4.1 Generators

As the groups being dealt with get larger, a certain type of subgroup can be found by exploring the use of the groups elements as generators.

Any element, a, from a group $(G, *)$ can be selected as a generator.

The subgroup $(H, *)$ generated by a, is then $\langle a \rangle = H = \{a, \ a^2, \ a^3, \ a^4, \ \dots \}$.

Once a term is found for which $a^k = e$, the generation halts.

Then $\langle a \rangle = H = \{a, \ a^2, \ a^3, \ a^4, \ \dots, \ e\}$

The type of subgroup found in this way is termed a cyclic subgroup.

4.2 Example

$*$	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

For the group D_4 find $\langle r^3 \rangle$, the subgroup generated by the element r^3

Teaching Video: http://www.NumberWonder.co.uk/v9108/4.mp4

[3 marks]

4.3 Order of Elements

The group of symmetries of the square, D_4, is of order 8.

This can be written as $|D_4| = 8$

The same word is also applied to the elements of a set being used as a group.

The Order of an Element

The order of an element a in a group $(G, *)$ with identity e is the smallest positive integer k such that $a^k = e$

For example, in the group D_4, the element r has order 4 because $r^4 = e$ which corresponds to four 90° rotations of a square take it back to its starting position.

This could be written as $|r| = 4$

4.4 Cyclic groups

Sometimes, but not always, an element in a group generates the entire group. Such a group is termed cyclic.

Cyclic Groups

$(G, *)$ is cyclic if and only if there exists an element a such that $|a| = |G|$

This element is termed a generator of the group.

Equivalently, a cyclic group is a group in which every element can be written in the form a^k, where a is the group generator and k is a positive integer.

Geometrically, in two dimensions, cyclic groups correspond to figures that have rotational symmetry and no mirror symmetry with the exception of a figure that only has a single mirror symmetry.

4.5 A Divisibility Restriction

Just as Lagrange's theorem restricted the possible orders of subgroup of any given group, the possible order of elements of any given group is restricted.

Possible Orders of Elements

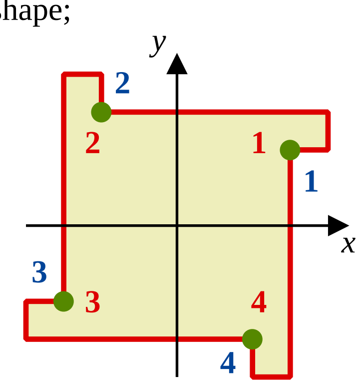
If $(G, *)$ has a finite number of elements, then, for every $a \in G$, the order of a divides the order of G. In other words, $|a|$ divides $|G|$

4.6 Exercise

Marks Available: 50

Question 1

Consider the following shape;



(i) Does the shape have any lines of mirror symmetry ?

[1 mark]

(ii) Does the shape have any rotational symmetry ?

[1 mark]

(iii) Will the symmetry group for this shape be cyclic under composition of symmetries ?

[1 mark]

(iv) In two line permutation notation, a symmetry of this shape is described as,

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

What symmetry of the shape does this correspond to ?

[1 mark]

(v) What is the order of the element a ?

[1 mark]

(vi) Produce a Cayley table of $\langle a \rangle$, the subgroup generated by a

[2 marks]

Question 2

The group shown is for addition modulo 12 on the set of least residues modulo 12;

$+_{12}$	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11	0
2	2	3	4	5	6	7	8	9	10	11	0	1
3	3	4	5	6	7	8	9	10	11	0	1	2
4	4	5	6	7	8	9	10	11	0	1	2	3
5	5	6	7	8	9	10	11	0	1	2	3	4
6	6	7	8	9	10	11	0	1	2	3	4	5
7	7	8	9	10	11	0	1	2	3	4	5	6
8	8	9	10	11	0	1	2	3	4	5	6	7
9	9	10	11	0	1	2	3	4	5	6	7	8
10	10	11	0	1	2	3	4	5	6	7	8	9
11	11	0	1	2	3	4	5	6	7	8	9	10

(i) Complete the table below;

Element	Subgroup Generated	Element's Order
0	$\langle 0 \rangle = \{0\}$	1
1		
2		
3		
4		
5		
6		
7		
8		
9		
10	$\langle 10 \rangle = \{0, 2, 4, 6, 8, 10\}$	6
11	$\langle 11 \rangle = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$	12

[6 marks]

(ii) Is the group cyclic ?
Justify your answer.

[2 marks]

Question 3

G has elements $\{e,\ a,\ a^2,\ a^3,\ b,\ ba,\ ba^2,\ ba^3\}$ under a binary operation $*$ with Cayley table given by;

$*$	e	a	a^2	a^3	b	ba	ba^2	ba^3
e	e	a	a^2	a^3	b	ba	ba^2	ba^3
a	a	a^2	a^3	e	ba^3	b	ba	ba^2
a^2	a^2	a^3	e	a	ba^2	ba^3	b	ba
a^3	a^3	e	a	a^2	ba	ba^2	ba^3	b
b	b	ba	ba^2	ba^3	a^2	a^3	e	a
ba	ba	ba^2	ba^3	b	a	a^2	a^3	e
ba^2	ba^2	ba^3	b	ba	e	a	a^2	a^3
ba^3	ba^3	b	ba	ba^2	a^3	e	a	a^2

(i) State the order of the group.

[1 mark]

(ii) State the order of a and the order of b.

[2 marks]

(iii) What is $b * ba$?

[1 mark]

(iv) State the inverse of ba^2

[1 mark]

(v) Find and list the elements of a subgroup of order 4

[1 mark]

(vi) State the orders of the subgroups that Lagrange's theorem states can not exist for this group.

[1 mark]

Question 4
Further A-Level Examination question from June 2017, FP3, Q4a (OCR)

The composition table for a group G of order 6 is given below.

	a	***b***	***c***	***d***	***e***	***f***
a	*c*	*f*	*e*	*b*	*a*	*d*
b	*f*	*a*	*d*	*e*	*b*	*c*
c	*e*	*d*	*a*	*f*	*c*	*b*
d	*b*	*e*	*f*	*c*	*d*	*a*
e	*a*	*b*	*c*	*d*	*e*	*f*
f	*d*	*c*	*b*	*a*	*f*	*e*

(i) State the identity element.

[1 mark]

(ii) State the order of each element.

[3 marks]

(iii) Write the inverse of each element.

[3 marks]

(iv) Determine whether G is cyclic.

[2 marks]

(v) List all the proper subgroups†
Comment on the order of these groups in relation to Lagrange's theorem.

[3 marks]

† The proper subgroups exclude the two trivial subgroups which are the subgroup of order 1 that contains only the identity element and the subgroup of order 6 that is a copy of the whole group.

Question 5
Open University Examination Question from October 1992, M101, Q16

Consider the group G with the following Cayley table,

$\times_{10}$	2	4	6	8
2	4	8	2	6
4	8	6	4	2
6	2	4	6	8
8	6	2	8	4

(i) What is the identity element of G ?
Give a brief reason for your answer.

[2 marks]

(ii) Write down the inverse of 8

[1 mark]

(iii) Find all the cyclic subgroups of G, giving a generator in each case.

[3 marks]

(iv) Is G a cyclic group ?
Give a brief reason for your answer.

[2 marks]

Question 6

The set $S = \{1, 3, 7, 9, 11, 13, 17, 19\}$ forms a group under multiplication modulo 20

(i) Explain why S cannot have a subgroup of order 3

[1 mark]

(ii) Find the order of each element of S

[3 marks]

(iii) Find three different subgroups of S, each of order 4

[4 marks]