9/13

P69 #10

$D_4 = \{I, R, R^2, R^3, H, HR, HR^2, HR^3\}$

Cyclic subgroups of order 4.

$\langle R \rangle = \{I, R, R^2, R^3\} = \langle R^3 \rangle$

Other subgroups of order 4:

$\{I, H, R^2, HR^2\}, \{I, R^2, HR, HR^3\}$

$(HR)(HR) = HHR^3R = I$

$(HR)(HR^3) = HHR^3R^3 = R^2$

$(HR^3)(HR) = HHRR = R^2$

P70 #20

$a, b \in G$

$o(ab) = o(ba)$

$o(ab) = n \Rightarrow \underbrace{(ab)(ab)\cdots(ab)}_{n} = e.$

$\Rightarrow a(ba)^{n-1}b = e \Rightarrow (ba)^{n-1}b = a^{-1}$

$\Rightarrow (ba)^{n-1}(ba) = a^{-1}a = e \Rightarrow (ba)^n = e$

$\Rightarrow o(ba) = n.$

Test #1, Friday 9/15:

#1. gcd, lcm, relatively prime, prime

Ex(1) $5n+2$, $7n+3$ are relatively prime.

$$(-7)(5n+2)+(5)(7n+3)=1$$
$$\Rightarrow \gcd\{5n+2, 7n+3\}=1$$

Ex(2) $\gcd(a,bc)=1 \Leftrightarrow \gcd(a,b)=1 \;\&\; \gcd(a,c)=1$

#2. Mathematical induction:

Ex(1) $17 \mid (2^n 3^{2n}-1) \quad \forall n \geq 1$

Ex(2) $a, b \in G$ group. Show that
$(a^{-1}ba)^n = a^{-1}b^n a \quad \forall n \geq 1$

$n=1$ true

Assume $(a^{-1}ba)^n = a^{-1}b^n a$

$$(a^{-1}ba)^{n+1} = (a^{-1}ba)^n (a^{-1}ba)$$
$$= a^{-1}b^n \underline{a a^{-1}} ba = a^{-1}b^{n+1}a$$

#3. Equivalence relations & equivalence classes.

Ex(1) $\mathbb{R}$ = set of real numbers.

$x, y \in \mathbb{R}$ define $x \sim y$ if $x - y \in \mathbb{Z}$

Show that $\sim$ is an equivalence relation and find the distinct equivalence classes.

$x \sim x$ since $x - x = 0 \in \mathbb{Z}$

$x \sim y \Rightarrow x - y \in \mathbb{Z} \Rightarrow y - x = -(x-y) \in \mathbb{Z}$

$\Rightarrow y \sim x$

$x \sim y$ & $y \sim z \Rightarrow x - y, y - z \in \mathbb{Z}$

$\Rightarrow (x-y) + (y-z) \in \mathbb{Z} \Rightarrow x - z \in \mathbb{Z}$

$\Rightarrow x \sim z$

$[0] = \mathbb{Z}$, $0 < x < 1$

$[x] = \{x + n \mid n \in \mathbb{Z}\}$, $[1] = [0]$

$\Rightarrow \{[x] \mid 0 \leq x < 1\}$ are the distinct equivalence classes.

#4. Group of symmetries.

#5. Groups $\mathbb{Z}_n$ & $U(n)$

#6. Group properties.

Ex(1) $\begin{pmatrix} 2 & 2 \\ 3 & 5 \end{pmatrix}^{-1} = ?$ in $GL(2, \mathbb{Z}_{11})$

Ex(2) $G = \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} \mid a \in \mathbb{R}_{\neq 0} \right\}$ group under matrix multiplication.

$$e = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}, \quad \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}^{-1} = ?$$

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

We showed that any subgroup of $\mathbb{Z}$ is cyclic.

Thm: Let G be a cyclic group and H any subgroup. Then H is cyclic.

Pf (idea)
$$G = \langle a \rangle \quad , a \in G$$
$$= \{ a^i \mid i \in \mathbb{Z} \}$$

If $H = \{e\}$, then $H = \langle e \rangle$

Assume $|H| > 1$.

$b \in H \Rightarrow b = a^i$ for some $i \in \mathbb{Z}$

Since $b^{-1} \in H \Rightarrow a^{-i} \in H$

Choose k to be the smallest positive integer such that $a^k \in H$.

Claim: $H = \langle a^k \rangle$

$\langle a^k \rangle \subseteq H$ since $a^k \in H$

$H \subseteq \langle a^k \rangle$ (use division algorithm.)

Ex(1) $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$

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

$\Rightarrow \mathbb{Z}_8 = \langle k \rangle \Leftrightarrow \gcd(k, 8) = 1$

Thm: $\mathbb{Z}_n = \langle k \rangle \Leftrightarrow \gcd(k, n) = 1$.

Thm: $G = \langle a \rangle$, $o(a) = n$. Then

$G = \langle a^k \rangle$ if and only if $\gcd(k, n) = 1$.

Thm: $G = \langle a \rangle$, $o(a) = n$ $(\Rightarrow |G| = n)$

$(G = \{e, a, a^2, \cdots, a^{n-1}\})$

(1) H subgroup of G $\Rightarrow |H| \mid |G|$

(2) If $k \mid n$, then G has exactly one subgroup of order k, namely $\langle a^{n/k} \rangle$.

Ex(2) $G = \mathbb{Z}_{10} = \langle 1 \rangle = \langle 3 \rangle = \langle 7 \rangle = \langle 9 \rangle$

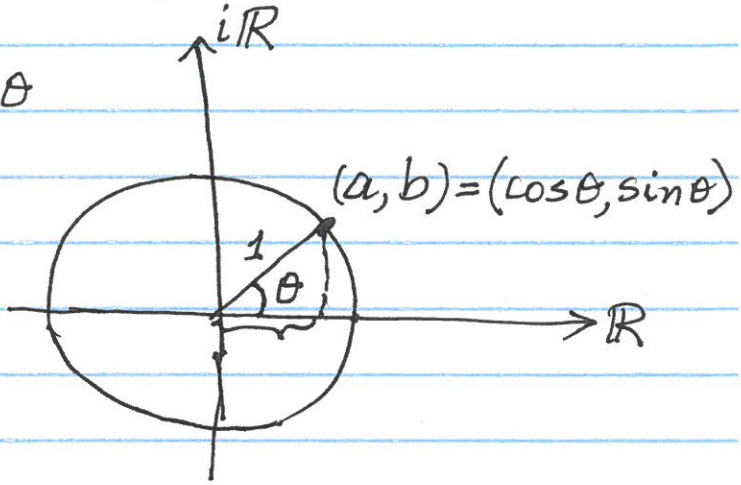
Other subgroups: $\langle 0 \rangle, \langle 2 \rangle, \langle 4 \rangle, \langle 5 \rangle, \langle 6 \rangle$

$\langle 8 \rangle$

$\langle 2 \rangle = \langle 4 \rangle = \langle 6 \rangle = \langle 8 \rangle$

#71 Page 73

$$H = \{ a+bi \mid a, b \in \mathbb{R},\ a^2+b^2 = 1 \}$$



$$a+bi = \cos\theta + i\sin\theta = e^{i\theta}$$

$$H = \{ e^{i\theta} \mid 0 \le \theta \le 2\pi \}$$

$e^0 = 1$ identity

$\parallel$

$1+0i$

$e^{i\theta_1} \cdot e^{i\theta_2} = e^{i(\theta_1+\theta_2)} \in H$

$$(e^{i\theta})^{-1} = e^{-i\theta} = \cos(-\theta) + i\sin(-\theta)$$

$$= \cos(\theta) - i\sin(\theta) \in H$$

$$(a+bi)^{-1} = \frac{1}{(a+bi)} \cdot \frac{(a-bi)}{(a-bi)} = \frac{a-bi}{a^2+b^2} = a-bi \in H.$$

Ex(1) $\mathbb{Z} = \langle 1 \rangle$

H subgroup $\Rightarrow$ H is cyclic.

Ex(2) $\mathbb{Z}_{20} = \{0, 1, \cdots, 19\}$

$= \langle 1 \rangle = \langle 3 \rangle = \langle 7 \rangle = \langle 9 \rangle$

$= \langle 11 \rangle = \langle 13 \rangle = \langle 17 \rangle = \langle 19 \rangle$

$k \mid 20 \quad (\Rightarrow k = 1, 2, 4, 5, 10, 20)$

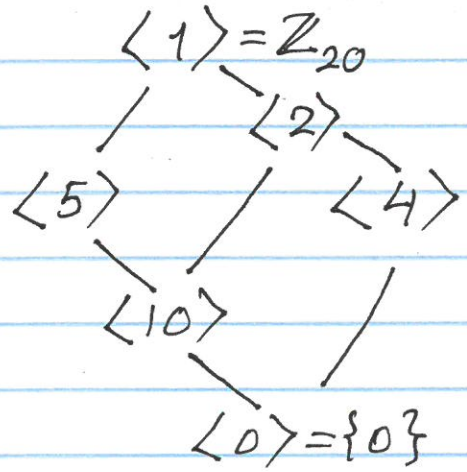
$k = 1 : \langle a^{n/k} \rangle = \langle 1^{20} \rangle \quad (a = 1, n = 20)$

$= \langle 0 \rangle$

$k = 2 : \langle 1^{20/2} \rangle = \langle 10 \rangle$

$k = 4 : \langle 5 \rangle \; ; \; k = 5 : \langle 4 \rangle$

$k = 10 : \langle 2 \rangle \; ; \; k = 20 : \langle 1 \rangle$



subgroup lattice of $\mathbb{Z}_{20}$.

Thm $G = \langle a \rangle$, $o(a) = n$ $(\Rightarrow |G| = n)$

(1) # of elts in G of order n
$= |\{k \mid \gcd(k, n)\}|$
and those elts are $\{a^k \mid \gcd(k, n) = 1\}$

(2) Suppose $d \mid n$. Then G contains the unique subgroup $\langle a^{n/d} \rangle$ of order d. Any elt. of order d in G must be in $\langle a^{n/d} \rangle$. Hence

# of elements of order d in G
$= |\{k \mid \gcd(k, d) = 1\}|$
and those elts are $\{(a^{n/d})^k \mid \gcd(k, d) = 1\}$.

Ex (3) How many elts of order 10 are in $\mathbb{Z}_{20}$? What are they?

$\{k \mid \gcd(k, 10) = 1\} = \{1, 3, 7, 9\}$

# of elts of order 10 in $\mathbb{Z}_{20}$ is (4).

Those order 10 elts are: $2^1 = 2$, $2^3 = 6$, $2^7 = 14$, $2^9 = 18$.

HW P85 #1, 2, 3, 5, 9, 10, 13, 22, 32, 33, 38, 53, 63, 70.