INSTRUCTIONS—Read Carefully
• Time: 50 minutes
• There are 4 problems.
• Write your name legibly at the top of this page.
• No calculators or other electronic devices are allowed. (You won’t need them.)
• Show all your work. Partial credit will be given for substantial progress towards the solution. No credit will be given for answers with no explanation, except for Problem #1, which is a True/False question and has no partial credit.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Value</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100</strong></td>
<td>**        **</td>
</tr>
</tbody>
</table>
**Problem 1.** (20 points) This is a TRUE/FALSE question. For each statement, circle whether it is true or false. You do not need to give a reason for your answer. The scoring for this problem is:

- Correct Answer = 2.5 points,
- Blank = 1 point,
- Incorrect Answer = 0 points.

**Solution.** I didn’t ask you to give a reason for your answer, but I’ll provide a reason.

(a) Let \( V \) be finite-dimensional a vector space, let \( \mathcal{B} \) be a basis of \( V \), and let \( \mathcal{S} \) be a spanning set. Then always \( \#\mathcal{B} \leq \#\mathcal{S} \).

True

We know that every spanning set contains a basis, so \( \mathcal{S} \) contains a basis, and every basis has the same number of elements, so \( \mathcal{S} \) must be at least as large as \( \mathcal{B} \).

(b) Let \( V \) be a finite-dimensional vector space, let \( \mathcal{B} \) be a basis of \( V \), and let \( \mathcal{L} \) be a linearly independent set. Then \( \#\mathcal{B} \leq \#\mathcal{L} \).

False

Similarly, we know that every linearly independent set can be extended to a basis, so \( \mathcal{L} \) can’t be larger than \( \mathcal{B} \). This inequality is going the wrong direction to be true. As a particular example, take any vector \( v \in \mathcal{B} \) and let \( \mathcal{L} = \mathcal{B} \setminus \{v\} \). Then \( \mathcal{L} \) is linearly independent and smaller than \( \mathcal{B} \).

(c) Every element of a ring has an additive inverse.

True

Addition makes the elements of a ring into an abelian group, so in particular, every element has an inverse.

(d) Every element of a field has an multiplicative inverse.

False

This is almost true, but not quite, since 0 never has an inverse.

(e) Let \( G \) be a group, and let \( \phi : G \to G \) be the map \( \phi(g) = g^2 \). Then \( \{g \in G : \phi(g) = e\} \) is always a normal subgroup of \( G \).

False

The set looks like its the kernel of the homomorphism \( \phi \), but unfortunately \( \phi \) isn’t a homomorphism (unless \( G \) is an abelian group). So in general the set isn’t even a subgroup, much less a normal subgroup. As a particular example, consider \( D_3 \), the dihedral group. It
has one element of order 1, three elements of order 2 (the flips), and two elements of order 3 (the non-trivial rotations). So in this case \( \{ g \in D_3 : \phi(g) = e \} \) has 4 elements, so Lagrange says that it can’t be a subgroup of \( D_3 \), which has 6 elements.

(f) Addition in a field is commutative.

True

A field is a special kind of ring, and the definition of ring says that addition makes the ring into a commutative group.

(g) Let \( F \) be a field, and let \( f(x) \in F[x] \) be an irreducible polynomial. Then the only way to factor \( f(x) \) as \( f(x) = g(x)h(x) \) with \( g(x), h(x) \in F[x] \) is to have either \( g(x) = \pm 1 \) or \( h(x) = \pm 1 \).

False

This looks like the definition of prime number in \( \mathbb{Z} \), but it’s not quite right for a polynomial ring, since for any non-zero constant \( c \in F^* \), we can factor \( f(x) \) as \( f(x) = c^{-1} \cdot cf(x) \). The correct definition is that only way to factor \( f(x) \) as \( f(x) = g(x)h(x) \) with \( g(x), h(x) \in F[x] \) is to have either \( g(x) \in F^* \) or \( h(x) \in F^* \).

(h) Suppose that a finite group \( G \) acts on a finite set \( X \). Then it is always true that for every \( x \in X \), the orbit \( Gx \) of \( x \) has more elements than the stabilizer \( G_x \) of \( x \).

False

Sometimes the orbit is larger, sometimes the stabilizer is larger. As an example showing that the statement is false, let \( G \) act trivially on a set \( X \). Then every orbit has 1 element, since \( Gx = \{ x \} \), and every stabilizer is as large as possible, \( G_x = G \). In particular, \#G_x > #Gx.

(i) Let \( G \) be a group and let \( H \) be a subgroup. Then \( H \) is a normal subgroup of \( G \) if and only if \( g^{-1}Hg^{-1} = H \) for every \( g \in G \).

True

Our definition was that \( H \) is normal if \( g^{-1}Hg = H \) for every \( g \in G \). But as \( g \) ranges over the elements of \( G \), so does \( g^{-1} \), so we equally well have that

\[ H \text{ is normal} \iff (g^{-1})^{-1}Hg^{-1} = H \quad \text{for all } g \in G. \]

Since \( (g^{-1})^{-1} = g \), this is exactly the desired statement.

(j) There are no fields with 91 elements.

True

This is true, since 91 = 7 \cdot 13, and we know that every finite field has \( p^d \) elements for some prime \( p \) and some \( d \geq 1 \).
Problem 2. (25 points) Let $F$ be a field, and let $V$ be the vector space of polynomials of degree at most $n$, that is,

$$V = \{ a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n : a_0, a_1, \ldots, a_n \in F \}.$$ 

Let $D : V \to V$ be the map that sends a polynomial to its derivative,

$$D(a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n) = a_1 + 2a_2 X + 3a_3 X^2 + \cdots + na_n X^{n-1}.$$ 

(a) Prove that $D$ is an $F$-linear transformation.

(b) Assume that $F$ has characteristic 0. The image of $D$ and the null space (kernel) of $D$ are defined by:

- $\text{Image}(D) = \{ D(p(x)) : p(x) \in V \}$,
- $\text{Null}(D) = \{ p(x) \in V : D(p(x)) = 0 \}$.

Write down a basis for $\text{Image}(D)$ and $\text{Null}(D)$. What are their dimensions?

(c) Suppose instead that $F$ has characteristic $p$ for some prime $p > 0$, for example, suppose that $F = \mathbb{F}_p$. Write down a basis for $\text{Null}(D)$ and compute its dimension.

Solution. (a)

$$D(p(X) + q(X)) = D \left( \sum_{k=0}^{n} a_k X^k + \sum_{k=0}^{n} b_k X^k \right) = D \left( \sum_{k=0}^{n} (a_k + b_k) X^k \right)$$

$$= \sum_{k=1}^{n} k(a_k + b_k) X^{k-1} = \sum_{k=1}^{n} ka_k X^{k-1} + \sum_{k=1}^{n} kb_k X^{k-1}$$

$$= D \left( \sum_{k=0}^{n} a_k X^k \right) + D \left( \sum_{k=0}^{n} b_k X^k \right) = D(p(X)) + D(q(X)).$$

Similarly,

$$D(cp(X)) = D \left( c \sum_{k=0}^{n} a_k X^k \right) = D \left( c \sum_{k=0}^{n} a_k X^k \right) = \sum_{k=0}^{n} kca_k X^{k-1}$$

$$= c \sum_{k=0}^{n} ka_k X^{k-1} = cD \left( \sum_{k=0}^{n} a_k X^k \right) = cD(p(X)).$$

(b) When we apply $D$, the degree of a polynomial goes down by 1, so the image of $D$ is every polynomial of degree at most $n - 1$. More precisely, given any polynomial

$$q(X) = \sum_{k=0}^{n-1} b_k X^k,$$
we see that \( q(X) \) is in the image of \( D \), since

\[
D \left( \sum_{k=1}^{n} k^{-1} b_k X^k \right) = q(X).
\]

Note that it’s okay to take \( k^{-1} \) in \( F \), since \( F \) has characteristic 0, so \( k \neq 0 \) in \( F \) for all \( k \geq 1 \). This proves that

\[
\text{Basis for Image}(D) = \{1, X, \ldots, X^{n-1}\},
\]

and

\[
\dim \text{Image}(D) = n.
\]

Suppose \( p(X) = \sum a_k X^k \) in \text{Null}(D). This means that

\[
\sum_{k=0}^{n} k a_k X^{k-1} = 0, \quad \text{so} \quad k a_k = 0 \quad \text{for all} \quad 0 \leq k \leq n.
\]

For \( k = 0 \), we can take any value for \( a_0 \), but for \( k \geq 1 \), since \( k \neq 0 \) in \( F \), we must have \( a_k = 0 \). Hence the kernel of \( D \) consists of the constant polynomials,

\[
\text{Basis for Null}(D) = \{1\}
\]

and

\[
\dim \text{Null}(D) = 1.
\]

(c) This is similar to (c), except that now the condition \( k a_k = 0 \) does not always imply that \( a_k = 0 \). Indeed, we’re in a field where \( p = 0 \), and more generally, any multiple of \( p \) is 0. It follows that

\[
D(X^k) = kX^{k-1} = 0 \quad \text{for all} \quad k \text{ such that} \quad p \mid k.
\]

Hence

\[
\text{Basis for Null}(D) = \{X^{pj} : 0 \leq j \leq n/p\}
\]

and

\[
\dim \text{Null}(D) = \left\lfloor \frac{n}{p} \right\rfloor + 1.
\]

**Problem 3.** (25 points) Let \( F \) be a field, and suppose that the polynomial \( X^2 + X + 1 \) is irreducible in \( F[X] \). Let

\[
K = F[X]/(X^2 + X + 1)F[X]
\]

be the quotient ring. We know from class that \( K \) is a field. We will put bars over polynomials to indicate that they represent elements of \( K \), for example, we write \( \overline{X} + 2 \) for the corresponding element of \( K \). In other words, if we let \( I \) be the ideal \( I = (X^2 + X + 1)F[X] \), then \( \overline{X} + 2 \) is shorthand for the coset \( (X + 2) + I \).

(a) Find a polynomial \( p(X) \in F[X] \) of degree at most 1 satisfying

\[
p(X) = \frac{X+3}{2X+1}.
\]

\[
\overline{p(X)} = (\overline{X} + 3) \cdot (2\overline{X} + 1).
\]
(b) Find a polynomial \( q(X) \in F[X] \) satisfying
\[
q(X) \cdot (X+1) = 1.
\]
In other words, find a multiplicative inverse for \( X+1 \) in the field \( K \).

(c) Find a polynomial \( r(X) \in F[X] \) satisfying
\[
r(X)^2 = -3.
\]
In other words, find a square root of \(-3\) in the field \( K \).

**Solution.** (a) First we multiply
\[
(X + 3)(2X + 1) = 2X^2 + 7X + 3.
\]
Then we use the fact that \( X^2 + X + 1 = 0 \) in \( K \). In general, we’d divide by \( X^2 + X + 1 \) and take the remainder, but in this case, we just need to subtract,
\[
(X + 3) \cdot (2X + 1) = 2X^2 + 7X + 3
= (2X^2 + 7X + 3) - 2(X^2 + X + 1)
= 5X + 1.
\]

(b) There are various ways to do this problem, but the most direct is simply to write
\[
(aX + b) \cdot (X + 1) = 1,
\]
multiply it out, and solve for \( a \) and \( b \). But remember to use the fact that \( X^2 + X + 1 = 0 \). Thus
\[
(aX + b) \cdot (X + 1) = aX^2 + (a + b)X + b
= (aX^2 + (a + b)X + b) - a(X^2 + X + 1)
= bX + (b - a).
\]
We want this to equal \( 1 \), so we need
\[
b = 0 \quad \text{and} \quad b - a = 1.
\]
So \( b = 0 \) and \( a = -1 \). In other words, we can take \( q(X) = -X \), and then
\[
(-X) \cdot (X + 1) = 1.
\]

(c) We want
\[
(aX + b)^2 = -3.
\]
Multiplying this out gives
\[
a^2X^2 + 2abX + b^2 = -3.
\]
Subtracting \( a^2(X^2 + X + 1) \) from the left-hand side, which is allowed, since this quantity equals \( 0 \) in \( K \), we want to find \( a \) and \( b \) so that

\[
(2ab - a^2)X + (b^2 - a^2) = -3.
\]

So we need

\[
a(2b - a) = 0 \quad \text{and} \quad b^2 - a^2 = -3.
\]

The first equation says that either \( a = 0 \), or \( a = 2b \).

If we set \( a = 0 \), then the second equation gives \( b^2 = -3 \). But there might not be any element of \( F \) whose square is \( -3 \). So we turn to the second possibility, namely

\[
a = 2b.
\]

Substituting this into \( b^2 - a^2 = -3 \) gives

\[
\begin{align*}
  b^2 - (2b)^2 &= -3, \\
-3b^2 &= -3, \\
  b^2 &= 1.
\end{align*}
\]

This has the solution \( b = \pm 1 \) in \( F \). And then we take \( a = 2b = 2 \). This proves that

\[
r(X) = 2X + 1 \quad \text{satisfies} \quad r(X)^2 = (2X + 1)^2 = -3.
\]

**Problem 4.** (25 points) Let \( \pi \in S_9 \) be the permutation defined by

\[
\begin{array}{cccccccc}
  1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
  3 & 5 & 2 & 4 & 1 & 9 & 7 & 6 & 8
\end{array}
\]

Let

\[
G = \{e, \pi, \pi^2, \pi^3, \ldots\}
\]

be the subgroup of \( S_9 \) generated by the powers of \( \pi \).

(a) Describe the orbits of \( G \) acting on the set \{1, 2, \ldots, 9\}.

(b) For which elements \( x \) of \{1, 2, \ldots, 9\} is the stabilizer \( G_x \) equal to all of \( G \)?

(c) What is the stabilizer of the element \( 3 \in \{1, 2, \ldots, 9\} \)? In other words, describe the subgroup \( G_3 \).

**Solution.** (a) We start with 1 and compute its orbit as we repeatedly apply \( \pi \).

\[
1 \xrightarrow{\pi} 3 \xrightarrow{\pi} 2 \xrightarrow{\pi} 5 \xrightarrow{\pi} 1.
\]
So 1, 2, 3, 5 are in the same orbit. Next we find the orbit of 4. Hmmm... \( \pi(4) = 4 \), so the orbit of 4 is just 4. Similarly, \( \pi(7) = 7 \), so the orbit of 7 is 7. Finally, we see that 6, 8, and 9 form an orbit, since

\[
6 \xrightarrow{\pi} 9 \xrightarrow{\pi} 8 \xrightarrow{\pi} 6.
\]

So \( G \) has four orbits:

- \( G \cdot 1 = G \cdot 2 = G \cdot 3 = G \cdot 5 = \{1, 2, 3, 5\} \),
- \( G \cdot 6 = G \cdot 8 = G \cdot 9 = \{6, 8, 9\} \),
- \( G \cdot 4 = \{4\} \),
- \( G \cdot 7 = \{7\} \).

(b) The elements 4 and 7 are fixed by \( \pi \), so they are also fixed by all powers of \( \pi \). Hence

\[
\text{4 and 7 have stabilizers } G_4 = G_7 = G,
\]

None of the other elements of \( \{1, 2, \ldots , 9\} \) are fixed by \( \pi \), so their stabilizers cannot be all of \( G \).

(c) From (a) we see that 3, \( \pi(3), \pi^2(3), \pi^3(3) \) are distinct, but \( \pi^4(3) = 3 \). So \( \pi^4 \) is in the stabilizer of 3, and similarly so are \( \pi^8, \pi^{12}, \pi^{16}, \ldots \). So the stabilizer \( G_3 \) is all powers of \( \pi^4 \). However, we can note that \( \pi^{12} \) actually fixes every element in \( \{1, 2, \ldots , 9\} \), and that’s the smallest power of \( \pi \) that fixes every element, so \( \pi \) has order 12. In particular, \( \pi^{12} = e \), so

\[
\text{Stabilizer of } 3 = G_3 = \{e, \pi^4, \pi^8\}.
\]