~~Ch 4~~, Pt A: # 1, 2, 4, 8, 21, 22, 24, 31

1) $\mathbb{Z}_6 = \langle 1 \rangle = \langle 5 \rangle$

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

$\mathbb{Z}_{20} = \langle 1 \rangle = \langle 3 \rangle = \langle 7 \rangle = \langle 9 \rangle = \langle 11 \rangle = \langle 13 \rangle = \langle 17 \rangle = \langle 19 \rangle$

2) $\langle a \rangle$ has generators a^1, a^5

$\langle b \rangle$ has generators b, b^3, b^5, b^7

$\langle c \rangle$ has generators $c, c^3, c^7, c^9, c^{11}, c^{13}, c^{17}, c^{19}$

4) In $\mathbb{Z}_{18}$: $\left.\begin{aligned} \langle 3 \rangle &= \{3, 6, 9, 12, 15, 0\} \\ \langle 15 \rangle &= \{15, 12, 9, 6, 3, 0\} \end{aligned}\right\}$ same!

In $\langle a \rangle$: $\langle a^3 \rangle = \{a^3, a^6, a^9, a^{12}, a^{15}, e\} = \langle a^{15} \rangle$

8) $a \in G$, $|a| = 15$

a) $|a^3| = |a^6| = |a^9| = |a^{12}| = 5$

b) $|a^5| = |a^{10}| = 3$

c) $|a^2| = |a^4| = |a^8| = |a^{14}| = 15$

21) G grp, $a \in G$

a) $a^{12} = e \Rightarrow |a| = 1, 2, 3, 4, 6$, or 12

b) $a^m = e \Rightarrow |a| \mid m$

c) $|G| = 24$, G cyclic. If $a^8 \neq e$ and $a^{12} \neq e$ show $\langle a \rangle = G$.

Since $a \in G$, $|a| = 1, 2, 3, 4, 6, 8, 12$ or 24. Since $a^8 \neq e$, $|a| \neq 1, 2, 4, 8$.

Additionally $a^{12} \neq e$ implies $|a| \neq 1, 2, 3, 4, 6$, or 12. So $|a| = 24$.

But $\langle a \rangle \subseteq G$ and $|\langle a \rangle| = 24 = |G|$ so $\langle a \rangle = G$.

22) Let G have order 3. Then $G = \{e, a, b\}$ for some $a, b \neq e$, $a \neq b$.

Since G grp, $ab \in G$. If $ab = e$, $a = b^{-1}$.

$$\left.\begin{array}{l} \text{If } ab = a, \quad b = e \Rightarrow\Leftarrow \\ \text{If } ab = b, \quad a = e \Rightarrow\Leftarrow \end{array}\right\} \text{ so } a = b^{-1} \Rightarrow b = a^{-1}$$

so $G = \{e, a, a^{-1}\}$. Now $a^2 \in G$. If $a^2 = e$, $a = a^{-1} \Rightarrow\Leftarrow$

If $a^2 = a$, $a = e \Rightarrow\Leftarrow$

so $a^2 = a^{-1}$ and $G = \{e, a, a^2\} = \langle a \rangle$.

24) $a \in G$ grp. Prove $\langle a \rangle$ is a subgrp of $C(a)$.

Since $a a = a^2 = a a$, $a \in C(a)$. So by closure $\langle a \rangle \subseteq C(a)$.

31) G grp, $|G| < \infty$.

Show $\exists\, n \in \mathbb{Z}_{>0}$ s.t. $a^n = e$ $\forall a \in G$.

$|G| < \infty$ so $G = \{g_1, g_2, \ldots, g_m, e\}$ for some m.

Let $n = |g_1||g_2| \cdots |g_m|$

Then $a^n = (a^{|a|})^{n/|a|} = e$. and $\frac{n}{|a|} \in \mathbb{Z}_{>0}$.

Ch 4 Slns # 10, 13, 15, 29, 33, 35, 37, 42, 53, 55, 60, 62, 64

10) $\mathbb{Z}_{24}$, H = subgp of order 8 = $\{3, 6, 9, 12, 15, 18, 21, 0\}$

$\boxed{H = \langle 3\rangle = \langle 9\rangle = \langle 15\rangle = \langle 21\rangle}$

need gcd $(i, 8) = 1$ ← 1, 3, 5, 7

$1\cdot 3 = 3$, $3\cdot 3 = 9$, $5\cdot 3 = 15$, $7\cdot 3 = 21$

$G = \langle a\rangle$, $|a| = 24$

$H = \{a^3, a^6, a^9, a^{12}, a^{15}, a^{18}, a^{21}, e\}$

$\boxed{H = \langle a^3\rangle = \langle a^9\rangle = \langle a^{15}\rangle = \langle a^{21}\rangle}$

13) $\mathbb{Z}_{24}$, $\langle 21\rangle \cap \langle 10\rangle$

$\langle 21\rangle = \{21, 18, 15, 12, 9, 6, 3, 0\}$

$\langle 10\rangle = \{10, 20, 6, 16, 2, 12, 22, 8, 18, 4, 14, 0\}$

$= \{2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 0\}$

so $\langle 21\rangle \cap \langle 21\rangle = \{6, 12, 18, 0\}$

$= \boxed{\langle 6\rangle}$

$G = \langle a\rangle$, $|a| = 24$, $\langle a^{21}\rangle \cap \langle a^{10}\rangle$

$\langle a^{21}\rangle \cap \langle a^{10}\rangle = \boxed{\langle a^6\rangle}$

$\boxed{\langle a^m\rangle \cap \langle a^n\rangle = \langle a^{\operatorname{lcm}(m,n)}\rangle \quad \text{note: this is non-obvious; there is something to prove here}}$

15) G an Abelian grp, $H = \{g \in G \mid |g| \mid 12\}$. Prove H subgrp G.

closure: $g, h \in H$ so $|g| \mid 12$, $|h| \mid 12$

Thn $|gh| \mid 12$ since $(gh)^{12} = g^{12}h^{12} = e$.

So $gh \in H$

Inverses: $g \in H \Rightarrow |g| \mid 12$ but $|g| = |g^{-1}|$ so $|g^{-1}| \mid 12 \Rightarrow g^{-1} \in H$.

- There is nothing special abt 12 so $H = \{g \in G \mid |g| \mid k\}$ where G is an abelian grp and k is a positive integer is a subgrp.

29) $\mathbb{Z}_{8,000,000}$ elements of order 8 $\langle a \rangle$, $|a| = 8,000,000$

$|\langle 1000000 \rangle| = 8$ $|\langle a^{1000000} \rangle| = 8$

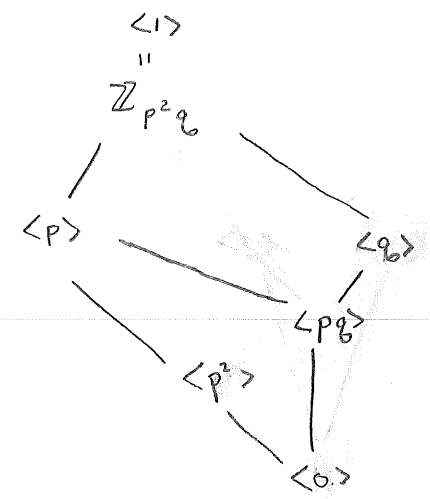
So: 1000 000, 3 000 000, 5 000 000, 7 000 000

So $a^{1000\,000}$, $a^{3000\,000}$, $a^{5000\,000}$, $a^{7000\,000}$

we know this is it b/c this is the only subgrp of order 8, by the fundamental thm of cyclic groups, and it must contain all of the elements of order 8.

33) $\mathbb{Z}_{p^2 q}$, $p \neq q$, p, q prime

Subgrps:	$\langle e \rangle$	$\langle p^2 \rangle$	$\langle q \rangle$	$\langle p \rangle$	G	$\langle pq \rangle$
Order	1	q	p^2	pq	$p^2 q$	p
			3, 9, 12, 15, 18	✓ 5, 10, 5,	✓	15,



35) $\mathbb{Z}_{p^n}$, $n \in \mathbb{Z}_{>0}$, p prime

$\langle 1 \rangle = \mathbb{Z}_{p^n}$
|
$\langle p \rangle$
|
$\langle p^2 \rangle$
⋮
$\langle p^{n-1} \rangle$
|
$\langle 0 \rangle$

37) Show $(\mathbb{Q}^+, \times)$ not cyclic.

Assume it is. Then $\forall x \in \mathbb{Q}^+$, $x = \left(\frac{a}{b}\right)^k$ for a fixed $\frac{a}{b}$ and some k. (a, b rel. prime) obv. $b \neq 1$ and $a \neq 1$

In particular, $2 = \left(\frac{a}{b}\right)^k$. Clearly $k \neq 1, 0, -1$. If $n > 1$, $2 = \frac{a^k}{b^k} \Rightarrow$

$2b^k = a^k \Rightarrow 2 | a^k \Rightarrow 2 | a$. But, similarly, $2 | b$. $\Rightarrow\Leftarrow$.

we can similarly argue the case for $n < 1$.

42) Suppose $a, b \in G$, a & b commute, $|a|$ & $|b|$ finite.

What are the possibilities for $|ab|$?

Clearly $(ab)^{|a||b|} = e$ so $|ab| \mid |a| \cdot |b|$ so $|ab|$ is a divisor of $\text{lcm}(|a|, |b|)$.

moreover, $(ab)^{\text{lcm}(|a|, |b|)} = e$

53) p prime, G grp, G has more than $p-1$ elements of order p.

Then G can't be cyclic b/c $\phi(p) = p-1$. If G is infinite, and cyclic, this clearly doesn't happen

55) $\mathbb{Z}_{40}$; $1 \cdot 4 = 4$, $3 \cdot 4 = 12$, $7 \cdot 4 = 28$, $9 \cdot 4 = 36$

$\langle x \rangle$: x^4, x^{12}, x^{28}, x^{36}

60) G Abelian, G has cyclic subgrps of order 4 & 6.

What other size cyclic groups must G contain?

$\text{lcm}(4, 6) = 12$ so has a grp of order 12.

but this is itself a grp that is cyclic so there are cyclic subgrps

of sizes corresponding to each divisor of 12

So $\boxed{1, 2, 3, 4, 6, 12}$

In general, cyclic subgrp. for each divisor of $\text{lcm}(n, m)$

62) $U(49)$ cyclic of order 42; how many generators?

$\phi(42) = \phi(2 \cdot 3 \cdot 7) = \phi(2)\phi(3)\phi(7) = 1 \cdot 2 \cdot 6 = \boxed{12}$

64) $a, b \in G$, $|a|$ & $|b|$ rel. prime. Show $\langle a \rangle \cap \langle b \rangle = \{e\}$

Assume not. Then $\exists\, x \in \langle a \rangle \cap \langle b \rangle$ s.t. $x \neq e$.

so $\langle x \rangle \subseteq \langle a \rangle$ and $\langle x \rangle \subseteq \langle b \rangle$.

Thus $|\langle x \rangle| \mid |\langle a \rangle|$ and $|\langle x \rangle| \mid |\langle b \rangle|$

so $|x| \mid |a|$ and $|x| \mid |b|$

so $\gcd(|a|, |b|) \geq |x|$ $\Rightarrow \Leftarrow$