SOLUTIONS TO PROBLEMS 21 – 24 (FOR LECTURE 6)

**P21** Suppose $|a| = 24$. Find generator $\langle a^{21}\rangle \cap \langle a^{10}\rangle$ then, generalize for $\langle a^m\rangle \cap \langle a^n\rangle$. Gallian #13 of Chpt. 4

$$\langle a^{21}\rangle \cap \langle a^{10}\rangle = \{ x \mid \exists k, l \in \mathbb{Z} \text{ and } (a^{21})^k = (a^{10})^l = x \}$$

Thus $a^{21k} = a^{10l} \Rightarrow a^{21k - 10l} = e$

since $|a| = 24$ we find $21k - 10l$ is divided by 24.

that is $24 \mid (21k - 10l)$ or $21k - 10l = 24j$ for some $j \in \mathbb{Z}$.

Equivalently, solve $21k - 10l = 0 \mod 24$.

Naturally, we see $k = 10$ and $l = 21$ as a sol$^{\underline{n}}$

That is to observe $(a^{21})^{10} = (a^{10})^{21}$ where $\text{lcm}(10, 21) = 10(21)$.

Simplifying, $210 = 18 \mod 24$ $\therefore$ $\boxed{a^{18} \text{ generates } \langle a^{21}\rangle \cap \langle a^{10}\rangle}$

**Remark:** we we're not asked to find <u>all</u> generators of $\langle a^{21}\rangle \cap \langle a^{10}\rangle$. Note, $|a^{18}| = \dfrac{24}{\gcd(24,18)} = \dfrac{24}{6} = 4$.
Thus $\langle a^{21}\rangle \cap \langle a^{10}\rangle = \{1, a^{18}, a^{36}, a^{54}\} = \{1, a^{18}, a^{12}, a^{6}\}$.
Since $U(4) = \{1, 3\}$ we note $(a^{18})^3 = a^{54} = a^6$ also generates $\langle a^{21}\rangle \cap \langle a^{10}\rangle$.

Generally, if $a^k = e$, that is $|a| = k$ if $x \in \langle a^m\rangle \cap \langle a^n\rangle$ then $x = (a^m)^l$ and $x = (a^n)^j$ and $a^{ml - nj} = e$. Hence, we need to find $l, j$ for which $k \mid (ml - nj)$ that is solve $ml - nj = 0 \mod (k)$. Choosing $l = n$, $j = m$ gives a sol$^{\underline{n}}$, but, it might not serve as a generator.
In contrast, if $ml = nj = \text{lcm}(m,n)$ then no smaller $x$ has $x = ml = nj$. For example, $\langle a^8\rangle \cap \langle a^{12}\rangle$ in $|a| = 100$ has generator $a^{24}$ since $\text{lcm}(8,12) = 24$, whereas $a^{8(12)} = a^{96}$ would not generate $\langle a^8\rangle \cap \langle a^{12}\rangle$.

PROBLEM 22  294 has divisors in $\mathbb{N}$ of 1, 2, 3, 6, 12, 7, 14, 21, 42, 49, 98, 147, 294

(a.) $294 = 2(147) = 2(3)(49) = 2(3)(7)(7)$

| order | 1 | 2 | 3 | 6 | 7 | 14 | 21 | 42 | 49 | 98 | 147 | 294 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| # of order above | 1 | 1 | 2 | 2 | 6 | 6 | 12 | 12 | 42 | 42 | 84 | 84 |

Using my announcement, $\phi(ab) = \phi(a)\phi(b)$ for $\gcd(a,b) = 1$ and $\phi(p^k) = p^k - p^{k-1}$

$\phi(21) = \phi(3)\phi(7) = 2(6)$

$\phi(42) = \phi(6)\phi(7) = 2(6)$

$\phi(49) = \phi(7^2) = 7^2 - 7 = 42$

$\phi(98) = \phi(2)\phi(49) = 1(42) = 42$

$\phi(147) = \phi(3)\phi(49) = 2(42) = 84$

$\phi(294) = \phi(6)\phi(49) = 2(42) = 84$

- Notice, $1+1+2+2+6+6+12+12+42+42+84+84 = 294$ which is a nice check on my work. Every element of $\mathbb{Z}_{294}$ has an order.

- The elements of a given order are easily deduced from the theory in LECTURES 6 & 7 or Chpt. 4 of Gallian.
  - For example, since $\frac{294}{3} = 98$ we have $|\langle 98 \rangle| = 3$ and $U(3) = \{1, 2\}$ tells me $2(98) = 196$ also generates the subgroup of order 3; $\langle 98 \rangle = \{0, 98, 196\}$.
  - or, since $\frac{294}{21} = 14$ we have $|\langle 14 \rangle| = 21$ and since $U(21) = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$ we are able to generate $\langle 14 \rangle$ by $2(14), 4(14), 5(14), 8(14), \ldots, 19(14), 20(14)$ there are 12 generators for the 21-element subgroup $\langle 14 \rangle$.

P22 continued

(b.) $D_{294} = \{1, x, \dots, x^{293}, y, xy, \dots, x^{293}y\}$ ; $x^{294}=1$, $y^2=1$, $(xy)^2=1$.

The subgroup $\langle x \rangle$ has order 294 and hence the same structure as $\mathbb{Z}_{294}$. For example,

$$\langle x^{98} \rangle = \{1, x^{98}, x^{196}\}$$ is order 3 with 2 generators

thus, among $\{1, x, \dots, x^{293}\}$ we have 2 elements of order 3.

The question that remains, what are the orders of $y, xy, \dots, x^{293}y$ ?

**Claim:** $|x^j y| = 2$ for $j = 0, 1, 2, \dots, 293$.

Proof: $j=0$ gives $x^j y = y$ and by assumption $y^2 = 1$. Suppose inductively $|x^j y| = 2$ for some $j \in \mathbb{N}$. Consider, As usual $(xy)(xy) = 1 \Rightarrow xy = yx^{-1}$ and $yx = x^{-1}y$ etc.

$$\begin{aligned}
(x^{j+1}y)(x^{j+1}y) &= x^{j+1}yx\,x^j y && : \text{def}^{\underline{n}} \text{ of } x^{j+1} \\
&= x^{j+1}x^{-1}yx^j y && : yx = x^{-1}y \\
&= (x^j y)(x^j y) && : \text{def}^{\underline{n}} \text{ of power.} \\
&= 1 && : \text{induct. hypo.}
\end{aligned}$$

Hence $|x^j y| = 2$ for $j = 0, 1, 2, \dots, 293$ by induction // Thus, we find all the terms with $y$ in $D_{294}$ are order 2,

| order | 1 | 2 | 3 | 6 | 7 | 14 | 21 | 42 | 49 | 98 | 147 | 294 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| # elements of this order | 1 | 295 | 2 | 2 | 6 | 6 | 12 | 12 | 42 | 42 | 84 | 84 |

P22 continued

(c.) how many elements of order 8 in $\mathbb{Z}_{1440000}$? List them.

$\frac{1440000}{8} = 180{,}000 \leftarrow$ element of order 8.

$\phi(8) = |U(8)| = |\{1,3,5,7\}| = 4 \leftarrow$ # of order 8 elements.

Also, $3(180{,}000)$, $5(180{,}000)$, $7(180{,}000)$

In summary, $\boxed{180{,}000 \,/\, 540{,}000 \,/\, 1{,}260{,}000 \,/\, 900{,}000}$

//

(d.) how many elements of order 7 in $\mathbb{Z}_{1440000}$?

Notice $7 \nmid 1440000$ hence there is no element of order 7 in $\mathbb{Z}_{1440000}$.

— (If there was, $\langle a \rangle$ with $7a = 0$ and $|a| = 7 \Rightarrow |\langle a \rangle| = 7$ and hence $7 \mid 1440000$ by Fund. Thm of cyclic groups but $7 \nmid 1440000$ so there is no such element) —

$\boxed{P23}$ Let $g \in G$ for some group $G$ and suppose $|g| = 120$. List the distinct elements of $\langle g^{100} \rangle$ is $g^{30} \in \langle g^{100} \rangle$?

I'll do better than was asked here. By Th$^{m}$ 1.6.15

$$\langle g^{100} \rangle = \langle g^{\gcd(120,100)} \rangle = \langle g^{20} \rangle \ \& \ |a^{100}| = \frac{120}{\gcd(120,100)} = 6$$

hence $\langle g^{100} \rangle = \langle g^{20} \rangle = \boxed{\{1, g^{20}, g^{40}, g^{60}, g^{80}, g^{100}\}}$

No, $g^{30} \notin \langle g^{100} \rangle$. Notice, $U(6) = \{1, 5\}$ so the only generator besides $g^{100}$ is $(g^{100})^5 = g^{500} = g^{20}$ or, you could look at it as $(g^{20})^5 = g^{100}$. All roads lead to just two generators for $\langle g^{100} \rangle$.

$\boxed{P24}$ Let $g, x \in G$ for some group $G$

(i) Show that $|x| = |gxg^{-1}|$

Suppose $|x| = \infty$ that is $x^n \neq e$ for all $n \in \mathbb{Z}$.
Next, let $y = gxg^{-1}$ and suppose $\exists n$ for which $y^n = e$ $(n < \infty)$
then $y^n = \underbrace{(gxg^{-1})(gxg^{-1}) \cdots (gxg^{-1})}_{n\text{-copies}} = g\underbrace{xexe \cdots x}_{n\text{-}x\text{'s}}g^{-1} = gx^ng^{-1} = e$
thus $g^{-1}eg = g^{-1}gx^ng^{-1}g \Rightarrow e = x^n$ (a contradiction to $|x| = \infty$)
Hence $\nexists n \in \mathbb{N}$ for which $y = gxg^{-1}$ has $y^n = e$ $\therefore$ $|gxg^{-1}| = \infty$.

//

Suppose $|x| = n \in \mathbb{N}$. Let $y = gxg^{-1}$ and observe

$y^m = \underbrace{(gxg^{-1})(gxg^{-1}) \cdots (gxg^{-1})}_{m\text{-copies}} = gx^mg^{-1}$ hence

$y^n = gx^ng^{-1} = geg^{-1} = gg^{-1} = e$ $\therefore$ $|y| \leq n$ $(|gxg^{-1}| \leq n)$

If $y^j = e$ for $j < n$ then $gx^jg^{-1} = e \Rightarrow x^j = g^{-1}eg = e$ for $j < n$ which contradicts $|x| = n$ $\therefore$ $y^j \neq e$ for $j = 1, 2, \ldots n-1$ and we conclude $|gxg^{-1}| = n$. Hence, in all cases, $|x| = |gxg^{-1}|$. //