Honors Linear Algebra **Fall 2024**
HW7: Rings, Ideals, and Factorizations **Due: 10/27/2024**

Problem 1. (Exact Sequences of a Pair in a PID). Let R be a principle ideal domain (PID). Let $a, b \in R$, not both of which are 0. Define $f : R \times R \longrightarrow R$ by $f(s,t) = sa + tb$. Note that $R \times R$ is also a commutive ring with 1 when addition and multiplication are defined coordinate-wise:

(1) $(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$

(2) $(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2)$

(3) $r \cdot (a, b) = (ra, rb)$

*Further note that $R \times R$ is an R-module with scalar multiplication defined by (3)

(a) Show that f satisfies

(i) $f(x + y) = f(x) + f(y)$ for all $x, y \in R \times R$

(ii) $f(rx) = rf(x)$ for $r \in R$, $x \in R \times R$

Hence f is an R-module homomorphism

We begin by verifying the two properties of f.

(i) For $f(x + y) = f(x) + f(y)$, let $x = (s_1, t_1)$ and $y = (s_2, t_2)$ in $R \times R$. Then

$$\begin{aligned} f((s_1, t_1) + (s_2, t_2)) &= f(s_1 + s_2, t_1 + t_2) = (s_1 + s_2)a + (t_1 + t_2)b \\ &= s_1 a + s_2 a + t_1 b + t_2 b = f(s_1, t_1) + f(s_2, t_2). \end{aligned}$$

(ii) For $f(rx) = rf(x)$, let $x = (s, t)$. Then

$$f(r(s,t)) = f(rs, rt) = (rs)a + (rt)b = r(sa + tb) = rf(s,t).$$

Since both properties hold, f is an R-module homomorphism.

(b) Show that $\operatorname{im} f \subseteq R$ is non-empty and is closed under addition and scalar multiplication; that is $\operatorname{im} f$ is an R-submodule of R.

Let $f(s,t) = sa + tb$. The image of f, denoted by $\operatorname{im} f$, is non-empty because $f(0,0) = 0 \in R$.

Next, we show closure under addition. Let $(s_1, t_1), (s_2, t_2) \in R \times R$. Then

$$f(s_1, t_1) + f(s_2, t_2) = (s_1 a + t_1 b) + (s_2 a + t_2 b) = (s_1 + s_2)a + (t_1 + t_2)b = f((s_1, t_1) + (s_2, t_2)).$$

For closure under scalar multiplication, let $r \in R$. Then

$$rf(s,t) = r(sa + tb) = (rs)a + (rt)b = f(rs, rt).$$

Thus, $\operatorname{im} f$ is an R-submodule of R.

(c) Compute $\operatorname{im} f$.

The image of f consists of all elements of the form $sa+tb$ for $s, t \in R$. Therefore, the image of f is the ideal generated by a and b, that is,

$$\operatorname{im} f = (a, b).$$

(d) Show that $\ker f \subseteq R \times R$ is an R-submodule of $R \times R$.

The kernel of f is given by

$$\ker(f) = \{(s,t) \in R \times R \mid sa + tb = 0\}.$$

Clearly, $0 \in \ker(f)$, so the kernel is non-empty. Let $(s_1, t_1), (s_2, t_2) \in \ker(f)$. Then

$$f(s_1 + s_2, t_1 + t_2) = (s_1 + s_2)a + (t_1 + t_2)b = (s_1 a + t_1 b) + (s_2 a + t_2 b) = 0,$$

so $(s_1 + s_2, t_1 + t_2) \in \ker(f)$.

For scalar multiplication, let $r \in R$. Then

$$f(r(s,t)) = (rs)a + (rt)b = r(sa + tb) = r \cdot 0 = 0,$$

so $r(s,t) \in \ker(f)$. Thus, $\ker(f)$ is an R-submodule of $R \times R$.

(e) Determine $\ker f$ explicitly: Show that there exists a function $g : R \longrightarrow R \times R$ of the form $g(r) = (r\alpha, r\beta)$ for some $\alpha, \beta \in R$ such that $\operatorname{im} g = \ker f$. Note that g satisfies the analogue of (i) and (ii) above (i.e. is an R-module homomorphism).

We begin by noting that

$$\ker(f) = \{(s,t) \in R \times R \mid sa + tb = 0\}.$$

This means that for any $(s,t) \in \ker(f)$, $sa = -tb$, so there is a relationship between s and t. We can express this explicitly using a function $g : R \to R \times R$.

Define $g(r) = (r\alpha, r\beta)$ where $\alpha = b/\gcd(a,b)$ and $\beta = -a/\gcd(a,b)$. Then for any $r \in R$, we have

$$g(r) = \left(r \cdot \frac{b}{\gcd(a,b)}, r \cdot \frac{-a}{\gcd(a,b)} \right).$$

This satisfies the condition that $sa + tb = 0$, and hence $\operatorname{im} g = \ker f$.

Moreover, g satisfies the properties of an R-module homomorphism, as $g(r + r') = g(r) + g(r')$ and $g(kr) = kg(r)$ for all $r, r' \in R$ and $k \in R$.

(f) Show that there exists an exact sequence of R-modules

$$0 \longrightarrow X \xrightarrow{i} R \times R \xrightarrow{f} R \xrightarrow{p} Y \longrightarrow 0$$

What are X, i, Y, p?

We want to show that the following sequence is exact:

$$0 \longrightarrow X \xrightarrow{i} R \times R \xrightarrow{f} R \xrightarrow{p} Y \longrightarrow 0.$$

Recall that the sequence is exact if the image of each map is equal to the kernel of the next.

- $X = \ker(f) = \{(s,t) \in R \times R \mid sa + tb = 0\}$.
- The map i is the inclusion map from X into $R \times R$.
- The map $f : R \times R \to R$ is defined by $f(s,t) = sa + tb$.
- $Y = R/\operatorname{im}(f) = R/(a,b)$ is the quotient of R by the ideal generated by a and b.
- The map $p : R \to Y$ is the natural projection map.

Thus, we have the exact sequence:

$$0 \longrightarrow \ker(f) \xrightarrow{i} R \times R \xrightarrow{f} R \xrightarrow{p} R/(a,b) \longrightarrow 0.$$

(g) Determine precisely all solution $(s,t), s,t \in R$ of the equation $sa + tb = \operatorname{ged}(a,b)$ where $\operatorname{ged}(a,b)$ denotes the greatest common divisor of a and b.

We are tasked with solving the equation

$$sa + tb = \gcd(a,b).$$

By Bezout's identity, there exist integers s_0 and t_0 such that

$$s_0 a + t_0 b = \gcd(a,b).$$

These integers can be found using the extended Euclidean algorithm.

The general solution to this equation is given by

$$s = s_0 + k \cdot \frac{b}{\gcd(a,b)}, \quad t = t_0 - k \cdot \frac{a}{\gcd(a,b)}$$

for some integer k. Thus, all solutions (s,t) are of this form, where s_0 and t_0 are particular solutions and $k \in R$ is arbitrary.

Problem 2. Let $\mathbb{F}$ be an arbitrary field.

(a) Show that the intersection of an arbitrary number of ideals in $\mathbb{F}[x]$ is an deal in $\mathbb{F}[x]$.

Let $\{I_\lambda\}_{\lambda \in \Lambda}$ be an arbitrary family of ideals in $\mathbb{F}[x]$, where Λ is an index set. We define the intersection of these ideals as

$$I = \bigcap_{\lambda \in \Lambda} I_\lambda.$$

We need to verify that I satisfies the properties of an ideal.

1. Closure under addition:
Let $f, g \in I$. This means that $f, g \in I_\lambda$ for all $\lambda \in \Lambda$. Since each I_λ is an ideal, we have $f + g \in I_\lambda$ for all λ. Therefore, $f + g \in I$, so I is closed under addition.

2. Closure under multiplication by elements of $\mathbb{F}[x]$:
Let $f \in I$ and $h \in \mathbb{F}[x]$. Since $f \in I_\lambda$ for all λ, and each I_λ is an ideal, it follows that $hf \in I_\lambda$ for all λ. Therefore, $hf \in I$, so I is closed under multiplication by elements of $\mathbb{F}[x]$.

Thus, $I = \bigcap_{\lambda\in\Lambda} I_\lambda$ is an ideal of $\mathbb{F}[x]$.

(b) Let $f_1, \ldots, f_k \in \mathbb{F}[x]$. The ideal generated by these is

$$(f_1, \ldots f_k) = \{g_1 f_1 + \cdots g_k f_k \quad | \quad g_i \in \mathbb{F}[x]\}$$

the set of all $\mathbb{F}[x]$-linear combinations of $f_1, \ldots, f_k$. Show that this ideal is precisely the intersection of ideals which contain all f_i, $1 \le i \le k$.

Let $f_1, \ldots, f_k \in \mathbb{F}[x]$, and consider the ideal generated by these polynomials:

$$(f_1, \ldots, f_k) = \{g_1 f_1 + \cdots + g_k f_k \mid g_1, \ldots, g_k \in \mathbb{F}[x]\}.$$

We aim to show that this ideal is equal to the intersection of all ideals in $\mathbb{F}[x]$ that contain $f_1, \ldots, f_k$.

Let I be any ideal containing $f_1, \ldots, f_k$. Since I is an ideal, any linear combination of $f_1, \ldots, f_k$ with coefficients from $\mathbb{F}[x]$ must also be in I. Therefore, the ideal $(f_1, \ldots, f_k)$ is contained in every ideal that contains $f_1, \ldots, f_k$. This gives the inclusion

$$(f_1, \ldots, f_k) \subseteq \bigcap_{I \supseteq \{f_1, \ldots, f_k\}} I.$$

Conversely, let $f \in \bigcap_{I \supseteq \{f_1, \ldots, f_k\}} I$. This means that f is in every ideal that contains $f_1, \ldots, f_k$. Since $(f_1, \ldots, f_k)$ is the smallest ideal containing $f_1, \ldots, f_k$, it follows that $f \in (f_1, \ldots, f_k)$. Therefore, we have the reverse inclusion

$$\bigcap_{I \supseteq \{f_1, \ldots, f_k\}} I \subseteq (f_1, \ldots, f_k).$$

Thus, we conclude that

$$(f_1, \ldots, f_k) = \bigcap_{I \supseteq \{f_1, \ldots, f_k\}} I.$$

Problem 3. Let $\mathbb{F}$ be a field and let $f \in \mathbb{F}[y]$ be a polynomial. Since the ideal $I = (f)$ generated by f is a subspace of $\mathbb{F}[x]$, we can form the quotient vector space $\mathbb{F}[y]/(f)$. Assume that f is not constant. (This exercise is the rigorous definition of root adjunction).

(a) For $a, b \in \mathbb{F}[y]$, show $a + (f) = b + (f)$ if and only if f divides $a - b$.

We need to show that $a + (f) = b + (f)$ if and only if f divides $a - b$.

1. Showing $\implies$:
This equality means that $a - b \in (f)$, i.e., $a - b = qf$ for some $q \in \mathbb{F}[y]$. Hence, f divides $a - b$.

2. Showing $\impliedby$:
This means that $a - b = qf$ for some $q \in \mathbb{F}[y]$. Thus, $a = b + qf$, so $a + (f) = b + (f)$.

Therefore, $a + (f) = b + (f)$ if and only if f divides $a - b$.

(b) Show $\mathbb{F}[y]/(f)$ has a well-defined multiplication operation given by

$$(a + (f))(b + (f)) := ab + (f)$$

(In other words, if $a + (f) = a' + (f)$ and $b + (f) = b' + (f)$, show that $ab + (f) = a'b' + (f)$). Conclude that $\mathbb{F}[y]/(f)$ is an $\mathbb{F}$-algebra, and that there is a natural one-to-one homomorphism $\mathbb{F} \longrightarrow \mathbb{F}[y]/(f)$ (hence we can consider $\mathbb{F}$ as a subring).

We need to show that if $a + (f) = a' + (f)$ and $b + (f) = b' + (f)$, then $ab + (f) = a'b' + (f)$.

Since $a + (f) = a' + (f)$, we have $a - a' \in (f)$, so $a = a' + qf$ for some $q \in \mathbb{F}[y]$. Similarly, $b + (f) = b' + (f)$ implies $b = b' + rf$ for some $r \in \mathbb{F}[y]$.

Now,

$$ab = (a' + qf)(b' + rf) = a'b' + a'rf + b'qf + qfrf.$$

Since $f \in (f)$, we know that $a'rf + b'qf + qfrf \in (f)$. Therefore,

$$ab + (f) = a'b' + (f).$$

Thus, the multiplication operation is well-defined.

Since both addition and multiplication are well-defined, $\mathbb{F}[y]/(f)$ is an $\mathbb{F}$-algebra. The map $\mathbb{F} \longrightarrow \mathbb{F}[y]/(f)$ defined by $c \mapsto c + (f)$ is a one-to-one homomorphism, so $\mathbb{F}$ can be considered as a subring of $\mathbb{F}[y]/(f)$.

(c) Prove that $\mathbb{F}[x]/(f)$ is a field if and only if f is irreducible

For $\mathbb{F}[x]/(f)$ to be a field, every non-zero element must have a multiplicative inverse. We examine this by considering the irreducibility of f.

Showing $\implies$:
Suppose f is irreducible. Then any polynomial $g \in \mathbb{F}[x]$ that is not a multiple of f will have no non-trivial factors common with f, because f is irreducible. By Bezout's theorem, there exist polynomials $a, b \in \mathbb{F}[x]$ such that $ag + bf = 1$. In $\mathbb{F}[x]/(f)$, this implies $ag \equiv 1 \pmod{f}$, so g has a multiplicative inverse in $\mathbb{F}[x]/(f)$. Thus, $\mathbb{F}[x]/(f)$ is a field.

Showing $\impliedby$:
Conversely, assume $\mathbb{F}[x]/(f)$ is a field. Then, by definition, every non-zero element has a

multiplicative inverse. Suppose f were not irreducible. Then $f = gh$ for some non-constant polynomials $g, h \in \mathbb{F}[x]$ with $\deg(g), \deg(h) < \deg(f)$. In $\mathbb{F}[x]/(f)$, g and h would be non-zero elements whose product is zero, contradicting the fact that $\mathbb{F}[x]/(f)$ is a field (since fields have no zero divisors). Therefore, f must be irreducible.

Thus, $\mathbb{F}[x]/(f)$ is a field if and only if f is irreducible.

(d) Let f be a irreducible and let $K = \mathbb{F}[y]/(f)$. Let $h \in \mathbb{F}[x]$. For $a \in K$ (or indeed for any $\mathbb{F}$-algebra K), we can evaluate $h(a) \in K$ as usual. Show that there is an $a \in K$ such that $f(a) = 0$. Hence we have constructed a field K which contains $\mathbb{F}$ and which contains a root of the irreducible polynomial f.

Let f be an irreducible polynomial over $\mathbb{F}$, and let $K = \mathbb{F}[y]/(f)$. Define a as the equivalence class of y in K, denoted by $a = y + (f)$. We claim that $f(a) = 0$ in K.

Since $a = y+(f)$, any polynomial evaluated at a corresponds to its remainder when divided by f. Therefore, evaluating $f(a)$ in K yields:

$$f(a) = f(y + (f)) = f(y) + (f) = 0 + (f) = 0 \text{ in } K.$$

Thus, a is a root of f in K.

Since K is a field extension of $\mathbb{F}$ that contains a root a of the irreducible polynomial f, we have constructed a field K containing both $\mathbb{F}$ and a root of f.

Problem 4. (Ring 20)

(a) Let $\mathbb{F}$ be a field and let $\mathbb{F}^{\mathbb{F}}$ denote the set of all functions from $\mathbb{F}$ to $\mathbb{F}$. Recall that this is a ring under the usual definition and multiplication of functions (that is, add or multiply their values). As is shown above, there is a function $E : \mathbb{F}[x] \longrightarrow \mathbb{F}^{\mathbb{F}}$ given by sending the formal polynomial in $\mathbb{F}[x]$ to the function which is computed by using the given polynomial as the formula for computation. This function E preserves both addition and multiplication (it is what is called a *ring homomorphism*). Further it was noted that this function is not always one-to-one. Prove that it is one-to-one if and only if $\mathbb{F}$ is an infinite field. Prove that it is onto if and only if $\mathbb{F}$ is a finite field. Show that the kernel of E (the polynomials that go to 0) is an ideal of $\mathbb{F}[x]$. Give an explicit monic generator of this ideal.

Checking One-to-one:
Suppose $\mathbb{F}$ is an infinite field. Assume $p(x) \in \mathbb{F}[x]$ and $E(p) = 0$, meaning $p(a) = 0$ for all $a \in \mathbb{F}$. Since a non-zero polynomial of degree d has at most d roots in an infinite field, $p(x)$ must be the zero polynomial. Therefore, E is injective when $\mathbb{F}$ is infinite.

Conversely, if $\mathbb{F}$ is finite, a non-zero polynomial in $\mathbb{F}[x]$ could map to the zero function if it has roots at all elements of $\mathbb{F}$. Thus, E is not injective in this case.

Checking Onto:
If $\mathbb{F}$ is finite, say with q elements, every function from $\mathbb{F}$ to $\mathbb{F}$ can be represented by a polynomial using Lagrange interpolation. Thus, E is onto when $\mathbb{F}$ is finite.

Conversely, if $\mathbb{F}$ is infinite, there are more functions from $\mathbb{F}$ to $\mathbb{F}$ than there are polynomials in $\mathbb{F}[x]$, so E cannot be onto.

Chekcing $\ker E$ and its Monic Generator:
$\ker E$ consists of polynomials $p(x) \in \mathbb{F}[x]$ that evaluate to zero for all elements of $\mathbb{F}$. If $\mathbb{F}$ has q elements, then $p(x) = 0$ for all $x \in \mathbb{F}$ if and only if $p(x)$ is a multiple of the polynomial $x^q - x$, by Fermat's Little Theorem. Thus, the $\ker E$ is the principal ideal generated by $x^q - x$, which is a monic polynomial.

(b) If $\mathbb{F}$ has q elements, show that the generator you found in the preceding part is equal to $x^q - x$.

If $\mathbb{F}$ has q elements, every element $a \in \mathbb{F}$ satisfies $a^q = a$ (by Fermat's Little Theorem or properties of finite fields). This implies that the polynomial $f(x) = x^q - x$ evaluates to zero for each $a \in \mathbb{F}$.

Thus, $x^q - x$ is a polynomial that vanishes on all elements of $\mathbb{F}$, meaning it generates the kernel of E when $\mathbb{F}$ is a finite field with q elements, as established in the previous part.

Problem 5. Let $\overline{} : \mathbb{C} \longrightarrow \mathbb{C}$ denote ordinary complex conjugation. Show that it is an isomorphism of fields. (Even an $\mathbb{R}$-algebra isomorphism). Show that it induces an isomorphism of ringside

$$\overline{} : \mathbb{C}[x] \longrightarrow \mathbb{C}[x]$$

by defining $\overline{h} = \overline{b_0} + \overline{b_0}x + \cdots + \overline{b_k}x^k$ for $h = b_0 + b_1x + \cdots + b_kx^k \in \mathbb{C}[x]$.

Showing that Complex Conjugation is a Field Isomorphism:
Consider the map $\overline{} : \mathbb{C} \to \mathbb{C}$ defined by complex conjugation, i.e., for any $z = a + bi \in \mathbb{C}$ (where $a, b \in \mathbb{R}$), we have $\overline{z} = a - bi$. To show that this map is an isomorphism of fields, we need to prove that it preserves addition, multiplication, and the multiplicative identity, and that it is bijective.

(1) Addition: For $z_1, z_2 \in \mathbb{C}$, we have $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$.
(2) Multiplication: For $z_1, z_2 \in \mathbb{C}$, $\overline{z_1 z_2} = \overline{z_1} \cdot \overline{z_2}$.
(3) Identity: The multiplicative identity in $\mathbb{C}$ is 1, and $\overline{1} = 1$.

Additionally, complex conjugation is bijective, as each $z \in \mathbb{C}$ has a unique conjugate $\overline{z}$, and applying conjugation twice gives back the original element: $\overline{\overline{z}} = z$. Therefore, complex conjugation is a field isomorphism.

Since complex conjugation also fixes each real number, it is an $\mathbb{R}$-algebra isomorphism.

Showing that Conjugation Induces a Ring Isomorphism on $\mathbb{C}[x]$:
Define the map $\overline{} : \mathbb{C}[x] \to \mathbb{C}[x]$ by applying conjugation to the coefficients of any polynomial. For $h(x) = b_0 + b_1x + \cdots + b_kx^k \in \mathbb{C}[x]$, we define $\overline{h(x)} = \overline{b_0} + \overline{b_1}x + \cdots + \overline{b_k}x^k$.

(1) Preservation of Addition: For $f(x), g(x) \in \mathbb{C}[x]$, we have $\overline{f(x) + g(x)} = \overline{f(x)} + \overline{g(x)}$ since conjugation of complex numbers preserves addition.
(2) Preservation of Multiplication: Similarly, for $f(x), g(x) \in \mathbb{C}[x]$, we have $\overline{f(x) \cdot g(x)} = \overline{f(x)} \cdot \overline{g(x)}$, since conjugation preserves multiplication of coefficients.

Thus, conjugation on the coefficients defines an isomorphism of the ring $\mathbb{C}[x]$.

Problem 6. The following is the Euclidean algorithm for computing the greatest common denominator of non-zero polynomials f_0 and f_1 in $\mathbb{F}[x]$ (note that all of its steps can be computed by hand). Let's assume that we have labelled f_0 and f_1 so that $\deg(f_1) \leq \deg(f_0)$. Then define f_2 to be the remainder of f_0 when divided by f_1. Note that either $\deg(f_2) < \deg(f_1)$ of $f_2 = 0$. In general, inductively define f_{i+1} to be the remainder of f_{i-1} by f_i for as long as $f_i \neq 0$. Set d to be the monic polynomial associated to f_k.

(a) Prove that d is the greatest common denominator of f_0 and f_1.

Let $f_0, f_1 \in \mathbb{F}[x]$ be two non-zero polynomials, where we define the sequence of polynomials $f_2, f_3, \ldots, f_k$ such that each f_{i+1} is the remainder of f_{i-1} divided by f_i (i.e., $f_{i+1} = f_{i-1} \mod f_i$) until we reach a zero remainder, at which point $f_k \neq 0$ but $f_{k+1} = 0$.

At each step in the Euclidean algorithm, each f_{i+1} divides both f_0 and f_1, so the last non-zero remainder f_k divides all previous f_i. The monic polynomial d associated with f_k is therefore the greatest common divisor of f_0 and f_1 since it divides both polynomials and any common divisor of f_0 and f_1 must also divide d.

(b) Use the Euclidean algorithm to find the greatest common denominator of $x^5 + x^4 + 3x^3 + 2x^2 + 3x + 2$ and $x^4 + x^3 - 2x^2 - 4x - 8$ in $\mathbb{Q}[x]$.

Let $f_0 = x^5 + x^4 + 3x^3 + 2x^2 + 3x + 2$ and $f_1 = x^4 + x^3 - 2x^2 - 4x - 8$. Perform polynomial division to find the remainder $f_2 = f_0 \mod f_1$, and continue with the Euclidean algorithm:

First dividing f_0 by f_1:

$$f_0 = f_1 \cdot x + (3x^3 + 6x^2 + 7x + 10)$$

so $f_2 = 3x^3 + 6x^2 + 7x + 10$.

Then dividing f_1 by f_2:

$$f_1 = f_2 \cdot \frac{1}{3}x + \left(-\frac{5}{3}x^2 - \frac{17}{3}x - \frac{34}{3}\right)$$

so $f_3 = -\frac{5}{3}x^2 - \frac{17}{3}x - \frac{34}{3}$.

You continue until reaching a remainder of zero.

The last non-zero remainder will be the greatest common divisor d.

(c) Let K be a subfield of F, and suppose $f, g \in \mathbb{K}[x]$. Let I_k be the ideal generated by f and g in $\mathbb{K}[x]$, and let $I_{\mathbb{F}}$ be the initial ideal generated by f and g in $\mathbb{F}[x]$. Prove that $I_{\mathbb{K}}$ and $I_{\mathbb{F}}$ have the same monic generator.

Let $I_{\mathbb{K}} = (f, g)$ in $\mathbb{K}[x]$ and $I_{\mathbb{F}} = (f, g)$ in $\mathbb{F}[x]$. Since $\mathbb{K} \subset \mathbb{F}$, the operations in $\mathbb{K}[x]$ are preserved in $\mathbb{F}[x]$. The Euclidean algorithm applied in both $\mathbb{K}[x]$ and $\mathbb{F}[x]$ will yield the same monic greatest common divisor d, ensuring $I_{\mathbb{K}}$ and $I_{\mathbb{F}}$ share this monic generator.

(d) Let $\mathbb{K}$ be a subfield of the complex numbers $\mathbb{C}$, and let $f \in \mathbb{K}[x]$. Suppose that f as a complex polynomial has a double root (that is, a root $\alpha \in \mathbb{C}$ of multiplicity ≥ 2). Prove that f is reducible in $\mathbb{K}[x]$.

Suppose $f \in \mathbb{K}[x]$ has a double root $\alpha \in \mathbb{C}$. Then $f(x) = (x-\alpha)^2 g(x)$ for some $g(x) \in \mathbb{C}[x]$, which implies f can be factored non-trivially over $\mathbb{K}[x]$ if $\alpha \in \mathbb{K}$, or over a field extension of $\mathbb{K}$ if $\alpha \notin \mathbb{K}$. In either case, f is reducible in $\mathbb{K}[x]$.

(e) Show that the following process can be used to compute the greatest common divisor d of f_0, f_1 and at the same time yield s, t so that $sf_0 + tf_1 = d$.

(i) Put $X = (1, 0, f_0)$, $Y = (0, 1, f_1)$, and $Z = (0, 0, 0)$.

(ii) Divide the third component of X by the third component of Y to obtain q and r (Division Algorithm)

(iii) If $r = 0$, terminate the algorithm with $Y = (s, t, d)$. If $r \neq 0$, replace Z by Y, Y by $X - qY$ and X by Z. Note that Z is really just a temporary place to store the value of Y. Repeat step (ii).

Find a way to interpret the preceding process as the multiplication of a certain 2 by 3 matrix on the left by elementary matrices with integer entries (i.e. row operations)

We can interpret the process as follows:

(i) Initial Setup:
We start with a 2×3 matrix A defined as:

$$A = \begin{pmatrix} 1 & 0 & f_0 \\ 0 & 1 & f_1 \end{pmatrix}$$

This matrix represents the coefficients of the linear combinations of f_0 and f_1 along with their respective indices.

(ii) Division and Row Operations:
We perform the division of the third component of X by the third component of Y to obtain q and r as follows:

$$f_0 = qf_1 + r$$

This can be represented by the row operation:

$$R_1 \leftarrow R_1 - qR_2$$

Thus, the updated matrix becomes:

$$A' = \begin{pmatrix} 1 & 0 & r \\ 0 & 1 & f_1 \end{pmatrix}$$

(iii) Iterative Steps:
If $r \neq 0$, we set Z to Y (the second row becomes the first row) and update Y and X:

$$X \leftarrow Z, \quad Y \leftarrow \begin{pmatrix} 1 & 0 & r \end{pmatrix}$$

and replace X with Z. The process continues with another row operation:

$$R_2 \leftarrow R_2 - \frac{r}{f_1} R_1$$

(iii) Termination:
This process continues until $r = 0$, at which point we terminate the algorithm with $Y = (s, t, d)$ where $d = \gcd(f_0, f_1)$ and s and t are the coefficients such that:

$$s f_0 + t f_1 = d$$

In summary, the greatest common divisor d can be computed using matrix A and performing a series of row operations, represented as multiplications by elementary matrices with integer entries. This interpretation illustrates how each step corresponds to manipulations of the rows in the matrix, ultimately yielding s, t, and d.