RI Mathematics Masterclass Series

Seeing Behind the Curtain...
a crash course in Group Theory

3rd February, 2024

What are we doing today?

The story today...

- Higher level mathematics is abstraction!

What are we doing today?

The story today...

- Higher level mathematics is abstraction!
- Why care about remainders?

What are we doing today?

The story today...

- Higher level mathematics is abstraction!
- Why care about remainders?
- Combining symmetries.

What are we doing today?

The story today...

- Higher level mathematics is abstraction!
- Why care about remainders?
- Combining symmetries.
- Reorderings of numbers.

What are we doing today?

The story today...

- Higher level mathematics is abstraction!
- Why care about remainders?
- Combining symmetries.
- Reorderings of numbers.
- Same thing, different name?

What are we doing today?

The story today...

- Higher level mathematics is abstraction!
- Why care about remainders?
- Combining symmetries.
- Reorderings of numbers.
- Same thing, different name?

From **concrete** examples... to an **abstract** concept.

Modular Arithmetic, or, why are remainders useful?

You learned a long time ago about remainders: what is left over when I divide 24 by 7?

Modular Arithmetic, or, why are remainders useful?

You learned a long time ago about remainders: what is left over when I divide 24 by 7?

$$24 \div 7 = 3 \text{ remainder } 3$$

Modular Arithmetic, or, why are remainders useful?

You learned a long time ago about remainders: what is left over when I divide 24 by 7?

$$\begin{aligned} 24 &= 21 + 3 \\ &= 7 \times 3 + 3 \end{aligned}$$

Modular Arithmetic, or, why are remainders useful?

You learned a long time ago about remainders: what is left over when I divide 24 by 7? Why not write $\frac{24}{7}$?

'Clock' Arithmetic

If the time is $14:00$, it is 2 o'clock.

We are working *modulo* 12.

To get the time in the 12 hour form, we need to work out the **remainder** that we get by dividing the time by 12.

‘Clock’ Arithmetic

Example. 16 : 00 is 4 o’clock because

$$16 \div 12 = 1 \text{ remainder } 4.$$

‘Clock’ Arithmetic

Example. 16 : 00 is 4 o’clock because

$$16 \div 12 = 1 \text{ remainder } 4.$$

Sometimes the remainder is the only thing we care about!

'Clock' Arithmetic

Exercise. If today is Saturday, what day of the week will it be in 107 days?

‘Clock’ Arithmetic

Exercise. If today is Saturday, what day of the week will it be in 107 days?

Answer. $107 = 15 \times 7 + 2$, so $107 \div 7 = 15$ remainder 2.

‘Clock’ Arithmetic

Exercise. If today is Saturday, what day of the week will it be in 107 days?
Answer. $107 = 15 \times 7 + 2$, so $107 \div 7 = 15$ remainder 2. So we move two days in the week from a Saturday to a **Monday.**

Modular Arithmetic

In higher level mathematics, we tend to write this as

$$107 = 2 \mod 7.$$

When we write mod, this is short for *modulo*, which means nothing more than remainder. In algebraic terms:

$x = y \mod z \iff$ y is the remainder when x is divided by z.

Modular Arithmetic

Some quick-fire questions for everyone...

Modular Arithmetic

Some quick-fire questions for everyone...

What is $4 \mod 5$?

Modular Arithmetic

Some quick-fire questions for everyone...

$$\text{What is } 4 \mod 5?$$

Well, $5 = 0 \times 5 + 4$, so the remainder is 4. This gives

$$4 \mod 5 = 4.$$

Nothing too exciting here...

Modular Arithmetic

Some quick-fire questions for everyone...

What is $65 \mod 4$?

Modular Arithmetic

Some quick-fire questions for everyone...

$$\text{What is } 65 \mod 4?$$

Well, $65 = 16 \times 4 + 1$, so the remainder is 1. This gives

$$64 \mod 4 = 1.$$

Modular Arithmetic

Some quick-fire questions for everyone...

What is $-2 \mod 6$?

Modular Arithmetic

Some quick-fire questions for everyone...

$$\text{What is } -2 \mod 6?$$

Well, $-2 = -1 \times 6 + 4$, so the remainder is 4. This gives

$$-2 \mod 6 = 4.$$

Modular Arithmetic

Modular addition... how does it work?

We write $x +_n y = z$ to mean that $z = x + y \mod n$.

To perform modular addition, can calculate $x + y$ first and then calculate this modulo n **or** can calculate x and y modulo n and then add the result.

Modular Arithmetic

$$
\begin{aligned}
14 +_{10} 8 &= 14 + 8 \mod 10 \\
&= 22 \mod 10 \\
&= 2
\end{aligned}
$$

Modular Arithmetic

$$\begin{aligned} 14 +_{10} 8 &= 14 + 8 \mod 10 \\ &= (4 \mod 10) + (8 \mod 10) \\ &= 12 \mod 10 \\ &= 2 \end{aligned}$$

Modular Arithmetic

$$
\begin{aligned}
14 +_{10} 8 &= 14 + 8 \mod 10 \\
&= (4 \mod 10) + (-2 \mod 10) \\
&= 2 \mod 10 \\
&= 2
\end{aligned}
$$

Modular Arithmetic Tables

Exercise! Construct tables that show modular addition for $+_3$ and $+_6$. Whilst constructing these tables, think about any properties of the tables that you notice.

$+_3$	0	1	2
0			
1			
2			

$+_6$	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

Modular Arithmetic Tables

Hints...

$+_3$	0	1	2
0			
1			
2			

- Are there any symmetries to your tables?
- How many times does each number appear in the table?
- Do any rows/columns remain unchanged?

Modular Arithmetic Tables

Hints...

$+_3$	0	1	2
0			
1			
2			

- Are there any symmetries to your tables?
- How many times does each number appear in the table?
- Do any rows/columns remain unchanged?
- Can we always get back to 0? How?

Modular Arithmetic Tables

Here are the tables filled in.

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$+_6$	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

The tables are symmetric about the diagonal. What does this tell us?

Modular Arithmetic Tables

Here are the tables filled in.

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$+_6$	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

Each number appears only once in each row and column (Latin square property).

Modular Arithmetic Tables

Here are the tables filled in.

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$+_6$	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

The rows and columns where we add 0 remain unchanged (0 is called an additive identity).

Modular Arithmetic Tables

Here are the tables filled in.

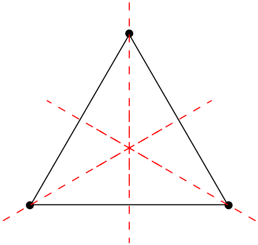
$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$+_6$	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

To get back to 0 from 0, we add 0. To get back to 0 from 1 we add 2, etc. We can always get back to the identity!

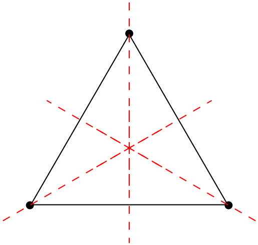
Symmetries of Shapes: Equilateral Triangle

What is a symmetry? What are the symmetries of an equilateral triangle?



Symmetries of Shapes: Equilateral Triangle

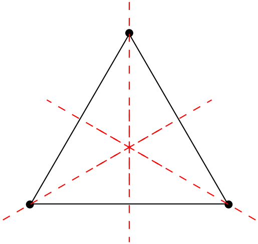
What is a symmetry? What are the symmetries of an equilateral triangle?



How many symmetries of the triangle are there?

Symmetries of Shapes: Equilateral Triangle

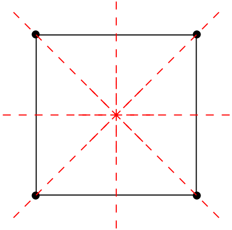
What is a symmetry? What are the symmetries of an equilateral triangle?



Rotations by $0^\circ, 120^\circ, 240^\circ$ and reflections in each line of symmetry.

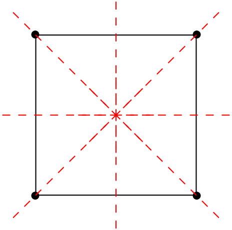
Symmetries of Shapes: Square

How many symmetries of the square are there?



Symmetries of Shapes: Square

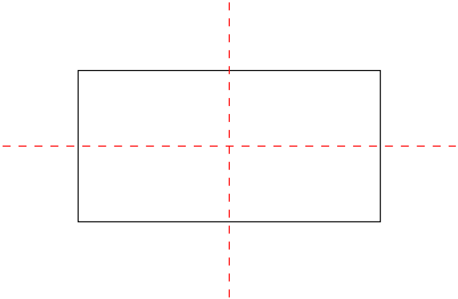
How many symmetries of the square are there?



Rotations by $0^\circ, 90^\circ, 180^\circ, 270^\circ$ and reflections in each line of symmetry.

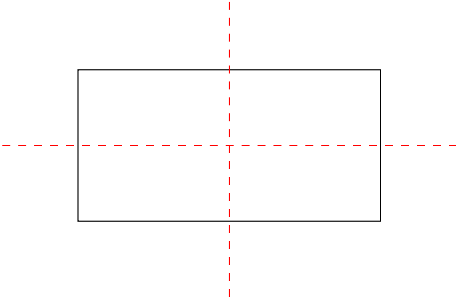
Symmetries of Shapes: Rectangle

How many symmetries of the rectangle are there?



Symmetries of Shapes: Rectangle

How many symmetries of the rectangle are there?



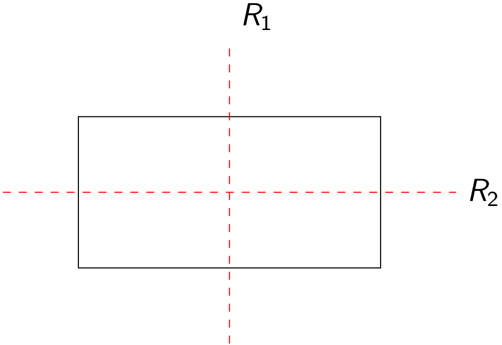
Rotations by $0^\circ, 180^\circ$ and reflections in its two lines of symmetry.

Symmetries of Shapes

We now want to do a similar thing to when we made tables for $+_n$, but for the symmetries of the shapes.

Symmetries of Shapes

Example.



And rotations I of 0° and θ of 180°.

Symmetries of Shapes

We can write this in a ‘multiplication’ table as before.

	I	θ	R_1	R_2
I	I	θ	R_1	R_2
θ	θ	I	$\theta R_1 = R_2$	R_1
R_1	R_1	R_2	I	θ
R_2	R_2	R_1	θ	I,

where θR_1 means ‘do R_1 first and then do θ’.

Tables of Symmetries

Workshop time!

- Fill in the 'multiplication' tables for the symmetries of the triangle and if you have time for the square.
- There will be instructions in your workshop rooms.
- Discuss any properties of the tables that you notice.

Tables of Symmetries

Some questions...

- Are these tables symmetric? What does this tell us?
- Are any rows/columns unchanged?
- Can we always get back to the original shape?
- Can we undo each symmetry?

Tables of Symmetries

The table for the triangle.

	I	θ(120)	θ(240)	R3	R1	R2
I	I	θ(120)	θ(240)	R3	R1	R2
θ(120)	θ(120)	θ(240)	I	R1	R2	R3
θ(240)	θ(240)	I	θ(120)	R2	R3	R1
R3	R3	R2	R1	I	θ(240)	θ(120)
R1	R1	R3	R2	θ(120)	I	θ(240)
R2	R2	R1	R3	θ(240)	θ(120)	I

Permutations

A permutation is a reordering of a list of numbers. We can write them in the following way:

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

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

Permutations

A permutation is a reordering of a list of numbers. But... the following are **NOT** examples

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

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

Permutations

Question. How many permutations are there of $1, 2, 3$? How many of $1, 2, ..., n$?

Composing Permutations

How can we combine (compose) permutations? Best explained through examples.

Composing Permutations

Example. (We work right to left)

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Composing Permutations

Example. (We work right to left)

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

What happens to 1?

Composing Permutations

Example. (We work right to left)

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

What happens to 1? $1 \mapsto 3$ then $3 \mapsto 3$. So $1 \mapsto 3$.

Composing Permutations

Example. (We work right to left)

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

What happens to 2?

Composing Permutations

Example. (We work right to left)

$$\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}.$$

What happens to 2? $2 \mapsto 2$ then $2 \mapsto 1$. So $2 \mapsto 1$.

Composing Permutations

Example. (We work right to left)

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Then 3 must go to 2. Overall, we had $1 \mapsto 3$, $2 \mapsto 1$, $3 \mapsto 2$, which we can write as $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$.

Permutation Tables

Remember we said that there are 6 permutations of $1, 2, 3$ since $3! = 6$. So if we label them as follows

- $I = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$
- $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$
- $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \sigma^2$
- $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$
- $\tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \sigma\tau$
- $\tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \sigma^2\tau$

can we construct a multiplication table like before? Hint: Work out what $\tau\sigma$ is (this will help with finding others!)

Permutation Tables

Workshop time!

- Construct the multiplication table for the 6 permutations on the previous slide.
- There will be instructions in your workshop rooms.
- Be careful about order you perform the permutations in! We work from right to left.
- Discuss any properties of the tables that you notice.

Permutation table for $1, 2, 3$.

$\circ$	ι	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
ι	ι	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
σ	σ	σ^2	ι	$\sigma\tau$	$\sigma^2\tau$	τ
σ^2	σ^2	ι	σ	$\sigma^2\tau$	τ	$\sigma\tau$
τ	τ	$\sigma^2\tau$	$\sigma\tau$	ι	σ^2	σ
$\sigma\tau$	$\sigma\tau$	τ	$\sigma^2\tau$	σ	ι	σ^2
$\sigma^2\tau$	$\sigma^2\tau$	$\sigma\tau$	τ	σ^2	σ	ι

Groups

What were the properties we noticed in all of our earlier examples?

- The tables were Latin squares.

Groups

What were the properties we noticed in all of our earlier examples?

- The tables were Latin squares.
- Closed under the operation.

Groups

What were the properties we noticed in all of our earlier examples?

- The tables were Latin squares.
- Closed under the operation.
- There was an identity I (do nothing) object.

Groups

What were the properties we noticed in all of our earlier examples?

- The tables were Latin squares.
- Closed under the operation.
- There was an identity I (do nothing) object.
- You could always undo an operation and get back to I (inverses).

Groups

What were the properties we noticed in all of our earlier examples?

- The tables were Latin squares.
- Closed under the operation.
- There was an identity I (do nothing) object.
- You could always undo an operation and get back to I (inverses).
- Trickier to see... associativity: $a(bc) = (ab)c$.

Groups

What were the properties we noticed in all of our earlier examples?

- The tables were Latin squares.
- Closed under the operation.
- There was an identity I (do nothing) object.
- You could always undo an operation and get back to I (inverses).
- Trickier to see... associativity: $a(bc) = (ab)c$.
- Some of the tables (not all!) were also commutative.

Groups

These properties give us the notion of a **group**. This is an **abstraction** of the different objects we've seen. The numbers under modular addition, the symmetries of regular polygons, and permutations of numbers all have properties in common.

Groups

A group is a set of things which we can combine using an operation and which satisfies the following **group axioms**.

- Closed under the operation (we don't get anything outside of the things we've started with).
- Associative $a(bc) = (ab)c$.
- There is an identity element (do nothing element).
- Every element has an inverse (can get back to the identity).

Groups

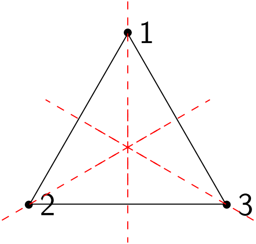
A group allows us to capture the behaviour of these different objects without specific details of what the object is.

- Look over your tables that you've constructed today. Are any of them the same up to relabelling?

Groups

- Look over your tables that you've constructed today. Are any of them the same up to relabelling?

The symmetries of triangle are 'the same' as the permutations of $1, 2, 3$.



But these were **not** the same as the numbers $1, 2, 3, 4, 5, 6$ with modular addition. Why not?

Groups

Have a think about what the connection is between the symmetries of the triangle and permutations of $1, 2, 3$. Hint: try labelling the vertices of your triangle.

Groups

By labelling the vertices of a triangle with $1, 2$ and 3, we notice that all of the symmetries of the triangle can be seen to be permutations of $1, 2, 3$.

Groups

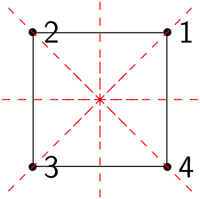
Do you think the symmetries of the square are the same as the permutations of $1, 2, 3, 4$? Hint: think about the size of each of these groups.

Groups

These groups can't be the same! There are 8 symmetries of the square but $4! = 24$ permutations of $1, 2, 3, 4$.

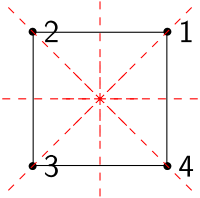
Subgroups

But if we labelled the vertices of the square, why does the same argument as with the triangle not work?



Subgroups

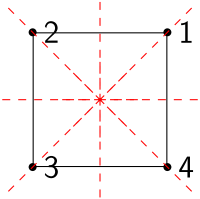
But if we labelled the vertices of the square, why does the same argument as with the triangle not work?



Not every permutation of $1, 2, 3, 4$ can be a symmetry of the square! Can you think of one?

Subgroups

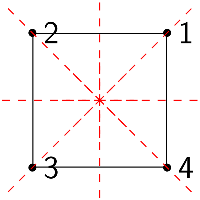
But if we labelled the vertices of the square, why does the same argument as with the triangle not work?



For example, we cannot keep 1 fixed and take $2 \mapsto 3$, $3 \mapsto 4$, i.e. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$ is not a symmetry of the square.

Subgroups

But if we labelled the vertices of the square, why does the same argument as with the triangle not work?



$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$ is not a symmetry of the square. One way is to see that this permutation would change the distances between vertex 1 and vertex 2. If the distance in the picture is 1, what would the distance change to after applying this permutation?

Subgroups

So, whilst every symmetry of the square is a permutation of $1, 2, 3, 4$, the opposite is not true. This tells us that the group of symmetries of the square 'sits inside' of the group of permutations of $1, 2, 3, 4$.

Subgroups

When one group ‘sits inside’ another it is called a **subgroup** of the larger group. Looking at our tables from earlier today, can you find any subgroups? Hint: you may need to use a similar idea of relabelling that we have used before.

Summary

What have we learnt today?

- We looked at modular arithmetic and learnt why remainders are useful.

Summary

What have we learnt today?

- We looked at modular arithmetic and learnt why remainders are useful.
- We looked at symmetries of shapes and how to 'combine' these symmetries.

Summary

What have we learnt today?

- We looked at modular arithmetic and learnt why remainders are useful.
- We looked at symmetries of shapes and how to 'combine' these symmetries.
- We saw how permutations (reorderings of numbers) can be combined.

Summary

What have we learnt today?

- We looked at modular arithmetic and learnt why remainders are useful.
- We looked at symmetries of shapes and how to 'combine' these symmetries.
- We saw how permutations (reorderings of numbers) can be combined.
- We **abstracted** the properties these objects had in common to introduce the idea of a group.

Summary

What have we learnt today?

- We looked at modular arithmetic and learnt why remainders are useful.
- We looked at symmetries of shapes and how to 'combine' these symmetries.
- We saw how permutations (reorderings of numbers) can be combined.
- We **abstracted** the properties these objects had in common to introduce the idea of a group.
- The main take-away message: Lots of **different** ideas can be described by **one** idea.

Summary

What have we learnt today?

- We looked at modular arithmetic and learnt why remainders are useful.
- We looked at symmetries of shapes and how to 'combine' these symmetries.
- We saw how permutations (reorderings of numbers) can be combined.
- We **abstracted** the properties these objects had in common to introduce the idea of a group.
- The main take-away message: Lots of **different** ideas can be described by **one** idea.

Summary

What have we learnt today? In higher mathematics, you can then just work with this one idea, and from this you can learn things about all of the concrete examples.