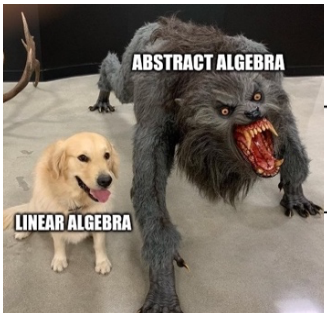
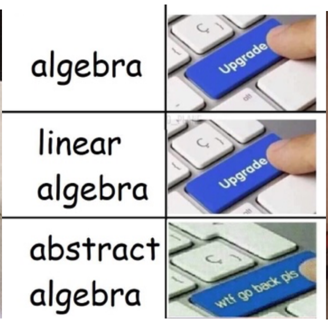
# Abstract Algebra - Groups





## Table of Contents

# 1 Groups Introduction

## 1.1 Intuition

Group are abstract. They generalise a lot of different things from arithmetic, algebra, geometry and more. Let's recap what was mentioned at the start of vector spaces as this extends to groups!

When studying arithmetic you learn how to add, subtract, multiply and divide different kinds of numbers (Integers, fractions, real numbers, complex numbers). The one day you suddenly realise that addition is subtraction in disguise.
$7-4$ is in fact the same as $7+-4$ so instead of subtracting you're adding a negative number. Similarly, division is multiplication in disguise. $9 \div 5$ is the same as $9 \times \frac{1}{5}$ . Instead of dividing you're really multiplying by a fraction. So, in arithmetic there are only really 2 operations, addition and multiplication. For addition opposites are negative numbers and for multiplication opposites are reciprocals.

In abstract algebra we use the word inverse instead of opposite. If you combine a number with its inverse you get a special number called an identity element. For addition, identity is 0. If you add 5 and it's inverse $-5$ you get 0. What makes 0 unique is if you add it to any number, that number doesn't change ; it retains its identity. For multiplication the identity is 1. Why? If you multiply a number by its inverse i.e. its reciprocal, you get 1. What makes 1 special? If you multiply it by any number, that number does not change. So, for both **addition and multiplication we have numbers, we have inverses, we have identity elements, hence we have a group and are now ready to understand a group definition** ☺

**Group Definition:**
Group is a **set of elements** (we use the word elements rather than numbers to be more abstract) with **one operation *** (most commonly + or x for addition or multiplication) that lets you **combine any 2 elements** and remain a member of the group. Just like with vectors spaces, we need to check some of the usual properties for groups (4 properties this time). Remember to **check the properties for the based on the** operation for the group.

- **Closure** – combining any elements under the operation will always make a member of that set and you only get one unique answer

  If you combine 2 elements in the group, the result is also in the group. It is important to realise that if you take any 2 elements of a group and you can build another element in that group! We say the group is closed under the operation.

- **Associativity** - If we re-group the operation we will get the same answer. We need associativity because without associativity we couldn't solve the simplest equations.

- **Inverse element** - undoes an element
  - Inverse element of $+$: the element that brings you back to identity i.e. the element that gives you 0

    e.g. $3 \Longrightarrow$ inverse is -3
  - Inverse element of $\times$: the element that brings you back to identity i.e the element to give you 1
    - e.g. $3 \Longrightarrow$ inverse is $\frac{1}{3}$

- **Identity element** (aka neutral element ) - does nothing. It leaves an element of a set unchanged when combined with it
  - Identity element of $+$: 0 is the identity element
  - Identity element of $\times$: 1 is the identity element

Understand that each element has an inverse, if you combine an element with its inverse you get an element which we call the identity

**Watch out**! Groups do not need to be commutative. If a group is not commutative, when we re- order the operation we do not get the same answer.

So, a group has
- Set of elements
- Single operation *
- Is closed under the operation * – if combine 2 elements in the group by doing * you get a third elements in the group
- Identity elements
- Every element has an inverse and combining it with its inverse gives you the identity element
- The elements obey the associative property.

Let's say we want to define the set integers under addition. We want our definition to be as simple as possible, the simpler the better
We want to be able to solve basic equations. If we are going to generalise/abstract algebra then we need to be able to solve equations and keep track of the properties used along the way

| Question | Properties |
|---|---|
| $\boldsymbol{x+3=5}$ | • Subtracting is adding negative numbers, so we need **inverses** |
| $(\boldsymbol{x+3})+(-\boldsymbol{3})=\boldsymbol{5}+(-\boldsymbol{3})$ | |
| $(\boldsymbol{x+3})+(-\boldsymbol{3})=\boldsymbol{5}+(-\boldsymbol{3})$ | • If we simplify the right-hand side we get 2. The simple act of adding these 2 integers requires a **closed** operation. |
| $(\boldsymbol{x+3})+(-\boldsymbol{3})=\boldsymbol{2}$ | |
| $\boldsymbol{x}+[\boldsymbol{3}+(-\boldsymbol{3})]=\boldsymbol{2}$ | • We regroup numbers on the left-hand side. To do this we need the **associate** property |
| $\boldsymbol{x}+\boldsymbol{0}=\boldsymbol{2}$ | • $3+-3=0$ the **identity** element |

So, the definition of a group is the simplest definition that will let you sole a basic equation.

The best way to further get to grips with the basics of groups is through examples. Determine whether the following are groups:

The notation used for groups is a bracket with the set and then a comma and the operation. $(\text{set}, \text{operation})$.
In other words $(\ldots,")$ we say this aloud as this as group of … under ". Under " is the jargon used to specify the group operation
Recall that

- $\mathbb{Z}^{\times}$ or $\mathbb{Z}^{*}$ is used to mean $\mathbb{Z}-\{0\}$
- $\mathbb{Z}^{+}$ or $\mathbb{Z}_{+}$ means positive integers
- $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}_n$ means integers mod n

## Addition Examples

**i. Set of integers under addition. We write this as $(\mathbb{Z},+)$**

- Closure – if we add 2 integers we get another integer hence satisfied
- Associativity – the order in which we add integers does not matter
- Inverse element – every integer has an additive inverse which is the negative version of the number
- Identity element – the additive identity 0 is an integer

Yes $(\mathbb{Z},+)$ is a group. All conditions are satisfied (closed under addition, associative, has an inverse and an identity element)

**ii. Set of positive integers under addition $(\mathbb{Z}^{+},+)$**

- Closure – if we add 2 positive integers we get another positive integer hence satisfied
- Associativity – the order in which we add positive integers does not matter
- Inverse element – this fails. we need negative integers to get identity element of addition which is 0
- Identity element – we don't need to even both to check this since the inverse broke down

$(\mathbb{Z}^{+},+)$ not a group, no additive inverse

**iii. Set of real numbers under addition $(\mathbb{R},+)$**

- Closure – if we add 2 real numbers we get another real number hence satisfied
- Associativity – the order in which we add real numbers does not matter
- Inverse element – every real number has an additive inverse which is the negative
- Identity element – the additive identity 0 is real number

Yes $(\mathbb{R},+)$ a group. All conditions satisfied (closed under addition, associative, has an inverse and an identity element)

**iv. Set of positive integers under addition $(\mathbb{R}^{+},+)$**

- Closure – if we add 2 positive real numbers we get another positive real number hence satisfied
- Associativity – the order in which we add positive real numbers does not matter
- Inverse element – this fails. we need negative real numbers to get identity element of addition which is 0
- Identity element – we don't need to even both to check this since the inverse broke down

$(\mathbb{R}^{+},+)$ not a group, additive no inverse

**v. Set of integers mod n under addition $(\mathbb{Z}_n,+)$**

Recall these are the integers mod n $=\{0,1,2,3,4,\ldots n-1\}$

Yes $(\mathbb{Z}_n,+)$ is a group. All conditions are satisfied (closed under addition, associative, has an inverse and an identity element)

## Multiplication Examples

**vi. Set of positive integers under multiplication** $(\mathbb{R},\times)$

- Closure – if we multiply 2 real numbers we get another real number hence satisfied
- Associativity – the order in which we add multiply real numbers does not matter
- Inverse element – this fails. We need negative reciprocals to get the identity element of multiplication which is 1 which works except for the element 0 since we can.t divide by 0,
- Identity element – we don't need to even both to check this since the inverse broke down

Not a group. 0 does not have a multiplicative inverse

**vii. Set of positive integers under multiplication** $(\mathbb{R}-\{\mathbf{0}\},\times)$

This is now a group without including 0 is because zero has no multiplicative inverse. Remember to be a group, every element must have an inverse.

Yes a group. All conditions satisfied. (closed under addition, associative, has an inverse and an identity element)

**viii. Set of integers under multiplication** $(\mathbb{Z},\times)$

We need reciprocals to get back to the identity element 1. Not all elements have inverses, only 1 and $-1$ will have inverses. Inverse of 2 is $\frac{1}{2}$ and this is not an integer. 0 cannot be divided by zero.

Not a group. All numbers except 1 and $-1$ do not have a multiplicative inverse under the integers.

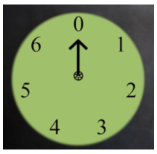
**ix. Set of positive integers mod n under multiplication** $(\mathbb{Z}_n-\{\mathbf{0}\},\times)$

Yes, but **only if** n is prime.

## 1.2 Common Types Of Groups

There are a wide variety of groups. Notice below how we are using the same tool to solve many different kinds of problems. It took Mathematicians a while to recognise this notion of using the same tool in completely different settings. The following examples highlight this well and this is important to understand when dealing with groups.

### Clock/Modular Arithmetic (integers mod n) $\mathbb{Z}_n$



Here we have the integers mod 7

Imagine you live on an alien planet where each day is 7 hours long. Here a clock has 7 hours. You might be tempted to number them 1-7.
Computer science tells us its best to begin counting with 0 so let's number 0-6

As far as clock is covered just 7 numbers

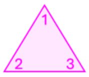
Can add and subtract any 2 of these numbers
3+5 = 1 (start at 3 and add 5 more hours end up at 1)
4+3 = 0 (start at 4 and add 3 more hours end up at the top)
1-3 = 5 (start at 1 and move counter-clockwise 3 hours end up at 5)

Clock arithmetic is also called modular arithmetic
Here there are 7 hours so we call them the integers mod 7.

This has many many applications in maths and computer science.

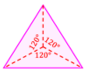
### Symmetries of a shape (important example)

Consider an equilateral triangle. Number the vertices 1, 2 and 3

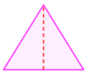


Puzzle: How many different ways can you pick up the triangle, rotate and flip it around and then set it back down so that it is in the same starting orientation?

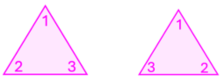
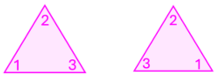
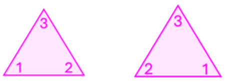
- Call a rotation 120° clockwise $r$



- Call a flip about the vertical $y$ axis $f$ for flip

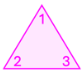


Considering all orderings of the 3 numbers

| Put 1 at vertex - swap 2 and 3 | Put 2 at vertex - swap 1 and 3 | Put 3 at vertex - swap 1 and 2 |
|---|---|---|
|  |  |  |

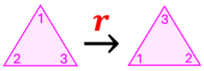
So, clearly we know there are 6 possible options. We could have gotten this quickly by doing 3! = 6
Let's apply these transformations in terms of flips and rotation

**Transformation 1:**
If we do nothing to the triangle the triangle is unchanged 1 (identity)

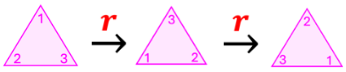


What other ways can you rotate and flip triangle so that it overlaps itself?

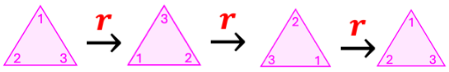
**Transformation 2:**
If we rotate once (a rotation 120° clockwise). We call this transformation $r$ for rotation



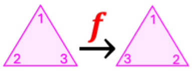
**Transformations 3:**
If we rotate twice we call this $r^2$ since we applied $r$ twice



Note: If we rotate three times and return to starting position, this means $r^3 = 1$ hence NOT a new transformation

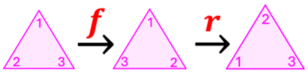


**Transformation 4:** flip once about the vertical axis $f$

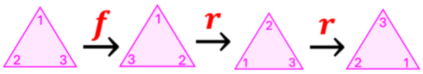


Note: If we flip twice return to starting position so $f^2 = 1$ hence NOT a new transformation

**Transformation 5:** flip and then rotate which we call $rf$



**Transformation 6**: flip and then rotate twice which we call $r^2f$



This covers all possible transformations. There are 6 transformations all together.

$$1, r, r^2, f, rf, r^2f$$

Notice how there are only 2 basic transformations (all the elements in the set are generated/obtained by $r$ and $f$, by simply raising them to powers

- rotation $r$
- flip about vertical axis $f$

Confused how we chose these 6 transformations and no more? For now just realise that any other transformation combination will could have chosen would give us one of the 6 same triangles above. For example reflecting twice and then rotate twice is the same as rotating twice. See the generators section later on. It will go over this in detail.

This is one way to study a shape in geometry by looking at all the ways to transform the shape on to itself. These transformations are called symmetries and you will see if it in more detail in the symmetries section.

### Integers under addition $\mathbb{Z}$
$\{\ldots -3, -2, -1, 0, 1, 2 \ldots\}$

Set of all whole numbers

We can add and subtract any 2 integers but subtracting is adding with neg numbers

$$7 - 11 = 7 + -11 == 4$$

For this reason we say the operation is a single operation addition

If we add any 2 integers get another integer (we say the integers are closed under addition)

If we divide one integer by another may get a number outside the set of integers 3 divided by 5 is $\frac{3}{5}$ which is not in the set of integers so integers we say the integers are not closed under division since when you divide 2 integers you may get a number outside the set of integers

One number which has a unique property. This is the number 0. If we add 0 to any integer, we get the same integer. 0 has no effect when adding.

Believe it or not there is a close relationship between symmetries of a shape and clock arithmetic!

The examples above are 3 very different examples. However, these 3 very different examples have in common? The **properties** of groups! Let's check them for each:

| **Clock/Modular Arithmetic (integers mod n)** $\mathbb{Z}_n$ | **Symmetries of a shape** | **Integers under addition** $\mathbb{Z}$ $\{\ldots -3, -2, -1, 0, 1, 2 \ldots\}$ |
|---|---|---|
| Set of objects (elements):<br>The numbers 0-6 | Set of objects (elements):<br>The 6 geometric transformations which we also call symmetries (the set is not the triangle) | Set of objects (elements):<br>infinite collection of whole numbers |
| Operation: **A way to combine any 2 elements**<br>Addition and we use the symbol $+$<br>$+$ is used to show we are combining any 2 elements in the set using addition<br>Why $+$ sign? In modular arithmetic we use the plus sign even though addition means something different on the clock (like with integers subtraction is redundant since any subtraction problem can be re-written as an addition problem for example $2-4$ is the same as $2+3$) | Operation: **A way to combine any 2 elements**<br>This is neither addition not multiplication but it common to use multiplication x symbol. We can use a different symbol but people tend to reuse $+$ and $\times$ symbols a lot with groups.<br>I prefer to use $\circ$ as the symbol to **denote composition** like apply a rotation and then a flip for example. | **Operation: A way to combine any 2 elements**<br>Addition and we use the symbol $+$<br>$+$ is used to show we are combining any 2 elements in the set using addition |
| Closure:<br>Closed under the operation addition. If we pick any 2 elements in the set (say a and b) and combine them using addition we get another element in the set. | Closure:<br>Closed under the operation addition. If we pick any 2 elements in the set (say a and b) and combine them using composition or rotations or flips we get another element in the set. | Closure:<br>Closed under the operation addition. If we pick any 2 elements in the set (say a and b) and combine them using addition we get another element in the set |
| Identity element: **no effect when combined w/ other elements**<br>This has no effect when combined with other elements via addition.<br>This identity element is 0> take any number x on clock and add 0 you get x | Identity element: **no effect when combined w/ other elements**<br>Identity element is transformation 1. This is the transformation where you pick up and drop triangle unchanged). If multiply any transformation y but transformation 1 you still get transformation y | Identity element: **no effect when combined w/ other elements**<br>This has no effect when combined with other elements via addition.<br>This is 0. For any integer $z$<br>$z+0 = z$ and $0+z=z$ |
| Inverse: **For any element there is a opposite element**<br>inverse of 3 is $-3$ but $-3$ is just 4 on the clock so we say the inverse of 3 is 4 and 3+4 = 0 the identity element<br><br>$+$ sign for your operation means inverse is written as $-x$.<br>$x \to -x$<br>Combining $x$ with its inverse gives you the identity element of addition which is 0<br>$x+(-x)=0$ | Inverse: **For any element there is a opposite element**<br>Each transformation has an opposite as well. For example the inverse of the element $r$ which rotates 120 clockwise is the transformation that is a double rotation which is $r^2$. This is because doing 3 rotations makes a compete circle returning you to the starting position. In other words, if you multiply $r$ and $r^2$ you get 1, the identity element for the symmetries.<br><br>$\times$ sign for operation means inverse is written as $x^{-1}$.<br>$x \to x^{-1}$<br>Combining $x$ with its inverse gives you the multiplication identity element 1<br>$x \times \frac{1}{x} = 1$ | Inverse: **For any element there is a opposite element**<br><br>inverse of 3 is $-3$ and inverse of 7 is $-7$ and so on. If you add element and its inverse you get 0 the identity element<br><br>$+$ sign for your operation means inverse is written as $-x$.<br>$x \to -x$<br>Combining $x$ with its inverse gives you the identity element of addition which is 0<br>$x+(-x)=0$ |

The final property is the associative property. When combining 3 elements it doesn't matter how you group them. You can start by combining first 2 elements or you can start with last 2 elements. Either way you'll end up with the same answer.

| Associative:<br>$(a+b)+c = a+(b+c)$ | Associative:<br>$(a \times b) \times c = a \times (b \times c)$ | Associative:<br>$(a+b)+c = a+(b+c)$ |
|---|---|---|

This is often a property people take of granted but important nonetheless. If grouping did a difference much of mathematics would come to a screeching halt!

Now let's give a more formal general definition of a group since you should be ready ☺

- **set of elements** G
- has an operation which allow you to combine any 2 elements. Common symbols for the operation are $+$ and $\times$ but when speaking generally we will use * hence we use the **operations** $+, \times, *$
- group is **closed** under this operation (this means if you combine any 2 elements in the group you get another element in the group)
$$x, y \in G \Longrightarrow x * y \in G$$
- each element $x$ has an **inverse**. This is an object that has the opposite effect of $x$ and when you combine $x$ and its inverse you get the identity element which we call $e$
$$x * x^{-1} = e$$
- If you combine any element with the **identity** element $e$ you get $y$
$$y * e = e * y = y$$
- **associativity**
$$(a * b) * c = a * (b * c)$$

Notice that **groups are not required to be commutative**!!! This is not included since it would exclude many important examples like the group of symmetries. Take the triangle example where a flip follow by a rotation gives you something different that a rotation followed by a group.

If a group is commutative we call it a commutative group (another common name is group). If a group is not commutative we say non-commutative or non-abelian.

**A Vector Space is built using the scalars from a Field, and the vectors from an Abelian Group.**

## 1.3 Calculation Examples

All these examples are groups which have an infinite number of elements. We will later consider groups with a finite number of elements (see the group tables section). Let's now look at some examples which are not as straight forward as the original examples

**Example 1:** Prove that G=$\mathbb{R}$, $a*b=a-b$ is a group

This time we have the operation , $a*b=a-b$

$$a*b=a-b$$

Let's check associativity first

$$a*(b*c)=(a*b)*c$$

**Work on LHS $a*(b*c)$**

LHS = $a*(b*c)$

Apply the rule to bracket

$$b-c$$

Hence we have

$$a*(b-c)$$

Apply the rule again

$$a-(b-c)$$

$$=a-b+c$$

**Work on RHS $(a*b)*c$ next:**

RHS = $(a*b)*c$

Apply the rule to bracket

$$\mathrm{a-b}$$

Hence we have

$$(\mathrm{a-b})*\mathrm{c}$$

Apply the rule again

$$\mathrm{a-b-c}$$

LHS≠RHS ∴ not associative. We do not need to check any further. G is not a group

**Example 2:** Prove that G=$\mathbb{R}-\{-2\}$, $a*b=ab+2a+2b+2$ is a group

This is the group of real numbers except 2

**Associativity:**

$$a*b=ab+2a+2b+2$$

If associative $a*(b*c)=(a*b)*c$

**Work on LHS $a*(b*c)$ first:**

LHS = $a*(b*c)$

Apply the rule to bracket

$$bc+2b+2c+2$$

Hence we have

$$a*(bc+2b+2c+2)$$

Apply the rule again

$$a(bc+2b+2c+2)+2a+2(bc+2b+2c+2)+2$$

Simplify

$$=abc+2ab+2ac+2a+2a+2bc+4b+4c+4+2$$

$$=abc+2ab+2ac+2bc+4a+4b+4c+6$$

**Work on RHS $(a*b)*c$ next:**

RHS = $(a*b)*c$

Apply the rule to bracket

$$ab+2a+2b+2$$

Hence we have

$$(ab+2a+2b+2)*c$$

Apply the rule again

$$(ab+2a+2b+2)c+2a+2(ab+2a+2b+2)+2c+2$$

Simplify

$$=abc+2ac+2bc+2c+2ab+4a+4b+4+2c+2$$

$$=abc+2ab+2ac+2bc+4a+4b+4c+6$$

LHS= RHS ∴ associative

**Identity**

We always write $a*e=e*a=a$
since the identity element leaves unchanged

Now we use the rule and solve for $e$

**Step 1: Consider $a*e=a$ and solve for e**

Apply the rule to LHS

$$ae+2a+2e+2=a$$

We need to make $e$ the subject

$$ae+2e=-a-2$$
$$e(a+2)=-a-2$$
$$e=\frac{-(a+2)}{a+2}$$
$$e=-1$$

We don't need to check below since we know associative. It is enough to check the properties on one side above, but we will do it anyway

**Step 2: Consider $e*a=a$ and solve for e**

Apply the rule to LHS

$$ea+2e+2a+2=a$$

We need to make $e$ the subject

$$ea+2e=-a-2$$
$$e(a+2)=-a-2$$
$$e=\frac{-(a+2)}{a+2}$$
$$e=-1$$

Hence identity element exists $(-1)$

Note: To be quicker we could have plugged $e=-1$ found in step 1 into step 2 $e*a$ and checked that we ended up with $a$

**Inverse**

We always write $a*b=b*a=e$
since the inverse gives us the identity

we know $e=-1$
$a*b=b*a=-1$

Now we use the rule and solve for $b$ and then check whether any values of a would cause b to not be in the group

**Step 1: Consider $a*b=-1$**

Apply the rule to LHS

$$ab+2a+2b+2=-1$$

We need to make $b$ the subject

$$ab+2b=-3-2a$$
$$b(a+2)=-3-2a$$
$$b=\frac{-(3+2a)}{a+2}$$

$a\neq-2$ by definition of the group since it is real numbers except 2 so b is well defined

We don't need to check below since we know associative. It is enough to check the properties on one side above, but we will do it anyway

**Step 1: Consider $b*a=-1$**

Apply the rule to LHS

$$ab+2b+2a+2=-1$$

We need to make $b$ the subject

$$ab+2b=-3-2a$$
$$b(a+2)=-3-2a$$
$$b=\frac{-(3+2a)}{a+2}$$

$a\neq-2$ by definition of the group since it is real numbers except 2 so b is well defined

Finally we can say G is a group

Try the following examples

- G=$\{x\in\mathbb{R}, x\neq-1\}$, $a*b=2a+2b+2ab+2$
- G=$\mathbb{R}-\{-2\}$, $a*b=a+b+ab(a+b)$
- G=$\{x\in\mathbb{R}: x\geq0\}$, $a*b=+\sqrt{a^2+b^2}$
- G=$\mathbb{R}$, $a*b=\sqrt[3]{a^3+b^3}$

# 2 Formal Definition Of A Group

Now that you understand and have a feel for groups, we are in a position to get more formal. Recall a group is a set of elements with one operation. We use * to be more abstract - think of * as some mathematical rule which will be given to you in the question

More formally we define a group as:
A set G with a binary operation * on G such that

i. G is associative
ii. G is closed under *
iii. G has an identity element (usually denoted e)
iv. Each element of G has an inverse

Note: Group does not necessarily have to be commutative. If it is, we call it an abelian group

**Further definitions to thoroughly understand the definition above:**
**Binary operation** on a group G? Simply a rule assigning any element a and b of G another element of G (denoted a*b where * could be anything such as +,-, x or any harder combinations of operations)

More formally we write this as:
A function $\mathbf{G} \times \mathbf{G} \to \mathbf{G}$ (i.e we start with a group **G**, we assign it another element from the same group **G** and we get an element out which is in the same group **G**

**Closure**: What does having closure mean? Operation will always make a member of that set and you only get one unique answer which is a real number

**Associative**: It is what it says! "associate" or group". If we re-group we will get the same answer

More formally we write this as:
A binary operation * is associative if for all a,b,c ∈s , a*(b*c)=(a*b)*c
Remember to do what is inside the bracket first

**Identity element:** (aka neutral element ) "does nothing". It leaves an element of a set unchanged when combined with it
Identity element of $+$: 0 is the identity element
Identity element of $\times$: 1 is the identity element

More formally we write this as:
G has an identity element * if ∃ an element e∈ s such that ∀a ∈ s a*e=a=e*a

How do we apply this ?
Solve a*e=a and e*a=a for the identity e
If you get two different values of e then substitute e back into a*e and e*a to see which gives you a. Only one will!

**Inverse element:** "undo an element (call it a) that gives the identity when composed with a. It generalises the concept of negation and reciprocation
Inverse element of $+$: the element that brings you back to identity i.e. the element that gives you 0
Inverse element of $\times$: the element that brings you back to identity i.e the element to give you 1 (multiply by reciprocal i.e. $\frac{1}{a}$)

More formally we write it as:
An element b is an inverse of a is a*b=e=b*a
How do we apply this?
Using value of e found above, solve both a*b and b*a for b. Show that it is well defined in the group
(if no identity then don't both even checking for inverse since inverse just takes you back to the identity)

**Remember we don't need commutativity for a group. If a group also happens to have commutativity then we call it an abelian group which we will encounter more of later on!**

## 2.1 Group tables (aka Cayley Tables):

Before, in secondary school when you learnt arithmetic you were told to memorise multiplication tables that showed how to multiply the integers 1 through 12.

In abstract algebra, you begin to work with new types of numbers. Groups behave very different than the numbers in arithmetic.

When first starting out with groups, it is helpful to go back to basics and make a group multiplication table. A group table describes the operation (i.e. the interaction between the elements) of a finite group. It describes the structure of a finite group by showing all the possible products of all the group's elements in a square table reminiscent of an addition or multiplication table. Many properties of a group – such as whether or not it is abelian (commutative, which elements are inverses of which elements, and the size and contents of the group's centre can be discovered from its Cayley table.

A group table is a bit like solving a sudoku puzzle!

**Steps:**
Put group operation in top left-hand corner
List the elements in the same order in the header row and header column, starting with the identity element

**$\{1, -1, i, -i\}$ under multiplication**

1 is the identity element under multiplication so start with this in the header for the rows and columns

| $\times$ | $1$ | $-1$ | $i$ | $-i$ |
|---|---|---|---|---|
| $1$ | $1$ | $-1$ | $i$ | $-i$ |
| $-1$ | $-1$ | $1$ | $-i$ | $i$ |
| $i$ | $i$ | $-i$ | $-1$ | $1$ |
| $-i$ | $-i$ | $i$ | $1$ | $-1$ |

We can see the inverses from where the inside of the table has 1:

- Multiplicative inverse of 1 is 1
  This is because $1x\ 1 = 1$
- Multiplicative inverse of $-1$ is $-1$
  This is because $-1x - 1 = 1$
- Multiplicative inverse of $i$ is $-i$.
  This is because $i(-i) = 1$
- Multiplicative inverse of $-i$ is $i$.

**$\mathbb{Z}_4$ under addition**

0 is the identity element under addition so start with this in the header for the rows and columns

| $\times$ | $0$ | $1$ | $2$ | $3$ |
|---|---|---|---|---|
| $0$ | $0$ | $1$ | $2$ | $3$ |
| $1$ | $1$ | $2$ | $3$ | $4$ |
| $2$ | $2$ | $3$ | $4$ | $5$ |
| $3$ | $3$ | $4$ | $5$ | $6$ |

We can simplify this mod 4

| $\times$ | $0$ | $1$ | $2$ | $3$ |
|---|---|---|---|---|
| $0$ | $0$ | $1$ | $2$ | $3$ |
| $1$ | $1$ | $2$ | $3$ | $0$ |
| $2$ | $2$ | $3$ | $0$ | $1$ |
| $3$ | $3$ | $0$ | $1$ | $2$ |

We can see the inverses from where the inside of the table has 0

- Additive inverse of 0 is 0
- Additive inverse of 1 is 3
  This is because 1+3 =4 which is zero mod 4
- Additive inverse of 2 is 2. This is because $2 + 2 = 4$ which is 0 mod 4
- Additive inverse of 3 is 1. This is because $3 + 1 = 4$ which is 0 mod 4

**$\mathbb{Z}_3{}^*$ under multiplication**

Elements are $\{1,2\}$
The superscript tells us that we can't include 0

| $\times$ | $2$ | $2$ |
|---|---|---|
| $1$ | $1$ | $2$ |
| $2$ | $2$ | $4$ |

We can simplify this mod 3

| $\times$ | $2$ | $2$ |
|---|---|---|
| $1$ | $1$ | $2$ |
| $2$ | $2$ | $1$ |

Interesting features to note about Cayley Tables:

i. If start with identity element then the first row and first column just repeat the elements in the headers since if multiply any element by the identity you get the same element
ii. Every result **appears exactly once** in **each column and row**
iii. All results inside the table will be a member of the group (closure)
iv. Every row and every column contains the identity element. Why? Because in a group every element has an inverse.
v. The table is sometimes **symmetric about the diagonal**. If you flip the group along the diagonal you get the same table. This is because the group is **abelian**. If group were non abelian then the multiplication table would not be symmetric so a table is useful for telling us if a group is abelian
vi. It is not generally possible to determine whether or not an operation is associative simply by glancing at its Cayley table, as it is with commutativity
**vii.** There are **no duplicate elements in any row or column** (we're not counting the headers). Each row and each column contain all the group elements in some order. This happens for every group!

## 2.2 Field Tables

**Example 1:**

Write down multiplication table for $\mathbb{F}_7^\times$ and find the inverse of each element

Hint: all elements coprime to 7

**Multiplication Table:**

| $\times$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 2 | 4 | 6 | 1 | 3 | 5 |
| 3 | 3 | 6 | 2 | 5 | 1 | 4 |
| 4 | 4 | 1 | 5 | 2 | 6 | 3 |
| 5 | 5 | 3 | 1 | 6 | 4 | 2 |
| 6 | 6 | 5 | 4 | 3 | 2 | 1 |

Where the 1 is in the table gives us the inverses

$1^{-1} = 1$

$2^{-1} = 4$

$3^{-1} = 5$

$4^{-1} = 2$

$5^{-1} = 3$

$6^{-1} = 6$

There is no inverse for 0 under multiplication

**Example 2:**

$\mathbb{F}_2$ – a field with 2 elements $\{0,1\}$

Think of:

0 ~ even integers

1~ odd integers

**Addition Table:**

| $+$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

$0^{-1} = 1$

$1^{-1} = 0$

**Multiplication Table:**

| $\times$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

$1^{-1} = 1$

There is no inverse for 0 under multiplication

**Example 3:**

$\mathbb{F}_3$ – a field with 3 elements $\{0, 1, 2\}$

0={integers exactly divisible by 3}

1={integers remainder =1 mod 3}

2={integers remainder =2 mod 3}

**Addition Table:**

| $+$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

$0^{-1} = 0$

$1^{-1} = 0$

$2^{-1} = 2$

**Multiplication Table:**

| $\times$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 |
| 2 | 0 | 2 | 1 |

$1^{-1} = 1$

$2^{-1} = 2$

There is no inverse for 0 under multiplication

**Example 4:**

Consider the set {0,1,2,3} which are the remainders mod 4

**Addition Table:**

| $+$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

**Multiplication Table:**

| $\times$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 |
| 2 | 0 | 2 | 0 | 2 |
| 3 | 0 | 3 | 2 | 1 |

This is not a field so not $\mathbb{F}_4$ since the element 2 does not have a multiplicative inverse

**Example 5:**

Consider the set {0,1,2,3, 4} which are the remainders mod 5

This set is just $\mathbb{F}_5$

**Multiplication Table:**

| $\times$ | 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 |

Can you spot a pattern?

$\mathbb{F}_n$ is isomorphic to $\mathbb{Z}_n$ ($\mathbb{F}_n \cong \mathbb{Z}_n$ iff n is prime) You don't need to know what **isomorphic** means yet, but keep this in mind for later on that it loosely means 'the same as'.

$$\mathbb{F}_n \cong \mathbb{Z}_n \textbf{ for n prime}$$

Note: $\mathbb{F}_n = \{0,1,2,3,4, \dots . n-1)$ where n is prime. Don't confuse this with $\mathbb{F}^n = (x_1, x_2, \dots x_n) = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$

# 3 Symmetric Groups – An important group

The symmetric group $S_n$ is a group of permutations on a set with $n$ elements. Let's look at an example to get some intuition.

$S_3$ is the **group of ALL permutations** on a set with 3 elements

While you can use any integers, to keep things simple we will use the integers 1, 2 and 3.

Permutations of $\{1,2,3\}$

$$S_3 = \{1,2,3\}$$

There are 3! ways (i.e. 6 ways) to permute this set. The 6 permutations are the elements of the group $S_3$. What are all the possible orders we can write of 123 (we expect there to be 6)?

123
132
321
213
231
312

Hence we say this group has 3! elements. The size of a group is also called **the order** and written using an absolute value symbol, $|S_3| = 6$

Don't confuse the **order of a group** with the order of an element. The order of an element looks the same, but means the same but something different. You will learn about the order of an element sction later on.

Consider the permutation 231 for example. This permutation takes 123 and replaces it with 231 since

1 2 3
↓↓↓
2 3 1

- 1 is replaced with 2
- 2 is replaced with 3
- 3 is replaced with 1

We can write all the possible permutations with a more compact way to represent permutations.

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

The **top row in** each is the **inputs** (the elements of the set)
The **bottom row** in each the **outputs** (the values each number is mapped to/goes to)

This is a time saving notation. There are other ways to represent permutations so be aware of this in case your lecture uses a different representation.

This says

- 1 stays 1, 2 stays 2 and 3 stays 3
- 1 goes to 2, 2 goes to 1 and 3 stays 3
- 1 goes to 3, 2 stays 2 and 3 goes to 1
- 1 stays 1, 2 goes to 3 and 3 goes to 2
- 1 goes to 2, 2 goes to 3 and 3 goes to 1
- 1 goes to 3, 2 goes to 1 and 3 goes to 2

You will often see this written in a shorter way as

$$S_3 = \{e, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$$

Every group has an operation *. What is the group operation here? How do you combine any 2 permutations?

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

Remember you apply the permutations from **right to left** just like composing functions.

Let's pick 2 elements

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

Let's re- colour code for explanation

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

Why did we link these colours?

- On the right 1 maps to 2 and we then check what 2 does on the left. 2 maps to 3 hence $1 \rightarrow 2 \rightarrow 3$

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

So, the result is 1 maps to 3

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

- On the right 2 maps to 3 and we then check what 3 does on the left. 3 maps to 2 hence 2 → 3 → 2

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

So, the result is 2 maps to 2

$$\begin{pmatrix}&2&\\&2&\end{pmatrix}$$

- On the right 3 maps to 1 and we then check what 1 does on the left. 1 maps to 1 hence 3 → 1 → 1

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

So, the result is 3 maps to 1

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

Our final result is

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

The result is a permutation 321 which we expect to be an element of our set since we have closure and it is $\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$ i.e. $(1,3)$ which we have already een above is a member of our set

What happens if we multiply them in the reverse order?

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

We get

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

This is the permutation 213 which is different than 321.

Hence the group $S_3$ is not commutative. This means $S_3$ is a non abelian group. In fact aside from the groups $S_1$ and $S_2$, all symmetric groups are non-abelia

We can also build a Cayley table (try this as an exercise)

| ○ | $\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}=e$ | $\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ |
|---|---|---|---|---|---|---|
| $\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}=e$ | $\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ |
| $\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ |
| $\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ |
| $\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ |
| $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ |
| $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ |

Notice how we always put the left column element first. You could have done right first, but whatever you choose to do pick the same convention throughout!

$$s_3=\left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\right\}$$

Doing the multiplication in each cell gives

| ○ | $\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}=e$ | $\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ |
|---|---|---|---|---|---|---|
| $\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}=e$ | $\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ |
| $\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$ |
| $\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$ |
| $\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$ |
| $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$ |
| $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$ | $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ |

Notice how every row and every column contains a member in the set only once which we expect.

We can see that the table is not symmetrical about the diagonal ain diagonal hence not Abelian!

**An aside (optional reading) in functions and bijections:**

$$s_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

A permutation acts like a function. More specifically, it is a **bijection** from the $\{1,2,3\}$ to itself

$$f\{1,2,3\} \to \{1,2,3\}$$

For example 231

$$\begin{array}{c} 1\ 2\ 3 \\ \downarrow\downarrow\downarrow \\ 2\ 3\ 1 \end{array}$$

This means

$$f(1) = 2$$
$$f(2) = 3$$
$$f(3) = 1$$

**Treating the permutations as functions allows us to define group operation** $*$. Multiplication in $S_3$ is just function composition!
For example to multiply the permutations 231 and 312

$$\begin{array}{c} 1\ 2\ 3 \\ \downarrow\downarrow\downarrow \\ 2\ 3\ 1 \end{array} \quad * \quad \begin{array}{c} 1\ 2\ 3 \\ \downarrow\downarrow\downarrow \\ 3\ 1\ 2 \end{array}$$

Start by writing these permutations as bijections $f$ and $g$

$$\begin{array}{ll} f(1) = 2 & g(1) = 3 \\ f(2) = 3 & g(2) = 1 \\ f(3) = 1 & g(3) = 2 \end{array}$$

Next we compose $f$ and $g$. This gives us the bijection sending 1 to 1, 2 to 2 and 3 to 3

$$f \circ g(1) = 1$$
$$f \circ g(2) = 2$$
$$f \circ g(3) = 3$$

This is a trivial permutation and is the identity element in the group $S_3$
All we really need to know though is what the numbers 1, 2 and 3 map to!
The function notation just gets in the way hence the way we did it above

Now let's look at $S_4$. We use the set

$$\{1,2,3,4\}$$

$$|S_4| = 24$$

Earlier we wrote these as functions

$$\begin{array}{c} 1\ 2\ 3\ 4 \\ \downarrow\downarrow\downarrow\downarrow \\ 1\ 3\ 4\ 2 \end{array} \qquad \begin{array}{c} 1\ 2\ 3\ 4 \\ \downarrow\downarrow\downarrow\downarrow \\ 4\ 3\ 2\ 1 \end{array}$$

$$\begin{array}{ll} f(1) = 1 & g(1) = 4 \\ f(2) = 3 & g(2) = 3 \\ f(3) = 4 & g(3) = 2 \\ f(4) = 2 & g(4) = 1 \end{array}$$

But all we really need to know is what the numbers 1, 2,3 4 map to. The function notation just gets in the way!

We can write the permutations like this.

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

Let's practice using this compact notation.

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

Remember you apply the permutations from **right to left** just like composing functions.

Let's colour code for explanation

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

On the right 1 maps to 4 and on the left 4 maps to 4 hence $1 \to 4 \to 2$

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

So the result is 1 maps to 2

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

Next, we see 2 maps to 3 and on the left 3 maps to 4 hence $2 \to 3 \to 4$
So, the result is 2 maps to 4

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

Next, we see 3 maps to 2 and on the left 2 maps to 3 hence 3 → 2 → 3
So, the result is 3 maps to 3

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

Next, we see 4 maps to 1 and on the left 1 maps to 1 hence 4 → 1 → 1
So, the result is 4 maps to 1

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

The result is a permutation 2431

What happens if we multiply them in the reverse order?

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

We get

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

We get a different permutation when we switch order. The group $S_4$ is not commutative as expected!

## 3.1 Summary

The symmetric group $S_n$ is a group of permutations on a set with $n$ elements. A permutation is just a re-arrangement of the set. In this the notation, S stands for symmetric and symmetric group and $n$ tells you the size of the set being permuted. There are n! ways to permute a set with n elements. So $S_n$ is a finite group with n! elements.

$S_n$ =group of permutations on a set with n elements

It is common to use the integers 1 though $n$ rather than the permutations I wrote before

$$S_n = \{1, 2, 3, \dots n\}$$

Just remember that the elements of the group are not the numbers 1 through $n$, but rather the permutations in this set!!

- $S$ means symmetric
- subscript $n$ means the set has $n$ elements $S_n = \{1,2,3, \dots, n\}$.
- Symmetric group $S_n$ has $n!$ elements and we say the order of $S_n$ is $n!$ i.e. $|S_n| = n!$
  In other words, there are n! ways to arrange this set of integers (n! possible permutations) so the group $S_n$ is a finite group of n! elements
- $n \geq 3$ then is $S_3$ non-symmetric

If you think of a permutation as a bijection from the set to itself then the group operation is function composition. While you can write a permutation as a function it is easier to write simply the inputs and outputs!

Symmetric groups are important since every finite group is a subgroup of a symmetric group (known as Cayley's theorem)

## 3.2 Symmetric Groups Versus Permutation Groups

What is the difference between a permutation group and a symmetric group? A symmetric group is the **group of ALL permutations** on a set with 3 elements

$$s_3 = \left\{\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}\right\}$$

A permutation group is a group formed from the permutations of any set. For example

$$\left\{\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}\right\}$$

So, every symmetric group is a permutation group, but not every permutation group is a symmetric group

# 4 Orders and Generators

## 4.1 Order Of A Group

We use the notation $|G|$ in order to mention the order of a group G. The order of a group is the number of elements in the group. Group is called infinite if $|G| = \infty$ or finite if $|G| < \infty$

| $G = (\mathbb{Z}, +)$ | $S_n$ |
|---|---|
| This the is set of integers under addition<br>This looks like {0,1,2,3,4,5,……}<br>Hence order is infinite i.e. $|\mathbb{Z}| = \infty$ | The order of the group is $n$! Since n! elements |

Note: order of a subgroup divides the order of a group (see subgroup section later on)

## 4.2 Order Of An Element

Each element of a group has an order. in English, the order is how many times do we need to do apply the operation before we get the identity hence how many times do we need to do repeated addition and get 0 or how many times you do repeated multiplication and get 1 for multiplication)

The question to ask yourself if is:
"ow many times do I need to perform the operation on the element until I get the identity (FOR THE FIRST TIME!)" Those n times that you perform this operation on the element until you got the identity is the order of that particular element.

**Example 1** Set of integers under addition $(\mathbb{Z}, +)$
Order of any element is infinite

- Pick the element 2. 2+2 is 4. Plus 2 is 6 etc. Repeated addition will never give us the additive identity 0. So, the order of 2 is infinite $|2| = \infty$
- The same applies to any other chosen element

**Example 2** Set of real numbers except 0 under multiplication $(\mathbb{R} - \{0\}, \times)$
Let's see if repeated multiplication will give us the identity 1

- Pick the element 1: $1^1 = 1 =$ identity so order of 1 is 1 i.e. $|1| = 1$
- Pick the element $-1$: $(-1)^2 = 1 =$ identity so order of $-1$ is 2 i.e. $|-1| = 2$

Note: Other than 1 and $-1$, no other non-zero real can be raised to a positive integer power to get 1, so all other real numbers have infinite order in this group

**Example 3** {1,2,4,7,8,11,13,14; X mod 15}

- Pick element 1: $1^1 = 1 =$ identity so order of 1 is 1 i.e. $|1| = 1$
- Pick element 2.: $2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 1 =$ identity so order of 2 is 4 i.e. $|2| = 4$
- Pick element 7: $7^1 = 7, 7^2 = 4, 7^3 = 13, 7^4 = 1 =$ Identity so order of 7 is 1 i.e. $|7| = 4$
- Pick element 11: $11^1 = 11, 11^2 = 1 = identity$ so order of 11 is 2 i.e. $|11| = 2$

Finding the orders of all the other elements quickly we get $|4| = 2, |8| = 4, |13| = 4, |14| = 2$
The set of orders is {1,2,4}
Hint: If the numbers to power end up big and you want to do calculations quicker, then modulo the base numbers first before powering. Furthermore you can also build powers using previous powers answers

This is an abelian (commutative) group. You can check the Cayley table if you're in doubt (symmetry along the diagonal). Take note of how the order of the elements of an abelian group form a subgroup of the group {1,2,4} is a subgroup of {1,2,4,7,8,11,13,14}.

**Example 4** Set of complex numbers except 0 addition $(\mathbb{C} - \{0\}, \times)$
There are infinitely many complex numbers z where $z^n = 1$, known as the roots of unity

- Pick element $i$ : $i^4 = 1 =$ identity so order of $i$ is 4 i.e. $|i| = 4$

**Example 5:** Consider the symmetric group

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

Recall we can write this as

$$S_3 = \{e, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$$

Note: (3,1,2) is not in the set since $3 \to 1 \to 2$ which is the same as (1,2,3)

Let's check the orders or all elements:

| | |
|---|---|
| $(\mathbf{1,2})$: $\begin{pmatrix} 1 & 2 \\ 2 & 1 \\ 1 & 2 \end{pmatrix}$ order 2<br>$(\mathbf{1,3})$: $\begin{pmatrix} 1 & 3 \\ 3 & 1 \\ 1 & 3 \end{pmatrix}$ order 2<br>$(\mathbf{2,3})$: $\begin{pmatrix} 2 & 3 \\ 3 & 2 \\ 2 & 3 \end{pmatrix}$ order 2 | $(\mathbf{1,2,3})$: $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \\ 1 & 2 & 3 \end{pmatrix}$ order 3<br>$(\mathbf{1,3,2})$: $\begin{pmatrix} 1 & 3 & 2 \\ 3 & 2 & 1 \\ 2 & 1 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ order 3 |

(1,2) has order 2
(1,3) has order 2
(2,3) has order 2
(1,2,3) has order 3
(1,3,2) has order 3
The set of orders is {2,3}

**Example 6:** The set of anticlockwise rotation matrices

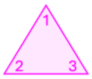
- Pick the rotation represented by $M = \begin{pmatrix} \frac{\sqrt{3}}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix}$. $M^{12} = 1$ so $|M| = 12$

Now you should be ready for the formla definition of the other of an element:
The order of an element in a group is the least positive integer n such that $g^n = e$
We say if g∈ $G$ then $g \dots \dots g = e$ i.e. $g^n = e$

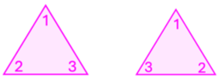
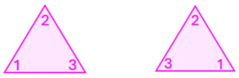
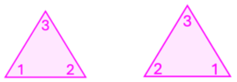
Note: If no n such that $\mathrm{g^n = e}$ then we say element has infinite order. Recall that $e = 0$ for addition and that $e = 1$ for multiplication

## 4.3 Generators Of A Group

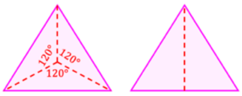
A generator means you can obtain any element in the group by raising the generator to a power. Let's consider our previous example of the symmetries of a 3 sided equilateral triangle. This is the best example to get an intuition and sold understanding of generators!



The symmetries of an equilateral triangle is the set of all possible moves from the starting position. We can clearly see that there are 6 possible combinations of the vertices 1,2, 3 since this is just permuting 123. Being systematic about it we can see:

| Put 1 at vertex - swap 2 and 3 | Put 2 at vertex - swap 1 and 3 | Put 3 at vertex - swap 1 and 2 |
|---|---|---|
|  |  |  |

We can use rotations (anticlockwise) and reflections to generate all of the 6 possible triangles above! Let



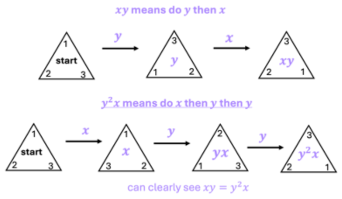
In our previous example we used the letters $f$ and $r$, but let's use $x$ and $y$ this time since these are the most commonly used letters.

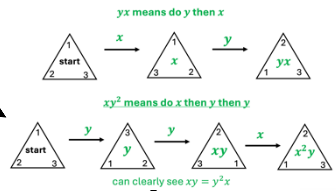
$x = \text{reflections}, y = \text{rotations (anticlockwise)}$

The group operation allows us to put moves together to get other moves. The group operation here is composition and $xy$ means do $y$ first and then $x$. Note: This is not commutative. A reflection follow by a rotation gives you something different that a rotation followed by a reflection hence $xy \neq yx$

The longest way to find the generators of this group would be to first list every single possible option. We need to ask ourselves, what are our options that we can do to the triangle reflection $(x)$ and rotation $(y)$ wise? We never need to rotate as much as three times or reflect twice since it does nothing/brings us back to the same thing. Let's start by writing them out

1) **Do nothing i.e. stay the same (identity) $e$**
2) **rotate once $y$**
3) **rotate twice $y^2$**
4) rotate three times $y^3 = e$ (same as 1 hence this is nothing new)
5) **reflect once $x$**
6) reflect twice $x^2 = e$ (same as 1 hence this is nothing new)
7) **reflect once and then rotate once $yx$**
8) **reflect once and then rotate twice $y^2x$**
9) reflect twice and then rotate once $yx^2 = y$ (same as 2 hence this is nothing new)
10) reflect twice and then rotate twice $y^2x^2 = y^2$ (same as 3 hence this is nothing new)
11) rotate once and then reflect once $xy$ (same as number 8 $y^2x$ but not obvious – see image)
12) rotate twice and then reflect once $xy^2$ (same as number 7 $yx$ but not obvious – see image)


$xy$ means do $y$ then $x$
start
1
2
3
$y$
$y$
$x$
$xy$
$y^2x$ means do $x$ then $y$ then $y$
start
$x$
$x$
$y$
$yx$
$y$
$y^2x$
can clearly see $xy = y^2x$


$yx$ means do $y$ then $x$
start
1
2
3
$x$
$x$
$y$
$yx$
$xy^2$ means do $x$ then $y$ then $y$
start
$y$
$y$
$y$
$xy$
$x$
$x^2y$
can clearly see $xy = y^2x$

Note: We don't' need to include more options as similarly, all the higher powers of $y$ and $x$ than this will simplify down too. Every 3 rotations of 120 degrees is the same as not moving it at all, so $y^7 = y^6 y$ hence 2 full rotations and then the actually-important single rotation of 120° hence $y^7 = y$.

It looks like there are **8 distinct options** above (6 blue and 2 grey) but we will see that 2 of them are the same (talking about the same triangle, just with different names). Hence, we have the following 6 possible transformations

$$\boldsymbol{e, y, y^2, x, yx}, y^2x$$

Note: or we could have instead said $\boldsymbol{e, y, y^2, x}, xy, \boldsymbol{xy^2}$

Aside from unchanging transformation ($e$) which doesn't change anything, each of the 6 **transformations** are combinations of the 2 actions (a rotation and a reflection). Notice how we can apply any two transformations by first applying one and then the other. In particular, if you multiply any transformation by the identity (doing nothing to the triangle) you get the same transformation since the identity doesn't change the triangle.

If you're still confused with the options written above you can draw the following table.

| ● | $e$ | $x$ | $y$ | $y^2$ |
|---|---|---|---|---|
| $e$ | $e$ | $x$ | $y$ | $y^2$ |
| $x$ | $x$ | $x^2 = e$ | $xy$ | $xy^2$ |
| $y$ | $y$ | $yx$ | $y^2$ | $y^3 = e$ |
| $y^2$ | $y^2$ | $y^2x$ | $y^3 = e$ | $y^4 = y$ |

This table is useful as it shows that$e, x, y, y^2$ are not enough.
It shows that we have the need for others
We know from above $xy = y^2x$ and $yx = xy^2$

Let's draw a Cayley table for all elements $\boldsymbol{e, y, y^2, x, yx, y^2x}$ (Note: we could have also instead done $e, y, y^2, x, xy, xy^2$)

| ● | $e$ | $y$ | $y^2$ | $x$ | $yx$ | $y^2x$ |
|---|---|---|---|---|---|---|
| $e$ | $e$ | $y$ | $y^2$ | $x$ | $yx$ | $y^2x$ |
| $y$ | $y$ | $y^2$ | $e$ | $yx$ | $y^2x$ | $x$ |
| $y^2$ | $y^2$ | $e$ | $y$ | $y^2x$ | $x$ | $yx$ |
| $x$ | $x$ | $y^2x$ | $yx$ | $e$ | $y^2$ | $y$ |
| $yx$ | $yx$ | $x$ | $y^2x$ | $y$ | $e$ | $y^2$ |
| $y^2x$ | $y^2x$ | $yx$ | $x$ | $y^2$ | $y$ | $e$ |

Notice how we always put the left column element first when we compose. You could have done right first, but whatever you choose to do pick the same convention throughout!

The table on the left has already been simplified for you.
We know $x^2 = e, y^3 = e, xy = y^2x$ and can use this to help us simplify

Let's look at a few calculations to see how we got the simplified results on the left:
How did we get $x \circ y^2x$?
$x \circ y^2x = x(y^2x) = x(xy) = x^2y = y$
This should also be intuitive, since rotating 120° anticlockwise is the same as flipping the shape, rotating 240° anticlockwise, and then flipping the shape back. Understanding not just how transformations can be represented in algebra, but also how to work with those algebraic expression will make higher level questions easier!

How did we get $yx$?
$x \circ y^2 = xy^2 = (xy)y = (y^2x)y = y^2(xy) = y^2(y^2x) = y^4x = y^3yx = yx$

How did we get $e$?
$(yx)(yx) = y(xy)x = y(y^2x)x = y^3x^2 = e$

How did we get $e$?
$(y^2x)(y^2x) = (xy)(y^2x) = xy^3x = x^2 = e$

Notice how inside the table everything is either $e, y, y^2, x, yx, y^2x$
Also notice how only one identity $e$ in each row/column and every row/column has all distinct elements.
Note: Sometimes lecturers will use 1 instead of $e$.
Something to note:
In English $xy = y^2x$ means whenever $y$ moves past $x$ it becomes $y^2$
We can also use this to help simplify the table

As you have probably realised, a multiplication is not the most efficient way to display all options. We can write this in a much more efficient way with generators and relations.

We know rotating 3 times brings us back to the same place hence $y^3 = e$ and reflecting twice brings us back to the same place hence $x^2 = e$ and also that $xy = y^2x$ or we could use instead that $yx = xy^2$

So, we can write

$$\{\boldsymbol{x}, \boldsymbol{y} : x^2 = e, y^3 = e, xy = y^2x\} \text{ or } \{\boldsymbol{x}, \boldsymbol{y} : x^2 = e, y^3 = e, yx = xy^2\}$$

You'll often see this written to include the group elements too

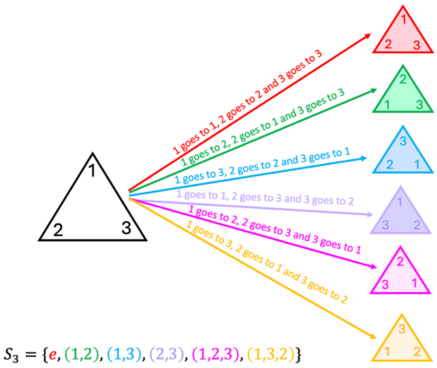
$$\{\boldsymbol{x}, \boldsymbol{y} : e, y, y^2, x, yx, y^2x \mid x^2 = e, y^3 = e, xy = y^2x\} \text{ or } \{\boldsymbol{x}, \boldsymbol{y} : e, y, y^2, x, xy, xy^2 \mid x^2 = e, y^3 = e, yx = xy^2\}$$

Make sure you understand that:
$x, y$ are the generators (raising $x$ and $y$ to certain powers is enough to generate the entire group)
$x^2 = e, y^2 = e, xy = y^2x$ are the relations/rules

- If rotate 3 times, go back to original so $y^2 = identity = e$
- If reflect 2 times, go back to original so $x^2 = identity = e$
- If reflect three times then rotate three times same as reflect once

In other words, from the generators and rules we can get/reach every type of transformation $e, y, y^2, x, yx, y^2x$ and the group has order 6. They specify the group entirely.

The symmetries of an equilateral triangle are in fact just permutations!


1
2
3
1 goes to 1, 2 goes to 2 and 3 goes to 3
1 goes to 2, 2 goes to 1 and 3 goes to 3
1 goes to 3, 2 goes to 2 and 3 goes to 1
1 goes to 1, 2 goes to 3 and 3 goes to 2
1 goes to 2, 2 goes to 3 and 3 goes to 1
1 goes to 3, 2 goes to 1 and 3 goes to 2

$S_3 = \{e, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$

There is another group $\boldsymbol{D_{2n}}$ called the Dihedral group which is the group of symmetries of a regular n sided polygon which should now make sense. Some courses use the notation $\boldsymbol{D_n}$ instead, so be careful.

So, we can say that $D_6$ is the symmetries of an equilateral triangle. Furthermore

$$\boldsymbol{D_6 \cong S_3}$$

Both of these sets are generated by 2 elements, $x$ and $y$

**Note:** ≅ means isomorphic. You will learn this in detail later, but keep this example in mind when first studying isomorphisms.

# 5 Cyclic Groups

A cyclic group is a group that can be generated by a single element. Cyclic groups have the property that all of the elements of the group can be obtained by repeatedly applying the group operation to a particular single group element. You only need to find 1 generator to prove a group is cyclic!

| | | | |
|---|---|---|---|
| $(\mathbb{Z},+)$<br>**(integers under addition)**<br><br>This is the set<br>{…,-5,-4,-3,-2,-1,0,1,2,3,4,5…}<br><br>The order of the group is infinite since infinite number of elements in the group i.e. $\lvert G\rvert = \infty$<br><br>The order of ANY element picked in this group is infinite<br><br>Let's pick element 2<br>2+2=4<br>2+2+2= 6<br>etc<br>So, the order of 2 is infinite i.e. $\lvert 2\rvert = \infty$<br><br>Now, let's look for a generator<br>1=1<br>1+1=2<br>1+1+1=3<br>1+1+1+1=4<br>1+1+1+1+1=5<br>etc<br><br>1 can generate all elements in the group (all integers) therefore group cyclic. Applying repeated addition to 1 generates every element of the group!<br><br>Note: 2 is not a generator though since 2,4,6 and can't generate all integers from this | $(\mathbb{Z}_6,+)$<br>**(integers mod 5 without 0 under addition)**<br><br>This is the set {0,1,2,3,4,5}<br><br>The order of the group is six since six elements in the group i.e. $\lvert G\rvert = 6$<br><br>Now, let pick all elements and find their orders<br>Pick element 0 : 0=0=$identity$ so order of 0 is 1 i.e. $\lvert 0\rvert = 1$<br><br>Pick element 1 : $1+1+1+1+1+1 = 6 = 0 = identity$ so order of 1 is 6 i.e. $\lvert 1\rvert = 6$<br><br>Pick element 2: 2+2+2= $6 = 0 = identity$ so order of 2 is 3 i.e. $\lvert 2\rvert = 3$<br><br>Pick element 3: 3+3= $6 = 0 = identity$ so order of 3 is 2 i.e. $\lvert 3\rvert = 2$<br><br>Pick element 4: 4+4+4= $12 = 0 = identity$ so order of 3 is 2 i.e. $\lvert 4\rvert = 4$<br><br>Pick element 5: 5+5+5= $12 = 0 = identity$ so order of 3 is 2 i.e. $\lvert 5\rvert = 6$<br><br>Now, let's look for a generator<br>1=1<br>1+1=2<br>1+1+1=3<br>1+1+1+1=4<br>1+1+1+1+1=5<br>1 can generate all elements in the group (all integers) therefore group cyclic<br>Note: 2 is not a generator though since 2,4,6 and can't generate all integers from this | **$(\mathbb{Z}_5{}^{*},\mathbf{x})$ or $(\mathbb{Z}/5\mathbb{Z}-\{\mathbf{0}\},\times)$**<br>**(integers mod 5 without 0 under multiplication)**<br><br>Note: This would not be a group if zero was included. 0 has no inverse. It would also not be a group is n was not prime.<br><br>This is the set {1,2,3,4}<br>The order of the group is 4 since 4 elements in the group<br><br>Now, let pick a few elements and find their order<br><br>Pick element 1 : $1^1 = 1 = identity$ so order of 1 is 1 i.e. $\lvert 1\rvert = 1$<br><br>Pick element 2: $(2)^4 = 16 = 1 = \text{identity}$ so order of 2 is 4 i.e. $\lvert 2\rvert = 4$<br><br>Pick element 3: $(3)^4 = 81 = 1 = identity$ so order of 3 i 4 i.e. $\lvert 3\rvert = 4$<br><br>Pick element 4: $(4)^2 = 16 = 1 = 1identity$ so order of 4 is 2 i.e. $\lvert 4\rvert = 2$<br><br>Now, let's look for a generator<br>This is the set {1,2,3,4}<br>$2^0 = 1$<br>$2^1 = 2$<br>$2^2 = 4$<br>$2^3 = 8 = 3$<br>$2^4 = 16 = 1$<br>2 can generate all elements in the group therefore group is cyclic<br>$4^0 = 1$<br>$4^1 = 4$<br>$4^2 = 16 = 1$<br>$4^3 = 64 = 4$<br>$4^3 = 64 = 4$<br>4 cannot generate all of the set, so 4 is not a generator | **$C_3$**<br>**(cyclic group of order 3)**<br><br>Generally speaking this group is the symmetries of a regular n sided polygon<br>(cyclic group of order n)<br>$C_n$ = $\{1, x, \dots, x^{n-1}\ \ I\ \ x^n = 1)\}$<br><br>$C_3$ integers mod 3 $C_3$=$\{1, x, x^2\ \ I\ \ x^3 = 1)\}$<br><br>The order of the group is 3 since 3 elements in the group<br><br>Now, let pick all elements and find their order<br>Pick element 1 : $1^1 = 1 = identity$ so order of 1 is 1 i.e. $\lvert 1\rvert = 1$<br><br>Pick element $x$ : $(x)^3 = 1 = \text{identity}$ so order of x is 3 i.e. $\lvert x\rvert = 3$<br><br>Pick element $x^2$ : $(x^2)^3 = 1 = \text{identity}$ so order of $x^2$ is 3 i.e. $\lvert x^2\rvert = 3$<br><br>Now, let's look for generator<br>$x^0 = 1$<br>$x^1 = x$<br>$x^2 = x^2$<br>$x$ can generate all elements in the group therefore group is cyclic<br><br>$(x^2)^0 = 1$<br>$(x^2)^1 = x^2$<br>$(x^2)^2 = x^4 = x$<br><br>1 cannot generate all of the set, so 1 is not a generator. Only $x\ and\ x^2\ are$<br><br>$\begin{array}{c\|ccc} \cdot & 1 & x & x^2 \\ \hline 1 & 1 & x & x^2 \\ x & x & x^2 & x^3=1 \\ x^2 & x^2 & 1 & x \end{array}$<br><br>**Generators are a power coprime to the group (in other words the power of a generator of a cyclic group is coprime to the order of the group)** |
| $(\mathbb{R},+)$<br><br>See the solution above for this | $(\mathbb{R}-\{\mathbf{0}\},\times)$<br><br>The order of the group is infinite since infinite number of elements in the group i.e. $\lvert G\rvert = \infty$<br><br>Pick element 1: $1^1 = 1 = identity$ so order of 1 is 1 i.e. $\lvert 1\rvert = 1$<br>Pick element -1: $(-1)^2 = 1 = identity$ so order of -1 is 2 i.e. $\lvert -1\rvert = 2$<br><br>Note: Other than 1 and -1, no other non-zero real numbers can be raised to a positive integer power to get 1 so all other real numbers have infinite order in this group<br><br>Now, let's look for a generator<br>$2^0 = 1$<br>$2^1 = 2$<br>$2^2 = 4$<br>$2^3 = 8 = 3$<br>$2^4 = 16 = 1$<br>2 cannot generate all elements (all real numbers)<br><br>In fact no number can generate all really numbers, therefore group is not cyclic | $(\mathbb{C}-\{\mathbf{0}\},\times)$<br><br>The order of the group is infinite since infinite number of elements in the group i.e. $\lvert G\rvert = \infty$<br><br>Now, let pick an element and find its order<br>Pick element $i$ : $\text{i}^4 = 1 = identity$ so order of $i$ is 4 i.e. $\lvert \text{i}\rvert = 4$<br><br>Now, let's look for a generator<br><br>This is the set {1,2,3,4}<br>$i^0 = 1$<br>$2^1 = 2$<br>$2^2 = 4$<br>$2^3 = 8 = 3$<br>$2^4 = 16 = 1$<br>2 can generate all elements in the group therefore group is cyclic<br>$4^0 = 1$<br>$4^1 = 4$<br>$4^2 = 16 = 1$<br>$4^3 = 64 = 4$<br>$4^3 = 64 = 4$<br>4 cannot generate all of the set, so 4 is not a generator | **Integers mod n**<br>{0,1,2,,3 ..n−1}<br><br>This a cyclic group under addition modulo n<br><br>Exercise: What are the generators of this group?<br><br>You can draw a multiplication table to help!<br><br>. |

. In other words, 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.

Note: **all cyclic groups are abelian** which are groups in which elements commute. However, not all abelian groups and necessarily cyclic.

**Brief Summaries for later on (come back to this section to understand fully once you have studied groups in more detail):**

**Symmetric Groups:**

- $\boldsymbol{S_n}$ =**symmetric** group = group of **permutations** on a set with n elements (there are n! elements hence the order is n!)

$$S_n = \{\mathrm{e}, y, \dots ,\ y^{n-1}, xy, \dots x^{n-1}y \ \mid\ x^2 = \mathrm{e}, y^{\mathrm{n}} = \mathrm{e}, xy = \mathrm{y}^{n-1}x\}$$

$x$ =reflections and $y$ =rotations

$yx$ means do $x$ 1st and then $y$ after

In English $xy = \mathrm{y}^{n-1}x$ means whenever y moves past $x$ it becomes $\mathrm{y}^{n-1}$
For example: $xy^2 = y^4x$
You can then get everything from these rules

Note: You'll often see this group written as Sym (M). For example the equilateral triangles we write Sym (T)

- $\boldsymbol{D_{2n}}$ = **Dihedral** group = group of **symmetries** of a regular n sided polygon (defined under multiplication)

$$D_{2n}= \{1, x, \dots ,\ x^{n-1}, y, xy, \dots , x^{n-1}y \ \mid\ x^n = 1, y^2 = 1, yx = x^{n-1}\, y\}$$

where $x = \text{rotations and } y = \text{reflections}$

$$\boldsymbol{D_6 \cong S_3}$$

which would be symmetries of a triangle (see isomorphism section later)

Recall that a symmetric group is the group of ALL permutations on a set with 3 elements A permutation group is just a subgroup of a symmetric group. Every finite group is isomorphic to a subgroup of a permutation group. You can get it by just numbering the elements and then observe how the group acting on itself permutes the elements.

**Cyclic Groups:**

- $\boldsymbol{C_n}$

$$C_n = \{1, x, \dots , x^{n-1} \ | x^n = 1\}$$

How to get the orders of each element:

- order of 1 is obviously always 1
- order of element with a power that doesn't fit into $n$ at all (coprime to $n$) is always $n$
- Intuitively just ask yourself what power you need to raise power to get n (if number fits into n i.e. divisible)
- In general, in $C_n$ with generator $\alpha$, the order of $\alpha^m$ is $\frac{n}{gcd\,(n,m)}$. If $gcd(n, m) = 1$, then $\alpha^m$ generates $C_n$

$$(\mathbb{Z}/\boldsymbol{n}\mathbb{Z}, +) \cong \boldsymbol{c_n} \textbf{ for n prime (see isomorphism section later on)}$$

How does this group differ to the 2 groups mentioned above?

- $C_n$ is generated by a single element. $D_n$ is always generated by two: a reflection and a rotation. $D_n$ is non-abelian, $C_n$is abelian. Therefore, they can't be isomorphic.
- All cyclic groups are NOT isomorphic to a permutation group! Permutation groups have order $n!$, whereas cyclic groups have order n. For instance, there's no permutation group of order 5. However, every group is a subgroup of a permutation group - this is known as Cayley's Theorem, and the proof is just to argue that every group acts on itself by left multiplication, so it has to be a subgroup of all permutations of the underlying set.

**Other Common Groups:**

- $\boldsymbol{Q_n}$ **Quarternion Group**

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k \ I \ i^2 = j^2 = k^2 = -1, ij = k = -ji\}$$

- **G** $\boldsymbol{L_n}(\mathbb{R})$ **General linear group**
  Invertible $nxn$ matrices with det$\neq 0$
  G $L$ is short for General Linear and subscript n tells us $nxn$ matrix and $\mathbb{R}$ tells us numbers in matrix are real numbers

## 5.1 Subgroup Definition

Again, this is just about checking properties. H is a subgroup of G if the following **3 properties** are satisfied

1) e$\in H$
2) Closure: g , h$\in H \Rightarrow$ gh$\in H$
   Note: gh doesn't mean multiplication. It means composition
   +: g + h
   ×: g$\circ h$
3) Inverse: g $\in H \Rightarrow g^{-1} \in H$

## 5.2 Fields versus Groups

In a sense, a field is pretty much a set F that is a commutative group in two ways at the same time: that is, it is a group with respect to addition, and it is also a group with respect to multiplication if you ignore the additive identity 0 since we cannot divide by 0!

Every field is a group but not every group is a field. Fields require commutativity too and have 2 operations not just one!
A **group** has a SINGLE binary operation, usually called "multiplication" but sometimes called "addition", especially if it **is** commutative. A **field** has TWO binary operations, usually called "addition" and "multiplication". Both of them are always commutative. **Groups** model symmetries.

## 5.3 Extended Definition of a Field (combines groups)

**Mini summary:**
In abstract algebra there is a wide variety of operations (geometric transformations, function composition and matrix multiplication). But many sets of elements have the familiar operations from arithmetic - addition subtraction multiplication and division . Loosely speaking, if you can add and subtract have group. If you can add subtract multiply you have a ring. But if you're lucky and can get all 4 operations the result is an object that behaves similarly to the numbers you learnt about in arithmetic and algebra. We call these fields.

We have talked about this before but it bears repeating. Recall in abstract algebra subtraction is the same as adding with negatives

$3-5$ is the same as 3 plus $-5$

so instead of saying can add and subtract say there is addition and additive inverse.

There is also a multiplicative inverse.

$\frac{3}{5}$ is same as 3 times $\frac{1}{5}$

Instead of saying can multiply and divide in abstract algebra say there is multiplication and multiplicative inverses

The additive inverse of 5 is $-5$

The multiplicative inverse of 5 is $\frac{1}{5}$

So, in arithmetic we learn about addition, subtraction, multiplication and division. In abstract algebra we speak of addition, additive inverse, multiplication and multiplicative inverses. It is shift in thinking, but it is key to understanding the more abstract objects

We are now ready to talk about fields. To motivate the definition we will look at a collection 6 groups some of which come with additional features. By adding features we are familiar with from real and complex numbers we will arrive at the full definition of a field. Consider these 6 sets:

- $\mathbb{Z}$ : These are not a field since there is no multiplicative inverse for 2 or 3. For example we can't have $\frac{1}{2}$ since $\frac{1}{2} \notin \mathbb{Z}$
- $\mathbb{R}^{2\times3}$ : 2 x 3 real matrices

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix}$$

- $\mathbb{R}^{2\times2}$ : 2 x 2 real matrices
- $\mathbb{Q}$ : This is the set of numbers that can be a fraction $\frac{p}{q}$ where p is an integer and q is a natural number
- $\mathbb{Z}/5\mathbb{Z}$ integers mod 5
- $\mathbb{Z}/6\mathbb{Z}$ integers mod 6

Firstly we will check the addition properties and then we will check the multiplication properties and lastly inverses and identities:

- all 6 sets are groups under addition. They are closed under addition. You can add any 2 elements together and the sum is in the set .
- The negative of each element is in the set
- There is an additive identity and associative property holds

Therefore all 6 groups are commutative under addition

So as a first pass, all 6 examples are commutative groups under addition . The next feature we want to include is multiplication. We can multiply any 2 integers or rational numbers together. We can also multiply any two numbers mod n for any n. That leaves the 2 sets of matrices. We can multiply 2 square matrices but can't multiply 2x3 matrices by each other. The dimensions are incompatible for multiplication.

So only 5 of the 6 examples advance to the next round of commutative groups with multiplication. Just as all the groups are commutative under addition, in a field we would like multiplication to be commutative as well (unlike vector spaces). After all the real and complex numbers are both commutative and they are a pleasure to work with!

The integers and rational numbers are both commutative under multiplication, so they advance. Also the integers mod n are commutative under multiplication for any n. We are about to lose another candidate - the 2x2 matrices are not commutative under multiplication. There are infinite number of examples where matrix multiplication is not commutative and here is on example. So only 4 out of the 6 groups are commutative under multiplication.

Next, we want each number to have a multiplicative inverse. The additive inverse 0 is a big exception here. We can't divide by 0 so 0 is not included in $\mathbb{Z}$. But still $\mathbb{Z}$ doesn't' work. In set of $\mathbb{Z}$ only 1 and $-1$ have multiplicative inverses, none of the other integers have one. For example, the inverse of 2 under multiplication is $\frac{1}{2}$ which is not an integer. So we lose $\mathbb{Z}$. We also lose the integers mod 6 since 2, 3 and 4 do not have inverses mod 6 under multiplication

However, Mod 5 is different. Here every non zero number has a multiplicative inverse. You can check looking at multiplication table for this set. So, the only 2 to advance are $\mathbb{Q}$ and $\mathbb{Z}/5\mathbb{Z}$ . Both these sets have the multiplicative identity which is 1 which is not a surprise since product of number and multiplicative inverse is 1.

$\mathbb{Q}$ and $\mathbb{Z}/5\mathbb{Z}$ are the only winners. They both share a similar set of properties. Both of these two are commutative groups under addition. They both have a second operation multiplication which makes them rings. Furthermore, multiplication is commutative so they are commutative rings. Better still, other than 0 every number has a **multiplicative inverse**. It is this last property brings them over the top and turns them into fields.

**We are now ready for a more advanced definition using groups - more compact:**

A set $\mathbb{F}$ of elements with 2 operations (+, x)

Both operations are connected by the distributive properties

- Operations are connected by the distributive property - addition and multiplication are connected through the familiar distributive rule
$$a \times (b + c) = ab + ac$$

All the elements of $\mathbb{F}$ form a commutative group

- $\mathbb{F}$ is a commutative group under addition (+)
$$a + b = b + a$$
- $\mathbb{F}^{\times}$ is a commutative group under multiplication if omit 0 (since can't divide by 0)
$$a \times b = b \times a$$

So we can define a field with groups

$< F, + >$ is a commutative group (under addition the elements are a commutative group)

$< F^{\times}, \times >$ is a commutative group (under multiplication the non-zero elements are a commutative group)

$$a \times (b + c) = ab + ac$$
$$(b + c) \times a = ba + ca$$

This is the compact definition of a field. You could have defined a field and make no mention of groups whatsoever as I did in an earlier section and just give a complete list of all their properties a field must satisfy but you lose sight of the fact that a **field is actually two groups with <u>two operations</u> at the same time.**

Let's return to our examples of $\mathbb{Q}$ and $\mathbb{Z}/5\mathbb{Z}$

- $\mathbb{Q}$= infinite field
- $\mathbb{Z}/5\mathbb{Z}$ =finite field. But these are not only finite field. $\mathbb{Z}/p\mathbb{Z}$ for any prime p also a field. Together these form the starting points for all fields. That is if pick any field $\mathbb{F}$ then it will contain only and only one of these fields a subfields $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$ etc. WE can this field prime fields.

And lastly, a group doesn't necessarily mean a field!! Watch out! A group has a single binary operation, usually called "multiplication" but sometimes called "addition", especially if it is commutative. A field has two binary operations, usually called "addition" and "multiplication". Both of them are always commutative. Groups model symmetries.