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.