# PMATH 347 Groups and Rings, Solutions to the Midterm Test, Spring 2024

**1:** (a) Show that $U_{21}$ is not cyclic.

Solution: In $U_{21} = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$ we have

| $k$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| $2^k$ | 1 | 2 | 4 | 8 | 16 | 11 | 1 |

Since $|8| = |20| = 2$ and a cyclic group has at most one element of order 2, $U_{21}$ cannot be cyclic.

(b) Show that $U_{26}$ is cyclic.

Solution: In $U_{26} = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$ we have

| $k$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| $7^k$ | 1 | 7 | 23 | 5 | 9 | 11 | 25 |

Since $|U_{26}| = 12$ we must have $|7| = 1, 2, 3, 4, 6$ or 12. From the above table, $|7| \neq 1, 2, 3, 4$ or 6, so we must have $|7| = 12$. Thus $U_{26} = \langle 7 \rangle$.

(c) Let $a \in G$ with $|a| = 40$. List all the elements $x = a^k \in \langle a \rangle$ such that $|x^6| = 10$.

Solution: Since $\varphi(10) = 4$, there are 4 elements of order 10. Note that $|a^4| = 10$ and $U_{10} = \{1, 3, 7, 9\}$ so the 4 elements of order 10 are $a^{4\cdot 1}$, $a^{4\cdot 3}$, $a^{4\cdot 7}$ and $a^{4\cdot 9}$. Thus for $x = a^k \in \langle a \rangle$ we have

$$\begin{aligned} |x^6| = 10 &\iff x^6 \in \{a^4, a^{12}, a^{28}, a^{36}\} \iff a^{6k} \in \{a^4, a^{12}, a^{28}, a^{36}\} \iff 6k \in \{4, 12, 28, 36\} \ (\bmod\ 40) \\ &\iff 3k \in \{2, 6, 14, 18\} \ (\bmod\ 20) \iff k \in \{14, 2, 18, 6\} \ (\bmod\ 20)\,. \end{aligned}$$

Thus the required elements are $x = a^2, a^6, a^{14}, a^{18}, a^{22}, a^{26}, a^{34}, a^{38}$.

**2:** (a) Find every $X \in D_{15}$ such that $X^5 F_1 = F_4 X$.

Solution: When $X = R_k$ we have

$$\begin{aligned} X^5 F_1 = F_4 X &\iff R_{5k} F_1 = F_4 R_k \iff F_{5k+1} = F_{4-k} \iff 5k+1 = 4-k \ (\bmod 15) \\ &\iff 6k = 3 \ (\bmod 15) \iff 2k = 1 \ (\bmod 5) \iff k = 3 \ (\bmod 5) \end{aligned}$$

and when $X = F_k$ we have

$$\begin{aligned} X^5 F_1 = F_4 X &\iff F_k F_1 = F_4 F_k \iff R_{k-1} = R_{4-k} \iff k-1 = 4-k \ (\bmod 15) \\ &\iff 2k = 5 \ (\bmod 15) \iff k = 10 \ (\bmod 15)\,. \end{aligned}$$

Thus the solutions are $X = R_3, R_8, R_{13}, F_{10}$.

(b) List all of the elements in each conjugacy class in $D_{10}$.

Solution: First we find the conjugacy classes of each rotation $R_\ell$. Since $R_k R_\ell R_{-k} = R_k R_{\ell-k} = R_\ell$ and $F_k R_\ell F_k = F_k F_{\ell+k} = R_{-\ell}$ we have $Cl(R_\ell) = \{R_\ell, R_{-\ell}\}$. Next we find the conjugacy class of each reflection $F_\ell$. Since $R_k F_\ell R_{-k} = R_k F_{\ell+k} = F_{\ell+2k}$ and $F_k F_\ell F_k = F_k R_{\ell-k} = F_{2k-\ell}$ we have $Cl(F_\ell) = \{F_{\ell+2k} | k \in \mathbb{Z}_5\}$. Thus the distinct conjugacy classes are

$$\{I\}\ ,\ \{R_1, R_9\}\ ,\ \{R_2, R_8\}\ ,\ \{R_3, R_7\}\ ,\ \{R_4, R_6\}\ ,\ \{R_5\}\ ,\ \{F_0, F_2, F_4, F_6, F_8\}\ ,\ \{F_1, F_3, F_5, F_7, F_9\}.$$

(c) Find two non-cyclic subgroups of order 6 in $D_9$.

Solution: We have $D_9 = \{I, R_1, R_2, R_3, \cdots, R_8, F_0, F_1, \cdots, F_8\}$. Note that

$$D_3 = \{I, R_3, R_6, F_0, F_3, F_6\}$$

is one subgroup of $D_9$. Another is

$$H = \{I, R_3, R_6, F_1, F_4, F_7\}\,;$$

indeed we have $I \in H$ and $H$ is closed under composition since $R_{3k} R_{3\ell} = R_{3(k-\ell)}$, $R_{3k} F_{3\ell+1} = F_{3(k+\ell)+1}$, $F_{3k+1} R_{3\ell} = F_{3(k-\ell)+1}$ and $F_{3k+1} F_{3\ell+1} = R_{3(k-\ell)}$. These two subgroups are not cyclic since they each contain 3 reflections $F_k$ which are of order 2 (and a cyclic group can have at most one element of order 2).

**3:** (a) Find the number of elements of each order in the group $\mathbb{Z}_4 \times \mathbb{Z}_{10}$.

Solution: We make a table listing all possibilities for $|a|$ and $|b|$ with $a \in \mathbb{Z}_4$ and $b \in \mathbb{Z}_{10}$, then summarize the results in a second table.

| $\lvert a\rvert$ | # of $a$ | $\lvert b\rvert$ | # of | $\lvert(a,b)\rvert$ | # of $(a,b)$ |
|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 |
| | | 2 | 1 | 2 | 1 |
| | | 5 | 4 | 5 | 4 |
| | | 10 | 4 | 10 | 4 |
| 2 | 1 | 1 | 1 | 2 | 1 |
| | | 2 | 1 | 2 | 1 |
| | | 5 | 4 | 10 | 4 |
| | | 10 | 4 | 10 | 4 |
| 4 | 2 | 1 | 1 | 4 | 2 |
| | | 2 | 1 | 4 | 2 |
| | | 5 | 4 | 20 | 8 |
| | | 10 | 4 | 20 | 8 |

| $\lvert(a,b)\rvert$ | # of $(a,b)$ |
|---|---|
| 1 | 1 |
| 2 | 3 |
| 4 | 4 |
| 5 | 4 |
| 10 | 12 |
| 20 | 12 |

(b) Find the number of elements of order 6 in $A_9$.

Solution: We list the possible cycle types for $\alpha \in S_9$ with $|\alpha| = 6$, we determine the parity $(-1)^\alpha$ for each, and when $(-1)^\alpha = 1$, so that $\alpha \in A_9$, we count the number of such $\alpha$.

| cycle type of $\alpha$ | $(-1)^\alpha$ | # of such $\alpha$ |
|---|---|---|
| $(abcdef)(ghi)$ | $-1$ | |
| $(abcdef)(gh)$ | $1$ | $\binom{9}{6} \cdot 5! \cdot \binom{3}{2} = 84 \cdot 120 \cdot 3$ |
| $(abcdef)$ | $-1$ | |
| $(abc)(def)(gh)$ | $-1$ | |
| $(abc)(de)(fg)(hi)$ | $-1$ | |
| $(abc)(de)(fg)$ | $1$ | $\binom{9}{3} \cdot 2 \cdot \binom{6}{4} \cdot 3 = 84 \cdot 2 \cdot 15 \cdot 3$ |
| $(abc)(de)$ | $-1$ | |

Thus the number of $\alpha \in A_9$ with $|\alpha| = 6$ is $84 \cdot 360 + 84 \cdot 90 = 84 \cdot 450 = 42 \cdot 900 = 37800$.

**4:** (a) Show that for all $p, q \in \mathbb{Q}$, the subgroup of $\mathbb{Q}$ generated by $\{p, q\}$ is cyclic.

Solution: Let $p, q \in \mathbb{Q}$. Write $p = \frac{k}{n}$ and $q = \frac{\ell}{m}$ where $k, \ell \in \mathbb{Z}$ and $n, m \in \mathbb{Z}^+$. For $r = \frac{1}{nm}$ we have $p = kr \in \langle r \rangle$ and $q = \ell r \in \langle r \rangle$ so that $\langle p, q \rangle \leq \langle r \rangle$. Since $\langle p, q \rangle$ is a subgroup of a cyclic group, it is cyclic.

In fact, we can find a formula for a generator of $\langle p, q \rangle$. To do this, write $p = \frac{k}{n}$ and $q = \frac{\ell}{n}$ where $k, \ell, n \in \mathbb{Z}$ with $n \neq 0$ (we are using a common denominator for $p$ and $q$). Let $d = \gcd(k, \ell)$. We claim that $\langle p, q \rangle = \left\langle \frac{d}{n} \right\rangle$. Writing $k = ds$ and $\ell = dt$, we have $p = \frac{k}{n} = \frac{ds}{n} \in \left\langle \frac{d}{n} \right\rangle$ and $q = \frac{\ell}{n} = \frac{dt}{n} \in \left\langle \frac{d}{n} \right\rangle$ and so $\{p, q\} \subseteq \left\langle \frac{d}{n} \right\rangle \leq \mathbb{Q}$ and hence $\langle p, q \rangle \leq \left\langle \frac{d}{n} \right\rangle$. On the other hand, choosing $s, t \in \mathbb{Z}$ so that $ks + \ell t = d$ we obtain $\frac{d}{n} = \frac{ks + \ell t}{n} = as + bt \in \langle a, b \rangle$ and so $\left\langle \frac{d}{n} \right\rangle \leq \langle p, q \rangle$.

(b) Let $a, b \in \mathbb{Z}^+$ with $\gcd(a, b) = 1$ and let $S = \left\{ \frac{ka}{b^n} \,\middle|\, k \in \mathbb{Z}, n \in \mathbb{Z}^+ \right\}$. Show that $S$ is the subring of $\mathbb{Q}$ generated by $\frac{a}{b}$.

Solution: Let $R$ be the subring of $\mathbb{Q}$ generated by $\frac{a}{b}$. Note that $S$ is a ring because $0 = \frac{0 \cdot a}{b^1} \in S$, and given $x, y \in S$, say $x = \frac{ka}{b^n}$ and $y = \frac{\ell a}{b^m}$ where $k, \ell \in \mathbb{Z}$ and $n, m \in \mathbb{Z}^+$, we have $-x = \frac{(-k)a}{b^n} \in S$, $x + y = \frac{(b^m k + b^n \ell)a}{b^{n+m}} \in S$ and $xy = \frac{(k\ell a)a}{b^{n+m}} \in S$. Since $S$ is a ring and $\frac{a}{b} \in S$, we have $R \subseteq S$.

Since $\gcd(a, b) = 1$ we can choose $s, t \in \mathbb{Z}$ such that $as + bt = 1$. We have $\frac{a}{b} \in R$. Let $n \geq 1$ and suppose, inductively, that $\frac{a}{b^n} \in R$. Since $\frac{a}{b^n} \in R$ we have $\frac{as}{b^n} \in R$ and $\frac{at}{b^n} \in R$, hence $\frac{a}{b^{n+1}} = \frac{a(as+bt)}{b^{n+1}} = \frac{a}{b} \cdot \frac{as}{b^n} + \frac{at}{b^n} \in R$. By induction, $\frac{a}{b^n} \in R$ for all $n \in \mathbb{Z}^+$, hence $\frac{ka}{b^n} \in R$ for all $k \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$, so that $S \subseteq R$.

(c) Determine whether for all $p, q \in \mathbb{Q}$ there exists $a \in \mathbb{Q}$ such that the subring of $\mathbb{Q}$ generated by $\{p, q\}$ is also generated (as a subring) by $\{a\}$.

Solution: This is true. For $X \subseteq \mathbb{Q}$, let $\langle X \rangle$ denote the additive subgroup of $\mathbb{Q}$ generated by $X$, and let $[X]$ denote the subring of $\mathbb{Q}$ generated by $X$, and note that $\langle X \rangle \subseteq [X]$. Let $p, q \in \mathbb{Q}$. By Part (a), we can choose $a \in \mathbb{Q}$ such that $\langle p, q \rangle = \langle a \rangle$. Since $\{p, q\} \subseteq \langle a \rangle \subseteq [a]$, and $[a]$ is a subring of $\mathbb{Q}$, we have $[p, q] \subseteq [a]$. Since $a \in \langle p, q \rangle \subseteq [p, q]$ and $[p, q]$ is a subring of $\mathbb{Q}$, we have $[a] \subseteq [p, q]$.