SOLUTIONS TO PROBLEMS 25 – 28 FOR LECTURE 7

$\boxed{P25}$ #24 of pg. 83 Gallian

$\boxed{\text{For any } a \in G \text{ (a group) show } \langle a \rangle \leq C(a)}$

Notice $\langle a \rangle \leq G$ is known from our previous work. Thus, it suffices to demonstrate $\langle a \rangle \subseteq C(a)$ since we know $\langle a \rangle$ is non-empty and closed under the group operation. Let $a^k \in \langle a \rangle$ where $k \in \mathbb{Z}$

Notice, $\underline{a^k a = a^{k+1} = a a^k}_{\,*}$ thus $a^k \in C(a)$

and we conclude $\langle a \rangle \leq C(a)$. //

<u>Remark:</u> it's not a bad thing if you proved $\langle a \rangle \leq G$ in the process of solving $\boxed{P25}$. I'm also operating under the assumption we know how to prove $a^k a^j = a^{k+j}$ hence we're free to use laws of exponents in (*)

$\boxed{P26}$ Subgroup Lattice Diagrams / # 32, 33 and 34 on pg. 84 Gallian

#32) $\mathbb{Z}_{12}$ has 1, 2, 3, 4, 6, 12 as positive divisors

$$\begin{tikzcd}
 & \langle 1 \rangle & \\
\langle 3 \rangle \arrow[ur] & & \langle 2 \rangle \arrow[ul] \\
\langle 6 \rangle \arrow[u] \arrow[urr] & & \langle 4 \rangle \arrow[u] \\
 & \langle 0 \rangle \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

#34) $\mathbb{Z}_8$ has 1, 2, 4, 8 as divisors

$$\begin{tikzcd}
\langle 1 \rangle \\
\langle 2 \rangle \arrow[u] \\
\langle 4 \rangle \arrow[u] \\
\langle 0 \rangle \arrow[u]
\end{tikzcd}$$

#33) $\mathbb{Z}_{p^2q}$ where $p \neq q$ are primes, have divisors p, p^2, q, pq, p^2q of $\mathbb{Z}_{p^2q}$

$$\begin{tikzcd}
 & \langle 1 \rangle & \\
\langle p \rangle \arrow[ur] & & \langle q \rangle \arrow[ul] \\
\langle p^2 \rangle \arrow[u] & & \langle pq \rangle \arrow[u] \arrow[ull] \\
 & \langle 0 \rangle \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

P27 Gallian exercise # 41 of Chpt. 4

Suppose $a, b \in G$ (a group) and $|a| = m$ and $|b| = n$.
If $\langle a\rangle \cap \langle b\rangle = \{e\}$, prove that G contains an element whose order is $\text{lcm}(m,n)$ provided we assume $ab = ba$.
Show this may fail when considering $a, b \in G$ with $ab \neq ba$.

I'll follow Gallian's hint.

Let $t = \text{lcm}(m,n)$ and $|ab| = s$. Note $t = mm'$ and $t = nn'$ for some m', n'.

Since $ab = ba$ we have $(ab)^t = a^t b^t = a^{mm'} b^{nn'} = (a^m)^{m'} (b^n)^{n'} = e$,

as $a^m = e$ and $b^n = e$ since $|a| = m$ and $|b| = n$ was assumed from the outset. Observe $(ab)^t = e$ and $|ab| = s$ thus $s \mid t$.

Note also $e = (ab)^s = a^s b^s \Rightarrow a^s = b^{-s} \Rightarrow a^s, b^{-s} \in \langle a\rangle \cap \langle b\rangle = \{e\}$.

but $a^m = e$ and $a^s = e \Rightarrow m \mid s$

and $b^n = e$ and $b^{-s} = e \Rightarrow n \mid s$

Hence $t = \text{lcm}(m,n)$ also divides s. So, $s \mid t$ and $t \mid s$ hence $\underline{s = t}$.

In summary ab has order $\text{lcm}(|a|, |b|)$ provided $\langle a\rangle \cap \langle b\rangle = \{e\}$ and $ab = ba$.

//

Nonabelian case, consider $D_3 = \{1, x, x^2, y, xy, x^2y\}$ — $x^3 = 1$, $y^2 = 1$, $(xy)^2 = 1$

$a = xy$ and $b = x^2y$ have order two and $\langle a\rangle = \{1, xy\}$ and $\langle b\rangle = \{1, x^2y\}$ so $\langle a\rangle \cap \langle b\rangle = \{1\}$.
Aww... this is not the one I want...

$a = x$ and $b = xy$ has $\text{lcm}(|a|, |b|) = 6$
$\langle a\rangle = \{1, x, x^2\}$ & $\langle b\rangle = \{1, xy\}$ have $\langle a\rangle \cap \langle b\rangle = \{1\}$

yet there is no element of order 6 in D_3. In fact, 1 has order 1, $\{y, xy, x^2y\}$ order 2, $\{x, x^2\}$ order 3, that's it.

28 If G is an Abelian group which contains cyclic subgroups of orders 4 and 5 then what other sizes of cyclic subgroups must G contain?

Notice, G is not given to be cyclic so we cannot simply argue from Th^{m} 1.7.5. Some calculation is needed here. We have $a \in G$ for which $|a| = 4$ and

$\langle a \rangle = \{e, a, a^2, a^3\}$ the cyclic subgroup of order 4.

Likewise, $\exists\, b \in G$ for which $|b| = 5$ and $|\langle b \rangle| = 5$.

Consider $\langle a^2 \rangle = \{e, a^2\} \leq \langle a \rangle \leq G$ thus $|\langle a^2 \rangle| = 2$.

Also, $(ab)^{20} = a^{20} b^{20}$ as $ab = ba \Rightarrow (ab)^n = a^n b^n$ (prove it!)

thus $(ab)^{20} = (a^4)^5 (b^5)^4 = e$ and $(ab)^j = a^j b^j \neq e$ as

$20 = \text{lcm}(4,5)$ it is the first number to make a common multiple of both 4 and 5 hence $|ab| = 20$ and we find $\langle ab \rangle$ is cyclic subgroup of order 20.

$\langle ab \rangle = \{e, ab, a^2b^2, a^3b^3, b^4, a, a^2b, \dots, a^3b^4\}$ (no particular order intended)

Notice $\text{lcm}(2,5) = 10$ and $(a^2 b)^{10} = a^{20} b^{10} = (a^4)^5 (b^5)^2 = e$

and we have $\langle a^2 b \rangle$ a cyclic subgroup of order 10

Finally, $\langle e \rangle = \{e\}$ is cyclic subgroup of order 1.

In summary, we also get $\underbrace{\langle a^2 \rangle}_{\text{order: } 2}$, $\underbrace{\langle a^2 b \rangle}_{10}$, $\underbrace{\langle ab \rangle}_{20}$ and $\underbrace{\langle e \rangle}_{1}$

—(this problem is way easier if G is cyclic!)—