easily proved.

**Theorem 7.27** *For all Abelian groups  $G$ , the factor group  $G/tG$  is torsion-free.*

To put this another way: Every Abelian group is an extension of a torsion group by a torsion-free group. But this is not as strong as Theorem 7.23 for there exist groups whose torsion subgroups are not direct factors. One such example is the cartesian product over all primes  $p$  of the cyclic groups  $C_p$ .

Properties of both torsion and torsion-free groups have been investigated, a fairly clear characterisation of torsion groups has been given, but only limited information is available on the structure of torsion-free groups. In 1945 the Russian mathematician Kulikov proved

**Theorem 7.28** *Every Abelian torsion group  $G$  can be expressed as an extension of a direct product of cyclic groups by a divisible group.*

This result is derived using so called *basic subgroups*, we shall define these now. First we need (remember that  $G^n = \{g^n : g \in G\}$ )

**Definition 7.29** A subgroup  $J$  of a group  $G$  is called *pure* in  $G$  if

$$J \cap G^n = J^n \quad \text{for all } n \in \mathbb{Z}.$$

We always have  $J \cap G^n \geq J^n$ , so it is the reverse inequality that is important here. The following facts are not difficult to prove.

- (a) In a direct product  $G = H \times J$ , both  $H$  and  $J$  are pure in  $G$ .
- (b) If  $J \leq G$  and  $G/J$  is torsion-free, then  $J$  is pure in  $G$ . Hence the torsion subgroup  $tG$  of  $G$  is pure in  $G$ .
- (c) If  $J$  is pure in  $G$  and  $J \leq H \leq G$ , then  $H/J$  is pure in  $G/J$  if, and only if,  $H$  is pure in  $G$ .
- (d) A non-divisible  $p$ -group contains a pure non-neutral cyclic subgroup.
- (e) Suppose  $G$  is a  $p$ -group,  $X$  is an independent subset of  $G$  (Problem 7.14),  $\langle X \rangle$  is pure in  $G$ , and no proper superset of  $X$  has these properties (so  $X$  is a maximal pure-independent subset of  $G$ ), then  $G/\langle X \rangle$  is divisible.

We can now define ‘basic’ by

**Definition 7.30** A subgroup  $J$  of an Abelian torsion group  $G$  is called *basic* if the following three conditions hold.

- (i)  $J$  is a pure subgroup of  $G$ ,
- (ii)  $J$  is a direct product of cyclic groups,
- (iii) the factor group  $G/J$  is divisible.

Using Problem 7.14 and the properties (a) to (e) above it is relatively easy to prove that all torsion groups possess basic subgroups and, using this, Kulikov’s Theorem (Theorem 7.28) follows directly.

There are two important corollaries.

**Corollary 7.31** (i) *If  $G$  has finite exponent (Definition 2.19), then  $G$  is isomorphic to a direct product of cyclic groups.*

(ii) *If  $G$  is indecomposable, that is it cannot be expressed as a direct product with non-neutral factors, then  $G$  is either torsion or torsion-free.*

The first of these corollaries shows that an elementary Abelian  $p$ -group (Problem 4.18) can be represented as a direct product of copies of  $C_p$  and, by Corollary 2.12, all groups with exponent 2 have this property. The rational group  $\mathbb{Q}$  is an example of an indecomposable group, it is torsion-free. But  $\mathbb{R}^*$  is an example of a group which is neither torsion nor torsion-free, so by the second corollary it can be expressed as a direct product, in this case the factors are isomorphic to  $\mathbb{R}^+$  and  $C_2$ .

Lastly in this brief survey we shall consider one aspect of the theory of torsion-free groups. Every torsion-free group can be treated as a subgroup of the multiplicative group of a vector space over  $\mathbb{Q}$ , see Corollary 7.24. Hence we make the following

**Definition 7.32** For a torsion-free group  $G$ , the *rank* is the number of elements in a maximal independent subset (Problem 7.14) of the vector space over  $\mathbb{Q}$  of which  $G$  is a subgroup.

There are many unanswered questions about rank  $n$  groups for large  $n$ , but the case  $n = 1$  is well known. In this case it is the subgroups of  $\mathbb{Q}$  that are being investigated. We noted in Problem 2.11(ii) that the following are subgroups of  $\mathbb{Q}$ :

- (i)  $\mathbb{Z}$ ,
- (ii) the set of all rational numbers of the form  $a/2^n$  where  $a, n \in \mathbb{Z}$ ,  $a$  is odd and  $n \geq 0$ , the so-called *dyadic rationals*,
- (iii) the set of all rational numbers with square-free denominators.

Many variations on these examples exist hence we make the following

**Definition 7.33** If  $a/b \in \mathbb{Q} \setminus \{0\}$  with  $(a, b) = 1$ ,  $p$  is a prime,  $a = p^r a'$ ,  $b = p^s b'$  and  $(a', p) = (b', p) = 1$ , then the  $p$ -height  $h_p(a/b)$  of  $a/b$  equals  $s - r$ ; and we set  $h_p(0) = 0$ .

So the  $p$ -height of an integer is less than or equal to zero, the 2-height of the dyadic rational  $a/2^n$  is  $n$ , and the  $p$ -height of a rational with a square-free denominator is at most 1.

We also make

**Definition 7.34** (i) A sequence  $(a_0, a_1, \dots)$  where each  $a_i$  denotes a non-negative integer or the symbol  $\infty$  is called a *characteristic*.

- (ii) Two characteristics are said to be *equivalent* if
  - (a) the symbol  $\infty$  occurs in the same position in each characteristic, and
  - (b) the finite entries differ (that is they are replaced by other finite entries) at only finite many positions.

It is clear that Definition 7.34 defines an equivalence relation on the set of characteristics. We can attach a characteristic to each subgroup of  $\mathbb{Q}$  as follows. If  $H \leq \mathbb{Q}$ , let  $h_p(H)$  denote the least upper bound (which may be  $\infty$ ) of  $h_p(a/b)$  for  $a/b \in H$ , then the characteristic of  $H$  is defined as

$$(h_2(H), h_3(H), \dots, h_{p_i}(H), \dots).$$

For the group  $\mathbb{Q}$  itself the characteristic is  $(\infty, \infty, \dots)$  because the numbers  $1/p^n$  belong to  $\mathbb{Q}$  for all primes  $p$  and all positive integers  $n$ . Also the characteristic of  $\mathbb{Z}$  is  $(0, 0, 0, \dots)$ , the characteristic of the dyadic rationals is  $(\infty, 0, 0, \dots)$ , and the characteristic of the rationals with square-free denominators is  $(1, 1, 1, \dots)$ ; the reader should check these statements. It is easily shown that the characteristic of two elements of a subgroup  $H$  of  $\mathbb{Q}$  are equivalent. For instance in  $\mathbb{Z}$  the characteristic of 0 is  $(0, 0, 0, \dots)$  whilst the characteristic of 432, say, is  $(-4, -3, 0, 0, \dots)$ .

For the rank 1 case we have

**Theorem 7.35** (i) *Two subgroups of  $\mathbb{Q}$  are isomorphic if, and only if, they have equivalent characteristics.*

(ii) *For each equivalence class of characteristics there exists a subgroup of  $\mathbb{Q}$  with a characteristic in this class.*

It follows from this result that the group  $\mathbb{Q}$  has uncountably many subgroups as there are uncountably many inequivalent characteristics. As an exercise write down as many subgroups of  $\mathbb{Q}$  as you can.

For further developments, proofs of the theorems given above, examples, and problems the reader should read one or more of the references given at the beginning of this section.



## 9.4W Schur-Zassenhaus Theorem

In this **Web Section** we establish one of the most important theorems of finite group theory — the Schur-Zassenhaus Theorem which gives a condition under which complements of Hall subgroups exist. A *Hall subgroup*  $H$  of a finite group  $G$ , is one whose order has no common factor (except 1) with its index, that is

$$(o(H), [G : H]) = 1.$$

Sylow subgroups are examples of Hall subgroups, also  $S_4$  is isomorphic to a Hall subgroup of  $S_5$  for we have  $o(S_4) = 24$  and  $[S_5 : S_4] = 5$ . We shall consider these subgroups in more detail in Chapter 11. The Schur-Zassenhaus Theorem says that if  $H$  is a normal Hall subgroup of  $G$ , then  $H$  always has at least one complement in  $G$ , see Definition 6.19, and secondly, all such subgroups are conjugate. For example, it shows that if  $P$  is a normal Sylow subgroup of  $G$ , then  $P$  has a complement  $J$  and  $G = PJ$ . The normality condition is essential as the following example shows. Let  $G = A_5$  and  $J = \langle (1, 2, 3) \rangle \simeq C_3$ , then  $o(J) = 3$ ,  $[G : J] = 20$  and  $(20, 3) = 1$ , but  $A_5$  does not contain a subgroup of order 20, and so no complement of  $J$  can exist.

The main point to note here is that if  $G$  has a *normal* Hall subgroup  $K$ , then  $G$  is isomorphic to a semi-direct product of  $K$  by a subgroup isomorphic to  $G/K$ ; we sometimes say that  $G$  is *split* over  $K$ . In this case the extension which passes from  $K$  to  $G$  is of a fairly straightforward and well-understood type; the situation can become much more complicated if  $o(K)$  and  $o(G/K)$  have common factors. The theorem was proved by Schur about a century ago in the case when  $G/K$  is cyclic, and the full result was proved by Zassenhaus in 1937 using some ideas from cohomology theory for the Abelian case which we shall introduce in the latter part of the proof. We also give a second proof of this case using so-called *crossed homomorphisms*.

**Theorem 9.19** (Schur-Zassenhaus Theorem) *Suppose  $G$  is a finite group,  $o(G) = mn$ ,  $(m, n) = 1$ ,  $K \triangleleft G$  and  $o(K) = m$ , then  $K$  has a complement  $H$  in  $G$  with  $G = KH$  and  $o(H) = n$ .*

The derivation of this result is quite long and introduces some new notions, it has been split into a number of manageable stages and relies on many of the results proved earlier. As noted above we give two proofs for the main Abelian case.

*Proof.* **Stage 1** – It is sufficient to show  $G$  has a subgroup  $H$  that has order  $n$ .

We have  $K \triangleleft G$  and  $o(K) = m$ . If  $H$  exists with  $o(H) = n$  then, by Lagrange's Theorem (Theorem 2.27)  $K \cap H = \langle e \rangle$  (no non-neutral element in  $K$  has an order dividing  $n$ , and vice versa), and so by Theorem 5.8,  $o(KH) = o(H)o(K) = o(G)$  which shows that  $KH = G$ .

The main proof is by induction on  $o(G)$ , so if  $o(G_1) < o(G)$  and  $G_1$  has a normal Hall subgroup  $K_1$ , then  $K_1$  has a complement in  $G_1$ .

*Stage 2* – We may assume that  $K$  has a normal Sylow subgroup  $P$ .

Suppose  $P$  is a Sylow subgroup of  $K$  (Theorem 6.7). As  $K \triangleleft G$ , the Frattini Argument (Lemma 6.14) shows that  $G = N_G(P)K$ . Also by Problem 5.13(iii) and the normality of  $K$  we have

$$N_K(P) = N_G(P) \cap K \triangleleft N_G(P),$$

and so by the Second Isomorphism Theorem (Theorem 4.15),

$$G/K = N_G(P)K/K \simeq N_G(P)/(N_G(P) \cap K) = N_G(P)/N_K(P).$$

By hypothesis this shows that  $[N_G(P) : N_K(P)] = n$ . Further, as  $N_K(P) \leq K$  we have  $o(N_K(P)) \mid o(K)$ . These two statements imply that  $N_K(P)$  is a normal Hall subgroup of  $N_G(P)$ . Now if  $N_G(P) < G$ , the inductive hypothesis provides a subgroup  $J$  of  $N_G(P)$  with  $o(J) = n$ , and by subgroup transitivity,  $J$  is also a subgroup of  $G$  of order  $n$ . The result follows in this case, and so we may assume that  $N_G(P) = G$ , that is  $P \triangleleft G$ .

*Stage 3* – We may assume that  $K$  is a Sylow subgroup  $P$ .

By Stage 2 we may suppose  $P \triangleleft G$ . As  $K \triangleleft G$ , the Correspondence Theorem (Theorem 4.16) gives  $K/P \triangleleft G/P$ , and so  $[G/P : K/P] = [G : K] = n$ . Now  $o(K/P) \mid o(K)$  by Lagrange's Theorem (Theorem 2.27), and  $o(G/P) < o(G)$ , hence the inductive hypothesis again provides a subgroup of the form  $L/P$  with order  $n$  and where  $P \triangleleft L \leq G$  (note we are assuming that  $P \triangleleft G$ ). Now  $L \cap K$  is a subgroup of both  $L$  and  $K$ , and so  $o(L \cap K)$  divides both  $o(L)$  and  $o(K)$ . But

$$o(L) = n \cdot o(P) \quad \text{and} \quad (n, o(K)) = 1, \quad \text{hence} \quad o(L \cap K) \leq o(P).$$

On the other hand,  $P \leq L$  and  $P \leq K$ , and so  $P \leq L \cap K$ . Together these show that  $L \cap K = P$  which in turn gives  $L < G$ . Hence as  $o(P)$  and  $o(L/P)$  are coprime and  $o(L/P) = n$ , the inductive hypothesis provides a subgroup of  $L$  with order  $n$  which is also a subgroup of  $G$ . Therefore we may assume that  $K = P$ .

*Stage 4* – The case when  $K$  is a non-Abelian  $p$ -group.

By Lemma 5.21,  $\langle e \rangle \neq Z(K) \triangleleft K$ , and by Problem 4.16,  $Z(K) \triangleleft G$ . Further by the Correspondence Theorem (Theorem 4.16),  $K/Z(K)$  is a normal subgroup of  $G/Z(K)$  with order  $n$ . Therefore the inductive hypothesis provides a subgroup of the form

$$M/Z(K) \text{ of } G/Z(K) \text{ with order } n, \text{ and where } Z(K) \triangleleft M \leq G.$$

As in Stage 3, we have  $M \cap K = Z(K)$ , the reader should check this, and so  $M < G$ . Also  $o(Z(K))$  and  $o(M/Z(K))$  are coprime, and  $o(M/Z(K)) = n$ , hence using the inductive hypothesis again we see that  $M$  has a subgroup of order  $n$ , and so this is also true for  $G$ .

Therefore we may assume that  $K$  is Abelian.

### Stage 5 – The case when $K$ is Abelian

For this main part of the derivation we shall give two proofs. In some ways they are fairly similar, but they introduce distinct new ideas – the *cocycle identity* and the *crossed homomorphism* – and so it seems worthwhile to give both. In some ways the second is more ‘in line’ with the rest of the work in the book and this web section.

#### First proof in the Abelian case

The group  $K$  is a  $p$ -group but this fact will play no role in what follows. To aid clarity we have reintroduced the dot notation “ $\cdot$ ” when referring to the group operation in the Abelian subgroup  $K$ .

##### Stage 5.1 – Cocycle identity.

In this stage we define a new action and derive one of its properties called the *cocycle identity*, for a similar identity see Lemma 9.12. Let  $C = G/K$  and let  $\mathbf{c} \in C$ , so  $\mathbf{c}$  is a coset of  $K$  in  $G$ . (Note that here we are not following our usual convention where we use upper case letters for sets.) If  $g, g' \in \mathbf{c}$ , then by Lemma 2.22,  $g^{-1}g' \in K$ , and so  $gkg^{-1} = g'k(g')^{-1}$  for all  $k \in K$  as  $K$  is Abelian in this Stage. Hence we can define an action of  $C$  on  $K$  by

$$k \backslash \mathbf{c} = gkg^{-1} \quad \text{for } k \in K, \quad \mathbf{c} \in C = G/K, \quad \text{and } g \in \mathbf{c}. \quad (9.16)$$

This action has two further properties which the reader should check:

$$(kk') \backslash \mathbf{c} = k \backslash \mathbf{c} \cdot k' \backslash \mathbf{c} \quad \text{and} \quad (k^{-1}) \backslash \mathbf{c} = (k \backslash \mathbf{c})^{-1}. \quad (9.17)$$

Choose a transversal  $T = \{t_{\mathbf{c}} : \mathbf{c} \in C\}$  for  $C$ , see Web Section 4.6. So  $o(T) = n$  and  $t_{\mathbf{c}}$  is a representative in  $G$  of the coset  $\mathbf{c}$  in  $C$ . Using basic coset and transversal properties we have

$$t_{\mathbf{c}_1\mathbf{c}_2}^{-1}K = (t_{\mathbf{c}_1\mathbf{c}_2}K)^{-1} = (\mathbf{c}_1\mathbf{c}_2)^{-1} = \mathbf{c}_2^{-1}\mathbf{c}_1^{-1} = (t_{\mathbf{c}_1}t_{\mathbf{c}_2})^{-1}K,$$

where  $\mathbf{c}_1$  and  $\mathbf{c}_2$  are cosets of  $C = G/K$ . By Lemma 2.22 this gives

$$t_{\mathbf{c}_1}t_{\mathbf{c}_2}t_{\mathbf{c}_1\mathbf{c}_2}^{-1} \in K.$$

Hence we can define a function  $\theta : C \times C \rightarrow K$  by

$$t_{\mathbf{c}_1}t_{\mathbf{c}_2} = (\mathbf{c}_1, \mathbf{c}_2)\theta t_{\mathbf{c}_1\mathbf{c}_2}. \quad (9.18)$$

Now using (9.16) and (9.18) we obtain

$$\begin{aligned} t_{\mathbf{c}_1}(t_{\mathbf{c}_2}t_{\mathbf{c}_3}) &= t_{\mathbf{c}_1}(\mathbf{c}_2, \mathbf{c}_3)\theta t_{\mathbf{c}_2\mathbf{c}_3} = t_{\mathbf{c}_1}(\mathbf{c}_2, \mathbf{c}_3)\theta t_{\mathbf{c}_1}^{-1}t_{\mathbf{c}_1}t_{\mathbf{c}_2\mathbf{c}_3} \\ &= ((\mathbf{c}_2, \mathbf{c}_3)\theta \backslash \mathbf{c}_1) \cdot (\mathbf{c}_1, \mathbf{c}_2\mathbf{c}_3)\theta \cdot t_{\mathbf{c}_1\mathbf{c}_2\mathbf{c}_3}, \end{aligned}$$

and

$$(t_{\mathbf{c}_1}t_{\mathbf{c}_2})t_{\mathbf{c}_3} = (\mathbf{c}_1, \mathbf{c}_2)\theta t_{\mathbf{c}_1\mathbf{c}_2}t_{\mathbf{c}_3} = (\mathbf{c}_1, \mathbf{c}_2)\theta \cdot (\mathbf{c}_1\mathbf{c}_2, \mathbf{c}_3)\theta \cdot t_{\mathbf{c}_1\mathbf{c}_2\mathbf{c}_3}.$$

Combining these equations and using associativity we obtain the so-called *cocycle identity*

$$(\mathbf{c}_2, \mathbf{c}_3)\theta \backslash \mathbf{c}_1 \cdot (\mathbf{c}_1, \mathbf{c}_2\mathbf{c}_3)\theta = (\mathbf{c}_1, \mathbf{c}_2)\theta \cdot (\mathbf{c}_1\mathbf{c}_2, \mathbf{c}_3)\theta, \quad (9.19)$$

which holds for all  $\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3 \in C$ .

*Stage 5.2* – An extension of the cocycle identity, see (9.21) below.

First we define a map  $\psi : C \rightarrow K$  by

$$\mathbf{d}\psi = \prod_{\mathbf{c} \in C} (\mathbf{d}, \mathbf{c})\theta,$$

for  $\mathbf{d} \in C$ . Working in the Abelian group  $K$  we have, where  $n = o(C)$ ,

$$\begin{aligned} ((\mathbf{c}_1, \mathbf{c}_2)\theta)^n \cdot \mathbf{c}_1\mathbf{c}_2\psi &= \prod_{\mathbf{c}_3 \in C} \left( (\mathbf{c}_1, \mathbf{c}_2)\theta \cdot (\mathbf{c}_1\mathbf{c}_2, \mathbf{c}_3)\theta \right) \\ &= \prod_{\mathbf{c}_3 \in C} \left( ((\mathbf{c}_2, \mathbf{c}_3)\theta) \backslash \mathbf{c}_1 \cdot (\mathbf{c}_1, \mathbf{c}_2\mathbf{c}_3)\theta \right) \\ &\quad \text{using the cocycle identity (9.19)} \\ &= \left( \prod_{\mathbf{c} \in C} (\mathbf{c}_2, \mathbf{c})\theta \right) \backslash \mathbf{c}_1 \cdot \prod_{\mathbf{c} \in C} (\mathbf{c}_1, \mathbf{c})\theta \\ &= (\mathbf{c}_2\psi) \backslash \mathbf{c}_1 \cdot \mathbf{c}_1\psi \end{aligned} \quad (9.20)$$

using (9.17) and Theorem 2.8 in the penultimate line, and the definition of  $\psi$  in the last line.

As  $K$  is Abelian and  $(n, o(K)) = 1$ , the  $n$ -th power map:  $k \rightarrow k^n$  for  $k \in K$  is an automorphism of  $K$  (Use the fact that if  $0 \leq r < n$ , then there exists, by the Euclidean Algorithm and GCD condition, an integer  $s$  with the property  $sn \equiv r \pmod{o(K)}$ ).). Hence as the inverse of an automorphism is also an automorphism, the  $n$ -th root map on  $K$ :  $k \rightarrow k^{1/n}$  is again an automorphism of  $K$  as also is the map on  $K$  sending  $k$  to  $k^{-1/n}$ . Therefore, if we define  $\xi : C \rightarrow K$  by

$$\mathbf{c}\xi = (\mathbf{c}\psi)^{-1/n} \quad \text{for } \mathbf{c} \in C,$$

we have, by (9.20) and as  $K$  is Abelian,

$$(\mathbf{c}_1\mathbf{c}_2)\xi = \mathbf{c}_1\xi \cdot (\mathbf{c}_2\xi) \backslash \mathbf{c}_1 \cdot (\mathbf{c}_1, \mathbf{c}_2)\theta \quad (9.21)$$

our extension of the cocycle identity.

*Stage 5.3* – Completion of the argument.

First, using (9.21) we define an injective homomorphism from  $C$  to  $G$ , its image will be the required subgroup of  $G$ . By (9.21) we have

$$\begin{aligned} (\mathbf{c}_1\mathbf{c}_2)\xi t_{\mathbf{c}_1\mathbf{c}_2} &= \mathbf{c}_1\xi \cdot (\mathbf{c}_2\xi) \backslash \mathbf{c}_1 \cdot (\mathbf{c}_1, \mathbf{c}_2)\theta t_{\mathbf{c}_1\mathbf{c}_2} \\ &= \mathbf{c}_1\xi \cdot t_{\mathbf{c}_1}\mathbf{c}_2\xi t_{\mathbf{c}_1}^{-1} \cdot t_{\mathbf{c}_1}t_{\mathbf{c}_2} \\ &\quad \text{by (9.16) and (9.18)} \\ &= \mathbf{c}_1\xi t_{\mathbf{c}_1} \cdot \mathbf{c}_2\xi t_{\mathbf{c}_2}. \end{aligned}$$

Therefore if we define  $\nu : C \rightarrow G$  by

$$\mathbf{c}\nu = \mathbf{c}\xi t_{\mathbf{c}} \quad \text{for } \mathbf{c} \in C \quad \text{and} \quad t_{\mathbf{c}} \in T,$$

the calculation above shows that  $\nu$  is a homomorphism from  $C$  to  $G$ . This homomorphism is injective by definition of the transversal, for if  $\mathbf{c} \in C$  and  $\mathbf{c} \neq e$ , then  $t_{\mathbf{c}} \notin K$ , and so  $\mathbf{c}\xi t_{\mathbf{c}} \neq e$  which shows that  $\ker \nu = \langle e \rangle$ . Finally as  $o(C) = o(G/K) = n$ , we see that  $\text{im } \nu$  is a subgroup of  $G$  of order  $n$  as required.  $\square$

### Second proof in the Abelian case

We begin by introducing crossed homomorphisms.

**Definition 9.20** (i) Let  $K \triangleleft G$ . A mapping  $\theta : G \rightarrow K$  is called a *crossed homomorphism*  $G$  to  $K$  if

$$(ab)\theta = b^{-1}(a\theta)b(b\theta) \quad \text{for all } a, b \in G. \quad (9.22)$$

(ii) The kernel of  $\theta$ ,  $\ker \theta$ , equals  $\{a \in G : a\theta = e\}$ .

By definition,  $a\theta \in K$  for all  $a \in G$ , so in examples this fact needs to be checked. Clearly if  $G$  is Abelian then a crossed homomorphism is just a homomorphism. A more informative example is as follows. Choose a fixed  $b \in K$  and define  $\theta_b$  by

$$a\theta_b = [a, b] \quad \text{for all } a \in G.$$

Clearly  $a\theta_b \in K$  as  $K$  is normal in  $G$ , and it is easily checked that  $[aa', b] = a'^{-1}[a, b]a'[a', b]$ , and so  $\theta_b$  is an example of a crossed homomorphism; its kernel equals  $C_G(b)$ , a subgroup of  $G$ . In the next lemma we show that the kernel of a general crossed homomorphism is always a subgroup of  $G$ , it is usually not normal.

**Lemma 9.21** Suppose  $K \triangleleft G$  and  $\theta$  is a crossed homomorphism  $G$  to  $K$ .

- (i)  $e\theta = e$ .
- (ii)  $\ker \theta \leq G$ .
- (iii) For  $a, b \in G$ , we have  $a\theta = b\theta$  if, and only if,  $Ka = Kb$ .
- (iv)  $o(G\theta) = [G : K]$  where as usual  $G\theta = \{g\theta : g \in G\}$ .

*Proof.* We shall derive (ii) and leave the remaining parts as an exercise for the reader, see Problem 9.16. By (i)  $\ker \theta$  is not empty. Secondly if  $j \in \ker \theta$ , then by (i)

$$e = e\theta = (jj^{-1})\theta = j(j\theta)j^{-1}(j^{-1}\theta) = j^{-1}\theta,$$

and so we also have  $j^{-1} \in \ker \theta$ . (Note, by definition  $j\theta \in K$  and  $K \triangleleft G$ .) Similarly by (9.22) we have  $(ab)\theta \in \ker \theta$  provided  $a\theta, b\theta \in \ker \theta$ , and (ii) follows by Theorem 2.13.  $\square$

We shall now construct a new crossed homomorphism using transversals; see Definition 4.24 on Web page 331. Note that we also used transversals in the first proof of the Schur-Zassenhaus Theorem. Suppose  $K$  is a normal Abelian subgroup of the finite group  $G$ . Let  $\mathcal{T}$  denote the collection of all transversals of  $K$  in  $G$ , as  $K$  is Abelian left and right transversals are identical. For  $a, b \in G$  we write  $a \approx b$  if, and only if,  $a$  and  $b$  belong to the same coset of  $K$  in  $G$ . So as  $K$  is both normal and Abelian

$$a \approx b \text{ if and only if } Ka = Kb \text{ if and only if } aK = bK.$$

If  $T_1, T_2 \in \mathcal{T}$ , then the relation  $\approx$  defined above is a bijection between  $T_1$  and  $T_2$ . We define a mapping  $\chi : G \rightarrow K$  by

$$(T_1, T_2)\chi = \prod^* a^{-1}b$$

where the product  $\prod^*$  is taken over all pairs of elements  $\{a, b\}$  in  $G$  such that  $a \in T_1$ ,  $b \in T_2$  and  $a \approx b$ . As  $K$  is Abelian, the mapping  $\chi$  is well-defined because in this case the order of the terms in the product is immaterial.

*Example.* Let  $G = D_4 = \langle g, h \mid g^4 = h^2 = (gh)^2 = e \rangle$  and  $H = \langle g^2 \rangle \triangleleft G$ . The cosets are  $\{e, g^2\}, \{g, g^3\}, \{h, g^2h\}, \{gh, g^3h\}$ , and two of the possible 16 transversals are

$$T_1 = \{e, g, h, gh\} \quad \text{and} \quad T_2 = \{g^2, g^3, g^2h, gh\}.$$

Here we have  $e \approx g^2$ ,  $g \approx g^3$ ,  $h \approx g^2h$  and  $gh \approx gh$ , and so

$$(T_1, T_2)\chi = g^2 \cdot g^2 \cdot hg^2h \cdot e = g^2.$$

We also have  $T_2h = \{g^2h, g^3h, g^2, g\}$ , and  $(T_2, T_2h)\chi = e \cdot g^2 \cdot e \cdot g^2 = e = h^4$ ; see the lemma below.

**Lemma 9.22** *Suppose  $G$  is finite,  $K$  is a normal Abelian subgroup of  $G$ , and  $T, T_i$ ,  $i = 1, 2, 3$ , are transversals of  $K$  in  $G$ .*

- (i)  $(T_1, T_2)\chi(T_2, T_3)\chi = (T_1, T_3)\chi$ .
- (ii) If  $a \in G$ , then  $(T_1a, T_2a)\chi = a^{-1}(T_1, T_2)\chi a$ .
- (iii) For  $a \in K$  we have  $(T, Ta)\chi = a^{[G:K]}$ .

*Proof.* Straightforward using Lemma 9.21. For example in (i) note that  $(a^{-1}b)(b^{-1}c) = a^{-1}c$ . And for (iii) if  $k \in K$  then  $aK = akK$ , and so  $a \approx ak$ . The reader should fill in the details.  $\square$

We can now give the second proof of the Abelian case of the Schur-Zassenhaus Theorem.

*Second proof of the Abelian case.* Let  $T$  be some transversal of  $K$  in  $G$ . Define a map  $\theta : G \rightarrow K$  by

$$a\theta = (T, Ta)\chi \quad \text{for } a \in G. \quad (9.23)$$

By Lemma 9.22(iii),  $\theta$  is a map from  $G$  into  $K$ . It is also a crossed homomorphism, for by Lemma 9.22 again

$$\begin{aligned}(ab)\theta &= (T, Tab)\chi = (T, Tb)\chi(Tb, Tab)\chi \\ &= (T, Tb)\chi b^{-1}(T, Ta)b = b^{-1}(a\theta)b(b\theta),\end{aligned}$$

as  $K$  is Abelian. Further by Lemma 9.22(iii), if  $c \in K$ , then

$$c\theta = (T, Tc)\chi = c^{[G:K]}.$$

But by hypothesis,  $[G : K]$  and  $o(K)$  are coprime, and so there exists an integer  $r$  satisfying  $r[G : K] \equiv 1 \pmod{o(K)}$ . This implies that the map defined by

$$c \rightarrow c^r$$

is the inverse of  $\theta$ . Hence  $\theta$  is surjective, and so  $G\theta = K$ . Now let  $J = \ker \theta$ , by Lemma 9.21(ii)  $J \leq G$ . We also have  $o(K) = o(G\theta) = [G : K]$  by Lemma 9.21(iv). This gives

$$o(J)o(K) = o(G) \quad \text{and} \quad o(J) = [G : K].$$

Therefore  $J$  is the required complement subgroup and the theorem is proved.  $\square$

The reader should note the similarities and differences between these two proofs of the Abelian case.

As we commented above this result can be extended as follows.

**Theorem 9.23** *If  $K$  is a Hall normal subgroup of  $G$  and if at least one of  $K$  and  $G/K$  is soluble, then all conjugates of  $K$  in  $G$ , that is all subgroups proved to exist by Theorem 9.19, are conjugate in  $G$ .*

*Notes.* (a) Note the comparison with the Sylow theory, Theorem 6.9.

(b) The solubility condition can be removed using the Feit-Thompson Odd Order Theorem. This result states that all groups of odd order are soluble, and we cannot have both  $o(K)$  and  $o(G/K)$  divisible by 2 when  $K$  is a Hall subgroup.

(c) A proof in the Abelian case of Theorem 9.23 is given in Problem 9.19, and a proof in the general case can be found in Issacs [2008], page 82, or Scott [1964], Chapter 9.

Gaschütz proved the following related result.

**Theorem 9.24** *If  $K$  is a Abelian normal subgroup of a finite group  $G$ , the the following statements are equivalent.*

- (a)  $K$  has a complement in  $G$ ,
- (b) If  $P$  is a Sylow subgroup of  $G$ , then  $K \cap P$  has a complement in  $P$ .

A proof is given in Problem 9.26. This result may be false if  $K$  is not Abelian, see page 225 in the third reference below.

More details concerning these results can be found in Scott [1964] Chapter 9, Rose [1978] Chapter 10, Rotman [1994] Chapter 7, and Issacs [2008] Chapter 3.

## 9.5 Problems 9W

**Problem 9.16** Give proofs of the remaining parts of Lemma 9.21 and of the three parts of Lemma 9.22.

**Problem 9.17** (i) Let  $F$  be a finite field whose characteristic is not equal to 2, and let  $G$  be the group of  $3 \times 3$  matrices of the form

$$\begin{pmatrix} A & O \\ v & 1 \end{pmatrix} = M$$

where  $A \in GL_2(F)$ ,  $v$  is a element of the 2-dimensional vector space over  $F$ , and  $O$  is the 2-dimensional zero column vector. Further let  $J$  be the subgroup of  $G$  consisting of those matrices whose submatrix  $A$  in the definition above has the form  $\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}$ , and let  $H$  be the subgroup of  $J$  of those matrices with  $c = 0$ .

(i) Show that  $H \triangleleft G$ .

(ii) Prove that  $G$  is isomorphic to a semi-direct product of  $H$  by  $GL_2(F)$ .

(iii) Further prove that  $J$  possesses a complement of  $H$  which is not contained in any complement of  $H$  in  $G$ . This result is false if  $o(F) = 2$ . (Hint. Show that if  $L \leq J$ ,  $J = HL$ ,  $H \cap L = \langle e \rangle$  and  $L$  is contained in a complement of  $H$  in  $G$ , then  $C_G(L)$  contains an element of order 2.)

**Problem 9.18** Suppose  $p > q$ . Show that every group of order  $p^2q$  has a normal Sylow  $p$ -subgroup, and classify all such groups.

**Problem 9.19** Prove Theorem 9.23 in the Abelian case using the following method based on the second proof of the Abelian case of the Schur-Zassenhaus Theorem (Theorem 9.19).

Method. Let  $H$  be a complement of  $K$  in  $G$ , then  $H$  is a transversal for  $K$ , and let  $c = (H, T)\chi \in K$ . By Theorem 9.22(iii) and as  $\theta$  is surjective, find  $d \in K$  to satisfy:  $d\theta = c$ . Now show that  $d^{-1}Hd$  is the required complement. To do this we will need to show that  $(d^{-1}hd)\theta = h^{-1}ch \cdot h\theta \cdot c$  which gives  $(d^{-1}hd)\theta = e$ .

**Problem 9.20** Suppose  $K \triangleleft G$ ,  $(o(K), [G; K]) = 1$ ,  $J \leq G$ ,  $o(J) \mid [G : K]$  and either  $J$  or  $K$  is soluble. Prove that  $J$  is contained in a complement of  $K$  in  $G$ .

**Problem 9.21** Let  $P$  be a Sylow  $p$ -subgroup of  $G$  which is contained in  $Z(G)$ , and let the set of elements of  $G$  whose orders are not divisible by  $p$  be denoted by  $C$ . Show that  $C$  is a subgroup of  $G$ , and  $G \simeq C \times P$ .



**Problem 9.22** Suppose  $K \triangleleft G$ ,  $[G : K] = m$ ,  $K$  is Abelian, and all elements of  $K$  can be uniquely expressed as  $m$ -powers. Prove that  $K$  has a complement in  $G$ .

**Problem 9.23** Suppose  $K_1$  and  $K_2$  are normal subgroups of  $G$ . Show that if, for  $i = 1, 2$ ,  $K_i$  has a complement  $H_i$  in  $G$ , and  $K_2 \leq H_1$ , then  $K_1 K_2$  also has a complement in  $G$ .

**Problem 9.24** Give an example of a group  $G$  with a normal subgroup  $K$  with the following properties. (a)  $G$  can be expressed as a semi-direct product over  $K$  and (b) the conjugates of  $K$  do not form a single conjugacy class.

**Problem 9.25** Suppose  $G$  is a soluble group,  $K \triangleleft G$ , and  $H$  is a Hall subgroup of  $K$ . Show that  $G \simeq K N_G(H)$ .

**Problem 9.26** (i) Suppose  $K \triangleleft G$  and  $H$  is a Sylow  $p$ -subgroup of  $G$ . Show that  $H \cap K$  is a Sylow  $p$ -subgroup of  $K$ .

(ii) Give a proof of Gaschütz's result Theorem 9.24 using the following method.

(a) implies (b). By (i)  $P \cap K$  is a Sylow  $p$ -subgroup of  $K$ , also as  $K$  is Abelian, there exists  $L \leq K$  with the property:  $K = (K \cap P)L$ , and by (a) there exists  $J \leq G$  with the properties:  $G = JK$  and  $J \cap K = \langle e \rangle$ . Now use Problem 2.18 to show that  $JL$  is the required complement in  $P$ .

(b) implies (a). As usual let  $G_p$  denote the subgroup of the  $p$ -elements of  $G$ . If  $p \mid o(G)$ , then  $K_p \triangleleft G$  and  $K_p \leq P_p$ . By (b)  $K_p$  has a complement in  $P_p$ , and by the Schur-Zassenhaus Theorem (Theorem 9.19)  $K_p$  has a complement  $M_p$  in  $G$ . Let  $M = \bigcap_p M_p$ . Now use Problem 2.15 and Theorem 5.8 to complete the proof.

**Problem 9.27** Let  $G$  be a soluble group, and let  $H$  be a proper subgroup of  $G$  with smallest possible index. Prove that  $H \triangleleft G$ , a result due to Berkovich.

## 12.6 Further Topics on Simple Groups

This Web Section has three parts (a), (b) and (c). Part (a) gives a brief descriptions of the 56 (isomorphism classes of) simple groups of order less than  $10^6$ , part (b) provides a second proof of the simplicity of the linear groups  $L_n(q)$ , and part (c) discusses an ingenious method for constructing a version of the Steiner system  $S(5, 6, 12)$  from which several versions of  $S(4, 5, 11)$ , the system for  $M_{11}$ , can be computed.

### 12.6(a) Simple Groups of Order less than $10^6$

The table below and the notes on the following five pages lists the basic facts concerning the non-Abelian simple groups of order less than  $10^6$ . Further details are given in the ATLAS (1985), note that some of the most interesting and important groups, for example the Mathieu group  $M_{24}$ , have orders in excess of  $10^8$  and in many cases considerably more.

Simple group	Order	Prime factor count	Schur multi. group	Outer auto. group	Min simple or N-group	Simple group	Order	Prime factor count	Schur multi. group	Outer auto. group	Min simple or N-group
$A_5^*$	60	4	$C_2$	$C_2$	m-s	$L_2(73)$	194472	7	$C_2$	$C_2$	m-s
$A_6^*$	360	6	$C_6$	$C_2^2$	N-g	$L_2(79)$	246480	8	$C_2$	$C_2$	N-g
$A_7$	2520	7	$C_6$	$C_2$	N-g	$L_2(64)$	262080	11	$\langle e \rangle$	$C_6$	N-g
$A_8^*$	20160	10	$C_2$	$C_2$	-	$L_2(81)$	265680	10	$C_2$	$C_2 \times C_4$	N-g
$A_9$	181440	12	$C_2$	$C_2$	-	$L_2(83)$	285852	6	$C_2$	$C_2$	m-s
$L_2(4)^*$	60	4	$C_2$	$C_2$	m-s	$L_2(89)$	352440	8	$C_2$	$C_2$	N-g
$L_2(5)^*$	60	4	$C_2$	$C_2$	m-s	$L_2(97)$	456288	9	$C_2$	$C_2$	m-s
$L_2(7)^*$	168	5	$C_2$	$C_2$	m-s	$L_2(101)$	515100	7	$C_2$	$C_2$	N-g
$L_2(9)^*$	360	6	$C_6$	$C_2^2$	N-g	$L_2(103)$	546312	7	$C_2$	$C_2$	m-s
$L_2(8)$	504	6	$C_2$	$C_3$	m-s	$L_2(107)$	612468	7	$C_2$	$C_2$	m-s
$L_2(11)$	660	5	$C_2$	$C_2$	N-g	$L_2(109)$	647460	8	$C_2$	$C_2$	N-g
$L_2(13)$	1092	5	$C_2$	$C_2$	m-s	$L_2(113)$	721392	8	$C_2$	$C_2$	m-s
$L_2(17)$	2448	7	$C_2$	$C_2$	m-s	$L_2(121)$	885720	8	$C_2$	$C_2 \times C_2$	N-g
$L_2(19)$	3420	6	$C_2$	$C_2$	N-g	$L_2(125)$	976500	9	$C_2$	$C_6$	N-g
$L_2(16)$	4080	7	$\langle e \rangle$	$C_4$	N-g	$L_3(2)^*$	168	5	$C_2$	$C_2$	m-s
$L_2(23)$	6072	6	$C_2$	$C_2$	m-s	$L_3(3)$	5616	8	$\langle e \rangle$	$C_2$	m-s
$L_2(25)$	7800	7	$C_2$	$C_2^2$	N-g	$L_3(4)$	20160	10	$C_3 \times C_4^2$	$D_6$	-
$L_2(27)$	9828	7	$C_2$	$C_6$	m-s	$L_3(5)$	372000	10	$\langle e \rangle$	$C_2$	-
$L_2(29)$	12180	6	$C_2$	$C_2$	N-g	$L_4(2)^*$	20160	10	$C_2$	$C_2$	-
$L_2(31)$	14480	8	$C_2$	$C_2$	N-g	$U_3(3)$	6048	9	$\langle e \rangle$	$C_2$	N-g
$L_2(37)$	25308	6	$C_2$	$C_2$	m-s	$U_3(4)$	62400	10	$\langle e \rangle$	$C_4$	-
$L_2(32)$	32736	8	$\langle e \rangle$	$C_5$	m-s	$U_3(5)$	126000	10	$C_3$	$D_3$	-
$L_2(41)$	34440	7	$C_2$	$C_2$	N-g	$U_4(2)^*$	25920	11	$C_2$	$C_2$	-
$L_2(43)$	39732	6	$C_2$	$C_2$	m-s	$S_4(3)^*$	25920	11	$C_2$	$C_2$	-
$L_2(47)$	51888	7	$C_2$	$C_2$	m-s	$S_4(4)$	979200	13	$\langle e \rangle$	$C_4$	-
$L_2(49)$	58800	9	$C_2$	$C_2^2$	N-g	$Sz(8)$	29120	9	$C_2 \times C_2$	$C_3$	m-s
$L_2(53)$	74412	7	$C_2$	$C_2$	m-s	$M_{11}$	7920	8	$\langle e \rangle$	$\langle e \rangle$	N-g
$L_2(59)$	102660	6	$C_2$	$C_2$	N-g	$M_{12}$	95040	11	$C_2$	$C_2$	-
$L_2(61)$	113460	6	$C_2$	$C_2$	N-g	$M_{22}$	443520	12	$C_{12}$	$C_2$	-
$L_2(67)$	150348	6	$C_2$	$C_2$	m-s	$J_1$	175560	8	$\langle e \rangle$	$\langle e \rangle$	-
$L_2(71)$	178920	8	$C_2$	$C_2$	N-g	$J_2$	604800	13	$C_2$	$C_2$	-

TABLE 1 – NON-ABELIAN SIMPLE GROUPS WITH ORDER LESS THAN  $10^6$

*Notes.* (a) The outer automorphism and Schur multiplier groups (Columns 4 and 5 above) are considered at the end of this subsection. Thompson (1968) defined an *N-group*, N-g, to be a group in which the normalisers of all of its non-neutral soluble subgroups are themselves soluble, and a group is called *minimum simple*, m-s, if *all* of its proper subgroups are soluble. As a development of his, and Feit's, work on the odd order problem published in 1963, he was able to determine those simple groups that have the properties m-s and/or N-g. His Main Theorem is as follows:

Each non-soluble *N-group* is isomorphic to a group  $G$  which satisfies:  
 $\text{Inn } H \leq G \leq \text{Aut } H$  where  $H$  is one of the following *N-groups*

$$L_2(q) \ (q > 3), \ Sz(2^{2n+1}) \ (n \geq 1), \ A_7, \ L_3(3), \ U_3(3) \text{ and } M_{11},$$

see Sections 12.3 and 12.4, and (c) below (for the Suzuki groups  $Sz$ ). As a corollary to this theorem, Thompson was also able to list the minimal simple groups: If  $p$  denotes an odd prime they are

$$L_2(2^p), \ L_2(3^p), \ L_2(p), \ Sz(2^p), \text{ and } L_3(3),$$

where in the third case  $p > 3$  and  $p \equiv 3$  or  $7 \pmod{10}$ . Column 6 of the table on the previous page lists this data for the groups under discussion. As an exercise the reader should consider why the second list above is smaller than the first, see Problem 12.16W. Note that both  $A_5$  and  $A_6$  occur in the second list, see (b) below.

(b) The stars ( $\star$ ) in Table 1 overleaf indicate that the isomorphism class of the group listed contains more than one group in the table; we have

$$\begin{aligned} A_5 &\simeq L_2(4) \simeq L_2(5) \\ A_6 &\simeq L_2(9) \\ A_8 &\simeq L_4(2) \\ L_2(7) &\simeq L_3(2) \\ U_4(2) &\simeq S_4(3), \end{aligned}$$

see Problems 6.16, 12.4, 12.6, 12.7 and 12.17, and the ATLAS. The group  $A_8$  is not isomorphic to  $L_3(4)$  even though these groups have the same order. For instance the group  $A_8$  contains elements of order 15 whilst  $L_3(4)$  contains no element of order larger than 7, a number of other distinctions have been found; see Problem 12.13. Infinitely many pairs of non-isomorphic simple groups with the same order exist, but there are no triples. This is a consequence of the classification given by CFGS.

(c) The *Suzuki groups*  $Sz(2^{2n+1})$ ,  $n = 1, 2, \dots$  were discovered by Muchio Suzuki in 1959. Later it was realised that they can also be treated as the (twisted) Chevalley groups  ${}^2B_2(2^{2n+1})$ . One definition is as a set of  $4 \times 4$  matrices over  $\mathbb{F}_{2^{2n+1}}$  which 'preserve' a collection of vectors whose coordinates satisfy a special quadratic condition; we shall consider these groups in **Web Section 14.3**. They are the only non-Abelian simple groups whose orders are not divisible by 3, another result due to Thompson.

(d) Below we give brief descriptions of the groups in the table not so far mentioned in the text, or discussed in **Web Chapter 14**; they are  $S_4(4)$ ,  $M_{22}$ ,  $J_1$  and  $J_2$ . The unitary groups  $U_3(4)$  to  $U_4(2)$  have similar definitions to that given for  $U_3(3)$  on pages 265 to 267. The following data gives a partial list of their maximal subgroups, full details can be found in the ATLAS.  $U_3(4) : A_5 \times C_5$ ,  $S_3 \rtimes C_5^2$  and  $F_{13,3}$ ;  $U_3(5) : A_7$ ,  $C_2S_5$  and  $M_{10}$  which is isomorphic to the group  $D$  defined on page 268; and  $U_4(2) : A_5 \rtimes C_2^4$ ,  $S_6$  and  $S_4 \rtimes C_3^3$ .

One definition of the Mathieu group  $M_{12}$  was given on page 268 and its connection with the Steiner system  $S(5, 6, 12)$  will be considered on page 395. With  $M_{24}$  it is the only group that is 5-transitive if we exclude the symmetric and alternating cases. Several definitions are given in the ATLAS including the following presentation

$$M_{12} \simeq \langle a, b, c \mid a^{11} = b^2 = c^2 = (ab)^3 = (ac)^3 = (bc)^{10} = a^2(bc)^2a(bc)^8 = e \rangle.$$

The maximal subgroups are isomorphic copies of  $M_{11}$ , an extension of  $T_2$  by  $A_6$ ,  $C_2S_4 \rtimes C_3^2$ ,  $C_2 \times S_5$ , an extension of an Extra Special group of order 32 by  $S_3$ ,  $D_6 \rtimes C_4^2$ , and  $A_4 \times S_3$ .

**$S_4(4)$  – The symplectic group of order 4 defined over  $\mathbb{F}_4$**  The definition of the group  $S_n(q)$  is similar to that for the unitary group  $U_n(q)$ . As before we work over the field  $\mathbb{F}_{q^2}$ , the dimension  $n$  must now be even. The hermitian form fixed by matrices in  $U_n(q)$  is replaced by an ‘alternating form’ of the type

$$x_1y_{m+1} + x_2y_{m+2} + \cdots + x_my_{2m} - x_{m+1}y_1 - x_{m+2}y_2 - \cdots - x_{2m}y_m$$

and matrices in  $S_{2m}(q)$  where  $n = 2m$  fix a form of this type. If we have  $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in S_{2m}(q)$  where  $A, B, C$  and  $D$  are  $m \times m$ , then

$$A^\top C = C^\top A, B^\top D = D^\top B, A^\top D - C^\top B = I_{2m},$$

where  $\top$  denotes the transpose. All matrices have determinant 1, and  $S_{2m}(q)$  is obtained by factoring out the scalar matrices as in the linear and unitary cases, the centre has order  $(q-1, 2)$  in this case. We have  $S_2(q) \simeq L_2(q)$  for all prime powers  $q$ ,  $S_4(2) \simeq S_6$ , and as noted on page 388 we have  $S_4(3) \simeq U_4(2)$ . Also

$$o(S_{2m}(q)) = q^{m^2}(q^{2m} - 1)(q^{2m-2} - 1) \cdots (q^2 - 1)/(q-1, 2).$$

The group  $S_4(4) \times C_2$  has a presentation as follows:

$$\begin{aligned} \langle a_1, \dots, a_5 \mid a_1^2 = a_2^2 = a_3^2 = a_4^2 = a_5^2 = (a_1a_2)^5 = (a_1a_3)^2 = (a_1a_4)^2 = (a_1a_5)^2 \\ = (a_2a_3)^5 = (a_2a_4)^2 = (a_2a_5)^2 = (a_3a_4)^3 = (a_3a_5)^2 = (a_4a_5)^3 = (a_1a_2a_3)^4 = e \rangle \end{aligned}$$

The order of  $S_4(4)$  is  $2^8 \cdot 3^2 \cdot 5^2 \cdot 17$ , and its maximal subgroups are isomorphic copies of  $(A_5 \times C_3) \rtimes C_2^6$ ,  $C_2 \rtimes L_2(16)$  and  $S_6$ . See the ATLAS for further details.

**$M_{22}$  – The third Mathieu group** J. A. Todd gave the following definition. Let

$$\begin{aligned}\alpha_1 &= (4, 15)(6, 18)(7, 8)(9, 13)(10, 16)(11, 21)(12, 19)(20, 22), \\ \alpha_2 &= (4, 10)(6, 11)(7, 12)(8, 19)(9, 22)(13, 20)(15, 16)(18, 21), \\ \alpha_3 &= (4, 20)(6, 8)(7, 18)(9, 16)(10, 13)(11, 19)(12, 21)(15, 22), \\ \alpha_4 &= (4, 8)(6, 20)(7, 15)(9, 21)(10, 19)(11, 13)(12, 16)(18, 22), \\ \beta &= (3, 4)(5, 22)(6, 18)(7, 12)(8, 21)(11, 19)(13, 14)(16, 17), \\ \gamma &= (2, 3)(6, 18)(9, 21)(10, 12)(11, 13)(14, 17)(16, 19)(20, 22), \\ \delta &= (1, 2)(6, 15)(7, 10)(8, 11)(9, 19)(14, 17)(16, 22)(20, 21).\end{aligned}$$

The permutations  $\alpha_1, \dots, \alpha_4$  generate an isomorphic copy of  $C_2^4$  (an elementary Abelian 2-group of maximal order in the group). If we add  $\beta$  to  $\alpha_1, \dots, \alpha_4$  we obtain a group  $H_1$  of order 960 isomorphic to a semi-direct product  $A_5 \rtimes C_2^4$ , then if we add  $\gamma$  to  $H_1$  we obtain a group  $H_2$ , of order 20160, isomorphic to  $L_4(3)$ , and finally if we add  $\delta$  to  $H_2$  we obtain the group  $M_{22}$ , with order  $443520 = 48 \cdot 20 \cdot 21 \cdot 22$ , and defined as a subgroup of  $A_{22}$ .<sup>8</sup>

Secondly, let  $\theta = \alpha_2\alpha_3$ ,  $\sigma = \beta\alpha_1\alpha_2\beta$  and  $\tau = \gamma\beta\alpha_1\alpha_3\beta\delta\gamma$ , and let

$$H_3 = \langle \alpha_1, \dots, \alpha_4, \delta, \sigma, \tau \rangle.$$

Then  $o(H_3) = 384$ ,  $H_3 \simeq S_4 \rtimes C_2^4 \simeq C_{M_{22}}(\theta)$ . Janko has shown that  $M_{22}$  can be defined as the unique group containing a so-called 2-central involution  $a$  such that  $C_{M_{22}}(a) \simeq H_3$ . A number of presentations have been given, the following can be found in the ATLAS (1985)

$$\begin{aligned}M_{22} &\simeq \langle a_1 \dots, a_5 \mid a_1^2 = a_2^2 = a_3^2 = a_4^2 = a_5^2 = (a_i a_j)^2 [*] \\ &= (a_1 a_2)^3 = (a_2 a_3)^5 = (a_3 a_4)^3 = (a_1 a_5)^4 = (a_3 a_5)^3 \\ &= (a_1 a_2 a_5)^3 = (a_1 a_2 a_3)^5 [= (a_2 a_3 a_5)^5] \\ &= (a_1 a_5 a_3 a_4)^4 = (a_1 a_2 a_3 a_5)^8 = e \rangle.\end{aligned}$$

The first square brackets  $[*]$  indicates that  $i$  and  $j$  range from 1 to 5 when this relation does not contradict one given in the following line (for instance  $i = 1$  and  $j = 2$ ), and the second square brackets imply that this condition is not strictly necessary. The group  $M_{22}$  is also closely related to the Steiner system  $S(3, 6, 22)$ , that is the automorphism group of this system is isomorphic to an extension of  $M_{22}$  by  $C_2$  – note not  $M_{22}$  itself. Maximal subgroups of  $M_{22}$  are isomorphic copies of  $L_4(3)$  (the group  $H_2$  mentioned above),  $A_6 \rtimes C_2^4$ ,  $A_7$ ,  $S_5 \rtimes C_2^4$  (one of these subgroups and  $H_1$ , defined above, give a generating set for the whole group),  $L_3(2) \rtimes C_2^3$ , and  $L_2(11)$ .

**$J_1$  – The first Janko Group** Z. Janko (1965) defined  $J_1$  as the unique group with the properties: (i) its Sylow 2-subgroups are (elementary) Abelian,

<sup>8</sup> If we define  $\mu = (1, 23)(5, 17)(6, 8)(7, 12)(9, 15)(11, 19)(16, 22)(18, 21)$  and  $\nu = (23, 24)(6, 10)(7, 15)(9, 21)(12, 18)(14, 17)(16, 22)(19, 20)$ , then we have  $\langle \alpha_1, \dots, \delta, \mu \rangle \simeq M_{23}$  and  $\langle \alpha_1, \dots, \delta, \mu, \nu \rangle \simeq M_{24}$ ; so  $M_{23}$  is isomorphic to a subgroup of  $A_{23}$  and  $M_{24}$  is isomorphic to a subgroup of  $A_{24}$ . Also  $o(M_{23}) = o(M_{22}) \cdot 23$  and  $o(M_{24}) = o(M_{23}) \cdot 24$ .

(ii) it has no subgroup of index 2, and (iii) it contains an involution  $a$  such that  $C_{J_1}(a) \simeq A_5 \times C_2$ ; see page 103. It can also be generated by two matrices defined over  $GL_7(11)$ , and as a subgroup of  $A_{266}$ . One of its presentations is

$$\begin{aligned} \langle a_1, \dots, a_5 \mid a_1^2 = a_2^2 = a_3^2 = a_4^2 = a_5^2 = (a_1 a_2)^3 = (a_2 a_3)^5 = (a_3 a_4)^3 \\ = (a_4 a_5)^5 = (a_i a_j)^2 [*] = (a_1 a_2 a_3)^5 = e, a_1 = (a_3 a_4 a_5)^5 \rangle, \end{aligned}$$

(for  $[*]$  see the presentation for  $M_{22}$ ). It has order  $2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$  and, in 1965, it was the first sporadic group discovered in nearly 100 years, that is after Mathieu discovered his groups in the 1860s and 1870s. See Janko's remarkable 1965 paper and the ATLAS for further details. The maximal subgroups of  $J_1$  are isomorphic copies of  $L_2(11)$ ,  $A_5 \times C_2$ ,  $F_{19,6}$ ,  $F_{11,10}$  and  $F_{7,6}$ .

**$J_2$  – The second Janko Group, sometimes also known as the *Hall-Janko Group* or the *Hall-Janko-Wales Group*** This group can be defined as a subgroup of  $A_{100}$  generated by three elements, of orders 7, 8 and 2, respectively; see Hall and Wales (1968). Janko defined it as the unique group satisfying the following conditions: (i) it is simple, (ii) it has order 604800, (iii) it has exactly two conjugacy classes of involutions, and (iv) it contains an involution  $a$  such that  $C_{J_2}(a)$  is isomorphic to an extension of  $N$  by  $A_5$  where  $N$  is a so-called central extension (of total order 32) of  $Q_2$  and  $D_4$ . One presentation of  $J_2$  is

$$\langle a, b \mid a^2 = b^3 = y^{15} = (y(y^3 z^2)^2 z)^2 = (y^3 z(y^2 z^2)^2)^2 = e \rangle,$$

where  $y = ab$  and  $z = ab^2$ . See the paper quoted above for further details. The maximal subgroups of  $J_2$  are isomorphic copies of the following groups

$U_3(3)$  (page 265), an extension of  $PGL_2(9)$  by  $C_3$ ,  $A_5 \rtimes N$ ,

$A_5 \times A_4$ ,  $A_5 \times D_5$ ,  $C_2 \rtimes L_3(2)$  and  $A_5$ .

( $PGL_n(p)$  is defined in a similar manner to  $L_n(p)$ , that is as  $GL_n(p)$  factored by its centre, see page 170.)

### ***Outer Automorphism and Schur Multiplier Groups***

The outer automorphism and Schur multiplier groups are important in the character theory of simple groups, and they have connections with certain well-behaved extensions which we consider now. The outer automorphism group  $\text{out}(G) = H$  of a group  $G$  was defined on page 82. If the order of  $H$  is larger than one, then the theory discussed in Section 9.2 guarantees the existence of an extension group  $J$  of  $G$  by  $H$ . Also there is a close relationship between the character tables of  $G$  and  $J$ , once the character table for  $G$  has been constructed, there is a fairly automatic procedure for the construction of the table for  $J$  when  $H$  is relatively small. For example if  $G = A_5$ , then  $\text{out}(G) \simeq C_2$  and there exists an extension of  $A_5$  by  $C_2$  which, of course, is isomorphic to  $S_5$ . Secondly, if  $G = U_3(3)$ , where again  $\text{out}(G) \simeq C_2$ , we gave a presentation of the semi-direct product of  $U_3(3)$  by  $C_2$  on page 266.

The Schur multiplier deals with the reverse situation, that is when the group  $G$  is isomorphic to a factor group of the extension. And again there is a close connection between the character tables of the groups involved. The multiplier can be defined as follows. An extension  $J$  of  $H$  by  $G$  is called *central* if  $H \leq Z(J)$  and  $G \simeq J/H$ .<sup>9</sup> One example is given by taking  $H$  to be an arbitrary Abelian group and  $J = G \times H$ . To avoid this rather straightforward case we also require  $H$  to belong to the derived subgroup of  $J$ . Hence given  $G$  we are looking for  $H$  and  $J$  satisfying

$$H \leq Z(J) \cap J' \quad \text{and} \quad G \simeq J/H,$$

see Theorem 10.18; note this implies that  $H$  is Abelian. It can be shown that there always exists a unique maximal solution  $H$ . This subgroup  $H$  is called the *Schur multiplier* of  $G$  and it is usually denoted by  $M(G)$ , some examples are given in the table on page 387. It can also be shown that if  $G$  is simple (in fact we only need  $G$  to be perfect) and  $H = M(G)$ , then  $J$  is unique (up to isomorphism). It is called the *cover* or the *Schur representation group* of the group  $G$ .

Two further definitions have been given. First  $M(G)$  can be defined as the cohomology group  $H^2(G, \mathbb{C}^*)$ , see the references quoted below. Secondly, if  $G$  is given by the presentation

$$G = \langle a_1, \dots, a_k \mid x_1 = \dots = x_l = e \rangle, \quad (12.12)$$

where each  $x_j$  is a word using the letters  $a_1, \dots, a_k$ , then the extension  $J$  can be given a presentation in the following form. Using  $a_1, \dots, a_k, c_1, \dots, c_l$  and  $x_1, \dots, x_l$  given in (12.12), the relations of  $J$  are

$$x_j = c_j \quad \text{and} \quad a_i c_j = c_j a_i \quad \text{for all} \quad 1 \leq i \leq k \quad \text{and} \quad i \leq j \leq l,$$

and the Schur multiplier  $M(G)$  equals  $\langle c_1, \dots, c_l \rangle \cap J'$ . As with the outer automorphism group case there is a close connection between the character tables of  $G$  and  $J$ .

These two constructions can sometimes be combined to form ‘double extensions’  $H$  by  $G$  by  $J$ , but in this case we lose uniqueness. For an example consider the group  $SL_2(5)$ . Its centre is isomorphic to  $C_2$  which also equals its derived subgroup, and as we have seen previously

$$A_5 \simeq SL_2(5)/C_2,$$

that is  $M(A_5) \simeq C_2$ . (To be more precise this only shows that  $M(A_5) \geq C_2$ , further arguments are needed to establish the isomorphism.) Also two distinct groups arise which are extensions of the type  $C_2$  by  $A_5$  by  $C_2$ . A similar result holds for  $A_n$  if  $n > 7$ , but the situation is more complicated for  $A_6$  and  $A_7$ : see Sections 4 and 6 of the ATLAS (1985), and Chapter 2, Section 7, in Suzuki (1982).

---

<sup>9</sup> Refer to Definition 9.11. In a central extension the maps  $\vartheta_a$  in the factor set satisfy  $\vartheta_a = e$  for all  $a \in A$ . Hence the cocycle identity has a simplified form.

## 12.6(b) A New Proof of the Simplicity of $L_n(q)$

In this section we give a second proof of the simplicity of the groups  $L_n(q)$  (when  $q > 3$  if  $n = 2$ ) using Iwasawa's Lemma which was proved in [Web Section 5.4](#), page 357. This proof has the advantage that it deals with all cases in one 'go' and shows clearly where the conditions are needed but, compared with the first proof, it requires more preliminary material. Iwasawa's Lemma only applies to permutation groups which are both perfect and primitive but this is sufficient for a good proportion of the classical groups. We begin the proof by showing that the groups  $SL_n(q)$  have these properties (with two exceptions).

In Section 12.2 we defined a *transvection*  $E_{ij}(r)$  as the identity matrix  $I_n$  with the additional entry  $r$  in the  $(i, j)$ th place where  $r \neq 0$  and  $i \neq j$ . We showed there that

$$E_{ij}(r)^{-1} = E_{ij}(-r). \quad (12.13)$$

**Lemma 12.15** *The group  $SL_n(q)$  is generated by its transvections.*

*Proof.* See Lemmas 12.8 and 12.11. The proof is straightforward using the elementary operations, and the fact that an elementary operation can be performed by pre- or post-multiplying the given matrix by a transvection. As the determinant of a transvection is 1, this can all be carried out in  $SL_n(q)$ .  $\square$

**Lemma 12.16** *The group  $SL_n(q)$  is perfect provided  $q > 3$  when  $n = 2$ .*

Note that neither  $SL_2(2) (\simeq D_3)$  nor  $SL_2(3)$  is perfect, see Section 8.2.

*Proof.* By Lemmas 12.8 and 12.11 it is sufficient to show that each transvection can be written as a commutator. Suppose first  $n > 2$  and  $1 \leq i, j, k \leq n$  where  $i, j$  and  $k$  are distinct (and so we need  $n$  to be at least 3). Using (12.13) it is easy to check that

$$[E_{ik}(1), E_{kj}(r)] = E_{ij}(r),$$

and this proves the result in this case.

For the case  $n = 2$  we argue as in the last part of the proof of Theorem 12.10. Let  $a, b \in \mathbb{F}_q \setminus \{0\}$ , and let

$$A = \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}.$$

Then we have

$$[A, B] = E_{12}(b(1 - a^2)).$$

Now as  $q = o(\mathbb{F}_q) > 3$  we can choose  $a$  to satisfy  $1 - a^2 \neq 0$ . Hence for an arbitrary  $c \in \mathbb{F}_q$  we can choose  $a$  and  $b$  to satisfy  $c = b(1 - a^2)$  which gives the result in this case. For the remaining case note that  $E_{21}(c) = [(B^{-1})^\top, (A^{-1})^\top]$ .  $\square$



Next we introduce some further linear algebra properties. If  $V$  is an  $n$ -dimensional vector space defined over the field  $\mathbb{F}_q$ , then the elements of  $GL_n(q)$ , or  $SL_n(q)$ , transform  $V$  to itself, and so we can say that  $GL_n(q)$  or  $SL_n(q)$  act on  $V$  – the ‘natural action’; note that this action obeys the basic action axioms (5.1) given in Section 5.1. (They do, of course, also depend on the basis chosen for  $V$ .)

**Lemma 12.17** *Suppose  $V$  is an  $n$ -dimensional vector space defined over  $\mathbb{F}_q$ , and  $n \geq 2$ . The natural action of  $SL_n(q)$  on the set of 1-dimensional subspaces of  $V$  defined above is doubly transitive.*

*Proof.* A matrix in  $SL_n(q)$  maps the set of 1-dimensional subspaces to itself. As  $n \geq 2$  we can ask if this action is doubly transitive. Let  $u_1, u_2, w_1, w_2 \in V$  where  $u_1 \neq u_2$  and  $w_1 \neq w_2$ , and let the 1-dimensional subspaces containing these vectors be denoted by  $U_1, U_2, V_1, V_2$ , respectively. (So for instance  $U_1 = \{cu_1 : c \in \mathbb{F}_q\}$ .) As  $u_1 \neq u_2$  and  $w_1 \neq w_2$  we can find  $u_3, \dots, u_n$  so that both  $\{u_1, \dots, u_n\}$  and  $\{w_1, \dots, w_n\}$  are bases for  $V$ , and there exists a matrix  $A$  in  $GL_n(q)$  which transforms the first of these bases to the second. Is  $A$  in  $SL_n(q)$ ? If not, suppose its determinant  $\det A$  equals  $a$ . Now  $w_1/a, w_2, \dots, w_n$  is also a basis for  $V$ , and if we repeat the above procedure with this new basis, then the corresponding matrix  $A$  will have determinant 1, and so it will belong to  $SL_n(q)$ . This shows that the group  $SL_n(q)$  is doubly transitive.  $\square$

We come now to  $L_n(q)$ , that is  $SL_n(q)$  factored by its centre  $Z$ , the set of scalar matrices. As  $Z$  acts neutrally on the set of 1-dimensional subspaces of  $V$ , the natural action on  $SL_n(q)$  is also an action of  $L_n(q)$ .

**Lemma 12.18** (i) *If  $n \geq 2$ , then  $L_n(q)$  is a doubly transitive permutation group.*

(ii) *The degree of the group, that is the order of the set upon which  $L_n(q)$  acts, equals  $(q^n - 1)/(q - 1)$ .*

*Proof.* (i) This follows from the discussion above. (ii) We leave this as an exercise for the reader, note that  $(q^n - 1)/(q - 1)$  is the number of 1-dimensional subspaces in the underlying vector space.  $\square$

We are now ready to prove our main result.

**Theorem 12.19** *The group  $L_n(q)$  is simple provided  $q > 3$  when  $n = 2$ .*

*Proof.* We shall use Iwasawa’s Lemma (Theorem 5.40) given in **Web Section 5.4**. The first condition is that  $L_n(q)$  should be a primitive permutation group, this follows from Lemma 12.17 and Corollary 5.37 in **Web Section 5.4**. The second condition is that the group should be perfect, and this follows from Lemma 12.16 using the Correspondence Theorem (Theorem 4.16). This is the only point where the exceptions in the theorem apply.

Let  $v_i$  be an element of a basis for the underlying  $n$ -dimensional vector space  $V$  ( $1 \leq i \leq n$ ), see Lemma 12.17, and let  $U_i$  be the 1-dimensional subspace containing  $v_i$  (so  $U_i = \{cv_i : c \in \mathbb{F}_q\}$ ). Further let

$$H_i = \text{stab}_{SL_n(q)}(U_i).$$

Now  $H_i$  acts on the vector space  $V/U_i$ , and induces a group homomorphism from  $H_i$  to the group of invertible linear maps on  $V/U_i$ . Let  $K_i$  be the kernel of this map, so  $K_i$  is the group of all matrices that stabilise  $U_i$  in  $SL_n(q)$ , and act neutrally on  $V/U_i$ . Hence if  $A \in K_i$ , then  $\det A = 1$ . Further, the linear map induced on  $V/U_i$  by  $A$  is the identity map, and it has determinant 1. Hence we can take the matrix of this map in the form

$$A = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ c_i & \dots & c_{i-1} & 1 & c_{i+1} & \dots & c_n \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix} \quad \text{for } c_j \in \mathbb{F}_q,$$

with zeros at all other entries. The collection of all matrices of type  $A$  forms an Abelian subgroup of  $SL_n(q)$  (reader, check), and this subgroup is normal as it is the kernel of a homomorphism.

Further, as  $SL_n(q)$  acts on the set of 1-dimensional subspaces of  $V$  and  $K_i$  is determined by the vector  $v_i$ , we see that the collection of groups  $K_i$  are conjugate in  $SL_n(q)$ . But each transvection  $E_{jk}(r)$  belongs to one of the  $K_i$  ( $1 \leq i \leq n$ ), and so, by Lemma 12.15, the normal closure of  $K_1$  is  $SL_n(q)$ . (Note that we could have taken any one of the groups  $K_i$  in place of  $K_1$ .)

Lastly we use the Correspondence Theorem (Theorem 4.16). The factor group  $H_1/Z(H_1)$  is a point stabiliser of the permutation group  $L_n(q)$ , and  $K_1/Z(K_1)$  is an Abelian normal subgroup of  $H_1/Z(H_1)$ . Also the normal closure of  $K_1/Z(K_1)$  is  $L_n(q)$ . Hence we have satisfied all of the conditions in Iwasawa's Lemma, and so the result follows.  $\square$

This method can also be applied to establish the simplicity of a number of other classes of groups including the Unitary, Symplectic and Orthogonal Groups, and some other individual groups.

### 12.6(c) Constructing $S(5, 6, 12)$ and $S(4, 5, 11)$

The following procedure constructs a version of the Steiner system  $S(5, 6, 12)$ . Versions of  $S(4, 5, 11)$  can be read off directly; in fact it gives several versions of two types, see below. For further details on this construction see Curtis (1984); the author called it "a pocket calculator for  $M_{12}$ ". Chapter 11 in Conway and Sloane (1993) is also of relevance here. We work on the projective line modulo 11, which we take as

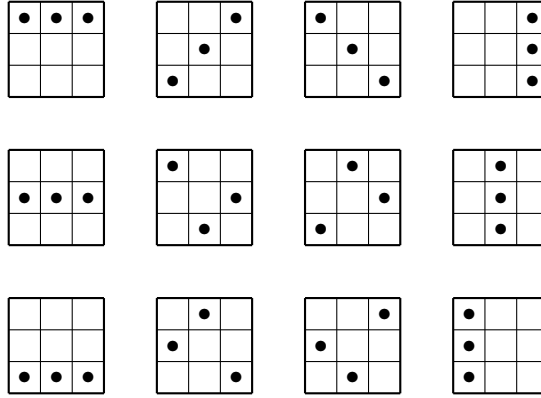
$$\mathcal{P} = \{\infty, 0, 1, \dots, 9, 10\},$$

and we consider  $3 \times 3$  arrays of elements in  $\mathcal{P}$  of the form

$$\begin{array}{c|c|c} a_1 & a_2 & a_3 \\ \hline b_1 & b_2 & b_3 \\ \hline c_1 & c_2 & c_3 \end{array}$$

We need to define three types of subsets of these arrays. First, a *line* (or *triple*) is one of the twelve 3-element subsets listed below. Think of an array as a “torus”, that is identify the top and bottom edges, and then the left and right edges. The first diagram below illustrates these lines. So for example  $\{a_1, b_3, c_2\}$  is a line, one of the three ‘anti-diagonals’, see the second entry in the second column of the diagram below. The lines are

$$\begin{aligned} &\{a_1, a_2, a_3\}, \{b_1, b_2, b_3\}, \{c_1, c_2, c_3\}, \{a_3, b_2, c_1\}, \{a_1, b_3, c_2\}, \{a_2, b_1, c_3\}, \\ &\{a_1, b_2, c_3\}, \{a_3, b_1, c_2\}, \{a_2, b_3, c_1\}, \{a_i, b_i, c_i\} \text{ for } i = 1, 2, 3. \end{aligned}$$

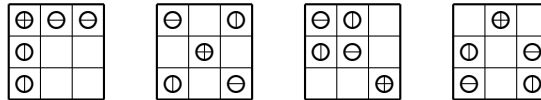


THE TWELVE LINES IN AN ARRAY

Secondly, a *cross* is a union of two perpendicular lines (horizontal and vertical lines are perpendicular, as are diagonal and anti-diagonal lines), there are 18 as follows.

$$\begin{aligned} &\{a_1, a_2, a_3, b_1, c_1\}^* \quad \{a_1, a_2, a_3, b_3, c_3\} \quad \{a_3, b_3, c_1, c_2, c_3\} \\ &\{a_1, b_1, c_1, c_2, c_3\} \quad \{a_1, a_2, a_3, b_2, c_2\} \quad \{a_3, b_1, b_2, b_3, c_3\} \\ &\{a_2, b_2, c_1, c_2, c_3\} \quad \{a_1, b_1, b_2, b_3, c_1\} \quad \{a_2, b_1, b_2, b_3, c_2\} \\ &\{a_1, a_3, b_2, c_1, c_3\}^* \quad \{a_1, a_2, b_1, b_2, c_3\}^* \quad \{a_2, a_3, b_2, b_3, c_1\} \\ &\{a_3, b_1, b_2, c_1, c_2\} \quad \{a_2, a_3, b_2, b_3, c_1\} \quad \{a_2, b_1, b_3, c_1, c_3\}^* \\ &\{a_1, a_2, b_3, c_1, c_2\} \quad \{a_1, a_3, b_1, b_3, c_2\} \quad \{a_2, a_3, b_1, c_2, c_3\}. \end{aligned}$$

Four of these crosses, marked with an asterisk above, are illustrated in the second diagram below.



The third collection contains the *squares* which are the complements of the crosses in the array on page 396, so again there are 18 and each have four elements. For example the first is  $\{b_2, b_3, c_2, c_3\}$ .

The algorithm is constructed using the following three arrays. These arrays were produced using the fact that if we select from the system  $S(5, 6, 12)$  those hexads that contain a fixed triple then we obtain a version of the Steiner system  $S(2, 3, 9)$ . We take  $\{0, 1, \infty\}$  as the fixed triple, see Rows 19 and 20 in Table 3 on page 398; but note that we could have taken an arbitrary triple from  $\mathcal{P}$  as the fixed triple – reader, try one. Each line in these arrays belongs to this smaller system defined on the set  $\{2, 3, \dots, 10\}$ . The arrays are

6	10	3
2	7	4
5	9	8

 $\infty$ -array

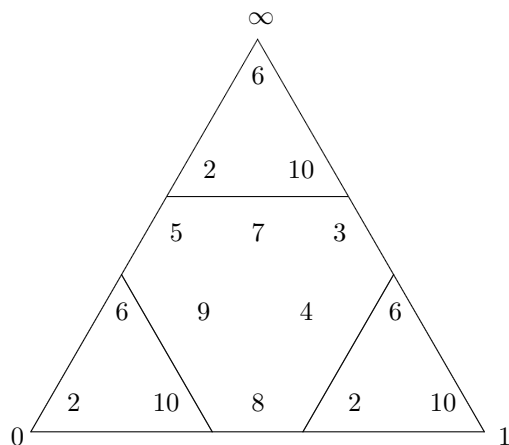
2	6	5
10	9	7
8	4	3

0-array

10	2	8
6	4	9
3	7	5

1-array

These three arrays can be combined into one triangular array called the ‘kitten’. A similar device called MOG (Miracle Octad Generator) has been constructed for  $M_{24}$ , hence the name! In fact the kitten can be embedded in MOG, see the paper quoted above and the ATLAS (1985) for further details. Each of the three arrays above form part of this triangular array. For example the  $\infty$ -array can be obtained from the diagram below by simply ignoring the two lower outer triangles and rotating.

CALCULATOR FOR  $M_{12}$  – THE ‘KITTEN’

The elements of the Steiner system  $S(5, 6, 12)$  (‘hexads’ of six elements in  $\mathcal{P}$ ) consist of the following sets:

- (a)  $\infty$  and a cross from the  $\infty$ -array; 0 and a cross from the 0-array; and 1 and a cross from the 1-array; there are 54 in total, see Columns 1 to 3 in Table 3.

(b)  $\infty, 0$  and a square from the 1-array;  $\infty, 1$  and a square from the 0-array; and  $0, 1$  and a square from the  $\infty$ -array; there are again 54 in total, see Columns 4 to 6 in Table 3.

(c) The union of  $\{\infty, 0, 1\}$  and a line, and the union of two parallel lines; 24 in total, the last four rows in Table 3. ‘Parallel’ is defined in a similar manner to perpendicular, for instance:  $\{a_3, b_1, c_2\}$  and  $\{a_2, b_3, c_1\}$  are parallel, see the third column of the first diagram on page 396.

These hexads are listed in the table below, the bold entries will be explained on page 399.

$\infty, \mathbf{2,3,4,6,9}$	0,2,3,4,7,9	1,2,3,4,5,7	$\infty, 0, 2, 3, 4, 5$	$\infty, 1, 2, 3, 4, 10$	0,1,2,3,4,6
$\infty, 2, 3, 4, 7, 8$	$\mathbf{0,2,3,4,8,10}$	1,2,3,4,8,9	$\infty, 0, 2, 3, 6, 8$	$\infty, \mathbf{1,2,3,5,8}$	0,1,2,3,5,10
$\infty, 2, 3, 5, 6, 10$	$\mathbf{0,2,3,5,6,7}$	1,2,3,5,6,9	$\infty, 0, 2, 3, 7, 10$	$\infty, 1, 2, 3, 6, 7$	0,1,2,3,7,8
$\infty, 2, 3, 5, 7, 9$	0,2,3,5,8,9	1,2,3,6,8,10	$\infty, 0, 2, 4, 6, 10$	$\infty, 1, 2, 4, 5, 9$	0,1,2,4,5,8
$\infty, 2, 3, 8, 9, 10$	0,2,3,6,9,10	$\mathbf{1,2,3,7,9,10}$	$\infty, 0, 2, 4, 8, 9$	$\infty, 1, 2, 4, 6, 8$	0,1,2,4,9,10
$\infty, 2, 4, 5, 6, 7$	0,2,4,5,6,9	$\mathbf{1,2,4,5,6,10}$	$\infty, 0, 2, 5, 7, 8$	$\infty, 1, 2, 5, 7, 10$	0,1,2,5,7,9
$\infty, 2, 4, 5, 8, 10$	0,2,4,5,7,10	1,2,4,6,7,9	$\infty, \mathbf{0,2,5,9,10}$	$\infty, 1, 2, 6, 9, 10$	0,1,2,6,7,10
$\infty, 2, 4, 7, 9, 10$	0,2,4,6,7,8	1,2,4,7,8,10	$\infty, 0, 2, 6, 7, 9$	$\infty, 1, 2, 7, 8, 9$	$\mathbf{0,1,2,6,8,9}$
$\infty, 2, 5, 6, 8, 9$	0,2,5,6,8,10	1,2,5,6,7,8	$\infty, 0, 3, 4, 6, 7$	$\infty, 1, 3, 4, 5, 6$	$\mathbf{0,1,3,4,5,9^*}$
$\infty, \mathbf{2,6,7,8,10}$	0,2,7,8,9,10	1,2,5,8,9,10	$\infty, 0, 3, 4, 9, 10$	$\infty, 1, 3, 4, 7, 9$	0,1,3,4,7,10
$\infty, \mathbf{3,4,5,7,10}$	0,3,4,5,6,10	1,3,4,5,8,10	$\infty, 0, 3, 5, 6, 9$	$\infty, 1, 3, 5, 9, 10$	0,1,3,5,6,8
$\infty, 3, 4, 5, 8, 9$	0,3,4,5,7,8	$\mathbf{1,3,4,6,7,8}$	$\infty, 0, 3, 5, 8, 10$	$\infty, 1, 3, 6, 8, 9$	0,1,3,6,7,9
$\infty, 3, 4, 6, 8, 10$	0,3,4,6,8,9	1,3,4,6,9,10	$\infty, \mathbf{0,3,7,8,9}$	$\infty, 1, 3, 7, 8, 10$	0,1,3,8,9,10
$\infty, 3, 5, 6, 7, 8$	0,3,5,7,9,10	1,3,5,6,7,10	$\infty, \mathbf{0,4,5,6,8}$	$\infty, 1, 4, 5, 7, 8$	0,1,4,5,6,7
$\infty, 3, 6, 7, 9, 10$	0,3,6,7,8,10	1,3,5,7,8,9	$\infty, 0, 4, 5, 7, 9$	$\infty, 1, 4, 6, 7, 10$	0,1,4,6,8,10
$\infty, 4, 5, 6, 9, 10$	0,4,5,8,9,10	1,4,5,6,8,9	$\infty, 0, 4, 7, 8, 10$	$\infty, \mathbf{1,4,8,9,10}$	0,1,4,7,8,9
$\infty, 4, 6, 7, 8, 9$	$\mathbf{0,4,6,7,9,10}$	1,4,5,7,9,10	$\infty, 0, 5, 6, 7, 10$	$\infty, \mathbf{1,5,6,7,9}$	0,1,5,6,9,10
$\infty, 5, 7, 8, 9, 10$	0,5,6,7,8,9	1,6,7,8,9,10	$\infty, 0, 6, 8, 9, 10$	$\infty, 1, 5, 6, 8, 10$	$\mathbf{0,1,5,7,8,10}$
$\infty, 0, 1, 2, 3, 9$	$\infty, \mathbf{0,1,2,4,7}$	$\infty, 0, 1, 2, 5, 6$	$\infty, 0, 1, 2, 8, 10$	$\infty, 0, 1, 3, 4, 8$	$\infty, 0, 1, 3, 5, 7$
$\infty, \mathbf{0,1,3,6,10}$	$\infty, 0, 1, 4, 5, 10$	$\infty, 0, 1, 4, 6, 9$	$\infty, 0, 1, 5, 8, 9$	$\infty, 0, 1, 6, 7, 8$	$\infty, 0, 1, 7, 9, 10$
2,3,4,5,6,8	2,3,4,5,9,10	2,3,4,6,7,10	2,3,5,7,8,10	2,3,6,7,8,9	$\mathbf{2,4,5,7,8,9}$
2,4,6,8,9,10	2,5,6,7,9,10	3,4,5,6,7,9	3,4,7,8,9,10	$\mathbf{3,5,6,8,9,10}$	4,5,6,7,8,10

TABLE 3 – A VERSION OF THE STEINER SYSTEM  $S(5, 6, 12)$ 

The reader should choose an arbitrary pentad (5-tuple) in  $\mathcal{P}$  and check that it occurs in exactly one hexad in the table above. As noted in Section 12.4, several versions of the Steiner system  $S(4, 5, 11)$  can now be read off this table. For example, take the 66 entries above which include 0 (columns 2, 4 and 6, and rows 19 and 20), delete the entry 0 from each hexad, and the resulting set is a version of  $S(4, 5, 11)$  defined on  $\{\infty, 1, 2, \dots, 10\}$ ; again the reader should choose a 4-tuple and check that it occurs in only one pentad. There is nothing special about 0, for example we could take the 66 entries which include 3, say, delete 3 in each case and then we have a version of  $S(4, 5, 11)$  on  $\{\infty, 0, 1, 2, 4, \dots, 10\}$ .

Table 3 can also be constructed by starting with 0 and the five quadratic residues modulo 11, that is the hexad  $\{0, 1, 3, 4, 5, 9\}$  marked with a star in Table 3 above, and applying the following two procedures:

$\theta : \{a_1, \dots, a_6\}\theta = \{a_1 + 1, \dots, a_6 + 1\}$  modulo 11; and  
 $\psi$  : interchange 0 and 1, 2 and 10, 3 and 5, 4 and 9, and leave 6, 7, 8 and  $\infty$  fixed (the mirror reflection about the line through the point  $\infty$  and the mid-point of the line  $(0, 1)$  in the ‘kitten’ diagram on page 397),

then we obtain a version of the Steiner system for  $M_{11}$  defined on the set  $\{0, 1, \dots, 10\}$  (and so leaving  $\infty$  fixed); that is  $\theta$  and  $\psi$  generate  $M_{11}$  as a subgroup of  $M_{12}$ . Also if we apply  $\theta$  and  $\sigma$  where

$\sigma$  : interchange 1 and  $\infty$ , 4 and 7, 5 and 8, 6 and 10, and leave 0, 2, 3 and 9 fixed (the mirror reflection about the line through the lower left-hand point 0 and the mid-point of the line  $(1, \infty)$ );

then we obtain the 22 hexads set bold in Table 3 on page 398. This provides another way to obtain  $M_{11}$ , this time 3-transitive on a 12-element set; see the note at the end of Section 12.4. This system has 22 members and each triple of integers in the chosen range occurs in exactly two members of the system.

It is also of interest that if we apply  $\theta$  and the procedure  $\tau$  where

$\tau$  : cyclically permute 0, 1 and  $\infty$ ; 2, 10 and 6; 3, 5 and 8; and 4, 7 and 9 (this corresponds to the map  $x \rightarrow (1 - x)^{-1}$  modulo 11),

then we obtain a copy of  $L_2(11)$  as a subgroup of  $M_{12}$ . The permutation  $\tau$  can be formed by rotating anticlockwise all of the triangles in the kitten diagram on page 397.

*New Book* At about the time the main text of this book appeared in print, another was published (also by Springer) which provides an introduction to the theory of finite simple groups:

Wilson, R. A. [2009], *The Finite Simple Groups*.

This book gives detailed descriptions of all finite non-Abelian simple groups — alternating, classical (linear, symplectic, unitary and orthogonal), exceptional (Suzuki, and both small and large Ree), and sporadic (partitioned as the Suzuki chain including  $J_2$ , the Fischer groups, the Monster and its subgroups, and the *Pariahs* (!) including the remaining Janko groups). It concentrates on the code-theoretical and more purely-algebraic aspects of the theory (for example by introducing the octonians and Jordan algebras when discussing the Ree groups). It also gives a detailed account of the maximal subgroups of all finite simple groups. Read in conjunction with the ATLAS [1985], this new work provides the reader with a good introduction to the whole area covered by CFGS.

## 12.7 Problems 12W

**Problem 12.16** Explain why the list of minimal simple groups given on page 388 is smaller than the list of N-groups.

**Problem 12.17** Show that  $A_8 \simeq L_4(2)$ . This can be done directly by finding six matrices in  $L_4(2)$  which satisfy the relations in the presentation for  $A_8$  given on page 249. Or one can argue as follows. Note that  $L_4(2) (\simeq GL_4(2))$  is isomorphic to the automorphism group of the elementary Abelian group  $C_2^4$ , then work in a group which has a subgroup of this type, for example  $L_3(4)$ . See also Conway and Sloane (1993), page 270.

**Problem 12.18** (i) Show that the normaliser of a Sylow 13-subgroup of the group  $L_3(3)$  has order 39, and it is a maximal subgroup of the group. Use the work in Section 12.2, the Sylow theory, and Burnside's Normal Complement Theorem (Theorem 6.17(20)). You can take for granted that the centraliser of the Sylow 13-subgroup has odd order.

(ii) Using Burnside's  $p^r q^s$ -theorem, deduce  $L_3(3)$  is minimal simple.

**Problem 12.19** Derive the simplicity of  $M_{11}$  using the following method. Let  $K$  be a proper non-neutral normal subgroup of  $M_{11}$  of minimal order. Use Theorem 5.38 in Web Section 5.4. to show that  $K$  is transitive, and so prove that its order is divisible by 11. Now note that  $K$  contains a Sylow 11-subgroup  $P$  which is cyclic and transitive. Next show that  $P = C_{M_{11}}(P)$ . Further note that  $[N_{M_{11}}(P) : P] = 1$  or 5. To do this you will first need to show that  $o(N_{M_{11}}(P))$  is odd, then use the  $N/C$ -theorem (Theorem 5.26). Next show that  $P$  is self-normalising in  $K$ . Finally apply the Burnside Normal Complement Theorem (Theorem 6.17) to obtain a contradiction.

**Problem 12.20** This problem refers to the work discussed at the end of this section (Subsection (c)). On  $\mathcal{P}$  let

$\nu$  : interchange 0 and  $\infty$ , 2 and 6, 3 and 8, 7 and 9,

and leave 1, 4, 5 and 10 fixed.

What group do you obtain using  $\theta$  (as defined on page 399) and  $\nu$ ?

**Problem 12.21** For each of the Mathieu groups we have: if  $G$  is a simple group with order  $o(M_j)$  where  $j = 11, 12, 22, 23$  or 24, then  $G \simeq M_j$ . Investigate what is needed to prove this in the case when  $j = 11$ .

## Chapter 13

# Representation and Character Theory

Representation theory has formed an integral part of the theory of finite groups since Frobenius, Schur and others did their pioneering work over a century ago. The solution of CFSG would not have been possible without it. In this theory the ideas, methods and theorems of linear algebra are applied to establish essential group properties, one of which is the famous result of Feit and Thompson which states that all groups of odd order are soluble – a major first step in the solution of the simple group problem. Character theory is an important part of representation theory where the representing matrices are ‘replaced’ by complex numbers which are easier to work with. We shall see that every finite group  $G$  has a ‘character table’ which is a square array of complex numbers and, using this table, a number of properties of  $G$  can be ‘read off’; for instance we can use the table for  $G$  to list the normal subgroups of  $G$ .

This chapter and the next should be treated as a single piece of work, together they provide an introduction to some aspects of representation and character theory. Unlike others in the book, this chapter is mostly theoretical developing enough basic material for the applications to be discussed in Chapter 14. These applications include

The construction of character tables for some small groups including all those with order not more than 12,  $A_5$ , the Chapter 8 groups, and some others;

A proof of Burnside’s  $p^r q^s$ -theorem first discussed in Chapter 11; and  
Some development of the theory of ‘Frobenius Groups’; a non-Abelian group of order  $pq$  being an example (Theorem 6.11). This work will introduce a number of new groups including the Suzuki Groups discussed briefly in Section 12.4.

A summary of the main character properties is given at the end of the chapter, this is sufficient for the reader who only needs to study the applications. For a more extensive review of character theory the reader is recommended to consult the following texts as the author has done on many occasions:

Huppert, B. (1991) *Character theory of finite groups*. de Gruyter.

Issacs, I. M. (1976, reprinted 2006) *Character theory of finite groups*.  
AMS Chelsea



James, G. and Liebeck, M. (1993) *Representations and characters of groups*. Cambridge University Press.

Here and in Chapter 14 we shall assume that the reader has a working knowledge of basic linear algebra including

- (a) vector spaces, subspaces, bases, and dimension;
- (b) linear maps and their representation by matrices. Also both Jordan and rational canonical forms will be used in the examples;
- (c) direct sums of vector spaces,<sup>1</sup> the notions here are of course closely related to those presented in Section 7.2 relating to direct products of Abelian groups;
- (d) the basic facts about inner and Hermitian products.

The books by Halmos (1974a), Finkbeiner, D. (1966, *Introduction to matrices and linear transformations*. Freeman, San Francisco), or Rose (2002), amongst many others, will provide all that is needed.

All vector spaces and matrices discussed are defined over the complex number field  $\mathbb{C}$ . We use this field because at some essential points in the theory we require our ground field to have characteristic zero, and be algebraically closed. Hence all polynomial equations with rational coefficients have at least one real or complex root.

## 13.1 Representations and Modules

In this chapter and the next  $G$  always denotes a finite group, and we write  $GL_n$  for  $GL_n(\mathbb{C})$  the group of all non-singular  $n \times n$  matrices defined over the complex field  $\mathbb{C}$ ; this is our ‘representing group’. We begin by giving the basic

**Definition 13.1** (i) A *representation* of  $G$  is a homomorphism  $\theta : G \rightarrow GL_n$ . The *degree* of  $\theta$  is  $n$ .

(ii) The *kernel* of the representation  $\theta$  is  $\ker \theta$ , the kernel of the homomorphism  $\theta$ .

(iii) A representation  $\theta$  is called *trivial* if, and only if, the homomorphism  $\theta$  is trivial (see Definition 4.2), and it is called *faithful* if, and only if,  $\ker \theta = \langle e \rangle$ .

(iv) Two representations  $\theta_1$  and  $\theta_2$  of the same group  $G$  are called *equivalent* if there exists a non-singular matrix  $A \in GL_n$  with the property

$$g\theta_2 = A^{-1}(g\theta_1)A \quad \text{for all } g \in G. \quad (13.1)$$

The relation defined by (13.1) is an equivalence relation (see Definition A1 in Appendix A), the reader should check this.

---

<sup>1</sup> In vector space theory the term ‘direct sum’ is normally used instead of ‘direct product’, see Chapter 7.

*Example.* We give below four representations of the dihedral group  $D_3 = \langle a, b \mid a^3 = b^2 = e, bab = a^2 \rangle$ .

(a) The homomorphism which maps every element of  $D_3$  to  $I_4$ , the  $4 \times 4$  identity matrix, is the trivial representation of  $D_3$  of degree 4.

(b) If we map  $a \mapsto (1)$  and  $b \mapsto (-1)$ , then the corresponding representation is non-faithful (reader, why?) and it has degree 1.

(c) Let  $\omega = e^{2\pi i/3}$  (so  $\omega \in \mathbb{C}$  and  $\omega^3 = 1$ ), and let the representation  $\theta_1$  be given by

$$a\theta_1 = \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix} \quad \text{and} \quad b\theta_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

with an extension to all of  $D_3$  using the homomorphism equation. It is faithful and has degree 2.

(d) The mapping  $\theta_2$  from  $D_3$  to  $GL_2$  given by

$$\begin{aligned} e &\mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & a &\mapsto \begin{pmatrix} \omega & 2\omega(1-\omega) \\ 0 & \omega^2 \end{pmatrix} & a^2 &\mapsto \begin{pmatrix} \omega^2 & 2\omega(\omega-1) \\ 0 & \omega \end{pmatrix} \\ b &\mapsto \begin{pmatrix} 2 & 5 \\ -1 & -2 \end{pmatrix} & ab &\mapsto \begin{pmatrix} 2\omega & \omega(4+\omega) \\ -\omega & -2\omega \end{pmatrix} & a^2b &\mapsto \begin{pmatrix} 2\omega^2 & \omega(4\omega+1) \\ -\omega^2 & -2\omega^2 \end{pmatrix}, \end{aligned}$$

provides another faithful degree 2 representation of  $D_3$  which is equivalent to the representation  $\theta_1$  defined in (c) above. In fact, if we let  $A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ , then  $g\theta_2 = A^{-1}g\theta_1A$  for all  $g \in D_3$  as the reader can check.

## Introduction to $G$ -modules

We usually discuss representations of a group  $G$  via  $G$ -modules. A  $G$ -module  $V$  is a ‘hybrid’ system in which  $G$  acts on the vector space  $V$ , and these actions are also linear maps on  $V$ . In the theorems in this section we show that a representation of  $G$  can be interpreted as a  $G$ -module and vice versa, and equivalent representations are associated with the ‘same’  $G$ -module.

**Definition 13.2** A vector space  $V$  defined over  $\mathbb{C}$  is called a  $G$ -module<sup>2</sup> if a ‘product’ of the form  $vg$  is defined which satisfies the following five conditions for all  $u, v \in V$ ,  $c \in \mathbb{C}$  and  $g, h \in G$ :

- (i)  $vg \in V$ ,
- (ii)  $(u + v)g = ug + vg$ ,    (iii)  $(cv)g = c(vg)$ ,
- (iv)  $ve = v$ ,    and    (v)  $v(gh) = (vg)h$ .

By (i), (ii) and (iii) the map  $v \mapsto vg$  is a linear map on the vector space  $V$ , and (iv) and (v) give an action of  $G$  on the ‘set’  $V$ .

*Examples.* (a) The vector space  $\langle v \rangle$  generated by  $v$  with  $vg = v$  for  $g \in G$  and  $v \in V$  is clearly a  $G$ -module, it is called a *trivial  $G$ -module*.

<sup>2</sup> Technically this is a *right  $G$ -module*.

(b) The 0-dimensional vector space  $\langle 0 \rangle$ , with  $0g = 0$  for all  $g \in G$  also clearly forms a  $G$ -module which we call the *zero  $G$ -module*.

(c) The *standard example* Let  $V = \mathbb{C}^n$  with a representation  $\theta : G \rightarrow GL_n$ . Define the product  $vg$  by

$$vg = v(g\theta).$$

The properties (i) to (v) above follow immediately as  $V$  is a vector space and  $\theta$  is a homomorphism.

(d) *Permutation module* Let  $G = S_3$  and let  $V$  be a 3-dimensional vector space with basis  $\{v_1, v_2, v_3\}$ . For  $g \in S_3$  ( $g$  is a permutation of  $\{1, 2, 3\}$ ) define

$$v_i g = v_{ig}, \quad \text{for } i = 1, 2, 3.$$

Clearly  $v_i e = v_i$ , and for  $g, h \in S_3$

$$v_i gh = v_{i(gh)} = v_{(ig)h} = (v_i g)h.$$

By linearity this can be extended to give a  $S_3$ -module. Similar examples can be constructed for  $S_n$ ,  $n = 4, 5, \dots$ , and their subgroups.

(e) The *regular  $G$ -module*  $\mathbb{C}G$  Construct the vector space  $W$  with basis  $\{g_1 = e, \dots, g_n\}$  where  $g_i \in G$  and  $o(G) = n$ , the elements of  $W$  have the form  $v = c_{i_1}g_{i_1} + \dots + c_{i_k}g_{i_k}$  where  $c_{i_j} \in \mathbb{C}$ ,  $g_{i_j} \in G$ , and  $\{i_1, \dots, i_k\} \subseteq \{1, \dots, n\}$ . (Think of  $v$  as the vector  $(c_{i_1}, \dots, c_{i_j})$  where the elements of  $G$  determine the position of its entries.) Using Theorem 2.8, the module product is given by

$$vh = c_{i_1}g_{i_1}h + \dots + c_{i_k}g_{i_k}h \quad \text{where } h \in G.$$

Check that the module axioms (Definition 13.2) hold, see Problem 13.1.

Different matrices can represent the same linear map on  $V$ , this is related to the choice of bases for  $V$ . Hence we need to bring these bases into our theory. Using  $G$ -modules avoids this, but in some cases we need to consider the underlying spaces, see Definition 13.1(iv) and Theorem 13.4. Given a  $G$ -module  $V$ , the map  $v \mapsto vg$  is a linear map by definition, and so if  $V$  has a basis  $\mathcal{B}$ , this map is represented by a matrix depending on  $\mathcal{B}$ . We denote this  $n \times n$  matrix (where  $n = \dim V$ ) by

$$(g; \mathcal{B}).$$

**Theorem 13.3** (i) Suppose  $\theta : G \rightarrow GL_n$  is a representation of  $G$ . Let  $V = \mathbb{C}^n$  be a copy of the  $n$ -dimensional vector space over  $\mathbb{C}$ . The space  $V$  becomes a  $G$ -module if we define the module product  $vg$  by

$$vg = v(g\theta) \quad \text{for } v \in V \text{ and } g \in G. \quad (13.2)$$

Also there is a basis  $\mathcal{B}$  for  $V$  which satisfies

$$g\theta = (g; \mathcal{B}) \quad \text{for all } g \in G. \quad (13.3)$$

(ii) Conversely, if  $V$  is a  $G$ -module with basis  $\mathcal{B}$ , then the map

$$g \mapsto (g; \mathcal{B}) \quad \text{where } g \in G$$

defines a representation of  $G$ .

*Proof.* (i) We need to verify the five conditions in Definition 13.2. The first follows by definition, the second and third follow using matrix addition and scalar multiplication, and the last two follow because the representation  $\theta$  is a group homomorphism. Hence  $V$  is a  $G$ -module with the product given by (13.2). If we take  $\mathcal{B} = \{(1, 0, \dots, 0), \dots, (0, \dots, 0, 1)\}$  as the basis for  $V$ , then (13.3) also follows.

(ii) As  $V$  is a  $G$ -module with basis  $\mathcal{B}$ , we have  $v(gh) = (vg)h$  for  $g, h \in G$  and  $v \in \mathcal{B}$ . Hence by linearity

$$(gh; \mathcal{B}) = (g; \mathcal{B})(h; \mathcal{B}) \quad \text{and so} \quad (e; \mathcal{B}) = (g; \mathcal{B})(g^{-1}; \mathcal{B})$$

for  $g \in G$ . But  $ve = v$  for  $v \in V$ , and so  $(e; \mathcal{B}) = I_n$ , the  $n \times n$  identity matrix. This shows that  $(g; \mathcal{B})$  is invertible, and so it belongs to  $GL_n$ ; that is the map  $g \mapsto (g; \mathcal{B})$  gives a representation of  $G$ .  $\square$

We now consider equivalent representations, see Definition 13.1(iv), and Examples (c) and (d) on page 403.

**Theorem 13.4** Suppose  $V$  is a  $G$ -module with basis  $\mathcal{B}$  and  $\theta : G \rightarrow GL_n$  is a representation of  $G$ .

(i) If  $\mathcal{B}_1$  is another basis for  $V$ , then the representation  $\theta_1$  of  $G$  given by

$$g\theta_1 = (g; \mathcal{B}_1) \quad \text{for all } g \in G$$

is equivalent to  $\theta$ .

(ii) If  $\theta_2$  is a representation of  $G$  which is equivalent to  $\theta$ , then there exists a basis  $\mathcal{B}_2$  of  $V$  which satisfies

$$g\theta_2 = (g; \mathcal{B}_2) \quad \text{for all } g \in G.$$

*Proof.* (i) Let  $C$  be the non-singular matrix which transforms the basis  $\mathcal{B}$  (of  $V$ ) to the basis  $\mathcal{B}_1$ . Then we have

$$(g; \mathcal{B}) = C^{-1}(g; \mathcal{B}_1)C$$

for all  $g \in G$  (see (13.3)) which shows immediately that  $\theta$  and  $\theta_1$  are equivalent.

(ii) As  $\theta$  and  $\theta_2$  are equivalent, we can find a non-singular matrix  $C'$  to satisfy

$$g\theta = (C')^{-1}(g\theta_2)C'$$

for all  $g \in G$ . Now let  $\mathcal{B}_2$  be the basis of  $V$  formed by applying  $C'$  to the basis  $\mathcal{B}$ . Then the equation in (i) gives  $(g; \mathcal{B}) = (C')^{-1}(g; \mathcal{B}_2)C'$ , from which we obtain  $g\theta_2 = (g; \mathcal{B}_2)$  for all  $g \in G$ .  $\square$

See Example (d) on page 403, here if we take  $\mathcal{B} = \{(1, 0), (0, 1)\}$  and  $C = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}$ , then  $\mathcal{B}_2 = \{(1, 2), (0, 1)\}$ .

Subsystems of  $G$ -modules are given by the following

**Definition 13.5** A subset  $U$  of a  $G$ -module  $V$  is called a  $G$ -submodule of  $V$  if (a)  $U$  is a (vector) subspace of  $V$ , and (b)  $ug \in U$  for  $u \in U$  and  $g \in G$ .

We shall see below that  $G$ -submodules of a  $G$ -module behave much like normal subgroups in a group. Some examples are given after the next definition.

We look now at the natural maps between modules.

**Definition 13.6** (i) A map  $\phi : V_1 \rightarrow V_2$ , where  $V_1$  and  $V_2$  are  $G$ -modules, is called a  $G$ -homomorphism if it is a linear map between  $V_1$  and  $V_2$  (considered as vector spaces), and for all  $v \in V_1$  and  $g \in G$  we have

$$(vg)\phi = (v\phi)g.$$

The *kernel* and *image* are defined as for group homomorphisms, that is  $\ker \phi = \{v \in V_1 : v\phi = 0\}$  and  $\text{im } \phi = \{v\phi : v \in V_1\}$ .

(ii) A  $G$ -homomorphism  $\phi$  is called a  $G$ -isomorphism if  $\phi$  is an invertible linear map; in this case we write  $V_1 \cong V_2$ .

*Examples.* (a) Let  $V$  be a  $G$ -module and  $c \in \mathbb{C}$ . The map  $\theta_1$  given by  $v\theta_1 = cv$ , for  $v \in V$ , is a  $G$ -homomorphism. The reader should check this and find the kernel and image; see Problem 13.1.

(b) Let  $V$  be the permutation module given in Example (d) on page 404 and let  $U = \langle u \rangle$  be a trivial  $G$ -module; see Example (a) given at the bottom of page 403. Define  $\theta_2$  by

$$(c_1v_1 + c_2v_2 + c_3v_3)\theta_2 = (c_1 + c_2 + c_3)u, \quad \text{where } c_i \in \mathbb{C}.$$

So  $v_i\theta_2 = u$  for  $i = 1, 2$  and  $3$ . Clearly  $\theta_2$  is linear, and if  $v = \sum_{i=1}^3 c_i v_i$  and  $g \in S_3$ , then

$$\begin{aligned} (vg)\theta_2 &= (c_1v_{1g} + c_2v_{2g} + c_3v_{3g})\theta_2 = (c_1 + c_2 + c_3)u, \quad \text{and} \\ (v\theta_2)g &= (c_1 + c_2 + c_3)ug = (c_1 + c_2 + c_3)u. \end{aligned}$$

In the first line above  $(1g, 2g, 3g)$  is a permutation of  $(1, 2, 3)$  as the group is  $S_3$  in this example. Hence  $\theta_2$  is a  $S_3$ -homomorphism, the kernel is  $\{c_1v_1 + c_2v_2 + c_3v_3 : c_1 + c_2 + c_3 = 0\}$ , and the image is  $U$ . We shall return to this useful example later.

The following result is important, note that unlike normal subgroups in the group case, both the kernel and the image of  $\phi$  are  $G$ -submodules.

**Theorem 13.7** Suppose  $V_1$  and  $V_2$  are  $G$ -modules and  $\phi : V_1 \rightarrow V_2$  is a  $G$ -homomorphism.

- (i)  $\ker \phi$  is a  $G$ -submodule of  $V_1$ , and  $\text{im } \phi$  is a  $G$ -submodule of  $V_2$ .
- (ii) If  $\phi$  is a  $G$ -isomorphism, then the map  $\phi^{-1} : V_2 \rightarrow V_1$  is also a  $G$ -isomorphism.

*Proof.* (i) Both  $\ker \phi$  and  $\operatorname{im} \phi$  are (vector) subspaces as  $\phi$  is a linear map. Secondly, if  $v \in \ker \phi$  and  $g \in G$ , then using Definition 13.6 we have

$$(vg)\phi = (v\phi)g = 0g = 0 \quad \text{and so} \quad vg \in \ker \phi,$$

that is  $\ker \phi$  is a  $G$ -submodule of  $V_1$ . Further if  $v' \in \operatorname{im} \phi$ , then we can find  $u \in V_1$  to satisfy  $v' = u\phi$ , and

$$v'g = (u\phi)g = (ug)\phi \in \operatorname{im} \phi,$$

that is  $\operatorname{im} \phi$  is a  $G$ -submodule of  $V_2$ .

(ii)  $\phi^{-1}$  is a non-singular linear map by definition (see Appendix A). Also for  $v \in V_2$  and  $g \in G$  we have, as  $\phi$  is a  $G$ -homomorphism,

$$((v\phi^{-1})g)\phi = ((v\phi^{-1})\phi)g = vg = ((vg)\phi^{-1})\phi.$$

But  $\phi$  is a  $G$ -isomorphism, and so the result follows.  $\square$

For an example see (b) on page 406.

The following will be useful later, it shows that representations are equivalent if, and only if, the corresponding modules are isomorphic.

**Theorem 13.8** *Suppose  $V_1$  and  $V_2$  are  $G$ -modules.*

(i)  $V_1 \cong V_2$  if, and only if, there are bases  $\mathcal{B}_i$  for  $V_i$ ,  $i = 1, 2$ , which satisfy, for all  $g \in G$ ,

$$(g; \mathcal{B}_1) = (g; \mathcal{B}_2). \quad (13.4)$$

(ii) If  $V_1$  has basis  $\mathcal{B}$  and  $V_2$  has basis  $\mathcal{B}'$ , then the representations

$$\theta_1 : g \mapsto (g; \mathcal{B}) \quad \text{and} \quad \theta_2 : g \mapsto (g; \mathcal{B}')$$

are equivalent if, and only if,  $V_1 \cong V_2$ .

*Proof.* (i) Suppose  $\phi : V_1 \rightarrow V_2$  is a  $G$ -isomorphism, and  $\{v_1, \dots, v_n\}$  is the basis  $\mathcal{B}_1$ . For  $g \in G$  and  $i = 1, \dots, n$  we have

$$v_i g = c_{i1}v_1 + \dots + c_{in}v_n.$$

Let  $w_i = v_i\phi$  where  $c_{ij} \in \mathbb{C}$  and  $w_i \in V_2$ . Then

$$\begin{aligned} w_i g &= (v_i\phi)g = (v_i g)\phi = (c_{i1}v_1 + \dots + c_{in}v_n)\phi \\ &= c_{i1}v_1\phi + \dots + c_{in}v_n\phi = c_{i1}w_1 + \dots + c_{in}w_n. \end{aligned}$$

As this holds for each  $i$  the result follows by linearity.

Conversely, suppose  $\mathcal{B}_1 = \{v_1, \dots, v_n\}$  is a basis for  $V_1$  and  $\mathcal{B}_2 = \{w_1, \dots, w_n\}$  is a basis for  $V_2$  both of which satisfy (13.4) for all  $g \in G$ . Further, suppose  $\psi$  is the non-singular linear map given by  $v_i\psi = w_i$  for  $i = 1, \dots, n$ . Now using (13.4) we have  $(v_i g)\psi = (v_i\psi)g$  for each  $i = 1, \dots, n$  and  $g \in G$ . Hence  $\psi$  is a  $G$ -isomorphism, and (i) follows.

(ii) This follows by (i) and Theorem 13.4.  $\square$

## 13.2 Theorems of Schur and Maschke

We begin with

**Definition 13.9** A non-zero  $G$ -module  $V$  is called *irreducible*, or sometimes *simple*, if it contains no  $G$ -submodules apart from  $\langle 0 \rangle$  and  $V$ , otherwise it is called *reducible*.

A vector space  $V$  (with  $\dim V = n$ ) defined over a field  $F$  is isomorphic to  $F^n$ , the direct sum of  $n$  copies of the field  $F$  – it is isomorphic to a direct sum of  $n$  subspaces each with dimension 1. A similar result holds for  $G$ -modules except that the summands often have dimension larger than one because the summands in question are irreducible (Definition 13.9), and so they have no proper non-zero submodules. There is an analogy here with integer unique factorisation. The module result follows from the theorems of I. Schur and H. Maschke to be proved in this section. We begin with Schur's Lemma which characterises irreducible modules. We use the symbol  $\iota_V$  to denote the identity (linear) map on  $V$  ( $v\iota_V = v$  for all  $v \in V$ ).

**Theorem 13.10** (Schur's Lemma) *Suppose  $V_1$  and  $V_2$  are irreducible  $G$ -modules.*

- (i) *A  $G$ -homomorphism  $\phi : V_1 \rightarrow V_2$  is either a  $G$ -isomorphism or the trivial homomorphism:  $v\phi = 0$ , for all  $v \in V_1$ .*
- (ii) *A  $G$ -isomorphism  $\psi : V_1 \rightarrow V_1$  is a scalar multiple of the identity map  $\iota_{V_1}$ .*

*Proof.* (i) Suppose  $\phi$  is not the trivial homomorphism. So there exists  $v \in V$  satisfying  $v\phi \neq 0$  which implies  $\text{im } \phi \neq \langle 0 \rangle$ . Hence by Theorem 13.7, and as  $V_2$  is irreducible, we have  $\text{im } \phi = V_2$ . Using Theorem 13.7 again, this shows that  $\ker \phi \neq V_1$ , and so  $\ker \phi = \langle 0 \rangle$  as  $V_1$  is irreducible; that is  $\phi$  is a  $G$ -isomorphism, see Definition 13.6.

(ii) A non-singular linear map on  $V_1$  has at least one eigenvalue  $c$  in the complex field  $\mathbb{C}$ . This follows because  $\mathbb{C}$  is algebraically closed, and as a consequence a non-zero eigenvector also exists. This shows that  $\ker(\psi - c\iota_{V_1}) \neq \langle 0 \rangle$ . The module  $V_1$  is irreducible, and so by Theorem 13.7,  $\ker(\psi - c\iota_{V_1}) = V_1$  which gives the result.  $\square$

Both the the matrix version and the converse of this result are given in Problem 13.4.

*Example.* We apply the matrix version of Schur's result given in Problem 13.4. Let  $C_4 = \langle a : a^4 = e \rangle$ , and define a representation  $\sigma : C_4 \rightarrow GL_2$  by

$$a\sigma = \begin{pmatrix} i & 0 \\ 0 & -1 \end{pmatrix}.$$

Now the matrix  $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$  commutes with  $g\sigma$  for all  $g \in C_4$ , and so by the matrix version of Schur's Lemma it follows that the  $C_4$ -module associated with  $\sigma$  is reducible. This also follows from the theorem below or by direct calculation using the subspaces  $\langle (1, 0) \rangle$  and  $\langle (0, 1) \rangle$ .

An almost immediate consequence of Schur's result shows that all irreducible representations of a finite Abelian group have degree 1 as we prove now.

**Theorem 13.11** *If  $G$  is Abelian, then every irreducible  $G$ -module has dimension 1.*

*Proof.* If  $V$  is an irreducible  $G$ -module and  $a \in G$ , then

$$(vg)a = (va)g \quad \text{for all } g \in G$$

as  $G$  is Abelian. Hence the non-singular linear map  $v \mapsto va$  is a  $G$ -homomorphism (Definition 13.6), and so by Schur's Lemma

$$va = c^*v \quad \text{for some suitably chosen } c^* \in \mathbb{C} \text{ depending on } a.$$

But  $V$  is irreducible, and so  $\dim V = 1$ ; for if not  $V$  would contain a 1-dimensional submodule.  $\square$

Using this result we can list the irreducible representations of a cyclic group as follows: Let  $G = C_n = \langle a \rangle$ , let  $\omega = e^{2\pi i/n}$ , and let  $r$  satisfy  $1 \leq r < n$ , then the  $r$ -th irreducible representation  $\theta_r$  of  $G$  is given by

$$a^s \theta_r = \omega^{rs} \quad \text{for } 0 \leq s < n.$$

These equations do indeed give the irreducible representations of  $G$  as each have degree 1. Using this and the Fundamental Theorem of Abelian Groups (Theorem 7.12) all irreducible representations of a finite Abelian group can be given. Theorem 13.11 is sufficient for our purposes, more details can be found in the references quoted at the beginning of this chapter.

### ***Maschke's Theorem***

If  $V$  is a  $G$ -module and  $U_1$  is a submodule, we can always find another submodule  $U_2$  so that  $V = U_1 \oplus U_2$ , the direct sum of  $U_1$  and  $U_2$ . We give this remarkable result now, it was first proved by Maschke in 1898. The proof is constructive providing a method for building  $U_2$  given  $U_1$  and  $V$ .

**Theorem 13.12** (Maschke's Theorem) *If  $U_1$  is a  $G$ -submodule of the  $G$ -module  $V$ , then we can find another  $G$ -submodule  $U_2$  of  $V$  to satisfy*

$$V = U_1 \oplus U_2.$$

Note that Maschke's result is invalid if the group  $G$  is infinite, or if  $o(G)$  is finite AND we work over a field of positive characteristic  $p$  where  $p \mid o(G)$ .

*Proof.* Note first that  $U_1$  is a *subspace* (of  $V$ ), let  $\{u_1, \dots, u_r\}$  be a basis. By a standard property of vector spaces we can find vectors  $u_{r+1}, \dots, u_n \in V \setminus U_1$  so that  $\{u_1, \dots, u_r, u_{r+1}, \dots, u_n\}$  is a basis for  $V$ . Let  $W$  be the subspace of  $V$  generated by the set  $\{u_{r+1}, \dots, u_n\}$ . Then



$$V = U_1 \oplus W, \quad (13.5)$$

that is the vector space  $V$  is isomorphic to the direct sum of the subspaces  $U_1$  and  $W$ . To prove the theorem we ‘adjust’  $W$  so that it forms a submodule whilst insuring that (13.5) still holds.

If  $v \in V$ , then  $v$  can be expressed in the form  $v = u + w$  where  $u \in U_1$ ,  $w \in W$ , and both  $u$  and  $w$  are *unique*; this follows because the sum in (13.5) is direct. Hence the map  $\psi : V \rightarrow V$  given by  $v\psi = u$  where  $v \in V$  is well-defined and linear, it has kernel  $W$  and image  $U_1$ . The ‘adjustment’ mentioned above is constructed using the map  $\phi$  on  $V$  which is defined as follows. If  $g \in G$  and  $v \in V$ , let

$$v\phi = \frac{1}{o(G)} \sum_{g \in G} vg\psi g^{-1}. \quad (13.6)$$

Note that (a) by our convention,  $vg\psi g^{-1} = ((vg)\psi)g^{-1}$  using the product in  $V$ , and (b) if  $\psi$  is a  $G$ -homomorphism then  $\phi = \psi$ . In general  $\psi$  is not a  $G$ -homomorphism, but it is a linear map on  $V$  whose image is contained in  $U_1$ . On the other hand  $\phi$  is a  $G$ -homomorphism as we show now.

If  $j \in G$ , we have  $(vj)g\psi g^{-1} = v(jg)\psi g^{-1}j^{-1}j = (vh\psi h^{-1})j$  provided  $h = jg$  by (v) in Definition 13.2. Hence

$$(vj)\phi = \frac{1}{o(G)} \sum_{g \in G} (vj)g\psi g^{-1} = \frac{1}{o(G)} \sum_{h \in G} (vh\psi h^{-1})j = (v\phi)j$$

by Theorem 2.8, that is  $\phi$  is a  $G$ -homomorphism. The map  $\phi$  is also idempotent, that is it satisfies

$$\phi^2 = \phi. \quad (13.7)$$

For if  $u \in U_1$  and  $g \in G$ , then  $ug \in U_1$  (as  $U_1$  is a  $G$ -module), and so  $(ug)\psi = ug$  and  $((ug)\psi)g^{-1} = u$ . Hence

$$u\phi = \frac{1}{o(G)} \sum_{g \in G} ug\psi g^{-1} = \frac{1}{o(G)} \sum_{g \in G} u = u. \quad (13.8)$$

Now if  $v \in V$ ,  $v\phi \in U_1$  (by definition of  $U_1$  and (13.6)), and so  $(v\phi)\phi = v\phi$  by (13.8). This holds for all  $v \in V$ , hence (13.7) follows. By Problem A4(iii) in Appendix A, this shows that  $\phi$  is a projection of  $V$  onto  $U_1$ . As it is also a  $G$ -homomorphism, we can now define  $U_2 = \ker \phi$ , then  $U_2$  is a  $G$ -submodule by Theorem 13.3, and so finally  $V = U_1 \oplus U_2$ , a direct sum of two  $G$ -submodules.  $\square$

*Example.* We extend Examples (d) on page 404 and (b) on page 406 concerning the permutation module  $V$  for  $S_3$ . We showed in the second of these examples that  $U_1 = \langle v_1 + v_2 + v_3 \rangle$  is a  $G$ -submodule of  $V$ , so by Maschke’s Theorem above, there exists another  $G$ -submodule  $U_2$  with the property  $V = U_1 \oplus U_2$ . Following the procedure given in the proof above, let

$W = \langle v_2, v_3 \rangle$ . As subspaces  $V = U_1 \oplus W$ , but  $W$  is not a  $G$ -submodule. The projection map  $\psi$  from  $V$  to  $U_1$  given by

$$v_1\psi = v_1 + v_2 + v_3, v_2\psi = 0, v_3\psi = 0$$

is a  $G$ -homomorphism, see Problem 13.1. Again following the proof of Maschke's Theorem above let  $\phi$  be defined by

$$v_i\phi = \frac{1}{3}(v_1 + v_2 + v_3) \quad \text{for } i = 1, 2, 3.$$

This is a  $G$ -homomorphism, and its kernel is a  $G$ -submodule of  $V$  (by Theorem 13.3) which we can take to be  $U_2$ . In fact we can set

$$U_2 = \ker \phi = \langle v_2 - v_1, v_3 - v_1 \rangle.$$

Our first application gives the following important theorem, to state it we need

**Definition 13.13** A  $G$ -module is called *completely reducible*, or sometimes *semi-simple*, if it can be expressed as a direct sum  $V = U_1 \oplus \cdots \oplus U_n$  where each  $U_i$  is irreducible and  $n \geq 1$ .

**Theorem 13.14** *Every non-zero  $G$ -module is completely reducible.*

As with Maschke's Theorem this result fails if we change our underlying field  $\mathbb{C}$  to one with positive characteristic  $p$  where  $p \mid o(G)$ , even if it is algebraically closed.

*Proof.* If  $V$  is irreducible, there is nothing to prove. Hence we may suppose  $V$  contains a proper non-zero  $G$ -submodule  $U_1$ . By Maschke's Theorem (Theorem 13.12) we can find another  $G$ -submodule  $U_2$  to satisfy  $V = U_1 \oplus U_2$ . If both  $U_1$  and  $U_2$  are irreducible then we are done, if not we can use induction on the dimension of  $V$  as both  $U_1$  and  $U_2$  have smaller dimension than  $\dim V$ .  $\square$

Our second application of Maschke's Theorem shows we can sometimes assume that the matrices  $(g; \mathcal{B})$  used in Theorem 13.3 are diagonal provided we choose the 'right' basis  $\mathcal{B}$ . But note this result only applies to *individual* elements  $g$  in  $G$ .

**Theorem 13.15** *Suppose  $V$  is a non-zero  $G$ -module and  $g \in G$ .*

- (i) *We can find a basis  $\mathcal{B}$  for  $V$  so that  $(g; \mathcal{B})$  is diagonal.*
- (ii) *The diagonal entries of the matrix given in (i) are  $m$ -th roots of unity where  $g$  has order  $m$  in  $G$ .*

*Proof.* Let  $J$  be the cyclic subgroup of  $G$  generated by  $g$  with order  $m$ , and let  $W$  be a non-zero  $J$ -module. By Theorem 13.14 we can write  $W$  as

$$W = U_1 \oplus \cdots \oplus U_t,$$

where each  $U_i$  is irreducible. As  $J$  is Abelian we have by Theorem 13.11,  $\dim U_i = 1$  for  $i = 1, \dots, t$ ; and so each  $U_i$  has a single generating vector  $u_i$ , say. Hence as  $U_i$  is a  $G$ -module of dimension 1 (and so is automatically irreducible). Further, by Schur's Lemma (Theorem 13.10) we can find integers  $r_j$  to satisfy

$$u_j g = \omega^{r_j} u_j \quad (13.9)$$

for each  $i$  where  $\omega = e^{2\pi i/m}$ . Note  $r_i \in \mathbb{Z}$ , this follows from the comment below the proof of Theorem 13.11. Therefore if we take  $\{u_1, \dots, u_t\}$  as the basis  $\mathcal{B}$  for  $W$ , then (13.9) gives

$$(g; \mathcal{B}) = \begin{pmatrix} \omega^{r_1} & 0 & \dots & 0 \\ 0 & \omega^{r_2} & \dots & 0 \\ \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & \omega^{r_t} \end{pmatrix}.$$

Both parts of the theorem now follow.  $\square$

### 13.3 Characters and Orthogonality Relations

Characters will be introduced now and their basic orthogonality properties will be established. The work is of a similar level to that of the previous sections, but some proofs are quite long and involved, so time will be needed to assimilate them; writing them out in detail in the  $2 \times 2$  case can sometimes help. The *trace* of a matrix  $A$ ,  $\text{tr}(A)$  is defined as the sum of the main diagonal elements of  $A$ : If  $A = (a_{ij})$ , then  $\text{tr}(A) = \sum_{i=1}^n a_{ii}$ . We have, for square matrices  $A$  and  $B$ , see Problem 13.7,

$$\begin{array}{ll} \text{(a)} & \text{tr}(A + B) = \text{tr}(A) + \text{tr}(B), \quad \text{(b)} \quad \text{tr}(cA) = c \text{tr}(A) \text{ for } c \in \mathbb{C}, \\ \text{(c)} & \text{tr}(AB) = \text{tr}(BA), \quad \text{(d)} \quad \text{tr}(B^{-1}AB) = \text{tr}(A). \end{array}$$

These properties are used widely in the sequel. In both linear algebra and our representation theory it is surprising how much information about a matrix is retained by the trace. Below we define the character of a representation as the trace of the corresponding matrix, and we call a character *irreducible* if its corresponding  $G$ -module is irreducible. Each group  $G$  has attached to it a collection of irreducible characters, and many of the properties of  $G$  can be obtained by studying this collection.

**Definition 13.16** Let  $G$  be a finite group.

(i) A *class function*  $\psi$  on  $G$  is a function mapping the elements of  $G$  into  $\mathbb{C}$  which takes the same value for each element of a conjugacy class of  $G$ : If  $j = h^{-1}gh$  and  $g, h, j \in G$ , then  $\psi(j) = \psi(g)$ . The collection of all class functions on  $G$  is denoted by  $CF(G)$ .

(ii) If  $V$  is a non-zero  $G$ -module and  $\theta$  is a corresponding representation (Theorem 13.3), then the function  $\chi$  mapping elements of  $G$  to  $\mathbb{C}$  defined by

$$\chi(g) = \text{tr}(g\theta) \quad \text{for } g \in G$$

is called the *character* of the  $G$ -module  $V$ , and of the representation  $\theta$  (Theorem 13.17(ii)). The *degree* of the character  $\chi$  is the degree of the corresponding representation, if  $g\theta$  is an  $n \times n$  matrix then the degree of  $\chi$  is  $n$ .

(iii) The character of the trivial representation of  $G$ ,  $1_G$ , is called the *principal character*,<sup>3</sup> and  $1_G = 1$  for all  $g \in G$ . In character tables  $1_G$  is usually written as  $\chi_1$ .

*Example.* Consider the representation given in Example (c) on page 403. The character  $\chi$  of this representation of  $D_3 (\simeq S_3)$  is calculated as follows. We have  $\chi(e) = \text{tr}(I_2) = 2$ , and

$$\chi(a) = \text{tr}\left(\begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}\right) = \omega + \omega^2 = -1, \quad \chi(b) = \text{tr}\left(\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right) = 0.$$

Similar calculations which the reader should check show that  $\chi(a^2) = -1$  and  $\chi(ab) = \chi(a^2b) = 0$ . Note that (a)  $\chi$  is constant on the conjugacy classes of  $D_3$ , and (b) we obtain the same values for  $\chi$  if we use the equivalent representation for  $D_3$  given in Example (d) on page 404; reader check. This character for  $D_3$  is called the *minor permutation* character (Problem 13.16).

We shall see later that  $CF(G)$  can be treated as a vector space over  $\mathbb{C}$ , and the irreducible characters to be defined below act as a basis for this space. The simplest character properties are as follows, note particularly (ii) below, it shows that equivalent representations have the same character.

**Theorem 13.17** (i) A character  $\chi$  for  $G$  is a class function for  $G$ .

(ii) If  $V_1$  and  $V_2$  are isomorphic  $G$ -modules, then their characters are equal.

(iii) If  $V_i$  are  $G$ -modules with characters  $\chi_i$ , where  $1 \leq i \leq m$ , and  $V = V_1 \oplus \cdots \oplus V_m$ , then the character  $\chi$  of  $V$  is given by

$$\chi = \sum_{i=1}^m \chi_i.$$

*Proof.* (i) Let  $\theta$  be a representation of  $G$  corresponding to the  $G$ -module  $V$ , and suppose  $g\theta = (g; \mathcal{B})$ , see Theorem 13.4, then for  $a, g \in G$  we have using properties of the trace function given opposite and the fact that  $\theta$  is a homomorphism,

$$\begin{aligned} \chi(a^{-1}ga) &= \text{tr}(a^{-1}ga\theta) = \text{tr}((a\theta)^{-1}g\theta a\theta) \\ &= \text{tr}((a; \mathcal{B})^{-1}(g; \mathcal{B})(a; \mathcal{B})) = \text{tr}(g; \mathcal{B}) = \text{tr}(g\theta) = \chi(g). \end{aligned}$$

<sup>3</sup> Some authors use the term *trivial character* but this gives the wrong impression for it is the only character which is attached to every group, and so it plays a more important role in character theory than the trivial homomorphism does in group theory as a whole.

(ii) By Theorem 13.8 we can find bases  $\mathcal{B}_1$  for  $V_1$  and  $\mathcal{B}_2$  for  $V_2$  with the property  $(g; \mathcal{B}_1) = (g; \mathcal{B}_2)$  for all  $g \in G$ . Now if we take the trace of each of these matrices we obtain the result.

(iii) We can choose a basis for  $V$  so that the matrix of the representation associated with the  $G$ -module  $V$  is in diagonal block form where the  $i$ -th block is the matrix corresponding to the  $G$ -module  $V_i$ . It is now clear that the trace of the matrix for  $V$  is the sum of the traces of the individual blocks.  $\square$

## Orthogonality Relations

The orthogonality relations are amongst the most important tools in character theory, we shall develop them now. We use the following standard conventions: (a) the notation  $(a_{ij})$  stands for the matrix whose  $(i, j)$ th entry is  $a_{ij}$ , a complex number, and (b) the *delta function*  $\delta_{ij}$  stands for the function which takes the value 1 if  $i = j$ , and 0 if  $i \neq j$ .

The first orthogonality relation is given by the following

**Theorem 13.18** *Suppose  $\theta_1$  and  $\theta_2$  are irreducible representations of  $G$  with corresponding  $G$ -modules  $V_1$  and  $V_2$ , and degrees  $n_1$  and  $n_2$ , respectively. Further suppose their representing matrices are given by*

$$g\theta_1 = (a_{ij}(g)) \quad \text{and} \quad g\theta_2 = (b_{ij}(g)) \quad \text{for } g \in G.$$

*If  $\theta_1$  and  $\theta_2$  are not equivalent, and so  $V_1 \not\cong V_2$ , then for all  $i, j, k$  and  $l$*

$$\begin{aligned} \text{(i)} \quad & \sum_{g \in G} a_{ij}(g)b_{kl}(g^{-1}) = 0, \\ \text{(ii)} \quad & \sum_{g \in G} a_{ij}(g)a_{kl}(g^{-1}) = \delta_{jk}\delta_{il}o(G)/n_1. \end{aligned}$$

*Proof.* Let  $C = (c_{jk})$  be an arbitrary  $n_1 \times n_2$  matrix, and let

$$D(C) = \sum_{g \in G} (a_{ij}(g))C(b_{kl}(g^{-1})).$$

This is also an  $n_1 \times n_2$  matrix. We show first that  $D(C)$  represents a  $G$ -homomorphism, a consequence of the following calculation. We have, for all  $h \in G$ ,

$$\begin{aligned} (a_{ij}(h))D(C) &= \sum_{g \in G} (a_{ij}(h))(a_{ij}(g))C(b_{kl}(g^{-1}))(b_{kl}(h^{-1}))(b_{kl}(h)) \\ &= \sum_{g \in G} (a_{ij}(hg))C(b_{kl}((hg)^{-1}))(b_{kl}(h)) \\ &\quad \text{as } \theta_1 \text{ and } \theta_2 \text{ are homomorphisms} \\ &= D(C)(b_{kl}(h)) \end{aligned} \tag{13.10}$$

by Theorem 2.8 as  $(b_{kl}(h))^{-1} = (b_{kl}(h^{-1}))$  by Theorem 13.3. Hence  $D(C)$  defines a  $G$ -homomorphism.

(i) By Schur's Lemma (Theorem 13.10), as both  $V_1$  and  $V_2$  are irreducible and inequivalent, and as  $D(C) : V_1 \rightarrow V_2$  is a  $G$ -homomorphism, we have  $D(C) = O$  (the zero matrix) for all choices of the coefficients  $c_{ij}$  of  $C$ . Hence if we set  $c_{rs} = \delta_{rj}\delta_{sk}$  (and so  $c_{rs}$  depends on  $j$  and  $k$ ), then the  $(i, l)$ th entry of  $D(C)$  gives

$$0 = \sum_{g \in G} \sum_{r,s} a_{ir}(g) \delta_{rj} \delta_{sk} b_{sl}(g^{-1}) = \sum_{g \in G} a_{ij}(g) b_{kl}(g^{-1}),$$

and (i) follows. Note that the inner sum of the middle expression above is the  $(i, l)$ th term of the triple matrix product  $(a_{ir}(g))(c_{rs})(b_{sl}(g^{-1}))$ .

(ii) Using Schur's Lemma again, if  $V_1 = V_2$  (and so  $n_1 = n_2$ ), then

$$D(C) = t_C I_{n_1} \quad (13.11)$$

for some complex constant  $t_C$  depending on  $C$ . This gives

$$t_C n_1 = \text{tr}(D(C)) = \text{tr}\left(\sum_{g \in G} (a_{ij}(g)) C (a_{kl}(g^{-1}))\right) = o(G) \text{tr}(C)$$

applying the trace properties (a) and (d) on page 412 to establish the last equation. Now using the same values of  $c_{rs}$  as in (i), and writing  $C = C_{jk}$ , we see that  $\text{tr}(C_{jk}) = \delta_{jk}$ , and so  $t_{C_{jk}} n_1 = o(G) \delta_{jk}$ . (Note  $\delta_{1j} \delta_{1k} + \cdots + \delta_{nj} \delta_{nk} = \delta_{jk}$ .) Combining this with equation (13.11) we obtain

$$\sum_{g \in G} (a_{ij}(g)) C_{jk} (a_{kl}(g^{-1})) = (\delta_{jk} o(G) / n_1) I_{n_1}.$$

Taking corresponding individual entries of these matrices we have finally

$$\sum_{g \in G} a_{ij}(g) a_{kl}(g^{-1}) = \delta_{jk} \delta_{il} o(G) / n_1. \quad \square$$

The following 'character version' of this theorem is due to Frobenius.

**Theorem 13.19** *Using the notation given in Theorem 13.18, let  $\chi_i$  be the character of the  $G$ -module  $V_i$  and so also of the representation  $\theta_i$ , for  $i = 1, 2$ . If  $V_1 \not\cong V_2$ , then*

$$\begin{aligned} \sum_{g \in G} \chi_1(g) \chi_2(g^{-1}) &= 0, \quad \text{and} \\ \sum_{g \in G} \chi_1(g) \chi_1(g^{-1}) &= o(G). \end{aligned}$$

*Proof.* As  $\chi_1(g) = \text{tr}((a_{ij}(g)))$  and  $\chi_2(g^{-1}) = \text{tr}((b_{ij}(g^{-1})))$  we have

$$\begin{aligned} \sum_{g \in G} \chi_1(g) \chi_2(g^{-1}) &= \sum_{g \in G} \sum_{i,j} a_{ii}(g) b_{jj}(g^{-1}) \\ &= \sum_{i,j} \sum_{g \in G} a_{ii}(g) b_{jj}(g^{-1}) = 0. \end{aligned}$$

using Theorem 13.18. A similar argument gives the second equation, in this case matrices are  $n_1 \times n_1$ .  $\square$

The next lemma collects together some further basic character properties.

**Lemma 13.20** *Suppose  $\chi$  is a character of a  $G$ -module  $V$  with degree  $n$ , and suppose  $\theta$  is a corresponding representation.*

- (i)  $\chi(e) = \dim V$ .
- (ii) *If  $g \in G$  and  $o(g) = r$ , then  $\chi(g)$  is a sum of  $r$ -th roots of unity.*
- (iii)  $\chi(g^{-1}) = \overline{\chi(g)}$  for all  $g \in G$ .
- (iv) *For all  $g \in G$*

$$|\chi(g)| \leq \chi(e),$$

*and equality occurs if, and only if,  $g\theta = cI_n$  for some  $c \in \mathbb{C}$ .*

- (v)  $\ker \theta = \{g \in G : \chi(g) = \chi(e)\}$ .

- (vi)  $\sum_{g \in G} \chi(g)\chi(g^{-1}) > 0$ .

*Proof.* (i) Suppose  $\dim V = n$ , and  $\mathcal{B}$  is a basis for  $V$ . Then  $(e; \mathcal{B}) = I_n$ , see the proof of Theorem 13.3, and so  $\chi(e) = \text{tr}(e; \mathcal{B}) = \text{tr} I_n = n$ .

(ii) By Theorem 13.15 we can find a basis  $\mathcal{B}$  for  $V$  so that the matrix  $(g; \mathcal{B})$  is diagonal. Then  $(g\theta)^r = g^r\theta = e\theta = I_n$ . Each diagonal element of  $(g; \mathcal{B})$  is an  $r$ -th root of unity, and the result follows as  $\chi(g)$  equals the sum of these diagonal elements.

(iii) Following on from (ii) suppose the diagonal elements of  $(g; \mathcal{B})$  are  $\omega_1, \dots, \omega_n$ . The diagonal elements of  $(g^{-1}; \mathcal{B})$  are  $\omega_1^{-1}, \dots, \omega_n^{-1}$ , and  $\omega_i^{-1} = \overline{\omega_i}$  (as the  $\omega$  are roots of unity). The result follows using some elementary complex number properties.

(iv) By (ii),  $\chi(g)$  is a sum of the form  $\omega_1 + \dots + \omega_n$ , say, where  $|\omega_i| = 1$  for all  $i$ . Hence

$$|\chi(g)| = |\omega_1 + \dots + \omega_n| \leq |\omega_1| + \dots + |\omega_n| = n = \chi(e).$$

Now note that equality can only occur if  $\omega_1 = \dots = \omega_n$  in which case  $(g; \mathcal{B}) = \omega_1 I_n$ . Conversely, if  $g\theta = cI_n$  for some  $c \in \mathbb{C}$ , then  $c$  is an  $r$ -th root of unity and  $\chi(g) = nc$ . Hence by (i)  $|\chi(g)| = n = \chi(e)$ .

(v) If  $g \in \ker \theta$  then  $g\theta = I_n$ , and so  $\chi(g) = n = \chi(e)$ . Conversely if  $\chi(g) = \chi(e)$ , then by (iv)  $g\theta = cI_n$  for some  $c \in \mathbb{C}$  and all  $g \in G$  including  $g = e$ . Hence  $c = 1$  and  $g \in \ker \chi$ .

(vi) This follows immediately from (ii) as  $\chi(g)\chi(g^{-1}) = \chi(g)\overline{\chi(g)} = |\chi(g)|^2 \geq 0$ , and  $\chi(g) \neq 0$  for at least one element  $g$  in  $G$ .  $\square$

In Example (e) on page 404 we introduced the *regular module* of  $G$  denoted by  $\mathbb{C}G$ . We can now use this module to obtain some more character properties for  $G$ . By Theorem 13.14 we can express this module as a direct sum of the form

$$\mathbb{C}G = r_1 V_1 \oplus \cdots \oplus r_t V_t, \quad (13.12)$$

where  $t, r_1, \dots, r_t$  are positive integers, and  $V_1, \dots, V_t$  are irreducible  $G$ -modules non-isomorphic in pairs.



**Theorem 13.21** Suppose  $\mathbb{C}G$  is expressed as in (13.12) and has character  $\rho$ , and for  $i = 1, \dots, t$  suppose  $V_i$  has character  $\chi_i$ .

- (i)  $\chi_i(e) = r_i = \dim V_i$  for  $i = 1, \dots, t$ .
- (ii)  $\sum_{i=1}^t \chi_i(e)\chi_i(g) = \rho(g) = \begin{cases} o(G) & \text{if } g = e, \\ 0 & \text{if } g \neq e. \end{cases}$
- (iii)  $\sum_{i=1}^t r_i^2 = o(G)$ .
- (iv) Every irreducible  $G$ -module  $V$  occurs in the sum (13.12).

*Proof.* By definition the elements of  $G$  form a basis for the regular  $G$ -module  $\mathbb{C}G$ . Hence by (13.12), and Theorems 2.8 and 13.17(iii)

$$\sum_{i=1}^t r_i \chi_i(g) = \rho(g) = \begin{cases} o(G) & \text{if } g = e \\ 0 & \text{if } g \neq e \end{cases} \quad (13.13)$$

Now suppose  $\chi$  is a character of an irreducible  $G$ -module. If we multiply equation (13.13) throughout by  $\chi(g^{-1})$ , and sum over all  $g \in G$ , we obtain

$$o(G)\chi(e) = \sum_{g \in G} \rho(g)\chi(g^{-1}) = \sum_{i=1}^t r_i \sum_{g \in G} \chi_i(g)\chi(g^{-1}).$$

(Note that as there is only one non-zero term on the right-hand side of (13.13) the equation above starts with a single term.) If we set  $\chi = \chi_j$  in this equation (i) follows by Theorem 13.19 and Lemma 13.20(i).

(ii) This follows using the same theorem, and (iii) follows from (i) and (ii).

(iv) If we assume that the irreducible character  $\chi$  does not equal  $\chi_i$  for all  $i$  in the range  $1 \leq i \leq t$ , then  $\chi(e) = 0$  which is impossible by Lemma 13.20(i); hence (iv) follows.  $\square$

We now bring conjugacy classes into our theory and, as we shall see, they play an important role. Let  $\mathcal{C}\ell_1 = \{e\}, \dots, \mathcal{C}\ell_{h(G)}$  be a list of the conjugacy classes of  $G$ ; where as usual  $h(G)$  denotes the class number. We set  $\mathcal{C}\ell_i^{-1} = \{g^{-1} : g \in \mathcal{C}\ell_i\}$ ; it is another conjugacy class of  $G$  (Problem 5.7). For each  $i$  in the range  $1, \dots, h(G)$ , let  $i^*$  be given by:  $\mathcal{C}\ell_{i^*} = \mathcal{C}\ell_i^{-1}$ . Further, for the regular module  $\mathbb{C}G$  we define  $b_i$ ,  $i = 1, \dots, h(G)$ , and  $Z(\mathbb{C}G)$  by

$$b_i = \sum_{g \in \mathcal{C}\ell_i} g,$$

and

$$Z(\mathbb{C}G) = \{a : a \in \mathbb{C}G \text{ and } ac = ca \text{ for all } c \in \mathbb{C}G\};$$

see Problem 13.6. Note the similarity with the centre of a group.

**Lemma 13.22** Using the notation set out above we have

- (i) The set  $B = \{b_1, \dots, b_{h(G)}\}$  forms a basis for  $Z(\mathbb{C}G)$  over  $\mathbb{C}$ .

(ii) *Non-negative integers  $s_{ijk}$  can be found to satisfy*

$$b_i b_j = \sum_{k=1}^{h(G)} s_{ijk} b_k \quad \text{for } 1 \leq i, j, k \leq h(G). \quad (13.14)$$

$$(iii) \quad s_{ij1} = \begin{cases} 0 & \text{if } j \neq i^* \\ o(\mathcal{C}\ell_i) & \text{if } j = i^* \end{cases}$$

where  $i^*$  was defined on the previous page.

*Proof.* (i) Suppose  $a \in Z(\mathbb{C}G)$ . As  $a \in \mathbb{C}G$  we can write  $a = \sum a_g g$  for suitably chosen integers  $a_g$  depending on  $a$ . Now  $a \in Z(\mathbb{C}G)$  if, and only if,  $a = h^{-1}ah$  for all  $h \in G$ . Hence the integers  $a_g$  are constant as  $g$  ranges over the conjugacy classes  $\mathcal{C}\ell_i$ . Therefore we can write

$$a = \sum_{i=1}^{h(G)} r_i b_i \quad \text{where } r_i \in \mathbb{Z}^+.$$

The integers  $r_i$  are positive and depend on the terms of  $a_g$ , and the  $b_i$  were defined on page 417. So  $Z(\mathbb{C}G)$  is generated by  $B$ . Further, as conjugacy classes are pair-wise disjoint, this equation shows that the elements of the set  $B$  is linearly independent over  $\mathbb{C}$ , and so form a basis for  $Z(\mathbb{C}G)$ .

(ii) By (i) each element of  $Z(\mathbb{C}G)$  can be expressed as a linear combination of basis elements, hence  $s_{ijk} \in \mathbb{Z}$  and (13.14) holds. These integers are non-negative, for by (13.14) the integer  $s_{ijk}$  counts the number of pairs  $(c_1, c_2)$  where  $c_1 \in \mathcal{C}\ell_i$ ,  $c_2 \in \mathcal{C}\ell_j$  and  $c_1 c_2 \in \mathcal{C}\ell_k$ , and so being a counting function it must be non-negative.

(iii) Note first  $\mathcal{C}\ell_1 = \{e\}$ . Using the notation in (ii), if  $j \neq i^*$  then  $c_1 c_2 \neq e$  for all  $c_1 \in \mathcal{C}\ell_i$  and  $c_2 \in \mathcal{C}\ell_j$ ; hence  $s_{ij1} = 0$ . But if  $j = i^*$ , then for every  $c_1 \in \mathcal{C}\ell_i$  there is a unique  $c_2 \in \mathcal{C}\ell_j$  with the property:  $c_1 c_2 = e$ ; so in this case  $s_{ijk} = o(\mathcal{C}\ell_i)$ .  $\square$

The following rather technical lemma will be used to establish our second set of orthogonality relations (Theorem 13.24). Part (ii) will also be used in the proof of Lemma 14.1.

**Lemma 13.23** (i) *Suppose  $\chi$  is a character of an irreducible  $G$ -module, and  $t_i = o(\mathcal{C}\ell_i)$  for  $1 \leq i \leq h(G)$ .*

$$t_i \chi(g_i) / \chi(e) \cdot t_j \chi(g_j) / \chi(e) = \sum_{k=1}^{h(G)} s_{ijk} t_k \chi(g_k) / \chi(e).$$

(ii) *The complex number  $t_i \chi(g_i) / \chi(e)$  is an eigenvalue of the matrix whose  $(j, k)$ th entry is  $s_{ijk}$  as given in Lemma 13.22.*

*Proof.* Let  $\theta$  be a representation associated with  $\chi$ , that is a homomorphism from  $G$  to  $GL_n$ . We can extend  $\theta$  to a homomorphism from  $\mathbb{C}G$  to  $GL_n$  by setting

$$(a_1 g_1 + \cdots + a_m g_m) \theta = a_1 (g_1 \theta) + \cdots + a_m (g_m \theta)$$

where  $m = o(G)$ . By Lemma 13.22, the elements  $b_i$  belong to the centre of  $\mathbb{C}G$ , and so commute with all  $g \in G$ . Therefore if  $c_i \in Z(\mathbb{C}G)$  then  $c_i \theta g \theta = g \theta c_i \theta$  for all  $g \in G$ . By Problem 13.6 we have

$$c_i \theta = q_i I_n \quad \text{for some } q_i \in \mathbb{C}, \quad (13.15)$$

where  $n$  equals the degree of  $\theta$ . Now taking traces we obtain

$$q_i \chi(e) = \text{tr}(q_i I_n) = \text{tr}\left(\sum_{g \in \mathcal{C}\ell_i} g \theta\right) = t_i \chi(g_i),$$

or  $q_i = t_i \chi(g_i) / \chi(e)$  where  $t_i = o(\mathcal{C}\ell_i)$ . But by Lemma 13.22 and as  $\theta$  is a homomorphism we obtain

$$c_i \theta \cdot c_j \theta = \sum_{k=1}^{h(G)} s_{ijk} c_k \theta.$$

(i) now follows using (13.15).

(ii) If  $S_i = (s_{ijk})$  is the matrix whose  $(j, k)$ th entry is  $s_{ijk}$ , and  $\mathbf{v} = (r_1, \dots, r_{h(G)})$ , then we have  $\mathbf{v} S_i = q_i \mathbf{v}$ . Hence  $\mathbf{v}$  is an eigenvector for  $S_i$ ; note that  $r_1 = 1$ , and so  $\mathbf{v}$  is not the zero vector.  $\square$

Using this result we can now derive the second set of orthogonal relations, now summed over characters rather than elements. As usual we let  $\mathcal{C}\ell\{g\}$  denote the conjugacy class of  $G$  that contains  $g$ .

**Theorem 13.24** (Column Orthogonality Relations) *Suppose  $\chi_1, \dots, \chi_l$  are the characters of the irreducible  $G$ -modules, then*

$$\sum_{r=1}^l \chi_r(g) \chi_r(h^{-1}) = \begin{cases} 0 & \text{if } h \notin \mathcal{C}\ell\{g\} \\ o(C_G(g)) & \text{if } h \in \mathcal{C}\ell\{g\} \end{cases} \quad (13.16)$$

*Proof.* By Lemma 13.23 applied to  $\chi_r$  and using the notation set up there we have

$$t_i \chi_r(g_i) \cdot t_j \chi_r(g_j) = \sum_{k=1}^{h(G)} s_{ijk} t_k \chi_r(g_k) \chi_r(e).$$

Summing over  $r = 1, \dots, l$  and using Theorem 13.21(ii) this gives

$$\begin{aligned} t_i t_j \sum_{r=1}^l \chi_r(g_i) \chi_r(g_j) &= \sum_{k=1}^{h(G)} s_{ijk} t_k \sum_{r=1}^l \chi_r(g_k) \chi_r(e) \\ &= s_{ij1} t_1 o(G) = s_{ij1} o(G) \end{aligned}$$

as  $t_1 = o(\mathcal{C}\ell\{e\}) = 1$ . Now by Lemma 13.22(iii) and Problem 5.7,  $s_{ij1} = 0$  if  $g_j^{-1} \notin \mathcal{C}\ell\{g_i\}$ , and  $s_{ij1} = o(\mathcal{C}\ell\{g_i\}) = t_i$ , if  $g_j^{-1} \in \mathcal{C}\ell\{g_i\}$ . Therefore

$$t_j \sum_{r=1}^l \chi_k(g_i) \chi_k(g_i^{-1}) = \delta_{ij} o(G).$$

The first part of the theorem follows. The second part also follows using Theorem 5.19.  $\square$

The set of all class functions  $CF(G)$  of a group  $G$  can be given the structure of an *Hermitian vector space*. It is a space of dimension  $h(G)$  over  $\mathbb{C}$  with an Hermitian product  $\langle \cdot, \cdot \rangle_G$  defined as follows.

**Definition 13.25** For  $f_1, f_2 \in CF(G)$  the function  $\langle \cdot, \cdot \rangle_G : CF(G) \times CF(G) \rightarrow \mathbb{C}$  is given by

$$\langle f_1, f_2 \rangle_G = \frac{1}{o(G)} \sum_{g \in G} f_1(g) \overline{f_2(g)}.$$

*Example.* Suppose  $G = C_4 \simeq \langle a \rangle$  where  $a^4 = e$ . Let class functions  $\alpha$  and  $\beta$  be given by  $\alpha e = 3, \alpha a = i, \alpha a^2 = 1, \alpha a^3 = -i$  and  $\beta e = 2, \beta a = 1 + i, \beta a^2 = 0, \beta a^3 = 1$ , then

$$\begin{aligned} \langle \alpha, \alpha \rangle_{C_4} &= (1/4)(3^2 + i(-i) + 1^2 + (-i)i) = 3 \\ \langle \alpha, \beta \rangle_{C_4} &= (1/4)(3 \cdot 2 + i(1 - i) + 1 \cdot 0 + (-i) \cdot 1) = 7/4 \\ \langle \beta, \beta \rangle_{C_4} &= (1/4)(2^2 + (1 + i)(1 - i) + 0 + 1^2) = 7/4. \end{aligned}$$

Reader, repeat this calculation by replacing the last equation by  $\beta a^3 = 1 - i$ .

The following useful Hermitian and related properties follow easily from the orthogonality relations proved above.

**Theorem 13.26** (i) *There are exactly  $h(G)$  irreducible  $G$ -modules (up to isomorphism).*

(ii) *For  $i = 1, \dots, h(G)$ , if  $\chi_i$  is the character of the  $i$ -th irreducible  $G$ -module given by (i) then  $\{\chi_1, \dots, \chi_{h(G)}\}$  is an orthonormal basis for  $CF(G)$ .*

(iii)  $\langle \chi_i, \chi_j \rangle_G = \delta_{ij}$  for  $1 \leq i, j \leq h(G)$ .

(iv)  $\sum_{i=1}^{h(G)} \chi_i(e)^2 = o(G)$ .

*Proof.* (i) Let  $\chi_1, \dots, \chi_l$  be a list of the characters of the irreducible  $G$ -modules. By Definition 13.25, Lemma 13.20(iii) and Theorem 13.19 we have

$$o(G) \langle \chi_i, \chi_j \rangle_G = \sum_{g \in G} \chi_i(g) \overline{\chi_j(g)} = \sum_{g \in G} \chi_i(g) \chi_j(g^{-1}) = \delta_{ij} o(G). \quad (13.17)$$

This shows that the set  $\{\chi_1, \dots, \chi_{h(G)}\}$  is linearly independent in  $CF(G)$ , and so

$$l \leq \dim CF(G) = h(G).$$

Suppose now  $l < \dim CF(G)$ , and let  $A$  denote the  $l \times h(G)$  matrix whose  $(i, j)$ th entry is  $\chi_i(g_j)$  where  $g_j \in \mathcal{C}\ell\{j\}$ , the  $j$ -th conjugacy class of  $G$ . By assumption

$$\text{rank of } A \leq l < h(G),$$

that is the  $h(G)$  rows of  $A$  are linearly dependent; hence we can find complex numbers  $r_1, \dots, r_{h(G)}$  at least one of which is non-zero to satisfy

$$\sum_{j=1}^{h(G)} r_j \chi_i(g_j) = 0 \quad \text{for } i = 1, \dots, l.$$

Using these equations and Theorem 13.24 we obtain

$$\begin{aligned} 0 &= \sum_{i=1}^l \left( \sum_{j=1}^{h(G)} r_j \chi_i(g_j) \right) \chi_i(g_k^{-1}) \\ &= \sum_{j=1}^{h(G)} r_j \sum_{i=1}^l \chi_i(g_j) \chi_i(g_k^{-1}) \\ &= \sum_{j=1}^{h(G)} r_j \delta_{jk} o(G)/o(\mathcal{C}\ell\{g_k\}) = r_k o(G)/o(\mathcal{C}\ell\{g_k\}). \end{aligned}$$

Hence as  $o(G)/o(\mathcal{C}\ell\{g_k\}) \neq 0$ , we have  $r_k = 0$  for  $k = 1, \dots, h(G)$  which contradicts our assumption above. Therefore  $l = h(G)$ , and (i) follows.

(ii) and (iii) follow directly from (i), and (iv) follows from the last equation in (13.17) by putting  $g = e$  and  $i = j$ .  $\square$

This result enables to make the following

**Definition 13.27** (i) A character for  $G$  is called *irreducible* if, and only if, it is the character of an irreducible  $G$ -module.

(ii) The kernel  $\ker \theta$  of a representation  $\theta$  of a group  $G$  with character  $\chi$  is called the *kernel* of  $\chi$ , and it is denoted by  $\ker \chi$ .

(iii) The *character table* of  $G$  is the  $h(G) \times h(G)$  matrix whose  $(i, j)$ th entry is  $\chi_i(g_j)$  where  $\chi_i$  is the  $i$ -th irreducible character of  $G$ , and  $g_j$  is a representative of the  $j$ -th conjugacy class of  $G$  where  $1 \leq i, j \leq h(G)$ .

Two points. (a) By Theorem 13.26 a group  $G$  has exactly  $h(G)$  irreducible characters.

(b) The wording in (iii) suggests that there exists some kind of canonical ordering of the irreducible characters, but this is not so – they form an unordered set. The ordering of the rows of a character table is more or less random, although it is usual to place the principal character at the top, and order them by the size of their values for the neutral element.

*Example.* We shall construct the character table for  $S_3$ , more examples are given in Section 14.1. The conjugacy classes of  $S_3$  are

$$\{e\}, \{(1, 2), (1, 3), (2, 3)\} \quad \text{and} \quad \{(1, 2, 3), (1, 3, 2)\}.$$

Hence as  $h(S_3) = 3$ , the character table is  $3 \times 3$  and  $S_3$  has three irreducible characters  $\chi_i$ ,  $i = 1, 2, 3$  (by Theorem 13.20(i)). The first  $\chi_1$  is the principal character where  $\chi_1(g) = 1$  for all  $g \in S_3$ , and for the second we can take the character we constructed in the Example on page 413. If we let the values of  $\chi_3$  be given by:

$$\chi_3(e) = r, \quad \chi_3((1, 2)) = s, \quad \text{and} \quad \chi_3((1, 2, 3)) = t$$

where  $r, s, t \in \mathbb{C}$ , then the character table can be written as follows.

$g$	$e$	2-cycle	3-cycle
$\chi_1(g)$	1	1	1
$\chi_2(g)$	2	0	-1
$\chi_3(g)$	$r$	$s$	$t$

CHARACTER TABLE FOR  $S_3$ 

To complete the table we need to calculate  $r, s$  and  $t$ . By Theorem 13.26(iv) we have, working on the first column,  $1^2 + 2^2 + r^2 = o(S_3) = 6$ , hence  $r = \pm 1$ , but by Theorem 13.21(i)  $r > 0$ , and so  $r = 1$ . Now using the Column Orthogonality Relations (Theorem 13.24), working on the first and second columns we obtain  $1 \cdot 1 + 2 \cdot 0 + r \cdot s = 1 + s = 0$ , and so  $s = -1$ , and working on the first and third columns we obtain  $1 \cdot 1 + 2 \cdot -1 + r \cdot t = -1 + t$ , and so  $t = 1$ . The second character  $\chi_2$  is called the minor permutation character, see Problem 13.16, and for the third character see Problem 13.18.

Finally in this section we give a useful condition for irreducibility:

**Theorem 13.28** *A character  $\chi$  is irreducible if, and only if,  $\langle \chi, \chi \rangle_G = 1$ .*

*Proof.* By Theorem 13.26, if  $\chi = n_1\chi_1 + \cdots + n_{h(G)}\chi_{h(G)}$  where  $n_i$  is a non-negative integer, and  $\chi_i$  is a character of an irreducible  $G$ -module, for each  $i = 1, \dots, h(G)$ , then by Theorem 13.21(iv)

$$\langle \chi, \chi \rangle_G = \sum_{i=1}^{h(G)} n_i^2.$$

So  $\chi$  is irreducible, that is we have  $\chi = \chi_i$  for some  $i$  if, and only if,  $\langle \chi, \chi \rangle_G = 1$ .  $\square$

*Example.* Using this condition we can see that the three characters given in the example above are irreducible. By Theorems 3.6 and 5.19 the orders of the centralisers of  $S_3$  are 6, 2 and 3, respectively. Hence for  $\chi_1$  we have

$$1^2/6 + 1^2/2 + 1^2/3 = 1,$$

similarly for  $\chi_2$  and  $\chi_3$  we have

$$2^2/6 + 0^2/2 + (-1)^2/3 = 1 \quad \text{and} \quad 1^2/6 + (-1)^2/2 + 1^2/3 = 1,$$

that is these three characters are irreducible.

## 13.4 Lifts and Normal Subgroups

In this, the last of the theoretical sections, we give some further easily developed character properties. Each of the main elementary group constructions – subgroups and extensions, factor groups and direct products – provide important developments in character theory. We shall mainly be concerned with properties associated with factor groups, the so-called *lifts*, and some products as these are sufficient for the material to be presented in Chapter

14. We shall see that given a character of a factor group  $G/K$ , we can almost immediately write down a character for  $G$ , and irreducibility is preserved. We shall also be able to determine the linear characters of a group, that is those with degree 1. For further properties the reader should consult the references quoted in the introduction to this chapter.

We begin with the basic facts about *lifts*. First we have

**Lemma 13.29** *Suppose  $K$  is a normal subgroup of  $G$ , and  $\chi$  is a character of  $G/K$ . Let the class function  $\hat{\chi}$  on  $G$  be defined by*

$$\hat{\chi}(g) = \chi(gK) \quad \text{for } g \in G.$$

*Then  $\hat{\chi}$  is a character for  $G$ , and it has the same degree as  $\chi$ .*

*Proof.* Let  $\sigma : G/K \rightarrow GL_n$  be a representation (homomorphism) of  $G/K$  with character  $\chi$ . Also let  $\theta$  be the natural homomorphism (Definition 4.13) mapping  $G$  into  $G/K$ . The composition  $\theta\sigma : G \rightarrow G/K \rightarrow GL_n$  is a homomorphism, and so it is also a representation of  $G$ . Its character  $\chi^*$  satisfies

$$\chi^*(g) = \text{tr}(g\theta\sigma) = \text{tr}((gK)\sigma) = \chi(gK) = \hat{\chi}(g) \quad \text{for all } g \in G,$$

and so  $\chi^* = \hat{\chi}$ . Further  $\chi(K) = \hat{\chi}(e)$ , hence  $\chi$  and  $\hat{\chi}$  have the same degree by Lemma 13.20.  $\square$

**Definition 13.30** The character  $\hat{\chi}$  of  $G$  given in Lemma 13.29 is called the *lift* to  $G$  of the character  $\chi$  of  $G/K$ .

The next result shows the close relationship between a character  $\chi$  and its lift  $\hat{\chi}$ .

**Theorem 13.31** *Suppose  $K \triangleleft G$ .*

- (i) *There is a one-to-one correspondence between the characters of  $G/K$  and the characters  $\hat{\chi}$  of  $G$  which satisfy  $K \leq \ker \hat{\chi}$ .*
- (ii) *In the correspondence given in (i) an irreducible character of  $G/K$  corresponds to an irreducible character of  $G$  which contains  $K$  in its kernel.*

*Proof.* (i) Let  $\chi$  be a character of  $G/K$  and let  $\hat{\chi}$  be its lift to  $G$ . We have  $\chi(K) = \hat{\chi}(e)$  and, if  $k \in K$ , and so  $kK = K$ , then

$$\hat{\chi}(k) = \chi(kK) = \chi(K) = \hat{\chi}(e).$$

Hence  $K \leq \ker \hat{\chi}$ . Conversely, let  $\hat{\chi}$  be a character of  $G$  with  $K \leq \ker \hat{\chi}$ . Further, let  $\hat{\sigma}$  be the representation of  $G$  corresponding to  $\hat{\chi}$  where  $\hat{\chi}(e) = n$ . If  $g_1, g_2 \in K$  and  $g_1K = g_2K$ , then  $g_2^{-1}g_1 \in K$  and so  $(g_2^{-1}g_1)\hat{\sigma} = I_n$  which gives  $g_1\hat{\sigma} = g_2\hat{\sigma}$ . Hence if we define  $\sigma$  by

$$(gK)\sigma = g\hat{\sigma} \quad \text{for } g \in G,$$

it is well-defined. Further

$$((gK)(hK))\sigma = (ghK)\sigma = gh\hat{\sigma} = g\hat{\sigma}h\hat{\sigma} = (gK)\sigma(hK)\sigma$$

for  $g, h \in G$ . Now if  $\chi$  is the character of  $\sigma$ , a representation of  $G/K$ , we have  $\chi(gK) = \hat{\chi}(g)$  for all  $g \in G$ , hence  $\hat{\chi}$  is the lift of  $\chi$  to  $G$ . This establishes the one-to-one correspondence.

(ii) Irreducibility. If  $W$  is a subspace of the vector space  $\mathbb{C}^n$ , we have

$$w(g\hat{\chi}) \in W \text{ for } w \in W \text{ if and only if } w(gK)\sigma \in W \text{ for } w \in W.$$

This shows that  $W$  is a  $G$ -submodule of  $\mathbb{C}^n$  if, and only if,  $W$  is a  $G/K$ -submodule of  $\mathbb{C}^n$ . Hence  $\hat{\sigma}$  is irreducible if, and only if,  $\sigma$  is irreducible, and so the same holds for the characters.  $\square$

*Example.* The group  $E$  was described on pages 177 to 183. It has a normal subgroup  $J = \langle a^2 \rangle \triangleleft E$ , and  $o(J) = 2$ . The character  $\chi_2$  of  $J$  satisfies  $\chi_2(e) = 1$ ,  $\chi_2(a^2) = -1$ . This character lifts to  $E$  as follows: Those conjugacy classes which involve even powers of  $a$  lift to 1, and those involving odd powers lift to  $-1$ ; see the character table (second row) on page 457.

## Normal Subgroups

As we have commented several times before, given a group  $G$  it is important to be able to construct its normal subgroups. We show now that we can use the character table for  $G$  to do this easily. For a character  $\chi$  of  $G$  we have

$$\ker \chi = \{g \in G : \chi(g) = \chi(e)\} \triangleleft G,$$

see Definition 13.27. Also the intersection of several character kernels of  $G$  forms a normal subgroup of  $G$  (Theorem 2.30). A vital fact in the theory is the fact that the converse is also true as we show in the next result.

**Theorem 13.32** *Suppose  $K \triangleleft G$ . There exist irreducible characters  $\chi_1, \dots, \chi_r$  of  $G$  with the property*

$$K = \bigcap_{i=1}^r \ker \chi_i.$$

*Proof.* We note first that if  $g \in \ker \chi$  for all irreducible characters  $\chi$ , then  $\chi(g) = \chi(e)$  for all  $\chi$ , and so  $g = e$  by Problem 13.17. Now suppose  $\rho_1, \dots, \rho_s$  is a list of the irreducible characters of  $G/K$ , then

$$\bigcap_{i=1}^s \ker \rho_i = \{K\}$$

the neutral element of  $G/K$ . For  $1 \leq j \leq s$  let  $\chi_{i_j}$  be the lift to  $G$  of the character  $\rho_j$ . If  $g \in \ker \chi_{i_j}$  then

$$\rho_j(K) = \chi_{i_j}(e) = \chi_{i_j}(g) = \rho_j(gK),$$

and so  $gK \in \ker \rho_j$ . Hence if  $g \in \bigcap_{j=1}^s \ker \chi_{i_j}$ , then  $gK \in \bigcap_{j=1}^s \ker \rho_j = \{K\}$  which implies that  $g \in K$ . This gives the result.  $\square$



The reader should check that in the case  $G \triangleleft G$  the corresponding intersection only contains the principal character.

**Corollary 13.33** *A group  $G$  is simple if, and only if,*

$$\chi(g) \neq \chi(e)$$

*for all  $g \in G$  where  $g \neq e$ , and all non-principal irreducible characters  $\chi$ .*

*Proof.* If  $\chi$  is irreducible and  $\chi(g) = \chi(e)$  for some  $g \neq e$ , then  $g \in \ker \chi$  by definition and  $\ker \chi \neq \langle e \rangle$ . Also if  $\sigma$  is the representation associated with  $\chi$ , then  $\ker \sigma = \ker \chi$  and  $\ker \sigma \neq G$  as  $\chi$  is non-principal and irreducible. Hence  $G$  is not simple. Conversely if  $K \triangleleft G$  and  $K$  is proper and non-trivial, then by Theorem 13.32,  $K$  is the intersection of some character kernels, the result follows.  $\square$

For an example see the character table for  $A_5$  on page 439.

## Linear Characters

We begin with

**Definition 13.34** A character is called *linear* if it has degree 1.

Two facts follow immediately if  $\chi$  is a linear character for  $G$ .

- (a)  $\chi$  is a representation (homomorphism) of  $G$  by definition.
- (b)  $\chi(e) = 1$  by Theorem 13.21(i).

When constructing a character table for a group  $G$  it is best to find the linear characters first, and usually this is straightforward as the following result shows.

- Theorem 13.35**
- (i) *If  $\chi$  is a linear character, then  $G' \leq \ker \chi$ .*
  - (ii) *Each linear character of  $G$  is the lift of an irreducible character of  $G/G'$ .*
  - (iii) *If  $G$  has  $t$  linear characters, then  $t \mid o(G)$ .*

*Proof.* (i) By (a) above we have, for  $g, h \in G$ ,

$$\chi(g^{-1}h^{-1}gh) = \chi(g^{-1})\chi(h^{-1})\chi(g)\chi(h) = 1,$$

as  $\chi$  is a homomorphism in this case, and so  $G' \leq \ker \chi$ .

(ii) Let  $t = o(G/G')$ . As  $G/G'$  is Abelian (Problem 4.6), its irreducible characters all have degree 1 (Theorem 13.11). Suppose they are  $\chi_1, \dots, \chi_t$ , and their lifts to  $G$  are  $\hat{\chi}_1, \dots, \hat{\chi}_t$ . By Lemma 13.20 they are also linear, and  $G' \leq \ker \chi_i$  for  $i = 1, \dots, t$ . This gives the result.

(iii) This follows from (ii) by Lagrange's Theorem (Theorem 2.27).  $\square$

*Example.* Again we consider the group  $E$  (as in the example opposite). Here  $E/E' \simeq C_2 \times C_2$ , and so by Theorem 13.35,  $E$  has four linear characters, the lifts of the four (linear) characters of  $C_2 \times C_2$ ; see pages 177ff, 435 and 457

As noted earlier we shall not discuss general character products (they are defined using so-called ‘tensor products’, see the references quoted at the beginning of this chapter), but products where one factor is linear can be dealt with easily and are useful.

**Theorem 13.36** *Suppose  $\chi$  and  $\psi$  are characters of a group  $G$  and  $\psi$  is linear. If we define  $\chi\psi$  by*

$$\chi\psi(g) = \chi(g)\psi(g) \quad \text{for } g \in G,$$

*then  $\chi\psi$  is a character of  $G$ , and  $\chi$  is irreducible if, and only if,  $\chi\psi$  is also irreducible.*

*Proof.* Let  $\sigma$  be a representation of  $G$  with character  $\chi$ , and define  $\sigma\psi$  by

$$g(\sigma\psi) = \psi(g)(g\sigma) \quad \text{for } g \in G,$$

that is  $g(\sigma\psi)$  is the square matrix  $g\sigma$  multiplied by the complex number  $\psi(g)$ . Both  $\sigma$  and  $\psi$  are homomorphisms, and so  $\sigma\psi$  is also a homomorphism, and the trace of the matrix  $g(\sigma\psi)$  is given by

$$\text{tr}(g(\sigma\psi)) = \psi(g) \cdot \text{tr}(g\sigma) = \psi(g)\chi(g).$$

Therefore  $\sigma\psi$  is a representation of  $G$  with character  $\chi\psi$ .

For the second part note that  $\psi(g)$  is a root of unity, and so  $\psi(g)\overline{\psi(g)} = 1$ , and hence

$$\begin{aligned} \langle \chi\psi, \chi\psi \rangle_G &= (1/o(G)) \sum_{g \in G} \chi(g)\psi(g)\overline{\chi(g)\psi(g)} \\ &= (1/o(G)) \sum_{g \in G} \chi(g)\overline{\chi(g)} = \langle \chi, \chi \rangle_G. \end{aligned}$$

Therefore  $\langle \chi\psi, \chi\psi \rangle_G = 1$  if, and only if,  $\langle \chi, \chi \rangle_G = 1$ , and the theorem follows by Theorem 13.28.  $\square$

*Example.* Let  $G = S_4$  with conjugacy classes:  $\{e\}$ , 2-cycles, 3-cycles, 2-cycles  $\times$  2-cycles, and 4-cycles. By Problem 13.16 the minor permutation character for this group has values  $\{3, 1, 0, -1, -1\}$ , and by Problem 13.18 a linear character (using even and odd permutations) has values  $\{1, -1, 1, 1, -1\}$ . So Theorem 13.36 provides another character with values  $\{3, -1, 0, -1, 1\}$  which can easily be checked to be irreducible using Theorem 13.28.

### Summary of Character Properties

We end this chapter with a resumé of the basic character properties. Suppose we are given a group  $G$  with class number  $h(G)$ . We always work over the complex field  $\mathbb{C}$ .

- (a) There are  $h(G)$  irreducible representations  $\theta_1, \dots, \theta_{h(G)}$  of  $G$ .
- (b) To each representation  $\theta$  we associate a character  $\chi$ , its values are the traces of the corresponding matrices used in this representation.

- (c) By (a) there are  $h(G)$  irreducible characters  $\chi_1, \dots, \chi_{h(G)}$ , their values are sums of roots of unity.
- (d) A character is a class function, and so is constant on a conjugacy class of  $G$ .
- (e) An Abelian group of order  $n$  has  $n$  irreducible characters all of which have degree 1.
- (f) Column Orthogonal Relations: The sum  $\sum_{r=1}^{h(G)} \chi_r(g) \chi_r(h^{-1})$  equals zero if  $h \notin \mathcal{C}\ell\{g\}$ , and equals  $o(C_G(g))$  if  $h \in \mathcal{C}\ell\{g\}$ .
- (g) We associate with  $G$  a square  $h(G) \times h(G)$  array, or matrix, its character table. The  $(i, j)$ th entry is  $\chi_i(g_j)$  where  $g_j$  is a representative of the  $j$ -th conjugacy class of  $G$ , and  $\chi_i$  is the  $i$ th irreducible character. (Note that the order in which the characters and/or the conjugacy classes are presented is more or less arbitrary.)
- (h) Irreducible characters of a factor group  $G/K$  can be lifted to irreducible characters of  $G$ .
- (i) The linear characters of  $G$  are the lifts of the characters of  $G/G'$ .
- (j) The normal subgroups of  $G$  are determined by its character table.

Note that different groups can have identical character tables, for example with  $D_4$  and  $Q_8$ , see page 436 and Problem 14.4.

## 13.5 Problems 13

**Problem 13.1** (i) Fill in the details in Example (a) on page 406.

(ii) Show that projections are  $G$ -homomorphisms.

(iii) Let  $C_2 = \langle a : a^2 = e \rangle$ . Show that the map  $\psi$  of the regular module  $\mathbb{C}C_2$  to itself defined by

$$(c_1e + c_2a)\psi = (c_1 - c_2)(e - a) \quad \text{for } c_1, c_2 \in \mathbb{C},$$

is a  $C_2$ -homomorphism, and deduce  $\psi^2 = 2\psi$ .

**Problem 13.2** (i) Let  $C_3 = \langle a : a^3 = e \rangle$  and  $B = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$ , and define  $\theta : C_3 \rightarrow GL_2$  by:  $a^r \theta = B^r$  for  $r = 0, 1, 2$ . Show that this defines a representation of the group  $C_3$ .

(ii) Let  $V$  be the 2-dimensional  $C_3$ -module with basis  $\{v_1, v_2\}$  where

$$v_1a = -v_1 - v_2 \quad \text{and} \quad v_2a = v_1.$$

Use (i) to show that this defines a  $C_3$ -module. Is it irreducible?

**Problem 13.3** Continuing the previous problem, let  $\mathcal{B}$  denote the  $V$ -basis  $\{v_1, v_2\}$ , and let  $\mathcal{B}'$  denote the basis  $\{u_1, u_2\}$  where  $u_1 = v_1$  and  $u_2 = 2v_1 - v_2$ . Show that

$$(e; \mathcal{B}') = I_2, (a; \mathcal{B}') = \begin{pmatrix} 1 & -1 \\ 3 & -2 \end{pmatrix}, (a^2; \mathcal{B}') = \begin{pmatrix} -2 & 1 \\ -3 & 1 \end{pmatrix},$$

and find a  $2 \times 2$  matrix  $C$  to satisfy  $(g; \mathcal{B}) = C^{-1}(g; \mathcal{B}')C$  for all  $g \in C_3$ .

**Problem 13.4 ♦** (i) Suppose  $V$  is a non-zero  $G$ -module, and every  $G$ -homomorphism mapping  $V$  to itself is a scalar multiple of the map  $1_V$ . Show that  $V$  is irreducible. This is of course the converse of Schur's Lemma (Theorem 13.10), and it can be derived using Maschke's Theorem.

(ii) Suppose  $\phi : G \rightarrow GL_n$  is a representation of  $G$ . Show that  $\phi$  is irreducible if, and only if, all matrices  $C$  which satisfy

$$(g\phi)C = C(g\phi) \quad \text{for all } g \in G$$

have the form  $C = cI_n$  for some  $c \in \mathbb{C}$ .

(iii) Give an example of a group  $G$ , a  $G$ -module  $V$ , and a  $G$ -homomorphism  $\varphi : V \rightarrow V$  with the property  $V \neq \ker \varphi \oplus \text{im } \varphi$ .

**Problem 13.5** Suppose  $D_n = \langle a, b \mid a^n = b^2 = (ab)^2 = e \rangle$  is the  $n$ th dihedral group.

(i) Let  $\theta_1$  be given by  $\theta_1(a) = 1, \theta_1(b) = -1$ . Show that  $\theta_1$  is a representation of  $D_n$  of degree 1.

(ii) Give an example of a faithful representation of  $D_4$  with degree 3.

(iii) Define the  $2 \times 2$  matrices  $A, B, C$  and  $D$  by

$$A = \begin{pmatrix} e^{i\pi/3} & 0 \\ 0 & e^{-i\pi/3} \end{pmatrix}, B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$C = \begin{pmatrix} 1/2 & \sqrt{3}/2 \\ -\sqrt{3}/2 & 1/2 \end{pmatrix}, D = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Secondly, define the functions  $\phi_i : D_6 \rightarrow GL_2$ ,  $i = 1, \dots, 4$ , by

$$\begin{aligned} \phi_1 : a^r b^s &\mapsto A^r B^s, & \phi_2 : a^r b^s &\mapsto A^{3r} (-B)^s, \\ \phi_3 : a^r b^s &\mapsto (-A)^r B^s, & \phi_4 : a^r b^s &\mapsto C^r D^s, \end{aligned}$$

where  $0 \leq r < 6$  and  $0 \leq s < 2$ . Show that each  $\phi_i$  is a representation of  $D_6$ , and determine which are faithful and which are equivalent.

(iv) Show that there is a representation  $\sigma$  of  $D_4$  with the properties

$$a\sigma = \begin{pmatrix} -7 & 10 \\ -5 & 7 \end{pmatrix}, \quad b\sigma = \begin{pmatrix} -5 & 6 \\ -4 & 5 \end{pmatrix}.$$

Calculate all matrices  $A$  which satisfy  $A(g\sigma) = (g\sigma)A$  for all  $g \in D_4$ , and determine whether  $\sigma$  is irreducible; see Problem 13.4(ii). Secondly do the same calculation for the representation  $\tau$  where  $a\tau = \begin{pmatrix} 5 & -6 \\ 4 & -5 \end{pmatrix}$  and  $b\tau = \begin{pmatrix} -5 & 6 \\ -4 & 5 \end{pmatrix}$ .

**Problem 13.6** ♦ This problem concerns the entity  $Z(\mathbb{C}G)$  which was defined on page 417.

(i) Show that if  $K \triangleleft G$ , then  $\sum_{k \in K} k \in Z(\mathbb{C}G)$ .

(ii) Suppose  $V$  is an irreducible  $G$ -module, and  $h \in Z(\mathbb{C}G)$ . Using Schur's Lemma (Theorem 13.10) prove that there exists  $c \in \mathbb{C}$  with the property

$$vh = cv \quad \text{for all } v \in V.$$

(iii) If there exists a faithful irreducible  $G$ -module, deduce  $Z(G)$  is cyclic.

(iv) Use (iii) to give an example of a group  $G$  with no faithful irreducible  $G$ -module. (Hint. One example has order 4.)

(v) Suppose  $G$  is finite and all of its irreducible  $G$ -modules have dimension 1. Show that  $G$  is Abelian. (Hint. Use Theorem 13.14.)

**Problem 13.7** ♦ Prove the trace properties (a) to (d) given on page 412, and give an example to show that  $\text{tr}AB$  need not equal  $\text{tr}A \text{tr}B$ .

**Problem 13.8** ♦ (i) Show that if  $\chi$  is a faithful irreducible character of a group  $G$ , then

$$Z(G) = \{g \in G : |\chi(g)| = \chi(e)\}$$

where the vertical bars denote the complex absolute value function.

(ii) Prove that if  $a \in G$  and  $a \neq e$ , then  $\chi(a) \neq \chi(e)$  for at least one irreducible character of  $G$ .

(iii) If  $\chi_1, \dots, \chi_r$  is a list of the irreducible characters of a group  $G$ , show that

$$Z(G) = \{g \in G : \sum_{i=1}^r \chi_i(g) \overline{\chi_i(g)} = o(G)\}.$$

**Problem 13.9** Suppose  $G$  is finite and  $\sigma : G \rightarrow GL_2$  is a 2-dimensional representation. Suppose further there exist  $g, h \in G$  with the property:  $g\sigma$  and  $h\sigma$  do not commute. Use a consequence of Maschke's Theorem (Theorem 13.12) to show that  $\sigma$  is irreducible.

**Problem 13.10** Show that  $\langle \xi, \chi \rangle_G = \chi(e)$  where  $\xi$  is the regular character for  $G$  and  $\chi$  is an arbitrary character for  $G$ .

**Problem 13.11** In this problem you should use the character table for  $S_3$  given on page 422. This group has three conjugacy classes, they are  $\{e\}$ ,  $\{(1, 2), (1, 3), (2, 3)\}$  and  $\{(1, 2, 3), (1, 3, 2)\}$ . Define the following class functions on  $S_3$  with the values given as follows:  $\tau_1 : \{1, 0, 0\}$ ,  $\tau_2 : \{0, 1, 0\}$ ,  $\tau_3 : \{0, 0, 1\}$ ,  $\tau_4 : \{15, -5, 9\}$  and  $\tau_5 : \{15, -5, -6\}$ . Express each of these class functions as linear combinations of the irreducible characters of  $S_3$ , and determine which form characters of the group  $S_3$ .

**Problem 13.12** Suppose  $C_G$  is the matrix formed by the entries of the character table for  $G$ .

(i) Show that  $\det C_G$  is nonzero, and it takes either a real, or a pure imaginary, value.

(ii) If  $c_i$  is a representative of the  $i$ th conjugacy class of  $G$ , prove that

$$(\det C_G)^2 = \prod_{i=1}^r o(C_G(c_i)).$$

(iii) Find  $\det(C_G)$  when  $G$  is (a)  $C_3$ , (b)  $C_2 \times C_2$ , and (c)  $A_5$ . In each case what determines the sign?

**Problem 13.13** Using Problem 3.6 find the character table for the group  $F_{7,3}$ . (Hint. This group has a cyclic subgroup of order 7 and a cyclic factor group of order 3.)

**Problem 13.14** A group of order 12 has six conjugacy classes with class representatives  $e, g_2, \dots, g_6$ , and irreducible characters  $\chi_1, \chi_2$  which take the values  $1, -1, i, 1, -1, -i$  and  $2, 2, 0, -1, -1, 0$ , respectively. Using Theorem 13.36 complete the character table for the group in question.

**Problem 13.15** A group  $G$  of order 8 has five conjugacy classes with orders  $1, 1, 2, 2, 2$  and class representatives  $R = \{e, g_2, \dots, g_5\}$ , respectively. Three of the irreducible characters of  $G$  take the following values on  $R$ :  $1, 1, 1, -1, -1$ ;  $1, 1, -1, 1, -1$ ; and  $1, 1, -1, -1, 1$ . Find the remaining two irreducible characters.

**Problem 13.16** ♦ (i) Let  $G \leq S_n$ , let  $V$  be an  $n$ -dimensional vector space defined over  $\mathbb{C}$  with basis  $\{v_1, \dots, v_n\}$ , and for  $g \in G$  define

$$v_i g = v_{ig} \quad \text{for } g \in G.$$

Using linearity show that this procedure defines a  $G$ -module. You should refer to Example (d) on page 404.

(ii) Let  $\rho$  be the character of the  $G$ -module defined in (i). Show that, if  $g \in G$ ,

$$\rho(g) = o(\{i : 1 \leq i \leq n \text{ and } ig = i\}).$$

The character  $\rho$  is called the *permutation character* of  $G$

(iii) Define  $\xi : G \rightarrow \mathbb{Z}$  by

$$\xi(g) = \rho(g) - 1 \quad \text{for } g \in G.$$

Show that  $\xi$  is a character of  $G$  which we call the *minor permutation character* of  $G$ . (Hint. See Example (c) on page 403.)

(iv) Calculate the minor permutation characters for the groups  $A_4$  and  $S_5$ , and determine if either is irreducible?

**Problem 13.17** (i) Show that the irreducible characters of a group  $G$  form a basis of the vector space of all class functions  $CF(G)$  of  $G$ . (Hint. Use Theorem 13.26.)

(ii) Suppose  $\tau$  is a class function on  $G$ . Using (i) prove that

$$\tau = \sum_{i=1}^{h(G)} c_i \chi_i$$

where  $c_i$  is a complex number given by  $c_i = \langle \tau, \chi_i \rangle_G$  for  $i = 1, \dots, h(G)$ .

(iii) Let  $g, h \in G$ . Show that  $h$  is conjugate to  $g$  in  $G$  if, and only if,  $\chi(h) = \chi(g)$  for all characters  $\chi$  of  $G$ . (Hint. Use (ii).)

(iv) Deduce  $g^{-1}$  is conjugate to  $g$  in  $G$  if, and only if,  $\chi(g)$  is real for all characters  $\chi$  of  $G$ .

**Problem 13.18** ♦ (i) For the group  $S_n$  define  $\xi$  by:  $\xi(\sigma) = 1$  if  $\sigma$  is even, and  $\xi(\sigma) = -1$  if  $\sigma$  is odd, where in each case  $\sigma \in S_n$ . Show that  $\xi$  is an irreducible character of  $S_n$ .

(ii) Show that if  $n > 1$  then  $S_n$  has exactly two linear characters, and list them.

(iii) For  $n > 2$  how many linear characters does  $A_n$  have?

(iv) If a non-Abelian group  $G$  has only one linear character, does it necessarily follow that  $G$  is simple?

**Problem 13.19** (Restriction to a subgroup) Suppose  $H \leq G$  and  $\chi$  is a character of  $G$ .

(i) Let  $\chi \downarrow H$  be the function  $\chi$  with its domain restricted to  $H$ . Show that  $\chi \downarrow H$  is a character of  $H$ , it is called a *restricted character*.

(ii) Using the character table for  $S_4$  given on page 455 construct five characters for  $S_3$  using restriction, and determine which are irreducible.

(iii) Suppose  $\chi$  is irreducible, and  $\phi_1, \dots, \phi_r$  is a list of the irreducible characters for  $H$ . Show that

$$\chi \downarrow H = s_1 \phi_1 + \dots + s_r \phi_r$$

where each  $s_i$  is a non-negative integer. Further show that

$$\sum_{i=1}^r s_i^2 \leq [G : H].$$

(Hint. Use Theorem 13.26.)

(iv) Using (iii), express each restricted character constructed in (ii) as a sum of irreducible characters for  $S_3$ , and so obtain again the character table for  $S_3$ .

(v) Do the same calculations as in (ii) and (iv) for the alternating groups  $A_5$  (see page 439 for its character table) and  $A_4$ . Do you obtain the complete character table for  $A_4$  in this way?

Details concerning the last three problems given below which are of a more challenging nature can be found in Huppert (1998).

**Problem 13.20\*** Suppose  $o(G)$  is odd, and  $1_G, \chi_2, \dots, \chi_r$  is a list of the irreducible characters of the group  $G$  where  $h(G)$  is the class number of  $G$ .

(i) Prove that  $\overline{\chi_i} \neq \chi_i$  for  $i = 2, \dots, r$ . (Hint. Use orthogonality and the fact that  $1/2$  is not an algebraic integer.)

(ii) Show that  $h(G) \equiv o(G) \pmod{16}$ , a result due to Burnside. (Hint. Pair off the non-principal characters and use orthogonality again.) What does this imply for groups of odd order less than 16?

**Problem 13.21\*** A famous result of Frobenius and Schur states: If  $\chi$  is an irreducible character of  $G$ , then

$$\chi(e) \mid [G : Z(G)],$$

see Huppert (1998), page 68. Use this to show that if  $G$  is a non-Abelian simple group, then  $\chi(e) \neq 2$  for all irreducible characters  $\chi$  of  $G$ . (Hint. Assume the contrary, and so  $G$  has a faithful representation of degree 2, and note that  $G = G'$  in this case.) The result of Frobenius and Schur is not strictly necessary here, but this problem has given us the opportunity to introduce this important result to you, the reader.

**Problem 13.22\*** One of Burnside's many results states that if  $\chi$  is an irreducible character of a finite group  $G$  and  $\chi(e) > 1$ , then  $\chi(g) = 0$  for some  $g \in G$ . Investigate what is needed to prove this result. Also check that it is correct for the character tables given in this chapter and the next.



## Chapter 14

# Character Tables, and Theorems of Burnside and Frobenius

Representation and character theory has proved to be extremely useful in answering questions about finite groups. It is also widely used of other branches of mathematics and beyond, see for example James and Liebeck (1993), Chapter 30. The solution of a number of the most important theorems in the subject would not exist without it, for example it played a vital role in the proof of the Feit-Thompson Theorem and in CFSG. In this chapter we give three applications. First, using the theory developed in Chapter 13 we construct a number of character tables, these include the tables for most groups of order 12 or less,  $S_4$  (in the problem section), and  $A_5$ . A number of properties of a group can be ‘read off’ its character table once it has been constructed, for example its normal subgroup structure; see Theorem 13.32. Also these tables can be used to determine nilpotency and/or solubility, but note there exist pairs of groups with identical character tables and distinct second derived subgroups (Hubbert (1998), page 44). It is a convenient fact that many of the more ‘interesting’ larger groups have relatively small character tables (because their element conjugacy classes are large), so for example the character table for  $M_{11}$  (with order 7920) is only  $10 \times 10$ .

Secondly, we give a proof of Burnside’s  $p^r q^s$ -theorem using character theory. This was probably the first major success of the theory published in 1903. It enables us to deduce that if only two distinct primes divide the order of a group, then it is soluble. Non-character-theoretic proofs have been found recently by H. Bender but they are much longer, see for example Issacs (2008), Chapter 7.

Our final application is to the so-called Frobenius theory. We noted several times in the book that a result which asserts the existence of a normal subgroup is important and, under certain conditions, this is exactly what Frobenius’s result does. It was first developed in terms of permutation groups, nowadays a more direct approach is used and we shall follow this here. We give four applications, the last allows us to define the *Suzuki groups* first discussed in Chapter 12.

## 14.1 Character Tables

As noted on the previous page in this section we construct the character tables for a number of familiar groups of small order, and we shall begin with the cyclic groups.

### *Character Tables for Cyclic Groups*

In Theorem 13.11 we showed that all irreducible representations of cyclic groups have degree 1, and so all irreducible characters of cyclic groups have degree 1. Also in an Abelian group each conjugacy class has order one. Hence a cyclic group of order  $n$  has  $n$  irreducible characters. Suppose  $C_n \simeq \langle a \rangle$  and  $a^n = e$ . Let  $\omega$  be a primitive  $n$ -th root of unity, so  $\omega^n = 1$ , and no smaller positive power satisfies this equation. Define a series of characters  $\chi_r$  by

$$\chi_r(a^k) = \omega^{rk} \quad \text{for } k = 0, 1, \dots, n-1,$$

where  $r$  is some fixed integer in the range  $0 \leq r < n$ . Hence we obtain  $n$  irreducible characters for  $C_n$ , that is one for each  $r$  in the given range. As an example we write down the character table for  $C_3$  as follows, here  $\omega = (-1 + \sqrt{-3})/2$ .

$g$	$e$	$a$	$a^2$
$\chi_1$	1	1	1
$\chi_2$	1	$\omega$	$\omega^2$
$\chi_3$	1	$\omega^2$	$\omega$

TABLE 1 CHARACTER TABLE FOR  $C_3$

If we take  $\omega = (-1 - \sqrt{3})/2$ , then we obtain the same table except that the second and third rows are interchanged. Similar tables can be constructed for all cyclic groups, the reader should write down the tables for  $C_2$  and  $C_4$ , see Problem 14.1. We shall not give the tables for the remaining Abelian groups in our chosen range. Roughly speaking the character table for  $C_n \times C_m$  can be constructed by ‘multiplying together’ the tables for  $C_n$  and  $C_m$ .<sup>1</sup> As an example we shall construct the table for  $C_2 \times C_2$ . The method we use is non-standard, that is we do not obtain the table by ‘multiplying together’ two copies of the table for  $C_2$ .

Let  $C_2 \times C_2 \simeq \langle a, b \mid a^2 = b^2 = e, ab = ba \rangle = G$ . This group is Abelian and so all of its irreducible characters have degree 1, and there are four of them. Also  $\langle a \rangle \triangleleft G$ , so the two irreducible characters for  $C_2$  can be lifted, see Theorem 13.31, to characters of  $G$ . Hence this character table for  $G$  has the following form where we still need to justify the entries in the third and

<sup>1</sup> This procedure involves the use of the ‘tensor product’, see the references quoted in the Introduction to Chapter 13.

fourth rows. (Note that this table contains three copies of the array  $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$  ‘multiplied’ by 1, and one copy ‘multiplied’ by  $-1$  corresponding to the entries in the table for  $C_2$ .)

$g$	$e$	$a$	$b$	$ab$
$\chi_1$	1	1	1	1
$\chi_2$	1	-1	1	-1
$\chi_3$	1	1	-1	-1
$\chi_4$	1	-1	-1	1

TABLE 2 CHARACTER TABLE FOR  $C_2 \times C_2$ 

The first column is correct as each character has degree 1 (see Lemma 13.20(i)), that is  $\chi_i(e) = 1$  for  $i = 1, \dots, 4$ . To justify the remaining entries in the third and fourth rows we first rewrite them as

$$\chi_3 : 1, r_1, r_2, r_3 \quad \text{and} \quad \chi_4 : 1, s_1, s_2, s_3.$$

Then using the Column Orthogonality Relations (Theorem 13.24) on the second column, and then on the first and second columns, we obtain

$$1^2 + (-1)^2 + r_1^2 + s_1^2 = 4 = o(C_2 \times C_2) \quad \text{and} \quad 1 \cdot 1 + 1 \cdot -1 + 1 \cdot r_1 + 1 \cdot s_1 = 0,$$

so  $r_1^2 + s_1^2 = 2$  and  $r_1 = -s_1$ , which in turn give  $r_1 = \pm 1$  and  $s_1 = \mp 1$ . At this stage in the calculation there is a choice of sign, so we choose  $r_1 = 1$  and  $s_1 = -1$ . If we make the other choice then rows 3 and 4 in the table would be interchanged. Exactly similar calculations using Theorem 13.24 again will give the remaining entries; see Problem 14.2.

### *Character Tables for Dihedral Groups*

We shall construct the character tables for the groups  $D_m$ . In Problem 14.3 we give the case when  $m$  is odd, and here we treat the case when  $m$  is even. Let  $n = m/2$  throughout, so  $m = 2n$ . The dihedral group  $D_{2n}$  (of order  $4n$ ) has a presentation

$$D_{2n} \simeq \langle a, b \mid a^{2n} = b^2 = e, bab = a^{2n-1} \rangle.$$

Our first step is to list the conjugacy classes, there are  $n + 3$  of them:

$$\begin{aligned} &\{e\}, \{a^n\}, \{a, a^{2n-1}\}, \{a^2, a^{2n-2}\}, \dots, \{a^{n-1}, a^{n+1}\}, \\ &\{b, a^2b, \dots, a^{2n-2}b\}, \{ab, a^3b, \dots, a^{2n-1}b\}. \end{aligned} \quad (14.1)$$

In each case we take the first entry of the sets in (14.1) as the conjugacy class representatives. The orders of these classes are  $1, 1, 2, 2, \dots, 2, n, n$ , respectively, with  $n - 1$  of order two.

We can construct several degree 2 representations (over  $\mathbb{C}$ ) of this group as follows. Let  $\sigma_n = e^{\pi i/n}$ , and let  $A_r$  and  $B$  be given by

$$A_r = \begin{pmatrix} \sigma_n^r & 0 \\ 0 & \sigma_n^{2n-r} \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Then for each fixed  $r = 1, 2, \dots, n-1$  we have

$$A_r^{2n} = B^2 = I_2 \quad \text{and} \quad BA_rB = A_r^{2n-1},$$

that is  $\langle A_r, B \rangle$  is a matrix representation the group  $D_{2n}$  over  $\mathbb{C}$  for  $r$  in the range  $1, \dots, n-1$ . The question arises: Are these representations irreducible (Definition 13.9)? The answer is yes provided  $r$  is in the given range, and this follows from Problem 13.5. Hence by taking traces we obtain  $n-1$  irreducible characters for our group, and they all have degree 2; see the table below. We need to find the remaining four. We have  $\langle a^2 \rangle \triangleleft D_{2n}$ , and

$$D_{2n}/\langle a^2 \rangle = \{\langle a^2 \rangle, a\langle a^2 \rangle, b\langle a^2 \rangle, ab\langle a^2 \rangle\}.$$

This factor group is isomorphic to  $C_2 \times C_2$  whose character table was given in Table 2 above. Hence the four remaining irreducible characters can be constructed as lifts to  $D_{2n}$  of the characters in Table 2; see Theorem 13.31. If a conjugacy class in (14.1) involves even powers of  $a$ , that is a member of the collection

$$e, \{a^2, a^{2n-2}\}, \{a^4, a^{2n-4}\}, \dots,$$

then we lift the first column of Table 2 to the columns for the conjugacy classes in this collection. Similarly if a conjugacy class involves odd powers of  $a$ , we lift the second column of Table 2 to the columns for the odd power conjugacy classes. Note that the second class in (14.1) will lift to the first column if  $n$  is even, and to the second if  $n$  is odd. Further for the penultimate class in (14.1) we lift the third column in Table 2 to the last but one column in Table 3, and for the last class we lift the last column in Table 2 to the last column of Table 3. These procedures provide  $n+3$  irreducible characters, and so we obtain the character table for  $D_{2n}$  when  $n > 1$  as given below.

$g$ $o(C_{D_{2n}}(g))$	$e$ $4n$	$a^n$ $4n$	$a$ $2n$	$\dots$ $\dots$	$a^{n-1}$ $2n$	$b$ $4$	$ab$ $4$
$\chi_1$	1	1	1	$\dots$	1	1	1
$\chi_2$	1	$(-1)^n$	-1	$\dots$	$(-1)^{n-1}$	1	-1
$\chi_3$	1	1	1	$\dots$	1	-1	-1
$\chi_4$	1	$(-1)^n$	-1	$\dots$	$(-1)^{n-1}$	-1	1
$\chi_5$	2	-2	$\sigma_n + \sigma_n^{2n-1}$	$\dots$	$\sigma_n^{n-1} + \sigma_n^{n+1}$	0	0
$\chi_6$	2	2	$\sigma_n^2 + \sigma_n^{2n-2}$	$\dots$	$\sigma_n^{n-2} + \sigma_n^{n+2}$	0	0
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$\chi_{n+3}$	2	$(-2)^n$	$\sigma_n^{n-1} + \sigma_n^{n+1}$	$\dots$	$\sigma_n + \sigma_n^{2n-1}$	0	0

TABLE 3 CHARACTER TABLE FOR  $D_{2n}$  WITH ORDER  $4n$

For non-Abelian groups it is usual to include the second row in Table 3 giving the orders of the centralisers of the corresponding elements so that the Column Orthogonality Relations can be readily applied. Note also that the  $(r+4, s+2)$ th entry in this table, for  $1 \leq r \leq n-1$  and  $1 \leq s \leq n-1$ , is  $\sigma_n^{rs} + \sigma_n^{-rs}$  where  $\sigma_n^{2n} = 1$ . Reader: how many normal subgroups does the group have?

### *Character Table for $A_4$*

In Problem 3.3 we showed that  $A_4$ , treated as a permutation group, has four conjugacy classes with class representatives

$$e, (1, 2)(3, 4), (1, 2, 3), (1, 3, 2),$$

and orders 1, 3, 4, 4; respectively. Now  $A'_4 \simeq C_2 \times C_2$ , see Problem 3.10, and so the factor group  $A_4/A'_4 \simeq C_3$ . Hence  $A_4$  has three linear irreducible characters, the lifts of the three irreducible characters of  $C_3$ ; see Table 1 above and Theorem 13.31. Also the minor permutation character  $\xi$  for  $A_4$ , see Problem 13.16, is irreducible. This follows from Theorem 13.28 and the simple calculation

$$\langle \xi, \xi \rangle_{A_4} = 3^2/12 + (-1)^2/4 + 0/3 + 0/3 = 1.$$

Hence we can write down directly the character table for this group as

$\begin{matrix} g \\ o(C_{A_4}(g)) \end{matrix}$	$e$ 12	$(1, 2)(3, 4)$ 4	$(1, 2, 3)$ 3	$(1, 3, 2)$ 3
$\chi_1$	1	1	1	1
$\chi_2$	1	1	$\omega$	$\omega^2$
$\chi_3$	1	1	$\omega^2$	$\omega$
$\chi_4$	3	-1	0	0

TABLE 4 CHARACTER TABLE FOR  $A_4$

Here  $\chi_4 = \xi$ . As an exercise check that the Column Orthogonality Relations apply in this example.

### *Character Table for Dicyclic Group $Q_3$*

The dicyclic group  $Q_3$  has the presentation  $\langle a, b \mid a^3 = b^2 = (ab)^2 \rangle$ ; it has six conjugacy classes with class representatives:

$$e, a^3, a, a^2, b, ab.$$

Their orders are 1, 1, 2, 2, 3, 3, respectively; see page 159. Hence  $Q_3$  has six irreducible characters. Referring again to page 159 we see that  $\langle a^2 \rangle \triangleleft Q_3$  and

$o(\langle a^2 \rangle) = 3$ , hence  $Q_3/\langle a^2 \rangle \simeq C_4$  where this factor group has the elements  $\langle a^2 \rangle, b\langle a^2 \rangle, a\langle a^2 \rangle = b^2\langle a^2 \rangle$  and  $ab\langle a^2 \rangle = b^3\langle a^2 \rangle$ .

By Theorem 13.31, as  $Q_3/\langle a^2 \rangle$  is cyclic of order 4 we can immediately write down four irreducible linear characters for  $Q_3$  as lifts of the corresponding characters for  $C_4$  given in Problem 14.1. Further, as  $12 = 4 \cdot 1 + 2^2 + 2^2$  is the only solution in integers larger than one of an equation of the type  $12 = 4 + x^2 + y^2 \cdots$ , by Theorem 13.26(iv) we see that the two remaining irreducible characters both have degree 2. Hence the character table for  $Q_3$  can be taken in the following form

$g$ $o(C_{Q_3}(g))$	$e$ 12	$a^3$ 12	$a$ 6	$a^2$ 6	$b$ 4	$ab$ 4
$\chi_1$	1	1	1	1	1	1
$\chi_2$	1	-1	-1	1	$i$	$-i$
$\chi_3$	1	1	1	1	-1	-1
$\chi_4$	1	-1	-1	1	$-i$	$i$
$\chi_5$	2	2	-1	-1	0	0
$\chi_6$	2	-2	1	-1	0	0

TABLE 5 CHARACTER TABLE FOR  $Q_3$ 

where we need to justify the entries in the last two rows. The first four entries of the first and fourth columns are lifts of the first column of the table for  $C_4$ , the second and third are lifts of the third column for  $C_4$ , the fifth is a lift of the second column for  $C_4$ , and the sixth is a lift from the fourth column for  $C_4$ . To establish rows 5 and 6 we first rewrite them as

$$\chi_5 : 2, r_1, r_2, r_3, r_4, r_5 \quad \text{and} \quad \chi_6 : 2, s_1, s_2, s_3, s_4, s_5.$$

Then using the Column Orthogonality Relations (Theorem 13.24) first on row two, and then on rows one and two, we obtain

$$4 + r_1^2 + s_1^2 = 12 \quad \text{and} \quad 0 + 2r_1 + 2s_1 = 0$$

which imply that  $r_1 = \pm 2$  and  $s_1 = \mp 2$ . As these characters have the same degree we can choose the signs so that  $r_1 = 2$  and  $s_1 = -2$ . Using the orthogonality relations (Theorem 13.24) again now applied to the relevant columns we obtain the equations

$$\begin{aligned} 2r_2 + 2s_2 &= 0, & 4 + 2r_2 - 2s_2 &= 0, \\ 2r_3 - 2s_3 &= 0, & 4 + 2r_3 + 2s_3 &= 0, \\ 2r_4 + 2s_4 &= 0, & 2r_4 - 2s_4 &= 0, \\ 2r_5 + 2s_5 &= 0, & 2r_5 - 2s_5 &= 0, \end{aligned}$$

and the values given in the table above follow easily. We can deduce from the table that  $Q_3$  has three proper non-neutral normal subgroups, see pages 424 and 425; reader list them.

### Character Table for $A_5$

As a final example we construct the character table for  $A_5$ . Different constructions of this table can be found in, for example, James and Liebeck (1993) and Huppert (1998). In some ways these are more natural compared with the construction given below, but they both use aspects of the theory that we have not covered in Chapter 13. In Problem 3.3 we showed that  $A_5$ , treated as a permutation group, has five conjugacy classes, and we can take the following as class representatives:

$$e, (1, 2)(3, 4), (2, 4, 5), (1, 2, 3, 4, 5), (1, 3, 5, 2, 4).$$

Note that  $(1, 2, 3, 4, 5)(1, 2)(3, 4) = (2, 4, 5)$ , all 3-cycles are conjugate in  $A_5$  (see the proof of Lemma 3.13), and  $(1, 2, 3, 4, 5)^2 = (1, 3, 5, 2, 4)$ . By Theorem 13.26 this shows that  $A_5$  has five irreducible characters  $\chi_i, i = 1, \dots, 5$ . We can write two down immediately: the principal character  $\chi_1$ , and the minor permutation character  $\chi_2$ , see the table below, and Problem 13.16. Reader: you need to check that this second character is irreducible. Further by Theorem 13.21, and as  $\chi_1(e) = 1$  and  $\chi_2(e) = 4$ , we have

$$60 = o(A_5) = \sum_{i=1}^5 \chi_i^2(e) = 17 + \sum_{i=3}^5 \chi_i^2.$$

The only solution in integers  $r_i$  larger than one of the equation  $43 = r_1^2 + r_2^2 + r_3^2$  is  $r_1 = r_2 = 3$  and  $r_3 = 5$  where some rearrangement of the suffixes may be necessary. This shows that two of the remaining three irreducible characters have degree 3 and the last has degree 5, that is  $\chi_3(e) = \chi_4(e) = 3$  and  $\chi_5(e) = 5$ . In Problem 3.27W we gave a 3-dimensional representation of  $A_5$  over  $\mathbb{C}$ . By taking traces (see (ii) in the quoted problem) we can immediately write down the two degree 3 irreducible characters. We obtain *two* irreducible characters because there are two distinct primitive fifth roots of unity. Hence the character table for  $A_5$  is given by

$g$ $o(C_{A_5}(g))$	$e$ 60	$(1, 2)(3, 4)$ 4	$(2, 4, 5)$ 3	$(1, 2, 3, 4, 5)$ 5	$(1, 3, 5, 2, 4)$ 5
$\chi_1$	1	1	1	1	1
$\chi_2$	4	0	1	-1	-1
$\chi_3$	3	-1	0	$(1 + \sqrt{5})/2$	$(1 - \sqrt{5})/2$
$\chi_4$	3	-1	0	$(1 - \sqrt{5})/2$	$(1 + \sqrt{5})/2$
$\chi_5$	5	1	-1	0	0

TABLE 6 CHARACTER TABLE FOR  $A_5$ 

To see that the last row of this table is correct we argue as follows. Rewrite this row as  $5, r, s, t, u$ . Using Column Orthogonality (Theorem 13.24) we have  $3 + r^2 = 4$  (using column 2) and  $5r - 5 = 0$  (using columns 1 and 2), hence  $r = 1$ . Similarly we have  $2 + s^2 = 3$  and  $5 + 5s = 0$ , hence  $s = -1$ . We leave the remaining two cases for the reader to evaluate. Note that, by Corollary 13.33, this construction provides a new proof of the simplicity of  $A_5$  for using

the table above we see immediately that the only proper normal subgroup of  $A_5$  is  $\langle e \rangle$ , in each of the remaining rows the first entry is not repeated.

Further examples are given in the problem section, these include the character tables for the three groups discussed in Chapter 8.

## 14.2 Burnside's $p^r q^s$ -Theorem

We come now to one of the early successes of representation theory: Burnside's  $p^r q^s$ -theorem first proved in 1903. In Theorem 6.5 we showed that, amongst other facts, all  $p$ -groups are soluble. Burnside's result extends this to show that every group whose order has at most two distinct prime factors is soluble. Note that  $p$ -groups satisfy the stronger condition of being nilpotent, but this does not hold in the  $p^r q^s$  case; an example is  $S_3$ . Also Burnside's result does not extend to three primes; the group  $A_5$  is an example.

The proof uses some of the character theory results that were proved in Chapter 13. It also uses some properties of the algebraic integers in an essential way as is shown in the next lemma, the basic facts are discussed in the appendix to this chapter.

**Lemma 14.1** (i) *If  $\chi$  is a character of  $G$  and  $g \in G$ , then  $\chi(g)$  is an algebraic integer.*

(ii) *If  $\chi$  is an irreducible character of  $G$ ,  $g \in G$  and  $\mathcal{Cl}\{g\}$  is the conjugacy class of  $G$  which contains  $g$ , then*

$$o(\mathcal{Cl}\{g\})\chi(g)/\chi(e) \text{ is an algebraic integer.}$$

*Proof.* (i) By Lemma 13.20,  $\chi(g)$  is a sum of roots of unity. Clearly a root of unity is an algebraic integer, and so (i) follows by Theorem B19 (Appendix to this chapter).

(ii) By Lemma 13.23(ii),  $o(\mathcal{Cl}\{g\})\chi(g)/\chi(e)$  is an eigenvalue of a non-singular  $n \times n$  matrix  $C$  with integer entries, and so it is a root of the equation

$$\det(C - xI_n) = 0.$$

But this is a monic polynomial equation in the variable  $x$  with integer coefficients. By definition its roots are algebraic integers, and so the result follows.  $\square$

The next lemma, which uses Lemma 13.20(iv), is essential for both of Burnside's results below.

**Lemma 14.2** *Suppose  $\theta$  is an irreducible representation of  $G$  with character  $\chi$ ,  $g \in G$ , and  $\mathcal{Cl}\{g\}$  is the corresponding conjugacy class of  $G$ . If  $(\chi(e), o(\mathcal{Cl}\{g\})) = 1$  then either*

$$(i) \quad |\chi(g)| = \chi(e), \quad \text{or} \quad (ii) \quad \chi(g) = 0.$$



*Proof.* As  $(\chi(e), o(\mathcal{C}\ell\{g\})) = 1$ , using the Euclidean Algorithm (Theorem B2) we can find integers  $r$  and  $s$  to satisfy  $r\chi(e) + s o(\mathcal{C}\ell\{g\}) = 1$ , this gives, multiplying by  $\chi(g)/\chi(e)$ ,

$$r\chi(g) + s o(\mathcal{C}\ell\{g\})\chi(g)/\chi(e) = \chi(g)/\chi(e).$$

By Lemma 14.1, both  $\chi(g)$  and  $o(\mathcal{C}\ell\{g\})\chi(g)/\chi(e)$  are algebraic integers, hence

$$\chi(g)/\chi(e) \text{ is an algebraic integer.} \quad (14.2)$$

By Lemmas 13.20(i), (ii) and (iv),  $\chi(g)$  is a sum of roots of unity of the form:

$$\chi(g) = w_1 + \cdots + w_t \quad \text{and} \quad |\chi(g)| \leq \chi(e), \quad (14.3)$$

where  $t = \chi(e)$ . So either  $|\chi(g)| = \chi(e)$ , that is (i) holds, or  $|\chi(g)| < \chi(e)$ . This second possibility implies  $\chi(g) = 0$  as we show now. Using (14.2) let

$$f(x) = x^n + r_1 x^{n-1} + \cdots + r_n \quad \text{where} \quad r_i \in \mathbb{Z} \quad \text{for} \quad i = 1, \dots, n$$

be the (unique) monic polynomial of minimal degree with root  $\chi(g)/\chi(e)$ . As the conjugate of a root of unity is another root of unity, we have by (14.2), each conjugate of  $\chi(g)/\chi(e)$ , that is each root of  $f(x) = 0$ , can be written in the form

$$(w'_1 + \cdots + w'_t)/t$$

where  $w'_i$  is a root of unity for  $i = 1, \dots, t$ . Using the same procedure as in the proof of (14.3), it follows that the modulus of each of these expressions is less than or equal to 1. Hence if  $y$  denotes the product of all of these moduli, then we have

$$0 \leq y < 1 \quad \text{and} \quad y = \pm r_n \in \mathbb{Z},$$

using standard monic polynomial properties. The only possible conclusion from these facts is:  $y = 0$ , and then  $f(x) = x$  with a single root 0. The result follows.  $\square$

The first of Burnside's theorems is as follows. Conjugacy classes were defined in Chapter 5 where we proved that the order of a conjugacy class always divides the order of the corresponding group (Theorem 5.19). Burnside's result shows that if the order of a conjugacy class is a power of a prime, then the group cannot be simple provided it is not cyclic. The proof uses character theory and some properties of algebraic integers. Also, the  $p^r q^s$ -theorem follows directly from it.

**Theorem 14.3** *Suppose  $\mathcal{C}\ell$  is a conjugacy class of  $G$  not equal to  $\{e\}$ . If for some prime  $p$  and non-negative integer  $n$  we have  $o(\mathcal{C}\ell) = p^n$ , then  $G$  cannot be a non-Abelian simple group.*

*Proof.* Suppose  $G$  is a non-Abelian simple group. Let  $\mathcal{C}\ell = \mathcal{C}\ell\{g\} = \{a^{-1}ga : a \in G\}$  where  $g \neq e$ . If  $o(\mathcal{C}\ell) = 1$  then  $g \in Z(G)$ , and so

$Z(G) \neq \langle e \rangle$ . If  $Z(G) = G$  then  $G$  is Abelian, otherwise  $Z(G)$  is a non-neutral proper normal subgroup of  $G$ , and so  $G$  is not simple. Both of these cases are ruled out by our supposition, and so we may assume that  $o(\mathcal{C}\ell) = p^n > 1$ .

Let  $\chi_1, \dots, \chi_{h(G)}$  be a list of the irreducible characters of  $G$  with  $\chi_1(g) = 1$  for all  $g \in G$ . We make the following hypothesis:

$$\text{For some } i > 1 \text{ and } g \in G, \quad \chi_i(g) \neq 0 \quad \text{and} \quad p \nmid \chi_i(e). \quad (14.4)$$

The theorem's conditions give  $(o(\mathcal{C}\ell), \chi_i(e)) = 1$  and so, by Lemma 14.2,  $|\chi(g)| = \chi(e)$ . If  $\theta_i$  is the representation of degree  $n_i$  of  $G$  corresponding to the character  $\chi_i$ , and  $r \in \mathbb{C}$ , then by Schur's Lemma (Theorem 13.10)

$$g\theta_i = rI_{n_i}.$$

There are two possibilities:

- (a)  $\langle e \rangle < \ker \chi_i \triangleleft G$  and  $\ker \chi_i \neq G$ ,
- (b)  $\theta_i$  is faithful.

If (a) holds then  $G$  is not simple, and if (b) holds then  $g \in Z(G)$  where  $g \neq e$ , and again  $G$  is not simple as we argued above. Therefore (14.4) is false and so we may assume that  $\chi_i(g) = 0$  for all  $i > 1$  subject to the condition  $p \nmid \chi_i(e)$ . But by Theorem 13.24 we have

$$0 = 1 + \sum_{i=2}^{h(G)} \chi_i(e)\chi_i(g) = 1 + p \cdot \sum_{i=2}^{h(G)} (\chi_i(e)/p)\chi_i(g).$$

Each term in the second sum is either 0 (when  $\chi_i(g) = 0$ ), or is an integer multiple of  $\chi_i(g)$  (by the above argument  $p \mid \chi_i(e)$  when  $\chi_i(g) \neq 0$ ). Rewriting we have

$$\sum_{i=2}^{h(G)} (\chi_i(e)/p)\chi_i(g) = -1/p.$$

But this is impossible because the left-hand side is a sum of integer multiples of algebraic integers, and so is itself an algebraic integer, whereas  $-1/p$  is not an algebraic integer. Hence our original supposition ( $G$  is simple) is false and so the result follows.  $\square$

Using this we can now deduce Burnside's famous 2-prime result.

**Theorem 14.4** (Burnside's  $p^r q^s$ -Theorem) *If  $o(G) = p^r q^s$  where  $p$  and  $q$  are primes, and  $r$  and  $s$  are non-negative integers, then  $G$  is soluble.*

*Proof.* If  $G$  is Abelian, or  $p = q$ , or either  $r$  or  $s$  equals 0, then the result follows from Theorem 11.6 (in each of these cases the group is nilpotent). Also, by Problem 11.6, it is sufficient to show that  $G$  is not simple and non-Abelian. Let  $P$  be a Sylow  $p$ -subgroup of  $G$ , and let  $g \in Z(P)$ . By Lemma 5.21 we may assume that  $g \neq e$ . This gives  $C_G(g) \geq P$ , as  $g$  commutes with every element of  $P$ . So by Theorem 5.19

$$o(\mathcal{C}\ell\{g\}) = [G : C_G(g)] = q^t$$

for some integer  $t$  with  $0 \leq t \leq r$ . If  $t = 0$  then  $g \in Z(G)$ , and so  $G$  is not simple, and if  $t > 0$  then Theorem 14.3 applies, and again  $G$  is not simple.  $\square$

### *Some comments and extensions of Burnside's results*

(a) Although Burnside's theorems are important applications of character and representation theory, attempts have been made to give purely group-theoretic derivations. Bender has given a proof of the  $p^r q^s$ -theorem which does not use character theory, it is long and quite difficult; versions are given in Huppert and Blackburn III (1982b) and Issacs (2008). No non-character theory proof of the first Burnside Theorem (Theorem 14.3) is known.

(b) Burnside's first theorem has been extended by Kazarin to:

If  $g \in G, g \neq e$  and  $o(\mathcal{C}\ell\{g\}) = p^r$  where  $p$  is prime and  $r > 0$ , then the set  $\mathcal{C}\ell\{g\}$  generates a *soluble* normal subgroup of  $G$ .

For a proof see Huppert (1998).

(c) Burnside's  $p^r q^s$ -theorem is best possible in the sense that there exist (infinitely many) non-soluble groups whose orders have three distinct prime factors. There are eight simple groups (up to isomorphism) in this class, see Chapter 12 and the ATLAS (1985). Further  $SL_2(5)$ ,  $S_5$  and  $S_6$  are examples of non-soluble non-simple groups whose orders have three distinct prime factors (that is 2, 3 and 5), and so also a direct (or semi-direct) product of any of these groups with a 2-, 3- or 5-group (or with themselves!) would form another non-soluble non-simple group with order having three distinct prime factors.

(d) With the completion of the proofs of Burnside's theorems we have also completed the proof of Hall's Second Theorem (Theorem 11.14), the two-prime case of Hall's theorem follows directly from the Sylow theory (Theorem 11.4).

(e) As in (b) attempts have been made to establish some properties of the normal subgroup(s) postulated by the  $p^r q^s$ -theorem. An important one is as follows. Suppose  $o(G) = p^r q^s$  and  $p^r > q^s$ , then  $G$  has Sylow  $p$ -subgroup(s)  $P_i$ . If there is more than one then we can define the *p-radical*  $O_p(G)$  by

$$O_p(G) = \cap_i P_i,$$

where the intersection runs over all Sylow  $p$ -subgroups of  $G$ , and it forms a normal subgroup of  $G$ ; see Problem 6.9(vi). The question arises:

$$\text{When is } O_p(G) \neq \langle e \rangle?$$

Burnside, with some later corrections, showed that this holds in most cases. The exceptions make use of some primes which arise in elementary number

theory and are somewhat surprising. (We need to consider cases when the integer  $o(P) (= p^r)$  divides  $o(GL_s(q)) (= \prod_{i=0}^{s-1} (q^s - q^i))$ .) It can be shown that  $O_p(G) > \langle e \rangle$  if  $p^r > q^s$  except possibly in one of the following three cases:

- (i)  $p = 2$  and  $q = 2^n + 1$  where this number is a ‘Fermat’ prime (and so  $n$  is a power of 2), only five of which are known at the present time; they are 3, 5, 17, 257 and 65537.
- (ii)  $p = 2^m - 1$  and  $q = 2$ . Here  $p$  must be a ‘Mersenne’ prime (and so  $m$  is also prime), at the present time 40 are known.
- (iii)  $p = 2$  and  $q = 7$ . In this case an example has been given for a group with order  $2^{23} \cdot 7^8$ .

Further details can be found in Burnside (1904), Rose (1978), Huppert (1998), and Problem 14.13.

### 14.3 Frobenius Groups

Frobenius’s theorem gives a method for constructing certain groups with designated normal subgroups and, as we have seen previously, a result that postulates the existence of normal subgroups is always of importance in the theory. We begin by considering an easy example. Let  $G = S_3$  and  $H = \langle (1, 2) \rangle \leq S_3$ . We have  $(1, 3)(1, 2)(1, 3) = (2, 3) = (1, 3, 2)(1, 2)(1, 2, 3)$  and  $(2, 3)(1, 2)(2, 3) = (1, 2) = (1, 2, 3)(1, 2)(1, 3, 2)$  *et cetera*. These show that

$$H \cap g^{-1}Hg = \langle e \rangle \quad \text{for all } g \in G \setminus H. \quad (14.5)$$

Frobenius now defines a set (in fact a normal subgroup)  $K$  by

$$K = G \setminus \bigcup_{g \in G} g^{-1}(H \setminus \langle e \rangle)g = S_3 \setminus \{(1, 2), (1, 3), (2, 3)\}.$$

Clearly in this case

$$K = \{e, (1, 2, 3), (1, 3, 2)\} \triangleleft S_3,$$

and we do not need any deep theory to prove this. Frobenius’s theorem states that a similar construction can always be undertaken provided a condition similar to (14.5) holds. We prove this result now making extensive use of the character theory developed in Chapter 13. A ‘non-character’ theory proof exists (see Huppert 1998), but it only works if we assume that the Feit-Thompson Theorem (all odd order groups are soluble) has been established, but the proof (which is very difficult) of this result uses representation theory in an essential way. Frobenius originally derived his theorem using permutation groups, we shall discuss this approach once we have proved the main theorem. We begin with the following

**Lemma 14.5** *Suppose  $H \leq G$ ,  $H$  satisfies condition (14.5),  $h \in H$  and  $h \neq e$ . If  $g \in G$  and  $g^{-1}hg \in H$ , then  $g \in H$ .*

*Proof.* As  $g^{-1}hg \in H$ , we have  $g^{-1}hg \in H \cap g^{-1}Hg$ . So if  $g \notin H$ , then by (14.6) we have  $H \cap g^{-1}Hg = \langle e \rangle$ . This implies that  $g^{-1}hg = e$ , and so also  $h = e$ . But  $h \neq e$ , hence our assumption is false and  $g \in H$ .  $\square$

We now state and prove our main theorem.

**Theorem 14.6** (Frobenius's Theorem) *Suppose  $H$  is a proper non-neutral subgroup of  $G$  and (14.5) holds, that is*

$$H \cap g^{-1}Hg = \langle e \rangle \quad \text{for all } g \in G \setminus H. \quad (14.6)$$

*Let  $K$  be defined by*

$$K = G \setminus \bigcup_{g \in G} g^{-1}(H \setminus \langle e \rangle)g. \quad (14.7)$$

*Then  $K \triangleleft G$ ,  $G = KH$  and  $H \cap K = \langle e \rangle$ .*

The proof of this result given below is due to Weilandt. It is quite long, and so we have split it up into a number of more manageable parts. In the main part, Sublemmas 2 to 5, we show that  $K$  can be treated as the kernel of a character, and so its normality will follow.

**Sublemma 1** *The set  $K$  is closed under inner automorphisms.*

*Proof.* Suppose not, that is suppose for some  $g, h \in G$  we have  $g \in K$  and  $h^{-1}gh \notin K$ . Using (14.6) this gives  $h^{-1}gh \in j^{-1}(H \setminus \langle e \rangle)j$  for some  $j \in G$ . But then  $g \in (jh^{-1})^{-1}(H \setminus \langle e \rangle)(jh^{-1})$ , and  $g \notin K$ . This is a contradiction, and so Sublemma 1 follows.  $\square$

Clearly  $e \in K$  and  $K$  is closed under inverses (Problem 14.15). Hence we need to show that  $K$  is closed under its operation which is the main part of the proof. We proceed as follows. Let  $\phi$  be an arbitrary irreducible character for  $H$  which is not the principal character  $1_H$ , and define  $\psi$  by

$$\psi(g) = \begin{cases} \phi(e) & \text{if } g \in K \\ \phi(a^{-1}ga) & \text{if } a^{-1}ga \in H \setminus \langle e \rangle \text{ where } a \in G. \end{cases}$$

**Sublemma 2** *The function  $\psi$  given above is well-defined.*

*Proof.* Suppose  $a^{-1}ga, b^{-1}gb \in H \setminus \langle e \rangle$ . Then  $b^{-1}gb \in (a^{-1}b)^{-1}H(a^{-1}b)$  and so

$$e \neq b^{-1}gb \in H \cap (a^{-1}b)^{-1}H(a^{-1}b).$$

But by our main assumption (14.6) this implies that  $a^{-1}b \in H$  and so  $\phi(b^{-1}gb) = \phi(b^{-1}aa^{-1}ga a^{-1}b) = \phi(a^{-1}ga)$  as  $\phi$  is a class function; that is  $\psi$  is well-defined.  $\square$

Our next task is to show that

**Sublemma 3** *The function  $\psi$  is a class function for  $G$  (Definition 13.16).*

*Proof.* There are two cases to consider corresponding to the two lines in the definition of  $\psi$  above. First suppose  $g \in K$ , then by (i)  $a^{-1}ga \in K$  for  $a \in G$ , and so

$$\psi(a^{-1}ga) = \phi(e) = \psi(g).$$

Secondly suppose  $g \in G \setminus K$ , so  $g \neq e$  and  $g = c^{-1}hc$  for some  $h \in H$  and  $c \in G$ . Now if  $b \in G$

$$b^{-1}gb = b^{-1}c^{-1}hcb \in (cb)^{-1}H(cb) \quad \text{and so} \quad \psi(b^{-1}gb) = \phi(h) = \psi(g).$$

This proves Sublemma 3.  $\square$

Now suppose  $\chi_1 = 1_G, \dots, \chi_{h(G)}$  is a list of the irreducible characters of the group  $G$ . Set

$$\rho = \psi - \phi(e)\chi_1. \quad (14.8)$$

In the next sublemma we provide an evaluation of this function.

**Sublemma 4** *The function  $\rho$  defined above can be expressed by*

$$\rho = \sum_{i=1}^{h(G)} r_i \chi_i$$

where  $r_i \in \mathbb{Z}, i = 1, \dots, h(G)$ , and  $r_1 = -\phi(e)$ .

Later we show that  $r_i \geq 0$ , and  $r_j = 0$  for all but one value of  $j$ . Before reading this proof the reader should refer to Problem 13.19.

*Proof.* First note that  $\rho(k) = 0$  for  $k \in K$  by definition and as  $\chi_1(e) = 1$ , so we can argue as follows.

$$\begin{aligned} r_i &= \langle \rho, \chi_i \rangle_G && \text{see Theorem 13.28} \\ &= 1/o(G) \sum_{g \in G \setminus K} \rho(g) \chi_i(g^{-1}) && \text{by Definition 13.25 and} \\ &&& \text{as } \rho \text{ is zero on } K \\ &= \frac{1}{o(G)} \frac{o(G)}{o(H)} \sum_{h \in H \setminus \{e\}} \rho(h) \chi_i(h^{-1}). \end{aligned}$$

This last equation follows from Lemma 14.5 as class functions are constant on conjugacy classes. Hence as  $\rho(e) = 0$

$$\begin{aligned} r_i &= 1/o(H) \sum_{h \in H} \rho(h) \chi_i(h^{-1}) \\ &= \langle \rho, \chi_i \rangle_H && \text{by Definition 13.25} \\ &= \langle \psi - \phi(e)\chi_1, \chi_i \rangle_H && \text{by definition of } \rho. \end{aligned}$$

Now note that the restriction (Problem 13.19) of  $\chi_i$  to  $H$  can be expressed as a linear combination, with coefficients in  $\mathbb{Z}$  of the irreducible characters of  $H$ , hence  $r_i \in \mathbb{Z}$  for  $i = 1, \dots, h(G)$ . Also repeating the above argument we have

$$r_1 = \langle \rho, 1_G \rangle_G = \langle \phi - \phi(e)1_H, 1_H \rangle_H = -\phi(e). \quad \square$$

Next we show, using Sublemma 4, that

**Sublemma 5** *The function  $\rho$  is an irreducible character of  $G$ .*

*Proof.* Using an argument similar to that above we have

$$\begin{aligned}
 \sum_{i=1}^{h(G)} r_i^2 &= \langle \rho, \rho \rangle_G && \text{by Theorem 13.28} \\
 &= \frac{1}{o(G)} \frac{o(G)}{o(H)} \sum_{h \in H \setminus \{e\}} |\rho(h)|^2 && \text{as above} \\
 &= \langle \rho, \rho \rangle_H && \text{as } \rho(e) = 0 \\
 &= \langle \phi - \phi(e) 1_H, \phi - \phi(e) 1_H \rangle_H && \text{by definition} \\
 &= 1 + \phi(e)^2 = 1 + r_1^2 && \text{by Theorem 13.21.}
 \end{aligned}$$

By Sublemma 4 each  $r_i$  is an integer, and so each  $r_i^2$  is a non-negative integer. Hence the only possibility is that  $r_j = \pm 1$  for some  $j$ , and  $r_l = 0$  if  $l \neq j$ . Therefore

$$\rho = \psi - \phi(e)\chi_1 = \pm\chi_j - \phi(e)\chi_1$$

where  $\chi_j$  is irreducible. But by definition  $\psi(e) = \phi(e) > 0$ , hence  $\rho = \chi_j - \phi(e)\chi_1$ .  $\square$

For the final part of the proof let  $\phi_i$ , for  $i = 1, \dots, h(H)$ , be a list of the irreducible characters of  $H$  where  $\phi_1 = 1_H$ , and let  $\theta$  be the regular character of  $H$  (see page 404), that is

$$\theta = \sum_{i=1}^{h(H)} \phi_i(e)\phi_i.$$

Sublemmas 2 to 5 can now be applied to each  $\phi_i$  in turn. So for  $i = 1, \dots, h(H)$  we have  $\psi_i(k) = \phi_i(e)$ , if  $k \in K$ , and  $\psi_i(g) = \phi_i(a^{-1}ga)$  where  $a^{-1}ga \in H \setminus \{e\}$  for some  $a \in G$ . Define  $\xi$  by

$$\xi = \chi_1 + \sum_{i=2}^{h(H)} \phi_i(e)\psi_i,$$

this gives

$$\xi(e) = 1 + \sum_{i=2}^{h(H)} \phi_i(e)^2 = o(H) \quad \text{by Theorem 13.21(iii)}$$

We also have using the equation above

$$\ker \xi = \{g \in G : \xi(g) = \xi(e) = o(H)\}.$$

We can now prove our main subresult which is given overleaf.

**Sublemma 6**  $K = \ker \xi$ .

*Proof.* We show first that

$$K \subseteq \ker \xi \quad (14.9)$$

as follows. If  $k \in K$  we have

$$\xi(k) = 1 + \sum_{i=2}^{h(H)} \phi_i(e) \psi_i(k) = 1 + \sum \phi_i(e)^2 = o(H) = \xi(e)$$

which proves the inclusion (14.9). For the reverse inclusion suppose  $h \in H$ , then

$$\xi(h) = 1 + \sum_{i=2}^{h(H)} \phi_i(e) \psi_i(h) = \sum_{i=1}^{h(H)} \phi_i(e) \phi_i = \theta(h)$$

where  $\theta$  is the regular character; see above. This gives

$$H \cap \ker \xi = \langle e \rangle \quad (14.10)$$

as  $\ker \theta = \langle e \rangle$  and  $\theta$  is faithful. We also have using (14.7) and Lagrange's Theorem (Theorem 2.27)

$$o(K) = o(G) - [G : H](o(H) - 1) = [G : H]. \quad (14.11)$$

Now using Theorem 5.8 we obtain

$$\begin{aligned} o(H \ker \xi) &= \frac{o(H)o(\ker \xi)}{o(H \cap \ker \xi)} = o(H)o(\ker \xi) \quad \text{by (14.10)} \\ &\geq o(H)o(K) \quad \text{by (14.9)} \\ &= o(G) \end{aligned}$$

by (14.11). This gives  $o(\ker \xi) = o(K)$ , and so by (14.9)  $K = \ker \xi \triangleleft G$ .  $\square$

*Proof of Theorem 14.10* Sublemma 6 shows that  $K$  is a normal subgroup of  $G$ . Also (14.10) shows that

$$G = KH \quad \text{and} \quad K \cap H = \langle e \rangle,$$

and so the proof of Frobenius's theorem is complete.  $\square$

Bender has given an elementary non-character theoretic proof of the result, but it only applies in the case when  $o(H)$  is even; see for example Kurzweil and Stallmacher (2004), page 83.

**Definition 14.7** A group  $G$  with subgroup  $H$  satisfying the conditions of Theorem 14.6 is called a *Frobenius group* with respect to  $H$ , and the normal subgroup  $K$  given by the theorem is called the *Frobenius kernel* of  $G$ . The subgroup  $H$  is called a *Frobenius complement*.



In the example  $G = S_3$  with respect to  $H = \langle(1, 2)\rangle$  given at the beginning of this section, the Frobenius kernel is the normal subgroup  $\langle(1, 2, 3)\rangle$ , and we have the same kernel with respect to each of the three subgroups of  $S_3$  with order 2, so each can act as a Frobenius complement in this case.

### ***Fixed-point-free automorphisms***

A Frobenius group  $G$  with respect to  $H$  having Frobenius kernel  $K$  is clearly a semi-direct product of  $K$  by  $H$ ; see the last line in the proof above and Chapter 7. It has another property related to the notion of *fixed-point-free* automorphisms which we discuss now. We begin with

**Definition 14.8** Suppose  $\sigma$  is an automorphism of a group  $G$  which is not the identity map. The map  $\sigma$  is called *fixed-point-free* on  $G$  if, and only if,  $g\sigma \neq g$  for all  $g \in G$  where  $g \neq e$ .

For an example we return to the group  $S_3$  discussed above. We can define an automorphism  $\sigma_h$  of  $K$  by

$$g\sigma_h = h^{-1}gh \quad \text{for } h \in H \setminus \{e\} = \{(1, 2)\} \quad \text{and } g \in K \setminus \{e\}.$$

This is fixed-point-free on  $K$  for we have  $(1, 2)(1, 2, 3)(1, 2) = (1, 3, 2) \neq (1, 2, 3)$  and  $(1, 2)(1, 3, 2)(1, 2) = (1, 2, 3) \neq (1, 3, 2)$ .

The relationship between Frobenius's Theorem and fixed-point-free automorphisms is given by the following

**Theorem 14.9** For a group  $G$  the following two statements are equivalent.

- (i) The group  $G$  is Frobenius with Frobenius complement  $H$  and Frobenius kernel  $K$ .
- (ii) If  $H < G$ ,  $K \triangleleft G$ ,  $H \neq \langle e \rangle$ ,  $G = KH$  and  $h \in H \setminus \langle e \rangle$ , then the automorphism  $\tau_h$  defined by

$$\tau_h(k) = h^{-1}kh$$

is fixed-point-free on  $K$ .

*Proof.* (i) implies (ii). We only need to show that the automorphism is fixed-point-free. Suppose not, that is suppose  $\tau_h(k) = h^{-1}kh = k$  for some  $k \in K \setminus \{e\}$  and  $h \in H \setminus \{e\}$ . This gives  $h^{-1}k^{-1}h = k^{-1}$ , and so

$$k^{-1}hk = hh^{-1}k^{-1}hk = hk^{-1}k = h \in H.$$

Hence  $h \in H \cap k^{-1}Hk$ , and so, as  $h \neq e$ , Frobenius's Theorem implies that  $k = e$  is the only fixed-point of  $\tau_h$ .

(ii) implies (i). For the converse we first need to show that  $K \cap H = \langle e \rangle$ . Suppose  $k \in K \cap H$  and  $k \neq e$ . The equation  $k^{-1}kk = k$  provides a fixed-point for  $\tau_k$ , and so, as  $k \in H$ , the hypothesis gives  $k = e$ , and  $K \cap H = \langle e \rangle$  follows. Secondly, suppose  $h_1 \in H \cap g^{-1}Hg$  for some  $g \in G \setminus H$ ; we need to show that  $h_1 = e$ . As  $G = KH$  (given) we can find  $k \in K$  and  $h \in H$  to satisfy:  $g = kh$  and  $k \neq e$ . We also have

$h_1 \in g^{-1}Hg$ , and so combining these we can find  $h_2 \in H$  to satisfy:

$$h_1 = k^{-1}h_2k \in H \cap k^{-1}Hk.$$

Also  $h_1h_2^{-1} \in H$  and, as  $K \triangleleft G$  by hypothesis,

$$h_1h_2^{-1} = k^{-1}h_2kh_2^{-1} \in K.$$

These give  $h_1h_2^{-1} \in K \cap H = \langle e \rangle$ , and so  $h_2 = h_1 = k^{-1}h_2k$ , or rewriting

$$k = h_2^{-1}kh_2 \quad \text{and} \quad k \neq e.$$

This is only possible if  $h_2 = e$ , then also  $h_1 = e$ , and  $H \cap g^{-1}Hg = \langle e \rangle$  follows.  $\square$

Below we give some examples, but first we list some of the more important auxiliary properties of Frobenius groups.

### ***Main Properties of Frobenius Groups***

Suppose  $G$  is a Frobenius group with Frobenius complement  $H$  and Frobenius kernel  $K$ . The following facts have been established.

- (a)  $o(H) \mid o(K) - 1$ . This gives  $([G : K], o(K)) = 1$ , and so  $K$  is a characteristic subgroup of  $G$ ; see Problem 4.24.
- (b) All complements of  $K$  in  $G$  are conjugate to  $H$ .
- (c) The Frobenius kernel  $K$  is nilpotent; this important fact is due to Thompson, indeed he proved it in his Ph.D. thesis!
- (d) The Sylow subgroups of  $H$  are either cyclic or have the form  $Q_{2^n}$ , a dicyclic group. This second case only arises for 2-subgroups. Hence if  $2 \nmid o(H)$ , then all Sylow subgroups of  $H$  are cyclic which implies that  $H$  is soluble (Section 11.1 and Theorem 6.18).
- (e) If  $2 \mid o(H)$ , then  $H$  has only one involution,  $j$  say, and  $j^{-1}kj = k^{-1}$  for all  $k \in K$  which in turn implies that  $K$  is Abelian. If  $H$  is not soluble, see (d), and  $H^{(r)}$  is the last non-neutral term in the derived series for  $H$  (so  $H^{(r)} = H^{(r+1)} \neq \langle e \rangle$ , see page 234), then  $H^{(r)} \simeq SL_2(5)$ ; a remarkable result which is due to Zassenhaus.

Derivations of most of these properties can be found in Huppert (1998).

Finally we give four examples to illustrate the important results discussed in this section.

#### ***Example 1. Groups of order $pq$***

In Problem 6.14 we showed that a non-Abelian group  $G$  with  $o(G) = pq$  where  $p$  and  $q$  are prime and  $p \mid q - 1$ , has a presentation of the form

$$G \simeq \langle a, b \mid a^q = b^p = e, b^{-1}ab = a^r \rangle$$

where  $r^p \equiv 1 \pmod{q}$  and  $r^t \not\equiv 1 \pmod{q}$  for  $0 < t < p$ . We show now that if  $K = \langle a \rangle \triangleleft G$  and  $H = \langle b \rangle \leq G$ , then  $G$  is Frobenius with respect to  $H$ , and has Frobenius kernel  $K$ . We have  $G = KH$  by Lagrange's Theorem, and so we need to show that  $H \cap g^{-1}Hg = \langle e \rangle$  provided  $g \notin H$ , that is  $g = b^t a^u$  for some  $t$  and  $u$  with  $u \neq 0$ . Let  $b^m = h \in H$ , then

$$g^{-1}hg = (b^t a^u)^{-1} b^m (b^t a^u) = a^{-u} b^m a^u = b^m a^{u(1-r^m)} \notin H$$

because  $u \neq 0$  and  $r^m \not\equiv 1 \pmod{q}$  if  $0 < m < p$ . This gives the required condition, and so  $G$  is Frobenius with respect to  $H$  and it has kernel  $K$ . Note that in this case both the Frobenius complement and kernel are cyclic. It is likely that it was this example, or similar, which led Frobenius to develop his theory. See Problem 3.6 where a permutation version is given; as noted above Frobenius first presented his theorem in terms of permutation groups.

**Example 2. Frobenius groups with kernels of large nilpotency class**

In (c) on page 450 we stated that the kernel of a Frobenius group is always nilpotent, we give here an example whose Frobenius kernel has a large nilpotency class. We work over the field  $\mathbb{F}_{11}$ , and let  $K = IT_3(11)$ , see Problem 3.15, and  $A$  be the  $3 \times 3$  diagonal matrix with diagonal entries 1, 3 and 4. Note that  $1^5 = 3^5 = 4^5 = 1$  in  $\mathbb{F}_{11}$ , and neither  $3^m$  nor  $4^m$  equal 1, if  $0 < m < 5$ . (There is nothing special about 1, 3 or 4, we could use any three distinct members of the set  $\{1, 3, 4, 5, 9\}$ , quadratic residues modulo 11.) Lastly let  $H = \langle A \rangle$ ; we have  $A^5 = I_3$  and  $H$  is a cyclic group of order 5. Now  $H$  acts fixed-point-freely on  $K$ , for if

$$\begin{pmatrix} 1 & t & u \\ 0 & 1 & v \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 4 \end{pmatrix}^{-m} \begin{pmatrix} 1 & t & u \\ 0 & 1 & v \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 4 \end{pmatrix}^m = \begin{pmatrix} 1 & 3^m t & 4^m u \\ 0 & 1 & 5^m v \\ 0 & 0 & 1 \end{pmatrix},$$

and  $0 < m < 5$ , then  $t = u = v = 0$ . Hence by Theorem 14.9, the group  $KH$ , a subgroup of  $GL_3(11)$  with order  $5 \cdot 11^3 = 6655$ , is Frobenius, and by Problem 3.15 the kernel  $K$  is nilpotent with class 2.

Similar examples exist using the groups  $IT_n(p)$ , provided the prime 5 in the above calculation is replaced by another prime  $q$  with  $q > n$ , and we work over  $\mathbb{F}_p$  where  $p$  is again prime and  $q \mid p-1$ . The Frobenius group then has a kernel with nilpotency class  $n-1$ .

**Example 3. A Frobenius group whose complement is not soluble**

As noted above Zassenhaus has shown that a non-soluble Frobenius complement will always 'involve' the group  $SL_2(5)$ , see (e) on page 450, and Passman (1968), page 202. Here we give an example of a Frobenius group whose complement is this group. It can be shown that <sup>2</sup>

<sup>2</sup> We have shown that  $SL_2(5)/Z(SL_2(5)) \simeq A_5$  (see Problem 3.19), and so the presentation on page 452 can be constructed using Problem 3.26W which gives a presentation of  $A_5$ ; see Passman (1968), page 202 for details.

$$SL_2(5) \simeq \langle a, b, c \mid a^3 = b^5 = c^2, cac = a, cbc = b, (ab)^2 = c \rangle. \quad (14.12)$$

We work over  $\mathbb{F}_{29}$ ; we choose 29 because it is larger than 5, both  $-1$  and  $5$  are quadratic residues modulo 29, and it is the smallest prime satisfying these conditions. Define the following three matrices in  $GL_2(29)$

$$A = \begin{pmatrix} 28 & 1 \\ 28 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 17 \\ 17 & 23 \end{pmatrix}, \quad C = \begin{pmatrix} 28 & 0 \\ 0 & 28 \end{pmatrix}.$$

A straightforward series of matrix calculations using the relations in (14.12) shows that if we set  $a \mapsto A, b \mapsto B$  and  $c \mapsto C$ , then the group  $\langle A, B, C \rangle \simeq SL_2(5)$ . Now

$$\text{if } (r, s)D = (r, s) \text{ then } r = s = 0 \text{ for all } D \in \langle A, B, C \rangle. \quad (14.13)$$

If we let  $K = C_{29} \times C_{29}$ , and we treat  $K$  as the 2-dimensional vector space over  $\mathbb{F}_{29}$ , then (14.13) gives a fixed-point-free automorphism of  $K$ . Hence  $(C_{29} \times C_{29})SL_2(5)$  is Frobenius with a non-soluble complement.

### ***Suzuki Groups***

For our last example we consider some Frobenius groups which are subgroups of  $GL_4(2^{2m+1})$  for  $m = 1, 2, \dots$ , some extensions will give an important class of simple groups – *Suzuki groups*. For the first of these we work over the field  $\mathbb{F}_8$  (so  $m = 1$ ), and begin by defining the matrices

$$A(a, b) = \begin{pmatrix} 1 & a & b & a^6 + ab + b^4 \\ 0 & 1 & a^4 & a^5 + b \\ 0 & 0 & 1 & a \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

and

$$B(c) = \begin{pmatrix} c^{-3} & 0 & 0 & 0 \\ 0 & c^{-2} & 0 & 0 \\ 0 & 0 & c^2 & 0 \\ 0 & 0 & 0 & c^3 \end{pmatrix},$$

where  $a, b, c \in \mathbb{F}_8$  and  $c \neq 0$ . The following three properties are easily proved:

- (i)  $A(a', b')A(a, b) = A(a' + a, a'a^4 + b' + b)$ ,
- (ii)  $B(c)B(d) = B(cd)$  provided  $c, d \neq 0$ ,
- (iii)  $B(c)^{-1}A(a, b)B(c) = A(ac, bc^5)$ .

(Use the facts that in  $\mathbb{F}_8$  we have  $(a + c)^6 = a^6 + a^4c^2 + a^2c^4 + c^6$  and  $(b^4c)^4 = b^2c^4$  as the multiplicative group of this field has order 7.) Let

$$K = \langle A(a, b) \mid a, b \in \mathbb{F}_8 \rangle \quad \text{and} \quad H = \langle B(c) \mid c \in \mathbb{F}_8 \setminus \{0\} \rangle.$$

First we note that  $K$  is a non-Abelian 2-group with exponent 4 and order 64, and

$$K' = Z(K) = \{A(0, b) \mid b \in \mathbb{F}_8\},$$

as the reader can easily check, note that  $K$  has nilpotency class 2. Now  $KH$  is Frobenius with order  $64 \cdot 7 = 448$ . This follows because  $K \triangleleft KH$  by (iii), and  $H$  acts fixed-point-freely on  $K$  because, by (iii) again,  $A(a, b) = A(ac, bc^5)$  is only possible if  $c = 1$ .

We use this group to construct the first Suzuki group  $Sz(8)$ . Let

$$C = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix},$$

and define

$$Sz(8) = \langle A(a, b), B(c), C \mid a, b \in \mathbb{F}_8, c \in \mathbb{F}_8 \setminus \{0\} \rangle.$$

It can be shown that this group is simple and has order  $65 \cdot 448 = 29120$ ; see Huppert and Blackburn III (1982b). Also it is possible to give a (finite) geometrical description as follows. We work in the 3-dimensional projective space over  $\mathbb{F}_8$ , which we label  $\mathbf{P}_3$ . (The space  $\mathbf{P}_3$  has coordinates of the form  $(a : b : c : d)$  where at least one of  $a, b, c$  and  $d$  is non-zero, and if  $t \neq 0$  then  $(a : b : c : d) = (ta : tb : tc : td)$ . Also points with coordinates  $(0 : b : c : d)$  are said to lie on the ‘plane at infinity’.) Let  $\mathcal{O}$  denote the set of points

$$P(r, s) = (1 : r : s : r^6 + rs + s^4) \text{ for } r, s \in \mathbb{F}_8, \text{ and } P(\infty) = (0 : 0 : 0 : 1).$$

The object  $\mathcal{O}$  is called an *ovoid* which means that it is ‘sphere-like’ or ‘convex’. To be more precise, no line in  $\mathbf{P}_3$  meets  $\mathcal{O}$  in more than two points. For example the points on the line through  $P(0, 0)$  and  $P(\infty)$  have coordinates  $a(1 : 0 : 0 : 0) + b(0 : 0 : 0 : 1) = (a : 0 : 0 : b)$ , and this point only lies on  $\mathcal{O}$  if  $a = 0$  or if  $b = 0$ , so is either  $P(0, 0)$  or  $P(\infty)$ ; the reader should check the remaining cases. The relationship with  $Sz(8)$  is given by

**Theorem 14.10** (i) *The group of collineations (this is the name given to a linear map in projective space) which map  $\mathcal{O}$  to itself is isomorphic to  $Sz(8)$ .*

(ii) *The order of  $Sz(8)$  equals 65 times the order of the Frobenius group  $KH$ , that is  $65 \cdot 448 = 29120 = 2^6 \cdot 5 \cdot 7 \cdot 13$ .*

(iii) *The group  $Sz(8)$  is simple.*

(iv) *If  $p$  is odd, then all Sylow  $p$ -subgroups of  $Sz(8)$  are cyclic.*

For a proof see Huppert and Blackburn III (1982b), pages 182 to 194, and for (iv) see Theorem 6.18. Note that

- (a) the factor 65 in (ii) arises because  $o(\mathcal{O}) = 65$ ,
- (b) The simplicity result in (iii) is a consequence of (i),
- (c) The prime 3 does not divide  $o(Sz(8))$ , and

(d) the Sylow 2-subgroups of  $Sz(8)$  are isomorphic to  $K$ , and so are not cyclic. (It has been shown that the only non-Abelian simple groups with this property are  $L_2(2^n)$ ,  $L_2(p)$ ,  $Sz(2^{2n+1})$ , and the Janko group  $J_1$  (web page 390) where  $n > 1$  and  $p > 3$ .)

The construction given above is only the first of an infinite family. In the general case we work over the field  $\mathbb{F}_{2^{2n+1}}$ ,  $n = 1, 2, \dots$ . The matrix  $A(a, b)$  is replaced by

$$A_n(a, b) = \begin{pmatrix} 1 & a & b & a\xi a^2 + ab + b\xi \\ 0 & 1 & a\xi & a\xi a + b \\ 0 & 0 & 1 & a \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \text{for } a, b \in \mathbb{F}_{2^{2n+1}},$$

where  $\xi$  is the automorphism of the multiplicative group of  $\mathbb{F}_{2^{2n+1}}$  defined by  $a\xi = a^{2^{n+1}}$  (so  $a\xi^2 = a^2$ ), and the matrix  $B(c)$  is replaced by  $B_n(c)$  which is again diagonal with diagonal entries  $c^{-1-2^n}$ ,  $c^{-2^n}$ ,  $c^{2^n}$  and  $c^{1+2^n}$ . Now we define

$$Sz(2^{2n+1}) = \langle A_n(a, b), B_n(c), C \mid a, b, c \in \mathbb{F}_{2^{2n+1}} \text{ and } c \neq 0 \rangle.$$

The main properties of these groups are as follows.

- (i)  $Sz(2^{2n+1})$  is simple for  $n = 1, 2, \dots$ . This is proved as before by first showing that an ovoid similar to that defined above is invariant under collineations associated with the group.
- (ii) The order of  $Sz(2^{2n+1})$  is  $q^2(q-1)(q^2+1)$  where  $q = 2^{2n+1}$ . It is easily seen that this order is *not* divisible by 3. Note that both  $q$  and  $q^2+1$  are congruent to 2 modulo 3. Thompson has shown that the order of every non-Abelian simple group is divisible by 3 or 5, and it is known that the order must be even (the Feit-Thompson Theorem). It can be also be shown that the only simple groups whose orders are not divisible by 3 are the Suzuki groups. There is a whole range of groups whose orders are not divisible by 5, see Problem 14.23 and the ATLAS.
- (iii) For odd primes  $p$ , all Sylow  $p$ -subgroups of all Suzuki groups are cyclic.
- (iv) If  $g \in Sz(q)$  and  $g \neq e$ , then the centraliser  $C_{Sz(q)}(g)$  is nilpotent. The only other non-Abelian simple groups with this property are  $L_3(4)$ ,  $L_2(2^n)$ ,  $L_2(9)$  and  $L_2(p)$  where  $p$  is a Fermat or Mersenne prime; see page 444.
- (v) The only outer automorphisms of  $Sz(q)$  are those generated by field automorphisms of  $\mathbb{F}_q$ .
- (vi) When first discovered in 1960, these groups were thought to be new. But it was soon realised that they had been studied in another guise some years previously by Chevalley, for the Suzuki group  $Sz(2^{2n+1})$  is in fact isomorphic to the so-called *Twisted Chevalley Group*  ${}^2B_2(2^{2n+1})$ . For further details see the ATLAS (1985) page xv.
- (vii) Amongst the Suzuki groups  $Sz(8)$  has a number of individual properties; for instance (a) it is the only one ‘involved’ (is a factor group of

a subgroup of the group in question) in a sporadic group – the Rudalis group  $Ru$  (and possibly the friendly giant  $M$ , an open problem); and  
 (b) it is the only Suzuki group with a non-neutral Schur multiplier –  $C_2^2$ ; see web page 391.

Some proofs and more details can be found in the reference quoted above.

But finally we ask: How did these groups arise in the first place? In the 1930's Zassenhaus and others were studying permutation representations of the groups  $L_2(p)$ ; see Chapter 12. He noted that they have three particular properties:

- (a) they are doubly transitive,
- (b) each non-neutral element has at most two fixed points, and
- (c) they do not possess a regular normal subgroup.

For a definition of ‘regular’ see Problem 3.8. Note that if  $G$  is a permutation group on  $X$ , and  $H$  is a regular normal subgroup of  $G$ , then  $o(H) = o(X)$ , also in Frobenius’s Theorem (Theorem 14.6), the Frobenius kernel is a regular normal subgroup. Nowadays groups whose permutation representations satisfy properties (a), (b) and (c) are called *Zassenhaus groups*. Zassenhaus tried to show that the only groups satisfying (a) to (c) are the linear groups  $L_2(p)$ , but he did not succeed because it is not true. In 1960 Suzuki discovered his class of groups  $Sz(q)$ , and he was able to show that each  $Sz(q)$  is in fact Zassenhaus, and he and several other group-theorists proved finally that there are no other examples. And this illustrates one of the main ‘methods’ in the theory – the classification method which can be stated as follows: Introduce a collection of properties, like (a), (b) and (c) above, find some groups with these properties, and then show that – and this is usually the hardest part to establish – no other groups satisfy these properties. CFSG was solved using this and similar strategies on several sets of properties, and showing finally that these sets cover all possibilities!

## 14.4 Problems 14

**Problem 14.1** Write out the character tables for the groups  $C_2$  and  $C_4$ .

**Problem 14.2** (i) Complete the character table calculations for the group  $C_2 \times C_2$  started on page 435.

(ii) Confirm directly that the Column Orthogonality Relations hold for the group  $A_4$  using Table 4 on page 437.

**Problem 14.3** ♦ Construct the character tables for the groups  $D_n$  when  $n$  is odd.

**Problem 14.4** Construct the character table for the quaternion group  $Q_2$ . What do you notice about this table and the one given for a group of order 8 ( $D_4$ ) in Section 14.1.

**Problem 14.5** ♦ (i) You are given the result: If  $\omega$  is an  $n$ -th root of unity then

$$\sum_{1 \leq i \leq n, (i,n)=1} \omega^i \quad \text{is an integer.}$$

Using Theorem 13.15 and Corollary B20 on page 460, show that if  $g \in G$ ,  $o(g) = n$  and  $g$  is conjugate to  $g^i$  for all  $i$  in the range  $1 \leq i \leq n$  with  $(i, n) = 1$ , then  $\chi(g)$  is an integer for all characters  $\chi$  of  $G$ .

(ii) Use (i) to show that all character values of all symmetric groups  $S_n$  are rational integers.

**Problem 14.6** Using the previous problem show that the character table given for the permutation group  $S_4$  below is correct.

$g$ $o(C_{S_4}(g))$	$e$ 24	$(1, 2)$ 4	$(1, 2, 3)$ 3	$(1, 2, 3, 4)$ 4	$(1, 2)(3, 4)$ 8
$\chi_1$	1	1	1	1	1
$\chi_2$	1	-1	1	-1	1
$\chi_3$	2	0	-1	0	2
$\chi_4$	3	1	0	-1	-1
$\chi_5$	3	-1	0	1	-1

TABLE 7. CHARACTER TABLE FOR  $S_4$ 

**Problem 14.7** ♦ Using the theory of tensor products (see for example James and Liebeck (1994), Chapter 19) it can be shown that if  $\chi$  is a character of a group  $G$ , then so are  $\chi_S$  and  $\chi_A$  where, for  $g \in G$ ,

$$\chi_S(g) = (\chi^2(g) + \chi(g^2))/2 \quad \text{and} \quad \chi_A(g) = (\chi^2(g) - \chi(g^2))/2.$$

Neither of these new characters need be irreducible even if  $\chi$  is irreducible. Use these, and the fix (Problem 13.16) and linear characters to construct the character table for  $S_5$ . (Hint. The character table is  $7 \times 7$ .)

**Problem 14.8** The character table for the group  $SL_2(3)$  is given below where  $\omega = e^{2\pi i/3}$ . Show that this table is correct using Section 8.2, and one of the tables given in Section 14.1.

$g$ $o(C_{SL_2(3)}(g))$	$e$ 24	$a^3$ 24	$a^2$ 6	$b^2$ 6	$ab$ 4	$a$ 6	$b$ 6
$\chi_1$	1	1	1	1	1	1	1
$\chi_2$	1	1	$\omega$	$\omega^2$	1	$\omega^2$	$\omega$
$\chi_3$	1	1	$\omega^2$	$\omega$	1	$\omega$	$\omega^2$
$\chi_4$	3	3	0	0	-1	0	0
$\chi_5$	2	-2	-1	-1	0	1	1
$\chi_6$	2	-2	$-\omega$	$-\omega^2$	0	$\omega^2$	$\omega$
$\chi_7$	2	-2	$-\omega^2$	$-\omega$	0	$\omega$	$\omega^2$

TABLE 8. CHARACTER TABLE FOR  $SL_2(3)$



**Problem 14.9** (i) Let  $\omega$  be a cube root of unity. Show that the mapping

$$a \mapsto \begin{pmatrix} \omega & 0 \\ 0 & -\omega^{-1} \end{pmatrix} \quad \text{and} \quad d \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

gives a 2-dimensional representation of the group  $E$  discussed in Section 8.3; use the presentation (8.8) of  $E$  given on page 182. Apply this to calculate all of the irreducible representations of  $E$ .

(ii) Use (i) to justify the character table for  $E$  given below.

$g$ $o(C_E(g))$	$e$ 24	$a^2$ 24	$b$ 12	$c$ 12	$a^2c$ 12	$bc$ 12	$bc^2$ 12	$a$ 4	$ab$ 4
$\chi_1$	1	1	1	1	1	1	1	1	1
$\chi_2$	1	1	1	1	1	1	1	-1	-1
$\chi_3$	1	1	-1	1	1	-1	-1	1	-1
$\chi_4$	1	1	-1	1	1	-1	-1	-1	1
$\chi_5$	2	-2	0	2	-2	0	0	0	0
$\chi_6$	2	2	-2	-1	-1	1	1	0	0
$\chi_7$	2	2	2	-1	-1	-1	-1	0	0
$\chi_8$	2	-2	0	-1	1	$-i\sqrt{3}$	$i\sqrt{3}$	0	0
$\chi_9$	2	-2	0	-1	1	$i\sqrt{3}$	$-i\sqrt{3}$	0	0

TABLE 9. CHARACTER TABLE FOR  $E$

**Problem 14.10** Use Burnside's first theorem (Theorem 14.3) to show that no group of order 1200 can be simple.

**Problem 14.11**  $\blacklozenge$  Prove that if  $H$  is an Abelian subgroup of a non-Abelian simple group  $G$ , then  $[G : H]$  has at least two prime factors. (Hint. Consider a centraliser of an element of  $H$  and use Theorem 14.3.)

**Problem 14.12** Prove the following result due to P. Hall (Section 11.2):

If  $G$  is finite and every maximal subgroup has prime or prime-squared index, then  $G$  is soluble.

Method. Let  $G_0$  be a counter-example with smallest possible order and let  $p_0$  be the largest prime factor of  $o(G_0)$ . Consider  $P_0$ , a Sylow  $p_0$ -subgroup of  $G_0$ , and treat the cases  $P_0$  normal, and  $P_0$  not normal, separately, choose a maximal subgroup  $H$  of  $G_0$  which contains  $N_{G_0}(P_0)$ , and use Problem 6.10(i) and Burnside's Theorem.

**Problem 14.13** The problem refers to Note (e) on page 443.

(i) Suppose  $o(G) = p^r q^s$  where  $p$  and  $q$  are primes. Let  $P_1, \dots, P_m$  be a list of the Sylow  $p$ -subgroups of  $G$ , and suppose  $m > 1$ . Show that if  $P_i \cap P_j = \langle e \rangle$  if  $i \neq j$ , then each  $P_i$  is cyclic.

(ii) It was stated in Note (e) that the situation described in (i) can only arise in three particular cases. Give examples for the first two.

**Problem 14.14** Show that a group  $G$  with a subgroup  $H$  which is nilpotent and has prime power index is soluble.

**Problem 14.15** Show that in the statement of Frobenius's Theorem (Theorem 14.6) the set  $K$  is closed under inverses and contains the neutral element. (Hint. See the proof of Sublemma 1 on page 445.)

**Problem 14.16** Prove that the centre of a Frobenius group is isomorphic to the neutral subgroup.

**Problem 14.17** Let  $n > 1$ . Show that the dihedral group  $D_n$  is Frobenius if, and only if,  $n$  is odd.

**Problem 14.18** Show that  $Q_2$  can act fixed-point-freely on  $C_3 \times C_3$ . (Hint. Think of this latter group as a vector space of dimension 2 over  $\mathbb{F}_3$ ). Hence show how to construct a Frobenius group of order 72.

**Problem 14.19** Let  $H = ES_2(7)$ , see Problem 6.5.

(i) Show that the mapping given by  $a \mapsto a^2c$ ,  $b \mapsto b^2$ ,  $c \mapsto c^4$  defines an automorphism of  $H$  of order 3.

(ii) Show that the semi-direct product  $C_3 \rtimes H$  provides an example of a Frobenius group with a non-Abelian Frobenius kernel.

**Problem 14.20** Let  $\sigma$  be a fixed-point-free automorphism of  $G$  of order  $n$ .

(i) Show that if  $(m, n) = 1$  then  $\sigma^m$  is also fixed-point-free.

(ii) Let  $\nu$  be given by  $g\nu = g^{-1}(g\sigma)$ . Show that  $\nu$  is an isomorphism.

(iii) Show that if  $g$  and  $g\sigma$  are conjugate in  $G$ , then  $g = e$ .

(iv) Further show that if  $g \in G$ , then  $g \cdot g\sigma \cdots g\sigma^{n-1} = e$ .

(v) If  $n = 2$ , prove that  $g^{-1} = g\sigma$  for  $g \in G$ , and deduce  $G$  is Abelian.

**Problem 14.21** Suppose  $H \leq GL_m(F)$  and  $o(H) = pq$  where  $p$  and  $q$  are primes which can be equal. Prove that  $H$  is cyclic.

**Problem 14.22** Let  $G = GL_2(7)$ . Show that  $G$  has a subgroup of order 12 which has no fixed points when it is applied to the vector space of dimension 2 defined over the field  $\mathbb{F}_7$ .

**Problem 14.23** Give examples to show that there are infinitely many simple groups whose orders are not divisible by 5, see (ii) on page 454.

**Problem 14.24** (i) Suppose  $G$  is a Frobenius group with Frobenius kernel  $K$  and complement  $H$ . Show that if  $J \triangleleft G$ , then  $J \leq K$  or  $K \leq J$ .

(ii) Prove that  $o(H) \mid o(K) - 1$ , and so deduce  $(o(K), [G : K]) = 1$ . This shows that  $K$  is a characteristic subgroup of  $G$ , see Problem 4.22.

(iii) Using Thompson's Theorem (see (c) on page 450) show that  $K = F(G)$ , the Fitting subgroup of  $G$ .

## Appendix B2 Algebraic Integers

A character of a group  $G$  is a function from  $G$  into the ring of algebraic integers  $A$ . Here we describe the basic properties of the elements of  $A$ . For further details see, for example, Stewart, I. N. and Tall, D. O. *Algebraic Number Theory*, Chapman and Hall, London, 1979. This subsection is intended as an addition to Appendix B.

**Definition B17** An *algebraic integer* is a complex number which satisfies a monic (that is the leading coefficient is 1) polynomial equation with rational integer coefficients.

For example  $7, 1+i, \sqrt{3}$  and  $(1+\sqrt{-3})/2$  are all algebraic integers. The reader should check this.

For our purposes the main facts we need to know about the set of algebraic integers  $A$  is that it is closed under addition, subtraction and multiplication. Addition and multiplication are clearly associative and there exists a multiplicative identity 1, hence  $A$  forms an integral domain. We need to prove one lemma before we can derive our main result.

**Lemma B18** Let  $z_1, \dots, z_m$  be a set of complex numbers, and let  $Z$  denote the collection of all sums of the form

$$\sum_{i=1}^m r_i z_i \quad \text{where } r_i \in \mathbb{Z}.$$

If  $y \in \mathbb{C}$  and  $yz \in Z$  for all  $z \in Z$ , then  $y$  is an algebraic integer.

*Proof.* The set  $Z$  is clearly closed under addition and scalar multiplication by elements of  $\mathbb{Z}$ . As  $yz_i \in Z$  for  $1 \leq i \leq m$  by hypothesis, we can find rational integers  $r_{ij}$  to satisfy

$$yz_i = \sum_{j=1}^m r_{ij} z_j \quad \text{for } i = 1, \dots, m.$$

Rewriting this equation we have

$$\sum_{j=1}^m (r_{ij} - \delta_{ij}y) z_j = 0 \quad \text{for } i = 1, \dots, m,$$

where  $\delta_{ij} = 0$  if  $i \neq j$ , and  $\delta_{ii} = 1$ . Hence this set of  $m$  homogeneous equations in  $m$  variables has a nonzero solution (by hypothesis and because the result clearly holds if  $y = 0$ ), and so

$$\det(r_{ij} - \delta_{ij}y) = 0.$$

The result follows because this equation can be rewritten as a polynomial equation in  $y$  with integer coefficients (as  $r_{ij} \in \mathbb{Z}$ ) and leading coefficient 1. The only term in the sum defining the determinant above which involves  $y^n$  is the product of its diagonal elements, viz:  $\prod_{i=1}^m (r_{ii} - y)$ , and the coefficient of  $y$  in this product is  $\pm 1$ .  $\square$

**Theorem B19** *The set of algebraic integers is closed under addition and multiplication, and so forms an integral domain.*

*Proof.* Let  $y_1$  and  $y_2$  be algebraic integers satisfying monic polynomial equations (with integer coefficients) of degrees  $n_1$  and  $n_2$ , respectively. Further, define

$$z_{ij} = y_1^i y_2^j \quad \text{for } 0 \leq i < n_1 \quad \text{and} \quad 0 \leq j < n_2,$$

and let  $Z_1$  denote the set of sums of the form

$$\sum_{i=0}^{n_1-1} \sum_{j=0}^{n_2-1} r_{ij} z_{ij},$$

where  $r_{ij} \in \mathbb{Z}$ . The elements of  $Z_1$  are clearly complex numbers, and set  $Z_1$  is closed under addition and scalar multiplication by elements of  $\mathbb{Z}$ , and so that it satisfies the conditions set out in Lemma B18. It is now a simple matter to check that

$$y_k z_{ij}, \quad (y_1 + y_2) z_{ij} \quad \text{and} \quad y_1 y_2 z_{ij}$$

all belong to  $Z_1$  for  $0 \leq i < n_1, 0 \leq j < n_2$  and  $k = 1, 2$ . Note that if  $y_k^{n_k}$  occurs in a calculation, then it can be replaced by a polynomial expression in lower powers of  $y_k$  using its defining equation. Hence by Lemma B18, both  $y_1 + y_2$  and  $y_1 y_2$  are algebraic integers. The result now follows as the remaining properties are inherited from the complex numbers.  $\square$

Note that the two proofs above work in a *module* over  $\mathbb{Z}$ . A module is similar to a vector space except that the underlying field is replaced by an integral domain which in this case is  $\mathbb{Z}$ .

The following corollary is used in both Chapters 13 and 14.

**Corollary B20** *If a complex number  $y$  is both an algebraic integer and a rational number, then it belongs to  $\mathbb{Z}$ .*

*Proof.* By hypothesis  $y$  satisfies a polynomial equation of the form

$$y^n + r_1 y^{n-1} + \cdots + r_n = 0 \quad \text{where } r_i \in \mathbb{Z} \quad \text{for } i = 1, \dots, n.$$

Suppose  $n > 1$ . Now  $y$  is also a rational number, and so  $y = a/b$  for some  $a, b \in \mathbb{Z}$  where  $b \neq 0$  and  $(a, b) = 1$ . Substituting this value of  $y$  in the equation above and multiplying by  $b^n$  we obtain

$$0 = a^n + r_1 a^{n-1} b + \cdots + r_n b^n = a^n + b(r_1 a^{n-1} + \cdots + r_n b^{n-1}).$$

This is impossible if  $n > 1$  because  $(a^n, b) = 1$  by definition.  $\square$

## Solution Appendix

### Answers and Solutions to Problems

Answers, hints and/or sketch solutions to most of the problems are given below. If a problem has wide applicability then a fuller solution is provided. Note that in some cases other methods will exist; you may find better, clearer and/or shorter solutions compared with those given below. *It is important to note that a number of these ‘solutions’ are incomplete, there are often details for you to fill in.* Please notify the author about any errors or omissions.

#### Solutions 2

**Problem 2.1** (i) Let  $X = \{g : g \in G\}$  and, for  $a \in G$ , let  $Y_a = \{ag : g \in G\}$ . By closure  $Y_a \subseteq X$ , and for each  $g \in G$ ,  $g = a(a^{-1}g)$  and so  $X = \{a(a^{-1}g) : g \in G\} \subseteq Y_a$ ; hence  $X = Y_a$ . Secondly, if  $Z = \{g^{-1} : g \in G\}$ , then  $Z \subseteq X$  as  $G$  is closed under inverses, but  $g = (g^{-1})^{-1}$  and so  $X = \{(g^{-1})^{-1} : g \in G\} \subseteq Z$ , hence  $Z = X$ .

(ii) Use induction on  $n$  for the term  $g = g_1 \odot g_2 \odot \cdots \odot g_n$  when  $n > 2$ . For  $n = 3$  the associativity axiom applies. Secondly, assume that the result holds for all bracketings of expressions with  $m$  elements where  $m < n$ . Consider two bracketings of  $g$ :

$$(g_1 \odot \cdots \odot g_j) \odot (g_{j+1} \odot \cdots \odot g_n) \text{ and } (g_1 \odot \cdots \odot g_k) \odot (g_{k+1} \odot \cdots \odot g_n) \quad (2.1)$$

where  $j \leq k$ . If  $j = k$  use the inductive hypothesis on the terms in the round brackets, and if  $j < k$ , use the inductive hypothesis again to rewrite (2.1) as

$$(g_1 \odot \cdots \odot g_j) \odot ((g_{j+1} \odot \cdots \odot g_k) \odot (g_{k+1} \odot \cdots \odot g_n)) \quad \text{and}$$

$$((g_1 \odot \cdots \odot g_j) \odot (g_{j+1} \odot \cdots \odot g_k)) \odot (g_{k+1} \odot \cdots \odot g_n).$$

Now use associativity. A similar argument applies if  $j > k$ . A further inductive argument is needed if more pairs of brackets are involved.

**Problem 2.2** (i) The operation is closed by definition, it is associative as  $\mathbb{Z}$  has this property, the neutral element is 0, and the inverse of  $a$  is  $7 - a$ , for  $0 \leq a \leq 6$ . Abelian.

(ii) The operation is closed and associative as in (i), the neutral element is 1, and the inverses are given by:  $1 \cdot 1 \equiv 2 \cdot 4 \equiv 3 \cdot 5 \equiv 6 \cdot 6 \equiv 1 \pmod{7}$ . Abelian.

(iii) The operation is closed and associative as in  $\mathbb{Q}$ , the neutral element is  $-3$ , and the inverse of  $a$  is  $-a - 6$ . Abelian.

(iv) Matrix multiplication is closed and associative, the neutral element is  $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ , and if  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ , then  $A^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} / \det A$ . Not Abelian.

(v) We have  $A^2 = B^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in Q$ , and so  $A^4 = B^4 = I_2$ . Also  $BA = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} = A^3B$ , and so  $BA^2 = (BA)A = (A^3B)A = A^6B = A^2B$ ; similarly  $BA^3 = AB = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ . As  $A^2 = B^2$ , these equations show that the group has eight elements:  $I_2, A, A^2, A^3, B, AB, A^2B$  and  $A^3B$ . The group axioms follow using  $(AB)^{-1} = BA = A^3B$  *et cetera*. Not Abelian, for example  $AB \neq BA$ . This is a representation of the quaternion group  $Q_2$ ; see page 118.

(vi)  $f_1$  acts as the neutral element. To establish closure all cases have to be checked separately, for instance, if  $x \in \mathbb{R}$ ,

$$f_3(f_4(x)) = 1 - f_4(x) = 1 - (1/(1-x)) = -x/(1-x) = f_5(x), \text{ and} \\ f_3(f_4(\infty)) = 1 - f_4(\infty) = 1 - (1/\infty) = 1 = f_5(\infty).$$

We have  $f_1, f_2, f_3$  and  $f_5$  are self inverse,  $f_4^{-1} = f_6$  and  $f_6^{-1} = f_4$ . The group is isomorphic to the dihedral group  $D_3$ ; for example map  $f_4$  to  $\alpha$  and  $f_2$  to  $\beta$  in the definition on page 3. Not Abelian.

(vii) If  $\theta$  and  $\phi$  are isometries, then

$$d(x, y) = d(\theta(x), \theta(y)) = d(\phi(\theta(x)), \phi(\theta(y))),$$

and so the set is closed under composition because composition of two bijections is a bijection. Composition is also associative, and the neutral element is the identity function  $\iota(x) = x$  for all  $x$ . Lastly, if  $\theta$  is an isometry (and so is a bijection), then  $\theta^{-1}$  is a bijection (see page 281), and

$$d(\theta^{-1}(x), \theta^{-1}(y)) = d(\theta(\theta^{-1}(x)), \theta(\theta^{-1}(y))) = d(x, y),$$

hence  $\theta^{-1}$  is also an isometry. Not Abelian, for example try rotation by  $\pi/3$  and reflection in the  $x$ -axis..

**Problem 2.3** (i) Associativity fails because  $(a - b) - c \neq a - (b - c)$  in general.

(ii) There is no neutral element and closure fails.

(iii) Not closed, for instance  $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ .

(iv)  $0 \in \mathbb{Q}$  but it has no inverse.

**Problem 2.4** (i) Let  $a \in S$ , so there exist  $c$  and  $c'$  satisfying  $ac = a$  and  $c'a = a$ . Show first  $c = c'$ . For if  $b \in S$ , there exist  $d$  and  $d'$  satisfying  $ad = b = d'a$ , so

$$bc = (d'a)c = d'(ac) = d'a = b,$$

that is,  $c$  is a right neutral element. This holds for all  $b \in S$ , and so for  $b = c'$ , hence  $c'c = c'$ . Similarly using  $ad = b$  we have  $c'c = c$ , and so  $c = c'$ .

Uniqueness follows because we have shown that *all* solutions  $x$  of  $bx = b$  equal  $c$ , a solution of  $xb = b$ . Therefore the neutral element properties hold, so let  $c = c' = e$ . Using the given conditions again, for  $a \in S$ , there exist  $a'$  and  $a''$  satisfying  $aa' = e = a''a$ , and then  $a'' = a''e = a''(aa') = ea' = a'$ . Lastly uniqueness can be proved as above.

(ii) First note that  $aa^*$  and  $a^*a$  are idempotents because the given equation shows that

$$aa^*aa^* = aa^* \quad \text{and} \quad a^*aa^*a = a^*a. \quad (2.2)$$

Now the given equation (twice) shows that  $(aa^*a)(a^*a^{**}a^*) = aa^*$ , hence by (2.2) we have

$$(aa^*)a^{**}a^*aa^* = (aa^*aa^*)a^{**}a^*aa^* = (aa^*a)(a^*a^{**}a^*)aa^* = (aa^*)aa^* = aa^*,$$

which by the given uniqueness property proves

$$a^{**}a^* = (aa^*)^*. \quad (2.3)$$

By (2.2) we also have  $aa^*aa^*aa^* = aa^*$ , and so applying the uniqueness property again we obtain  $(aa^*)^* = aa^*$ . Combining this with (2.3) gives  $a^{**}a^* = aa^*$ , and using the given equation again we obtain  $a^* = a^*(a^{**}a^*) = a^*(aa^*)$ , hence by the uniqueness property

$$a^{**} = a \quad \text{and} \quad aa^* = (aa^*)^*$$

by (2.3). Now continue, you need to show that  $aa^* = bb^*$  so that you can take  $aa^*$  as the unique neutral element.

**Problem ♦ 2.5** (i) Apply Theorem 2.13; note that  $H \leq G$ , and so  $H$  is not empty.

(ii)  $H \cap J = H$  is equivalent to  $H \subseteq J$ , so apply (i).

(iii) By Theorem 2.34, both  $H$  and  $J$  are cyclic. Suppose  $H = \langle a \rangle$  and  $J = \langle b \rangle$ . If  $H \cap J \neq \langle e \rangle$ , then there exists integers  $k$  and  $l$  satisfying  $1 \leq k, l < p$  and  $a^k = b^l$ . As  $(k, p) = 1$  we can find an integer  $m$  to satisfy  $km \equiv 1 \pmod{p}$ . Then  $a = a^{km} = b^{lm}$  and so  $H \subseteq J$ ; reversing this argument gives  $H = J$ .

**Problem 2.6**  $SS = \{s_1s_2 : s_1, s_2 \in S\}$ , so  $SS \subseteq S$  by group closure, also  $S \subseteq SS$  because  $se \in SS$  for  $s \in S$ . Secondly suppose  $TT = T$ , so  $T$  is closed under the group operation (for if  $t_1, t_2 \in T$ , then  $t_1t_2 \in TT = T$ ) and it is non-empty by definition. Since  $T$  is not empty, we use Theorem 2.7(iii) for inverses and the neutral element; hence  $T \leq G$ . False if  $G$  is infinite, an example is  $G = \mathbb{Z}$  and  $T$  is the non-negative integers.

**Problem ♦ 2.7** (i) If  $(gh)^n = e$ , then  $e = h(gh)^n h^{-1} = (hg)^n$ . If  $o(gh)$  is finite, this shows that  $o(hg) \mid o(gh)$ ; now reverse argument to obtain equality. This also shows that if  $o(gh)$  is finite, so is  $o(hg)$ ; hence take contrapositive in the infinite case.

(ii) Suppose  $m > 0$ . We have

$$m \frac{n}{(m, n)} = n \frac{m}{(m, n)} \quad \text{and} \quad \frac{m}{(m, n)}, \frac{n}{(n, m)} \in \mathbb{Z},$$

so  $(g^m)^{n/(m, n)} = e$  which gives  $o(g^m) \mid n/(m, n)$ . If not equal reverse argument to obtain a contradiction as in (iv) below. If  $m = 0$ , then  $(m, n) = n$  and  $g^0 = e$ , and if  $m < 0$  use  $g^{-n} = e$ .

(iii) Use (ii) and the Euclidean algorithm.

(iv) Suppose first  $(m, n) = 1$ , then  $\text{LCM}(m, n) = mn$ . We have  $(gh)^{mn} = (g^m)^n (h^n)^m = e$ , and so  $o(gh) = m_1 n_1$  where  $m_1 \mid m$  and  $n_1 \mid n$ . If  $m_1 < m$ . We have

$$(g^{m_1 n_1} h^{m_1 n_1})^{n/n_1} = e, \text{ so } g^{m_1 n} h^{m_1 n} = e,$$

and so  $g^{m_1 n} = e$  as  $o(h) = n$ . There exist integers  $r$  and  $s$  with  $rm + sn = 1$  or  $snm_1 = m_1 - rmm_1$ , hence  $e = g^{snm_1} = g^{m_1}$  as  $g^{m_1 n} = e$  which implies that  $o(g) \leq m_1 < m$ , a contradiction. If  $m$  and  $n$  have a common factor, remove it first and repeat this argument.

(v) By Lagrange's Theorem (Theorem 2.27), the order of each element of  $G$  divides  $o(G)$ , hence  $g^{o(G)} = e$  for all  $g \in G$ . Second part follows by definition.

(vi) By (iv) we have  $g^{mn} = e$ . Also by the Euclidean Algorithm (Theorem B2), as  $(m, n) = 1$ , there exist  $r, s \in \mathbb{Z}$  satisfying  $rm + sn = 1$ . Put  $a = g^{sn}$  and  $b = g^{rm}$ , then  $ab = g = ba$  and  $a^m = e = b^n$ . Suppose also  $a'b' = g = b'a'$  and  $(a')^m = e = (b')^n$ , then  $(a')^m (b')^m = (a'b')^m = (ab)^m = a^m b^m$  which gives  $(b')^{rm} = b^{rm}$ . But  $rm = 1 - sn$ , and so  $b = b'$ . Using a similar argument we have  $a = a'$ .

(vii) For example let  $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$  and  $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ . Then  $A^4 = B^3 = I_2$ , but  $AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$  which has infinite order in  $GL_2(\mathbb{Q})$  as  $(AB)^r = \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}$ .

**Problem 2.8** (i) As  $o(G) < \infty$  we can pair off elements  $a_i$  of order larger than 2 (so  $a_i \neq a_i^{-1}$ ) by  $\{(a_1, a_1^{-1}), (a_2, a_2^{-1}), \dots\}$ . Hence if  $o(G)$  is even, there are an even number of elements of order 1 or 2 in  $G$ , but there is exactly one element  $e$  of order 1.

(ii) We have  $o((\mathbb{Z}/p\mathbb{Z})^*) = p - 1$  (every positive integer less than  $p$  is coprime to  $p$ ), so by Problem 2.7(v), if  $g \in (\mathbb{Z}/p\mathbb{Z})^*$  then  $o(g^{p-1}) = e$ .

(iii) Use (i) as  $p - 1$  is the only element of order 2 in  $(\mathbb{Z}/p\mathbb{Z})^*$ , hence  $(p - 2)! \equiv 1 \pmod{p}$  as inverses are unique.

**Problem 2.9** We have  $g_1 = e$ , and so the table has the following form, where the operation is defined by elements in the top row times elements in the left-hand column,



	$e$	$g_2$	$\dots$	$g_n$
$e$	$e$	$g_2$	$\dots$	$g_n$
$g_2$	$g_2$	$*$	$\dots$	$*$
$\vdots$	$\vdots$	$\vdots$	$\dots$	$\vdots$
$g_n$	$g_n$	$*$	$\dots$	$*$

and each row and each column inside the box is a permutation of  $\{g_1, \dots, g_n\}$  with determined first entry, see Theorem 2.8. The converse does not hold as the example  $T$  below shows. The operation given by  $T$  is closed and it has a neutral element and inverses. But it is not associative, and left and right inverses are not always equal. For instance  $(g_3g_4)g_2 = g_5g_2 = g_3$  and  $g_3(g_4g_2) = g_3g_5 = g_4$ , also  $g_2g_4 = e$  and  $g_3g_2 = e$ .

$T$	$e$	$g_2$	$g_3$	$g_4$	$g_5$
$e$	$e$	$g_2$	$g_3$	$g_4$	$g_5$
$g_2$	$g_2$	$g_4$	$e$	$g_5$	$g_3$
$g_3$	$g_3$	$g_5$	$g_2$	$e$	$g_4$
$g_4$	$g_4$	$e$	$g_5$	$g_3$	$g_2$
$g_5$	$g_5$	$g_3$	$g_4$	$g_2$	$e$

**Problem 2.10** (i) Use  $(-1)^2 = 1$ , normal as  $\mathbb{R}^*$  is Abelian.

(ii) Clearly  $e \in X$  as  $e$  fixes all elements. If  $\sigma$  and  $\tau$  are perms. which fix 3, so do  $\sigma\tau$  and  $\sigma^{-1}$ , see page 43. Not normal, eg:  $(2, 3, 4)(2, 4)(2, 4, 3) = (3, 4)$  which moves 3; for cyclic notation see page 44.

(iiia) A normal subgroup. For  $\det I_2 = 1$ , if  $\det A = \det B = 1$  then  $\det A^{-1}B = 1$ , and  $\det C^{-1}AC = 1$ , for all  $C \in GL_2(\mathbb{Q})$ .

(iiib) A subgroup. For  $I_n$  is upper triangular, and if  $A$  and  $B$  are upper triangular, so are  $AB$  and  $A^{-1}$  (Lemma 3.16). Not normal. For example the conjugate of  $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$  by  $\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$  has lower left entry  $-1$ .

(iv)  $|1| = 1$ , and if  $|x|, |y| = 1$  then  $|xy| = |x^{-1}| = 1$ ; normal as group is Abelian.

(v) The set  $Z$  is not empty as the identity function  $\iota$ , where  $\iota(x) = x$  for all  $x$ , is differentiable. If  $f$  and  $g$  are differentiable, so is  $f \circ g$  as  $(d/dx)(f(g(x))) = f'(g(x))g'(x)$  where the primes denote differentiation, also as  $f^{-1}(f(x)) = x$  we have  $(d/dx)(f^{-1}(x)) = 1/(f'(f^{-1}(x)))$ . Normal.

**Problem 2.11** (i) Suppose  $H \leq \mathbb{C}^*$  and  $o(H) = n$ , then if  $h \in H$  we have  $h^n = 1$ , the neutral element of  $\mathbb{C}^*$ , by Problem 2.7(v). Hence  $h$  is an  $n$ -th root of unity, and so must belong to the set of all  $n$ -th roots of unity  $\{e^{2\pi ir/n} : r = 0, 1, \dots, n-1\}$  which has  $n$  members. But  $H$  also has  $n$  members, and so  $H = \langle e^{2\pi i/n} \rangle$ , the cyclic group generated by  $e^{2\pi i/n}$ .

(ii) The group  $\mathbb{Q}$  has infinitely many subgroups, examples are:  $\langle e \rangle$ ;  $\mathbb{Z}$ ; set of rational numbers with square-free denominators;  $\{a/p^n : a, n \in \mathbb{Z}, p \text{ a prime}, n \geq 0\}$ ; and set of rationals with a finite decimal expansion. For further details see Web Section 7.5 where we show that  $\mathbb{Q}$  has uncountably many subgroups which can be characterised in detail.

**Problem 2.12** (i)  $\{a, -a\}$ , one for each  $a \in \mathbb{R}^+$ .

(ii) Left cosets are  $(3, n)S_5^{(3)}$ , and right cosets are  $S_5^{(3)}(3, n)$ , for  $n = 1, \dots, 6$ , where  $S_5^{(3)}$  is the subgroup ( $\simeq S_5$ ) of the group of all permutations on  $\{1, \dots, 6\}$  which fix 3; see Chapter 3.

(iiia)  $\{A : \det A = t\}$ , one coset for each  $t \in \mathbb{Q}^*$ .

(iiib) The left coset of  $\begin{pmatrix} x & y \\ z & w \end{pmatrix}$  is set of matrices of the form  $\begin{pmatrix} ax & * \\ az & * \end{pmatrix}$  where  $a \neq 0$ , similar for right cosets.

(iv)  $\{se^{i\theta} : \theta \in \mathbb{R}\}$ , one for each positive real number  $s$ ; they form concentric circles in the complex plane with centre the origin and radius  $s$ .

(v) Cosets relate to the cardinality of the set of points where the functions are continuous but not differentiable, so one coset for each finite integer and many infinite cases. This is hard and requires a knowledge of transfinite ordinals!!

**Problem 2.13** (i) No, see Lemma 2.22. If  $H, J \leq G$  and  $sH = tJ$ , then  $t \in sH$ , and so  $sH = tH$  which gives  $tH = tJ$  and  $t^{-1}H = t^{-1}J$ . Hence  $H = t^{-1}HtH = t^{-1}JtJ = J$ .

(ii) Suppose  $a \in G \setminus H$ . We claim  $\langle a \rangle = G$ . For if not, there exists a maximal subgroup  $J$  satisfying  $\langle a \rangle \leq J < G$ , with possibly  $J = \langle a \rangle$ . But there is only one maximal subgroup by hypothesis, and so  $J = H$  and  $\langle a \rangle \leq H$  which contradicts our assumption that  $a \notin H$ . Note that the converse is false.

**Problem ♦ 2.14** (i) We have  $K \leq H$  and  $g^{-1}kg \in K$  for all  $g \in G$  and  $k \in K$ , so  $h^{-1}kh \in K$  for  $h \in H$  and  $k \in K$  (as  $H \subseteq G$ ), hence  $K \triangleleft H$ .

(ii) If  $J \leq Z(G) \triangleleft G$ , then  $J \leq G$  by Corollary 2.14. Also as  $J \subseteq Z(G)$ , for  $g \in G$  and  $j \in J$ , we have  $gj = jg$  or  $g^{-1}jg = j \in J$ . Hence  $J \triangleleft G$ .

(iii)  $\bigcap K_i \leq G$  by Theorem 2.15. Suppose  $g \in G$  and  $k \in \bigcap K_i$ . Then  $k \in K_i$  for all  $i$ , and as  $K_i \triangleleft G$ , we have  $g^{-1}kg \in K_i$ , again for all  $i$ , hence  $g^{-1}kg \in \bigcap K_i$ .

(iv) Note first  $e \in K \cap H$  and  $K \cap H \subseteq J \cap H$  as  $K \subseteq J$ . Hence  $K \cap H \leq J \cap H$  by Corollary 2.14. For normality we have  $j^{-1}kj \in K$ , for  $j \in J$  and  $k \in K$  (by hypothesis), so this also holds for  $j \in J \cap H$  and  $k \in K \cap H$ . Further, under the same conditions  $j, k \in H$ , and so  $j^{-1}kj \in H$  (as  $H \leq G$ ). Hence  $j^{-1}kj \in K \cap H$  and  $K \cap H \triangleleft J \cap H$ .

**Problem ♦ 2.15** (i) By Lagrange's Theorem (Theorem 2.27),  $o(G) = o(J)[G : J] = o(H)[G : H]$  and  $o(J) = o(H)[J : H]$ , so use substitution.

(ii) As  $H \cap J \leq H \leq G$  we have by (i)  $[G : H \cap J] = [G : H][H : H \cap J]$ , and similarly  $[G : H \cap J] = [G : J][J : H \cap J]$ . These show that the LCM of  $[G : H]$  and  $[G : J]$  divides  $[G : H \cap J]$ . Now if  $[G : H]$  and  $[G : J]$  are coprime, then these equations give  $[G : H] = [J : H \cap J]$  and  $[G : J] = [H : H \cap J]$ .

**Problem ♦ 2.16** (i) We have  $[e, e] = e \in G'$  and  $[a, b]^{-1} = [b, a]$ , so  $G' \leq G$  as closure is given by definition. Also

$$g^{-1}[a, b]g = g^{-1}a^{-1}gg^{-1}b^{-1}gg^{-1}agg^{-1}bg = [g^{-1}ag, g^{-1}bg]$$

which gives normality.

(iia)  $Z' = \langle e \rangle$ , the derived subgroup of an Abelian group is  $\langle e \rangle$ .

(iib) If  $D_3 = \langle a, b \mid a^3 = b^2 = e, bab = a^2 \rangle$ , then  $a^{-1}b^{-1}ab = a$  and  $b^{-1}a^{-1}ba = a^2$  *et cetera*; hence  $D'_3 = \langle a \mid a^3 = e \rangle$ .

(iic) We have  $[A, B] = [B, A] = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = C$ ; so derived subgroup is  $\langle C \rangle$ .

(iii) For  $a, b \in G$ , we have  $a^{-1}b^{-1}ab \in J$  (as  $G' \subseteq J$ ), and so if  $a \in G$  and  $b^{-1} \in J$  then  $a^{-1}bab^{-1} = j \in J$ , hence  $a^{-1}ba = jb \in J$ , that is  $J \triangleleft G$ .

(iv) If  $K \not\leq Z(G)$ , then there exist  $g \in G$  and  $k, k' \in K$  with  $g^{-1}kg = k'$  and  $k \neq k'$ . But then  $[g, k^{-1}] = k'k^{-1} \neq e$ , so  $K \cap G' \neq \langle e \rangle$ .

(v) As  $K \triangleleft G$ ,  $g^{-1}kg \in K$  for  $g \in G$  and  $k \in K$ . Now if  $k^{-1}g^{-1}kg \in J$  and  $g_1 \in G$ , then  $g_1^{-1}(k^{-1}g^{-1}kg)g_1 = (g_1^{-1}k^{-1}g_1)(g_1^{-1}g^{-1}g_1)(g_1^{-1}kg_1)(g_1^{-1}gg_1) \in [K, G] = J$ . Hence  $J \triangleleft G$  as  $J \leq G$  by definition, and  $J \leq K$  follows similarly. This property also be established by using the Correspondence Theorem (Theorem 4.16).

**Problem 2.17** (i)  $[a, b]^{-1} = (a^{-1}b^{-1}ab)^{-1} = b^{-1}a^{-1}ba = [b, a]$ .

(iia) Use induction several times. We have if  $r > 0$ ,  $[a^{r+1}, b]$

$$= a^{-1}a^{-r}b^{-1}a^r(bb^{-1})ab = a^{-1}[a^r, b]b^{-1}ab = a^{-1}[a, b]^r b^{-1}ab = [a, b]^{r+1},$$

by Theorem 2.7(iv) and the hypothesis. Similarly for  $s > 0$  we have  $[a, b^s] = [a, b]^s$ . For negative powers use  $[a^{-1}, b] = [a, b]^{-1}$  *et cetera*, because  $[a^{-1}, b][a, b] = a[a, b]b^{-1}a^{-1}b = e$  using given conditions.

(iib) Use induction, there is nothing to prove if  $t = 1$ . Main step:

$$\begin{aligned} (ab)^{t+1} &= ab(ab)^t = aba^tb^t[b, a]^{t(t-1)/2} \\ &= a^{t+1}a^{-t}ba^tb^{-1}b^{t+1}[b, a]^{t(t-1)/2} \\ &= a^{t+1}[a^t, b^{-1}]b^{t+1}[b, a]^{t(t-1)/2} \\ &= a^{t+1}b^{t+1}[b, a]^{t(t+1)/2}. \end{aligned}$$

Note that by (i) and (iia)  $[b, a]^t = [a^t, b^{-1}]$ , and we use the given conditions for the last equation.

(iii)  $(b^{-1}[a, c]b)[b, c] = b^{-1}a^{-1}c^{-1}acbb^{-1}c^{-1}bc = b^{-1}a^{-1}c^{-1}abc = [ab, c]$ . Second part similar.

(iv) Expand out and cancel terms as in (iii).

(v) Use induction. First let  $m = 1$ . Clear if  $n = 1$ , so suppose true for  $n > 1$ . We have, using  $(g^{-1}[h, j]g)^{-1} = g^{-1}[j, h]g$  *et cetera*,

$$[a_1, b_1 \cdots b_{n+1}] = [a_1, b_{n+1}](b_{n+1}^{-1}[a_1, b_1 \cdots b_n]b_{n+1}),$$

and by the inductive hypothesis this is a product of conjugates of commutators (note  $b_{n+1} \in H$ ). The general case follows similarly.

(vi) Let  $h_i \in H$ ,  $j_i \in J$ . By the results above we have

$$h_2^{-1}[h_1, j_1]h_2 = [h_1h_2, j_1][h_2, j_1]^{-1} \in [H, J],$$

$$j_2^{-1}[h_1j_1]j_2 = [h_1, j_2]^{-1}[h_1, j_1j_2] \in [H, J].$$

If  $g \in [H, J]$ , then  $g = c_1 \dots c_n$  where  $c_i = [a_i, b_i]^s$  for  $s = \pm 1$ ,  $a_i \in H$  and  $b_i \in J$ . The equations above show that  $d^{-1}cd \in [H, J]$  if  $d \in H$  or  $d \in J$ . Hence as  $G = \langle H, J \rangle$ , we see that  $g^{-1}cg \in [H, J]$  for all  $g \in G$  giving normality.

**Problem ♦ 2.18** (i) Show first  $A(B \cap C) \subseteq B \cap (AC)$ . For if  $gh \in A(B \cap C)$  where  $g \in A$  and  $h \in B \cap C$ , then  $gh \in AB = B$  as  $A \leq B$  and  $gh \in AC$ , and so  $gh \in B \cap (AC)$ . Conversely, if  $j \in B \cap (AC)$ , then  $j = ac \in AC$  where  $a \in A$  and  $c \in C$ . This gives  $a^{-1}j = c \in B \cap C$  (as  $A \leq B$  and  $j \in B$ ). Hence  $j \in A(B \cap C)$  because  $a^{-1} \in A$ . Result follows as this holds for all  $j \in B \cap (AC)$ .

(ii) Use (i).

(iii) We have  $B = B \cap (BC)$  [as  $B \subseteq BC$ ]  $= B \cap (AC) = A(B \cap C)$  [by (i)]  $= A(A \cap C) = A$  [as  $A \cap C \subseteq A$ ]. Note that if  $G$  is finite this result can also be proved using Problem 2.27 or Theorem 5.8.

(iv) This follows from (i), for using the given conditions we have  $AB \cap CD = A(B \cap CD) = AC(B \cap D)$ .

**Problem ♦ 2.19** (i) If  $[G : H] = 2$ , there are *two* cosets, one of which is  $H$ . So  $G = H \cup aH = H \cup Hb$  with disjoint unions, for all  $a, b \in G \setminus H$ , hence  $aH = G \setminus H = Hb$  for all  $a, b \notin H$ ; that is  $H \triangleleft G$ .

Second part. Choose  $a \notin H$ , so  $a \in bH$  for some  $b \notin H$ . If  $a^2 \notin H$  then  $a^2 \in bH$ , hence  $ab^{-1} = h_1$  and  $a^2b^{-1} = h_2$  where  $h_i \in H$ . These give  $a = h_2h_1^{-1} \in H$ , a contradiction, see Lemma 2.22.

(ii) By Lagrange's Theorem (Theorem 2.27),  $o(H) \mid o(G)$ , hence  $o(G)/o(H) \geq 2$  if  $H \neq G$ . For second part use (i).

(iii) Let  $G = D_4 = \langle a, b \mid a^4 = b^2 = e, bab = a^3 \rangle$ . By (i)  $H = \langle a^2, b \rangle \triangleleft G$  and  $J = \langle b \rangle \triangleleft H$ . But  $J$  is not normal in  $G$  because  $a^{-1}ba = a^2b \notin J$ .

(iv) The result is obvious if  $H \subseteq J$  or  $J \subseteq H$ . Suppose all elements of  $G$  belong to  $H$  or  $J$ . Let  $h \in H \setminus J$  and  $j \in J \setminus H$ . Now  $hj \in G$ , so  $hj \in H$  or  $hj \in J$  by supposition. If the former case holds,  $hj = h' \in H$  so  $j = h'h^{-1} \in H$ , impossible; argue similarly in the second case. If  $G$  is finite, then a second proof is:  $o(H), o(J) \leq o(G)/2$  by (ii). As  $e \in H$  and  $e \in J$ , we have  $o(H \cup J) < o(G)$ , hence there is an element in  $G$  not in  $H \cup J$ .

(v) As  $HJ = JH$ , every term  $hj$ ,  $h \in H$  and  $j \in J$  can be written in the form  $j'h'$  where  $j' \in J$  and  $h' \in H$ . Now use Theorem 2.13.

**Problem 2.20** (i)  $o(G) = 4$ . By Lagrange's Theorem (Theorem 2.27), if  $e \neq a \in G$ , then  $o(a) = 2$  or  $4$ . If  $o(a) = 4$  then the elements of  $G$  are  $a, a^2, a^3$  and  $a^4 = e$ , and the group is cyclic with generator  $a$ . Otherwise all non-neutral elements have order 2, and so the group is Abelian by Corollary 2.20. Hence if  $a$  and  $b$  are two of these elements, the third is  $ab$  where  $ba = ab$ , and the group is isomorphic to  $T_2$ , a product of two cyclic groups of order 2.

(ii)  $o(G) = 6$ . As above the non-neutral elements have orders 2, 3 or 6. Also, by Problem 2.8(i),  $G$  contains at least one element of order 2,  $a$  say. If all non-neutral elements have order 2, then as in the second part of (i),  $G$  is Abelian and there exist order two elements  $b, c \in G$ . But then  $ab, ac, bc$  and  $abc$  all belong to  $G$ , and are distinct, which gives at least eight elements in  $G$  which is impossible.

Hence  $G$  contains an element of order 3 or 6, but if  $o(b) = 6$  then  $o(b^2) = 3$ ; therefore  $G$  contains an element  $c$ , say, of order 3. If  $G$  does contain an element of order 6, then  $G$  is cyclic (see (i)). Hence we may suppose, if  $G$  is not cyclic, then  $G$  contains  $e, a$  (of order 2), and  $c, c^2$  (both of order 3). By Problem 2.19(i),  $\langle c \rangle \triangleleft G$ , and so

$$a^{-1}ca = aca \in \langle c \rangle \quad \text{which gives} \quad aca = e, c \text{ or } c^2.$$

If  $aca = e$  then  $c = a^2 = e$  which is impossible. If  $aca = c$  then  $ac = ca$ ,  $o(ac) = 6$  (note  $acac = c^2$ ,  $(ac)^3 = a$ , *et cetera*), and  $G$  is cyclic as above. Hence we may assume that  $aca = c^2$ , or equivalently  $ca = ac^2$ . This further shows that  $c^2a = cac^2 = ac^4 = ac$ . Therefore  $G$  contains the 6 elements  $e, a, c, c^2, ac = c^2a$  and  $ac^2 = ca$ , and  $G$  is isomorphic to the dihedral group  $D_3$ .

**Problem 2.21** Suppose first  $n = 2$ . Define a map  $\theta$  from the set of left cosets of  $H_1 \cap H_2$  in  $G$  to the set of pairs whose first entry is a left coset of  $H_1$ , and second entry is a left coset of  $H_2$  by

$$(x(H_1 \cap H_2))\theta = (xH_1, xH_2).$$

This is well-defined by Lemma 2.22, and if  $(xH_1, xH_2) = (yH_1, yH_2)$  then  $xH_1 = yH_1, xH_2 = yH_2$ , so  $x^{-1}y \in H_1$  and  $x^{-1}y \in H_2$ , and hence  $x^{-1}y \in H_1 \cap H_2$  and  $x(H_1 \cap H_2) = y(H_1 \cap H_2)$  by Lemma 2.22 again. Therefore  $\theta$  is injective which gives result as  $[G : H_1 \cap H_2]$  is the number of left cosets of  $H_1 \cap H_2$  in  $G$ . The general result follows from this by induction. Note that by Problem 2.15 we have equality in this expression if  $[G : H_1]$  and  $[G : H_2]$  are coprime integers.

**Problem 2.22** Use Theorem 2.15, Problem 2.21.

**Problem ♦ 2.23** (i)  $e = g^{-1}eg \in g^{-1}Hg$ , so the set is not empty. Also if  $a, b \in g^{-1}Hg$ , then  $a = g^{-1}hg, b = g^{-1}jg$  for  $h, j \in H$ , and  $a^{-1}b = g^{-1}h^{-1}jg \in g^{-1}Hg$ , so the subgroup conditions are satisfied.

(ii) Define a map  $\theta : H \rightarrow g^{-1}Hg$  by  $h\theta = g^{-1}hg$  for  $h \in H$ , this is a bijection which gives result.

(iii) If  $j \in g^{-1}Hg$ , then  $j = g^{-1}hg$  for some  $h \in H$  and so  $g j g^{-1} = h \in H$ . This shows that

$$g^{-1}Hg \subseteq \{j \in G : g j g^{-1} \in H\}.$$

For the converse, if  $k$  belongs to the RHS then  $g k g^{-1} = h \in H$  which gives  $k = g^{-1}hg$ , and so the opposite inclusion also follows.

**Problem ♦ 2.24** (i) By (i) in Problem 2.23 and Theorem 2.15,

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

Normality. Suppose  $x \in G$  and  $a \in \text{core}(H)$ , so  $a \in g^{-1}Hg$  for all  $g \in G$ . We have  $x^{-1}ax = (gx)^{-1}h(gx)$  for  $h \in H$ , that is  $x^{-1}ax$  equals a conjugate of  $h$  by an element  $(gx)$  in  $G$ . This holds for all  $g \in G$ , and so  $x^{-1}ax \in \bigcap_{g \in G} g^{-1}Hg$ , and hence  $\text{core}(H) \triangleleft G$ .

(ii) Note  $\text{core}(H) \subseteq H$  by definition. If  $J \leq H$  and  $J \triangleleft G$  then  $g^{-1}Jg \subseteq g^{-1}Hg$ , for all  $g \in G$ , hence  $J \leq \text{core}(H)$ .

(iii) This follows from (ii) for if there were two distinct maximal normal subgroups we could form their join which would contain both of them; see Theorem 2.30.

**Problem 2.25** (i) This follows from Problem 2.14(iii).

(ii) Let  $K = \langle g^{-1}Hg \mid g \in G \rangle$ . As  $H \leq H^*$  and  $H^* \triangleleft G$ , if  $g \in G$  and  $h \in H$ , then  $g^{-1}hg \in H^*$ , hence  $K \leq H^*$  by closure in  $H^*$ . Conversely note first that  $K \triangleleft G$ . For  $K \leq G$  by definition, and if  $j \in G$ , then for  $i = 1, 2, \dots$ ,  $g_i^{-1}h_i g_i \in K$ , and so  $j^{-1}(g_i^{-1}h_i g_i)j = (g_i j)^{-1}h_i(g_i j) \in K$  as  $g_i j \in G$ ; this gives normality. But  $H^*$  is the intersection of all normal subgroups containing  $H$ , hence  $H^* \leq K$  and equality follows.

(iii) Use the same method as in the proof of Theorem 2.17.

**Problem 2.26** (i)  $Z(\mathbb{Z}) = \mathbb{Z}$ , the centre of an Abelian group is the group itself.

(ii) Suppose  $D_4 = \langle a, b \mid a^4 = b^2 = (ab)^2 = e \rangle$ . Neither  $a$  nor  $a^3$  commute with  $b$ , so  $a, a^3, b \notin Z(D_4)$ , but  $a^2$  commutes with  $a$  and  $b$ . Hence  $Z(D_4) = \{e, a^2\}$ , a cyclic group of order 2.

(iii)  $Z(D_5) = \langle e \rangle$ , no power of  $a$  commutes with  $b$ .

(iv) If  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Z(GL_2(\mathbb{Q}))$ ,  $X = \begin{pmatrix} x & y \\ z & t \end{pmatrix} \in GL_2(\mathbb{Q})$ , then

$$AX = \begin{pmatrix} ax + bz & ay + bt \\ cx + dz & cy + dt \end{pmatrix} = \begin{pmatrix} xa + yc & xb + yd \\ za + tc & zb + td \end{pmatrix} = XA,$$

and so  $ax + bz = xa + yc$  or  $bz = cy$ , for all  $y, z \in \mathbb{Q}$ , which gives  $b = c = 0$ . We also have  $ay + bt = xb + yd$ , or  $y(a - d) = b(x - t) = 0$ , which gives  $a = d$ . Hence  $Z(GL_2(\mathbb{Q}))$  is the set of scalar matrices  $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$  where  $a \in \mathbb{Q}$  and  $a \neq 0$ .

(v)  $Z(S_3) = \langle e \rangle$ , no non-neutral element commutes both with two and with three cycles.

**Problem 2.27** Let  $Y = \{(ha, a^{-1}j) : a \in H \cap J\}$ . As  $haa^{-1}j = hj = g$ , we have  $g\theta^{-1} \subseteq Y$ . Now if  $(h_i, j_i) \in g\theta^{-1}$ ,  $i = 1, 2$  and  $h_1j_1 = g = h_2j_2$ , then  $h_1^{-1}h_2 = j_1j_2^{-1} = a$ , say, where  $a \in H \cap J$ . This gives  $h_2 = h_1a$  and  $j_2 = a^{-1}j_1$ , and so  $g\theta^{-1} \supseteq Y$ . Also  $(ha, a^{-1}j) = (hb, b^{-1}j)$  implies  $a = b$  by cancellation. Therefore  $o(g\theta^{-1}) = o(H \cap J)$ , that is  $o(g\theta^{-1})$  is independent of  $g$ . The result follows.

**Problem ♦ 2.28** Let  $J$  be the subgroup of  $G$  generated by all involutions in  $G$ , we have  $o(J) > 1$  by the quoted problem. If  $g \in G$  and  $o(J) = 2$ , then  $(g^{-1}jg)^2 = g^{-1}j^2g = e$ , and so  $g^{-1}jg$  has order 2 and therefore belongs to  $J$ . Secondly if  $o(j_1) = o(j_2) = 2$ , then  $g^{-1}j_1j_2g = (g^{-1}j_1g)(g^{-1}j_2g)$ , a product of elements of order 2. Hence  $J \triangleleft G$ , but  $G$  is simple, and so  $J = G$ . Note that the result also applies for infinite groups.

**Problem 2.29** (i) and (ii) Clearly  $a \in HaJ$ , and if  $b \in HaJ$ , then  $b = haj$  ( $h \in H, j \in J$ ) and  $HbJ = HhajJ = HaJ$ .

(iii) Use: If  $Haj_1 = Haj_2$ , then  $h \in H$  exists satisfying  $aj_1 = haj_2$  ( $j_i \in J$ ) or  $j_1j_2^{-1} = a^{-1}ha \in a^{-1}Ha$  as  $j_1j_2^{-1} \in J$  clearly holds.

(iv) Use (ii) and (iii).

(v) Two double cosets:  $\langle(1, 2, 3)\rangle(1, 2)\langle(1, 2, 3, 4)\rangle =$   
 $\{(1, 2), (1, 3), (2, 3), (1, 2, 4), (1, 3, 4), (1, 4)(2, 3), (1, 3, 2, 4), (1, 4, 2, 3), (2, 4),$   
 $(1, 4, 3), (2, 4, 3), (1, 2)(3, 4)\},$

and

$\langle(1, 2, 3)\rangle(1, 2)\langle(1, 4)(2, 3)\rangle = \{(1, 2), (1, 3), (2, 3), (1, 4), (1, 2, 3, 4), (1, 3, 2, 4)\}.$

**Problem 2.30** (i)  $e \in J_1$  so  $e \in J$ ; if  $j \in J$ , then for some  $i$  we have  $j \in J_i$ , so  $j^{-1} \in J_i \leq J$ ; and if  $j, k \in J$ , then  $j \in J_{i_1}$  and  $k \in J_{i_2}$ , so if  $i = \max(i_1, i_2)$ , then  $j, k \in J_i \leq J$ .

(ii) Suppose  $K \triangleleft J$  and  $J_i$  is simple. By Problem 2.14(iv) we have  $K \cap J_i \triangleleft J_i$ , so either  $K \cap J_i = \langle e \rangle$  which can only happen if  $K = \langle e \rangle$ , or  $J_i \leq K$ . But as  $J_i$  is simple for infinitely many  $i$ , this gives  $J \leq K$ .

## Solutions 3

**Problem ♦ 3.1** (i) We have  $(1, k)(1, j)(1, k) = (j, k)$  if  $j \neq k$  and  $j, k \geq 2$ , now use Lemma 3.5.

(ii) For  $j > 1$ , use  $(1, j)(j, j+1)(1, j) = (1, j+1)$ , induction, and (i); see Problem 3.21.

(iii) For  $j > 1$  we have  $(1, 2, \dots, n)^{-1}(1, j)(1, 2, \dots, n) = (2, j+1)$  and  $(2, j+1)(1, 2)(2, j+1) = (1, j+1)$ , now use (i) and induction.

(iv) If  $i, j, k$  and  $l$  are distinct, use  $(i, j)(k, l)(i, j)(k, l) = (k, l, m)$  and Theorem 3.12.

**Problem 3.2** If  $\sigma = (1, 2, 3)(4, 5, 6)$  and  $\alpha = (1, 2, 3, 4, 5, 6)$  then

$$\alpha^{-1}\sigma\alpha = (1, 5, 6)(2, 3, 4) = \tau.$$

There are 17 further solutions  $\alpha$  to  $\sigma\alpha = \alpha\tau$ , they are:

$(1, 4), (2, 5)(3, 6), (1, 2, 3, 4), (1, 3, 2, 4), (1, 4, 5, 6), (1, 4, 6, 5), (1, 5, 2, 6, 3),$   
 $(1, 6, 3, 5, 2), (2, 5, 3, 6, 4), (2, 5, 4, 3, 6), (2, 6)(1, 5, 4, 3), (3, 5)(1, 6, 4, 2),$   
 $(1, 5, 3)(2, 6, 4), (1, 6, 2)(3, 5, 4), (1, 2, 3, 4, 5, 6), (1, 3, 2, 4, 5, 6),$   
 $(1, 2, 3, 4, 6, 5),$  and  $(1, 3, 2, 4, 6, 5).$

**Problem ♦ 3.3** Use Theorem 3.6. (i) We have  $S_3 (\simeq D_3)$  has three classes:  $\{e\}, \{(1, 2), (1, 3), (2, 3)\}$  and  $\{(1, 2, 3), (1, 3, 2)\}$ .

(ii)  $S_4$  has five classes:  $\{e\}$ , six 2-cycles, eight 3-cycles, six 4-cycles, and three 2-cycle by 2-cycles.

(iii)  $S_5$  has seven classes:  $\{e\}$ , ten 2-cycles, twenty 3-cycles, thirty 4-cycles, twenty-four 5-cycles, fifteen 2-cycle by 2-cycles, and twenty 2-cycles by 3-cycles making 120 elements in all.

For the alternating groups we argue as follows. We have, for example,

$$(1, 2, 3)(1, 2)(3, 4)(1, 3, 2) = (1, 3)(2, 4)$$

and  $(3, 4, 5)(1, 2)(3, 4)(3, 5, 4) = (1, 2)(3, 5)$ ; these and similar identities show that products of two distinct 2-cycles are conjugate in alternating groups  $A_n$  for  $n \geq 4$ . Hence we have:

(iv) As  $A_3$  is Abelian, it has three singleton conjugacy classes:  $\{(1, 2, 3)\}, \{(1, 3, 2)\}$  and  $\{e\}$ .

(v)  $A_4$  has four conjugacy classes:  $\{e\}$ , two, each containing four 3-cycles, and one containing three 2-cycle by 2-cycles (see above). Theorem 5.19 shows that the number of conjugates of an element in  $G$  divides  $o(G)$ , and so the eight 3-cycles cannot form a single conjugacy class. By direct calculation the classes are:  $\{(1, 2, 3), (1, 4, 3), (1, 2, 4), (2, 4, 3)\}$  and  $\{(1, 3, 2), (1, 3, 4), (1, 4, 2), (2, 3, 4)\}$  (note  $4 \mid 12$ ).

(vi)  $A_5$  has five classes:  $\{e\}$ , twenty 3-cycles, fifteen 2-cycle by 2-cycles, and two classes each containing twelve 5-cycles. All 3-cycles are conjugate by Theorem 3.12 ( $n > 4$  in this result). The third claim follows as above, and



the last statement is best proved using results from Section 5.2. But by direct calculation we see that the first class contains

$$(1,2,3,4,5), (1,2,4,5,3), (1,2,5,3,4), \\ (1,3,4,2,5), (1,4,2,3,5) \text{ and } (1,4,5,2,3),$$

and their inverses (so 12 in all), and the second class contains the remaining twelve 5-cycles. Note that for each pair of conjugate 5-cycles there are five conjugating elements, so for example the conjugating elements for the pair  $(1, 2, 3, 4, 5)$  and  $(1, 2, 4, 5, 3)$  (that is  $\sigma : \sigma^{-1}(1, 2, 3, 4, 5)\sigma = (1, 2, 4, 5, 3)$ ) are  $(1, 3, 2)$ ,  $(3, 4, 5)$ ,  $(1, 4)(3, 5)$ ,  $(1, 2, 4, 3, 5)$  and  $(1, 5, 4, 2, 3)$ .

(vii) A normal subgroup is a union of conjugacy classes one of which must be  $\{e\}$  (Theorem 2.29(ii)), also the order of a subgroup divides the order of the group by Lagrange's Theorem. By (ii) possible orders for proper non-neutral normal subgroups are 1+3 (the neutral element and three 2-cycle by 2-cycles) and 1+3+8 (the even permutations). Both of these form subgroups of  $S_4$  because they are closed under products and inverses, and therefore are normal.

(viii) Similarly the conjugacy classes of  $A_4$  have orders 1, 3 and 4 (twice), and  $o(A_4) = 12$ , hence  $A_4$  has a normal subgroup of order 4 as in  $S_4$  above, it is often denoted by  $V$ . This is the only non-neutral proper normal subgroup of any alternating group.

**Problem 3.4** (i) As  $\sigma$  and  $\tau$  are disjoint, they apply to disjoint subsets of the underlying set  $N = \{1, \dots, n\}$  upon which  $S_n$  is acting. But  $\tau^{-1} = \sigma$  and so if the cycle  $(a, b, \dots)$  occurs in  $\sigma$ , the cycle  $(\dots, b, a)$  occurs in  $\tau$  which contradicts the hypothesis.

(ii) No. For example let  $\sigma = (1, 2)(3, 4)$ ,  $\tau = (5, 6)$  and  $\nu = (1, 3)$ ; here  $\sigma\nu = (1, 2, 3, 4)$  and  $\nu\sigma = (4, 3, 2, 1)$ .

(iii)  $\sigma$  has the form  $(i, i\sigma, i\sigma^2, \dots)$  and  $\tau$  has the form  $(i, i\tau, i\tau^2, \dots)$ . So corresponding entries are equal, but do they have the same length? Yes, for if the length of  $\sigma$  is  $k$  and of  $\tau$  is  $l$ , and  $k < l$ . Then  $i\sigma^k = i$  whilst  $i\tau^k \neq i$ , a contradiction.

(iv) By Theorem 3.4 suppose  $\sigma = \tau_1 \dots \tau_r$  where the  $\tau_i$  are disjoint cycles which commute in pairs. So  $\iota = \sigma^p = \tau_1^p \dots \tau_r^p$ , and hence  $\tau_s^p = \iota$  for  $1 \leq s \leq r$ . If  $o(\tau_s) = m < p$ , then we can find integers  $t, u$  to satisfy  $tp + um = 1$  (Euclidean Algorithm (Theorem B2)), and  $\tau_s = \tau_s^{tp+um} = \iota$ . In this problem  $e$  and  $\iota$  are synonymous.

**Problem 3.5** If  $\sigma \in S_n$ , then  $\sigma = \tau_1 \tau_2 \dots \tau_r$  where each  $\tau_i$  is a cycle of length  $t_i$ , say, and  $t_1 + \dots + t_r = n$ ; note, some may be 1-cycles. Now the order of a  $k$ -cycle is  $k$ , the order of a  $k$ -cycle by  $l$ -cycle is  $\text{LCM}(k, l)$  provided  $k + l \leq n$ , *et cetera*. So the order of  $\sigma$  is  $\text{LCM}(t_1, \dots, t_r)$ . For  $S_7$ , the orders are 1, 2,  $\dots$ , 7 (cycles and others, for example a 2-cycle  $\times$  2-cycle  $\times$  3-cycle has order 6), 10 (2-cycle  $\times$  5-cycle), and 12 (3-cycle  $\times$  4-cycle).

For  $A_n$  we need the extra condition:  $2 \mid ((t_1 - 1) + \dots + (t_r - 1))$ . For  $A_7$  the orders are 1, 3, 5, 7 (cycles), 2 (2-cycle  $\times$  2-cycle), 3 again (3-cycle  $\times$  3-cycle), 4 (2-cycle  $\times$  4-cycle), and 6 (2-cycle  $\times$  2-cycle  $\times$  3-cycle).

**Problem 3.6** As  $q$  is prime it has a primitive root,  $m$  say. Let  $r = m^{(q-1)/p}$ , then  $r^p \equiv 1 \pmod{q}$  and  $r^t \not\equiv 1 \pmod{q}$  for  $0 < t < p$ . With this choice of  $r$  we have

$$1\tau_r^t \equiv r^t \pmod{q},$$

so the first  $p$ -cycle in  $\tau_r$  is  $(1, r, r^2, \dots, r^{p-1})$ . Now suppose  $c$  is the smallest integer not in this cycle, then  $(c, cr, cr^2, \dots, cr^{p-1})$  is the second  $p$ -cycle disjoint from the first. Continue. Note that  $\tau_r$  maps  $q$  to  $q$ . Now  $\sigma^q = \tau_r^p = e$ . Also  $\tau_r^{-1}\sigma\tau_r$  maps  $kr \rightarrow k \rightarrow k+1 \rightarrow (k+1)r$ , so it maps  $q \rightarrow 1, 1 \rightarrow r+1$ , *et cetera*, that is  $\tau_r^{-1}\sigma\tau_r = \sigma^r$ , which in turn gives  $\sigma^t\tau_r^u = \tau_r^u\sigma^{r^t u}$ . So every element of the group can be expressed as a power of  $\tau_r$  followed by a power of  $\sigma$ . Therefore, changing symbols, the group has the presentation

$$\langle a, b \mid a^q = b^p = e, b^{-1}ab = a^r \rangle.$$

There are a number of choices for  $r$  but they all give rise to isomorphic groups. For example if we replace  $r$  by  $r^u$  (modulo  $q$ ), then we should also replace  $b$  by  $b^u$ . Groups of this type are called *Frobenius* or *metacyclic*, see page 130.

**Problem ♦ 3.7** (i) In  $A_{n+2}$  the set of permutations  $X$  which leave  $n+1$  and  $n+2$  fixed forms a copy of  $A_n$  (and so ‘half’ of  $S_n$ ) in  $A_{n+2}$ . Secondly, if  $\tau$  is an odd permutation in  $S_n$  then  $\tau(n+1, n+2)$  is an even in  $A_{n+2}$ . Let  $Y = \{\tau(n+1, n+2) : \tau \in S_n, \tau \text{ odd}\}$ , then  $X \cup Y \leq A_{n+2}$ . Show this by noting that disjoint cycles commute (Theorem 3.4), and  $(n+1, n+2)^2 = e$ .

(ii) Use the quoted facts and Problem 2.14(iv); note that the only subgroup of  $S_n$  with index 2 is isomorphic to  $A_n$ .

**Problem 3.8** (i) We have  $\theta^{n/r} = (a_1, \dots, a_r) \dots (d_1, \dots, d_r) = \sigma$ . Also, if  $\phi = (c_1, \dots, c_n)$  and  $k \mid n$ ,  $\phi^{n/k} = (c_1, c_{k+1}, \dots, c_{(n-k)+1}) \dots (c_k, c_{2k}, \dots, c_n)$ . This only works for divisors  $k$  of  $n$ .

(ii) This follows from (i), if  $n = p$  the only divisors are 1 or  $p$ .

**Problem 3.9** (i) The problem is badly worded, it should ask for an estimate of the number of copies of  $S_k$  that occur in  $S_n$ . Let  $Y$  be a  $k$ -element subset of  $X = \{1, \dots, n\}$ ,  $k \leq n$ . The set of permutations which fix all elements in  $X \setminus Y$  clearly forms an isomorphic copy of  $S_k$  in  $S_n$ . There are  $\binom{n}{k}$  choices for  $Y$  and so at least  $\binom{n}{k}$  copies of  $S_k$  in  $S_n$ .

(ii) By (i)  $S_Y$  and  $S_Z$  are subgroups of  $S_n$  (isomorphic to  $S_k$  and  $S_{n-k}$ , respectively). If  $\sigma_1$  and  $\sigma_2$  are perms. of  $Y$ , and  $\tau_1$  and  $\tau_2$  are perms. of  $Z$ , then by Theorem 3.4  $(\sigma_1\tau_1)^{-1}(\sigma_2\tau_2) = \sigma_1^{-1}\sigma_2\tau_1^{-1}\tau_2 \in S_Y \times S_Z$ . As  $S_Y \times S_Z$  is not empty, it forms a subgroup of  $S_n$ . [By Theorem 7.3, it is also a direct product. For  $S_Y \cap S_Z = e$ , and if  $\theta, \sigma \in S_Y$  and  $\tau \in S_Z$ , then  $(\sigma\tau)^{-1}\theta(\sigma\tau) = \tau^{-1}(\sigma^{-1}\theta\sigma)\tau = \sigma^{-1}\theta\sigma \in S_Y$  by Theorem 3.4 again. This shows that  $S_Y \triangleleft S_Y \times S_Z$  *et cetera*.] For maximality show that the set generated by  $S_Y, S_Z$  and a suitably chosen 2-cycle in fact contains all 2-cycles, and then use Theorem 3.4 (note  $k \neq n-k$ ).

(iii) By (ii),  $S_n \times S_n$  is isomorphic to a subgroup of  $S_{2n}$  of products of perms.  $\sigma\tau$  where  $\sigma$  is a perm. on  $Y = \{1, \dots, n\}$ , and  $\tau$  is a perm. on  $Z = \{n+1, \dots, 2n\}$ . Let  $\xi = (1, n+1)(2, n+2) \dots (n, 2n) \in S_{2n}$ .

Now for example

$$\xi\sigma\tau = \begin{pmatrix} 1 & \cdots & n & n+1 & \cdots & 2n \\ (n+1)\tau & \cdots & (2n)\tau & 1\sigma & \cdots & n\sigma \end{pmatrix}.$$

This shows that the group generated by  $\xi$  and the elements of  $S_n \times S_n$  is a subgroup of the group of all perms. on  $Y \cup Z$ , that is  $S_{2n}$ . It is proper as this subgroup has order  $2(n!)^2 < (2n)!$  when  $n > 1$ ; note also this subgroup preserves the partition of  $Y$  and  $Z$  whilst  $S_{2n}$  does not. For example see Section 8.1 where  $S_4$  is discussed, the subgroup generated by the order 2 elements  $(1, 2)$ ,  $(3, 4)$  and  $(1, 3)(2, 4)$  has order 8, and is isomorphic to  $D_4$  in this case; see page 156.

**Problem ♦ 3.10** (i) First consider the permutation representation. It has three elements of order 2:  $(1, 2)(3, 4)$ ,  $(1, 3)(2, 4)$ ,  $(1, 4)(2, 3)$ , and eight elements of order 3:  $(1, 2, 3)$ ,  $(1, 3, 2)$ ,  $(1, 3, 4)$ ,  $(1, 4, 3)$ ,  $(2, 3, 4)$ ,  $(2, 4, 3)$ ,  $(1, 4, 2)$ ,  $(1, 2, 4)$  (written as inverse pairs). By direct calculation we see that any set containing an element of order 2 and an element of order 3 generates the whole group, see Theorem 3.3.

Secondly we have, again by direct calculation, the elements of  $\langle a, b \mid a^2 = b^3 = (ab)^3 = e \rangle$  are

$$e; a, bab^2, b^2ab; b, b^2, ab, b^2a, ab^2, ba, aba, bab,$$

the second, third and fourth have order 2, and the last eight have order 3. (For this use  $babab = a$  and  $ababa = b^2$  to show that  $abab = ab^2 = b^2a \dots$ ) Hence both groups have order 12, and if we map  $a \mapsto (1, 2)(3, 4)$  and  $b \mapsto (1, 2, 3)$ , then we obtain an isomorphism. In this correspondence the two lists above ‘agree’, so for example  $bab \mapsto (1, 2, 4)$ , and the isomorphism gives  $(ab^2)(bab) = b$  and  $(2, 3, 4)(1, 2, 4) = (1, 2, 3)$  *et cetera*.

Note that in this problem by symmetry group we mean the rotational symmetry group; see **Web Section 2.6**. For the third group if we map a rotation by  $\pi$  about the centres of opposite edges to  $a$ , and rotation by  $2\pi/3$  about a line through a vertex and the centre of its opposite face to  $b$ , we obtain a one-to-one correspondence between groups (b) and (c). The reader should try this with a model of a tetrahedron.

(ii) By Lagrange’s Theorem (Theorem 2.27), non-neutral proper subgroups of  $A_4$  can only have orders 2, 3, 4 or 6. It cannot have a subgroup of order 6 as this would be normal, see Problems 3.3 and 2.19(i). It also cannot have a cyclic subgroup of order 4 as it contains no element of order 4. So the possibilities are  $C_2$ ,  $C_3$  and  $T_2$ . As  $A_4$  contains exactly three elements of order 2, it has three subgroups of type  $C_2$ , one for each element of order 2, and one of type  $T_2$ . This last subgroup is normal by Theorem 3.6. By Problem 3.3,  $A_4$  has four subgroups of type  $C_3$ . None is normal, use Theorem 3.6 again, and see the Sylow theory in Chapter 6.

**Problem 3.11** (i) In  $H$  we have  $a^5 = b^4 = e$  and  $ba^2 = ab$ . So  $ba^4 = ba^2a^2 = aba^2 = a^2b$ ,  $ba = ba^6 = ba^4a^2 = a^2ba^2 = a^3b$ , and  $ba^3 = ba^8 = a^3ba^2 = a^4b$ ; hence  $ba^r = a^{3r}b$ . Similarly  $b^2a = bba = ba^3b = a^4b^2$  *et cetera*.

Hence  $b^s a^r = a^{3^s r} b^s$  which shows that the group has 20 elements because each expression in  $a$  and  $b$  can be replaced by one of the form  $a^r b^s$  where  $0 \leq r < 5$  and  $0 \leq s < 4$ , and  $a^r b^s = e$  implies  $r = s = 0$ . Construct a copy which is a subgroup of  $S_5$  as follows. Let  $a \mapsto \sigma = (1, 2, 3, 4, 5)$ , so  $\sigma^5 = e$ . Now look for a 4-cycle  $\tau$  to satisfy  $\sigma\tau = \tau\sigma^2$ . We have  $a^2 \mapsto (1, 3, 5, 2, 4)$ , and so if we let  $b \mapsto \begin{pmatrix} 2 & 3 & 4 & 5 \\ r & s & t & u \end{pmatrix}$ , then

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \\ r & s & t & u & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & r & s & t & u \\ 3 & \cdot & \cdot & \cdot & \cdot \end{pmatrix} = \tau\sigma^2,$$

This gives  $1\sigma^2 = 3$ , so  $r = 3$  (bottom left-hand entries in the matrices above). As  $3\sigma^2 = 5$  we have  $s = 5$ , and continuing we obtain  $t = 2$  and  $u = 4$ . Hence  $\tau : b \mapsto (2, 3, 5, 4)$ , and the representation is complete. Similar constructions give maximal subgroups of order  $2n(2n+1)$  in  $S_{2n+1}$ . There is a maximal subgroup of order 42 in  $S_7$  with presentation  $\langle \sigma, \tau \mid \sigma^7 = \tau^6 = e, \sigma\tau = \tau\sigma^3 \rangle$  where

$$\sigma \mapsto (1, 2, 3, 4, 5, 6, 7), \quad \tau \mapsto (2, 4, 3, 7, 5, 6).$$

The reader should also refer to the last part of **Web Section 6.5**.

(ii)  $A_5$  has fifteen cyclic subgroups of order 2 ( $\langle (1, 2)(3, 4) \rangle, \dots$ ), ten of order 3 ( $\langle (1, 2, 3) \rangle, \dots$ ), and six of order 5 ( $\langle (1, 2, 3, 4, 5) \rangle, \dots$ ); also five of type  $T_2 \simeq C_2 \times C_2$ . By Problem 3.7,  $S_3 \leq A_5$ , for instance the subgroup generated by  $(1, 2, 3)$  and  $(4, 5)$ ; there are ten copies of  $S_3$  in all;  $C_6$  is not a subgroup because  $A_5$  contains no elements of order 6. There are no subgroups of order 7, 8 or 9 as these integers do not divide  $o(A_5)$ .

**Problem 3.12** (i) Each row has one '1' and  $n-1$  zeros by definition, same for columns as  $\sigma$  is a bijection on  $\{1, 2, \dots, n\}$ .

(ii) By definition  $\det((a_{i,j}))$  is a sum of terms of form  $\pm a_{1,1\tau} a_{2,2\tau} \dots a_{n,n\tau}$ , one for each  $\tau \in S_n$ . Each term is zero except when  $\tau = \sigma$ , and this term equals  $\pm 1$ , and so the determinant equals  $\pm 1$ .

(iii) The inverse of a matrix in  $P_n$  is its transpose;  $I_n$  corresponds to the identity permutation; and  $P_n$  is closed under matrix multiplication. Hence  $P_n \leq GL_n(F)$ . Not normal, for instance  $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & -3 \\ 1 & -2 \end{pmatrix} \notin P_2$ .

(iv) A matrix corresponding to a 2-cycle is  $I_n$  with one pair of rows interchanged, so it has determinant  $-1$ . Hence, if  $\sigma$  is a product of an even number of 2-cycles (that is, it is even), then the determinant of the matrix corresponding to  $\sigma$  is an even power of  $-1$ , that is 1.

**Problem 3.13** (i)  $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ ,  $I_2$  and  $\begin{pmatrix} \eta^5 & 0 \\ 0 & \eta \end{pmatrix}$ .

(ii)  $D = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ .

(iii) The elements of the group are  $C^t D^u$  for  $0 \leq t \leq 5$  and  $0 \leq u \leq 1$ , twelve in all. The group has the presentation  $\langle c, d \mid c^6 = e, c^3 = d^2, d^{-1}cd = c^5 \rangle$  and this can be rewritten as  $\langle c, d \mid c^3 = d^2 = (cd)^2 \rangle$ ; a presentation of dicyclic group  $Q_3$ , see pages 59 and 159.

**Problem 3.14** Suppose the 4-element field consists of  $\{0, 1, c, c+1\}$  where  $c^2 = c+1$  and we work modulo 2 (so  $1 = -1$ ). Let  $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ , then  $A^2 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$  and  $A^3 = I_2$  giving an order 3 cyclic subgroup in  $GL_2(2)$ . Secondly, for each  $2 \times 2$  matrix  $C \in GL_2(4)$  we define a  $4 \times 4$  matrix  $C^* \in GL_4(2)$  as follows: if 0 occurs in  $C$  replace it by the  $2 \times 2$  zero matrix  $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ , if 1 occurs in  $C$  replace it by  $I_2$ , if  $c$  occurs in  $C$  replace it by the  $2 \times 2$  matrix  $A$  defined above, and if  $c+1 = c^2$  occurs in  $C$  replace it by  $A^2$ . This defines a map from  $GL_2(4)$  to  $GL_4(2)$ , you need to check that all matrices  $C^*$  constructed in this way have determinant 1.

Using the methods given in Chapter 4 we can show that this map is an injective homomorphism, or the subgroup condition (Theorem 2.13) can be applied. Note that we have  $o(GL_4(2)) = 20160$  and  $o(GL_2(4)) = 180$ ; see Chapter 12, especially Problem 12.13.

**Problem ♦ 3.15** If  $A = (a_{ij}), B = (b_{ij}) \in UT_n(F)$ , then  $a_{ij} = b_{ij} = 0$  if  $i > j$ , and the  $(i, j)$ th term of  $AB$  is

$$a_{ii}b_{ij} + \cdots + a_{ij}b_{jj}, \quad (3.1)$$

if  $i \leq j$ . Also the subdiagonals of  $A^{-1}$  consist entirely of zeros, and the diagonal is

$$(a_{11}^{-1}, \dots, a_{nn}^{-1}); \quad (3.2)$$

note that as  $A$  is non-singular,  $a_{ii} \neq 0$ , for  $i = 1, \dots, n$ . The first superdiagonal of  $A^{-1}$  is

$$(-a_{12}/a_{11}a_{22}, \dots, -a_{n-1,n}/a_{n-1,n-1}a_{nn}), \quad (3.3)$$

the second superdiagonal is

$$\left( (a_{12}a_{23} - a_{13}a_{22})/a_{11}a_{22}a_{33}, \dots, \right. \\ \left. (a_{n-2,n-1}a_{n-1,n} - a_{n-2,n}a_{n-1,n-1})/a_{n-2,n-2}a_{n-1,n-1}a_{nn} \right), \quad (3.4)$$

(note  $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$ ) with similar expressions for the remaining superdiagonals.

(i) By (3.1) above the diagonal of  $AB$  is  $(a_{11}b_{11}, \dots, a_{nn}b_{nn})$ , so use (3.2), and Theorems 2.13 and 2.29.

(ii) By (3.3), (3.4), ... above, if the first  $r$  superdiagonals of  $A$  consist entirely of zeros, this also holds for  $A^{-1}$ , so use again Theorems 2.13 and 2.29.

(iii) If  $A \in IT_n(F)$  and  $a$  is an entry in  $A$  above the main diagonal, then it can equal an arbitrary element in  $F$ . So in this case there are  $p$  choices, and as there are  $n(n-1)/2$  such entries, the order of  $IT_n(F)$  is  $p^{n(n-1)/2}$ . Now use Theorem 3.15(iii) with  $q = p$ .

(iv) If the  $(r+1)$ st superdiagonal of  $IZT_{n,r}(F)$  (that is the first with non-zero elements) is  $a_{1,r+1}, a_{2,r+2}, \dots, a_{n-r,n}$ , then the  $(r+1)$ st superdiagonal of

$IZT_{n,r}(F)^{-1}$  is  $-a_{1,r+1}, \dots, -a_{n-r,n}$ . Use this to show by direct calculation that the  $(r+1)$ st superdiagonal of the commutator mentioned in the problem consists entirely of zeros.

**Problem 3.16** The conjugacy classes of  $A_5$  have orders 1 ( $e$ ), 12 (5-cycles, two classes), 15 (2-cycles  $\times$  2-cycles) and 20 (3-cycles). Including 1 the only divisors of 60 we can make using these integers are 1 and 60.

**Problem 3.17** Suppose  $T = \{a_1/b_1, \dots, a_k/b_k\}$  is a generating set for  $\mathbb{Q}$  (with addition). As this set is finite there exists a prime  $p$  which does not divide  $b_1, \dots, b_{k-1}$  or  $b_k$ , and it easily follows that  $1/p$  cannot be expressed as a sum of integer multiples of the elements of  $T$ .

**Problem 3.18** One representation is as follows. Map  $a \mapsto (1, 2, 3, 4)$  and  $b \mapsto (1, 4, 2)$ , then  $ab = (2, 3)$  and  $a^4 = b^3 = (ab)^2 = e$  and so the given group is a homomorphic image of  $S_4$  because we can construct all 2-cycles in  $S_4$  using  $(1, 2, 3, 4)$  and  $(1, 4, 2)$ . Now the given group is a copy of  $S_4$  as it only has 24 elements.

Using the relations  $a^4 = b^3 = e$ ,  $a^3 = bab$  and  $b^2 = aba$  we see that the elements are

$e$  (neutral element);  
 $ab, ba, b^2ab^2, ab^2a^2b, a^2ba^3, a^3ba^2$  (2-cycles);  
 $a^2, ba^2b^2, b^2a^2b$  (2-cycle by 2-cycles);  
 $b, b^2, a^2b, a^2b^2, ba^2, b^2a^2, aba, ab^2a$  (3-cycles); and  
 $a, a^3, ab^2, a^3b, ba^3, b^2a$  (4-cycles).

For the second part we have, for example, if  $a = (1, 2, 3, 4)$  and  $b = (1, 2)$  then  $ab = (2, 3, 4)$ , if  $a = (1, 2, 3)$  and  $b = (3, 4)$  then  $ab = (1, 2, 4, 3)$ , if  $a = (1, 2, 3)$  and  $b = (1, 3, 2, 4)$  then  $ab = (1, 4)$ , if  $a = (1, 2)$  and  $b = (2, 3, 4)$  then  $ab = (1, 3, 2, 4)$ , and if  $a = (1, 2)$  and  $b = (1, 4, 3, 2)$  then  $ab = (2, 4, 3)$ . Hence all six permutations of the powers are possible.

**Problem 3.19** (i) Let  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(p)$  and  $A^2 = I_2$ . Then

$$a^2 + bc = bc + d^2 = ad - bc = 1$$

and so  $a(a+d) = 2$ , that is  $a+d \neq 0$ . But also

$$b(a+d) = c(a+d) = 0,$$

hence  $b = c = 0$  and  $a^2 = d^2 = 1$ . Now also  $a = d$ , and the equation  $a^2 = 1$  has exactly two solutions  $a = 1$  and  $a = p-1$  (see Theorem B10) which give the scalar matrices in  $SL_2(p)$ . Note all equations are modulo  $p > 2$ .

(ii) Nine classes. We give a class representative followed in brackets by the order of elements in the class and the size of the class:  $I_2$  (1,1),  $\begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}$  (1,1),  $\begin{pmatrix} 0 & 1 \\ 4 & 4 \end{pmatrix}$  (3,20),  $\begin{pmatrix} 0 & 1 \\ 4 & 0 \end{pmatrix}$  (4,30),  $\begin{pmatrix} 0 & 1 \\ 4 & 2 \end{pmatrix}$  (5,12),  $\begin{pmatrix} 0 & 2 \\ 2 & 2 \end{pmatrix}$  (5,12),  $\begin{pmatrix} 0 & 1 \\ 4 & 1 \end{pmatrix}$  (6,20),  $\begin{pmatrix} 0 & 1 \\ 4 & 3 \end{pmatrix}$  (10,12), and  $\begin{pmatrix} 0 & 2 \\ 2 & 3 \end{pmatrix}$  (10,12). Note two classes of order 5 and two of order 10, each with twelve elements.

(iii) Use the same method as in the solution of Problem 3.16.

(iv) If  $A = \begin{pmatrix} 0 & 1 \\ 4 & 1 \end{pmatrix}$ ,  $B = \begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix}$ ,  $C = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$  and  $D = \begin{pmatrix} 0 & 1 \\ 4 & 0 \end{pmatrix}$ , then  $\langle A, B \rangle \simeq SL_2(3)$ ,  $\langle C, D \rangle \simeq Q_5$  and  $\langle B, D \rangle \simeq Q_3$ .

**Problem ♦ 3.20** (i) As  $c^2 = d^2 = e$ , the elements of  $D$  have the form

$$cdc \dots c = (cd)^{r_1}c, \quad cdc \dots d = (cd)^{r_2},$$

$$dcd \dots c = c^2dcd \dots c = c(cd)^{r_3}c \quad \text{or} \quad dcd \dots d = c^2dcd \dots c = c(cd)^{r_4}$$

for suitable choices of the  $r_i$ . The first and fourth are self-inverse, whilst the inverse of the second is  $c(cd)^{r_2}c$ , and the inverse of the third is  $(cd)^{r_3}$ . Hence  $D$  is generated by  $c$  and  $cd$ . Clearly  $A, K \leq D$ , and  $K \triangleleft D$  because  $c^{-1}(cd)^rc = (dc)^r = (cd)^{-r}$  et cetera. Also  $A \cap K = \langle e \rangle$  for if  $c = (cd)^r$ , then  $d(cd)^{r-1} = e$  which gives  $d = e$  and  $D = \langle c \rangle$ , a group of order 2.

(ii) Suppose  $o(cd) = n$ . If  $n = 1$  then  $D = \langle c \rangle \simeq C_2$ , if  $n = 2$  then  $D$  is Abelian and so is isomorphic to  $T_2$ , if  $3 \leq n < \infty$  then  $D$  is a new presentation of the dihedral group  $D_n$ , and if  $n$  is infinite we obtain a new infinite group  $D_\infty$  called the *infinite dihedral group*.

**Problem 3.21** (ia) Using  $\mathcal{P}_j, \mathcal{P}_k$  and  $\mathcal{Q}_{jk}$  we have  $e = a_j a_k a_j a_k$  and so  $a_j a_k = a_j^2 a_k a_j a_k^2 = a_k a_j$  for  $k < j - 1$ .

(ib) Also, using  $\mathcal{R}_l, \mathcal{P}_l$  and  $\mathcal{P}_{l+1}$ , we have  $a_l a_{l+1} a_l a_{l+1} a_l a_{l+1} = e$  and so  $a_{l+1} a_l a_{l+1} = a_l a_{l+1} a_l$ .

(ii) Consider  $Hy$ . If  $y = e$ , then  $Ha_i = H$  if  $i < n$  (by definition of  $H$ ), and  $Ha_n \in Z$ . Secondly consider  $(Ha_n \dots a_r)a_i$ , where  $1 \leq r \leq n$ , there are four cases.

(a)  $i < r - 1$ . By (ia)  $a_i$  commutes with  $a_j$  if  $j > i - 1$ , and so

$$(Ha_n \dots a_r)a_i = Ha_i a_n \dots a_r = Ha_n \dots a_r$$

as  $a_i \in H$ .

(b)  $i = r - 1$ . Here  $(Ha_n \dots a_r)a_{r-1} = Ha_n \dots a_{r-1}$ .

(c)  $i = r$ . By  $\mathcal{P}_r$  we have  $(Ha_n \dots a_r)a_r = Ha_n \dots a_{r+1}$ .

(d)  $i > r$ . By (ia) and (ib) and moving  $a_i$  to lie between  $a_{i-1}$  and  $a_{i-2}$ ,

$$\begin{aligned} (Ha_n \dots a_r)a_i &= Ha_n \dots a_{i+1}(a_i a_{i-1} a_i)a_{i-2} \dots a_r \\ &= Ha_n \dots a_{i+1}(a_{i-1} a_i a_{i-1})a_{i-2} \dots a_r = Ha_{i-1} a_n \dots a_r \\ &= Ha_n \dots a_r. \end{aligned}$$

Now count up to check that a permutation of  $Z$  has been constructed.

(iii) Using  $\mathcal{P}_i, \mathcal{Q}_{jk}$ , (ia) and (ib) it follows that every element of  $G$  belongs to one of the cosets in  $Z$ , and so  $[G : H] \leq n + 1$  as  $Z$  has  $n + 1$  elements. By the inductive hypothesis if we assume that  $o(H) \leq (n)!$ , it follows by Lagrange's Theorem (Theorem 2.27) that  $o(G) \leq (n + 1)!$ .

(iv) Finally let  $a_i \mapsto (i, i + 1)$ , for  $1 \leq i \leq n$ . By Problem 3.1, the set

of perms.  $\{a_1, \dots, a_n\}$  generates  $S_{n+1}$ . Now  $a_i^2 = e$  as  $a_i$  is a 2-cycle; if  $k < j-1$ ,  $(a_k a_j)^2 = (k, k+1)(j, j+1)(k, k+1)(j, j+1) = e$  as disjoint cycles commute; and if  $l < n$ ,  $(a_l a_{l+1})^3 = (l, l+1, l+2)^3 = e$ . This shows that  $G$  is a homomorphic image of  $S_{n+1}$ . But by (iii)  $o(G) \leq o(S_{n+1})$ , hence we have equality.

**Problem 3.22** (i) The matrices satisfy  $A^m = B^2 = (AB)^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ .

(ii) In  $Q_m$  we have  $o(a^r b) = 4$  for all  $r$ , so look at the powers of  $a$ .

(iii) Use the fact that the relations of  $D_m$  are  $a^m = b^2 = (ab)^2 = e$ .

**Problem 3.23** The non-neutral elements are  $a, b, c, aba = cbc, bab = cac, aca = bcb, abab = bcba = caca = (1, 2)(3, 4)(5, 6)(7, 8)$  (order 2), and  $ab, bc, ca, ba, cb, ac, abc = bca = cab = (1, 8, 2, 7)(3, 6, 4, 5)$ ,  $acb = (1, 7, 2, 8)(3, 5, 4, 6) = bac = cba$  (order 4), so  $o(F) = 16$ . There are 23 subgroups, 17 normal. The proper non-neutral subgroups are  $\langle abab \rangle = F' \simeq C_2$ ; six further subgroups isomorphic to  $C_2$  not normal  $\langle a \rangle, \dots$ ; four isomorphic to  $C_4$ ,  $\langle ab \rangle, \dots$  including  $\langle abc \rangle = Z(F)$ ; three isomorphic to  $C_2 \times C_2$ ,  $\langle a, abab \rangle, \dots$ ; three isomorphic to  $C_4 \times C_2$ ,  $\langle ab, c \rangle, \dots$ ; three isomorphic to  $D_4$ ,  $\langle ab, a \rangle, \dots$ ; and one isomorphic to  $Q_2$  consisting  $e, abab$  and the six elements of order 4. All are normal except those indicated. A presentation is as follows, it is not unique,

$$\langle a, b, c : a^2 = b^2 = c^2 = e, abc = bca = cab \rangle.$$

See Problem 8.12.

**Problem 3.24** The following matrices generate  $GL_2(3)$  and have orders 8, 2 and 3, respectively.

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Also in  $S_8$  we can set  $a \mapsto (1, 2, 3, 4, 5, 6, 7, 8)$ ,  $b \mapsto (2, 4)(3, 7)(6, 8)$  and  $c \mapsto (2, 7, 8)(3, 4, 6)$ . As noted in the statement of the problem, these solutions are in no way unique. For the presentation you need to show that each of its elements can be written in the form  $a^r b^s c^t$  for  $0 \leq r < 8, 0 \leq s < 2$ , and  $0 \leq t < 3$ , and if  $a^r b^s c^t = e$  then  $r = s = t = 0$ .



## Solutions 4

**Problem 4.1** (ia) We have  $a\theta = \cos a + i \sin a = e^{ia}$ , so  $(a+b)\theta = e^{i(a+b)} = e^{ia}e^{ib} = a\theta b\theta$ . (ib) Same as (ia), isomorphism as  $(\ln_2 a)\phi_2 = 2^{\ln_2 a} = a$ , for all  $a \in \mathbb{R}^+$ . (ic)  $(a+b)\phi_3 = -a-b = a\phi_3 + b\phi_3$ , an automorphism.

(ii) As  $a\phi = e$  for all  $a \in G$ ,  $(a+b)\phi = e = ee = a\phi b\phi$ .

(iii) Use Lemma 3.8.

(iv) This follows as  $\det(AB) = \det A \det B$  for  $A, B \in GL_2(F)$ .

(v) The map  $f: \mathbb{R}^2 \rightarrow \mathbb{R}$  given by  $f(x, y) = x$  satisfies  $f(x_1 + x_2, y_1 + y_2) = x_1 + x_2 = f(x_1, y_1) + f(x_2, y_2)$ .

**Problem 4.2** (i)  $GL_2(2) = \{I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, A_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, A_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, A_3 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, B_1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, B_2 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\}$  with matrix multiplication modulo 2. We have  $A_1^2 = A_2^2 = A_3^2 = B_1^3 = B_2^3 = I_2$ . Define  $\theta_1: GL_2(2) \rightarrow S_3$  by  $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\theta_1 = (1, 2, 3)$  and  $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\theta_1 = (1, 2)$ , and check by cases that  $(AB)\theta_1 = A\theta_1 B\theta_1$  for the map is clearly bijective.

(ii) We have  $F_1 = F \setminus \{1\}$  with operation  $a * b = a + b - ab$ . It is closed, for if  $a + b - ab = 1$  then  $(1-a)(1-b) = 0$  but  $1 \notin F_1$ ; the neutral element is 0; the inverse of  $a$  is  $a/(a-1)$ ; and it is associative because

$$\begin{aligned} (a + b - ab) + c - (a + b - ab)c &= a + b + c - ab - ac - bc + abc \\ &= a + (b + c - bc) - a(b + c - bc). \end{aligned}$$

Define  $\theta_2: F^* \rightarrow F_1$  by  $a\theta_2 = 1 - a$ . This is clearly bijective and  $(a * b)\theta_2 = 1 - (a + b - ab) = (1-a)(1-b) = a\theta_2 b\theta_2$ .

(iii) A polynomial  $f(x)$  has the form  $a_0 + a_1x + \dots + a_kx^k$  where  $a_i \in \mathbb{Z}$ , and an element  $m \in \mathbb{Q}^+$  has the prime factorisation  $p_0^{a_0}p_1^{a_1}\dots p_k^{a_k}$  again with  $a_i \in \mathbb{Z}$ , and where  $p_i$  is the  $i$ -th prime number with  $p_0 = 2$ . So we can define a map  $\theta_3$  from polynomials  $f(x)$  to rational numbers  $m$  by: The zero polynomial is mapped to 1, and  $(a_0 + a_1x + \dots + a_kx^k)\theta_3 = p_0^{a_0}p_1^{a_1}\dots p_k^{a_k}$ . If  $f_1(x) = a'_0 + \dots$ , then

$$\begin{aligned} (f(x) + f_1(x))\theta_3 &= ((a_0 + a'_0) + \dots)\theta_3 \\ &= p_0^{a_0+a'_0}\dots = p_0^{a_0}\dots p_0^{a'_0}\dots \\ &= f(x)\theta_3 f_1(x)\theta_3. \end{aligned}$$

**Problem 4.3** (i) If  $g, h \in G$ ,  $(g \circ h)(\phi\psi) = ((gh)\phi)\psi = (g\phi h\phi)\psi$  [ $\phi$  is a homomorphism]  $= (g\phi)\psi(h\phi)\psi$  [ $\psi$  is a homomorphism]  $= (g(\phi\psi))(h(\phi\psi))$ .

(ii) As  $e\phi = e$ ,  $e \in \text{im}(\phi)$ , and if  $a, b \in \text{im}(\phi)$  there exist  $a_1, b_1$  satisfying  $a_1\phi = a$  and  $b_1\phi = b$ . This gives  $a_1^{-1}\phi = a^{-1}$  and  $a^{-1}b = a_1^{-1}\phi b_1\phi = a_1^{-1}b_1\phi$ , that is  $a^{-1}b \in \text{im}(\phi)$ .

(iii) We have  $ab\phi = a\phi b\phi$  when  $a, b \in H$ , and so  $ab \in H$ , that is  $\phi'$  is well-defined, and it is a homomorphism because  $\phi$  is a homomorphism.

(iv) The map  $\phi$  is an isomorphism, and so it is a bijection, hence  $\phi^{-1}$  is also a bijection, see Appendix A. If  $a\phi = a_1$  and  $b\phi = b_1$  then  $a_1\phi^{-1} = a$ ,  $b_1\phi^{-1} = b$  and  $ab = a_1\phi^{-1}b_1\phi^{-1}$ . But  $ab\phi = a\phi b\phi = a_1b_1$  so  $ab = (a_1b_1)\phi^{-1}$ .

(v) Each element  $x \in X$  can be written in the form  $x = g\theta$  for some  $g \in G$ , and different  $g$  give rise to different  $x$ . Define an operation on  $X$  by: If  $x_1 = g_1\theta$  and  $x_2 = g_2\theta$ , then  $x_1x_2 = g_1\theta g_2\theta = g_1g_2\theta$ . This gives the set  $X$  a group structure, and the four basic axioms for this new group follow directly from those for  $G$ .

**Problem 4.4** (i) If  $C = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ,  $X = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$  and  $CX = XC$  for all matrices  $X$ , then  $b = c = 0$  and  $a = d = 1$  or  $2$ ; hence  $o(Z(G)) = 2$ .

(ii) A transversal (that is a list of coset representatives) is  $I_2$  and  $\{C_i\}$ , for  $i = 2, \dots, 12$ , where  $C_2 = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$ ,  $C_3 = \begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix}$ ,  $C_4 = \begin{pmatrix} 0 & 1 \\ 2 & 2 \end{pmatrix}$ ,  $C_5 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ ,  $C_6 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ ,  $C_7 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ ,  $C_8 = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$ ,  $C_9 = \begin{pmatrix} 1 & 1 \\ 2 & 0 \end{pmatrix}$ ,  $C_{10} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ ,  $C_{11} = \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix}$ , and  $C_{12} = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}$ .

(iii) If  $C_1 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$ , then  $C_2^2 = C_8^2 = C_{12}^2 = C_1$ ,  $C_4^3 = C_5^3 = C_6^3 = C_7^3 = C_{10}^3 = I_2$ , and  $C_3^3 = C_9^3 = C_{11}^3 = C_1$ . Three elements of order 2 and eight of order 3.

(iv) If  $C$  is the coset containing  $C_2$  and  $D$  contains  $C_5$ , then using coset product we have:  $C^3 = D^2 = (CD)^3 = I_2$  where  $CD$  is the coset containing  $C_9$ , now use Problem 3.10(b) and see Section 7.3.

**Problem ♦ 4.5** (i) If  $\phi$  is a homomorphism,  $g\phi = g^{-1}$  and  $h\phi = h^{-1}$ , then  $g^{-1}h^{-1} = g\phi h\phi = (gh)\phi = (gh)^{-1} = h^{-1}g^{-1}$ . This holds for all  $g, h \in G$ , so  $G$  is Abelian; now reverse argument.

(ii) Let  $X = \{a^{-1}(a\theta) : a \in G\}$ . Suppose  $a^{-1}(a\theta) = b^{-1}(b\theta)$ . This gives  $ba^{-1} = b\theta(a\theta)^{-1} = b\theta(a^{-1}\theta) = (ba^{-1})\theta$ , as  $\theta$  is a homomorphism. By conditions (a) and (b) this shows that  $ba^{-1} = e$ , that is  $a = b$ . Hence  $o(X) = o(G)$ , so  $X = G$ , as  $G$  is finite, and each element of  $G$  can be written in the form of the product  $a^{-1}(a\theta)$  for some  $a \in G$ .

Let  $g \in G$ , so by above there exists  $a \in G$  such that  $g = a^{-1}(a\theta)$ . Now  $g\theta = (a^{-1}(a\theta))\theta = (a^{-1})\theta a\theta^2 = (a^{-1}\theta)a$  (by hypothesis), and  $g^{-1} = (a^{-1}(a\theta))^{-1} = (a\theta)^{-1}(a^{-1})^{-1} = (a^{-1}\theta)a$  (as  $\theta$  is a homomorphism). Hence  $g\theta = g^{-1}$  for all  $g \in G$ , and so by (i)  $G$  is Abelian.

**Problem ♦ 4.6** (i) As  $G$  is Abelian, if  $a, b \in G$  then  $aHbH = abH = baH = bHaH$ . This also follows from the Third Isomorphism Theorem (Theorem 4.17).

(ii) See Problem 2.16.  $G/K$  exists as  $K \triangleleft G$ . If  $G/K$  is Abelian and  $a, b \in G$ , then  $abK = aKbK = bKaK = baK$  and  $[a, b] = a^{-1}b^{-1}ab \in K$ . This gives  $G' \leq K$ . Now reverse the argument for the converse using  $K \triangleleft G$ .

(iii) As  $S_n/A_n$  is Abelian,  $S'_n \subseteq A_n$  by (ii), and for the converse note that each 3-cycle can be written as a commutator:  $(i, j, k) = [(i, k), (i, k, j, l)]$ . A separate adhoc argument is needed when  $n < 4$ .

(iv) We have

$$J \triangleleft G \quad \text{and} \quad H_2 \triangleleft H_1. \quad (4.1)$$

For  $j, j' \in J$  and  $h, h' \in H_2$  we have  $(jh)^{-1}(j'h') = h^{-1}(j^{-1}j')h'$ , by (4.1) and there exists  $h'' \in H_2$  satisfying  $h^{-1}(j^{-1}j') = (j^{-1}j')h''$ . Now use Theorem 2.13. So  $JH_2 \leq JH_1 \leq G$ .

For normality we need to show that  $a = (jh_1)^{-1}j'h_2(jh_1) \in JH_2$  where  $h_1 \in H_1, h_2 \in H_2$  and  $j, j' \in J$ . By (4.1) if  $g \in G$  and  $j \in J$  we can find  $j_1 \in J$  to satisfy  $gj = j_1g$ , and so applying this twice, first with  $g = h_1^{-1}$ , then with  $g = h_1^{-1}h_2$ , we have

$$a = (h_1^{-1}j^{-1}j'h_2)jh_1 = j_1(h_1^{-1}h_2)jh_1 = j_1j_2h_1^{-1}h_2h_1,$$

for suitably chosen  $j_1$  and  $j_2$  in  $J$ . Hence  $JH_2 \triangleleft JH_1$  follows by (4.1). Now  $JH_1/JH_2 = JH_2H_1/JH_2$  [as  $H_2 \leq H_1$ ]  $= H_1/(H_1 \cap JH_2)$  [by the Second Isomorphism Theorem (Theorem 4.15)]  $= (H_1/H_2)/((H_1 \cap JH_2)/H_2)$ , by the Third Isomorphism Theorem (Theorem 4.17). Now use (i).

**Problem 4.7** (i) We have  $g^n K = (gK)^n = K$ , so  $g^n \in K$ .

(ii) Integers  $r$  and  $s$  exist satisfying  $rm + sn = 1$ , so  $g = g^{rm}g^{sn}$  but  $g^n \in K$  by (i) and  $g^m \in K$  by hypothesis, hence  $g \in K$ .

**Problem 4.8** (i) Use Problem 4.6(ii).

(ii) Use the definition.

**Problem ♦ 4.9** (i) For  $n > 0$  use induction as  $a^{n+1}\theta = a^n\theta a\theta$ , and for  $n < 0$  use Lemma 4.4.

(ii) First show  $\theta'$  is well-defined using: If  $aK = bK$  then  $a^{-1}b\theta = e$ , so  $a\theta = b\theta$ . The factor group  $G/K$  exists by definition, and  $(aKbK)\theta' = (abK)\theta' = ab\theta = a\theta b\theta = (aK)\theta'(bK)\theta'$ .

(iii) Use  $[j_1, j_2]\theta = (j_1^{-1}j_2^{-1}j_1j_2)\theta = [j_1\theta, j_2\theta]$  for  $j_1, j_2 \in J$ , and Lemma 4.3(ii).

**Problem 4.10** (i) Define  $\theta : G \rightarrow G$  by  $g\theta = g^n, g \in G$ , this is a homomorphism by given condition. The kernel is  $G_n = \{g \in G : g^n = e\} \triangleleft G$ , and the image is  $G^n = \{g^n : g \in G\} \leq G$ , see Lemma 4.3 and Theorem 4.2(ii). Also

$$g^{-1}a^ng = g^{-1}agg^{-1}ag \dots g^{-1}ag = (g^{-1}ag)^n$$

for all  $a, g \in G$ , so  $G^n \triangleleft G$ . By the First Isomorphism Theorem (Theorem 4.11), we have  $G/G_n \simeq G^n$ , hence  $o(G^n) = o(G/G_n) = [G : G_n]$  by Theorem 2.27.

(ii) If  $n = 2$  then  $abab = a^2b^2$ , or  $ba = ab$ . If  $n = 3$  then  $ababab = a^3b^3$ , and so  $(ba)^2 = a^2b^2$ . This gives

$$a^3b^2 = a(a^2b^2) = ababa = (ab)^2a = b^2a^3.$$

But  $o(a)$  is not divisible by 3, as  $3 \nmid o(G)$ , and so we can choose  $c \in G$  to satisfy  $c^2 = a^3$ . Now use first part as this applies for all  $a, b \in G$ .

**Problem ♦ 4.11** Suppose  $K, K_1 \triangleleft G$ ,  $o(K) (= o(K_1))$ , and  $K \neq K_1$ . So there is  $k \in K_1 \setminus K$ . Using the natural map  $G \rightarrow G/K$ , the Correspondence Theorem (Theorem 4.16) gives  $G/K \geq KK_1/K > \langle e \rangle$ . But the Second Isomorphism Theorem (Theorem 4.15) gives

$$KK_1/K \simeq K_1/(K \cap K_1), \quad \text{hence} \quad o(K_1/(K \cap K_1)) \mid [G : K].$$

If  $K \neq K_1$ , then  $o(K_1/(K \cap K_1))$  is a proper divisor of  $o(K_1) = o(K)$ , that is  $o(K)$  and  $[G : K]$  have a common factor larger than 1 contrary to assumption.

**Problem 4.12** For  $g, h \in G$ , using the coset and direct products we have

$$\begin{aligned} gh\theta &= (ghK_1, \dots, ghK_n) \\ &= (gK_1hK_1, \dots, gK_nhK_n) = (gK_1, \dots, gK_n)(hK_1, \dots, hK_n) \\ &= g\theta h\theta. \end{aligned}$$

The kernel is the set of  $g$  which satisfy  $gK_i = K_i$  for all  $i$ , that is  $g \in \bigcap_{i=1}^n K_i$ , and so the result follows by Corollary 4.12.

**Problem ♦ 4.13** (i) – Theorem 4.16(ii). We have  $H\theta \leq G_2$  by (i) of Theorem 4.16. As  $K \triangleleft G_1$ , if  $g \in G_1$  and  $k \in K$ , we have  $g^{-1}kg = k_1 \in K$  and  $g^{-1}kg\theta = (g\theta)^{-1}k\theta g\theta = k_1\theta$ . But  $\theta$  is surjective, so every element of  $G_2$  has the form  $g\theta$  for some  $g \in G_1$ , hence  $H\theta \triangleleft G_2$ .

Secondly, define a map  $\psi : G_1 \rightarrow G_1/H\theta$  by  $g\psi = (g\theta)H\theta$  for  $g \in G_1$ . The map  $\psi$  is surjective because  $\theta$  is surjective, and it is a homomorphism because

$$gh\psi = (gh\theta)H\theta = (g\theta)(h\theta)H\theta = (g\theta)H\theta(h\theta)H\theta = g\psi h\psi.$$

The kernel is  $H$ , for if  $h \in H$  then  $h\theta \in H\theta$ . Hence by the First Isomorphism Theorem (Theorem 4.11)

$$G_1/\ker \psi = G_1/H \simeq G_2/H\theta.$$

(i) – Theorem 4.16(iii). If  $a, b \in J\theta^{-1}$ , there exist  $x, y \in J$  satisfying  $x = a\theta$  and  $y = b\theta$ . Now  $J \leq G_2$  so  $x^{-1}y \in J$ ,  $(a\theta)^{-1}b\theta \in J$ ,  $(a^{-1}b)\theta \in J$ , and so finally  $a^{-1}b \in J\theta^{-1}$ . Hence  $J\theta^{-1} \leq G_1$  as  $e \in J\theta^{-1}$ . Clearly  $K \subseteq J\theta^{-1}$  therefore  $K \leq J\theta^{-1}$  by Corollary 2.14.

(ii) Let  $\theta$  be the natural homomorphism  $G \rightarrow G/K$ , it is surjective with kernel  $K$ ; so the Correspondence Theorem applies. Now  $G/K$  is simple, so  $G$  has no normal non-neutral subgroup  $J$  satisfying  $K < J < G$ . Conversely, if no such  $J$  exists, then  $G/K$  has no non-neutral proper normal subgroup.

(iii) By (ii)  $G/H$  is simple. Suppose it is not cyclic of prime order, so there exists  $J/H$  such that  $\langle e \rangle < J/H < G/H$ , and by the Correspondence Theorem  $H < J < G$  which is impossible as  $H$  is maximal. For the required example let  $G = S_5$  and  $H = \langle (1, 2, 3, 4, 5), (2, 3, 5, 4) \rangle$ ; see Problem 3.11. Now  $H$  is maximal (use a computer check, or see Problem 3.9) and  $[G : H] = 6$ , but  $H$  is not normal; for example  $(1, 2)(1, 2, 3, 4, 5)(1, 2) = (1, 3, 4, 5, 2) \notin H$ , and also 6 is not prime!

(iv) If homomorphism  $\xi$  exists with  $\phi = \theta \circ \xi$ , then  $K\phi = e$  and so  $K \subseteq \ker \phi$ . Conversely  $\xi$  is well-defined by Lemma 2.22, and it is a homomorphism (use coset product and the fact that  $\phi$  is a homomorphism). This gives  $\ker \xi = G/K$ . Now using the First Homomorphism Theorem we have

$$G/\ker \phi = G\phi \simeq (G/K)\xi \simeq (G/K)/(\ker \phi/K).$$

**Problem 4.14** (i) The map  $\xi$  is well-defined, for if  $aJ = bJ$  then  $a \in bJ \subseteq bK$ , and so  $aK = bK$  by Lemma 2.22. Now  $\xi$  is surjective by definition, and it is a homomorphism because

$$(aJbJ)\xi = (abJ)\xi = abK = aKbK = (aJ\xi)(bJ\xi)$$

using coset product. Also  $\ker \xi = \{aJ : (aJ)\xi = aK = K\}$ , that is  $aJ \in \ker \xi$  if, and only if,  $a \in K$ . Hence as  $J \subseteq K$  we have  $\ker \xi = K/J$ .

(ii) Use (i) and the First Isomorphism Theorem (Theorem 4.11).

**Problem 4.15** (i)  $o(G) = pn$ . If  $n = 1$  the result follows by Lagrange's Theorem (Theorem 2.27), so suppose it holds for Abelian groups of order  $pm$  where  $m < n$ . Let  $a \in G$  with  $o(a) = t$ . If  $p \mid t$ , then  $o(a^{t/p}) = p$ , so we may suppose  $p \nmid t$ .

Now  $\langle a \rangle \triangleleft G$  and  $G/\langle a \rangle$  is an Abelian group of order  $pn/t$ . As  $p \nmid t$ , we have  $t \mid n$ , so  $n = tn_1$  for some integer  $n_1 < n$ , and  $o(G/\langle a \rangle) = pn_1$ . By the inductive hypothesis  $G/\langle a \rangle$  contains an element  $c$  of order  $p$ . This shows, using the Correspondence Theorem, that  $G$  contains an element  $b$  whose order is a multiple of  $p$ . Now apply the first case again.

(ii) If  $H = \langle a \rangle$  and  $J = \langle b \rangle$ , we have  $o(ab) = mn$  and so  $G \simeq \langle ab \rangle$ .

(iii) Example. Let  $G = D_3 = \langle a, b \mid a^3 = b^2 = (ab)^2 = e \rangle$ ,  $H = \langle a \rangle$  and  $J = \langle b \rangle$ . The subgroups  $H$  and  $J$  are prime order cyclic, and  $G$  is not cyclic. But of course  $J$  is not normal.

**Problem ♦ 4.16** (i) Example. Let  $G = S_5$ ,  $H \simeq S_3$  defined on the set  $\{1, 2, 3\}$  and  $J$  be the group generated by  $H$  and the 2-cycle  $(4, 5)$ , so  $J \simeq S_3 \times C_2$  see Chapter 7. Here  $Z(H) = Z(G) = \langle e \rangle$  but  $Z(J) = \langle (4, 5) \rangle \simeq C_2$ ; see Problem 7.4(i).

(ii) Suppose  $G/Z(G)$  is cyclic, so left cosets have the form  $a^t Z(G)$  for  $t \in \mathbb{Z}$  and some fixed  $a \in G$ . Hence every element  $g \in G$  has the form  $g = a^t c$  for some  $t \in \mathbb{Z}$  and  $c \in Z(G)$ . Now if  $g_i = a^{t_i} c_i$ ,  $i = 1, 2$ , then

$$g_1 g_2 = a^{t_1} c_1 a^{t_2} c_2 = a^{t_2+t_1} c_2 c_1 \text{ [as } c_1 \in Z(G)] = a^{t_2} c_2 a^{t_1} c_1 = g_2 g_1,$$

as  $c_2 \in Z(G)$ . This shows that  $G$  is Abelian, now take the contra-positive.

(iii) Suppose  $K = \{e, k\}$  with  $k^2 = e$ . If  $g \in G$  then by normality  $g^{-1}kg \in K$ , so  $g^{-1}kg = e$  or  $k$ . If the former,  $k = e$ , and if the latter,  $kg = gk$  for all  $g \in G$ ; hence  $K \leq Z(G)$ .

(iv) This is another extension of the Correspondence Theorem (Theorem 4.16). We have  $J = G\theta$  and  $hg = gh$  for all  $g \in G$  and  $h \in H$ , hence  $h\theta g\theta = g\theta h\theta$ ; that is  $H\theta \leq Z(G\theta)$ .

(v)  $HZ(G) \leq G$  by Lemma 4.14, and if  $h_i \in H$  and  $z_i \in Z(G)$ , then  $h_1 z_1 h_2 z_2 = h_1 (h_2 z_2) z_1$  [as  $z_1 \in Z(G)$ ]  $= h_2 h_1 z_2 z_1$  [as  $H$  is Abelian]  $= h_2 z_2 h_1 z_1$  [as  $z_2 \in Z(G)$ ].

(vi) Use Problem 4.22. Second part: No – For example, let  $G = S_3$  and  $K = \langle (1, 2, 3) \rangle \simeq C_3$ .  $K \triangleleft G$  (as the index is 2) and  $Z(K) = K$  (as  $K$  is Abelian), but  $Z(G) = \langle e \rangle$ , see Problem 2.26(iv).

(vii) We have  $[J, G] \leq K$  gives  $j^{-1}g^{-1}jg \in K$  for  $j \in J$  and  $g \in G$ , or  $jg = gjk$  for  $g \in G, j \in J$  and some  $k \in K$ . Hence  $jKgK = jgK = gjkK = gKjK$ , that is  $J/K \leq Z(G/K)$ . Now reverse argument.

(viii) Using the Second Isomorphism Theorem (Theorem 4.15) we obtain  $Z(G)/(Z(G) \cap K) \simeq Z(G)K/K$ . Further  $Z(G)K/K \subseteq Z(G/K)$  if and only if  $zkKz'k'K = z'k'KzkK$ , or  $zkz'k'K = z'k'zkK$ , for all  $z, z' \in Z(G)$  and  $k, k' \in K$ . But both  $z$  and  $z'$  commute with all elements of  $G$ , and  $kk'K = k'kK$  for all  $k, k' \in K$ .

**Problem 4.17** If  $x = \sum_{g \in G} m_g g$  and  $y = \sum_{g \in G} n_g g$ , then  $x + y = \sum_{g \in G} (m_g + n_g)g$  and  $rx = \sum_{g \in G} r m_g g$  for  $m_g, n_g, r \in F$ . Also  $(x + y)\theta_h = x\theta_h + y\theta_h$ ,  $(rx)\theta_h = r(x\theta_h)$ ,  $\theta_{hj} = \theta_h\theta_j$  and  $\theta_e$  is the identity map on  $U$ . Now if  $h \in \ker \theta$ , then  $x\theta = x$  for all  $x \in U$ , so  $gh = g$  giving  $h = e$ .

**Problem ♦ 4.18** (i) Check the vector space axioms. The new addition  $+$  forms an Abelian group (as  $G$  is Abelian),  $\mathcal{G}$  is closed under the new scalar multiplication, the vector space zero is  $e$  (as  $x^1 = x$ ), and  $(x^a)^b = x^{ab}$ ,  $c(x + y) = (xy)^c = x^c y^c = cx + cy$  and  $(c + d)x = x^{c+d} = x^c x^d = cx + cy$ .

(ii) The rules for subgroups exactly follow those for vector subspaces.

(iii) An endomorphism  $\theta$  of  $G$  corresponds to a linear map in  $\mathcal{G}$  and vice versa. For in  $G$  we have  $x\theta y\theta = xy\theta$ , and so in  $\mathcal{G}$  we have  $(x + y)\theta = x\theta + y\theta$  and  $(cx)\theta = (x^c)\theta = (x\theta)^c = c(x\theta)$ . This argument reverses. A linear map can be represented by a non-singular matrix, that is by a member of  $GL_m(p)$ , and a non-singular linear map is an automorphism of  $\mathcal{G}$ .

**Problem 4.19** (ia)  $\mathbb{Z}$  is cyclic. An automorphism maps generators to generators, and so as this group has only two generators, 1 and  $-1$ , there can only be two automorphisms; the first is the identity map and the second maps  $1 \mapsto -1$  and so maps  $n \mapsto -n$  for all  $n \in \mathbb{Z}$ . Hence  $\text{Aut}(\mathbb{Z}) \simeq C_2$ .

(ib)  $\text{Aut } T_2 \simeq S_3$ . If  $L = T_2 \setminus \{e\}$  then as  $o(L) = 3$  all permutations of  $L$  are automorphisms  $\phi$  of  $T_2$  provided we set  $e\phi = e$  because all elements of  $L$  have order 2. See problem 4.18(iii).

(ic)  $\text{Aut } S_3 \simeq S_3$ . As in (ib) all permutations of the elements of order 2 in  $S_3$  generate automorphisms as the elements of order 3 can be expressed as products of elements of order 2.

(id)  $\text{Aut } C_4 \simeq C_2$ . There is only one element of order 2, so all automorphisms map this element to itself. Hence there are two automorphisms, the first is the identity map, and the second interchanges the two elements of order 4.

(ie) By Theorems 4.23 and B16,  $\text{Aut}(C_{p^n}) \simeq C_{p^{n-1}(p-1)}$ .

(ii) No. Suppose  $D_8 = \langle a, b \mid a^8 = b^2 = e, bab = a^7 \rangle$ , then as in the example on page 83 there is an automorphism  $\phi : a \mapsto a, b \mapsto ab$  which satisfies  $\phi^8 = \iota$ . But for this group there are four elements of order 8, that is  $a, a^3, a^5$  and  $a^7$ , and so there are four automorphisms

$$\psi_i : a \mapsto a^{2^{i+1}}, b \mapsto b \quad \text{for } i = 0, 1, 2, 3.$$

Hence using the methods in the example quoted above, there are 32 automorphisms and the automorphism group is isomorphic to an extension of  $D_8$  by  $C_2$ ; the copy of  $D_8$  is obtained if we only consider the automorphisms  $\psi_0, \psi_2$  and  $\phi$  and their powers and products.

(iii) If  $o(G) = 1$  or  $2$ , the only automorphism is the identity map as automorphisms map  $e$  to  $e$ . Conversely suppose  $\text{Aut } G = \langle e \rangle$ . So consequently all inner automorphisms equal the identity map, that is  $a^{-1}ga = g$  for all  $a, g \in G$ , and hence  $G$  is Abelian. Now the map  $\psi$  defined by  $a\psi = a^{-1}$  is an automorphism (for  $(ab)\psi = b^{-1}a^{-1} = a^{-1}b^{-1} = a\psi b\psi$ ), and so all elements of  $G$  have order at most 2, that is  $G$  is an elementary Abelian 2-group, see Problem 4.18 above. But by (iii) in this problem if  $G$  has order larger than 2, then there exists a non-identity automorphism (that is a non-singular linear map) which is a contradiction.

**Problem 4.20** (i) Use Problem 3.1 and check that  $(1, j)\psi^2 = (1, j)$  for  $j = 2, \dots, 6$ . Begin with

$$\begin{aligned} (1, 2)\psi^2 &= (1, 5)(2, 3)(4, 6)\psi \\ &= (1, 5)\psi(1, 2)\psi(1, 3)\psi(1, 2)\psi(1, 4)\psi(1, 6)\psi(1, 4)\psi \\ &= (1, 2)(3, 6)(4, 5) \dots (1, 3)(2, 4)(5, 6) = (1, 2). \end{aligned}$$

(ii) The symmetric group  $S_6$  has six subgroups isomorphic to  $S_5$ , each of which contains the set of permutations that fix a particular element of the set  $\{1, 2, 3, 4, 5, 6\}$ . This is typical of all symmetric groups. But because of the facts given in (i)  $S_6$  has a further set of six subgroups isomorphic to  $S_5$  obtained by looking at collections of products of four 2-cycles. For instance the elements

$$(1, 4)(2, 6)(3, 5), (1, 2)(3, 4)(5, 6), (1, 4)(2, 5)(3, 6) \quad \text{and} \quad (1, 5)(2, 6)(3, 4)$$

generate a copy of  $S_5$ . To see this we note that these four elements in  $S_6$  satisfy the relations in the presentation of  $S_6$  given in Problem 3.21 with  $n = 4$ . For example if we label these four permutations  $a, b, c, d$  respectively, then  $ab, bc, cd$  have order 3, and  $ac, ad, bd$  have order 2. The remaining five subgroups can be obtained by permuting the entries 4, 5 and 6. Note that each subgroup contains ten of the fifteen products of three 2-cycles, but four are sufficient to generate the subgroup. Two notable facts about these new subgroups are: They contain no 2-cycles, and unlike the first set of six subgroups they are transitive on the six-element set  $\{1, 2, 3, 4, 5, 6\}$ .

**Problem 4.21** Conjugations by even elements define inner automorphisms in  $A_5$ , but by Theorem 3.3, conjugation by odd elements (that is members

of  $S_5 \setminus A_5$ ) also define automorphisms of  $A_5$ . This can be extended to show that the automorphism group of  $A_5$  is isomorphic to  $S_5$ . And in fact this also applies if '5' is replaced by an integer larger than 6.

**Problem ♦ 4.22** (i) If  $\phi$  is an automorphism, so is  $\phi^{-1}$ , that is  $H\phi^{-1} \subseteq H$  as  $H$  is characteristic. So  $H = (H\phi^{-1})\phi \subseteq H\phi$ , but  $H\phi \subseteq H$  and equality follows.

(ii) If  $H \triangleleft G$ , then  $g^{-1}Hg \subseteq H$  for all  $g \in G$ , but if  $\nu$  is an inner automorphism then for some  $g \in G$  we have  $h\nu = g^{-1}hg$ , that is  $H\nu \subseteq H$ ; this argument reverses.

(iii) If  $K \text{ char } G$  and  $\phi$  is an automorphism of  $G$ , then  $K\phi = K$  by (i). Hence if we restrict the domain of  $\phi$  to  $K$ , the resulting map  $\phi|_K$  is an automorphism of  $K$ . But  $H \text{ char } K$  and so  $H\phi = H(\phi|_K) = H$ , that is we have  $H \text{ char } G$ .

(iv) If  $a \in G$  and  $\psi$  is the inner automorphism given by  $g\psi = a^{-1}ga$ , then as  $K \triangleleft G$  we have  $\psi|_K$  is an automorphism of  $K$ . But  $J \text{ char } K$ , and so  $J\psi|_K \leq J$ ; that is, if  $j \in J$  then  $a^{-1}ja = j\psi \in J$ . For a counter example to the last part let  $G = A_4, H = V = \langle (1,2)(3,4), (1,3)(2,4) \rangle$  (with order 4), and  $J = \langle (1,2)(3,4) \rangle$  (with order 2). We have  $H \text{ char } G$  as  $H$  contains all of the elements of order 2 and automorphisms map elements of order 2 to elements of order 2, and  $J \triangleleft H$  as the index is 2, but  $J$  is not a normal subgroup of  $G$ .

(v) If  $G = \langle a \rangle$ ,  $o(a) = n$  and  $\phi$  is an automorphism, then  $a\phi = a^m$  for some  $m$  satisfying  $(m, n) = 1$ ; see the proof of Theorem 4.23. Also if  $H \leq G$ , then  $H = \langle a^t \rangle$  for some  $t | n$  by Theorem 4.20. Hence  $(t, m) = 1$ , and so  $\phi$  maps  $H$  to itself, that is  $H$  is a characteristic subgroup of  $G$ .

(vi) Let  $\phi$  be an automorphism of  $G$  and  $a \in Z(G)$ , then for all  $g \in G$  we have  $a\phi g\phi = g\phi a\phi$ . If we set  $h = g\phi^{-1}$  (note  $\phi^{-1}$  is also an automorphism), then this equation gives  $a\phi h = ha\phi$  for all  $h \in G$ , that is  $Z(G)\phi \subseteq Z(G)$ .

(vii) We have, for  $a, b \in G$ ,

$$[a, b]\phi = (a^{-1}b^{-1}ab)\phi = (a\phi)^{-1}(b\phi)^{-1}(a\phi)(b\phi) = [a\phi, b\phi] \in G'.$$

Therefore  $G'\phi \subseteq G'$ .

(viii) Let  $G = \langle a, b : a^2 = b^2 = e, ab = ba \rangle$  be the 4-group  $T_2$ , and let the automorphism  $\phi$  be given by  $e\phi = e, a\phi = b, b\phi = a$  and  $ab\phi = ab$ . Now  $\langle a \rangle \triangleleft G$ , but it is not characteristic because  $\langle a \rangle\phi = \langle b \rangle \not\subseteq \langle a \rangle$ .



## Solutions 5

**Problem 5.1** (i) Two orbits:  $\{1, 2, 3\}, \{4\}$ ;  $\text{stab}(x) = \langle e \rangle$  if  $x = 1, 2, 3$ , and is  $G$  if  $x = 4$ .

(ii) and (iii) One orbit, and all stabilisers equal  $\langle e \rangle$ .

(iv) Two orbits:  $\{1, 2\}, \{3, 4\}$ ;  $\text{stab}(1) = \text{stab}(2) = \{e, (3, 4)\}$  and  $\text{stab}(3) = \text{stab}(4) = \{e, (1, 2)\}$ .

(v) One orbit. Given  $x$  and  $y$  there is an even permutation mapping  $x$  to  $y$ ;  $\text{stab}(j)$  equals set of elements of  $A_4$  which fix  $j$ . For instance  $\text{stab}(1) = \{e, (2, 3, 4), (2, 4, 3)\} \simeq A_3 \simeq C_3$ .

(vi) If  $v \in V$ , orbit of  $v$  is  $\{w : w = v \setminus a \text{ for } a \in F^*\} = \{va : a \in F^*\}$ . Also  $\text{stab}(v) = \{1\}$  if  $v \neq 0$ , and  $\text{stab}(v) = F^*$  if  $v = 0$ .

(vii) Note first  $f(x_1, \dots, x_n) \setminus \sigma = f(x_{1\sigma}, \dots, x_{n\sigma})$  is a polynomial in  $x_1, \dots, x_n$ ; so  $\sigma$  maps  $\mathbb{Q}[x_1, \dots, x_n]$  into itself. If  $\iota$  is the identity permutation then  $f \setminus \iota = f$ , and for  $\sigma, \tau \in S_n$  using associativity of composition we have

$$\begin{aligned} f(x_1, \dots, x_n) \setminus \sigma\tau &= f(x_{1(\sigma\tau)}, \dots, x_{n(\sigma\tau)}) \\ &= f(x_{(1\sigma)\tau}, \dots, x_{(n\sigma)\tau}) \\ &= f(x_{1\sigma}, \dots, x_{n\sigma}) \setminus \tau \\ &= (f(x_1, \dots, x_n) \setminus \sigma) \setminus \tau; \end{aligned}$$

this gives an action. Hence the orbit of  $f$  is the set of all polynomials obtained by replacing some of the variables with others. For example, if  $f = x_1 + c$  then the orbit of  $f$  is the set  $\{x_i + c : i = 1, \dots, n\}$ , and if  $f = x_1^2 + \dots + x_n^2$  then the orbit of  $f$  is  $f$  itself. The stabiliser of  $f$  is the subgroup of all elements  $\sigma$  of  $S_n$  such that  $f \setminus \sigma = f$ ; for example, the stabiliser of  $x_1 + c$  is  $\langle e \rangle$ , and the stabiliser of  $x_1^2 + \dots + x_n^2$  is  $S_n$ .

By the Orbit-stabiliser Theorem (Theorem 5.7) we have  $o(\mathcal{O}_f) = [S_n : \text{stab}(f)]$ , also  $o(S_n) = n!$ , hence  $o(\mathcal{O}_f)$  is a divisor of  $n!$  by Lagrange's Theorem (Theorem 2.27).

**Problem 5.2** Suppose  $o(G) = p^r q^s$ ,  $o(H) = p^t q^u$ ,  $o(J) = p^v q^w$ , where  $t, v \leq r$  and  $u, w \leq s$ . The hypothesis implies either (a)  $t = r$  and  $w = s$ , or (b)  $v = r$  and  $u = s$ . Suppose (a), the proof is the same for (b) and can be extended if more primes are involved. Now  $H \cap J \leq H$ , so  $o(H \cap J) \mid p^t q^u$ , and  $H \cap J \leq J$ , so  $o(H \cap J) \mid p^v q^w$ . Hence

$$o(H \cap J) \mid p^v q^u \quad \text{which gives} \quad o(H \cap J) \leq p^v q^u.$$

By hypothesis and Theorem 5.8 we have

$$o(HJ)o(H \cap J) = o(H)o(J) = p^{t+v} q^{u+w} = o(G)p^v q^u.$$

Combining these statements shows that  $o(HJ) \geq o(G)$ , therefore  $HJ = G$ . For the second part use Theorem 5.8 again. See also Problem 2.18.

♦ **Problem 5.3** (i) Suppose the orbits are  $X_1, \dots, X_k$ . Now  $o(G) = p^t$ , and the Orbit-stabiliser Theorem (Theorem 5.8) gives  $o(X_i) \mid o(G)$ , hence for each  $i$ , we have  $o(X_i) = p^{u_i}$  for some  $u_i = 0, 1, 2, \dots$ . If  $o(X_i) = 1$  for  $i = 1, \dots, r$ , and  $o(X_i) = p^{s_i} > 1$  for  $i = r+1, \dots, k$  relabelling if necessary, then as  $o(X) = o(X_1) + \dots + o(X_k)$ , we have  $o(X) = r + p^{s_1} + \dots$ . The result follows as  $r = o(\text{fix}(G, X))$ .

(ii) By Lemma 5.21,  $Z(G) \neq \langle e \rangle$ . Also as  $J$  is a disjoint union of its conjugacy classes (it is normal)  $\mathcal{C}_1 = \{e\}, \mathcal{C}_2, \dots$ . If  $J \cap Z(G) = \langle e \rangle$ , then  $o(\mathcal{C}_i) > 1$  for  $i = 2, 3, \dots$ , this follows from the Class Equation (Theorem 5.20). Therefore  $o(J) = 1 + o(\mathcal{C}_2) + \dots \equiv 1 \pmod{p}$  which is impossible as  $p \mid o(J)$  by hypothesis.

**Problem 5.4** (i) Use:  $g \in \text{stab}_G(x \setminus h)$  iff  $(x \setminus h) \setminus g = x \setminus h$  iff  $x \setminus hgh^{-1} = x$  iff  $hgh^{-1} \in \text{stab}_G(x)$  iff  $g \in h^{-1} \text{stab}_G(x) h$ ; and apply Problem 2.23(ii). Or we can argue as follows: If  $y \in \mathcal{O}\{x\}$  then  $\mathcal{O}\{y\} = \mathcal{O}\{x\}$ , and therefore by Theorem 5.7  $[G : \text{stab}(x)] = [G : \text{stab}(y)]$  which gives the result.

(ii) The sum  $\sum(o(\text{fix}(g, X)))$  counts each  $x \in X$  a total of  $\text{stab}_G(x)$  times by definition of the stabiliser. Also if  $y \in \mathcal{O}\{x\}$ , we have by (i)  $o(\text{stab}_G(x)) = o(\text{stab}_G(y))$ . Now use Theorem 5.7 to show that each orbit contributes  $o(G)$  to the sum, and so counts the number of orbits. This is sometimes called ‘Burnside’s Counting Lemma’.

(iii) By transitivity  $m = 1$ , also  $o(\text{fix}(e, X)) = o(X) > 1$ , so  $o(\text{fix}(g, X))$  cannot be positive for all  $g \in G$ .

**Problem 5.5** (i) If  $o(G) = n$ , then the two given conjugacy classes have order 1 (for the class  $\{e\}$ ) and  $n-1$  (for the rest), and both of these integers divide  $n$  by Theorem 5.19.

(ii) Suppose  $G$  is simple and  $[G : H] = 2, 3$  or  $4$ , then by Theorem 5.15  $\text{core}(H) = \langle e \rangle$ , and  $G$  is isomorphic to a (transitive) subgroup of  $S_2, S_3$  or  $S_4$ , respectively.

(iii) Fix  $a \in G$ . The set of  $b$  such that  $ab = ba$  is the centraliser  $C_G(a)$ , and we have  $o(C_G(a)) = o(G)/o(\mathcal{C}\ell\{a\})$ . If  $c \in \mathcal{C}\ell\{a\}$  then  $\mathcal{C}\ell\{c\} = \mathcal{C}\ell\{a\}$ , and so  $o(C_G(c)) = o(C_G(a))$ . Hence the number of pairs  $\{a, b\}$  with  $ab = ba$  as  $a$  ranges over its conjugacy class is  $o(\mathcal{C}\ell\{a\}) \cdot o(C_G(a)) = o(G)$ . We can now sum over the  $h(G)$  conjugacy classes of  $G$ .

**Problem ♦ 5.6** Use Theorem 5.15 and Problem 2.24 to show that  $K = \text{core}(K)$ ; note that  $o(G)$  has no prime factor smaller than  $p_0$ .

**Problem 5.7** (i) Use: If  $h = a^{-1}ga$  then  $h^{-1} = a^{-1}g^{-1}a$ .

(ii) If  $D_4 = \langle a, b : a^4 = b^2 = e, bab = a^3 \rangle$ , the conjugacy classes are  $\{e\}, \{a^2\}, \{a, a^3\}, \{b, a^2b\}$  and  $\{ab, a^3b\}$ ; all self-inverse. The conjugacy classes for  $A_4$  are  $\{e\}, \{(1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}, \{(1, 2, 3), (1, 4, 2), (1, 3, 4), (2, 4, 3)\}$  and  $\{(1, 3, 2), (1, 2, 4), (1, 4, 3), (2, 3, 4)\}$ . The first two are self-inverse, the inverse of third is the fourth and vice versa. For  $SL_2(3)$ , see Section 8.2. In the table on page 172 (here rows correspond to conjugacy classes) the first, second and fifth rows give self-inverse classes, the inverse of row three is row four, and the inverse of row six is row seven.

**Problem 5.8** (i) Use Theorem 2.13. If  $gx = xg$ , for  $x \in X$  and  $g \in C_G(x)$ , then  $xg^{-1} = g^{-1}x$  *et cetera*.

(ii) Use Definition 2.32.

(iii) If  $h \in H$ , then  $C_G(H) \subseteq C_G(h)$  by definition, now use the fact that this holds for all  $h \in H$ .

(iv) We have  $H \leq C_G(J)$ , so  $hj = jh$  for all  $h \in H$  and  $j \in J$ . As  $H \leq J$  this shows that  $j \in Z(H)$  for all  $j \in J$ ; the result follows.

(v) For first part use the definition and for second part we have  $a \in g^{-1}C_G(H)g$ , iff  $gag^{-1} \in C_G(H)$ , iff  $gag^{-1}$  commutes with  $h$  for all  $h \in H$ , iff  $gag^{-1}h = h g a g^{-1}$  for all  $h \in H$ , iff  $ag^{-1}hg = g^{-1}hga$  for all  $h \in H$ , and so iff  $a \in C_G(g^{-1}Hg)$ .

(vi)  $g \in C_G(H)$  iff  $ghg^{-1} = h$  for all  $h \in H$ , and  $g \in N_G(H)$  iff  $ghg^{-1} \in H$  for all  $h \in H$ .

(vii) If  $C_G(H) = \langle e \rangle$ , there is  $h \in H$  such that  $ah \neq ha$  for all  $a \in G \setminus \langle e \rangle$  which implies  $Z(J) = \langle e \rangle$  for all  $J$  in the given range. If  $C_G(H) \neq \langle e \rangle$ , there exists  $b \in G$  satisfying  $b \neq e$  and  $bh = hb$  for all  $h \in H$ . This shows that  $\langle b \rangle H \leq G$  and  $b \in Z(\langle b \rangle H)$ , impossible by hypothesis.

**Problem 5.9** (i) If  $D_6 = \langle a, b \mid a^6 = b^2 = (ab)^2 = e \rangle$ , then  $C(e) = C(a^3) = D_6$ ,  $C(a^t) = \langle a \rangle$  if  $3 \nmid t$ , and  $C(ba^t) = \langle ba^t, a^3 \rangle$ , so the centraliser of each element of order 2 has order 4.

For  $S_4$  see Problem 5.26. Similarly for (ii).

(iii) We have  $A_5$  is the disjoint union of five conjugacy classes, they are  $\{e\}$ , twenty 3-cycles, twelve 5-cycles, twelve 5-cycles, and fifteen 2-cycles  $\times$  2-cycles; see Problem 3.3. So the numerical Class Equation (Theorem 5.20(ii)) for  $A_5$  gives

$$60 = 1 + 20 + 12 + 12 + 15.$$

The centralisers of the 3- and 5-cycles are the cyclic groups they generate (of orders 3 and 5, respectively), and

$$C_{A_5}((1, 2)(3, 4)) = \{e, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}.$$

**Problem 5.10** Note that a permutation on the set  $\{m+1, \dots, n\}$  commutes with  $\tau$ , also any power of  $\tau$  commutes with  $\tau$ . Now check that there is nothing else in  $C_{S_n}(\tau)$ .

**Problem 5.11** (i) As  $Z(G) \triangleleft G$ , we have  $\langle a \rangle Z(G) \leq G$  if  $a \in G$  (Lemma 4.14(ii)), and if  $h \in Z(G)$  then  $ah = ha$ . Now note that  $a \notin Z(G)$ .

(ii) As  $H$  is Abelian,  $H \leq C_G(H)$ . Use (i) to show that if  $a \in C_G(H) \setminus H$  then  $H$  is not maximal Abelian.

**Problem 5.12** (i) Use definition.

(ii) If  $a \in C_G(C_G(A))$  then  $ay = ya$  for all  $y \in C_G(A)$ , that is for all  $y$  such that  $yc = cy$  for all  $c \in A$ . This is true for all  $a \in A$ .

(iii) By (i) and (ii) we have  $C_G(A) \supseteq C_G(C_G(C_G(A)))$ , and for the reverse inclusion substitute  $C_G(A)$  for  $A$  in (ii).

**Problem ♦ 5.13** (i) Suppose  $H \triangleleft K$  and  $N_G(H) < K$ . There exists  $k \in K \setminus N_G(H)$ , and for  $h \in H$ ,  $k^{-1}hk \in H$ . But  $k \notin N_G(H) = \{g \in G : g^{-1}Hg = H\}$  which is a contradiction.

(ii) We have, where  $h, h' \in H$ ,

$$\begin{aligned} g^{-1}N_G(H)g &= \{x : x = g^{-1}ag \text{ and for all } h \text{ there exists } h' \text{ with } a^{-1}ha = h'\} \\ &= \{x : x = g^{-1}ag \text{ and for all } h \text{ there exists } h' \\ &\quad \text{with } gg^{-1}a^{-1}gg^{-1}hgg^{-1}agg^{-1} = h'\} \\ &= \{x : \text{for all } h \text{ there exists } h' \text{ with } gx^{-1}g^{-1}hgxg^{-1} = h'\} \\ &= \{x : \text{for all } h \text{ there exists } h' \text{ with } x^{-1}g^{-1}hgx = g^{-1}h'g\} \\ &= N_G(g^{-1}Hg). \end{aligned}$$

(iii)  $N_J(H) = \{g \in J : g^{-1}Hg = H\}$ , so  $N_J(H) \subseteq J$ , and  $N_J(H) \subseteq N_G(H)$  as  $J \leq G$ ; hence  $N_J(H) \subseteq N_G(H) \cap J$ . But if  $k \in N_G(H) \cap J$  then  $k \in J$  and  $k^{-1}Hk = H$ . This gives  $k \in N_J(H)$  and equality follows.

(iv) If  $[H, K] \leq H$ , then for  $h \in H$  and  $k \in K$  we have  $[h, k] = h^{-1}k^{-1}hk \in H$ , and so  $k^{-1}hk \in H$  and  $k^{-1}Hk \leq H$ . We can interchange  $k$  and  $k^{-1}$ , and so  $kHk^{-1} \leq H$ , that is  $k^{-1}Hk = H$  and  $k \in N_G(H)$ . For the converse, if  $k \in N_G(H)$  and  $h \in H$ , then  $[h, k] = h^{-1}(k^{-1}hk) \in H$ .

(v) Use the coset action, so the set  $X$  equals the collection of right cosets of  $J$  in  $G$ , and  $o(X) \equiv 0 \pmod{p}$  by hypothesis. By Problem 5.3 this shows that  $o(\text{fix}(J, G)) \equiv 0 \pmod{p}$ . But  $J$  is fixed by this action, hence at least two elements of  $X$  are fixed (as  $p \geq 2$ ). Suppose the second is  $Jg$  where  $Jg \neq J$ . So  $g \notin J$  and  $g^{-1}Jg = J$ , but this implies that  $g \in N_G(J)$  giving the result. Easier arguments exist using the Sylow theory.

**Problem 5.14** (i) Let  $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in GL_2(\mathbb{Q})$ , then  $dA^{-1} = \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}$  where  $d = \det A \neq 0$ . Now if  $A \in N_G(D)$ , then  $C = A^{-1} \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} A \in D$ , for all non-zero  $x, y \in \mathbb{Q}$ . The off-diagonal entries of  $C$  are

$$a_{11}a_{21}(y - x) \quad \text{and} \quad a_{12}a_{22}(x - y).$$

As these are zero we obtain either  $a_{11} = a_{22} = 0$ , or  $a_{12} = a_{21} = 0$  (we cannot have  $a_{11} = a_{12} = 0$  because  $A$  is non-singular). Hence  $A$  is diagonal or anti-diagonal, and  $N_G(D)$  is the subgroup of diagonal and anti-diagonal matrices in  $GL_2(\mathbb{Q})$ .

(ii) In the  $3 \times 3$  case  $N_G(D)$  is the subgroup of all matrices with one non-zero entry in every row and column; see Problems 3.12 and 3.15.

**Problem 5.15** (i) We have  $H \leq N_G(H) \leq G$ . Let  $o(H) = r$ ,  $o(N_G(H)) = rs$  and  $o(G) = rst$  [by Lagrange's Theorem (Theorem 2.27)]. By Lemma 5.25(iii) the number of conjugates of  $H$  in  $G$  is  $t$ , so by Problem 2.23(ii) the total number of elements of  $G$  in a conjugacy class of  $H$  is less than  $rt$ , that

is less than  $rst$  the order of  $G$  even if  $s = 1$ .

(ii) Let  $H$  be a maximal subgroup of  $G$ . By (i) we can find  $a \in G$  such that it does not belong to  $H$  or any of its conjugates.

Now either  $\langle a \rangle = G$  or  $\langle a \rangle < G$ . If the latter, there exists a maximal  $J < G$  with  $\langle a \rangle \leq J < G$ , but  $J$  is conjugate to  $H$ , and so  $a \notin J$ , a contradiction.

**Problem 5.16** (i) We have  $N_G(K) = G$  and  $\text{Aut } K$  is Abelian (Theorem 4.23), so by Problem 5.8(vi) we have  $G = C_G(K)$ , that is each element of  $K$  commutes with each element of  $G$ .

(ii) This is similar using Theorem 4.23 again.

(iii) We have  $G/C_G(K)$  is isomorphic to a subgroup of a finite group, that is  $\text{Aut } K$ , now argue as in (i).

**Problem 5.17** (i) By (i) in Problem 5.13  $H \leq N_G(K)$  and by (ii) of this problem  $N_G(K) \leq N_G(C_G(K))$ , (a) follows. (b) Now  $C_G(K) = N_G(K)$ , so  $H \leq C_G(K)$  which gives  $K \leq Z(H)$  by definition of the centraliser.

(ii) We have  $H \leq Z(N_G(H))$  if and only if  $hk = kh$  for all  $h \in H$  and  $k \in N_G(H)$ . But  $C_G(H) = \{g \in G : gh = hg \text{ for all } h \in H\}$  and  $N_G(H) = \{g \in G : \text{for all } h \in H \text{ there exists } h' \in H \text{ such that } gh = h'g\}$ . So if  $hk = kh$  for all  $h \in H$  and  $k \in N_G(H)$ , the  $h'$  in the definition of  $N_G(H)$  equals  $h$  in all cases, that is  $N_G(H) = C_G(H)$ . This argument reverses.

**Problem 5.18** If  $o(Z(G)) = 3, 5$  or  $15$ , then  $G$  is Abelian by Problem 4.16(ii) (as 3 and 5 are both prime). In this group conjugacy classes of order larger than 1 have orders 3 or 5. The Class Equation (Theorem 5.20) now shows that the only possibility is that  $G$  has three classes of order 3 and one of order 5. The class with order 5 contains all of the elements of  $G$  with order 3, but elements of order 3 occur in pairs:  $\{c, c^2\}$  with  $c^3 = e$  which is a contradiction as 5 is odd.

**Problem 5.19** (i)  $Z(G)$  is the set of scalar matrices (Problem 2.26), and so  $o(Z(G)) = 2$ .

(ii) The matrix  $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$  is non-singular provided  $a \neq 0 \neq c$ , so there are two choices for both  $a$  and  $c$ , and three for  $b$ ; therefore  $o(H) = 12$ , and so by (i)  $Z(G) \leq H$ .

(iii) Let  $h^{-1}gh \in H$  where  $h = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  and  $g = \begin{pmatrix} r & s \\ 0 & u \end{pmatrix}$ . The lower left-hand entry of  $h^{-1}gh$  is 0 when  $ac(r - u) + c^2s = 0$ . This holds for all non-singular matrices  $h = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  when  $s = 0$  and  $r = u$ , or by (i) when  $g \in Z(G)$ . Therefore  $\text{core}(H) = Z(G)$ .

(iv) By Theorem 5.15,  $G/\text{core}(H) = G/Z(G)$  is isomorphic to a subgroup of  $S_4$  as  $[G : H] = 4$ , see (ii). But  $o(G/Z(G)) = 24$ , and so  $G/Z(G) \simeq S_4$ .

**Problem 5.20** Let  $H$  be the normal closure of  $\langle a \rangle$  in  $G$ , see Problem 2.25. As  $C_G(a) \triangleleft G$ ,  $H \leq C_G(a)$ ; see quoted problem. This problem also shows that  $H$  can be expressed as

$$H = \langle g^{-1}a^u g : g \in G, u \in \mathbb{Z} \rangle.$$

We have  $H \triangleleft G$  but is it Abelian? We need

$$(g^{-1}a^t g)(g_1^{-1}a^u g_1) = (g_1^{-1}a^u g_1)(g^{-1}a^t g) \quad \text{for } g, g_1 \in G, t, u \in \mathbb{Z},$$

or rearranging the terms in this expression

$$(g_1 g^{-1} a^t g g_1^{-1}) a^u = a^u (g_1 g^{-1} a^t g g_1^{-1}).$$

But this follows as  $H$  is contained in the centraliser of  $a$  in  $G$ . For a counter example see page 103. In this example  $C_{D_3}(b)$  is a non-normal subgroup of  $D_3$  but  $\langle b \rangle$  is Abelian.

**Problem 5.21** (i) Let  $h^{-1}ah = b$ , then the set  $\{g \in G : g^{-1}ag = b\} = \{g \in G : g^{-1}ag = h^{-1}ah\} = \{g \in G : (gh^{-1})^{-1}a(gh^{-1}) = a\} = C_G(a)$  for as  $g$  ranges over  $G$  so does  $gh^{-1}$  (Theorem 2.8).

(ii) By Theorems 2.27 and 5.19,  $o(C_G(a))o(\mathcal{C}\ell(a)) = o(G)$ . Hence

$$o(C_G(a)) \geq o(G/G') \quad \text{if and only if} \quad o(G)/o(\mathcal{C}\ell(a)) \geq o(G)/o(G')$$

$$\text{if and only if} \quad o(G') \geq o(\mathcal{C}\ell(a)).$$

Let  $\theta : \mathcal{C}\ell(a) \rightarrow G'$  be given by  $g^{-1}ag\theta = [a, g] = a^{-1}g^{-1}ag$  where  $g \in G$ . Now  $g^{-1}ag = h^{-1}ah$  if and only if  $a^{-1}g^{-1}ag = a^{-1}h^{-1}ah$ , and so  $\theta$  is an injective map. Hence as  $o(G)$  is finite, the number of conjugates of  $a$  in  $G$  is less than or equal to the order of  $G'$ .

(iii) As  $K \triangleleft G$  and  $[G : K] = p$ ,  $G/K \simeq C_p$  and there exists  $a \in G$  such that if  $g \in G$  then  $g = a^t k$  for  $0 \leq t < p$  and  $k \in K$ . Hence if  $b = g^{-1}cg$  then  $b = h^{-1}a^{-t}ca^t h$ . But  $C_K(c) < C_G(c)$ , and so  $a$  and  $c$  commute giving  $b = h^{-1}ch$ .

**Problem ♦ 5.22** (i) Suppose  $Z(G) = \langle e \rangle$  and  $r$  is the class number. So  $G$  has one class of order 1 and  $r - 1$  classes of order at least  $p_0$  where  $p_0$  is the smallest prime dividing  $o(G)$ . Hence by the Class Equation (Theorem 5.20)  $1 + (r - 1)p_0 \leq o(G)$ . But  $p_0 \mid o(G)$ , and so  $rp_0 \mid o(G)$  giving  $rp_0 \leq o(G)$ . Now take contra-positive.

(ii) As  $G$  is not Abelian  $Z(G) < G$ , and so  $o(Z(G)) \leq o(G)/2$ . If we have equality, then  $G/Z(G)$  has order 2 and so is cyclic, but then by Problem 4.16(ii)  $G$  is Abelian. Hence  $r - o(Z(G)) \geq 1$ , if we have equality then there is only one conjugacy class  $\mathcal{C}$  of order larger than 1 and so its order is in fact larger than  $o(G)/2$ . But by the Class Equation this would imply that the corresponding centraliser had an order strictly between 1 and 2.

(iii)  $o(Z(G)) \neq 1$  by Lemma 5.21,  $o(Z(G)) \neq p^2$  by Problem 4.16(ii), and  $o(Z(G)) \neq p^3$  as  $G$  is not Abelian; hence  $o(Z(G)) = p$ . Further, as  $Z(G) \triangleleft G$  (Lemma 2.20),  $G/Z(G)$  is Abelian with order  $p^2$  (Theorem 5.22), hence  $G' \subseteq Z(G)$  by Problem 4.6. But  $G' \neq \langle e \rangle$  because  $G$  is not Abelian, therefore  $G' = Z(G)$ . Next we ask: Could  $G$  have a conjugacy class of order  $p^2$ ? No, for if  $o(\mathcal{C}\ell(y)) = p^2$ , then by Theorem 5.19  $[G : C_G(y)] = p^2$ , and so  $o(C_G(y)) = p$ . But by Problem 5.21(ii),  $p = o(C_G(y)) \geq o(G/Z(G)) = p^2$ ; a contradiction. Hence  $G$  has  $p$  conjugacy classes of order 1 (the centre) and  $s$ , say, conjugacy classes of order  $p$ , so  $c = p + s$  and the Class Equation gives

$$p^3 = o(G) = o(Z(G)) + \sum_{i=1}^r o(\mathcal{C}\ell(y_i)) = p + sp,$$

hence  $s = p^2 - 1$  and  $r = p^2 + p - 1$ .

**Problem 5.23** (i) Suppose  $j^{-1}aj = b$ . Then  $C(b) = \{g : gb = bg\} = \{g : gj^{-1}aj = j^{-1}ajg\} = \{g : jgj^{-1}a = ajgj^{-1}\} = \{j^{-1}hj : ha = ah\} = j^{-1}C(a)j$ .

(ii) As each element of  $G$  lies in exactly one conjugacy class,  $o(G) = \sum o(\mathcal{C}\ell(x_i))$  where  $x_i$  is a representative of the  $i$ -th conjugacy class ( $1 \leq i \leq r$ ), and the sum is taken over these classes. By Theorem 5.19, this gives

$$o(G) = \sum [G : C_G(x_i)] = \sum o(G)/c_i \quad \text{where} \quad c_i = o(C_G(x_i)),$$

and so  $1 = 1/c_1 + \cdots + 1/c_r$ .

(iii) For fixed  $r$  the above equation only has finitely many solutions, see Problem B4. Hence there can only be finitely many groups with  $r$  conjugacy classes.

(iv) For  $r \leq 3$ , the solutions are  $1 = 1/1 = 1/2 + 1/2 = 1/2 + 1/3 + 1/6 = 1/2 + 1/4 + 1/4 = 1/3 + 1/3 + 1/3$ . The solution  $1/2 + 1/2$  corresponds to the group  $C_2$ ;  $1/3 + 1/3 + 1/3$  corresponds to  $C_3$ ;  $1/2 + 1/3 + 1/6$  corresponds to  $S_3$ ; whilst  $1/2 + 1/4 + 1/4$  does not correspond to a group.

**Problem 5.24** By Lemma 5.25 the number of conjugate subgroups  $g^{-1}Hg$  is bounded by  $[G : H]$ , and the minimum overlap between two of them is  $\langle e \rangle$ . So

$$o\left(\bigcup_{g \in G} g^{-1}Hg\right) \leq 1 + (o(H) - 1)[G : H],$$

now use Lagrange's Theorem (Theorem 2.27). If  $H$  satisfies the given condition, then

$$\bigcup_{g \in G} g^{-1}Hg = G$$

and so  $[G : H] = 1$ . See also Problem 5.15(i).

**Problem 5.25** (a) If we take  $\sigma = (1, 2, 3)$ , then  $(4, 5)$  commutes with  $(1, 2, 3)$ , and so  $(4, 5) \in C_{S_n}(\sigma)$ .

(b) This follows from the definition of the centraliser.

(c) We have  $[C_{S_n}(\sigma) : C_{A_n}(\sigma)] = [C_{S_n}(\sigma) : C_{S_n}(\sigma) \cap A_n] = [A_n C_{S_n}(\sigma) : A_n]$  [by Theorem 5.8]  $= [S_n : A_n] = 2$ , as  $A_n$  contains all even perms. and  $C_{S_n}(\sigma)$  contains at least one odd perm.

(d) By Theorem 5.19 we have  $[A_n, C_{A_n}(\sigma)] = o(\mathcal{C}\ell_{A_n}(\sigma))$ . As  $\mathcal{C}\ell_{A_n}(\sigma) \subseteq \mathcal{C}\ell_{S_n}(\sigma)$ , with (iii) this shows that  $o(\mathcal{C}\ell_{S_n}(\sigma)) = o(\mathcal{C}\ell_{A_n}(\sigma))$ .

**Problem 5.26** For  $G_1 = S_4$  the element centralisers are:  $C(e) = G_1$ ,  $C((1, 2)) = \langle (1, 2), (3, 4) \rangle \simeq T_2$ ,  $C((1, 2)(3, 4)) = \langle (1, 2), (1, 3, 2, 4) \rangle \simeq D_4$ ,  $C((1, 2, 3)) = \langle (1, 2, 3) \rangle \simeq C_3$ , and  $C((1, 2, 3, 4)) = \langle (1, 2, 3, 4) \rangle \simeq C_4$ .

The subgroup centralisers and normalisers are:

- (i)  $C(\langle e \rangle) = N(\langle e \rangle) = G_1$ ;
- (ii)  $C(\langle(1, 2)\rangle) = N(\langle(1, 2)\rangle) = \langle(1, 2), (3, 4)\rangle \simeq T_2$ ;
- (iii)  $C(\langle(1, 2)(3, 4)\rangle) = N(\langle(1, 2)(3, 4)\rangle) = \langle(1, 3, 2, 4), (1, 2)\rangle \simeq D_4$ ;
- (iv)  $C(\langle(1, 2, 3)\rangle) = \langle(1, 2, 3)\rangle$ ,  $N(\langle(1, 2, 3)\rangle) = \langle(1, 2, 3), (1, 2)\rangle \simeq S_3$ ,  
 $N/C \simeq C_2 \simeq \text{Aut}(C_3)$ ;
- (v)  $C(\langle(1, 2, 3, 4)\rangle) = \langle(1, 2, 3, 4)\rangle$ ,  $N(\langle(1, 2, 3, 4)\rangle) = \langle(1, 2, 3, 4), (1, 3)\rangle$ ,  
 $\simeq D_4$ ,  $N/C \simeq C_2 \simeq \text{Aut}(C_4)$ ;
- (vi)  $C(\langle(1, 2)(3, 4), (1, 3)(2, 4)\rangle) = \langle(1, 2)(3, 4), (1, 3)(2, 4)\rangle$ ,  
 $N(\langle(1, 2)(3, 4), (1, 3)(2, 4)\rangle) = G_1$ ,  $N/C \simeq S_3 \simeq \text{Aut}(T_2)$ ;
- (vii)  $C(\langle(1, 2), (3, 4)\rangle) = \langle(1, 2), (3, 4)\rangle$ ,  $N(\langle(1, 2), (3, 4)\rangle) = \langle(1, 3, 2, 4), (1, 2)\rangle$ ,  $N/C \simeq C_2 \simeq \text{Aut}(T_2) \simeq S_3$ ;
- (viii)  $C(\langle(1, 2, 3), (1, 2)\rangle) = \langle e \rangle$ ,  $N(\langle(1, 2, 3), (1, 2)\rangle) = \langle(1, 2, 3), (1, 2)\rangle$ ,  
 $N/C \simeq S_3 \simeq \text{Aut}(S_3)$ ;
- (ix)  $C(\langle(1, 2, 3, 4), (1, 3)\rangle) = \langle(1, 3)(2, 4), (1, 3)\rangle$ ,  $N(\langle(1, 2, 3, 4), (1, 3)\rangle) = \langle(1, 2, 3, 4), (1, 3)\rangle$ ,  $N/C \simeq T_2 \simeq \text{Aut}(D_4) \simeq D_4$ ;
- (x)  $C(A_4) = \langle e \rangle$ ,  $N(A_4) = G_1$ ,  $N/C \simeq S_4 \simeq \text{Aut}(A_4)$ ;
- (xi)  $C(G_1) = \langle e \rangle$ ,  $N(G_1) = G_1$ ,  $N/C \simeq S_4 \simeq \text{Aut}(S_4)$ .

For  $G_2 = SL_2(3)$  the element centralisers are:  $C(e) = G_2$ ,  $C(\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}) = G_2$ , the centraliser of an order 3 element  $g$  is the subgroup of order 6 generated by  $g$  and  $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$ , and the centralisers of the order 4 and 6 elements are the cyclic groups they generate.

The subgroup centralisers and normalisers of  $SL_2(3)$  are:

- (i)  $C(\langle e \rangle) = N(\langle e \rangle) = G_2$ ;
- (ii)  $C(\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}) = N(\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}) = G_2$ ;
- (iii)  $C(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}) = N(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}) = \langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \rangle$ ,  
a matrix of order 3 has centraliser and normaliser of order 6;
- (iv) Centraliser of an order 4 subgroup is itself, normaliser of an order 4 subgroup is the normal subgroup isomorphic to  $Q_2$ ,  $N/C \simeq C_2 \simeq \text{Aut}(C_4)$ ;
- (v) Centraliser and normaliser of a subgroup of order 6 are both themselves;
- (vi) and (vii) Centraliser of both  $Q_2$  and  $G_2$  are  $\langle \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \rangle$ , isomorphic to  $C_2$ , normaliser of both  $Q_2$  and  $G_2$  are  $G_2$ . In each case  $N/C \simeq A_4$ , and  $\text{Aut}(Q_2)$  and  $\text{Aut}(SL_2(3))$  are both isomorphic to  $S_4$ , see Problem 5.19 and Section 8.2.

Finally note that Burnside's Normal Complement Theorem (Theorem 6.17) only applies in case (iii) for the second group  $G_2$ , and in this case the subgroup in question has the normal complement  $\langle \begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix} \rangle \simeq Q_2$ . In the other cases where  $o(N/C) = 1$  the corresponding subgroup is not Sylow.



## Solutions 6

**Problem ♦ 6.1** (i) We have  $K$  is maximal and  $K \triangleleft G$ . Now as  $G/K$  is a  $p$ -group, by Cauchy's Theorem (Theorem 6.2) it contains an element of order  $p$ , and so a subgroup of order  $p$  with the form  $J/K$  for some  $J$  satisfying  $K \triangleleft J \leq G$ ; this follows using the Correspondence Theorem (Theorem 4.16). But  $K$  is maximal, hence  $J = G$  and  $[G : K] = p$ .

(ii) Suppose the cyclic group  $G$  has generator  $a$ . By Theorem 4.20,  $G$  has a unique subgroup  $H$  generated by  $a^p$  which has index  $p$  in  $G$ . If  $h \in H$  then  $h$  is a power of  $a^p$ , that is  $h = (a^p)^r = (a^r)^p$  for some  $r \in \mathbb{Z}$ , and so every element in  $H$  is a  $p$ -power. Now use Problem 2.13(ii) and see Theorem 6.6. See also Section 10.2.

(iii) As  $G$  is a  $p$ -group, the conjugacy classes have orders  $1, p, p^2, \dots$ . Also  $K \triangleleft G$ , so  $K$  is a union of conjugacy classes. But  $o(K) = p$  and  $\{e\}$  is a conjugacy class in  $K$ . Therefore  $K$  consists entirely of elements whose conjugacy classes have order 1, that is they belong to  $Z(G)$ .

**Problem 6.2** (i) Note automorphisms map  $p$ -elements to  $p$ -elements.

(ii) Let  $a, b \in G$  with  $a^p = b^p = e$ . By Problem 4.6,  $G' \leq Z(G)$ , and so  $[a, b] \in Z(G)$ . Now  $e = a^p = b^{-1}a^pb = (b^{-1}ab)^p = (a[a, b])^p = a^p[a, b]^p$  [by Problem 2.17(ii) with  $t = p$ ]  $= [a, b]^p$ . This shows that  $(ab)^p = a^pb^p$  which gives closure.

**Problem 6.3** There are five group types, three of which are Abelian with all of their subgroups normal and  $Z(G) = G$ . Subgroup lattice diagrams are given on pages 547 to 551.

(i)  $G$  is cyclic, so  $G \simeq \langle a \mid a^8 = e \rangle$ . By Theorem 4.20, the proper non-neutral subgroups are  $\langle a^2 \rangle \simeq C_4$ ,  $\langle a^4 \rangle \simeq C_2$ .

(ii)  $G$  is Abelian and all elements have order 2, that is  $G$  is elementary Abelian (Problem 4.18). We can write  $G$  as  $\langle a, b, c \mid a^2 = b^2 = c^2 = e, ab = ba, bc = cb, ca = ac \rangle$ . It has 7 elements of order 2, and so 7 subgroups of order 2:  $\langle a \rangle, \dots, \langle abc \rangle$ . By trial we see that it also has 7 subgroups of order 4 each isomorphic to  $T_2$ :  $\langle a, b \rangle, \langle a, c \rangle, \langle b, c \rangle, \langle ab, bc \rangle, \langle a, bc \rangle, \langle b, ac \rangle$  and  $\langle c, ab \rangle$ . There are 21 (unordered) subsets of a 7-element set, and each subgroup isomorphic to  $T_2$  contains three of them; hence seven in all.

(iii) The third Abelian possibility is that  $G$  not cyclic and it has an element of order 4, so we can write  $G$  as  $\langle a, b \mid a^4 = b^2 = e, ab = ba \rangle$  with elements  $e$  (order 1),  $a^2, b, a^2b$  (order 2) and  $a, a^3, ab, a^3b$  (order 4). Hence there are three subgroups of order 2. There are also 3 subgroups of order 4:  $\langle a \rangle, \langle ab \rangle$  (isomorphic to  $C_4$ ) and  $\langle a^2, b \rangle \simeq T_2$ .

(iv)  $G = \langle a, b \mid a^4 = b^2 = e, ba = a^3b \rangle \simeq D_4$ . The non-neutral elements are  $a^2, b, ab, a^2b, a^3b$  (order 2) and  $a, a^3$  (order 4). Hence  $G$  has five subgroups isomorphic to  $C_2$  and one isomorphic to  $C_4$ . By trial we see that it also has two isomorphic to  $T_2$ :  $\langle a^2, b \rangle, \langle a^2, ab \rangle$ . (A subgroup of order 4 is normal and so contains the "central" involution  $a^2$ , hence adding another involution generates a copy of  $T_2$ .) As the only non-neutral element that commutes with both  $a$  and  $b$  is  $a^2$  we have  $Z(G) = \langle a^2 \rangle \simeq C_2$ , and so checking cosets we

deduce  $G/Z(G) = \langle aZ, bZ \rangle \simeq T_2$ . The centre  $Z(G)$  and the three subgroups of order 4 are normal (see Problem 2.19). By trial the others are not, they do not commute with  $a$ .

(v)  $G = \langle a, b \mid a^4 = e, b^2 = a^2, ba = a^3b \rangle \simeq Q_2$ . The non-neutral elements are  $a^2$  (order 2) and  $a, a^3 = ab^2 = b^2a, b, ab, a^2b = b^3 = ba^2, a^3b = ab^3$  (order 4). Hence  $G$  has only one subgroup of order 2:  $\langle a^2 \rangle$ , and three of order 4:  $\langle a \rangle, \langle b \rangle$  and  $\langle ab \rangle$  which are all cyclic. As above only  $e$  and  $a^2$  commute with all elements and so  $Z(G) = \langle a^2 \rangle$ , and checking cosets we have  $G/Z(G) = \langle aZ, bZ \rangle \simeq T_2$ . Subgroups have index 2 or equal  $Z(G)$ , and so are ALL normal – a very unusual feature – that is the group is called *Hamiltonian*, see Problem 7.13.

**Problem 6.4** (i) In  $G_1$  we have  $ba^r b = a^{-3r}$  for  $r \in \mathbb{Z}$ , hence  $a = b^2 ab^2 = b(bab)b = ba^{-3}b = a^9$  which gives  $a^8 = e$ . Similarly in  $G_2$ . Now in  $G_1$ ,  $a^r b = ba^{-3r}$ , and so all elements of  $G_1$  have the form  $a^r b^s$  for  $0 \leq r < 8$  and  $0 \leq b < 2$ . Again the same is true for  $G_2$ . Check that if  $a^r b^s = e$ , then  $r = s = 0$ .

(ii) Subgroups of  $G_1$  are  $\langle e \rangle, \langle a^4 \rangle, \langle b \rangle, \langle a^4 b \rangle$  (Order 2);  $\langle a^4, b \rangle (\simeq T_2)$ ;  $\langle a^2 \rangle, \langle a^2 b \rangle$  (cyclic, order 4);  $\langle a \rangle, \langle ab \rangle$  (cyclic, order 8);  $\langle a^2, b \rangle (\simeq C_4 \times C_2)$ ; and  $G_1$  – all normal except  $\langle b \rangle$  and  $\langle a^4 b \rangle$  which are conjugate.

Subgroups of  $G_2$  are  $\langle e \rangle^*, \langle a^4 \rangle^*, \langle b \rangle, \langle a^2 b \rangle, \langle a^4 b \rangle, \langle a^6 b \rangle$  (Order 2);  $\langle a^4, b \rangle, \langle a^4, a^2 b \rangle (\simeq T_2)$ ;  $\langle a^2 \rangle, \langle ab \rangle, \langle a^3 b \rangle (\simeq C_4)$ ;  $\langle a \rangle^* (\simeq C_8)$ ;  $\langle a^2, b \rangle^* (\simeq D_4)$ ;  $\langle a^2, ab \rangle^* (\simeq Q_2)$ ; and  $G_2^*$  – those marked  $*$  are normal. Note that this group has three non-isomorphic subgroups of order 8 only one of which is Abelian.

(iii) Both groups have three maximal subgroups of order 8, normal subgroups of all powers of 2 dividing 16, and a five-term normal series (see Chapter 9).

(iv) In  $G_1$  we have  $\langle a^4 \rangle = (G_1)' < Z(G_1) = \langle a^2 \rangle$ , and in  $G_2$  we have  $\langle a^4 \rangle = Z(G_2) < (G_2)' = \langle a^2 \rangle$ .

(v) The subgroup lattices of  $G_1$  and  $C_8 \times C_2$  are identical except for the ‘top’ group. But note that their ‘normal’ subgroup lattices are not identical because one group is Abelian whilst the other is not. The reader should draw diagrams of these lattices; see pages 557 and 558.

**Problem 6.5** (i) Let  $\phi$  be the natural homomorphism  $G \rightarrow G/Z(G)$ . As  $G/Z(G)$  is Abelian and has order  $p^2$ , see Problems 5.3 and 4.16(ii), it has a normal subgroup  $H/Z(G)$ , say, of order  $p$ . The Correspondence Theorem (Theorem 4.16) now shows that  $G$  has a normal subgroup  $H$  of order  $p^2$ . There are two possibilities (a)  $H$  contains an element of order  $p^2$  (and so is cyclic), and (b) all non-neutral elements of  $H$  have order  $p$  (and so  $H$  is an elementary Abelian  $p$ -group).

Case (a) –  $H = \langle a \rangle$  where  $a^{p^2} = e$  and  $a^p \neq e$ . Let  $b \in G \setminus \langle a \rangle$ . As  $H \triangleleft G$ ,  $b^{-1}ab = a^r$  for some integer  $r$ . Now  $b^{-1}a^s b = a^{rs}$  and  $b^{-t}ab^t = a^{r^t}$ . Hence as  $b^p \in H$ , we have  $r^p \equiv 1 \pmod{p^2}$  which gives  $r = 1 + up$  for some integer  $u$ . If we replace  $b$  by  $a^u b$ , we obtain the first group.

Case (b) –  $H = \langle a \rangle \times \langle b \rangle$  where  $a$  and  $b$  have order  $p$ ; see Chapter 7. If  $c = [a, b]$ , then by Problem 4.6,  $c \in Z(G)$ , that is  $ca = ac$  and  $cb = bc$ . If  $p = 2$  then  $G$  is Abelian (see Corollary 2.11, in fact it is an elementary Abelian 2-group), but it is not Abelian if  $p > 2$ .

(ii) Working over a  $p$ -element field we can take, for example,

$$a = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, b = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, c = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

(iii)  $ES_1(3)$ . The proper subgroups are  $\langle a \rangle, \langle ab \rangle, \langle ab^2 \rangle (\simeq C_9)$ ;  $\langle a^3, b \rangle (\simeq C_3 \times C_3)$ ;  $\langle a^3 \rangle, \langle b \rangle, \langle a^3b \rangle, \langle a^6b \rangle (\simeq C_3)$  and  $\langle e \rangle$ , all are normal except  $\langle b \rangle, \langle a^3b \rangle$  and  $\langle a^6b \rangle$ , and second to fifth are maximal. The centre is  $\langle a^3 \rangle$ .

$ES_2(3)$ . The proper subgroups are  $\langle c, a \rangle, \langle c, b \rangle, \langle c, ab \rangle, \langle c, ab^2 \rangle (\simeq C_3 \times C_3)$ ;  $\langle c \rangle, \langle a \rangle, \langle b \rangle, \langle ac \rangle, \langle ac^2 \rangle, \langle bc \rangle, \langle bc^2 \rangle, \langle ab \rangle, \langle ab^2 \rangle, \langle a^2b \rangle, \langle a^2b^2 \rangle, \langle abc \rangle, \langle a^2bc^2 \rangle (\simeq C_3)$  and  $\langle e \rangle$ . Second to fifth are maximal, and first to sixth and  $\langle e \rangle$  are normal, and the centre is  $\langle c \rangle$ .

**Problem 6.6** If  $o(G) = p^2$  use Theorem 5.22 and the fact that  $C_p \times C_p$  contains  $p$  subgroups of order  $p$ . If  $o(G) = p^3$  then, apart from  $C_{p^3}$ , each of the groups involved ( $C_{p^2} \times C_p, C_p^3, ES_1(p)$  and  $ES_2(p)$ ) have more than one subgroup of order  $p$ ; see the previous problem and Section 7.2. This fact can also be proved directly using Theorem 10.21 and Problem 2.17(ii); see Doerk and Hawkes [1992], page 204. Note that the result is false for  $p = 2$ ,  $Q_2$  has a unique subgroup of order 2 and it is clearly not cyclic (or Abelian).

If  $o(G) = p^n$  where  $n > 3$  then, by Theorem 6.5, we can find  $K$  to satisfy:  $K \triangleleft G$  and  $o(K) = p$ . Suppose  $G/K$  has two subgroups,  $H/K$  and  $J/K$ , of order  $p$ . We may assume that  $H/K \leq Z(G/K)$  (see Chapter 10). It follows that  $HJ \leq G$  and  $o(HJ) = p^3$  (use Theorem 5.8). Now by the case above, this group has a unique subgroup of order  $p^2$ , and so  $H = J$ ,  $G/K$  has a unique subgroup of order  $p$ , and so is cyclic. Let  $G = \langle K, a \rangle$  and  $A = \langle a \rangle$ . If  $G \cap A = \langle e \rangle$ , then  $G$  has two subgroups of order  $p$ , they are  $\{c \in A : c^p = e\}$  and  $K$ , which is impossible. Therefore  $K \leq A$  and  $G = KA = A$ .

**Problem 6.7** (i) The group is Abelian by definition. Using the relations we have  $a_0^p = e$  and  $a_n^{p^{n+1}} = a_{n-1}^{p^n} = \cdots = a_0^p = e$ , and so the order of every generator is a power of  $p$ , hence all elements are  $p$ -elements as the group is Abelian.

(ii) Use the equations above.

(iii) If  $H \leq C_{p^\infty}$  and  $H$  contains infinitely many of the  $a_n$ , then  $H = C_{p^\infty}$  by (ii). But if  $H$  only contains  $a_{i_1}, \dots, a_{i_k}$ , where  $i_1 < \cdots < i_k$ , then by (ii) again  $H = \langle a_{i_k} \rangle$ .

**Problem 6.8** (ia) As  $3^2$  is the largest power of 3 dividing  $o(S_6)$ , by Theorem 4.22 a Sylow 3-subgroup of  $S_6$  is isomorphic to either  $C_9$  or  $C_3 \times C_3$ . Using the quoted problem we see that  $S_6$  contains no element of order 9. We can also note directly that  $C_3 \times C_3 \simeq l(1, 2, 3), (4, 5, 6)$  is a Sylow 3-subgroup of  $S_6$ .

(ib) By Problem 3.7,  $S_4$  is isomorphic to a subgroup of  $A_6$ , and the Sylow 2-subgroups of  $S_4$  are isomorphic to  $D_4$  so the same is true for  $A_6$ .

(ic)  $o(SL_2(5)) = 120$ , so a Sylow 2-subgroup has order 8. Using the quoted problem the only order 8 group with a single element of order 2 is  $Q_8$ , so this is the isomorphism type of the Sylow 2-subgroups in this case.

(ii) Let  $D_n = \langle a, b \mid a^n = b^2 = e, ba = a^{n-1}b \rangle$ . The elements of this group are:  $e, a, \dots, a^{n-1}, b, ab, \dots, a^{n-1}b$  where  $o(ab^t) = 2$  for  $t = 0, \dots, n-1$ , and the  $n$  Sylow 2-subgroups are  $\langle ab^t \rangle$ , all of order 2;  $n$  in all. Note that by the Sylow theory  $n_2$  is odd and divides  $n$ . The rest are subgroups of the cyclic subgroup  $\langle a \rangle$  which has odd order. Now use Theorem 4.20.

If  $n = 2^k$  the result is clearly not true, also  $D_6$  has a Sylow 2-subgroup isomorphic to  $T_2$ , *et cetera*.

(iii) We have  $H \simeq S_3 \times S_3$  with  $o(H) = 36$ , and so  $H$  has Sylow 2-subgroups of order 4 (nine in all). Let  $P_1 = \langle (1, 2), (4, 5) \rangle$ ,  $P_2 = \langle (2, 3), (5, 6) \rangle$  and  $P_3 = \langle (1, 2), (5, 6) \rangle$  for example.

**Problem ♦ 6.9** (i)  $P$  is contained in both  $Q$  and  $H$  and so  $P \leq Q \cap H$ . But  $Q \cap H$  is a  $p$ -subgroup of  $H$ , and  $P$  is a  $p$ -subgroup of  $H$  of highest possible power, hence we have equality.

(ii) We use Sylow 2 and 5. If  $P$  is a Sylow  $p$ -subgroup of  $G$ , then  $KP \leq G$  by Theorem 2.30. Also  $P \leq KP$ , and  $KP$  is a  $p$ -group. But  $P$  is a  $p$ -subgroup of  $G$  of maximum  $p$ -order, hence  $P = KP$  which in turn implies  $K \leq P$ .

(iii) See Problem 5.13(v).

(iv) Let  $G$  act by conjugation on  $K$  (so  $k \cdot g = g^{-1}kg$  for  $g \in G$  and  $k \in K$ ), and restrict this action to  $P$  (page 98), that is  $P$  acts by conjugation on  $K$ .

$$\text{fix}(K, P) = \{k \in K : j^{-1}kj = k \text{ for all } j \in P\} = K \cap C_G(P) = \langle e \rangle.$$

This last equation holds because  $o(C_G(P))$  is a power of  $p$  and by hypothesis  $(o(K), p) = 1$ . By Problem 5.3(i),  $o(\text{fix}(K, P)) \equiv o(K) \pmod{p}$ , hence  $o(K) \equiv 1 \pmod{p}$ .

(v) Automorphisms map Sylow  $p$ -subgroups to Sylow  $p$ -subgroups, so  $O_p(G)$  is a characteristic subgroup of  $G$  (Problem 4.22), the second part follows directly from (i).

(vi) Let  $P_i$  be a Sylow  $p$ -subgroup of  $G$ . If  $a \in P_i$  for all  $i$ , then  $g^{-1}ag \in g^{-1}P_i g$  for all  $i$  and all  $g \in G$ . But by Sylow 2 the set of conjugates of the set of Sylow  $p$ -subgroups is just the set of Sylow  $p$ -subgroups itself. Hence if  $a \in \bigcap P_i$  then  $g^{-1}ag \in \bigcap P_i$  for all  $g \in G$ . Now use Theorem 2.15.

**Problem ♦ 6.10** (i) By Sylow 4,  $n_p(G) \equiv n_p(H) \equiv 1 \pmod{p}$ , so by Theorem 6.8(ii) we have

$$[G : N_G(P)] \equiv [H : N_H(P)] \equiv 1 \pmod{p}.$$

But  $N_H(P) \leq H \leq G$  hence  $[G : N_G(P)] = [G : H][H : N_H(P)]$  and the result follows.

(ii) There exists  $a \in G$  with  $h = a^{-1}ga$ , and so  $h \in a^{-1}C_G(P)a = C_G(a^{-1}Pa)$ . Also  $P, a^{-1}Pa \leq C_G(h)$  and they are Sylow subgroups of  $C_G(h)$ . Hence by Sylow 2 there exists  $b \in C_G(h)$  satisfying  $P = b^{-1}(a^{-1}Pa)b$ , which gives  $ab \in N_G(P)$  and  $b^{-1}a^{-1}gab = b^{-1}hb = h$ .

(iii)  $P$  is a Sylow  $p$ -subgroup of  $G$ ,  $o(P) = p^r$  and  $o(G) = \dots p^r \dots$ . Then  $o(KP) = \dots p^s \dots$  for some  $s \leq r$ , and if  $o(K) = \dots p^t \dots$  then  $o(K \cap P) = p^u$  for some  $u \leq t$ . By Theorem 5.8 we have

$$o(K)o(P) = o(KP)o(K \cap P), \quad \text{and so} \quad p^r p^t = p^s p^u,$$

which gives  $s = r$  and  $u = t$ . Hence  $K \cap P$  is a Sylow  $p$ -subgroup of  $K$ , as powers of  $p$  agree, and  $o(KP) = \dots p^r \dots$ .

Secondly  $K \triangleleft G$ , so  $K \triangleleft KP$ , and by the Correspondence Theorem (Theorem 4.16) as the  $p$ -powers of  $o(G)$  and  $o(KP)$  are equal (to  $p^r$ ), we see that the  $p$ -powers of  $o(G/K)$  and  $o(KP/K)$  are also equal (to  $p^{r-t}$  in this case). Now the Second Isomorphism Theorem (Theorem 4.15) gives  $KP/K \simeq P/(K \cap P)$ , the right-hand side is a factor group of a  $p$ -group, and so is itself a  $p$ -group, therefore the left-hand side is also a  $p$ -group and this proves that  $KP/K$  is a Sylow  $p$ -subgroup of  $G/K$ .

(iv) One example is as follows. Let  $G = A_6$ . Note  $S_4 \leq A_6$  (see Problem 3.7) and the powers of 2 in the prime factorisation of both  $o(A_6)$  and  $o(S_4)$  are equal (to  $2^3$ ). Now  $P = \langle (1, 2, 3, 4), (1, 3) \rangle \simeq D_4$  is a Sylow 2-subgroup of  $S_4$  (Chapter 8), so it is also isomorphic to a Sylow 2-subgroup of  $A_6$  by the Sylow theory, and we can take it as  $\langle (1, 2, 3, 4)(5, 6), (1, 3)(5, 6) \rangle$ . Let  $J$  be the group of all even permutations of the set  $\{1, 2, 3, 5, 6\}$ , then  $A_5 \simeq J \leq A_6$ ,  $o(J) = 60$  and  $o(P) = 8$ . Now  $P \cap J = \langle (1, 3)(5, 6) \rangle$  and  $o(P \cap J) = 2$ , so  $P \cap J$  is not a Sylow 2-subgroup of  $J$  as such a group would have order 4. Note that you could also use Problem 6.8(iii).

(v) This follows from (iii) as  $KP/K$  is just some Sylow subgroup of  $G$ .

**Problem 6.11** (i) If  $H = \langle P_1, \dots, P_r \rangle$ , then  $H \leq G$  and  $o(P_i) \mid o(H)$  for  $i = 1, \dots, r$ . This shows that  $o(H) = o(G)$  and so  $H = G$ . Use Theorem 5.8 when  $r = 2$ .

(ii) First we have

$$(K_1 \cap P)(K_2 \cap P) \leq K_1 K_2 \cap P.$$

Suppose  $P$  is a  $p$ -group,  $o(K_i) = \dots p^{r_i} \dots$  and  $o(K_1 K_2) = \dots p^s \dots$ . By Problem 6.10(iii)  $o(K_i \cap P) = p^{r_i}$  and  $o(K_1 K_2 \cap P) = p^s$ . So if  $o(K_1 \cap K_2) = \dots p^t \dots$ , then by Theorem 5.8

$$o(K_i \cap P)(K_2 \cap P) = p^{r_1+r_2}/p^t = p^s = o(K_1 K_2 \cap P),$$

and the result follows. For the second part use Problem 2.18 (Dedekind's Identity).

(iii) By (i),  $P = P_1 \cap H$  and  $Q = Q_1 \cap H$ , and  $P$  and  $Q$  are distinct. As  $P$  is a Sylow  $p$ -subgroup of  $H$ , by Sylow 5 there exists a Sylow  $p$ -subgroup  $P_1$

of  $G$  with  $P_1 \geq P$ . Result follows by (ii).

(iv) Use (iii) and Sylow 5, if  $P$  is a Sylow  $p$ -subgroup of  $H$  then  $P$  is a  $p$ -subgroup of  $G$ , and so it is contained in a Sylow  $p$ -subgroup of  $G$ .

(v) By the quoted problem we have  $[G : H] = \sum_{c \in C} [J : J \cap c^{-1}Hc]$  where  $C$  is a set of double coset representatives. Now as  $H$  is Sylow,  $p \nmid [G : H]$ , so there is a  $c \in C$  such that  $p \nmid [J : J \cap c^{-1}Hc]$ . Also  $J \cap c^{-1}Hc$  is a  $p$ -group, and hence it is a Sylow  $p$ -subgroup of  $J$ , now put  $a = c$ .

**Problem 6.12** (i) We have  $o(S_p) = p!$ , so a Sylow  $p$ -subgroup  $P$  has order  $p$  and is isomorphic to  $C_p$ . But  $S_p$  contains  $(p-1)!$  permutations which are  $p$ -cycles, and so  $(p-2)!$  Sylow  $p$ -subgroups (see Problem 2.5(iii)). Therefore  $[S_p : N_{S_p}(P)] = n_p = (p-2)!$  which gives  $o(N_{S_p}(P)) = p(p-1)$ . Also  $P \triangleleft N_{S_p}(P)$ , so  $N_{S_p}(P)$  is a subgroup of  $S_p$  of order  $p(p-1)$  with a normal cyclic subgroup  $P$  of order  $p$ . Further development will depend on the factorisation of  $p-1$ , for an example see Problem 3.11.

(ii) Suppose  $n_p > 1$  and  $P = N_G(P)$  for all Sylow  $p$ -subgroups  $P$  of  $G$ . As  $G$  is a transitive subgroup of  $S_p$ ,  $P \simeq C_p$ . By the Sylow theory,  $G$  has  $(p-1)n_p = o(G) - n_p$  elements of order  $p$ . None of these elements is fixed by  $G$  (as it is transitive), so  $G$  has at most  $n_p$  fixed elements. Each stabiliser  $\text{stab}_G(i)$  ( $1 \leq i \leq p$ ) has  $n_p$  elements which possess one fixed point. It follows that all stabilisers have order 1, and so are equal. Now refer to the first proof of Sylow's main theorem. Hence the group has a unique Sylow  $p$ -subgroup contrary to our assumption. Now see Problem 12.15.

**Problem 6.13** (i) If  $n_3 = 4$ , then  $G$  has eight elements of order 3, and so only four elements of order 1, 2 or 4. But a Sylow 2-subgroup has order 4, and so it must be unique.

(ii) The possible orders for  $G$  are 5, 10, 15, 20 and 30. Now  $n_5 = 1$  follows directly from the Sylow theory in the first four cases. If  $n_5 \neq 1$  in the fifth case, then  $n_5 = 6$  and the group contains 24 elements of order 5. Further if  $a$  is an involution in  $G$ ,  $P$  is a Sylow 5-subgroup of  $G$  (and so  $P = N_G(P)$ ), then conjugation of  $a$  by the elements of  $P$  gives five distinct involutions in  $G$ . Hence  $G$  has no element of order 3 which is impossible by Cauchy's Theorem (Theorem 6.2).

(iii) Ten subgroups isomorphic to  $C_3$  generated by  $(1, 2, 3)$ ,  $(1, 2, 4)$ ,  $(1, 2, 5)$ ,  $(1, 3, 4)$ ,  $(1, 3, 5)$ ,  $(1, 4, 5)$ ,  $(2, 3, 4)$ ,  $(2, 3, 5)$ ,  $(2, 4, 5)$  and  $(3, 4, 5)$ ; five subgroups isomorphic to  $T_2$ , the first is generated by  $(1, 2)(3, 4)$  and  $(1, 3)(2, 4)$  and the remainder are similar noting that there are five ways of choosing four elements out of five; and six subgroups isomorphic to  $C_5$  generated by  $(1, 2, 3, 4, 5)$ ,  $(1, 2, 3, 5, 4)$ ,  $(1, 2, 4, 3, 5)$ ,  $(1, 2, 4, 5, 3)$ ,  $(1, 2, 5, 3, 4)$ , and  $(1, 2, 5, 4, 3)$ .

**Problem 6.14** By Theorems 6.2 and 6.11 the group  $G$  contains elements  $a$  and  $b$  with  $o(a) = q$ ,  $o(b) = p$ , where  $K = \langle a \rangle \triangleleft G$  and  $H = \langle b \rangle \leq G$ . Also by the normality of  $K$ ,  $b^{-1}ab = a^r$  for some  $r \neq 1$ . So  $b^{-t}ab^t = a^{r^t}$  and  $a^s b^t = b^t a^{r^t s}$ . Hence  $G$  has the presentation

$$G \simeq \langle a, b \mid a^q = b^p = e, b^{-1}ab = a^r \rangle.$$

Further this gives  $a = b^{-p}ab^p = a^{r^p}$ , so  $r^p \equiv 1 \pmod{q}$ . The integer  $r$  exists by the theory of primitive roots; see Appendix B. In fact there are  $p-1$  possibilities modulo  $p$  for  $r$  which can be written as  $r, r^2, \dots, r^{p-1}$ . These possibilities do not give rise to distinct groups, for if we replace  $r$  by  $r^k$ , say, then we obtain the original group if we also replace the generator  $b$  by  $b^k$ , and  $H$  is cyclic of prime order so every non-neutral element can act as a generator of the group. This is an example of a Frobenius group, see **Web Section 14.3**.

**Problem ♦ 6.15** Groups of order less than 60. By theorems proved in this chapter, groups whose orders are prime powers, or have three or fewer (not necessarily distinct) prime factors, possess normal subgroups. The remaining cases are (a) 24, (b) 36, (c) 40, (d) 48, (e) 54, and (f) 56; we treat each of these in turn.

(a)  $o(G) = 24 = 2^3 \cdot 3$ . Always look at the larger primes first! We have  $n_3 \equiv 1 \pmod{8}$  and  $n_3 \mid 8$  so  $n_3 = 1$  or 4. If  $n_3 = 4$ ,  $G$  is simple, and  $H$  is a Sylow 3-subgroup of  $G$ , then  $\text{core}(H) = \langle e \rangle$  giving an injection of  $G$  into  $S_4$  (Theorem 5.15). Comparing orders implies that  $G \simeq S_4$ , but  $A_4 \triangleleft S_4$  which gives a contradiction.

(b)  $o(G) = 36 = 2^2 \cdot 3^2$ . The group  $G$  has a Sylow 3-subgroup  $H$  (of order 9) with index  $[G : H] = 4$ . As in (a), if  $G$  is simple then Theorem 5.15 provides an injection of  $G$  into  $S_4$  which is impossible because  $o(G) = 36$  and  $o(S_4) = 24$ .

(c)  $o(G) = 40 = 2^3 \cdot 5$ . By Sylow 4 we have  $n_5 \equiv 1 \pmod{5}$  and  $n_5 \mid 8$ , which gives  $n_5 = 1$  and  $G$  has a normal cyclic subgroup of order 5.

(d)  $o(G) = 48 = 2^4 \cdot 3$ . The method given in (a) also applies here. Note that if  $n_3 = 16$ , then the group has 32 elements of order 3 which implies that the Sylow 2-subgroup is unique. See also Problem 6.17(iii).

(e)  $o(G) = 54 = 2 \cdot 3^3$ . A Sylow 3-subgroup has index 2 and so is normal by Problem 2.19.

(f)  $o(G) = 56 = 2^3 \cdot 7$ . By Sylow 4 we see that  $n_2 \equiv 1 \pmod{2}$ ,  $n_2 \mid 7$ ,  $n_7 \equiv 1 \pmod{7}$  and  $n_7 \mid 8$ , so  $n_2 = 1$  or 7, and  $n_7 = 1$  or 8. If  $n_7 = 8$ , then  $G$  has 48 elements of order 7, the neutral element, and only seven other elements, that is there would be only one Sylow 2-subgroup. Hence either  $n_2 = 1$  or  $n_7 = 1$  or both.

**Problem 6.16** (i) The group  $G$  has order 60 and six Sylow 5-subgroups. Suppose  $K \triangleleft G$  where  $1 < o(K) < 60$ . If  $5 \mid o(K)$ , then by Problem 6.13(ii)  $K$  contains a normal Sylow 5-subgroup  $P$ . Now  $P$  is characteristic in  $K$  and so normal in  $G$ ; see Problem 4.22. If  $5 \nmid o(K)$ , then  $5 \mid o(G/K)$ , and by Problem 6.13(ii) again we have

$$\langle e \rangle < PK/K \triangleleft G/K \quad \text{and so} \quad PK \triangleleft G.$$

This shows that  $PK = G$  (as  $5 \mid o(PK)$ ), and so every proper non-neutral normal subgroup  $K$  of  $G$  has order 12. But by Problem 6.13(i) we see that  $K$  contains a normal, and so characteristic, Sylow subgroup which is normal in  $G$  but not of order 12 which is a contradiction.

(ii) Suppose  $G$  is a simple group of order 60. It has no subgroups of index 2, 3 or 4; use the same proof as for  $A_5$  on page 101. Next we show that  $G$  does have a subgroup of index 5. Suppose not. By Sylow 4,  $G$  has 15 Sylow 2-subgroups. By Sylow 4,  $n_2 = [G : N_G(P)]$  where  $P$  is a Sylow 2-subgroup, and  $o(N_G(P)) < 12$  by supposition.

Next we show that  $G$  has 45 elements of order a power of 2. Let  $P_1$  and  $P_2$  be distinct Sylow 2-subgroups of  $G$ , and let  $a \in P_1 \cap P_2$  where  $a \neq e$ . Since  $P_1$  and  $P_2$  are Abelian, we see that

$$o(C_G(a)) > 4; \text{ but } 4 \mid o(C_G(a)) \text{ as } P_1 < C_G(a).$$

Hence  $[G : C_G(a)] \leq 5$  which by the first statement implies that  $G = C_G(a)$ . But in turn this implies that  $a \in Z(G)$ , so  $Z(G) \neq \langle e \rangle$ , and hence  $G$  has a proper non-neutral normal subgroup which is contrary to assumption that  $G$  is simple. Therefore  $P_1 \cap P_2 = \langle e \rangle$ , and so  $G$  has 45 elements of order 2 or 4. But if  $G$  is simple it also has six Sylow 5-subgroups, and so it has 24 elements of order 5. But  $24 + 45 > 60$ , therefore our supposition is false and  $G$  does indeed have a subgroup of index 5.

Now by Theorem 5.15, and as  $G$  is simple, there is an injective homomorphism of  $G$  into  $S_5$ . Hence we can treat  $G$  as a subgroup of  $S_5$ . Suppose  $G \neq A_5$ , so  $GA_5 = S_5$  by Problem 2.19(ii). Further by Theorem 5.8,  $o(G \cap A_5) = o(G)o(A_5)/o(GA_5) = 30$ . Hence  $G \cap A_5 \leq G$  with order  $o(G)/2$ , and so  $G \cap A_5$  is normal (by Problem 2.19 again) which is impossible as  $G$  is simple. Therefore  $G \simeq A_5$ .

**Problem 6.17** (i)  $90 = 2 \cdot 3^2 \cdot 5$ , so if  $G$  is simple,  $n_5 = 6$  and  $n_3 = 10$ . If each pair of Sylow 3-subgroups has neutral intersection, then the group has 24 elements of order 5 and 80 of order 3 or 9 which is impossible. So suppose  $P$  and  $Q$  are distinct Sylow 3-subgroups and  $o(R) = 3$ , then  $P, Q < S$  and  $9 \mid o(S)$ , so  $o(S) = 18, 45$  or  $90$ . If  $o(S) = 18$ , Theorem 5.15 gives an injective homomorphism of  $G$  into  $S_5$ , but  $90 \nmid 120$ ; if  $o(S) = 45$ , then  $S \triangleleft G$  (Problem 2.19(i)); and if  $o(S) = 90$ , then  $R \triangleleft G$  by Theorem 5.16.

(ii)  $108 = 3^3(3+1)$ , we give proof for  $p^r(p+1)$  where  $r > 1$ . If  $G$  is simple, then  $n_p = p+1$ , so by Theorem 5.15, there is an injective homomorphism of  $G$  into  $S_{p+1}$ . This is not possible as  $o(S_{p+1})$  is not divisible by  $p^r(p+1)$ , the order of  $G$ ; note  $r > 1$ .

(iii)  $112 = 2^4 \cdot 7$ , we give the proof for  $p^n \cdot q$ . Note first that the Sylow theory implies that  $n_p = q$  if  $G$  is simple. If each pair of Sylow  $p$ -subgroups has neutral intersection, then  $G$  possesses  $q(p^n - 1)$  elements of order a power of  $p$ , and so only  $q$  others. These elements will form a single subgroup of order  $q$  which must be normal by Sylow 3.

Now if  $S$  has a unique Sylow  $p$ -subgroup  $T$  contained in  $U$ , a Sylow  $p$ -subgroup of  $G$ , it would also contain  $N_P(R)$ , and so by the given inequality,  $R$  is a proper subgroup of  $P \cap U$ . By the maximal property of  $R$ , this implies that  $P = U$ . A similar argument shows that  $Q = U$ , but  $P$  and  $Q$  are distinct. Now the Sylow theory implies that  $S$  has  $q$  Sylow  $p$ -subgroups, and all of these contain  $R$  (use Problem 6.9(iii)).



Using Problem 6.9(vii) this shows that every Sylow  $p$ -subgroup of  $G$  contains  $R$ , and by Sylow 2 this further shows that  $R \triangleleft G$ . Hence by the supposed simplicity of  $G$  we have  $R = \langle e \rangle$ .

(iv)  $132 = 2^2 \cdot 3 \cdot 11$ . By Sylow 4 we have  $n_2 = 1, 3, 11$  or  $33$ ,  $n_3 = 1, 4$  or  $22$ , and  $n_{11} = 1$  or  $12$ . If the group  $G$  simple, then  $n_2 \geq 3, n_3 \geq 4$  and  $n_{11} = 12$ . So  $G$  has at least six elements of order 2 or 4, eight of order 3, and 120 of order 11, totalling 134 which is impossible as  $o(G) = 132$ .

(v)  $144 = 2^4 \cdot 3^2$  and  $n_3 = 1, 4$  or  $16$ . If  $n_3 = 4$  use Theorem 5.15 and  $36 \nmid 24$ . If  $n_3 = 16$  and all pairs of Sylow 3-subgroups have neutral intersection, then the group has 128 elements of order 3 or 9, and so only 16 others which shows that  $n_2$  cannot be larger than 1. If  $P$  and  $Q$  are distinct Sylow 3-subgroups of  $G$ ,  $R = P \cap Q$  and  $S = N_G(R)$ , then as in (ii)  $o(S) = 18, 36, 72$  or  $144$ . If  $o(S) = 18$ , use the fact that a group of order 18 has a normal subgroup of order 9. (If  $P$  is a normal  $p$ -subgroup of  $S$ , then  $S \leq N_G(P)$ , and so  $n_3 \leq 8$ ; Problem 2.19); if  $o(S) = 36$ , use Theorem 5.15; if  $o(S) = 72$ , then  $S \triangleleft G$ ; and if  $o(S) = 144$ , then  $R \triangleleft G$ .

As a further exercise you could now check that the only non-Abelian simple groups of order less than 360 are of order 60 or 168. For example if  $o(G) = 120$  begin by constructing a map into  $S_6$  using a suitable normaliser property.

**Problem 6.18** Let  $Q_2 = \langle a, b \mid a^2 = b^2 = (ab)^2 \rangle$ . The maximal subgroups are  $\langle a \rangle$ ,  $\langle b \rangle$  and  $\langle ab \rangle$ , note that  $b^{-1}ab = a^3$ ,  $a^{-1}ba = b^3$  and  $a^{-1}(ab)a = (ab)^3$  *et cetera*, and so there is an action of  $\text{Aut}(Q_2)$  on the maximal subgroups of  $Q_2$  defined by conjugation, and by Theorem 5.12 there exists a homomorphism  $\phi : \text{Aut}(Q_2) \rightarrow S_3$  ( $S_3$  because there are three maximal subgroups). This is surjective by the equations above, for example one automorphism interchanges  $a$  and  $b$  throughout, another interchanges  $a$  and  $ab$  throughout.

Now by Corollary 5.27,  $\text{Inn}(Q_2) \simeq Q_2/Z(Q_2) \simeq C_2 \times C_2$ ; see Problem 6.3. Also  $\ker \phi \leq \text{Inn}(Q_2)$ . One inner automorphism maps  $a \mapsto a^3$  and  $b \mapsto b$ . Hence  $o(\ker \phi) = 4$ , and so  $o(\text{Aut}(Q_2)) = 24$ . Which group of order 24 is it? There are a number of ways to answer this, see page 171, for instance show directly that  $Z(\text{Aut}(Q_2)) = \langle e \rangle$  or show that all subgroups of  $\text{Aut}(Q_2)$  of order 2 or 3 are not normal.

**Problem 6.19** In  $S_5$  we have  $n_5 \equiv 1 \pmod{5}$  and  $n_5 \mid 24$ , so  $n_5 = 1$  or  $6$ , by Sylow 4. But  $S_5$  contains 24 elements of order 5, so  $n_5 = 6$ , and using Sylow 4 again this gives  $[N_{S_5}(P) : P] = 6$  or  $o(N_{S_5}(P)) = 20$  where  $P$  is a Sylow 5-subgroup. If we take  $P = \langle (1, 2, 3, 4, 5) \rangle$ , then as  $\tau^{-1}\sigma\tau = (1, 3, 5, 2, 4) = \sigma^2$ , we have  $\tau \in N_{S_5}(P)$ . Hence both  $\sigma$  and  $\tau$  belong to  $N_{S_5}(P)$ , and so  $J = \langle \sigma, \tau \rangle \leq N_{S_5}(P)$ . But  $o(\sigma) = 5$  and  $o(\tau) = 4$ , hence  $o(J) \geq 20$  and so  $J = N_{S_5}(P)$ .

**Problem ♦ 6.20** (i) We have  $P$  is a Sylow subgroup of  $G$ ,  $H \triangleleft G$ , and  $P \triangleleft H$ . The Frattini argument (Theorem 6.14) gives  $G = N_G(P)H$ . But if  $P \triangleleft H$  then  $H \leq N_G(P)$ , hence  $G = N_G(P)H = N_G(P)$  and so  $P \triangleleft G$ .

(ii) Suppose the number of prime factors of  $o(G)$  is  $t$  and  $p^*$  is the largest. The result holds when  $t = 2$  by Theorem 6.11. Using induction suppose the result holds for all groups  $G_1$  where  $o(G_1)$  is square-free and the number of its prime factors is less than  $t$ . By the given fact there exists  $H \triangleleft G$ ; and  $o(H)$

has fewer than  $t$  prime factors, as  $o(G)$  is square-free. There are two cases.

(a) If  $p^*$  is the largest prime factor of  $o(H)$ , then the inductive hypothesis gives  $P$ , a Sylow  $p^*$ -subgroup of  $H$  normal in  $H$ . By the first part  $P \triangleleft G$ .

(b) Secondly, suppose  $p^* \nmid o(H)$ ; but  $p^* \mid o(G)$ , and so  $p^* \mid o(G/H)$ . By the inductive hypothesis,  $G/H$  has a normal Sylow  $p^*$ -subgroup  $P_1$ , say. Let  $\theta$  be the natural homomorphism  $G \rightarrow G/H$  (see Definition 4.13), and let  $J = P_1\theta^{-1}$ . Using the Correspondence Theorem (Theorem 4.16) we have

$$[G : J] = [G/H : P_1], \text{ and } p^* \nmid [G : J] \text{ as } p^* \nmid [G/H : P_1];$$

this shows that  $p^* \mid o(J)$ . Let  $P^*$  be a Sylow  $p^*$ -subgroup of  $J$ , and so  $P^*$  is also a Sylow  $p^*$ -subgroup of  $G$ . Now by Problem 6.10(iii),  $P^*H/H$  is a Sylow  $p^*$ -subgroup of  $G/H$ , and  $P^*H/H = P^*\theta \subseteq J\theta = P_1$ . Hence  $P_1 = P^*H/H$ , and the Second Isomorphism Theorem gives  $P^*H/H \simeq P^*/(P^* \cap H) \simeq P^*$  as  $P^*$  is cyclic.

Therefore  $P^* = P_1$  and the result follows because these facts show that there is a unique Sylow  $p^*$ -subgroup of  $G$  which is normal by Sylow 3.

**Problem 6.21** (i) Using Dedekind's Law (Problem 2.18) we have, as  $H \cap K_1 \leq H$ ,

$$(H \cap K_1)(H \cap K_2) = H \cap (H \cap K_1)K_2 = H,$$

because  $H \leq (H \cap K_1)K_2$  and  $K_1K_2 = G$ .

(ii) Let  $G = S_4$ ,  $K_1 = V (\simeq T_2)$ ,  $K_2 = \langle (1, 2, 3), (1, 2) \rangle \simeq S_3$  and  $H = \langle (1, 2, 3, 4), (1, 3) \rangle \simeq D_4$ ; see Section 8.1. Now  $H \cap K_1 = V$ ,  $H \cap K_2 = \langle e \rangle$  and so the RHS equals  $V$  and  $V < H$ .

(iii) Using the factor group definition we have

$$N_{G/K}(KP/K) = KN_G(KP)/K.$$

Now  $P$  is a Sylow  $p$ -subgroup of  $KP$ , as  $(o(K), p) = 1$ , and  $KP \triangleleft N_G(KP)$ . Hence the Frattini Argument (Theorem 6.14) gives

$$N_G(KP) = KPN_{N_G(KP)}(P) = KPN_G(P) = KN_G(P);$$

Use a conjugation argument for the second inequality, and  $P \leq N_G(P)$  for the third. Now combine identities.

(iv) Put  $K_1 = K \cap H$ . By (iii)

$$N_{H/K_1}(K_1P/K_1) = K_1N_H(P)/K_1.$$

Using the Second Isomorphism Theorem (Theorem 4.15) this gives

$$K_1N_G(P)/K_1 = N_{G/K_1}(K_1P/K_1) = K_1N_H(P)/K_1,$$

which shows that

$$N_H(P) \leq N_G(P) \leq K_1N_H(P).$$

The result now follows by Problem 2.18(ii).

**Problem 6.22** (i) Note that  $g^{-1}P_i g$  is a Sylow  $p$ -subgroup by Sylow 2, and if  $g^{-1}P_i g = g^{-1}P_j g$  then  $P_i = P_j$ . Also  $gh\theta = g\theta h\theta$  as  $g^{-1}(h^{-1}P_i h)g = (hg)^{-1}P_i(hg)$ , and so  $\theta$  is a homomorphism. Now  $g \in \ker \theta$  if and only if  $g\theta$  is the identity perm. So  $g^{-1}P_i g = P_i$  for all  $i$ , that is  $g \in N_G(P_i)$  for all  $i$ . Therefore  $\ker \theta = \bigcap_i N_G(P_i)$ .

(ii)  $D_n$  has  $n$  Sylow 2-subgroups (see Problem 6.8(ii)), each isomorphic to  $C_2$ . So  $n_2 = n$ , which gives  $N_G(P_i) = P_i$ , and the intersection is  $\langle e \rangle$ , that is  $\theta$  is injective and there is a copy of  $D_n$  in  $S_n$ .

**Problem 6.23** (a) The group  $GL_2(3)$  has one element of order 1, thirteen of order 2, eight of order 3, six of order 4, eight of order 6, and twelve of order 8.

(b) To show that  $H$  is a subgroup either use direct calculation, or note that if we put (for example)  $a = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$  and  $b = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$ , then  $a^2 = b^2 = (ab)^2$  which are the defining equations of the quaternion group  $Q_2$ . It is normal because the order of a conjugate of an element of order 2 or 4 is itself an element of order 2 or 4.

(c)  $GL_2(3)$  has 32 elements whose orders are a power of 2, so by the Sylow theory, this group has three Sylow 2-subgroups and, by Problem 6.8(i),  $H$  is a subgroup of each of them. Choose an element of order 8 and its powers, add to  $H$ , and by direct calculation show that a subgroup of order 16 results. This can be done twice more.

(d) Now show that the group has three Sylow 2-subgroups each of which has a presentation of the form

$$\langle a, b \mid a^8 = b^2 = e, bab = a^3 \rangle,$$

these subgroups are called *semi-dihedral*. The three values of  $a$  can be taken as  $\begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}$ ,  $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$  and  $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ , and the three values of  $b$  are then  $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ ,  $\begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}$  and  $\begin{pmatrix} 2 & 0 \\ 2 & 1 \end{pmatrix}$ , respectively.

(e) Three pairs of order 4 elements of  $K$  with suitably chosen elements of order 2 give three copies of  $D_4$ , with similar calculations for copies of  $D_3$  and  $D_6$  (Problem 5.19). Hence the 55 subgroups are:  $\langle e \rangle$ , thirteen copies of  $C_2$ , four of  $C_3$ , three of  $C_4$ , three of  $C_6$ , three of  $C_8$ , six of  $C_2 \times C_2$ , eight of  $D_3$ , three of  $D_4$ , four of  $D_6$ , one of  $Q_2$ , one of  $SL_2(3)$  (see Section 8.2), the three semi-dihedral subgroups mentioned above, and the group itself. The only non-neutral proper normal subgroups are the centre (isomorphic to  $C_2$ ),  $H$  and  $SL_2(3)$  (Problem 2.19).

## Solutions 7

**Problem 7.1** (i) – Lemma 7.5. (i) and (ii) follow from the definitions; if  $h$  and  $j$  do not commute in  $H_1$ , say, then  $(h, e, \dots, e)$  and  $(j, e, \dots, e)$  do not commute in the product, and vice versa. For (iii) use the isomorphism given by the map  $(j, (k, l)) \mapsto ((j, k), l)$  for  $j \in J, k \in K$  and  $l \in L$ ; a similar argument applies in (iv). For (v) let  $\phi_i$  be defined by  $(h_1, \dots, h_n)\phi_i = h_i$  and proceed as in the proof of Lemma 7.2.

(i) – Theorem 7.6. Follow the proof of Theorem 7.4 by showing that if  $g \in G$ , then  $g$  has the unique representation:  $g = h_1 \dots h_n$  where  $h_i \in H_i$ , and also the order of the terms in this product is unimportant (consider each pair  $\{H_i, H_j\}$  in turn). Now as in the proof of Theorem 7.4, define  $\psi$  by  $g\psi = h_1 \dots h_n$  and proceed as before.

(ii) You only need to check condition (iii) and this follows by Lagrange's Theorem (Theorem 2.27).

**Problem ♦ 7.2** (i) Expand  $[(a, b), (c, d)] = (a, b)^{-1}(c, d)^{-1}(a, b)(c, d) = (a^{-1}c^{-1}ac, b^{-1}d^{-1}bd) = ([a, c], [b, d])$ , and use this to define an isomorphism.

(ii)  $(e, e) \in H \times J$ , and if  $(h_1, j_1), (h_2, j_2) \in H \times J$ , then  $(h_1, j_1)^{-1}(h_2, j_2) = (h_1^{-1}h_2, j_1^{-1}j_2) \in H \times J$ , as  $H \leq G$  and  $J \leq K$ . Also  $(g, k)^{-1}(h, j)(g, k) = (g^{-1}hg, k^{-1}jk) \in H \times J$  as  $H \triangleleft G$  and  $J \triangleleft K$ .

Secondly, define a map  $\theta : G \times K \rightarrow G/H \times K/J$  by  $(g, k)\theta = (gH, kJ)$ . It is clearly surjective and

$$\begin{aligned} (g_1, k_1)(g_2, k_2)\theta &= (g_1g_2, k_1k_2)\theta = (g_1g_2H, k_1k_2J) = (g_1Hg_2H, k_1Jk_2J) \\ &= (g_1H, k_1J)(g_2H, k_2J) = (g_1, k_1)\theta(g_2, k_2)\theta \end{aligned}$$

using coset multiplication and properties of the direct product. Hence  $\theta$  is a homomorphism, and its kernel is  $\{(g, k) : (g, k)\theta = (H, J)\} = H \times J$ . The First Isomorphism Theorem gives  $(G \times K)/(H \times J) \simeq G/H \times K/J$ .

(iii) We have  $J \cap K \triangleleft G$ , so by the Correspondence Theorem (Theorem 4.16) we obtain  $J/(J \cap K), K/(J \cap K) \triangleleft G/(J \cap K)$ . Also  $J/(J \cap K) \cap K/(J \cap K) = \langle e \rangle$  (check elements). If  $g \in G$ , then  $g = jk$  for  $j \in J, k \in K$ , so

$$g(J \cap K) = jk(J \cap K) = j(J \cap K)k(J \cap K) \in (J/(J \cap K))(K/(J \cap K)),$$

and

$$(J/(J \cap K))(K/(J \cap K)) \simeq J/(J \cap K) \times K/(J \cap K).$$

**Problem 7.3** (i) If  $H \simeq J$ , identify  $H$  with  $J$  and let  $D = \{(h, h) : h \in H\}$ , note that  $(h^{-1}, e)(h, h) = (e, h)$ . For the converse use the Second Isomorphism Theorem (Theorem 4.15).

(ii) Use the same method as in the proof of Lemma 7.8 to show that  $H \times (J \cap L)$  is isomorphic to a subgroup of  $L$ . Then note that  $L = H(J \cap L)$ , for if  $l \in L$  then  $l \in G$ , and so  $l = hj$  where  $h \in H$  and  $j \in J$ . But  $h \in L$ , hence  $h^{-1}l = j \in L$ , and so  $j \in J \cap L$  and  $hj \in H(J \cap L)$ .

**Problem 7.4** (i) If  $n = 2$  and  $h_i, h'_i \in Z(H_i), i = 1, 2$ , then  $(h_1, h_2)(h'_1, h'_2) = (h_1 h'_1, h_2 h'_2) = (h'_1 h_1, h'_2 h_2) = (h'_1, h'_2)(h_1, h_2)$ . Now use induction.

(ii) Again suppose first  $n = 2$ , and let  $j_r \in H_1$  and  $k_r \in H_2$ , all  $r$ . As we have a direct product, each  $j_r$  commutes with every  $k_s$  and vice versa, so

$$\begin{aligned} [j_1 k_1, j_2 k_2] &= k_1^{-1} j_1^{-1} k_2^{-1} j_2^{-1} j_1 k_1 j_2 k_2 \\ &= j_1^{-1} j_2^{-1} j_1 j_2 k_1^{-1} k_2^{-1} k_1 k_2 = [j_1, j_2][k_1, k_2], \end{aligned}$$

now use this identity.

(iii) We have  $H_i, K \triangleleft G$ , so  $[H_i, K] \leq H_i \cap K \triangleleft G$ . Also as in (ii)  $[G, K] = [H_1, K] \dots [H_n, K]$ , and so this is a subgroup of  $(H_i \cap K) \dots (H_n \cap K) = G^*$ , say. So  $[K, K] \leq G^*$ , but  $K = K' = [K, K]$  which gives the result.

**Problem 7.5** (i) If  $\text{ex}(G)$  has prime factorisation  $\prod_i p_i^{s_i}$ , then for each  $i$  there exists  $h_i \in G$  with  $o(h_i) = p_i^{s_i} t_i$  for some  $t_i$  with  $(p_i, t_i) = 1$ . Let  $g_i = h_i^{t_i}$  then  $o(g_i) = p_i^{s_i}$ , so let  $g = \prod_i g_i$ , then  $o(g) = \text{ex}(G)$ .

(ii) By Problem 2.7, the element  $g$  constructed in (i) will act as a generator of  $G$  as its order equals  $o(G)$ .

(iii) If  $F$  is the given field, let  $r = \text{ex}(F^*)$  where  $F^*$  is the multiplicative group of  $F$ . By (i) the polynomial  $x^r - 1$  has at least  $r$  non-zero roots in the field, but it cannot have more by assumption.

**Problem 7.6** (i) Note first that there is a mistake in the statement of the problem: The subgroup  $J$  must be normal for the result to hold as the following example shows. Let  $G = \langle (1, 2, 3, 4), (1, 2) \rangle \simeq S_4$  and  $H = \langle (5, 6, 7), (5, 6) \rangle \simeq S_3$ , so  $G \times H \simeq S_4 \times S_3$ . If  $J = \langle (3, 4)(6, 7), (2, 3, 4)(5, 6, 7) \rangle$ , then  $J \simeq S_3$  and so it is not Abelian,  $J \leq G \times H$  but not normal, and  $J \cap G = J \cap H = \langle e \rangle$ .

Now suppose  $L = G \times H$  and  $J \triangleleft L$ , then  $[J, G] \leq J \cap G$  and  $[J, H] \leq J \cap H$ , and using Problem 2.17(iii) we obtain

$$[J, L] = [J, G][J, H] \leq (J \cap G)(J \cap H).$$

If either  $J \cap G$  or  $J \cap H$  is non-neutral then we are done, otherwise  $[J, L] = \langle e \rangle$  which implies that  $J$  is Abelian.

(ii) Let  $G = \langle a_1 \rangle \times \dots \times \langle a_5 \rangle$ , a direct product of five copies of  $C_p$ , and let  $H_1 = \langle a_1, a_2 a_3 \rangle$ ,  $H_2 = \langle a_2, a_3 \rangle$  and  $H_3 = \langle a_4, a_5 \rangle$ . The direct product of the  $H_i$  has order  $p^6$ , and so not isomorphic to  $G$ .

**Problem ♦ 7.7** (a) Given  $r$  and  $s$  with  $r \leq s$ , the group  $C_{p^s} = \langle x \rangle$  has a subgroup of order  $p^r$  which is cyclic, and generated by  $x^{p^{s-r}}$  (by Theorem 4.20); and (b) if  $H_i \leq G_i, i = 1, \dots, k$ , with each  $G_i$  Abelian of order  $p_i^{s_i}$ , then

$$H_1 \times \dots \times H_k \leq G_1 \times \dots \times G_k.$$

So, if  $n = p_1^{s_1} \dots p_k^{s_k}, m = p_1^{r_1} \dots p_k^{r_k}$ , and  $r_i \leq s_i$  for  $i = 1, \dots, k$ , we obtain a subgroup of order  $m$  by (b) and the Basis Theorem of Finite Abelian Groups (Theorem 7.12) *provided* for each  $i$  we can find a subgroup  $J_i$  of order  $p_i^{r_i}$  in

an Abelian group  $K_i$  of order  $p_i^{s_i}$ .

Fix  $p_i = p$ , and suppose  $G$  is an Abelian group of order  $p^s$ . By Theorem 7.12  $G \simeq C_1 \times \cdots \times C_v$  where  $C_i$  is cyclic,  $o(C_i) = p^{u_i}$ , and  $u_1 + \cdots + u_v = s$ . We need to find  $H$  to satisfy:  $H \leq G$  and  $o(H) = p^r$  for some  $r \leq s$ . Choose  $x_1, \dots, x_v$  such that for all  $i$ ,  $0 \leq x_i \leq u_i$  and  $x_1 + \cdots + x_v = r$ , there may be many such solutions, and so many different  $H$ .

By (a) if  $C_i$  is cyclic with order  $p^{u_i}$ , then it has a cyclic subgroup  $C'_i$  of order  $p^{x_i}$ , and (by (b))  $C'_1 \times \cdots \times C'_v \leq C_1 \times \cdots \times C_v$ , with  $o(C'_1 \times \cdots \times C'_v) = p^r$  and  $o(C_1 \times \cdots \times C_v) = p^s$ .

**Problem 7.8** (i) First  $385 = 5 \cdot 7 \cdot 11$ , and so there is only one Abelian group:  $C_{385}$ . Secondly  $432 = 2^4 \cdot 3^3$ . As  $4 = 3+1 = 2+2 = 2+1+1 = 1+1+1+1$ , there are five Abelian groups of order 16:  $C_{2^4}$ ,  $C_{2^3} \times C_2$ ,  $C_{2^2} \times C_{2^2}$ ,  $C_{2^2} \times C_2 \times C_2$  and  $C_2 \times C_2 \times C_2 \times C_2$ . Similarly as  $3 = 2+1 = 1+1+1$ , there are three Abelian groups of order 27:  $C_{27}$ ,  $C_9 \times C_3$ , and  $C_3 \times C_3 \times C_3$ . Hence there are 15 Abelian groups of order 432:  $C_{16} \times C_{27}$ ,  $\dots$ . For example  $C_{72} \times C_6$  occurs in this list as  $C_{72} \simeq C_8 \times C_9$  and  $C_6 \simeq C_2 \times C_3$ , hence  $C_{72} \times C_6 \simeq C_8 \times C_2 \times C_9 \times C_3$ .

(iia) As  $891 = 3^4 \cdot 11$ , the Sylow theory gives

$$n_3 \equiv 1 \pmod{3}, \quad n_3 \mid 11, \quad \text{and} \quad n_{11} \equiv 1 \pmod{11}, \quad n_{11} \mid 81,$$

which in turn give  $n_3 = n_{11} = 1$ . Hence a group  $G$  with order 891 has normal subgroups  $J$  of order 81 and  $K$  of order 11. Clearly  $J \cap K = \langle e \rangle$  for  $J$  only contains elements which have order a power of 3, and  $K$  only contains elements of order 11. Also  $JK = G$ , for by Theorem 5.8,  $o(J \cap K)o(JK) = o(J)o(K)$  which shows that  $o(JK) = o(G)$ . Now apply Theorem 7.4.

(iib) Here  $405 = 3^4 \cdot 5$ , and as above  $n_3 = 1$ , but  $n_5 = 1$  or 81. If  $n_5 = 1$ , we obtain 14 direct product groups as in (i); and if  $n_5 = 81$  there is one possible further group isomorphic to:  $C_5 \rtimes C_3^4$ . If  $C_5$  is generated by  $a$ , then the 320 elements of order 5 are  $a^r b$  where  $r = 1, 2, 3$  or 4, and  $b$  is an element of  $C_3^4$  (all  $b$  have order 3 and there are 80 of them). Note that the Sylow theory implies that  $n_3 = 1$  in this group. You need to show that if  $G \simeq C_5 \rtimes H$ , where  $H$  is a normal subgroup of  $G$  with order 81, then  $H$  is Abelian and all elements have order 3. One way to do this is to use Theorem 11.11, in fact this group only has one non-neutral proper normal subgroup.

**Problem 7.9** If there is a unique maximal subgroup use Problem 2.13(ii). If not, by Theorem 7.8  $G$  is a direct product of its Sylow subgroups, there cannot be more than two factors because the maximal subgroups are simple. Now use the fact that the only simple  $p$ -groups are the cyclic  $p$ -groups.

**Problem 7.10** Suppose  $\phi \in \text{Aut } G$  and  $\psi \in \text{Aut } H$ . For  $(g, h) \in G \times H$  define  $\theta_{\phi, \psi}$  by

$$(g, h)\theta_{\phi, \psi} = (g\phi, h\psi) \quad \text{for } g \in G, h \in H.$$

This is an automorphism of  $G \times H$ , for it is bijective as  $\phi$  and  $\psi$  are bijective, and

$$\begin{aligned}
((g, h)(g', h'))\theta_{\phi, \psi} &= (gg'\phi, hh'\psi) = (g\phi, h\psi)(g'\phi, h'\psi) \\
&= (g, h)\theta_{\phi, \psi}(g', h')\theta_{\phi, \psi}.
\end{aligned}$$

Now define  $\xi : \text{Aut } G \times \text{Aut } H \rightarrow \text{Aut } (G \times H)$  by  $(\phi, \psi)\xi = \theta_{\phi, \psi}$ . This is a homomorphism for we have

$$\begin{aligned}
(g, h)\theta_{\phi\phi', \psi\psi'} &= (g\phi\phi', h\psi\psi') = ((g\phi)\phi', (h\psi)\psi') = (g\phi, h\psi)\theta_{\phi', \psi'} \\
&= [(g, h)\theta_{\phi, \psi}]\theta_{\phi', \psi'} = (g, h)[\theta_{\phi, \psi} \circ \theta_{\phi', \psi'}],
\end{aligned}$$

for all  $g \in G$  and  $h \in H$ . Also  $\xi$  is easily seen to be injective as  $\phi$  and  $\psi$  have this property, and for surjectivity we argue as follows. For  $\chi \in \text{Aut } (G \times H)$  we need  $\phi_1 \in \text{Aut } G$  and  $\psi_1 \in \text{Aut } H$  to satisfy  $(g, h)\chi = (g\phi_1, h\psi_1)$  for all  $g \in G$  and  $h \in H$ . Now  $(g, h)\chi^{o(H)} = (g\phi^{o(H)}, h\psi^{o(H)})$  and  $h\psi^{o(H)} = e$  for all  $h \in H$ . But  $(o(G), o(H)) = 1$  and so  $\phi^{o(H)}$  is an automorphism of  $G$  and we can define  $\phi_1$  by  $g\phi_1 = (g, e)\chi^{o(H)}$ . The automorphism  $\psi_1$  can be defined similarly which gives the required surjectivity property.

**Problem 7.11** (i) Suppose  $c \in G$ ,  $o(c) = m$  and  $m \nmid n$ . Show that  $o(gc) = \text{LCM}(m, n) > n$ , and so obtain a contradiction.

(ii) For example in  $S_3$  the largest order is 3, but this group also contains elements of order 2;  $S_4$  is another example.

(iii) If  $g \notin J$ , then  $\langle J, g \rangle$  intersects non-neutrally with  $H$  giving the required  $h, j$  and  $r$ .

(iv) The second statement follows from the first by Theorem 7.4. For the converse, suppose  $H \times J < G$ , choose an element of order  $p$  in  $G/(H \cap K)$  and apply (iii).

(v) Let  $H = \langle g \rangle$  and  $J$  be as in (iii).

**Problem 7.12** Suppose  $G$  is CS and let  $H = \{g \in G : g^p = e\} \leq G$  where  $p \mid o(G)$ . If  $\theta \in \text{Aut } G$  and  $h \in H$ , then  $(h\theta)^p = (h^p)\theta = e$  and  $H \text{ char } G$ . By Cauchy's Theorem (Theorem 6.2), there exists  $g \in H$  with  $o(g) = p$  and so  $g \in H$  and  $H \neq \langle e \rangle$ . But  $G$  is CS and so  $G = H$ . For the converse suppose now  $G$  is elementary. By Problem 4.18 we can treat  $G$  as a vector space over the field  $\mathbb{F}_p$  for some prime  $p$ . In fact  $G$  has the representation  $G \simeq C_p \times \cdots \times C_p$  with a finite number of factors. If  $J$  is a non-neutral subgroup of  $G$ ,  $j \in J$  and  $l \in G$  where  $j, l \neq e$ , then there exists an invertible linear map  $\phi$  on the vector space  $G$  with  $l = j\phi$ . But  $\phi \in \text{Aut } G$  and  $J \text{ char } G$ . Hence we have  $G$  has the property CS.

**Problem 7.13** We are given  $G = Q_2 \times T \times O$ , so if  $H \leq G$ , Lemma 7.8 implies

$$H = ((Q_2 \times T) \cap H) \times (O \cap H).$$

Now  $O \triangleleft G$  (by properties of the direct product), so we may suppose  $G = Q_2 \times T$ , a 2-group. If  $Q_2 \cap H = \langle e \rangle$ , then all elements of  $H$  have order 2, and hence  $H \triangleleft G$  by Problem 4.18(iii). If  $Q_2 \cap H > \langle e \rangle$ , then  $H \geq Q'_2 = G'$  (as the derived subgroup of  $Q_2$  equals its centre and has order 2) which implies that  $H \triangleleft G$  by Problem 2.16(iii).

**Problem ♦ 7.14** (i) Clearly  $\langle a_1, \dots, a_k \rangle = \langle a_1 \rangle \cdots \langle a_k \rangle$ , and the subgroups are normal because the group is Abelian. The condition

$$\langle a_i \rangle \cap \langle a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_k \rangle$$

is equivalent to the given condition.

(ii) All  $a \in G$  where  $a \neq e$  satisfy  $o(a) = p$ , so  $o(\langle a \rangle) = p$ , also if  $a_i, a_j \in G$ ,  $\langle a_i \rangle \cap \langle a_j \rangle$  equals  $\langle e \rangle$  or  $\langle a_i \rangle$ , now use (i) and Problem 4.18.

**Problem 7.15** (i) Note that as  $G$  and  $H$  are elementary they can be treated as vector spaces over  $\mathbb{Z}/p\mathbb{Z}$ , see Problem 4.18.

(ii) Let  $D_k$  be the direct product of all of the cyclic factors  $C_i$  of order  $p^k$  where  $D_k = \langle e \rangle$  if there are no such factors. So  $G \simeq D_1 \times \cdots \times D_t$  for some integer  $t$ , and further  $p^k G = p^k D_{k+1} \times \cdots \times p^k D_t$ . This gives  $p^k G / p^{k+1} G \simeq p^k D_{k+1} \times p^k D_{k+2} / p^{k+1} D_{k+2} \times \cdots$ , and now we can use (i).

(iii) Use (ii).

(iv) If  $\phi : G \rightarrow H$  is an isomorphism, then  $(p^k G)\phi = p^k H$ , and we can apply the Correspondence Theorem (Theorem 4.16). Reverse argument for converse.

(v) We have (a) if  $\theta : G \rightarrow H$  is a homomorphism then, for all  $p$ ,  $G_p \theta$  is a subgroup of  $H_p$ ; and (b)  $G \simeq H$  if and only if  $G_p \simeq H_p$  for all primes  $p$ . These facts give the result; the condition is:

$$U_p(k, G) = U_p(k, H) \quad \text{for all } p \text{ and } k.$$

For more details see Rotman [1994], pages 131 to 133.

**Problem ♦ 7.16** We have  $K \triangleleft J$  as  $K \triangleleft G$ ,  $A \cap J \leq J$  and  $(A \cap J) \cap K = \langle e \rangle$ , as  $A \cap K = \langle e \rangle$ , so  $(A \cap J) \rtimes K$  exists and is isomorphic to a subgroup of  $J$ . Suppose  $j \in J \setminus (A \cap J) \rtimes K$ , then  $j = ak$ ,  $a \in A$  and  $k \in K$  as  $J \in A \rtimes K$ . Hence  $a = jk^{-1}$ , but  $a \in A$  so  $a \in A \cap J$ . Therefore as  $k \in K$  we have  $j = ak \in (A \cap J) \rtimes K$ ; a contradiction.

**Problem 7.17** (i) We have  $C_{15} \simeq C_5 \times C_3$ , a direct product so *a fortiori* a semi-direct product.

(ii)  $A_4 \triangleleft S_4$ ,  $C_2 \simeq \langle (1, 2) \rangle \leq S_4$ ,  $A_4 \langle (1, 2) \rangle = S_4$  as  $o(A_4 \langle (1, 2) \rangle) > o(A_4)$  (Problem 2.19), and  $A_4 \cap \langle (1, 2) \rangle = \langle e \rangle$ ; hence  $S_4 \simeq C_2 \rtimes A_4$ .

(iii)  $Q_2$  is not a semi-direct product. Each pair of non-neutral subgroups has non-neutral intersection, because every non-neutral subgroup of  $Q_2$  contains the unique element of order 2 in  $Q_2$ ; see page 119.

(iv) Let  $A = \langle \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{Q}^* \rangle$  and  $K = SL_2(\mathbb{Q})$ . Then we have  $A \leq GL_2(\mathbb{Q})$ ,  $K \triangleleft GL_2(\mathbb{Q})$  by Theorem 3.15,  $A \cap K = \langle e \rangle$  and also  $AK = GL_2(\mathbb{Q})$  for if  $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Q})$  and  $\det X = t$ , then  $Y = \begin{pmatrix} a/t & b/t \\ c & d \end{pmatrix} \in SL_2(\mathbb{Q})$  and  $\begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix} Y = X$ . Hence  $GL_2(\mathbb{Q}) \simeq A \rtimes K$ .

(v) We gave a representation of  $S_4$  as a semi-direct product in (ii), another is as follows. Let  $V = \{e, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$  then  $V \triangleleft S_4$ ; see Problem 3.3. Also the set  $S$  of perms. on the set  $\{1, 2, 3\}$  forms a subgroup



of  $S_4$  isomorphic to  $S_3$ , that is  $S \leq S_4$ , and clearly  $S \cap V = \langle e \rangle$ . Hence  $S_4 \simeq S \rtimes V$ . For further examples see Chapter 8, but  $C_{15} \times C_2 \simeq C_5 \times C_6$  is another, perhaps slightly trivial, example.

**Problem 7.18** Let  $H = \langle a \rangle$ . As  $H\phi = H\psi$ ,  $a\phi$  and  $a\psi$  are generators of the same (cyclic) subgroup of  $\text{Aut } J$ . So there exist  $r, s \in \mathbb{Z}$  satisfying  $(a\phi)^r = a\psi$  and  $(a\psi)^s = a\phi$ . As  $H$  is cyclic and  $\phi$  and  $\psi$  are homomorphisms, these give  $(h^a)\phi = h\psi$  and  $(h^b)\psi = h\phi$  for all  $h \in H$ . Define  $\theta : H \rtimes_\psi J \rightarrow H \rtimes_\phi J$  by  $(h, j)\theta = (h^a, j)$ . Using the semi-direct product operation we have

$$\begin{aligned} ((h_1, j_1)(h_2, j_2))\theta &= (h_1 h_2, (j_1(h_2\psi))j_2)\theta = ((h_1 h_2)^a, (j_1(h_2\psi))j_2) \\ &= (h_1^a h_2^a, (j_1(h_2^a\phi))j_2) = (h_1^a, j_1)(h_2^a, j_2) \\ &= (h_1, j_1)\theta(h_2, j_2)\theta. \end{aligned}$$

We also have  $\theta' : H \rtimes_\phi J \rightarrow H \rtimes_\psi J$ , defined by  $(h, j)\theta' = (h^b, j)$ , is a homomorphism. Now  $\theta \circ \theta' : (h, j) \mapsto (h^{ab}, j)$ , and  $a\phi = a\psi^s = (a^{rs})\phi$ , so as  $\phi$  is injective,  $a^{rs} = a$  and hence  $h^{rs} = h$  for all  $h \in H$ . This shows that  $\theta \circ \theta'$  is the identity map on  $H \rtimes_\phi J$ , and similarly we have  $\theta' \circ \theta$  is the identity map on  $H \rtimes_\psi J$ , and the result follows.

**Problem 7.19** (i) Use the hint to show that  $G^* \triangleleft \text{Hol}(G)$  from which we also obtain  $\text{Hol}(G) = G^* \text{Aut } G$ . Now  $\xi_a \in \text{Aut } G$  if, and only if,  $a = e$  (note  $\xi_a$  is an isomorphism only if  $a = e$ ). So  $G^* \cap \text{Aut } G = \langle e \rangle$ , and we have a semidirect product.

(ii)  $\text{Hol}(C_n) = C_n$  if  $n = 1, 2$ ,  $\text{Hol}(C_n) \simeq D_n$  if  $n = 3, 4$  or  $6$ , and  $\text{Hol}(C_5)$  is isomorphic to the group of order 20 given in the quoted problem.

**Problem 7.20** The group  $C_4$  has two automorphisms: the identity map, and the map  $x \mapsto x^3$  which interchanges the two elements of order 4. So we obtain two semi-direct products. The first is  $C_4 \times C_4$  with three elements of order 2 and twelve of order 4, and 14 proper subgroups:  $\langle e \rangle$ , three of order 2, seven of order 4 (six of which are cyclic), three isomorphic to  $C_4 \times C_2$ .

For the second group  $H$  if we take  $a, b$  as the generators, we have using the semi-direct product construction  $a^4 = b^4 = e$ ,  $a^r b^s = b^s a^r$  if  $2 \mid rs$ , and  $a^r b^s = b^{3s} a^r$  if  $2 \nmid rs$ . The non-neutral elements of  $H$  are:

$$\begin{aligned} &a^2, b^2, ab, ab^3, a^3b, a^2b^2, a^3b^3 \text{ [order 2], and} \\ &a, b, a^3, b^3, ab^2, a^2b, a^2b^3, a^3b^2 \text{ [order 4].} \end{aligned}$$

There are 23 subgroups ( $\langle e \rangle$ , seven of order 2, four cyclic of order 4, seven of type  $T_2$ , three of order 8, and  $H$ ), all are Abelian except  $H$  itself, eleven are normal, the centre is  $\langle a^2, b^2 \rangle$ , with order 4, and the three of order 8 are:  $\langle a, b^2 \rangle$ ,  $\langle a^2, b \rangle$  ( $\simeq C_4 \times C_2$ ) and  $\langle a^2, b^2, ab \rangle$  which is elementary Abelian. One presentations of  $H$  is

$$\langle a, b \mid a^4 = b^4 = e, b^3 a = ab \rangle,$$

see Problem 8.12.

**Problem 7.21** By the Sylow theory and Theorem 6.9,  $G$  has a unique normal cyclic subgroup  $P$  of order  $q$ , either 1 or  $q$  cyclic subgroups of order  $p$  each of which have intersection  $\langle e \rangle$  with  $Q$ . If  $J$  is a subgroup of order  $p$ , by Lagrange's Theorem (Theorem 2.27),  $G = PJ$ , and so  $G \simeq J \rtimes P$ . If there is only one subgroup  $J$ , it is normal (by the Sylow theory), and so  $G$  is the direct product of  $J$  and  $P$  and, as both of these are cyclic,  $G \simeq C_{pq}$  by Theorem 7.6. Also by the Sylow theory,  $G$  can only have  $q$  subgroups  $J$  if  $p \mid q - 1$ . So you have to show that if this condition is satisfied, then there can only be one non-Abelian group (up to isomorphism) of order  $pq$ .

Using the semi-direct product theory you need to consider the possible homomorphisms  $\xi$  from  $J \simeq C_p$  to  $\text{Aut } P \simeq C_{q-1}$ . If the condition above was not satisfied the only possible homomorphism would be the trivial one, and the product would be direct. As  $\text{Aut } P$  is cyclic, the image of  $J$  under  $\xi$  is the unique cyclic subgroup of order  $p$ . For uniqueness use Problem 7.18.

**Problem 7.22**  $G \simeq C_{12} : \langle e \rangle$ ,  $C_2$ ,  $C_3$ ,  $C_4$ ,  $C_6$ , and  $G$ ; all unique.

$G \simeq C_6 \times C_2 : \langle e \rangle$ ,  $C_2 - 3$  copies,  $C_3$ ,  $T_2$ ,  $C_6 - 3$  copies, and  $G$ .

$G \simeq D_6 : \langle e \rangle$ ,  $C_2 - 7$  copies,  $C_3$ ,  $T_2 - 3$  copies,  $C_6$ ,  $D_3 - 2$  copies and  $G$ . The centre is  $\langle a^3 \rangle$ , the derived subgroup is  $\langle a^2 \rangle$ , and the Fitting subgroup is  $\langle a \rangle$  (note that  $D_3$  is not nilpotent),

$G \simeq Q_8 : \langle e \rangle$ ,  $C_2$ ,  $C_3$ ,  $C_4 - 3$  copies,  $C_6$ , and  $G$ . The centre is  $\langle a^3 \rangle$ , the derived subgroup is  $\langle a^2 \rangle$ , and the Fitting subgroup is  $\langle a \rangle$ .

See Problem 3.10 for  $A_4$ ; the centre is  $\langle e \rangle$ , and the derived and Fitting subgroups are both isomorphic to the unique subgroup of order 4.

Subgroup lattice diagrams for these groups are given on pages 552 to 556.

**Problem 7.23** (a) In this case  $\langle a \rangle \cap \langle b \rangle = \langle e \rangle$ , and as  $\langle b \rangle$  is maximal, it is normal (Theorem 6.5). Hence  $G \simeq \langle a \rangle \rtimes \langle b \rangle$ .

(b) We have  $(aZ(G))^p = Z(G)$ ,  $a^p \in Z(G)$  with  $a^p \neq e$ ; and so  $a^p = b^{tp}$ .

(c) Replacement gives  $a^p = b^{-p}$  and we still have  $a \notin \langle b \rangle$ . By Problem 6.5,  $G' = Z(G)$ , and by Problem 2.17 we have  $(ab)^p = a^p b^p [b, a]^{p(p-1)/2} = e$ .

(d) Use (c).

(e) By the Sylow theory  $\text{Aut } C_{p^2}$  has a *unique* Sylow  $p$ -subgroup of order  $p$ . So there is an injective homomorphism from  $C_p \rightarrow \text{Aut } C_{p^2}$ , and any two such have the same image. Now use the quoted problem.

**Problem 7.24** Follow the method given. We have  $84 = 4 \cdot 3 \cdot 7$ ,  $n_3 \equiv 1 \pmod{3}$  and  $n \mid 28$  by the Sylow theory. Hence by hypothesis we have  $n_3 = 28$ . But then  $[G : N_G(P)] = 28$  if  $P$  is a Sylow 3-subgroup, hence  $N_G(P) = P = C_G(P)$  as  $P$  is Abelian. Therefore the main condition for Burnside's Normal Complement Theorem (Theorem 6.17) applies, and  $P$  has a normal complement  $J$  of order 28. Note also  $G$  has 56 elements of order 3, so only 28 of order different from 3. Further  $n_7 \equiv 1 \pmod{7}$  and  $n_7 \mid 12$  which shows that  $n_7 = 1$  and  $G$  has a unique (normal) subgroup  $K$  of order 7.

## Solutions 8

**Problem 8.1** (a) The largest factor groups are as follows:  $D_3$  for  $S_4$  (the smallest non-neutral normal subgroup is  $V$  with order 4);  $A_4$  for  $SL_2(3)$  (Problem 3.4); and  $D_6$  for  $E$ , note that  $\langle a^2 \rangle \triangleleft E$ .

(b) Centralisers. For  $S_4$  we have  $C(\langle(1, 2)\rangle) = \langle(1, 2), (3, 4)\rangle$ ,  $C(\langle(1, 2, 3)\rangle) = \langle(1, 2, 3)\rangle$ ,  $C(\langle(1, 2, 3, 4)\rangle) = \langle(1, 2, 3, 4)\rangle$  and  $C(\langle(1, 2)(3, 4)\rangle) = \langle(1, 4, 2, 3), (1, 2)\rangle \simeq D_4$ ; for  $SL_2(3)$  we have  $C(a^3) = SL_2(3)$  [the centre],  $C(a^2) = \langle a \rangle$  [order 6],  $C(ab) = \langle ab \rangle$ , and  $C(a) = \langle a \rangle$ ; and for  $E$  we have  $C(a^2) = E$  [the centre],  $C(a) = C(b) = C(c) = C(bc) = \langle a^2, bc \rangle \simeq C_6 \times C_2$ ,  $C(ac) = \langle ac \rangle$  and  $C(abc) = \langle abca^2 \rangle$  [order 4].

(c) Normalisers. In  $S_4$  we have

$$\begin{aligned} N(\langle(1, 2)\rangle) &= \langle(1, 2), (3, 4)\rangle, \\ N(\langle(1, 2, 3)\rangle) &= \langle(1, 2, 3), (2, 3)\rangle \simeq D_3, \\ N(\langle(1, 2, 3, 4)\rangle) &= N(\langle(1, 2), (3, 4)\rangle) = N(\langle(1, 2)(3, 4)\rangle) \\ &= \langle(1, 2, 3, 4), (2, 4)\rangle \simeq D_4, \end{aligned}$$

also  $\langle(1, 2, 3), (2, 3)\rangle$  and  $D_4$  are self-normalising, and the normalisers of  $V$  and  $A_4$  are both equal to  $S_4$ . For  $SL_2(3)$  we have  $N(\langle a^2 \rangle) = \langle a \rangle$ ,  $N(\langle ab \rangle) = Q_2$ ,  $\langle a \rangle$  is self-normalising, and the normalisers of  $\langle a^3 \rangle$  and  $Q_2$  are both equal to  $SL_2(3)$ . For  $E$  we have: all subgroups with a '1' in the diagram on page 180 have  $E$  as their normaliser,  $N(\langle b \rangle) = \langle a^2, bc \rangle$ ,  $N(\langle abc \rangle) = \langle abc, a^2 \rangle$ ,  $N(\langle ac \rangle) = N(\langle a^2, abc \rangle) = \langle ac, b \rangle$ ,  $N(\langle c, ab \rangle) = \langle a^2 c, ab \rangle$  [order 12],  $N(\langle bc \rangle) = \langle a^2, bc \rangle$ , and  $\langle ac, b \rangle$  is self-normalising.

**Problem ♦ 8.2** By Sylow 4,  $n_2 \equiv 1 \pmod{2}$  and  $n_2 \mid 3$ , and so  $n_2 = 1$  or 3. If it equals 1 the result follows, so suppose it is 3 and let  $P_1, P_2$  and  $P_3$  be the three Sylow 2-subgroups. By Theorem 5.8, if  $J = P_1 \cap P_2$ ,

$$o(P_1 P_2) o(J) = o(P_1) o(P_2), \quad (8.1)$$

and as  $P_1 P_2 \subseteq G$ , we have  $24o(J) \geq 64$ , or  $o(J) \geq 4$ . But  $o(J) < 8$  as  $P_1 \neq P_2$ , and so  $o(J) = 4$ . Now as the indices are 2, we have  $J \triangleleft P_1$  and  $J \triangleleft P_2$  (Problem 2.19). Also  $N_G(J)$  is the largest subgroup of  $G$  in which  $J$  is normal (Problem 5.13(i)), hence

$$P_1, P_2 \leq N_G(J), \quad \text{so} \quad \langle P_1, P_2 \rangle \leq N_G(J).$$

Further  $P_1 P_2 \subseteq \langle P_1, P_2 \rangle$  (note  $P_1 P_2$  is not a subgroup), and so by (8.1)  $o(\langle P_1, P_2 \rangle) \geq 16$ . But the largest proper subgroup of  $G$  has order at most 12, and so both  $\langle P_1, P_2 \rangle$  and  $N_G(J)$  equal  $G$ , and  $J \triangleleft G$ . In the examples discussed in this chapter  $V \triangleleft S_4$  where  $o(V) = 4$ ,  $Q_2 \triangleleft SL_2(3)$  where  $o(Q_2) = 8$ , and  $\langle a^2, b \rangle \triangleleft E$  where  $o(\langle a^2, b \rangle) = 4$ .

**Problem 8.3** (i) As  $ab = ba^2$  we have  $ab^2 = ba^2b = baba^2 = b^2a^4 = b^2a$ , and  $a^2b = aba^2 = ba$  which gives  $a^2b^2 = bab = b^2a^2$ . Hence  $b^2$  commutes with  $a$ , and the elements of the group are

$$e; b^4 [2]; a, a^2 [3]; b^2, b^6 [4]; ab^4, a^2b^4 [6];$$

$$b, b^3, b^5, b^7, ab, ab^3, ab^5, ab^7, a^2b, a^2b^3, a^2b^5, a^2b^7 [8]; ab^2, ab^6, a^2b^2, a^2b^6 [12],$$

where the figures in square brackets denote the orders of the elements or subgroups (see below).

(ii) *Subgroups* The cyclic subgroups are

$$\langle e \rangle, \langle b^4 \rangle [2], \langle a \rangle [3], \langle b^2 \rangle [4], \langle ab^4 \rangle [6], \langle b \rangle, \langle ab \rangle, \langle a^2b \rangle [8] \text{ and } \langle ab^2 \rangle [12].$$

There are no other proper non-neutral subgroups because the group has only one element of order 2, and three of order 4, and  $C_2 \times C_2, D_3, C_4 \times C_2, C_2 \times C_2 \times C_2, D_4, C_6 \times C_2, A_4, Q_3$  and  $D_6$  all have more than one element of order 2. Also  $Q_2$ , which has exactly one element of order 2, has six elements of order 4.

*Sylow subgroups* They are  $\langle a \rangle$  of order three, unique so normal; and  $\langle b \rangle, \langle ab \rangle, \langle a^2b \rangle$  cyclic of order eight, so not normal. Note all other subgroups are normal because  $b^2$  commutes with  $a$ .

(iii) *Centre*  $\langle b^2 \rangle$  with order four, and  $b^2$  commutes with  $a$ , but  $b$  does not commute with  $a$ .

*Derived subgroup*  $[a, b] = a^2b^7ab = a$  and  $[b, a] = a$ , so  $F'_{3,8} = \langle a \rangle$ .

(iv) *Semi-direct product* Let  $A = \langle b \rangle$  and  $K = \langle a \rangle$ , then  $F_{3,8} = AK, A \cap K = \langle e \rangle, A \leq F_{3,8}$  and  $K \triangleleft F_{3,8}$ . Also  $\text{Aut } K \simeq C_2 = \langle t \rangle$ , say, so there are two homomorphisms. The first (trivial) associates the identity automorphism with all elements of  $A$  (giving the direct product  $C_8 \times C_3$ ), and the second  $\gamma$ , say, maps  $b^{2k}$  to  $e$  and  $b^{2k+1}$  to  $t$ , and so  $b^ra^sb^ua^v = b^{r+u}(a^s(b^u\gamma))a^v$  which agrees with the product in  $F_{3,8}$ .

(v) *Frattini subgroup* The maximal subgroups are  $\langle b \rangle, \langle ab \rangle, \langle a^2b \rangle$  and  $\langle ab^2 \rangle$ , hence  $\Phi(G) = \langle b^2 \rangle$  with order 4.

*Fitting subgroup* The maximal normal cyclic (so nilpotent) subgroup is  $\langle ab^2 \rangle$  with order 12.

**Problem 8.4** (i) We have  $c = dcdcd$  and  $d = cdcdc$ , and so

$$d(cd)^{12} = (dcdcd)(cdcdc)(dcdcd)(cdcdc)(dcdcd) = cdcdc = d$$

which gives  $(cd)^{12} = e$  and so  $c^8 = d^8 = e$ .

(ii) We have  $(c^3d)^3 = (c^2cd)^3 = (cd)^{12} = e$ ,  $c(c^3d)c^{-1} = (cd)^8 = (c^3d)^2$ . These show that the elements of  $G$  are:

$$e; c^4; c^3d, d^3c; c^2, c^6; c^7d (= d^6cd), d^7c (= c^6dc) \\ c, d, c^3, d^3, c^5, d^5, c^7, d^7, cdc, c^3dc, c^5dc, c^7dc; cd, dc, c^5d, d^5c.$$

Note that  $c^7d = (cd)^{10}$  (use  $c = dcdcd$  three times) so  $(c^7d)^6 = (cd)^{60} = e$ , and  $(cdc)^8 = cdc^2 \cdots c^2dc = cd^{22}c = cd^6c = c(cd)^9c = c^8 = e$  *et cetera*. The orders of the elements in this list and that given in Problem 8.3 agree.

(iii) Map  $G \rightarrow F_{3,8}$  by setting  $a \mapsto c^3d$  and  $b \mapsto c$ , the calculations above give the relations of  $F_{3,8}$ , and as the orders agree we see that  $G \simeq F_{3,8}$ . The reverse map  $F_{3,8} \rightarrow G$  is given by  $c \mapsto b$  and  $d \mapsto b^5a$ .

Further  $F_{3,8} \leq S_{11}$  which follows if we set  $a \mapsto (9, 10, 11)$  and  $b \mapsto (1, 2, 3, 4, 5, 6, 7, 8)(9, 10)$ , or  $c = b$  and  $d \mapsto (1, 6, 3, 8, 5, 2, 7, 4)(9, 11)$ . We also have  $F_{3,8} \leq U_3(3)$ , see Chapter 12.

**Problem 8.5** (i) Consider involutions,  $S_4$  has two types: 2-cycles with six in all, and 2-cycles  $\times$  2-cycles with a total of three. An automorphism maps involutions to involutions, but also as the classes are different sizes (6 and 3) an automorphism must map 2-cycles to 2-cycles. Note further by Lemma 3.5 that  $S_4$  is generated by its 2-cycles. If the automorphism  $\theta$  maps  $(1, 2)$  to  $(i, j)$ , then this is given by the conjugation  $(1, i)(2, j)(1, 2)(1, i)(2, j) = (i, j)$  where if, for example,  $i = 1$  we treat  $(1, i)$  as the identity perm. This gives the result. For the general  $S_n$  case see Rotman [1994] page 158.

(ii) Using the given substitutions and the relations of the second presentation we have  $a^2 = (c_1a_1)^2 = e$ ,  $b^3 = a_1^6 = e$  and  $ab = c_1a_1^3 = c_1$  which gives  $(ab)^4 = e$ . Conversely again using the given substitutions and the relations of the first presentation we have  $a_1^3 = b^6 = e$ ,  $c_1^4 = (ab)^4 = e$ ,  $c_1a_1 = ab^3 = a$  so  $(c_1a_1)^2 = e$ ,

$$(b_1c_1)^2 = abab^2abab^2ab = abab(bababab)bab = (ab)^4 = e$$

as  $bababab = a$ ,

$$(a_1b_1)^2 = b^2abab^2b^2abab^2 = b^2(ab)^4b = b^3 = e,$$

and lastly

$$b_1^3 = abab(babab)(babab)b = abab(ab^2a)(ab^2a)b = (ab)^4 = e,$$

as  $a^2 = b^3 = e$  and  $babab = ab^2a$ .

**Problem 8.6** (i) We have as above  $a_1^3 = a^6 = e$ ,  $b_1a_1b_1 = b^4a^2b^4 = ba^2b$  and  $a_1b_1a_1 = a^2b^4a^2 = bab^6ab = ba^2b$  using  $a^2 = bab$ . Now using the permutation representation we see that  $a_1 \mapsto (3, 7, 6)(4, 8, 5)$  and  $b_1 \mapsto (1, 4, 6)(2, 3, 5)$  which after some checking gives  $a = b_1^2a_1b_1^2$  and  $b = a_1b_1^2a_1$ .

(ii) Clearly  $SL_2(3) \not\leq S_4$  (as  $Z(S_4) = \langle e \rangle$ ). Suppose  $SL_2(3) \leq S_5$ . A Sylow 2-subgroup of  $SL_2(3)$  is isomorphic to  $Q_2$ , and is a subgroup of a Sylow 2-subgroup,  $P$ , say, of  $S_5$  by Sylow 5. But  $P \simeq D_4 \not\cong Q_2$ . A similar argument applies for both  $S_6$  and  $S_7$  because in each case its Sylow 2-subgroups are isomorphic to  $D_4 \times C_2$ , and  $Q_2$  would form a normal subgroup of one of these. Remember that  $Q_2$  only has one element of order 2.

**Problem 8.7** We have seen that  $E \leq A_7$  and clearly  $A_7 \leq A_8$ . We also have  $A_8 \simeq L_4(2)$ , see Problem 12.13, hence  $E$  is isomorphic to a subgroup of  $L_4(2)$ . The three matrices at the top of the next page clearly belong to  $GL_4(2) \simeq L_4(2)$  and the satisfy the relations in the definition of the group  $E$  given by (8.6) on page 177.

$$A = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}.$$

**Problem 8.8** (i) We have  $a^5 = bab$  and  $b = aba$ , so the elements are  $a^r$  and  $a^r b$  for  $0 \leq r < 12$  where  $ba^r = a^{12-r}b$ . This gives one element of order 1, one of order 2, two of order 3, 14 of order 4, two of order 6 and four of order 12. There are 18 subgroups including:  $\langle a^s \rangle$  for  $s = 1, 2, 3, 4$  and 6,  $\langle a^s b \rangle$  for  $0 \leq s \leq 5$  all of which are cyclic,  $\langle a^3, a^t b \rangle \simeq Q_2$  for  $t = 0, 1, 2$ , and  $\langle a^2, a^u b \rangle \simeq Q_3$  for  $u = 0$  or 3. So all subgroups are either cyclic or dicyclic. The centre is  $\langle a^6 \rangle$ , of order 2, and the derived subgroup is  $\langle a^2 \rangle$  of order 6.

(ii) Follow the method given in the question.

**Problem 8.9** One way to study this group is by its representation

$$A_4 \times C_2 \simeq \langle (1, 2, 3), (1, 2)(3, 4)(5, 6) \rangle,$$

a subgroup of  $S_6$ . It also has the presentation:  $\langle a, b \mid a^3 = b^2 = [a, b]^2 = e \rangle$ , to see this map  $a \mapsto (1, 2, 3)$  and  $b \mapsto (1, 2)(3, 4)(5, 6)$ , then  $[a, b] \mapsto (1, 3)(2, 4)$ . The elements are:

$e$  – order 1;  
 $b, aba^2, a^2ba, a^2bab, aba^2b, ababa, (ab)^3$  – order 2;  
 $a, a^2, bab, ba^2b, (ab)^2, (ba^2)^2, (ba)^2, (a^2b)^2$  – order 3; and  
 $ab, ba, a^2b, ba^2, aba, a^2ba^2, babab, ba^2ba^2b$  – order 6;

so the group has elements of order 1, 2, 3 and 6 only. The element  $ababab = bababa$  maps to  $(5, 6)$ , and the set  $\{e, aba^2b, a^2bab, ababa\}$  forms a normal subgroup corresponding to  $V$  in  $A_4$ . The other normal (proper, non-neutral) subgroups are  $\bar{U} = \langle (5, 6) \rangle$ ,  $\langle V, (5, 6) \rangle$  and  $A_4$ . The maximal subgroups are  $A_4$ ,  $\langle V, (5, 6) \rangle$  and four of order six:  $\langle (5, 6), C \rangle$  where  $C$  is a 3-cycle in  $A_4$ . There are 26 subgroups in all in twelve conjugacy classes. The centre is  $\langle (ab)^3 \rangle$  with order 2, and the derived subgroup is  $V$ . Further note that

- (a) the group can be represented as:  $C_3 \rtimes C_2^3$ , see Problem 8.10;
- (b) it has a second permutation representation:  $\langle (1, 2, 3, 4, 5, 6), (1, 4) \rangle$  which is transitive a subgroup of  $S_6$ , and so it has a very different nature compared with one fixing one element of the underlying set; and
- (c) it is the only non-Abelian group of order 24 with no elements of order 4.

**Problem 8.10** Let  $K$  be the unique Sylow 3-subgroup, it is normal by Sylow 3. The Sylow theory also implies that  $G$  has at least one subgroup  $H$  of order 8. Clearly  $H \cap K = \langle e \rangle$  and  $G = HK$  (consider the orders). Hence  $G$  can be represented as a semi-direct product of  $H$  by  $K$ . There are five choices for  $H$  (see Section 6.1), and  $\text{Aut}(K) \simeq C_2$  (Theorem 4.23). Hence we can list all groups of order 24 with a unique Sylow 3-subgroup by listing all non-isomorphic semi-direct products of  $H$  by  $C_3 (\simeq K)$  where  $o(H) = 8$ . That is

we need to find all homomorphisms mapping  $H \rightarrow C_2 = \langle t \rangle$  where  $o(H) = 8$ . This further implies that we need to consider the (normal) subgroups of order 4 in the subgroups  $H$ . We consider each of these in turn, see Section 6.1. It will also help to refer to Lemma 7.15 and Theorem 7.17.

$H = C_8 = \langle a \rangle$ . Two homomorphisms: trivial (giving  $C_{24} \simeq C_8 \times C_3$ ), and  $\gamma_1$  where  $a^{2r}\gamma_1 = e$  and  $a^{2r+1}\gamma_1 = t$  (giving  $F_{3,8}$ , Problem 8.3).

$H = C_4 \times C_2 = \langle a \rangle \times \langle b \rangle$ . Three homomorphisms: trivial (giving  $C_{12} \times C_2$ ), second mapping elements of the cyclic subgroup of order 4 (of  $H$ ) to the identity automorphism (giving  $D_3 \times C_4$ ), and third mapping elements of the subgroup isomorphic to  $T_2$  to the identity automorphism (giving  $Q_3 \times C_2$ ).

$H = C_2 \times C_2 \times C_2 = \langle a \rangle \times \langle b \rangle \times \langle c \rangle$ . Four homomorphisms: trivial (giving  $C_6 \times C_2 \times C_2$ ), second mapping elements of a copy of  $T_2$  to the identity automorphism (giving  $D_6 \times C_2$ ); as  $H$  in this case has three subgroups all isomorphic to  $T_2$ , the third and fourth homomorphisms are similar and give rise to the same group  $D_6 \times C_2$ .

$H = D_4 = \langle a, b \mid a^4 = b^2 = e, ba = a^3b \rangle$ . Four homomorphisms: trivial (giving  $D_4 \times C_3$ ), second mapping elements of the cyclic subgroup of order 4 (of  $H$ ) to the identity automorphism (giving  $D_{12}$ ), third and fourth both mapping a copy of  $T_2$  (note  $D_4$  has two such subgroups) to the identity automorphism (both giving  $E$ ).

$H = Q_2 = \langle a, b \mid a^2 = b^2 = (ab)^2 \rangle$ . Four homomorphisms: trivial (giving  $Q_2 \times C_3$ ). Also in this case the subgroup  $H$  has three distinct cyclic subgroups of order 4 so we have three distinct automorphisms each mapping one of these cyclic subgroups to the identity automorphism, and also each give rise to the group  $Q_6$ .

**Problem 8.11** As the group  $G$  has four Sylow 3-subgroups,  $n_3 = 4$ , so by the Sylow theory if  $P$  is a Sylow 3-subgroup,  $o(N_G(P)) = 6$ . A group of order 6 has a unique normal subgroup of order 3, so the intersection of the normalisers of two Sylow  $p$ -subgroups has order 1 or 2. Hence by Theorem 5.15,  $G/\text{core}(N_G(P))$  is isomorphic to a subgroup of  $S_4$ , as  $[G : N_G(P)] = 4$ . If the core has order 1, then  $G$  is isomorphic to a subgroup of  $S_4$ . But it has order 24 and so is isomorphic to  $S_4$ .

If the core (Problem 1.24) of  $N_G(P)$  has order 2, then for a similar reason to that above  $G/\text{core}(N_G(P)) \simeq A_4$  because  $A_4$  is the only subgroup of  $S_4$  with order 12. Now  $A_4$  has a normal subgroup  $V$  of order 4, hence by the Correspondence Theorem (Theorem 4.16)  $G$  has a normal subgroup  $K$  of order 8. Therefore we can express  $G$  as a semi-direct product  $G \simeq P \rtimes K$  as  $P$  has order 3 and so has no non-neutral element in common with  $K$ . By the given fact  $K$  can only be isomorphic to two of the five possible groups of order 8, that is  $C_2^3$  or  $Q_2$ . Therefore finally we obtain two further groups of order 24, they are  $C_3 \rtimes C_2^3 \simeq A_4 \times C_2$  and  $C_3 \rtimes Q_2 \simeq SL_2(3)$ . For the first of these isomorphisms note that  $A_4$  can itself be expressed as a semi-direct product, for we have  $A_4 \simeq C_3 \rtimes C_2^2$  (Section 7.3 and Problem 8.9), and for the second we can use the results derived in Section 8.2.

**Problem 8.12** The main data are given in the following table where A stands for Abelian.

Group	Elts. of order 2;4;8	No. subgps. A;non-A	No. normal A;non-A	Max. subgps. All of order 8	Centre	Derived subgp.
$C_{16}$	1;2;4	5;0	5;0	$C'$	'G'	$\langle e \rangle$
$C_4 \times C_4$	3;12;0	15;0	15;0	$C'' - 3$	'G'	$\langle e \rangle$
$C_4 \rtimes C_4$	3;12;0	22;1	10;1	$C'' - 3$	$C_2^2$	$C_2$
$C_2 \times C_8$	3;4;8	11;0	11;0	$C' - 2, C''$	'G'	$\langle e \rangle$
$C_2 \rtimes_1 C_8$	3;4;8	10;1	8;1	$C' - 2, C''$	$C_4$	$C_2$
$D_8$	9;2;4	16;3	5;2	$C', D - 2$	$C_2$	$C_4$
$C_2 \rtimes_2 C_8$	5;6;4	12;3	4;3	$C', D, Q$	$C_2$	$C_4$
$Q_4$	1;10;4	8;3	4;3	$C', Q - 2$	$C_2$	$C_4$
$C_4 \times C_2^2$	7;8;0	27;0	27;0	$C' - 4, C'' - 2, C'''$	'G'	$\langle e \rangle$
$C_4 \rtimes C_2^2$	7;8;0	22;1	10;1	$C'' - 2, C'''$	$C_2^2$	$C_2$
$D_4 \times C_2$	11;4;0	30;5	14;5	$C'', C''' - 2, D - 4$	$C_4$	$C_2$
$Q_2 \times C_2$	3;12;0	14;5	14;5	$C'' - 3, Q - 4$	$C_4$	$C_2$
$F$	7;8;0	18;5	12;5	$C'' - 3, D - 3, Q$	$C_4$	$C_2$
$C_2^4$	15;0;0	67;0	67;0	$C''' - 15$	'G'	$\langle e \rangle$

*Notes.* The cyclic group  $C_{16}$  also has eight elements of order 16. The fourth to seventh groups are all semi-direct products of  $C_2$  by  $C_8$ ;  $C_8$  has four automorphisms  $\theta_i$  where  $a\theta_i = a^{2^i+1}$  for  $i = 0, 1, 2, 3$ ; see Problem 6.4 where it is shown that the fourth and fifth groups have identical subgroup lattices; see diagrams on pages 557 and 558. In the maximal subgroup column,  $C', C'', C''', D$  and  $Q$  stand for  $C_8, C_4 \times C_2, C_2^3, D_4$  and  $Q_2$ , respectively. Also (a) the group  $C_4 \rtimes C_4$  is discussed in Problem 7.20, (b)  $Q_2 \times C_2$  is 'Hamiltonian', see Problem 7.13, and (c) the group  $F$  can be taken as  $C_2 \rtimes D_4$  or  $C_2 \rtimes Q_2$ , see Problem 3.23.



## Solutions 9

**Problem 9.1** Use the facts that under the equivalence relation (a) the sets of factors are unordered and (b) two equivalent series have the same number of factors.

**Problem 9.2** (ia)  $\langle e \rangle \triangleleft C_2 \triangleleft V \triangleleft A_4 \triangleleft S_4$ , there are three different series as there are three possibilities for the second factor; see Section 8.1. (ib)  $\langle e \rangle \triangleleft C_2 \triangleleft C_2 \times C_2 \triangleleft A_4$ , again there are three possibilities; see Problem 3.10, (ic)  $\langle e \rangle \triangleleft C_2 \triangleleft C_4 \triangleleft Q_2 \triangleleft SL_2(3)$ , again three possibilities; see Section 8.2. (id)  $\langle e \rangle \triangleleft C_3 \triangleleft C_6 \triangleleft D_6 \triangleleft E$ , there are six others, see the diagram on page 180. Note that none of these series are normal series, see Problem 9.15.

(ii)  $C_6$  and  $S_3$  with factors  $C_2$  and  $C_3$ , is the smallest example, there are many others.

**Problem 9.3** Suppose the given composition series for  $G$  is  $\langle e \rangle \triangleleft H_1 \triangleleft \cdots \triangleleft H_m = G$ . By Problem 2.14, the series  $\langle e \rangle \cap K \triangleleft H_1 \cap K \triangleleft \cdots \triangleleft H_m \cap K = K$  is a subnormal series which, after the removal of redundant terms forms a composition series for  $K$ ; use Lemma 9.2 to check this. Also  $\langle e \rangle = \langle e \rangle K / K \triangleleft H_1 K / K \triangleleft \cdots \triangleleft H_m K / K = G / K$  can similarly be made into a composition series for  $G / K$ . Now using the Correspondence Theorem (Theorem 4.16) on  $G$  with normal subgroup  $K$  we can construct a subnormal series from  $K$  to  $G$ , and combining these two series gives the result.

**Problem 9.4** (i) If  $G$  is finite, use Theorem 9.3. If not, refer to the **Web Appendix** to Chapter 7. If  $G$  contains infinite order elements, it cannot have a composition series because  $\mathbb{Z}$  does not have one (if  $K \triangleleft \mathbb{Z}$  then  $\mathbb{Z}/K \simeq \mathbb{Z}$ ; see Theorem 4.19). If the group is countable and all elements have finite order, then infinite direct products are involved. So for example, the group  $C_p \times C_p \times \cdots$  with infinitely many factors  $C_p$  clearly does not have a composition series (which must have finite length).

A full proof of this result needs more facts about infinite Abelian groups than are given in the book; see for example Kaplansky [1969] for more information.

(ii) If  $C_{p^n} = \langle a \rangle$ , then the only composition series is

$$\langle e \rangle \triangleleft \langle a^{p^{n-1}} \rangle \triangleleft \langle a^{p^{n-2}} \rangle \triangleleft \cdots \triangleleft \langle a^p \rangle \triangleleft \langle a \rangle$$

with all factors isomorphic to  $C_p$ , see Problem 4.20.

(iii) If  $F$  is finite use Theorem 9.3(i), and if  $F$  is infinite then the argument used to show that  $\mathbb{Z}$  does not have a composition series can be applied.

(iv) Use **Web Problem 3.31**, the group  $A_{(\mathbb{N})}$  is simple, and so has a two term composition series, and  $\mathbb{Z}$  is a subgroup with no composition series.

**Problem ♦ 9.5** (i) If a composition series has the form  $\cdots \triangleleft G_i \triangleleft G_{i+1} \triangleleft \cdots$  where  $o(G_{i+1}/G_i) = pq \dots$  then, as the group is finite Abelian, we can insert a new term between  $G_i$  and  $G_{i+1}$  with a factor of order  $p$  contradicting the

definition of a composition series.

(ii) This is similar to (i) using Theorem 6.5.

**Problem 9.6** (i) Suppose  $G$  has two composition series:

$$\langle e \rangle \triangleleft H \triangleleft G \quad \text{and} \quad \langle e \rangle \triangleleft J \triangleleft G, \quad (9.2)$$

where  $H \neq J$ . Now  $H$  and  $J$  are simple by Theorem 9.3. By Lemma 9.2 we have  $\langle e \rangle \triangleleft H \cap J \triangleleft H$ , but both series in (9.2) are composition series, so  $H \cap J = \langle e \rangle$ , also by Problem 2.19 we have  $H \triangleleft HJ \triangleleft G$ , hence  $HJ = G$ . Now use Theorem 7.4. In fact this shows that  $G \simeq H \times J$ .

(ii) See for example Problem 9.4(ii) with  $n$  large.

**Problem 9.7** Refinements are  $\langle e \rangle \triangleleft pq\mathbb{Z} \triangleleft p\mathbb{Z} \triangleleft \mathbb{Z}$ , and  $\langle e \rangle \triangleleft pq\mathbb{Z} \triangleleft q\mathbb{Z} \triangleleft \mathbb{Z}$ , with factors isomorphic to  $pq\mathbb{Z}$ ,  $C_p$  and  $C_q$ .

**Problem ♦ 9.8** (i) If  $H \triangleleft H_1 \triangleleft \cdots \triangleleft G$  is a subnormal series from  $H$  to  $G$ , then by Lemma 4.14(i)  $H \cap J \triangleleft H_1 \cap J \triangleleft \cdots \triangleleft G \cap J = J$  is the required series.

(ii) Use (i).

(iii) Use the Correspondence Theorem (Theorem 4.16).

**Problem 9.9** (i) Use Definition 9.9 and Lagrange's Theorem (Theorem 2.27).

(ii) Use (i) and induction.

**Problem 9.10** (i) There are two cases: the direct product  $C_3 \times C_2 \times C_2$ , and  $D_6 = \langle a, b \mid a^6 = b^2 = e, bab = a^5 \rangle$ . In this second case  $\langle a^2 \rangle \simeq C_3 \triangleleft D_6$  and  $\langle a^3, b \rangle \simeq C_2 \times C_2$ . Note that  $C_3$  has only two automorphisms, and Theorem 9.17 applied in this case gives  $k_0 = e$ ,  $(a, b)\xi = e$  for all  $a, b$ , and so all extensions are semidirect.

**Problem 9.11** (i) This follows immediately from the Basis Theorem for Finite Abelian Groups (Theorem 7.12).

(ii) The group  $\mathbb{Z}$  has just two automorphisms: the identity map, and the 'minus map' where  $a \mapsto -a$ . Also in Theorem 9.17,  $k_0 = e$  and so all extensions are semidirect. Hence we obtain two extensions: the direct product  $\mathbb{Z} \times C_2$ , and the infinite dihedral group; see Problem 3.20. In this second case if we take  $\{0, 1\}$  with addition modulo 2 as a representation of  $C_2$ , the operation is given by:

$$\begin{aligned} (0, x)(0, y) &= (0, x + y), & (1, x)(0, y) &= (1, x + y), \\ (0, x)(1, y) &= (1, -x + y), & (1, x)(1, y) &= (0, -x + y) \end{aligned}$$

for all  $x, y \in \mathbb{Z}$ .

**Problem 9.12** Note that  $Q_2$  has three normal subgroups isomorphic to  $C_4$  and one isomorphic to  $C_2$ , so four possible definitions by extensions. In each case the intersection property for a semidirect product fails.

**Problem 9.13** (a) We have  $(e, e)(a, k) = (ea, (e, a)\xi \odot e\vartheta_a \odot k) = (a, k)$ .

(b) Using the definitions we have

$$(a, k)(a, k)^{-1} = (aa^{-1}, (a, a^{-1})\xi \odot k\vartheta_{a^{-1}} \odot ((a^{-1}, a)\xi)^{-1} \odot k^{-1})\vartheta_a^{-1} = (e, z),$$

say. Now as  $\vartheta_a$  is an automorphism, if  $z\vartheta_a = e$  then  $z = e$ . Applying  $\vartheta_a$  to  $z$  we obtain using (iii) in Definition 9.14 in the second line

$$\begin{aligned} z\vartheta_a &= ((a, a^{-1})\xi)\vartheta_a \odot k\vartheta_{a^{-1}}\vartheta_a \odot ((a^{-1}, a)\xi)^{-1} \odot k^{-1} \\ &= ((a, a^{-1})\xi)\vartheta_a \odot (((a^{-1}, a)\xi)^{-1} \odot k \odot (a^{-1}, a)\xi) \odot ((a^{-1}, a)\xi)^{-1} \odot k^{-1} \\ &= ((a, a^{-1})\xi)\vartheta_a \odot ((a^{-1}, a)\xi)^{-1} = e, \end{aligned}$$

using (ii) in Definition 9.14 with  $a_1 = a_3 = a$  and  $a_2 = a^{-1}$ .

**Problem 9.14** Suppose  $o(G) = pq$  where  $p < q$ , so  $G$  has a normal Sylow  $q$ -subgroup  $P$ , say, and 1 or  $q$  Sylow  $p$ -subgroups. In the first case  $G \simeq C_p \times C_q (\simeq C_{pq})$ . In the second case  $G$  is a cyclic extension of  $P$  by a subgroup of  $G$  with order  $p$ . But as  $(p, q) = 1$ , applying Theorem 9.17 we have  $k_0 = e$ , and so all extensions are semidirect. The theory will provide several but they are all isomorphic. Note that as  $o(\text{Aut}(P)) = q - 1$ , the condition  $p \mid q - 1$  is necessary for the map  $\psi$  in Theorem 9.17 to exist.

**Problem 9.15** (i) Use the fact that if  $G$  has a chief series,  $H$  and  $K$  are normal subgroups of  $G$ , and  $H < K$ , then  $K/H$  is a chief factor for  $G$  if and only if it is a minimal normal subgroup of  $G/K$ .

(ii) Use induction and the Correspondence Theorem (Theorem 4.16), there is little to prove if the group is simple.

(iii) Again use the Correspondence Theorem and a property of minimal normality.

(iv) Let  $K$  be a minimal normal subgroup of  $G$ , and  $H_1$  be a maximal normal subgroup of  $K$ , note  $K/H_1$  is simple. Further, let  $H_1, \dots, H_j$  be the conjugates of  $H_1$  in  $G$ ; each  $H_i$  is maximal normal in  $K$  as  $K \triangleleft G$ . Show that  $K/H_i$  are mutually isomorphic and, using a conjugation argument, show that

$$H_1 \cap \dots \cap H_j = \langle e \rangle.$$

Now using induction on  $i$  prove that  $K/(H_1 \cap \dots \cap H_i)$  is isomorphic to a direct product of copies of  $K/H_1$ . The result follows by putting  $i = r$ .

(va)  $\langle e \rangle \triangleleft V \triangleleft A_4 \triangleleft S_4$ , this has one less term than the corresponding composition series;

(vb)  $\langle e \rangle \triangleleft V \triangleleft A_4$ ;

(vc)  $\langle e \rangle \triangleleft C_2^2 \triangleleft C_2^3 \triangleleft A_4 \times C_2$ ;

(vd)  $\langle e \rangle \triangleleft \langle a^3 \rangle \triangleleft \langle ab, ba \rangle \triangleleft SL_2(3)$ ;

(ve)  $\langle e \rangle \triangleleft \langle c \rangle \triangleleft \langle a^2c \rangle \triangleleft \langle a, c \rangle \triangleleft E$ .

## Solutions 10

**Problem ♦ 10.1** We have if  $g \in \mathcal{Z}_{n+1}$ , then  $g\mathcal{Z}_n \in Z(G/\mathcal{Z}_n)$  which implies that  $g\mathcal{Z}_n$  commutes with  $a\mathcal{Z}_n$  for all  $a \in G$ , that is  $[a, g] \in \mathcal{Z}_n$ . This argument reverses.

**Problem 10.2** (i)  $S_4$  is centreless so its hypercentre is  $\langle e \rangle$ . The hypercentre for  $SL_2(3)$  is its centre, and for  $E$  it is  $\langle a^2, b \rangle \simeq C_2 \times C_2$  (and so not the centre); to prove these facts use Problem 10.1.

(ii) Suppose  $D_n = \langle a, b \mid a^n = b^2 = e, bab = a^{n-1} \rangle$ . If  $n = 2^k$  then  $o(D_n) = 2^{k+1}$ , so  $D_n$  is a 2-group, and hence nilpotent (Theorem 10.6). If  $n = 2^k r$  where  $r > 1$  is odd, then  $o(a^{2^k}) = r$ ,  $o(b) = 2$ , and  $ba^{2^k} = a^{2^k(u-1)}b$ . Now apply Theorem 10.9(ix). This second part can also be established by showing that the Sylow 2-subgroups are not normal and using Theorem 10.9(vii)

(iii) Use Problem 3.15(iv) and Definition 10.1, or see Robinson (1982), page 123.

(iv) By Definitions 10.1 and 10.5 we have  $\mathcal{D}_{n+1}(G) = [\dots [[G, G], G] \dots, G] = \langle e \rangle$ , ( $n+1$  copies of  $G$ ) if, and only if,  $G$  is nilpotent with class  $n$ .

**Problem 10.3** Elements of the group  $G$  can be treated as infinite sequences  $z = (g_1, \dots, g_i, \dots)$  where  $g_i \in H_i$  for all  $i$ , and  $g_i = e$  for all but finitely many positive integers  $i$ . The product is component-wise as in the finite direct case. As each  $g_i$  has order a power of  $p$ , each  $z$  also has an order which is a power of  $p$  because it only has finitely many non-neutral entries. Hence  $G$  is a  $p$ -group, and  $H_n$  is isomorphic to a subgroup of  $G$ . Now consider sequences with an element of  $H_n$  at the  $n$ -entry and  $e$  in all other entries.

Suppose  $G$  is nilpotent with class  $m$  and  $n > m$ . So we have a group of nilpotency class  $m$  with a subgroup of larger nilpotency class, that is  $n$ . But this is impossible for an easy extension of of Theorem 10.6(iii) shows that the nilpotency class of a subgroup cannot be larger than the nilpotency class of the group itself.

**Problem ♦ 10.4** (i) If the nilpotency class number  $r$  is 1, then  $G' = \langle e \rangle$ . If  $r > 1$ , then by the inductive hypothesis  $H/Z(H) = G/Z(G)$  which gives  $G = HZ(G)$ . Now using Problem 2.17 we have

$$G' = [HZ(G), HZ(G)] = H' \quad \text{and so} \quad G = HG' = HH' = H.$$

(ii) If the nilpotency class number is  $r$ , then

$$H \leq H\mathcal{Z}_1(G) \leq H\mathcal{Z}_2(G) \leq \dots \leq H\mathcal{Z}_r(G) = HG = G$$

is a subnormal series. Also  $H$  normalises  $H\mathcal{Z}_i(G)$  and  $\mathcal{Z}_{i+1}(G)$  normalises  $H\mathcal{Z}_i(G)$  because

$$[\mathcal{Z}_{i+1}, H\mathcal{Z}_i(G)] \leq [\mathcal{Z}_{i+1}(G), G] \leq \mathcal{Z}_i(G) \leq H\mathcal{Z}_i(G).$$

Now use Theorem 10.9.

**Problem ♦ 10.5** (i) For fixed  $g \in G$  we have  $a\theta = [g, a]$  for  $a \in G$ . Now  $ab\theta = g^{-1}b^{-1}a^{-1}gab$  and  $a\theta b\theta = g^{-1}a^{-1}gag^{-1}b^{-1}gb$ . These are equal if  $b^{-1}a^{-1}ga = a^{-1}gag^{-1}b^{-1}g$  or

$$(a^{-1}gag^{-1})b^{-1}(ga^{-1}g^{-1}a)b = [a, g^{-1}]b^{-1}[g^{-1}, a]b = e.$$

But  $G$  has nilpotency class 2, and so  $G' \leq Z(G)$  which implies that this equation is indeed true by Problem 2.17(i). Hence  $\theta$  is an endomorphism of  $G$ . Now clearly  $\ker \theta = C_G(g)$ , and therefore this centraliser is a normal subgroup of  $G$ .

(ii) Use the definitions and the proof methods applied in the derivation of Theorem 10.6.

(iii) If  $D_{2^n} = \langle a, b : a^{2^n} = b^2 = (ab)^2 = e \rangle$ , then the lower central series for  $D_{2^n}$  is

$$D_{2^n}, \langle a^2 \rangle, \langle a^4 \rangle, \dots, \langle a^{2^{n-1}} \rangle, \langle e \rangle$$

hence the nilpotency class is  $n$ .

**Problem 10.6** This can be done by repeating the proof of Theorem 10.4. In the first part replace  $\mathcal{D}_{r+1}$  by  $H_{r+1}$  and show that  $H_{r+1} \leq \mathcal{Z}_{s-r}$ , and in the second part replace  $\mathcal{Z}_t$  by  $H_t$  and show that  $\mathcal{D}_{(s+1)-t} \leq H_t$ .

**Problem ♦ 10.7** If  $G$  is nilpotent, then  $G/J$  is also nilpotent by Theorem 10.6(iv). Conversely if  $G/J$  is nilpotent, and  $H \leq G$ , then by Theorem 10.9(v) we have  $HJ/J \triangleleft G/J$ , and so  $HJ \triangleleft G$  by the Correspondence Theorem (Theorem 4.16). But as  $J \leq Z(G)$ , we also have  $H \triangleleft HJ$  which gives  $H \triangleleft G$ . The result now follows by using Theorem 10.9(v) again.

**Problem ♦ 10.8** As  $G$  is nilpotent, it is isomorphic to a direct product of  $p$ -groups, its Sylow  $p$ -subgroups, where  $p \mid n$  (Theorem 10.9). Also a  $p$ -group of order  $p^r$  has subgroups of all orders  $p^s$  where  $s \leq r$ . Using the prime factorisation of  $m$  and these results we can construct a direct product of order  $m$  via Lemma 7.5 which will form a subgroup of order  $m$  in  $G$ .

**Problem 10.9** (xii) This was given by Problem 10.7.

(xiii) and (xiv) We show that Theorem 10.9(iv) implies (xiii) implies (xiv) implies (xii). The first implication follows from Lemma 5.21 using Problem 7.4.

For the second implication we argue as follows. Suppose (xiii) holds and assume that  $G \neq \langle e \rangle$ , then  $Z(G) \neq \langle e \rangle$ . A factor group of  $G$  also satisfies (xiii). So using induction on  $o(G)$  we have if  $K \triangleleft G$ , either  $K/Z(K) \simeq \langle e \rangle$  or  $[K/Z(K), G/Z(G)] < K/Z(K)$  by (xiii). In the first case we have  $K \leq Z(G)$  and  $[K, G] \simeq \langle e \rangle < K$ , and in the second case  $[K, G] < K$  follows because the derived subgroup of a group is a characteristic subgroup of that group (Problem 4.22). So in both cases we have (xiv).

Now suppose (xiv) holds. Let  $G > \langle e \rangle$  and let  $L$  be a minimal normal subgroup of  $G$ ; see page 235. As  $[L, G] \triangleleft G$  (see Theorem 2.30) we obtain  $[L, G] = \langle e \rangle$  and so

$$L \leq Z(G).$$

Now suppose  $L < K \triangleleft G$  and  $[K/L, G/L] = K/L$ . This gives  $K = [K, G]L$ . (To see this use: if  $\theta$  is an endomorphism of  $G$  and  $a, b \in G$ , then  $[a, b]\theta = [a\theta, b\theta]$ .) This implies

$$[K, G] = [[K, G], G].$$

Applying (xiv) this property shows that  $[K, G] = \langle e \rangle$ , and so  $K = L$  which contradicts our supposition. We can also use this argument to show that  $G/K$  satisfies (xiv). Therefore by applying induction on  $o(G)$  we may suppose  $G/K$  is nilpotent. But then using by Problem 10.7, we see finally that the original group  $G$  is nilpotent.

**Problem 10.10** (i) Let  $a \in H_1$ ,  $b \in H_2$  and  $c \in H_3$ , then by hypothesis

$$c^{-1}[b, c^{-1}, a]c \in K \quad \text{and} \quad a^{-1}[c, a^{-1}, b]a \in K.$$

Using the Hall-Witt Identity (Problem 2.17) these show that

$$b^{-1}[a, b^{-1}, c]b \in K \quad \text{and so} \quad [a, b^{-1}, c] \in K$$

as  $K \triangleleft G$ . Hence for all  $a, b, c \in K$  we have  $[a, b, c] \in K$ . But  $[H_2, H_3, H_1] = [H_3, H_2, H_1]$  and  $[H_3, H_1, H_2] = [H_1, H_3, H_2]$ , and so  $[[a, b^{-1}], c] = [b, a, c] \in K$ . Now note that in general if  $a_i, b_j \in G$  and  $J = \langle \dots, a_i, \dots, b_j, \dots \rangle$  then  $[a_1, \dots, a_m, b_1, \dots, b_n]$  can be expressed as a product of terms of the form  $j_{r,s}^{-1}[a_r, b_s]j_{r,s}$  where  $1 \leq r \leq m$ ,  $1 \leq s \leq n$  and  $j_{r,s} \in J$ . These  $j$  elements depend on the order of the terms in the product. Therefore we have

$$[H_1, H_2, H_3] = [[H_1, H_2], H_3] \in K.$$

(ii) This follows directly from (i) with  $K = \langle e \rangle$ .

(iii) Using the fact:  $z^{-1}[x, y]z = [z^{-1}xz, z^{-1}yz]$  when  $x, y, z \in G$  and Lemma 3.14(iii), as  $H_i \triangleleft G$  we have  $[H_2, H_3, H_1][H_3, H_1, H_2]$  is also normal, and so the result follows from (i).

(iv) Use the method suggested.

(v) Use induction on  $i$ . First we have  $[\mathcal{D}_1(G), \mathcal{Z}_j(G)] = [G, \mathcal{Z}_j(G)] \leq \mathcal{Z}_{j-1}(G)$  for all  $j$ , see page 211. For the inductive step applying the Three Subgroup Lemma we obtain (where we write  $\mathcal{D}_i$  for  $\mathcal{D}_i(G)$  *et cetera*.)

$$\begin{aligned} [\mathcal{D}_{i+1}, \mathcal{Z}_j] &= [[\mathcal{D}_i, G], \mathcal{Z}_j] \leq [[G, \mathcal{Z}_j], \mathcal{D}_i][[\mathcal{Z}_j, \mathcal{D}_i], G] \\ &\leq [\mathcal{Z}_{j-1}, \mathcal{D}_i][\mathcal{Z}_{j-i}, G] \leq \mathcal{Z}_{j-(i+1)}. \end{aligned}$$

**Problem 10.11** (i) Note that by Problem 10.10(v)  $[\mathcal{D}_i(G), \mathcal{Z}_i(G)] = \langle e \rangle$ . But

$$\mathcal{D}_{(j+1)-i}(G) \leq \mathcal{Z}_i(G)$$

(see the proof of Theorem 10.4), and so  $[\mathcal{D}_i(G), \mathcal{D}_{(j+1)-i}(G)] = \langle e \rangle$  which gives the result.

(ii) We have where all products run from 0 to  $n$  (note that some careful consideration using Problem 2.17 is needed for the first equality)

$$\begin{aligned} [L_n, G] &= \prod [[K_{n-i}, K_i], G] \leq \prod [K_{n-i}, [K_i, G]] [[K_{n-i}, G], K_i] \\ &\leq \prod [K_{n-i}, K_{i+1}] [K_i, K_{n-(i+1)}] \leq L_{n+1}. \end{aligned}$$

(iii) By assumption we have  $\mathcal{D}_{l+1}(G) \leq L_0 = K'$ , and so

$$K_{l+2i+1} \leq \mathcal{D}_{l+2i} \leq L_{2i-1} \leq [K, K_i].$$

Hence if

$$K_i \leq \mathcal{D}_{i+1}(G) \leq \mathcal{D}_{j+1}(K) \quad \text{then} \quad K_{l+2i+1} \leq \mathcal{D}_{l+2i}(G) \leq \mathcal{D}_{j+2}(K).$$

But  $K_l \leq \mathcal{D}_{l+1}(G) \leq K_1$ , and so by induction on  $j$  we obtain

$$K_i \leq \mathcal{D}_{i+1}(G) \leq \mathcal{D}_j(K) \quad \text{when} \quad i = (2^j - 1)l - 2^{j-1} + 1.$$

Finally use the given hypothesis that  $K$  has nilpotency class  $j$ .

**Problem 10.12** (i) As  $\mathcal{Z}_0(G) = \langle e \rangle$  and  $\mathcal{Z}_r(G) = G$  for some integer  $r$ , there exists minimal  $s \leq r$  such that  $K \cap \mathcal{Z}_s(G) \neq \langle e \rangle$ . As  $K \triangleleft G$  we have  $[K \cap \mathcal{Z}_s(G), G] \leq K \cap [\mathcal{Z}_s(G), G] \leq K \cap \mathcal{Z}_{s-1}(G) = \langle e \rangle$ , that is  $[K \cap \mathcal{Z}_s(G), G] = \langle e \rangle$  and so  $K \cap \mathcal{Z}_s(G) \leq Z(G)$ , the result follows as this group clearly belongs to  $K$ . This can also be derived using the methods of Chapter 5.

(ii) Use (i) and the fact that  $H \cap Z(G) \triangleleft H$  since subgroups of  $Z(G)$  are normal in  $G$  (Problem 2.14(ii)) and  $H \leq G$ .

(iii) The subgroup  $J$  is Abelian, so  $J \leq C_G(J)$ . For converse, suppose  $C_G(J) \setminus J$  is not empty. As  $J \triangleleft G$ , we have by Problem 5.8,  $g^{-1}C_G(J)g = C_G(J)$  for all  $g \in G$ , so  $C_G(J) \triangleleft G$ . Hence by the Correspondence Theorem (Theorem 4.16)  $C_G(J)/J$  is a non-neutral normal subgroup of  $G/J$ . Applying (i) we can find a coset  $hJ \in (C_G(J)/J) \cap Z(G/J)$ , and using Theorem 4.16 again we have  $\langle J, h \rangle$  is a normal Abelian subgroup of  $G$  strictly containing  $J$  contradicting the maximality of  $J$ .

**Problem 10.13** For  $A_5$ :  $\langle e \rangle$  and  $\langle e \rangle$ ; for  $C_{32}$ :  $C_{16}$  (cyclic groups have unique maximal subgroups) and  $C_{32}$ ; for  $D_{12} = \langle a, b \mid a^{12} = b^2 = (ab)^2 = e \rangle$ :  $\langle a^6 \rangle \simeq C_2$  and  $\langle a \rangle \simeq C_{12}$ , and for  $S_n$ :  $\langle e \rangle$  (Problem 3.9), and  $C_2 \times C_2$  if  $n = 4$  (Section 8.1) and  $\langle e \rangle$  if  $n > 4$  (in which case there are no non-neutral normal nilpotent subgroups – the only subnormal subgroups are symmetric or alternating).

**Problem ♦ 10.14** Suppose  $K \leq \Phi(G)$  and  $H < G$ . There is a maximal  $L$  such that  $H \leq L < G$ , and  $K \leq L$ . Therefore  $HK \leq L < G$ , a contradiction. Conversely suppose  $K \not\leq \Phi(G)$ . So  $G \neq \langle e \rangle$ , and by definition there is a maximal subgroup  $M$  of  $G$  with the property  $K \not\leq M$ . Hence  $M < MK \leq G$  by Lemma 4.14. Now the maximality of  $M$  implies that  $MK = G$  as required in the problem.

**Problem 10.15** (i) Use the fact that if  $H, J \leq G$  and  $\theta$  is an endomorphism of  $G$  (a map  $G \rightarrow G$ ), then  $(H \cap J)\theta \leq H\theta \cap J\theta$ .

(ii) This example was suggested by Ben Fairbairn. Let  $G$  be the group of all  $2 \times 2$  upper-triangular matrices with determinant 1 defined over  $\mathbb{F}_9$  (Problems 3.15 and 12.1). The subgroup  $H = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in \mathbb{F}_9 \right\}$  is normal in  $G$ . It has order 9 and it is the unique Sylow 3-subgroup in  $G$ . Also the subgroup  $J$  of diagonal matrices in  $G$  is cyclic and has order 8. (It forms a Sylow 2-subgroup, there are nine in all with generators  $\begin{pmatrix} c & x \\ 0 & c^7 \end{pmatrix}$  one for each  $x \in \mathbb{F}_9$  where  $c$  is a multiplicative generator of  $\mathbb{F}_9$ .) It follows easily that  $G$  is isomorphic to the semi-direct product  $J \rtimes H$ . Two other normal subgroups are given as follows:  $H' = \left\{ \begin{pmatrix} a & x \\ 0 & a \end{pmatrix} : x \in \mathbb{F}_9, a = 1 \text{ or } 2 \right\}$  with order 18, and  $H'' = \left\{ \begin{pmatrix} y & x \\ 0 & z \end{pmatrix} : x \in \mathbb{F}_9, \{y, z\} = \{1, 1\}, \{2, 2\}, \{c^2, c^6\} \text{ or } \{c^6, c^2\} \right\}$  with order 36.

The maximal subgroups of  $G$  are  $H''$  and the nine Sylow 2-subgroups, and so  $\Phi(G) = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \simeq C_2$ . Incidentally this subgroup is also isomorphic to  $Z(G)$ . Now as  $H' \triangleleft G$ , we can define an endomorphism  $\vartheta : G \rightarrow C_4$  in the usual way. (The four cosets of  $H'$  in  $G$  are generated by  $\begin{pmatrix} c & 0 \\ 0 & c^7 \end{pmatrix} H'$  and its second, third and fourth powers. As  $\Phi(G) \leq H'$ , we have  $\Phi(G)\vartheta \simeq \langle e \rangle$ , but  $\Phi(G\vartheta) \simeq \Phi(C_4) \simeq C_2$ .

**Problem ♦ 10.16** Let  $P$  be a Sylow  $p$ -subgroup of  $J$ . This gives  $KP/K$  is a Sylow  $p$ -subgroup of  $J/K$  (see Problem 6.10). Now as  $J/K$  is nilpotent, we have  $KP/K$  is a characteristic subgroup of  $J/K$ , and so  $KP \triangleleft G$ . Also  $P$  is a Sylow  $p$ -subgroup of  $KP$ , and hence using the Frattini Argument (Theorem 6.14) we have  $G = N_G(P)K \leq N_G\Phi(G)$ . By Lemma 10.14 this shows that  $G = N_G(P)$  and  $P \triangleleft G$ . As this argument holds for all Sylow subgroups of  $G$  the result follows by Theorem 10.9(vii).

**Problem 10.17** If  $G = H \times J$  and  $L$  is a maximal subgroup of  $H$ , then  $L \times J$  is a maximal subgroup of  $G$ , see Problem 7.3(ii). Therefore  $\Phi(G) \leq L \times J$ , and so  $\Phi(G) \leq \Phi(H) \times J$ . This gives the result.

**Problem 10.18** (i) If  $G = S_4$  then  $\Phi(G) = \langle e \rangle$ . We also have  $H = \langle (1, 2, 3, 4), (1, 3) \rangle < G$  and  $H$  is isomorphic to  $D_4$ . Therefore  $\Phi(H) = \langle a^2 \rangle \not\leq \langle e \rangle = \Phi(G)$ .

(ii) Note first that the question needs to be amended so that  $K$  is a *proper* subgroup of  $\Phi(H)$ . Suppose  $K \not\leq \Phi(G)$ , so there exists a maximal subgroup  $L$  of  $G$  with  $K \not\leq L$  and  $G = KL$  (as  $L$  is maximal). Hence  $H = H \cap KL = (H \cap L)K$  (by Problem 2.18(i)), so  $H = H \cap L$  (by Theorem 10.12) that is  $H \leq L$ . This gives  $K \leq \Phi(H) \leq H \leq L \leq G$  contradicting our hypothesis.

(iii) Use (ii).

**Problem 10.19** (i) Let  $J$  be minimal subject to the condition:  $G = JK$ . We have  $J \cap K \triangleleft J$  as  $K$  is normal, and  $J \cap K \triangleleft K$  as  $K$  is Abelian, so  $J \cap K \triangleleft JK = G$ . If we assume that  $J \cap K \leq \Phi(H)$ , then by Problem 10.18(ii)  $J \cap K \leq \Phi(G) \cap K = \langle e \rangle$  by hypothesis, and we have the required subgroup. Hence suppose  $J \cap K \not\leq H$  for some  $H$  which is a maximal subgroup of  $J$ . But in this case  $J = H(J \cap K)$  and  $G = JK = HK$  which contradicts the minimality of  $J$ . Therefore our assumption is valid.

(ii) One example from Chapter 8 is as follows. Using the notation of Section 8.3 let  $G = E$ , then  $\Phi(G) = \langle a^2 \rangle$ , so let  $K = \langle c \rangle$ . In this case we can take



$J = \langle a, b \rangle$ . Note that this phenomenon can also occur if  $\Phi(G) = \langle e \rangle$ , for example if  $G = S_4$ . Let  $K = V$ , the subgroup generated by the 2-cycles  $\times$  2-cycles, and then we can take  $J = \langle (1, 2, 3), (1, 2) \rangle$ ; there are four choices for the subgroup  $J$ .

**Problem 10.20** (i) If  $g \in G$  then by conjugation  $g$  induces an automorphism,  $\theta_g$  say, of  $K$ , that is  $\theta_g$  is a homomorphism  $G \rightarrow \text{Aut}(K)$ . We have

$$K\theta_g = \text{Inn}(K) \leq (\Phi(G))\theta_g \leq \Phi(G\theta_g)$$

using Problem 10.15. But  $\text{Inn}(K) \triangleleft \text{Aut}(K)$  (Theorem 5.26), and so by Problem 10.18(ii) we have  $\text{Inn}(K) \leq \Phi(\text{Aut}(K))$ .

(ii) Put  $K = \Phi(G)$  in (i).

(iii) If  $D_4 = \langle a, b : a^4 = b^2 = (ab)^2 = e \rangle$ , then  $\Phi(D_4) = \langle a^2 \rangle \simeq C_2$ , and  $\text{Inn}(D_4) \simeq C_2 \times C_2$  (see page 84). Now apply (ii) with  $G = D_4$ .

**Problem 10.21** (i) Let  $H$  be a maximal subgroup of  $G$ , then by Theorem 6.6 we have  $H \triangleleft G$  and  $[G : H] = p$ . This shows that  $G/H$  is Abelian, and so  $G' \leq H$  (Problem 4.6). Also  $G'$  has exponent  $p$ , and so  $a^p \in H$  for all  $a \in G$ . Hence  $G'G^p \leq \Phi(G)$ . Conversely, note first that  $G/G'G^p$  is an Abelian group with exponent  $p$  and so can be treated as a vector space over  $\mathbb{F}_p$ , and  $\Phi(G/G'G^p) = \langle e \rangle$  (Lemma 10.19). Also if  $J \triangleleft G$  and  $J \leq \Phi(G)$ , then  $\Phi(G)$  is the inverse image (using the natural map) of  $\Phi(G/J)$  because, via the Correspondence Theorem (Theorem 4.16), maximal subgroups correspond. Now the reverse inclusion  $\Phi(G) \leq G'G^p$  follows.

(ii) As  $G'G^p = \Phi(G)$ , the factor group  $G/\Phi(G)$  is an Abelian group with exponent  $p$  which can be treated as a vector space over  $\mathbb{F}_p$ .

**Problem 10.22** (i) If  $a, g \in G$ , then  $[a, g^p] = [a, g]^p = e$  and so  $g^p \in Z(G)$ . Consequently every element of  $G/Z(G)$  has order  $p$  and as  $G$  is a finite  $p$ -group we see that  $G/Z(G)$  is an elementary Abelian  $p$ -group.

(ii) We have  $o(Z(G)) \neq 1$  by Lemma 5.14, it is not  $p^2$  by Problem 4.15 (for otherwise  $G/Z(G)$  would be cyclic), and it is not  $p^3$  as  $G$  is not Abelian. So  $Z(G)$  is cyclic with order  $p$ . Also by Theorem 10.1,  $G' \leq Z(G)$ , and  $G' \neq \langle e \rangle$  as  $G$  is not Abelian, hence  $G' = Z(G)$ . Now use Problem 10.21 to show that  $\Phi(G) = G'$ .

**Problem 10.23** (i) One method uses Problem 10.21(i). If  $p = 2$  we show that all commutators belong to  $G^2$ . Suppose  $o(a) = 2^k$  and  $o(b) = 2^l$ . Now

$$[a, b] = a^{2^k-1}b^{2^l-1}ab = a^{2^k-2}ab^{2^l-1}ab^{2^l-1}b^2 = (a^{2^{k-1}-1})^2(ab^{2^l-1})^2b^2,$$

a product of squares. This shows that  $\Phi(G) \leq G^2$ , now apply Problem 10.21 for the reverse inequality.

(ii) Let  $p = 3$  in the second group given in Problem 6.5, that is  $ES_2(3)$  generated by  $a, b$  and  $c$ . Here all elements  $x$  satisfy  $x^3 = e$ , so  $\langle x^3 \mid x \in G \rangle = \langle e \rangle$  whilst  $\Phi(G) = \langle c \rangle$ ; see Problem 10.22. The first group in Problem 6.5,  $ES_1(3)$ , does satisfy the condition given in (i).

**Problem 10.24** (i) Use Problem 9.16 with  $K = \Phi(G)$  and  $J/K = F(G/K)$ . As  $J/K$  is nilpotent (Theorem 10.22 and Definition 10.23), the quoted problem shows that  $J$  is nilpotent, which implies  $F(G/\Phi(G)) \leq F(G)/\Phi(G)$ . For the converse, as  $F(G)$  is nilpotent, we see that  $F(G)/\Phi(G)$  is a nilpotent subgroup of  $G/\Phi(G)$ . Hence  $F(G)/\Phi(G) \leq F(G/\Phi(G))$  which gives the result.

(ii) For  $S_4$  we have  $\Phi(S_4) = \langle e \rangle$ , and so the result is trivial in this case. For  $SL_2(3)$  we have  $\Phi(SL_2(3)) \simeq C_2$  (which also equals the centre) and  $F(SL_2(3)) \simeq Q_2$ . Now  $Q_2/C_2 \simeq C_2 \times C_2$ , and  $SL_2(3)/C_2 \simeq A_4$  (Problem 4.4). Now note that  $F(A_4)$  is the largest nilpotent normal subgroup of  $A_4$  that is  $C_2 \times C_2$  generated by the 2-cycles  $\times$  2-cycles. For  $E$  we have  $\Phi(E) \simeq C_2$  and  $F(E) \simeq C_6 \times C_2$ . Now clearly  $F(E)/\Phi(E) \simeq C_6$ . We also have  $E/\Phi(E) \simeq D_6$ , and the largest nilpotent normal subgroup of  $D_6 = \langle a, b : a^6 = b^2 = (ab)^2 = e \rangle$  is  $\langle a \rangle \simeq C_6$ . For the details on these constructions see Chapter 8.

**Problem 10.25** (i) Let  $i$  be the largest integer satisfying  $K \cap G^{(i)} \neq \langle e \rangle$ ; see page 234. So  $(K \cap G^{(i)})' \leq K \cap G^{(i+1)} = \langle e \rangle$ , and it follows that  $K \cap G^{(i)}$  is Abelian and is normal in  $G$ .

(ii) Suppose first  $C_G(F(G)) \not\leq F(G)$ . By (i) we can find  $J$  so that  $J/F(G) \triangleleft G/F(G)$ ,  $F(G) < J \leq C_G(F(G))F(G)$ , and  $J/F(G)$  is Abelian. Now  $J = J \cap (C_G(F(G))) = (J \cap C_G(F(G)))F(G)$  by Problem 2.18. This shows that

$$\mathcal{D}_3(J \cap C_G(F(G))) \leq [J', C_G(F(G))] \leq [F(G), C_G(F(G))] = \langle e \rangle,$$

which in turn shows that  $J \cap C_G(F(G)) \leq F(G)$  and  $J = F(G)$ . This contradiction now shows that  $C_G(F(G)) \leq F(G)$  which in turn implies that  $C_G(F(G)) = Z(F(G))$ .

(iii) As  $G$  is soluble it contains a non-neutral normal subgroup, this follows from (i).

(iv) Use Problem 10.24(i) and (iii).

**Problem 10.26** (i)  $\langle e \rangle \triangleleft C_3 \triangleleft S_3$  is a supersoluble series for  $S_3$ . But  $S_4$  is not supersoluble, its normal series  $\langle e \rangle \triangleleft V \triangleleft A_4 \triangleleft S_4$  has a non-cyclic factor  $V \simeq T_2$ .

(ii) Assume  $\mathcal{S} = (H_0, \dots, H_m)$  is a supersoluble series for  $G$ . Its factors are cyclic, so suppose  $H_{i+1}/H_i \simeq C_k$ . Now  $\mathcal{S}$  can be refined by inserting new terms between  $H_i$  and  $H_{i+1}$  so that the new factors have prime orders corresponding to the prime factors of  $k$ . This can be done for all factors in  $\mathcal{S}$ .

(iii) See the proofs of Theorems 11.2 and 11.3. Now see (i). The group  $V$  is finite Abelian so supersoluble, and  $S_4/V \simeq S_3$  is also supersoluble, but  $S_4$  is not supersoluble.

(iv) If  $J_0, \dots, J_m$  and  $K_0, \dots, K_n$  are supersoluble series for  $G$  and  $H$ , respectively, then

$$J_0 \times K_0, \dots, J_m \times K_0, J_m \times K_1, \dots, J_m \times K_n$$

is a supersoluble series for  $G \times H$ .

(v) Finite  $p$ -groups are supersoluble by Theorem 6.4. So the result holds by this, (iv), and Theorem 10.9(viii). Now note that  $S_3$  is not nilpotent, and  $S_4$  is not supersoluble.

(vi) Let  $H_0, \dots, H_m$  be a supersoluble series for  $G$ , and let  $J_i = H_i \cap G'$ . Now  $J_0, \dots, J_m$  is a supersoluble series for  $G'$ . Also if  $g \in G$  then  $g$  induces an automorphism of  $J_{i+1}/J_i$  (by conjugation), so

$$G/L \preceq \text{Aut}(J_{i+1}/J_i) \quad \text{where} \quad L/J_i = C_{G/J_i}(J_{i+1}/J_i).$$

But  $J_{i+1}/J_i$  is cyclic (by definition), so by Theorem 4.23 it follows that  $G/L$  is Abelian. Therefore  $L \geq G'$  (Problem 4.6), and hence

$$J_{i+1}/J_i \leq Z(G'/J_i),$$

that is  $J_0, \dots, J_m$  is an upper central series for  $G'$ .

(vii) Suppose  $H_0, \dots, H_m$  is a supersoluble series for  $G/K$ , and  $\theta$  is the natural homomorphism  $G$  to  $G/K$ , then

$$\langle e \rangle \triangleleft H_0\theta^{-1} = K \triangleleft H_1\theta^{-1} \triangleleft \dots \triangleleft H_m\theta^{-1} = G$$

is a supersoluble series for  $G$ .

(viii) Zappa has shown that the terms of a supersoluble series can be rearranged so that all of the factors of odd order come first followed by those of even order. This can now be used to prove the result, see the quoted reference.

(ix) This is a substantial problem, try to establish each of the following propositions in turn. (a) If  $G$  is supersoluble, then all of its maximal subgroups have prime index in  $G$ . (b) Using induction on  $o(G)$  and Problem 11.9(ii), show that all subgroups of  $G$  are reverse Lagrange. (c) For the converse, again use induction on  $o(G)$ . Note first that  $G$  has at least one normal Sylow  $p$ -subgroup  $P$  where  $p \mid o(G)$ . (d) Use the inductive hypothesis and Hall's Theorems (Chapter 10) to show that  $G/P$  is supersoluble. (e) By hypothesis, there exists a subgroup  $L$  of  $G$  with  $[G : L] = p$ . Prove that  $L \cap P \triangleleft G$  and  $G/(L \cap P)$  is supersoluble. (f) Suppose we can choose a subgroup  $K$  of  $G$  satisfying  $K \triangleleft G$ ,  $K \leq L \cap P$  and  $o(K)$  is as small as possible. Now  $K = \langle e \rangle$  and we can complete the argument. But if  $K \neq \langle e \rangle$ , then  $[K, P] < K$ , so consider the chief factor (see Problem 9.15)  $K/M$  of  $L$  with  $[K, P] \leq M < K$ , and use this to show that  $K = \langle e \rangle$ . For further details see Rose [1978], page 292.

(x) The real numbers  $\mathbb{R}$  form an example of a non-supersoluble Abelian group. This group does not have a finite series with cyclic (finite or infinite) factors, in any such series at least one factor must be uncountable. Of course all finite Abelian groups are supersoluble.

## Solutions 11

**Problem 11.1** (ia) Coefficients are rational, so we may assume that the leading coefficient is 1, hence the cubic has the form  $f(y) = y^3 + ry^2 + sy + t$  where  $r, s, t \in \mathbb{Q}$ . Put  $y = x - r/3$ .

(ib) Use

$$\begin{aligned} 0 &= (u + v)^3 + a(u + v) + b \\ &= u^3 + 3u^2v + 3uv^2 + v^3 + au + av + b \\ &= u^3 + v^3 + (u + v)(3uv + a) + b. \end{aligned}$$

(ic) Set  $v = -a/3u$ , then  $2u^3 = -b + \sqrt{(b^2 + 4a^3/27)}$ .

(iia and b) For (iia) proceed as above and for (iib) we have

$$\begin{aligned} x^4 + ax^2 + bx + c &= (x^2 + rx + s)(x^2 + ux + t) \\ &= x^4 + (r + u)x^3 + (s + t + ru)x^2 + (rt + su)x + st, \end{aligned}$$

so put  $r + u = 0$ ,  $s + t - r^2 = a$ ,  $r(t - s) = b$  and  $st = c$ . Second and third equations give  $2t = r^2 + a + b/r$  and  $2s = r^2 + a - b/r$ . So fourth gives  $4c = 4st = (r^2 + a + b/r)(r^2 + a - b/r) = r^4 + 2ar^2 + a^2 - b^2/r^2$ .

**Problem 11.2** (ia) Suppose  $D_n = \langle a, b \mid a^n = b^2 = e, bab = a^{n-1} \rangle$ . We have  $\langle a \rangle \triangleleft D_n$  and  $D_n/\langle a \rangle \simeq C_2$ . Now use Theorems 11.4 and 11.6.

(ib) This is similar to (ia).

(ic) We have  $\langle e \rangle \triangleleft V \triangleleft A_4 \triangleleft S_4$  is a soluble series for  $S_4$ ; see Section 8.1.

(ii) By Lemma 7.3 and Theorem 7.4,  $G \triangleleft G \times H$  and  $(G \times H)/G \simeq H$ . This can also be done by combining the soluble series for  $G$  and  $H$  and using properties of the direct product.

**Problem 11.3** (i) By Problem 3.19, the only subnormal series for  $SL_2(5)$  with more than two terms is:  $\langle e \rangle \triangleleft C_2 \triangleleft SL_2(5)$ , and so this series is a composition series for  $SL_2(5)$  (use the Jordan-Hölder Theorem (Theorem 9.5)). Hence  $SL_2(5)/C_2$  is simple (in fact it is isomorphic to  $A_5$ , see Problem 6.16). Therefore  $SL_2(5)$  is not soluble.

(ii) If  $o(G) = p < 200$ , then  $G \simeq C_p$  which is soluble. If  $o(G) < 60$  or  $o(G) = 60$  and  $G \not\simeq A_5$ , then use Problems 6.15 and 6.16, and Theorem 11.4. This can be extended to groups satisfying  $o(G) < 120$ . At least three non-soluble groups of order 120 exist, they include  $S_5, SL_2(5), A_5 \times C_2$ . There is a (unique) simple (and so non-soluble) group of order 168, see Problem 12.7, and at least one of order 180, that is  $A_5 \times C_3$ . In fact these six groups complete the list of non-soluble groups of order less than 200, a fair amount of checking is needed to establish this; see the GAP program and Section 6.7 in the ATLAS.

**Problem 11.4** Suppose  $G$  is the smallest non-soluble group of order  $p^2q^2$  or  $p^nq$ . If  $G$  is not simple, it has a normal subgroup  $K$  where  $1 < o(K) < o(G)$ , and by minimality it is soluble; as is  $G/K$  for the same reason. We can now use Theorem 11.4.

*Case 1* –  $o(G) = p^n q$ . Using the first part and the Sylow theory we have  $n_p = q$ , so let  $P_1$  and  $P_2$  be distinct Sylow  $p$ -subgroups of  $G$  and let  $L = P_1 \cap P_2$ . There are two subcases. *Subcase 1* – for all choices of  $P_1$  and  $P_2$ ,  $L = \langle e \rangle$ . In this case  $G$  has  $q(p^n - 1)$  elements of order a power  $p$ , and so only  $q$  others. But  $G$  has at least one Sylow  $q$ -subgroup of order  $q$ , and as it is unique it is normal contradicting the simplicity of  $G$ . *Subcase 2* –  $L \neq \langle e \rangle$ , we may suppose  $L$  has maximal order. It is a  $p$ -group so nilpotent, hence by Theorem 10.9(iv), if

$$M_i = N_G(P_i), \quad \text{we have} \quad L \triangleleft M = \langle M_1, M_2 \rangle.$$

By Sylow 5, if  $M$  is a  $p$ -group, it is contained in some Sylow  $p$ -subgroup of  $G$ , say  $P^*$ . We have

$$P_1 \leq M_1 \leq M,$$

but as  $P_1$  is maximal (it has prime index) and  $P_2 \leq M$ , we see that  $P_1 \neq M$ . Hence  $M = G$  and  $L \triangleleft G$  which contradicts the simplicity of  $G$ .

*Case 2* –  $o(G) = p^2 q^2$  with  $q < p$ . Here  $n_p = q^2$ , and if  $L$  is defined as above and  $L = \langle e \rangle$  then the same argument applies. So suppose  $L \neq \langle e \rangle$ . In this case each  $P_i$  is Abelian, and so  $L \triangleleft \langle P_1, P_2 \rangle = J$ , and  $J \neq G$  (as  $G$  is simple). This further implies  $[G : J] = q$ , and by Theorem 5.15, we have  $o(G) \mid q!$  which is impossible as  $p > q$ .

**Problem ♦ 11.5** (i) Suppose we have  $\dots \triangleleft A \triangleleft B \triangleleft \dots$  with  $B/A$  Abelian, and  $A \triangleleft C \triangleleft B$ . We can deduce that  $C/A$  and  $B/C$  are both Abelian using Theorems 4.16 and 4.17, and Problem 4.6(i).

(ii) Yes. Use the facts that an infinite simple group  $H$  has the composition series  $\langle e \rangle \triangleleft H$ , and a soluble series for an infinite group must have at least one ‘infinite step’  $A \triangleleft B$  (where  $o(B/A) = \infty$ ). Consider  $\langle e \rangle \triangleleft A/A \triangleleft B/A$ .

(iii) Use the definition and Theorems 7.12, 7.7 and 6.5.

(iv) Use Problem 9.15.

**Problem 11.6** (i) We assume that  $r, s > 0$ . Now  $G$  has a Sylow  $q$ -subgroup  $P$ , and  $Z(P) > \langle e \rangle$  by Lemma 5.21. Let  $g \in Z(P)$  with  $g \neq e$ , so  $P < C_G(g)$  and

$$o(\mathcal{C}\ell\{g\}) = [G : C_G(g)] = p^u$$

for some integer  $u$ . If  $u = 0$  then  $g \in Z(G)$ , and so  $G$  is not simple (as  $Z(G) \triangleleft G$ ), and if  $u > 0$  then  $G$  is not simple by Burnside’s result. Therefore if  $o(G) = p^r q^s$ , then  $G$  is not simple. Suppose  $G$  is of smallest order such that  $G$  is not soluble. As it is not simple, it has a normal subgroup  $H$  of order  $p^{r_1} q^{s_1} < o(G)$ , so  $H$  (and also  $G/H$ ) are soluble, now use Theorem 11.4.

(ii) Suppose  $G$  is not Abelian. If all odd-order groups are soluble and  $G$  is simple, then  $G$  must have even order.

Conversely if all simple groups have even order and  $G$  has odd order then it possesses a non-neutral proper normal subgroup  $K$ , and  $o(K)$  and  $o(G/K)$  are also odd. Suppose  $K$  is smallest (by size of its order) which is not soluble, it will have a normal subgroup  $H$  of smaller order, so apply Theorem 11.4 to it and  $K/H$ .

(iii) See Theorem 6.18, the group has a normal cyclic subgroup  $\langle a \rangle$ . A substantial number of simple groups come close; for example  $A_5, L_2(11)$  and  $J_1$  have Abelian Sylow subgroups many of which are cyclic.

**Problem ♦ 11.7** (i) If  $G$  is non-Abelian and soluble, then its derived series has at least three terms including  $\langle e \rangle$  and  $G$ , its second from bottom term will be non-neutral, normal and Abelian by Theorem 11.10.

(ii) If  $G$  is not soluble, then its derived series does not reach  $\langle e \rangle$ , that is there is an integer  $k$  such that  $G^{(k)} = G^{(k+1)} = (G^{(k)})'$  giving the required perfect subgroup. Note that  $G$  itself might be perfect.

**Problem 11.8** (i) One example is  $SL_2(3)$ ; see Section 8.2.

(ii) A Reverse Lagrange group will have a  $p$ -complement for all primes dividing the order of the group, so will be soluble by Hall's Second Theorem. Or we can argue as follows. First we show that  $G$  must have a proper non-neutral normal subgroup. Let  $o(G) = p_1 p_2 \dots$  where  $p_1 \leq p_2 \leq \dots$ . There exists a subgroup  $H$  of  $G$  with  $[G : H] = p_1$ , so by Theorem 5.15, if  $\text{core}(H) = \langle e \rangle$  then  $G$  is isomorphic to a subgroup of  $S_{p_1}$ . Hence  $p_1 p_2 \dots \mid p_1!$  which is only possible if  $p_2 = \dots = 1$  and  $G \simeq C_{p_1}$ . Therefore if we exclude this case, the subresult follows. Now use induction and Theorem 11.4; start by assuming that  $G_1$  is Reverse Lagrange and not soluble, and has the smallest possible order with these two properties.

**Problem ♦ 11.9** (i) The subnormal series  $\langle e \rangle \triangleleft J \triangleleft K \triangleleft G$  can be refined to a chief series, see Problem 9.15 (iii) and (iv). By definition,  $J$  and  $K$  are consecutive terms in this series, so  $K/J$  is elementary Abelian by Problem 9.15 again.

(ii) Let  $J = \text{core}(H)$  and  $K$  be minimal subject to the condition  $J < K$ . Using the definitions of the core, and of  $K$ , we have  $K \not\leq H$ , and so by maximality of  $H$  we have  $KH = G$ . Next we show

$$K \cap H = J. \quad (11.1)$$

We have  $J \leq K \cap H \leq K$  and  $K \cap H \triangleleft H$  (Lemma 4.14). So by (i)  $K/J$  is Abelian, and by applying the Correspondence Theorem (Theorem 4.16) we have  $K \cap H \triangleleft K$ . These show that

$$N_G(K \cap H) \geq \langle K, H \rangle = G.$$

Hence  $K \cap H \triangleleft G$ , and so by the definition of  $J$  this gives (11.1). Therefore using the Second Isomorphism Theorem (Theorem 4.15) we obtain

$$[G : H] = [KH : H] = [K : K \cap H] = [K : J].$$

Finally by (i) again, as  $[K : J]$  is a prime power so is  $[G : H]$ .

**Problem ♦ 11.10** (i) Use Theorems 4.16 and 11.2 to 11.4.

(ii) Use Lemma 4.14 and (i).

(iii) Yes, let  $G = A_5 \times C_2$ . Here  $A_5$  forms a maximal normal subgroup.

**Problem 11.11** One example is  $A_5 \times C_6$  which is not soluble. It has order 360, and contains maximal subgroups of index 2, that is  $A_5 \times C_3$ ; of index 3, that is  $A_5 \times C_2$ ; and of index 5, that is  $A_4 \times C_6$ .

**Problem 11.12** The group  $G$  is soluble, so by Theorem 11.10 if, for some  $k$ ,  $G^{(k)} = G^{(k+1)}$ , then  $G^{(k)} = \langle e \rangle$ . The solubility also implies that  $G^{(k)} = \langle e \rangle$  for some  $k$  which in turn implies that  $G^{(k-1)}$  is cyclic. Repeating the argument if necessary we may therefore assume that  $G^{(3)} = \langle e \rangle$  and so  $G^{(2)}$  is cyclic.

By Theorem 11.10,  $G^{(2)} \triangleleft G$ , and so by the  $N/C$  theorem (Theorem 5.26)

$$C_G(G^{(2)}) \triangleleft N_G(G^{(2)}) = G \quad \text{and} \quad G/C_G(G^{(2)}) \preceq \text{Aut } G^{(2)}.$$

Now  $G^{(2)}$  is cyclic, and so by Theorem 4.23,  $\text{Aut } G^{(2)}$  is Abelian, and hence  $G/C_G(G^{(2)})$  is also Abelian, which in turn by Problem 4.6(ii) implies

$$G' \leq C_G(G^{(2)}), \quad \text{and so} \quad G^{(2)} \leq Z(G'),$$

by (iv) on page 104. We also have  $G'/G^{(2)}$  is cyclic, and so this gives by the Correspondence Theorem (Theorem 4.16)  $G'/Z(G')$  is cyclic. Therefore using Problem 4.16(ii) we have:  $G'$  is Abelian and so  $G^{(2)} = \langle e \rangle$ .

**Problem 11.13** We show first that  $G$  is soluble using induction on  $o(G)$ , if  $o(G) = 1$  there is nothing to prove. Now let  $o(G) > 1$  and let  $p_0$  be the smallest prime dividing  $o(G)$ . By Burnside's Normal Complement Theorem (Theorem 6.17),  $G$  has a normal  $p_0$ -complement  $K$ , say, so  $K \triangleleft G$  and  $G/K \simeq P$  where  $P$  is a Sylow  $p_0$ -subgroup of  $G$ . Using Theorem 6.9(i) we see that all Sylow subgroups of  $K$  are cyclic, hence  $K$  is soluble by the inductive hypothesis. Further  $P$  is a  $p_0$ -group, and so is soluble. Therefore  $G$  is soluble by Theorem 11.4.

Now by Problem 4.6(ii),  $G^{(n)}/G^{(n-1)}$  is Abelian for  $n = 0, 1, \dots$ , and all of its subgroups are cyclic. Hence they are themselves cyclic, this follows using the Sylow theory and Problem 4.15(ii). Therefore by Problem 11.12,  $G^{(2)} = G^{(3)} = \langle e \rangle$  and the result follows.

**Problem 11.14** (ia) If  $G_1$  is not simple, it has a proper normal subgroup  $K$  which is soluble by the definition of  $G_1$ , as is  $G_1/K$  for the same reason. But then  $G_1$  is soluble by Theorem 11.4.

(ib) Suppose every pair of distinct maximal subgroups has neutral intersection. Now  $H_1 = N_{G_1}(H_1)$ , and if  $o(H_1) = m$ , then  $H_1$  has  $o(G_1)/m$  conjugates all of which have neutral intersection. So the conjugates of  $H_1$  have  $(m-1)o(G_1)/m = o(G_1) - o(G_1)/m = r$  non-neutral elements. As  $m > 1$ , we have  $(o(G_1) - 1)/2 < r < o(G_1) - 1$ , but this is impossible as each non-neutral element of  $G_1$  belongs to exactly one maximal subgroup (because of the neutral intersection of the subgroups containing them), and so there are  $o(G_1) - 1$  in total.

(ic) Let  $L = N_{G_1}(J)$ , then  $J \neq N_{H_1}(J)$  by Theorem 10.7 as  $J$  is nilpotent, so  $J < L \cap H_1$ . By (ia)  $L < G_1$ , and so it is contained in some maximal  $H$  of  $G_1$ . It follows that  $J < L \cap H_1 \leq H \cap H_1$  contradicting the maximality

property of  $J$ .

(id) By (ib and c) the counter-example postulated in (ia) does not exist.

(ii) As finite Abelian groups are nilpotent, (i) shows that  $G' < G$  by Theorem 11.10, and  $G' \triangleleft G$  by Problem 2.16. But then  $G'$  is Abelian, and so  $G'' = \langle e \rangle$ .

**Problem ♦ 11.15** By Theorem 2.30 we have  $[H, J] \triangleleft G$ , and by Problem 2.16  $G' \leq [H, J]$ , hence  $G' = [H, J]$ . If  $h_i \in H$  and  $j_i \in J$  we have  $h_2^{-1}j_1h_2 = h_3j_3$  and  $j_2^{-1}h_1j_2 = j_4h_4$ . Note also  $[h, h'] = e$  and  $[h, h'j] = [h, j]$  as  $H$  is Abelian, and so by Problem 2.17(iii)  $j^{-1}[h, j']j = [j^{-1}hj, j']$ , *et cetera*. Hence we have

$$\begin{aligned} (h_2j_2)^{-1}[h_1, j_1]h_2j_2 &= j_2^{-1}[h_1, h_2^{-1}j_1h_2]j_2 = j_2^{-1}[h_1, h_3j_3]j_2 \\ &= j_2^{-1}[h_1, j_3]j_2 = [j_2^{-1}h_1j_2, j_3] = [j_4h_4, j_3] = [h_4, j_3], \end{aligned}$$

and similarly

$$\begin{aligned} (j_2h_2)^{-1}[h_1, j_1]j_2h_2 &= h_2^{-1}[j_4h_4, j_2]h_2 \\ &= h_2^{-1}[h_4, j_1]h_2 = [h_4, h_3j_3] = [h_4, j_3]. \end{aligned}$$

This shows that  $[H, J] = G'$  is Abelian, and so  $G'' = \langle e \rangle$  which implies that  $G$  is soluble. Other proof methods are possible.

**Problem 11.16**  $A_5$  : this group has a 5-complement which is isomorphic to  $A_4$ , but no 2- or 3-complements, see page 101.

$A_6$  : this group has no  $p$ -complements. The maximal subgroups of this group are isomorphic to  $A_5$ ,  $S_4$  or  $C_4 \rtimes C_3^2$  (with order 36). Hence  $A_6$  cannot have subgroups of order 45 (index 8) or 40 (index 9). By Theorem 5.15 it cannot have a subgroup of order 72 (index 5).

$L_2(7)$  : this group has a 2-complement isomorphic to  $F_{7,3}$  and a 7-complement isomorphic to  $S_4$ , but no 3-complement, such a subgroup would have order 56 which is impossible by Theorem 5.15.

**Problem 11.17** First note that both  $S_3$  and  $S_4$  are their own Hall  $\{2, 3\}$ -subgroups.  $S_4$  is an example of a Hall  $\{2, 3\}$ -subgroup of  $S_5$ . A Hall  $\{2, 3\}$ -subgroup of  $S_6$  would have index 5 which is impossible by Theorem 5.15. Finally, Problem 3.9 shows that  $S_3 \times S_4$  is isomorphic to a Hall  $\{2, 3\}$ -subgroup of  $S_7$ , and  $S_4 \text{ wr } C_2$  (or  $S_4 \wr C_2$ ) is isomorphic to a Hall  $\{2, 3\}$ -subgroup of  $S_8$  (Problem 3.9(iii)).

**Problem 11.18** (i) Use the definitions.

(ii) The symmetric group  $S_5$  has subgroups isomorphic to  $C_3$  generated by 3-cycles, and  $C_5$  generated by 5-cycles, but it has no subgroup of order 15, such a subgroup would be isomorphic to  $C_{15}$  but the group contains no elements of order 15.

(iii) A Hall  $\{2, 5\}$ -subgroup of  $S_5$  would have order 40, but  $S_5$  has no subgroup of this order (use Theorem 5.15). On the other hand  $S_5$  does have a  $\{2, 5\}$ -subgroup of order 20, see Problem 3.11.



(iv)  $GL_3(2)$  (which is isomorphic to  $L_2(7)$ , see Chapter 12) has two sets of subgroups each isomorphic to  $S_4$ . An example from the first set is generated by

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix},$$

and an example from the second set is generated by

$$\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Note that in both cases the first generating element has order 3, the second has order 2, and their products both have order 4; see Problem 3.18. Matrices in the first example above only fix  $(0, 0, 0)$  in the 3-dimensional vector space defined over  $\mathbb{F}_2$ , that is they only fix one point in the space, but in the second example every matrix fixes two points  $(0, 0, 0)$  and  $(0, 0, 1)$  – a line in the space. For this reason the examples cannot be conjugate, even though they are isomorphic.

(v) The group  $L_2(11)$  has order 660, and it has non-isomorphic subgroups of order 12 and index 55 (so Hall  $\{2, 3\}$ -subgroups). For example if the group is given by the permutation representation stated on page 295, then

$$D_6 \simeq \langle (1, 3)(2, 7, 11, 5, 10, 9)(4, 8, 6), (1, 3)(2, 11)(4, 8)(5, 9) \rangle \leq L_2(11),$$

$$A_4 \simeq \langle (1, 3, 2)(4, 6, 5)(7, 9, 8), (1, 3)(2, 11)(4, 8)(5, 9) \rangle \leq L_2(11).$$

**Problem ♦ 11.19** (i) Clear.

(ii) Use Problem 2.23.

(iii) Use Problem 2.15.

(iv) Use the Correspondence Theorem (Theorem 4.16).

**Problem 11.20** (i) For  $S_4$  one example is  $\langle (1, 2, 3, 4), (1, 3) \rangle$  and  $\langle (1, 2, 3) \rangle$ ; for  $SL_2(3)$  take the copy of  $Q_2$  and one of the Sylow 3-subgroups; and for  $E$  use the definition.

(ii) Sylow 3- or 5-subgroups of  $S_5$  are cyclic in the form  $\langle (a, b, c) \rangle$  or  $\langle (a, b, c, d, e) \rangle$ , but these never commute.

(iii) Condition 6. Take  $P_1 = \langle (1, 2, 3, 4), (1, 3) \rangle$  as a Sylow 2-subgroup. Condition 7. Use Problem 3.18.

**Problem 11.21** This is a project not directly relevant to the chapter, so is left as an exercise for the reader to complete. See Suzuki [1986], pages 102 and 103.

## Problems 12

**Problem 12.1** We have  $c^3 = 2c + 1$ ,  $c^4 = 2$ ,  $c^5 = 2c$ ,  $c^6 = 2c + 2$ ,  $c^7 = c + 2$ ,  $c^8 = 1$ ,  $\bar{c} = 2c + 1$ ,  $\bar{c}^2 = 2c + 2$ ,  $\bar{c}^3 = c$ ,  $\bar{c}^4 = 2$ ,  $\bar{c}^5 = c^7 = c + 2$ ,  $\bar{c}^6 = c + 1$ ,  $\bar{c}^7 = c^5 = 2c$ ,  $\bar{c}^8 = 1$ ,  $c + \bar{c} = c^3 + \bar{c}^3 = c^4 + \bar{c}^4 = 1$ ,  $c^2 + \bar{c}^2 = c^6 + \bar{c}^6 = 0$  and  $c^5 + \bar{c}^5 = c^7 + \bar{c}^7 = 2$ .

**Problem 12.2** Examples of Steiner systems for the given parameters are as follows.

- (a)  $\{1, 2, 3\} \{1, 4, 5\} \{1, 6, 7\} \{1, 8, 9\} \{2, 4, 6\} \{2, 5, 8\}$   
 $\{2, 7, 9\} \{3, 4, 9\} \{3, 5, 7\} \{3, 6, 8\} \{4, 7, 8\} \{5, 6, 9\}.$
- (b)  $\{1, 2, 3, 4\} \{1, 5, 6, 7\} \{1, 8, 9, 10\} \{1, 11, 12, 13\} \{2, 5, 8, 11\} \{2, 6, 9, 12\} \{2, 7, 10, 13\}$   
 $\{3, 5, 9, 13\} \{3, 6, 10, 11\} \{3, 7, 8, 12\} \{4, 5, 10, 12\} \{4, 6, 8, 13\} \{4, 7, 9, 11\}.$
- (c)  $\{1, 2, 3, 4\} \{1, 2, 5, 6\} \{1, 2, 7, 8\} \{1, 3, 5, 7\} \{1, 3, 6, 8\} \{1, 4, 5, 8\} \{1, 4, 6, 7\}$   
 $\{2, 3, 5, 8\} \{2, 3, 6, 7\} \{2, 4, 6, 8\} \{2, 4, 5, 7\} \{3, 4, 5, 6\} \{3, 4, 7, 8\} \{5, 6, 7, 8\}.$
- (d)

$\{1, 2, 3, 4, 5\}$	$\{1, 2, 3, 6, 7\}$	$\{1, 2, 3, 8, 9\}$	$\{1, 2, 3, 10, 11\}$	$\{1, 2, 4, 6, 9\}$	$\{1, 2, 4, 7, 10\}$
$\{1, 2, 4, 8, 11\}$	$\{1, 2, 5, 6, 11\}$	$\{1, 2, 5, 7, 8\}$	$\{1, 2, 5, 9, 10\}$	$\{1, 2, 6, 8, 10\}$	$\{1, 2, 7, 9, 11\}$
$\{1, 3, 4, 6, 8\}$	$\{1, 3, 4, 7, 11\}$	$\{1, 3, 4, 9, 10\}$	$\{1, 3, 5, 6, 10\}$	$\{1, 3, 5, 7, 9\}$	$\{1, 3, 5, 8, 11\}$
$\{1, 3, 6, 9, 11\}$	$\{1, 3, 7, 8, 10\}$	$\{1, 4, 5, 6, 7\}$	$\{1, 4, 5, 8, 10\}$	$\{1, 4, 5, 9, 11\}$	$\{1, 4, 6, 10, 11\}$
$\{1, 4, 7, 8, 9\}$	$\{1, 5, 6, 8, 9\}$	$\{1, 5, 7, 10, 11\}$	$\{1, 6, 7, 8, 11\}$	$\{1, 6, 7, 9, 10\}$	$\{1, 8, 9, 10, 11\}$
$\{2, 3, 4, 6, 11\}$	$\{2, 3, 4, 7, 9\}$	$\{2, 3, 4, 8, 10\}$	$\{2, 3, 5, 6, 8\}$	$\{2, 3, 5, 7, 10\}$	$\{2, 3, 5, 9, 11\}$
$\{2, 3, 6, 9, 10\}$	$\{2, 3, 7, 8, 11\}$	$\{2, 4, 5, 6, 10\}$	$\{2, 4, 5, 8, 9\}$	$\{2, 4, 5, 7, 11\}$	$\{2, 4, 6, 7, 8\}$
$\{2, 4, 9, 10, 11\}$	$\{2, 5, 6, 7, 9\}$	$\{2, 5, 8, 10, 11\}$	$\{2, 6, 7, 10, 11\}$	$\{2, 6, 8, 9, 11\}$	$\{2, 7, 8, 9, 10\}$
$\{3, 4, 5, 6, 9\}$	$\{3, 4, 5, 7, 8\}$	$\{3, 4, 5, 10, 11\}$	$\{3, 4, 6, 7, 10\}$	$\{3, 4, 8, 9, 11\}$	$\{3, 5, 6, 7, 11\}$
$\{3, 5, 8, 9, 10\}$	$\{3, 6, 7, 8, 9\}$	$\{3, 6, 8, 10, 11\}$	$\{3, 7, 9, 10, 11\}$	$\{4, 5, 6, 8, 11\}$	$\{4, 5, 7, 9, 10\}$
$\{4, 6, 7, 9, 11\}$	$\{4, 6, 8, 9, 10\}$	$\{4, 7, 8, 10, 11\}$	$\{5, 6, 7, 8, 10\}$	$\{5, 6, 9, 10, 11\}$	$\{5, 7, 8, 9, 11\}$

This system was constructed ‘ad hoc’ starting with  $\{1, 2, 3, 4, 5\}$ . Other methods are given in the **Web Appendix** to Chapter 12.

(ii) Two non-isomorphic Steiner systems  $S(2, 3, 13)$  with 26 members can be generated as follows. In each case the first 13 members are  $(1, 3, 9)$  (a subset of the set of the quadratic residues mod 13) and its twelve translates by the map  $x \mapsto x + 1$  giving a set of 13 triples in all. The second set of 13 triples can be either  $(1, 2, 5)$  or  $(1, 2, 11)$  and their translates under the same map.

(iii) This is a version of  $S(2, 3, 7)$ .

**Problem ♦ 12.3** If  $u = 1$ , then we are counting those members of the Steiner system which contain  $a_1$ . Ignoring  $a_1$  these members form a version of the system  $S(r - 1, s - 1, t - 1)$ , so use Theorem 12.2 again. Similarly if  $u = 2$ , and we look for the members containing  $a_1$  and  $a_2$ , we have a version of the system  $S(r - 2, s - 2, t - 2)$ . Now carry on.

**Problem 12.4** (i) A non-singular square matrix can be diagonalised using elementary row and column operations, and each of these operations can be performed by pre- or post-multiplying the given matrix by an elementary matrix. Note that as all matrices in  $SL_n(q)$  have determinant 1, the elementary operation that multiplies a row or column by a non-zero constant is not required. For further details see any standard text of linear algebra.

(ii) Examples are as follows. First,  $A_6$  is generated by the perms.  $a = (1, 2, 3, 4, 5)$  and  $b = (1, 4, 6, 3, 2)$ , and  $a$  and  $b$  satisfy the presentation given. Secondly,  $SL_2(9)$  is generated by  $A = \begin{pmatrix} 0 & 1 \\ 2 & c^5 \end{pmatrix}$  and  $B = \begin{pmatrix} c^2 & 1 \\ c^3 & 2 \end{pmatrix}$  (Problem 12.1), where  $A^5 = B^{10} = (AB)^4 = (A^4B)^8 = I_2$ . The group  $L_2(9)$  can be formed by factoring  $SL_2(9)$  by its centre  $Z$ . This centre contains two elements:  $I_2$  and  $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$ , so by ‘identifying’  $A$  and  $-A$  throughout for  $A \in SL_2(9)$  (consider the cosets of  $SL_2(9)$  by its centre) we obtain a group isomorphic to  $A_6$ . This can also be done by using the presentation for  $A_6$  given on page 249. Again working in  $SL_2(9)$  we need four  $2 \times 2$  matrices  $C_i$  which satisfy  $(C_i Z)^3 = Z$  and  $(C_i C_j Z)^2 = Z$  for  $1 \leq i, j \leq 4$  where  $i \neq j$ . One set is given by

$$\begin{pmatrix} 0 & 2 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & c^2 \\ c^2 & 0 \end{pmatrix}, \begin{pmatrix} 1 & c^2 \\ c^2 & 0 \end{pmatrix},$$

where  $c$  is a generator of the multiplicative group of the field  $\mathbb{F}_9$ .

**Problem ♦ 12.5** With  $A$  and  $B$  as given we have  $AB^2AB = \begin{pmatrix} 1 & 0 \\ a^{2p-4} & 1 \end{pmatrix}$  and  $ABAB^2 = \begin{pmatrix} 1 & a^{2-1} \\ 0 & 1 \end{pmatrix}$ ; now take powers and use Lemma 12.8; note that  $p \geq 5$ . The order of  $A$  is  $p-1$  and the order of  $B$  is 3.

**Problem 12.6** (i) Straight-forward calculation.

(ii) Note that  $(0, 0, 1)R = (0, 1, 1)$  so  $R$  maps point 1 to point 2 *et cetera*, similarly for  $S$ . Using the labelling given in pages 253 and 254 we can associate  $R$  with  $(1, 2, 3, 4, 5, 6, 7)$  and  $S$  with  $(1, 7)(3, 6)$ . These give  $R^4S = (1, 5, 2, 3)(4, 7)$  and  $RS = (1, 2, 6)(3, 4, 5)$  as required.

(iii) One solution is as follows. If  $C = SR^3SR^5S = (1, 4, 3)(2, 6, 7)$ , then  $\langle R, C \rangle \simeq F_{7,3}$ , and if  $D = SR^4SR^2S = (1, 3, 7)(2, 5, 4)$ , then  $R^4S \cdot D = (1, 4)(2, 7)$ , that is  $R^4S$  and  $D$  generate a subgroup isomorphic to  $S_4$ , see Problem 3.18.

**Problem 12.7** (i) By Sylow:  $n_7 \equiv 1 \pmod{7}$  and  $n_7 \mid 24$ , so  $n_7 = 8$ , and by Theorem 6.10,  $[G : N_G(P)] = 8$  and  $o(N_G(P)) = 21$ . So as  $H = N_G(P)$  is not Abelian, it is a semi-direct product of  $C_7$  by  $C_3$  (Section 7.3), that is  $H \simeq \langle a, b \mid a^7 = b^3 = e, b^2ab = a^2 \rangle \simeq F_{7,3}$ ,  $ab = ba^2$  and  $ba = a^4b$ .

(ii) As  $o(b) = 3$ ,  $\langle b \rangle$  is a Sylow 3-subgroup of  $G$ . By the Sylow theory,  $n_3 = 4, 7$  or  $28$ .  $n_3 \neq 4$  by Theorem 5.15,  $n_3 \neq 7$ , we leave this as an exercise for the reader, and so  $n_3 = 28$ ,  $o(N_J(\langle b \rangle)) = 6$  and  $N_J(\langle b \rangle) \simeq \langle b, c \mid b^3 = c^2 = e, bc = cb^2 \rangle$ .

(iii) We have eight cosets each with 21 elements, so  $G$  is the union of the cosets in  $\mathcal{C}$  provided we can show that they are disjoint.  $H \neq cH$  as  $c \notin H$ , and if  $cH = acH$  then  $cac \in H$  but as  $H$  is the normaliser of  $\langle a \rangle$  this implies that  $c \in H$  which is impossible. Similar arguments cover the remaining cases.

(iv) Premultiplying each member of  $\mathcal{C}$  by  $g \in G$  permutes  $\mathcal{C}$ , and so we obtain an element of  $S_8$ . Let  $\theta$  be the corresponding map, this is an injective homomorphism, see the first example in Section 5.2. Note that  $G\theta = G\theta'$  as  $G$  is simple, and so  $G\theta \leq S'_8 \simeq A_8$ . Now  $a\theta = (2, 3, 4, 5, 6, 7, 8)$  because

$a \in H$  and so  $aH = H$ , and  $a(a^t cH) = a^{t+1} cH$ . Also as  $ba^t = a^{4t}b$  and  $ba^t cH = a^{4t}bcH$ , we have  $b\theta = (3, 6, 4)(5, 7, 8)$ , as  $bH = H$  (note  $b \in H$ ) and  $b(cH) = cb^2H = cH$ .

(v) and (vi) Continuing as above we have  $c(H) = cH$  and  $c(cH) = c^2H = H$  (as  $o(c) = 2$ ), so  $c\theta$  maps 1 to 2 and 2 to 1. Now  $c\theta$  can map 3 to 5 or 7 or 8. If 3 is mapped to 5, then  $c\theta = (1, 2)(3, 5)(4, 7)(6, 8)$  with similar expressions in the other two cases. We have

$$(3, 6, 4)(5, 7, 8)(1, 2)(3, 5)(4, 7)(6, 8)(3, 4, 6)(5, 8, 7) = (1, 2)(3, 7)(4, 8)(5, 6)$$

*et cetera*, this and similar identities gives the equalities, and the result follows because we started with an ‘arbitrary’ simple group of order 168.

**Problem 12.8** First, the elements of  $L_2(11)$  are defined as cosets each containing pairs of matrices of the form  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$  and  $\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$ , and so  $\theta_A$  has domain  $L_2(11)$ . We have (a) the map  $\theta_A$  is a perm. of  $\mathcal{P}$  as  $A \in L_2(11)$  is non-singular; (b) composition of maps corresponds to matrix multiplication, and (c) the identity map  $z \rightarrow z$  corresponds to the identity matrix  $I_2$ .

For the next part use transvections as discussed in Section 12.2. Note that  $\alpha$  has order 11 and corresponds to the perm.  $(0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10)$ ,  $\beta$  has order 2 and corresponds to the perm.  $(0, \infty)(1, 10)(2, 5)(3, 7)(4, 8)(6, 9)$ , as we are working over the field  $\mathbb{F}_{11}$ . If we set  $a \mapsto \alpha$  and  $b \mapsto \beta$ , then the relations in the presentation (12.5) given on page 261 are satisfied.

**Problem 12.9** By Theorem 5.15, as  $L_2(11)$  is simple it cannot have a proper subgroup of index less than 11, that is of order more than 60. By Lagrange’s Theorem (Theorem 2.27) further possible subgroup orders are 55, 44, 33, 30, 22, 20, 15, 12 and 11 as well as some smaller ones. The group does have (maximal) subgroups of orders 60, 55 and 12 and no others.

To see this each possible order must be checked in turn. So for example it cannot have subgroups of order 15 or 33 as these would be cyclic but the group does not possess elements of order either 15 or 33. Also note that the group has no elements of order 4, and products of elements of orders 2 and 11 give elements of order 3, 5 or 6. On the positive side there are maximal subgroups isomorphic to  $A_5$ ,  $F_{11,5}$  and  $D_6$ .

For  $A_5$ , one method is as follows: Use the presentation  $\mathcal{P}_3$  for  $A_5$  given in Web Section 3.6, choose three elements of  $L_2(11)$  each with order 3 such that the orders of their products is 2 in all cases. One example is

$$(1, 2, 8)(3, 6, 9)(4, 10, 11)(5, 7, 12), (1, 6, 7)(2, 5, 4)(3, 10, 12)(8, 11, 9), \\ (1, 5, 3)(2, 9, 10)(4, 7, 8)(6, 12, 11).$$

This can also be done by using  $\mathcal{P}_2$  from the same Web Section, and choosing two elements of order 5 which satisfy the relevant relations. One choice is

$$(1, 3, 2, 4, 11)(5, 8, 7, 10, 12), (1, 7, 6, 8, 4)(2, 5, 10, 11, 9).$$

For  $F_{11,5}$  generated by an element  $a$  of order 11, and  $b$  of order 5, let  $a$  be the cyclic perm. of order 11 given in the previous problem (ie one not using

the symbol  $\infty$ , here replace  $\infty$  by 12 and add one to each finite symbol), and look for products of two disjoint 5-cycles again not using the symbol  $\infty$ . An example for  $b$  is  $(1, 7, 6, 8, 4)(2, 5, 10, 11, 9)$  where  $b^4ab = a^9$ .

Lastly for  $D_6$ , take  $b$  from the previous problem as a generator of order 2, and look for an element  $c$  of order 6 (that is a product of two disjoint 6-cycles) to satisfy the  $D_6$  relation:  $bcb = c^5$ . One example for  $c$  is  $(1, 5, 4, 11, 10, 3)(2, 8, 9, 12, 6, 7)$ . As above we have replaced the basic symbols  $0, 1, \dots, 10$  by  $1, 2, \dots, 11$ , and  $\infty$  by 12.

**Problem 12.10** First obtain ten equations for the coefficients of an order 2 matrix  $C \in L_3(3)$ , the first is  $\det C = 1$ , and the remaining nine equate corresponding entries in  $C$  and  $C^{-1}$ . The top row of  $C$  can be a triple of elements from the set  $\{0, 1, 2\}$  allowing repetitions except  $(0, 0, 0)$ . Show that for each of these triples there are three corresponding order 2 matrices, except for the triple  $(1, 0, 0)$  when there are nine, and for the triple  $(2, 0, 0)$  when there are 36. One set of order 2 matrices which generate  $L_3(3)$  is

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 2 & 0 \\ 1 & 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 2 & 1 \\ 1 & 1 & 1 \\ 2 & 1 & 1 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 2 & 0 \\ 2 & 0 & 2 \end{pmatrix}.$$

We have  $o(A) = 2, o(BCBC) = 3, o(AC) = 4, o(BC) = 6, o(ABCBC) = 8$  and  $o(ABC) = 13$ . For the second part note that one (of many) solution is:

$$\langle (5, 6, 7)(8, 9, 10)(11, 12, 13), (1, 5, 2)(3, 6, 11)(4, 7, 8)(9, 12, 13) \rangle,$$

and

$$\langle (1, 4)(3, 8)(6, 7)(9, 10), (1, 7)(2, 3)(4, 10)(11, 13), (1, 12)(3, 9)(5, 10)(8, 13) \rangle.$$

It has been shown by Malle, Saxl and Wiegel that all finite groups except  $U_3(3)$  can be generated by three involutions, the proof needs CFSG.

**12.11** (i) Note that  $2^2 \equiv 1 \pmod{3}$ .

(ii) If  $(a_{ij})$  belongs to the centraliser of  $A$ , then  $a_{13} = a_{31}, a_{11} = a_{33}, 2a_{12} = a_{32}$  and  $2a_{21} = a_{23}$ . Further as  $\det(A_{ij}) = 1$ , these give

$$(a_{11} + a_{13})(a_{22}(a_{11} + 2a_{13}) + a_{12}a_{21}) = 1.$$

Count the number of solutions over  $\mathbb{F}_3$ ; there are 12 if  $a_{22} = 0$ , 18 if  $a_{22} = 1$ , and 18 if  $a_{22} = 2$ . Now use Theorem 5.19.

(iii) Using (ii) and the presentation of  $GL_2(3)$  given in Problem 3.24, let

$$a \mapsto \begin{pmatrix} 0 & 1 & 2 \\ 1 & 1 & 2 \\ 2 & 2 & 0 \end{pmatrix}, \quad b \mapsto \begin{pmatrix} 0 & 0 & 2 \\ 0 & 2 & 0 \\ 2 & 0 & 0 \end{pmatrix}, \quad c \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}.$$

Each of these matrices commute with  $A$ , and they generate a copy of  $GL_2(3)$  in  $L_3(3)$ .

**12.12** (i) Examples are:  $A^4$ , order 2;  $(AB)^2$ , order 3;  $A^2$ , order 4;  $AB$ , order 6;  $B$ , order 7;  $A$ , order 8; and  $A^5BAB$ , order 12.

(ii) Note that

$$\det C = c_3 a_1 \overline{a_1} + c_2 a_2 \overline{a_2} + c_1 a_3 \overline{a_3} - a_1 \overline{a_2 a_3} - \overline{a_1} a_2 a_3 - c_1 c_2 c_3 = 1.$$

Also as  $C = C^{-1}$  we have equating corresponding entries

$$\begin{aligned} a_1 \overline{a_1} &= c_1(1 + c_2), & c_1 \overline{a_3} &= a_1(1 + \overline{a_2}) \\ a_2 \overline{a_2} &= c_2 + c_1 c_3, & c_2 \overline{a_2} &= a_2 + \overline{a_1} a_3 \\ a_3 \overline{a_3} &= c_3(1 + c_2), & c_3 \overline{a_1} &= a_3(1 + \overline{a_2}). \end{aligned}$$

Taking  $a_2$  equal to each member of  $\mathbb{F}_9$  in turn, count matrices as follows:

If  $a_2 = 0$ , then  $a_1 a_3 = 0$  (use the fourth equation above). If  $a_1 = 0$ , then  $c_1 \neq 0$  ( $C$  is non-singular), so  $c_2 = 2$  (first equation), so  $a_3 = 0$  (second equation). Hence  $a_1 = a_2 = a_3 = 0$ ,  $c_2 = 2$  and  $c_1 c_3 = 1$  (third equation). There are now two possibilities:  $c_1 = c_3 = 1$  or  $c_1 = c_3 = 2$  giving two (of our 63) matrices. The remaining cases are similar. If  $a_2 = 1$  then  $c_2 = 0$ , we obtain four matrices with  $c_1 = c_3 = 1$  and four with  $c_1 = c_3 = 2$ ; if  $a_2 = 2$  then  $c_2 = 1$ , with one diagonal matrix, eight upper triangular matrices (with  $c_1 = 1$ ), and eight lower triangular (with  $c_3 = 1$ ); if  $a_2 = c$  or  $c^3$  then  $c_2 = 1, c_1 = c_3$ , with 16 matrices; if  $a_2 = c^2$  or  $c^6$  then  $c_2 = 2, c_1 \neq c_3$ ,  $a_1 = a_3 = 0$ , with four matrices; and if  $a_2 = c^5$  or  $c^7$  then  $c_2 = 0, c_1 \neq c_3$ , with 16 matrices. Hence we have found all 63 matrices required.

(iii) One example is as follows. Take

$$c = (5, 8)(6, 7)(9, 12)(10, 11)(13, 16)(14, 15)(17, 20)(18, 19)(21, 24)(22, 23)(25, 28)(26, 27),$$

then an element of order 4 which commutes with this and belongs to the group is

$$d = (5, 6, 8, 7)(9, 10, 12, 11)(13, 20, 16, 17)(14, 19, 15, 18)(21, 27, 24, 26)(22, 28, 23, 25),$$

note that its cube also has this property. Now look for elements of the group whose first cycle(s) are elements of  $S_4$  defined on  $\{1, 2, 3, 4\}$ . You will find that for each element of  $S_4$ , say  $\sigma = (1, 2, 3)$ , there are four elements of  $U_3(3)$  which commute with  $c$  and begin with the chosen cycle; so for our chosen example  $\sigma$  they are

$$(1, 2, 3)(5, 17, 26, 8, 20, 27)(6, 13, 21, 7, 16, 24)(9, 14, 28, 12, 15, 25)(10, 19, 23, 11, 18, 22),$$

and its product with  $d, d^2$  or  $d^3$ . These four elements form a coset (of order 3) of the normal subgroup  $\langle d \rangle$  in  $J$ .

**Problem 12.13** For the first proof note that  $B_1^2$  is diagonal with diagonal entries  $\{a_1^2, a_2^2, a_3^2\}$  so  $B_1$  is an involution only if it belongs to the centre; the top left-hand entry of  $B_3^2$  is zero and so  $B_3$  cannot be an involution; and if  $b_3 = 0$  then  $B_2^2$  has diagonal  $\{b_1^2, b_2, b_2\}$  and the product of these entries must equal 1. Apply (a), then use Problem 5.21(iii) as  $L_3(4) \triangleleft SL_3(4)$  and  $[SL_3(4) : L_3(4)] = 3$ , a prime.

For the second proof note that the order of the centre of the first given Sylow 2-subgroup of  $L_4(2)$  (with order 64) is 2, whilst the order of the centre of the second given Sylow 2-subgroup, now of  $L_3(4)$  and again with order 64, is 4. Hence the groups cannot be isomorphic.

**Problem 12.14** Use the notation  $\alpha_1, \dots$  set up in Section 12.4.

(i) Apply conjugation. For this solution we write  $a \setminus b$  for the conjugate of  $a$  by  $b$ , that is  $b^{-1}ab$ . One solution is as follows:  $\alpha_1 = \phi\psi \setminus \theta^{-1}\phi^{-1}$ ,  $\alpha_2 = \alpha_1^2 \setminus \psi$ ,  $\beta_2 = \psi^3 \setminus \phi^5\nu\theta^4\phi$ ,  $\gamma_1 = \psi^2 \setminus \theta^4\phi^3$ , and  $\gamma_2 = \nu \setminus \gamma_1\beta_2^3$ . For the converse note that  $\phi = (\gamma_2\alpha_1\beta_2\gamma_1)^4 \setminus \psi\alpha_2^2\psi^2\gamma_2$ . For the presentation note that  $\phi\setminus\theta = \phi^4$  and  $\theta\setminus\psi = \theta^2$ .

(ii)  $\langle \alpha_1, \alpha_2 \rangle \simeq C_3 \times C_3$  is a Sylow 3-subgroup,  $\langle \theta \rangle \simeq C_5$  is a Sylow 5-subgroup, and  $\langle \phi \rangle \simeq C_{11}$  is a Sylow 11-subgroup. For the prime 2 we have:  $\delta^8 = \gamma_2^2 = e$  and  $\gamma_2\delta\gamma_2 = \delta^3$ , hence  $\langle \delta, \gamma_2 \rangle$  is a Sylow 2-subgroup. It is isomorphic to a semi-dihedral group of order 16; see Problem 6.4. Note that  $M_{11}$  has 495 Sylow 2-subgroups, 55 Sylow 3-subgroups, 396 Sylow 5-subgroups and 144 Sylow 11-subgroups.

(iii) One method is as follows. Let  $\epsilon = \delta^4 = (1, 4)(2, 6)(3, 5)(8, 9)$  be the chosen involution. By (i)  $\epsilon$  commutes with  $\delta, \gamma_1$  and  $\gamma_2$ , and so after some computer algebra checking we see that  $C_{M_{11}}(\epsilon) = \langle \delta, \gamma_1, \gamma_2 \rangle = H$  with order 48. Note  $M_{11}$  has 165 involutions all of which are conjugate, so by Theorem 5.19 we have  $o(H) = 48$ . Now  $\delta = (1, 2, 9, 3, 4, 6, 8, 5)(10, 11)$ , so if we take  $\nu = (1, 3, 9)(4, 5, 8)(7, 10, 11)$  (then  $\delta\nu = (1, 2)(3, 5)(4, 6)(7, 10)$ ) and  $D = \{e, \epsilon\}$ , then  $\delta D$  and  $\nu D$  generate a copy of  $S_4$  using the standard coset product. Hence  $H$  is isomorphic to an extension of  $C_2$  by  $S_4$ .

(iv) One set of involutions is:

$$\begin{aligned} a &= (4, 7)(5, 8)(6, 9)(10, 11), \\ b &= (1, 10)(2, 5)(4, 11)(8, 9), \\ c &= (1, 5)(2, 9)(3, 11)(8, 10), \\ d &= (2, 3)(5, 6)(8, 9)(10, 11). \end{aligned}$$

**Problem 12.15** (i) The orbits of  $K$  under the coset action are permuted by  $G$ , and as  $G$  is transitive and  $K$  is non-neutral, all of these orbits are of the same order  $p$ , and  $K$  is transitive. From this we see that there is a Sylow  $p$ -subgroup  $Q$  of  $G$  which is a subgroup of  $H$ . By Sylow 2, all Sylow  $p$ -subgroups are conjugate in  $G$ , and so they all belong to  $K$  as  $K$  is normal. Therefore  $o(K) = pn_p s$  where  $s \mid t$  and  $s > 1$ . Now use Problem 6.11(ii) to show that  $K = G$ .

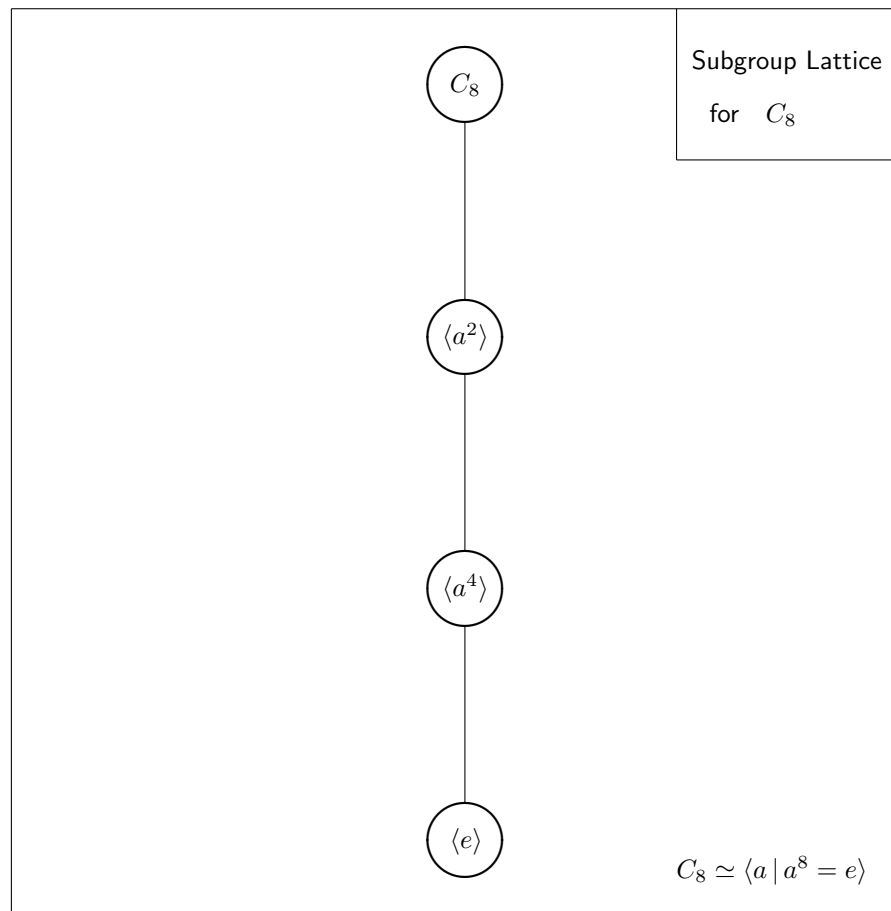
(ii) By our first definition,  $M_{11}$  is a transitive subgroup of  $S_{11}$  and it has order  $n = 7920 = 8 \cdot 9 \cdot 10 \cdot 11$ . We have  $n/11 = 720 \equiv 5 \pmod{11}$ , hence using (i) we can take  $t = 5$  and  $n_{11} = 144 > 1$ , as  $n_{11} \equiv 1 \pmod{11}$ . Now apply (i). For  $M_{23}$  we have  $n' = o(M_{23}) = 48 \cdot 20 \cdot 21 \cdot 22 \cdot 23$ ,  $n'/23 \equiv 11 \pmod{23}$ , so  $t = 11$ ,  $n_{23} = 40320 > 1$ , and  $n_{23} \equiv 1 \pmod{23}$ .

## Subgroup Lattices

The diagrams on this and the next eleven pages illustrate the subgroup lattice structure for groups of order 8 and 12, and two of order 16. They follow the same style as those in the main text. Except possibly for the ‘top’ group all circles in these diagrams represent cyclic groups, and ovals mainly represent direct products of two cyclic groups except where indicated (for  $D_6$ ).

### Subgroups of $C_8$

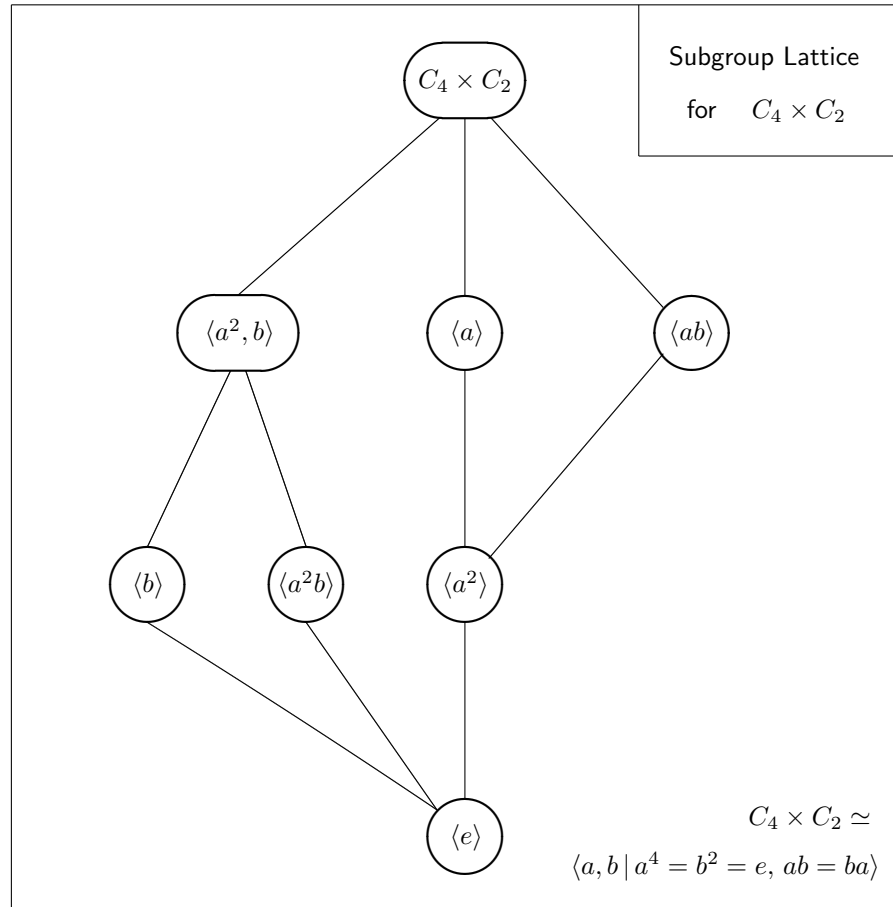
The diagram given below for  $C_8$  is very simple reflecting the fact that prime-power order cyclic groups have only a limited range of subgroups; see Theorem 4.20. The proper non-neutral subgroups are  $\langle a^4 \rangle \simeq C_2$  and  $\langle a^2 \rangle \simeq C_4$ .





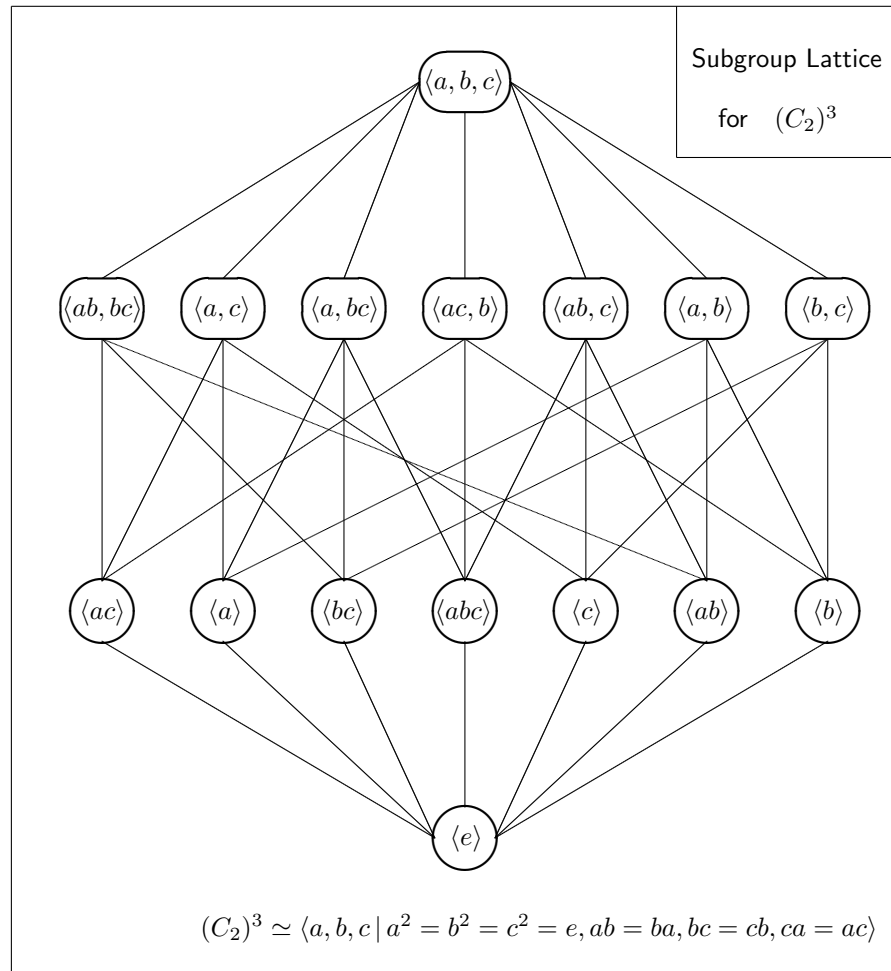
### Subgroups of $C_4 \times C_2$

The second diagram gives the lattice structure for  $C_4 \times C_2$ , note that it is slightly more complicated than that given on the previous page for  $C_8$ . The proper non-neutral subgroups are  $\langle a^2 \rangle$ ,  $\langle b \rangle$  and  $\langle a^2b \rangle$  isomorphic to  $C_2$ ,  $\langle a \rangle$  and  $\langle ab \rangle$  isomorphic to  $C_4$ , and  $\langle a^2, b \rangle$  isomorphic to  $T_2$ .



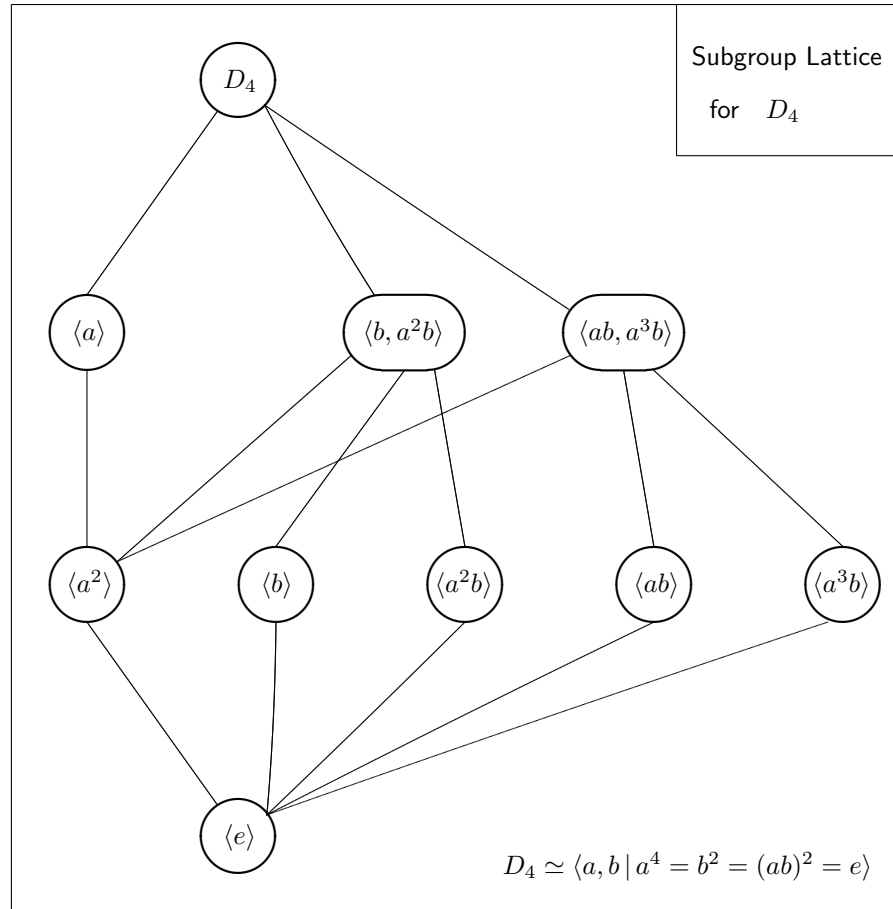
### Subgroups of $(C_2)^3$

Of the groups illustrated the lattice structure for  $(C_2)^3$  given below is one of the most complicated. The proper non-neutral subgroups are  $\langle a \rangle, \dots, \langle abc \rangle$ , seven in all each isomorphic to  $C_2$ , and seven copies of  $T_2$  as given in the diagram below. Also the automorphism group for this group is isomorphic to  $L_2(7)$  ( $\simeq L_3(2)$ ) with order 168. If we treat  $(C_2)^3$  as a three-dimensional vector space over  $\mathbb{F}_2$  (Problem 4.18), then an automorphism of the group corresponds to a non-singular linear map of this vector space. These maps ‘permute’ the seven non-neutral elements  $a, b, \dots, abc$ , see the lower main row in the diagram.



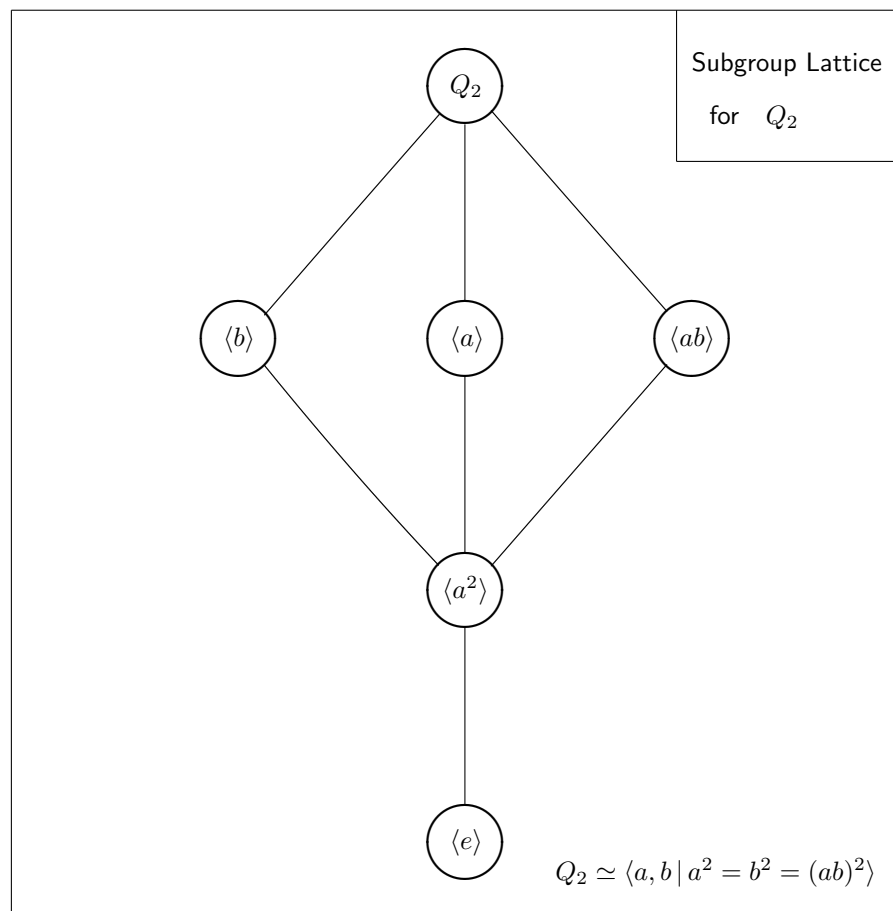
### Subgroups of $D_4$

The fourth diagram illustrates the subgroup structure for the dihedral group  $D_4$ . The proper non-neutral subgroups are  $\langle a^2 \rangle$ ,  $\langle b \rangle$ ,  $\langle ab \rangle$ ,  $\langle a^2b \rangle$  and  $\langle a^3b \rangle$  isomorphic to  $C_2$  (the first is normal whilst the others are not),  $\langle a \rangle \simeq C_4$ , and  $\langle b, a^2b \rangle$  and  $\langle ab, a^3b \rangle$  isomorphic to  $T_2$ . These last three subgroups are normal, they each have index 2 in the main group.

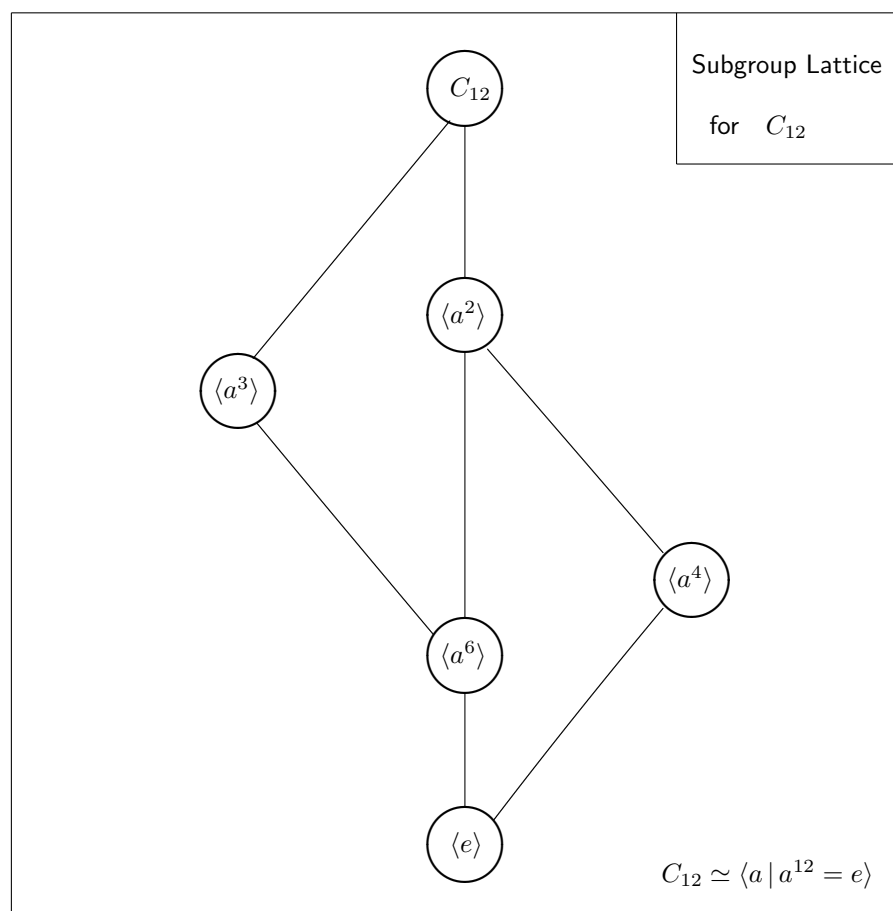


### Subgroups of $Q_2$

The last of the order 8 group diagrams is for the quaternion group  $Q_2$ . Notice that it has a rather simple structure. The three cyclic subgroups,  $\langle a \rangle$ ,  $\langle b \rangle$  and  $\langle ab \rangle$ , have index 2 and so are normal, the centre is  $\langle a^2 \rangle$  with order 2, and the remaining subgroups are  $\langle e \rangle$  and the group itself. Hence all of its subgroups are normal – a rare occurrence, and the group is called *Hamiltonian*. See the discussion on page 119.

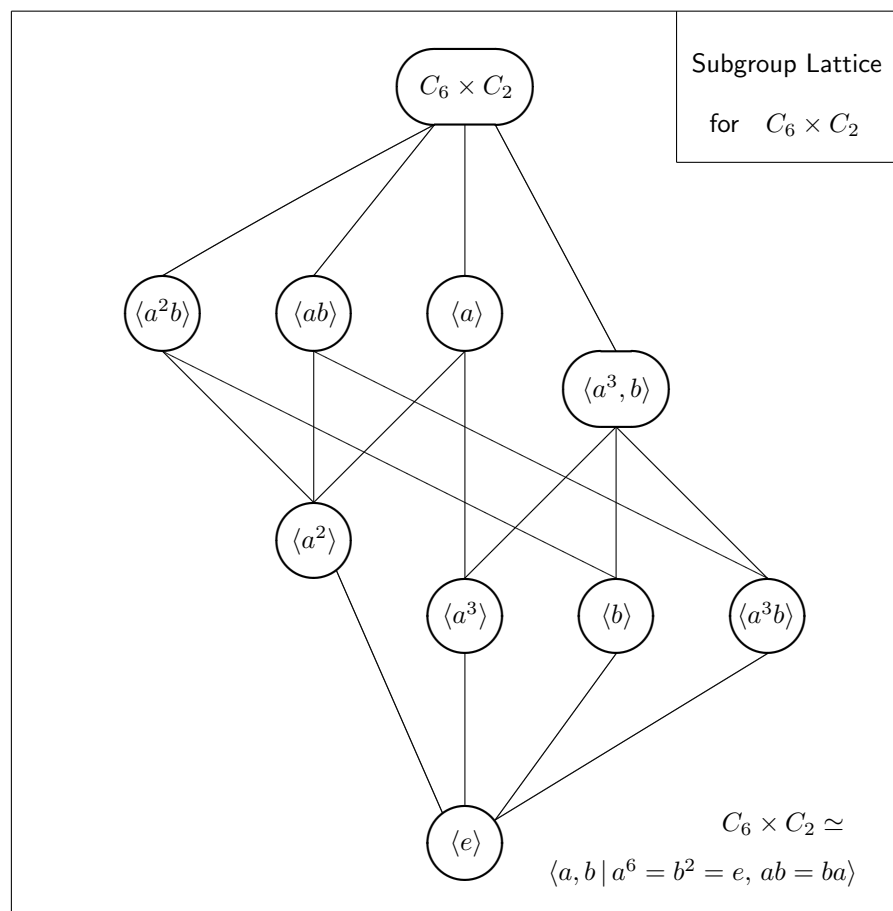


The first of the diagrams of the order 12 groups is for  $C_{12}$ , it is slightly more complicated than that for  $C_8$  because the integer 12 have more divisors. The proper non-neutral subgroups are  $\langle a^6 \rangle \simeq C_2$ ,  $\langle a^4 \rangle \simeq C_3$ ,  $\langle a^3 \rangle \simeq C_4$  and  $\langle a^2 \rangle \simeq C_6$ .



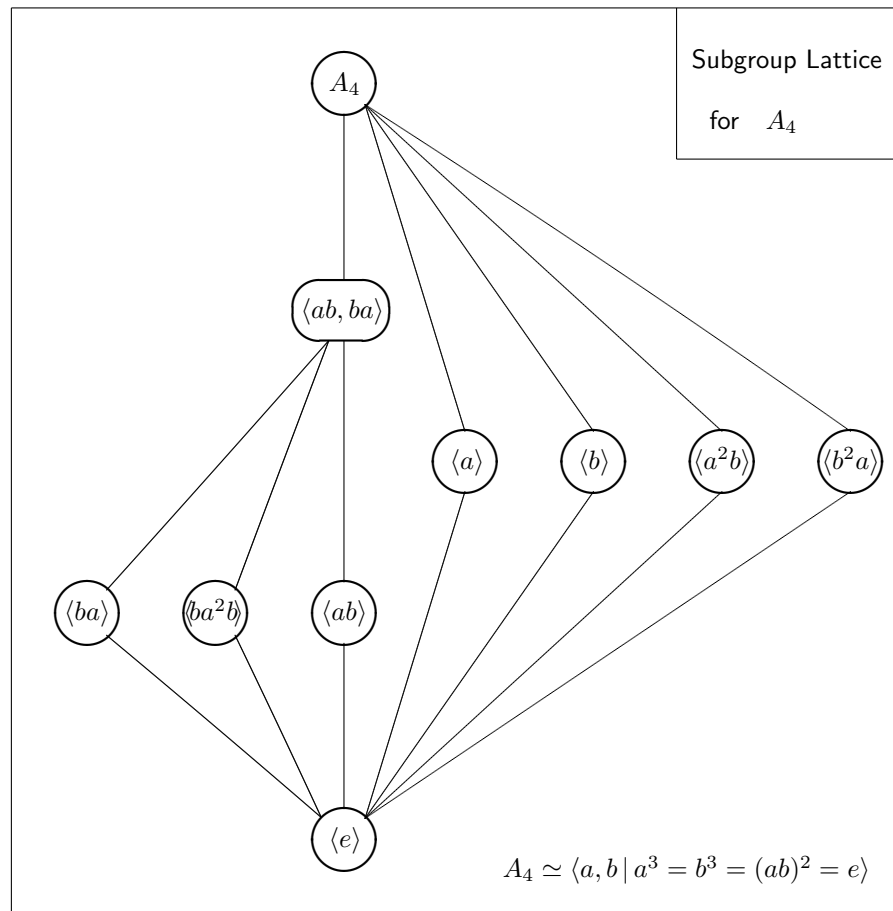
**Subgroups of  $C_6 \times C_2$** 

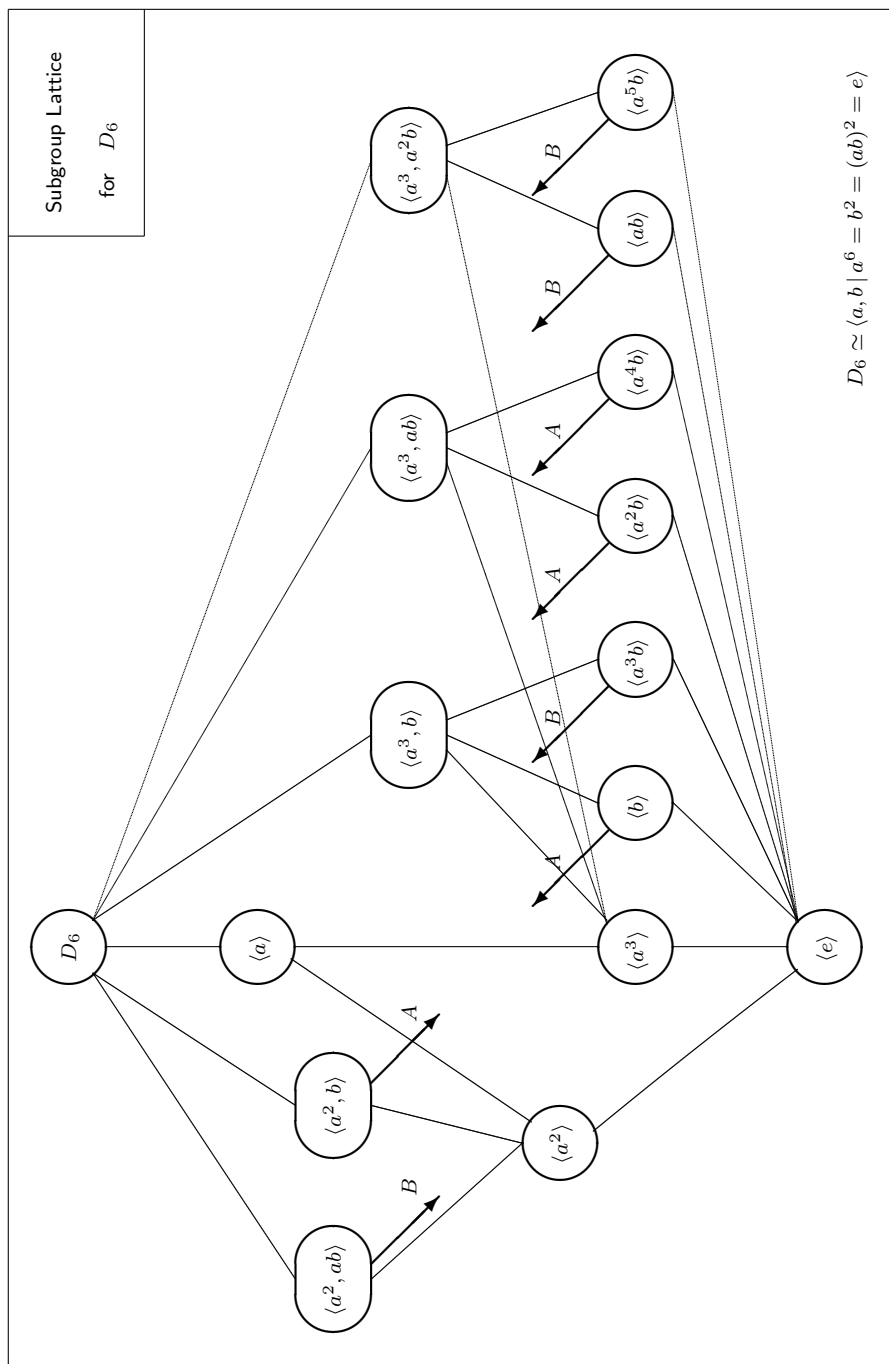
This diagram is for the group  $C_6 \times C_2$ , it has a similar structure to that for  $C_4 \times C_2$ . The proper non-neutral subgroups are  $\langle a^3 \rangle$ ,  $\langle b \rangle$  and  $\langle a^2b \rangle$  isomorphic to  $C_2$ ,  $\langle a^2 \rangle \simeq C_3$ ,  $\langle a^2, b \rangle \simeq T_2$ , and  $\langle a \rangle$ ,  $\langle ab \rangle$  and  $\langle a^2b \rangle$  isomorphic to  $C_6$ .



### Subgroups of $A_4$

The diagram below gives the subgroup lattice structure for the alternating group  $A_4$ . This is the only illustrated group which is not *Reverse Lagrange*, that is  $A_4$  has no subgroups (or elements) of order 6. But unlike all other alternating groups it has a normal subgroup isomorphic to  $C_2 \times C_2$ , its unique Sylow 3-subgroup. The remaining proper non-neutral subgroups are  $\langle ab \rangle$ ,  $\langle ba \rangle$  and  $\langle ba^2b \rangle$  isomorphic to  $C_2$ , and  $\langle a \rangle$ ,  $\langle b \rangle$ ,  $\langle a^2b \rangle$  and  $\langle b^2a \rangle$  isomorphic to  $C_3$ , none of which is normal.

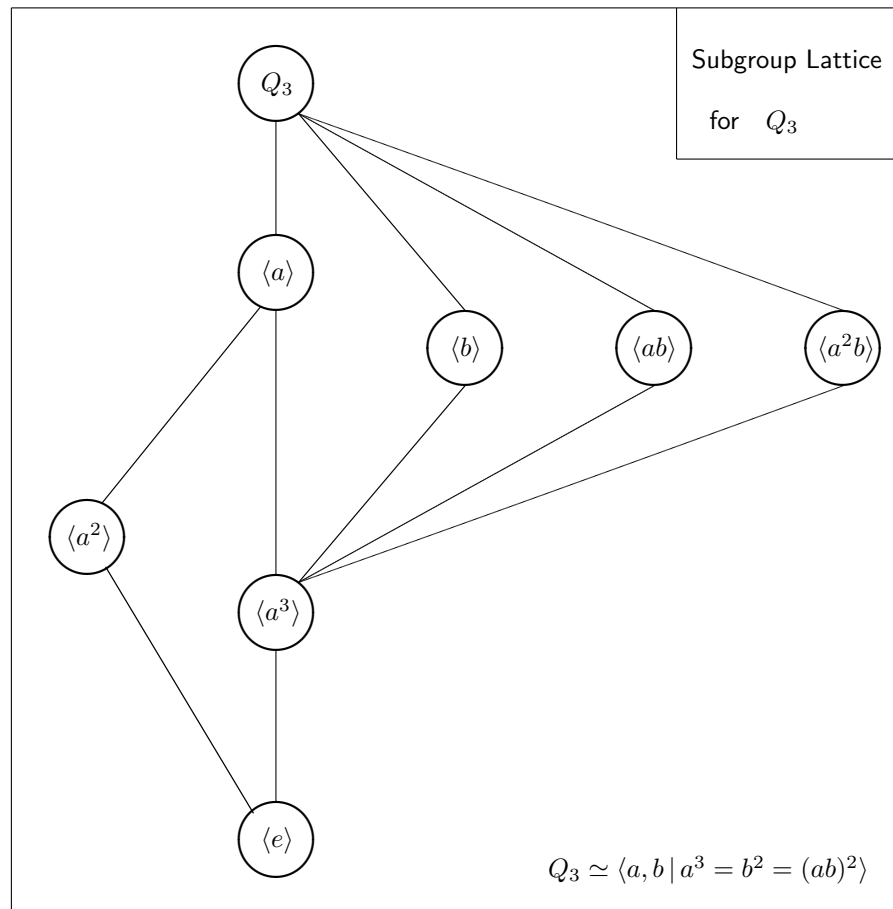






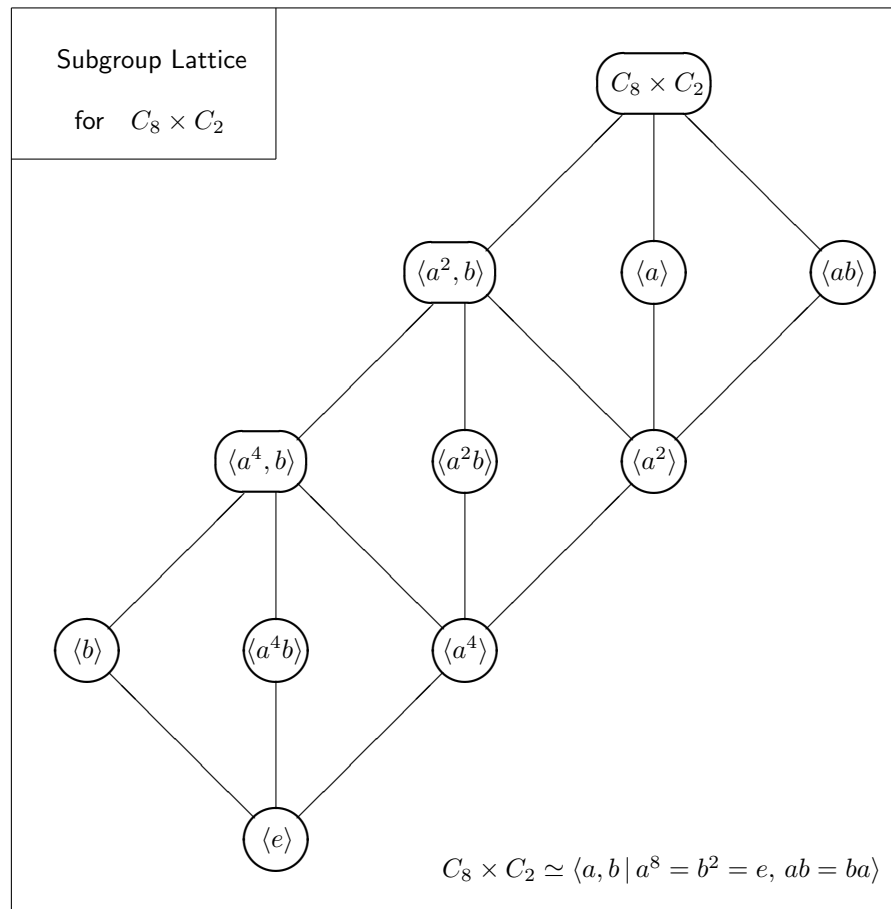
The diagram for  $D_6$  is given on the previous page. It shows that this group has 14 proper non-neutral subgroups, they are  $\langle a^3 \rangle, \langle b \rangle, \langle a^3 b \rangle, \langle a^2 b \rangle, \langle a^4 b \rangle, \langle ab \rangle$  and  $\langle a^5 \rangle$  each isomorphic to  $C_2$  (the first is normal but the others are not);  $\langle a^2 \rangle \simeq C_3$ ;  $\langle a^3, b \rangle, \langle a^3, ab \rangle$  and  $\langle a^3, a^2 b \rangle$  isomorphic to  $T_2$ ;  $\langle a \rangle \simeq C_6$ ; and  $\langle a^2, b \rangle$  and  $\langle a^2, ab \rangle$  isomorphic to  $D_3$ . The last three and  $\langle a^2 \rangle$  are normal.

The last order 12 group diagram is for the dicyclic group  $Q_3$ . Note the similarity to that for  $Q_2$  given on page 551. Note also all of its proper non-neutral subgroups are cyclic, they are  $\langle a^3 \rangle \simeq C_2$ ,  $\langle a^2 \rangle \simeq C_3$  and  $\langle a \rangle \simeq C_6$  which are all normal, and  $\langle b \rangle$ ,  $\langle ab \rangle$  and  $\langle a^2b \rangle$  isomorphic to  $C_4$ .

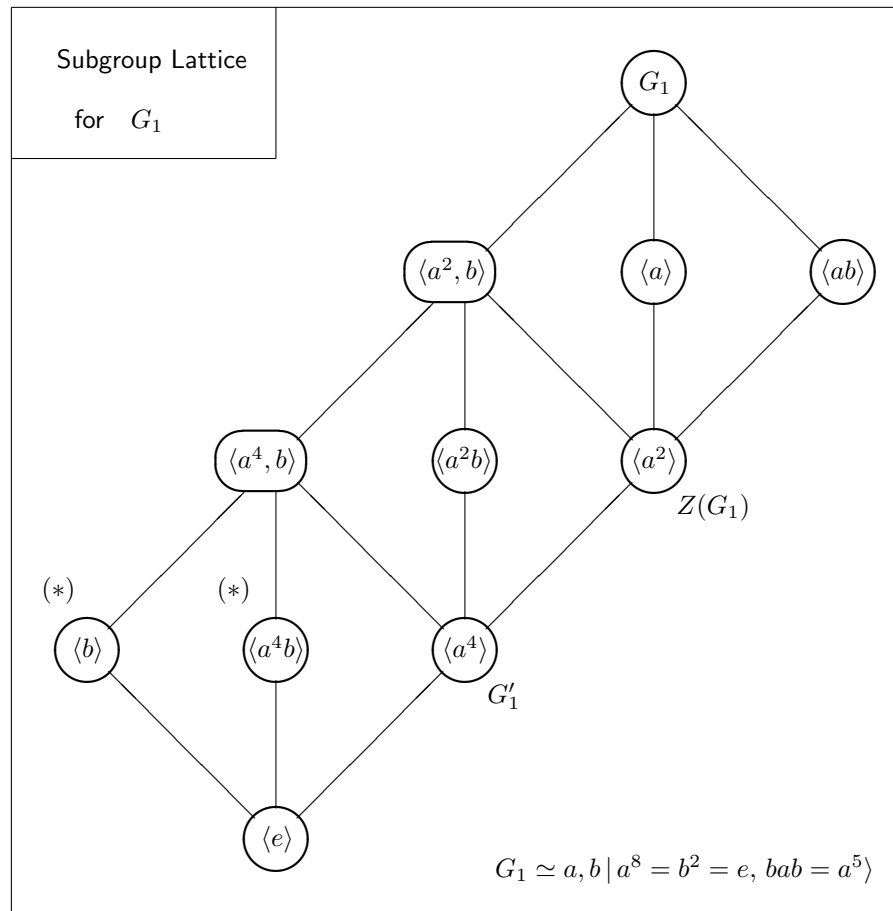


### Subgroups of $C_8 \times C_2$

The last two diagrams are for two particular groups of order 16, see Problem 8.12. They are identical except for their 'top' groups, and so illustrate the fact that particular groups cannot be characterised by their subgroup lattice diagrams alone. The first of these, for  $C_8 \times C_2$ , should be compared with those for  $C_4 \times C_2$  and  $C_6 \times C_2$ . The proper non-neutral subgroups are  $\langle a^4 \rangle$ ,  $\langle b \rangle$  and  $\langle a^4b \rangle$  isomorphic to  $C_2$ ,  $\langle a^2 \rangle$  and  $\langle a^2b \rangle$  isomorphic to  $C_4$ ,  $\langle a^4, b \rangle \simeq T_2$ ,  $\langle a \rangle$  and  $\langle ab \rangle$  isomorphic to  $C_8$ , and  $\langle a^2, b \rangle \simeq C_4 \times C_2$ .



As noted above the subgroup diagram below for the group  $G_1$  which was defined in Problem 6.4 is identical to that for  $C_8 \times C_2$  given on page 557, and so its list of proper subgroups is identical. But many other features are different. For example in the normal subgroup structure the two subgroups isomorphic to  $C_2$  marked with (\*) should be deleted, the centre of the group is  $\langle a^2 \rangle$  (not the whole group), and the derived subgroup  $G'_1$  is  $\langle a^4 \rangle$  (and not  $\langle e \rangle$ ).





<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