Groups

Questions

Q1.

A binary operation $\star$ on the set of non-negative integers, $\mathbb{Z}_0^+$, is defined by

$$m \star n = |m - n| \qquad m, n \in \mathbb{Z}_0^+$$

(a) Explain why $\mathbb{Z}_0^+$ is closed under the operation $\star$

(1)

(b) Show that 0 is an identity for $(\mathbb{Z}_0^+, \star)$

(2)

(c) Show that all elements of $\mathbb{Z}_0^+$ have an inverse under $\star$

(2)

(d) Determine if $\mathbb{Z}_0^+$ forms a group under $\star$, giving clear justification for your answer.

(3)

(Total for question = 8 marks)

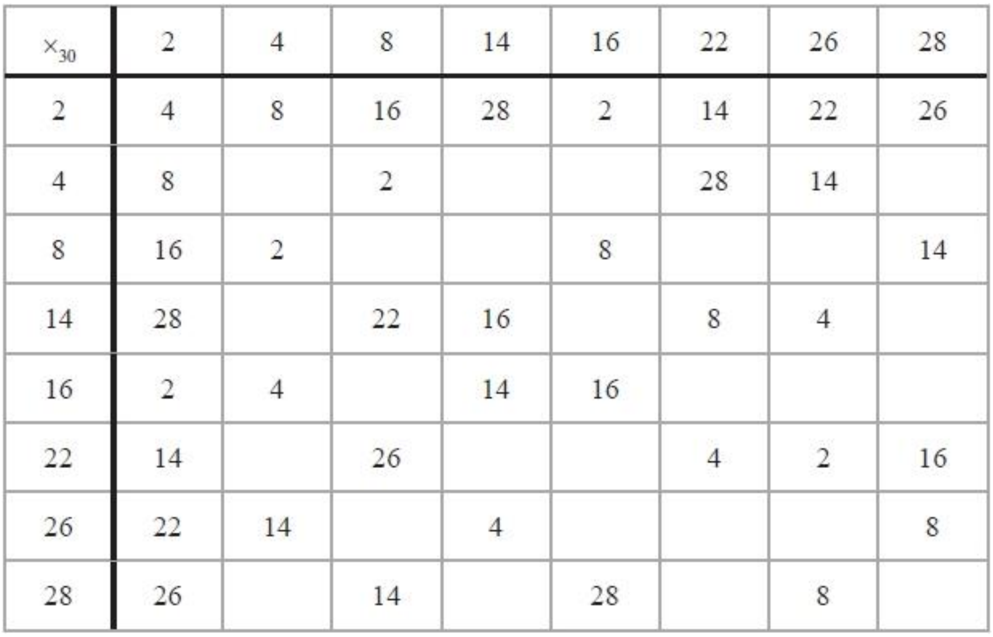
Q2.

(i) Let *G* be a group of order 5 291 848

Without performing any division, use proof by contradiction to show that *G* cannot have a subgroup of order 11

(3)

(ii) (a) Complete the following Cayley table for the set *X* = 2,4,8,14,16,22,26,28 with the operation of multiplication modulo 30



$\times_{30}$	2	4	8	14	16	22	26	28
2	4	8	16	28	2	14	22	26
4	8		2			28	14	
8	16	2			8			14
14	28		22	16		8	4	
16	2	4		14	16			
22	14		26			4	2	16
26	22	14		4				8
28	26		14		28		8	

(b) Hence determine whether the set *X* with the operation of multiplication modulo 30 forms a group.

[You may assume multiplication modulo *n* is an associative operation.]

(6)

(Total for question = 9 marks)

Q3.

(i) A binary operation * is defined on positive real numbers by

$$a * b = a + b + ab$$

Prove that the operation * is associative.

(4)

(ii) The set *G* = 1, 2, 3, 4, 5, 6 forms a group under the operation of multiplication modulo 7

(a) Show that *G* is cyclic.

(2)

The set *H* = 1, 5, 7, 11, 13, 17 forms a group under the operation of multiplication modulo 18

(b) List all the subgroups of *H*.

(3)

(c) Describe an isomorphism between *G* and *H*.

(3)

(Total for question = 12 marks)

Q4.

The set *e*,*p*, *q*, *r*, *s* forms a group, *A*, under the operation *

Given that *e* is the identity element and that

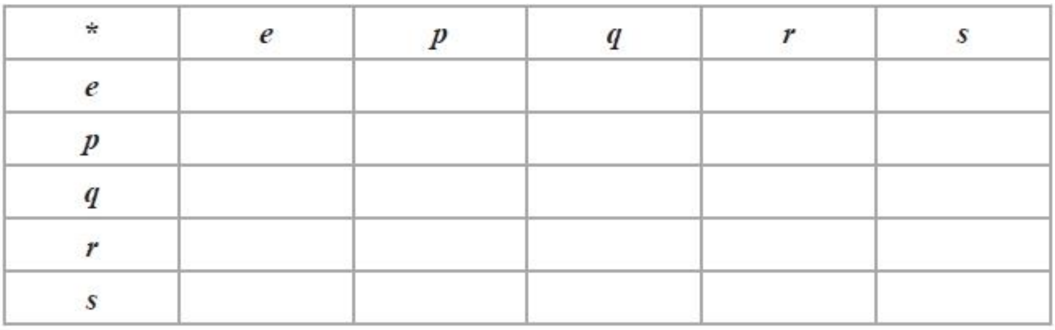
$$p*p = s \qquad s*s = r \qquad p*p*p = q$$

(a) show that

(i) $p*q = r$
(ii) $s*p = q$

(2)

(b) Hence complete the Cayley table below.



*	*e*	*p*	*q*	*r*	*s*
e					
p					
q					
r					
s					

(2)

(c) Use your table to find $p*q*r*s$

(1)

A student states that there is a subgroup of *A* of order 3

(d) Comment on the validity of this statement, giving a reason for your answer.

(2)

(Total for question = 7 marks)

Q5.

The set G = 1, 3, 7, 9, 11, 13, 17, 19 under the binary operation of multiplication modulo 20 forms a group.

(a) Find the inverse of each element of G.

(3)

(b) Find the order of each element of G.

(3)

(c) Find a subgroup of G of order 4

(1)

(d) Explain how the subgroup you found in part (c) satisfies Lagrange's theorem.

(1)

(Total for question = 8 marks)

Q6.

Let G be a group of order $46^{46} + 47^{47}$

Using Fermat's Little Theorem and explaining your reasoning, determine which of the following are possible orders for a subgroup of G

(i) 11

(ii) 21

(7)

(Total for question = 7 marks)

Q7.

The group S_4 is the set of all possible permutations that can be performed on the four numbers 1, 2, 3 and 4, under the operation of composition.

For the group S_4

(a) write down the identity element,

(1)

(b) write down the inverse of the element *a*, where

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$$

(1)

(c) demonstrate that the operation of composition is associative using the following elements

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \quad b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \quad \text{and } c = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

(2)

(d) Explain why it is possible for the group S_4 to have a subgroup of order 4
You do not need to find such a subgroup.

(2)

(Total for question = 6 marks)

Q8.

The operation * is defined on the set S = 0, 2, 3, 4, 5, 6   by x*y = x + y – xy (mod 7)

*	0	2	3	4	5	6
0						
2		0				
3						5
4						
5		4				
6						

(a)   (i)   Complete the Cayley table shown above

(ii) Show that S is a group under the operation *
(You may assume the associative law is satisfied.)

(6)

(b)   Show that the element 4 has order 3

(2)

(c)   Find an element which generates the group and express each of the elements in terms of this generator.

(3)

(Total for question = 11 marks)

Q9.

(i) A group *G* contains distinct elements *a*, *b* and *e* where *e* is the identity element and the group operation is multiplication.

Given $a^2b = ba$, prove $ab \neq ba$

(4)

(ii) The set *H* = 1, 2, 4, 7, 8, 11, 13, 14 forms a group under the operation of multiplication modulo 15

(a) Find the order of each element of *H*.

(3)

(b) Find three subgroups of *H* each of order 4, and describe each of these subgroups.

(4)

The elements of another group *J* are the matrices $\begin{pmatrix} \cos\left(\frac{k\pi}{4}\right) & \sin\left(\frac{k\pi}{4}\right) \\ -\sin\left(\frac{k\pi}{4}\right) & \cos\left(\frac{k\pi}{4}\right) \end{pmatrix}$ where $k = 1, 2, 3, 4, 5, 6, 7, 8$ and the group operation is matrix multiplication.

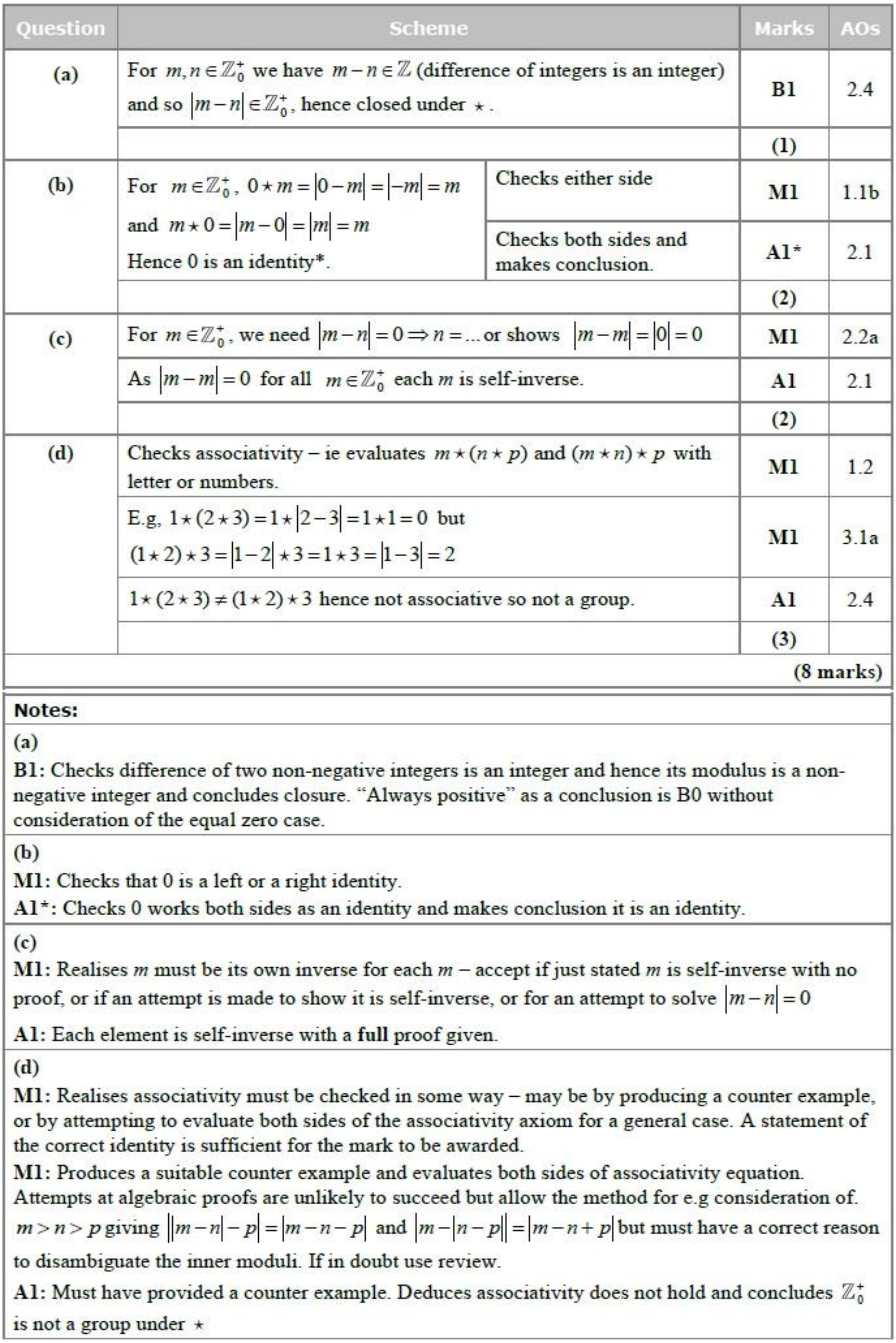
(c) Determine whether *H* and *J* are isomorphic, giving a reason for your answer.

(2)

(Total for question = 13 marks)

Mark Scheme - Groups

Q1.



Question	Scheme		Marks	AOs
(a)	For $m, n \in \mathbb{Z}_0^+$ we have $m-n \in \mathbb{Z}$ (difference of integers is an integer) and so $\lvert m-n \rvert \in \mathbb{Z}_0^+$, hence closed under $\star$.		B1	2.4
			(1)	
(b)	For $m \in \mathbb{Z}_0^+$, $0 \star m = \lvert 0-m \rvert = \lvert -m \rvert = m$ and $m \star 0 = \lvert m-0 \rvert = \lvert m \rvert = m$ Hence 0 is an identity*.	Checks either side	M1	1.1b
		Checks both sides and makes conclusion.	A1*	2.1
			(2)	
(c)	For $m \in \mathbb{Z}_0^+$, we need $\lvert m-n \rvert = 0 \Rightarrow n = ...$ or shows $\lvert m-m \rvert = \lvert 0 \rvert = 0$		M1	2.2a
	As $\lvert m-m \rvert = 0$ for all $m \in \mathbb{Z}_0^+$ each m is self-inverse.		A1	2.1
			(2)	
(d)	Checks associativity – ie evaluates $m \star (n \star p)$ and $(m \star n) \star p$ with letter or numbers.		M1	1.2
	E.g. $1 \star (2 \star 3) = 1 \star \lvert 2-3 \rvert = 1 \star 1 = 0$ but $(1 \star 2) \star 3 = \lvert 1-2 \rvert \star 3 = 1 \star 3 = \lvert 1-3 \rvert = 2$		M1	3.1a
	$1 \star (2 \star 3) \neq (1 \star 2) \star 3$ hence not associative so not a group.		A1	2.4
			(3)	
			(8 marks)	

Notes:

(a)

B1: Checks difference of two non-negative integers is an integer and hence its modulus is a non-negative integer and concludes closure. "Always positive" as a conclusion is B0 without consideration of the equal zero case.

(b)

M1: Checks that 0 is a left or a right identity.

A1*: Checks 0 works both sides as an identity and makes conclusion it is an identity.

(c)

M1: Realises m must be its own inverse for each m – accept if just stated m is self-inverse with no proof, or if an attempt is made to show it is self-inverse, or for an attempt to solve $\lvert m-n \rvert = 0$

A1: Each element is self-inverse with a **full** proof given.

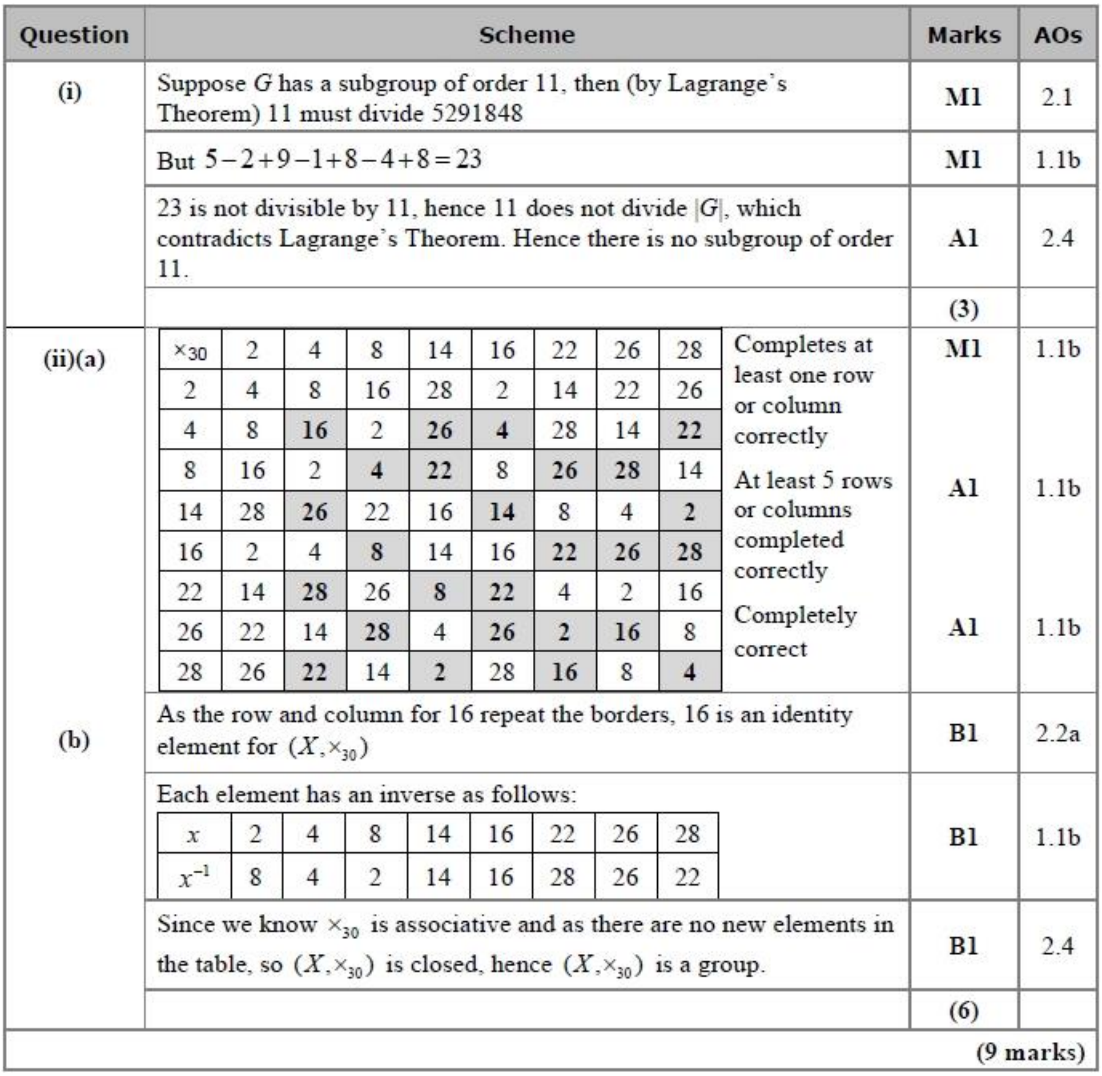
(d)

M1: Realises associativity must be checked in some way – may be by producing a counter example, or by attempting to evaluate both sides of the associativity axiom for a general case. A statement of the correct identity is sufficient for the mark to be awarded.

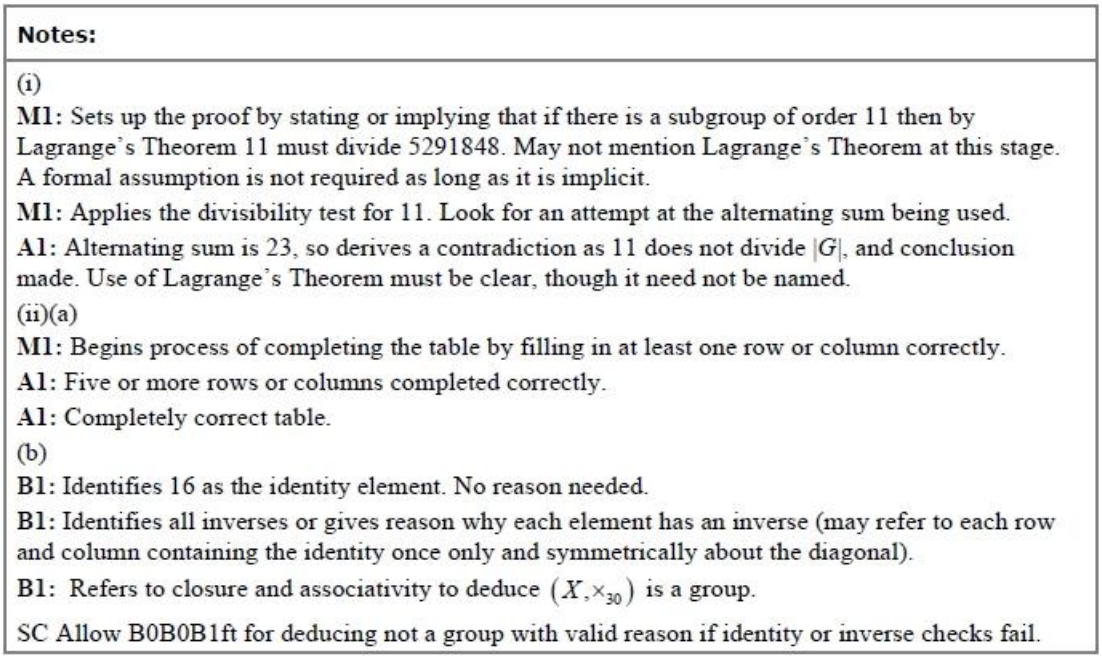
M1: Produces a suitable counter example and evaluates both sides of associativity equation. Attempts at algebraic proofs are unlikely to succeed but allow the method for e.g consideration of. $m > n > p$ giving $\lvert \lvert m-n \rvert - p \rvert = \lvert m-n-p \rvert$ and $\lvert m - \lvert n-p \rvert \rvert = \lvert m-n+p \rvert$ but must have a correct reason to disambiguate the inner moduli. If in doubt use review.

A1: Must have provided a counter example. Deduces associativity does not hold and concludes $\mathbb{Z}_0^+$ is not a group under $\star$

Q2.



<table>
<tr><th>Question</th><th>Scheme</th><th>Marks</th><th>AOs</th></tr>
<tr><td>(i)</td><td>Suppose G has a subgroup of order 11, then (by Lagrange's Theorem) 11 must divide 5291848</td><td>M1</td><td>2.1</td></tr>
<tr><td></td><td>But $5-2+9-1+8-4+8=23$</td><td>M1</td><td>1.1b</td></tr>
<tr><td></td><td>23 is not divisible by 11, hence 11 does not divide $|G|$, which contradicts Lagrange's Theorem. Hence there is no subgroup of order 11.</td><td>A1</td><td>2.4</td></tr>
<tr><td></td><td></td><td>(3)</td><td></td></tr>
<tr><td>(ii)(a)</td><td>
<table>
<tr><td>$\times_{30}$</td><td>2</td><td>4</td><td>8</td><td>14</td><td>16</td><td>22</td><td>26</td><td>28</td></tr>
<tr><td>2</td><td>4</td><td>8</td><td>16</td><td>28</td><td>2</td><td>14</td><td>22</td><td>26</td></tr>
<tr><td>4</td><td>8</td><td><b>16</b></td><td>2</td><td><b>26</b></td><td><b>4</b></td><td>28</td><td>14</td><td><b>22</b></td></tr>
<tr><td>8</td><td>16</td><td>2</td><td><b>4</b></td><td><b>22</b></td><td>8</td><td><b>26</b></td><td><b>28</b></td><td>14</td></tr>
<tr><td>14</td><td>28</td><td><b>26</b></td><td>22</td><td>16</td><td><b>14</b></td><td>8</td><td>4</td><td><b>2</b></td></tr>
<tr><td>16</td><td>2</td><td>4</td><td><b>8</b></td><td>14</td><td>16</td><td><b>22</b></td><td><b>26</b></td><td><b>28</b></td></tr>
<tr><td>22</td><td>14</td><td><b>28</b></td><td>26</td><td><b>8</b></td><td><b>22</b></td><td>4</td><td>2</td><td>16</td></tr>
<tr><td>26</td><td>22</td><td>14</td><td><b>28</b></td><td>4</td><td><b>26</b></td><td><b>2</b></td><td><b>16</b></td><td>8</td></tr>
<tr><td>28</td><td>26</td><td><b>22</b></td><td>14</td><td><b>2</b></td><td>28</td><td><b>16</b></td><td>8</td><td><b>4</b></td></tr>
</table>
Completes at least one row or column correctly
At least 5 rows or columns completed correctly
Completely correct</td><td>M1
A1
A1</td><td>1.1b
1.1b
1.1b</td></tr>
<tr><td>(b)</td><td>As the row and column for 16 repeat the borders, 16 is an identity element for $(X,\times_{30})$</td><td>B1</td><td>2.2a</td></tr>
<tr><td></td><td>Each element has an inverse as follows:
<table>
<tr><td>x</td><td>2</td><td>4</td><td>8</td><td>14</td><td>16</td><td>22</td><td>26</td><td>28</td></tr>
<tr><td>x^{-1}</td><td>8</td><td>4</td><td>2</td><td>14</td><td>16</td><td>28</td><td>26</td><td>22</td></tr>
</table></td><td>B1</td><td>1.1b</td></tr>
<tr><td></td><td>Since we know $\times_{30}$ is associative and as there are no new elements in the table, so $(X,\times_{30})$ is closed, hence $(X,\times_{30})$ is a group.</td><td>B1</td><td>2.4</td></tr>
<tr><td></td><td></td><td>(6)</td><td></td></tr>
<tr><td colspan="4">(9 marks)</td></tr>
</table>



Notes:

(i)

M1: Sets up the proof by stating or implying that if there is a subgroup of order 11 then by Lagrange's Theorem 11 must divide 5291848. May not mention Lagrange's Theorem at this stage. A formal assumption is not required as long as it is implicit.

M1: Applies the divisibility test for 11. Look for an attempt at the alternating sum being used.

A1: Alternating sum is 23, so derives a contradiction as 11 does not divide $|G|$, and conclusion made. Use of Lagrange's Theorem must be clear, though it need not be named.

(ii)(a)

M1: Begins process of completing the table by filling in at least one row or column correctly.

A1: Five or more rows or columns completed correctly.

A1: Completely correct table.

(b)

B1: Identifies 16 as the identity element. No reason needed.

B1: Identifies all inverses or gives reason why each element has an inverse (may refer to each row and column containing the identity once only and symmetrically about the diagonal).

B1: Refers to closure and associativity to deduce $(X, \times_{30})$ is a group.

SC Allow B0B0B1ft for deducing not a group with valid reason if identity or inverse checks fail.

Q3.

Question	Scheme	Marks	AOs
(i)	$(a*b)*c=(a+b+ab)*c=a+b+ab+c+(a+b+ab)c$	M1	2.1
	$a*(b*c)=a*(b+c+bc)=a+b+c+bc+a(b+c+bc)$	M1	2.1
	$\underline{a+b+ab+c+(a+b+ab)c}=a+b+c+bc+ab+ac+abc$ $=\underline{a+b+c+bc+a(b+c+bc)}$	A1	2.2a
	so $(a*b)*c=a*(b*c)$ which means * is associative	A1	2.4
		(4)	
(ii)(a)	$3^2=2\quad 3^3=6\quad 3^4=4\quad 3^5=5\quad 3^6=1$ or $5^2=4\quad 5^3=6\quad 5^4=2\quad 5^5=3\quad 5^6=1$	M1	2.1
	Or special case for M1A0 if powers not shown: 3 has order 6 so generates the group		
	3 (or 5) has order 6 and so generates the group so *G* is cyclic	A1	2.4
		(2)	
(b)	{1}, *H*	B1	1.1b
	{1, 17} **or** {1, 7, 13}	M1	1.1b
	{1, 17} **and** {1, 7, 13} (and no others)	A1	1.1b
		(3)	
(c)	$\begin{array}{ccccccc} G & 1 & 2 & 3 & 4 & 5 & 6 \\ H & 1 & 7 & 5 & 13 & 11 & 17 \end{array}$ **or** $\begin{array}{ccccccc} G & 1 & 2 & 3 & 4 & 5 & 6 \\ H & 1 & 13 & 11 & 7 & 5 & 17 \end{array}$	M1 A1 A1	3.1a 1.1b 1.1b
		(3)	
		(12 marks)	

Notes

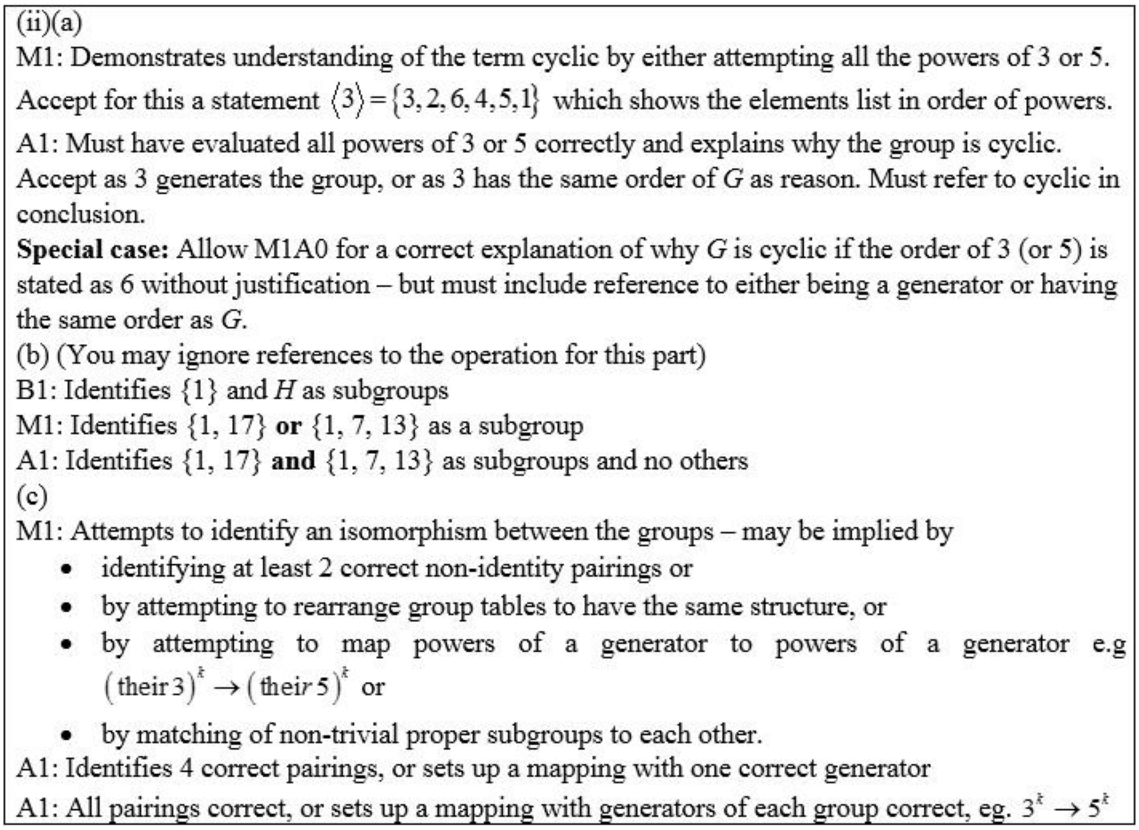
(i)

M1: Begins proof by correctly expanding ($a*b$)*c **or** a*(b*c) to an expression in *a*, *b* and *c*. Note they may expand as $(a*b)*c=(a*b)+c+(a*b)c=a+b+ab+c+(a+b+ab)c$ which is equally fine.

M1: Makes progress towards the required result by attempting to expand both ($a*b$)*c **and** a*(b*c), but be generous with the attempts for this method. May achieve this by working from left to right, so look for arriving at the other expression through a chain of equalities.

A1: For both underlined expressions (but accept eg. $c(a + b + ab)$ for $(a + b + ab)c$) and a correct expansion seen for each independently or part of a chain as shown. The expansion may have terms in different orders.

A1: Explains that $(a*b)*c=a*(b*c)$ means that * is associative. Depends on both M marks and a correct expression having been found.



(ii)(a)

M1: Demonstrates understanding of the term cyclic by either attempting all the powers of 3 or 5. Accept for this a statement $\langle 3\rangle = \{3, 2, 6, 4, 5, 1\}$ which shows the elements list in order of powers.

A1: Must have evaluated all powers of 3 or 5 correctly and explains why the group is cyclic. Accept as 3 generates the group, or as 3 has the same order of *G* as reason. Must refer to cyclic in conclusion.

Special case: Allow M1A0 for a correct explanation of why *G* is cyclic if the order of 3 (or 5) is stated as 6 without justification – but must include reference to either being a generator or having the same order as *G*.

(b) (You may ignore references to the operation for this part)

B1: Identifies {1} and *H* as subgroups

M1: Identifies {1, 17} **or** {1, 7, 13} as a subgroup

A1: Identifies {1, 17} **and** {1, 7, 13} as subgroups and no others

(c)

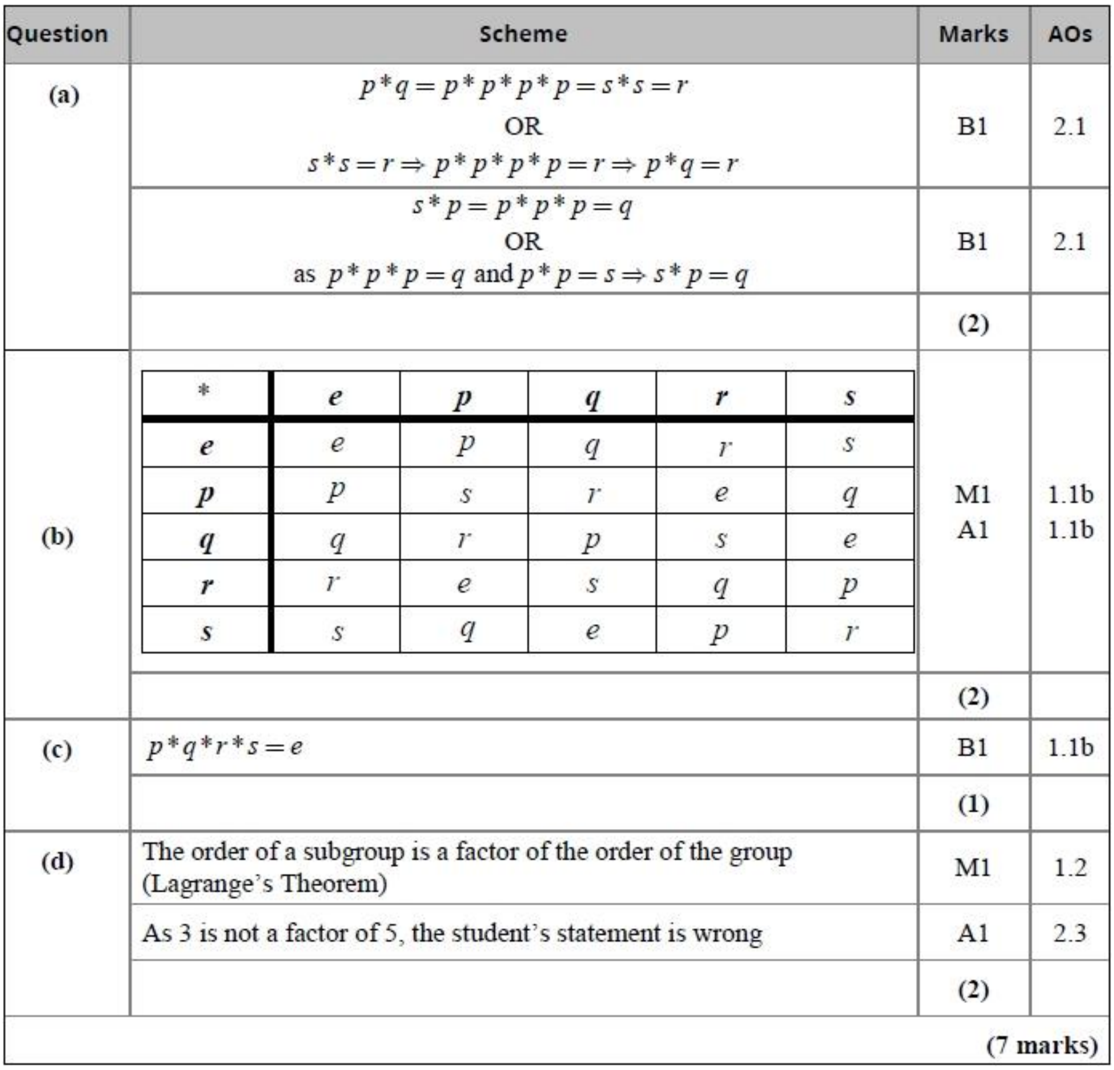
M1: Attempts to identify an isomorphism between the groups – may be implied by

- identifying at least 2 correct non-identity pairings or
- by attempting to rearrange group tables to have the same structure, or
- by attempting to map powers of a generator to powers of a generator e.g $(\text{their } 3)^k \rightarrow (\text{their } 5)^k$ or
- by matching of non-trivial proper subgroups to each other.

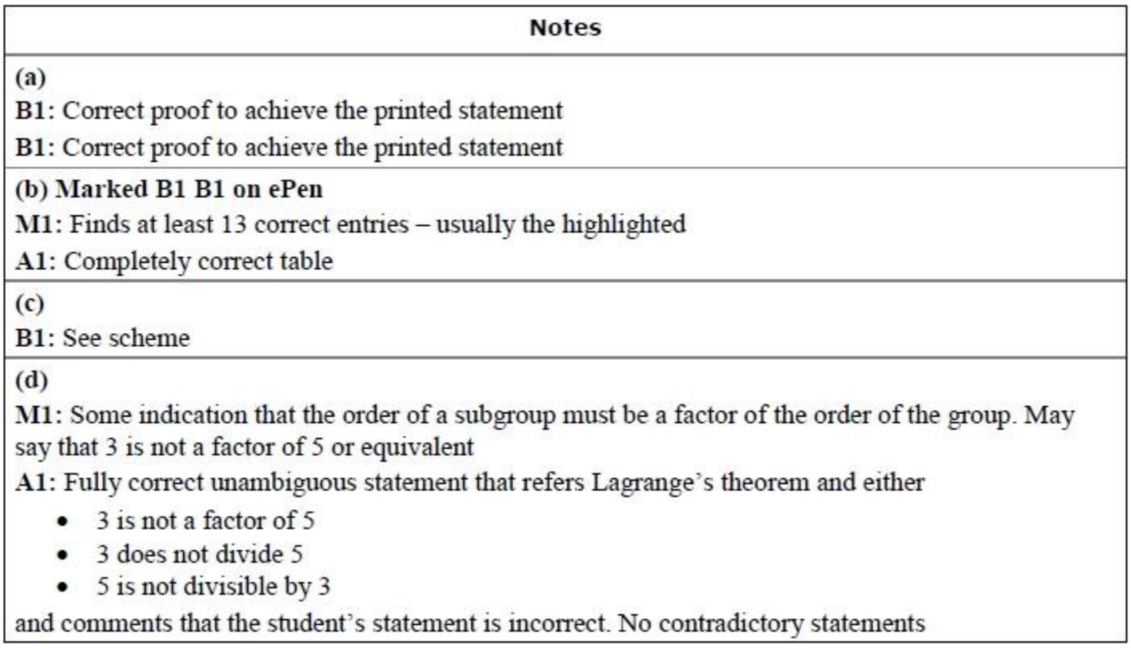
A1: Identifies 4 correct pairings, or sets up a mapping with one correct generator

A1: All pairings correct, or sets up a mapping with generators of each group correct, eg. $3^k \rightarrow 5^k$

Q4.

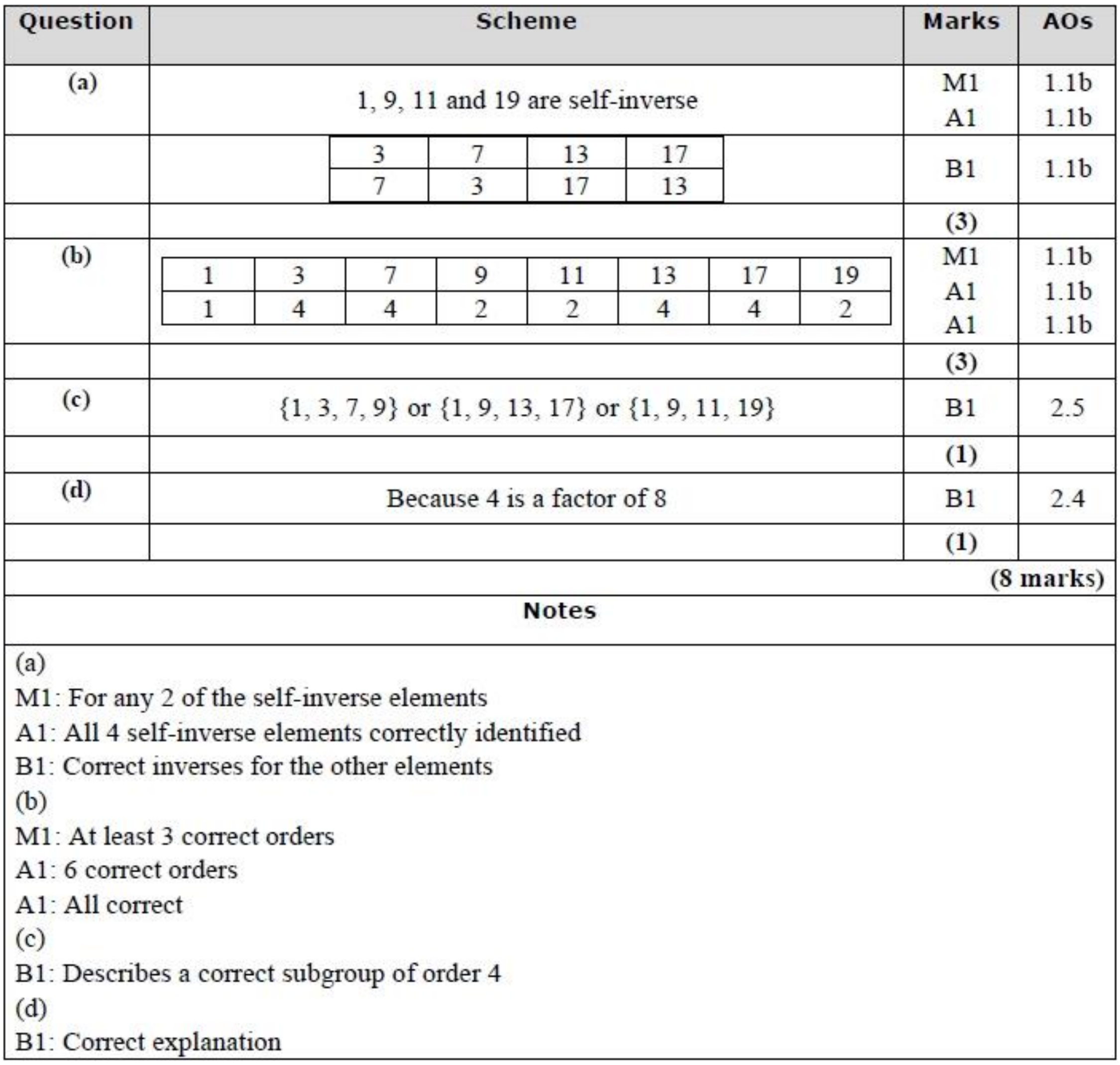


<table>
<tr><th>Question</th><th>Scheme</th><th>Marks</th><th>AOs</th></tr>
<tr><td>(a)</td><td>$p*q=p*p*p*p=s*s=r$
OR
$s*s=r\Rightarrow p*p*p*p=r\Rightarrow p*q=r$</td><td>B1</td><td>2.1</td></tr>
<tr><td></td><td>$s*p=p*p*p=q$
OR
as $p*p*p=q$ and $p*p=s\Rightarrow s*p=q$</td><td>B1</td><td>2.1</td></tr>
<tr><td></td><td></td><td>(2)</td><td></td></tr>
<tr><td>(b)</td><td>
<table>
<tr><th>*</th><th>e</th><th>p</th><th>q</th><th>r</th><th>s</th></tr>
<tr><td>e</td><td>e</td><td>p</td><td>q</td><td>r</td><td>s</td></tr>
<tr><td>p</td><td>p</td><td>s</td><td>r</td><td>e</td><td>q</td></tr>
<tr><td>q</td><td>q</td><td>r</td><td>p</td><td>s</td><td>e</td></tr>
<tr><td>r</td><td>r</td><td>e</td><td>s</td><td>q</td><td>p</td></tr>
<tr><td>s</td><td>s</td><td>q</td><td>e</td><td>p</td><td>r</td></tr>
</table>
</td><td>M1
A1</td><td>1.1b
1.1b</td></tr>
<tr><td></td><td></td><td>(2)</td><td></td></tr>
<tr><td>(c)</td><td>$p*q*r*s=e$</td><td>B1</td><td>1.1b</td></tr>
<tr><td></td><td></td><td>(1)</td><td></td></tr>
<tr><td>(d)</td><td>The order of a subgroup is a factor of the order of the group (Lagrange's Theorem)</td><td>M1</td><td>1.2</td></tr>
<tr><td></td><td>As 3 is not a factor of 5, the student's statement is wrong</td><td>A1</td><td>2.3</td></tr>
<tr><td></td><td></td><td>(2)</td><td></td></tr>
<tr><td colspan="4">(7 marks)</td></tr>
</table>



Notes
(a) **B1:** Correct proof to achieve the printed statement **B1:** Correct proof to achieve the printed statement
(b) Marked B1 B1 on ePen **M1:** Finds at least 13 correct entries – usually the highlighted **A1:** Completely correct table
(c) **B1:** See scheme
(d) **M1:** Some indication that the order of a subgroup must be a factor of the order of the group. May say that 3 is not a factor of 5 or equivalent **A1:** Fully correct unambiguous statement that refers Lagrange's theorem and either • 3 is not a factor of 5 • 3 does not divide 5 • 5 is not divisible by 3 and comments that the student's statement is incorrect. No contradictory statements

Q5.



<table>
<tr><th>Question</th><th>Scheme</th><th>Marks</th><th>AOs</th></tr>
<tr><td>(a)</td><td>1, 9, 11 and 19 are self-inverse</td><td>M1
A1</td><td>1.1b
1.1b</td></tr>
<tr><td></td><td><table><tr><td>3</td><td>7</td><td>13</td><td>17</td></tr><tr><td>7</td><td>3</td><td>17</td><td>13</td></tr></table></td><td>B1</td><td>1.1b</td></tr>
<tr><td></td><td></td><td>(3)</td><td></td></tr>
<tr><td>(b)</td><td><table><tr><td>1</td><td>3</td><td>7</td><td>9</td><td>11</td><td>13</td><td>17</td><td>19</td></tr><tr><td>1</td><td>4</td><td>4</td><td>2</td><td>2</td><td>4</td><td>4</td><td>2</td></tr></table></td><td>M1
A1
A1</td><td>1.1b
1.1b
1.1b</td></tr>
<tr><td></td><td></td><td>(3)</td><td></td></tr>
<tr><td>(c)</td><td>{1, 3, 7, 9} or {1, 9, 13, 17} or {1, 9, 11, 19}</td><td>B1</td><td>2.5</td></tr>
<tr><td></td><td></td><td>(1)</td><td></td></tr>
<tr><td>(d)</td><td>Because 4 is a factor of 8</td><td>B1</td><td>2.4</td></tr>
<tr><td></td><td></td><td>(1)</td><td></td></tr>
<tr><td colspan="4">(8 marks)</td></tr>
<tr><th colspan="4">Notes</th></tr>
<tr><td colspan="4">(a)
M1: For any 2 of the self-inverse elements
A1: All 4 self-inverse elements correctly identified
B1: Correct inverses for the other elements
(b)
M1: At least 3 correct orders
A1: 6 correct orders
A1: All correct
(c)
B1: Describes a correct subgroup of order 4
(d)
B1: Correct explanation</td></tr>
</table>

Q6.

Question	Scheme	Marks	AOs
(i)	(Order of a subgroup must divide the order of a group by Lagrange's Theorem), so need to check if 11 (and/or 21) divides $46^{46}+47^{47}$ and by FLT, e.g. $a^{11-1}=a^{10}\equiv 1(\text{mod } 11)$, so	M1	1.1b
	$46^{46}+47^{47}\equiv 2^{4\times 10+6}+3^{4\times 10+7}\equiv 2^6+3^7\equiv 64+(3^3)^2\times 3$ $\equiv 9+5^2\times 3\equiv 84\equiv 7(\text{mod } 11)$	M1	3.1a
	Hence 11 is not a divisor of $46^{46}+47^{47}$ so not a possible order for a subgroup.	A1	2.2a
(ii)	$21=7\times 3$ so need to check for factors of 7 and 3, using $a^2\equiv 1(\text{mod } 3)$ and $a^6\equiv 1(\text{mod } 7)$	M1	3.1a
	$46^{46}+47^{47}\equiv 1^{46}+2^{47}\equiv 1+2^{2\times 23+1}\equiv 1+2^1\equiv 3\equiv 0(\text{mod } 3)$	M1	1.1b
	$46^{46}+47^{47}\equiv 4^{46}+(-2)^{47}\equiv 4^{6\times 7+4}+(-2)^{6\times 7+5}\equiv 4^4+(-2)^5$ $\equiv 16^2-32\equiv 9^2-4\equiv 81-4\equiv 77\equiv 0(\text{mod } 7)$	M1	2.1
	As $46^{46}+47^{47}$ divisible by both 3 and 7 it is divisible by 21 and hence this is a possible order for a subgroup.	A1	2.4
		(7)	
(7 marks)			

Notes:

(i)

M1: For an attempt to apply a correct Fermat's Little theorem at least once in the question with either p = 11, p = 7 or p = 3 on either the 46^{46} or 47^{47} term.

M1: Applies FLT and congruence arithmetic fully to find the residue of $46^{46}+47^{47}$ modulo 11. There will be lots of different routes, so look for an attempt to apply FLT that leads to determining if 11 is a divisor or not.

A1: $46^{46}+47^{47}\equiv 7(\text{mod } 11)$ (accept equivalents as long as it is clear it is not congruent to 0) and deduces it is not a possible order for a subgroup.

(ii)

M1: Applies checks for both 7 and 3 as divisors of $46^{46}+47^{47}$ via similar strategy.

M1: Applies FLT with p = 3 to find a smaller residue modulo 3. Other routes are possible.

M1: Applies FLT with p = 7 to find a smaller residue modulo 7. Other routes are possible.

A1: Shows $46^{46}+47^{47}$ congruent to 0 modulo 3 and modulo7, and deduces 21 divides $46^{46}+47^{47}$ hence it is a possible order for a subgroup.

Alt:

M1: Reduces the bases modulo 21 and applies a power reduction technique using congruences for at least one of the power of 46 or 47

M1: Reduces fully by congruence arithmetic either the 46^{46} or 47^{47} term.

M1: Reduces fully by congruence arithmetic both the 46^{46} and 47^{47} terms

A1: Shows $46^{46}+47^{47}$ congruent to 0 modulo 21, and deduces 21 divides $46^{46}+47^{47}$ hence it is a possible order for a subgroup.

Q7.

Question	Scheme	Marks	AOs
(a)	$\{e =\}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$	B1	1.1b
		(1)	
(b)	$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$	B1	1.1b
		(1)	
(c)	Demonstrates that, for example: $[a \circ b] \circ c = \left[\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}\right] \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$ $= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ $a \circ [b \circ c] = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \circ \left[\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}\right]$ $= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$	M1	2.1
	So $[a \circ b] \circ c = a \circ [b \circ c]$ or associative	A1	2.4
		(2)	
(d)	The order of the group is 24 or 4!	B1	1.1b
	4 is a factor of 24 or **4/24** therefore **it is possible** for a subgroup to have order 4.	B1ft	2.4
		(2)	
		(6 marks)	

Notes:

(a)

B1: See scheme

(b)

B1: See scheme

(c)

M1: Shows two calculations in an attempt to show associative, e,g, $[a \circ b] \circ c$and $a \circ [b \circ c]$. There must be an intermediate line of working with evidence of using the permutations. Condone the wrong order for this mark.

A1: Correct calculations leading to $[a \circ b] \circ c = a \circ [b \circ c]$ or states associative

Note Incorrect order scores M1 A0

$$[a \circ b] \circ c = \left[\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}\right] \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

(d)

B1: Order is 24 or 4!

B1ft: Follow through on their order of the group, draws the correct conclusion

Q8.

<table>
<tr><th>Question</th><th>Scheme</th><th>Marks</th><th>AOs</th></tr>
<tr><td>(a)</td><td>(i)
<table>
<tr><td>*</td><td>0</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td></tr>
<tr><td>0</td><td>0</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td></tr>
<tr><td>2</td><td>2</td><td>0</td><td></td><td></td><td>4</td><td></td></tr>
<tr><td>3</td><td>3</td><td></td><td></td><td></td><td></td><td>5</td></tr>
<tr><td>4</td><td>4</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>5</td><td>5</td><td>4</td><td></td><td></td><td></td><td></td></tr>
<tr><td>6</td><td>6</td><td></td><td>5</td><td></td><td></td><td></td></tr>
</table></td><td>M1</td><td>1.1b</td></tr>
<tr><td></td><td>
<table>
<tr><td>*</td><td>0</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td></tr>
<tr><td>0</td><td>0</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td></tr>
<tr><td>2</td><td>2</td><td>0</td><td>6</td><td>5</td><td>4</td><td>3</td></tr>
<tr><td>3</td><td>3</td><td>6</td><td>4</td><td>2</td><td>0</td><td>5</td></tr>
<tr><td>4</td><td>4</td><td>5</td><td>2</td><td>6</td><td>3</td><td>0</td></tr>
<tr><td>5</td><td>5</td><td>4</td><td>0</td><td>3</td><td>6</td><td>2</td></tr>
<tr><td>6</td><td>6</td><td>3</td><td>5</td><td>0</td><td>2</td><td>4</td></tr>
</table></td><td>M1 A1</td><td>1.1b
1.1b</td></tr>
<tr><td></td><td>(ii) Identity is zero and there is closure as shown above</td><td>M1</td><td>2.1</td></tr>
<tr><td></td><td>3 and 5 are inverses, 4 and 6 are inverses, 2 is self inverse,
0 is identity so is self inverse</td><td>M1</td><td>2.5</td></tr>
<tr><td></td><td>Associative law may be assumed so <i>S</i> forms a group</td><td>A1</td><td>1.1b</td></tr>
<tr><td></td><td></td><td>(6)</td><td></td></tr>
</table>

(b)	4*4*4 = 4* (4 * 4) = 4 * 6 or 4*4*4 = (4* 4) * 4 = 6* 4	M1	2.1
	= 0 (the identity) so 4 has order 3	A1	2.2a
		(2)	
(c)	3 and 5 each have order 6 so either generates the group	M1	3.1a
	Either $3^1 = 3,\ 3^2 = 4,\ 3^3 = 2,\ 3^4 = 6,\ 3^5 = 5,\ 3^6 = 0$ **Or** $5^1 = 5,\ 5^2 = 6,\ 5^3 = 2,\ 5^4 = 4,\ 5^5 = 3,\ 5^6 = 0$	A1, A1	1.1b 1.1b
		(3)	
			(11 marks)

Notes:

(a)(i)

M1: Begins completing the table – obtaining correct first row and first column and using symmetry
M1: Mostly correct – three rows or three columns correct (so demonstrates understanding of using *
A1: Completely correct

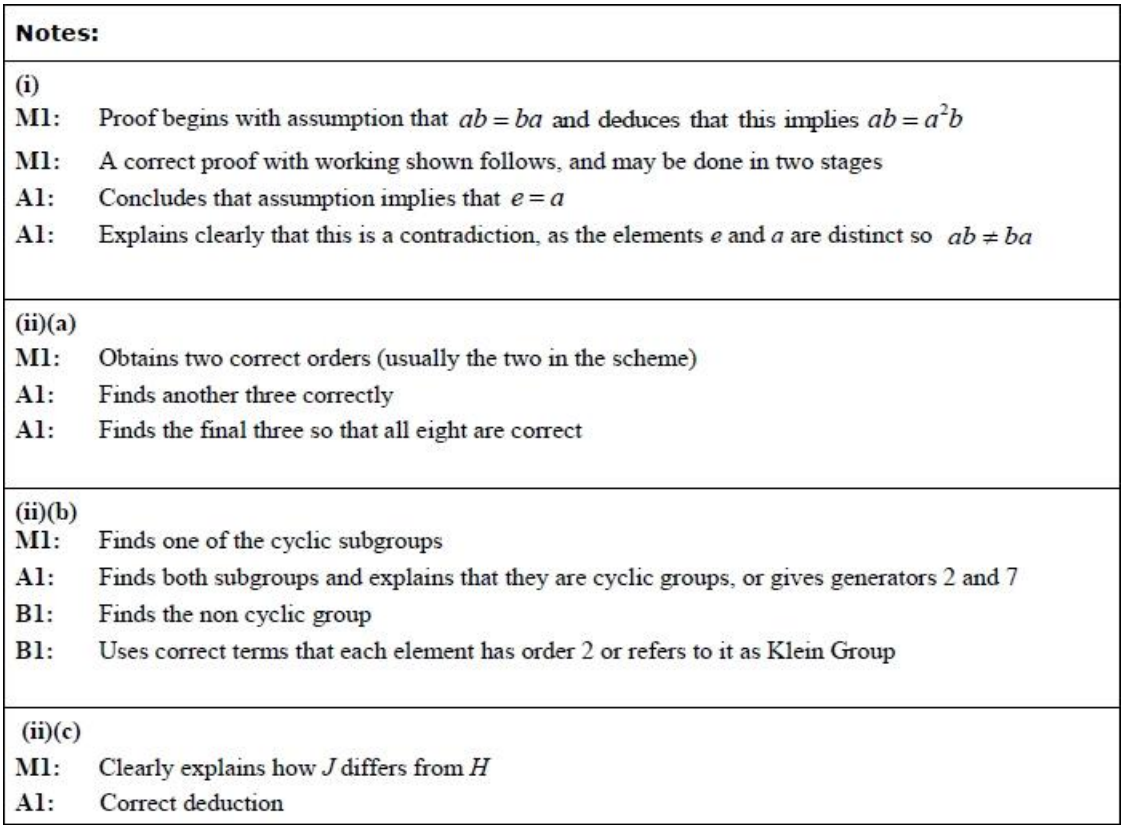
(a)(ii)

M1: States closure and identifies the identity as zero
M1: Finds inverses for each element

A1: States that associative law is satisfied and so all axioms satisfied and *S* is a group
(b) **M1:** Clearly begins process to find 4*4*4 reaching 6*4 or 4*6 with clear explanation **A1:** Gives answer as zero, states identity and deduces that order is 3
(c) **M1:** Finds either 3 or 5 or both **A1:** Expresses four of the six terms as powers of either generator correctly (may omit identity and generator itself) **A1:** Expresses all six terms correctly in terms of either 3 or 5 (Do not need to give both)

Q9.

Question	Scheme	Marks	AOs
(i)	If we assume $ab = ba$; as $a^2b = ba$ then $ab = a^2b$	M1	2.1
	So $a^{-1}abb^{-1} = a^{-1}a^2bb^{-1}$	M1	2.1
	So $e = a$	A1	2.2a
	But this is a contradiction, as the elements *e* and *a* are distinct so $ab \neq ba$	A1	2.4
		(4)	
(ii)(a)	2 has order 4 and 4 has order 2	M1	1.1b
	7, 8 and 13 have order 4	A1	1.1b
	11 and 14 have order 2 and 1 has order 1	A1	1.1b
		(3)	
(ii)(b)	Finds the subgroup $\{1, 2, 4, 8\}$ or the subgroup $\{1, 7, 4, 13\}$	M1	1.1b
	Finds both and refers to them as cyclic groups, or gives generator 2 and generator 7	A1	2.4
	Finds $\{1, 4, 11, 14\}$	B1	2.2a
	States each element has order 2 or refers to it as Klein Group	B1	2.5
		(4)	
(ii)(c)	*J* has an element of order 8, (*H* does not) or *J* is a cyclic group (*H* is not) or other valid reason	M1	2.4
	They are not isomorphic	A1	2.2a
		(2)	
			(13 marks)



Notes:

(i)

M1: Proof begins with assumption that $ab = ba$ and deduces that this implies $ab = a^2b$

M1: A correct proof with working shown follows, and may be done in two stages

A1: Concludes that assumption implies that $e = a$

A1: Explains clearly that this is a contradiction, as the elements *e* and *a* are distinct so $ab \neq ba$

(ii)(a)

M1: Obtains two correct orders (usually the two in the scheme)

A1: Finds another three correctly

A1: Finds the final three so that all eight are correct

(ii)(b)

M1: Finds one of the cyclic subgroups

A1: Finds both subgroups and explains that they are cyclic groups, or gives generators 2 and 7

B1: Finds the non cyclic group

B1: Uses correct terms that each element has order 2 or refers to it as Klein Group

(ii)(c)

M1: Clearly explains how *J* differs from *H*

A1: Correct deduction