Degree Topics in Mathematics

Subgroups and Lagrange's Theorem

You will need to look at the *Groups* and *Cayley tables* activities from this set of resources before studying this activity.

A **subgroup** is a 'group within a group'.

Recall the axioms for checking whether a set and a binary operation * form a group:

1. S is closed under *
2. * is associative
3. There is an identity element e which is a member of S
4. Every element of S has an inverse

When checking whether or not a subset of a group forms a subgroup, we check only three of the four axioms – we do not need to check axiom 2, as if the binary operation * is associative on the larger set, it will automatically be associative on the subset.

Hence, the axioms for checking a **subgroup** are:

1. S is closed under *

2. There is an identity element e which is a member of S

3. Every element of S has an inverse

For example, for the group ($\mathbb{R}$, +) the set of integers $\mathbb{Z}$ forms a subgroup. Checking each axiom:

1. Adding two integers produces an integer so $\mathbb{Z}$ is closed under addition.
2. The element 0 is the identity element under addition.
3. For any integer z, there is an integer (-z) which is its inverse.

Task 1

Produce a Cayley table for the group G = $(\mathbb{Z}_6, +)$ i.e. addition modulo 6.

Determine which of the following subsets are subgroups of G:

(i) {0, 3} (ii) {0, 1, 2} (iii) {0, 2, 4} (iv) {0} (v) {0, 1, 2, 3, 4, 5}

(vi) {0, 1, 2, 3, 4}

You may noticed in Task 1 that the size of the subgroups of $(\mathbb{Z}_6, +)$ are 1, 2, 3 and 6. This is not a coincidence, and has in fact been proven to be true for all finite groups.

Joseph-Louis **Lagrange** (1736 – 1813) was an Italian born mathematician who worked in areas such as calculus, number theory and astronomy.

He was also very influential in the establishment of new standard units of measurement in the 1790s, including the metre and kilogram.

Lagrange's Theorem states that the order (size) of a subgroup of a finite group G is a factor of the order of G.

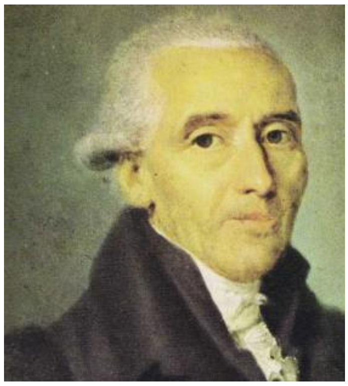


Image taken from http://www.mlahanas.de/Physics/Bios/images/JosephLouisLagrange.jpg

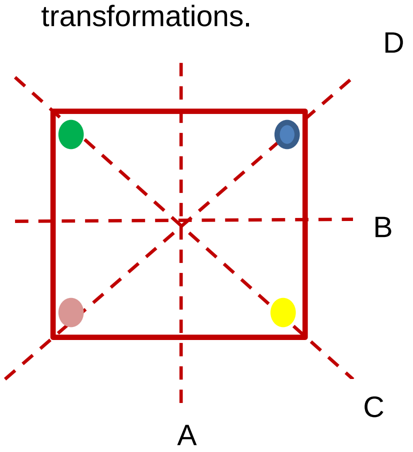
It is also worth noting that every group G has at least two subgroups:

- The whole group G is itself is classified as a subgroup
- The subgroup {e} which only contains the identity element. This is called the **trivial subgroup**.

Task 2

Produce a Cayley table for the symmetry group G of this square under the given transformations.

The coloured dots are provided to help identify the position of each corner under the transformations.



e = leave shape unchanged

a = reflection in line A

b = reflection in line B

c = reflection in line C

d = reflection in line D

f = clockwise rotation of 90°

g = anticlockwise rotation of 90°

h = rotation of 180°

Using Lagrange's Theorem as a guide, try to find all the possible subgroups of G.

(**HINT**: There are ten subgroups of G. Remember that every subgroup must contain e and that some elements are self-inverse which can help spot subgroups).

Solutions

Task 1

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Here we can see that the identity element is 0 so any subgroup must contain this element.

(i) {0, 3} – this subset contains the identity element and the element 3 is self-inverse. The set is closed. Therefore this is a subgroup.

(ii) {0, 1, 2} – this is not closed as, for example, 2 + 2 = 4 and 4 is not in this subset. Therefore this cannot be a subgroup.

(iii) {0, 2, 4} – this subset contains the identity element. Considering all the pairings e.g. 2 + 4 = 0, we can see the subset is closed. 2 has an inverse or 4 and 4 has an inverse of 2, so each element has an inverse. Hence this is a subgroup.

(iv) {0} - this is the trivial subgroup.

(v) {0, 1, 2, 3, 4, 5} – the whole group is considered to be a subgroup.

(vi) {0, 1, 2, 3, 4} – this is not closed as, for example, 1 + 4 = 5 and 5 is not in this subset. Therefore this cannot be a subgroup.

Task 2

	e	a	b	c	d	f	g	h
e	e	a	b	c	d	f	g	h
a	a	e	h	g	f	d	c	b
b	b	h	e	f	g	c	d	a
c	c	g	f	e	h	a	b	d
d	d	f	g	h	e	b	a	c
f	f	d	c	a	b	h	e	g
g	g	c	d	b	a	e	h	f
h	h	b	a	d	c	g	f	e

Lagrange's Theorem tells us that the subgroups will have order 1, 2, 4 or 8. We also know that a, b, c, d and h are self-inverse.

The subgroups are: {e}, {e, a}, {e, b}, {e, c}, {e, d}, {e, h}, {e, f, g, h}, {e, a, b, h}, {e, c, d, h} and {e, a, b, c, d, f, g, h}.