MAT301H1F Groups and Symmetry: Problem Set 3 Solutions

November 18, 2017

Questions From the Textbook: for odd-numbered questions see the back of the book.

- Chapter 8: #8 Is $\mathbb{Z}_3 \oplus \mathbb{Z}_9 \approx \mathbb{Z}_{27}$?

  Solution: No. $\mathbb{Z}_{27}$ has an element of order 27; but $\mathbb{Z}_3 \oplus \mathbb{Z}_9$ does not:

  $$(a,b) \in \mathbb{Z}_3 \oplus \mathbb{Z}_9 \Rightarrow |a| = 1 \text{ or } 3, |b| = 1, 3 \text{ or } 9.$$

  Thus $|(a,b)| = \operatorname{lcm}(|a|,|b|) \leq 9$.

- Chapter 8: #12

  Solution: four non-isomorphic groups of order 12 are $A_4, D_6, \mathbb{Z}_{12}, \mathbb{Z}_2 \oplus \mathbb{Z}_6$. The first two are non-Abelian, but D_6 contains an element of order 6 while A_4 doesn't. The last two are Abelian, but $\mathbb{Z}_{12}$ contains an element of order 12 while $\mathbb{Z}_2 \oplus \mathbb{Z}_6$ doesn't. Aside: there are only *five* non-isomorphic groups of order 12; what is the other one? Not an easy question to answer.

- Chapter 8: #14

  Solution: even though D_n has a cyclic subgroup (of rotations) of order n, it is not isomorphic to $\mathbb{Z}_n \oplus \mathbb{Z}_2$ because the latter is Abelian while D_n is not.

- Chapter 8: #26 Given that $S_3 \oplus \mathbb{Z}_2$ is isomorphic to one of $A_4, D_6, \mathbb{Z}_{12}, \mathbb{Z}_2 \oplus \mathbb{Z}_6$ (see Question 12), which one is it, by elimination?

  Solution: since $S_3 \oplus \mathbb{Z}_2$ is non-Abelian it must be one of A_4, D_6. But since A_4 contains no element of order 6, and $S_3 \oplus \mathbb{Z}_2$ does, it must be D_6. (This is equivalent to saying $D_3 \oplus \mathbb{Z}_2 \approx D_6$.)

- Chapter 8: #28 List six non-isomorphic, non-Abelian groups of order 24.

  Solution: here are seven, where $\mathcal{Q}$ represents the quaternion group:

Group	elements of order 2	elements of order 3	elements of order 4	elements order 6	elements of order 8	elements of order 12
S_4	9	8	6	0	0	0
D_{12}	13	2	2	2	0	4
$A_4 \oplus \mathbb{Z}_2$	7	8	0	8	0	0
$D_6 \oplus \mathbb{Z}_2$	15	4	0	2	0	0
$D_4 \oplus \mathbb{Z}_3$	5	2	2	10	0	4
$\mathcal{Q} \oplus \mathbb{Z}_3$	1	2	6	2	0	12
$D_3 \oplus \mathbb{Z}_4$	7	2	8	2	0	4

  Isomorphic groups must have the same number of elements of each order, so none of the above groups are isomorphic to each other. (Although, you should double-check these entries!)

- Chapter 8: #42 Is $U(40) \oplus \mathbb{Z}_6 \approx U(72) \oplus \mathbb{Z}_4$?

  Solution: Yes.

  $$U(40) \oplus \mathbb{Z}_6 \approx U(5) \oplus U(8) \oplus \mathbb{Z}_6 \approx \mathbb{Z}_4 \oplus U(8) \oplus \mathbb{Z}_6$$

  and

  $$U(72) \oplus \mathbb{Z}_4 \approx U(8) \oplus U(9) \oplus \mathbb{Z}_4,$$

  and the result follows since $U(9) \approx \mathbb{Z}_6$. (Because $|U(9)| = 6$ and $|2| = 6$.)

- Chapter 8: #50 Is $\mathbb{Z}_{10} \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_6 \approx \mathbb{Z}_{60} \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_2$?

  Solution: Yes.

  $$\mathbb{Z}_{10} \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_6 \approx \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$$

  and

  $$\mathbb{Z}_{60} \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_2 \approx \mathbb{Z}_3 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2.$$

  Is $\mathbb{Z}_{10} \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_6 \approx \mathbb{Z}_{15} \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{12}$? No.

  $$\mathbb{Z}_{10} \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_6 \approx \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$$

  but

  $$\mathbb{Z}_{15} \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{12} \approx \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_4,$$

  and $\mathbb{Z}_4$ is not isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$; one is cyclic the other isn't.

- Chapter 8: #62

  Solution: $U(165) \approx U(3) \oplus U(5) \oplus U(11) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{10}$.

- Chapter 8: #70 $U(144) \approx U(140)$

  Note: for Questions 70 and 72 it helps to use the results from page 161, which I don't believe I mentioned in class:

  $$U(4) \approx \mathbb{Z}_2 \text{ and } U(2^n) \approx \mathbb{Z}_{2^{n-2}} \oplus \mathbb{Z}_2, \text{ for } n \geq 3,$$

  and

  $$U(p^n) \approx \mathbb{Z}_{p^n - p^{n-1}}, \text{ if } p \text{ is an odd prime.}$$

  Then:

  $$U(144) \approx U(16) \oplus U(9) \approx \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus Z_6$$

  and

  $$U(140) \approx U(4) \oplus U(5) \oplus U(7) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_6.$$

- Chapter 8: #72 Find n such that $U(n) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_9$.

  Solution: use $\mathbb{Z}_4 \approx U(5)$ and $\mathbb{Z}_2 \oplus \mathbb{Z}_9 \approx \mathbb{Z}_{18} \approx U(27)$. Then

  $$U(135) = U(5 \cdot 27) \approx U(5) \oplus U(27) \approx \mathbb{Z}_4 \oplus \mathbb{Z}_{18} \approx \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9.$$

- Chapter 9: #8 Prove that $\langle 3 \rangle / \langle 12 \rangle \approx \mathbb{Z}_4$ and that $\langle 8 \rangle / \langle 48 \rangle \approx \mathbb{Z}_6$

  Solution: $\langle 3 \rangle = \{0, \pm 3, \pm 6, \ldots, \pm 3m, \ldots\}$, $\langle 12 \rangle = \{0, \pm 12, \pm 24, \cdots \pm 12n, \ldots\} \leq \langle 3 \rangle$. Then

  $$\langle 3 \rangle / \langle 12 \rangle = \{p + \langle 12 \rangle \mid p \in \langle 3 \rangle\} = \{3m + \langle 12 \rangle \mid m \in \mathbb{Z}\}$$

  Then

  $$3m + \langle 12 \rangle = 3n + \langle 12 \rangle \Leftrightarrow 3m - 3n \in \langle 12 \rangle \Leftrightarrow m - n \in \langle 4 \rangle \Leftrightarrow m \equiv n \bmod 4.$$

  Thus

  $$\langle 3 \rangle / \langle 12 \rangle = \{\langle 12 \rangle, 3 + \langle 12 \rangle, 6 + \langle 12 \rangle, 9 + \langle 12 \rangle\} \approx \mathbb{Z}_4.$$

  Similarly, $\langle 8 \rangle / \langle 48 \rangle \approx \mathbb{Z}_6$; and in general, $\langle k \rangle / \langle n \rangle \approx \mathbb{Z}_{n/k}$, if k divides n.

- Chapter 9: #9 Prove that if $[G : H] = 2$, then $H \lhd G$.

  Solution: Let $x \in G$ such that $x \notin H$. Then

  $$G = H \cup xH = H \cup Hx.$$

  Thus $xH = Hx \Leftrightarrow xHx^{-1} = H$. If $x \in H$, then obviously $xHx^{-1} = H$, because $H \leq G$. Thus for all $x \in G$, $xHx^{-1} = H$ and $H \lhd G$.

- Chapter 9: #14 The order of $14 + \langle 8 \rangle$ in $\mathbb{Z}_{24}/\langle 8 \rangle$ is 4.

  Solution: find the least positive integer m such that

  $$m(14 + \langle 8 \rangle) = \langle 8 \rangle \Leftrightarrow 14m \in \langle 8 \rangle.$$

  The solution is $m = 4$.

- Chapter 9: #18 $|\mathbb{Z}_{60}/\langle 15 \rangle| = 15$

  Solution: in $\mathbb{Z}_{60}$, $\langle 15 \rangle = \{0, 15, 30, 45\}$. Thus $|\langle 15 \rangle| = 4$ and

  $$|\mathbb{Z}_{60}/\langle 15 \rangle| = \frac{60}{4} = 15.$$

- Chapter 9: #20

  Solution: in $U(20)$, $U_5(20) = \{x \in U(20) \mid x \equiv 1 \bmod 5\} = \{1, 11\}$. Then the elements in $U(20)/U_5(20)$ are

  $$U_5(20), 3U_5(20), 7U_5(20), 9U_5(20), \text{ or as sets, } \{1, 11\}, \{3, 13\}, \{7, 17\}, \{9, 19\}.$$

- Chapter 9: #24 Determine by elimination which of the following groups $\mathbb{Z}_4 \oplus \mathbb{Z}_{12}/\langle (2, 2) \rangle$ is isomorphic to: $\mathbb{Z}_8, \mathbb{Z}_4 \oplus \mathbb{Z}_2$, or $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$? Answer: $\mathbb{Z}_4 \oplus \mathbb{Z}_2$.

  First of all, $|\langle (2, 2) \rangle| = 6$ and $|\mathbb{Z}_4 \oplus \mathbb{Z}_{12}/\langle (2, 2) \rangle| = 48/6 = 8$, and of each of the three given possible groups has order 8. So we will have to look at the number of elements with given order to eliminate some of the possibilities. We have $\langle (2, 2) \rangle = \{(2, 2), (0, 4), (2, 6), (0, 8), (2, 10), (0, 0)\}$. Then for any $(a, b) \in \mathbb{Z}_4 \oplus \mathbb{Z}_{12}$,

  $$4((a, b) + \langle (2, 2) \rangle) = (4a, 4b) + \langle (2, 2) \rangle = (0, 4b) + \langle (2, 2) \rangle = \langle (2, 2) \rangle,$$

  since $4b = 0, 4$ or 8, in $\mathbb{Z}_{12}$. So there is no element of order 8, but there is one of order 4: $(0, 1) + \langle (2, 2) \rangle$.

- Chapter 9: #25 Let $G = U(32)$ and $H = \{1, 15\}$. Determine by elimination which of the following groups G/H is isomorphic to: $\mathbb{Z}_8, \mathbb{Z}_4 \oplus \mathbb{Z}_2$, or $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$?

  Again, the orders match: $|U(32)/H| = |U(32)|/2 = 16/2 = 8$. Consider $3H$; its order is 8, since

  $$3^2H = 9H = \{9, 7\} \neq H \text{ and } 3^4H = \{81, 1215\} = \{17, 31\} \neq H.$$

  Therefore $U(32)/H$ is cyclic and we must have $U(32)/H \approx \mathbb{Z}_8$.

- Chapter 9: #30 Express $U(165)$ as an internal direct product of proper subgroups in four different ways.

  First of all, $165 = 3 \cdot 5 \cdot 11$, so as an *external* direct product,

  $$U(165) \approx U(3) \oplus U(5) \oplus U(11).$$

  To express $U(165)$ as an *internal* direct product you can use the subgroups $U_t(165)$, where t divides 165:

1. $U(165) = U_3(165) \times U_{55}(165) \approx U(3) \oplus U(55)$.
2. $U(165) = U_5(165) \times U_{33}(165) \approx U(5) \oplus U(33)$.
3. $U(165) = U_{11}(165) \times U_{15}(165) \approx U(11) \oplus U(15)$.
4. $U(165) = U_3(165) \times U_5(165) \times U_{11}(165) \approx U(3) \oplus U(5) \oplus U(11)$.

- Chapter 9: #34 In $\mathbb{Z}$, let $H = \langle 5 \rangle = \{0, \pm 5, \pm 10, \dots\}, K = \langle 7 \rangle = \{0, \pm 7, \pm, 14, \dots\}$. Then $H \cap K = \{0\}$ and, since the operation in $\mathbb{Z}$ is addition,

  $$H + K = \{5m + 7n \mid m, n \in \mathbb{Z}\}.$$

  Since 5 and 7 are relatively prime, there are integers a and b such that $5a + 7b = 1$. Thus $1 \in H + K$, and so $\mathbb{Z} = \langle 1 \rangle \subset H + K$, implying $\mathbb{Z} = H + K$. So, yes: $\mathbb{Z}$ is the internal direct product of H and K.

- Chapter 9: #50 If $|G| = pq$, where p and q are primes, not necessarily distinct, then $|Z(G)| = 1$ or pq.

  Proof: let $n = |Z(G)|$. Then n divides pq, so $n = 1, p, q$ or pq. We need only rule out the two intermediate possibilities. But this follows immediately from Chapter 7, #38: in any group G, the index of $Z(G)$ in G cannot be prime. If $|Z(G)| = p$, then $[G : Z(G)] = q$; and if $|Z(G)| = q$, then $[G : Z(G)] = p$; contradicting Chapter 7, #38.

- Chapter 9: #66 Let $|G| = p^n m$, where p is prime and $gcd(p, m) = 1$. If $H \lhd G$ and $|H| = p^n$, and K is any other subgroup of G with $|K| = p^k$, then $K \subset H$.

  Proof: suppose $x \in K$. Then $xH \in G/H$ and $(xH)^m = H$ since the order of the factor group is $|G/H| = |G|/|H| = m$. On the other hand, $x^{p^k} = e$ since $|K| = p^k$, and so $(xH)^{p^k} = x^{p^k}H = eH = H$ and $|xH|$ must also divide p^k. But p^k and m are relatively prime, so $|xH| = 1 \Leftrightarrow x \in H$. Thus $x \in K \Rightarrow x \in H$; that is $K \subset H$.

- Chapter 10: #18
  - Can there be a homomorphism from $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ onto $\mathbb{Z}_8$?

    No. If $f : \mathbb{Z}_4 \oplus \mathbb{Z}_4 \longrightarrow \mathbb{Z}_8$ is an onto homomorphism, then there must be an element $(a, b) \in \mathbb{Z}_4 \oplus \mathbb{Z}_4$ such that $|f(a, b)| = 8$. This is impossible since $|(a, b)|$ is at most 4, and $|f(a, b)|$ must divide $|(a, b)|$.
  - Can there be a homomorphism from $\mathbb{Z}_{16}$ onto $\mathbb{Z}_2 \oplus \mathbb{Z}_2$?

    No. Let $f : \mathbb{Z}_{16} \longrightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_2$ be an onto homomorphism. Since $\mathbb{Z}_{16}$ is cyclic, f is completely determined by $f(1)$. If f is onto, then $|f(1)| = 2$, meaning $f(1) = (1, 0), (0, 1)$ or $(1, 1)$. On the other hand, if f is onto, $|\ker(f)| = 16/4 = 4$, and then $\ker(f) = \langle 4 \rangle$, the only subgroup of order 4 in $\mathbb{Z}_{16}$. This leads to a contradiction, since $f(2) = 2f(1) = (0, 0)$ but $2 \notin \ker(f)$.

- Chapter 10: #20
  - How many homomorphisms are there from $\mathbb{Z}_{20}$ onto $\mathbb{Z}_8$?

    None. Since f onto implies $|\mathrm{im}\,(f)| = 8$, but 8 does not divide 20.
  - How many homomorphisms are there from $\mathbb{Z}_{20}$ to $\mathbb{Z}_8$?

    Four. Let $f : \mathbb{Z}_{20} \longrightarrow \mathbb{Z}_8$ be a homomorphism; it is completely determined by $f(1)$, since $\mathbb{Z}_{20}$ is cyclic. Then $|f(1)|$ divides 20 and 8, implying that $|f(1)| = 1, 2$ or 4, and that $|\ker(f)| = 20, 10$ or 5, respectively. In the first case $f(x) = 0$; in the second case $f(1) = 4$ and $f(x) = 4x$; in the last case, $f(1) = 2$ or 6 and $f(x) = 2x$ or $6x$.

- Chapter 10: #28

  If $\phi : S_4 \longrightarrow \mathbb{Z}_2$ is onto, then $|\text{im}\,(\phi)| = 2$ and so $|\ker(\phi)| = 12$. Thus $\ker(\phi) = A_4$, the only (normal) subgroup of S_4 with order 12. The other normal subgroups of S_4 are itself, $V = \{(1),(12)(34),(13)(24),(14)(23)\}$, and $\{(1)\}$. But $\ker(\phi)$ can't be the latter two subgroups, since then $|\text{im}\,(\phi)| = 6$ or 24, respectively. Thus the only other possibility is that $\ker(\phi) = S_4$ and $\phi(\sigma) = 0$.

- Chapter 10: #30 Suppose $\phi : G \longrightarrow \mathbb{Z}_6 \oplus \mathbb{Z}_2$ is onto and $|\ker(\phi)| = 5$. Then G must have normal subgroups of orders 5, 10, 15, 20, 30 and 60.

  Proof: use the fact (Theorem 10.2, part 8) that if $H \lhd \mathbb{Z}_6 \oplus \mathbb{Z}_2$ then

  $$\phi^{-1}(H) = \{x \in G \mid \phi(x) \in H\} \lhd G.$$

  Every subgroup H of $\mathbb{Z}_6 \oplus \mathbb{Z}_2$ is normal. The eight possible subgroups of $\mathbb{Z}_6 \oplus \mathbb{Z}_2$ are

  $$\mathbb{Z}_6 \oplus \mathbb{Z}_2, \mathbb{Z}_3 \oplus \mathbb{Z}_2, \mathbb{Z}_2 \oplus \mathbb{Z}_2, \mathbb{Z}_1 \oplus \mathbb{Z}_2; \mathbb{Z}_6 \oplus \mathbb{Z}_1, \mathbb{Z}_3 \oplus \mathbb{Z}_1, \mathbb{Z}_2 \oplus \mathbb{Z}_1 \text{ and } \mathbb{Z}_1 \oplus \mathbb{Z}_1,$$

  which have orders $12, 6, 4, 2, 6, 3, 2$ and 1, respectively. Since ϕ is 5 to 1, the inverse images of these groups must have orders $60, 30, 20, 10, 30, 15, 10$ and 5, respectively.

- Chapter 10: #34 There is no homomorphism from A_4 onto $\mathbb{Z}_2$.

  Proof: if $|\text{im}\,(\phi)| = 2$ then $|\ker(\phi)| = 6$, but A_4 has no subgroup of order 6, let alone a normal subgroup of order 6.

- Chapter 10: #44 Let k divide n and suppose $f : U(n) \longrightarrow U(k)$ by $f(x) = x \bmod k$. Then $\ker(f) = U_k(n)$.

  Proof: $\ker(f) = \{x \in U(n) \mid x \equiv 1 \bmod k\} = U_k(n)$.

Other Questions:

1. Let $SO(2,\mathbb{R}) = \{A \in O(2,\mathbb{R}) \mid \det(A) = 1\}$. By considering the function $f : \mathbb{R} \longrightarrow SO(2,\mathbb{R})$ defined by $f(\theta) = [R_\theta]$, show that

$$\mathbb{R}/2\pi\mathbb{Z} \approx SO(2,\mathbb{R}).$$

(Compare with Chapter 10, #56.) Can you conclude that $\mathbb{R}/\mathbb{Z} \approx SO(2,\mathbb{R})$? Explain.

Solution: first show f is a homomorphism:

$$\begin{aligned}
f(\alpha)f(\beta) = [R_\alpha][R_\beta] &= \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}\begin{bmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{bmatrix} \\
&= \begin{bmatrix} \cos\alpha\cos\beta - \sin\alpha\sin\beta & -\cos\alpha\sin\beta - \sin\alpha\cos\beta \\ \sin\alpha\cos\beta + \cos\alpha\sin\beta & -\sin\alpha\sin\beta + \cos\alpha\cos\beta \end{bmatrix} \\
&= \begin{bmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{bmatrix} \\
&= [R_{\alpha+\beta}] = f(\alpha+\beta)
\end{aligned}$$

Now $\ker(f) = \{\theta \in \mathbb{R} \mid [R_\theta] = I\} = \{2\,k\,\pi \mid k \in \mathbb{Z}\} = 2\pi\mathbb{Z}$; so by the First Isomorphism Theorem,

$$\mathbb{R}/\ker(f) \approx \operatorname{im}(f) \Leftrightarrow \mathbb{R}/(2\pi\mathbb{Z}) \approx SO(2,\mathbb{R}),$$

since f is onto. (Every $A \in O(2,\mathbb{R})$ with $\det(A) = 1$ is a rotation matrix.) Finally, define $g : R/\mathbb{Z} \longrightarrow \mathbb{R}/2\pi\mathbb{Z}$ by

$$g(x+\mathbb{Z}) = 2\pi x + 2\pi\mathbb{Z}.$$

Then g is an isomorphism:

1. g is well-defined and one-to-one:

$$\begin{aligned}
x+\mathbb{Z} = y+\mathbb{Z} &\Leftrightarrow x - y = k, \text{ some } k \in \mathbb{Z} \\
&\Leftrightarrow 2\pi(x-y) = 2\pi k, \text{ some } k \in \mathbb{Z} \\
&\Leftrightarrow 2\pi x - 2\pi y \in 2\pi\mathbb{Z} \\
&\Leftrightarrow 2\pi x + 2\pi\mathbb{Z} = 2\pi y + 2\pi\mathbb{Z} \\
&\Leftrightarrow g(x+\mathbb{Z}) = g(y+\mathbb{Z})
\end{aligned}$$

2. g is a homomorphism:

$$g(x+y+\mathbb{Z}) = 2\pi(x+y) + 2\pi\mathbb{Z} = 2\pi x + 2\pi y + 2\pi\mathbb{Z} = g(x+\mathbb{Z}) + g(y+\mathbb{Z}).$$

3. g is onto: given $r \in \mathbb{R}$, then $g(r/(2\pi)+\mathbb{Z}) = r + 2\pi\mathbb{Z}$.

2. As demonstrated in class the symmetry group of a cube, $S(C)$, consists of the following 48 matrices

$$\begin{bmatrix} \pm1 & 0 & 0 \\ 0 & \pm1 & 0 \\ 0 & 0 & \pm1 \end{bmatrix}, \begin{bmatrix} 0 & \pm1 & 0 \\ 0 & 0 & \pm1 \\ \pm1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & \pm1 \\ \pm1 & 0 & 0 \\ 0 & \pm1 & 0 \end{bmatrix},$$

$$\begin{bmatrix} \pm1 & 0 & 0 \\ 0 & 0 & \pm1 \\ 0 & \pm1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & \pm1 \\ 0 & \pm1 & 0 \\ \pm1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & \pm1 & 0 \\ \pm1 & 0 & 0 \\ 0 & 0 & \pm1 \end{bmatrix},$$

together with usual matrix multiplication. As covered in Problem Set 2, all of the following are homomorphisms:

- $\Phi : S(C) \longrightarrow S(C)$ defined by $\Phi((a_{ij})) = (a_{ij}^2)$
- $\det : S(C) \longrightarrow \{1, -1\}$, where $\det(A)$ is the determinant of A.
- $p : S(C) \longrightarrow \{1, -1\}$ defined by $p(A) = \det(\Phi(A))$
- $q : S(C) \longrightarrow \{1, -1\}$ defined by $q(A) = \det(A\,\Phi(A))$
- $f : S(C) \longrightarrow S(C)$ defined by $f(A) = p(A)\,A$, which is actually an automorphism of $S(C)$.

(a) Find all the normal subgroups of $S(C)$. (You may assume that of the 98 subgroups of $S(C)$, only **nine** of them are normal subgroups.)

Solution: use that kernels are always normal subgroups, and that the intersection of normal subgroups is also normal. They are—although its not necessary to list all the matrices:

1. $S(C)$ itself,
2. the trivial subgroup $\{I\}$,
3. $\mathcal{Z}$, the center of $S(C)$, $\mathcal{Z} = \{I, -I\}$,
4. $$\mathcal{D} = \ker(\Phi) = \left\{ \begin{bmatrix} \pm 1 & 0 & 0 \\ 0 & \pm 1 & 0 \\ 0 & 0 & \pm 1 \end{bmatrix} \right\}$$
5. $\mathcal{V} = \{A \in \ker(\Phi) \mid \det(A) = 1\} = \ker(\det) \cap \ker(\Phi) =$
$$\left\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right\}.$$
6. $\mathcal{P} = \ker(p) = \{A \in S(C) \mid p(A) = 1\} = \{A \in S(C) \mid \det(\Phi(A)) = 1\} =$
$$\left\{ \begin{bmatrix} \pm 1 & 0 & 0 \\ 0 & \pm 1 & 0 \\ 0 & 0 & \pm 1 \end{bmatrix}, \begin{bmatrix} 0 & \pm 1 & 0 \\ 0 & 0 & \pm 1 \\ \pm 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & \pm 1 \\ \pm 1 & 0 & 0 \\ 0 & \pm 1 & 0 \end{bmatrix} \right\}.$$
7. $\mathcal{Q} = \ker(q) = \{A \in S(C) \mid q(A) = 1\} = \{A \in S(C) \mid \det(A\,\Phi(A)) = 1\} =$
$$\left\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \right.$$
$$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & -1 \\ -1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & 0 \end{bmatrix},$$
$$\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & -1 \\ 1 & 0 & 0 \\ 0 & -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & -1 \\ -1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{bmatrix},$$
$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{bmatrix},$$
$$\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & -1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \Bigg\}.$$

In summary, $\ker(q)$ consists of all the matrices in $S(C)$ with an *even* number of -1's.

8. $\mathcal{R} = \ker(\det) = \{A \in S(C) \mid \det(A) = 1\} =$

$$\Bigg\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

$$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & -1 \\ -1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & -1 \\ 1 & 0 & 0 \\ 0 & -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & -1 \\ -1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{bmatrix},$$

$$\begin{bmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 0 & -1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{bmatrix} \Bigg\}.$$

As mentioned in class, $\ker(\det)$ consists of all the matrices in $S(C)$ that represent rotational symmetries of the cube. And as proved in Theorem 7.5, $\ker(\det) \approx S_4$.

9. $\mathcal{A} = \ker(p) \cap \ker(q) \cap \ker(\det) = \{A \in S(C) \mid p(A) = q(A) = \det(A) = 1\} =$

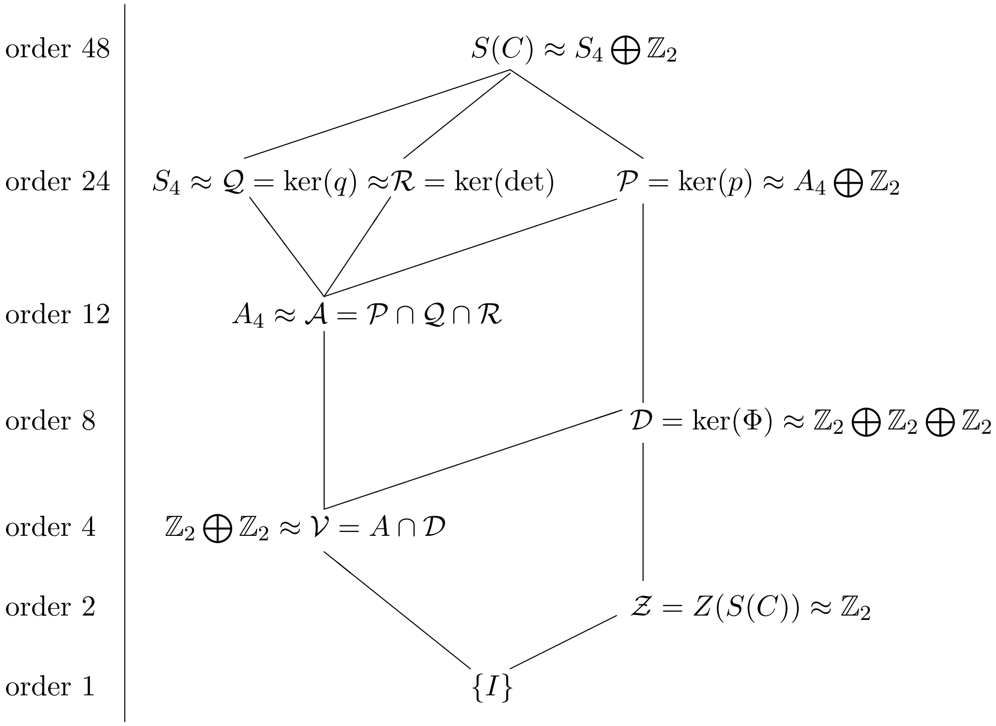
$$\Bigg\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

$$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & -1 \\ -1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & -1 \\ 1 & 0 & 0 \\ 0 & -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & -1 \\ -1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{bmatrix} \Bigg\}.$$

(b) What is the subgroup lattice of all normal subgroups of $S(C)$?

Solution: if you didn't list the matrices, you can still conclude that $\mathcal{P}, \mathcal{Q}, \mathcal{R}$ all have order 24 by the First Isomorphism Theorem, since p, q and det are all onto homomorphisms with images of order 2. The lattice of normal subgroups of $S(C)$, including information from parts (a) and (c), is



with

$$\mathcal{P} = \ker(p),\ \mathcal{Q} = \ker(q),\ \mathcal{R} = \ker(\det),\ \mathcal{A} = \mathcal{P} \cap \mathcal{Q} \cap \mathcal{R},\ \mathcal{D} = \ker(\Phi),\ \mathcal{Z} = Z(S(C)),$$

and $\mathcal{V} = \ker(\Phi) \cap \ker(\det)$.

(c) Except for the subgroup $\{I\}$, indicate in terms of $S_4, A_4, \mathbb{Z}_2$ or external direct products of two or more of these groups, to which group each normal subgroup of $S(C)$ is isomorphic.

Solution: from Problem Set 2 we know $\mathcal{Q} \approx \mathcal{R}$, and from Theorem 7.5, Chapter 7, we know that $\mathcal{R} \approx S_4$. So we can say

$$\mathcal{Z} \approx \mathbb{Z}_2,\ \mathcal{V} \approx \mathbb{Z}_2 \oplus \mathbb{Z}_2,\ \mathcal{D} \approx \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2,\ \mathcal{A} \approx A_4,\ \mathcal{P} \approx A_4 \oplus \mathcal{Z}_2,\ \mathcal{Q} \approx \mathcal{R} \approx S_4,\ S(C) \approx S_4 \oplus \mathbb{Z}_2$$

since

$$\mathcal{P} = \mathcal{A} \times \mathcal{Z} \text{ and } S(C) = \mathcal{R} \times \mathcal{Z}.$$

Finally, $\mathcal{A} \approx A_4$ since $\mathcal{A}$ is a subgroup of $\mathcal{R} \approx S_4$ with 12 elements, three of which have order 2 and eight of which have order 3. The only such subgroup of S_4 is A_4.

(d) For each normal subgroup H of $S(C)$, find a homomorphism $g : S(C) \longrightarrow S(C)$ such that $H = \ker(g)$. In each case, what is $\mathrm{im}\,(g)$ and what is it isomorphic to?

Solution: Table 1 lists sixteen possible homomorphisms from $S(C)$ to $S(C)$, in terms of $\Phi, \det, p, q$ and f, with their kernels and images. (Doubtless, there are others.) The groups $\mathcal{P}, \mathcal{Q}, \mathcal{R}, \mathcal{A}, \mathcal{D}, \mathcal{V}, \mathcal{Z}$ have already been defined; the other groups in Table 1 are

- $\mathcal{G} = \mathrm{im}\,(\Phi) =$

$$\left\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right\},$$

  which is isomorphic to D_3.
- $\mathcal{H} = \mathrm{im}\,(\Phi_p) = f(\mathcal{G})$, since $f(\Phi(A)) =$ $p(\Phi(A))\,\Phi(A) = \det(\Phi(\Phi(A)))\,\Phi(A) = \det(\Phi(A))\,\Phi(A) = p(A)\,\Phi(A) = \Phi_p(A)$. Thus

$$\mathcal{H} = \left\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \right.$$

$$\left. \begin{bmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \end{bmatrix} \right\} \approx D_3.$$

- $\mathcal{S} = \mathcal{G} \cup (-I\,\mathcal{G}) = \mathcal{G} \times \mathcal{Z} \approx D_3 \oplus \mathbb{Z}_2 \approx D_6$.
- $$\mathcal{W} = \left\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right\} \approx \mathbb{Z}_2 \oplus \mathbb{Z}_2.$$
- $$\mathcal{X} = \left\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix} \right\} \approx \mathbb{Z}_2 \oplus \mathbb{Z}_2.$$
- $$\mathcal{Y} = \left\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix} \right\} \approx \mathbb{Z}_2 \oplus \mathbb{Z}_2.$$

For items 10, 11 and 12 in Table 1 we used the facts that p, q and det satisfy $p(A)p(A) = q(A)q(A) = \det(A)\det(A) = 1$, and that

$$p(A)q(A) = \det(A),\ \ q(A)\det(A) = p(A),\ \ p(A)\det(A) = q(A).$$

For item 2 we used the fact that $\det(\det(A)\,A) = \det(A)^3\,\det(A) = 1$. For item 3 we used

$$q(q(A)\,A) = \det(q(A)A\,\Phi(q(A)A)) = q(A)^3\det(A\,\Phi(A)) = q(A)^3 q(A) = 1.$$

	homomorphism $g : S(C) \longrightarrow S(C)$	$\ker(g)$	$\mathrm{im}\,(g)$	factors of $S(C)$
1	$\iota(A) = A$	$\{I\}$	$S(C)$	ι is an isomorphism
2	$\iota_d(A) = \det(A)\, A$	$\mathcal{Z}$	$\mathcal{R}$	$S(C)/\mathcal{Z} \approx R \approx S_4$
3	$\iota_q(A) = q(A)\, A$	$\mathcal{Z}$	$\mathcal{Q}$	$S(C)/\mathcal{Z} \approx Q \approx S_4$
4	$f(A) = \iota_p(A) = p(A)\, A$	$\{I\}$	$S(C)$	f is an isomorphism
5	$\Phi((a_{ij})) = (a_{ij}^2)$	$\mathcal{D}$	$\mathcal{G}$	$S(C)/\mathcal{D} \approx \mathcal{G} \approx D_3$
6	$\Phi_d(A) = \det(A)\, \Phi(A)$	$\mathcal{V}$	$\mathcal{S}$	$S(C)/\mathcal{V} \approx \mathcal{S} \approx D_6$
7	$\Phi_q(A) = q(A)\, \Phi(A)$	$\mathcal{V}$	$\mathcal{S}$	$S(C)/\mathcal{V} \approx \mathcal{S} \approx D_6$
8	$\Phi_p(A) = p(A)\, \Phi(A)$	$\mathcal{D}$	$\mathcal{H}$	$S(C)/\mathcal{D} \approx \mathcal{H} \approx D_3$
9	$\Omega(A) = \begin{bmatrix} p(A) & 0 & 0 \\ 0 & q(A) & 0 \\ 0 & 0 & \det(A) \end{bmatrix}$	$\mathcal{A}$	$\mathcal{V}$	$S(C)/\mathcal{A} \approx \mathcal{V} \approx \mathbb{Z}_2 \oplus \mathbb{Z}_2$
10	$\Omega_d(A) = \det(A)\, \Omega(A) = \begin{bmatrix} q(A) & 0 & 0 \\ 0 & p(A) & 0 \\ 0 & 0 & 1 \end{bmatrix}$	$\mathcal{A}$	$\mathcal{W}$	$S(C)/\mathcal{A} \approx \mathcal{W} \approx \mathbb{Z}_2 \oplus \mathbb{Z}_2$
11	$\Omega_q(A) = q(A)\, \Omega(A) = \begin{bmatrix} \det(A) & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & p(A) \end{bmatrix}$	$\mathcal{A}$	$\mathcal{X}$	$S(C)/\mathcal{A} \approx \mathcal{X} \approx \mathbb{Z}_2 \oplus \mathbb{Z}_2$
12	$\Omega_p(A) = p(A)\, \Omega(A) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \det(A) & 0 \\ 0 & 0 & q(A) \end{bmatrix}$	$\mathcal{A}$	$\mathcal{Y}$	$S(C)/\mathcal{A} \approx \mathcal{Y} \approx \mathbb{Z}_2 \oplus \mathbb{Z}_2$
13	$i(A) = I$	$S(C)$	$\{I\}$	$S(C)/S(C) \approx \{I\}$
14	$i_d(A) = \det(A)\, I$	$\mathcal{R}$	$\mathcal{Z}$	$S(C)/\mathcal{R} \approx \mathcal{Z} \approx \mathbb{Z}_2$
15	$i_q(A) = q(A)\, I$	$\mathcal{Q}$	$\mathcal{Z}$	$S(C)/\mathcal{Q} \approx \mathcal{Z} \approx \mathbb{Z}_2$
16	$i_p(A) = p(A)\, I$	$\mathcal{P}$	$\mathcal{Z}$	$S(C)/\mathcal{P} \approx \mathcal{Z} \approx \mathbb{Z}_2$

Table 1: Sixteen homomorphisms on $S(C)$, with kernel and image.

(e) To which group is $\mathrm{Inn}\,(S(C))$ isomorphic?

Solution: from Theorem 9.4 in the book, we know

$$\mathrm{Inn}\,(S(C)) \approx S(C)/\mathcal{Z},$$

where $\mathcal{Z} = Z(S(C)) = \{I, -I\}$. On the other hand, from items 2 or 3 in Table 1, we know that

$$S(C)/\mathcal{Z} \approx S_4.$$

Thus $\mathrm{Inn}\,(S(C)) \approx S_4$.

(f) Explain why the automorphism $f : S(C) \longrightarrow S(C)$ is not an inner automorphism of $S(C)$.

Solution: assume $f(x) = \phi_A(x) = AXA^{-1}$, for all matrices $X \in S(C)$, for some $A \in S(C)$. Then

$$\det(f(X)) = \det(AXA^{-1}) \Leftrightarrow \det(p(X)\,X) = \det(X) \Leftrightarrow p(X)\,\det(X) = \det(X) \Leftrightarrow p(X) = 1,$$

which last statement is *not* true. OR: recall that if H is a normal subgroup of G and $\phi_g : G \longrightarrow G$ is an inner automorphism of G, then $\phi_g(H) = H$. Now consider f applied to $\mathcal{Q} = \ker(q) \lhd S(C)$:

$$A \in \mathcal{Q} \Leftrightarrow q(A) = 1 \Leftrightarrow \det(A\,\Phi(A)) = 1 \Leftrightarrow \det(A)\,\det(\Phi(A)) = 1.$$

Consequently, (as done in Problem Set 2)

$$\begin{aligned}
\det(f(A)) &= \det\,(p(A)\,A)\\
&= (p(A))^3\,\det(A), \text{ since } A \text{ is a } 3\times 3 \text{ matrix}\\
&= (\det(\Phi(A)))^3\,\det(A)\\
&= (\det(\Phi(A)))^2\,(\det(\Phi(A))\,\det(A))\\
&= (\pm 1)^2 \cdot 1 = 1,
\end{aligned}$$

and so $f(A) \in \ker(\det) = \mathcal{R}$. That is, $f(\mathcal{Q}) \subset \mathcal{R}$. But since both of these subgroups have order 24, we can conclude

$$f(\mathcal{Q}) = \mathcal{R} \neq \mathcal{Q}.$$

Thus f cannot be an inner automorphism of $S(C)$. (f is called an *outer* automorphism.)

3. Prove that for any group G, $\mathrm{Inn}\,(G) \lhd \mathrm{Aut}\,(G)$.

Solution: let $\phi_g \in \mathrm{Inn}\,(G)$ and let $h \in \mathrm{Aut}\,(G))$. Then, for $x \in G$,

$$\begin{aligned}
(h \circ \phi_g \circ h^{-1})(x) &= h(\phi_g(h^{-1}(x)))\\
&= h(g\,h^{-1}(x)\,g^{-1})\\
&= h(g)\,h(h^{-1}(x))\,h(g^{-1})\\
&= h(g)\,x\,(h(g))^{-1}\\
&= \phi_{h(g)}(x)
\end{aligned}$$

Thus $h \circ \phi_g \circ h^{-1} = \phi_{h(g)} \in \mathrm{Inn}\,(G)$ and $\mathrm{Inn}\,(G) \lhd \mathrm{Aut}\,(G)$.