Chapter 4 #2. $|\langle a\rangle| = 6$

a^k is a generator iff $\gcd(6,k)=1$

So, a^5 is the only other generator.

$|\langle b\rangle| = 8 \Rightarrow b^k$ is a generator iff $\gcd(8,k)=1$

So, a^3, a^5, a^7 are the other generators

$|\langle c\rangle| = 20 \Rightarrow c^k$ is a generator iff $\gcd(20,k)=1$

So, $a^3, a^7, a^9, a^{11}, a^{13}, a^{17}, a^{19}$ are the other generators.

#4. $\mathbb{Z}_{18}$: $\langle 3\rangle = \langle 3,6,9,12,15,0\rangle$

$\langle 15\rangle = \langle 15,12,9,6,3,0\rangle$

#8. $|a|=15 \Rightarrow a^{15}=e$ and $|\langle a\rangle| = 15$

a) $|a^3| = \frac{15}{\gcd(15,3)} = 5$

Since $\gcd(15,3)=\gcd(15,6)=\gcd(15,9)=\gcd(15,12)$

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

Similarly $|a^5|=|a^{10}| = \frac{15}{5} = 2$

c) $|a^2|=|a^4|=|a^8|=|a^{14}| = \frac{15}{1} = 15$

#10. $G=\langle a\rangle$ and let $|a|=24$.

List all generators for the subgroup of order 8.

Gis cyclic so any subgroup is cyclic and is generated by a^k by some $k \in \mathbb{Z}$

Also, $|\langle a^k\rangle| = \frac{24}{\gcd(24,k)} = 8$

$\Rightarrow \gcd(24,k) = 3$

$\Rightarrow k = 3, 9, 15, 21$

So generators for the subgroup of order 8 are a^3, a^9, a^{15}, a^{21}.

#13. $|a|=24$

Find $\langle a^{21}\rangle \cap \langle a^{10}\rangle$.

$\langle a^{21}\rangle = \langle a^3\rangle$ because

$\langle a^{21}\rangle = \frac{24}{\gcd(24,21)} = \frac{24}{\gcd(24,3)} = \langle a^3\rangle$

Similarly b/c $\gcd(24,10)=\gcd(24,2)$ we have $\langle a^{10}\rangle = \langle a^2\rangle$

So, $\langle a^{21}\rangle \cap \langle a^{10}\rangle = \langle a^3\rangle \cap \langle a^2\rangle$

$x \in \langle a^2\rangle \Rightarrow x = a^{2k}$ for some k

$x \in \langle a^3\rangle \Rightarrow x = a^{3l}$ for some l.

Then $2k = 3l \pmod{24}$

(Recall that $a^i = a^j$ iff $n \mid i-j$)

This says that the exponent is a multiple of both 2 and 3 so it is a multiple of 6.

Therefore if $x \in \langle a^3\rangle \cap \langle a^2\rangle$ then $x = (a^6)^t$ for some t.

On the other hand,

$a^{6t} = (a^2)^{3t} \in \langle a^2\rangle$

also $a^{6t} = (a^3)^{2t} \in \langle a^3\rangle$

$\Rightarrow a^{6t} \in \langle a^2 \cap a^3\rangle$

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

In general, a generator for $\langle a^m\rangle \cap \langle a^n\rangle$ is $a^{\text{lcm}(m,n)}$

In part a for example,

$\langle a^{21}\rangle \cap \langle a^{10}\rangle = \langle a^{\text{lcm}(21,10)}\rangle$

$= \langle a^{210}\rangle$

because $\gcd(24,210)=\gcd(24,6)$

$= \langle a^6\rangle$

proof $a^z \in \langle a^m\rangle \cap \langle a^n\rangle \Rightarrow z = tm$ & $z = qn$.

$\Rightarrow m \mid z$ and $n \mid z$

$\Rightarrow z \mid \text{lcm}(m,n)$

$\Rightarrow a^z \in \langle a^{\text{lcm}(m,n)}\rangle$

Conversely if $a^z \in a^{\text{lcm}(m,n)}$ then $\Rightarrow z = \text{lcm}(m,n)\,s$

$\Rightarrow z = mt$ and $z = nq$ for some m, q

$\Rightarrow a^z \in \langle a^m\rangle \cap \langle a^n\rangle$

40) Let $m,n \in \mathbb{Z}$. Find a generator for $\langle m\rangle \cap \langle n\rangle$

We proved the general case for this statement in problem 13.

Because $\mathbb{Z}$ is generated by 1, we have $a=1$, $\langle m\rangle = \langle m\cdot 1\rangle = \langle n\cdot 1\rangle$

So, the generator is $\text{lcm}(m,n)$.

#46) Let $|x|=40$. List all elements of $\langle x\rangle$ that have order 10

$$\langle x\rangle = \{ x^k \mid k=0,1,\dots,39\}$$

$$|x^k| = |\langle x^k\rangle| = \frac{40}{\gcd(40,k)} = 10$$

$\Rightarrow \gcd(40,k) = 4 \Rightarrow k = 4, 12, 28, 36$

So, $x^4, x^{12}, x^{28}, x^{36}$ have order 10.

(Note that we expect to have $\phi(10)$ elements of order 10 and that's what we get)

#54) G group

Let $a,b \in G$. If $\gcd(|a|,|b|)=1$ show that $\langle a\rangle \cap \langle b\rangle = \{e\}$

Proof Suppose $\exists\ c \in \langle a\rangle \cap \langle b\rangle$ and $c \neq e$

$\Rightarrow c \in \langle a\rangle$ and $c \in \langle b\rangle$

$\Rightarrow c = a^t$ for some $t < |a|$, $c = b^s$ for some $s < |b|$

Then $c^{|a|} = (a^t)^{|a|} = (a^{|a|})^t = e$.

But $c^{|a|} = (b^s)^{|a|} = b^{s|a|} = e$.

Then $|b| \mid s|a|$ (divides). That is $\frac{s|a|}{|b|}$ is an integer.

Since $s < |b|$, $|a|$ should have a common factor with $|b|$ to cancel out the denominator.

But $|a|$ and $|b|$ are relatively prime so we get a contradiction.

The contradiction comes from our assumption that there is a $c \neq e$ in $\langle a\rangle \cap \langle b\rangle$.

So, $\langle a\rangle \cap \langle b\rangle = \phi$.

#62 Prove that

$$H = \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \mid n \in \mathbb{Z} \right\}$$

is a cyclic group of $GL(2,\mathbb{R})$

1) $H \neq \phi$ b/c $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in H$

2) $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ = identity in H

3) $\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -n \\ 0 & 1 \end{bmatrix}$

(check that $\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & -n \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & -n \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$)

Claim $H = \left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\rangle$

Can any element $\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$ be written as a power of $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$?

Yes.

$$\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n$$

Proof: Use induction

Initial case $n=1$

$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^1$ ✓ true

Assume works for n.

$\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n$

Show for $n+1$.

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{n+1} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$ by inductive assumption

$$= \begin{bmatrix} 1 & n+1 \\ 0 & 1 \end{bmatrix}$$

So, works for all $n \in \mathbb{Z}^+$