Lecture 2

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

2.1 Properties of Groups

All possible additions modulo 5 can be summarised by the table;

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

This is a well known group called the cyclic group, C_5
It is alive with patterns such as,

- In any given row each of the five possible least residues occur once and once only
- In any given column each of the five possible least residues occur once and once only

Taken together this pattern is referred to as the Latin square property of a group.
All groups have this Latin square property.

Another of the key ideas behind what makes this a group are the facts that,

◊ There is a defined set, $G = \{ 0, 1, 2, 3, 4 \}$
◊ There is a binary operation defined upon G, addition modulo 5

A Binary Operation

A binary operation on a set is a calculation that combines two elements of the set to produce another element of the set.

To be a group there must be an element that "does nothing", in this case the number zero. When zero is added on to any of the other elements it leaves them unchanged. This special element is called the identity element, *e*.

Furthermore, to be a group, each element must have an inverse.
The inverse of 2, for example, is 3 because when 2 and 3 are combined in either order, the result is the identity element.

$$2 + 3 \equiv 0 \pmod 5 \qquad \text{and} \qquad 3 + 2 \equiv 0 \pmod 5$$

There are two other conditions that must be satisfied.
One is termed “Closure” which means that under the binary operation of the group it's not possible to obtain an answer that is outside of the group.
The final condition is that “Associativity” holds.
Briefly, this requires that for any three elements in the group, *a*, *b*, and *c*, where the brackets are placed must make no difference.

That is, $a + (b + c) \equiv (a + b) + c \pmod{5}$

2.2 Dismissed, then Reformed

All possible multiplications modulo 5 can be summarised by the table;

$\times_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

This is not a group because, for example, the Latin square property does not hold.
However, if zero is removed from the set of least residues modulo 5, it is !

2.3 Example

Prove that $G = \{ 1,\ 2,\ 3,\ 4 \}$ under multiplication modulo 5 is a group.

Teaching Video: http://www.NumberWonder.co.uk/v9108/2.mp4

[6 marks]

2.4 Exercise

Marks Available : 40

Question 1

The set G = { 1, 5, 7, 11, 13, 17 } forms a group under multiplication modulo 18. Natasha has constructed most of its Cayley table;

$\times_{18}$	1	5	7	11	13	17
1	1	5		11	13	17
5	5	7	17	1		13
7		17		5	1	11
11	11	1	5	13		7
13	13		1		7	5
17	17	13	11	7	5	1

(i) Complete the Cayley table for Natasha.

[2 marks]

(ii) What is this group's identity element ?

[1 mark]

(iii) What is the inverse of the number 5 ?

[1 mark]

(iv) What is the inverse of the number 17 ?

[1 mark]

Question 2

A binary operation on integers, $*$, is defined as $x * y = x^2 y$

Determine the value of,

(i) $5 * 6$ **(ii)** $6 * 5$

[2 marks]

Question 3

Walter is investigating if the set $G = \{ 1, 3, 7, 9 \}$ forms a group under multiplication modulo 12 and has started to try and construct a Cayley table;

$\times_{12}$	1	3	7	9
1	1	3	7	9
3	3	9		
7	7		1	3
9	9		3	

(i) Complete the table.

[2 marks]

(ii) Is the closure property satisfied ?

[1 mark]

(iii) Give at least one reason why a group has not been formed.

[1 mark]

Question 4

A binary operation on $\mathbb{Z}$ is defined by $a * b = ab + 1$

(a) Determine the value of,

(i) $4 * 7$ **(ii)** $(-3) * 5$

[2 marks]

(b) By considering the integers 2, 3 and 4 show that $*$ is not associative.

[2 marks]

Question 5

The set G = { 0, 1, 2, 4, 5, 6 } forms a group under the binary operation,

$$x \circ y = x + y + 2xy \pmod 7$$

Sebastian has started to constructed this group's Cayley table;

○	0	1	2	4	5	6
0		1				
1		4				
2						
4					0	2
5						
6					1	

(i) Complete the Cayley table for Sebastian.

[3 marks]

(ii) What is this group's identity element ?

[1 mark]

(iii) What is the inverse of the number 5 ?

[1 mark]

(iv) What is the inverse of the number 1 ?

[1 mark]

(v) Which element, other than the identity element, is self-inverse ?

[1 mark]

Question 6

Let G be the set of (positive) odd numbers.

Let $\circ$ be the binary operation acting on G, $x \circ y = x^2y$

Prove that G is closed under $\circ$

[2 marks]

Question 7

Let $G = \{ 1, 2, 3, 4, 5 \}$

Under an unknown binary operation, $\otimes$, the following table is obtained.

$\otimes$	1	2	3	4	5
1	1	2	3	4	5
2	2	1	5	3	4
3	3	4	2	5	1
4	4	5	1	2	3
5	5	3	4	1	2

Tom claims, "As the table has the Latin square property it is a group".
Paul, however, is doubtful and sets about proving Tom's claim is false.

(a) Show that the following two calculations yield different answers;

(i) $2 \otimes (5 \otimes 3)$ **(ii)** $(2 \otimes 5) \otimes 3$

[2 marks]

(b) What property does part (a) show the table not to have ?

[1 mark]

Whilst all Cayley tables for a group have the Latin square property, this question shows that not all tables with the Latin square property are groups.
Latin squares that are not groups are termed quasigroups.
The study of quasigroups is well beyond A-Level mathematics.

Question 8

The operation $\circ$ is defined by $x \circ y = xy + x$ where $x, y \in \mathbb{R}$

By considering associativity, show that $\mathbb{R}$ does not form a group under $\circ$

[4 marks]

Question 9

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	…	$a\circ x$	…	$a\circ y$	…
…	…	…	…	…	…

And under the assumption that the same element occurs twice,

$$\begin{aligned} a \circ x &= a \circ y \\ a^{-1} \circ (a \circ x) &= a^{-1} \circ (a \circ y) && \text{Every element in a group has an inverse} \\ (a^{-1} \circ a) \circ x &= (a^{-1} \circ a) \circ y && \text{A group has associativity} \\ e \circ x &= e \circ y && e \text{ is the identity element} \\ x &= y \end{aligned}$$

But this contradicts the starting assumption that *x* and *y* are distinct elements.
∴ 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.

[2 marks]

Question 10

(a) Given that $f(x) = \dfrac{3x - 1}{7x - 2}$, show that $ff(x) = \dfrac{2x - 1}{7x - 3}$

[3 marks]

(b) Given that, as before, $f(x) = \dfrac{3x - 1}{7x - 2}$, show that $fff(x) = x$

[3 marks]

(c) With $G = \{ f(x),\ ff(x),\ fff(x) \}$ and the binary operation $\circ$ being composition of functions, a group if formed.
Here are a couple of ways of writing out the Cayley table for this group;

$\circ$	$f(x)$	$ff(x)$	$fff(x)$
$f(x)$	$ff(x)$	$fff(x)$	$f(x)$
$ff(x)$	$fff(x)$	$f(x)$	$ff(x)$
$fff(x)$	$f(x)$	$ff(x)$	$fff(x)$

$\circ$	$\frac{3x-1}{7x-2}$	$\frac{2x-1}{7x-3}$	x
$\frac{3x-1}{7x-2}$	$\frac{2x-1}{7x-3}$	x	$\frac{3x-1}{7x-2}$
$\frac{2x-1}{7x-3}$	x	$\frac{3x-1}{7x-2}$	$\frac{2x-1}{7x-3}$
x	$\frac{3x-1}{7x-2}$	$\frac{2x-1}{7x-3}$	x

(i) What is the identity element of this group ?

[1 mark]

(ii) What is $fff(x) \circ ff(x)$?

[1 mark]

(iii) What is the inverse of the element $ff(x)$?

[1 mark]