Lecture 5: Subgroups, groups of small order

G = group of rotational symmetries of regular hexagon

H = group of isometries of triangle.

Last time we saw that G and H are not isomorphic.

Here is another proof:

If we take any two elements x and y of G, we have $xy = yx$.

However, in H, there exist pairs such that this is not true.

Ex: Use the above observations to show that G and H are not isomorphic.

Theorem Let G and H be groups. Let $\varphi : G \longrightarrow H$ be a group isomorphism. Then, the function $\varphi^{-1} : H \longrightarrow G$ is also a group isomorphism.

Proof: We already know that φ^{-1} is a 1-1 correspondence.

We need to verify that if x, y are in H, then
$\varphi^{-1}(xy) = \varphi^{-1}(x) \cdot \varphi^{-1}(y)$.

To see this, we observe that

$$\varphi(\varphi^{-1}(x) \cdot \varphi^{-1}(y)) = \varphi(\varphi^{-1}(x)) \cdot \varphi(\varphi^{-1}(y)) = xy.$$

But, we also have $\varphi(\varphi^{-1}(xy)) = xy$. As $\varphi^{-1}(xy)$ and $\varphi^{-1}(x) \cdot \varphi^{-1}(y)$ have the same image under φ, they must be equal. This completes the proof.

Subgroups

Let $(G, *)$ be a group. A subgroup of G is a subset $H \subseteq G$ such that $*$ gives a binary operation on H, which gives H the structure of a group.

More precisely, we say that the subset H is a subgroup if the following are true:

(1) 1_G is in H.

(2) x, y in $H \Longrightarrow x * y$ in H

(3) x in $H \Longrightarrow x^{-1}$ in H.

Note that we do not need to check that the binary operation on H is associative as $*$ is known to be associative.

This is why we did not include this condition.

Example

Let A be a subset of the plane. Then, if G is the group of isometries of A, G is a subgroup of $\mathrm{Perm}(A)$.

Example

Let G be any group. Then G is a subgroup of itself. Any subgroup of G that is not equal to the whole of G is called a <u>proper</u> subgroup of G.

Example

Let G be a group and let x be any element of G.

Then, the set

$$\langle x \rangle = \{x^n \mid n \text{ is an integer}\}$$
$$= \{1_G, x, x^{-1}, x^2, x^{-2}, \dots\}$$

is a subgroup of G.

(Check this.)

Example

Let m be any integer.

We define $m\mathbb{Z}$ to be the set of all integer multiples of m.

Then $m\mathbb{Z}$ is a subgroup of $\mathbb{Z}$.

Indeed, any element x of $m\mathbb{Z}$ may be written as $x = md$ for some integer d.

So, $-x = m(-d)$. and so $-x$ is also in $m\mathbb{Z}$.

Let x any y be in $m\mathbb{Z}$

Want to show: $x+y$ is in $m\mathbb{Z}$

There exist integers d_1 and d_2 such that $x = md_1$ and $y = md_2$

So $x + y = md_1 + md_2$

$= m(d_1 + d_2)$.

So $x + y$ is in $m\mathbb{Z}$

<u>Question</u>: Are there any other subgroups of $\mathbb{Z}$?

A test for subgroups

Proposition Let G be group. Let H be a non-empty subset of G. Then H is a subgroup of G if and only if for any x, y in H, the element xy^{-1} is in H.

Proof

Suppose H is a subgroup of G. Let x, y be in H. Then, y^{-1} is in H. So xy^{-1} is in H. Thus the condition in the statement of the proposition holds.

Conversely, suppose we know that for any x, y in H, the element xy^{-1} is in H.

Let x be any element of H. (Recall – H is non-empty).

Thus, $x \cdot x^{-1} = 1_G$ is in H.

__Inverses__ Now, let x be any element of H.

As 1_G and x are in H, so is $1_G \cdot x^{-1} = x^{-1}$.

__Products__ Let x, y be in H.

Then y^{-1} is in H. So $x \cdot (y^{-1})^{-1} = xy$ is in H. Thus H is a subgroup. //

Order of a group.

Definition Let G be a group. The cardinality of the set G (i.e. the number of elements in G) is called the **order** of G.

A **finite group** is a group having finite order.

Finite groups

Let G be a finite group.

Let x be an element of G.

Then, the set

$$\langle x \rangle = \{x^n \mid n \text{ is an integer}\}$$

is a subgroup of G.

Thus, $\langle x \rangle$ is also a finite set.

Let $|G| = r$

In the sequence $1, x, x^2, \ldots x^r$, all elements cannot be distinct.

So, for some positive integers $m < n$, we have $x^m = x^n$.

So $x^{n-m} = 1_G$.

Also $n \leq r \implies n-m \leq r$.

Thus, we have proved the following.

<u>Theorem</u> Let G be a finite group. Then, for any element x of G, there exists a positive integer $d \leqslant |G|$ such that $x^d = 1$.

Groups of small order.

Can we list all groups of order n? (List "up to isomorphism")

We will do this for some small values of n.

$n = 1 \rightsquigarrow$ Easy

$\{1_G\}$ — This is the only group of order 1.

$\underline{n=2.}$

Let G be a group of order 2.

Then, G contains 1_G and some other element x.

We already know $x \cdot 1_G = 1_G \cdot x = x$.

What is x^2 ?

If $x^2 = x$, we can cancel x from both sides to get $x = 1_G$.

But we assumed $x \neq 1_G$

So, $x^2 \neq x$.

So, $x^2 = 1_G$.

So, the multiplication table is

	1	x
1	1	x
x	x	1

Thus, there is only one group of order 2.

$\underline{n=3}$

Let G be a group of order 3.

Let us list the elements.

$\{1, x, y\}$

What is x^2?

$x^2 \neq x$ (by the same argument as before.)

Suppose $x^2 = 1$.

So, $\{1, x^2\}$ is a subgroup of G.

<u>List</u>: 1 x

y

What is yx?

If $yx = 1$, $y = x^{-1}$. But as $x^2 = 1$,

we have $x^{-1} = x$. So $x = y$ — contra.

So $yx \neq 1$.

If $yx = x$, we get $y = 1$

(by cancelling x). But $y \neq 1$ — contra.

So $yx \neq x$.

If $yx = y$, we get $x = 1$

by cancelling y. But $x \neq 1$ — contra.

So yx cannot be defined. — contra.

So $x^2 \neq 1$.

So $x^2 = y$.

So, our list is $\{1, x, x^2\}$.

What is $x \cdot x^2$?

If $x \cdot x^2 = x$, we get $x^2 = 1$ — contra.

If $x \cdot x^2 = x^2$, we get $x = 1$ — contra.

So, $x \cdot x^2 = 1$.

So, there is only one group of order 3.

	1	x	x^2
1	1	x	x^2
x	x	x^2	1
x^2	x^2	1	x

$\underline{n=4}$

Let G have order 4.

Let x be an element of G such that $x \neq 1$.

Let us list the powers of x.

$1, x, x^2, \ldots$

We know that there exists $d \leq 4$ such that $x^d = 1$.

We know that $x \neq 1$.

Suppose $x^2 = 1$.

<u>List</u> $1, \quad x$

$y, \quad z$.

We have already seen that

yx cannot be equal to 1, x or y.

So $yx = z$.

<u>List</u>. $\quad 1 \quad x$

$\quad\quad y \quad yx$.

What is y^2?

$y^2 \neq y$ as $y \neq 1$

If $y^2 = yx$, $y = x$ which is not true.

So we have two case: $y^2 = x$ or

$y^2 = 1$.

<u>Case</u>: $y^2 = x$.

So, the elements are $1, y, y^2, y^3$ (all distinct)

y^4 is some element of this set.

$y^4 = y \Rightarrow y^3 = 1$ — contra.

$y^4 = y^2 \Longrightarrow y^2 = 1$ — contra

$y^4 = y^3 \Longrightarrow y = 1$ — contra.

So $y^4 = 1$.

So, the group is

	1	y	y^2	y^3
1	1	y	y^2	y^3
y	y	y^2	y^3	1
y^2	y^2	y^3	1	y
y^3	y^3	1	y	y^2

<u>Case</u> $y^2 = 1$ <u>List</u>: $1 \quad x$

$y \quad yx$

What is xy?

If $xy = 1$, $y = x^{-1}$.

But $x^2 = 1 \implies x = x^{-1}$.

So $x = y$ — contra.

So, $xy \neq 1$.

If $xy = x$, then $y = 1$ — contra.

If $xy = y$, then $x = 1$ — contra.

So $xy = yx$.

Now we can calculate all products easily.

e.g. $(xy)(xy) = x(yx)y$

$= x(xy)y$

$= x^2 \cdot y^2 = 1.$

	1	x	y	yx
1	1	x	y	yx
x	x	1	yx	y
y	y	yx	1	x.
yx	yx	y	x	1

(Ex: Check this.)

Now we are done with the case $x^2 = 1$.

What if $x^2 \neq 1$, but $x^3 = 1$?

<u>List:</u> $1 \quad x \quad x^2$

y

What is yx?

(This is similar to earlier calculations.)

If $yx = 1$, then $y = x^{-1} = x^2$. — contra.

If $yx = x$, then $y = 1$ — contra

If $yx = x^2$, then $y = x$ — contra.

So yx cannot be defined.

So, $x^3 = 1$ is not possible.

So, we are now left with the case $x^2 \neq 1$, $x^3 \neq 1$, $x^4 = 1$.

<u>List</u>: $1, x, x^2, x^3$.

This gives a group isomorphic to one we already have (in the case $x^2 = 1$, $y^2 = x$ earlier).

So, there are 2 groups of order 4.