Lecture 6

Definition Let G be a group. Let x be an element of G. Let d be the smallest positive integer such that $x^d = 1$, if it exists. Then d is called the order of x.

If there is no positive integer d such that $x^d = 1$, we say that x has infinite order.

The order of x is denoted by $\mathrm{ord}(x)$ or $|x|$.

We have proved the following:

<u>Thm</u> Let G be a finite group. Then, for any $x \in G$, $\mathrm{ord}(x) \leq |G|$.

Find all groups of order n.

$n = 5$.

Let $x \in G$, $x \neq 1$.

Then, $2 \leq \operatorname{ord}(x) \leq 5$.

If $\operatorname{ord}(x) = 2$, let $y \in G$ such that $y \notin \langle x \rangle$.

Partial list:

$1 \quad x$

y

Is yx a new element or is yx in $\{1, x, y\}$?

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

If $yx = x$, $y = 1$ — contra.

If $yx = y$, $x = 1$ — contra.

So, yx is a new element.

Partial list:

$1 \quad x$

$y \quad yx.$

z

$\uparrow$

exists as $|G| = 5$.

Question:

What is zx?

If $zx = 1$, $z = x^{-1} = x$ — contra.

If $zx = x$, $z = 1$ — contra.

If $zx = y$, $z = yx^{-1} = yx$ — contra.

If $zx = yx$, $z = y$ — contra.

If $zx = z$, $x = 1$ — contra.

So zx needs to be a new element.

But $|G| = 5$. — contra.

So $\operatorname{ord}(x) \neq 2$.

Suppose $\operatorname{ord}(x) = 3$.

Partial list: $1 \quad x \quad x^2$

y.

Is yx a new element or is it in $\{1, x, x^2, y\}$?

If $yx = x^n$ for any n,

$y = x^{n-1}$ — contra.

If $yx = y$, $x = 1$ — contra.

So yx is a new element.

<u>List</u>

1	x	x^2
y	yx	

What about yx^2 ?

If $yx^2 = x^n$ for any n,

$y = x^{n-2}$ — contra

If $yx^2 = y$, $x^2 = 1$ — contra.

If $yx^2 = yx$, $x = 1$ — contra.

So yx^2 has to be a

new element. — contra.

So $\mathrm{ord}(x) \neq 3$.

Suppose $\text{ord}(x) = 4$.

<u>List</u> $\quad 1 \quad x \quad x^2 \quad x^3$

$\quad y.$

If $yx = x^n$ for some n,

$y = x^{n-1}$ — contra. (Similary $yx = y$ is not possible.)

So $\text{ord}(x) \neq 4$.

So $\operatorname{ord}(x) = 5$.

$G = \{1, x, x^2, x^3, x^4\}$.

So, there is only one group of order 5 ("up to isomorphism").

Generalizing this pattern.

Let G be a group.

Let $x \in G$ such that

$\mathrm{ord}(x) = d$.

Partial list : $1 \quad x \quad x^2 \quad \cdots \quad x^{d-1}$

Note that these are

distinct elements.

Indeed, suppose $x^i = x^j$ for some $i < j \leq d-1$.

Then $x^{j-i} = 1$.

But $0 < j-i \leq d-1 < d$.

But $d = \operatorname{ord}(x)$ and so $x^{j-i} \neq 1$ — contra.

If $\langle x \rangle = G$, we have listed all elements of G.

Otherwise, suppose y is such that $y \in G$, $y \notin \langle x \rangle$.

Then, we could write the row $y \quad yx \quad \cdots\cdots \quad yx^{d-1}$ below the first one.

1) Are all elements in this row distinct?

Yes. If $yx^i = yx^j$ for $i<j \leq d-1$, we see $x^i = x^j$. But we already know that $1, x, \dots x^{d-1}$ are all distinct.

2) <u>Is there some overlap with the first row</u>?

No. If $x^i = yx^j$ for any i, j, we get $y = x^{j-i}$.
But we are already assuming $y \notin \langle x \rangle$

So, we see that if $G \neq \langle x \rangle$, we can add a complete row $\{y, yx, \ldots, yx^{d-1}\} = y\langle x \rangle$ under the first one.

If this is the complete list of elements of G, we stop.

Otherwise, there is some $z \in G$, such that $z \notin \langle x \rangle$, $z \notin y\langle x \rangle$.

Then, we can try to write the third row containing $\{z, zx, \dots zx^{d-1}\} = z\langle x \rangle$.

By the same argument as before, these are d distinct elements.

No overlaps with first row

If $zx^i = x^j$ for some i, j

then $z = x^{j-i}$. But $z \notin \langle x \rangle$ — contra.

No overlaps with second row

If $zx^i = yx^j$ for some i, j

then $z = yx^{j-i} \in \underline{y\langle x \rangle}$.

— contra.

This process will continue until we exhaust the group. This process will end if $|G|$ is finite. Then we see that d divides $|G|$.

We have proved:

<u>Theorem</u> Let G be a finite group. Then, for any $x \in G$, $\mathrm{ord}(x)$ divides $|G|$.