PMATH 347 Groups and Rings, Solutions to Assignment 2

1: (a) Find $Z(D_n)$.

Solution: We have $D_1 = Z(D_1) = \{I\}$ and $D_2 = Z(D_2) = \{I, R_1, F_0, F_1\}$. Let $n \geq 2$. We claim that $Z(D_n) = \{I\}$ if n is odd and $Z(D_n) = \{I, R_{n/2}\}$ when n is even. Fix $k \in \mathbb{Z}_n$. Note that $F_k R_1 = F_{k-1}$ and $R_1 F_k = F_{k+1}$, but $F_{k-1} \neq F_{k+1}$ since $n \geq 2$ and so $F_k \notin Z(D_n)$. Let us determine whether $R_k \in D_n$. For $l \in \mathbb{Z}_n$, we have $R_k R_l = R_{k+l} = R_l R_k$, and we have $R_k F_l = F_{k+l}$ while $F_l R_k = F_{l-k}$ so that $R_k F_l = F_l R_k \iff k + l = l - k \iff 2k = 0$. Thus if n is odd then $R_k \in Z(D_n) \iff k = 0$ and if n is even then $R_k \in Z(D_n) \iff k = 0, \frac{n}{2}$.

(b) Find $Z\big(GL_n(\mathbb{R})\big)$.

Solution: We claim that $Z\big(GL_n(\mathbb{R})\big) = \big\{aI \big| a \in \mathbb{R}^*\big\}$. It is clear that for $a \in \mathbb{R}^*$ we have $aI \in Z\big(GL_n(\mathbb{R})\big)$ since $(aI)X = aX = X(aI)$ for all $X \in GL_n(\mathbb{R})$. Let $A \in Z\big(GL_n(\mathbb{R})\big)$. We must show that $A = aI$ for some $a \in \mathbb{R}^*$. For $1 \leq k, l \leq n$, let E_{kl} be the $n \times n$ matrix with a 1 in position (k, l) and all other entries equal to 0. Note that $I + E_{kl} \in GL_n(\mathbb{R})$. Since $A \in Z\big(GL_n(\mathbb{R})\big)$ we must have

$$0 = A(I + E_{kl}) - (I + E_{kl})A = AE_{kl} - E_{kl}A.$$

Note that AE_{kl} is the matrix whose columns are all equal to 0 except for the l^{th} column which is equal to the k^{th} column of A, and $E_{kl}A$ is the matrix whose rows are all zero except for the k^{th} row which is equal to the l^{th} row of A. Since $AE_{kl} - E_{kl}A = 0$, it follows that all entries on the k^{th} column of A, except for the entry a_{kk}, are equal to 0, and all the entries on the l^{th} row of A, except for a_{ll}, are equal to 0, and we have $a_{kk} - a_{ll} = 0$. Thus we have $A = aI$ where $a = a_{11} = a_{22} = \cdots = a_{nn}$.

(c) Let $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix} \in GL_3(\mathbb{Z}_5)$. Find the order of the centralizer of A in $GL_3(\mathbb{Z}_5)$.

Solution: Let $X = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \in GL_3(\mathbb{Z}_5)$. Then $AX = XA \iff \begin{pmatrix} a & b & c \\ d & e & f \\ 2g & 2h & 2i \end{pmatrix} = \begin{pmatrix} a & b & 2c \\ d & e & 2f \\ g & h & 2i \end{pmatrix}$ $\iff \big(2c = c\,,\ 2f = f\,,\ 2g = g \text{ and } 2h = h\big) \iff c = f = g = h = 0$. Thus the elements in $C(A)$ are the matrices $X \in GL_3(\mathbb{Z}_5)$ of the form

$$X = \begin{pmatrix} a & b & 0 \\ d & e & 0 \\ 0 & 0 & i \end{pmatrix}.$$

For X of the above form we have $\det(X) = \det \begin{pmatrix} a & b \\ d & e \end{pmatrix} \cdot \det(i)$, so $X \in GL_3(\mathbb{Z}_5)$ when $\begin{pmatrix} a & b \\ d & e \end{pmatrix} \in GL_2(\mathbb{Z}_5)$ and $(i) \in GL_1(\mathbb{Z}_5) = {\mathbb{Z}_5}^*$. Thus

$$\big|C(A)\big| = \big|GL_2(\mathbb{Z}_5)\big| \cdot \big|GL_1(\mathbb{Z}_5)\big| = (5^2 - 1)(5^2 - 5)(5 - 1) = 24 \cdot 20 \cdot 4 = 1920.$$

2: (a) Show that U_{22} is cyclic, U_{15} is not cyclic, and U_{2^n} is not cyclic for $n \geq 3$.

Solution: Note that $U(22) = \{1, 3, 5, 7, 9, 13, 15, 17, 19, 21\}$. We have

k	0	1	2	3	4	5	6	7	8	9	10
3^k	1	3	9	5	15	1					
7^k	1	7	5	13	3	21	15	17	9	19	1

and so $\langle 3 \rangle \neq U(22)$ but $\langle 7 \rangle = U(22)$. Thus $U(22)$ is cyclic and 7 is a generator.

Note that $U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$, and we have $\langle 1 \rangle = \{1\}$, $\langle 2 \rangle = \{1, 2, 4, 8\} = \langle 8 \rangle$, $\langle 4 \rangle = \{4\}$, $\langle 7 \rangle = \{1, 7, 4, 13\} = \langle 13 \rangle$ and $\langle 11 \rangle = \{1, 11\}$. Since none of the elements generate $U(15)$, it is not cyclic.

Note that $U^{2^n} = \{1, 3, 5, 7, \ldots 2^n - 1\}$. Notice that $(2^{n-1} \pm 1)^2 = 2^{2n-2} \pm 2^n + 1 = 1$ so $U(2^n)$ has at least 2 elements of order 2. But a cyclic group can have only $\varphi(2) = 1$ element of order 2. So $U(2^n)$ is not cyclic.

(b) Find the number of cyclic subgroups of $\mathbb{Z}_9 \times \mathbb{Z}_{15}$.

Solution: We make a table listing the orders of the elements $(a, b) \in \mathbb{Z}_9 \times \mathbb{Z}_{15}$.

$\lvert a \rvert$	# of such a	$\lvert b \rvert$	# of such B	$\lvert (a,b) \rvert$	# of such (a,b)
1	1	1	1	1	1
		3	2	3	2
		5	4	5	4
		15	8	15	8
3	2	1	1	3	2
		3	2	3	4
		5	4	15	8
		15	8	15	16
9	6	1	1	9	6
		3	2	9	12
		5	4	45	24
		15	8	45	48

Thus we find the following number of elements of each order n and hence, by dividing by $\varphi(n)$, we obtain the number of cyclic subgroups of order n, as follows.

n	1	3	5	9	15	45
# of (a, b) of order n	1	8	4	18	32	72
# of cyclic subgroups of order n	1	4	1	3	4	3

(c) Find a non-cyclic proper subgroup of $\mathbb{Z}_9 \times \mathbb{Z}_{15}$.

Solution: The subgroup $\langle 3 \rangle \times \langle 5 \rangle$ is not cyclic. Indeed in $\langle 3 \rangle = \{0, 3, 6\} \leq \mathbb{Z}_9$ we have $|3| = |6| = 3$ and in $\langle 5 \rangle = \{0, 5, 10\} \leq \mathbb{Z}_{15}$ we have $|5| = |10| = 3$, and so every non-identity element of $\langle 3 \rangle \times \langle 5 \rangle$ has order 3 (but if the group $\langle 3 \rangle \times \langle 5 \rangle$ was cyclic then it would have an element of order 9).

3: (a) Let G be a group and let $a, b \in G$. Show that $\langle ab, a^2b\rangle = \langle a, b\rangle$.

Solution: First we observe that for any subset $S \subseteq G$, since $\langle S\rangle$ is the intersection of all subgroups $H \leq G$ with $S \subseteq H$, it follows that if $S \subseteq H \leq G$ then $\langle S\rangle \leq H$. Since $ab \in \langle a, b\rangle$ and $a^2b = \langle a, b\rangle$ we have $\{ab, a^2b\} \subseteq \langle a, b\rangle \leq G$ and hence, by the above observation, we have $\langle ab, a^2b\rangle \leq \langle a, b\rangle$. Note that

$$(ab)(a^2b)^{-1}(ab) = ab\,b^{-1}a^{-2}ab = a\,a^{-1}b = b$$

so that we have $b = (ab)(a^2b)^{-1}(ab) \in \langle ab, a^2b\rangle$. It follows that we also have $b^{-1} \in \langle ab, a^2b\rangle$ so that $a = (ab)b^{-1} \in \langle ab, a^2b\rangle$. Since $a \in \langle ab, a^2b\rangle$ and $b \in \langle ab, a^b\rangle$ we have $\{a, b\} \subseteq \langle ab, a^2b\rangle$ hence $\langle a, b\rangle \leq \langle ab, a^2b\rangle$.

(b) Let $a, b \in \mathbb{Z}$ and let $d = \gcd(a, b)$. Show that in the group $\mathbb{Z}$ we have $\langle a, b\rangle = \langle d\rangle$.

Solution: Since $d|a$ we have $a \in \langle d\rangle$ and since $d|b$ we have $b \in \langle d\rangle$. Since $\{a, b\} \subseteq \langle d\rangle \leq \mathbb{Z}$, it follows, as observed in Part (a), that $\langle a, b\rangle \leq \langle d\rangle$. On the other hand, by Bézout's Identity, we can choose $s, t \in \mathbb{Z}$ such that $as + bt = d$ so we have $d \in \langle a, b\rangle$, so $\{d\} \subseteq \langle a, b\rangle$, hence $\langle d\rangle \leq \langle a, b\rangle$.

(c) Show that every finitely generated subgroup of $\mathbb{Q}$ is cyclic.

Solution: First we show that every subgroup of $\mathbb{Q}$ which is generated by two elements is cyclic. Let $a, b \in \mathbb{Q}$. Write $a = \frac{k}{n}$ and $b = \frac{l}{n}$ where $k, l, n \in \mathbb{Z}$ with $n \neq 0$ (we are using a common denominator for a and b). We claim that $\langle a, b\rangle = \left\langle \frac{d}{n}\right\rangle$ where $d = \gcd(k, l)$. Writing $k = ds$ and $l = dt$, we have $a = \frac{k}{n} = \frac{ds}{n} \in \left\langle \frac{d}{n}\right\rangle$ and $b = \frac{l}{n} = \frac{dt}{n} \in \left\langle \frac{d}{n}\right\rangle$ and so $\{a, b\} \subseteq \left\langle \frac{d}{n}\right\rangle \leq \mathbb{Z}$ and hence $\langle a, b\rangle \leq \left\langle \frac{d}{n}\right\rangle$. Conversely, choosing $s, t \in \mathbb{Z}$ so that $ks + lt = d$ we obtain $\frac{d}{n} = \frac{ks+lt}{n} = as + bt \in \langle a, b\rangle$ and so $\left\langle \frac{d}{n}\right\rangle \leq \langle a, b\rangle$.

Now let $n \geq 3$ and suppose, inductively, that every subgroup of $\mathbb{Q}$ which is generated by $n-1$ elements is cyclic. Let $a_1, a_2, \cdots, a_n \in \mathbb{Q}$. Choose $c \in \mathbb{Q}$ so that $\langle a_1, a_2, \cdots, a_{n-1}\rangle = \langle c\rangle$. We have $c \in \langle a_1, \cdots, a_{n-1}\rangle \leq \langle a_1, a_2, \cdots, a_n\rangle$ and we have $a_n \in \langle a_1, a_2, \cdots, a_n\rangle$ and so $\langle c, a_n\rangle \leq \langle a_1, a_2, \cdots, a_n\rangle$. We have $a_n \in \langle c, a_n\rangle$ and for each $i = 1, 2, \cdots, n-1$ we have $a_i \in \langle a_1, \cdots, a_{n-1}\rangle = \langle c\rangle \leq \langle c, a_n\rangle$ and so $\langle a_1, a_2, \cdots, a_n\rangle \leq \langle c, a_n\rangle$. Thus $\langle a_1, a_2, \cdots, a_n\rangle = \langle c, a_n\rangle$, which is cyclic, as shown above.

(d) Find a non-cyclic proper subgroup of $\mathbb{Q}$.

Solution: Let $H = \left\{ \frac{k}{2^n} \middle| k \in \mathbb{Z}, n \in \mathrm{N}\right\}$. Then $H \leq \mathbb{Q}$ since $0 = \frac{0}{2^0} \in H$ and for $\frac{k}{2^n} \in H$ and $\frac{l}{2^m} \in H$ we have $\frac{k}{2^n} + \frac{l}{2^m} = \frac{k\cdot 2^m + l\cdot 2^n}{2^{n+m}} \in H$ and we have $-\frac{k}{2^n} = \frac{-k}{2^n} \in H$. But H cannot be cyclic since the denominators of the elements in a cyclic group (when written in reduced form) are bounded: in the cyclic group $\left\langle \frac{a}{b}\right\rangle$, the denominator of each element $\frac{ka}{b}$ is at most b.

4: (a) List all of the elements $X \in D_{28}$ such that $F_5 X^3 = X^9 F_{13}$.

Solution: In D_{28} we have

$$\begin{aligned} F_5(F_k)^3 = (F_k)^9 F_{13} &\iff F_5 F_k = F_k F_{13} \iff R_{5-k} = R_{k-13} \\ \iff 5-k = k-13 \bmod 28 &\iff 2k = 18 \bmod 28 \iff k = 9 \bmod 14 \end{aligned}$$

and

$$\begin{aligned} F_5(R_k)^3 = (R_k)^9 F_{13} &\iff F_5 R_{3k} = R_{9k} F_{13} \iff F_{5-3k} = F_{9k+13} \\ &\iff 5 - 3k = 9k + 13 \bmod 28 \iff 12k = 20 \bmod 28 \\ &\iff 3k = 5 \bmod 7 \iff k = 4 \bmod 7. \end{aligned}$$

Thus the solutions X are given by $X = F_9, F_{23}, R_4, R_{11}.R_{18}, R_{25}$.

(b) Find all subgroups of D_n.

Solution: We claim that the distinct subgroups of D_n are the groups

$$\begin{aligned} \langle R_d \rangle &= \{I, R_d, R_{2d}, \cdots, R_{n-d}\} \text{ where } d \big| n \text{ , and} \\ \langle R_d, F_r \rangle &= \{I, R_d, R_{2d} \cdots, R_{n-d}, F_r, F_{r+d}, \cdots, F_{n+r-d}\} \text{ where } d \big| n \text{ and } 0 \le r < d. \end{aligned}$$

In particular, we remark that the number of distinct subgroups of D_n is equal to $\tau(n) + \sigma(n)$ where $\tau(n)$ is the number of divisors of n and $\sigma(n)$ is the sum of the divisors of n.

First we show that the group $\langle R_d, F_r \rangle$, where $d \big| n$ and $0 \le r < d$, is equal to the set

$$S = \{I, R_d, \cdots, R_{n-d}, F_r, F_{r+d}, \cdots, F_{n+r-d}\}.$$

For $t \in \mathbb{Z}$, we have $R_{td} = {R_d}^t \in \langle R_d, F_r \rangle$ and $F_{r+td} = R_{td} F_r = {R_d}^t F_r \in \langle R_d, F_r \rangle$ and so $S \subseteq \langle R_d, F_r \rangle$. Also, S is group since it contains I and it is closed under the operation and under inversion, since for $s, t \in \mathbb{Z}$ we have $R_{sd} R_{td} = R_{(s+t)d}$, $R_{sd} F_{r+td} = F_{r+(s+t)d}$, $F_{r+sd} R_{td} = F_{r+(s-t)d}$, $F_{r+sd} F_{r+td} = R_{(s-t)d}$, $(R_{td})^{-1} = R_{-td}$ and $(F_{r+td})^{-1} = F_{r+td}$. Since S is a group which contains R_d and F_r we have $\langle R_d, F_r \rangle \subseteq S$.

Next we show that the above groups $\langle R_d \rangle$ and $\langle R_d, F_r \rangle$ are the only subgroups of D_n. Let $H \le D_n$. If H contains no reflections, then $H \le C_n = \{I, R_1, R_2, \cdots, R_{n-1}\} = \langle R_1 \rangle$ and so, by the classification of subgroups of a cyclic group, we know that $H = \langle R_d \rangle = \{I, R_d, \cdots, R_{n-d}\}$ for some positive divisor $d \big| n$. Suppose that H contains at least one reflection, say $F_k \in H$. Note that $H \cap C_n \le C_n = \langle R_1 \rangle$ and so we have $H \cap C_n = \langle R_d \rangle$ for some $d \big| n$. Write $k = qd + r$ with $0 \le r < d$. Then $F_k = F_{qd+r} = R_{qd} F_r$ and so $F_r = F_k R_{-qd} \in H$. Since $R_d \in H$ and $F_r \in H$ we have $\langle R_d, F_r \rangle \subseteq H$. It remains to show that $H \subseteq \langle R_d, F_r \rangle$. We know that every rotation in H lies in $\langle R_d, F_r \rangle$ since $H \cap C_n = \langle R_d \rangle$. It remains to show that every reflection in H lies in $\langle R_d, F_r \rangle$. And indeed, we have

$$\begin{aligned} F_l \in H &\Longrightarrow R_{l-r} = F_l F_r \in H \Longrightarrow R_{l-r} \in H \cap C_n = \langle R_d \rangle \\ &\Longrightarrow d \big| (l-r) \Longrightarrow l = r \bmod d \Longrightarrow F_l \in S = \langle R_d, F_r \rangle. \end{aligned}$$