Lecture 3

Practice Problems Chapter 4
(1/1), (11/11), (12/12), (17/17), (18/18), (22/22), (29/29), (31/31) (85/71)

Solutions for PP Chapter 3.

(28/14) Let $H < \mathbb{Z}$ and $30, 40, 18 \in H$. What is H?

Note: $H < G$ means $H \leq G$ but $H \neq G$. "H is a proper subgroup of G"

$2 = \gcd(30, 40, 18)$
$30 \in H$
$18 \in H$
$30 - 18 = 12 \in H$
$40 - 12 - 12 - 12 = 4 \in H$
$18 - 4 - 4 - 4 - 4 = 2 \in H$
$H \ni 2$
So $\mathbb{Z} > H \geq 2\mathbb{Z}$

Claim: $H = 2\mathbb{Z}$
Proof: Suppose $H \neq 2\mathbb{Z}$
Then $\exists s \in H$ st. $s \notin 2\mathbb{Z}$. Then s is odd, i.e. $s = 2k+1$ for some $k \in \mathbb{Z}$.
So $s \in H, 2k \in H$, so $1 = s - 2k \in H$
Then $H = \mathbb{Z}$ which is a contradiction. ∎

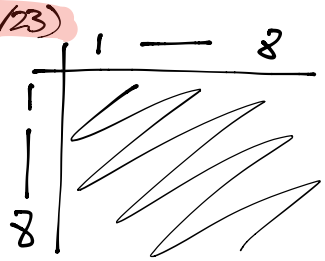
(34/20) G be a group, $a \in G$. Prove that $C(a) = C(a^{-1})$.

Pf: first prove $C(a) \leq C(a^{-1})$
Sps $g \in C(a)$, i.e. $ga = ag \iff a^{-1}ga = g \iff a^{-1}g = ga^{-1}$
$\Updownarrow$
$g \in C(a^{-1})$ ∎

(36/22)

	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	4	3	6	5	8	7
3	3	4	2	1	7	8	6	5
4	4	3	1	2	8	7	5	6
5	5	6	8	7	1	2	4	3
6	6	5	7	8	2	1	3	4
7	7	8	5	6	4	3	1	2
8	8	7	6	5	3	4	2	1

(37/23)



a. $C(2) = \{1, 2, 5, 6\}$
... Similarly ...
b. $Z(G) = \{1, 5\}$
c. $|1| = 1$
$|2| = |4| = |5| = |6| = |8| = 2$
$|3| = |7| = 4$

(38/24) a, b distinct group elements, prove either $a^2 \neq b^2$ or $a^3 \neq b^3$

Pf: (by contradiction)
Assume $a^2 = b^2$ and $a^3 = b^3$.
Also, $a \neq b$.
Since $a^2 = b^2$, $a^{-2} = b^{-2}$. Multiply $a^3 = b^3$ by a^{-2}, get $a = a^{-2}b^3 = b^{-2}b^3 = b$

Contradiction. ∎

(52/36) $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} \in SL(2, \mathbb{R})$.

Sol:
$|A| = 4$ as $A^4 = \begin{Bmatrix} 1 & 0 \\ 0 & 1 \end{Bmatrix}$ $\quad |B| = 3$, $\quad |AB| = \infty$

(55/39) G be symmetry group of a circle. Show G has elements of every finite order as well as elements of infinite order.

R_{x° is finite order iff x is in $\mathbb{Q}$.

(61/45) Sps G is a finite group. Sps $H \leq G$, and $g \in G$. And sps that n is the smallest int. s.t. $g^n \in H$. Prove that $n \mid |g|$.

Pf: Sps $n \nmid |g|$. Then $g = kn + r$ for some $0 < r < n$
Then $g^{|g|} = g^{kn} \cdot g^r = e$
so we have $g^r = (g^{kn})^{-1} \in H$. This is a contradiction. ∎

(68/52) $H = \{A \in GL(2, \mathbb{R}) \mid \det A \text{ is int. power of } 2\}$ Show H is a subgroup of $GL(2, \mathbb{R})$.

Last time:

Defn: A group G is cyclic, if $\exists a \in G$
$G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ we say G is generated by a.
In general, if $a \in G$. Then it's not always true that $G = \langle a \rangle$. But we always have $\langle a \rangle \leq G$.

Thm: Sps G is a group, and let $a \in G$. If a has infinite order then $a^i = a^j$ iff $i = j$. If a has finite order then $a^i = a^j$ iff $i \equiv j \bmod n$
Moreover $\langle a \rangle = \{e, a, a^2, \cdots, a^{n-1}\}$

Pf: Assume $|a| = \infty$
Sps $a^i = a^j$. Then $a^{i-j} = e$. But a has infinite order, so we must have $i - j = 0$
Now assume $|a| = n$
Sps $a^i = a^j$. Then $a^{i-j} = e$. Write $i - j = kn + r$, where $0 \le r \le n-1$. Then
$a^{i-j} = a^{kn} a^r$. So $a^r = e$. but $r \le n-1$. So $r = 0$. Thus $i \equiv j \bmod n$.
Finally, we have $\langle a \rangle = \{a^i \mid i \in \mathbb{Z}\} = \{e, a, \cdots, a^{n-1}\}$ b/c every int is congruent to some number in $\{0, \cdots, n-1\} \bmod n$. But none of #s in $\{0, \cdots, n-1\}$ are congruent to each other mod n.

■

Corollary: If $a^k = e$, then $n \mid k$.
Proof: $a^k = e \iff a^k = a^0$ by the thm, this means $k \equiv 0 \bmod n$. i.e. $n \mid k$ ■

Thm: Let $a \in G$ be an element of finite order n. Let k be a positive int. Then $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ and $|a^k| = n / \gcd(n,k)$

Pf: Let $d = \gcd(n,k)$.
Certainly $\langle a^k \rangle = \langle a^d \rangle$ just because $d \mid k$ so $k = rd$, $\exists r \in \mathbb{Z}$

So $a^k = (a^d)^r$
So we need to prove that $\langle a^d \rangle \subseteq \langle a^k \rangle$. i.e. $a^d = (a^k)^s$ for some $s \in \mathbb{Z}$.

But since $d = \gcd(n,k)$. $d = bn + ck$ for $b, c \in \mathbb{Z}$.
Thus $a^d = a^{bn} a^{ck} = e a^{ck} = (a^k)^c$.

So we know
$\langle a^k \rangle = \langle a^d \rangle = \{e, a^d, a^{2d}, \cdots (a^d)^{l-1}\}$
where $l = |a^d| = |\langle a^d \rangle|$
But d is the least positive int. r s.t. $\langle a^r \rangle = \langle a^k \rangle$

Want to conclude that $l = n/k$. Then we know that $|\langle a^d \rangle| = n/d$
Therefore $|\langle a^k \rangle| = n/d$.

■

Note: $d = \gcd(n_1, n_2, \cdots, n_k) \iff d$ is the least positive int. s.t. $d = c_1 n_1 + \cdots c_k n_k$ for $c_j \in \mathbb{Z}$

Proposition: Suppose $a \in G$. $|a| = n$. Then if $a^c \in \langle a^k \rangle$. and $c > 0$.
Then $c \ge d = \gcd(n,k)$.

Pf: Sps $a^c \in \langle a^k \rangle$. Then $a^c = a^{rk}$ for some $r \in \mathbb{Z}$. Then $c \equiv rk \bmod n$. So
$c = rk + sn$ $\exists s \in \mathbb{Z}$. Thus $c \ge d$.

Corollary 1: In a finite cyclic group, the order of elements divides the order of the group.

Corollary 2: Sps $a \in G$, $|a| = n$. Then $\langle a^i \rangle = \langle a^j \rangle$ iff $\gcd(n,i) = \gcd(n,j)$

$\langle a^{\gcd(n,i)} \rangle \quad \langle a^{\gcd(n,j)} \rangle$

Cor 3: Let $a \in G$. Let $|a| = n$. Then $\langle a \rangle = \langle a^j \rangle$ iff $\gcd(n,j) = 1$
For $\mathbb{Z}_n$, k is a generator iff $\gcd(k,n) = 1$.

Thm: Every subgroup of a cyclic group is cyclic.
If $|\langle a \rangle| = n$, then every subgroup of $\langle a \rangle$ has order dividing n.
Moreover, $\forall$ k dividing n, the group $\langle a \rangle$ has exactly one subgroup of order k, namely $\langle a^{n/k} \rangle$ $(k > 0)$

Pf: Let $G = \langle a \rangle$
Let $H \leq \langle a \rangle \ (= G)$
Let j = the least positive int. st. $a^j \in H$.
if no such j exists, then $H = \{e\}$. So assuming $H \neq \{e\}$, we have j defined.
We want to prove $H = \langle a^j \rangle$.
Assume $\langle a^j \rangle < H$. Then $\exists$ $x \in H$ s.t. $x \notin \langle a^j \rangle$. So $x = a^{kj+r}$ where $k \in \mathbb{Z}$, $0 < r < n$.
Thus $a^r = x \cdot a^{-kj} \in H$, which is a contradiction.

By a previous thm. we know all subgroups of $\langle a \rangle$ when $|a| = n$, look like $\langle a^d \rangle$ where $d | n$.

And we saw that $\langle a^k \rangle = \langle a^j \rangle$ iff $\gcd(k,n) = \gcd(j,n)$. And the order of $|\langle a^d \rangle| = n/d$.

Cor: The subgroup of $\mathbb{Z}_n$ are precisely $\langle n/k \rangle$

Def'n: Let $n > 0$ be an int. Then $\varphi(n) = \#$ of int. in $\{0, \cdots, n-1\}$ that is relatively prime to $n = |U(n)|$.

Thm: In a cyclic group of order n. $\forall d | n$ $(d > 0)$ $\exists$ exactly $\varphi(d)$ elements of order d.
Pf: Sps $G = \langle a \rangle$ and $|a| = n$. And sps $d | n$. Then $\langle a^{n/d} \rangle$ is a group of order d. And if x is order d, then $\langle x \rangle$ is also a group of ordered.
Thus $\langle x \rangle = \langle a^{n/d} \rangle$. So counting elements of order d is equivalent to counting generators of $\langle a^{n/d} \rangle$.
Equivalently, we want to prove that every cyclic group of order d has exactly $\varphi(d)$ generators. Let $H = \langle b \rangle$ be a group of order d.
But we know that $\langle b^i \rangle = \langle b \rangle$ iff $\gcd(i,d) = 1$.
So we exactly have $\varphi(d)$ choices. ∎

Cor: If G is a finite group, the number of elements of order d is a multiple of $\varphi(d)$.
Pf: Let $a \in G$ s.t. $|a| = d$.
Then $\langle a \rangle \leq G$. And $\langle a \rangle$ has precisely $\varphi(d)$ elements of order d. if all elements of order d lie in $\langle a \rangle$, then we're done. O.w., let $b \in G$ s.t. $|b| = d$ and $b \notin \langle a \rangle$.

Then any element $x \in \langle b \rangle$ of order d cannot lie in $\langle a \rangle$. So we get $\varphi(d)$ elements of ordered in $\langle b \rangle$.
Thus we have $2\varphi(d)$.
Repeating m times, we get $m\varphi(d)$ elements of order d.