1. (15 points) Show that \( \phi(x) = x^4 + x^3 + x^2 + x + 1 \) is irreducible over the rationals \( \mathbb{Q} \).

**Answer:** In order to show \( \phi(x) \) is irreducible over \( \mathbb{Q} \), we show \( \phi(x+1) \) is irreducible over \( \mathbb{Q} \).

Since \( \phi(x) = x^4 + x^3 + x^2 + x + 1 \), therefore \( \phi(x) \) can be rewritten as \( \phi(x+1) = (x+1)^5 - 1 = x^4 + 5x^3 + 10x^2 + 10x + 5 \).

Applying Eisenstein’s test with \( p = 5 \), we conclude that \( \phi(x+1) \) is irreducible over \( \mathbb{Q} \) and hence \( \phi(x) = x^4 + x^3 + x^2 + x + 1 \) is irreducible over the rationals \( \mathbb{Q} \).

2. (15 points) Let \( f(x) \in F[x] \), where \( F \) is a field, and \( a \in F \). Prove that \( f(a) \) is the remainder in the division of \( f(x) \) by \( x - a \).

**Answer:** Applying division algorithm, we get \( f(x) = (x - a)q(x) + r(x) \) with \( \text{deg}(r(x)) = 0 \). Hence the remainder \( r(x) \) is a constant, say, \( k \). Thus \( f(x) = (x - a)q(x) + k \). Letting \( x = a \), we get \( k = f(a) \). Hence \( f(a) \) is the remainder in the division of \( f(x) \) by \( x - a \).

3. (15 points) Construct a finite field of order 49 and list the elements of this field.

**Answer:** Since \( 49 = 7^2 \), we start with a field \( \mathbb{Z}_7 \) of characteristic 7 and look for an irreducible polynomial of degree 2 in \( \mathbb{Z}_7[x] \). It is easy to note that \( p(x) = x^2 + x + 1 \) has no zeros in \( \mathbb{Z}_7 \).

Hence, the polynomial \( p(x) = x^2 + x + 1 \) is irreducible in \( \mathbb{Z}_7[x] \). Thus \( \mathbb{Z}_7[x]/\langle x^2 + x + 1 \rangle \) is a field with 49 elements. The elements of this field are given by \( \mathbb{Z}_7[x]/\langle x^2 + x + 1 \rangle = \{ax + b + \langle x^2 + x + 1 \rangle \mid a, b \in \mathbb{Z}_7 \} \).

4. (15 points) Let \( n \) be a positive integer. Prove that if \( R \) is a ring with unity and of characteristic \( n \), then \( R \) contains a subring isomorphic to \( \mathbb{Z}_n \). (Hint: You may use the fact \( \phi : \mathbb{Z} \rightarrow R \) defined by \( \phi(n) = n \cdot 1 \) is a ring homomorphism.)

**Answer:** Let \( S = \{k \cdot 1 \mid k \in \mathbb{Z} \} \). Define a mapping \( \phi : \mathbb{Z} \rightarrow S \) by \( \phi(n) = n \cdot 1 \) for all \( n \in \mathbb{Z} \). Then \( \phi(\mathbb{Z}) = S \). Moreover, \( \phi \) is a ring homomorphism by Theorem 15.5. The kernel of this
ring homomorphism $\phi$ is given by $Ker \phi = \{ n \in \mathbb{Z} \mid \phi(n) = 0 \} = \{ n \in \mathbb{Z} \mid n \cdot 1 = 0 \} = < n >$. Also, this shows that $n$ is the characteristics on $\mathbb{R}$. By first isomorphism theorem, we have $\mathbb{Z}/Ker \phi \simeq S$ which is $\mathbb{Z}/ < n > \simeq S$. Since $\mathbb{Z}/ < n > = \mathbb{Z}_n$ we have $\mathbb{Z}_n \simeq S$. Hence $\mathbb{R}$ contains a subring isomorphic to $\mathbb{Z}_n$.

5. (15 points) Let $\mathbb{R}$ denote the ring of real numbers and $\mathbb{C}$ denote the ring of complex numbers. Let $\psi : \mathbb{R}[x]/\langle x^2 + 1 \rangle \to \mathbb{C}$ be a function defined as $\psi(a + bx + \langle x^2 + 1 \rangle) = a + bi$, where $a, b \in \mathbb{R}$. Prove that $\psi$ is a ring isomorphism.

**Answer:** It is easy to show that $\psi$ is one-to-one and onto. Hence we only show $\psi$ is a ring homomorphism. Since

$$
\psi((a + bx + < x^2 + 1 >) + (c + dx + < x^2 + 1 >)) = \\
\psi((a + c) + (b + d)x + < x^2 + 1 >) = \\
(a + c) + (b + d)i = \\
(a + bi) + (c + di) = \\
\psi(a + bx + < x^2 + 1 >) + \psi(c + dx + < x^2 + 1 >)
$$

and

$$
\psi((a + bx + < x^2 + 1 >)(c + dx + < x^2 + 1 >)) = \\
\psi((ac - bd) + (ad + bc)x + < x^2 + 1 >) = \\
(ac - bd) + (ad + bc)i = \\
(a + bi)(c + di) = \\
\psi(a + bx + < x^2 + 1 >) \psi(c + dx + < x^2 + 1 >),
$$

the function $\psi : \mathbb{R}[x]/\langle x^2 + 1 \rangle \to \mathbb{C}$ is a ring isomorphism.

6. (15 points) Show that the number of irreducible quadratics in the field $\mathbb{Z}_p[x]$, where $p$ is a prime, is equal to $\frac{p(p-1)^2}{2}$.

**Answer:** The number of quadratic polynomials of the form $ax^2 + bx + c$ where $a, b, c \in \mathbb{Z}_p$ and $a \neq 0$ is equal to $(p - 1)(p)(p) = (p - 1)p^2$.

The number of reducible polynomials in $\mathbb{Z}_p$ is equal to the number of distinct expressions of the form $a(x + \alpha)(x + \beta)$ and $a(x + \alpha)^2$ for $\alpha, \beta \in \mathbb{Z}_p$.

In $\mathbb{Z}_p$, the number of distinct expressions of the form $(x + \alpha)(x + \beta)$ is equal to $\binom{p}{2} = \frac{(p-1)p}{2}$. Hence the number of distinct expressions of the form $a(x + \alpha)(x + \beta)$ is equal to $(p - 1)\frac{(p-1)p}{2} = \frac{(p-1)^2p}{2}$. Similarly, the number of expressions of the form $a(x + \alpha)^2$ is $(p - 1)p$. 


Therefore, and homomorphisms are: Since $\phi$ and the order of $a < p$ or $\langle p \rangle$.

Answer: Determine the order of the field $\mathbb{Z}_p$.

Find all maximal ideals of the ring $\mathbb{Z}_3 \oplus \mathbb{Z}_4$, and for each maximal ideal $M$, determine the order of the field $\mathbb{Z}_3 \oplus \mathbb{Z}_4/M$.

Answer: In $\mathbb{Z}_3$, $< 0 > = \{0\}$, and $< 1 > = \langle 2 \rangle = \mathbb{Z}_3$. Similarly, in $\mathbb{Z}_4$, $< 0 > = \{0\}$, and $< 1 > = \langle 3 \rangle = \mathbb{Z}_4$ and $< 2 > = \{0, 2\}$. A maximal ideal will be of the form $< 1 > \oplus < p >$ or $< p > \oplus < 1 >$ where $p$ is a prime number. A maximal ideal could also take the form $< 1 > \oplus < 0 >$ or $< 0 > \oplus < 1 >$ if no such prime $p$ exists. Hence the maximal ideals of $\mathbb{Z}_3 \oplus \mathbb{Z}_4$ are:

$$M_1 = < 0 > \oplus < 1 > = \{(0, 0), (0, 1), (0, 2), (0, 3)\}$$

and

$$M_2 = < 1 > \oplus < 2 > = \{(0, 0), (1, 0), (2, 0), (0, 2), (1, 2), (2, 2)\}.$$

Therefore

$$|\mathbb{Z}_3 \oplus \mathbb{Z}_4/M_1| = \frac{12}{6} = 2 \quad \text{and} \quad |\mathbb{Z}_3 \oplus \mathbb{Z}_4/M_2| = \frac{12}{4} = 3.$$

9. (15 points) Determine all ring homomorphisms from the ring $(\mathbb{Z}_{10}, +, \cdot)$ to $(\mathbb{Z}_{15}, +, \cdot)$.

Answer: We know that $\phi : \mathbb{Z}_{10} \to \mathbb{Z}_{15}$ is a homomorphism, then $\phi(x) = ax$, where $a \in \mathbb{Z}_{15}$ and the order of $a$ divide 15 and 10. That is $|a|/15$ and $|a|/10$. Therefore $|a| = 1, 5$. In $\mathbb{Z}_{15}$, the elements $a$, for which $|a| = 1, 5$ are

$$a = 0, 3, 6, 9, 12.$$

Since $\phi$ is a ring homomorphism, $a^2$ has to be equal to $a$. Thus $a = 0, 6$. Therefore, the ring homomorphisms are:

$$\phi(x) = 0x, \quad \text{and} \quad \phi(x) = 6x.$$
10. (15 points) TRUE or FALSE:

T  (a) Every field has only two ideals, one ideal is {0} and other is F.

F  (b) The polynomial \( f(x) = 2x^2 - 2 \) is irreducible in \( \mathbb{Z}[x] \).

F  (c) The sum of the elements of a finite field is equal to its unity.

F  (d) Every principal ideal domain is a field.

F  (e) If \( F \) is a field, then \( F[x] \) may not be a principal ideal domain.

F  (f) If \( F \) is a field, then \( F[x] \) is also a field.

F  (g) Every polynomial of degree 4 is irreducible in \( \mathbb{Z}_7[x] \) if it has no zeros in \( \mathbb{Z}_7 \).

T  (h) The field of complex numbers is isomorphic to \( \mathbb{R}[x]/\langle x^2 + 1 \rangle \).

T  (i) There is only one isomorphism from real field \( \mathbb{R} \) to \( \mathbb{R} \).

F  (j) The integer 7, 176, 825, 942, 116, 027, 211 is divisible by 4

T  (k) The integer 7, 176, 825, 942, 116, 027, 211 is divisible by 3

T  (l) If the multiplicative identity 1 belongs to the ideal \( A \) of a ring \( R \), then \( A = R \)

T  (m) If \( p(x) \) is an irreducible polynomial in \( F[x] \), then \( F[x]/\langle p(x) \rangle \) is a field.

F  (n) If \( \phi : \mathbb{R} \to S \) is a ring homomorphism, then First Isomorphism theorem says that \( \mathbb{R}/\text{Ker}\phi \simeq S \).

T  (o) The set of all nilpotent elements of a ring is called the nil radical.