GROUPS

1. (a) \((a \ast b) \ast c = \left(\frac{ab}{a+b}\right) \ast c = \frac{abc}{a+b + c} = \frac{abc}{ab + ac + bc}\) \(\text{(M1) A1A1}\)

\[a \ast (b \ast c) = a \ast \left(\frac{bc}{b+c}\right) = \frac{abc}{a + \frac{bc}{b+c}} = \frac{abc}{ab + ac + bc}\]

\(\therefore (a \ast b) \ast c = a \ast (b \ast c)\)

so \(*\) is associative. \(\text{AG 7}\)

(b) Suppose \(e\) is an identity element, then \(e \ast a = a \ast e = a\)

\[ea = a\]

\[e + a = a\]

\[ea = ea + a\]

\(ea\) cancels on both sides so there is no solution for \(e\).

i.e. no identity element

\(\text{AG 4}\)

2. (a) \(a \# b = a + b + 1\)

Now \(b \# a = a + b + 1\) \(\text{(M1)}\)

Since + is commutative \(a \# b = b \# a\)

\(\Rightarrow \#\) is also a commutative operation. \(\text{(AG)}\)

\[(a \# b) \# c = (a + b + 1) \# c\]

\[= a + b + 1 + c + 1\]

\[= a + b + c + 2\]

\(a\#(b \# c) = a\#(b + c + 1)\)

\[= a + b + c + 1 + 1\]

\[= a + b + c + 2\]

\(\Rightarrow \#\) is also associative operation. \(\text{(AG)}\) \(\text{4}\)

(b) To show \((\mathbb{R}, \#)\) is a group we need to show closure, identity element exists, inverses exist and it is associative (already shown).

It is closed since \(a + b + 1 \in \mathbb{R}\) for \(a, b \in \mathbb{R}\). \(\text{(A1)}\)

There is a unique element \(e(e \in \mathbb{R})\) such that

\[p \# e = e \# p = p\] where \(p \in \mathbb{R}\)

\[\Rightarrow p + e + 1 = e + p + 1 = p\]

\(\Rightarrow e = -1\) as identity element \(\text{(A1)}\)

There are unique inverse elements for each element in \(\mathbb{R}\) such that

\[p \# p^{-1} = p^{-1} \# p = -1\]

\(\Rightarrow p + p^{-1} + 1 = p^{-1} + p + 1 = -1\)

\(\Rightarrow p^{-1} = -p - 2\)

Hence \((\mathbb{R}, \#)\) forms a group. \(\text{(AG)}\) \(\text{4}\)
3. (a) \( a, b \in T \Rightarrow a \ast b \in T \)  \[\text{(A1)}\]
if \( a \ast b = 1, ab - a - b + 2 = 1, \Rightarrow ab - a - b + 1 = 0 \)  \[\text{(M1)(A1)}\]
\( \Rightarrow (a - 1)(b - 1) = 0 \Rightarrow a = 1, \) or \( b = 1\) contradiction  \[\text{(M1)(R1)}\]
so \( a \ast b \in T, \) i.e. closed  \[\text{(AG)}\]

(b)
\[
(x \ast y) \ast z = (xy - x - y + 2) \ast z,  \tag{A1}
\]
\[
= xy - x - y + 2,  \tag{A1}
\]
\[
= x - y - x,  \tag{AG}
\]
\[
x \ast (y \ast z) = x(y - y + z + 2)  \tag{A1}
\]
\[
= x - y - x + 2,  \tag{A1}
\]
\[
= (x \ast y) \ast z  \tag{A1}
\]

Note: as the operation is clearly commutative, there is no need to check both left and right identity, or both left and right inverse below.

(c) \( a \ast e = a \Rightarrow e(a - 1) = 2(a - 1) \Rightarrow e = 2 \) (since \( a \neq 1 \)) \[\text{(M1)(A1)}\]
Hence 2 is the identity element for this operation.  \[\text{(A1)}\]

(d) \( a \ast a' = 2 \Rightarrow aa' - a - a' + 2 = 2 \Rightarrow a'(a - 1) = e \Rightarrow a' = a / (a - 1) \) \[\text{M1A1}\]
Hence \( 3' = 3/2 \) \[\text{A1}\]

(e) (i) The formula is true for \( n = 1 \) since \( a = (a - 1)^1 + 1 \). \[\text{R1}\]
Assume that it is true for \( n = k \), i.e. \( a \ast a \cdots a = (a - 1)^k + 1 \) \[\text{(M1)}\]
\[
k + 1 \text{ times}  \quad a \ast a \cdots a = \left( (a - 1)^k + 1 \right) \ast a = \left( (a - 1)^k + 1 \right) - a - 2 \tag{M1}
\]
\[
= (a - 1)^k \ast a - (a - 1)^k - 1 - a + 2  \tag{A1}
\]
\[
= (a - 1)^k (a - 1) + 1  \tag{A1}
\]
\[
= (a - 1)^{k+1} + 1  \tag{A1}
\]
so the formula is proven by mathematical induction. \[\text{R1}\]

(ii) We require \( a \ast a \cdots a = 2 \) \[\text{M1}\]
so that \( (a - 1)^n + 1 = 2 \) or \( (a - 1)^n = 1 \) \[\text{A1}\]
Apart from \( a = 2 \), the identity, the only solution is \( a = 0 \). \[\text{A1}\]
Since \( 0 \ast 0 = 2 \), the element 0 has order 2. \[\text{A1}\]

4. (a) Since \( \forall a \in G, e \ast a = a \ast e \) because \( e \) is the identity element of the group. \[\text{R2}\]
Then \( e \in H. \) \[\text{AG}\]
(b) Let \( x, y \in H \), then \( x \ast (y \ast a) = x \ast (y \ast a) \) (by associativity) \[\text{(R1)}\]
\[
= x \ast (a \ast y) \quad \text{(since } y \in H\text{)}  \tag{R1}
\]
\[
= (x \ast a) \ast y \quad \text{(associativity)}  \tag{R1}
\]
\[
= (a \ast x) \ast y \quad \text{(in } H\text{)}  \tag{R1}
\]
\[
= a \ast (x \ast y) \quad \text{(associativity)}  \tag{R1}
\]
Therefore, \( x \ast (y \ast a) = a \ast (x \ast y) \)
\[\Rightarrow (x \ast y) \in H. \] \[\text{AG}\]
(c) \[ e \cdot a = a \cdot e \] identity \hspace{2cm} (R1)
\[ (x^{-1} \cdot x) \cdot a = a \cdot (x^{-1} \cdot x) \] \hspace{2cm} (R1)
\[ x^{-1} \cdot (x \cdot a) = (a \cdot x^{-1}) \cdot x \] associativity \hspace{2cm} (R1)
\[ x^{-1} \cdot (a \cdot x) = (a \cdot x^{-1}) \cdot x \] \hspace{2cm} (R1)
\[ (x^{-1} \cdot a) \cdot x = (a \cdot x^{-1}) \cdot x \] associativity \hspace{2cm} (R1)
Therefore, \[ x^{-1} \cdot a = a \cdot x^{-1} \] cancellation law
and \[ x^{-1} \in H \] (R1)

**FINITE GROUPS – CAYLEY TABLES**

5. Closure - yes, because the table contains no other elements. \hspace{2cm} (R1)
Identity - yes, \( d \). \hspace{2cm} (R1)
Inverse - yes, every element has an inverse (or \( d \) appears in every row and column). \hspace{2cm} (R1)
Associativity - no because, \hspace{2cm} (R1)
\[ b \cdot (c \cdot e) = (b \cdot c) \cdot e = a \neq e = b \] (AI)

6. (a) **Note:** Award (A3) if one error, (A2) if 2 errors, (A1) if 3 errors, (A0) for more
\[
\begin{array}{cccc}
 a & b & c & d \\
 b & c & d & a \\
 c & d & a & b \\
 d & a & b & c \\
\end{array}
\]
(i) using inverse elements
\[ b \cdot x \cdot c \cdot a = d \cdot a \]
\[ \Rightarrow b \cdot x = a \] (AI)
\[ \Rightarrow d \cdot b \cdot x = d \cdot a \]
\[ \Rightarrow x = d \] (AI)
(ii) \[ a \cdot (x \cdot b) \cdot c \cdot a = b \cdot a \]
\[ \Rightarrow a \cdot (x \cdot b) = c \] (AI)
\[ \Rightarrow c \cdot a \cdot (x \cdot b) = c \cdot c \]
\[ \Rightarrow x \cdot b = b \] (AI)
\[ \Rightarrow x \cdot b \cdot d = b \cdot d \]
\[ \Rightarrow x = a \] (AI) 5

7. (a) The operation table is thus:
\[
\begin{array}{cccccccc}
 (*) & 1 & 3 & 4 & 9 & 10 & 12 \\
 1 & 1 & 3 & 4 & 9 & 10 & 12 \\
 3 & 3 & 9 & 12 & 1 & 4 & 10 \\
 4 & 4 & 12 & 3 & 10 & 1 & 9 \\
 9 & 9 & 1 & 10 & 3 & 12 & 4 \\
 10 & 10 & 4 & 1 & 12 & 9 & 3 \\
 12 & 12 & 10 & 9 & 4 & 3 & 1 \\
\end{array}
\]
**Note:** Award (A3) if one entry is incorrect, (A2) if two entries are incorrect, (AI) if three are incorrect, (A0) if four or more are incorrect.

(b) \( * \) is associative and commutative (known) \hspace{2cm} (A1)
The set is closed under \( * \) \hspace{2cm} (A1)
1 is the identity element \hspace{2cm} (A1)
Every element has an inverse because 1 is on each row (or column). \hspace{2cm} (A1) 4
(c) 1 is of order 1  
12 is of order 2  
3 and 9 are of order 3  
4 and 10 are of order 6

Note: If one answer is wrong, award (A1), if two or more answers are wrong award (A0).

(d) There are four subgroups:
   {1}  
   {1, 12}  (A1)  
   {1, 3, 9}  (A2)  
   {1, 3, 4, 9, 10, 12}

8.

(a) (i) $3 \otimes 5 = 15$  (A1)
   (ii) $3 \otimes 7 = 5$  (A1)
   (iii) $9 \otimes 11 = 3$  (A1)

(b) (i) The operation table is

<table>
<thead>
<tr>
<th>$\otimes$</th>
<th>1</th>
<th>3</th>
<th>5</th>
<th>7</th>
<th>9</th>
<th>11</th>
<th>13</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>7</td>
<td>9</td>
<td>11</td>
<td>13</td>
<td>15</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>9</td>
<td>15</td>
<td>5</td>
<td>11</td>
<td>3</td>
<td>7</td>
<td>13</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>15</td>
<td>9</td>
<td>3</td>
<td>13</td>
<td>7</td>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>5</td>
<td>3</td>
<td>11</td>
<td>15</td>
<td>13</td>
<td>11</td>
<td>9</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>11</td>
<td>13</td>
<td>11</td>
<td>3</td>
<td>13</td>
<td>5</td>
<td>7</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>1</td>
<td>7</td>
<td>13</td>
<td>3</td>
<td>9</td>
<td>5</td>
<td>15</td>
</tr>
<tr>
<td>13</td>
<td>13</td>
<td>7</td>
<td>1</td>
<td>11</td>
<td>5</td>
<td>15</td>
<td>9</td>
<td>3</td>
</tr>
<tr>
<td>15</td>
<td>15</td>
<td>13</td>
<td>11</td>
<td>9</td>
<td>7</td>
<td>5</td>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>

Note: Award (A2) if the circled numbers are correct, (A1) if 3 or 4 are correct, (A0) otherwise. The bold numbers were found in part (a)

(ii) Closure: The table shows that no new elements are generated. (RI)
   Identity: 1 is the identity. (RI)
   Inverse: Every row and column has a “1”. (RI)
   (Associative given).
   So $(S, \otimes)$ is a group. (AG) 5

(c) (i) Elements of order 2 are 7, 9, 15. (A2)

Note: Award (A1) if one correct element is given.

(ii) Elements of order 4 are 3, 5, 11, 13. (MI)(A1)

Note: If no working shown, award (MI)(A0) if one correct element is given. 4

(d) Using 3 as the generator, a sub-group of order 4 is $\{1, 3, 9, 11\}$. (MI)(A1)

Note: Another possibility is $\{1, 5, 9, 13\}$. 2
9. (a) \[(3\times9)\times13 = 13 \times13 = 1\] \hspace{1cm} (M1) 
and \[3\times(9\times13) = 3 \times5 = 1\] \hspace{1cm} (M1) 
hence \[(3\times9)\times13 = 3\times(9\times13)\] \hspace{1cm} (AG) 2

(b) To show that \((U, \ast)\) is a group we need to show that:

1. \(U\) is closed under \(\ast\). A table is an easy way of showing closure for this finite set.

\[
\begin{array}{ccccccc}
* & 1 & 3 & 5 & 9 & 11 & 13 \\
1 & 1 & 3 & 5 & 9 & 11 & 13 \\
3 & 3 & 9 & 1 & 13 & 5 & 11 \\
5 & 5 & 1 & 11 & 3 & 13 & 9 \\
9 & 9 & 13 & 3 & 11 & 1 & 5 \\
11 & 11 & 5 & 13 & 1 & 9 & 3 \\
13 & 13 & 11 & 9 & 5 & 3 & 1 \\
\end{array}
\]

Note: Award (C4) for a completely accurate table, (C3) for 1 or 2 errors, (C2) for 3 or 4 errors, (C1) for 5 or 6 errors, (C0) for 7 or more errors.

2. Since for each \(a, b \in U\), \(a \ast b \in U\), closure is shown. \hspace{1cm} (C1)
3. Since multiplication is associative, it is true in this case too. \hspace{1cm} (C1)
4. Since \(1 \ast a = a \ast 1 = a\) for all \(a \in U\), 1 is the identity. \hspace{1cm} (C2)
4. Since \(1 \ast a = a \ast 1 = a\) for all \(a \in U\), 1 is the identity. \hspace{1cm} (C1)
3. Since \(1 \ast a = a \ast 1 = a\) for all \(a \in U\), 1 is the identity. \hspace{1cm} (C1)
4. Since \(1 \ast a = a \ast 1 = a\) for all \(a \in U\), 1 is the identity. \hspace{1cm} (C1)
4. 1 appears in each row of the table once, so every element has a unique inverse. \hspace{1cm} (C2)
\[
(1^{-1} = 1, 3^{-1} = 5, 5^{-1} = 3, 9^{-1} = 11, 11^{-1} = 9, 13^{-1} + 13) \hspace{1cm} (C2) 11
\]

(c) (i) If \(G\) is a group and if there exists \(a \in G\), such that 
\[
G = \{a^n : n \in \mathbb{Z}\}
\]
Then \(G\) is a cyclic group and \(a\) is called a generator. \hspace{1cm} (C2) 2

(ii) By inspection:
\[
3 \text{ is a generator since:} \hspace{1cm} (M1) \\
3^2 = 9, 3^3 = 13, 3^4 = 11 \hspace{1cm} (A1)
\]
Also, 5 is a generator:
\[
5^2 = 11, 5^3 = 13, 5^4 = 9 \hspace{1cm} (M1) \\
5^5 = 3, 5^6 = 1 \hspace{1cm} (A1)
\]
9 cannot be a generator since \(9^3 = 1\) \hspace{1cm} (C1)

Similarly \(11^3 = 1\) and \(13^2 = 1\). \hspace{1cm} (C1) (C1) 7

(d) Since the order of this group is 6, by Lagrange’s Theorem, the proper subgroups can only have orders 2 or 3. \hspace{1cm} (R1)
Since 13 is the only self inverse \(13^2 = 1\), \hspace{1cm} (R1)
the only subgroup of order 2 is \(\{1, 13\}\) \hspace{1cm} (A1)
No sub-group may include 3 or 5 since these are the generators of the group.
The only elements left are 9 and 11. \hspace{1cm} (R1)
Now, \(9 \ast 11 = 1\), \(9^2 = 11\), and \(11^2 = 9\). \hspace{1cm} (M2)
Therefore, \(\{1, 9, 11\}\) is the other sub-group. \hspace{1cm} (A1) 7
PERMUTATION GROUPS

10. (a) Since \(3! = 6\), order of \(S = 6\). \(\text{(M1) (R1)} 2\)

(b) Members of \(S\) are:

\[ p_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \text{(AG)} \]

\[ p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \text{(A2) 2} \]

Note: Award \(A2\) for 3 correct permutations; \(A1\) for 2 (A0) for 1

\[ p_3 \circ p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \]

\[ p_4 \circ p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \]

\(\text{(M1)}\)

\(p_3 \circ p_4 \neq p_4 \circ p_3\) \(\text{(R1) 2}\)

Note: There are other possibilities to show that the group is not Abelian.

(c) \(p_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = p_2\)

\[ p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = p_0. \quad \text{(M1)} \]

(Note that \(p_0\) is the identity of the group \(S\).)

Hence \(\{p_0, p_1, p_2\}\) form a cyclic group of order 3 under composition. \(\text{(R1) 2}\)

Note: Some candidates may write \(\{p_0, p_1, p_2\}\) is a subgroup of order 3, (award \(A1\)), and write the following table, (award \(R1\)):

\[
\begin{array}{c|cccc}
\circ & p_0 & p_1 & p_2 \\
p_0 & p_0 & p_1 & p_2 \\
p_1 & p_1 & p_2 & p_0 \\
p_2 & p_2 & p_0 & p_1 \\
\end{array}
\]

11. (a) \(\begin{pmatrix} a & b & c & d \\ b & d & a & c \end{pmatrix}\) \(\text{(A1) 1}\)

(b) \(\begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}; \begin{pmatrix} a & b & c & d \\ b & a & c & d \end{pmatrix}\) \(\text{(A2) 2}\)

Note: There are many correct answers for the second permutation.

(c) \(\begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}\)

\(\begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix}; \begin{pmatrix} a & b & c & d \\ c & d & a & b \end{pmatrix}; \begin{pmatrix} a & b & c & d \\ d & a & b & c \end{pmatrix}\) \(\text{(A1)(A1)(A1)}\)

Let \(p, q, r, s\) be the four permutations in the subgroup. Closure is shown by the group table, i.e. \(\text{(M1)}\)

\[
\begin{array}{cccc}
p & q & r & s \\
p & p & q & r & s \\
q & q & r & s & p \\
r & r & s & p & q \\
s & s & p & q & r \\
\end{array}
\]

Inverse: each element has an inverse, \(\text{(M1)}\)

i.e. \(p^{-1} = p, q^{-1} = s, r^{-1} = r, s^{-1} = q.\) \(\text{(A1) 7}\)

Note: There are other possible answers.
GROUPS AND RELATIONS (COSETS)

12. (a) \(x^{-1}x = e \in H \Rightarrow x R x \Rightarrow R\) is reflexive

\(x R y \Rightarrow x^{-1}y \in H \Rightarrow (x^{-1}y)^{-1} \in H\)

\(x^{-1}y(x^{-1}y)^{-1} = e\) so \((x^{-1}y)^{-1} = y^{-1}x\)

\(y^{-1}x \in H \Rightarrow y R x \Rightarrow R\) is symmetric

\(x R y\) and \(y R z \Rightarrow x^{-1}y \in H\) and \(y^{-1}z \in H\)

\[\therefore (x^{-1}y)(y^{-1}z) \in H\] since \(H\) is closed.

\(x \in H \Rightarrow x^{-1}z \in H\)

\[\therefore x R z \Rightarrow R\) is transitive.

\(\therefore R\) is an equivalence relation.

(b) \(p^3 = q^2 = e \quad qp = p^2q\)

\[qp^2 = (qp)p = (p^2q)p = p^3(qp) = p^3(pq) = pq\]

\(\therefore \) The equivalence class is \(\{p^2, pq\}\)

OTHERWISE

The equivalence class of \(pq\) is the coset \(pqH\) which contains \(pq\) and \(pqp^2q = ppqq = p^2\).

Extra question

There are 3 equivalence classes (3 cosets)

\[H = \{e, p^2q\}\]

\[pH = \{p, q\}\]

\[p^2H = \{p^2, pq\}\]

ISOMORPHISMS

13. (a) \(f\) is injective since \(f(x) = f(y) \iff > 3^x = 3^y \iff > x = y\)

\(f\) is surjective since \(z \in \mathbb{R}^+, x = \log_3 (z) \in \mathbb{R}\) and \(z = f(x)\)

\(\text{For every } x, y \in (\mathbb{R}, +)\),

\[f(x + y) = 3^{(x + y)} = 3^x 3^y = f(x) \times f(y)\]

\[\therefore f^{-1}(z) = \log_3(z)\]

(b) \(f^{-1}(z) = \log_3(z)\)

14. (a) Since \((a + b\sqrt{2})(c + d \sqrt{2}) = ac + 2bd + (ad + bc)\sqrt{2}\),

and \((ac + 2bd)^2 - 2(ad + bc)^2 = (a^2 - 2b^2)(c^2 - 2d^2) \neq 0\),

\(S\) is closed under multiplication.

\(1 = 1 + 0\sqrt{2}\) is the neutral element.

Finally, \(\frac{a - b\sqrt{2}}{a^2 - 2b^2} \in S\)

\(\frac{a - b\sqrt{2}}{a^2 - 2b^2} (a + b\sqrt{2}) = 1\), so every element of \(S\) has an inverse.
(b) To show that $f(x)$ is an isomorphism, we need to show that it is injective, surjective and that it preserves the operation.

**Injection:** Let $x_1 = a + b\sqrt{2}, x_2 = c + d\sqrt{2}$

$$f(x_1) = f(x_2) \Rightarrow a - b\sqrt{2} = c - d\sqrt{2} \Rightarrow (a - c) + (d - b)\sqrt{2} = 0 \quad (M1)$$

$\Rightarrow a = c, \text{ and } b = d \Rightarrow x_1 = x_2 \quad (A1)$

**Surjection:** For every $y = a - b\sqrt{2}$ there is $x = a + b\sqrt{2}$ \quad (M1)(A1)

**Preserves operation:**

$$f(x_1 x_2) = f((a + b\sqrt{2})(c + d\sqrt{2})) = f(ac + 2bd + ad + bc)\sqrt{2} \quad (M1)$$

$$= ac + 2bd - (ad + bc)\sqrt{2} = (a - b\sqrt{2})(c - d\sqrt{2}) \quad (M1)$$

$$f(a + b\sqrt{2})f(c + d\sqrt{2}) = (f(x_1))(f(x_2))$$

15. (a)

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

(b)

<table>
<thead>
<tr>
<th>(*)</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>b</td>
<td>a</td>
<td>d</td>
<td>c</td>
</tr>
<tr>
<td>b</td>
<td>a</td>
<td>b</td>
<td>c</td>
<td>d</td>
</tr>
<tr>
<td>c</td>
<td>d</td>
<td>c</td>
<td>a</td>
<td>b</td>
</tr>
<tr>
<td>d</td>
<td>c</td>
<td>d</td>
<td>b</td>
<td>a</td>
</tr>
</tbody>
</table>

Notes: There are many other correct solutions, with a different ordering

Award (A4) if all entries are correct, (A3) if all but 1 entry are correct, (A2) if all but 2 entries are correct, (A1) if all but 3 entries are correct.

16. (a)

<table>
<thead>
<tr>
<th>o</th>
<th>f</th>
<th>g</th>
<th>h</th>
<th>j</th>
</tr>
</thead>
<tbody>
<tr>
<td>f</td>
<td>f</td>
<td>g</td>
<td>h</td>
<td>j</td>
</tr>
<tr>
<td>g</td>
<td>g</td>
<td>f</td>
<td>j</td>
<td>h</td>
</tr>
<tr>
<td>h</td>
<td>h</td>
<td>j</td>
<td>f</td>
<td>g</td>
</tr>
<tr>
<td>j</td>
<td>j</td>
<td>h</td>
<td>g</td>
<td>f</td>
</tr>
</tbody>
</table>

Note: Award (A3) for all correct, (A2) for 1 error, (A1) for 2 errors, (A0) otherwise.

(b) for $+_4$, the identity is 0, 1 has order 4, 2 has order 2 and 3 has order 4, \quad (A1)

for $\times_5$, the identity is 1, 2 has order 4, 3 has order 4 and 4 has order 2, \quad (A1)

Hence $+_4$ is isomorphic with $\times_5$. \quad (A1)

Corresponding elements are

$$0 \leftrightarrow 1, 1 \leftrightarrow 2, 2 \leftrightarrow 4, 3 \leftrightarrow 3, \text{ OR } 0 \leftrightarrow 1, 1 \leftrightarrow 3, 2 \leftrightarrow 4, 3 \leftrightarrow 2. \quad (A1)$$

Note: Corresponding elements must be correct for final (A1).
17. (a) By using the composition of functions we form the Cayley table

\[\begin{array}{c|cccc}
\circ & f_1 & f_2 & f_3 & f_4 \\
\hline
f_1 & f_1 & f_2 & f_3 & f_4 \\
f_2 & f_2 & f_1 & f_4 & f_3 \\
f_3 & f_3 & f_4 & f_1 & f_2 \\
f_4 & f_4 & f_3 & f_2 & f_1 \\
\end{array}\]

Note: For each error in the above table deduct one mark up to a maximum of three marks.

From the table, we see that \((T, \circ)\) is a closed and is commutative. \((R1)\)

\(f_i\) is the identity. \((A1)\)

\(f_i^{-1} = f_i, i = 1, 2, 3, 4.\) \((A1)\)

Since the composition of functions is an associative binary operation an Abelian group. \((AG)\)

(b) The Cayley table for the group \((G, \diamond)\) is given below:

\[\begin{array}{c|cccc}
\diamond & 1 & 3 & 5 & 7 \\
\hline
1 & 1 & 3 & 5 & 7 \\
3 & 3 & 1 & 7 & 5 \\
5 & 5 & 7 & 1 & 3 \\
7 & 7 & 5 & 3 & 1 \\
\end{array}\]

Note: For each error in the entries deduct one mark up to a maximum of two marks.

Define \(f: T \mapsto G\) such that \(f(f_1) = 1, f(f_2) = 3, f(f_3) = 5\) and \(f(f_4) = 7\) \((M1)\)

Since distinct elements are mapped onto distinct images, it is a bijection. \((R1)\)

Since the two Cayley tables match, the bijection is an isomorphism. \((R1)\)

Hence the two groups are isomorphic. \((AG)\)

18. (a) \(B\) is the set \(\{1, i, -1, -i\}\) \((A1)\)

This set is closed under multiplication.

Associative, since it is normal complex number multiplication. \((R1)\)

The identity element is 1. \((R1)\)

The inverse of \(i\) is \(-i\), and vice versa, 1 and \(-1\) are self inverses. \((R1)\)

(b) \[\begin{array}{c|cccc}
\times & 1 & 3 & 7 & 9 \\
\hline
1 & 1 & 3 & 7 & 9 \\
3 & 3 & 9 & 1 & 7 \\
7 & 7 & 1 & 9 & 3 \\
9 & 9 & 7 & 3 & 1 \\
\end{array}\]

(c) Order of 1 is 1

Order of 3 is 4, since \(3^4 = 1\) \((A1)\)

Order of 7 is 4, since \(7^4 = 1\) \((A1)\)

Order of 9 is 2, since \(9^2 = 1\) \((A1)\)

(d) The two groups will have a bijection in which the following correspond:

\(1 \leftrightarrow 1, 3 \leftrightarrow i, 7 \leftrightarrow i, \text{ and } 9 \leftrightarrow -1\) \((\text{or } 3 \leftrightarrow -i, 7 \leftrightarrow i)\) \((A1)\)

Both groups have the same structure, the bijection preserves the operation. \((R1)\)
19.

(a)

\[
\begin{array}{|c|c|c|c|}
\hline
& U & H & V \\
\hline
U & U & H & V \\
H & H & U & K \\
V & V & K & U \\
K & K & V & H \\
\hline
\end{array}
\]

Note: (A4) for 15-16 correct entries, (A3) for 13-14, (A2) for 11-12, (A1) for 9-10, (A0) o/w

(b) Closure: \( U, H, K \) and \( V \) are the only entries in the table. So it is closed. (A1)
Identity: \( U \), since \( UT = TU = T \) for all \( T \) in \( S \). (A1)
Inverses: \( U^{-1} = U, H^{-1} = H, V^{-1} = V, K^{-1} = K \) (A1)
Associativity: Given (AG)
Hence \( (S, \circ) \) forms a group. (R1) 4

(c) \( C = \{1, -1, i, -i\} \)

\[
\begin{array}{|c|c|c|c|}
\hline
\circ & 1 & -1 & i & -i \\
\hline
1 & 1 & -1 & i & -i \\
-1 & -1 & 1 & -i & i \\
1 & 1 & -i & -1 & 1 \\
-i & i & 1 & -1 \\
\hline
\end{array}
\]

Note: Award (A3) for 15-16 correct entries, (A2) for 13-14, (A1) for 11-12, (A0) for fewer

(d) Suppose \( f: S \rightarrow C \) is an isomorphism.
Then \( f(U) = 1 \), the identity in \( C \), since \( f \) preserves the group operation. (M1)(C1)
Assume \( f(H) = i, 1 = f(U) = f(H \circ H) = f(H) \circ f(H) \). (A1)
But \( f(H) = i \), and \( i \) is not its own inverse, so \( f \) is not an isomorphism. (R1) 4

Note: Accept other correctly justified solutions.
THEORETICAL

20. Let \( a^{-1} = b \) (M1)
Then \( e = b \times a = b \times a \times a \) (M1)
so that \( e = (b \times a) \times a = e \times a \) (M1)
and therefore \( e = a \) (M1)(AG)

Note: There are other correct solutions.

21. (a) If \( G \) is a group and \( H \) is a subgroup of \( G \) then the order of \( H \) is a divisor of the order of \( G \). (A2) 2
(b) Since the order of \( G \) is 24, the order of \( a \) must be 1, 2, 3, 4, 6, 8, 12 or 24 (R2)
The order cannot be 1, 2, 3, 6 or 12 since \( a^{12} \neq e \) (R1)
Also \( a^8 \neq e \) so that the order of \( a \) must be 24 (R1)
Therefore, \( a \) is a generator of \( G \), which must therefore be cyclic. (R1) 5

22. (a) A cyclic group is a group which is generated by one of its elements (or words to that effect). (M2) 2
(b) We can assume that \((G, \#)\) has at least two elements and hence contains an element, say \( b \), which is different from \( e \), its identity. (R1)
The order of \( b \) is equal to the order \( q \) of the subgroup it generates. (M1)
By Lagrange’s theorem \( q \) must be a factor of \( p \) and since \( p \) is prime either \( q = 1 \) or \( q = p \). (R1)
Since \( b \neq e \) we see that \( q \neq 1 \) and therefore \( q = p \). (R1)
But if the order of \( b \) is \( p \) then \( b \) generates \((G, \#)\) which is therefore cyclic. (R1) 5

23.
For \( a \in H \), \( a^{-1} \ast a = e \in H \) so \( H \) contains the identity. (A1)
For \( a \in H \), \( a^{-1} \ast a = a^{-1} \in H \) so \( H \) contains all the inverse elements. (A1)
\( \ast \) is associative on \( G \) and therefore on \( H \). (A1)
For \( a, b \in H \), \( a^{-1} \ast b = a^{-1} \ast b = a \ast b \in H \) so closure confirmed. (A1) (A1)
The four requirements are satisfied so \((H, \ast)\) is a subgroup. (R1)

24. Consider \( a \ast b \). This cannot be \( a \) or \( b \) since \( a \ast b = a \Rightarrow b = e \) which is not the case and similarly for \( b \). So \( a \ast b = \) either \( e \) or \( c \). (M1)
If \( a \ast b = e \), then \( a, b \) form an inverse pair so \( b \ast a = e \). (R1)
Suppose \( a \ast b = c \). Consider \( b \ast a \). As before, this cannot equal \( a \) or \( b \) and it cannot equal \( e \) either because that would imply that \( a \ast b = e \) which it is not. (R1)
It follows that \( b \ast a = c \). (R1)
Thus in both cases, \( a \ast b = b \ast a \). (R1)

25. Given \((G, \ast)\) is a cyclic group with identity \( e \) and \( G \neq \{e\} \) and \( G \) has no proper subgroups.
If \( G \) is of composite finite order and is cyclic, then there is \( x \in G \) such that \( x \) generates \( G \). (R1)
If \( |G| = p \times q, p, q \neq 1 \), then \( \langle x^q \rangle \) is a subgroup of \( G \) of order \( q \) which is impossible since \( G \) has no non-trivial proper subgroup. (M1)
Suppose the order of \( G \) is infinite. Then \( \langle x^2 \rangle \) is a proper subgroup of \( G \) which contradicts the fact that \( G \) has no proper subgroup. (A1)
So \( G \) is a finite cyclic group of prime order. (R1)
26. If one of the sets $H$ and $K$ is contained in the other then either $H \cup K = H$ or $H \cap K = K$.
In either case it is a subgroup of $(G, \cdot)$.

Only if:

Conversely, suppose that $(H \cup K, \cdot)$ is a subgroup of $(G, \cdot)$ and that $H$
is not contained in $K$.
Let $a$ be any element of $K$.

Then $ab \in H \cup K$ (since $(H \cup K, \cdot)$ is a group).

If $ab \in K$ then $b = a^{-1}ab \in K$ which is a contradiction of our hypothesis.

Hence $ab \not\in K$ and therefore $ab \not\in H$ so that $abb^{-1} \in H$
which shows that $K \subseteq H$ since $a$ was any element of $K$.

Therefore $H \subseteq K$ or $K \subseteq H$. (AG)

OR

Proof by contradiction: (M1)

If $K \not\subset H$ then there exists $m \in K, m \not\in H$ (C1)

And

If $H \not\subset K$ then there exists $n \in H, n \not\in K$. (C1)

Suppose $m \cdot n \in H$ then $m \cdot n \cdot n^{-1} \in H$ is a contradiction (C1)

Suppose $m \cdot n \not\in K$ then $n = m^{-1} \cdot m \cdot n \in K$ is a contradiction (C1)

Hence $m \cdot n \not\in H \cup K$ a contradiction (C1)

Therefore $H \subseteq K$ or $K \subseteq H$ (AG) 8

27. (a) Let $(G, \cdot)$ and $(H, \bullet)$ be two groups. They are said to be isomorphic
if there exists a one-to-one transformation $f : G \to H$ which is

surjective (onto) with the property that for all $x, y \in G, f(x \cdot y) = f(x) \bullet f(y)$. (C1)

Note: Some candidates may say that the groups $(G, \cdot)$ and $(H, \bullet)$
are isomorphic if they have the same Cayley table (or group
table). In that case award (C1).

(b) Since $f : G \rightarrow H, f(x) \in H$ for some $x \in G$.

Since $e'$ is the identity element in $H$,

$e' \bullet f(x) = f(x) = f(x \cdot e) = f(e) \bullet f(x)$. (M1)(A1)

By the right cancellation law, $e' = f(e)$. (M1) 4

(c) Suppose $G = \langle a \rangle$, the cyclic group generated by $a$, i.e. $n$ is the
smallest positive integer such that $a^n = e$, the identity in $G$.

Let $f : G \rightarrow H$ be an isomorphism. Let $f(a) = b \in H$.

$f(a^2) = f(a \cdot a) = f(a) \bullet f(a) = (f(a))^2$. (M1)

In general $f(a^m) = (f(a))^m, 1 \leq m \leq n$. (A1)

By (iii) (b) $(f(a))^n = e'$, the identity in $H$. Hence $b^n = e'$ and consequently $H$ is a cyclic group of order $n$ with generator $b$. (R1) 4
28. (a) Suppose $a$ is of order $n$ and is $a^{-1}$ of order $m$. 
Therefore $e = e * e = (a^{-1})m * a^n$ 
(M1)

If $m > n$, then $e = (a^{-1})m * n * (a^{-1})p * a^n = (a^{-1})m - n * (a^{-1} * a)^n$. 
(M1)

Hence $e = (a^{-1})m - n$. This implies $a^{-1}$ is of order $m - n < m$ 
which is a contradiction. So $m$ is not greater than $n$. 
(R1)

If $m < n$, $e = (a^{-1})m * a^n * a^{-m} = (a^{-1} * a)^m * a^{-m}$ 
(M1)

Hence $e = a^{-m}$, which implies $a$ is of order $n - m < n$. 
This is a contradiction. 
(R1)

Therefore $m = n$. 
(AG) 5

(b) Let $S(m)$ be the statement: $b^n = p^{-1} * a^n * p$.

$S(1)$ is true since we are given $b = p^{-1} * a * p$ 
(A1)

Assume $S(k)$ as the induction hypothesis. 
(M1)

$k^{k+1} = b^k * b = (p^{-1} * a^k * p) * (p^{-1} * a * p) = p^{-1} * a^{k+1} * p$ 
(M1)(R1)

which proves $S(k + 1)$.

Hence, by mathematical induction $b^n = p^{-1} * a^n * p$ ($n = 1, 2, \ldots$). 
(AG) 4

29. (a) $(xy)^2 = e$ 
Order of $xy = 2$ 
(M1)

$\Rightarrow (xy)(xy) = e \Rightarrow x(yx)y = e$ 
Associative property 
(M1)(M1)

$\Rightarrow xx(yx)y = xey$ 
Left and right–multiply 
(M1)

$\Rightarrow e(yx)e = xy$ 
Order of elements given 
(M1)

$\Rightarrow yx = xy$ 
(AG)

OR

Since $x$, $y$ and $xy$ are self–inverses, $x^{-1} = x$, $y^{-1} = y$ and $(xy)^{-1} = xy$ 
(R1)(R1)

Consider $xy = (xy)^{-1}$ 
(M1)

$= y^{-1}x^{-1}$ 
(M1)

$= yx$ 
(M1)(AG) 5

(b) Let $a$ be any element of a group, whose identity is $e$.

Let $a^{-1}$ be an inverse of $a$, and let $b$ be another inverse of $a$ different from $a^{-1}$.

Now, $b = be = b(aa^{-1}) = (ba)a^{-1}$; identity and associativity properties, 
(M1)

then, $b = ea^{-1} = a^{-1}$, which contradicts the assumption that $b \neq a^{-1}$, 
(M1)

therefore there is only one inverse of $a$, namely $a^{-1}$. 
(R1)

OR

Let $a$ be any element of a group whose identity is $e$. Let $b$ and $c$ be 
(M1)

inverses of $a$, so that $ab = ba = e$. 
Consider $b = b(ac)$

$= (ba)c$ 
(M1)

$= c$ 
(M1)

Thus any two inverses are equal, so the inverse is unique. 
(R1) 3

(c) If $G$ is Abelian, then $f(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = f(x)f(y)$ and $f$ 
is an isomorphism. 
(M1)(R1)

If $f$ is an isomorphism, then $f(xy) = f(x)f(y)$, that is, 
$(xy)^{-1} = x^{-1}y^{-1} = (yx)^{-1}$ 
Then $xy = yx$ 
(M1)

and hence $G$ is Abelian. 
(R1) 4

[9]