From last time:

Group is a set w/ a binary op $\cdot : G\times G \to G$ which is associative, has identity, inverses.

$(G,\cdot)$

S_n = permutation group

$= S_{\{1,\dots,n\}}$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

matrix rep: $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

$GL_n(\mathbb{R})$ $\quad$ $GL(V)$ $\leftarrow$ vector space

invertible/nonsingular linear transformations

<u>Def</u> If G is a group, $H\subset G$ a subset, we say that H is a subgroup of G if

1) $a,b\in H \Rightarrow ab\in H$
2) $e\in H$ $\qquad$ e = identity element
3) $a\in H \Rightarrow a^{-1}\in H$

Notice if H is a subgroup of G then H is a group w/ operation in G restricted to H

Notation $H < G$ to mean H is a subgroup.

Ex: $\mathbb{C}^+$ = additive group of complex numbers

$\mathbb{C}^\times$ = multiplicative group of nonzero complex #s.

$= \{z \in \mathbb{C} \mid z \neq 0\}$

$\mathbb{R}^+, \mathbb{R}^\times$ similarly

$\mathbb{R}^\times < \mathbb{C}^\times$

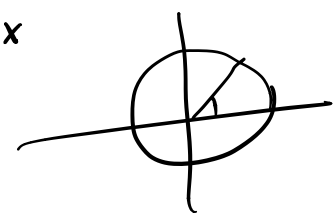
$\mathbb{R}^+ < \mathbb{C}^+$

$\{\pm 1\} < \mathbb{R}^\times < \mathbb{C}^\times$

$\mathbb{Z}^+ < \mathbb{R}^+$

$S^1 = \{z \in \mathbb{C} \mid |z| = 1\} < \mathbb{C}^\times$

$\{x+iy \mid x^2+y^2 = 1\}$



$\mathbb{Z}^+ \leftarrow$ super important group

def if $b \in \mathbb{Z}$, define $b\mathbb{Z} = \{bn \mid n \in \mathbb{Z}\}$

Note: $b\mathbb{Z} < \mathbb{Z}^+$

and in fact any subgroup of $\mathbb{Z}^+$ is of the form $b\mathbb{Z}$ for some b!

- closed
- identity
- inverses

$H < \mathbb{Z}^+$

$\boxed{b = \text{smallest pos. elmt in } H.}$

$$\left(\begin{matrix} H = \{4, 8, \ldots \\ 0, -4, -8 \end{matrix} \right)$$

$b\mathbb{Z} \subset H$ but why is $H \subset b\mathbb{Z}$?

if $a \in H$, write $a = bd + r$

$a \in H$, $b \in H$, $bd = \underbrace{b + b + \cdots + b}_{d \text{ times}}$ $\in H$

so $a + (-bd)$
$= a - bd \in H \Rightarrow r \in H$.

but Euclidean alg $\Rightarrow r < b$

$\Rightarrow r = 0 \Rightarrow a = bd \in b\mathbb{Z}$

$\square$.

Application / Examples

if $a, b \in \mathbb{Z}_{>0}$

$$a\mathbb{Z} + b\mathbb{Z} = \{an + bm \mid n, m \in \mathbb{Z}\} < \mathbb{Z}^+$$

$$(an + bm) + (an' + bm') = a(n+n') + b(m+m')$$

know it must be of the form $d\mathbb{Z}$ some d.

$\Rightarrow$ given a, b, $\exists d > 0$ s.t. $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} \supset a\mathbb{Z}, b\mathbb{Z} \ni a, b$

$\subset$ d is a lin. comb. of a & b

$\supset$ every lin. comb. of a & b is a mult. of d.

$\Rightarrow a$ is a mult. of d $\quad d \mid a$ $\quad$ and if $d' \mid a,\ d' \mid b$

$d \mid b$

$a, b \in d'\mathbb{Z}$

$b\mathbb{Z},\ a\mathbb{Z} < d'\mathbb{Z}$

$d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} < d'\mathbb{Z}$

$\Rightarrow d$ a mult. of d'

$d' \mid d$.

Yay! subgroups encode divisibility & gcd's.

Cyclic subgroups

If G is a group, $x \in G$, can consider multiples of x and its inverse.

$x,\ \underbrace{x \cdot x}_{x^2},\ x^3,\ x^4, \ldots$

$x^0 = e$

$x^{-1}, x^{-2}, x^{-3}, \ldots$

Def $\langle x \rangle = \{x^i \mid i \in \mathbb{Z}\} < G$ is called the cyclic subgroup generated by x.

$x^i x^j = x^{i+j}$

$x^3 = x^{-2} x^5$

$x^{-1} \cancel{x^{-1}} \cancel{x} xxxx = x^{-1} e\, xxxx$

$\underbrace{x^{-1} x}_{e} xxx$

$e xxx = xxx = x^3$

Given $x \in G$, consider $\{i \in \mathbb{Z} \mid x^i = e\} < \mathbb{Z}^+$

$$S_3 = S_{\{1,2,3\}} \ni \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \sigma$$

$$\sigma^2 \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 1 & 2 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \end{pmatrix} \begin{matrix} \sigma \\ \sigma \end{matrix} \qquad \sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$\sigma^3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e$$

$$\sigma^4 = \sigma\sigma^3 = \sigma e = \sigma \qquad \sigma^5 = \sigma^2 \quad \sigma^6 = e$$

$-3, 0, 3, 6, \overset{a}{\rightsquigarrow} \sigma^i = e$

$0 \rightarrow$

$\{i \mid x^i = e\} < \mathbb{Z}$ $\Big\}$ closed

$\Downarrow$ $\quad \Psi$

$i, j \quad x^i = e \quad x^j = e$

$x^{i+j} = x^i x^j = ee = e$

of form $d\mathbb{Z}$

$d > 0$

<u>Def</u> the <u>order</u> of x is the smallest pos. integer d s.t.

$x^d = e$ (i.e. gen. of $\{i \mid x^i = e\} < \mathbb{Z}^+$)

or order is ∞ if no such d exists.

$\langle 1 \rangle < \mathbb{Z}^+ \qquad x = 1$

infinite order. $\quad + \quad a + a = 2a \qquad (G, \cdot) \quad a \cdot a = a^2$

$X = \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix} \in GL_2(\mathbb{C})$

ords

$X^2 = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$ $\quad \underset{X^4}{\underset{\shortparallel}{(X^2)^2}} = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix} \leftarrow \neq X$

$X^6 = X^4 X^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2$

if $X^3 = I \Rightarrow X^4 = X$