Question 1: (i) Find all the units of $Z_7[x]$. (ii) Check whether Q ⊕ Q is an integral domain or not. (iii) Give an example of a subring S of a ring R which is not an ideal of R. (iv) Prove that a ring homomorphism carries an idempotent to an idempotent. (v) Let ϕ be a ring homomorphism from a ring R to a ring S. If R has unity 1, S ≠ {0} and ϕ is onto then prove that ϕ(1) is the unity of S. (vi) Let $f(x) = 2x^5 + 14x^2 - 21x + 7$. Is f(x) an irreducible polynomial over Q? Justify your answer. (vii) Let D be an integral domain. Suppose that p, q ∈ D and q ≠ 0. Show that if p is not a unit, then $\langle p \rangle$ is a proper subset of $\langle q \rangle$. (viii) Explain why $3x^2 + 6$ is reducible over Z.

(i) The **units of $Z_7[x]$** are the constant polynomials corresponding to the units of Z_7. Since 7 is a prime number, every non-zero element in Z_7 is a unit. Therefore, the units of $Z_7[x]$ are **{1, 2, 3, 4, 5, 6}**.

(ii) **Q ⊕ Q is not an integral domain**.

- An integral domain is a commutative ring with unity and no zero divisors.
- While Q ⊕ Q is a commutative ring with unity (1,1), it has zero divisors.
- For example, consider the non-zero elements (1, 0) and (0, 1) in Q ⊕ Q. Their product is (1, 0) * (0, 1) = (0, 0), which is the zero element. Since non-zero elements multiply to zero, Q ⊕ Q is not an integral domain.

(iii) An example of a **subring S of a ring R which is not an ideal of R** is:

- Let R be the ring of real numbers, $\mathbb{R}$.
- Let S be the set of integers, $\mathbb{Z}$.
- $\mathbb{Z}$ is a subring of $\mathbb{R}$ because it is closed under subtraction and multiplication, and contains 0.

- However, $\mathbb{Z}$ is not an ideal of $\mathbb{R}$. For instance, take $r = \frac{1}{2} \in \mathbb{R}$ and $s = 3 \in \mathbb{Z}$. Their product $r \cdot s = \frac{1}{2} \cdot 3 = \frac{3}{2}$ is not an integer, so it is not in $\mathbb{Z}$. This violates the ideal property.

(iv) To prove that a **ring homomorphism carries an idempotent to an idempotent**:

- Let $\phi: R \to S$ be a ring homomorphism.
- Let $e \in R$ be an idempotent element, meaning $e^2 = e$.
- We need to show that $\phi(e)$ is an idempotent in S, i.e., $(\phi(e))^2 = \phi(e)$.
- Since ϕ is a ring homomorphism, it preserves multiplication: $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in R$.
- Therefore, $(\phi(e))^2 = \phi(e)\phi(e) = \phi(e \cdot e)$.
- Because e is an idempotent, $e \cdot e = e$.
- So, $\phi(e \cdot e) = \phi(e)$.
- Thus, $(\phi(e))^2 = \phi(e)$, proving that $\phi(e)$ is an idempotent in S.

(v) To prove that $\phi(1)$ **is the unity of S** when ϕ is an onto ring homomorphism from R with unity 1 to S ≠ {0}:

- Let 1 be the unity of R, so $a \cdot 1 = 1 \cdot a = a$ for all $a \in R$.
- We want to show that $\phi(1)$ is the unity of S. This means for any $s \in S$, $s \cdot \phi(1) = \phi(1) \cdot s = s$.
- Since ϕ is onto, for any $s \in S$, there exists an $a \in R$ such that $\phi(a) = s$.
- Consider the product $s \cdot \phi(1)$:
  - $s \cdot \phi(1) = \phi(a) \cdot \phi(1)$ (since $s = \phi(a)$)

- $= \phi(a \cdot 1)$ (since ϕ is a homomorphism)
- $= \phi(a)$ (since 1 is the unity in R)
- $= s$.

- Similarly, consider the product $\phi(1) \cdot s$:
  - $\phi(1) \cdot s = \phi(1) \cdot \phi(a)$
  - $= \phi(1 \cdot a)$
  - $= \phi(a)$
  - $= s$.
- Since $s \cdot \phi(1) = \phi(1) \cdot s = s$ for all $s \in S$, $\phi(1)$ is the unity of S.

(vi) **Yes, $f(x) = 2x^5 + 14x^2 - 21x + 7$ is an irreducible polynomial over Q**.

- We can use **Eisenstein's Criterion**. For $f(x) = 2x^5 + 0x^4 + 0x^3 + 14x^2 - 21x + 7$, let's consider the prime $p = 7$.
  - i. p divides all coefficients except the leading coefficient: 7 divides 14, -21, and 7.
  - ii. p does not divide the leading coefficient: 7 does not divide 2.
  - iii. p^2 does not divide the constant term: $7^2 = 49$ does not divide 7.
- Since all conditions of Eisenstein's Criterion are met for $p = 7$, f(x) is irreducible over Q.

(vii) The statement as written, "Let D be an integral domain. Suppose that p, q ∈ D and q ≠ 0. Show that if p is not a unit, then $\langle p \rangle$ is a proper subset of $\langle q \rangle$", is **not universally true**.

- For example, in the integral domain $\mathbb{Z}$, let $p = 2$ (not a unit) and $q = 3$ (not a unit).
- $\langle 2 \rangle = \{\dots, -4, -2, 0, 2, 4, \dots\}$ (even integers).
- $\langle 3 \rangle = \{\dots, -6, -3, 0, 3, 6, \dots\}$ (multiples of 3).
- Neither $\langle 2 \rangle \subset \langle 3 \rangle$ nor $\langle 3 \rangle \subset \langle 2 \rangle$.
- The statement would be true if, for instance, q were a unit. If q is a unit, then $\langle q \rangle = D$. If p is not a unit, then $\langle p \rangle \neq D$. In this specific case, $\langle p \rangle$ would be a proper subset of $\langle q \rangle = D$. However, this condition on q is not given in the original question.

(viii) **3x² + 6 is reducible over Z** because it is not a primitive polynomial.

- A polynomial $f(x) \in \mathbb{Z}[x]$ is reducible over $\mathbb{Z}$ if it can be factored into a product of two non-constant polynomials with integer coefficients, or if its coefficients have a common divisor greater than 1 (i.e., it's not primitive).
- For $f(x) = 3x^2 + 6$, the coefficients (3 and 6) have a common divisor of 3 (which is greater than 1).
- We can factor it as $3(x^2 + 2)$.
- According to the definition of reducibility over $\mathbb{Z}$ (which requires a polynomial to be primitive to be considered irreducible), if the content (gcd of coefficients) is greater than 1, the polynomial is considered reducible.
- Since the content of $3x^2 + 6$ is 3, it is reducible over $\mathbb{Z}$.

Question 2: (a) Prove that intersection of two subrings in a ring R is a subring of R. Is the union of two subrings necessarily a subring of R? Justify your answer. (b) Find all the units, zero divisors and idempotent elements in $Z_3 \oplus Z_6$. (c) Prove that Z_n, the ring of integers modulo n, is a field if and only if n is a prime.

(a)

- **Proof that the intersection of two subrings in a ring R is a subring of R**:
  - Let S_1 and S_2 be two subrings of a ring R. We want to show that $S_1 \cap S_2$ is a subring.
  -
    i. **Non-empty**: Since S_1 and S_2 are subrings, they both contain the additive identity 0 of R. Thus, $0 \in S_1 \cap S_2$, so the intersection is non-empty.
  -
    ii. **Closure under subtraction**: Let $a, b \in S_1 \cap S_2$. This means $a, b \in S_1$ and $a, b \in S_2$. Since S_1 is a subring, $a - b \in S_1$. Since S_2 is a subring, $a - b \in S_2$. Therefore, $a - b \in S_1 \cap S_2$.
  -
    iii. **Closure under multiplication**: Let $a, b \in S_1 \cap S_2$. This means $a, b \in S_1$ and $a, b \in S_2$. Since S_1 is a subring, $a \cdot b \in S_1$. Since S_2 is a subring, $a \cdot b \in S_2$. Therefore, $a \cdot b \in S_1 \cap S_2$.
  - Since all conditions are satisfied, $S_1 \cap S_2$ is a subring of R.
- **Is the union of two subrings necessarily a subring of R? No, the union of two subrings is not necessarily a subring of R.**
  - **Justification**: Consider the ring $\mathbb{Z}_6$.

- Let $S_1 = \{0,2,4\}$ be a subring of $\mathbb{Z}_6$.
- Let $S_2 = \{0,3\}$ be a subring of $\mathbb{Z}_6$.
- The union is $S_1 \cup S_2 = \{0,2,3,4\}$.
- For $S_1 \cup S_2$ to be a subring, it must be closed under addition.
- Consider $2 \in S_1 \cup S_2$ and $3 \in S_1 \cup S_2$.
- Their sum is $2 + 3 = 5 \pmod 6$.
- However, $5 \notin S_1 \cup S_2$.
- Thus, $S_1 \cup S_2$ is not closed under addition, and therefore it is not a subring of $\mathbb{Z}_6$.

(b) To find all the **units, zero divisors, and idempotent elements in $\mathbf{Z_3 \oplus Z_6}$**:

- **Units**: An element $(a, b) \in \mathbb{Z}_3 \oplus \mathbb{Z}_6$ is a unit if and only if a is a unit in $\mathbb{Z}_3$ and b is a unit in $\mathbb{Z}_6$.
  - Units in $\mathbb{Z}_3$: $\{1,2\}$
  - Units in $\mathbb{Z}_6$: $\{1,5\}$ (elements coprime to 6)
  - The units in $\mathbb{Z}_3 \oplus \mathbb{Z}_6$ are: **(1, 1), (1, 5), (2, 1), (2, 5)**. There are $2 \times 2 = 4$ units.
- **Zero Divisors**: An element $(a, b) \in \mathbb{Z}_3 \oplus \mathbb{Z}_6$ is a zero divisor if $(a, b) \neq (0,0)$ and $(a, b)(c, d) = (0,0)$ for some $(c, d) \neq (0,0)$. This occurs if $a = 0$ and b is a zero divisor in $\mathbb{Z}_6$, or if $b = 0$ and a is a zero divisor in $\mathbb{Z}_3$, or if $a \neq 0$ and b is a zero divisor in $\mathbb{Z}_6$, or if $b \neq 0$ and a is a zero divisor in $\mathbb{Z}_3$.
  - $\mathbb{Z}_3$ is a field, so it has no non-zero zero divisors.
  - Zero divisors in $\mathbb{Z}_6$: $\{2,3,4\}$.
  - The zero divisors in $\mathbb{Z}_3 \oplus \mathbb{Z}_6$ are:

        - Elements where $a = 0$ and b is a non-unit and $b \neq 0$: (0, 2), (0, 3), (0, 4).
        - Elements where $a \neq 0$ and b is a zero divisor in $\mathbb{Z}_6$: (1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4).
    - The zero divisors are: **(0, 2), (0, 3), (0, 4), (1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4)**. There are $3 + 6 = 9$ zero divisors.
- **Idempotent Elements**: An element $(a, b) \in \mathbb{Z}_3 \oplus \mathbb{Z}_6$ is idempotent if $(a, b)^2 = (a, b)$, which means $a^2 = a$ in $\mathbb{Z}_3$ and $b^2 = b$ in $\mathbb{Z}_6$.
    - Idempotents in $\mathbb{Z}_3$: $0^2 = 0$, $1^2 = 1$, $2^2 = 4 \equiv 1 \pmod 3$. So, $\{0,1\}$.
    - Idempotents in $\mathbb{Z}_6$: $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 9 \equiv 3 \pmod 6$, $4^2 = 16 \equiv 4 \pmod 6$, $5^2 = 25 \equiv 1 \pmod 6$. So, $\{0,1,3,4\}$.
    - The idempotent elements in $\mathbb{Z}_3 \oplus \mathbb{Z}_6$ are:
        - (0, 0), (0, 1), (0, 3), (0, 4)
        - (1, 0), (1, 1), (1, 3), (1, 4)
    - There are $2 \times 4 = 8$ idempotent elements.

(c) To prove that $\mathbb{Z}_n$**, the ring of integers modulo n, is a field if and only if n is a prime**:

- **Part 1: If n is prime, then $\mathbb{Z}_n$ is a field.**
    - Assume n is a prime number. $\mathbb{Z}_n$ is a commutative ring with unity [1].
    - To show it's a field, we must show every non-zero element has a multiplicative inverse.
    - Let $[a]$ be a non-zero element in $\mathbb{Z}_n$, so $a \in \{1,2,\ldots,n-1\}$.
    - Since n is prime and a is between 1 and $n - 1$, gcd$(a, n) = 1$.

- By Bezout's identity, there exist integers x and y such that $ax + ny = 1$.
- Taking this equation modulo n, we get $ax \equiv 1 \pmod{n}$.
- This means $[x]$ is the multiplicative inverse of $[a]$ in $\mathbb{Z}_n$.
- Since every non-zero element has an inverse, $\mathbb{Z}_n$ is a field.

- **Part 2: If $\mathbb{Z}_n$ is a field, then n is prime.**
  - Assume $\mathbb{Z}_n$ is a field. A field has no non-zero zero divisors.
  - Suppose, for contradiction, that n is a composite number.
  - Then n can be written as $n = ab$ for some integers a and b where $1 < a < n$ and $1 < b < n$.
  - Consider the elements $[a]$ and $[b]$ in $\mathbb{Z}_n$. Since $1 < a < n$ and $1 < b < n$, neither $[a]$ nor $[b]$ is the zero element $[0]$ in $\mathbb{Z}_n$.
  - However, their product $[a][b] = [ab] = [n] = [0]$ in $\mathbb{Z}_n$.
  - This implies that $[a]$ and $[b]$ are non-zero zero divisors in $\mathbb{Z}_n$, which contradicts the fact that $\mathbb{Z}_n$ is a field.
  - Therefore, our assumption that n is composite must be false. Hence, n must be a prime number.
- From both parts, $\mathbb{Z}_n$ is a field if and only if n is a prime.

Question 3: (a) Let R be a commutative ring with unity and let U(R) denote the set of units of R. Prove that U(R) is a group under multiplication. Also, find U(Z[i]). (b) Define the characteristic of a ring. Prove that the characteristic of an integral domain is either 0 or prime. (c) Prove that in a commutative ring R with unity, an ideal A is a maximal ideal if and only if R/A is a field.

(a)

- **Proof that U(R) is a group under multiplication**:
  - Let U(R) be the set of units in a commutative ring R with unity 1.
  -
    i. **Closure**: Let $a, b \in U(R)$. This means $a^{-1}, b^{-1} \in R$. Consider the product ab. We need to show $ab \in U(R)$. $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a(1)a^{-1} = aa^{-1} = 1$. Similarly, $(b^{-1}a^{-1})(ab) = 1$. So, $(ab)^{-1} = b^{-1}a^{-1}$ exists in R, and thus $ab \in U(R)$.
  -
    ii. **Associativity**: Multiplication in R is associative, and U(R) is a subset of R, so multiplication is associative in U(R).
  -
    iii. **Identity Element**: Since R has unity 1, and $1 \cdot 1 = 1$, 1 has an inverse (itself). Thus, $1 \in U(R)$.
  -
    iv. **Inverse Element**: By definition, every element $a \in U(R)$ has a multiplicative inverse $a^{-1} \in R$. We need to show $a^{-1} \in U(R)$. Since $a^{-1} \cdot a = 1$ and $a \cdot a^{-1} = 1$, a^{-1} has an inverse (which is a). Thus, $a^{-1} \in U(R)$.
  - Therefore, U(R) is a group under multiplication.
- **Finding U(Z[i])**:
  - Z[i] is the ring of Gaussian integers, $\{a + bi \mid a, b \in \mathbb{Z}\}$.
  - An element $z = a + bi$ is a unit in Z[i] if there exists $w = c + di \in \mathbb{Z}[i]$ such that $zw = 1$.
  - Taking the norm of both sides: $N(zw) = N(1) \Rightarrow N(z)N(w) = 1$.

- The norm $N(a + bi) = a^2 + b^2$. Since a, b, c, d are integers, $a^2 + b^2$ and $c^2 + d^2$ are non-negative integers.
- For their product to be 1, both must be 1. So, $a^2 + b^2 = 1$.
- Integer solutions for $a^2 + b^2 = 1$ are:
  - If $a = \pm 1$, then $b = 0$, giving units 1 and -1.
  - If $a = 0$, then $b = \pm 1$, giving units i and $-i$.
- Thus, **U(Z[i]) = {1, -1, i, -i}**.

(b)

- **Definition of the Characteristic of a Ring**:
  - The **characteristic of a ring R**, denoted as char(R), is the smallest positive integer n such that $n \cdot x = 0$ for all $x \in R$ (where $n \cdot x$ means x added to itself n times).
  - If no such positive integer exists, the characteristic is defined to be 0.
- **Proof that the characteristic of an integral domain is either 0 or prime**:
  - Let D be an integral domain.
  - **Case 1: char(D) = 0**. If no such positive integer n exists, the characteristic is 0 by definition. This satisfies the condition.
  - **Case 2: char(D) = n > 0**.
    - Since D is an integral domain, it has a unity element 1.
    - By definition of characteristic, $n \cdot 1 = 0$.
    - Assume, for contradiction, that n is composite. So $n = ab$ for some integers a, b where $1 < a < n$ and $1 < b < n$.

- Then $n \cdot 1 = (ab) \cdot 1 = 0$. This can be rewritten as $(a \cdot 1)(b \cdot 1) = 0$.
- Since D is an integral domain, it has no zero divisors. Thus, if $(a \cdot 1)(b \cdot 1) = 0$, then either $a \cdot 1 = 0$ or $b \cdot 1 = 0$.
- If $a \cdot 1 = 0$, then a must be a multiple of the characteristic n. But $1 < a < n$, which is a contradiction.
- If $b \cdot 1 = 0$, then b must be a multiple of the characteristic n. But $1 < b < n$, which is also a contradiction.
- Since assuming n is composite leads to a contradiction, n must be a prime number.

- Therefore, the characteristic of an integral domain is either 0 or a prime number.

(c) To prove that **in a commutative ring R with unity, an ideal A is a maximal ideal if and only if R/A is a field**:

- **Part 1: If A is a maximal ideal, then R/A is a field.**
  - Assume A is a maximal ideal in a commutative ring R with unity.
  - Since A is maximal, it is a proper ideal, so $A \neq R$, which means R/A is not the zero ring and contains unity $1 + A$.
  - R/A is a commutative ring with unity. To show it's a field, we need every non-zero element to have a multiplicative inverse.
  - Let $x + A$ be a non-zero element in R/A, meaning $x \notin A$.
  - Consider the ideal $J = A + \langle x \rangle = \{a + rx \mid a \in A, r \in R\}$.
  - Since $x \notin A$, A is strictly contained in J ($A \subsetneq J$).
  - As A is maximal, and J is an ideal containing A, it must be that $J = R$.

- Since $1 \in R$, we have $1 \in J$, so $1 = a + rx$ for some $a \in A$ and $r \in R$.
- In R/A, this equation becomes $1 + A = (a + rx) + A$.
- Since $a \in A$, $a + A = 0 + A$.
- So, $1 + A = rx + A = (r + A)(x + A)$.
- This shows that $(r + A)$ is the multiplicative inverse of $(x + A)$.
- Thus, every non-zero element in R/A has an inverse, so R/A is a field.

- **Part 2: If R/A is a field, then A is a maximal ideal.**
  - Assume R/A is a field.
  - Since R/A is a field, it is not the zero ring, so $A \neq R$, meaning A is a proper ideal.
  - Let B be an ideal of R such that $A \subseteq B \subseteq R$. We want to show that either $B = A$ or $B = R$.
  - If $A = B$, we are done.
  - Assume $A \subsetneq B$. This means there exists an element $b \in B$ such that $b \notin A$.
  - Consider the element $b + A \in R/A$. Since $b \notin A$, $b + A$ is a non-zero element in R/A.
  - Since R/A is a field, $b + A$ must have a multiplicative inverse, say $r + A$, for some $r \in R$.
  - So, $(b + A)(r + A) = 1 + A$. This means $br + A = 1 + A$, which implies $1 - br \in A$.
  - Since $b \in B$ and $r \in R$, and B is an ideal, $br \in B$.
  - Since $1 - br \in A$ and $A \subseteq B$, we have $1 - br \in B$.

- Now, since $br \in B$ and $1 - br \in B$, their sum $(br) + (1 - br) = 1$ must be in B.
- Since $1 \in B$ and B is an ideal, for any $x \in R$, $x \cdot 1 = x \in B$.
- Thus, $R \subseteq B$. Since $B \subseteq R$, we have $B = R$.
- Therefore, A is a maximal ideal.

Question 4: (a) Prove that the ideal $\langle x \rangle$ is a prime ideal in Z[x] but not a maximal ideal in Z[x]. (b) Let ϕ be a ring homomorphism from a ring R onto a ring S. Prove that R/Ker ϕ ≈ S. (c) Determine all ring homomorphisms from $Z_4 \rightarrow Z_{10}$. (b) Let $f(x) = 5x^4 + 3x^3 + 1$ and $g(x) = 3x^2 + 2x + 1 \in Z_7[x]$. Determine the quotient and remainder obtained when f(x) is divided by g(x). (c) Prove that the product of two primitive polynomials is a primitive polynomial.

(a) To prove that the **ideal $\langle x \rangle$ is a prime ideal in Z[x] but not a maximal ideal in Z[x]**:

- **$\langle x \rangle$ is a prime ideal**:
  - An ideal P is prime if and only if the quotient ring R/P is an integral domain.
  - Consider the evaluation homomorphism $\psi: \mathbb{Z}[x] \rightarrow \mathbb{Z}$ defined by $\psi(f(x)) = f(0)$.
  - The kernel of this homomorphism is Ker$(\psi) = \{f(x) \in \mathbb{Z}[x] \mid f(0) = 0\}$, which is precisely the set of polynomials whose constant term is 0. These are exactly the multiples of x, so Ker$(\psi) = \langle x \rangle$.
  - By the First Isomorphism Theorem for Rings, $\mathbb{Z}[x]/$Ker$(\psi) \cong$ Im(ψ).
  - The image of ψ is all of $\mathbb{Z}$ (since for any integer k, the constant polynomial $f(x) = k$ maps to k).

- So, $\mathbb{Z}[x]/\langle x\rangle \cong \mathbb{Z}$.
- Since $\mathbb{Z}$ is an integral domain (it's a commutative ring with unity and no zero divisors), it follows that $\langle x\rangle$ is a prime ideal in $\mathbb{Z}[x]$.

- $\langle x\rangle$ **is not a maximal ideal**:
  - An ideal M is maximal if and only if the quotient ring R/M is a field.
  - From the previous point, we know that $\mathbb{Z}[x]/\langle x\rangle \cong \mathbb{Z}$.
  - However, $\mathbb{Z}$ is not a field (e.g., 2 has no multiplicative inverse in $\mathbb{Z}$).
  - Therefore, $\langle x\rangle$ is not a maximal ideal in $\mathbb{Z}[x]$.
  - Alternatively, to show it's not maximal, we can find an ideal I such that $\langle x\rangle \subsetneq I \subsetneq \mathbb{Z}[x]$.
  - Consider the ideal $I = \langle x, 2\rangle$. This ideal consists of all polynomials in $\mathbb{Z}[x]$ whose constant term is an even integer.
  - Clearly, $\langle x\rangle \subsetneq \langle x, 2\rangle$ (e.g., $2 \in \langle x, 2\rangle$ but $2 \notin \langle x\rangle$).
  - Also, $\langle x, 2\rangle \subsetneq \mathbb{Z}[x]$ (e.g., $1 \in \mathbb{Z}[x]$ but $1 \notin \langle x, 2\rangle$).
  - Since we found such an ideal I, $\langle x\rangle$ is not a maximal ideal.

(b) To prove that **R/Ker ϕ ≅ S** for a ring homomorphism ϕ from R onto S:

- This is the **First Isomorphism Theorem for Rings**.
- Let $\phi: R \to S$ be an onto ring homomorphism.
- Let $\text{Ker}(\phi) = \{r \in R \mid \phi(r) = 0_S\}$ be the kernel of ϕ. We know $\text{Ker}(\phi)$ is an ideal of R.
- Define a map $\bar{\phi}: R/\text{Ker}(\phi) \to S$ by $\bar{\phi}(r + \text{Ker}(\phi)) = \phi(r)$.
  -

i. **Well-defined**: If $r + \text{Ker}(\phi) = r' + \text{Ker}(\phi)$, then $r - r' \in \text{Ker}(\phi)$. Thus $\phi(r - r') = 0_S$. Since ϕ is a homomorphism, $\phi(r) - \phi(r') = 0_S$, which means $\phi(r) = \phi(r')$. So $\bar{\phi}(r + \text{Ker}(\phi)) = \bar{\phi}(r' + \text{Ker}(\phi))$, making it well-defined.

○

ii. **Homomorphism**:

- $\bar{\phi}((r + \text{Ker}(\phi)) + (r' + \text{Ker}(\phi))) = \bar{\phi}((r + r') + \text{Ker}(\phi)) = \phi(r + r') = \phi(r) + \phi(r') = \bar{\phi}(r + \text{Ker}(\phi)) + \bar{\phi}(r' + \text{Ker}(\phi))$. (Preserves addition)
- $\bar{\phi}((r + \text{Ker}(\phi))(r' + \text{Ker}(\phi))) = \bar{\phi}(rr' + \text{Ker}(\phi)) = \phi(rr') = \phi(r)\phi(r') = \bar{\phi}(r + \text{Ker}(\phi))\bar{\phi}(r' + \text{Ker}(\phi))$. (Preserves multiplication)

○

iii. **Injective (One-to-one)**: Suppose $\bar{\phi}(r + \text{Ker}(\phi)) = 0_S$. By definition, $\phi(r) = 0_S$. This means $r \in \text{Ker}(\phi)$. If $r \in \text{Ker}(\phi)$, then $r + \text{Ker}(\phi) = 0 + \text{Ker}(\phi)$, the zero element in $R/\text{Ker}(\phi)$. Thus, $\bar{\phi}$ is injective.

○

iv. **Surjective (Onto)**: Since $\phi: R \to S$ is onto, for any $s \in S$, there exists an $r \in R$ such that $\phi(r) = s$. Then, $\bar{\phi}(r + \text{Ker}(\phi)) = \phi(r) = s$. So $\bar{\phi}$ is surjective.

- Since $\bar{\phi}$ is a well-defined, injective, and surjective ring homomorphism, it is an isomorphism. Therefore, $R/\text{Ker}(\phi) \cong S$.

(c) To determine all **ring homomorphisms from $\mathbf{Z_4} \to \mathbf{Z_{10}}$**:

- Let $\phi: \mathbb{Z}_4 \to \mathbb{Z}_{10}$ be a ring homomorphism.

- A ring homomorphism must map the additive identity to the additive identity, so $\phi(0) = 0$.
- It must also map the unity of the domain to an idempotent element in the codomain. Let $\phi(1) = e$. Then $e^2 = e$ in $\mathbb{Z}_{10}$.
- The idempotent elements in $\mathbb{Z}_{10}$ are: $0,1,5,6$.
- Additionally, in $\mathbb{Z}_4$, we know $4 \cdot 1 = 0$. Applying the homomorphism:
    - $\phi(4 \cdot 1) = \phi(0) = 0$.
    - Also, $\phi(4 \cdot 1) = 4 \cdot \phi(1) = 4e$.
    - So, $4e \equiv 0 \pmod{10}$.
- Let's check each possible idempotent e:
    - i. If $e = 0$: $4 \cdot 0 = 0 \pmod{10}$. This is valid. In this case, $\phi(k) = k \cdot \phi(1) = k \cdot 0 = 0$ for all $k \in \mathbb{Z}_4$. This is the **trivial homomorphism**.
    - ii. If $e = 1$: $4 \cdot 1 = 4 \pmod{10}$. Since $4 \neq 0$, this is not a valid homomorphism.
    - iii. If $e = 5$: $4 \cdot 5 = 20 \pmod{10}$. Since $20 \equiv 0$, this is valid. In this case, $\phi(k) = k \cdot \phi(1) = 5k \pmod{10}$.
        - $\phi(0) = 0$
        - $\phi(1) = 5$
        - $\phi(2) = 10 \equiv 0$
        - $\phi(3) = 15 \equiv 5$ This is a **valid homomorphism**.

-
    iv. If $e = 6$: $4 \cdot 6 = 24 \pmod{10}$. Since $24 \equiv 4 \neq 0$, this is not a valid homomorphism.

- Therefore, there are **two ring homomorphisms** from $\mathbb{Z}_4$ to $\mathbb{Z}_{10}$:
  - i. $\phi_1(k) = 0$ for all $k \in \mathbb{Z}_4$.
  - ii. $\phi_2(k) = 5k \pmod{10}$ for all $k \in \mathbb{Z}_4$.

(b) To determine the **quotient and remainder obtained when f(x) = $5x^4$ + $3x^3$ + 1 is divided by g(x) = $3x^2$ + 2x + 1 in Z_7[x]**:

- We perform polynomial long division in $\mathbb{Z}_7[x]$. First, find the inverse of the leading coefficient of $g(x)$, which is $3^{-1} \pmod 7$. Since $3 \cdot 5 = 15 \equiv 1 \pmod 7$, $3^{-1} = 5$.
- **Step 1**: Divide $5x^4$ by $3x^2$. The coefficient is $5 \cdot 3^{-1} = 5 \cdot 5 = 25 \equiv 4 \pmod 7$. So the first term of the quotient is $4x^2$.
  - $4x^2(3x^2 + 2x + 1) = 12x^4 + 8x^3 + 4x^2 \equiv 5x^4 + x^3 + 4x^2 \pmod 7$.
  - Subtract this from $f(x)$: $(5x^4 + 3x^3 + 0x^2 + 0x + 1) - (5x^4 + x^3 + 4x^2) = (3-1)x^3 + (0-4)x^2 + 0x + 1 = 2x^3 - 4x^2 + 1 \equiv 2x^3 + 3x^2 + 1 \pmod 7$.
- **Step 2**: Divide $2x^3$ by $3x^2$. The coefficient is $2 \cdot 3^{-1} = 2 \cdot 5 = 10 \equiv 3 \pmod 7$. So the next term of the quotient is $3x$.
  - $3x(3x^2 + 2x + 1) = 9x^3 + 6x^2 + 3x \equiv 2x^3 + 6x^2 + 3x \pmod 7$.
  - Subtract this from the current remainder: $(2x^3 + 3x^2 + 0x + 1) - (2x^3 + 6x^2 + 3x) = (3-6)x^2 + (0-3)x + 1 = -3x^2 - 3x + 1 \equiv 4x^2 + 4x + 1 \pmod 7$.

- **Step 3**: Divide $4x^2$ by $3x^2$. The coefficient is $4 \cdot 3^{-1} = 4 \cdot 5 = 20 \equiv 6 \pmod 7$. So the next term of the quotient is 6.
  - $6(3x^2 + 2x + 1) = 18x^2 + 12x + 6 \equiv 4x^2 + 5x + 6 \pmod 7$.
  - Subtract this from the current remainder: $(4x^2 + 4x + 1) - (4x^2 + 5x + 6) = (4 - 5)x + (1 - 6) = -x - 5 \equiv 6x + 2 \pmod 7$.
- The degree of the remainder (6x + 2) is 1, which is less than the degree of the divisor $g(x)$ (which is 2).
- Therefore, the **quotient is** $q(x) = 4x^2 + 3x + 6$ and the **remainder is** $r(x) = 6x + 2$.

(c) To prove that the **product of two primitive polynomials is a primitive polynomial**:

- **Definition**: A polynomial $f(x) \in \mathbb{Z}[x]$ is primitive if the greatest common divisor of its coefficients is 1.
- **Proof**: Let $f(x)$ and $g(x)$ be two primitive polynomials in $\mathbb{Z}[x]$.
- Assume, for contradiction, that their product $h(x) = f(x)g(x)$ is not primitive.
- If $h(x)$ is not primitive, then there exists a prime number p that divides all coefficients of $h(x)$.
- Consider the homomorphism $\phi_p: \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ which reduces coefficients modulo p.
- Since p divides all coefficients of $h(x)$, $\phi_p(h(x)) = \bar{h}(x) = \bar{0}$ (the zero polynomial in $\mathbb{Z}_p[x]$).
- Since ϕ_p is a homomorphism, $\phi_p(f(x)g(x)) = \phi_p(f(x))\phi_p(g(x))$.
- So, $\bar{f}(x)\bar{g}(x) = \bar{h}(x) = \bar{0}$.

- Since p is prime, $\mathbb{Z}_p$ is a field. Consequently, $\mathbb{Z}_p[x]$ is an integral domain (polynomial ring over a field).
- In an integral domain, if a product is zero, at least one of the factors must be zero. Thus, either $\bar{f}(x) = \bar{0}$ or $\bar{g}(x) = \bar{0}$.
- If $\bar{f}(x) = \bar{0}$, it means all coefficients of $f(x)$ are divisible by p. This contradicts the assumption that $f(x)$ is primitive.
- Similarly, if $\bar{g}(x) = \bar{0}$, it means all coefficients of $g(x)$ are divisible by p. This contradicts the assumption that $g(x)$ is primitive.
- Since both possibilities lead to a contradiction, our initial assumption that $h(x)$ is not primitive must be false.
- Therefore, the product of two primitive polynomials is a primitive polynomial (this is known as Gauss's Lemma).

Question 5: (a) Let F be a field and let I = {$a_0 + a_1x + ... + a_nx^n$: $a_0, a_1, ..., a_n \in F$ and $a_0 + a_1 + ... + a_n = 0$}. Show that I is an ideal of F[x] and find a generator for I.

(a) To show that **I is an ideal of F[x] and find a generator for I**:

- **Showing I is an ideal**:
  - Consider the evaluation homomorphism $\phi: F[x] \to F$ defined by $\phi(p(x)) = p(1)$. This map sends a polynomial to the sum of its coefficients (when coefficients are treated as elements in F).
  - The set I is precisely the set of polynomials $p(x) \in F[x]$ such that $p(1) = 0$.
  - Therefore, I is the **kernel of the homomorphism** ϕ, i.e., $I =$ Ker(ϕ).
  - Since the kernel of any ring homomorphism is an ideal, I is an ideal of $F[x]$.

- **Finding a generator for I**:
  - By the **Factor Theorem**, if $p(1) = 0$, then $(x - 1)$ is a factor of $p(x)$.
  - Since F is a field, $F[x]$ is a Principal Ideal Domain (PID), meaning every ideal can be generated by a single element.
  - The polynomials in I are exactly those divisible by $(x - 1)$.
  - The polynomial $(x - 1)$ itself is in I, since its coefficients sum to $1 + (-1) = 0$.
  - Therefore, the ideal I is generated by $(\mathbf{x - 1})$. So, $I = \langle x - 1 \rangle$.

Question 6: (a) Show that p(x) = $x^3 + x + 1$ is an irreducible polynomial over Z_2. Let M = <$x^3 + x + 1$> be an ideal of $Z_2[x]$. Show that F = $Z_2[x]$ / M is a field of order 8. Exhibit all the 8 elements of F. Find the product of $x^2 + x + 1$ + M and $x^2 + 1$ + M and express it as a member of F. (b) In a principal ideal domain, prove that the element is irreducible if and only if it is prime. (c) Show that integral domain Z[t] is Euclidean Domain. Is Z[i] a Unique Factorization Domain? Justify.

(a)

- **Show that p(x) = $x^3 + x + 1$ is an irreducible polynomial over Z_2**:
  - A polynomial of degree 3 is irreducible over a field if and only if it has no roots in that field.
  - The elements of $\mathbb{Z}_2$ are 0 and 1.
  - $p(0) = 0^3 + 0 + 1 = 1 \pmod 2 \neq 0$.
  - $p(1) = 1^3 + 1 + 1 = 3 \equiv 1 \pmod 2 \neq 0$.
  - Since $p(x)$ has no roots in $\mathbb{Z}_2$, and its degree is 3, it is irreducible over $\mathbb{Z}_2$.

- **Show that F = Z_2[x] / M is a field of order 8**:
  - For a field F and an ideal $M = \langle p(x) \rangle$ where $p(x) \in F[x]$, the quotient ring $F[x]/M$ is a field if and only if $p(x)$ is an irreducible polynomial over F.
  - Since $p(x) = x^3 + x + 1$ is irreducible over $\mathbb{Z}_2$, $F = \mathbb{Z}_2[x]/\langle x^3 + x + 1 \rangle$ is a field.
  - The elements of this field are polynomials modulo $p(x)$, meaning they are represented by polynomials with degree less than deg$(p(x)) = 3$.
  - These elements are of the form $a_2x^2 + a_1x + a_0$, where $a_0, a_1, a_2 \in \mathbb{Z}_2 = \{0,1\}$.
  - There are $2 \times 2 \times 2 = 2^3 = 8$ possible combinations for the coefficients.
  - Thus, F is a field of order 8.
- **Exhibit all the 8 elements of F**:
  - The elements are of the form $a_2x^2 + a_1x + a_0 + M$:
    - $0 + M$
    - $1 + M$
    - $x + M$
    - $x + 1 + M$
    - $x^2 + M$
    - $x^2 + 1 + M$
    - $x^2 + x + M$
    - $x^2 + x + 1 + M$

- **Find the product of $x^2 + x + 1 + M$ and $x^2 + 1 + M$ and express it as a member of F**:
    - Let $A = x^2 + x + 1 + M$ and $B = x^2 + 1 + M$.
    - First, multiply the polynomials $(x^2 + x + 1)$ and $(x^2 + 1)$ in $\mathbb{Z}_2[x]$: $(x^2 + x + 1)(x^2 + 1) = x^2(x^2 + 1) + x(x^2 + 1) + 1(x^2 + 1) = x^4 + x^2 + x^3 + x + x^2 + 1 = x^4 + x^3 + (x^2 + x^2) + x + 1 = x^4 + x^3 + 0x^2 + x + 1$ (since $1 + 1 = 0$ in $\mathbb{Z}_2$) $= x^4 + x^3 + x + 1$.
    - Now, we reduce this polynomial modulo $M = \langle x^3 + x + 1\rangle$.
    - The relation we use is $x^3 + x + 1 = 0 \pmod{M}$, which implies $x^3 = x + 1 \pmod{M}$ (since adding or subtracting 1 is the same in $\mathbb{Z}_2$).
    - $x^4 + x^3 + x + 1 = x(x^3) + x^3 + x + 1$
    - Substitute $x^3 = x + 1$: $= x(x + 1) + (x + 1) + x + 1 = x^2 + x + x + 1 + x + 1 = x^2 + (x + x + x) + (1 + 1) = x^2 + 3x + 2 = x^2 + x + 0$ (since $3 \equiv 1 \pmod{2}$ and $2 \equiv 0 \pmod{2}$) $= x^2 + x$.
    - Therefore, the product is **x² + x + M**.

(b) To prove that **in a principal ideal domain, an element is irreducible if and only if it is prime**:

- **Definitions**:
    - An element p in an integral domain D is **irreducible** if p is a non-zero, non-unit element, and whenever $p = ab$, then either a is a unit or b is a unit.
    - An element p in an integral domain D is **prime** if p is a non-zero, non-unit element, and whenever p divides ab, then p divides a or p divides b.
    - A **Principal Ideal Domain (PID)** is an integral domain where every ideal is principal (generated by a single element).

- **Proof**:
  - **Part 1: If p is prime, then p is irreducible.**
    - Let p be a prime element in a PID D. Assume $p = ab$ for some $a, b \in D$.
    - Since p divides ab and p is prime, by definition, p divides a or p divides b.
    - Without loss of generality, assume p divides a. So, $a = pc$ for some $c \in D$.
    - Substituting this into $p = ab$: $p = (pc)b = pcb$.
    - Since D is an integral domain and $p \neq 0$, we can cancel p: $1 = cb$.
    - This means b is a unit (with inverse c).
    - Therefore, if p is prime, it is irreducible. (This part holds in any integral domain, not just PIDs).
  - **Part 2: If p is irreducible, then p is prime.**
    - Let p be an irreducible element in a PID D. Assume p divides ab for some $a, b \in D$.
    - We need to show that p divides a or p divides b.
    - Consider the ideal $\langle p \rangle$.
    - In a PID, an ideal $\langle p \rangle$ is maximal if and only if p is irreducible.
    - We know that in any commutative ring with unity, every maximal ideal is also a prime ideal.
    - Therefore, if p is irreducible in a PID, then $\langle p \rangle$ is a maximal ideal, which implies $\langle p \rangle$ is also a prime ideal.

- By the definition of a prime ideal, since $ab \in \langle p \rangle$ (because p divides ab), it follows that $a \in \langle p \rangle$ or $b \in \langle p \rangle$.
- If $a \in \langle p \rangle$, then p divides a.
- If $b \in \langle p \rangle$, then p divides b.
- Thus, p divides a or p divides b. Hence, p is prime.

- Combining both parts, in a PID, an element is irreducible if and only if it is prime.

(c) **Show that integral domain Z[t] is Euclidean Domain. Is Z[i] a Unique Factorization Domain? Justify.**

- **Z[t] is NOT a Euclidean Domain.**
  - A Euclidean Domain is an integral domain where a Euclidean algorithm (like polynomial long division) can be performed. This requires that for any $f(t), g(t) \in Z[t]$ with $g(t) \neq 0$, we can find $q(t), r(t) \in Z[t]$ such that $f(t) = q(t)g(t) + r(t)$, where $r(t) = 0$ or $\deg(r(t)) < \deg(g(t))$.
  - The standard degree function works for polynomial rings over a field (like F[t]), but not for Z[t].
  - For instance, consider dividing x by $2x$ in $\mathbb{Z}[x]$. The quotient would be $1/2$, which is not in $\mathbb{Z}[x]$.
  - More formally, $\mathbb{Z}[x]$ is not a PID because the ideal $\langle 2, x \rangle$ (polynomials with even constant terms) cannot be generated by a single polynomial. If it were generated by $p(x)$, then $p(x)$ would have to divide both 2 and x. The only common divisors are ± 1. But $\langle 1 \rangle = \mathbb{Z}[x] \neq \langle 2, x \rangle$.
  - Since every Euclidean Domain is a PID, and $\mathbb{Z}[x]$ is not a PID, $\mathbb{Z}[x]$ (or $\mathbb{Z}[t]$) is not a Euclidean Domain.
- **Yes, Z[i] is a Unique Factorization Domain (UFD).**

- **Justification**: A fundamental theorem states that every **Euclidean Domain (ED)** is a **Principal Ideal Domain (PID)**, and every **PID** is a **Unique Factorization Domain (UFD)**.
- $\mathbb{Z}[i]$ (the Gaussian integers) is a Euclidean Domain. The Euclidean function is the norm function $d(a+bi) = a^2 + b^2$.
- For any Gaussian integers z_1, z_2 with $z_2 \neq 0$, we can find $q, r \in \mathbb{Z}[i]$ such that $z_1 = qz_2 + r$, where $r = 0$ or $N(r) < N(z_2)$. This is done by finding z_1/z_2 in $\mathbb{C}$, rounding its real and imaginary parts to the nearest integers to get q, and then setting $r = z_1 - qz_2$.
- Since $\mathbb{Z}[i]$ is a Euclidean Domain, it is also a PID, and consequently, it is a UFD. This means that every non-zero, non-unit Gaussian integer can be uniquely factored into irreducible Gaussian integers (up to units and order of factors).