Group Theory

a) Groups

We can combine two numbers, using addition, to get another number:

$5+7=12$

We can combine two sets, using union, to get another set:

$(a,b,e,g)\cup(a,c,e,h,k)=(a,b,c,e,g,h,k)$

etc

A binary operation * combines two "things" to get another "thing".

A binary operation * is commutative if $p*q$ is always the same as $q*p$

For example, if we are combining numbers:

addition is commutative	$4+8=8+4$
subtraction is not commutative	$10-3\neq 3-10$
multiplication is commutative	$3\times 5=5\times 3$
division is not commutative	$24\div 6\neq 6\div 24$

A binary operation * is associative if $p*(q*r)$ is always the same as $(p*q)*r$

For example, if we are combining numbers:

addition is associative	$4+(3+8)=(4+3)+8$
subtraction is not associative	$20-(12-8)\neq(20-12)-8$
multiplication is associative	$3\times(4\times 5)=(3\times 4)\times 5$
division is not associative	$24\div(6\div 2)\neq(24\div 6)\div 2$

Example 1

Set $\{1,2,3,4,5,6\}$

Binary operation * where $p*q=pq, mod\,7$

For example:

$5*6=5\times 6=30=2, mod\,7$

Here is the combination table:

*	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

Note: $5*6$ appears in the 5 row and the 6 column etc

Note: the binary operation * is commutative because $5*6=6*5$ etc

(a) The set is closed under the binary operation. This means:

For all p and q in the set $p*q$ is in the set.

So all the numbers in the combination table are in the set.

(b) The set contains an identity element e This means:

For all p in the set $p*e=p$ and $e*p=p$

Here the identity element is 1

$1*1=1$ $2*1=2$ $3*1=3$ $4*1=4$ $5*1=5$ $6*1=6$

$1*1=1$ $1*2=2$ $1*3=3$ $1*4=4$ $1*5=5$ $1*6=6$

(c) Every element in the set has an inverse element in the set. This means:

For all p in the set there is an element p' in the set where $p*p'=e$ and $p'*p=e$

1 is it’s own inverse $1*1=1$

2 and 4 are inverses $2*4=1$ and $4*2=1$

3 and 5 are inverses $3*5=1$ and $5*3=1$

6 is it’s own inverse $6*6=1$

(d)The binary operation is associative.

You can check this for the above combination table.

Rules for a group:

A set of elements and a binary operation * is a group if:

The set is closed under *

The set contains an identity element

Every element in the set has an inverse element in the set

* is associative

So the set $\{1,2,3,4,5,6\}$ with the binary operation * where $p*q=pq, mod\,7$ is a group.

See Exercise

EXERCISE

1) Set $\{0,1,2,3\}$

Binary operation * where $p*q=p+q, mod\,4$

Complete the combination table and show we have a group.

2) We have these functions: $e(x)=x$ $f(x)=\frac{1}{x}$ $g(x)=-x$ $h(x)=-\frac{1}{x}$

Set $\{e,f,g,h\}$

Binary operation * where $f(x)*g(x)=f(g(x))$

Complete the combination table and show we have a group.

SOLUTIONS

1)

*	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Closed: all the numbers in the combination table are in the set.

Identity: 0

Inverses: 0 is its own inverse 1 and 3 are inverses 2 is its own inverse

Associative: you can check this for the above combination table.

2)

*	e	f	g	h
e	e	f	g	h
f	f	e	h	g
g	g	h	e	f
h	h	g	f	e

Closed: all the functions in the combination table are in the set.

Identity: e

Inverses: every function is its own inverse

Associative: you can check this for the above combination table.

Group Theorems

We have a group:

Set $\{e, a, b, c, d, f, g, ...\}$ where e is the identity element

Binary operation *

If we can prove a theorem, just using the rules for a group, then this theorem applies to all groups.

1. Cancellation theorem part 1

If $a*d=a*p$ then $d=p$

Proof

$a*d=a*p$

$a'*(a*d)=a'*(a*p)$

$(a'*a)*d=(a'*a)*p$

$e*d=e*p$

$d=p$

2. Cancellation theorem part 2

If $d*a=p*a$ then $d=p$

Can you prove this?

Note: if $a*d=p*a$ then we can't cancel to get $d=p$

3. Latin square theorem

Every group combination table is a Latin square.

(every element appears exactly once in each row and each column of the combination table)

Proof: (by contradiction) part 1

Assume c appears twice in the a row of the combination table.

Say $a*b=c$ and $a*f=c$ where b and f are different elements.

So $a*b=a*f$ so $b=f$ by the cancellation theorem. Contradiction.

Proof: (by contradiction) part 2

Assume c appears twice in the a column of the combination table.

Say $b*a=c$ and $f*a=c$ where b f are different elements

So $b*a=f*a$ so $b=f$ by the cancellation theorem. Contradiction.

Note: not every Latin square is a group combination table.

This Latin square is not a group combination table. There is no identity.

*	a	b	c
a	a	c	b
b	c	b	a
c	b	a	c

4. Equation solving theorem part 1

If $p*x=q$ then $x=p'*q$

Proof

$p*x=q$

$p'*(p*x)=p'*q$

$(p'*p)*x=p'*q$

$e*x=p'*q$

$x=p'*q$

5. Equation solving theorem part 2

If $x*p=q$ then $x=q*p'$

Can you prove this?

6. If $a*p=a$ then $p=e$

Proof

$a*p=a$

$a'*(a*p)=a'*a$

$(a'*a)*p=e$

$e*p=e$

$p=e$

7. $If\, a*p=e$ then $p=a'$

Can you prove this?

8. Inverse theorem

the inverse of $p*q$ is $q'*p'$

recall: if a and a' are inverses then $a*a'=e$ and $a'*a=e$

So we need to prove $(p*q)*(q'*p')=e$ and $(q'*p')*(p*q)=e$

Proof part 1

$$(p*q)*(q'*p')=p*(q*q')*p'=p*(e)*p'=(p*e)*p'=p*p'=e$$

Proof part 2

$$(q'*p')*(p*q)=\ldots=e$$

9. There is only one group with 3 elements

Proof

Set $\{e,a,b\}$

Let's start filling in the combination table.

*	e	a	b
e	e	a	b
a	a		
b	b		

There is only one way we can complete the table as a Latin square (try it)

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

We can check that this is a group (being a Latin square is necessary but not sufficient)

Closed: all the elements in the combination table are in the set.

Identity: e

Inverses: e is its own inverse a and b are inverses

Associative: you can check this for the above combination table.

Example

Set $\{0,1,2\}$

Binary operation * $a*b=a+b, mod\,3$

*	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

We can match up these elements with the elements $\{e,a,b\}$

$0 \leftrightarrow e$ $1 \leftrightarrow a$ $2 \leftrightarrow b$ and the two group tables will be the same.

10. There are only two groups with 4 elements

Proof

Set $\{e, a, b, c\}$

Let's start filling in the combination table.

*	e	a	b	c
e	e	a	b	c
a	a			
b	b			
c	c			

There are only four ways we can complete the table as a Latin square (try it)

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

*	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

*	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

Look at the second table and make the following changes:

change every a to b change every b to c change every c to a

then rewrite the table so that the rows and columns are in the order e, a, b, c

You then get the third table.

Look at the second table and make the following changes:

change every a to c change every b to a change every c to b

then rewrite the table so that the rows and columns are in the order e, a, b, c

You then get the fourth table.

So the second, third and fourth tables are really the same. So there are only two different ways we can complete the table as a Latin square and we can check that both are groups.

It can be shown that:

Number of elements	1	2	3	4	5	6	7	8	9	10	...
Number of groups	1	1	1	2	1	2	1	5	2	2	...

11. Symmetry theorem

The symmetries of any object form a group.

See chapters, Symmetries of a Rectangle, Symmetries of a Triangle

12. Lagrange’s theorem

The set $\{e, a, b, c\}$ with the binary operation * has four members. It is a group.

Lagrange’s theorem says:

If you take any member of the set, say b then $b*b*b*b=e$

In general:

The set $\{e, a, b, c\}$ with the binary operation * has n members. It is a group.

Lagrange’s theorem says:

If you take any member of the set, say b then $b*b*b*b*...*b=e$

Proof – too difficult

Example

The set $\{1,2,3,4,5,6\}$ with the binary operation * where $p*q=pq, mod\,7$ has six members. It is a group.

Lagrange’s theorem says:

If you take any member of the set, say 5 then:

$$5*5*5*5*5*5=1$$

But:

$$5*5*5*5*5*5=5^6, mod\,7$$

So Lagrange's theorem says:

$$5^6=1, mod\,7$$

Also:

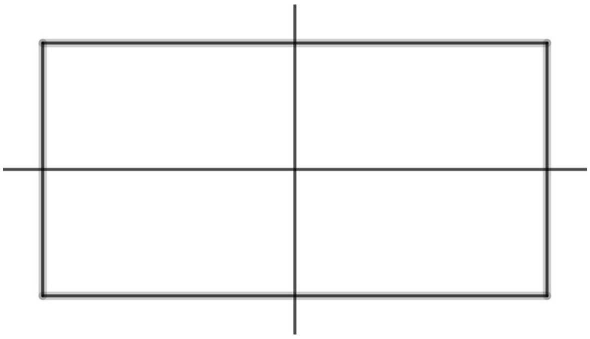
$$1^6=1, mod\,7 \quad 2^6=1, mod\,7 \quad 3^6=1, mod\,7 \quad 4^6=1, mod\,7 \quad 6^6=1, mod\,7$$

But this is Fermat's little theorem.

So Fermat's little theorem can now be seen as a special case of a more general theorem.

Symmetries of a Rectangle

If you take a rectangle and rotate it $180°$ about the centre then it looks exactly the same as it did before. We say the rectangle has rotation symmetry.



The symmetries of the rectangle are:

e do nothing

a rotate $180°$ about the centre

b rotate $180°$ about the x axis

c rotate $180°$ about the y axis

We can combine symmetries.

$a*b$ means you do b and then you do a This means you do b first.

Take a piece of card, in the shape of a rectangle.

If you do b and then do a it will end up in the same position as if you had just done c

Try it.

So $a*b$ is the same as c So $a*b=c$

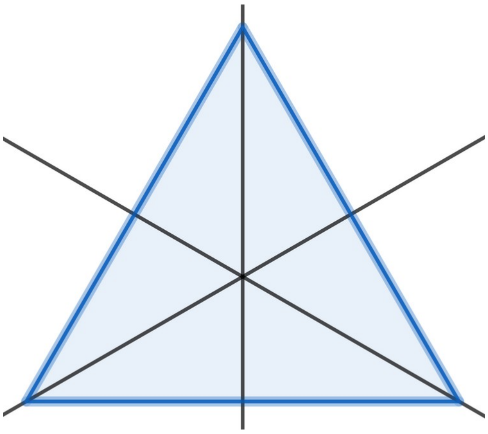
Here is the combination table. You should check some of these.

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Note: $a*b$ goes in the a row and the b column.

The set $\{e,a,b,c\}$ with the binary operation * forms a group.

Symmetries of a Triangle



The symmetries of the equilateral triangle are:

e do nothing

a rotate 120° about the centre (anticlockwise)

b rotate 240° about the centre (anticlockwise)

p rotate 180° about the line through the bottom left-hand corner

q rotate 180° about the line through the bottom right-hand corner

r rotate 180° about the line through the top corner

We can combine symmetries.

$a*p$ means you do p and then you do a This means you do p first.

Take a piece of card, in the shape of an equilateral triangle.

If you do p and then do a it will end up in the same position as if you had just done r

Try it.

So $a*p$ is the same as r So $a*p=r$

Show that $p*a=q$ So $a*p$ and $p*a$ are not the same.

* is not commutative.

Here is the combination table. You should check some of these.

*	e	p	q	r	a	b
e	e	p	q	r	a	b
p	p	e	a	b	q	r
q	q	b	e	a	r	p
r	r	a	b	e	p	q
a	a	r	p	q	b	e
b	b	q	r	p	e	a

Note $a*p$ goes in the a row and the p column.
And $p*a$ goes in the p row and the a column.

The set $\{e, p, q, r, a, b\}$ with the binary operation * forms a group.

Rearrangements

I have three ornaments in a line on my mantelpiece.

Let's call the left hand end of the mantelpiece, position 1. The middle, position 2 and the right hand end of the mantelpiece, position 3

Occasionally I decide to rearrange these ornaments. This means that I put them in a different order on the mantelpiece. The possible rearrangements are:

$P1$ Don't do anything

$P2$ Swap over the ornaments in positions 2 and 3

$P3$ Swap over the ornaments in positions 1 and 3

$P4$ Swap over the ornaments in positions 1 and 2

$P5$ Move each ornament one position to the left. The ornament that started in position 1 falls off the mantelpiece and is then put in position 3

$P6$ Move each ornament one position to the right. The ornament that started in position 3 falls off the mantelpiece and is then put in position 1

Let's call the ornaments A and B and C

If the ornaments start in the order A, B, C and I do $P5$ they will end up in the order B, C, A

If the ornaments start in the order C, B, A and I do $P5$ they will end up in the order B, A, C

etc

We can combine rearrangements.

$P4 * P2$ means you do $P2$ and then you do $P4$ This means you do $P2$ first.

Put the ornaments on the mantelpiece in any order.

If you do $P2$ and then do $P4$ they will end up in the same order as if you had just done $P6$

Try it.

So $P4 * P2 = P6$

Show that $P2 * P4 = P5$ So $P4 * P2$ and $P2 * P4$ are not the same.

* is not commutative.

Here is the combination table. You should check some of these.

*	P1	P2	P3	P4	P5	P6
P1	P1	P2	P3	P4	P5	P6
P2	P2	P1	P6	P5	P4	P3
P3	P3	P5	P1	P6	P2	P4
P4	P4	P6	P5	P1	P3	P2
P5	P5	P3	P4	P2	P6	P1
P6	P6	P4	P2	P3	P1	P5

Note $P2*P4$ goes in the P2 row and the P4 column.

And $P4*P2$ goes in the P4 row and the P2 column.

The set $\{P1,P2,P3,P4,P5,P6\}$ with the binary operation * forms a group.

A final thought …

Look at the chapter: Symmetry of a Triangle. We can pair-up these rearrangements with the symmetries of the triangle:

$P1 \rightarrow e$ $P2 \rightarrow p$ $P3 \rightarrow q$ $P4 \rightarrow r$ $P5 \rightarrow b$ $P6 \rightarrow a$

We find that these two groups are basically the same.

For example:

$P3*P5=P2$ and $q*b=p$

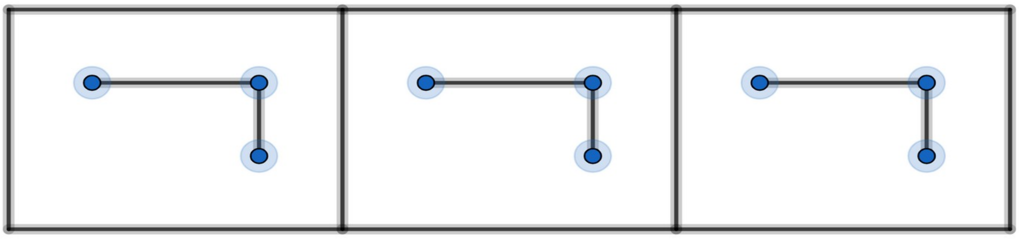
$P2*P4=P5$ and $p*r=b$

$P3*P2=P5$ and $q*p=b$

etc

We say these two groups are isomorphic which is a fancy way of saying they are basically the same.

Friezes



Here we have a row of identical tiles that extends indefinitely in both directions. The diagram shows just three of these tiles. Each tile has a design on it. This is called a frieze.

All friezes have translation symmetry with repeat distance d the length of the tile. (see footnote)

We can classify friezes by their other symmetries which can include:

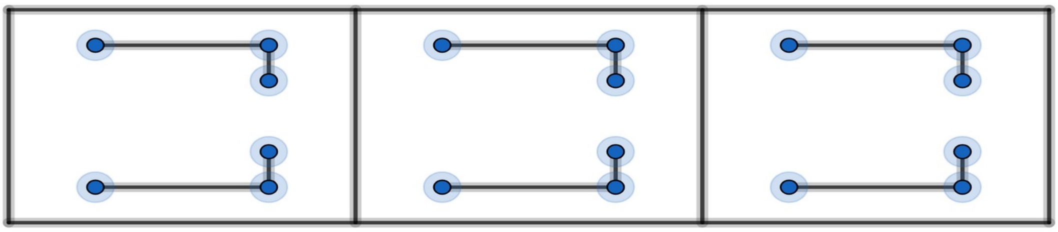
- horizontal mirror line along the middle of the frieze
- vertical mirror lines that are $d/2$ apart
- centres of $180°$ rotation that are $d/2$ apart
- glide-reflections with a glide distance $d/2$

Example 1

no other symmetries

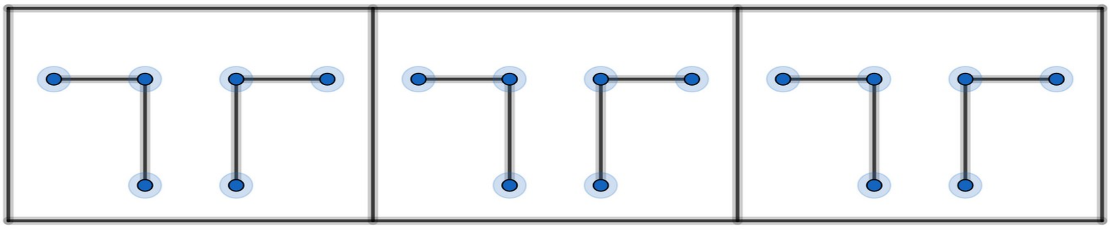
Example 2

horizontal mirror line – can you mark this on the diagram?



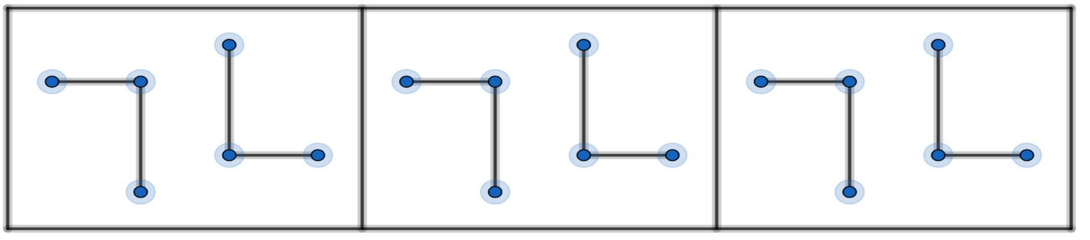
Example 3

vertical mirror lines – can you mark these on the diagram?



Example 4

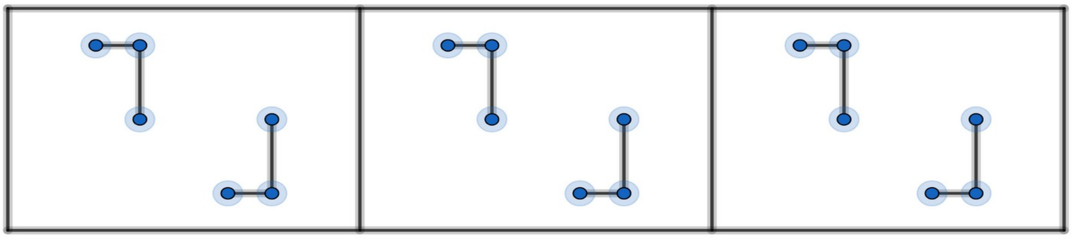
rotation – can you mark the centres of rotation on the diagram?



Example 5

glide-reflection

note: a glide-reflection is a combination of a translation and a reflection in a horizontal mirror line



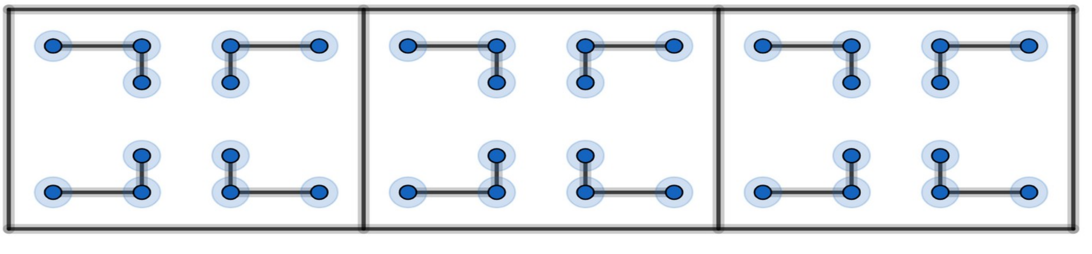
Example 6

horizontal mirror line

vertical mirror lines

rotation

can you mark these on the diagram?



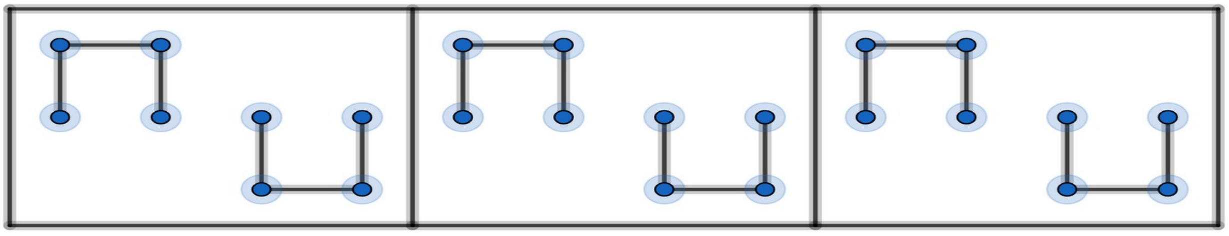
Example 7

vertical mirror lines

rotation

glide-reflection

can you mark these on the diagram?

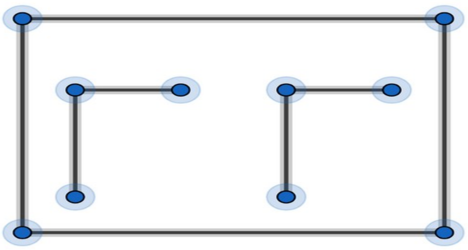


There are no more examples. There are only 7 frieze-symmetry-types. So every possible frieze can be classified as one of these 7 types.

Friezes repeat in one direction. Wallpapers repeat in two directions. It turns out that there are only 17 wallpaper-symmetry-types. So every possible wallpaper can be classified as one of these 17 types.

footnote:

What if our tile had length D and looked like this?



This individual tile has translation symmetry.

To keep things simple we will regard this as two tiles, each of length $d = D/2$