Feb9

Monday, February 8, 2021 10:39 PM

Defn G a group $H \subseteq G$ a subset.
H is a subgroup $H \leq G$ if

① $x, y \in H, \Rightarrow xy \in H$ Closure under mult

$\rightsquigarrow$ ② $x \in H, \Rightarrow x^{-1} \in H$ " " inversion.

WARNING
① is not enough, as we saw

$$(\mathbb{Z}_{\geq 0}, +) \subseteq (\mathbb{Z}, +)$$

↑ not a group

Exercise
If $H \subseteq G$ If $|H| < \infty$ & H closed under mult $\Longrightarrow H \leq G$.

Subgroups generated by one element

G a group. $x \in G$. I can form a subgroup

$$\langle x \rangle = \{ \ldots, x^{-2}, x^{-1}, 1, x, x^2, x^3, x^4, \ldots \}$$

$$= \{ x^n \mid n \in \mathbb{Z} \}$$

This is called the subgroup gen'd by x

It's a group

① $x^a \cdot x^b = x^{a+b} \in \langle x \rangle$

② $(x^a)^{-1} = x^{-a} \in \langle x \rangle$

Example

$$\{r^i\} = R \leq D_{2n}$$

$$\{\ldots, \overset{r^{n-1}}{\overset{\parallel}{r^{-1}}}, \boxed{1, r, r^2, r^3, \ldots, r^{n-1}}, \overset{1}{\overset{\parallel}{r^n}}, \overset{r}{\overset{\parallel}{r^{n+1}}}, \ldots\}$$

$$= \langle r \rangle$$

Saw $R \simeq \mathbb{Z}/n\mathbb{Z}$.

This analogy goes further

$x \in G$. $\langle x \rangle$ ← Always look like something we understand ($\mathbb{Z}$, or $\mathbb{Z}/n\mathbb{Z}$)

Def^n A group H is called a cyclic group if is generated by 1 element.

$$H = \langle x \rangle = \{ x^n \mid n \in \mathbb{Z} \}$$

x is called a generator for H.

Ex * $R = \langle r \rangle$

* $\mathbb{Z} = \langle 1 \rangle = \{ n \cdot 1 \mid n \in \mathbb{Z} \}$

$= \langle -1 \rangle \leftarrow$

* $\mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \rangle$

$= \{ \bar{1}, \bar{2}, \bar{3}, \dots, \overline{n-1}, \bar{n} = \bar{0} \}$.

Observations

① Generators may not be unique.

Exercise $H = \langle x \rangle \implies H = \langle x^{-1} \rangle$

② A cyclic group is abelian.

Pf/ $\alpha, \beta \in H = \langle x \rangle$

$\rightsquigarrow \alpha = x^a \qquad \beta = x^b$

$$\begin{aligned} \alpha\beta &= x^a \cdot x^b \\ &= x^{a+b} \\ &= x^{b+a} \\ &= x^b x^a \\ &= \beta\alpha \end{aligned}$$

UPSHOT G not abelian. any $x \in G$ gives $\langle x \rangle \leq G$ which is.

"each $x \in G$ is in an abelian subgroup"

HW2 #8(c) $|x| = n$ $x^a = x^b \iff a \equiv b \mod n$

Lemma $H = \langle x \rangle$. Then $|H| = |x|$

① If $|x| = n$

Then $H = \{1, x, x^2, \dots, x^{n-1}\}$

② If $|x| = \infty$

$\longrightarrow$ $\Longrightarrow x^a = x^b \iff a = b.$

Pf/ ① All $1, \dots, x^{n-1}$ distinct. $\leftarrow$ HW 2 #8

x^a any a. divide $a = nq + r$
$0 \leq r < n$

$\Longrightarrow x^a = x^r \in \{1, x, \dots x^{n-1}\}$ ✓

② $x^a = x^b$ $b \geq a$.

$x^{b-a} = 1$ but $|x| = \infty$

$\Longrightarrow b - a = 0$ $\varnothing$

Corollary to HW2 #8

If $|x| = n$.

Then $x^a = 1 \iff n \mid a$.

Theorem

Any 2 cyclic groups of the same order are isomorphic.

1) $\langle x \rangle, \langle y \rangle$ cyclic order n.

$$\begin{aligned} \phi : \langle x \rangle &\longrightarrow \langle y \rangle \\ x^k &\longmapsto y^k \end{aligned}$$

is an iso.

2) If $\langle x \rangle$ is infinite

$$\begin{aligned} \phi : \mathbb{Z} &\longrightarrow \langle x \rangle \\ k &\longmapsto x^k \end{aligned}$$

is an iso.

Proof

Well defined

HW2

$$\begin{aligned} x^k = x^l &\iff k \equiv l \mod n \\ &\iff y^k = y^l \\ &\iff \underline{\phi(x^k) = \phi(x^l)}. \end{aligned}$$

Also proves injective.

$\Longrightarrow$ Bijective (HW1 #5 b/c they are finite)

(also surjectivity is easy)

Homom

$$\phi(x^a x^b) = \phi(x^{a+b}) = y^{a+b} = y^a y^b = \phi(x^a)\phi(x^b) \quad \checkmark$$

② $$\begin{tikzcd} \mathbb{Z} \arrow[r] & \langle x \rangle \\ k \arrow[r, mapsto] & x^k . \end{tikzcd}$$

Hom: $x^{k+l} = x^k x^l$ ✓

Surj $x^k = \phi(k)$ ✓

Inj Lemma (2). ∅

Rmk $\mathbb{Z}/n\mathbb{Z}$ is cyclic of order n.

So if $\langle x \rangle$ is " " "

$$\begin{tikzcd} \mathbb{Z}/n\mathbb{Z} \arrow[r, "\simeq"] & \langle x \rangle \\ \bar{k} \arrow[r, mapsto] \arrow[u] & x^k \arrow[u] \end{tikzcd}$$

Def^n Cyclic group of order n is

$$\mathbb{Z}_n = \langle x \mid x^n = 1 \rangle$$

sometimes called C_n

Upshot G random group. $x \in G$.

$x \in \langle x \rangle \leq G$ iso to

↑ is cyclic. either $\mathbb{Z}_n$ or $\mathbb{Z}$

we know a lot about these groups...

What do we know about cyclic groups?

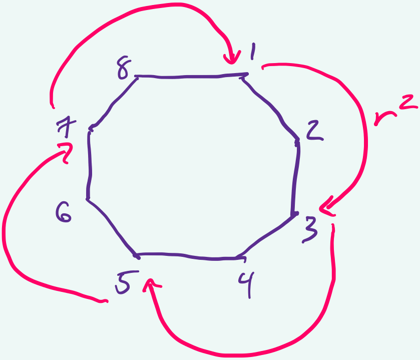
- * What are its subgroups.
- * Given some element, what is its order? ✓
- * What are its generators? ✓

Example

D_{16} = syms of octogon $\geq \langle r \rangle = R$

$$\langle r \rangle = \{1, r, r^2, \dots, r^7\}$$

$r^2 \in \langle r \rangle$, $r^3 \in \langle r \rangle$



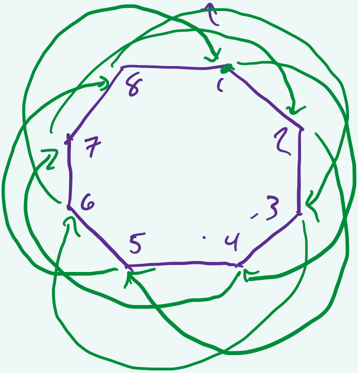
$\langle r^2 \rangle = \{r^2, r^4, r^6, 1\}$

$|\langle r \rangle| = 8$

$|\langle r^2 \rangle| = 4$

Are there other generators of r?

$r^7 = r^{-1}$ is one



$$\langle r^3 \rangle$$
$$\shortparallel$$
$$\{r^3, r^6, \overset{r}{\overset{\shortparallel}{r^9}}, r^4, r^7, \overset{r^2}{\overset{\shortparallel}{r^{10}}}, r^5, \overset{1}{\overset{\shortparallel}{r^8}}\}$$
$$\shortparallel$$
$$R.$$

r^3 not r or r^{-1}
but still gens r.

4 generators for R

check

$$\langle \underset{\uparrow}{r} \rangle = \langle \underset{\uparrow}{r^3} \rangle = \langle \underset{\uparrow}{r^5} \rangle = \langle \underset{\uparrow}{r^7} \rangle$$

Lemma G a group. $x, y \in G$.
If $x \in \langle y \rangle$ and $y \in \langle x \rangle$.
Then $\langle x \rangle = \langle y \rangle$.

Proof We will show $\langle x \rangle \leq \langle y \rangle$. Reverse inclusion symmetric.

$$x \in \langle y \rangle$$
$$\shortparallel$$
$$x = g^k$$

Random elt of $\langle x \rangle \ni x^a$

$$x^a = (g^k)^a = g^{ka} \in \langle y \rangle$$

$\rightsquigarrow$ $\langle x \rangle \leq \langle y \rangle$.

Showed

If $x \in \langle y \rangle \rightsquigarrow \langle x \rangle \le \langle y \rangle$.

Exercise $H \le G$ $x \in G$.

If $x \in H \Longrightarrow \langle x \rangle \le H$.

Prop* $x \in G$. $|x| = n$. $a \neq 0$. $a \in \mathbb{Z}$.

Let $d = \gcd(a,n)$.

$$\langle \underset{\uparrow}{x^a} \rangle = \langle \underset{\uparrow}{x^d} \rangle.$$

Proof

$d \mid a \Longrightarrow x^a = (x^{dk}) = (x^d)^k \in \langle x^d \rangle$

On other hand know $\exists$ $u, v \in \mathbb{Z}$ s.t.

$$d = au + nv$$

$$x^d = x^{au+nv} = x^{au} \cdot \cancel{x^{nv}}^{1}$$

$$= (x^a)^u \in \langle x^a \rangle$$

Lemma $\Longrightarrow \langle x^a \rangle = \langle x^d \rangle$.

Corollary $x \in G$. $|x| = n$. $a \in \mathbb{Z} \setminus \{0\}$

$\gcd(a,n) = d$.

$$|x^a| = \frac{n}{d}$$

Proof

$$|x^a| = |\langle x^a \rangle| = |\langle x^d \rangle| = n/d$$

$$\langle x^d \rangle = \{ x^d, d^{2d}, x^{3d}, \dots, x^{(\frac{n}{d}-1)d}, \overset{1}{\cancel{x^{\frac{n}{d}d}}} \}$$

↑ n/d elements. ∅

Corollary

Let $H = \langle x \rangle$ order n.

x^a generates $H \Longleftrightarrow \gcd(a,n) = 1$.

Pf/ $\Longleftarrow$ Prop

$\Longrightarrow \gcd(a,n) = 1 \Longrightarrow |\langle x^a \rangle| = n$

so has to be all of H ∅

Example

$\mathbb{Z}/12\mathbb{Z}$

generatos are $\{ \bar{a} \mid \gcd(a,12) = 1 \}$

$= \{ \bar{1}, \bar{5}, \bar{7}, \overline{11} \} \underset{set}{=} (\mathbb{Z}/12\mathbb{Z})^\times$

$$|\bar{8}| = \frac{12}{\gcd(8,12)} = \frac{12}{4} = 3$$

$2 \cdot \bar{8} = \overline{16} = \bar{4} \neq \bar{0}$

$3 \cdot \bar{8} = \overline{24} = \bar{0}$ ✓

Notice

We computed all of the cyclic subgroups of $H = \langle x \rangle$ cyclic group of order n.

$= \langle x^{\gcd(n,a)} \rangle$

$$\left\{ \begin{matrix} \text{Cyclic Subs} \\ \text{of } H \end{matrix} \right\} = \{ \langle x^a \rangle \mid a \in \mathbb{Z} \}$$

$$= \{ \underbrace{\langle x^d \rangle}_{} \mid d \mid n \}$$

Order of this subgroup is n/d.

Summarize

H has a unique cyclic subgroup of order n/d for each d dividing n. Fact That's all of them!!

Theorem

A subgroup of a cyclic group H is cyclic.

Proof $K \leq H = \langle x \rangle$ If $K = \{1\}$ we win.

Otherwise.

Let $a = \min\{k > 0 \text{ s.t. } x^k \in K\}$

Claim $K = \langle x^a \rangle$.

Suppose not. $\exists\ x^b \in K$ w/ $\underline{\underline{a \nmid b}}$

(replacing b w/ $-b$ we may assum $b > 0$)

Division $b = aq + r \leftarrow \quad 0 < r < a$

1) $x^b \in K$

2) $x^{aq} \in K \Longrightarrow a^{-aq} \in K$

↑ closure undr ·

↑ closure under inv.

3) $\underset{\substack{\| \\ x^r}}{x^{b-aq}} \in K$

Contradicts minimality of a.

So $a \mid b \quad \forall\ b$ w/ $x^b \in K$

$\Longrightarrow \langle x^a \rangle = K$ ∅

Examples

① Subgroups of $\mathbb{Z}$ are $n\mathbb{Z}$ (multiples of n).

② $R \leq D_{12}$

$\langle r \rangle \leftarrow$ order 6.

$\langle r^4 \rangle = \langle r^2 \rangle = \{1, r^2, r^4\} \leftarrow$ order 3

$\langle r^3 \rangle = \{1, r^3\} \longleftarrow$ order 2

③ Subs of $\mathbb{Z}/12\mathbb{Z}$

(a) $\mathbb{Z}/12\mathbb{Z} = \langle \bar{1} \rangle = \langle \bar{5} \rangle = \langle \bar{7} \rangle = \langle \overline{11} \rangle$ order 12

(b) $\langle \bar{2} \rangle$ order 6 $= \langle \overline{10} \rangle$

(c) $\langle \bar{3} \rangle$ Order 4 $= \langle \bar{9} \rangle$

$\longrightarrow$ (d) $\langle \bar{4} \rangle$ order 3 $= \langle \bar{8} \rangle$

(e) $\langle \bar{6} \rangle$ order 2

(f) $\langle \bar{0} \rangle$

Can I order subgroups of $\mathbb{Z}/12$ wrt inclusion.

$\langle \bar{2} \rangle \longleftarrow$ cyclic order 6.

Have a subgroup $A \leq \langle \bar{2} \rangle$ order 3

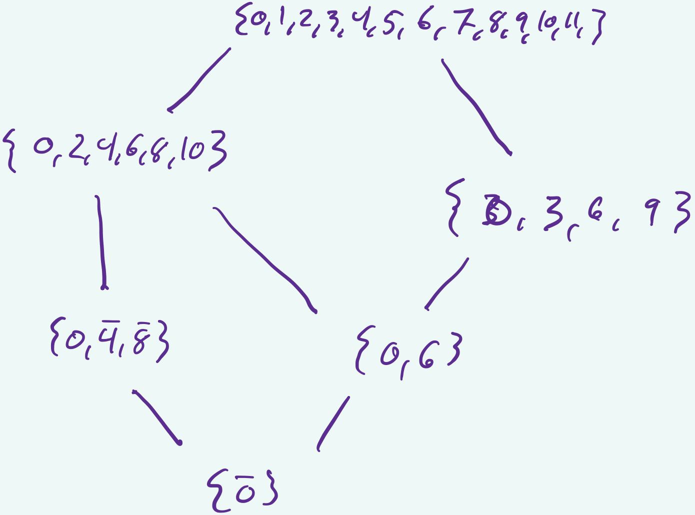
$$\underset{\substack{\uparrow \\ \text{order } 3}}{A} \leq \langle \bar{2} \rangle \leq \mathbb{Z}/12\mathbb{Z}$$

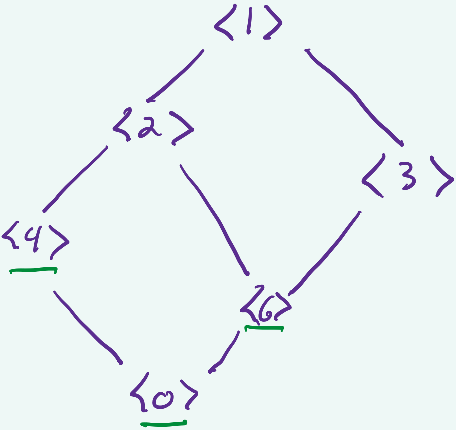
$\Longrightarrow A = \langle 4 \rangle.$

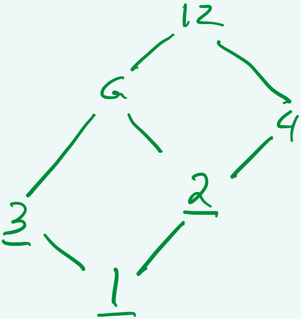
Similarly $B \leq \langle \bar{2} \rangle$ order 2 b/c $2 \mid 6$

$\Longrightarrow B = \langle \bar{6} \rangle$

Lattice of subgroups







Summarize

$$\left\{\begin{matrix}\text{Subgroups of } \mathbb{Z}_n \\ \text{ordered by} \\ \text{inclusion}\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{Divisors of } n \\ \text{ordered by "divides"}\end{matrix}\right\}$$

$$K_d = \langle x^{n/d} \rangle \longleftrightarrow d$$

check

$$K_d \leq K_{d'} \longleftrightarrow d \mid d'$$

Exercise Work this out carefully.

Upshot

- * Pinned down the structure of $\mathbb{Z}_n$ completely in terms of the divisors of n.
- * Lots of cyclic groups running around in G.

Corollary (Lagrange's Theorem for Cyclic groups)

H finite cyclic group

$K \leq H$ a subgroup

$$|K| \mid |H|.$$

Example p prime.

The only subgroups of $\mathbb{Z}_p$ are $\{1\}$ & $\mathbb{Z}_p$.

Next Time

- Saw $\langle x \rangle \leq G$ generated by one element.
- why not multiple elts?

$x, y \in G$

$$\langle x, y \rangle \leq G$$

$$\uparrow \{x^2, xy, \overbrace{x^5 y x^{-1} y^3 x y^{-3}}^{\text{words get long.}}, \dots\}$$

Pinning this down trickier.

Saw $\underset{\uparrow}{x} \in \underset{\uparrow}{H} \leq G \implies \underline{\underline{\langle x \rangle}} \leq H$

Use this to get a cleaner def^n of $\langle x, y \rangle$