Problem 1

The ring of integers is a PID.

(a) Define when a ring is called a principal ideal domain (PID).

(b) Prove that the ring of integers $\mathbb{Z}$ i a principal ideal domain. That is, show that every idear I of $\mathbb{Z}$ is generated by a single element, i.e., $I = (d) = \{kd; k \in \mathbb{Z}\}$ for some $d \in \mathbb{Z}$.

(c) Take two integers $m, n \in \mathbb{Z}$. The ideal generate by them is defined to be

$$(m, n) = \{am + bn; a, b \in \mathbb{Z}\}.$$

Find the integer d such that $(d) = (6, 15)$.

(a) A principal ideal domain (PID) is an integral domain in which every ideal is principal, meaning that it can be generated by a single element. In other words, for any ideal I in a PID, there exists an element d in the ring such that $I = (d) = \{rd; r \in R\}$, where R is the ring.

(b) *Proof.* To prove that the ring of integers $\mathbb{Z}$ is a principal ideal domain, we need to show that every ideal I in $\mathbb{Z}$ can be generated by a single integer. Let I be a non-zero ideal in $\mathbb{Z}$. Since I is non-empty, it contains some non-zero integers. Let d be the smallest positive integer in I (such a d exists by the well-ordering principle). We will show that $I = (d)$.
First, we show that $(d) \subseteq I$. By definition of (d), any element in (d) can be written as kd for some integer k. Since $d \in I$ and I is an ideal, it follows that $kd \in I$ for all integers k. Thus, every element of (d) is in I, so $(d) \subseteq I$.
Next, we show that $I \subseteq (d)$. Let a be any element in I. By the division algorithm, we can write a as:

$$a = qd + r,$$

where q is an integer and $0 \leq r < d$. Since $a \in I$ and $qd \in I$ (because $d \in I$ and I is an ideal), it follows that $r = a - qd \in I$. However, since d is the smallest positive integer in I, the only way for r to be in I and satisfy $0 \leq r < d$ is if $r = 0$. Therefore, we have:

$$a = qd.$$

This shows that every element a in I can be expressed as a multiple of d, so $a \in (d)$. Thus, we have $I \subseteq (d)$.
Combining both inclusions, we conclude that $I = (d)$. Therefore, every ideal in $\mathbb{Z}$ is principal, and hence $\mathbb{Z}$ is a principal ideal domain. □

(c) To find the integer d such that $(d) = (6, 15)$, we need to determine the greatest common divisor (gcd) of 6 and 15. The gcd of 6 and 15 is 3, since 3 is the largest integer that divides both 6 and 15 without leaving a remainder. Therefore, we have that $(d) = (6, 15)$ with $d = 3$.

Problem 2

Factoring real polynomials in over $\mathbb{C}$.

(a) Define what is a linear polynomial.
Let $f(x) = x^2 + bx + c \in \mathbb{R}[x]$.

(b) Factor $f(x)$ into product of linear polynomials over $\mathbb{C}$, i.e., into linear factors from $\mathbb{C}[x]$. Hint: Try the quadratic formula.

(c) Factorize the polynomial $f(x) = x^3 + 1$ into product of linear factors (polynomials) over $\mathbb{C}$.

(a) A linear polynomial is a polynomial of degree one, which can be expressed in the form $f(x) = ax + b$, where a and b are constants and $a \neq 0$.

(b) To factor the polynomial $f(x) = x^2 + bx + c$ into linear factors over $\mathbb{C}$, we can use the quadratic formula to find its roots. The roots of the polynomial are given by:

$$x = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

Let the roots be denoted as α_1 and α_2. Then, we can express the polynomial as:

$$f(x) = (x - \alpha_1)(x - \alpha_2).$$

(c) To factor the polynomial $f(x) = x^3 + 1$ into linear factors over $\mathbb{C}$, we can use the fact that $x^3 + 1$ can be factored using the sum of cubes formula:

$$x^3 + 1 = (x + 1)(x^2 - x + 1).$$

Next, we need to factor the quadratic $x^2 - x + 1$ over $\mathbb{C}$. Using the quadratic formula, we find the roots:

$$x = \frac{1 \pm \sqrt{(-1)^2 - 4 \cdot 1 \cdot 1}}{2 \cdot 1} = \frac{1 \pm \sqrt{-3}}{2} = \frac{1 \pm i\sqrt{3}}{2}.$$

Let the roots be denoted as $\alpha_1 = \frac{1+i\sqrt{3}}{2}$ and $\alpha_2 = \frac{1-i\sqrt{3}}{2}$. Thus, we can express the quadratic as:

$$x^2 - x + 1 = (x - \alpha_1)(x - \alpha_2).$$

Therefore, the complete factorization of $f(x) = x^3 + 1$ into linear factors over $\mathbb{C}$ is:

$$f(x) = (x + 1)(x - \alpha_1)(x - \alpha_2) = (x + 1)\left(x - \frac{1 + i\sqrt{3}}{2}\right)\left(x - \frac{1 - i\sqrt{3}}{2}\right).$$

Problem 3

Factoring in $\mathbb{R}[x]$.

(a) Let $\mathbb{F}$ be a field. Define when we say that a polynomial in $\mathbb{F}[x]$ is called irreducible.

(b) Let $f(x) \in \mathbb{R}[x]$

1. if $f(x) \in \mathbb{R}[x]$, and $\alpha \in \mathbb{C}$ is a root of f, then so is $\overline{\alpha}$.
2. Show that every non-constant irreducible polynomial in $\mathbb{R}[x]$ is of degree 1 or 2.

(c) Factor the following polynomials from $\mathbb{R}[x]$ into product of irreducibles over $\mathbb{R}$:

1. $x^3 - 1$
2. $x^4 + 1$
3. $x^6 - 1$

(a) A polynomial $f(x) \in \mathbb{F}[x]$ is called irreducible over the field $\mathbb{F}$ if it cannot be factored into the product of two non-constant polynomials in $\mathbb{F}[x]$. In other words, if $f(x) = g(x)h(x)$ for some polynomials $g(x), h(x) \in \mathbb{F}[x]$, then either $g(x)$ or $h(x)$ must be a constant polynomial.

(b) 1. *Proof.* Let $f(x) \in \mathbb{R}[x]$ and suppose $\alpha \in \mathbb{C}$ is a root of $f(x)$. Since the coefficients of $f(x)$ are real numbers, we can express $f(x)$ as:

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0,$$

where $a_i \in \mathbb{R}$ for all i. Taking the complex conjugate of both sides, we have:

$$\overline{f(x)} = \overline{a_n x^n} + \overline{a_{n-1} x^{n-1}} + \ldots + \overline{a_1 x} + \overline{a_0}.$$

Since the coefficients are real, we have $\overline{a_i} = a_i$ for all i. Thus, we can rewrite this as:

$$\overline{f(x)} = a_n \overline{x}^n + a_{n-1} \overline{x}^{n-1} + \ldots + a_1 \overline{x} + a_0.$$

Now, if α is a root of $f(x)$, then $f(\alpha) = 0$. Taking the complex conjugate, we get:

$$\overline{f(\alpha)} = f(\overline{\alpha}) = 0.$$

Therefore, $\overline{\alpha}$ is also a root of $f(x)$. □

2. *Proof.* Let $f(x) \in \mathbb{R}[x]$ be a non-constant irreducible polynomial. We will show that the degree of $f(x)$ must be either 1 or 2. Suppose, for the sake of contradiction, that the degree of $f(x)$ is greater than 2. Then, by the Fundamental Theorem of Algebra, $f(x)$ has at least one complex root α. By part (1), its complex conjugate $\overline{\alpha}$ is also a root of $f(x)$. Thus, we can factor $f(x)$ as:

$$f(x) = (x - \alpha)(x - \overline{\alpha})g(x),$$

where $g(x) \in \mathbb{C}[x]$ is a polynomial of degree at least 1. The product $(x-\alpha)(x-\overline{\alpha})$ is a quadratic polynomial with real coefficients, since:

$$(x-\alpha)(x-\overline{\alpha}) = x^2 - (\alpha + \overline{\alpha})x + \alpha\overline{\alpha} = x^2 - 2\text{Re}(\alpha)x + |\alpha|^2.$$

Therefore, we can express $f(x)$ as:

$$f(x) = q(x)g(x),$$

where $q(x) = (x-\alpha)(x-\overline{\alpha})$ is a quadratic polynomial with real coefficients. Since $g(x)$ has degree at least 1, this means that $f(x)$ can be factored into the product of two non-constant polynomials in $\mathbb{R}[x]$, contradicting the assumption that $f(x)$ is irreducible. Therefore, the degree of $f(x)$ must be either 1 or 2. □

3. 1. $x^3 - 1 = (x-1)(x^2+x+1)$, where $x-1$ is linear and x^2+x+1 is irreducible over $\mathbb{R}$.
   2. $x^4 + 1 = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1)$, where both quadratics are irreducible over $\mathbb{R}$.
   3. $x^6 - 1 = (x-1)(x+1)(x^2-x+1)(x^2+x+1)$, where $x-1$ and $x+1$ are linear, and both quadratics are irreducible over $\mathbb{R}$.

Problem 4

Irreducibles need not be primes.

(a) Recall that in an integral domain $\mathbb{R}$, a nonzero non-unit $q \in \mathbb{R}$ is prime if whenever $q|ab$ then either $q|a$ or $q|b$. A nonzero non-unit $q \in R$ is irreducible if whenever $q = ab$ then either a or b is a unit. Show that in an integral domain, every prime is irreducible.

(b) Consider the subring S of $\mathbb{C}$,

$$S = \{a + b\sqrt{-3} | a, b \in \mathbb{Z}\}.$$

Show that in this integral domain, $2 \in S$ is irreducible but not prime.

(c) Give an example of a commutative unital ring R, and prime element in R which is not irreducible.

(a) *Proof.* Let $\mathbb{R}$ be an integral domain, and let $q \in \mathbb{R}$ be a prime element. We need to show that q is irreducible. Suppose, for the sake of contradiction, that q is not irreducible. Then, we can write $q = ab$ for some non-unit elements $a, b \in \mathbb{R}$. Since q is prime, it follows that if $q|ab$, then either $q|a$ or $q|b$. However, since $q = ab$, we have that $q|ab$ trivially. Therefore, either $q|a$ or $q|b$. Without loss of generality, assume that $q|a$. This means there exists some element $c \in \mathbb{R}$ such that $a = qc$. Substituting this back into the equation for q, we have:

$$q = ab = (qc)b = q(cb).$$

Since $\mathbb{R}$ is an integral domain and $q \neq 0$, we can cancel q from both sides to obtain:

$$1 = cb.$$

This implies that b is a unit in $\mathbb{R}$, which contradicts our assumption that both a and b are non-units. Therefore, our initial assumption that q is not irreducible must be false. Hence, every prime element in an integral domain is irreducible. □

(b) *Proof.* Let $S = \{a + b\sqrt{-3} | a, b \in \mathbb{Z}\}$ be the subring of $\mathbb{C}$. We will show that $2 \in S$ is irreducible but not prime. First, we show that 2 is irreducible. Suppose that $2 = ab$ for some $a, b \in S$. We can express a and b as:

$$a = x + y\sqrt{-3}, \quad b = u + v\sqrt{-3},$$

where $x, y, u, v \in \mathbb{Z}$. Then, we have:

$$2 = (x + y\sqrt{-3})(u + v\sqrt{-3}) = (xu - 3yv) + (xv + yu)\sqrt{-3}.$$

Equating the real and imaginary parts, we get the system of equations:

$$xu - 3yv = 2,$$

$$xv + yu = 0.$$

From the second equation, we can express yu in terms of xv:

$$yu = -xv.$$

Substituting this into the first equation, we have:

$$xu + 3xv^2/y = 2.$$

Since x, y, u, v are integers, it follows that either x or y must be a unit in $\mathbb{Z}$, which means either a or b is a unit in S. Therefore, 2 is irreducible in S.
Next, we show that 2 is not prime. Consider the elements $1 + \sqrt{-3}$ and $1 - \sqrt{-3}$ in S. We have:

$$(1 + \sqrt{-3})(1 - \sqrt{-3}) = 1 - (-3) = 4.$$

Since $4 = 2 \cdot 2$, it follows that $2|4$. However, neither $2|(1 + \sqrt{-3})$ nor $2|(1 - \sqrt{-3})$, since dividing either by 2 does not yield an element in S. Therefore, 2 is not prime in S.

□

(c) Consider the ring $R = \mathbb{Z}/6\mathbb{Z}$. In this ring, the element $2+6\mathbb{Z}$ is prime because if $2+6\mathbb{Z}|ab+6\mathbb{Z}$, then either $2+6\mathbb{Z}|a+6\mathbb{Z}$ or $2 + 6\mathbb{Z}|b + 6\mathbb{Z}$. However, $2 + 6\mathbb{Z}$ is not irreducible because we can write:

$$2 + 6\mathbb{Z} = (2 + 6\mathbb{Z})(1 + 6\mathbb{Z}),$$

where neither $2 + 6\mathbb{Z}$ nor $1 + 6\mathbb{Z}$ is a unit in R. Thus, we have found a prime element in R that is not irreducible.

Problem 5

Eigenvalues over $\mathbb{R}$ and $\mathbb{C}$.
For each of the folowing linear transformations, find all eigenvalues. For each eigenvalue, find the corresponding eigenspace. In each case, do the problem first with $\mathbb{F} = \mathbb{R}$ and then again with $\mathbb{F} = \mathbb{C}$.

(a) $T : \mathbb{F}^3 \to \mathbb{F}^3$,

$$T(x_1, x_2, x_3) = (x_1 + x_2,\ x_2 + x_3,\ x_1 + x_3).$$

(b) $T : \mathbb{F}^2 \to \mathbb{F}^2$,

$$T(x_1, x_2) = (x_1 + x_2,\ x_1 - x_2).$$

(c) $T : \mathbb{F}^4 \to \mathbb{F}^4$,

$$T(x_1, x_2, x_3, x_4) = (x_2,\ 2x_3,\ 3x_4,\ 0).$$

(a) Matrix of T (standard basis): $A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$. Characteristic polynomial:

$$\det(A - \lambda I) = (1 - \lambda)^3 + 1 = 0.$$

Over $\mathbb{R}$ the only real root is $\lambda = 2$. Solving $(A - 2I)v = 0$ gives

$$v = (1, 1, 1)^T,$$

so eigenspace for $\lambda = 2$ is $\operatorname{span}\{(1, 1, 1)\}$.

Over $\mathbb{C}$ the other two eigenvalues are $\lambda = \frac{1}{2} \pm \frac{i\sqrt{3}}{2}$. Let $r = 1 - \lambda$ (so $r^3 = -1$). For each such λ an eigenvector is

$$v = (1, -r, r^2)^T,$$

and the conjugate eigenvalue has the conjugate eigenvector. Thus the three eigenspaces are $\operatorname{span}\{(1, 1, 1)\}$ and $\operatorname{span}\{(1, -r, r^2)\}, \operatorname{span}\{(1, -\overline{r}, \overline{r}^2)\}$.

(b) Matrix $A = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Characteristic polynomial: $\lambda^2 - 2 = 0$, so $\lambda = \pm\sqrt{2}$ (real).

For a general eigenvalue λ an eigenvector satisfies $(1-\lambda)x_1 + x_2 = 0$, so we may take

$$v = (1,\ \lambda - 1)^T.$$

Thus for $\lambda = \sqrt{2}$ an eigenvector is $(1, \sqrt{2} - 1)^T$, and for $\lambda = -\sqrt{2}$ an eigenvector is $(1, -\sqrt{2} - 1)^T$. The same answers hold over $\mathbb{C}$.

(c) Matrix of T is $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}$. Characteristic polynomial $\lambda^4 = 0$, so the only eigenvalue (over $\mathbb{R}$ and $\mathbb{C}$) is $\lambda = 0$. Solve $T(v) = 0$: $x_2 = 0,\ x_3 = 0,\ x_4 = 0$, so the eigenspace is $\operatorname{span}\{(1, 0, 0, 0)\}$.