

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	341
4.8	Problems 4W	???
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 5W	367
Web Section 7.5	Infinite Abelian Groups. A Brief Introduction	371
Web Section 9.4	Schur-Zassenhaus Theorem	381
9.5	Problems 9W	???

Web Section 12.6	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	389
12.7	Problem 12W	396
Web Chapter 13	Representation and Character Theory	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
Web Chapter 14	Character Tables and Theorems of Burnside and Frobenius	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
Web Solution Appendix	Answers and Solutions, Problems 2	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

Note: The following web material will be added later: Sections 4.6, 4.7, 4.8, 5.4, 5.5, 6.5, 6.6, 7.5, 9.4, 9.5, 12.6 and 12.7, and Chapters 13 and 14.

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 100,¹ 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 2×2 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

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

¹ 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 ξ_σ , 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 σ 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 ξ_σ is called the *standard conjugator* for σ .

(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 τ is a $(4r - 1)$ -cycle \times 1-cycle;

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

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

if $n = 4r + 3$, then τ 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 σ , 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 σ and τ 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} .

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 α and f_2 to β in the definition on page 3. Not Abelian.

(vii) If θ and ϕ 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 θ is an isometry (and so is a bijection), then θ^{-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 θ^{-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 σ and τ are perms. which fix 3, so do $\sigma\tau$ and σ^{-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 ι , 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:

$$\begin{aligned} (ab)^{t+1} &= ab(ab)^t = aba^t b^t [b, a]^{t(t-1)/2} \\ &= a^{t+1} a^{-t} b a^t b^{-1} b^{t+1} [b, a]^{t(t-1)/2} \\ &= a^{t+1} [a^t, b^{-1}] b^{t+1} [b, a]^{t(t-1)/2} \\ &= a^{t+1} b^{t+1} [b, a]^{t(t+1)/2}. \end{aligned}$$

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 θ 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 θ 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 α 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 σ and τ 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 σ , the cycle (\dots, b, a) occurs in τ 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) σ has the form $(i, i\sigma, i\sigma^2, \dots)$ and τ 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 σ is k and of τ 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 τ_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 ι are synonymous.

Problem 3.5 If $\sigma \in S_n$, then $\sigma = \tau_1 \tau_2 \dots \tau_r$ where each τ_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 σ 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 τ_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 τ_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 τ_r followed by a power of σ . 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 τ 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 σ_1 and σ_2 are perms. of Y , and τ_1 and τ_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 σ is a perm. on $Y = \{1, \dots, n\}$, and τ 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 ξ 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 π 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 τ 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 σ 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 ± 1 , and so the determinant equals ± 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 σ is a product of an even number of 2-cycles (that is, it is even), then the determinant of the matrix corresponding to σ 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 2×2 matrix $C \in GL_2(4)$ we define a 4×4 matrix $C^* \in GL_4(2)$ as follows: if 0 occurs in C replace it by the 2×2 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 2×2 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

$$\begin{aligned} & \left((a_{12}a_{23} - a_{13}a_{22})/a_{11}a_{22}a_{33}, \dots, \right. \\ & \left. (a_{n-2,n-1}a_{n-1,n} - a_{n-2,n}a_{n-1,n-1})/a_{n-2,n-2}a_{n-1,n-1}a_{nn} \right), \end{aligned} \quad (3.4)$$

(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_∞ 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 θ_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 $g, h \in G$, $(g \circ h)(\phi\psi) = ((gh)\phi)\psi = (g\phi h\phi)\psi$ [ϕ is a homomorphism] $= (g\phi)\psi(h\phi)\psi$ [ψ 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 ϕ' is well-defined, and it is a homomorphism because ϕ is a homomorphism.

(iv) The map ϕ is an isomorphism, and so it is a bijection, hence ϕ^{-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 ϕ 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 θ 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 θ 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 θ' 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 θ 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 ψ is surjective because θ 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 θ 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 $(1, 2)(1, 2, 3, 4, 5)(1, 2) = (1, 3, 4, 5, 2) \notin G$, and also 6 is not prime!

Problem 4.14 (i) The map ξ is well-defined, for if $aJ = bJ$ then $a \in bJ \subseteq bK$, and so $aK = bK$ by Lemma 2.22. Now ξ 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 $rx = \sum_{g \in G} rm_g g$ 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 θ_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 θ 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 ϕ 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

$$\psi_i : a \mapsto a^{2i+1}, b \mapsto b \quad \text{for } i = 0, 1, 2, 3.$$

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 ψ_0, ψ_2 and ϕ 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 ψ 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

$$(1, 4)(2, 6)(3, 5), (1, 2)(3, 4)(5, 6), (1, 4)(2, 5)(3, 6) \text{ and } (1, 5)(2, 6)(3, 4)$$

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 ϕ is an automorphism, so is ϕ^{-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 ν 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 ϕ is an automorphism of G , then $K\phi = K$ by (i). Hence if we restrict the domain of ϕ 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 ψ 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 ϕ 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 ϕ maps H to itself, that is H is a characteristic subgroup of G .

(vi) Let ϕ 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 ϕ^{-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 ϕ 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 σ maps $\mathbb{Q}[x_1, \dots, x_n]$ into itself. If ι 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 σ 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 $a g^{-1} h g = g^{-1} h g a$ 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 τ , also any power of τ commutes with τ . 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 3×3 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 θ 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 $0 \leq s < 2$. 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 ϕ 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 $C_3 \times C_3 \simeq \langle (1, 2, 3), (4, 5, 6) \rangle$ 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 σ and τ 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 θ 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 θ 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 θ 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 ϕ_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 ψ 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 θ 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 ϕ and ψ 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 ξ is easily seen to be injective as ϕ and ψ 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 ϕ_1 by $g\phi_1 = (g, e)\chi^{o(H)}$. The automorphism ψ_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 ϕ 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 ϕ and ψ 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 ϕ 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 ξ_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 ξ 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 ξ 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 γ , say, maps b^{2k} to e and b^{2k+1} to t , and so $b^r a^s b^u a^v = b^{r+u} (a^s (b^u \gamma)) a^v$ 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 θ 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 γ_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 θ_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 ϑ_a is an automorphism, if $z\vartheta_a = e$ then $z = e$. Applying ϑ_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 ψ 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 θ 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 θ 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 θ 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 2×2 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, θ_g say, of K , that is θ_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 $J = J \cap (C_G(F(G)))F(G)$ 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 θ 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 $K \not\subseteq H$, 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 2×2 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 θ 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 θ_A has domain $L_2(11)$. We have (a) the map θ_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 α has order 11 and corresponds to the perm. $(0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10)$, β 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 ∞ , here replace ∞ by 12 and add one to each finite symbol), and look for products of two disjoint 5-cycles again not using the symbol ∞ . 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 ∞ 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 σ 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 α_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) ϵ commutes with δ, γ_1 and γ_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 δD and νD 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 $n_{23} \equiv 1 \pmod{23}$.

Problems A

Problem A1 (i) $x \in X \cup (Y \cap Z)$ if and only if $x \in X$ or $(x \in Y$ and $x \in Z)$ if and only if $(x \in X$ and $x \in Y)$, or $(x \in X$ and $x \in Z)$ if and only if $x \in (X \cup Y) \cap (X \cup Z)$.

(ii) and (iii) Use a similar argument as that given in (i).

Problem A2 (ia) No; if x is an ancestor of y , then y is not an ancestor of x (a descendant!). (ib) Yes; if x and y have the same mother so do y and x , *et cetera*. The equivalence class of x is his (her) siblings.

(iia) No; $x < x$ and $x < x$ is false. (iib) No; $x < x$ or $x < x$ is also false.

(iii) Yes; a triangle is similar to itself, if x is similar to y then clearly y is similar to x , and if also y is similar to z , then x , y and z are all similar. The equivalence class of x is the set of all triangles that have the same angles to the triangle x .

Problem A3 (i) No; as \emptyset has no elements we cannot form pairs.

(ii) $x \in X$ and $x \in Y$ if and only if $(x, x) \in X \times Y$ and $(x, x) \in Y \times X$. There are n^2 common points.

Problem A4 (i) Not injective; for example (a, b) and $(2a, 2b)$ both map to a/b . Surjective; every fraction a/b has the preimage (a, b) .

(ii) Not injective or surjective; (a, b) and $(a + 1, b - 1)$ both map to $a + b$, and $1/2$, for instance, has no preimage.

(iii) Surjective but not injective; as both (a, b) and (c, b) map to b .

(iv) Bijective; if $2^a \neq 2^b$ then $a \neq b$, and for a positive real a there is a real b ($\log_2 a$) with $2^b = a$.

(v) Injective but not surjective; $a/2 \neq b/2$ implies $a \neq b$, but $1/3$ has no preimage, for instance.

(vi) Surjective but not injective; for example $[1/3] = [2/3]$.

Problem A5 If ψ is not surjective, then there is $y \in Y$ with no preimage; but then ψ is not injective for, by a counting argument, ψ must map at least two elements on the domain to one in the co-domain which implies that ψ is not a function. Argue similarly for the converse. Not true for infinite sets; for example in \mathbb{Z} if $a\psi = a + 1$, then ψ is surjective but not injective, and the converse holds as ψ is defined by: $2a\psi = a$ and $(2a + 1)\psi = a + 1$.

Problem A6 There are n^m functions ϕ from M to N (for each $a \in M$ there are n choices for $a\phi$).

(i) If ϕ is a bijection then $m = n$, and there are $n!$ bijections. (There are n choices for the first argument, $n - 1$ for the second, and so on.)

(ii) There are no injections if $m > n$, and $n!/(n - m)! = n! \binom{n}{m}$ if $m < n$.

(iii) There are $2^m - 2$ surjections if $n = 2$ and $m > 2$. (The only non-surjective maps are those that map the whole of m to 1, or to 2.) Now use

induction, in the general case there are $n^m - \binom{n}{1}(n-1)^m + \binom{n}{2}(n-2)^m - \cdots + (-1)^{m-1}n$ surjections if $m > n$, and none if $n > m$.

Problem A7 (i) The mapping $((x, y), z) \rightarrow (x, (y, z))$ is clearly bijective if $x \in X$, $y \in Y$ and $z \in Z$.

(ii) Use the fact that there is a bijection between \mathbb{Z}^+ and the set of all quadruples of elements of \mathbb{Z} .

(iii) One approach is as follows. For the non-negative rationals a/b first list them by the size of their numerator plus denominator sum $a + b$, and then linearly in increasing order by the size of the rational a/b itself:

$$0/1, 1/1, 1/2, 2/1, 1/3, 2/2, 3/1, 1/4, 2/3, 3/2, 4/1, 1/5, \dots$$

Secondly delete all improper fractions ($2/2$ for example). This gives a list of all positive rationals with no repetition, now count off: $0/1 \rightarrow 0, 1/1 \rightarrow 2, 1/2 \rightarrow 4, 2/1 \rightarrow 6, \dots$, so the n th positive rational is ‘numbered’ $2n$. Now do the same for the negative rationals numbering $-1/1$ by 1, $-1/2$ by 3, and so on. This gives a bijection between the set of the rationals and the set of the positive integers, the ‘standard’ countable set. Another approach uses Theorem B6 discussed in the next Appendix.

Problem A8 Suppose first ϕ is a bijection X to Y . If $y \in Y$ there is a unique $x \in X$ with $x\phi = y$. Define $\psi : Y \rightarrow X$ by $y\psi = x$ and use Theorem A2.

Conversely, if $\phi : X \rightarrow Y$ is such that another map $\psi : Y \rightarrow X$ exists satisfying $\phi \circ \psi = \psi \circ \phi = \iota$, then ϕ is bijective. For if $z \in Y$, then $z = z(\psi \circ \phi) = (z\psi)\phi$, that is $z \in Y$ has a preimage $z\psi \in X$; and secondly if $x_1\phi = x_2\phi$, then $(x_1\phi)\psi = (x_2\phi)\psi$ or $x_1 = x_2$, that is ϕ is injective.

Problem A9 Let $X = \{x, y\}$. (a) If $x \cdot x = x \cdot y = x$ and $y \cdot x = y \cdot y = y$, then operation is associative ($x \cdot y \cdot z = x$), but not commutative ($x \cdot y \neq y \cdot x$). (b) If $x \cdot x = y$ and $x \cdot y = y \cdot x = y \cdot y = x$, then operation is commutative (by definition), but not associative, for $x \cdot (x \cdot y) = x \cdot x = y$, but $(x \cdot x) \cdot y = y \cdot y = x$.

Problems B

Problem B1 Use the basic definitions.

Problem B2 Use Problem B1 and the definition.

Problem B3 Use Theorem B3 and the fact that if $ak > -a$, then $k \geq 0$.

Problem B4 Use induction on r , and assume that $m = 1/n_1 + \cdots + 1/n_r$ where m is a fixed rational number. Assume also that $n_1 \leq n_2 \leq \cdots \leq n_r$, this gives $m \leq r/n_1$, or $n_1 \leq r/m$. By hypothesis, for each $j \leq r/m$ there are only finite $(r-1)$ -tuples $\{n_2, \dots, n_r\}$ satisfying $m - 1/j = 1/n_2 + \cdots + 1/n_r$. Combining these facts gives the result for m . Now set $m = 1$. These numbers are sometimes called *Egyptian fractions*.

Problem B5 If $\mathcal{C} = \{c_1, \dots, c_{\phi(n)}\}$ is a set satisfying: $1 \leq c_i < n$, $(c_i, n) = 1$ and $(c_i, c_j) = 1$ for all $i \neq j$, then the set $\{ac_1, \dots, ac_{\phi(n)}\}$ has the same properties as \mathcal{C} provided $(a, n) = 1$. But modulo n these sets are the same, so the products of their elements are equal modulo n . Now cancel out all c_i from this equality.

Problem B6 Use the basic definitions, and in (iii) use Theorem B3.

Problem B7 By induction show first that $a^{2^n} \equiv 1 \pmod{2^{n+2}}$, so by Theorem B9 we have: $(a, p) = 1$ implies $a^{x(p^r)} \equiv 1 \pmod{p^r}$ for all primes p and positive integers r . Now use Problem B6(iii).

Problem B8 (i) Use induction, the result is true if $r = 2$. By the inductive hypothesis and the binomial theorem we have

$$(1 + ap)^{p^{r-1}} \equiv (1 + ap^{r-1})^p \equiv 1 + ap^r + z \pmod{p^{r+1}}$$

where z is a sum of terms all of which are divisible by p^{2r-1} . The result follows.

(ii) Use (i) with r replaced by $r + 1$, then as it stands.

(iii) Suppose c is a primitive root mod p which satisfies the condition given in the hint, then the order of $c^{p-1} \pmod{p^r}$ is p^{r-1} . Use this fact to obtain the result.

(iv) Note that if $\phi(p_i^{r_i}) > 1$ for $i = j$ and $i = k$, then

$$\text{LCM}(\dots, \phi(p_j^{r_j}), \dots, \phi(p_k^{r_k}), \dots) < \phi(\dots p_j^{r_j} \dots p_k^{r_k} \dots)$$

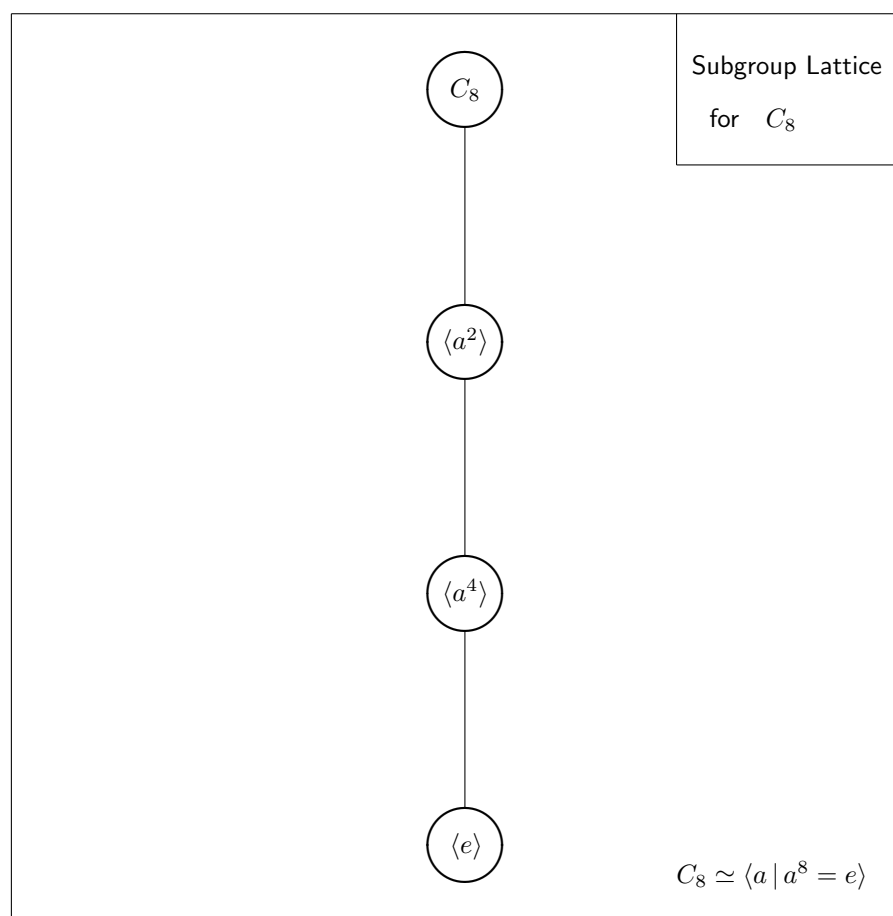
which means that a primitive root cannot exist in this case. For further details, see Rose [1999], pages 90 and 91.

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).

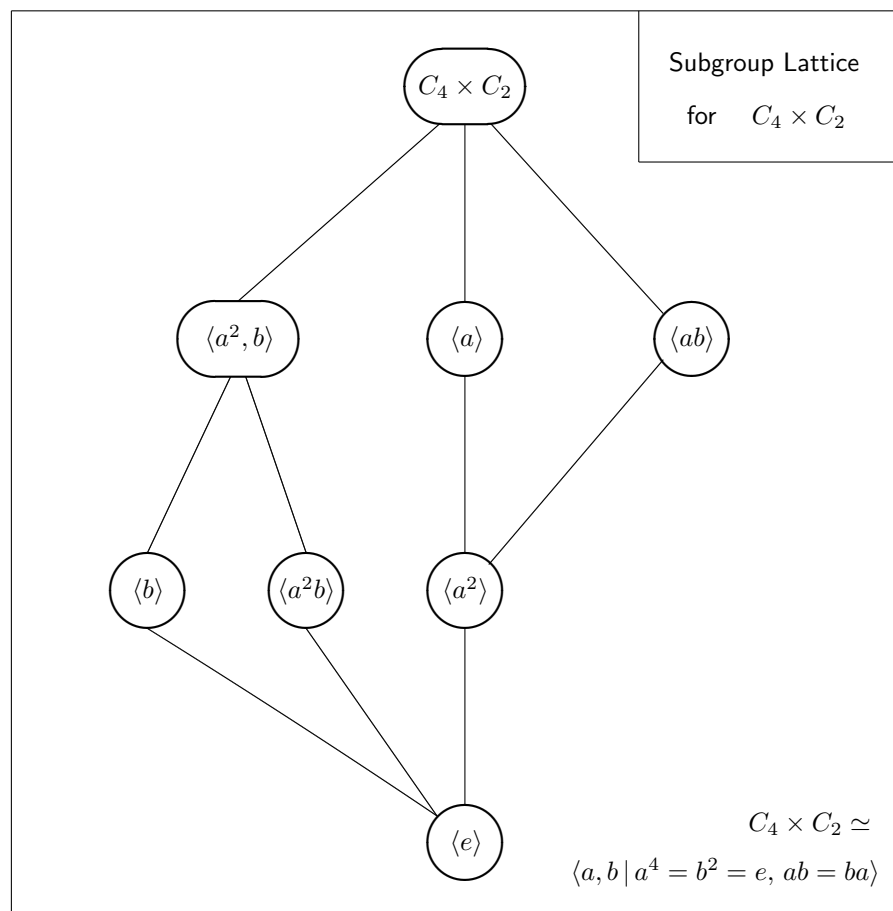
Subgroups of C_8

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 $\langle a^2 \rangle \simeq C_4$.



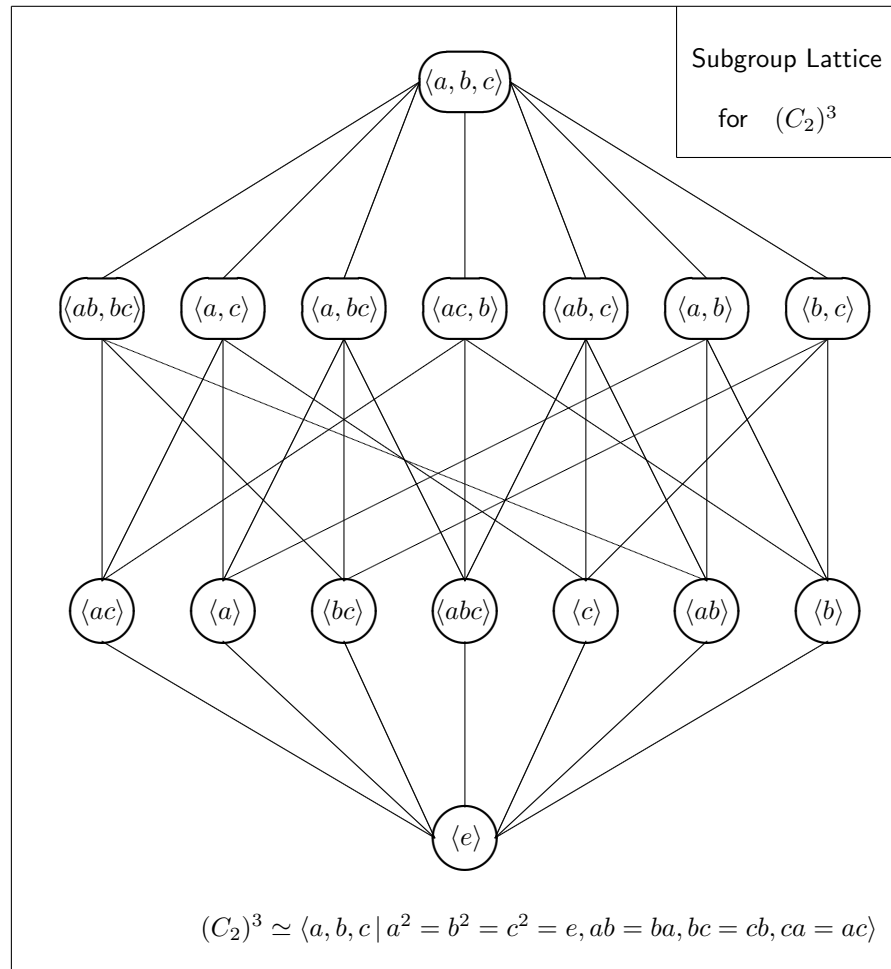
Subgroups of $C_4 \times C_2$

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 .



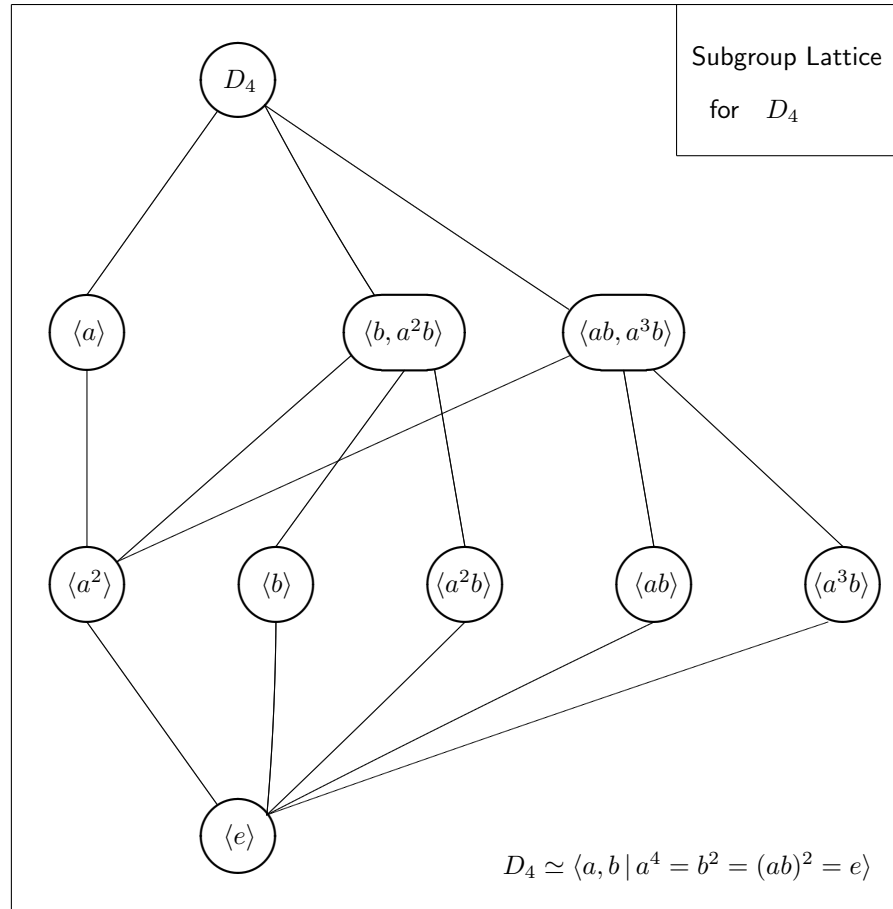
Subgroups of $(C_2)^3$

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.



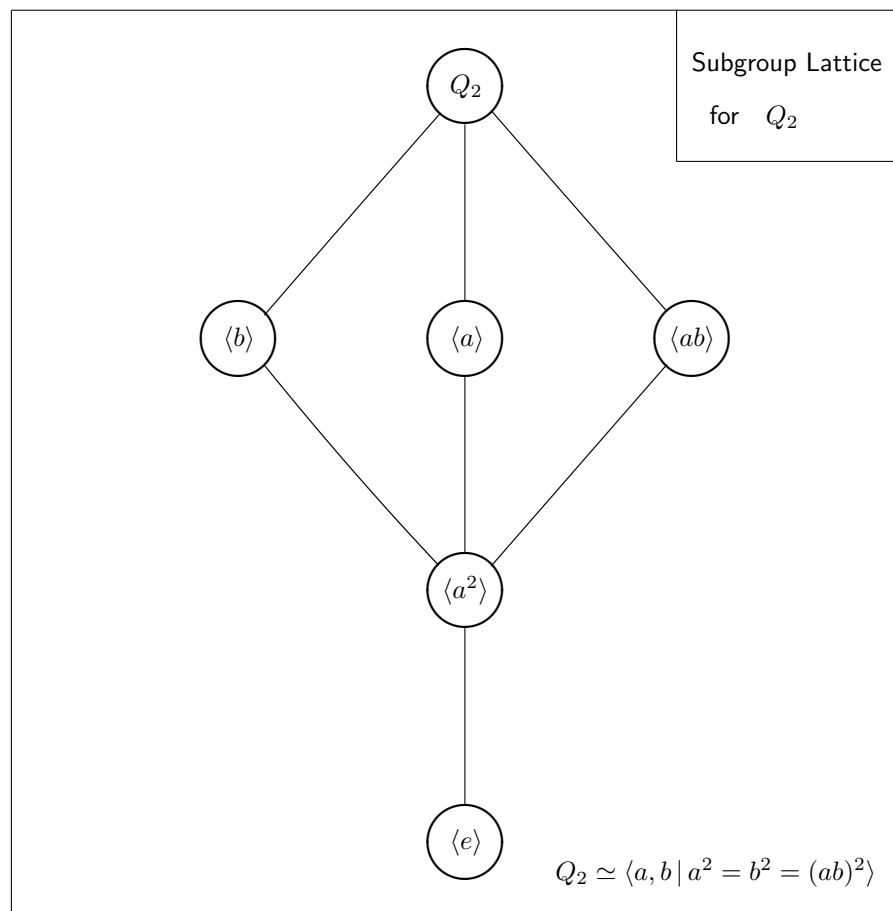
Subgroups of D_4

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.



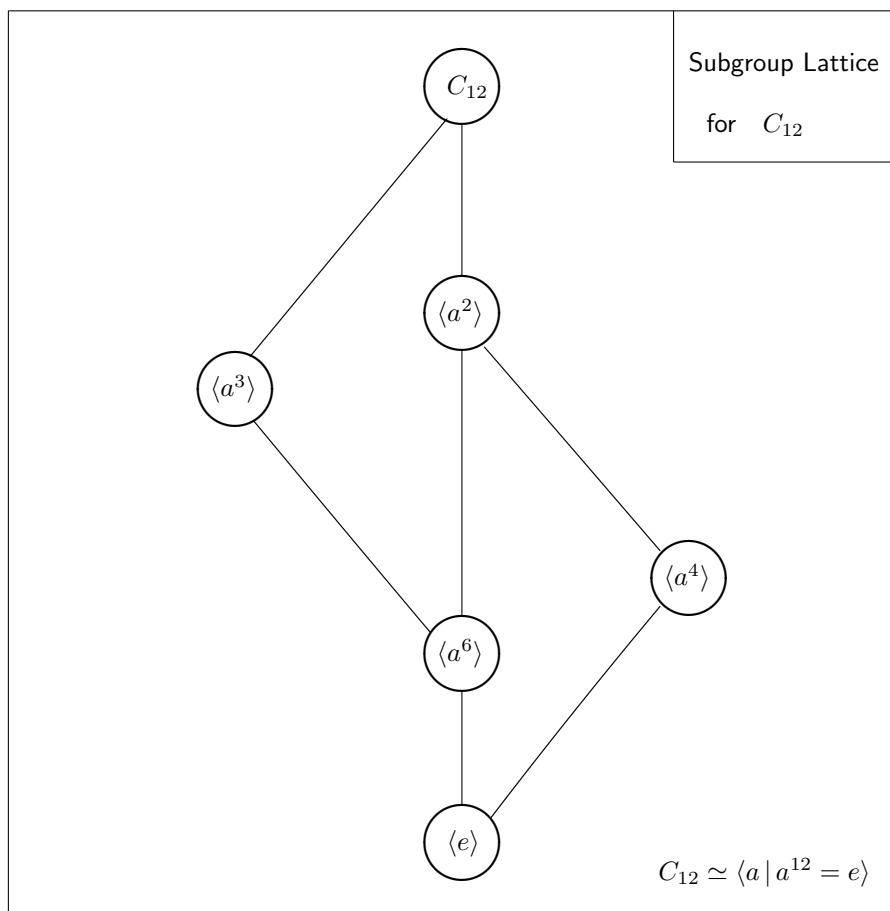
Subgroups of Q_2

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.



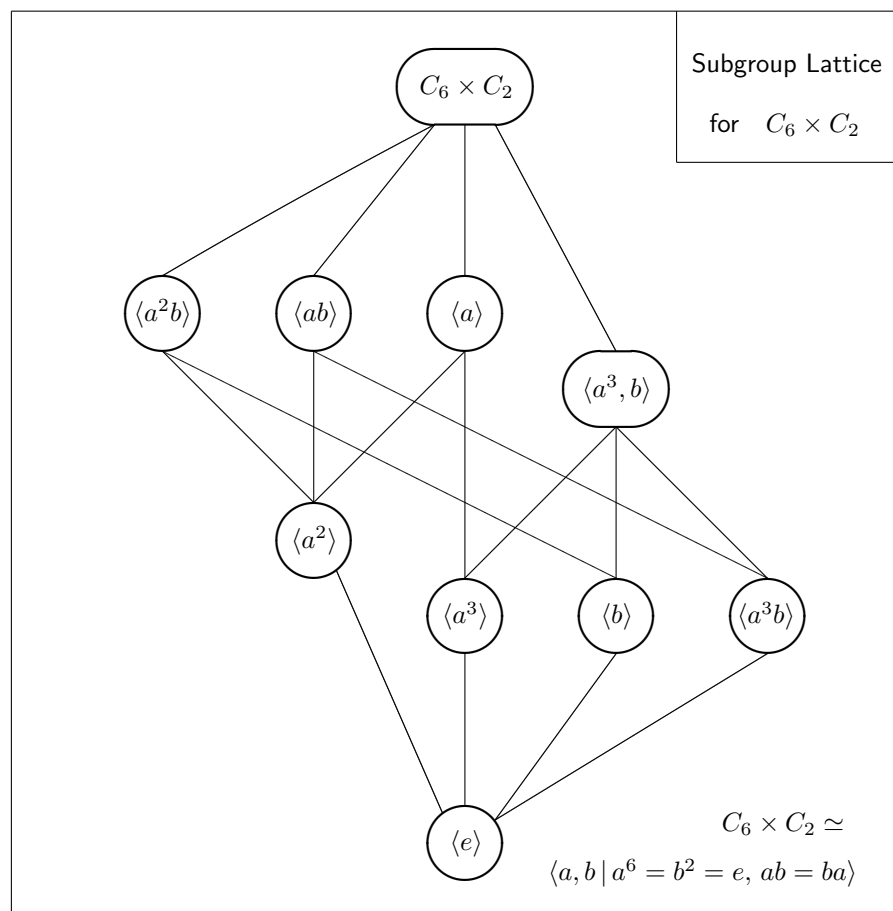
Subgroups of C_{12}

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 $\langle a^2 \rangle \simeq C_6$.



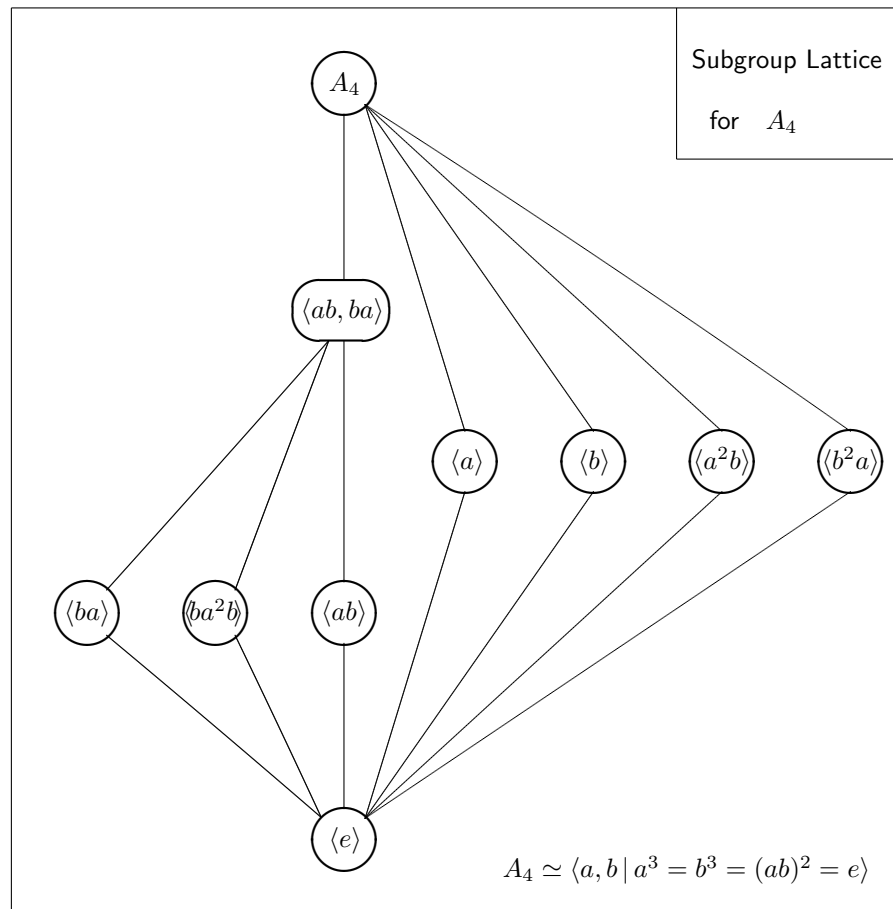
Subgroups of $C_6 \times C_2$

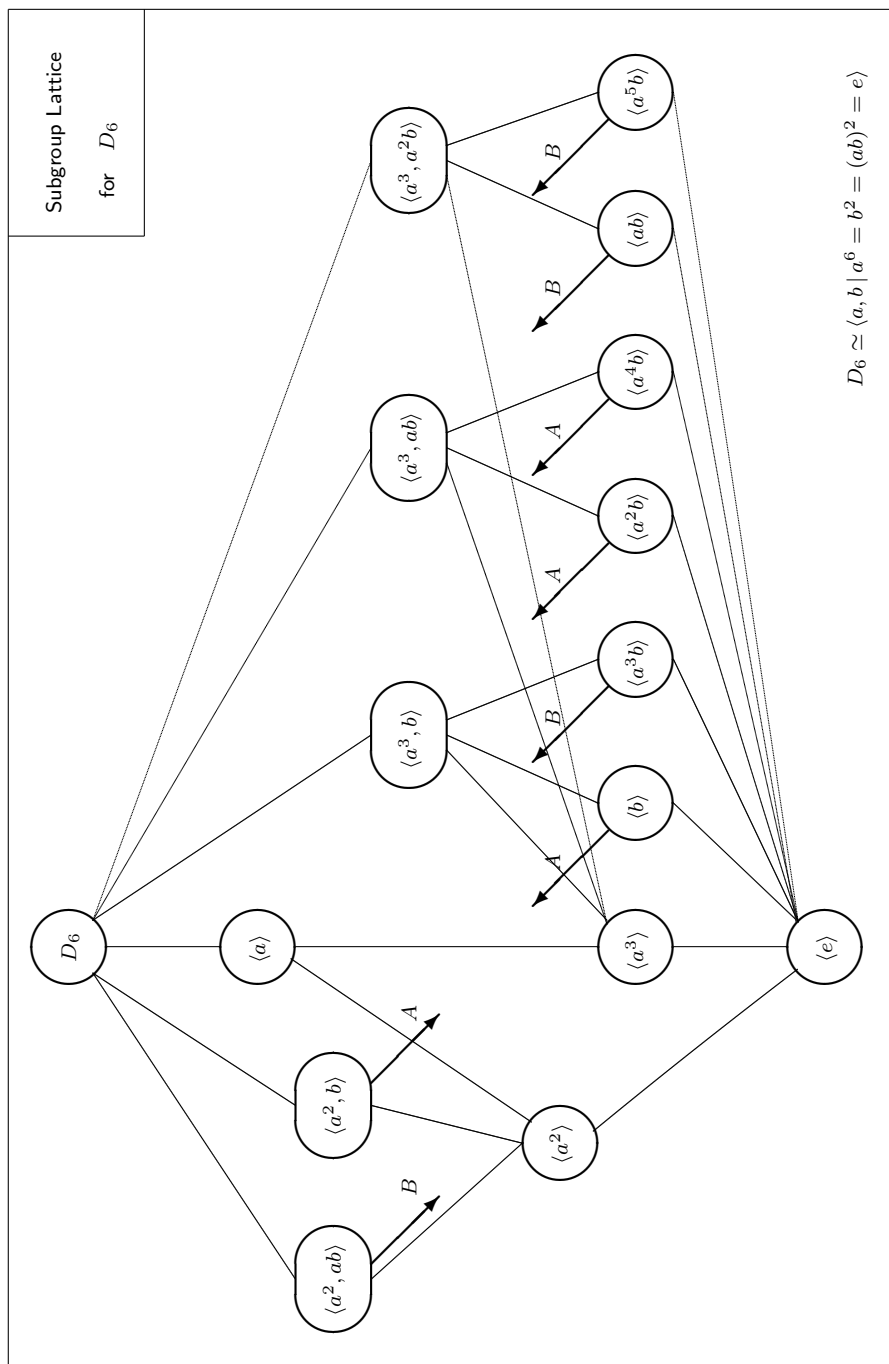
This diagram is for the group $C_6 \times C_2$, it has a similar structure to that for $C_4 \times C_2$. The proper non-neutral subgroups are $\langle a^3 \rangle$, $\langle b \rangle$ and $\langle a^2b \rangle$ isomorphic to C_2 , $\langle a^2 \rangle \simeq C_3$, $\langle a^2, b \rangle \simeq T_2$, 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.



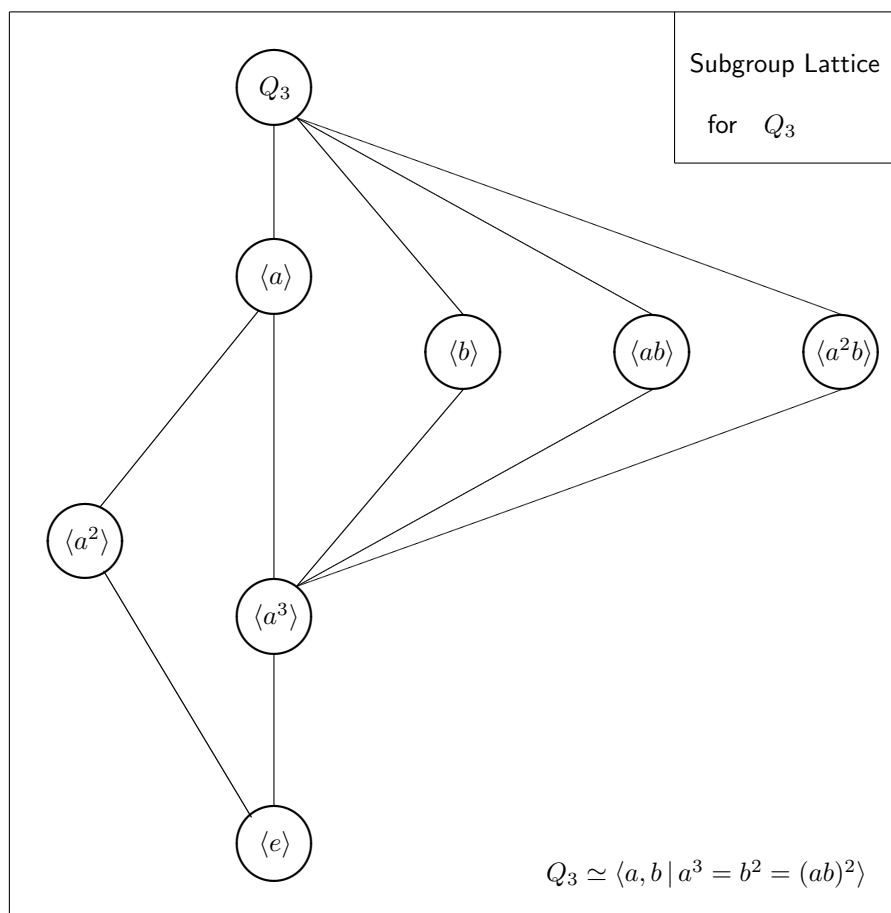


Subgroups of D_6

The diagram for D_6 is given on the previous page. It shows that this group has 14 proper non-neutral subgroups, they are $\langle a^3 \rangle, \langle b \rangle, \langle a^3b \rangle, \langle a^2b \rangle, \langle a^4b \rangle, \langle ab \rangle$ 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 $\langle a^3, a^2b \rangle$ 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.

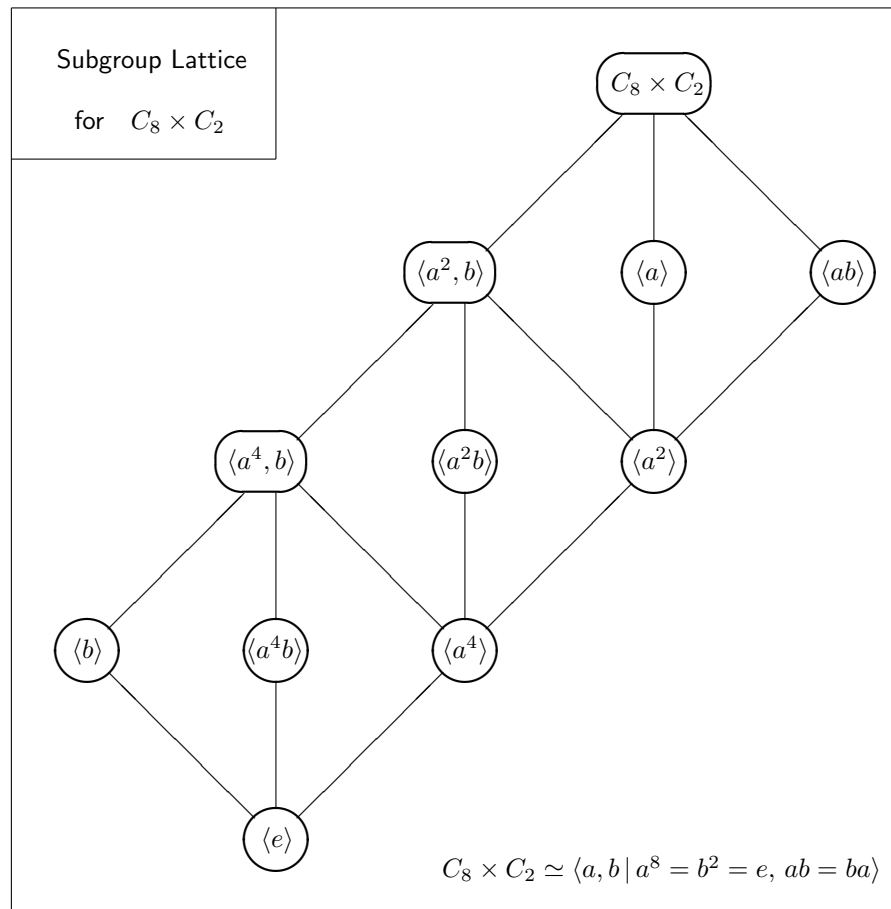
Subgroups of Q_3

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 .



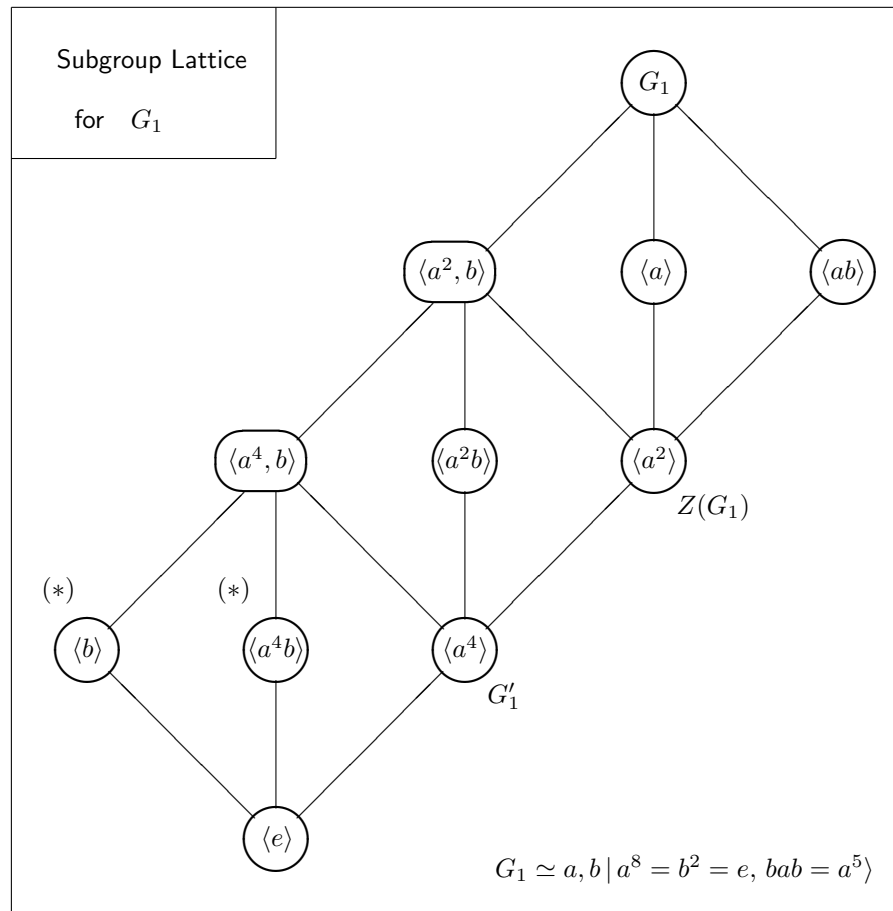
Subgroups of $C_8 \times C_2$

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 $\langle a^2, b \rangle \simeq C_4 \times C_2$.



Subgroups of G_1 defined in Problem 6.4

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