2/5

Quiz Everyone here! Yeah

- talk about cyclic groups, matrix groups, S_n.

Reminder G cyclic: $\exists g \in G$ s.t. $\langle g \rangle = G$.

such a g is called a generator. $\langle g \rangle = \langle g^{-1} \rangle$

"generator need not be unique"

for $g \in G$, the order of g, $o(g)$, equals the least positive integer k s.t. $g^k = e$, (if such a thing exists). if no such thing exists $o(g) = \infty$

We showed if $o(g) = d < \infty$, then $\langle g \rangle = \{g, g^2, g^3, \ldots, g^{d-1}, e\}$

Div. Alg. and these are all distinct: $|\langle g \rangle| = d$.

if $\langle g \rangle$ is finite, then g has finite order.

$g^j = g^k$, $j < k$

Question if $\exists g \in G$ $o(g) < \infty$, then is G finite.

No. $GL_2(\mathbb{R})$ $A = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$, $(2I)^k = 2^k I$

$$\langle A \rangle = \left\{ \begin{pmatrix} 2^k & 0 \\ 0 & 2^k \end{pmatrix} \middle| k \in \mathbb{Z} \right\}$$

$B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ $\langle B \rangle = \{B, I_2\}$.

(2)

~~if g~~

Cor if $g \in G$, and $o(g) = \infty$, then $|G| = \infty$

any subgroup that ~~cont~~ contains g will be infinite

Contrapositive if $|G| < \infty$, then every element has finite order.

$g \in G$ $\quad o(g) = 1$ iff $g = e$. $\quad \langle e \rangle = \{e\}$

$1 = |\langle g \rangle| =$ ~~$g\{e\}$~~ $\quad o(e) = 1$

then $\langle g \rangle = \{e\}$ + so $g = e$

---

there are examples $|G| = \infty$, but $o(g) < \infty$ $\forall g \in G$.

$\boxed{\text{all cyclic gps are abelian}}$

Theorem $\quad$ Suppose G is cyclic. then every subgroup of G is cyclic.

PF: Since G is cyclic, it has a generator. Choose $g \in G$. $\langle g \rangle = G$.

Let $H \leq G$ be an arbitrary subgroup.

Every element in H {is an element of G}, so

each $h \in H$ has the form $\quad h = g^k$ for some k.

Case 1 $H = \{e\} = \langle e \rangle$.

Case 2 $H \neq \{e\}$ $\quad$ Let $S = \{k \in \mathbb{N} \mid g^k \in H\}$. $\quad$ one of $\underline{k_1 - k} > 0$

$\exists h \neq e$ in H $\quad h = g^k$ def. $k \neq 0$ also $g^{-k} \in H$. (closed under inverses $\quad S \neq \emptyset$

(3) $\emptyset \neq S \subseteq \mathbb{N}$ Well-Ordering Principle of the $\mathbb{N}$

says S has a least element.

Call this least element m. $m \in S$.

if iK $K \in S$, then $M \leq S$

WTS that $\langle g^m \rangle = H$.

Clearly, $\langle g^m \rangle \subseteq H$. Pf: Let $x \in \langle g^m \rangle$.

$x = (g^m)^j$ some $j \in \mathbb{Z}$.

$= g^{mj}$ $\quad g \in H \Rightarrow g^{mj} \in H$

So $x \in H$.

(b/c H is closed under powers + inverses).

Next $H \subseteq \langle g^m \rangle$.

Let $x \in H$ + show ~~$x = g^r$~~ $x \in \langle g^m \rangle$

which means x has the form

$(g^m)^j$ some $j \in \mathbb{Z}$.

Now $x \in H$ + $H \subseteq G \Rightarrow x \in G = \langle g \rangle$ so $x = g^t$ $t \in \mathbb{Z}$.

Divide t by m Div. Alg. $t = mj + r$

$0 \leq r < m$. (aim to show $r = 0$.)

$x = g^t = g^{mj+r} = g^{mj} g^r$ $\quad g^{mj} \in H$ cuz $g^m \in H$.

mult. on left by $(g^{mj})^{-1}$ $\quad \underbrace{\underbrace{(g^{mj})^{-1}}_{\in H} \underbrace{x}_{\in H}}_{\in H} = g^r$ So $g^r \in H$. if $r \neq 0$, $r \in S$.

$r < m$ contradicts m is the least one

$r = 0$ $x \in \langle g^m \rangle$ m

④ Every subgroup of a cyclic group is itself cyclic.

So if you are tasked to find all subgps of a given group which happens to be cyclic. Just look at all $\underline{\langle g \rangle}$

$\underline{Ex}$ $\mathbb{Z}$ is cyclic. Any subgroup has the form $\langle n \rangle = n\mathbb{Z}$.

$\underline{Ex}$ $\underline{S_3}$ the set of permutations on $\{1,2,3\}$

$|S_n| = n!$ $\quad S_3 = \{e, (12), (13), (23), (123), (132)\}$.

$S_4 = \{e, (12), (13), (14), (23), (24), (34), (123), (132)$

$(124), (142)$

$(134)\ (143)$

$(234), (243)$

$(12)(34)$

$(13)(24)$

$(14)(23)$

(1234)

(1243)

(1324)

(1342)

(1423).

(1432)

⑤ $S_3 = \{e, (12), (13), (23), (123), (132)\}$

$\langle (12) \rangle = \{\cancel{e}(12), e\}$

$o(k\text{-cycle}) = k$ $\qquad \langle (13) \rangle = \{(13), e\}$ $\qquad (12)(12) =$

$\langle (23) \rangle = \{(23), e\}.$

$(123)(123)$

$\langle (123) \rangle = \{(123), (132), e\}.$ $\qquad = (132)$

$= \langle (132) \rangle$ $\qquad (123)(132) = e$

$$
\begin{tikzcd}
 & & S_3 \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle (12) \rangle \arrow[drr, dash] & \langle (13) \rangle \arrow[dr, dash] & \langle (23) \rangle \arrow[d, dash] & \langle (123) \rangle \arrow[dl, dash] \\
 & & \langle e \rangle &
\end{tikzcd}
$$

$(12)(13) = (132)$

$(12)(132) = (13)$

$H = \{e, (12), (13), (132), (123), (23)\}$ $\qquad (12)(123) = (23)$

$= S_3$

⑥ Lagrange's Theorem

If $|G| < \infty$ and $H \leq G$. then $|H| \,\big|\, |G|$.

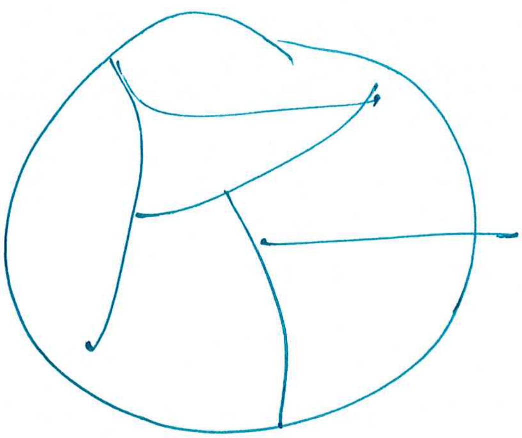
Pf: $H \leq G$. Let $g \in G$.

$$gH = \{x \in G \mid \exists h \in H \;\; x = gH\} \quad \text{coset}$$

$$= \{gh \mid h \in H\}$$

set of distinct cosets forms a partition of G.

$\{g_1H, g_2H, \dots, g_kH\}$



$\underline{eH = H}$

$g_1H \cup \dots \cup g_kH = G$

$g_iH \cap g_jH = \emptyset \quad i \neq j$

$\underline{|g_k| = |H|}$

$$|G| = |g_1H| + |g_2H| + \dots + |g_kH|$$

$$= k \cdot |H|. \qquad |H| \,\big|\, |G|.$$

$\cancel{f(\;) = g_1 h}$

$\cancel{f(g_1^{-1}h) =}$

$\forall g_i \quad |g_iH| = |H|.$

how to show two sets have same size

construct a bijection.

$f : H \to g_iH$

$f(h) = g_ih \qquad g_ih_1 = g_ih_2$