MIDTERM
Maximal Score: 200 points

Wednesday october 16th

Problem 1: (⋆⋆) 60 points
Let
\[ \mathbb{Q}(\sqrt{2}) := \{ a + b\sqrt{2} \mid a, b \in \mathbb{Q} \} \]
We admit that \( \mathbb{Q}(\sqrt{2}) \) is a subring of \( \mathbb{R} \).

1. Show that every non-zero element of \( \mathbb{Q}(\sqrt{2}) \) is invertible in \( \mathbb{Q}(\sqrt{2}) \). (Remark: Then, we have proven that \( \mathbb{Q}(\sqrt{2}) \) is a field.)

2. Let \( a \) be a rational number and \( b \) a positive rational such that \( \sqrt{b} \) is irrational. Prove that if \( a + \sqrt{b} \) is a root of some polynomial with rational coefficient then \( a - \sqrt{b} \) is also a root of this polynomial. (Hint: Compute the Euclidean division by \((x-a)^2 - b\) on \( \mathbb{Q}[x] \) and prove that \(((x-a)^2 - b)\) divides \( p(x) \).)

3. Show that there is an isomorphism
\[ \mathbb{Q}[x]/(x^2 - 2) \cong \mathbb{Q}(\sqrt{2}) \]

Solution:

1. Let \( a + b\sqrt{2} \) be a non-zero element of \( \mathbb{Q}(\sqrt{2}) \) then we have to check that the inverse in \( \mathbb{R} \) is in \( \mathbb{Q}(\sqrt{2}) \), but
\[
\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}
\]
where \( \frac{a}{a^2-2b^2} \in \mathbb{Q} \) and \( \frac{b}{a^2-2b^2} \in \mathbb{Q} \).

2. Denote by \( D(x) = ((x-a)^2 - b) \), then
\[ P(x) = D(x)Q(x) + cx + d = ((x-a)^2 - b)Q(x) + cx + d \]
where \( c, d \) are rational numbers (by virtue of the fact that the coefficients of \( P(x) \) and \( D(x) \) are all rational). But \( a + \sqrt{b} \) is a root of \( P(x) \):
\[ P(a + \sqrt{b}) = c(a + \sqrt{b}) + d = (a + \sqrt{b}) = 0. \]
This implies that \( c \) and \( d \) are 0, since otherwise the final equality could be arranged to suggest the irrationality of rational values (and vice versa). Hence \( P(x) = \)
$D(x)Q(x)$, for some quotient polynomial $Q(x)$ and $D(x)$ is a factor of $P(x)$.

(Remark: This property may be generalized as: if an irreducible polynomial $P$ has a root in common with a polynomial $Q$, then $P$ divides $Q$.)

3. We define the morphism

$$
\phi : \mathbb{Q}[x] \rightarrow \mathbb{Q}(\sqrt{2})
$$

$$
p(x) \mapsto p(\sqrt{2})
$$

\(\phi\) is clearly an morphism of rings, since:

- \(\phi(p(x) + r(x)) = p(\sqrt{2}) + r(\sqrt{2}) = \phi(p(x)) + \phi(r(x))\).
- \(\phi(p(x)r(x)) = p(\sqrt{2})r(\sqrt{2}) = \phi(p(x))\phi(r(x))\).

It is surjective since for any \(a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})\) we have \(p(bx + a) = b\sqrt{2} + a\). As we have seen in the previous question if \(p(\sqrt{2}) = 0\), we have that \(x^2 - 2\) divides \(p(x)\). Then \(\ker(\phi) \subseteq (x^2 + 1)\). The converse inclusion is clearly true.

Problem 2: \((\star)\) 15 points If \(r \in R\), \(R\) is an integral domain and \(r^2 = 1\), prove \(r = \pm 1\).

Solution:

By distributive law, \((r + 1)(r - 1) = r^2 - 1\). Thus, if \(r^2 - 1 = 0\) and \(R\) is an integral domain, then \(r + 1 = 0\) or \(r - 1 = 0\).

Problem 3: \((\star\star)\) 30 points (The questions are independent.)

1. Find the remainder and the quotient upon division of \(x^3\) by \(x^2 + x + 4\) in \((\mathbb{Z}/2\mathbb{Z})[x]\).

2. List all the irreducible monic quadratic polynomials in \((\mathbb{Z}/2\mathbb{Z})[x]\). Justify your answer.

Solution:

1. First \(x^2 + x + 4 = x^2 + x\) in \((\mathbb{Z}/2\mathbb{Z})[x]\). We do the division

\[
\begin{array}{c|cc}
\multicolumn{1}{r}{x^3} & x^2 + x & x - 1 \\
\hline
-(x^3 + x^2) & x^2 + x & \\
\hline & -x & \\
& -x^2 & \\
& x & \\
\end{array}
\]

Then \(x^3 = (x^2 + x)(x + 1) + x\).

2. All possible monic quadratic polynomials in \((\mathbb{Z}/2\mathbb{Z})[x]\) are \(x^2\), \(x^2 + x\), \(x^2 + 1\) and \(x^2 + x + 1\). The first two are clearly reducible. The third has 1 as zero and it factors as \((x + 1)(x - 1)\). The last is the only one that is irreducible since it has no roots on \((\mathbb{Z}/2\mathbb{Z})[x]\).

Problem 4: \((\star)\) 20 points

Prove that \(\sqrt[5]{\frac{17}{25}}\) is not a rational number. (Hint: It may be helpful to consider the polynomial \(f(x) = 25x^5 - 17\).)
**Solution:** Consider the polynomial \( f(x) = 25x^5 - 17. \) Note that this polynomial is irreducible over \( \mathbb{Q} \) by Eisenstein criterion applied with \( p = 17. \) If \( 5\sqrt{\frac{17}{25}} \) were in \( \mathbb{Q} \) then \( f(x) \) would be reducible as it would have a root in \( \mathbb{Q}, \) thus \( 5\sqrt{\frac{17}{25}} \notin \mathbb{Q}. \)

**Problem 5:** \((\star)\) 30 points Define \( W = \{ f \in \mathbb{R}_3[x] | f'(0) = 0 \}. \)

1. Prove that \( W \) is a subspace of \( \mathbb{R}_3[x] \) of the polynomial of degree less or equal to 3;
2. Find a basis for \( W \) (and prove that it is a basis).

**Solution:**

1. Take \( f, g \in W \) and \( k \in \mathbb{R}. \) By linearity of derivatives,

\[
(f + kg)'(0) = f'(0) + kg'(0) = 0 + k \times 0 = 0
\]

Thus \( f + kg \in W \) and we have proved the subspace criterion.

2. To find a generic element of \( W \) we start with the generic element of \( \mathbb{R}_3[x] \) and apply the constraint. Define \( f(x) = a + bx + cx^2 + dx^3. \) If \( f \in W, \) then

\[
0 = f'(0) = (b + 2cx + 3dx^2)|_{x=0} = b
\]

Thus,

\[
W = \{a + cx^2 + dx^3 : a, c, d \in \mathbb{R}\}.
\]

Let \( \beta = \{1, x^2, x^3\}. \) Clearly this is a spanning set given \( f \in W, \)

\[
f = a + cx^2 + dx^3
\]

Since \( 1, x^2 \) and \( x^3 \) all have different degrees they must be linearly independent. So \( \beta \) is indeed a basis.

**Problem 6:** \((\star \star)\) 20 points Prove that the two subrings of \( \mathbb{Z}: 2\mathbb{Z} \) and \( 3\mathbb{Z} \) are not isomorphic as rings.

**Solution:** We may construct a group homomorphism \( \phi : 2\mathbb{Z} \to 3\mathbb{Z}. \) Clearly this is only subjective if \( \phi(2) = \pm 3. \) Now, if we try to make \( \phi \) a ring homomorphism, \( \phi(2 + 2) = 2\phi(2) \) and \( \phi(2 \times 2) = \phi(2) \times \phi(2). \) These two values of \( \phi(4) \) are not consistent if \( \phi(2) = \pm 3. \) Thus there is no surjective ring homomorphism and so \( 2\mathbb{Z} \) and \( 3\mathbb{Z} \) are not isomorphic as rings.

**Problem 7:** \((\star)\) 35 points

1. Let \( n \in \mathbb{Z}_{\geq 2} \) and suppose that \( a_nx^n + \ldots + a_1x + a_0 \in \mathbb{Z}[x] \) has factor \( ax + b. \) Show that \( a|a_n \) and \( b|a_0. \)

2. **Bonus:** Suppose \( \alpha \) is a rational root of a monic polynomial in \( \mathbb{Z}[x]. \) prove that \( \alpha \) is an integer. (Hint: write \( \alpha = p/q \) where \( p \) and \( q \) are coprime, prove that then \( q|p \) and conclude.)
Solution:

1. Suppose that \( a_n x^n + \ldots + a_1 x + a_0 = (ax + b)(a_{n-1} x^{n-1} + \ldots + a_1 x + a_0) \), then

\[
\begin{align*}
ac_{n-1} &= a_n \\
b_{c_0} &= a_0
\end{align*}
\]

Therefore, \( a|a_n \) and \( b|a_0 \).

2. Let \( \alpha = \frac{p}{q} \) be a rational root of the polynomial

\[ x^n + b_{n-1} x^{n-1} + \ldots + b_1 x + b_0 \in \mathbb{Z}[x] \]

We may assume that \( p \) and \( q \) and coprime, then:

\[
\left(\frac{p}{q}\right)^n + b_{n-1} \left(\frac{p}{q}\right)^{n-1} + \ldots + b_1 \frac{p}{q} + b_0 = 0
\]

in \( \mathbb{Q}[x] \). Multiply the whole expression by \( q^n \) to get

\[
p^n + b_{n-1}pq + \ldots + b_1pq^n + b_0q^n = 0
\]

Therefore, \( q \) must divides \( p^n \). But \( p \) and \( q \) are coprime, so \( q \) must equal \( 1 \) therefore \( \alpha \) is an integer.

\[\text{1} \]

\[\text{\(1\)}(\star) = \text{easy} \quad (\star\star) = \text{medium} \quad (\star\star\star) = \text{challenge}\]