Math 412 — Final Exam
Practice Problems

Your Name:  

Your Instructor:  

---

1. **Do not open this exam until you are told to do so.**
2. This exam has 15 pages including this cover. There are 11 problems. Note that the problems are not of equal difficulty, so you may want to skip over and return to a problem on which you are stuck.
3. If the pages of your exam become separated, write your name on every page.
4. For any computations, make sure that you carefully show your work.
5. **Turn OFF all cell phones**, and remove all headphones.
6. If you need additional space for a problem, you may use the back of the page. However, please CLEARLY indicate that your work continues on the back of the page.

---

<table>
<thead>
<tr>
<th>Problem</th>
<th>Points</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
1. [0 points] Decide whether each of the following statements is true Always, Sometimes, or Never. No justification is needed.

(a) If $R$ and $S$ are nonzero fields then $R \times S$ is a field.

<table>
<thead>
<tr>
<th>Always</th>
<th>Sometimes</th>
<th>Never</th>
</tr>
</thead>
</table>

(b) $\mathbb{Z}[x]$ is an integral domain.

<table>
<thead>
<tr>
<th>Always</th>
<th>Sometimes</th>
<th>Never</th>
</tr>
</thead>
</table>

(c) If $G$ is cyclic then $G$ is abelian.

<table>
<thead>
<tr>
<th>Always</th>
<th>Sometimes</th>
<th>Never</th>
</tr>
</thead>
</table>

(d) If $G$ is a group and $a$ is a nonidentity element of $G$ then the function $f : G \to G$ defined by $f(g) = ag$ is a group homomorphism.

<table>
<thead>
<tr>
<th>Always</th>
<th>Sometimes</th>
<th>Never</th>
</tr>
</thead>
</table>

(e) If $N$ is a normal subgroup of a group $G$ then $gn = ng$ for every $n \in N$ and $g \in G$.

<table>
<thead>
<tr>
<th>Always</th>
<th>Sometimes</th>
<th>Never</th>
</tr>
</thead>
</table>

(f) If $G$ is not abelian and $N$ is a normal subgroup then $G/N$ is also not abelian.

<table>
<thead>
<tr>
<th>Always</th>
<th>Sometimes</th>
<th>Never</th>
</tr>
</thead>
</table>

(g) If $H$ and $K$ are subgroups of $G$ then $H \cup K$ is a subgroup of $G$.

<table>
<thead>
<tr>
<th>Always</th>
<th>Sometimes</th>
<th>Never</th>
</tr>
</thead>
</table>

(h) For any element $g$ of a group $G$ the centralizer of $g$ (i.e. the set of elements commuting with $g$) is abelian.

<table>
<thead>
<tr>
<th>Always</th>
<th>Sometimes</th>
<th>Never</th>
</tr>
</thead>
</table>

(i) The function $\phi(g) = r_g$ defines an action of a group $G$ on itself, where $r_g$ denotes multiplication on the right by $g$.

<table>
<thead>
<tr>
<th>Always</th>
<th>Sometimes</th>
<th>Never</th>
</tr>
</thead>
</table>

(j) Let $f(x)$ and $g(x)$ be polynomials in $F[x]$. If there are polynomials $p(x)$ and $q(x)$ with $p(x)f(x) + q(x)g(x) = x^2$ then the GCD of $f(x)$ and $g(x)$ is $x^2$.

<table>
<thead>
<tr>
<th>Always</th>
<th>Sometimes</th>
<th>Never</th>
</tr>
</thead>
</table>
2. [0 points]
For each of the following, give an example or prove that none exists.

(a) A group \(G\) whose center is a nontrivial proper subgroup.
(b) An integer divisible by distinct positive primes \(p\) and \(q\) but not divisible by \(pq\).
(c) A non-trivial group in which every element is its own inverse.
(d) A group \(G\) and a non-empty subset \(H \subset G\) such that \(H\) is closed under the group operation but \(H\) is not a subgroup of \(G\).
(e) A field with nine elements.
(f) A surjective homomorphism of rings \(f : R \to S\) such that \(R\) has an identity element but \(S\) does not.
(g) A positive integer \(n\) such that \(U(\mathbb{Z}_n)\) is not cyclic.
(h) A group of order 64 with a subgroup of order 4.
(i) An element of order 12 in \(S_8\).

Solution:

(a) \(D_4\) has two elements in its center: the identity and rotation by 180 degrees.
(b) This is impossible. Suppose \(p\) and \(q\) both divide \(n\). Thus we can write \(n = qr\) for some integer \(r\). By Euclid’s lemma \(p|r\), so that \(r = ps\) for some integer \(s\). But then \(n = qps\) is divisible by \(pq\).
(c) \(\mathbb{Z}_2\).
(d) The positive integers in \(\mathbb{Z}\) (with group operation +).
(e) By checking for linear factors, one can see that \(x^2 + x + [2]\) is irreducible over \(\mathbb{Z}_3\). Then \(\mathbb{Z}_3[x]/(x^2 + x + [2])\) is a field (because the polynomial is irreducible) and has nine elements: each coset has a unique representative \([a]x + [b] + I\).
(f) This is impossible: \(f(1_R)\) will be the identity in \(S\). Choose any \(s\) in \(S\). Since \(f\) is surjective, \(s = f(r)\) for some element \(r \in R\). Then

\[
f(1_R) \cdot s = f(1_R) \cdot f(r) = f(1_R \cdot r) = f(r) = s
\]

and similarly for the other side, proving the claim.
(g) \(n = 15\) will work, since \(U(\mathbb{Z}_{15}) = U(\mathbb{Z}_3 \times \mathbb{Z}_5) = U(\mathbb{Z}_3) \times U(\mathbb{Z}_5)\). The first group is isomorphic to \(\mathbb{Z}_2\) and the second is isomorphic to \(\mathbb{Z}_4\). But \(\mathbb{Z}_2 \times \mathbb{Z}_4\) is not cyclic.
(h) \(G = \mathbb{Z}_4 \times \mathbb{Z}_{16}\) will work, where the subgroup is given by \(\mathbb{Z}_4 \times \{[0]_{16}\}\).
(i) Consider the product of the elements

\[
a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 4 & 5 & 6 & 7 & 8 \end{pmatrix} \quad \text{and} \quad b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 5 & 6 & 7 & 4 & 8 \end{pmatrix}
\]

Since \(a\) and \(b\) permute totally different elements, they commute. Furthermore, the only way that \((ab)^k = e\) is if \(a^k\) and \(b^k\) both are equal to the identity. Again, this is because there is no interaction between the two. Since \(a\) has order 3 and \(b\) has order 4, the order of the product \(ab\) is 12.
3. [0 points] Prove each of the following statements.

a. [0 point] The kernel of a group homomorphism \( f : G \to H \) is a normal subgroup of \( G \).

\[ \text{Solution: We first check that } \ker(f) \text{ is a subgroup. It is non-empty because } f(e_G) = e_H. \]

\[ \text{It is closed under products since if } g \text{ and } h \text{ are both in the kernel then } gh \text{ satisfies} \]

\[ f(gh) = f(g)f(h) = e_H \cdot e_H = e_H \]

so \( gh \) is also in the kernel. It is closed under taking inverses since if \( g \) is in the kernel then \( f(g^{-1}) = f(g)^{-1} = e_H. \)

To show that \( \ker(f) \) is normal, we will show that it “absorbs conjugation.” So, suppose that \( n \in \ker(f) \) and \( g \in G \) are arbitrary elements. We must show that \( gng^{-1} \in \ker(f). \)

This is true because

\[ f(gng^{-1}) = f(g)f(n)f(g^{-1}) = f(g)e_Hf(g)^{-1} = f(g)f(g)^{-1} = e_H. \]

b. [0 point] Let \( G \) be a group. Define the set \( C = \{xyx^{-1}y^{-1} \mid x, y \in G\} \). Suppose that \( N \) is a normal subgroup of \( G \) that contains \( C \). Then \( G/N \) is abelian.

\[ \text{Solution: Consider arbitrary cosets } xN, yN \in G/N. \text{ We must show that } xN \cdot yN = yN \cdot xN, \text{ or equivalently, that} \]

\[ xN \cdot yN \cdot (xN)^{-1} \cdot (yN)^{-1} = N. \]

By the rules for multiplying cosets, the left side is equal to \( xyx^{-1}y^{-1}N \). But the element \( xyx^{-1}y^{-1} \) is contained in \( C \) and thus in \( N \). So \( xyx^{-1}y^{-1}N = N \) as desired.

c. [0 point] Let \( G \) be an abelian group and let \( F \) be the set of elements of \( G \) that have finite order. Then \( F \) is a subgroup of \( G \).

\[ \text{Solution: We use the subgroup criterion. } F \text{ is nonempty since the identity } e_G \text{ always has finite order 1. To show that } F \text{ is closed under multiplication, suppose that } a \text{ and } b \text{ are two elements of finite order. Since } G \text{ is abelian, } (ab)^k = a^kb^k \text{ for any integer } k. \text{ Thus, the order of } ab \text{ is certainly no greater than } |a||b|, \text{ as} \]

\[ (ab)^{|a||b|} = a^{|a||b|}b^{|a||b|} = (e_G)^{|b|}(e_G)^{|a|} = e_G. \]

\( F \) is also closed under inverses, since the order of \( a^{-1} \) is the same as the order of \( a. \) So \( F \) is a subgroup.
d. [0 point] If $R$ is an integral domain with only finitely many elements then $R$ is a field.

**Solution:** We must show that any nonzero element $a \in R$ has a multiplicative inverse. To this end, consider the sequence of elements $a, a^2, a^3, \ldots$. Since $R$ only has finitely many elements, at some point there must be a repetition on this list. In other words, there are positive integers $k < m$ so that $a^k = a^m$. Rearranging, we find $a^k(1 - a^{m-k}) = 0$. Since $R$ is an integral domain, one of these terms must be 0. Furthermore, since $R$ is an integral domain and $a \neq 0$ we have $a^k \neq 0$. Thus $1 - a^{m-k} = 0$, i.e. $1 = a^{m-k}$, and $a^{-1} = a^{m-k-1}$.

---

e. [0 point] Let $R$ be a ring with an identity. The characteristic of $R$ is defined to be the smallest positive integer $k$ such that $k1_R = 0_R$. Show that $f : \mathbb{Z} \to R$ defined by $f(a) = a1_R$ is a ring homomorphism. How is the kernel of $f$ related to the characteristic of $R$?

**Solution:** We first show that $f$ is a homomorphism. Suppose that $a$ and $b$ are any two integers. Then $f(a+b) = (a+b)1_R$ and $f(a) + f(b) = a1_R + b1_R$. These two terms agree since they are both just $a + b$ copies of $1_R$ added together. Similarly, $f(ab) = ab1_R$ and $f(a)f(b) = (a1_R)(b1_R)$ are the same. So $f$ is a homomorphism.

If the characteristic of $R$ is $k$, the kernel of $f$ is the ideal $k\mathbb{Z}$. Clearly this ideal is contained in the kernel. Conversely, we must show that this ideal contains the kernel. Suppose that $m \in ker(f)$. Since a gcd can be written as a linear combination, $(m, k) \in ker(f)$. But $(m, k) \leq k$ with equality if and only if $m \in k\mathbb{Z}$. Since $k$ is the smallest integer in the kernel, we see that we must have $m \in k\mathbb{Z}$. We have shown that every element in the kernel is also contained in $k\mathbb{Z}$, finishing the proof.
4. [0 points]

a. [0 point] Factor the polynomial \(x^3 - 2x^2 + 3x - 2\) in \(\mathbb{R}\).

Solution: Checking for roots by hand, we quickly see that \(f(1) = 0\). Thus, this polynomial is divisible by \((x - 1)\). Dividing by hand, we get \(x^2 - x + 2\). This latter polynomial is irreducible over \(\mathbb{R}\), since the two roots given by the quadratic equation both involve complex numbers. So

\[x^3 - 2x^2 + 3x - 2 = (x - 1)(x^2 - x + 2)\].

b. [0 point] Factor the polynomial \(3x^3 + 2x^2 + 4x + 1\) in \(\mathbb{Z}_5\).

Solution: Checking for roots by hand, we see that \(f([1]) = [0]\). Thus, this polynomial is divisible by \((x - [1])\). Dividing by hand, we obtain \([3]x^2 + [4]\). This polynomial is irreducible because it has no roots over \(\mathbb{Z}_5\). That is, we plug the numbers \([0]\) through \([4]\) into this equation and check that none give \([0]\). So


c. [0 point] Find all the solutions to the equation \(7x = 12\) in \(\mathbb{Z}_{17}\).

Solution: Since \(\mathbb{Z}_{17}\) is a field, this equation will have a unique solution. To find it, we must calculate the inverse of \([7]\). We need to use the Euclidean algorithm to write 1 as a linear combination

\[1 = 7x + 17y\]

and the inverse of 7 will then be \([x]\). So, we run the algorithm:

\[
\begin{align*}
17 &= 2 \cdot 7 + 3 \\
7 &= 2 \cdot 3 + 1 \\
3 &= 3 \cdot 1
\end{align*}
\]

Back-substituting, we find:

\[
\begin{align*}
3 &= 17 - 2 \cdot 7 \\
1 &= 7 - 2 \cdot 3 = 7 - 2(17 - 2 \cdot 7) = -2 \cdot 17 + 5 \cdot 7
\end{align*}
\]

So, \([7]^{-1} = [5]\) and the solution is \(x = [7]^{-1}[12] = [9]\).
5. [0 points] Let $G$ be a group and let $H$ be a normal subgroup of $G$. For any $g \in G$ and $xH \in G/H$ define
\[ g \circ xH = (gxg^{-1})H \]

a. [0 point] Show that $\circ$ is well-defined.

Solution: Suppose $x, y \in G$ with $xH = yH$ and let $g \in G$. To show that $\circ$ is well-defined, we must show that $(gxg^{-1})H = (gyg^{-1})H$, i.e. that $(gyg^{-1})^{-1}(gxg^{-1}) \in H$. Since $xH = yH$, we have $y^{-1}x \in H$. Now $(gyg^{-1})^{-1}(gxg^{-1}) = (g^{-1}y^{-1})(gx^{-1}) = g(y^{-1}x)g^{-1}$. Since $H$ is normal and $y^{-1}x \in H$ we have $g(y^{-1}x)g^{-1} \in H$. Hence $(gyg^{-1})^{-1}(gxg^{-1}) \in H$ and therefore $(gxg^{-1})H = (gyg^{-1})H$ so $\circ$ is indeed well-defined.

b. [0 point] Prove that $\circ$ gives an action of $G$ on $G/H$.

Solution: For $g \in G$, we define $\theta_g$ by $\theta_g(xH) = g \circ xH$. To prove that $\circ$ gives an action of $G$ on $G/H$, we must show that (i) $\theta_g \in \text{Sym}(G/H)$ and (ii) the map from $G$ to $\text{Sym}(G/H)$ given by $g \mapsto \theta_g$ is a homomorphism.

First, to prove (i), since we showed in (a) that $\theta_g$ is well-defined, it suffices to show that $\theta_g$ is bijective. Let $xH \in G/H$. Then $\theta_g((g^{-1}xg)H) = (g(g^{-1}xg)g^{-1})H = xH$, so since $g^{-1}xg \in G$, the map $\theta_g : G/H \rightarrow G/H$ is surjective. Now suppose that $\theta_g(xH) = \theta_g(yH)$. Then $(gxg^{-1})H = (gyg^{-1})H$ so $(gyg^{-1})^{-1}(gxg^{-1}) \in H$. Let $h = (gyg^{-1})^{-1}(gxg^{-1})$. Then $h = (gyg^{-1})^{-1}(gxg^{-1}) = (g^{-1}y^{-1})(gx^{-1}) = gy^{-1}xg^{-1} = y^{-1}x = g^{-1}hg = (g^{-1})h(g^{-1})^{-1}$. Since $h \in H$, $g^{-1} \in G$, and $H$ is normal in $G$, it follows that $(g^{-1})h(g^{-1})^{-1} \in H$ so $y^{-1}x \in H$. Thus $xH = yH$ so $\theta_g$ is injective.

To prove (ii), note that for all $xH \in G/H$ and all $g_1, g_2 \in G$, we have $\theta_{g_1} \circ \theta_{g_2}(xH) = \theta_{g_1}((g_2xg_2^{-1})H) = (g_1(g_2xg_2^{-1})g_1^{-1})H = (g_1g_2)x(g_1g_2^{-1})^{-1}H = \theta_{g_1g_2}(xH)$. Therefore $\theta_{g_1} \circ \theta_{g_2} = \theta_{g_1g_2}$ so the map from $G$ to $\text{Sym}(G/H)$ given by $g \mapsto \theta_g$ is indeed a homomorphism.
6. [0 points] Let $G$ denote the group $S_3 \times \mathbb{Z}_3$. Define $H$ to be the subgroup generated by the element $a = \left( \begin{array}{ccc} 1 & 2 & 3 \\ 2 & 3 & 1 \end{array} \right)$.

a. [0 point] Write down the left cosets of $H$.

**Solution:** By writing down powers of the element $a$, we see that $a^3$ is the identity. Thus,

$$H = \left\{ e, \left( \begin{array}{ccc} 1 & 2 & 3 \\ 2 & 3 & 1 \end{array} \right), \left[1\right] \right\}.$$  

Since $G$ has order 18 and $H$ has order 3, there should be 6 cosets. We list them one by one:

$$H = \left\{ \left( \begin{array}{ccc} 1 & 2 & 3 \\ 1 & 2 & 3 \end{array} \right), \left[0\right], \left( \begin{array}{ccc} 1 & 2 & 3 \\ 2 & 3 & 1 \end{array} \right), \left[1\right], \left( \begin{array}{ccc} 1 & 2 & 3 \\ 3 & 1 & 2 \end{array} \right), \left[2\right] \right\}.$$  

b. [0 point] Write down several right cosets and show that $H$ is not normal.

**Solution:** The right cosets of $H$ in $G$ are

$$H = \left\{ \left( \begin{array}{ccc} 1 & 2 & 3 \\ 1 & 2 & 3 \end{array} \right), \left[0\right], \left( \begin{array}{ccc} 1 & 2 & 3 \\ 2 & 3 & 1 \end{array} \right), \left[1\right], \left( \begin{array}{ccc} 1 & 2 & 3 \\ 3 & 1 & 2 \end{array} \right), \left[2\right] \right\}.$$  

Note that the first three are the same as the corresponding left cosets. However, the last three right cosets are NOT also left cosets. Hence $H$ is not normal in $G$.  

Hence, $H$ is not normal in $G$.  

Note that the first three are the same as the corresponding left cosets. However, the last three right cosets are NOT also left cosets. Hence $H$ is not normal in $G$.  


7. [0 points] Show that $GL_2(\mathbb{Z}_2)$ is isomorphic to $S_3$.

Solution: $GL_2(\mathbb{Z}_2)$ is the set of invertible 2-by-2 matrices with entries in the field $\mathbb{Z}_2$. First, note that there are $2^4 = 16$ 2-by-2 matrices with entries in $\mathbb{Z}_2$. Out of these, the invertible ones are:

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

Since (up to isomorphism) the only groups of order 6 are $\mathbb{Z}_6$ and $S_3$, to show that $GL_2(\mathbb{Z}_2)$ is isomorphic to $S_3$ it suffices to check that it is not commutative:

$$
\begin{bmatrix}
1 & 1 \\
0 & 1
\end{bmatrix} \begin{bmatrix}
0 & 1 \\
1 & 0
\end{bmatrix} = \begin{bmatrix}
1 & 1 \\
1 & 0
\end{bmatrix} \neq \begin{bmatrix}
1 & 0 \\
1 & 1
\end{bmatrix} = \begin{bmatrix}
0 & 1 \\
1 & 0
\end{bmatrix} \begin{bmatrix}
0 & 1 \\
1 & 1
\end{bmatrix}
$$
8. [0 points] Recall that any group acts on itself by conjugation. Find the orbits of this action for the groups $\mathbb{Z}_6$ and $D_4$.

**Solution:**
(Recall that *conjugation* is the action given by $g \mapsto \tau_g$ where $\tau_g$ is the inner automorphism defined by $\tau_g(x) = gxg^{-1}$ for all $x \in G$.)

$\mathbb{Z}_6$

Since $\mathbb{Z}_6$ is abelian, every inner automorphism of $\mathbb{Z}_6$ is trivial, i.e. the action of $\mathbb{Z}_6$ on itself by conjugation is trivial: For every $g \in \mathbb{Z}_6$ and all $x \in \mathbb{Z}_6$ $\tau_g(x) = g + x + (-g) = x$ so $\tau_g$ is the identity map. Hence, every element of $\mathbb{Z}_6$ is in a separate orbit, i.e. the orbits are $\{[0]\}, \{[1]\}, \{[2]\}, \{[3]\}, \{[4]\}$, and $\{[5]\}$.

$D_4$

We compute the orbits and find that they are $\{e\}, \{\rho, \rho^3\}, \{\rho^2\}, \{\lambda, \lambda \rho^2\}$, and $\{\lambda \rho, \lambda \rho^3\}$.

(Note that we have used the notation of the text for the elements of $D_4$.)
9. [0 points] The orthogonal group \( O(n) \) is a subgroup of \( GL_n(\mathbb{R}) \). It is defined to be

\[
O(n) = \{ M \in GL_n(\mathbb{R}) | M^T M = M M^T = I \}.
\]

This condition ensures that \( M \) preserves the dot product of any two vectors, i.e. \( Mv \cdot Mw = v \cdot w \). As a consequence, \( M \) also preserves the length of vectors and angles between them. Thus, \( O(n) \) consists of the “rigid” symmetries of \( \mathbb{R}^n \): rotations around the origin and reflections across lines passing through the origin.

In this question we will study the orthogonal group for \( n = 2 \) in a more hands-on way.

a. [0 point] It turns out that \( O(2) \) consists of the following symmetries as \( \theta \) varies over all the real numbers.

\[
\text{Rotation by } \theta : \begin{bmatrix}
\cos \theta & -\sin \theta \\
\sin \theta & \cos \theta
\end{bmatrix}
\]

\[
\text{Reflect over the line } y = \tan(\theta/2)x : \begin{bmatrix}
\cos \theta & \sin \theta \\
\sin \theta & -\cos \theta
\end{bmatrix}
\]

Show that this set of matrices is a subgroup of \( GL_2(\mathbb{R}) \).

Solution: We use the subgroup criterion. Certainly \( O(2) \) is nonempty. We check it is closed under multiplication by taking the product of two general elements. We take pairs of the above examples in turn. For example, the product of rotation by \( \theta \) with rotation by \( \phi \) is of course rotation by \( \theta + \phi \)

\[
\begin{bmatrix}
\cos \theta & -\sin \theta \\
\sin \theta & \cos \theta
\end{bmatrix}
\begin{bmatrix}
\cos \phi & -\sin \phi \\
\sin \phi & \cos \phi
\end{bmatrix}
= \begin{bmatrix}
(\cos \theta \cos \phi - \sin \theta \sin \phi) & (-\cos \theta \sin \phi - \sin \theta \cos \phi) \\
(\sin \theta \cos \phi + \cos \theta \sin \phi) & (-\sin \theta \sin \phi + \cos \theta \cos \phi)
\end{bmatrix}
= \begin{bmatrix}
\cos(\theta + \phi) & -\sin(\theta + \phi) \\
\sin(\theta + \phi) & \cos(\theta + \phi)
\end{bmatrix}
\]

Similarly, rotation by \( \theta \) followed by reflection by \( \phi/2 \) is reflection over \( (\theta + \phi)/2 \), and similarly the other way around. Finally, the product of two reflections is a rotation.

To show closure under inverses, just note the inverse of a reflection is itself and the inverse of rotation by \( \theta \) is rotation by \( -\theta \).

b. [0 point] For every \( k \geq 3 \), find an injective homomorphism \( f : D_k \rightarrow O(2) \). In particular \( O(2) \) has elements of every finite order. Are there any elements of infinite order?

Solution: \( D_k \) is defined to be the rotations and reflections fixing a regular \( k \)-gon. Of course, each is a subset (and in fact a subgroup) of \( O(2) \) under this definition. More explicitly, we can realize the rotation and reflections by setting \( \theta = 2\pi n/k \) as \( n \) varies. \( O(2) \) also has elements of infinite order. For example, if \( \theta \) is not a rational multiple of \( 2\pi \) then rotation by \( \theta \) has infinite order.

c. [0 point] Show that the determinant of any element of \( O(2) \) is either 1 or \(-1\).

Solution: For a rotation, we find the determinant is \((\cos \theta)^2 + (\sin \theta)^2 = 1\). For a reflection, we find the determinant is \(-1\).
d. [0 point] By the previous part there is a surjective group homomorphism \( \det : O(2) \to \{1, -1\} \) where the group operation on \( \{1, -1\} \) is multiplication. The kernel of \( \det \) is denoted by \( SO(2) \). Which elements of \( O(2) \) lie in \( SO(2) \)?

Solution: The kernel is precisely the set of rotations. In other words, \( SO(2) \) just consists of rotations.

e. [0 point] Is there an isomorphism \( O(2) \cong SO(2) \times \mathbb{Z}_2 \)?

Solution: No, there is no such isomorphism. The easiest way to see this is to note that the right hand side is commutative (certainly rotations commute!), while the left hand side is not.

f. [0 point] Prove that \( O(2) \) acts on \( \mathbb{R}^2 \) (by left multiplication). What is the orbit of a non-zero vector \( v \in \mathbb{R}^2 \)? What is the stabilizer \( O(2)_v \)?

Solution: The orbit of a vector \( v \) is the circle around the origin of radius \( |v| \). Since both rotations and reflections preserve the length of a vector \( v \), certainly the result of any element of \( O(2) \) acting on \( v \) will have the same length. So the orbit of \( v \) is contained in this circle. By choosing appropriate rotations, we can clearly map \( v \) to every point on the circle, so that the orbit really is the entire thing.

The stabilizer of \( v \) is the set of rotations and reflections fixing \( v \). The only rotation that fixes (a non-zero) \( v \) is the identity. The only reflection is the one whose axis contains \( v \).

Thus, the stabilizer \( O(2)_v \) consists of these two elements.

Remark: the orbit-stabilizer theorem in this context says that elements in the orbit of \( v \) - i.e. a circle - are in bijection with cosets of the stabilizer. One can show that each coset contains a unique rotation. Thus, rotations are in bijection with points of the circle, which seems sensible.
10. [0 points]
   a. [0 point] If $G$ is an abelian group, prove that left multiplication by $g^2$ defines an action of $G$ on itself.

   \textbf{Solution:} For $g \in G$, let $\phi_g : G \rightarrow G$ be the map defined by $\phi_g(x) = g^2x$. First we show that $\phi_g \in \text{Sym}(G)$, i.e. that $\phi_g$ is a bijection from $G$ to $G$. Let $y \in G$. Then $g^{-2}y \in G$ and $\phi_g(g^{-2}y) = g^2(g^{-2}y) = y$ so $\phi_g$ is surjective. Suppose now that $y, z \in G$ and $\phi_g(y) = \phi_g(z)$. Then $g^2y = g^2z$ and by cancellation in the group $G$, $y = z$. Thus $\phi_g$ is injective and $\phi_g \in \text{Sym}(G)$ as required.

   Now we show that the map $G \rightarrow \text{Sym}(G)$ given by $g \mapsto \phi_g$ is a homomorphism. Let $g_1, g_2 \in G$ and let $x \in G$. Then $\phi_{g_1} \circ \phi_{g_2}(x) = \phi_{g_1}(g_2^2x) = (g_1^2g_2^2x)$. Since $G$ is abelian, $g_1^2g_2^2x = (g_1g_2)^2x = \phi_{g_1g_2}(x)$. Thus $\phi_{g_1} \circ \phi_{g_2} = \phi_{g_1g_2}$, so the map $G \rightarrow \text{Sym}(G)$ given by $g \mapsto \phi_g$ is indeed a homomorphism.

   Hence left multiplication by $g^2$ defines an action of $G$ on itself when $G$ is abelian.

Consider now the specific case when $G = U(\mathbb{Z}_{21})$.

   b. [0 point] List the possible sizes of orbits of any action of $G$. (and explain how you know this). For each possible size in your list, find an element whose orbit under the action described in (a) is exactly that size or show that no such element exists.

   \textbf{Solution:} By the Orbit-Stabilizer Theorem, since the order of $G$ is 12, the possible sizes of orbits of any action are 1, 2, 3, 4, 6, and 12. However, we find that \{ $g^2 \mid g \in G$ \} = \{ [1], [4], [16] \}. So, under the action described in (a), the orbit of $x \in G$ is \{ $[1]x, [4]x, [16]x$ \}. Since $G$ is a group, $gx = hx$ if and only if $g = h$ (by cancellation). Therefore, the elements $[1]x, [4]x,$ and $[16]x$ are distinct, so every orbit of this action has size 3.

   All the orbits of the action described in (a) for the group $G = U(\mathbb{Z}_{21})$ are \{ $[1], [4], [16]$ \}, \{ $[2], [8], [11]$ \}, \{ $[5], [20], [17]$ \}, and \{ $[10], [19], [13]$ \}.

   (Note that these are also the cosets of $\langle [4] \rangle$ in $U(\mathbb{Z}_{21})$. Do you see why?)

   c. [0 point] For each of your elements in part (b), describe the stabilizer. Then verify the Orbit-Stabilizer Theorem for those elements.

   \textbf{Solution:} For every element $x \in G$, the stabilizer of $x$ is $\{ g \in G \mid g^2 = [1] \} = \{ [1], [8], [13], [20] \}$. Hence the stabilizer of every element has order 4. Since every orbit has 3 elements and $3 \cdot 4 = 12 = |U(\mathbb{Z}_{21})|$ the Orbit-Stabilizer Theorem is indeed verified in this example.
11. [0 points] For $k \in \mathbb{Z}$, define $\sigma_k : \mathbb{Z}[x] \to \mathbb{Z}[x]$ by $\sigma_k(f(x)) = f(x + k)$.

a. [0 point] Show that for all $k \in \mathbb{Z}$, $\sigma_k$ is an automorphism of the ring $\mathbb{Z}[x]$. (Recall that an automorphism of a ring $R$ is a bijective ring homomorphism from $R$ to $R$.)

**Solution:** Fix $k \in \mathbb{Z}$. First note that for any $f(x) \in \mathbb{Z}[[x]$ the polynomial $\sigma_k(f(x)) = f(x + k)$ is in $\mathbb{Z}[x]$ since $k$ is an integer.

Now, let $f(x), g(x) \in \mathbb{Z}[x]$. Then $\sigma_k(f(x) + g(x)) = \sigma_k((f + g)(x)) = (f + g)(x + k) = f(x + k) + g(x + k) = \sigma_k(f(x)) + \sigma_k(g(x))$. Similarly, $\sigma_k(f(x)g(x)) = \sigma_k((fg)(x)) = (fg)(x + k) = f(x+k)g(x+k) = \sigma_k(f(x))\sigma_k(g(x))$. Thus $\sigma_k$ is indeed a homomorphism from $\mathbb{Z}[x]$ to $\mathbb{Z}[x]$.

Let $f(x) \in \mathbb{Z}[x]$. Then $f(x-k)$ is also in $\mathbb{Z}[x]$ and $\sigma_k(f(x-k)) = f(x)$ so $\sigma_k$ is surjective. Finally, we compute the kernel of the homomorphism $\sigma_k$ to verify that it is injective. Let 0 denote the zero polynomial of $\mathbb{Z}[x]$. We have $\ker(\sigma_k) = \{f(x) \in \mathbb{Z}[x] | \sigma_k(f(x)) = 0\} = \{f(x) \in \mathbb{Z}[x] | f(x-k) = 0\} = \{0\}$. Thus $\sigma_k$ is injective.

So $\sigma_k$ is indeed a bijective ring homomorphism from $\mathbb{Z}[x]$ to $\mathbb{Z}[x]$ as claimed.

b. [0 point] Prove that $k \mapsto \sigma_k$ defines an action of the group $\mathbb{Z}$ on the set $\mathbb{Z}[x]$.

**Solution:** Since the set of automorphisms of $\mathbb{Z}[x]$ is a subset of $\text{Sym} (\mathbb{Z}[x])$, by part (a) it suffices to show that the map from $\mathbb{Z}$ to $\text{Sym} (\mathbb{Z}[x])$ given by $k \mapsto \sigma_k$ is a group homomorphism. So let $k_1, k_2 \in \mathbb{Z}$ and let $f(x) \in \mathbb{Z}[x]$. Then, since $\mathbb{Z}$ is an abelian group under addition, $\sigma_{k_1+k_2}(f(x)) = \sigma_{k_2+k_1}(f(x)) = f(x + (k_2 + k_1)) = f((x + k_2) + k_1) = \sigma_{k_1}(f(x + k_2)) = \sigma_{k_1}(\sigma_{k_2}(f(x))).$ Hence $\sigma_{k_1+k_2} = \sigma_{k_1} \circ \sigma_{k_2}$ for all $k_1, k_2 \in \mathbb{Z}$ and thus the map from $\mathbb{Z}$ to $\text{Sym} (\mathbb{Z}[x])$ given by $k \mapsto \sigma_k$ is indeed a group homomorphism and thus defines an action of the group $\mathbb{Z}$ on the set $\mathbb{Z}[x]$.

c. [0 point] Find the orbit and stabilizer of (i) $f(x) = 2$ and (ii) $g(x) = x^2$ under this action.

**Solution:**

(i) For $k \in \mathbb{Z}$ we have $\sigma_k(f(x)) = f(x + k) = f(x)$. So the orbit of $f(x)$ is the single element set $\{f(x)\}$ and the stabilizer of $f(x)$ is the entire group $\mathbb{Z}$.

(ii) For $k \in \mathbb{Z}$ we have $\sigma_k(g(x)) = g(x + k) = (x + k)^2$ so the orbit of $g(x)$ is the set of all polynomials of the form $(x + k)^2$ for some integer $k$. That is, the orbit of $g(x)$ is the infinite set $\{\ldots, (x - 2)^2, (x - 1)^2, x^2, (x + 1)^2, (x + 2)^2, \ldots\}$. The stabilizer of $g(x)$ is $\{k \in \mathbb{Z} | \sigma_k(g(x)) = g(x)\}$. Now $\sigma_k(g(x)) = g(x)$ if and only if $g(x+k) = g(x)$, i.e. if and only if $(x+k)^2 = x^2$. The only $k$ for which this is true is $k = 0$, so the stabilizer of $g(x)$ is the single element set $\{0\}$. 