Math 350, Spring 2025 Professor Rob Benedetto

Solutions to the Final Exam

1. **(25 points)** Find all subgroups of $C_3 \times C_3$. That is, in your writeup:
   - List all the subgroups,
   - Prove that each item in your list is indeed a subgroup, and
   - Prove that every subgroup does indeed appear on your list.

[*Hint*: There are 6 different subgroups in total. You may **not** assume that fact in your proofs; I just mention it to you for your convenience.]

Solution/Proof. Let $G = C_3 \times C_3$. Its subgroups are:

$$\boxed{C_3 \times C_3 = G,\ \langle(1,0)\rangle = C_3 \times \{0\},\ \langle(0,1)\rangle = \{0\} \times C_3,\ \langle(1,1)\rangle,\ \langle(1,2)\rangle,\ \{(0,0)\}}$$

All are subgroups:
- $C_3 \times C_3$ is the full group and hence is (the improper) subgroup.
- $\{(0,0)\}$ is just the identity and hence is (the trivial) subgroup.
- Each of the others is a cyclic subgroup generated by an element, and hence each is a subgroup.

All subgroups appear:
Note that $|G| = 3 \cdot 3 = 9$. Given an arbitrary subgroup $H \subseteq G$, we must have $|H| \,\big|\, |G|$ by Lagrange's Theorem, So $|H| \in \{1, 3, 9\}$.

If $|H| = 1$, then since the identity $(0,0)$ must belong to H, we have $H = \{(0,0)\}$.

If $|H| = 9$, then $H = G$.

If $|H| = 3$, then because 3 is prime, a Corollary of Lagrange tells us that H is cyclic. Thus, H must be of the form $\langle(a,b)\rangle$ for some $(a,b) \in G$ with $o((a,b)) = 3$.
By Theorem 6.1(i), we have $o((x,y)) = \text{lcm}(o(x), o(y))$ for any $(x,y) \in G$. Because $o(1) = o(2) = 3$ and $o(0) = 1$ in C_3, all elements of G have order 3 except the identity $(0,0)$. We now consider all eight such choices for the generator (a,b) of H:
- If (a,b) is $(1,0)$ or $(2,0)$, then $H = \langle(1,0)\rangle = \{(0,0),(1,0),(2,0)\} = \langle(2,0)\rangle$.
- If (a,b) is $(0,1)$ or $(0,2)$, then $H = \langle(0,1)\rangle = \{(0,0),(0,1),(0,2)\} = \langle(0,2)\rangle$.
- If (a,b) is $(1,1)$ or $(2,2)$, then $H = \langle(1,1)\rangle = \{(0,0),(1,1),(2,2)\} = \langle(2,2)\rangle$.
- If (a,b) is $(1,2)$ or $(2,1)$, then $H = \langle(1,2)\rangle = \{(0,0),(1,2),(2,1)\} = \langle(2,1)\rangle$. QED

---

2. **(25 points)** Consider the 200-element dihedral group

$$D_{100} = \{e, f, f^2, \ldots, f^{99}, g, fg, f^2g, \ldots, f^{99}g\}$$

of rotations and flips of a regular 100-sided polygon.
Let $h \in D_{100}$ be the flip $h = f^{18}g$, and let $H = Z(h)$ be the centralizer of h in D_{100}.
(That is, $H = \{x \in D_{100} \,|\, hx = xh\}$, which we know to be a subgroup, by HW 6, Problem 6.)

2a. Prove that $H = \{e, f^{50}, f^{18}g, f^{68}g\}$.

2b. Prove that H is **not** a normal subgroup of D_{100}.

Proof. (a): Define $H' = \{e, f^{50}, f^{18}g, f^{68}g\}$. We will prove that $H = H'$.
($\subseteq$): Given $x \in H = Z(h)$, write $x = f^i g^j$, where $0 \le i \le 99$ and $0 \le j \le 1$.
If $j = 0$, so that $x = f^i$, then

$$f^{18}f^{-i}g = f^{18}gf^i = hx = xh = f^i f^{18}g = f^{18}f^i g.$$

Multiplying on the left by f^{-18} and on the right by g, we get $f^{-i} = f^i$, so that $f^{2i} = e$, and hence $100|2i$, so that $50|i$, and hence either $i = 0$ or $i = 50$. That is, either $x = f^0 = e \in H'$ or $x = f^{50} \in H'$, as desired.

Otherwise, we have $j = 1$, so that $x = f^i g$, and hence

$$f^{18-i} = f^1 8 f^{-i} gg = f^{18} g f^i g = hx = xh = f^i g f^{18} g = f^i f^{-18} gg = f^{i-18}.$$

Thus, $f^{36-2i} = e$, and hence $100|(36-2i)$, so that $50|(18-i)$. That is, $i \equiv 18 \pmod{50}$, so that either $i = 18$ or $i = 68$. Hence, either $x = f^{18} g \in H'$, or $x = f^{68} g \in H'$, as desired. QED ($\subseteq$).

($\supseteq$): We simply check that each of the elements of H' commutes with h:
Two elements of H are e and h. We have $eh = he$ and $hh = hh$ trivially, so $e, h \in Z(h) = H$.
In addition, $f^{50} h = f^{68} g = f^{18} f^{50} g = f^{18} g f^{-50} = h f^{50}$, so that $f^{50} \in Z(h) = H$.
The last element of H' is $f^{68} g = f^{50} h$. We have $(f^{50} h)h = (h f^{50})h = h(f^{50} h)$,
so that $f^{50} h \in Z(h) = H$. QED

[**Alternative last line**: $Z(h)$ is closed under multiplication (it's a subgroup), so $f^{50} h \in Z(h) = H$.]

(b): Consider $f \in D_{100}$ and $h = f^{18} g \in H$. Then

$$f h f^{-1} = f(f^{18} g) f^{-1} = f^{19}(g f^{-1}) = f^{19}(fg) = f^{20} g \notin H,$$

and hence $H \not\trianglelefteq D_{100}$. QED

---

3. **(21 points)** Let $\varphi : A_4 \to C_8$ be a homomorphism, where A_4 is the (12-element) alternating group on 4 symbols, and C_8 is the cyclic group of order 8.
Prove that φ is the trivial homomorphism. That is, prove that $\varphi(g) = 0$ for all $g \in A_4$.

[**Hint**: if $\sigma \in A_4$ is a 3-cycle, what can you prove about $\varphi(\sigma)$?]

Proof. First, we claim that $\boxed{\text{for any 3-cycle } \sigma \in A_4, \text{ we have } \varphi(\sigma) = 0}$

To prove this claim, given such σ, let $m = o(\varphi(\sigma))$.
Since $o(\sigma) = 3$, Theorem 12.4(iii) tells us that $m|3$, so that m is 1 or 3.
On the other hand, by a Corollary of Lagrange, $m \,\big|\, |C_8|$, i.e., $m|8$, and hence $m \neq 3$.
Thus, $m = 1$. That is, $o(\varphi(\sigma)) = 1$, so that $\varphi(\sigma) = 0$. QED Claim

The kernel $\ker \varphi$ is a subgroup of A_4; by the Claim, every 3-cycle is in $\ker \varphi$. By Exercise 8.5 (Homework 9, Problem 2), there are 8 3-cycles in A_4, and $|A_4| = 12$. Therefore, setting $n = |\ker \varphi|$, we have $n \geq 8$ and, by Lagrange's Theorem, $n|12$. It follows that $n = 12$, and hence $\ker \varphi = A_4$. That is, $\varphi(g) = 0$ for all $g \in A_4$. QED

(**Alternative proof**, assuming the claim): Given any $g \in A_4$, first suppose that g is a 3-cycle; then we are done by the Claim. And if $g = e$, then $\varphi(g) = 0$ because φ is a homomorphism.

Otherwise, we know from Exercise 8.5 (Homework 9, Problem 2) that g is one of $(1,2)(3,4)$ or $(1,3)(2,4)$ or $(1,4)(2,3)$.
We have $(1,2)(3,4) = (1,2,3)(2,3,4)$, and hence $\varphi((1,2)(3,4)) = \varphi((1,2,3)) + \varphi((2,3,4)) = 0 + 0 = 0$ by the Claim.
Similarly, $\varphi((1,3)(2,4)) = \varphi((1,3,2)) + \varphi((3,2,4)) = 0 + 0 = 0$, and
$\varphi((1,4)(2,3)) = \varphi((1,4,2)) + \varphi((2,3,4)) = 0 + 0 = 0$. QED

---

4. **(15 points)** Let G_1, G_2, G_3 be groups, and let $\varphi : G_1 \to G_2$ and $\psi : G_2 \to G_3$ be homomorphisms. Suppose that ψ is onto, and that $\psi \circ \varphi$ is the trivial homomorphism.

4a. Prove that $\ker \psi \supseteq \varphi(G_1)$.

4b. If $\ker \psi = \varphi(G_1)$, prove that $G_3 \cong G_2/\varphi(G_1)$.

Proof. (a): Given $y \in \phi(G_1)$, there exists $x \in G_1$ such that $\varphi(x) = y$.
Thus, $\psi(y) = \psi(\varphi(x)) = e_3$, so $y \in \ker \psi$. QED (a)

(b): Assuming $\ker \psi = \phi(G_1)$, we have $G_2/\phi(G_1) = G_2/\ker \psi$, which is isomorphic to G_3 by the Fundamental Theorem of Group Homomorphisms, since ψ is onto. QED (b)

---

5. **(23 points)** Let R be a ring with unity. Define a relation $\sim$ on R by, for $a, b \in R$:

$$a \sim b \iff \exists u \in R^\times \text{ s.t. } b = au.$$

5a. Prove that $\sim$ is an equivalence relation on R.

5b. Suppose further that R is an integral domain.
For any $a, b \in R$, prove that $aR = bR$ if and only if $a \sim b$.
[Recall that aR denotes the principal ideal generated by a.]

Proof. (a): **Reflexive**: Given $a \in R$, we have $1_R \in R^\times$ and $a = 1_R a$, so $a \sim a$.

Symmetric: Given $a, b \in R$ such that $a \sim b$, there is a unit $u \in R^\times$ such that $b = au$. Then $u^{-1} \in R^\times$ is also a unit, and $bu^{-1} = a$, so that $b \sim a$.

Transitive: Given $a, b, c \in R$ such that $a \sim b$ and $b \sim c$, there are units $u, v \in R^\times$ such that $b = au$ and $c = bv$. Then $uv \in R^\times$ is also a unit, and $c = bv = (au)v = a(uv)$, so $a \sim c$. QED (a)

(b): Given $a, b \in R$ arbitrary.

($\Rightarrow$): We have $a = a1_R \in aR = bR$, so there is some $x \in R$ such that $a = bx$.
We also have $b = b1_R \in bR = aR$, so there is some $y \in R$ such that $b = ay$.
If $a = 0_R$, then $b = ay = 0_R \cdot y = 0_R = 0_R = a$, so $a \sim b$ (by reflexivity).
So we may assume for the rest of the proof that $a \neq 0_R$.

We have $a(yx) = (ay)x = bx = a = a1_R$, and hence $a(yx - 1_R) = 0_R$. Since $a \neq 0_R$ and R is an integral domain, it follows that $yx - 1_R = 0_R$, and hence $xy = yx = 1_R$. Thus, $y \in R^\times$ is a unit (with $y^{-1} = x$), so that the equation $b = ay$ yields that $a \sim b$. QED ($\Rightarrow$)

($\Leftarrow$): Since $a \sim b$, there is some $u \in R^\times$ such that $b = au$. We now prove $aR = bR$:

($\subseteq$): Given $ax \in aR$, we have $a = bu^{-1}$, and hence $ax = (bu^{-1})x = b(u^{-1}x) \in bR$. QED ($\subseteq$)

($\supseteq$): Given $by \in bR$, we have $by = (au)y = a(uy) \in aR$. QED ($\supseteq$)

QED (b)

---

6. **(21 points)** Let $\varphi : R \to S$ be an **onto** homomorphism of rings, and let $I \subseteq R$ be a **prime** ideal.
By Theorem 18.4(iv), we know that $\varphi(I)$ is an ideal of S.
Suppose that $\ker \varphi \subseteq I$. Prove that $\varphi(I)$ is a prime ideal of S.

Proof. As noted in the statement of the problem, we already know $\varphi(I)$ is an ideal of S.

Given $y_1, y_2 \in S$ such that $y_1 y_2 \in \varphi(I)$, there exists $t \in I$ such that $\varphi(t) = y_1 y_2$.
In addition, since φ is onto, there exist $x_1, x_2 \in R$ such that $\varphi(x_1) = y_1$ and $\varphi(x_2) = y_2$. Thus,

$$\varphi(x_1 x_2) = \varphi(x_1)\varphi(x_2) = y_1 y_2 = \varphi(t),$$

and hence $\varphi(x_1 x_2 - t) = \varphi(x_1 x_2) - \varphi(t) = 0_S$.
Therefore, $x_1 x_2 - t \in \ker \varphi \subseteq I$, and because we also have $t \in I$, it follows that $x_1 x_2 = (x_1 x_2 - t) + t \in I$.
Since I is a prime ideal, we have either $x_1 \in I$ or $x_2 \in I$.
If $x_1 \in I$, then $y_1 = \varphi(x_1) \in \varphi(I)$, as desired.
Otherwise, we have $x_2 \in I$, so $y_2 = \varphi(x_2) \in \varphi(I)$. QED

---

7. **(35 points)** Let R be a commutative ring, and let $I \subseteq R$ be an ideal. Define

$$J = \{r \in R \,|\, \text{there is an integer } n \geq 1 \text{ such that } r^n \in I\}.$$

7a. Let $x, y \in R$, and let $k \geq 1$ be a positive integer. Prove that there are integers $c_0, \ldots, c_k \in \mathbb{Z}$ such that $(x-y)^k = c_0x^k + c_1x^{k-1}y + c_2x^{k-2}y^2 + \cdots + c_{k-1}xy^{k-1} + c_ky^k$.
[*Suggestion*: Use induction on k.]

7b. Prove that J is an ideal of R.
[*Suggestion*: Part (a) may come in handy at some point.]

7c. Prove that the quotient ring R/J contains no nonzero nilpotent elements.

Proof. (a): By induction on k. For $k = 1$, $(x-y)^1 = x - y = 1x + (-1)y$ is already of the desired form.
Assuming the statement for a particular $k \geq 1$, and given $x, y \in R$, there are integers $c_0, \ldots, c_k \in \mathbb{Z}$ such that

$$(x-y)^k = c_0x^k + c_1x^{k-1}y + c_2x^{k-2}y^2 + \cdots + c_{k-1}xy^{k-1} + c_ky^k$$

Thus,

$$\begin{aligned}(x-y)^{k+1} &= (x-y)(x+y)^k = (x-y)\big(c_0x^k + c_1x^{k-1}y + \cdots + c_{k-1}xy^{k-1} + c_ky^k\big) \\ &= \big(c_0x^{k+1} + c_1x^ky + \cdots + c_kxy^k\big) - \big(c_0x^ky + c_1x^{k-1}y^2 + \cdots + c_ky^{k+1}\big) \\ &= c_0x^{k+1} + (c_1 - c_0)x^ky + \cdots + (c_{k-1} - c_k)xy^k + (-c_k)y^{k+1},\end{aligned}$$

which is of the desired form. QED (a)

(b): **Nonempty**: We have $0^1 = 0 \in I$, and hence $0 \in J$.

Subtraction: Given $x, y \in J$, there are integers $m, n \geq 1$ such that $x^m, y^n \in I$. Then by the Lemma applied to $k = m + n \geq 2$, there are integers c_i such that

$$(x-y)^k = c_0x^k + c_1x^{k-1}y + \cdots + c_{k-1}xy^{k-1} + c_ky^k$$

Each term in the sum on the right side is of the form $c_ix^{k-i}y^i$, where $c_i \in \mathbb{Z}$. If $i \geq n$, then the term is of the form ry^n with $r = c_ix^{k-i}y^{i-n} \in R$, and hence $ry^n \in I$. Otherwise, we have $0 \leq i \leq n-1$, so that the term is of the form sx^m with $s = c_ix^{n-i}y^i \in R$, and hence $sx^m \in I$.
Thus, we have $(x-y)^k \in I$, since it is a sum of elements of I. Therefore, $x - y \in J$.

Sticky: Given $x \in J$ and $r \in R$, there is an integer $n \geq 1$ such that $x^n \in I$. Then because R is commutative, we have $(rx)^n = r^nx^n \in I$. Thus, $xr = rx \in J$. QED (b)

(c): Given a nilpotent element $(J + a) \in R/J$, there is [by definition of nilpotent] some integer $n \geq 1$ such that $(J + a)^n = J + 0$. Therefore, $J + a^n = J + 0$, or equivalently, $a^n - 0 \in J$. Thus, there is some integer $m \geq 1$ such that $(a^n - 0)^m \in I$; that is, $a^{mn} \in I$. Since $mn \geq 1$ is an integer, then, we also have $a \in J$. Hence, $J + a = J + 0$.
We have just shown that the only nilpotent element in R/J is the zero element. QED (c)

---

8. **(35 points)** Let $\mathbb{F}_2 = \{0, 1\}$ denote the field of two elements (that the book calls $\mathbb{Z}_2$). Let $f = X^4 + X + 1 \in \mathbb{F}_2[X]$.

8a. Prove that f is irreducible in $\mathbb{F}_2[X]$.

8b. Use f and the ideas of Section 20 to construct a field with exactly 16 elements.

Don't forget to justify all of your claims. (As usual, you may quote theorems to do so, but for example, in part (b) you must prove that the object you construct is indeed a field, and that it has exactly 16 elements.)

Proof. (a). Suppose that $f = gh$ where $g, h \in \mathbb{F}_2[X]$ are non-units, so that $\deg g, \deg h \geq 1$.
We have $f(0) = 0 + 0 + 1 = 1 \neq 0$ and $f(1) = 1 + 1 + 1 = 1 \neq 0$, so that f has no factors in $\mathbb{F}_2[X]$ of degree 1.
Thus, since $\deg g + \deg h = \deg f = 4$, we have $\deg g = \deg h = 2$. Write $g = a_2X^2 + a_1X + a_0$ and $h = b_2X^2 + b_1X + b_0$, with $a_i, b_i \in \mathbb{F}_2$, and with $a_2, b_2 \neq 0$. In particular, $a_2 = b_2 = 1$, and we have

$$\begin{aligned} X^4 + X + 1 &= (X^2 + a_1X + a_0)(X^2 + b_1X + b_0) \\ &= X^4 + (a_1 + b_1)X^3 + (a_0 + a_1b_1 + b_0)X^2 + (a_0b_1 + a_1b_0)X + a_0b_0. \end{aligned}$$

Equating the constant terms on each side of this equation, we have $a_0b_0 = 1$, so that $a_0 = b_0 = 1$.
Therefore, equating the X terms, we have $a_1 + b_1 = 1$.
However, equating the X^3 terms, we have $a_1 + b_1 = 0$, a contradiction.
Thus, so such g and h exist, proving that f is irreducible. QED (a)

(b): Let I be the principal ideal $I = \langle f \rangle$ of $\mathbb{F}_2[X]$. Then I is a maximal ideal by Theorem 20.2, since f is irreducible.
Let $K = \mathbb{F}_2[X]/I$, which is a field by Theorem 17.7. It suffices to show that $|K| = 16$.

Claim 1: $K = \{I + a_0 + a_1X + a_2X^2 + a_3X^3 : a_i \in \mathbb{F}_2\}$

Proof of Claim 1. ($\supseteq$): This inclusion is clear, because K is the set of *all* right cosets $I + g$.
($\subseteq$): Given $I + g \in K$, by the division algorithm there are $q, r \in \mathbb{F}_2[X]$ with $g = qf + r$ and $\deg(r) < \deg(f) = 4$. That last condition means precisely that $r = a_0 + a_1X + a_2X^2 + a_3X^3$ for some $a_0, a_1, a_2, a_3 \in \mathbb{F}_2$. Meanwhile, the first condition says that $g - r = qf \in I$, and hence $I + g = I + r = I + a_0 + a_1X + a_2X^2 + a_3X^3 \in$ RHS. QED Claim 1

Claim 2: If $I + a_0 + a_1X + a_2X^2 + a_3X^3 = I + b_0 + b_1X + b_2X^2 + b_3X^3$, then $a_i = b_i$ for each i.

Proof of Claim 2. By the coset relation, we have $(a_0 - b_0) + (a_1 - b_1)X + (a_2 - b_2)X^2 + (a_3 - b_3)X^3 \in I$.
That is, there is some $h \in \mathbb{F}_2[X]$ such that $(a_0 - b_0) + (a_1 - b_1)X + (a_2 - b_2)X^2 + (a_3 - b_3)X^3 = hf$.
If $h \neq 0$, then $\deg(h) \geq 0$; so taking degrees of both sides, we get

$$3 \geq \deg\big((a_0 - b_0) + (a_1 - b_1)X + (a_2 - b_2)X^2 + (a_3 - b_3)X^3\big) = \deg(h) + \deg(f) \geq \deg(f) = 4,$$

a contradiction. Thus, $h = 0$, and therefore $a_0 - b_0 = a_1 - b_1 = a_2 - b_2 = a_3 - b_3 = 0$ QED Claim 2

We have just shown that each element of K has a unique coset representative of the form $a_0 + a_1X + a_2X^2 + a_3X^3$ with $a_i \in \mathbb{F}_2$. Since there are 2 choices for each coefficient, there are $2^4 = 16$ total possible choices of such coset representatives, and hence exactly 16 elements in K.

BONUS A. **(2 points)** Recall that A_6 denotes the alternating group on 6 objects, and S_4 is the symmetric group on 4 objects. Find an **injective** homomorphism $\varphi : S_4 \to A_6$. (And of course, prove all your claims.)

Answer/Proof. Each $\sigma \in S_4$ is a bijective function from $\{1, 2, 3, 4\}$ to itself. For each such σ, define $\varphi(\sigma)$ as a function from $\{1, 2, 3, 4, 5, 6\}$ to itself by

$$\big(\varphi(\sigma)\big)(i) = \begin{cases} \sigma(i) & \text{if } i \in \{1, 2, 3, 4\}, \\ 5 & \text{if } i = 5 \text{ and } \sigma \text{ is even}, \\ 6 & \text{if } i = 6 \text{ and } \sigma \text{ is even}, \\ 6 & \text{if } i = 5 \text{ and } \sigma \text{ is odd}, \\ 5 & \text{if } i = 6 \text{ and } \sigma \text{ is odd}. \end{cases}$$

That is, if we write σ and $\varphi(\sigma)$ in disjoint cycle notation, we have

$$\varphi(\sigma) = \begin{cases} \sigma & \text{if } \sigma \text{ is even,} \\ \sigma\,(5,6) & \text{if } \sigma \text{ is odd.} \end{cases}$$

Since $(5,6)$ is an odd permutation, the outputs above are all even permutations, and hence φ is indeed a function $\varphi : S_4 \to A_6$.

Claim 1: φ is a homomorphism

Proof of Claim 1. Given $\sigma, \tau \in S_4$, we must show that $\varphi(\sigma \circ \tau) = \varphi(\sigma) \circ \varphi(\tau)$, as functions from $\{1,2,3,4,5,6\}$ to itself.
Given $i \in \{1,2,3,4\}$, we have $\tau(i) \in \{1,2,3,4\}$ as well, and hence

$$\big(\varphi(\sigma \circ \tau)\big)(i) = (\sigma \circ \tau)(i) = \sigma\big(\tau(i)\big) = \big(\varphi(\sigma)\big)(\tau(i)) = \big(\varphi(\sigma)\big)\Big(\big(\varphi(\tau)\big)(i)\Big) = \big(\varphi(\sigma) \circ \varphi(\tau)\big)(i).$$

Given $i \in \{5,6\}$, we now wish to prove the same identity. If $i = 5$, let $j = 6$; and if $i = 6$, then let $j = 5$.

Case 1. If σ, τ are both even, then $\sigma\tau$ is even, and

$$\big(\varphi(\sigma \circ \tau)\big)(i) = i = \varphi(\sigma)(i) = \big(\varphi(\sigma)\big)\Big(\big(\varphi(\tau)\big)(i)\Big) = \big(\varphi(\sigma) \circ \varphi(\tau)\big)(i).$$

Case 2. If σ, τ are both odd, then $\sigma\tau$ is even, and

$$\big(\varphi(\sigma \circ \tau)\big)(i) = i = \varphi(\sigma)(j) = \big(\varphi(\sigma)\big)\Big(\big(\varphi(\tau)\big)(i)\Big) = \big(\varphi(\sigma) \circ \varphi(\tau)\big)(i).$$

Case 3. If σ is even and τ is odd, then $\sigma\tau$ is odd, and

$$\big(\varphi(\sigma \circ \tau)\big)(i) = j = \varphi(\sigma)(j) = \big(\varphi(\sigma)\big)\Big(\big(\varphi(\tau)\big)(i)\Big) = \big(\varphi(\sigma) \circ \varphi(\tau)\big)(i).$$

Case 4. If σ is odd and τ is even, then $\sigma\tau$ is odd, and

$$\big(\varphi(\sigma \circ \tau)\big)(i) = j = \varphi(\sigma)(i) = \big(\varphi(\sigma)\big)\Big(\big(\varphi(\tau)\big)(i)\Big) = \big(\varphi(\sigma) \circ \varphi(\tau)\big)(i).$$

Thus, for all $i \in \{1,2,3,4,5,6\}$, we have verified that $\big(\varphi(\sigma \circ \tau)\big)(i) = \big(\varphi(\sigma) \circ \varphi(\tau)\big)(i)$. QED Claim 1

Claim 2: φ is injective

Proof of Claim 2. By Exercise 13.19 (HW 16, Problem 2), it suffices to show $\ker \varphi = \{e\}$. The $(\supseteq)$ direction is clear, so we prove $(\subseteq)$.
Given $\sigma \in \ker \varphi$, we have $\varphi(\sigma) = e$. By definition of φ, then, for each $i \in \{1,2,3,4\}$, we must have $\sigma(i) = \big(\varphi(\sigma)\big)(i) = e(i) = i$. Since this is true for each $i \in \{1,2,3,4\}$, we have $\sigma = e$. QED Claim 2

Thus, we have constructed the desired injective homomorphism $\varphi : S_4 \to A_6$.

BONUS B. **(2 points)** Let $R = \mathbb{Z}[\sqrt{11}] = \{a + b\sqrt{11} \mid a, b \in \mathbb{Z}\}$, which is a subring of $\mathbb{R}$. Find a unit $u \in R^\times$ of infinite order in the group of units $R^\times$. (And of course, prove all your claims.)

Proof. Let $u = 10 + 3\sqrt{11} \in R$ and $v = 10 - 3\sqrt{11} \in R$.
Then $vu = uv = 100 - 11 \cdot 9 = 1$, so that u is a unit in R.
On the other hand, viewed as an element of the real line $\mathbb{R}$, we have $u > 1$, and hence

$$1 < u < u^2 < u^3 < \cdots,$$

so that $u^n \neq 1$ for all $n \geq 1$. Thus, the order of u (in the group $R^\times$) is $o(u) = \infty$. QED