PMATH 347 Groups and Rings, Solutions to Assignment 4

1: Show that no two of the groups $\mathbb{Z}_{24}$, U_{39}, D_{12}, S_4 and $SL(2,\mathbb{Z}_3)$ and are isomorphic.

Solution: In U_{39} we have $\langle 2\rangle=\{1,2,4,8,16,32,25,11,22,5,10,20\}$ so that in particular $|25|=2$, and also we have $38=-1$ so $|38|=2$. So in U_{39} there are at least 2 elements of order 2. Thus we cannot have $U_{39}\cong\mathbb{Z}_{24}$, since $\mathbb{Z}_{24}$ has only one element of order 2.

The groups D_{12} and S_4 are not abelian, so neither can be isomorphic to $\mathbb{Z}_{24}$ or to U_{39}. Also, D_{12} has 13 elements of order 2 (namely R_6 and the 12 reflections F_k) while S_4 has 9 elements of order 2 (6 of the form (ab) and 3 of the form $(ab)(cd)$) and so D_{12} is not isomorphic to S_4.

It remains to show that $SL_2(\mathbb{Z}_3)$ is not isomorphic to any of the other groups. Note that $SL_2(\mathbb{Z}_3)$ is not abelian, since for example $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ does not commute with $\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)$, and so $SL_2(\mathbb{Z}_3)$ cannot be isomorphic to $\mathbb{Z}_{24}$ or to U_{39}. Let $A=\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\in SL_2(\mathbb{Z}_3)$. Since $\det A=1$ we have $A^{-1}=\left(\begin{smallmatrix}d&-b\\-c&a\end{smallmatrix}\right)$ and so

$$A^2=I\iff A=A^{-1}\iff (a=d\text{ and }b=c=0)\iff A=\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\text{ or }\left(\begin{smallmatrix}2&0\\0&2\end{smallmatrix}\right).$$

Thus $SL_2(\mathbb{Z}_3)$ has only one element of order 2, namely $\left(\begin{smallmatrix}2&0\\0&2\end{smallmatrix}\right)$. Since D_{12} has 13 elements of order 2 and S_4 has 9 elements of order 2, $SL_2(\mathbb{Z}_3)$ cannot be isomorphic to either of these.

An alternate method is to find all 24 elements of $SL(2,\mathbb{Z}_3)$ and to find the order of each element. You should find 1 element of order 1, 1 of order 2, 8 of order 3, 6 of order 4 and 8 of order 6.

2: (a) Show that no two of the groups $\mathbb{Q}$, $\mathbb{Q}^*$ and $\mathbb{Q}^+$ are isomorphic.

Solution: In $\mathbb{Q}^*$ we have $(-1)^2=1$ so $\mathbb{Q}^*$ has an element of order 2, but in $\mathbb{Q}$, $\mathbb{Q}^+$ and $\mathbb{Q}^2$, all non-identity elements have infinite order. Thus $\mathbb{Q}^*$ is not isomorphic to any of the groups $\mathbb{Q}$, $\mathbb{Q}^+$ or $\mathbb{Q}^2$.

Note that $\mathbb{Q}^+$ cannot be isomorphic to either $\mathbb{Q}$ or $\mathbb{Q}^2$ because the element $2\in\mathbb{Q}^+$ has no square root but in $\mathbb{Q}$ and $\mathbb{Q}^2$ every element can be halved (if $\phi:\mathbb{Q}\to\mathbb{Q}^+$ was an isomorphism with $\phi(x)=2$ then we would have $\phi\big(\frac{x}{2}\big)^2=\phi\big(\frac{x}{2}+\frac{x}{2}\big)=\phi(x)=2$).

(b) Determine whether, for all $n,m\in\mathbb{Z}^+$, the groups $\mathbb{Q}^n$ and $\mathbb{Q}^m$ are isomorphic if and only if $n=m$.

Solution: This is true: let $n,m\in\mathbb{Z}^+$. If $n=m$ then $\mathbb{Q}^n=\mathbb{Q}^m$ so of course $\mathbb{Q}^n\cong\mathbb{Q}^m$. Suppose that $\mathbb{Q}^n\cong\mathbb{Q}^m$. Let $\phi:\mathbb{Q}^n\to\mathbb{Q}^m$ be a group isomorphism, meaning that ϕ is bijective wth $\phi(u+v)=\phi(u)+\phi(v)$ for all $u,v\in\mathbb{Q}^n$. Let $r\in\mathbb{Q}$ and $u\in\mathbb{Q}^n$, say $r=\frac{k}{\ell}$ with $k\in\mathbb{Z}$ and $\ell\in\mathbb{Z}^+$. Then

$$\phi(ru)=\phi\big(k\cdot\tfrac{1}{\ell}u\big)=k\phi\big(\tfrac{1}{\ell}u\big)=\tfrac{k}{\ell}\cdot\ell\phi\big(\tfrac{1}{\ell}u\big)=\tfrac{k}{\ell}\phi\big(\ell\cdot\tfrac{1}{\ell}u\big)=r\phi(u).$$

Thus $\phi:\mathbb{Q}^n\to\mathbb{Q}^m$ is a bijective linear map and hence, from linear algebra, $n=\dim(\mathbb{Q}^n)=\dim(\mathbb{Q}^m)=m$.

(c) Determine whether any two of the rings $\mathbb{Q}^2$, $\mathbb{Q}[\sqrt{2}\,]$ and $\mathbb{Q}[\sqrt{3}\,]$ are isomorphic (as rings).

Solution: We claim that no two of these rings are isomorphic. First we show that $\mathbb{Q}^2\not\cong\mathbb{Q}[\sqrt{2}]$. Suppose, for a contradiction, that $\phi:\mathbb{Q}[\sqrt{2}]\to\mathbb{Q}^2$ is a ring isomorphism. Let $(r,s)=\phi(\sqrt{2})$ with $r,s\in\mathbb{Q}$. Then

$$(r^2,s^2)=(r,s)^2=\phi(\sqrt{2})^2=\phi\big((\sqrt{2}\,)^2\big)=\phi(2)=\phi(2\cdot 1)=2\phi(1)=2(1,1)=(2,2)$$

and this is not possible since there is no $r\in\mathbb{Q}$ with $r^2=2$. A similar argument shows that $\mathbb{Q}^2\not\cong\mathbb{Q}[\sqrt{3}]$ (because there is no $r\in\mathbb{Q}$ with $r^2=3$).

Finally we show that $\mathbb{Q}[\sqrt{2}]\not\cong\mathbb{Q}[\sqrt{3}]$. Suppose, for a contradiction, that $\phi:\mathbb{Q}[\sqrt{2}]\to\mathbb{Q}[\sqrt{3}]$ is a ring isomorphism. Say $\phi(\sqrt{2})=r+s\sqrt{3}$ with $r,s\in\mathbb{Q}$. Then in $\mathbb{Q}[\sqrt{3}]$ we have

$$2=2\cdot 1=2\phi(1)=\phi(2)=\phi\big((\sqrt{2})^2\big)=\big(\phi(\sqrt{2})\big)^2=(r+s\sqrt{3})^2=(r^2+3s^2)+2\,rs\sqrt{3},$$

so that $r^2+3s^2=2$ and $2\,rs=0$. But $2\,rs=0$ implies that $r=0$ or $s=0$, so we cannot have $r^2+3s^2=2$.

3: (a) Find a subgroup of S_4 which is isomorphic to U_8.

Solution: We have $U_8 = \{1, 3, 5, 7\}$, and its multiplication table is

$$\begin{array}{c|cccc} & 1 & 3 & 5 & 7 \\ \hline 1 & 1 & 3 & 5 & 7 \\ 3 & 3 & 1 & 7 & 5 \\ 5 & 5 & 7 & 1 & 3 \\ 7 & 7 & 5 & 3 & 1 \end{array}$$

Each row shows how left multiplication by the corresponding element of U_8 permutes the elements of U_8, as in Cayley's theorem. If we associate the elements $1, 3, 5, 7$ of U_8 with the elements $1, 2, 3, 4$ of $\mathbb{Z}_4$ (in that order), the multiplication table corresponds to

$$\begin{array}{c|cccc} & 1 & 2 & 3 & 4 \\ \hline 1 & 1 & 2 & 3 & 4 \\ 2 & 2 & 1 & 4 & 3 \\ 3 & 3 & 4 & 1 & 2 \\ 4 & 4 & 3 & 2 & 1 \end{array}$$

Writing the permutations in each row in cycle notation, we have $U_8 \cong \{(1), (12)(34), (13)(24), (14)(23)\}$.

(b) Find a subgroup of S_4 which is isomorphic to $\text{Aut}\big(U_8\big)$.

Solution: Let $\phi \in \text{Aut}\big(U_8\big)$. Then $\phi(1) = 1$ and ϕ permutes the elements $3, 5, 7$. Suppose, conversely, that $\phi \in \text{Perm}\big(U_8\big)$ with $\phi(1) = 1$. We consider $\phi(ab)$ in 3 cases. In the case that $a = 1$ or $b = 1$, say $b = 1$, we have $\phi(ab) = \phi(a \cdot 1) = \phi(a) = \phi(a) \cdot 1 = \phi(a)\phi(1)$. In the case that $a \neq 1$, $b \neq 1$ and $a = b$, we have $\phi(ab) = \phi(a^2) = \phi(1) = 1 = \phi(a)^2$, since $x^2 = 1$ for all x. Finally, in the case that $1, a, b$ are distinct, the multiplication table shows that $ab = c$ where c is the other element of U_8 so that $1, a, b, c$ are distinct. Then $1 = \phi(1), \phi(a), \phi(b), \phi(c)$ are also distinct since ϕ is 1:1, and so $\phi(ab) = \phi(c) = \phi(a)\phi(b)$. In all 3 cases, we see that ϕ preserves the operation. Thus $\text{Aut}\big(U_8\big) = \big\{\phi \in \text{Perm}\big(U_8\big)\big|\phi(1) = 1\big\}$.

When we associate the elements $1, 3, 5, 7 \in U_8$ with the elements $1, 2, 3, 4 \in \mathbb{Z}_4$ (in that order), the automorphisms of U_8 correspond to the permutations of $\mathbb{Z}_4$ which fix 1 and permute 2,3,4. So we have $\text{Aut}\big(U_8\big) \cong \{(1), (23), (24), (34), (234), (243)\}$.

(c) Show that $\text{Aut}(\mathbb{Z}_n) \cong U_n$.

Solution: The group homomorphisms $\phi : \mathbb{Z}_n \to \mathbb{Z}_n$ are the maps ϕ_a given by $\phi_a(k) = ka$ where $a \in \mathbb{Z}_n$. Note that $\text{Image}(\phi_a) = \langle a \rangle$, so

$$\phi_a \text{ is bijective } \iff \text{Image}(\phi_a) = \mathbb{Z}_n \iff \langle a \rangle = \mathbb{Z}_n \iff |a| = n \iff \gcd(a, n) = 1 \iff a \in U_n\,.$$

Thus the map $\Phi : U_n \to \text{Aut}(\mathbb{Z}_n)$ given by $\Phi(a) = \phi_a$ is a bijection. Finally, note that Φ is a group homomorphism since for $a, b \in \mathbb{Z}_n$ we have $\big(\phi_a \circ \phi_b\big)(k) = \phi_a\big(\phi_b(k)\big) = \phi_a(kb) = kba = kab = \phi_{ab}(k)$ and so $\Phi(ab) = \phi_{ab} = \phi_a \circ \phi_b = \Phi(a)\Phi(b)$.

4: (a) Find a formula for the number of group homomorphisms $\phi : \mathbb{Z}_n \to \mathbb{Z}_m$, where $n, m \in \mathbb{Z}^+$.

Solution: Recall that the group homomorphisms $\phi : \mathbb{Z}_n \to \mathbb{Z}_m$ are the maps ϕ_a where $a \in \mathbb{Z}_m$ with $na = 0$. Let us determine which elements $a \in \mathbb{Z}_m$ satisfy $na = 0$. Let $d = \gcd(n, m)$ and say $n = sd$ and $m = td$. Then

$$na = 0 \in \mathbb{Z}_m \iff m\big|na \iff td\big|sda \iff t\big|sa \iff t\big|a \iff a \in \langle t \rangle \,.$$

Thus the number of distinct group homomorphisms is equal to $\big|\langle t \rangle\big| = d = \gcd(n, m)$.

(b) Find a formula for the number of group homomorphisms $\phi : \mathbb{Z}_n \times \mathbb{Z}_m \to \mathbb{Z}_\ell$, where $n, m, \ell \in \mathbb{Z}^+$.

Solution: Let $\phi : \mathbb{Z}_n \times \mathbb{Z}_m \to \mathbb{Z}_l$ be a group homomorphism. Note that if $\phi(1,0) = a$ and $\phi(0,1) = b$ then $\phi(s,t) = \phi\big(s(1,0) + t(0,1)\big) = s\phi(1,0) + t\phi(0,1) = sa + tb$, so ϕ is completely determined by the values $\phi(1,0)$ and $\phi(0,1)$. Also note that if $\phi(1,0) = a$ and $\phi(0,1) = b$ then we must have $na = \phi(n,0) = \phi(0,0) = 0$ and $mb = \phi(0,m) = \phi(0,0) = 0$. Given $a, b \in \mathbb{Z}_l$ with $na = 0$ and $mb = 0$, define $\phi_{a,b} : \mathbb{Z}_n \times \mathbb{Z}_m \to \mathbb{Z}_l$ by $\phi_{a,b}(s,t) = sa + tb$. Then $\phi_{a,b}$ is well-defined since if $s_1 = s_2 \mod n$ and $t_1 = t_2 \mod m$, say $s_1 = s_2 + nx$ and $t_1 = t_2 + my$, then in $\mathbb{Z}_l$ we have $s_1 a + t_1 b = (s_2 + nx)a + (t_2 + my)b = s_2 a + t_2 b$ since $na = mb = 0$. Also, $\phi_{a,b}$ is a group homomorphism since $\phi_{a,b}\big((s_1,t_1) + (s_2,t_2)\big) = \phi_{a,b}(s_1 + t_1, s_2 + t_2) = (s_1 + t_1)a + (s_2 + t_2)b = s_1 a + s_2 b + t_1 a + t_2 b = \phi_{a,b}(s_1, s_2) + \phi_{a,b}(s_2, t_2)$. Thus the group homomorphisms $\phi : \mathbb{Z}_n \times \mathbb{Z}_m \to \mathbb{Z}_l$ are the maps $\phi_{a,b}$ where $a, b \in \mathbb{Z}_l$ with $na = 0$ and $mb = 0$. From our solution to part (a), the number of elements $a \in \mathbb{Z}_l$ with $na = 0$ is equal to $\gcd(n,l)$ and the number of elements $b \in \mathbb{Z}_l$ with $mb = 0$ is $\gcd(m,l)$, and so the number of group homomorphisms $\phi : \mathbb{Z}_n \times \mathbb{Z}_m \to \mathbb{Z}_l$ is equal to $\gcd(n,l)\gcd(m,l)$.

(c) For a positive integer n, let $\omega(n)$ denote the number of distinct prime factors of n. Find a formula (in terms of n and m, using ω) for the number of ring homomorphisms $\phi : \mathbb{Z}_n \to \mathbb{Z}_m$, where $n, m \in \mathbb{Z}^+$.

Solution: Recall that the ring homomorphisms $\phi : \mathbb{Z}_n \to \mathbb{Z}_m$ are the maps $\phi_a : \mathbb{Z}_n \to \mathbb{Z}_m$ given by $\phi_a(k) = ka$ where $a \in \mathbb{Z}_m$ with $na = 0$ and $a^2 = a$, so the number of such ring homomorphisms is equal to the number of $a \in \mathbb{Z}_m$ with $na = 0$ and $a^2 = a$. Let $m = \prod_{i=1}^{\ell} {p_i}^{k_i}$ where the p_i are distinct primes and each $k_i \in \mathbb{Z}^+$. Then we have $\mathbb{Z}_m \cong \prod_{i=1}^{\ell} \mathbb{Z}_{{p_i}^{k_i}}$, so the number of $a \in \mathbb{Z}_m$ with $na = 0$ and $a^2 = a$ is equal to the number of $(a_1, a_2, \cdots, a_\ell) \in \prod_{i=1}^{\ell} \mathbb{Z}_{{p_i}^{k_i}}$ where each $a_i \in \mathbb{Z}_{{p_i}^{k_i}}$ with $na_i = 0$ and ${a_i}^2 = a_i$ in $\mathbb{Z}_{{p_i}^{k_i}}$. For $a_i \in \mathbb{Z}$ we have

$${a_i}^2 = a_i \text{ in } \mathbb{Z}_{{p_i}^{k_i}} \iff {p_i}^{k_i}\big|({a_i}^2 - a_i) \text{ in } \mathbb{Z} \iff ({p_i}^{k_i}\big|a_i \text{ or } {p_i}^{k_i}\big|(a_i - 1)) \text{ in } \mathbb{Z} \iff (a_i = 0 \text{ or } a_i = 1) \text{ in } \mathbb{Z}_{{p_i}^{k_i}}.$$

When $a_i = 0 \in \mathbb{Z}_{{p_i}^{k_i}}$ we have $na_i = 0 \in \mathbb{Z}_{{p_i}^{k_i}}$, and when $a_i = 1 \in \mathbb{Z}_{{p_i}^{k_i}}$ we have

$$na_i = 0 \text{ in } \mathbb{Z}_{{p_i}^{k_i}} \iff n = 0 \text{ in } \mathbb{Z}_{{p_i}^{k_i}} \iff {p_i}^{k_i}\big|n \text{ in } \mathbb{Z} \iff k_i = e_{p_i}(m) \le e_{p_i}(n)$$

where $e_{p_i}(n)$ denotes the exponent of the prime p_i in the prime factorization of n. When $k_i = e_{p_i}(m) \le e_{p_i}(n)$ there are two choices for a_i, namely $a_i \in \{0,1\}$, and otherwise there is only one choice for a_i, namely $a_i = 0$. Thus the number of required elements $(a_1, a_2, \cdots, a_\ell) \in \prod_{i=1}^{\ell} \mathbb{Z}_{{p_i}^{k_i}}$ is equal to 2 to the power of the number of indices i with $1 \le i \le \ell = \omega(m)$ for which $e_{p_i}(m) \le e_{p_i}(n)$, that is

$$2^{\omega(m) - \omega(m/\gcd(n,m))}.$$