2/3

cyclic subgroups.

$(G, *, e)$ $\quad g \in G$

$$\langle g \rangle = \{ g^k \mid k \in \mathbb{Z} \} = \{ x \in G \mid \exists k \in \mathbb{Z} \ x = g^k \}.$$

$\star$ $\langle g \rangle = \{ kg \mid k \in \mathbb{Z} \}$. is the cyclic subgroup gen. by G.

**Def** The group is called a <u>cyclic group</u> if $\exists g \in G$ s.t. $G = \langle g \rangle$.

**Ex** $G = (\mathbb{Z}, +, 0)$

$\langle 1 \rangle = \{ k \cdot 1 \mid k \in \mathbb{Z} \} = \{ k \mid k \in \mathbb{Z} \}$
$= \mathbb{Z}$.

cyclic groups

$G = (\mathbb{Z}/n\mathbb{Z}, \oplus, [0])$

$\langle [1] \rangle$

**Prop.** if G is a cyclic group, then it is abelian.

**Pf**:

(2) If P, then Q    conditional statement.

1) Direct proof

Assume / $\$$ P is true + then use properties/given from P to show Q is true.

2) Proof by contradiction.

$\$$ P is true and Q is false. then get a contradiction.

so Q is true. (I am not a constructivist.).

3) Proof by Contrapositive.

Assume / $\$$ not Q is true and show directly not P is true (or P is false)

Symbolic logic.  $P \to Q \Leftrightarrow \neg Q \to \neg P \Leftrightarrow \neg P \vee Q$

| $P$ | $Q$ | $P \to Q$ | $\neg Q \to \neg P$ |
|---|---|---|---|
| T | T | T | T |
| T | F | F | F |
| F | T | T | T |
| F | F | T | T |

(3) if $G$ is cyclic, then $G$ is abelian

Pf. Suppose $G$ is a cyclic group. WTS Show $G$ is abelian

In order to show $G$ is abelian we need to take arbitrary $x, y \in G$ & show $x * y = y * x$.

Since $G$ is a cyclic group. $\exists g \in G$ s.t. $\langle g \rangle = G$.

$x, y \in G = \langle g \rangle$ ~~so~~ $\exists j, k \in \mathbb{Z}$ s.t. $x = g^j$, $y = g^k$

$$x \cdot y = g^j \cdot g^k = g^{j+k} = g^{k+j} = g^k \cdot g^j = y \cdot x.$$

$\therefore$ $G$ is abelian. $\blacksquare$

Def. Suppose $G$ is a cyclic group. Any $g \in G$ s.t. $\langle g \rangle = G$ is called a generator for $G$.

Ex. Suppose $G$ is cyclic & $g$ is a gen. for $G$. Then so is $g^{-1}$.

In general, $\langle g \rangle = \langle g^{-1} \rangle$.

Pf: $x \in \langle g \rangle$ $\exists k \in \mathbb{Z}$ s.t. $x = g^k = g^{-(-k)}$
$= (g^{-1})^{-k} \in \langle g^{-1} \rangle$
$-k \in \mathbb{Z}$.

$\forall g \in G$ $\langle g \rangle \subseteq \langle g^{-1} \rangle$.

So $\langle g^{-1} \rangle \subseteq \langle (g^{-1})^{-1} \rangle = \langle g \rangle$. $\blacksquare$

(4) the only generators for $\mathbb{Z}$ are

$1, -1$. if $|n| > 1$. & by way of contradiction

$\cancel{\$}$BWOC

then $1 \notin \langle n \rangle$ if it were then $1 = n \cdot k$

$n, k \in \mathbb{Z}$.

Can't happen.

$\langle e \rangle = \{e\}$

---

Ex $\mathbb{Z}/4\mathbb{Z} = \{[0],[1],[2],[3]\}$.

gen. $[1]$, $[-1]=[3]$ are gen.

$[2] = \{k[2]\} = \{[2k]\} = \{[0],[2]\}$

$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n = \{0,\dots,n-1\}$.

$\mathbb{Z}_6$ 1,5 $\langle 2 \rangle = \{0,2,4\} = \langle 4 \rangle$

$\langle 3 \rangle = \{0,3\}$.

$\mathbb{Z}_5$ 1, 4.

$\langle 2 \rangle = \{0,2,4,1,3,\cancel{0}\} = \mathbb{Z}_5 = \langle 3 \rangle$

$\mathbb{Z}_8$ $\langle 1 \rangle = \langle 7 \rangle$ $\langle 3 \rangle = \langle 5 \rangle$

$\langle 2 \rangle = \langle 6 \rangle$ $\langle 4 \rangle =$

(5) quiz problem

$\mathbb{Z}_n$ (small n) give you K

list out elements in

$\langle K \rangle$

---

<u>Def</u> Let $g \in G$. The <u>order of g</u> is the least positive integer, d, such that $g^d = e$. (if such a thing exists.)

if none exists, then the order is $+\infty$ <u>note</u> $d \geq 1$

---

<u>Ex.</u> $\mathbb{Z}_6$ order of 2 equals 3.

$\mathbb{Z}$ order of 1 equals $+\infty$

---

if $|\langle g \rangle| < \infty$, then g has finite order.

(in other words if $\langle g \rangle$ is a finite set then there is a $d \in \mathbb{N}$ s.t. $g^d = e$.

<u>Pf:</u> $\{g, g^2, g^3, \ldots, g^n, \ldots\} \subseteq \langle g \rangle$ is finite. & $|\langle g \rangle| < \infty$

lots of repeats.

$\exists j, k \in \mathbb{N}$ s.t $g^j = g^k$, $j < k$, $k - j > 0$

$g^{-j} \cdot g^j = g^{-j} \cdot g^k = g^{k-j}$
$= e$

so there is a power $\in \mathbb{N}$ of $g$, $g^d = e$

(6) Conversely if $g$ has finite order then $|\langle g\rangle| < \infty$

Pf: Let $d$ be the order of $g$.
(this means $d$ is the least positive integer s.t. $g^d = e$.)

Claim

$$\langle g\rangle = \{g, g^2, \dots, g^{d-1}, g^d = e\}$$

$\subseteq$ subset

$\supseteq$ subset

Clearly, $\supseteq$ ✓

Let $x \in \langle g\rangle$ WTS $x = g^r$ some $r = 1, \dots, d$

$\exists\, k \in \mathbb{Z}$ s.t. $x = g^k$ Use the division alg.

write $k = qd + r$ $q, r \in \mathbb{Z}$, $0 \le r < d$.

$$x = g^k = g^{qd+r} = (g^d)^q \cdot g^r = e^q \cdot g^r = g^r$$

if $r = 0$ $x = g^0 = e = g^d$.

---

if we write $\{g, g^2, \dots, g^m\}$. the only thing we can conclude is that there are at most $m$ elements.

7 ~~of~~ order of $g$. $= \cancel{|g|}$ $\underline{o(g)}$

<u>Ex</u> $\mathbb{Z}$.

$|-7| = 7$ or $+\infty$ ??

ugh

$o(-7) = +\infty$

---

$\underline{o(g) = d}$. $\langle g \rangle = \{g, g^2, \dots, g^d\}$

so $|\langle g \rangle| \le d$.

So $|\langle g \rangle| = d$ by <u>Alex's proof</u>.

<u>Pf:</u> if not, then there are repeats so

Pf by contradiction $\exists \underline{1 \le j < k \le d}$ $g^j = g^k$ but then $g^{k-j} = e$.

$k - j < d$. contradicting that $d$ is the least pos. int. s.t. $g^d = e$.

---

G <u>finite group</u>. $g \in G$ ask for $o(g)$.

$\langle g \rangle = \{g, g^2, g^3, \dots, g^d = e\}$ $o(g) = d$

1st time.

8

$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in GL_2(\mathbb{R})$ $\qquad o(A) = ?$

$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$\left\{ \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \underbrace{\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}}_{A^2}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, I_2 \right\}$ next step

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

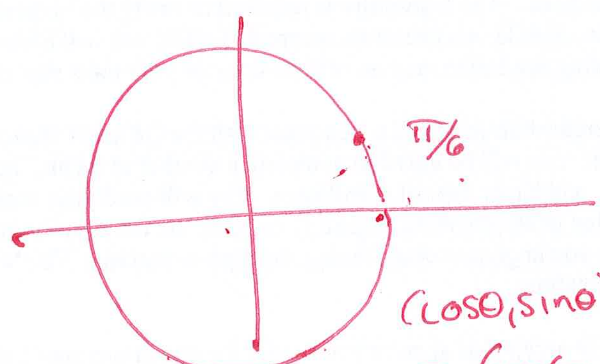
$g^j \cdot g^k = g^k \cdot g^j$

$\underline{g^k \cdot g = g \cdot g^k}$

$o(A) = 4$

---

$\begin{pmatrix} \frac{\sqrt{3}}{2} & \frac{1}{2} \\ -\frac{1}{2} & \sqrt{3}/2 \end{pmatrix}$




$(\cos\theta, \sin\theta)(\cos\alpha, \sin\alpha)$
$= (\cos(\theta+\alpha), \sin(\theta+\alpha))$

the unit circle from trig.

$(\cos\theta, \sin\theta)$

~~$(\cos\theta, \sin\theta$~~

$(a,b) = a + bi$

on $\mathbb{R}^2 \setminus \{0\}$ $\underline{(a,b)(c,d) = (ac - bd, ad + bc)}$

operation on $\mathbb{R}^2$

yes this is an abelian group

identity $= (1,0)$