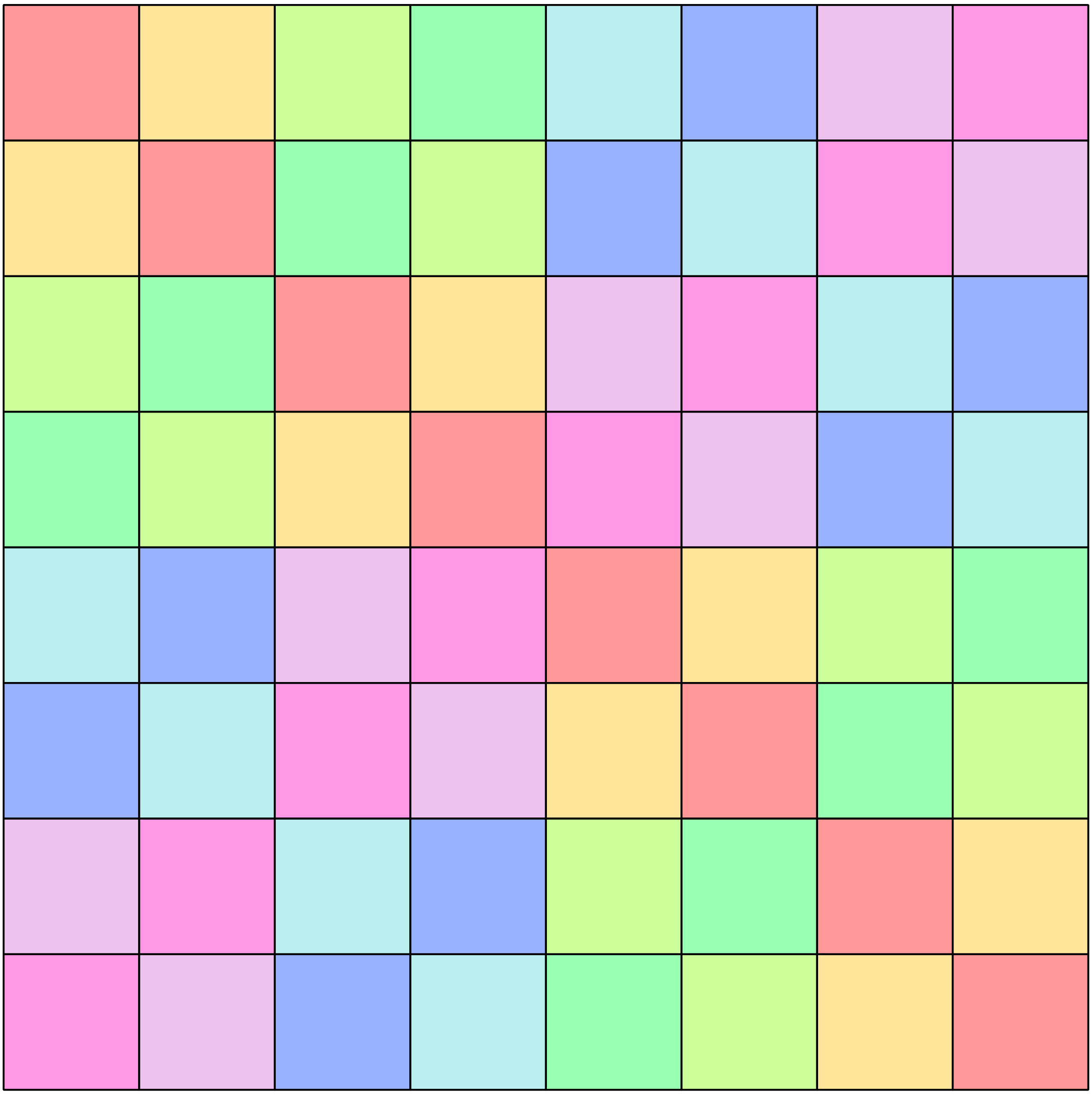
University Undergraduate Lectures in Mathematics
A First Year Course

GROUP THEORY

The Mathematics of Symmetry



G R O U P   T H E O R Y II

Lecture 1

University Undergraduate Lectures in Mathematics
A First Year Course
Group Theory II

1.1 Introduction

Welcome to Group Theory II, designed to follow on from Group Theory I. There, the focus was on getting an initial feel for the subject. With several key ideas now in place attention shifts to developing slicker notation, and exploring the structure of groups in a more abstract manner. There will still be much that is "hands on". Group Theory II assumes the knowledge of Group Theory I, along with topics taught during a first year at University, such as Matrices and Complex Numbers. Should there be a wish to revisit the earlier ideas, they are presented at;

- Group Theory I : http://www.NumberWonder.co.uk/Pages/Page9108.html

Any reader is welcome to contact me for a set of answers to any exercise in either Group Theory I or II: Martin Hansen : mhh@shrewsbury.org.uk

1.2 Axioms

Four axioms define exactly what a group is;

The Definition of a Group

If G is a set and $\circ$ is a binary operation defined on G, then $(G, \circ)$ is a group if the following four axioms hold:

- **Closure:** For all $g_1, g_2 \in G,\ g_1 \circ g_2 \in G$
- **Identity:** There exists an identity element $e \in G$.
  This is such that, for all $g \in G$, $g \circ e = g = e * g$
- **Inverses:** For each $g \in G$, there exists an inverse element $g^{-1} \in G$
  This is such that $g \circ g^{-1} = e = g^{-1} \circ g$
- **Associativity:** For all $g_1, g_2, g_3 \in G,\ \ g_1 \circ (g_2 \circ g_3) = (g_1 \circ g_2) \circ g_3$

Two immediate consequences are that,

- A group can have one, and only one, identity element.
- Each element has one, and only one, inverse.

An Abelian Group

A group is described as being Abelian if the binary operation is commutative.

In other words, if, for all $g_1,\ g_2 \in G,\ g_1 \circ g_2 = g_2 \circ g_1$

1.3 Subgroups

A subgroup is a group within a group.
A subgroup must inherit the identity element from the parent group and for every other element that is inherited, the inverse of that element must also be inherited.
All groups, G, have two "trivial" subgroups, one containing only the identity {e} and the other being a full copy of the group itself.
Subgroups that are not trivial, if any exist, are termed "proper" subgroups.

The Definition and Identification of a Subgroup

A subgroup of a group $(G, \circ)$ is a group $(H, \circ)$ where H is a subset of G.
To show a subset H is a subgroup of G, show the following axioms hold;

- **Closure:** For all $h_1, h_2 \in H$, the composite $h_1 \circ h_2 \in H$
- **Identity:** The identity element, $e_G \in H$
- **Inverses:** For each $h \in H$, the inverse $h^{-1} \in H$

1.4 Order and Generators

The order of a group $(G, \circ)$ is simply the number of elements in the set G.

For example, if $G = \{e, a, c\}$ then $|G| = n\{e, a, c\} = 3$
Each element of a group also has an order associated with it.

To explain how this is determined, first note that, for example, $x \circ x = x^2$
and that, in general,

$$\underbrace{x \circ x \circ x \circ \ldots \circ x}_{k \text{ of these}} = x^k$$

Let x be an element of a finite group G, and let k be the least positive integer such that $x^k = e$. Then the order of the element x is k.

The strategy to find the order k of the element x in the finite group G is to determine the following sequence of composites,

$$x, x^2, x^3, \ldots$$

until an integer k is reached such that $x^k = e$
Then the order of x is k
Furthermore, the sequence of composites will form a (cyclic) subgroup.
It is said that the element x has generated this subgroup and the notation used is,

$$\langle x \rangle = \{e, x^2, x^3, \ldots, x^{k-1}\} \text{ where } x^k = e$$

All cyclic subgroups of a group can be found by using, in turn, each elements of the group as a generator. Non-cyclic subgroups will not be found, however.

1.5 Cyclic Groups

Definition of a Cyclic Group
A group G of finite order k is cyclic if it contains an element x such that,

$$G = \{e, x, x^2, x^3, \dots, x^{k-1}\} \text{ where } x^k = e \quad (e \text{ is the identity element})$$

- In any group, an element and its inverse generate the same cyclic group.
- A group of order p, where p is prime, is cyclic.

1.6 Cayley Tables

Given a group $(G, \circ)$ a Cayley Table shows all possible compositions of the elements of the set G. For example, the set $G = \{1, 9, 11\}$ under the binary operation multiplication modulo 14 has the following Cayley table;

$\times_{14}$	**1**	**9**	**11**
1	**1**	**9**	**11**
9	**9**	**11**	**1**
11	**11**	**1**	**9**

1.7 The Latin Square Property

All Cayley Tables have The Latin Square Property.

When the group $(G, \circ)$ is presented as a Cayley table each element occurs

- once and once only in each row
- once and once only in each column

Although all groups when presented as a Cayley table have the Latin square property not all Latin Squares are groups.

1.8 Lagrange's Theorem

When searching for subgroups of a given group, Lagrange's Theorem provides information on the possible orders of the subgroups.

Lagrange's Theorem
If H is a subgroup of a finite group G, the order of H divides the order of G.

- It is also of use to know that the order of an element in a group G must likewise divide the order of G.

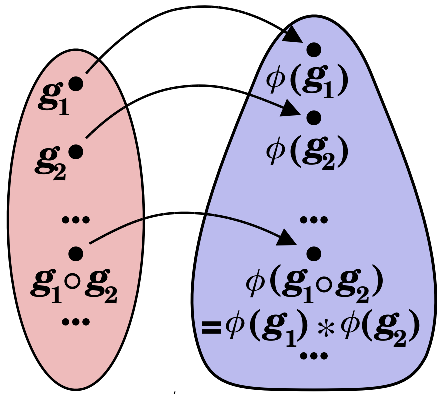
1.9 Isomorphic Groups

Two groups that are isomorphic have the same underlying structure.

Definition of Isomorphism

Two groups $(G, \circ)$ and $(H, *)$ are isomorphic, written $G \cong H$, if there exists a mapping $\phi\colon G \to H$ such that both of the following statements hold;

- ϕ is one-to-one onto
- For all $g_1,\ g_2 \in G,\ \phi(g_1 \circ g_2) = \phi(g_1) * \phi(g_2)$



$$(G, \circ) \xrightarrow{\phi} (H, *)$$

It is said that "group isomorphisms preserve identities, inverses, and the order of the groups and subgroups involved". These are all a consequence of the structure preserving relationship, that $\phi(g_1 \circ g_2) = \phi(g_1) * \phi(g_2)$. This key piece of algebra states that "The image of the composite is the composite of the images".

This can be pictured for two general finite groups as follows;

$\circ$	$\cdots$	g_2	$\cdots$
$\vdots$		$\vdots$	
g_1	$\cdots$	$g_1 \circ g_2$	$\cdots$
$\vdots$		$\vdots$	

$*$	$\cdots$	$\phi(g_2)$	$\cdots$
$\vdots$		$\vdots$	
$\phi(g_1)$	$\cdots$	$\phi(g_1) * \phi(g_2)$	$\cdots$
$\vdots$		$\vdots$	

$$(G, \circ) \xrightarrow{\phi} (H, *)$$

Some consequences of the definition of isomorphism are:

If $(G, \circ)$ and $(H, \circ)$ are isomorphic groups with identity elements e_G and e_H respectively, and $\phi: G \to H$ is an isomorphism from G to H then, for all $g \in G$ and integer values of k,

- $\phi(e_G) = e_H$ identity preserved
- $\phi(g^{-1}) = (\phi(g))^{-1}$ inverses preserved
- $\phi(g^k) = (\phi(g))^k$ orders of elements preserved
- $|G| = |H|$ order of group is preserved
- If G has n elements of order k, so does H
- If G has n subgroups of order k, so does H
- If J is a subgroup of G, then H has a subgroup isomorphic to J

- For groups of order 16 or greater, it is possible to find non-isomorphic groups with exactly the same number of elements of each order.
- A group of order p, for p prime, is isomorphic to the cyclic group of order p.

1.10 Example

Provide an axiomatic proof that the inverse of each element of a group is unique.

Teaching Video: http://www.NumberWonder.co.uk/v9110/1.mp4

[4 marks]

Having proven that each element, g, of a group, G, has a unique inverse it makes sense to talk of **the** inverse of an element.

The unique inverse of an element g is written g^{-1}

1.11 Exercise

Marks Available: 60

Question 1

Here is the first half of a proof that all Cayley group tables are Latin squares.

It begins with the assumption that there exists a row in a group's Cayley table in which the same element occurs twice.
So, given two distinct elements, x and y, in row a the situation is;

$\circ$	...	x	...	y	...
...	...	...	...	...	...
a	...	$a \circ x$	...	$a \circ y$	...
...	...	...	...	...	...

Under the assumption that the same element occurs twice,

$$a \circ x = a \circ y$$

$$a^{-1} \circ (a \circ x) = a^{-1} \circ (a \circ y) \qquad \text{Pre-multiply both sides}$$

$$(a^{-1} \circ a) \circ x = (a^{-1} \circ a) \circ y \qquad \text{(Associativity)}$$

$$e \circ x = e \circ y \qquad \text{(Inverses)}$$

$$x = y \qquad \text{(Identity)}$$

But this contradicts the starting assumption that x and y are distinct elements.
$\therefore$ the same element cannot occur twice in any row in a group Cayley table.

Complete the proof by showing that an element cannot occur twice in any column.

[4 marks]

Question 2

Provide an axiomatic proof that the identity element of a group is unique.

[4 marks]

Question 3

If x and y are elements of a group, prove that $(xy)^{-1} = y^{-1}x^{-1}$

[5 marks]

Question 4

An Abelian group $(G, \circ)$ contains elements a and b such that a is self-inverse and b is self-inverse. Prove that $a \circ b$ is also self inverse.
You may use the result proven in Question 3 if you wish.

[5 marks]

Question 5

If x, y are elements of a group G, and if all three of x, y, xy have order 2, prove that the group is Abelian.

[5 marks]

Question 6

Prove that, for a group of order 10, every proper subgroup must be cyclic.

[3 marks]

Question 7

Suppose that a, b are elements of a group and that $a^5 = e, \; b^4 = e, \; ab = b\,a^3$

Prove that,

(i) $a^2\,b = ba$

[5 marks]

(ii) $a\,b^3 = b^3\,a^2$

[5 marks]

Question 8

Further A-Level Examination Question from June 2018, FP3, Option 4, (OCR)

You are given that the set {1, 2, 4, 7, 8, 11, 13, 14} together with the binary operation of multiplication modulo 15 forms a group G.

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

[4 marks]

(ii) A subgroup of G has order n.
Write down the possible values of n.

[2 marks]

(iii) State all the proper cyclic subgroups of G

[4 marks]

(iv) For each of the following three cases, determine whether the set together with the binary operation forms a group. If the set does form a group, state whether or not it is isomorphic to *G*, justifying your answer. (You may assume associativity in each case)

(a) The set {0, 1, 2, 3, 4, 5, 6, 7} under addition modulo 8

(b) The set {1, 2, 3, 4, 5, 6, 7, 8} under multiplication modulo 9

(c) The set of matrices,

$$\left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\right.$$

$$\left.\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\right\}$$

together with the binary operation of matrix multiplication
(You may assume that the set is closed under matrix multiplication)

[14 marks]

1.12 Answers

1.12.1 Solution to 1.10 Example

The question ask for an axiomatic proof that the inverse of each element of a group is unique.

An axiomatic proof is one that only uses the defining properties of a group. They are: closure, identity, inverses and associativity.

When asked to show that something is unique, that there is only one of them, a fruitful line of approach is to assume that there are two. The claim is that there is only one, to which you say "Oh no there isn't !" and the maths bites back with "Oh yes there is !"

In other words “a proof by contradiction”.

Assume that y and z are two different inverses for the element x.
In consequence,

$$\begin{aligned} y &= ey && \text{where } e \text{ is the identity in the group (Identity)} \\ &= (zx)\,y && \text{since } z \text{ is an inverse for } x \text{ (Inverses)} \\ &= z\,(xy) && \text{(Associativity)} \\ &= ze && \text{since } y \text{ is an inverse for } x \text{ (Inverses)} \\ &= z && \text{as } e \text{ is the identity (Identity)} \end{aligned}$$

The assumption that y and z are different inverses to x results in a statement that y and z are the same.
$\therefore$ The inverse of each element of a group is unique. $\square$

[4 marks]

1.12.2 Solutions to 1.11 Exercise

Answer 1

Assume there exists a column in a Cayley table in which the same element occurs twice. Given two distinct elements, p and q, in column b the situation is;

$\circ$	**...**	$\boldsymbol{b}$	**...**
...	**...**	**...**	**...**
$\boldsymbol{p}$	**...**	$\boldsymbol{p \circ b}$	**...**
...	**...**	**...**	**...**
$\boldsymbol{q}$	**...**	$\boldsymbol{q \circ b}$	**...**
...	**...**	**...**	**...**

Under the assumption that the same element occurs twice,

$$p \circ b = q \circ b$$

$$(p \circ b) \circ b^{-1} = (q \circ b) \circ b^{-1} \qquad \text{Post-multiply both sides}$$

$$p \circ (b \circ b^{-1}) = q \circ (b \circ b^{-1}) \qquad \text{(Associativity)}$$

$$p \circ e = q \circ e \qquad \text{(Inverses)}$$

$$p = q \qquad \text{(Identity)}$$

But this contradicts the starting assumption that p and q are distinct elements.
$\therefore$ the same element cannot occur twice in any column in a group's Cayley table.

In conjunction, the two parts together prove that all group Cayley tables will be Latin squares.

$\square$

[4 marks]

Answer 2

Statement : The identity element of a group is unique.

Proof:

From the definition of a group;

- **Identity:** There exists an identity element $e \in G$.
  This is such that, for all $g \in G$, $g \circ e = g = e * g$

Assume that there exists a group which has two different identity elements.

Let those identity elements be, e_1 and e_2

Now, it must be true that $e_1 e_2 = e_2$ because e_1 is an identity element.

And, it must be true that $e_1 e_2 = e_1$ because e_2 is an identity element.

For both of the above two sentences to be true, $e_1 = e_2$

The assumption that e_1 and e_2 are different identity elements results in a statement that e_1 and e_2 are the same.

$\therefore$ The identity element of a group is unique. $\square$

[4 marks]

Answer 3

Statement: If x and y are elements of a group, $(xy)^{-1} = y^{-1}x^{-1}$

Proof:

From the definition of a group;

- **Inverses:** For each $g \in G$, there exists an inverse element $g^{-1} \in G$

  This is such that $g \circ g^{-1} = e = g^{-1} \circ g$

Thinking of xy as an element, g, of the group (closure) and $y^{-1}x^{-1}$ as another element, g^{-1}, of the group (closure) it has to be shown that,

$$(xy) \circ (y^{-1}x^{-1}) = e = (y^{-1}x^{-1}) \circ (xy)$$

Then, each of (xy) and $(y^{-1}x^{-1})$ is the other's inverse.

First, to show that $(xy) \circ (y^{-1}x^{-1}) = e$

$$\begin{aligned}
\text{LHS} &= (xy)(y^{-1}x^{-1}) \\
&= x(yy^{-1})x^{-1} && \text{(Associativity)} \\
&= x\,e\,x^{-1} && \text{(Inverses)} \\
&= x\,x^{-1} && \text{(Identity)} \\
&= e && \text{(Inverses)} \\
&= \text{RHS} && \square
\end{aligned}$$

Second, to show that $(y^{-1}x^{-1}) \circ (xy) = e$

$$\begin{aligned}
\text{LHS} &= (y^{-1}x^{-1})(xy) \\
&= y^{-1}(x^{-1}x)y && \text{(Associativity)} \\
&= y^{-1}\,e\,y && \text{(Inverses)} \\
&= y^{-1}y && \text{(Identity)} \\
&= e && \text{(Inverses)} \\
&= \text{RHS} && \square
\end{aligned}$$

Thus, $(xy)^{-1} = y^{-1}x^{-1}$ as required. $\square$

[5 marks]

Answer 4

Statement : When an Abelian group $(G, \circ)$ contains elements *a* and *b* such that *a* is self-inverse and *b* is self-inverse then $a \circ b$ is also self-inverse.

Proof:

When an element, *x*, is self-inverse it means that

$$x = x^{-1}$$

$$x\,x = x\,x^{-1} \qquad \text{pre-multiply both sides by } x$$

$$x^2 = e \qquad \text{(Identity)}$$

When two elements, *x* and *y* are in an Abelian group it means that the elements in the group are commutative. That is, $xy = yx$

To show that $a \circ b$ is self-inverse, show that $ab = (ab)^{-1}$

$$\begin{aligned}
\text{LHS} &= ab \\
&= e\,(ab)\,e && \text{(Identity)} \\
&= \left(a^{-1}\,a\right)(ab)\left(b\,b^{-1}\right) && \text{(Inverses)} \\
&= a^{-1}\,(a\,a)(b\,b)\,b^{-1} && \text{(Associativity)} \\
&= a^{-1}\,\left(a^2\right)\left(b^2\right)\,b^{-1} \\
&= a^{-1}\,(e)\,(e)\,b^{-1} && \text{(Identity)} \\
&= a^{-1}\,b^{-1} \\
&= b^{-1}\,a^{-1} && \text{As the group is Abelian} \\
&= (a\,b)^{-1} && \text{Using the Question 3 result} \\
&= \text{RHS} \qquad \square
\end{aligned}$$

[5 marks]

Answer 5

Statement: If x, y are elements of a group G, and if all three of x, y, xy have order 2, then that the group is Abelian.

Proof: Since xy has order 2,

$$
\begin{aligned}
(xy)^2 &= e \\
(xy)(xy) &= e \\
x(xy)(xy) &= xe && \text{Pre-multiply both sides by } x \\
(x\,x)y(xy) &= xe && \text{(Associativity)} \\
x^2 y(xy) &= xe \\
ey(xy) &= xe && \text{As } x \text{ has order 2} \\
y(xy) &= x && \text{(Identity)} \\
y(xy)y &= xy && \text{Post-multiply both sides by } y \\
yx(y\,y) &= xy && \text{(Associativity)} \\
yx\,y^2 &= xy \\
(yx)e &= xy && \text{As } y \text{ has order 2} \\
yx &= xy && \text{(Identity)}
\end{aligned}
$$

It has been shown that any two elements, x and y, are commutative.

$\therefore$ The group is Abelian $\square$

[5 marks]

Answer 6

Statement : Given a group of order 10, every proper subgroup must be cyclic.

Proof: By Lagrange's theorem, a group of order 10 can only have possible proper subgroups of order 2 or 5

A group (or subgroup) of prime order is cyclic.

Thus, every prober subgroup of a group of order 10 is cyclic.

[3 marks]

Answer 7

(i) **Statement:** Given that a, b are elements of a group and that

$$a^5 = e, \; b^4 = e, \; ab = b\,a^3 \text{ then } a^2 b = ba$$

Proof:

$$\begin{aligned}
\text{LHS} &= a^2 b \\
&= a(ab) \\
&= a\left(b\,a^3\right) \\
&= (ab)\,a^3 \\
&= \left(b\,a^3\right)a^3 \\
&= ba\left(a^5\right) \\
&= ba(e) \\
&= ba \\
&= \text{RHS} \qquad \square
\end{aligned}$$

[5 marks]

(ii) **Statement:** Given that a, b are elements of a group and that

$$a^5 = e,\ b^4 = e,\ ab = b\,a^3 \text{ then } a\,b^3 = b^3\,a^2$$

Lemma :

$$\begin{aligned} ab &= b\,a^3 \\ ab\,a^2 &= b\,a^3\,a^2 \\ ab\,a^2 &= b\,a^5 \\ ab\,a^2 &= b \end{aligned}$$

Proof:

$$\begin{aligned} \text{LHS} &= a\,b^3 \\ &= (ab)\,b^2 \\ &= (b\,a^3)\,b^2 \\ &= b\,a^2\,(ab)\,b \\ &= b\,a^2\,(b\,a^3)\,b \\ &= ba\,(ab\,a^2)\,(ab) \\ &= ba\,(b)\,(b\,a^3) \\ &= b\,(ab)\,b\,a^3 \\ &= b\,(b\,a^3)\,b\,a^3 \\ &= b^2\,a^2\,(ab\,a^2)\,a \\ &= b^2\,a^2\,(b)\,a \\ &= b^2\,a\,(ab)\,a \\ &= b^2\,a\,(ba^3)\,a \\ &= b^2\,(ab\,a^2)\,a^2 \\ &= b^2\,(b)\,a^2 \\ &= b^3\,a^2 \\ &= \text{RHS} \qquad \square \end{aligned}$$

[5 marks]

Answer 8

Although not asked for, a Cayley Table will be useful !

$\times_{15}$	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

(i) Using each element in turn as a generator;

$\langle 1 \rangle = \{1\}$ $\quad |1| = 1$

$\langle 2 \rangle = \{1, 2, 4, 8\}$ $\quad |2| = 4$

$\langle 4 \rangle = \{1, 4\}$ $\quad |4| = 2$

$\langle 7 \rangle = \{1, 4, 7, 13\}$ $\quad |7| = 4$

$\langle 8 \rangle = \{1, 2, 4, 8\}$ $\quad |8| = 4$

$\langle 11 \rangle = \{1, 11\}$ $\quad |11| = 2$

$\langle 13 \rangle = \{1, 4, 7, 13\}$ $\quad |13| = 4$

$\langle 14 \rangle = \{1, 14\}$ $\quad |14| = 2$

[4 marks]

(ii) The order of *G* is 8

Lagrange's theorem gives possible values of *n* as 1, 2, 4 or 8

[2 marks]

(iii) From part (i) the proper cyclic subgroups are,

{1, 4}, {1, 11}, {1,14}, {1, 2, 4, 8}, and {1, 4, 7, 13}

[4 marks]

(iv) **(a)** The set {0, 1, 2, 3, 4, 5, 6, 7} under addition modulo 8 forms a group because it is closed, and has 0 as identity. The inverse pairs are (1, 7), (2, 6), (3, 5) and 4 is self inverse.
It is a cyclic group because, for example, the element 1 generates the whole group.
No element of *G* generated the whole group in part (i) and so *G* is not cyclic.
$\therefore$ This group is not isomorphic with *G*

[6 marks]

(b) The set {1, 2, 3, 4, 5, 6, 7, 8} under multiplication modulo 9 is not a group because it is not closed; $3 \times 3 = 0 \pmod 9$

[2 marks]

(c) The set of matrices does form a group, initially suspected because they are all two dimensional transformation matrices.

$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity matrix

$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ is a rotation of 90° about the origin

$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ is a rotation of 180° about the origin

$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ is a rotation of 270° about the origin

$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is a reflection in $y = x$

$\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$ is a reflection in $y = -x$

$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ is reflection in the x-axis

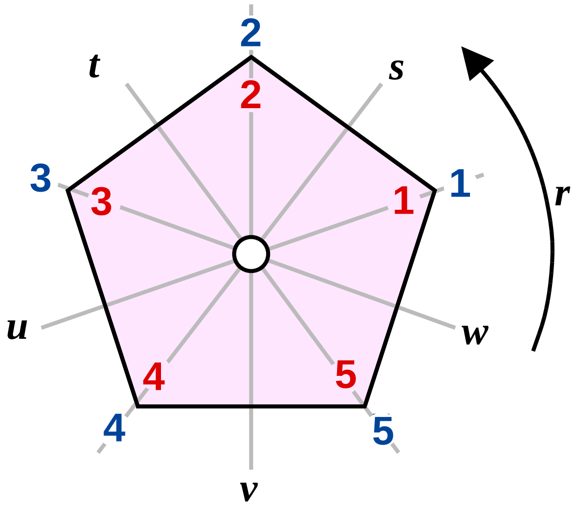
$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ is a reflection in the y-axis

So, $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ is the inverse of $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ with the other non-identity elements being self inverse.
With six self-inverse elements, this is not isomorphic to *G* which has only three.

[6 marks]

2.1 Cycle Notation

To study the symmetries of a regular pentagon, the five vertices are numbered from 1 to 5. The five lines of mirror symmetry are labelled s, t, u, v and w.
A rotation of 72° is denoted r, as shown in the diagram.



The set G is $\{e, \ r, \ r^2, r^3, \ r^4, s, t, u, v, w\}$, where the elements represent transformations. The identity is e and r^2, for example, is a rotation of 144°.
Under the binary operation "followed by" the group $(G, \circ)$ of symmetries of a regular pentagon is established.

Under the transformation r^2 the red vertices move into these blue positions:

$$1 \to 3, \quad 2 \to 4, \quad 3 \to 5, \quad 4 \to 1, \quad 5 \to 2$$

This can be expressed in two line permutation notation as,

$$r^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}$$

Similarly, the reflection in s can be written,

$$s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix}$$

However, this notation is cumbersome; the red line is always the same and how the shape actually moved is not clear at a glance.
In an improved notation, called "cycle notation" the movement instructions are lined up differently;

$$1 \to 3, \quad 3 \to 5, \quad 5 \to 2, \quad 2 \to 4, \quad 4 \to 1$$

The idea is to group like so;

$$1 \to (3, 3) \to (5, 5) \to (2, 2) \to (4, 4) \to 1$$

before throwing away the unnecessary blue doubles and commas;

$$r^2 = (1\,3\,5\,2\,4)$$

There is no necessity to start the cycle from 1 with the result that there are the following equivalent ways of describing the rotation of 144°;

$$r^2 = (1\,3\,5\,2\,4) = (3\,5\,2\,4\,1) = (5\,2\,4\,1\,3) = (2\,4\,1\,3\,5) = (4\,1\,3\,5\,2)$$

Not all of the pentagon's symmetry permutations cycle though all five digits as was the case in the above example.
To see this, consider the reflection *s*.
Here is the logic behind how that is written in cycle notation;

$$s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix}$$

$$1 \to 2, \quad 2 \to 1, \quad 3 \to 5, \quad 4 \to 4, \quad 5 \to 3$$

$$1 \to 2, \quad 2 \to 1 \quad : \quad 3 \to 5, \quad 5 \to 3, \quad : \quad 4 \to 4$$

$$1 \to (\,2, 2\,) \to 1 \quad : \quad 3 \to (\,5, 5\,) \to 3 \quad : \quad (\,4, 4\,)$$

$$s = (1\,2)(3\,5)(4)$$

By convention, any point that is fixed, such as in this case the 4, may be dropped.

$$\therefore\ s = (1\,2)(3\,5)$$

Again this can be written in a variety of equivalent ways;

$$s = (1\,2)(3\,5) = (1\,2)(5\,3) = (2\,1)(3\,5) = (2\,1)(5\,3)$$
$$= (3\,5)(1\,2) = (3\,5)(2\,1) = (5\,3)(1\,2) = (5\,3)(2\,1)$$

2.2 Composition

By continuing to work with the symmetry group of the pentagon and working in cycle notation, show that $s\,r^2 = w$

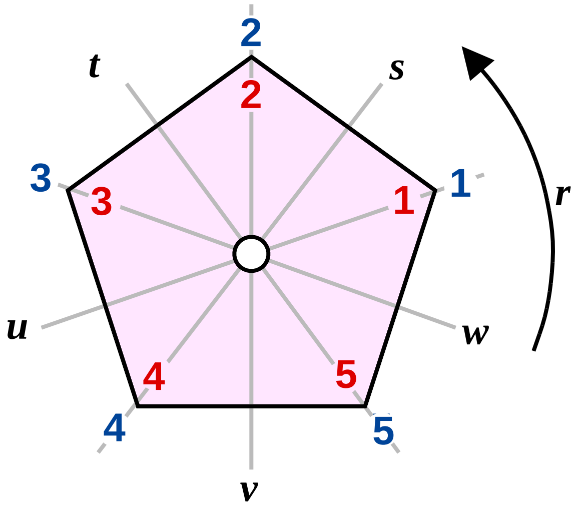
Teaching video: http://www.NumberWonder.co.uk/v9110/2.mp4

[4 marks]

2.3 Exercise

Marks Available: 40

Question 1



Complete the following table to show each of the symmetries of the pentagon written in cycle notation;

Symmetry	Cycle Notation
e	(1)(2)(3)(4)(5)
r	
r^2	(1 3 5 2 4)
r^3	
r^4	
s	(1 2) (3 5)
t	
u	
v	
w	(1 5) (2 4)

[5 marks]

Question 2

Show that $s\,r^2 \neq r^2\,s$

[2 marks]

Question 3

Complete the Cayley table for the group of symmetries of a regular pentagon.

$*$	e	r	r^2	r^3	r^4	s	t	u	v	w
e	e	r	r^2	r^3	r^4			u	v	w
r	r	r^2	r^3	r^4	e			s	t	u
r^2	r^2	r^3	r^4	e	r			v	w	s
r^3	r^3	r^4	e	r	r^2			t	u	v
r^4	r^4	e	r	r^2	r^3			w	s	t
s										
t										
u	u	w	t	v	s			e	r^3	r
v	v	s	u	w	t			r^2	e	r^3
w	w	t	v	s	u			r^4	r^2	e

[6 marks]

Question 4

A transposition written in cycle notation is a permutation amongst n elements which swaps exactly two of them.

For example, when working with the group of symmetries of the pentagon, the transposition $(1\ 4)$ can be invoked. This is in spite of the fact that there is no symmetry of the pentagon that swaps only the 1 with the 4, leaving all else fixed. That is, there was no pentagon symmetry that had the two-line permutation,

$$\chi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 1 & 5 \end{pmatrix}$$

(i) Verify that for the regular pentagon,

$$(1\ 2) \circ (3\ 1) \circ (4\ 1) \circ (1\ 5) = r^4$$

[2 marks]

(ii) To which symmetry of the pentagon is the following transposition equivalent ?

$$(2\ 4) \circ (1\ 2) \circ (2\ 3) \circ (5\ 2)$$

[2 marks]

(iii) To which symmetry of the pentagon is the following transposition equivalent ?

$$(5\ 3) \circ (3\ 2) \circ (4\ 3) \circ (1\ 3)$$

[2 marks]

Question 5
Any permutation can be decomposed into a composition of transpositions.
The decomposition is not unique (As was demonstrated by Question 4)
What is unique is whether the result has an even or an odd number of transpositions.

Permutation Decomposition Technique

$$(g_1\, g_2\, g_3 \ldots g_n) = (g_1\, g_n) \circ (g_1\, g_{n-1}) \circ \ldots \circ (g_1\, g_3) \circ (g_1\, g_2)$$

The symmetry of the pentagon, r^2, can be written is cycle notation in several ways including $(1\ 3\ 5\ 2\ 4)$ or $(5\ 2\ 4\ 1\ 3)$

Use the Permutation Decomposition Technique to write the following as a composition of transpositions;

(i) $r^2 = (1\ 3\ 5\ 2\ 4)$

[2 marks]

(ii) $r^2 = (5\ 2\ 4\ 1\ 3)$

[2 marks]

(iii) In both part (i) and part (ii) is the parity of the composition of transpositions odd or even ?

[1 mark]

There is a theorem, called the Parity Theorem, which confirms what the above suggests;

The Parity Theorem
A permutation cannot be written both as a composite of an even number of transpositions and as a composite of an odd number of transpositions.
In other words, the properties of being odd or being even are mutually exclusive for compositions of transpositions.

Question 6

Open University Examination Question, (M203) (edited)

The two-line symbols for permutations p and q in the permutation group S_6 are

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 1 & 3 & 6 & 5 \end{pmatrix} \text{ and } q = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 5 & 4 & 3 \end{pmatrix}$$

(a) Write down the permutations p, q, p^{-1} and q^{-1} in cycle form.

[4 marks]

(b) Determine the products $p \circ q$ and $q \circ p$ in cycle notation.

[2 marks]

(c) Write p and q as products of transpositions.
State the parity of p and q.

[4 marks]

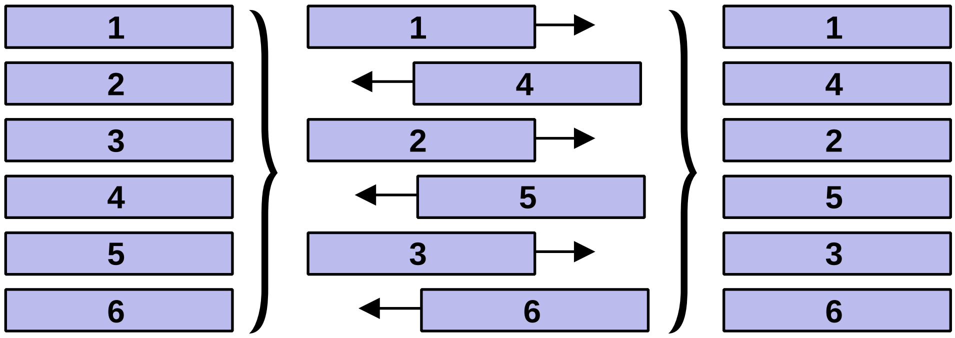
(d) Let r be the permutation in S_6 that is given in cycle form as $(2\ 3\ 4\ 5)$

Find a permutation s in S_6 such that $r \circ s = q \circ r$

[2 marks]

Question 7

A deck of six cards is cut exactly in half and a perfect riffle shuffle carried out. The diagram below shows this Faro shuffle.



(i) Write down in cycle notation the permutation of one such shuffle.

[1 mark]

(ii) Call the part (i) permutation s.

Calculate s^2, s^3 and so on until the identify permutation is reached.

The identity permutation could be written $e = (1)(2)(3)(4)(5)(6)$

[2 marks]

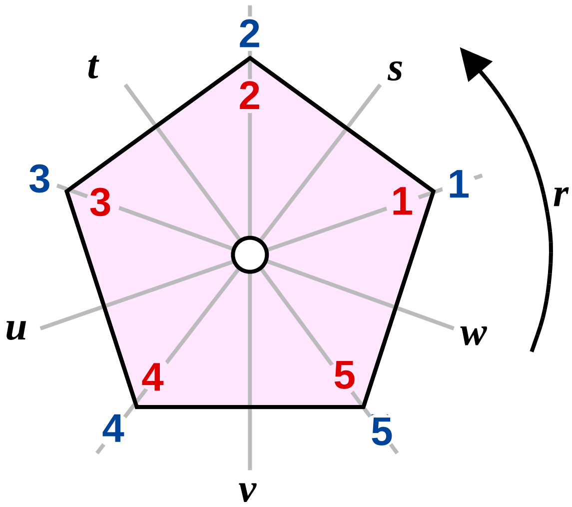
(iii) Explain the significance of your part (ii) answer in regards to the repeated perfect Faro riffle shuffling of the deck of six cards.

[1 mark]

2.4 Answers

2.4.1 Solution to 2.2 Example (Teaching Video)

By continuing to work with the symmetry group of the pentagon and working in cycle notation, show that $s\,r^2 = w$



w will
- keep 3 fixed
- swap 2 and 4
- swap 1 and 5

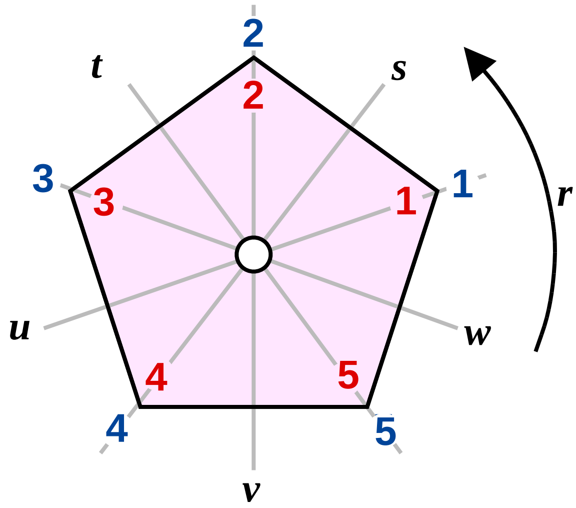
$\therefore\ w = (1\ 5)(2\ 4)$

$$\begin{aligned} \text{LHS} &= s\,r^2 \\ &= (1\ 2)(3\ 5) \circ (1\ 3\ 5\ 2\ 4) \\ &= (\ 1\ 5\ )(2\ 4) \\ &= w \\ &= \text{RHS} \quad \square \end{aligned}$$

[4 marks]

2.4.2 Solutions to 2.3 Exercise

Answer 1



Symmetry	Cycle Notation
e	$(1)(2)(3)(4)(5)$
r	$(1\,2\,3\,4\,5)$
r^2	$(1\,3\,5\,2\,4)$
r^3	$(1\,4\,2\,5\,3)$
r^4	$(1\,5\,4\,3\,2)$
s	$(1\,2)(3\,5)$
t	$(1\,4)(2\,3)$
u	$(2\,5)(3\,4)$
v	$(1\,3)(4\,5)$
w	$(1\,5)(2\,4)$

[5 marks]

Answer 2

From the teaching video, it is shown that, $s\,r^2 \;=\; w$

Experimentation, perhaps in your mind palace, suggests $r^2\,s \;=\; t$

Proving that is easy using cycle notation.

First of all, note that the pieces in play are

$$s \;=\; (1\;2)(3\;5)\,,\quad r^2 \;=\; (1\;3\;5\;2\;4)\ \text{and}\ t \;=\; (1\;4)(2\;3)$$

Proof:

$$\begin{aligned}
\text{LHS} &= r^2\,s \\
&= (1\;3\;5\;2\;4) \circ (1\;2)(3\;5) \\
&= (1\;4)(2\;3) \\
&= t \\
&= \text{RHS}
\end{aligned}$$

$$\therefore\; s\,r^2 \;\neq\; r^2\,s \qquad\qquad \square$$

[2 marks]

Answer 3

$*$	e	r	r^2	r^3	r^4	s	t	u	v	w
e	e	r	r^2	r^3	r^4	s	t	u	v	w
r	r	r^2	r^3	r^4	e	v	w	s	t	u
r^2	r^2	r^3	r^4	e	r	t	u	v	w	s
r^3	r^3	r^4	e	r	r^2	w	s	t	u	v
r^4	r^4	e	r	r^2	r^3	u	v	w	s	t
s	s	u	w	t	v	e	r^3	r	r^4	r^2
t	t	v	s	u	w	r^2	e	r^3	r	r^4
u	u	w	t	v	s	r^4	r^2	e	r^3	r
v	v	s	u	w	t	r	r^4	r^2	e	r^3
w	w	t	v	s	u	r^3	r	r^4	r^2	e

[6 marks]

Answer 4

(i) **Statement:** $(1\ 2) \circ (3\ 1) \circ (4\ 1) \circ (1\ 5) = r^4$

Proof: From Question 1, it is known that $r^4 = (1\ 5\ 4\ 3\ 2)$

$$\begin{aligned} \text{LHS} &= (1\ 2) \circ (3\ 1) \circ (4\ 1) \circ (1\ 5) \\ &= (1\ 5\ 4\ 3\ 2) \\ &= r^4 \\ &= \text{RHS} \qquad \square \end{aligned}$$

[2 marks]

(ii) $(2\ 4) \circ (1\ 2) \circ (2\ 3) \circ (5\ 2) = (1\ 4\ 2\ 5\ 3)$

$$= r^3$$

[2 marks]

(iii) $(5\ 3) \circ (3\ 2) \circ (4\ 3) \circ (1\ 3) = (1\ 4\ 2\ 5\ 3)$

$$= r^3$$

[2 marks]

Answer 5

(i) $r^2 = (1\ 3\ 5\ 2\ 4)$

$$= (1\ 4) \circ (1\ 2) \circ (1\ 5) \circ (1\ 3)$$

[2 marks]

(ii) $r^2 = (5\ 2\ 4\ 1\ 3)$

$$= (5\ 3) \circ (5\ 1) \circ (5\ 4) \circ (5\ 2)$$

[2 marks]

(iii) Even

[1 mark]

Answer 6

(a) $p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 1 & 3 & 6 & 5 \end{pmatrix} \Rightarrow p = (1\,4\,3)(5\,6)$

[1 mark]

$q = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 5 & 4 & 3 \end{pmatrix} \Rightarrow q = (1\,6\,3\,2)(4\,5)$

[1 mark]

$p^{-1} = (1\,3\,4)(5\,6)$

[1 mark]

$q^{-1} = (1\,2\,3\,6)(4\,5)$

[1 mark]

(b) $p \circ q = (1\,4\,3)(5\,6) \circ (1\,6\,3\,2)(4\,5)$

$= (\,1\,5\,3\,2\,4\,6\,)$

[1 mark]

$q \circ p = (1\,6\,3\,2)(4\,5) \circ (1\,4\,3)(5\,6)$

$= (1\,5\,3\,6\,4\,2)$

[1 mark]

(c) $p = (1\,4\,3)(5\,6)$

$= (1\,3) \circ (1\,4) \circ (5\,6)$ Parity of p is ODD

[2 marks]

$q = (1\,6\,3\,2)(4\,5)$

$= (1\,2) \circ (1\,3) \circ (1\,6) \circ (4\,5)$ Parity of q is EVEN

[2 marks]

(d) $r \circ s = q \circ r$

$r^{-1} \circ r \circ s = r^{-1} \circ q \circ r$ Pre-multiply both sides by r^{-1}

$s = r^{-1} \circ q \circ r$

$= (2\,3\,4\,5)^{-1} \circ (1\,6\,3\,2)(4\,5) \circ (2\,3\,4\,5)$

$= (2\,5\,4\,3) \circ (1\,6\,3\,2)(4\,5) \circ (2\,3\,4\,5)$

$= (1\,6\,2\,5)(3\,4)$

[2 marks]

Answer 7

(i) $$s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 5 & 3 & 6 \end{pmatrix}$$

$$= (2\,4\,5\,3)$$

[1 mark]

(ii)

$$\begin{aligned} s^2 &= (2\,4\,5\,3) \circ (2\,4\,5\,3) \\ &= (2\,5)(3\,4) \\ s^3 &= (2\,4\,5\,3) \circ (2\,5)(3\,4) \\ &= (2\,3\,5\,4) \\ s^4 &= (2\,4\,5\,3) \circ (2\,3\,5\,4) \\ &= (1)(2)(3)(4)(5)(6) \\ &= e \end{aligned}$$

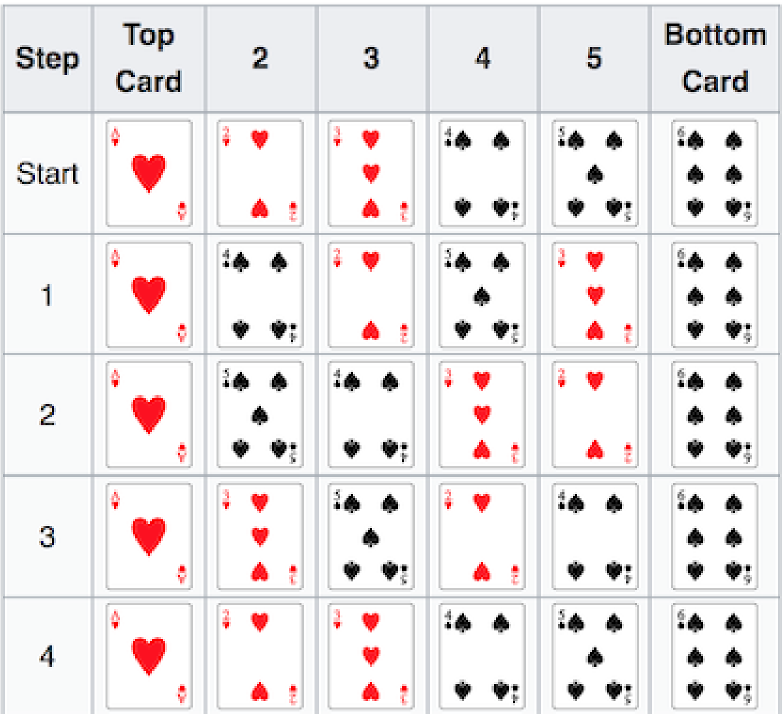
The identity permutation

[2 marks]

(iii) This question shows that after four perfect shuffles the deck of six cards is back in its original order.

[1 mark]

Here is a demonstration of the process;



Lecture 3

University Undergraduate Lectures in Mathematics
A First Year Course
Group Theory II

3.1 Permutations

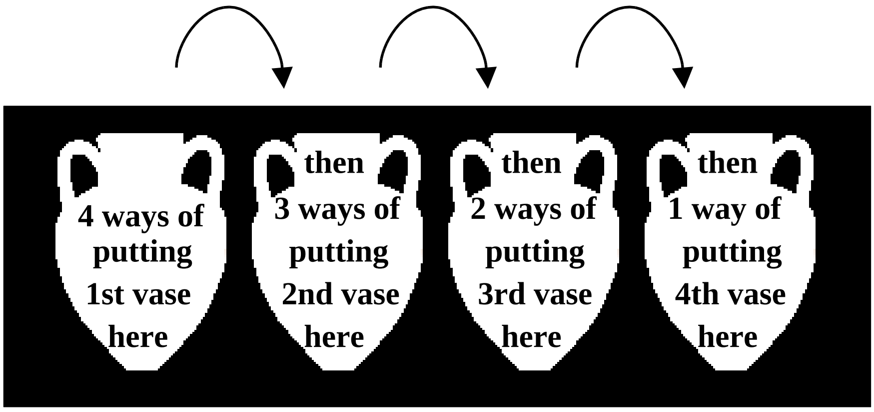
Given a set of objects, a permutation of them is a re-arrangement of them among themselves. For example, suppose there are four distinct vases on a shelf. The easiest way to identify them is to assign an integer to each.

They can now be permuted, for example by swapping vases 1 and 2 and swapping vases 3 and 4.

In two line permutation notation the rearrangement is captured by,

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

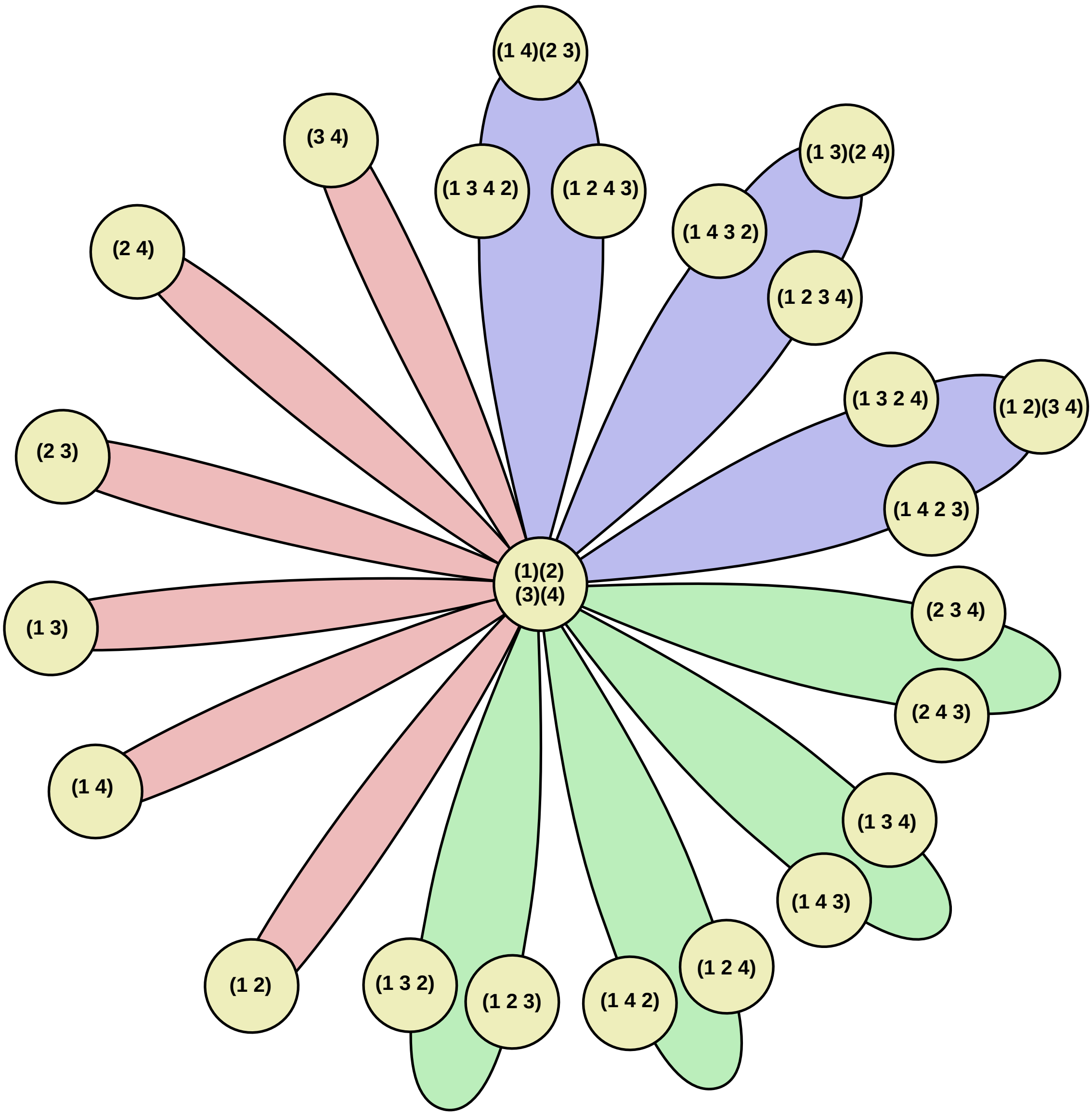
A key questions is,
“How many different possible arrangements of the four vases are there ?”



If the vases are taken off the shelf then, working from left to right, there are four possible vases from which one could be randomly chosen to put back first. Then, one of three possible vases could be randomly put back second with two possibilities after that and, finally, the only vase not yet chosen is put back on the shelf.

In total there are thus 4! possible permutations of the four vases.
All of these permutations under composition of permutations form a group called the Symmetric group of degree four, S_4

Here are all 24 permutations of S_4, written in cycle notation, on a Cycle Graph;



The Cycle Graph shows all the various cyclic subgroups of S_4

- The red petals show 6 cyclic subgroups of order 2
  They are: $\{e, (1\ 2)\}$, $\{e, (1\ 4)\}$, $\{e, (1\ 3)\}$, $\{e, (2\ 3)\}$, $\{e, (2\ 4)\}$ and $\{e, (3\ 4)\}$
- The green petals show 4 cyclic subgroups of order 3
  They are: $\{e, (2\ 3\ 4), (2\ 4\ 3)\}$, $\{e, (1\ 3\ 4), (1\ 4\ 3)\}$, $\{e, (1\ 2\ 4), (1\ 4\ 2)\}$ and $\{e, (1\ 2\ 3), (1\ 3\ 2)\}$
- The purple petals show 3 cyclic subgroups of order 4
  They are: $\{e, (1\ 3\ 4\ 2), (1\ 4)(2\ 3), (1\ 2\ 3\ 4)\}$, $\{e, (1\ 4\ 3\ 2), (1\ 3)(2\ 4), (1\ 2\ 3\ 4)\}$ and $\{e, (1\ 3\ 2\ 4), (1\ 2)(3\ 4), (1\ 4\ 2\ 3)\}$

3.2 The Symmetric Group S_n

The Permutation Group, (S_n, $\circ$)

A permutation of a finite set S is a rearrangement of the elements of S.
Specifically, permutation is a one-to-one function from S onto S.
Typically, the set S equals $\{1, 2, 3, 4, \ldots , n\}$ in which case the set is written S_n.
Under composition, "The Symmetric Group, S_n, of degree n" is formed.
The order of the group S_n is $n!$
It is non-Abelian for $n \geqslant 3$

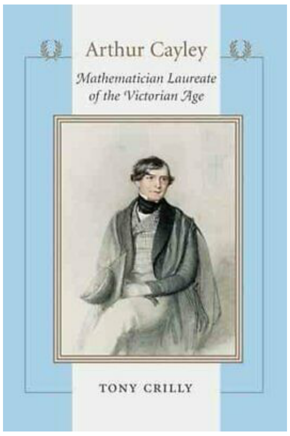
3.3 Cayley's Theorem

The symmetric Groups are important, particularly historically. They were the first type of group to be studied as such, and originally "group" meant "group of permutations". Many of the properties of general finite groups were discovered for the permutation groups in the nineteenth century before the abstract nature of groups was fully understood. In a certain sense, all finite groups are contained in the symmetric groups, a result known as Cayley's Theorem.

Cayley's Theorem

Every finite group is isomorphic to a permutation group.

- This remarkable result, shortly to be proven, suggests that only the symmetric groups need be studied. All else is within! However, with the order of the permutation group S_n being $n!$ the groups involved quickly become daunting to work with. S_9 for example, is of order 362,880.
- Arthur Cayley (1821-1895) was a prolific British Mathematician who made wide ranging contributions to Pure Mathematics including Algebra, Analytic Geometry and the theory of Matrices and determinants. Aged 42 he became a professor at Cambridge University, a post that allowed him to give up his "day job" as a lawyer and focus whole heartedly on his passion for mathematics.



The book *Arthur Cayley*, by Tony Crilly (2005)

Proof of Cayley's Theorem

Let G be a finite group with elements $g_1, g_2, g_3, \dots, g_n$.

With each element of G, associate a permutation of the n elements of G by assigning to that element the permutation obtained from its row in the Cayley table for the group.

For example, let x and y be two elements in G, with the consequence (due to closure) that xy is also an element in G.

The Cayley table will then be of the following form;

$\circ$	g_1	g_2	g_3	...	g_n
g_1					
...	...	...	...	...	...
x	$x\,g_1$	$x\,g_2$	$x\,g_3$	...	$x\,g_n$
...	...	...	...	...	...
y	$y\,g_1$	$y\,g_2$	$y\,g_3$	...	$y\,g_n$
...	...	...	...	...	...
$x\,y$	$x\,y\,g_1$	$x\,y\,g_2$	$x\,y\,g_3$	...	$x\,y\,g_n$
...	...	...	...	...	...
g_n					

The permutation obtained from x is,

$$P_x = \begin{pmatrix} g_1 & g_2 & g_3 & \cdots & g_n \\ x\,g_1 & x\,g_2 & x\,g_3 & \cdots & x\,g_n \end{pmatrix}$$

and from y is,

$$P_y = \begin{pmatrix} g_1 & g_2 & g_3 & \cdots & g_n \\ y\,g_1 & y\,g_2 & y\,g_3 & \cdots & y\,g_n \end{pmatrix}$$

Consider the composite, $P_x \circ P_y$

$$P_x \circ P_y = \begin{pmatrix} g_1 & g_2 & \dots & y\,t & \dots & g_n \\ x\,g_1 & x\,g_2 & \dots & x\,y\,t & \dots & x\,g_n \end{pmatrix} \circ \begin{pmatrix} g_1 & g_2 & \dots & t & \dots & g_n \\ y\,g_1 & y\,g_2 & \dots & y\,t & \dots & y\,g_n \end{pmatrix}$$

$$= \begin{pmatrix} g_1 & g_2 & \dots & t & \dots & g_n \\ x\,y\,g_1 & x\,y\,g_2 & \dots & xyt & \dots & xy\,g_n \end{pmatrix}$$

The above is showing that $P_x \circ P_y$ maps each element $t \in G$ to $x\,y\,t \in G$.

However, that is precisely what the permutation P_{xy} did in the Cayley table.

$$\therefore\ P_x \circ P_y = P_{xy}$$

The claim now is that the set of constructed permutations forms a subgroup of G which will be called P.
Checking the subgroup axioms hold (see 1.3 Subgroups):

Closure: The equation $P_x \circ P_y = P_{xy}$ shows that the composite of two of the constructed permutations is another of the constructed permutations. $\therefore$ P is closed.

Identity: The identity element e of G gives rise to the identity permutation P_e

$$P_e = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ e\,g_1 & e\,g_2 & \cdots & e\,g_n \end{pmatrix} = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1 & g_2 & \cdots & g_n \end{pmatrix}$$

$\therefore$ The subgroup P contains as identity, the identity of G, as required.

Inverses: $P_x \circ P_y = P_{xy}$ establishes that $P_{g^{-1}}$ is the inverse of P_g because

- $P_g \circ P_{g^{-1}} = P_{g\,g^{-1}} = P_e$
- $P_{g^{-1}} \circ P_g = P_{g^{-1}g} = P_e$

$\therefore$ For each element of G that's in H, the corresponding inverse element from G is also in H, as required.

Thus, the set of permutations $\{P_g \ : \ g \in G\}$ forms a group.

Furthermore, the equation $P_x \circ P_y = P_{xy}$ shows the constructed permutations combine in the same way as the corresponding original elements; the Cayley table for the constructed group is identical to the original Cayley table, but with g replaced by P_g. The mapping $g \to P_g$ is an isomorphism between the two groups.

That is $G \cong H$.

This concludes the proof of Cayley's theorem. □

3.3 Constructing a Cycle Graph

Cycle Graph Construction Strategy

Start with a graph containing only the identity element as a single node.

1. Pick an element not already in the graph.
2. Compute the cyclic subgroup generated by that element and add the cycle to the graph, connecting to already existing nodes as needed
3. If the graph contains a sub-cycle of the new cycle, delete the sub-cycle.
4. Repeat steps 1 to 3 until all of the (finitely many) elements have a node.

3.4 Example

Construct a cycle graph from the following Cayley table which is for the group of symmetries of a square, with *r* being a rotation of 90° about the centre, and *y*, *x*, *p* and *n* being reflections in the *y*-axis, *x*-axis, $y = x$ and $y = -x$ respectively.

*	e	r	r^2	r^3	y	x	p	n
e	e	r	r^2	r^3	y	x	p	n
r	r	r^2	r^3	e	n	p	y	x
r^2	r^2	r^3	e	r	x	y	n	p
r^3	r^3	e	r	r^2	p	n	x	y
y	y	p	x	n	e	r^2	r^3	r
x	x	n	y	p	r^2	e	r	r^3
p	p	x	n	y	r	r^3	e	r^2
n	n	y	p	x	r^3	r	r^2	e

Teaching video: http://www.NumberWonder.co.uk/v9110/3.mp4

[3 marks]

3.5 Exercise

Marks Available: 40

Question 1

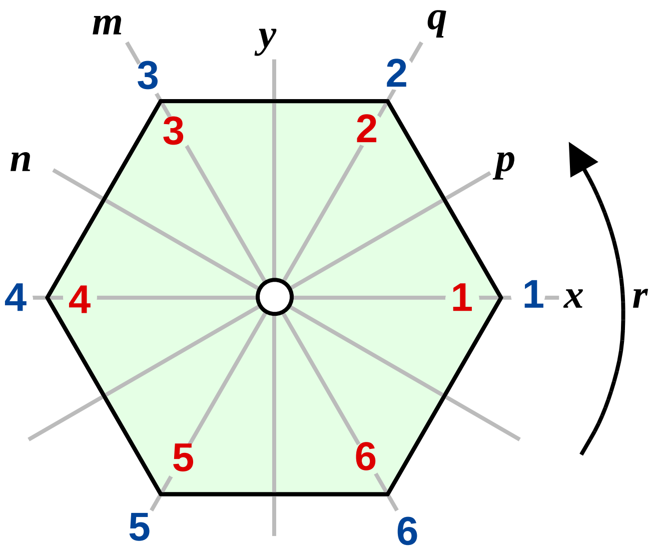
Construct a cycle graph from the following Cayley table which is for the group of symmetries of a regular pentagon that was studied in Lecture 2.

$*$	e	r	r^2	r^3	r^4	s	t	u	v	w
e	e	r	r^2	r^3	r^4	s	t	u	v	w
r	r	r^2	r^3	r^4	e	v	w	s	t	u
r^2	r^2	r^3	r^4	e	r	t	u	v	w	s
r^3	r^3	r^4	e	r	r^2	w	s	t	u	v
r^4	r^4	e	r	r^2	r^3	u	v	w	s	t
s	s	u	w	t	v	e	r^3	r	r^4	r^2
t	t	v	s	u	w	r^2	e	r^3	r	r^4
u	u	w	t	v	s	r^4	r^2	e	r^3	r
v	v	s	u	w	t	r	r^4	r^2	e	r^3
w	w	t	v	s	u	r^3	r	r^4	r^2	e

[3 marks]

Question 2

This question considers the symmetries of a regular hexagon. The six vertices are numbered from 1 to 6. The six lines of mirror symmetry are labelled x, p, q, y, m and n and a rotation of 60° is denoted r, as shown in the diagram.



(i) Draw the cycle graph for the group of symmetries, H, of the regular hexagon under the binary operation of composition of transformations.

[3 marks]

(ii) Complete the following table to show all the cyclic subgroups of H.

Subgroup	Order		Subgroup	Order		Subgroup	Order
$\{e\}$	1			2			3
$\{e, x\}$	2			2			6
	2			2		$\{e, x, p, q, y, m, n$	
	2			2		$r, r^2, r^3, r^4, r^5\}$	12

[3 marks]

(iii) For the symmetries of a regular hexagon, complete the following table for each symmetry to show,

- it's order (the same as the order of the associated permutation)
- how it would be written in permutation cycle notation
- one way it could be written as a composition of transpositions (the composition symbol $\circ$ may be omitted)
- the parity of the transpositions (whether odd or even)

Symmetry	Order	Cycle Notation	Transpositions	Parity
e	1	$(1)(2)(3)(4)(5)(6)$	none	even
r	6	$(1\ 2\ 3\ 4\ 5\ 6)$	$(1\ 6)(1\ 5)(1\ 4)(1\ 3)(1\ 2)$	odd
r^2	3	$(1\ 3\ 5)(2\ 4\ 6)$	$(1\ 5)(1\ 3)(2\ 6)(2\ 4)$	even
r^3				
r^4				
r^5				
x	2	$(2\ 6)(3\ 5)$	$(2\ 6)(3\ 5)$	even
p				
q				
y				
m	2	$(1\ 5)(2\ 4)$	$(1\ 5)(2\ 4)$	even
n				

[7 marks]

(iv) Robin suspects that all the elements with even parity form a (non-cyclic) subgroup of H. Construct the Cayley table for these elements and use it to help determine if Robin's suspicion is correct or not.

[3 marks]

(v) State a standard fundamental group to which H is isomorphic.

[1 mark]

(vi) Prove that for any group G, the elements with even parity form a subgroup. You may use the fact that,

- even and odd permutations combine according to the parity table;

+	even	odd
even	even	odd
odd	odd	even

[6 marks]

Question 3

Consider the cyclic group $\mathbb{Z}_p$, of order p where p is prime.

(i) Draw a cycle graph for $\mathbb{Z}_p$

[2 marks]

(ii) Explain why $\mathbb{Z}_p$ has no proper subgroups.

[2 marks]

Question 4

Consider a cyclic group of order p^2, where p is prime.

(i) How many proper subgroups will this group have ?
Give a reason for your answer.

Hint : It may be helpful to
first do this question
for a specific prime,
say $p = 11$

[2 marks]

(ii) For each subgroup found, list both the subgroup and its generator.

[2 marks]

Question 5
Show that any cyclic group of even order has exactly one element of order 2

[3 marks]

Question 6
Let G be a group, with identity element e, containing finite subgroups H and K.
If $|H|$ and $|K|$ are coprime, show that $H \cap K = \{e\}$

Assume that the intersection of two subgroups of a group is itself a subgroup†

[3 marks]

† For a proof see, for example, *Groups and Symmetry* by MA Armstrong, page 23

3.6 Answers

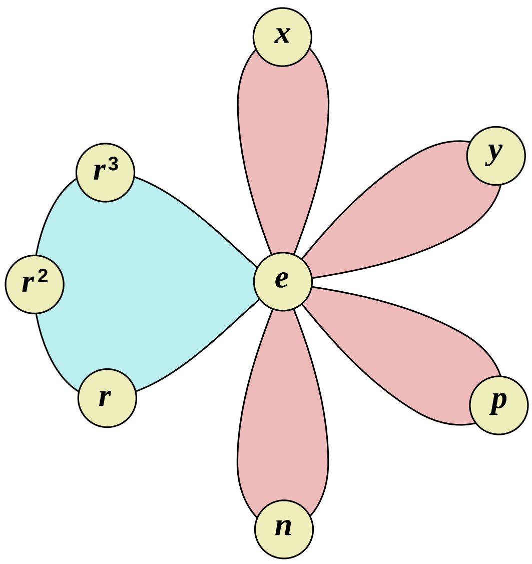
3.6.1 Solution to 3.4 Example (Teaching Video)

$*$	e	r	r^2	r^3	y	x	p	n
e	e	r	r^2	r^3	y	x	p	n
r	r	r^2	r^3	e	n	p	y	x
r^2	r^2	r^3	e	r	x	y	n	p
r^3	r^3	e	r	r^2	p	n	x	y
y	y	p	x	n	e	r^2	r^3	r
x	x	n	y	p	r^2	e	r	r^3
p	p	x	n	y	r	r^3	e	r^2
n	n	y	p	x	r^3	r	r^2	e

Cycle Graph Construction Strategy

Start with a graph containing only the identity element as a single node.

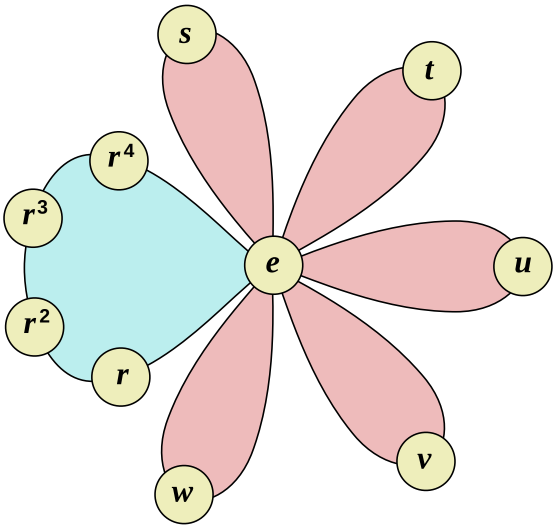
1. Pick an element not already in the graph.
2. Compute the cyclic subgroup generated by that element and add the cycle to the graph, connecting to already existing nodes as needed.
3. If the graph contains a sub-cycle of the new cycle, delete the sub-cycle.
4. Repeat steps 1 to 3 until all of the (finitely many) elements have a node.



[3 marks]

3.6.2 Solutions to 3.5 Exercise

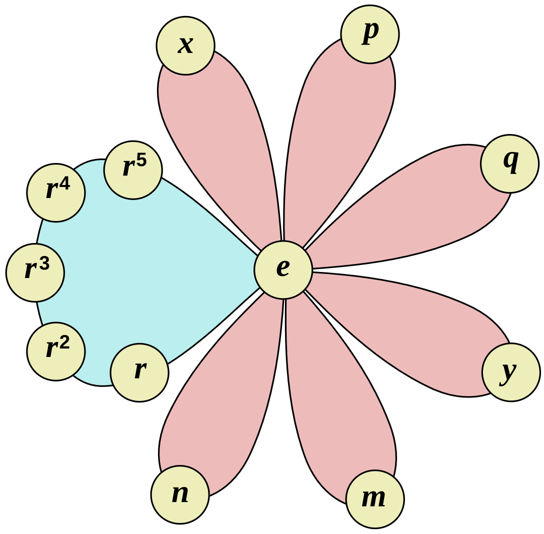
Answer 1



[3 marks]

Answer 2

(i)



[3 marks]

(ii)

Subgroup	Order		Subgroup	Order		Subgroup	Order
$\{e\}$	1		$\{e,\ y\}$	2		$\{e, r^2, r^4\}$	3
$\{e, x\}$	2		$\{e, m\}$	2		$\{e, r, r^2, r^3, r^4, r^5\}$	6
$\{e, p\}$	2		$\{e, n\}$	2		$\{e, x, p, q, y, m, n$	
$\{e, q\}$	2		$\{e, r^3\}$	2		$r, r^2, r^3, r^4, r^5\}$	12

[3 marks]

(iii)

Symmetry	Order	Cycle Notation	Transpositions	Parity
e	1	$(1)(2)(3)(4)(5)(6)$	none	even
r	6	$(1\ 2\ 3\ 4\ 5\ 6)$	$(1\ 6)(1\ 5)(1\ 4)(1\ 3)(1\ 2)$	odd
r^2	3	$(1\ 3\ 5)(2\ 4\ 6)$	$(1\ 5)(1\ 3)(2\ 6)(2\ 4)$	even
r^3	2	$(1\ 4)(2\ 5)(3\ 6)$	$(1\ 4)(2\ 5)(3\ 6)$	odd
r^4	3	$(1\ 5\ 3)(2\ 6\ 4)$	$(1\ 3)(1\ 5)(2\ 4)(2\ 6)$	even
r^5	6	$(1\ 6\ 5\ 4\ 3\ 2)$	$(1\ 2)(1\ 3)(1\ 4)(1\ 5)(1\ 6)$	odd
x	2	$(2\ 6)(3\ 5)$	$(2\ 6)(3\ 5)$	even
p	2	$(1\ 2)(3\ 6)(4\ 5)$	$(1\ 2)(3\ 6)(4\ 5)$	odd
q	2	$(1\ 3)(4\ 6)$	$(1\ 3)(4\ 6)$	even
y	2	$(1\ 4)(2\ 3)(5\ 6)$	$(1\ 4)(2\ 3)(5\ 6)$	odd
m	2	$(1\ 5)(2\ 4)$	$(1\ 5)(2\ 4)$	even
n	2	$(1\ 6)(2\ 5)(3\ 4)$	$(1\ 6)(2\ 5)(3\ 4)$	odd

[7 marks]

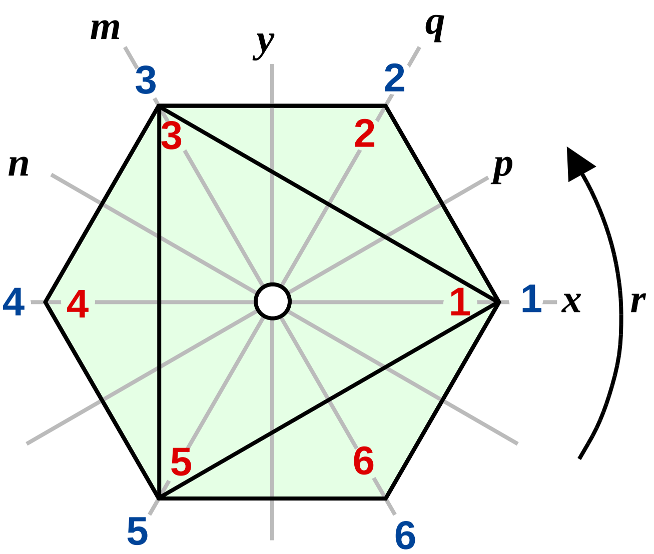
(iv) The elements with even parity are, $H = \{e,\ r^2,\ r^4,\ x,\ q,\ m\}$

$\circ$	e	r^2	r^4	x	q	m
e	e	r^2	r^4	x	q	m
r^2	r^2	r^4	e	q	m	x
r^4	r^4	e	r^2	m	x	q
x	x	m	q	e	r^4	r^2
q	q	x	m	r^2	e	r^4
m	m	q	x	r^4	r^2	e

[3 marks]

(v) $$H \cong S_3$$

There is a clever explanation as to why H is isomorphic to the permutation group S_3 which is most famously associated with the symmetry group for an equilateral triangle.
It's as if such a triangle has been drawn on the hexagon, like so;



[1 mark]

(vi) Prove that for any group G, the elements with even parity form a subgroup.
You may use the fact that,

- even and odd permutations combine according to the parity table;

$\circ$	even	odd
even	even	odd
odd	odd	even

Proof:
The three subgroup axioms need to be checked.

Closure: The subgroup is defined to be constructed from all elements of G which are even. Given any two elements of G that are even, the parity table shows that, when composed, the result is another even element. That is, $even \circ even = even$. $\therefore$ H is closed.

Identity: The identity of G is even, so this will be in H.

Inverses: Given any element $f \in H$, consider the parity of

$$f \circ f^{-1} = e$$

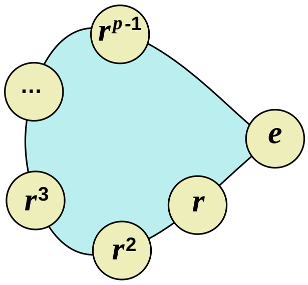
The parity table that the inverse is even and so in H

As H satisfies all three subgroup axioms, H is a subgroup of G $\square$

[6 marks]

Answer 3

(i)



[2 marks]

(ii) The cycle graph for a cyclic group consists of a single loop.
There can be no sub-cycles within this loop because a prime number only divides by itself and the number one.

The only subgroups are therefore $\{e\}$ and $\{e, r, r^2, r^3, \ldots, r^{p-1}\}$

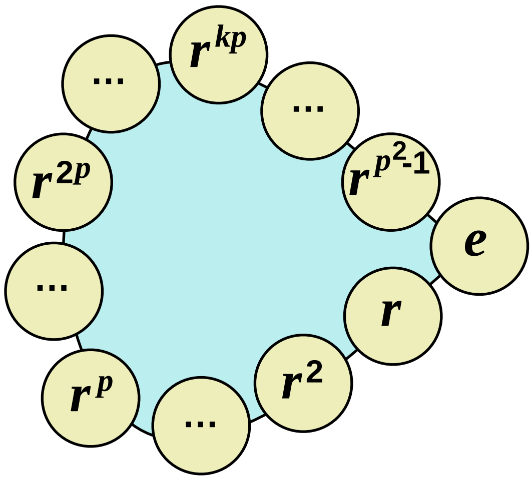
Neither of these is a proper sub-group.

$\therefore$ A cyclic group has no proper subgroups. □

[2 marks]

Answer 4

In the cycle diagram k is a positive integer with $k = p - 1$



(i) From the above cycle diagram, there will be one proper subgroup.

[2 marks]

(ii) $\langle r^p \rangle = \{e, r^p, r^{2p}, r^{3p}, \ldots, r^{kp}\}$ where $k = p - 1$

[2 marks]

Answer 5
Statement: A cyclic group of even order has exactly one element of order 2

Proof : If G is a finite cyclic group of order n, then G has a unique subgroup of order m for each m dividing n.
Now. if n is even, then G has a unique subgroup of order 2, hence one element of order 2 (as if G had two distinct elements of order 2, then there would be two distinct subgroups of order 2)

This question could be generalised to say that,
"A cyclic group of order n has exactly one subgroup of order m for each value of m that divides n"

[3 marks]

Answer 6
Statement:
Let G be a group, with identity element e, containing finite subgroups H and K.
If $|H|$ and $|K|$ are coprime, then $H \cap K = \{e\}$

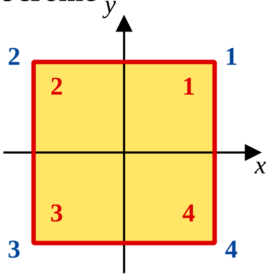
Proof:
By Lagrange's theorem $|H \cap K|$ must divide $|H|$ and must also divide $|K|$
Since the orders of H and K are relatively prime, necessarily $|H \cap K| = 1$
Therefore, $H \cap K = \{e\}$ ☐

[3 marks]

4.1 The Shuffled Square

Two mathematicians, Jerome and Emily, are labelling the vertices of a square ahead of setting up the cycle notation for the three symmetries; rotation of 90°, reflection in the line $y = x$ and reflection in the x-axis.
Here, side by side, are their proofs that the 90° rotation followed by a reflection in the line $y = x$ is equivalent to a reflection in the x-axis.
Notice that, right at the start, they label their squares differently.

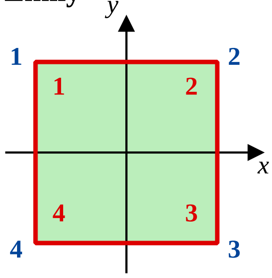
Jerome



From my diagram;

$$
\begin{aligned}
r &= (1\,2\,3\,4)\\
p &= (2\,4)\\
x &= (1\,4)(2\,3)\\
\text{LHS} &= p \circ r\\
&= (2\,4) \circ (1\,2\,3\,4\\
&= (1\,4)(2\,3)\\
&= x\\
&= \text{RHS} \qquad \square
\end{aligned}
$$

Emily



From my diagram;

$$
\begin{aligned}
R &= (1\,4\,3\,2)\\
P &= (1\,3)\\
X &= (1\,4)(2\,3)\\
\text{LHS} &= P \circ R\\
&= (1\,3) \circ (1\,4\,3\,2)\\
&= (1\,4)(2\,3)\\
&= X\\
&= \text{RHS} \qquad \square
\end{aligned}
$$

The group of symmetries associated with Jerome's square is clearly isomorphic to the group of symmetries of Emily's square. The isomorphism is simply,

Jerome's Label	ϕ $\rightarrow$	Emily's Label
1	$\rightarrow$	2
2	$\rightarrow$	1
3	$\rightarrow$	4
4	$\rightarrow$	3

Notice that, $\phi = (1\,2)(3\,4)$ but the operation "relabel the vertices" is NOT the same as the square's binary operation of symmetry compositions.
So, for example, writing $\phi \circ r = R$ is not true and, in fact, makes no sense at all.

However, one could write: $r = (1\,2\,3\,4) \xrightarrow{\phi} (2\,1\,4\,3) = (1\,4\,3\,2) = R$

Here is a table of all of Jerome's and all of Emily's symmetries;

For Jerome's Square			For Emily's Square	
e	$(1)(2)(3)(4)$		E	$(1)(2)(3)(4)$
r	$(1\,2\,3\,4)$		R	$(1\,4\,3\,2)$
r^2	$(1\,3)(2\,4)$		R^2	$(1\,3)(2\,4)$
r^3	$(1\,4\,3\,2)$		R^3	$(1\,2\,3\,4)$
x	$(1\,4)(2\,3)$		X	$(1\,4)(2\,3)$
y	$(1\,2)(3\,4)$		Y	$(1\,2)(3\,4)$
p	$(2\,4)$		P	$(1\,3)$
n	$(1\,3)$		N	$(2\,4)$

The eight symmetries of a square are a subgroup of S_4. The order of S_4 is 24 and yet, in spite of this, Jerome and Emily have exactly the same collection of eight permutations for their symmetries. Why has this happened ?

It's because the relabelling function, ϕ, in this case, happened to be the same permutation as one of the elements of the group; In fact, Jerome's square when reflected in the y-axis gives Emily's square.
The group property of closure then guarantees the same eight expressions when written in cycle notation will be in both Jerome's and Emily's symmetry list, but shuffled around.

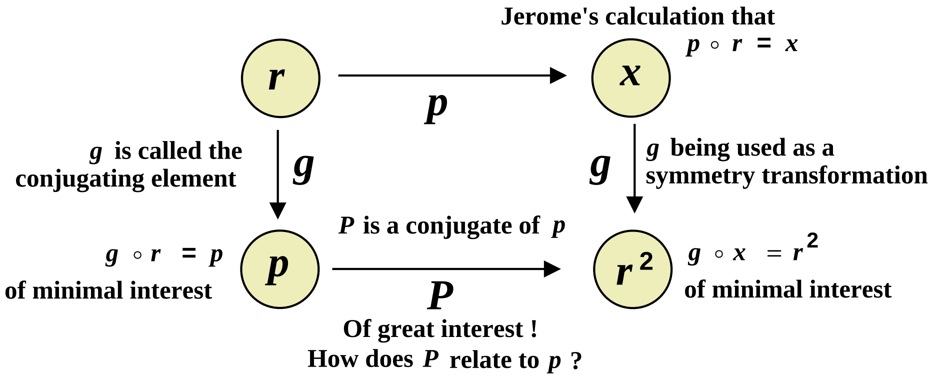
In consequence, the isomorphism between these two groups is, effectively, an isomorphism from the group back onto itself.

Definition : Automorphism
An automorphism of a group G is an isomorphism from G to G

- Not all possible relabellings of the square result in an automorphism.
  (This fact will be demonstrated in this lecture's exercises)

When a relabelled automorphism, ϕ, is used as if it were a symmetry composition it is called a conjugating element and, as it's an element from G, is often denoted g.

A diagram can now be drawn to show the effect g is having when treated, not as a renaming tool, but as a symmetry of the square. That is, a reflection in the, y-axis.



By traversing the diagram from r to r^2 by going both anticlockwise and clockwise and equating the result a relationship between P and p can be established,

$$P \circ g \circ r = r^2 \qquad \text{by working anticlockwise from } r \text{ to } r^2$$

$$g \circ p \circ r = r^2 \qquad \text{by working clockwise from } r \text{ to } r^2$$

$$\therefore \; P \circ g \circ r = g \circ p \circ r$$

$$P \circ g = g \circ p$$

$$P = g \circ p \circ g^{-1}$$

For Jerome's square, $P = (1\,2)(3\,4) \circ (2\,4) \circ (1\,2)(3\,4)$

$= (1\,3)$ note $g = g^{-1}$ in this case

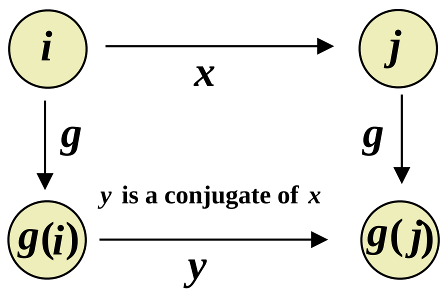
$= n \quad \therefore n$ is a conjugate of p

4.2 Generalising

Conjugate Elements

Let x and y be elements of a group G; then y is a conjugate of x in G if there exists an element $g \in G$ such that,

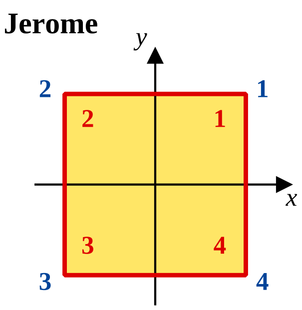
$$y = g\,x\,g^{-1}$$



Note: $i,\ j,\ g(i),\ g(j)$ are element of G but exactly which elements they are is unimportant when finding conjugates.

4.3 Example

With $g = (1\,2)(3\,4)$ as conjugating element determine the element that is the conjugate of $r = (1\,2\,3\,4)$ in Jerome's group of symmetries of a square.



Teaching Video: http://www.NumberWonder.co.uk/v9110/4.mp4

[2 marks]

4.4 Conjugacy Classes

Using $g = (1\,2)(3\,4)$ as the congugating element with each of the remaining elements of Jerome's group of symmetries of a square leads to the following;

Element	e	r	r^3	x	y	r^2	p	n
Conjugate	e	r^3	r	y	x	r^2	n	p

The congugating element, g, has partitioned the elements into the five conjugacy classes $\{e\}$, $\{r,\ r^3\}$, $\{x, y\}$, $\{r^2\}$, $\{p, n\}$

4.5 Cycle Structure Preserved

Conjugacy preserves cycle structure, which is intuitively obvious if it is recalled that an interpretation of what the conjugating element does in any permutation group is “rename”.

To be clear, conjugate elements must have the same cycle structure.
In the table above, for example both x and y have the cycle structure (- -)(- -)

As cycle structure determines order, a consequence of cycle structure being preserved is that conjugate elements must also have the same order.

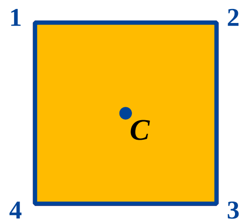
4.6 Exercise

Marks Available: 40

Question 1

University Mock Examination Question from 1995, M203, Q9 (OU)

Consider G, the symmetry group of the square below, with centre C.



Let $h \in G$ be the anticlockwise rotation through $\frac{\pi}{2}$ about the centre C, and let $g \in G$ be the reflection in the vertical axis through C.

(a) Write down h and g in cycle form, using numbering of the locations of the vertices as shown.

[2 marks]

(b) Write down the conjugate $g\,h\,g^{-1}$ of h, and state its order.

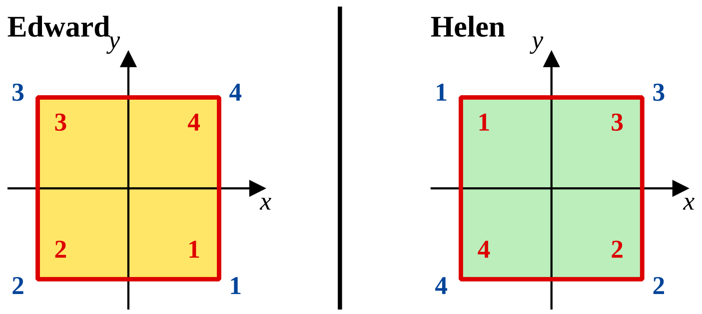
[2 marks]

(c) State whether or not g and h are conjugate, giving a brief reason for your answer.

[2 marks]

Question 2

Two mathematicians, Edward and Helen, are labelling the vertices of a square ahead of working out the symmetries of their squares in cycle notation. Notice that, right at the start, they labelled their squares differently.



(i) Complete the following table where,

- e, E : identity elements
- r, R : rotation of 90° about the square's centre
- x, X : reflection in the x-axis
- y, Y : reflection in the y-axis
- p, P : reflection in the line $y = x$
- n, N : reflection in the line $y = -x$

For Edward's Square			For Helen's Square	
e	(1)(2)(3)(4)		E	(1)(2)(3)(4)
r			R	
r^2			R^2	
r^3			R^3	
x			X	
y			Y	
p			P	
n			N	

[7 marks]

(ii) Explain why the relationship between Edward's and Helen's groups of symmetries of the square could be considered to be an isomorphism but not an automorphism.

[2 marks]

Question 3

University Assessment Question from 1996, M203, Q5(1) (OU)

(a) Find all elements in S_6 that conjugate $(1\ 5\ 3\ 6\ 4\ 2)$ to itself.

[5 marks]

(b) For each element found in part (a), give its order and parity.

[5 marks]

(c) Prove directly (verify that the subgroup axioms hold) that the set of elements that you found in part (a) is a subgroup of S_6 and identify this subgroup up to isomorphism. (In other words, identify a group of symmetries of some figure to which your subgroup is isomorphic)

[6 marks]

(d) Find all the elements in S_6 that conjugate $(1\ 5\ 3\ 6\ 4\ 2)$ to $(1\ 2\ 3\ 4\ 5\ 6)$

[5 marks]

(e) Chose one element, p, that conjugates $(1\ 5\ 3\ 6\ 4\ 2)$ to $(1\ 2\ 3\ 4\ 5\ 6)$ and show that the elements $p \circ x$, where x conjugates $(1\ 5\ 3\ 6\ 4\ 2)$ to itself (from part (a)), are precisely the elements found in part (d).

[4 marks]

4.7 Answers

4.7.1 Solutions to 4.3 Example (Teaching Video)

Let w be the conjugate of h in which case,

$$\begin{aligned} w &= g\,h\,g^{-1} \\ &= (1\ 2)(3\ 4) \circ (1\ 2\ 3\ 4) \circ (1\ 2)(3\ 4) \\ &= (1\ 4\ 3\ 2) \ \text{ which is } r^3 \end{aligned}$$

So r and r^3 are in the same conjugacy class

[2 marks]

4.7.2 Solutions to 4.6 Exercise

Answer 1

(a) $h = (1\ 4\ 3\ 2) \qquad g = (1\ 2)(3\ 4)$

[2 marks]

(b) Let w be the conjugate of h in which case,

$$\begin{aligned} w &= g\,h\,g^{-1} \\ &= (1\ 2)(3\ 4) \circ (1\ 4\ 3\ 2) \circ (1\ 2)(3\ 4) \qquad \text{as } g = g^{-1} \\ &= (1\ 2\ 3\ 4) \ \text{ which has order 3} \end{aligned}$$

[2 marks]

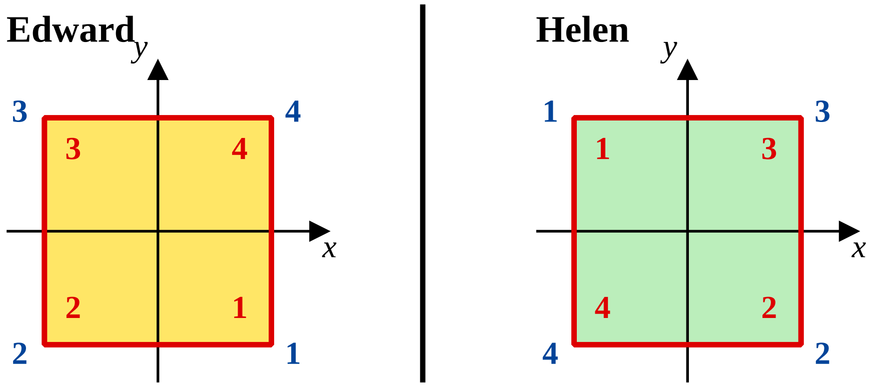
(c) The elements g and h are not conjugate.
Here are three reasons why;

- They are of different geometrical type.
  Conjugation preserves the property of reflection and the property of rotation.
  g is a reflection, h is a rotation.
- They are of different cycle type.
  Conjugation preserves cycle structure.
  g has the cycle structure (- -)(- -), h has the structure (- - - -)
- The order of each is different.
  Conjugation preserves the order of the elements.
  g is of order 2, h is of order 3

[2 marks]

Answer 2

(i)



The "renaming isomorphism" is $\phi = (1\,2\,4\,3)$ for Edward $\rightarrow$ Helen

For Edward's Square			For Helen's Square	
e	$(1)(2)(3)(4)$		E	$(1)(2)(3)(4)$
r	$(1\,4\,3\,2)$		R	$(1\,4\,2\,3)$
r^2	$(1\,3)(2\,4)$		R^2	$(1\,2)(3\,4)$
r^3	$(1\,2\,3\,4)$		R^3	$(1\,3\,2\,4)$
x	$(1\,4)(2\,3)$		X	$(1\,4)(2\,3)$
y	$(1\,2)(3\,4)$		Y	$(1\,3)(2\,4)$
p	$(1\,3)$		P	$(1\,2)$
n	$(2\,4)$		N	$(3\,4)$

[7 marks]

(ii) The renaming isomorphism does not match with any element in Edwards square. It will give rise to elements in Helen's square that are not in Edward's.
There is, in fact, no physical reflection or rotation that will provide a way to transform Edward's square onto Helen's.
An automorphism is a isomorphism from a group back onto itself but Helen's group has elements of S_4 in it that are not in Edwards.
So these two groups cannot be treated as if they were one and so no automorphism is possible.

[2 marks]

Answer 3

(a) The cycle $(1\,5\,3\,6\,4\,2)$ can be expressed in six variations that all describe the same cycle;

$$(1\,5\,3\,6\,4\,2) = (5\,3\,6\,4\,2\,1) = (3\,6\,4\,2\,1\,5)$$
$$= (6\,4\,2\,1\,5\,3) = (4\,2\,1\,5\,3\,6) = (2\,1\,5\,3\,6\,4)$$

Thinking of the conjugating elements, g_k for $1 \leqslant k \leqslant 6$ as "renaming" functions means that the elements required are;

$$g_1 = \begin{pmatrix} 1 & 5 & 3 & 6 & 4 & 2 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 5 & 3 & 6 & 4 & 2 \end{pmatrix} = e \qquad g_2 = \begin{pmatrix} 1 & 5 & 3 & 6 & 4 & 2 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 5 & 3 & 6 & 4 & 2 & 1 \end{pmatrix} = (1\,5\,3\,6\,4\,2)$$

$$g_3 = \begin{pmatrix} 1 & 5 & 3 & 6 & 4 & 2 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 6 & 4 & 2 & 1 & 5 \end{pmatrix} = (1\,3\,4)(2\,5\,6) \qquad g_4 = \begin{pmatrix} 1 & 5 & 3 & 6 & 4 & 2 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 6 & 4 & 2 & 1 & 5 & 3 \end{pmatrix} = (1\,6)(2\,3)(4\,5)$$

$$g_5 = \begin{pmatrix} 1 & 5 & 3 & 6 & 4 & 2 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 2 & 1 & 5 & 3 & 6 \end{pmatrix} = (1\,4\,3)(2\,6\,5) \qquad g_6 = \begin{pmatrix} 1 & 5 & 3 & 6 & 4 & 2 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 1 & 5 & 3 & 6 & 4 \end{pmatrix} = (1\,2\,4\,6\,3\,5)$$

[5 marks]

(b)

Element	Order	Parity
e	1	even
$(1\,5\,3\,6\,4\,2)$	6	odd
$(1\,3\,4)(2\,5\,6)$	3	even
$(1\,6)(2\,3)(4\,5)$	2	odd
$(1\,4\,3)(2\,6\,5)$	3	even
$(1\,2\,4\,6\,3\,5)$	6	odd

[5 marks]

(c)

$\circ$	e	(153642)	$(134)(256)$	$(16)(23)(45)$	$(143)(265)$	(124635)
e	e	(153642)	$(134)(256)$	$(16)(23)(45)$	$(143)(265)$	(124635)
(153642)	(153642)	$(134)(256)$	$(16)(23)(45)$	$(143)(265)$	(124635)	e
$(134)(256)$	$(134)(256)$	$(16)(23)(45)$	$(143)(265)$	(124635)	e	(153642)
$(16)(23)(45)$	$(16)(23)(45)$	$(143)(265)$	(124635)	e	(153642)	$(134)(256)$
$(143)(265)$	$(143)(265)$	(124635)	e	(153642)	$(134)(256)$	$(16)(23)(45)$
(124635)	(124635)	e	(153642)	$(134)(256)$	$(16)(23)(45)$	$(143)(265)$

Verifying the subgroup axioms;

Closure: No new elements were needed to complete the Cayley table.

If $H = \{e, (1\,5\,3\,6\,4\,2), (1\,3\,4)(2\,5\,6),$
$(1\,6)(2\,3)(4\,5), (1\,4\,3)(2\,6\,5), (1\,2\,4\,6\,3\,5)\}$

then, for all $h_1, h_2 \in H$, the composite $h_1h_2 \in H$

Identity: The identity element of S_6 belongs to H. That is, $e \in H$

Inverses: $(1\,5\,3\,6\,4\,2)$ has inverse $(2\,4\,6\,3\,5\,1)$, i.e. $(1\,2\,4\,6\,3\,5)$

$(1\,3\,4)(2\,5\,6)$ has inverse $(4\,3\,1)(6\,5\,2)$ i.e. $(1\,4\,3)(2\,6\,5)$

$(1\,6)(2\,3)(4\,5)$ has inverse $(6\,1)(3\,2)(5\,4)$ i.e. $(1\,6)(2\,3)(4\,5)$

$(1\,4\,3)(2\,6\,5)$ has inverse $(3\,4\,1)(5\,6\,2)$ i.e. $(1\,3\,4)(2\,5\,6)$

$(1\,2\,4\,6\,3\,5)$ has inverse $(5\,3\,6\,4\,2\,1)$ i.e. $(1\,5\,3\,6\,4\,2)$

e has inverse e

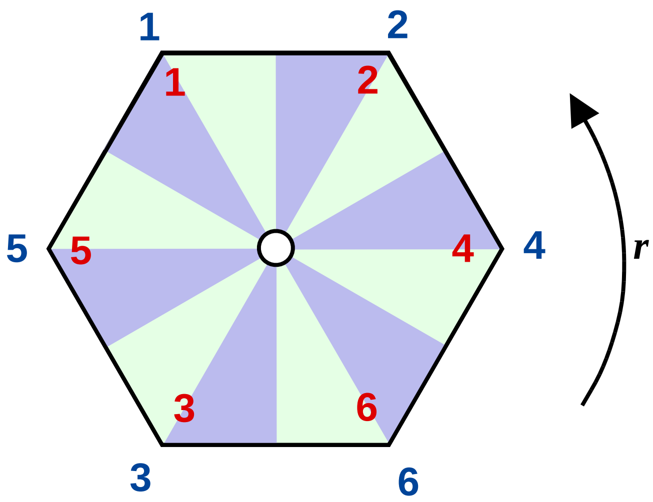
In other words, for each $h \in H$, the inverse $h^{-1} \in H$

$\therefore$ The set of elements do indeed form a subgroup of S_6

The subgroup of S_6 is isomorphic to the cyclic group $\mathbb{Z}_6$ of order 6

A geometric example of $\mathbb{Z}_6$ is the rotational symmetries of a regular hexagon.

If r is a rotation of 60° about the hexagon's centre, then;



$*$	e	r	r^2	r^3	r^4	r^5
e	e	r	r^2	r^3	r^4	r^5
r	r	r^2	r^3	r^4	r^5	e
r^2	r^2	r^3	r^4	r^5	e	r
r^3	r^3	r^4	r^5	e	r	r^2
r^4	r^4	r^5	e	r	r^2	r^3
r^5	r^5	e	r	r^2	r^3	r^4

$$\phi : H \to \mathbb{Z}_6 \quad \text{where } r^6 = e$$

$$\begin{aligned} e &\to e \\ (1\,5\,3\,6\,4\,2) &\to r \\ (1\,3\,4)(2\,5\,6) &\to r^2 \\ (1\,6)(2\,3)(4\,5) &\to r^3 \\ (1\,4\,3)(2\,6\,5) &\to r^4 \\ (1\,2\,4\,6\,3\,5) &\to r^5 \end{aligned}$$

[6 marks]

(d) The cycle $\begin{pmatrix}1\ 2\ 3\ 4\ 5\ 6\end{pmatrix}$ can be expressed in six variations that all describe the same cycle;

$$\begin{aligned} &\begin{pmatrix}1\ 2\ 3\ 4\ 5\ 6\end{pmatrix} = \begin{pmatrix}2\ 3\ 4\ 5\ 6\ 1\end{pmatrix} = \begin{pmatrix}3\ 4\ 5\ 6\ 1\ 2\end{pmatrix} \\ = &\begin{pmatrix}4\ 5\ 6\ 1\ 2\ 3\end{pmatrix} = \begin{pmatrix}5\ 6\ 1\ 2\ 3\ 4\end{pmatrix} = \begin{pmatrix}6\ 1\ 2\ 3\ 4\ 5\end{pmatrix}\end{aligned}$$

Thinking of the conjugating elements, g_k for $7 \leqslant k \leqslant 12$ as "renaming" functions means that the elements required are;

$$g_7 = \begin{pmatrix} 1 & 5 & 3 & 6 & 4 & 2 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} \qquad g_8 = \begin{pmatrix} 1 & 5 & 3 & 6 & 4 & 2 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix}$$

$$= \begin{pmatrix}2\ 6\ 4\ 5\end{pmatrix} \qquad\qquad = \begin{pmatrix}1\ 2\end{pmatrix}\begin{pmatrix}3\ 4\ 6\ 5\end{pmatrix}$$

$$g_9 = \begin{pmatrix} 1 & 5 & 3 & 6 & 4 & 2 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix} \qquad g_{10} = \begin{pmatrix} 1 & 5 & 3 & 6 & 4 & 2 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix}$$

$$= \begin{pmatrix}1\ 3\ 5\ 4\end{pmatrix} \qquad\qquad = \begin{pmatrix}1\ 4\ 2\ 3\ 6\end{pmatrix}$$

$$g_{11} = \begin{pmatrix} 1 & 5 & 3 & 6 & 4 & 2 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 5 & 6 & 1 & 2 & 3 & 4 \end{pmatrix} \qquad g_{12} = \begin{pmatrix} 1 & 5 & 3 & 6 & 4 & 2 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 6 & 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

$$= \begin{pmatrix}1\ 5\ 6\ 2\ 4\ 3\end{pmatrix} \qquad\qquad = \begin{pmatrix}1\ 6\ 3\ 2\ 5\end{pmatrix}$$

[5 marks]

(e) I'll choose $g_{11} = \begin{pmatrix}1\ 5\ 6\ 2\ 4\ 3\end{pmatrix}$ for my p and now take each x in turn;

- $p \circ g_1 = p \circ e = p = \begin{pmatrix}1\ 5\ 6\ 2\ 4\ 3\end{pmatrix} = g_{11}$
- $p \circ g_2 = \begin{pmatrix}1\ 5\ 6\ 2\ 4\ 3\end{pmatrix} \circ \begin{pmatrix}1\ 5\ 3\ 6\ 4\ 2\end{pmatrix} = \begin{pmatrix}1\ 6\ 3\ 2\ 5\end{pmatrix} = g_{12}$
- $p \circ g_3 = \begin{pmatrix}1\ 5\ 6\ 2\ 4\ 3\end{pmatrix} \circ \begin{pmatrix}1\ 3\ 4\end{pmatrix}\begin{pmatrix}2\ 5\ 6\end{pmatrix} = \begin{pmatrix}2\ 6\ 4\ 5\end{pmatrix} = g_7$
- $p \circ g_4 = \begin{pmatrix}1\ 5\ 6\ 2\ 4\ 3\end{pmatrix} \circ \begin{pmatrix}1\ 6\end{pmatrix}\begin{pmatrix}2\ 3\end{pmatrix}\begin{pmatrix}4\ 5\end{pmatrix} = \begin{pmatrix}1\ 2\end{pmatrix}\begin{pmatrix}3\ 4\ 6\ 5\end{pmatrix} = g_8$
- $p \circ g_5 = \begin{pmatrix}1\ 5\ 6\ 2\ 4\ 3\end{pmatrix} \circ \begin{pmatrix}1\ 4\ 3\end{pmatrix}\begin{pmatrix}2\ 6\ 5\end{pmatrix} = \begin{pmatrix}1\ 3\ 5\ 4\end{pmatrix} = g_9$
- $p \circ g_6 = \begin{pmatrix}1\ 5\ 6\ 2\ 4\ 3\end{pmatrix} \circ \begin{pmatrix}1\ 2\ 4\ 6\ 3\ 5\end{pmatrix} = \begin{pmatrix}1\ 4\ 2\ 3\ 6\end{pmatrix} = g_{10}$

Thus, the elements of $p \circ x$ are precisely the elements of part (d) $\square$

[4 marks]

4.7.3 Question 3 : Seeing the bigger picture

In part (a) the question looked at the six possible ways of labelling, for example, a hexagon without the anticlockwise order of the labels being altered.

In part (c) the question showed that the conjugating elements that performed the various possible relabelling actions did, in themselves, form a group, and that group was isomorphic to the group of symmetries of the hexagon. So, effectively, possible rotations of the labels were being looked art.

In part (d) the question looked at the six possible ways of relabelling the unconventionally labelled shape with the more conventional (1 2 3 4 5 6)

In part (e) the focus was on one particular relabelling.

It was shown, for example, $g_{11} \circ g_2 = g_{12}$