PMATH 347 Groups and Rings, Solutions to Assignment 6

1: Let $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ and $C = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, and let $Q_8 = \langle A, B \rangle \leq GL_2(\mathbb{C})$.

(a) Show that $Q_8 = \{I, A, B, C, -I, -A, -B, -C\}$ and make the multiplication table for Q_8.

Solution: Let $S = \{I, A, B, C, -I, -A, -B, -C\}$. Note that $A^2 = -I$ and $AB = C$ so we have

$$I = A^0 \ , \ A = A^1 \ , \ B = B^1 \ , \ C = AB \ , \ -I = A^2 \ , \ -A = A^3 \ , \ -B = A^2B \text{ and } -C = A^2C = A^3B$$

which all lie in $\langle A, B\rangle$. Thus we have $S \subseteq \langle A, B\rangle$. Here is the multiplication table for S:

$X\backslash Y$	I	A	B	C	$-I$	$-A$	$-B$	$-C$
I	I	A	B	C	$-I$	$-A$	$-B$	$-C$
A	A	$-I$	C	$-B$	$-A$	I	$-C$	B
B	B	$-C$	$-I$	A	$-B$	C	I	$-A$
C	C	B	$-A$	$-I$	$-C$	$-B$	A	I
$-I$	$-I$	$-A$	$-B$	$-C$	I	A	B	C
$-A$	$-A$	I	$-C$	B	A	$-I$	C	B
$-B$	$-B$	C	I	$-A$	B	$-C$	$-I$	A
$-C$	$-C$	$-B$	A	I	C	B	$-A$	$-I$

The table shows that the set S is closed under multiplication and that each element in S has an inverse in S, and hence $S \leq GL_2(\mathbb{C})$. Since $S \leq GL_2(\mathbb{C})$ and $\{A, B\} \subseteq S$ we have $\langle A, B\rangle \subseteq S$ by the definition of $\langle A, B\rangle$.

(b) Find the number of elements of each order in Q_8.

Solution: With the help of the multiplication table, we make a table of powers, and we list the order of each element on the last row.

X	I	A	B	C	$-I$	$-A$	$-B$	$-C$
X^2	I	$-I$	$-I$	$-I$	I	$-I$	$-I$	$-I$
X^3	I	$-A$	$-B$	$-C$	$-I$	A	B	C
X^4	I	I	I	I	I	I	I	I
$\lvert X\rvert$	1	4	4	4	2	4	4	4

We see that Q_8 has 1 element of order 1, 1 element of order 2, and 6 elements of order 8.

(c) Find an abelian group which has the same number of elements of each order as $\mathbb{Z}_2 \times Q_8$.

Solution: In $\mathbb{Z}_2 \times Q_8$ we have

$\lvert a\rvert$	#	$\lvert X\rvert$	#	$\lvert(a, X)\rvert$	#
1	1	1	1	1	1
		2	1	2	1
		4	6	4	6
2	1	1	1	2	1
		2	1	2	1
		4	6	4	6

$\lvert(a, X)\rvert$	#
1	1
2	3
4	12

and in $\mathbb{Z}_4 \times \mathbb{Z}_4$ we have

$\lvert a\rvert$	#	$\lvert b\rvert$	#	$\lvert(a, b)\rvert$	#
1	1	1	1	1	1
		2	1	2	1
		4	2	4	2
2	1	1	1	2	1
		2	1	2	1
		4	2	4	2
4	2	1	1	4	2
		2	1	4	2
		4	2	4	4

$\lvert(a, b)\rvert$	#
1	1
2	3
4	12

Thus the groups $\mathbb{Z}_2 \times Q_8$ and $\mathbb{Z}_4 \times \mathbb{Z}_4$ have the same number of elements of each order.

2: (a) Find a group of the form $\mathbb{Z}_{n_1}\times\cdots\times\mathbb{Z}_{n_l}$, with $n_i \big| n_{i+1}$ for all i, which is isomorphic to $\mathbb{Z}_{18}\times\mathbb{Z}_{60}\times\mathbb{Z}_{70}\times\mathbb{Z}_{100}$.

Solution: We have

$$\begin{aligned}\mathbb{Z}_{18}\times\mathbb{Z}_{60}\times\mathbb{Z}_{70}\times\mathbb{Z}_{100} &\cong (\mathbb{Z}_2\times\mathbb{Z}_9)\times(\mathbb{Z}_4\times\mathbb{Z}_3\times\mathbb{Z}_5)\times(\mathbb{Z}_2\times\mathbb{Z}_5\times\mathbb{Z}_7)\times(\mathbb{Z}_4\times\mathbb{Z}_5)\\ &\cong (\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_4\times\mathbb{Z}_4)\times(\mathbb{Z}_3\times\mathbb{Z}_9)\times(\mathbb{Z}_5\times\mathbb{Z}_5\times\mathbb{Z}_{25})\times(\mathbb{Z}_7)\\ &\cong (\mathbb{Z}_2)\times(\mathbb{Z}_2\times\mathbb{Z}_5)\times(\mathbb{Z}_4\times\mathbb{Z}_3\times\mathbb{Z}_5)\times(\mathbb{Z}_4\times\mathbb{Z}_9\times\mathbb{Z}_{25}\times\mathbb{Z}_7)\\ &\cong \mathbb{Z}_2\times\mathbb{Z}_{10}\times\mathbb{Z}_{60}\times\mathbb{Z}_{6300}\,.\end{aligned}$$

(b) Find a group of the form $\mathbb{Z}_{n_1}\times\cdots\times\mathbb{Z}_{n_l}$, with $n_i \big| n_{i+1}$ for all i, which is isomorphic to $U_{100}/\langle 21\rangle$.

Solution: Note that $|U_{100}| = \varphi(100) = \varphi(4)\varphi(25) = 2\cdot 20 = 40$. The powers of 21 modulo 100 are $(21^k)_{k\geq 0} = (1, 21, 41, 61, 81, 1, \cdots)$, so we have $\langle 21\rangle = \{1, 21, 41, 61, 81\}$ and $|\langle 21\rangle| = 5$. Thus $|G| = 8$ and so $G \cong \mathbb{Z}_8$, $\mathbb{Z}_2\times\mathbb{Z}_4$ or $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$. Since $3\notin\langle 21\rangle$, $3^2 = 9\notin\langle 21\rangle$, $3^3 = 27\notin\langle 21\rangle$ and $3^4 = 81\in\langle 21\rangle$, we see that the coset $3\langle 21\rangle$ has order 4 in G, and so $G\not\cong\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$ (which has no elements of order 4). Also we have $9^2 = 81\in\langle 21\rangle$ and $99^2 = (-1)^2 = 1\in\langle 21\rangle$ so the cosets $9\langle 21\rangle$ and $99\langle 21\rangle$ both have order 2. These cosets are distinct since $99/9 = 11\notin\langle 21\rangle$ so G has at least 2 elements of order 2 and hence $G\not\cong\mathbb{Z}_8$. Thus $G\cong\mathbb{Z}_2\times\mathbb{Z}_4$.

(c) Find the number of distinct abelian groups of order 2,000,000 (up to isomorphism).

Solution: We have $2,000,000 = 2^7 5^6$. The possible ways to choose $(k_1, k_2, \cdots, k_l)$ with $1\leq k_1\leq k_2\leq\cdots\leq k_l$ and $k_1+k_2+\cdots+k_l = 7$ are as follows $(1,1,1,1,1,1,1)$, $(1,1,1,1,1,2)$, $(1,1,1,2,2)$, $(1,2,2,2)$, $(1,1,1,1,3)$, $(1,1,2,3)$, $(2,2,3)$, $(1,3,3)$, $(1,1,1,4)$, $(1,2,4)$, $(3,4)$, $(1,1,5)$, $(2,5)$, $(1,6)$ and (7), and so there are 15 ways to choose the terms corresponding to 2^7. The possible ways to choose $(k_1, k_2, \cdots, k_l)$ with $1\leq k_1\leq k_2\leq\cdots\leq k_l$ and $k_1+k_2+\cdots+k_l = 6$ are as follows $(1,1,1,1,1,1)$, $(1,1,1,1,2)$, $(1,1,2,2)$, $(2,2,2)$, $(1,1,1,3)$, $(1,2,3)$, $(3,3)$, $(1,1,4)$, $(2,4)$, $(1,5)$ and (6), and so there are 11 ways to choose the terms corresponding to 2^6. Thus there are $15\cdot 11 = 165$ abelian groups of order 2,000,000.

(d) Determine which abelian group of order 72 has the most elements of order 6.

Solution: We have $72 = 2^3 3^2$. The abelian groups of order 72 are the groups of the form $G = H\times K$ where $H = \mathbb{Z}_8$, $\mathbb{Z}_4\times\mathbb{Z}_2$ or $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$, and $K = \mathbb{Z}_9$ or $\mathbb{Z}_3\times\mathbb{Z}_3$. The elements of order 6 in G are the elements (a, b) with $|a| = 2$ in H and $|B| = 3$ in K. Every non-identity element of $H = \mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$ has order 2, and every non-identity element of $K = \mathbb{Z}_3\times\mathbb{Z}_3$ has order 3. So the group $G = \mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_3\times\mathbb{Z}_3$ has the most elements of order 6.

3: (a) How many ways (up to D_9 symmetry) can the elements of C_9 be coloured using 3 colours?

Solution: Let S be the set of all possible colourings (without considering the D_9 symmetry) so $|S| = 3^9$. The action of D_9 on C_9 induces an action on S. We make a table showing the value of $\big|\text{Fix}(A)\big|$ for each $A \in D_9$.

A	# of such A	$\big\|\text{Fix}(A)\big\|$
I	1	3^9
R_3, R_6	2	3^3
$R_1, R_2, R_4, R_5 . R_7, R_8$	6	3^1
$F_0, F_1, F_2, \cdots, F_9$	9	3^5

So the number of colourings, up to the D_9 symmetry, is equal to the number of orbits which is equal to

$$\big|S/G\big| = \tfrac{1}{18}\big(1 \cdot 3^9 + 2 \cdot 3^3 + 6 \cdot 3^1 + 9 \cdot 3^5\big) = 1219\,.$$

(b) How many ways (up to rotational symmetry) can the 12 vertices of a regular icosahedron be coloured using 2 colours?

Solution: Let G be the rotation group of the regular icosahedron. If we consider the action of G on the set of 12 vertices of the icosahedron, which we label by $1, 2, \cdots 12$, then we have $\big|\text{Orb}(1)\big| = 12$ and $\big|\text{Stab}(1)\big| = 5$ and so $|G| = 12 \cdot 5 = 60$. Now, let S be the set of all colourings of the 12 vertices, (without considering rotational symmetry), so that $|S| = 2^{12}$,. The action of G on the set of vertices induces an action on S. We make a table showing $\big|\text{Fix}(R)\big|$ for each $R \in G$.

R	#	$\big\|\text{Fix}(R)\big\|$	
the identity	1	2^{12}	
rotation by $\pm\frac{2\pi}{3}$ about an axis through a pair of opposite faces	20	2^4	(4 groups of 3)
rotation by π about an axis through a pair of opposite edges	15	2^6	(6 groups of 2)
rotation by $\pm\frac{2\pi}{5}, \pm\frac{4\pi}{5}$ about an axis through a pair of opposite vertices	24	2^4	(2 vertices+ 2 groups of 5)

So the number of colourings, up to the rotational symmetry, is equal to the number of orbits which is

$$\big|S/G\big| = \tfrac{1}{60}\big(1 \cdot 2^{12} + 20 \cdot 2^4 + 15 \cdot 2^6 + 24 \cdot 2^4\big) = 96\,.$$

4: (a) Show that if G is a finite group with $|G|$ odd, and $a \in G$ with $\big|\mathrm{Cl}(a)\big| = 3$, then G is not simple.

Solution: Let G we a group with $|G|$ odd. Let $a \in G$ with $\big|\mathrm{Cl}(a)\big| = 3$. Let G act on itself by conjugation so that $\mathrm{Orb}(a) = \mathrm{Cl}(a)$. Let $H = \mathrm{Stab}(a)$. By the Orbit Stabilizer Theorem, we have $\big|G/H\big| = \big|\mathrm{Orb}(a)\big| = 3$. Since $|G|$ is even, 3 is the smallest prime divisor of $|G|$ and so we know that $H \trianglelefteq G$. Since $\big|G/H\big| = 3$ we cannot have $H = G$. Since $\big|\mathrm{Cl}(a)\big| = 3$ and $\mathrm{Cl}(e) = \{e\}$ so that $a \neq e$, and since $a \in \mathrm{Stab}(a)$, we know that $H \neq \{e\}$.

(b) Show that if a group G has a proper subgroup of finite index, then G has a proper normal subgroup of finite index.

Solution: Let G be a group with a proper subgroup $H \leq G$ with finite index $\big|G/H\big| = n$. Let G act on G/H by $a * (bH) = (ab)H$. Let $\rho : G \to \mathrm{Perm}(G/H)$ be the associated representation, given by $\rho(a)(bH) = (ab)H$. Let $K = \mathrm{Ker}(\rho) = \big\{a \in G \big| \rho(a) = I\big\} = \big\{a \in G \big| abH = bH \text{ for all } b \in G\big\}$. Note that $K \trianglelefteq G$. We have $K \leq H$ because if $a \in K$ then we have $aH = aeH = eH = H$ so that $a \in H$. Since $K \leq H \subsetneqq G$, we know that K is a proper normal subgroup of G. Also, by the First Isomorphism Theorem, we have $G/K \cong \rho(G) \leq \mathrm{Perm}(G/H)$ and so $\big|G/K\big| \leq \big|\mathrm{Perm}(G/H)\big| = n!$ so the index of K in G is finite.

(c) Show that if G is a group with $|G| = p^k$ where p is prime and $k \in \mathbb{Z}^+$, then $Z(G) \neq \{e\}$.

Solution: This follows quickly from the Conjugacy Class Equation. We provide a detailed solution which recalls the proof of the Conjugacy Class Equation. Let G act on itself by conjugation so that for each $a \in G$ we have $\mathrm{Orb}(a) = \mathrm{Cl}(a) = \{xax^{-1} | x \in G\}$. Note that

$$a \in Z(G) \iff xax^{-1} = a \text{ for all } x \in G \iff Cl(a) = \{a\} \iff |\mathrm{Cl}(a)| = 1.$$

By the Orbit Stabilizer Theorem, the order of each orbit divides $|G| = p^k$. For $i = 0, 1, \cdots, k$, let n_i be the number of orbits of size p^i. The orbits of size 1 are the orbits $\{a\}$ where $a \in Z(G)$ so we have $n_0 = |Z(G)|$. Since G is the disjoint union of the distinct orbits we have

$$p^k = |G| = \sum_{i=0}^{k} n_i p^i = n_0 + \sum_{i=1}^{k} n_i p^i = |Z(G)| + \sum_{i=1}^{k} n_i p^i$$

and so

$$|Z(G)| = p^k - \sum_{i=1}^{k} n_i p^i = 0 \mod p.$$

Since $e \in Z(G)$ so that $|Z(G)| \neq 0$, we have $|Z(G)| = kp$ for some $k \in \mathbb{Z}^+$. In particular, $Z(G) \neq \{e\}$.