Problem 1. Let $V$ be the $\mathbb{R}$-vector space of all polynomials $ax^2 + bx + c$ with $a, b, c \in \mathbb{R}$. For $p(x), q(x) \in V$, define

$$\langle p(x), q(x) \rangle = p'(0)q(0) + p(0)q'(0),$$

where $p'(x)$ denotes the derivative of $p(x)$.

(a) Verify that $\langle \cdot, \cdot \rangle$ is a symmetric bilinear form.

(b) Find an orthogonal basis of $\langle \cdot, \cdot \rangle$.

(c) What is the signature of $\langle \cdot, \cdot \rangle$?

Proof.

(a) It is symmetric because $\langle q(x), p(x) \rangle = q'(0)p(0) + q(0)p'(0) = \langle p(x), q(x) \rangle$.

$$\langle \lambda_1 p_1(x) + \lambda_2 p_2(x), q(x) \rangle = (\lambda_1 p_1'(0) + \lambda_2 p_2'(0))q(0) + (\lambda_1 p_1(0) + \lambda_2 p_2(0))q(0) =$$

$$= \lambda_1 (p_1'(0)q(0) + p_1(0)q'(0)) + \lambda_2 (p_2'(0)q(0) + p_2(0)q'(0)) = \lambda_1 \langle p_1(x), q(x) \rangle + \lambda_2 \langle p_2(x), q(x) \rangle.$$

So it is linear in the first factor. Because of the symmetry, it is also linear in the second factor.

(b) $x^2$ is perpendicular to everything, and $\langle 1, 1 \rangle = \langle x, x \rangle = 0$ and $\langle 1, x \rangle = 1$. If we use the basis $e_1 = 1 + x$, $e_2 = 1 - x$, and $e_3 = x^2$, then the matrix of the bilinear form is

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

So $e_1, e_2, e_3$ are orthogonal.

(c) The signature is $(1, 1, 1)$ (1 positive eigenvalue, 1 negative, and 1 zero eigenvalue).

Problem 2. List all the groups of order $2012 = 2^2 \cdot 503$ (503 is prime). List each of the groups exactly once, and also include the abelian groups.

Proof. The only abelian groups of order 2012 are $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/503\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/503\mathbb{Z}$. Let $G$ be a nonabelian group of order 2012. The number of 503-Sylow subgroups is congruent to 1 modulo 503 and divides 4. Therefore, there is a unique 503-Sylow subgroup $N$. So $N$ is normal and isomorphic to $\mathbb{Z}/503\mathbb{Z}$. Let $H$ be a 2-Sylow subgroup. Then $H$ has 4 elements and is isomorphic to $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Since $|H \cap N|$ divides 4 and 503 we have that $H \cap N = \{e\}$ and $|HN| = |H| \cdot |N|/|H \cap N| = 2012$, so $HN = G$. It follows that $G$ is a semidirect product $H \rtimes N$. Define $\phi : H \rightarrow \text{Aut}(N) \cong \mathbb{Z}/502\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/251\mathbb{Z}$ such that $\phi(h)$ is conjugation by $h$.

Suppose that $H$ is isomorphic to $\mathbb{Z}/4\mathbb{Z}$, and let $h$ be a generator of $H$. The only possibility is $\phi(h) = (1,0) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/251\mathbb{Z}$ and $G = \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/503\mathbb{Z}$ is a semi-direct product. (The group $G$ is a central extension of $D_{503}$ by $\mathbb{Z}/2\mathbb{Z}$).
Suppose that \( H \) is isomorphic to \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \). After a change of coordinates in \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \) we may assume that \( \phi(a, b) = (b, 0) \) for \( a, b \in \mathbb{Z}/2\mathbb{Z} \). In this case \( G \) is a semi-direct product \((\mathbb{Z}/2 \times \mathbb{Z}/2) \rtimes \mathbb{Z}/503\mathbb{Z} \cong \mathbb{Z}/2 \times (\mathbb{Z}/2 \rtimes \mathbb{Z}/503\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z} \times D_{503}. \)

\[\square\]

**Problem 3.** What is the Galois group of \( p(x) = x^3 - x + 4 \), considered over the ground fields

- (a) \( \mathbb{Z}/3\mathbb{Z} \);
- (b) \( \mathbb{R} \);
- (c) \( \mathbb{Q} \).

**Proof.**

(a) \( p(x) \) has no roots in \( \mathbb{Z}/3\mathbb{Z} \) so \( p(x) \) is irreducible. The Galois group is either \( S_3 \) or \( \mathbb{Z}/3\mathbb{Z} \). But the Galois group over a finite field is cyclic, so it must be \( \mathbb{Z}/3\mathbb{Z} \).

(b) \( p(x) \) has 1 real root and 2 complex roots, because \( p(x) > 0 \) for \( x \geq 1 \) and \( p(x) \) is increasing for \( x < 1 \). So the Galois group must be \( \mathbb{Z}/2\mathbb{Z} \).

(c) Since \( p(x) \) is irreducible over \( \mathbb{Z}/3\mathbb{Z} \), it is irreducible over \( \mathbb{Q} \). The Galois group is either \( S_3 \) or \( \mathbb{Z}/3\mathbb{Z} \). Since complex conjugation is a nontrivial element in the Galois group of order 2 (since \( p(x) \) has complex roots), the Galois group must be \( S_3 \).

\[\square\]

**Problem 4.** Suppose that \( V \) is an \( n \)-dimensional \( \mathbb{C} \)-vector space of dimension \( n \).

(a) Show that there exists a unique \( \mathbb{C} \)-linear map \( \psi : \Lambda^3 V \to (\Lambda^2 V) \otimes V \) such that

\[ \psi(a \wedge b \wedge c) = (b \wedge c) \otimes a + (c \wedge a) \otimes b + (a \wedge b) \otimes c. \]

(b) Show that \( \psi \) is injective.

**Proof.**

(a) Define \( \gamma : V \times V \times V \to (\Lambda^2 V) \otimes V \) by

\[ \gamma(a, b, c) = (b \wedge c) \otimes a + (c \wedge a) \otimes b + (a \wedge b) \otimes c. \]

It is easy to verify that \( \gamma \) is multi-linear. Also we have

\[ \gamma(b, a, c) = (a \wedge c) \otimes b + (c \wedge b) \otimes a + (b \wedge a) \otimes c = -(c \wedge a) \otimes b - (b \wedge c) \otimes a - (a \wedge b) \otimes c = -\gamma(a, b, c). \]

Similarly \( \gamma(a, c, b) = -\gamma(a, b, c) \) and \( \gamma(c, b, a) = -\gamma(a, b, c) \). So \( \gamma \) is skew-symmetric and by the universal property of \( \Lambda^3 V \), there exists a unique linear map \( \psi : \Lambda^3 V \to (\Lambda^2 V) \otimes V \) such that \( \psi(a \wedge b \wedge c) = \gamma(a, b, c) \) for all \( a, b, c \in V \).

(b) Choose a basis \( e_1, e_2, \ldots, e_n \) of \( V \). A basis of \( (\Lambda^2 V) \otimes V \) is given by all \( (e_i \wedge e_j) \otimes e_k \) where \( 1 \leq i < j \leq n \) and \( 1 \leq k \leq n \), and a basis of \( \Lambda^3 V \) is given by all \( 1 \leq i < j < k \leq n \). If \( i < j < k \), then

\[ \psi(e_i, e_j, e_k) = (e_j \wedge e_k) \otimes e_i - (e_i \wedge e_k) \otimes e_j + (e_i \wedge e_j) \otimes e_k. \]

Now all the basis vectors \( (e_j \wedge e_k) \otimes e_i, (e_i \wedge e_k) \otimes e_j, (e_i \wedge e_j) \otimes e_k \) with \( i < j < k \) are distinct, and therefore linearly independent. It follows that \( \{ \psi(e_i, e_j, e_k) \mid i < j < k \} \) is a linearly independent set of vectors. Hence \( \psi \) is injective.

\[\square\]

**Problem 5.** Suppose that \( G \) is a finite group such that the automorphism group \( \text{Aut}(G) \) is nilpotent. Show that \( G \) is nilpotent.
Proof. Define a group homomorphism $\phi : G \to \text{Aut}(G)$ such that $\phi(g) \in \text{Aut}(G)$ is conjugation by $g$. The kernel of $\phi$ is $Z(G)$, the center of $G$. The group $G/Z(G)$ is isomorphic to a subgroup of $\text{Aut}(G)$, so it is nilpotent. It follows that $G$ is nilpotent, for example by looking at the lower central series.
Problem 1. Let $T$ the $\mathbb{C}$-linear endomorphism of $\mathbb{C}[x]/((x^3 - x)^2)$ given by multiplication by $x^2$.

(a) What is the minimum polynomial of $T$?
(b) What is the Jordan canonical form of $T$?

Proof.
(a) Let $S$ be multiplication by $x$. Its minimum and characteristic polynomial is equal to $p(x) = (x^3 - x)^3 = x^6 - 2x^4 + x^2 = q(x^2)$, where $q(x) = x^3 - 2x^2 + x = x(x - 1)^2$. We have $q(T) = p(S^2) = 0$. Suppose that $r(x)$ is nonzero and $r(T) = 0$. Then we have $r(T) = r(S^2) = 0$ is zero, and $p(x)$ divides $r(x^2)$. This shows that the degree of $r$ is at least 3. So $q(x)$ is the minimum polynomial.

With respect to the basis $1,x^2,x^4,x,x^3,x^5$, the matrix of $T$ is given by

$$
\begin{pmatrix}
A & 0 \\
0 & A
\end{pmatrix}
$$

where $A$ is the companion matrix of $q(x)$. The Jordan normal form of $A$ is

$$
\begin{pmatrix}
1 & 1 & 0 \\
0 & 1 & 0 \\
0 & 0 & 0
\end{pmatrix},
$$

so the Jordan normal form of $T$ is

$$
\begin{pmatrix}
1 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}
$$

□

Problem 2. List all prime ideals in the ring $\mathbb{Z}[x]/(30, x^2 + 1)$. List each ideal exactly once. Which of these prime ideals are maximal?

Proof. Let $R = \mathbb{Z}[x]/(30, x^2 + 1)$. Suppose $\mathfrak{p}$ is a prime ideal. Since $30 = 2 \cdot 3 \cdot 5 \in \mathfrak{p}$ we have $2 \in \mathfrak{p}$, $3 \in \mathfrak{p}$ or $5 \in \mathfrak{p}$.

If $2 \in \mathfrak{p}$ Then $(x + 1)^2 = x^2 + 2x + 1 = (x^2 + 1) + 2x \in \mathfrak{p}$, so $(x + 1) \in \mathfrak{p}$. $R/(2, x + 1) = \mathbb{Z}/2\mathbb{Z}$ is a field, so $(2, x + 1)$ is a maximal ideal contained in $\mathfrak{p}$. Hence $\mathfrak{p} = (2, x + 1)$ is maximal.

If $3 \in \mathfrak{p}$, then $R/(3) = \mathbb{Z}/3\mathbb{Z}[x]/(x^2 + 1)$ is a field because $x^2 + 1$ is irreducible in $\mathbb{Z}/3\mathbb{Z}[x]$. So $(3)$ is maximal and $\mathfrak{p} = (3)$. 

1
If $5 \in p$, then $(x+2)(x+3) = x^2 + 5x + 1 = (x^2 + 1) + 5x \in p$. So either $(x+2) \in p$ and then $p = (5, x+2)$ is maximal, or otherwise $(x+3) \in p$ and $(5, x+3)$ is maximal. \hfill \Box

**Problem 3.** Let $\zeta \in \mathbb{C}$ be a primitive $8^{\text{th}}$ root of unity.

(a) What is the Galois group $\text{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q})$?
(b) How many subfields does $\mathbb{Q}(\zeta)$ have with $[L : \mathbb{Q}] = 2$?
(c) For each field $L$ in part (b), find an element $\alpha$ such that $\mathbb{Q}(\alpha) = L$. You may express $\alpha$ in terms of $\zeta$.

*Proof.*

(a) The Galois group is $G = (\mathbb{Z}/8\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(b) The group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ has 3 subgroups with 2 elements, namely

$$\langle (1, 0) \rangle, \langle (0, 1) \rangle, \langle (1, 1) \rangle.$$  

So there are 3 subfields $L$ with $[L : \mathbb{Q}] = 2$. Inside $(\mathbb{Z}/8\mathbb{Z})^*$, these groups are generated by $3, 5 = -3, 7 = -3$ respectively.

(c) Note that $\zeta = \frac{1}{2}\sqrt{2} + \frac{1}{2}\sqrt{2}i$ and $\zeta^{-1} = \frac{1}{2}\sqrt{2} - \frac{1}{2}\sqrt{2}i$. $i = \zeta^2$ is invariant under $\langle 5 \rangle$, $\zeta + \zeta^{-1} = \sqrt{2}$ is invariant under $\langle -1 \rangle$ and $\zeta - \zeta^{-1} = \sqrt{2}i$ is invariant under $\langle 3 \rangle$. So the three subfields are $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{2}i)$. \hfill \Box

**Problem 4.** Suppose that $S$ is a unique factorization domain, and $R$ is a subring of $S$ with the following property: if $f \in S$ and $g \in R$ such that $f$ divides $g$, then $f \in R$. Show that $R$ must also be a unique factorization domain.

*Proof.* If $f \in S^*$, then we have $f \cdot f^{-1} = 1 \in R$. It follows that $f, f^{-1} \in R$ and therefore $f \in R^*$. This proves that $R^* = S^*$.

Suppose that $f \in R$ is irreducible. Suppose that $f = f_1 f_2$ with $f_1, f_2 \in S$. Then $f_1, f_2 \in R$. So $f_1 \in R^* = S^*$ or $f_2 \in R^* = S^*$. It follows that $f$ is irreducible in $S$, because $f \notin S^* = R^*$. Suppose that

$$f_1 \cdots f_r = g_1 \cdots g_s$$

in $R$. Then $f_1, \ldots, f_r, g_1, \ldots, g_s$ are irreducible in $S$. So we have $r = s$ and, after rearranging $g_1, \ldots, g_s$ we have $f_i = \lambda_i g_i$ with $\lambda_i \in S^*$ for all $i$. From $\lambda_i \cdot \lambda_i^{-1} = 1 \in R$ follows that $\lambda_i, \lambda_i^{-1} \in R$, so $\lambda_i \in R^*$. This shows that $R$ is a UFD. \hfill \Box

**Problem 5.** Let $G$ be a group with $8 \cdot 7^m$ elements.

(a) Show that the number of 7-Sylow subgroups of $G$ is 1 or 8.
(b) Show that if $S_8$ is the symmetric group, and $\varphi : G \to S_8$ is a group homomorphism, then the image of $\varphi$ has $< 60$ elements.
(c) Show that $G$ is solvable.

*Proof.* (a) Let $n_7$ be the number of 7-Sylow subgroups. Then $n_7$ is congruent to 1 modulo 7 and a divisor of $8 = 2^3$. The only possibilities are $n_7 = 1$ and $n_7 = 8$.

(b) $|\varphi(G)|$ divides $|S_8| = 8!$ and $|G| = 8 \cdot 7^m$ and hence it divides $\gcd(8!, 8 \cdot 7^m) = 8 \cdot 7 = 56$.

(c) If there is a unique 7-Sylow subgroup $N$ of $G$, then $N$ is normal and $G/N$ and $N$ are solvable because they are $p$-groups. So $G$ is solvable. Suppose that there are 8 7-Sylow subgroups. Then $G$ acts transitively on the set of 7-Sylow subgroups and this defines a ring homomorphism $\varphi : G \to S_8$. Since the action is transitive, we have $8 \mid |\varphi(G)|$, so
\(|\ker \varphi(G)| = |G|/|\varphi(G)|\) is a power of 7. So \(\ker \varphi(G)\) is a 7-group and hence solvable. \(\varphi(G)\) has at most 56 elements by (b), so it is solvable as well. It follows that \(G\) is solvable. \qed