Document last updated: Thurs, Sep 19 2024

Abstract Algebra Notes

Week 3 Wed, Sep 18 2024

Today & Break before 8pm	**Next week**
Quiz 2	Tue: Hw 03 due by email
Lecture: laws of exponent (w/ induction) cyclic group	Wed: Quiz 3 (Topic: today's group quiz)
Group quiz	

Def A subset of S is called proper if it's not equal to S

Def G group.

The subgroup $\{e\}$ is called the trivial subgroup of G.

A subgroup of G is called proper if it's a proper subset of G.

Ex Let $5\mathbb{Z} \overset{\text{def}}{=} \{5k : k \in \mathbb{Z}\}$ be the set of all multiples of 5.

Then ① $0 \in 5\mathbb{Z}$

② $5\mathbb{Z}$ is closed under $+$: $5k_1 + 5k_2 = 5(k_1 + k_2)$

③ $5\mathbb{Z}$ is closed under taking inverses :

Inverse of $5k$ is $-(5k) = 5(-k) \in 5\mathbb{Z}$

Thus $5\mathbb{Z} \underset{\text{is a subgroup of}}{\leq} \mathbb{Z}$

Prop By the same reasoning, for any fixed $n \in \mathbb{Z}$,

the set $n\mathbb{Z} = \{nk : k \, \mathbb{Z}\}$ of all multiples of n

is also a subgroup of $\mathbb{Z}$.

Ex: Subgroups of $\mathbb{Z}_4 = \{0, 1, 2, 3\}$:

$$\begin{tikzcd}[arrows=dash]
\mathbb{Z}_4 \arrow[d] \\
\{0,2\} \arrow[d] \\
\{0\}
\end{tikzcd}$$

(No other proper subgroup H because
if 1 is in H, then $1, 1+1, 1+1+1, 1+1+1+1=0 \in H$
if 3 is in H, then $3, 3+3=2, 3+3+3=1, 3+3+3+3=0 \in H$)

This is called the subgroup lattice. Writing $\begin{array}{c} G \\ | \\ H \end{array}$ means $H \leq G$

Ex Subgroup lattice of $U(8) = \{1, 3, 5, 7\}$

$$\begin{tikzcd}[arrows=dash]
& U(8) \arrow[dl] \arrow[d] \arrow[dr] & \\
\{1,3\} \arrow[dr] & \{1,5\} \arrow[d] & \{1,7\} \arrow[dl] \\
& \{1\} &
\end{tikzcd}$$

Remark Both $\mathbb{Z}_4$ and $U(10)$ are both groups of order 4,

but we know they are not "the same"

because they have distinct subgroup lattices.

Principle of Well-ordering:

If S is a non-empty subset of the natural numbers $\mathbb{N}$, then S has a least element.

The Principle of Well-ordering is equivalent to the Principle of Mathematical Induction

Principle of Mathematical Induction

Let $P(n)$ be a statement which depends on n

IF :
- $P(n_0)$ is true (base case)
- For every $k \geqslant n_0$, $P(k)$ implies $P(k+1)$ (Inductive step)

THEN $P(n)$ is true for all $n \geqslant n_0$.

$\boxed{\text{Law of exponents}}$ (See Sec 3.2)

Recall $g^n \overset{\text{def}}{=} \underbrace{g \cdots g}_{n \text{ times}}$, $g^{-n} \overset{\text{def}}{=} \underbrace{g^{-1} \cdots g^{-1}}_{n \text{ times}} \overset{\text{def}}{=} (g^{-1})^n$, $g^0 = e$

$\boxed{\text{Thm 1}}$ Let G be a group, $g \in G$.

Then $(g^n)^{-1} = g^{-n}$ for $n \in \mathbb{N}$

Proof We will apply induction on n. (Done during class)

Base case $n=1$: $(g^1)^{-1} = g^{-1} = (g^{-1})^1$ by def.

Inductive step:

Inductive hypothesis

Suppose for some $k \in \mathbb{N}$ that $(g^k)^{-1} \overset{!}{=} g^{-k} \overset{\text{def}}{=} (g^{-1})^k$

(We need to show $(g^{k+1})^{-1} = g^{-(k+1)} \overset{\text{def}}{=} (g^{-1})^{k+1}$)

$(g^{k+1})^{-1} = (g^1 g^k)^{-1}$ by def

$= (g^k)^{-1} g^{-1}$ by "socks-shoes" property of inverses

$= (g^{-1})^k (g^{-1})^1$ by the inductive hypothesis

$= (g^{-1})^{k+1}$ by def

$\square$

$\boxed{\text{Thm 2}}$ Let G be a group, $g \in G$.

Then $g^{m+n} = g^m g^n$ for all $m, n \in \mathbb{Z}$.

Proof (long) Proof idea: Induction on n for $m \in \mathbb{Z}, n \in \mathbb{N}$
Do the case $m \in \mathbb{Z}, n \in \mathbb{Z}_{\leq 0}$ separately

- Case $m \in \mathbb{Z}, n = 0$: $g^{m+0} = g^m e = g^m g^0$ since $g^0 :\overset{\text{def}}{=} e$

- Case $m \in \mathbb{Z}, n \in \mathbb{N}$: We will prove this by induction on n

Base case $n = 1$:

if $m=0$, then $g^{0+1} = eg^1 = g^0 g^1$

if $m > 0$, then $g^{m+1} = \underbrace{g\,g\cdots g}_{m+1 \text{ times}} = g^m g^1$ by def

Also $g^{-m} = \underbrace{(g^{-1})\cdots(g^{-1})}_{m \text{ times}} = (g^{-1})^m$,

so
$$\begin{aligned} g^{-m+1} &= g^{-(m-1)} \\ &= \underbrace{g^{-1} g^{-1} \cdots g^{-1}}_{m-1 \text{ times}} \\ &= \underbrace{g^{-1} g^{-1} \cdots g^{-1}}_{m-1 \text{ times}} g^{-1} g \\ &= (g^{-1})^m g^1 = g^{-m} g^1 \end{aligned}$$

This shows that for all $m \in \mathbb{Z}$, $g^{m+1} = g^m g^1$.

Induction Step

Suppose that for some $k \geq 1$ we have

$g^{m+k} = g^m g^k$. (We need to prove $g^{m+k+1} = g^m g^{k+1}$)

$$\begin{aligned} g^{m+k+1} &= g^{m+k} g^1 && \text{by the base case} \\ &= g^m g^k g^1 && \text{by the inductive hypothesis} \\ &= g^m g^{k+1} && \text{by the base case.} \end{aligned}$$

Thus, by induction,

$\boxed{\text{for all } m \in \mathbb{Z}, \text{ we have } g^{m+n} = g^m g^n \text{ for } n \in \mathbb{N}}$ (*)

- Case $m \in \mathbb{Z}, n < 0$:

We will show $g^{m-n} = g^m g^{-n}$ for any integer $n \geq 1$.

$$g^m = g^{m-n+n}$$
$$= g^{m-n} g^n \quad \text{by } (*)$$

Multiply on the right by g^{-n}:

$$g^m g^{-n} = g^{m-n} g^n g^{-n}$$

$$g^m g^{-n} = g^{m-n} g^n (g^n)^{-1} \quad \text{by above } \boxed{\text{Thm } 1}$$

So $g^m g^{-n} = g^{m-n}$.

This concludes the proof that,

for any $m, n \in \mathbb{Z}$, we have $g^{m+n} = g^m g^n$ $\square$

—— end of proof of Thm 2 ——

$\boxed{\text{Thm 3}}$ Let G be a group, $g \in G$.
Then $(g^m)^n = g^{mn}$ for $m, n \in \mathbb{Z}$

Pf • Case $n=0$ or $m=0$:

If $n=0$, then $(g^m)^n = (g^m)^0 \overset{\text{def}}{=} e \overset{\text{def}}{=} g^0 = g^{m0} = g^{mn}$ for all $m \in \mathbb{Z}$ ✓

Similar argument for when $m=0$

• case $m \in \mathbb{Z}$, $n \in \mathbb{N}$:

We will prove this by induction on n.

Base case $n=1$: For all $m \in \mathbb{Z}$, $(g^m)^1 = g^m = g^{m \cdot 1}$

Induction Step

Suppose that for some $k \geq 1$ we have

$(g^m)^k = g^{mk}$. (We need to prove $(g^m)^{(k+1)} = g^{m(k+1)}$)

Then $(g^m)^{k+1} = (g^m)^k (g^m)^1$ by $\boxed{\text{Thm 2}}$

$= g^{mk} g^m$ by the inductive hypothesis

$= g^{mk+m}$ by $\boxed{\text{Thm 2}}$

$= g^{m(k+1)}$

Thus, by induction, for any $m \in \mathbb{Z}$ and $n \in \mathbb{N}$, $(g^m)^n = g^{mn}$

- Case first exponent is positive, second exponent is negative:

Assume $m, n > 0$. Then

$$\begin{aligned}
\big(\overset{\text{pos}}{g^{m}}\big)^{\overset{\text{neg}}{-n}} &= \left(\left(g^{m}\right)^{n}\right)^{-1} && \text{by } \boxed{\text{Thm 1}} \\
&= \left(g^{mn}\right)^{-1} && \text{by}
\end{aligned}$$

$$\begin{aligned}
&= g^{-mn} && \text{by } \boxed{\text{Thm 1}} \\
&= g^{m(-n)}
\end{aligned}$$

- Case both exponents are negative:

Assume $m, n \geqslant 1$.

Note that, for any $h \in G$ and $s \in \mathbb{N}$,

$$\left(h^{s}\right)^{-1} \underset{\boxed{\text{Thm 1}}}{=} h^{-s} = \left(h^{-1}\right)^{s}$$

Then
$$\begin{aligned}
\left(g^{-m}\right)^{-n} &= \left(\left(g^{-1}\right)^{m}\right)^{-n} \\
&= \left(\left(\left(g^{-1}\right)^{m}\right)^{-1}\right)^{n} \\
&= \left(\left(\left(g^{-1}\right)^{-1}\right)^{m}\right)^{n} \\
&= \left(g^{m}\right)^{n} && \text{by "socks-shoes property" } \left(g^{-1}\right)^{-1} = g \\
&= g^{mn} && \text{by}
\end{aligned}$$

—— end of proof of Thm 3 ——

Warning: $(xy)^k$ need not equal $x^k y^k$ in a non-abelian group

Cyclic groups (See Sec 4.1)

Def G group, $x \in G$

$$\langle x \rangle \overset{\text{def}}{=} \{x^k : k \in \mathbb{Z}\}$$

If the group operation is additive, write $\langle x \rangle = \{kx : k \in \mathbb{Z}\}$

Ex $G = \mathbb{Z}$, $\langle 1 \rangle = \mathbb{Z} = \langle -1 \rangle$,

$\langle 5 \rangle = \{5k : k \in \mathbb{Z}\} = \langle -5 \rangle$

$G = \mathbb{Z}_8$, $\langle 1 \rangle = \mathbb{Z}_8 = \langle 3 \rangle$

$\langle 2 \rangle = \{0, 2, 4, 6\}$

$\langle 4 \rangle = \{0, 4\}$

$G = U(10)$ $\langle 1 \rangle = \{1\}$

$\langle 3 \rangle = \{1, 3\}$

$\langle 7 \rangle = \{1, 7\}$

$\langle 9 \rangle = \{1, 9\}$

Thm $\langle x \rangle$ is a subgroup of G

Pf 1. $e = x^0 \in \langle x \rangle$

2. If $y, z \in \langle x \rangle$, then $y = x^m$ and $z = x^n$ for some $m, n \in \mathbb{Z}$

Thus $yz = x^m x^n = x^{m+n}$, so $yz \in \langle x \rangle$

3. If $y \in \langle x \rangle$, then $y = x^m$ for some $m \in \mathbb{Z}$

Then $y^{-1} = (x^m)^{-1} = x^{-m}$ by $\boxed{\text{Thm 1}}$ above

so $y^{-1} \in \langle x \rangle$.

Thus $\langle x \rangle \leq G$. $\square$

Thm $\langle x\rangle$ is the smallest subgroup of G containing x,

meaning: if $H \leq G$ and $x \in H$ then $\langle x\rangle \leq H$.

Proof Suppose $x \in H$ for some subgroup $H \leq G$.

We need to show $x^k \in H$ for all $k \in \mathbb{Z}$.

$k=0$: $x^0 = e \in H$ (by requirement that H contains the identity)

$k \in \mathbb{N}$: $x^k = \underbrace{x\,x \cdots x}_{k \text{ times}} \in H$ (since H is closed under the group operation)

$k=-1$: $x^{-1} \in H$ (Since H contains the inverse of each $h \in H$)

$k \in \mathbb{Z}_{\leq -1}$: $x^{-k} \underset{\boxed{\text{Thm 1}}}{=} (a^{-1})^k = \underbrace{a^{-1} \cdots a^{-1}}_{k} \in H$ (again by closure)

Therefore $\langle x\rangle = \{x^k : k \in \mathbb{Z}\} \leq H$. $\square$

Def $\langle x\rangle$ is called the cyclic subgroup of G generated by x.

Def A group G is called a cyclic group if $G = \langle x\rangle$ for some $x \in G$, and x is called a generator of G.

Ex $\mathbb{Z}$ is cyclic, 1 is a generator.
-1 is also a generator

$\langle 1\rangle = \mathbb{Z} = \langle -1\rangle$

Ex $\mathbb{Z}_{12}$ is cyclic, 1 is a generator.
Other possible generators are $5, 7, 11$

In fact, every $\mathbb{Z}_n$ is cyclic.

Ex $U(8)$ is not cyclic. We saw $\langle x\rangle \neq U(8)$ for all $x \in U(8)$.

From earlier: $\langle 1\rangle = \{1\}$ $\quad$ $\langle 5\rangle = \{1,5\}$

$\langle 3\rangle = \{1,3\}$ $\quad$ $\langle 7\rangle = \{1,7\}$

Ex $U(9) = \{1, 2, 4, 5, 7, 8\}$ is cyclic.

2 is a generator:

$$\begin{tikzcd} 1 \arrow[r, "\times 2"] & 2 \arrow[r, "\times 2"] & 4 \arrow[r, "\times 2"] & 8 \arrow[r, "\times 2"] & 7 \arrow[r, "\times 2"] & 5 \arrow[lllll, bend left, "\times 2"] \end{tikzcd}$$

This is a Cayley graph for $U(9)$

($U(5) = \{1,2,3,4\}$ from today's quiz is also cyclic.
2 is a generator:

$$\begin{tikzcd} 1 \arrow[r, "\times 2"] & 2 \arrow[r, "\times 2"] & 4 \arrow[r, "\times 2"] & 3 \arrow[lll, bend left, "\times 2"] \end{tikzcd}$$

This is a Cayley graph for $U(5)$)

<u>Fact / Def</u> Any cyclic group $\langle x \rangle$ has Cayley graph

$$\begin{tikzcd} e \arrow[r, "x"] & x \arrow[r, "x"] & x^2 \arrow[r, "x"] & x^3 \arrow[r] & \cdots\ x^{n-1} \arrow[llll, bend left, "x"] \end{tikzcd} \quad \text{if } \underbrace{|x|}_{\text{"order of } x\text{"}} = n$$

and

$$\cdots \longrightarrow x^{-1} \xrightarrow{x} e \xrightarrow{x} x \xrightarrow{x} x^2 \xrightarrow{x} x^3 \longrightarrow \cdots \quad \text{if } x \text{ has infinite order}$$

Ex $\mathbb{Z}_4 = \langle 1 \rangle$

$$\begin{tikzcd} 0 \arrow[r, "+1"] & 1 \arrow[r, "+1"] & 2 \arrow[r, "+1"] & 3 \arrow[lll, bend left, "+1"] \end{tikzcd}$$

Ex $\mathbb{Z}_n = \langle 1 \rangle$

$$\begin{tikzcd} 0 \arrow[r, "+1"] & 1 \arrow[r, "+1"] & \cdots \arrow[r, "+1"] & n-1 \arrow[lll, bend left] \end{tikzcd}$$

Ex $\mathbb{Z} = \langle 1 \rangle$ $\quad \cdots \rightarrow -2 \xrightarrow{+1} -1 \xrightarrow{+1} 0 \xrightarrow{+1} 1 \xrightarrow{+1} 2 \xrightarrow{+1} 3 \rightarrow \cdots$

<u>Remark</u>

- If $|x| = n$, $\langle x \rangle$ has a Cayley graph that is the same as a Cayley graph of $\mathbb{Z}_n$, so $\langle x \rangle$ is "the same" as $\mathbb{Z}_n$.
- If $|x| = \infty$, $\langle x \rangle$ has a Cayley graph that is the same as a Cayley graph of $\mathbb{Z}$, so $\langle x \rangle$ is "the same" as $\mathbb{Z}$.
- Properties about $\mathbb{Z}_n$ and $\mathbb{Z}$ hold for any cyclic group:

- Every cyclic group is abelian
- If $|x| = n \in \mathbb{N}$, then $e, x, x^2, \dots, x^{n-1}$ are distinct elements of G (no two powers in this list are equal) and $x^i = x^j$ iff $n \mid (i-j)$
- If $|x| = \infty$, then for all $k, l \in \mathbb{Z}$, if $k \neq l$ then $a^k \neq a^l$.
- If $G = \langle x \rangle$ is a cyclic group w/ generator x, then $\underbrace{|G|}_{\text{order / cardinality of } G} = |x|$

Corollary If G is a finite group, then $|x| \leq |G|$ for all $x \in G$. $|x| = |G|$ iff $G = \langle x \rangle$.

Pf $\langle x \rangle$ is a subset of G, and above we wrote that the cardinality of $\langle x \rangle$ is $|x|$. $\square$

Ex Let R be Counterclockwise rotation by $90°$

Then $\langle R \rangle = \{ R, \underbrace{R^2}_{\text{Rotation } 180°}, \underbrace{R^3}_{\text{Rotation } 270°}, Id \}$ is the same as $\mathbb{Z}_4$

Ex Let R be Counterclockwise rotation by $\sqrt{2}$

Then $\langle R \rangle = \{ \dots, R^{-2}, R^{-1}, Id, R, R^2, R^3, \dots \}$ because there are no k, l such that $k\sqrt{2} = l\, 360$, and $\langle R \rangle$ is the same group as $\mathbb{Z}$

sigma cycle notation

Ex Let $\sigma = (1\ 2\ 6\ 5)(3)(4)$ be a permutation in S_6.

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 3 & 4 & 1 & 5 \end{bmatrix}$$

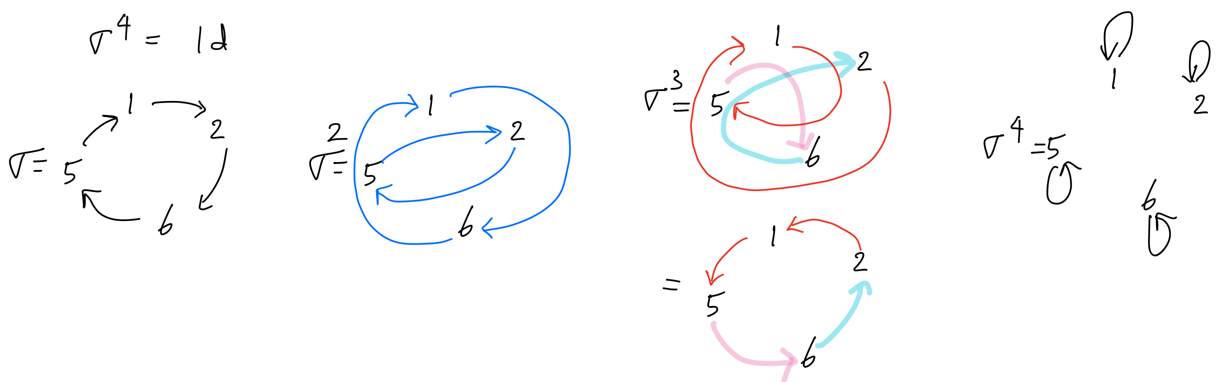
two-row notation

Read from right to left

$\sigma^2 = (1\ 2\ 6\ 5)\ (1\ 2\ 6\ 5) = (1\ 6)(2\ 5)$

$\sigma^3 = \sigma^2\sigma = (16)(25)\ (1\ 2\ 6\ 5) = (1\ 5\ 6\ 2)$

$\sigma^4 = \mathrm{Id}$



Then $\langle\sigma\rangle = \{(1265),\ (16)(25),\ (1562),\ \mathrm{Id}\}$
$= \{\ \sigma,\ \ \sigma^2\ ,\ \sigma^3,\ e\}$, the same group as $\mathbb{Z}_4$

Ex Let $\sigma = (126)(45) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 6 & 3 & 5 & 4 & 1 & 7 \end{bmatrix}$ in S_7

Group Quiz Exercise: find $\langle\sigma\rangle$

$\sigma^2 = (126)(45)(126)(45) = (162)$

$\sigma^3 = \underbrace{(162)}_{\sigma^2}\ \underbrace{(126)(45)}_{\sigma} = (45)$ Note: $(126)^{-1} = (162)$

$\sigma^4 = \underbrace{(45)}_{\sigma^3}\underbrace{(126)(45)}_{\sigma} = (126)$

$\sigma^5 = (126)(126)(45) = (162)(45)$

$\sigma^6 = (162)(45)(126)(45) = \mathrm{Id}$

Then $\langle\sigma\rangle = \{\sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5, \mathrm{Id}\}$, the same group as $\mathbb{Z}_6$

(Extra notes)

Thm Every subgroup of a cyclic group is cyclic.

Ex Subgroup lattice

$$\begin{tikzcd}[row sep=small]
\mathbb{Z}_4 = \{0,1,2,3\} \arrow[d, dash] \\
\langle 2 \rangle = \{0,2\} \arrow[d, dash] \\
\langle 0 \rangle = \{0\}
\end{tikzcd}
\qquad
\begin{tikzcd}[row sep=small]
\{\mathrm{Id}, \underset{\sigma}{(1265)}, \underset{\sigma^2}{(16)(25)}, \underset{\sigma^3}{(1562)}\} = \langle \sigma \rangle \arrow[d, dash] \\
\langle \sigma^2 \rangle = \{\mathrm{Id}, (16)(25)\} \arrow[d, dash] \\
\langle \mathrm{Id} \rangle - \{\mathrm{Id}\}
\end{tikzcd}$$

Ex

$$\begin{tikzcd}
& \mathbb{Z}_6 = \{0,1,2,3,4,5\} = \langle 1 \rangle = \langle 5 \rangle \arrow[dl, dash] \arrow[dr, dash] & \\
\langle 4 \rangle = \langle 2 \rangle = \{0,2,4\} \arrow[dr, dash] & & \{0,3\} = \langle 3 \rangle \arrow[dl, dash] \\
& \langle 0 \rangle = \{0\} &
\end{tikzcd}$$

Note

$\langle 2 \rangle = \langle 4 \rangle$ is a cyclic group of order three, so it is the same as $\mathbb{Z}_3$

$\langle 3 \rangle =$ ——— " ——— two, so it is the same as $\mathbb{Z}_2$

Ex The subgroups of $\mathbb{Z}$ are exactly $n\mathbb{Z}$ for $n = 0, 1, 2, \ldots$

Thm (Division algorithm)

Let $a, b \in \mathbb{Z}$ w/ $b > 0$. Then there exist unique integers q and r such that

$$a = bq + r$$

where $0 \leq r < b$

Proof (that every subgroup of a cyclic group is cyclic): (Extra notes)

Let $G = \langle x \rangle$ be a cyclic group w/ generator x.

Suppose H is a subgroup of G.

Case 1: H is the trivial subgroup $\{e\}$.

Then $H = \langle e \rangle$ is cyclic

Case 2: H is non trivial.

- So H contains some elt g not the identity.
- Then $g = x^n$ for some $n \in \mathbb{Z}_{\neq 0}$
- Since a subgroup is closed under taking inverses, $g^{-1} = x^{-n}$ must also be in H.
- Since either n or $-n$ is positive, H must contain some positive power of x.
- Let m be the smallest positive integer such that $x^m \in H$. (Such an m exists by the Principle of well-ordering.)

(Extra notes)

- **Claim** $H = \langle x^m \rangle$

Proof of claim

- Since $x^m \in H$, we know $\langle x^m \rangle \leq H$

of "the subgroup generated by x^m"
("the smallest subgroup of H containing x^m")

- Next, we will prove $H \leq \langle x^m \rangle$:

Let $h \in H$. Since $H \leq G = \langle x \rangle$, we have $h = x^k$ for some $k \in \mathbb{Z}$

- By the division algorithm, there are $q, r \in \mathbb{Z}$ with $0 \leq r < m$ such that $k = mq + r$.

- Thus $h = x^k = x^{mq+r} = x^{mq} x^r$ by $\boxed{\text{Thm } 2}$

- Multiply $x^k = x^{mq} x^r$ on the left by x^{-mq}:

$$x^{-mq} x^k = x^r$$

- So $x^r = x^{-mq} x^k \overset{\text{by } \boxed{\text{Thm } 3}}{=} (x^m)^{-q} x^k$ is in H,

since $x^k = h \in H$ (by assumption) and $x^m \in H$ (by).

- We said earlier that m is the smallest positive integer such that $x^m \in H$.

- Since $0 \leq r < m$, we must have $r = 0$.

- Thus $k = mq$, and $h = x^k = x^{mq} = (x^m)^q \in \langle x^m \rangle$.

- This proves $H \leq \langle x^m \rangle$.

— the end of proof —

(Extra notes)

Thm Let G be a group (not necessarily cyclic),

Let $x \in G$ be of order n.

If $k \in \mathbb{N}$, $\langle x^k \rangle = \langle x^{\gcd(n,k)} \rangle$

and $|x^k| = \dfrac{n}{\gcd(n,k)}$

In particular,

- $\langle x \rangle = \langle x^j \rangle$ iff $\gcd(n,j) = 1$
- In $\mathbb{Z}_n$, $\langle 1 \rangle = \langle j \rangle$ iff $\gcd(n,j) = 1$

Cor The order of an elt of a finite cyclic group divides the order of the group.

Pf Let n be the order of x.

An elt of $\langle x \rangle$ is of the form x^k,

so its order is $\dfrac{n}{\gcd(n,k)}$ $\square$

Ex $\mathbb{Z}_{30} = \{0, 1, \ldots, 29\} = \langle 1 \rangle = \langle 7 \rangle = \langle 11 \rangle = \ldots = \langle 29 \rangle$

Order of $\mathbb{Z}_{30}$ is 30.

Elt 20 has order $\dfrac{30}{\gcd(30,20)} = \dfrac{30}{10} = 3$

Elt 4 has order $\dfrac{30}{\gcd(30,4)} = \dfrac{30}{2} = 15$

Thm For each positive divisor k of n, the set $\langle \frac{n}{k} \rangle$ is the unique subgroup of $\mathbb{Z}_n$ of order k. These are the only subgroups of $\mathbb{Z}_n$.

Ex Subgroup lattice for $\mathbb{Z}_{30}$: