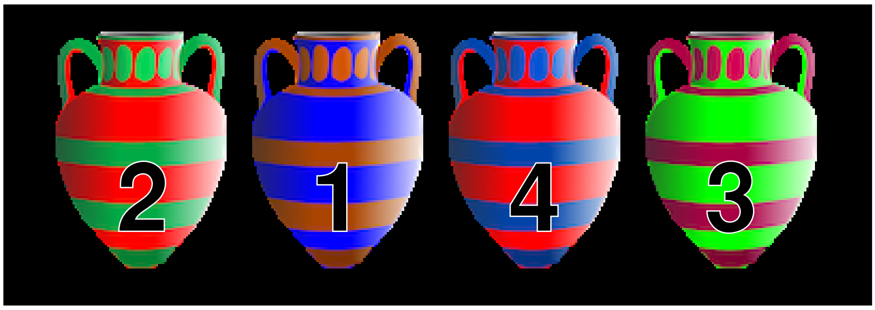
Lecture 3

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.

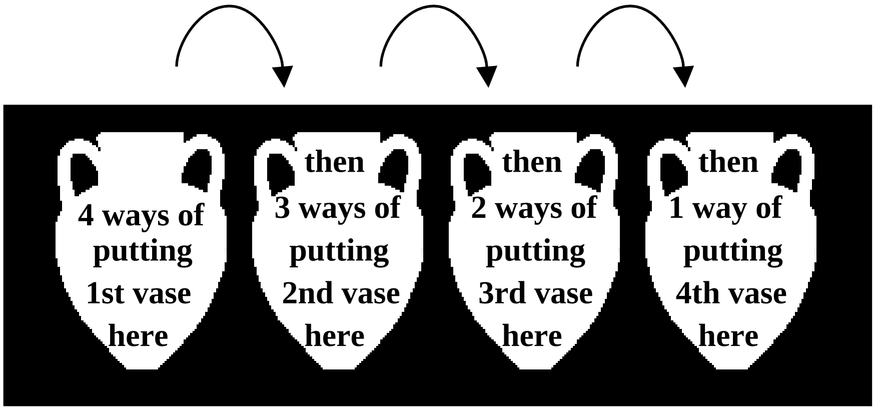
They can now be permutated, for example by swapping vases 1 and 2 and swapping vases 3 and 4.



In two line permutation notation the rearrangement is captured by,

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

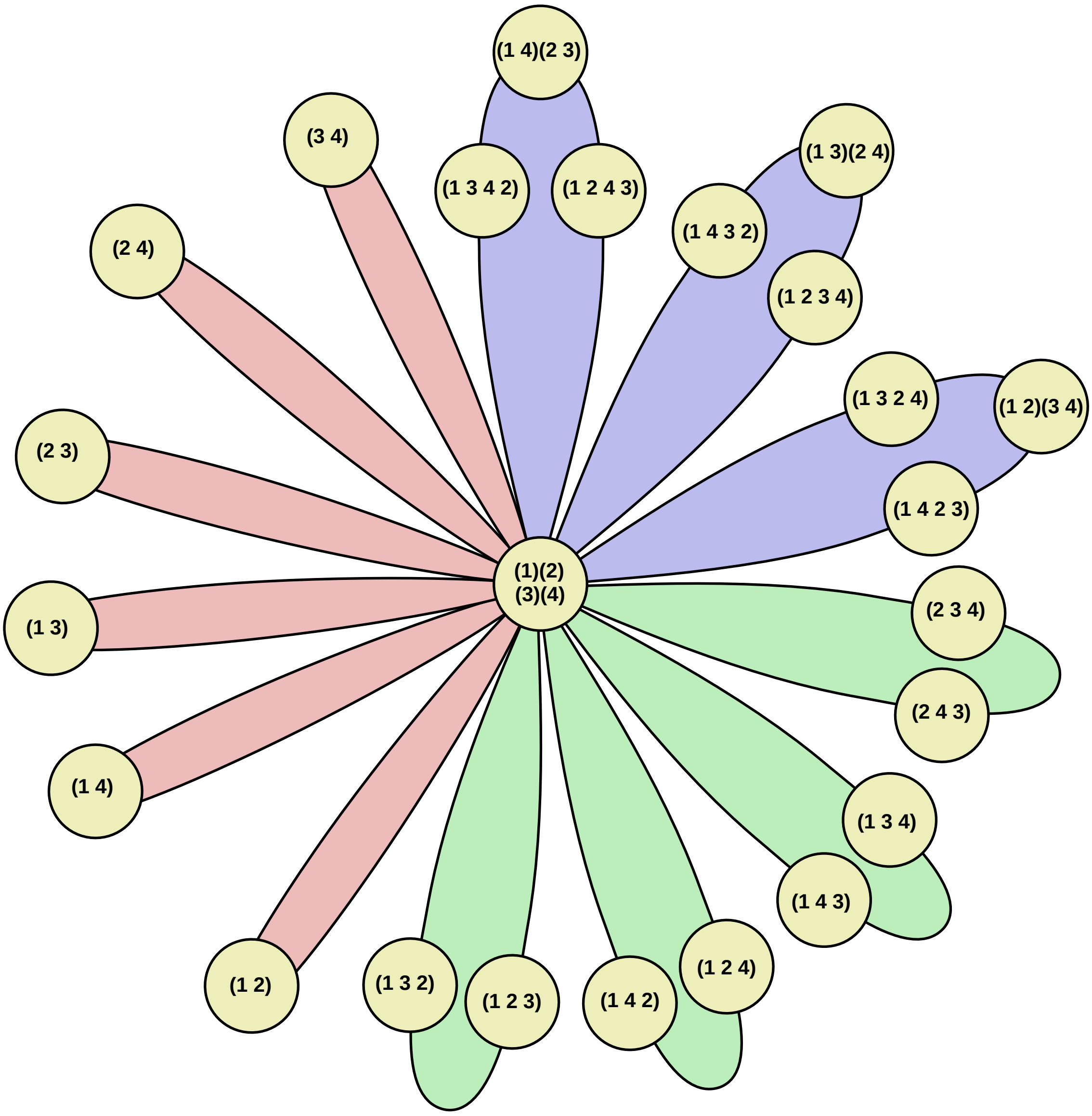
A key questions is,
“How many different possible arrangements of the four vases are there ?”


4 ways of putting 1st vase here
then 3 ways of putting 2nd vase here
then 2 ways of putting 3rd vase here
then 1 way of putting 4th vase here

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 $\{1, 2, 3, 4, \dots, n\}$ 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 $n \geqslant 3$

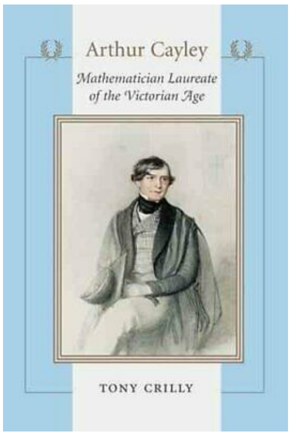
3.3 Cayley's Theorem

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 $g_1, g_2, g_3, \ldots, g_n$.

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

The permutation obtained from x is,

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

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, $P_x \circ P_y$

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

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

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 $g \rightarrow P_g$ 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

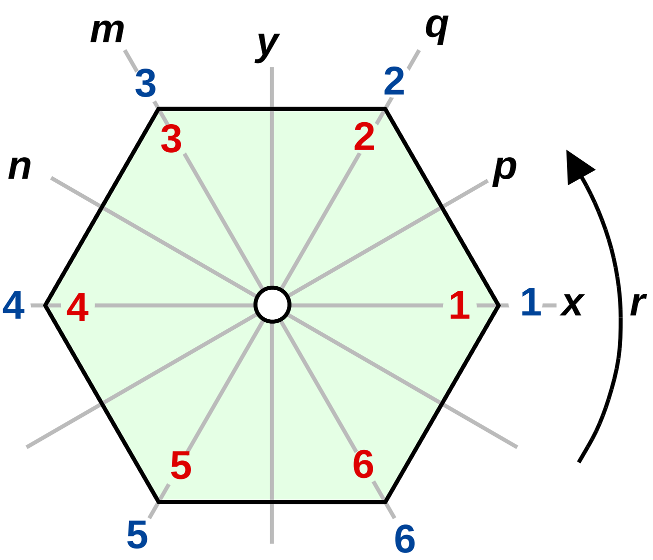
Construct a cycle graph from the following Cayley table which is for the group of symmetries of a regular pentagon that was studied in Lecture 2.

$*$	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		$\{e, x, p, q, y, m, n$ $r, r^2, r^3, r^4, r^5\}$	12
	2			2			

[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