PMATH 347 Groups and Rings, Solutions to Assignment 5

1: (a) Let $H = \big\{(1),(12)(34),(13)(24),(14)(23)\big\} \leq S_4$. Show that $H \trianglelefteq S_4$ and determine which of the two groups $\mathbb{Z}_6$ and S_3 is isomorphic to S_4/H.

Solution: Since $|S_4| = 24$ and $|H| = 4$, there are 6 left cosets; $(1)H = H$, $(12)H = \{(12),(34),(1324),(1423)\}$, $(13)H = \{(13),(1234),(24),(1432)\}$, $(14)H = \{(14),(1243),(1342),(23)\}$, $(123)H = \{(123),(134),(243),(142)\}$ and $(124)H = \{(124),(143),(132),(234)\}$.

Also, we have $H(1) = H$, $H(12) = \{(12),(34),(1423),(1324)\}$, $H(13) = \{(13),(1432),(24),(1234)\}$, $H(14) = \{(14),(1342),(1243),(23)\}$, $H(123) = \{(123),(243),(142),(134)\}$, $H(124) = \{(124),(234),(143),(132)\}$. Since the left cosets are equal to the right cosets, H is normal.

Since S_4/H has 6 elements, by the Classification of Groups of Order $2p$, where p is prime, we know that either $S_4/H \cong \mathbb{Z}_6$ or $S_4/H \cong D_3$. In S_4/H we have $\big((12)H\big)^2 = \big((13)H\big)^2 = \big((14)H\big)^2 = H$, so S_4/H has (at least) 3 elements of order 2 while $\mathbb{Z}_6$ has only 2 elements of order 2, so $S_4/H \cong D_3$.

(b) Let $H = \big\langle (2,-1),(2,3)\big\rangle \leq \mathbb{Z}^2$. Show that $\big|\mathbb{Z}^2/H\big| = 8$, determine which of the three groups $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$ or ${\mathbb{Z}_2}^3$ is isomorphic to $\mathbb{Z}^2/H$, and find a surjective group homomorphism ϕ from $\mathbb{Z}^2$ to one of these three groups with $\mathrm{Ker}(\phi) = H$.

Solution: First note that $\big\langle(2,-1),(2,3)\big\rangle = \big\langle(2,-1),(8,0)\big\rangle$. Indeed, we have $(2,-1) \in \big\langle(2,-1),(8,0)\big\rangle$ and $(2,3) = -3(2,-1) + 1(8,0) \in \big\langle(2,-1),(8,0)\big\rangle$, which implies that $\big\langle(2,-1),(2,3)\big\rangle \subseteq \big\langle(2,-1),(8,0)\big\rangle$, and we also have $(2,-1) \in \big\langle(2,-1),(2,3)\big\rangle$ and $(8,0) = 3(2,-1) + 1(2,2) \in \big\langle(2,-1),(2,3)\big\rangle$ which implies that $\big\langle(2,-1),(8,0)\big\rangle \subseteq \big\langle(2,-1),(2,3)\big\rangle$. Thus $H = \big\langle(2,-1),(8,0)\big\rangle = \mathrm{Span}_{\mathbb{Z}}\big\{(2,-1),(8,0)\big\}$.

Next, we claim that every coset is of the form $(r,0)+H$ for some integer r with $0 \leq r < 8$. To show this, let $(a,b) \in \mathbb{Z}^2$. Since $b(2,-1) \in H$, we have

$$(a,b) + H = (a,b) + b(2,-1) + H = (a+2b,0) + H\,.$$

Using the Division Algorithm, write $a + 2b = 8q + r$ with $0 \leq r < 8$. Then since $q(8,0) \in H$, we have

$$(a+2b,0) + H = (a+2b,0) - q(8,0) + H = (r,0) + H\,.$$

Thus every coset is of the form $(r,0)+H$ for some r with $0 \leq r < 8$, as claimed.

Next, we claim that the 8 cosets $(r,0)+H$ with $0 \leq r < 8$ are all distinct. To show this, suppose for a contradiction that $(r_1,0)+H = (r_2,0)+H$ with $0 \leq r_1 < r_2 < 8$. Let $r = r_2 - r_1$ and note that $0 < r < 8$. Then $(r,0)+H = \big((r_2,0)-(r_1,0)\big)+H = \big((r_2,0)+H\big) - \big((r_1,0)+H\big) = (0,0)+H = H$ and so we have $(r,0) \in H$. Since $H = \big\langle(2,-1),(8,0)\big\rangle$, this means that $(r,0) = k(2,-1) + l(8,0)$ for some $k,l \in \mathbb{Z}$. To have $(r,0) = k(2,-1) + l(8,0) = (2k+8l,-k)$ we must have $k = 0$ and $r = 8l$. But r cannot be a multiple of 8 since $0 < r < 8$, so we have the desired contradiction. Thus there are exactly 8 cosets so $\big|\mathbb{Z}^2/H\big| = 8$.

Also, note that $\mathbb{Z}^2/H = \big\{(r,0)+H \big| 0 \leq r < 8\big\} = \big\langle(1,0)+H\big\rangle$, and so we have $\mathbb{Z}^2/H \cong \mathbb{Z}_8$.

Finally, let $\phi : \mathbb{Z}^2 \to \mathbb{Z}_8$ be the group homomorphism given by $\phi(k,\ell) = k + 2\ell \in \mathbb{Z}_8$. We claim that $\mathrm{Ker}\,\phi = H$. Let $(k,\ell) \in \mathrm{Ker}\,\phi$. Then $k + 2\ell = 0$ in $\mathbb{Z}_8$, that is $k + 2\ell = 0 \mod 8$ in $\mathbb{Z}$. Choose $t \in \mathbb{Z}$ such that $k + 2\ell = 8t$. Then we have $(k,\ell) = -\ell(2,-1) + t(8,0) \in \mathrm{Span}\big\{(2,-1),(8,0)\big\} = H$. Now let $(k,\ell) \in H = \mathrm{Span}\big\{(2,-1),(2,3)\big\}$, say $(k,\ell) = s(2,-1) + t(2,3)$ where $s,t \in \mathbb{Z}$. Then $\phi(k,\ell) = k + 2\ell = (2s+2t) + 2(-s+3t) = 8t = 0 \in \mathbb{Z}_8$ so that $(k,\ell) \in \mathrm{Ker}\,\phi$.

2: (The Second Isomorphism Theorem) Let G be a group and let $H, K \leq G$.

(a) Show that $HK \leq G \iff HK = KH$.

Solution: Suppose that $HK \leq G$. Let $a \in HK$. Since $HK \leq G$ we also have $a^{-1} \in HK$, say $a^{-1} = hk$ (where here and below, h and h_i denote elements of H and k and k_i denote elements in K). Then $a = k^{-1}h^{-1} \in KH$ and so we have $HK \subseteq KH$. Let $b \in KH$, say $b = k_1h_1$. Then $b^{-1} = {h_1}^{-1}{k_1}^{-1} \in HK \subseteq KH$, say $b^{-1} = k_2h_2$. Then $b = {h_2}^{-1}{k_2}^{-1} \in HK$, and so we have $KH \subseteq HK$.

Conversely, suppose that $HK = KH$. Note that $e = e \cdot e \in HK$. Suppose $a, b \in HK$, say $a = h_1k_1$ and $b = h_2k_2$. Since $k_1h_2 \in KH = HK$ we can write $k_1h_2 = h_3k_3$. Then $ab = h_1k_1h_2k_2 = h_1h_3k_3k_2 \in HK$. Thus HK is closed under the operation. Also, we have $a^{-1} = {k_1}^{-1}{h_1}^{-1} \in KH = HK$ so HK is closed under inversion.

(b) Show that if $K \trianglelefteq G$ then $K \cap H \trianglelefteq H$, $KH \leq G$ and $K \trianglelefteq KH$.

Solution: Suppose that $K \trianglelefteq G$. We shall show that $K \cap H \trianglelefteq H$ in part (c) below. We claim that $KH \leq G$. Let $a \in HK$, say $a = hk$. Since $K \trianglelefteq G$ we have $hkh^{-1} \in K$ and so $a = hkh^{-1}h \in KH$. Thus $HK \subseteq KH$. Let $b \in KH$, say $b = kh$. Since $K \trianglelefteq G$ we have $h^{-1}kh \in K$ and so $b = h\,h^{-1}kh \in HK$. Thus $KH \subseteq HK$. Since $HK = KH$ we have $HK \leq G$, by part (a). Next we note that since $K \trianglelefteq G$ we have $K \trianglelefteq L$ for every group L with $K \leq L \leq G$ (since for $k \in K$ and $l \in L$ we have $lkl^{-1} \in K$), and so in particular $K \trianglelefteq HK$.

(c) Show that if $K \trianglelefteq G$ then $H/(K \cap H) \cong KH/K$.

Solution: Let $K \trianglelefteq G$. Note that $HK = KH \leq G$ and $K \trianglelefteq KH$ by Part (b). Define $\phi : H \to KH/K$ by $\phi(h) = hK$. Note that ϕ is well-defined since $h = e \cdot h \in KH$ so that $hK \in KH/K$. Note that ϕ is a homomorphism since $\phi(h_1h_2) = h_1h_2K = (h_1K)(h_2K) = \phi(h_1)\phi(h_2)$. Note that ϕ is surjective since given $b \in KH/K$, say $b = khK$, we have $kh \in KH = HK$, say $kh = h_1, k_1$, then $\phi(h_1) = h_1K = h_1k_1K = khK$. Finally, note that $\text{Ker}(\phi) = \{h \in H \big| \phi(h) = eK\} = \{h \in H \big| hK = K\} = \{h \in H \big| h \in K\} = K \cap H$ and so by the First Isomorphism Theorem we have $K \cap H \trianglelefteq H$, as required for Part (b), and $H\big/(K \cap H) \cong KH/H$.

(d) Show that (even if $K \ntrianglelefteq G$) we have $|H|\,|K| = |KH|\,|K \cap H|$ (you may suppose that G is finite).

Solution: Since KH is the disjoint union of the distinct cosets kH with $k \in K$, and since $|kH| = |H|$ for all $k \in K$, we have $|KH| = \big|\{kH | k \in K\}\big|\,|H|$. Define $\Phi : \{kH | k \in K\} \to K/(K \cap H)$ by $\Phi(kH) = k(K \cap H)$. Then Φ is well defined since $k_1H = k_2H \Longrightarrow {k_2}^{-1}k_1 \in K \Longrightarrow {k_2}^{-1}k_1 \in (K \cap H) \Longrightarrow k_1(K \cap H) = k_2(K \cap H)$, and Φ is injective since $k_1(K \cap H) = k_2(K \cap H) \Longrightarrow {k_2}^{-1}k_1 \in (K \cap H) \Longrightarrow {k_2}^{-1}k_1 \in K \Longrightarrow k_1H = k_2H$, and Φ is clearly surjective. Thus $\big|\{kH | k \in K\}\big| = \big|K/(K \cap H)\big|$ and so we have $|KH| = |K/(K \cap H)|\,|H|$ and hence $|H|\,|K| = |KH|\,|K \cap H|$.

3: (a) (The Normalizer/Centralizer Theorem) Let G be a group and let $H \leq G$. Recall that the **centralizer** of H in G is the group $C(H) = C_G(H) = \{a \in G \big| ax = xa \text{ for all } x \in H\} \leq G$ and the **normalizer** of H in G is the group $N(H) = N_G(H) = \{a \in G \big| aH = Ha\} \leq G$. Show that $C(H) \trianglelefteq N(H)$ and that $N(H)/C(H)$ is isomorphic to a subgroup of $\text{Aut}(H)$.

Solution: First we show that $N(H) \leq G$. We have $e \in N(H)$ since $eH = H = He$. Suppose that $a, b \in N(H)$, so we have $aH = Ha$ and $bH = Hb$. Let $x \in abH$, say $x = abh$. We have $bh \in bH = Hb$, say $bh = h_1 b$, and then we have $ah_1 \in aH = Ha$, say $ah_1 = h_2 a$. Then $x = abh = ah_1 b = h_2 ab \in Hab$. This shows that $abH \subseteq Hab$. Similarly, we have $Hab \subseteq abH$ so that $abH = Hab$, and so $ab \in N(H)$. Thus $N(H)$ is closed under the operation. Let $y \in a^{-1}H$, say $y = a^{-1}h$. We have $ha \in Ha = aH$, say $ha = ah_1$. Then $y = a^{-1}h = a^{-1}haa^{-1} = a^{-1}ah_1a^{-1} = h_1a^{-1} = Ha^{-1}$. This shows that $a^{-1}H \subseteq Ha^{-1}$. Similarly, $Ha^{-1} \subseteq a^{-1}H$ so that $a^{-1}H = Ha^{-1}$. Thus $a^{-1} \in N(H)$, so $N(H)$ is closed under inversion.

Also, note that $C(H) \subseteq N(H)$ since $a \in C(H) \Longrightarrow ah = ha$ for all $h \in H \Longrightarrow aH = Ha \Longrightarrow a \in N(H)$.

Define $\phi : N(H) \to \text{Aut}(H)$ by $\phi(a) = C_a$ where $C_a : H \to H$ is the (restriction of) the conjugation map given by $C_a(x) = axa^{-1}$ for all $x \in H$. To see that the map ϕ is well-defined, we note that for $a \in N(H)$ and $h \in H$, we have $ah \in aH = Ha$, say $ah = h_1 a$, and then $C_a(h) = aha^{-1} = h_1aa^{-1} = h_1 \in H$. It follows that the conjugation map $C_a : G \to G$ does restrict to give a map $C_a : H \to H$. This restriction is an automorphism with ${C_a}^{-1} = C_{a^{-1}}$ so ϕ is well-defined. The map ϕ is a homomorphism since $\phi(ab) = C_{ab} = C_aC_b = \phi(a)\phi(b)$. Also, we have

$$\begin{aligned}\text{Ker}(\phi) &= \{a \in N(H) \big| axa^{-1} = x \text{ for all } x \in H\} = \{a \in N(H) \big| ax = xa \text{ for all } x \in H\} \\ &= N(H) \cap C(H) = C(H) \text{ since } C(H) \subseteq N(H)\,.\end{aligned}$$

By the First Isomorphism Theorem, $C(H) \trianglelefteq N(H)$ and $N(H)/C(H) \cong \phi\big(N(H)\big) \leq \text{Perm}(H)$.

(b) (The Orbit/Stabilizer Theorem) Let A be a nonempty set and let G be a finite subgroup of $\text{Perm}(A)$. For $a \in A$, the **orbit** of a is the set $\text{Orb}(a) = \{\sigma(a) \,|\, \sigma \in G\} \subseteq A$, and the **stabilizer** of a is the set $\text{Stab}(a) = \{\sigma \in G \,|\, \sigma(a) = a\}$. Show that for all $a \in A$, we have $\text{Stab}(a) \leq G$ and $|G| = \big|\text{Orb}(a)\big|\,\big|\text{Stab}(a)\big|$.

Solution: We note that $\text{Stab}(a)$ is a subgroup of G by the Finite Subgroup Test because the identity element is the identity function I which satisfies $I(a) = a$ so that $I \in \text{Stab}(a)$, and because given $\sigma, \tau \in \text{Stab}(a)$ so that $\sigma(a) = a$ and $\tau(a) = a$, we have $(\sigma\tau)(a) = \sigma(\tau(a)) = \sigma(a) = a$ so that $\sigma\tau \in \text{Stab}(a)$.

Define $F : G/\text{Stab}(a) \to \text{Orb}(a)$ by $F\big(\sigma\,\text{Stab}(a)\big) = \sigma(a)$, where $\sigma \in G$. Note that F is well-defined because for $\sigma, \tau \in G$, if $\sigma\,\text{Stab}(a) = \tau\,\text{Stab}(a)$ then $\tau^{-1}\sigma \in \text{Stab}(a)$ so that $\tau^{-1}\sigma(a) = a$ and hence $\sigma(a) = \tau\tau^{-1}\sigma(a) = \tau(\tau^{-1}\sigma(a)) = \tau(a)$. The map F is clearly surjective, and F is also injective because, given $\sigma, \tau \in G$, if $F\big(\sigma\,\text{Stab}(a)\big) = F\big(\tau\,\text{Stab}(a)\big)$ then we have $\sigma(a) = \tau(a)$ and hence $\tau^{-1}\sigma(a) = a$ so that $\sigma\,\text{Stab}(a) = \tau\,\text{Stab}(a)$. Since F is bijective, we have $\big|G/\text{Stab}(a)\big| = \big|\text{Orb}(a)\big|$. By Lagrange's Theorem, it follows that $|G| = \big|G/\text{Stab}(a)\big|\,\big|\text{Stab}(a)\big| = \big|\text{Orb}(a)\big|\,\big|\text{Stab}(a)\big|$.

4: In this problem, when R is a ring and $X \subseteq R$, $\langle X \rangle$ denotes the ideal in R generated by X.

(a) Find the number of elements in $\mathbb{Z}^2/\langle(3,1)\rangle$.

Solution: More generally, let us find the number of elements in $\mathbb{Z}^2/\langle(a,b)\rangle$ where $a,b \in \mathbb{Z}$. For $(a,b) \in \mathbb{Z}^2$ we have $\langle(a,b)\rangle = \big\{(a,b)(s,t)\big|s,t \in \mathbb{Z}\big\} = \big\{(as,bt)\big|s,t \in \mathbb{Z}\big\}$. Define a map $\phi : \mathbb{Z}^2 \to \mathbb{Z}/\langle a\rangle \times \mathbb{Z}/\langle b\rangle$ by $\phi(k,l) = (k + \langle a\rangle, l + \langle b\rangle)$. It is easy to check that ϕ is a surjective ring homomorphism with

$$\mathrm{Ker}(\phi) = \big\{(k,l) \in \mathbb{Z}^2\big|k \in \langle a\rangle, l \in \langle b\rangle\big\} = \langle(a,b)\rangle.$$

Thus $\mathbb{Z}^2/\langle(a,b)\rangle \cong \mathbb{Z}/\langle a\rangle \times \mathbb{Z}/\langle b\rangle$. We conclude that if $a = 0$ or $b = 0$ then $\big|\mathbb{Z}^2/\langle(a,b)\rangle\big| = \infty$ and otherwise $\big|\mathbb{Z}^2/\langle(a,b)\rangle\big| = |a|\,|b|$. In particular, $\big|\mathbb{Z}^2/\langle(3,1)\rangle\big| = 3$.

(b) Find the number of elements in $\mathbb{Z}[i]/\langle 3+i\rangle$.

Solution: Note that

$$\langle 3+i\rangle = \big\{(3+i)(k+i\ell)\big|k,\ell \in \mathbb{Z}\big\} = \big\{k(3+i) + \ell(-1+3i)\big|k,\ell \in \mathbb{Z}\big\} = \mathrm{Span}_{\mathbb{Z}}\big\{(3+i),(-1+3i)\big\}\,.$$

Let $H = \mathrm{Span}_{\mathbb{Z}}\,\{(3,1),(-1,3)\} \subseteq \mathbb{Z}^2$. Define $\phi : \mathbb{Z}[i]/\langle 3+i\rangle \to \mathbb{Z}^2/H$ by $\phi\big((x+iy)+\langle 3+i\rangle\big) = (x,y)+H$. The map ϕ is clearly bijective (it is an isomorphism of groups, but not of rings) so we have $\big|\mathbb{Z}[i]/\langle 3+i\rangle\big| = \big|\mathbb{Z}^2/H\big|$. Consider the quotient group $\mathbb{Z}^2/H$. Since $(10,0) = 3(-1,3)-(3,1)$ and since $(3,1) = 3(1,0)+(0,1)$ we have

$$\begin{aligned} H &= \mathrm{Span}_{\mathbb{Z}}\big\{(3,1),(-1,3)\big\} = \mathrm{Span}_{\mathbb{Z}}\big\{(3,1),(10,0)\big\} = \mathrm{Span}_{\mathbb{Z}}\big\{10(1,0),(3,1)\big\} \text{ and} \\ \mathbb{Z}^2 &= \mathrm{Span}_{\mathbb{Z}}\big\{(1,0),(0,1)\big\} = \mathrm{Span}_{\mathbb{Z}}\big\{(1,0),(3,1)\big\}. \end{aligned}$$

As in the proof of the classification of subgroups of finite free abelian groups, we have $\mathbb{Z}^2/H \cong \mathbb{Z}_{10} \times \mathbb{Z}_1 \cong \mathbb{Z}_{10}$ (as groups) and so $\big|\mathbb{Z}[i]/\langle 3+i\rangle\big| = \big|\mathbb{Z}_{10}\big| = 10$.

(c) Determine whether $\mathbb{Z}_5[i]/\langle 2+i\rangle \cong \mathbb{Z}_5$.

Solution: We claim that $\mathbb{Z}_5[i]/\langle 2+i\rangle \cong \mathbb{Z}_5$. Note that

$$\begin{aligned} \langle 2+i\rangle &= \big\{(2+i)(k+il)\big|k,l \in \mathbb{Z}_5\big\} = \big\{(2k+4l) + i\,(k+2l)\big|k,l \in \mathbb{Z}_5\big\} \\ &= \big\{(2+i)(k+2l)\big|k,l \in \mathbb{Z}_5\big\} = \big\{(2+i)\,t\big|t \in \mathbb{Z}_5\big\} = \big\{a+ib\big|a = 2b\big\} \\ &= \big\{0, 2+i, 4+2i, 1+3i, 3+4i\big\}\,. \end{aligned}$$

Define $\phi : \mathbb{Z}_5[i] \to \mathbb{Z}_5$ by $\phi(a+ib) = a+3b$. Then ϕ is a ring homomorphism since

$$\begin{aligned} \phi((a+ib)+(c+id)) &= \phi((a+c)+i(b+d)) = (a+c)+3(b+d) = a+3b+c+3d = \phi(a+ib)+\phi(c+id) \\ \phi((a+ib)(c+id)) &= \phi((ac-bd)+i(ad+bc)) = (ac+4bd)+3(ad+bc) = ac+3ad+3bc+9bd \\ &= (a+3b)(c+3d) = \phi(a+ib)\phi(c+id)\,. \end{aligned}$$

Also, ϕ is clearly surjective and we have $\mathrm{Ker}(\phi) = \big\{a+ib\big|a+3b = 0\big\} = \big\{a+ib\big|a = 2b\big\} = \langle 2+i\rangle$. By the First Isomorphism Theorem, we have $\mathbb{Z}_5[i]/\langle 2+i\rangle \cong \mathbb{Z}_5$.