MATH 25800 (Honors Basic Algebra II) Problem Sets

Steven Labalme

February 25, 2023

Contents

1 Rings, Subrings, and Ring Homomorphisms **1**

2 Ideals and Vector Spaces **7**

3 Properties of Ideals **15**

4 Applications of Fraction Rings **21**

5 Misc. Ring Tools **30**

6 Getting Comfortable With Modules **35**

7 Modules Over PIDs **42**

References **51**

1 Rings, Subrings, and Ring Homomorphisms

1/11: **1.1.** Let R be a ring with identity. Show that R is a singleton if and only if $0_R = 1_R$.

Proof. Suppose first that R is a singleton. Let $x \in R$ be the sole element in R. Since $(R, +)$ is a group (necessarily the trivial group due to order), we know that $x = 0_R$. Since R is a ring with identity, x must be said identity, i.e., we know that $x = 1_R$. Therefore, by transitivity, $0_R = 1_R$, as desired.

Now suppose that $0_R = 1_R$. Pick $x, y \in R$ arbitrary. Then we have that

$$x = 1_R \times x = 0_R \times x = 0_R$$

and the same for y. Thus, by transitivity, $x = y$. Since any two elements of R are equal, R must be a singleton, as desired. □

Products

1.2. Let X, Y be sets and let R be a ring. Recall that pointwise addition and multiplication turns R^X and R^Y into rings. Let $f : X \to Y$ be a function. Define $f^* : R^Y \to R^X$ by $f^*(g) = g \circ f$ for all $g : Y \to R$. Prove that f^* is a ring homomorphism.

Proof. To prove that f^* is a ring homomorphism, it will suffice to check that $f^*(g_1 + g_2) = f^*(g_1) + f^*(g_2)$ and $f^*(g_1 \times g_2) = f^*(g_1) \times f^*(g_2)$ for all $g_1, g_2 \in R^Y$, and $f^*(1_{R^Y}) = 1_{R^X}$. Let's begin.

Let $g_1, g_2 \in R^Y$ be arbitrary. Then we have for any $x \in X$ that

$$\begin{aligned}
[f^*(g_1 + g_2)](x) &= [(g_1 + g_2) \circ f](x) \\
&= (g_1 + g_2)(f(x)) \\
&= g_1(f(x)) + g_2(f(x)) \\
&= (g_1 \circ f)(x) + (g_2 \circ f)(x) \\
&= [f^*(g_1)](x) + [f^*(g_2)](x) \\
&= [f^*(g_1) + f^*(g_2)](x)
\end{aligned}$$

as desired.

Let $g_1, g_2 \in R^Y$ be arbitrary. Then we have for any $x \in X$ that

$$\begin{aligned}
[f^*(g_1 \times g_2)](x) &= [(g_1 \times g_2) \circ f](x) \\
&= (g_1 \times g_2)(f(x)) \\
&= g_1(f(x)) \times g_2(f(x)) \\
&= (g_1 \circ f)(x) \times (g_2 \circ f)(x) \\
&= [f^*(g_1)](x) \times [f^*(g_2)](x) \\
&= [f^*(g_1) \times f^*(g_2)](x)
\end{aligned}$$

as desired.

Let $1_{R^Y} : Y \to R$ denote the identity of R^Y, that is, the constant function evaluating to 1_R at every $y \in Y$. Then for any $x \in X$,

$$[f^*(1_{R^Y})](x) = (1_{R^Y} \circ f)(x) = 1_{R^Y}(f(x)) = 1_R$$

where the last equality holds by the definition of 1_{R^Y} since $f(x) \in Y$. Thus, since $f^*(1_{R^Y}) : X \to R$ sends every $x \in X$ to 1_R, it must be equal to 1_{R^X} by the definition of the latter, as desired. □

1.3. Let $Y \subset X$. Define $\phi : R^Y \to R^X$ by the following rule: For any function $g : Y \to R \in R^Y$, let $\phi(g) : X \to R$ send

$$x \mapsto \begin{cases} g(x) & x \in Y \\ 0 & x \notin Y \end{cases}$$

State whether the assertions (i) and (ii) below are *true* or *false*. No proof required.

Warning: Make sure to use the definitions of "ring homomorphism" and "subring" from class!

(i) ϕ is a ring homomorphism.

Answer. False[1]. □

(ii) The image of ϕ is a subring of R^X.

Answer. False[2]. □

1.4. For any ring R, define the set $\Delta(R)$ by

$$\Delta(R) = \{(a, a) : a \in R\}$$

Note that $\Delta(R)$ is a subring of $R \times R$. Prove that if B is a subring of $\mathbb{Q} \times \mathbb{Q}$ that contains $\Delta(\mathbb{Q})$, then B is either $\Delta(\mathbb{Q})$ or $\mathbb{Q} \times \mathbb{Q}$.

Proof. We divide into two cases ($B = \Delta(\mathbb{Q})$ and $B \neq \Delta(\mathbb{Q})$). In the first case, we are immediately done. In the second case, start with the observation that if $\Delta(\mathbb{Q}) \subsetneq B$, then there exists $x \in B$ such that $x \notin \Delta(\mathbb{Q})$. It follows from class that the smallest subring of $\mathbb{Q} \times \mathbb{Q}$ containing $\Delta(\mathbb{Q})$ and $x \notin \Delta(\mathbb{Q})$ is $\Delta(\mathbb{Q})[x]$. Thus, showing that $\Delta(\mathbb{Q})[x] = \mathbb{Q} \times \mathbb{Q}$ will complete the proof.

We proceed via a bidirectional inclusion proof. Suppose first that $p \in \Delta(\mathbb{Q})[x]$. Each term $a_i x^i$ in p is the finite product of elements of $\mathbb{Q} \times \mathbb{Q}$, and thus is an element of $\mathbb{Q} \times \mathbb{Q}$ itself (since $\mathbb{Q} \times \mathbb{Q}$ is a closed ring). It follows that p is the finite sum of elements of $\mathbb{Q} \times \mathbb{Q}$ and hence is also an element of $\mathbb{Q} \times \mathbb{Q}$, as desired. Now suppose that $(q_1, q_2) \in \mathbb{Q} \times \mathbb{Q}$. Let $x = (x_1, x_2)$. Then[3]

$$\begin{aligned}(q_1, q_2) &= \left(\frac{q_2x_1 - q_1x_2}{x_1 - x_2} + \frac{q_1 - q_2}{x_1 - x_2} \cdot x_1, \frac{q_2x_1 - q_1x_2}{x_1 - x_2} + \frac{q_1 - q_2}{x_1 - x_2} \cdot x_2\right) \\ &= \underbrace{\left(\frac{q_2x_1 - q_1x_2}{x_1 - x_2}, \frac{q_2x_1 - q_1x_2}{x_1 - x_2}\right)}_{a_0} + \underbrace{\left(\frac{q_1 - q_2}{x_1 - x_2}, \frac{q_1 - q_2}{x_1 - x_2}\right)}_{a_1} \cdot (x_1, x_2) \\ &\in \Delta(\mathbb{Q})[x]\end{aligned}$$

as desired. Note that a_0, a_1 defined above are elements of $\Delta(\mathbb{Q})$ since $x_1 - x_2 \neq 0$ by hypothesis for this element not in $\Delta(\mathbb{Q})$. □

Basic Properties

1.7. Let $f : R_1 \to R_2$ be a ring homomorphism, and let R_3 be a subring of R_2. Prove that $f^{-1}(R_3)$ is a subring of R_1.

Proof. To prove that $f^{-1}(R_3) \subset R_1$ is a subring, it will suffice to show that it is closed under addition, multiplication, and additive inverses, and that $1_{R_1} \in f^{-1}(R_3)$. Let's begin.

Let $a, b \in f^{-1}(R_3)$ be arbitrary. Then $f(a), f(b) \in R_3$. It follows that $f(a) + f(b) \in R_3$, hence $f(a + b) \in R_3$ since $f(a + b) = f(a) + f(b)$. Therefore, $a + b \in f^{-1}(R_3)$, as desired.

[1] $\phi(1_{R^Y}) \neq 1_{R^X}$ if $Y \subsetneq X$.

[2] $\phi(R^Y)$ does not contain an identity unless $Y = X$.

[3] Derivation: Solve $(a, a) + (b, b)(x_1, x_2) = (q_1, q_2)$. Geometrically, this problem is equivalent to identifying $\Delta(\mathbb{Q})$ with the subspace $y = x$ of $\mathbb{R}^2$ and noting that we only need one additional linearly independent element (x_1, x_2) where $x_1 \neq x_2$ to allow us to reach every other point in $\mathbb{R}^2$.

An analogous argument holds for closure under multiplication.

Let $a \in f^{-1}(R_3)$ be arbitrary. Then $f(a) \in R_3$. It follows that $-f(a) \in R_3$, hence $f(-a) \in R_3$ since $f : (R_1, +) \to (R_2, +)$ being a group homomorphism means that

$$\begin{aligned} f(0) &= 0 \\ f(a + (-a)) &= 0 \\ f(a) + f(-a) &= 0 \\ -f(a) + f(a) + f(-a) &= -f(a) + 0 \\ f(-a) &= -f(a) \end{aligned}$$

Therefore, $-a \in f^{-1}(R_3)$, as desired.

Since f is a ring homomorphism, $f(1_{R_1}) = 1_{R_2}$. Since R_3 is a subring of R_2, $1_{R_2} \in R_3$. Therefore, $1_{R_1} \in f^{-1}(R_3)$, as desired. □

1.9. Show that $A \cap B$ is a subring of R if both A, B are subrings of R.

Proof. Suppose $A, B \subset R$ are subrings. To prove that $A \cap B$ is a subring, it will suffice to show that it is closed under addition, multiplication, and additive inverses, and that $1_R \in A \cap B$. Let's begin.

Let $a, b \in A \cap B$ be arbitrary. Then $a, b \in A$ and $a, b \in B$. It follows from the closure of A under addition (resp. multiplication, additive inverses) that $a + b, ab, -a \in A$. Analogously, $a + b, ab, -a \in B$. Therefore, $a + b, ab, -a \in A \cap B$, as desired.

Since A, B are subrings, $1_R \in A, B$. Therefore, $1_R \in A \cap B$, as desired. □

Recall the following lemma from MATH 25700: Let $(A, +)$ be an abelian group, and let $a \in A$. Then there is a unique group homomorphism $f : \mathbb{Z} \to A$ such that $f(1) = a$. Additionally, $f(n) = na$ for all $n \in \mathbb{Z}$.

1.10. Let 1_R denote the multiplicative identity of a ring R. The above lemma then defines $na \in R$ for every $a \in R$ and $n \in \mathbb{Z}$. In particular, we define $n_R = n(1_R)$ for every integer $n \in \mathbb{Z}$. Prove that $n_R \cdot a = na$ for every $a \in R$ and $n \in \mathbb{Z}$.

Proof. Let $a \in R$ and $n \in \mathbb{Z}$ be arbitrary. We divide into three cases ($n > 0$, $n = 0$, and $n < 0$). If $n > 0$, then we have by iterating the distributive law that

$$n_R \cdot a = \underbrace{(1_R + \cdots + 1_R)}_{n \text{ times}} \cdot a = \underbrace{(1_R \cdot a) + \cdots + (1_R \cdot a)}_{n \text{ times}} = \underbrace{a + \cdots + a}_{n \text{ times}} = na$$

as desired. If $n = 0$, then $n_R = 0(1_R) = 0_R$. Thus,

$$n_R \cdot a = 0_R \cdot a = 0 = 0a = na$$

as desired. If $n < 0$, then $n_R = -1 \cdot (-n_R)$, where $-n_R > 0$. Thus, apply case 1 and factor the -1 back in at the end. □

1.11. With notation as above, show that $f : \mathbb{Z} \to R$ given by $f(n) = n_R$ is a ring homomorphism.

Proof. To prove that f is a ring homomorphism, it will suffice to check that $f(n+m) = f(n) + f(m)$ and $f(nm) = f(n)f(m)$ for all $n, m \in \mathbb{Z}$, and $f(1) = 1_R$. Let's begin.

Let $n, m \in \mathbb{Z}$ be arbitrary. Then

$$\begin{aligned} f(n+m) &= (n+m)_R \\ &= (n+m) \cdot 1_R \\ &= \underbrace{1_R + \cdots + 1_R}_{n+m \text{ times}} \\ &= \underbrace{1_R + \cdots + 1_R}_{n \text{ times}} + \underbrace{1_R + \cdots + 1_R}_{m \text{ times}} \\ &= n(1_R) + m(1_R) \\ &= n_R + m_R \\ &= f(n) + f(m) \end{aligned}$$

as desired. Note that this only treats the case $n, m > 0$; all other would have to be addressed in extended casework, similar to what was done in Exercise 1.10.

Let $n, m \in \mathbb{Z}$ be arbitrary. Then

$$\begin{aligned} f(nm) &= (nm)_R \\ &= (nm) \cdot 1_R \\ &= \sum_{i=1}^{nm} 1_R \\ &= \sum_{i=1}^{n} \sum_{i=1}^{m} 1_R \\ &= \sum_{i=1}^{n} m(1_R) \\ &= n \cdot m(1_R) \\ &= n_R \cdot m(1_R) && \text{Problem 1.10} \\ &= n_R \cdot m_R \\ &= f(n)f(m) \end{aligned}$$

as desired. Same as before with the extra casework for negative numbers[4].

By definition, f is the unique homomorphism sending $1 \mapsto 1_R$, as desired. □

The commutativity of a ring is required for all the identities of high school algebra. The next two problems (1.12 and 1.13) are instances.

1.12. Prove that the following are equivalent.

(i) R is a commutative ring.
(ii) $(a+b)(a-b) = a^2 - b^2$ for all $a, b \in R$.
(iii) $(a+b)^2 = a^2 + 2ab + b^2$ for all $a, b \in R$.

Proof.
(i) ⇒ (ii): Suppose R is a commutative ring, and let $a, b \in R$ be arbitrary. Then by the ring axioms (e.g., distributive law, etc.),

$$(a+b)(a-b) = a(a+(-b)) + b(a+(-b)) = aa + a(-b) + ba + b(-b) = a^2 - ab + ab - b^2 = a^2 - b^2$$

as desired.

[4]For full credit in this problem, I would have to show more of this casework.

(ii) ⇒ (iii): Suppose $(a+b)(a-b) = a^2 - b^2$ for all $a, b \in R$. Then

$$\begin{aligned} a^2 - b^2 &= a^2 - ab + ba - b^2 \\ ab &= ba \end{aligned}$$

Thus,

$$(a+b)^2 = (a+b)(a+b) = a(a+b) + b(a+b) = aa + ab + ba + bb = aa + ab + ab + bb = a^2 + 2ab + b^2$$

as desired.

(iii) ⇒ (i): Suppose $(a+b)^2 = a^2 + 2ab + b^2$ for all $a, b \in R$. Let $a, b \in R$ be arbitrary. Then

$$\begin{aligned} a^2 + ab + ab + b^2 &= a^2 + ab + ba + b^2 \\ ab &= ba \end{aligned}$$

so a, b commute. Therefore, R is commutative, as desired. □

1.14. For this problem, you only have to state whether each of the nine assertions (i), . . . , (ix) is *true* or *false*. No proofs are required.

Given sets X, Y, the set of all functions $f : Y \to X$ is denoted by X^Y. Let $(A, +)$ be an abelian group. Given functions $f, g : Y \to A$, define $f + g : Y \to A$ by pointwise addition, i.e., let

$$(f+g)(y) = f(y) + g(y)$$

for all $y \in Y$.

(i) The above binary operation + on A^Y gives A^Y the structure of an abelian group.

Answer. True. □

For (ii) and (iii) below, we continue with $Y = A$ where $(A, +)$ is an abelian group. In an attempt to give A^A the structure of a ring — for functions $f, g : A \to A$ — we take $\circ$ as the second binary operation. Here, $(f \circ g)(a) = f(g(a))$ for all $a \in A$.

(ii) The right distributive law, i.e., $(f+g) \circ h = f \circ h + g \circ h$ holds for all functions $f, g, h : A \to A$.

Answer. True. □

(iii) The left distributive law, i.e., $f \circ (g+h) = f \circ g + f \circ h$ holds for all functions $f, g, h : A \to A$.

Answer. False. □

(iv) The identity function $\mathrm{id}_A : A \to A$ given by $\mathrm{id}_A(a) = a$ for all $a \in A$ satisfies

$$\mathrm{id}_A \circ f = f = f \circ \mathrm{id}_A$$

for all $f : A \to A$.

Answer. True. □

If you have solved the above problems correctly, you would have seen that $(A^A, +, \circ)$ is *not* a ring. In an endeavor to produce a ring employing the same binary operations + and $\circ$, we replace A^A by its subset $\mathrm{End}(A) = \{f : A \to A : f \text{ is a group homomorphism}\}$.

(v) For $f, g \in \mathrm{End}(A)$, both $f + g$ and $f \circ g$ belong to $\mathrm{End}(A)$.

Answer. True. □

(vi) The left and right distributive laws hold for $(\mathrm{End}(A), +, \circ)$.

Answer. True. □

(vii) $(\mathrm{End}(A), +, \circ)$ is a ring (with two-sided multiplicative identity).

Answer. True. □

(viii) $(\mathrm{End}(A), +, \circ)$ is a commutative ring for all abelian groups $(A, +)$.

Answer. False[5]. □

(ix) If $A = \mathbb{Z} \times \mathbb{Z}$, then $\mathrm{End}(A)$ is isomorphic to the ring of 2×2 matrices with integer coefficients.

Answer. True[6]. □

[5]Counterexample: Let K denote the Klein 4-group. Define $f, g \in \mathrm{End}(K)$ by $(x, y) \mapsto (0, x)$ and $(x, y) \mapsto (0, y)$, respectively. Then f, g are group homomorphisms, but $(f \circ g)(1, 0) = (0, 0) \neq (0, 1) = (g \circ f)(1, 0)$, so $f \circ g \neq g \circ f$, as desired.

[6]Since matrices are linear transformations, they are group homomorphisms. On the other hand, any $f \in \mathrm{End}(A)$ respects addition (as a homomorphism) and scalar multiplication (since $af = f + \cdots + f$ a times for any $a \in \mathbb{Z}$). Thus, any endomorphism on $\mathbb{Z} \times \mathbb{Z}$ is a linear transformation and hence has a matrix representation.

2 Ideals and Vector Spaces

Problems from the Textbook

1/18: **2.1.** Exercise 7.1.9 of Dummit and Foote (2004): For a fixed element $a \in R$, define

$$C(a) = \{r \in R \mid ra = ar\}$$

Prove that $C(a)$ is a subring of R containing a. Prove that the center of R is the intersection of the subrings $C(a)$ over all $a \in R$.

Proof. Since $a \in R$ and $aa = aa$ by reflexivity, $C(a)$ contains a.

To prove that $C(a)$ is a subring of R, it will suffice to show that $C(a)$ is closed under addition, multiplication, and inverses, and that $1_R \in C(a)$. Let's begin.

Addition: Let $r, s \in C(a)$ be arbitrary. As elements of $C(a)$, we know that $ra = ar$ and $sa = as$. It follows by the additive property of equality and the distributive law for rings that

$$ra + sa = ar + as$$
$$(r + s)a = a(r + s)$$

Therefore, $r + s \in C(a)$, as desired.

Multiplication: This argument is analogous to the previous one, except that the critical step is

$$(rs)a = r(sa) = r(as) = (ra)s = (ar)s = a(rs)$$

Inverses: Likewise, this argument is analogous to the previous two, except that the critical step is

$$(-r)a = -(ra) = -(ar) = a(-r)$$

Identity: We have by the definition of the multiplicative identity that

$$a = 1_R a = a1_R$$

where the second equality above gives the desired result.

As defined in Exercise 7.1.7 of Dummit and Foote (2004), the center of R is the set

$$Z(R) = \{z \in R \mid zr = rz \ \forall \ r \in R\}$$

We will prove that

$$Z(R) = \bigcap_{a \in R} C(a)$$

via a bidirectional inclusion proof. Suppose first that $z \in Z(R)$. To confirm that $z \in \bigcap_{a \in R} C(a)$, it will suffice to determine if $z \in C(a)$ for all $a \in R$. Let $a \in R$ be arbitrary. By the definition of $Z(R)$, $za = az$. Thus, by the definition of $C(a)$, $z \in C(a)$, as desired. Now suppose that $z \in \bigcap_{a \in R} C(a)$. To confirm that $z \in Z(R)$, it will suffice to determine if $zr = rz$ for all $r \in R$. Let $r \in R$ be arbitrary. By hypothesis, $z \in C(r)$. Thus, $zr = rz$, as desired. □

2.2. Exercise 7.2.3(b-c) of Dummit and Foote (2004): Define the set $R[[X]]$ of **formal power series** in the indeterminate X with coefficients from R to be all formal infinite sums

$$\sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots$$

Define addition and multiplication of power series in the same way as for power series with real or complex coefficients, i.e., extend polynomial addition and multiplication to power series as though they were "polynomials of infinite degree:"

$$\left(\sum_{n=0}^{\infty} a_n x^n\right) + \left(\sum_{n=0}^{\infty} b_n x^n\right) = \sum_{n=0}^{\infty} (a_n + b_n) x^n$$
$$\left(\sum_{n=0}^{\infty} a_n x^n\right) \times \left(\sum_{n=0}^{\infty} b_n x^n\right) = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k b_{n-k}\right) x^n$$

(The term "formal" is used here to indicate that convergence is not considered, so that formal power series need not represent functions on R.)

(b) Show that $1 - x$ is a unit in $R[[X]]$ with inverse $1 + x + x^2 + \cdots$.

Proof. Note that

$$1 - x = \sum_{n=0}^{\infty} a_n x^n \qquad\qquad 1 + x + x^2 + \cdots = \sum_{n=0}^{\infty} b_n x^n$$

under the definitions

$$a_n = \begin{cases} 1 & n = 0 \\ -1 & n = 1 \\ 0 & n \geq 2 \end{cases} \qquad\qquad b_n = 1$$

Thus, both objects are elements of $R[[X]]$. All that remains is to show that

$$(1 - x)\left(\sum_{n=0}^{\infty} x^n\right) = 1$$

Invoking the definition of multiplication on formal power series, we have that the above equals

$$\sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k 1\right) x^n = 1 + \sum_{n=1}^{\infty} \left[(1)(1) + (-1)(1) + \sum_{k=2}^{n} (0)(1)\right] x^n = 1 + \sum_{n=1}^{\infty} 0x^n = 1$$

as desired. □

(c) Prove that $\sum_{n=0}^{\infty} a_n x^n$ is a unit in $R[[X]]$ iff a_0 is a unit in R.

Proof. Suppose first that $\sum_{n=0}^{\infty} a_n x^n$ is a unit in $R[[X]]$. Then there exists some $\sum_{n=0}^{\infty} b_n x^n \in R[[X]]$ such that

$$1 = \left(\sum_{n=0}^{\infty} a_n x^n\right)\left(\sum_{n=0}^{\infty} b_n x^n\right)$$
$$1 + \sum_{n=1}^{\infty} 0x^n = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k b_{n-k}\right) x^n$$

It follows by comparing terms that we must have $a_0 b_0 = 1$. Therefore, a_0 is a unit in R.

Now suppose that a_0 is a unit in R. Let $\sum_{n=0}^{\infty} a_n x^n$ be a polynomial in $R[[X]]$ having a_0 as its constant term. To prove that $\sum_{n=0}^{\infty} a_n x^n$ is a unit in $R[[X]]$, it will suffice to find a polynomial $\sum_{n=0}^{\infty} b_n x^n \in R[[X]]$ such that

$$\left(\sum_{n=0}^{\infty} a_n x^n\right)\left(\sum_{n=0}^{\infty} b_n x^n\right) = 1$$

To construct such a polynomial, we recursively define $b_0, b_1, \ldots$ using strong induction. For the base case b_0, let this be the element of R that makes $a_0 b_0 = 1$ (such an element is guaranteed to exist by the supposition that a_0 is a unit in R). Now suppose inductively that we have defined $b_0, \ldots, b_{n-1}$. We define b_n via

$$b_n = -b_0 \sum_{k=1}^{n} a_k b_{n-k}$$

It follows from this definition that

$$\begin{aligned}
\left(\sum_{n=0}^{\infty} a_n x^n\right)\left(\sum_{n=0}^{\infty} b_n x^n\right) &= \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n} a_k b_{n-k}\right) x^n \\
&= a_0 b_0 X^0 + \sum_{n=1}^{\infty}\left(a_0 b_n + \sum_{k=1}^{n} a_k b_{n-k}\right) x^n \\
&= 1 \cdot 1 + \sum_{n=1}^{\infty}\left(-a_0 b_0 \sum_{k=1}^{n} a_k b_{n-k} + \sum_{k=1}^{n} a_k b_{n-k}\right) x^n \\
&= 1 + \sum_{n=1}^{\infty}\left(-1 \sum_{k=1}^{n} a_k b_{n-k} + \sum_{k=1}^{n} a_k b_{n-k}\right) x^n \\
&= 1
\end{aligned}$$

as desired. □

2.3. Exercise 7.3.24 of Dummit and Foote (2004): Let $\varphi : R \to S$ be a ring homomorphism.

(a) Prove that if J is an ideal of S, then $\varphi^{-1}(J)$ is an ideal of R. Apply this to the special case when R is a subring of S and φ is the inclusion homomorphism to deduce that if J is an ideal of S, then $J \cap R$ is an ideal of R.

Proof. Let $I = \varphi^{-1}(J)$. To prove that I is an ideal of R, it will suffice to show that $(I, +) \leq (R, +)$, and $aI \subset I$ and $Ia \subset I$ for all $a \in R$. Let's begin.
Since $\varphi : (R, +) \to (S, +)$ is a group homomorphism and $J \leq S$, the preimage $I = \varphi^{-1}(J)$ is a subgroup of $(R, +)$ — see Exercise 3.1.1 of Dummit and Foote (2004) for further justification. Moving on, let $a \in R$ and $i \in I$ be arbitrary. It follows by the definition of I that $\varphi(i) = j$ for some $j \in J$. Thus, $\varphi(ai) = \varphi(a)\varphi(i) = \varphi(a)j \in J$ since φ is a ring homomorphism, $\varphi(a) \in S$, and J is an ideal of S. Therefore, $ai \in \varphi^{-1}(J) = I$, as desired. An analogous argument verifies that $Ia \subset I$ for all $a \in R$.

Now let R be a subring of S and $\varphi = i$ be the canonical injection. By the above result, $i^{-1}(J)$ is an ideal of R. Thus, to prove that $J \cap R$ is an ideal of R, it will suffice to show that $J \cap R = i^{-1}(J)$. Let $I = i^{-1}(J)$. Since i is the inclusion map, $I = i^{-1}(J)$ is the set of all $r \in R$ such that $r = i(r) \in J$. In other words, if $r \in I$, then $r \in R$ and $r \in J$; thus, $I \subset J \cap R$. On the other hand, if $r \in J \cap R$, then $r \in J$ and $r \in R$. Since $r \in R$, $r = i(r)$. This combined with the fact that $r \in J$ implies that $i(r) = r \in J$. Thus, $r \in i^{-1}(J)$, so $J \cap R \subset I$, as desired. □

(b) Prove that if φ is surjective and I is an ideal of R, then $\varphi(I)$ is an ideal of S. Give an example where this fails if φ is not surjective.

Proof. To prove that $J = \varphi(I)$ is an ideal of S, it will suffice to show that $(J, +) \leq (S, +)$, and $bJ \subset J$ and $Jb \subset J$ for all $b \in S$. Let's begin.
Since $(I, +) \leq (R, +)$, we can define a restricted group homomorphism $\varphi : (I, +) \to (S, +)$. It follows from Proposition 3.1 of Dummit and Foote (2004) that the image $(J, +) = \varphi(I)$ is a subgroup of $(S, +)$, as desired. Moving on, let $b \in S$ and $j \in J$ be arbitrary. Since $b \in S$ and φ is surjective, there exists $a \in R$ such that $\varphi(a) = b$. Since $j \in J$, there exists $i \in I$ such that $\varphi(i) = j$. Since I is an ideal of R, $i \in I$, and $a \in R$, we know that $ai \in I$. Thus,

$$bj = \varphi(a)\varphi(i) = \varphi(ai) \in J$$

Therefore, $bJ \subset J$, as desired. An analogous argument verifies that $Jb \subset J$ for all $b \in S$.

Consider $\varphi : \mathbb{Z} \to \mathbb{Z}$ defined by $\varphi(z) = z \bmod 3$. Then $\varphi(2\mathbb{Z}) = \{0, 1, 2\}$. Taking $a = 2$, for example, shows that $\varphi(2\mathbb{Z})$ is not closed under multiplication since $a2 = 4 \notin \varphi(2\mathbb{Z})$. □

2.4. Exercise 7.4.27 of Dummit and Foote (2004): Let R be a commutative ring with $1 \neq 0$. Prove that if a is a nilpotent element of R, then $1 - ab$ is a unit for all $b \in R$.

Proof. Let $b \in R$ be arbitrary. To prove that $1 - ab$ is a unit in R commutative, it will suffice to find a $v \in R$ such that $(1 - ab)v = 1$. Since a is nilpotent, there exists $m \in \mathbb{N}$ such that $a^m = 0$. Thus, let

$$v = \sum_{k=0}^{m-1} (ab)^k$$

Then

$$\begin{aligned}(1 - ab)v &= 1 + ab + \cdots + (ab)^{m-1} - ab - (ab)^2 - \cdots - (ab)^m \\ &= 1 - (ab)^m \\ &= 1 - a^m b^m \\ &= 1 - 0 \cdot b^m \\ &= 1\end{aligned}$$

as desired. □

2.5. Exercise 7.4.33 of Dummit and Foote (2004): Let R be the ring of all continuous functions from the closed interval $[0, 1]$ to $\mathbb{R}$, and for each $c \in [0, 1]$, let $M_c = \{f \in R \mid f(c) = 0\}$. (Recall that M_c was shown to be a maximal ideal of R.)

(a) Prove that if M is any maximal ideal of R, then there is a real number $c \in [0, 1]$ such that $M = M_c$.

Proof. Let M be an arbitrary maximal ideal of R, and suppose for the sake of contradiction that $M \neq M_c$ for any $c \in [0, 1]$. We now divide into two cases ($M \subset M_c$ for some $c \in [0, 1]$ and $M \not\subset M_c$ for any $c \in [0, 1]$). If $M \subset M_c$ for some $c \in [0, 1]$, then since M is a maximal ideal, $M = M_c$, a contradiction. We devote the remainder of this proof to a treatment of the other case. In this treatment, we will construct a function $h \in M$ that is a unit, which will imply a contradiction by the results of Section 7.4.

We first define a set of functions $\{f_c\} \subset M$ that we will later deform and combine into h. Suppose $M \not\subset M_c$ for any $c \in [0, 1]$. Then for all $c \in [0, 1]$, there exists $f_c \in M$ such that $f_c(c) \neq 0$. Moreover, we may take $f_c(c) > 0$ WLOG: If $f_c(c) < 0$, then since M is an ideal, $-1_R \cdot f_c \in M$ and $(-1_R \cdot f_c)(c) > 0$, so we may redefine $f_c := -f_c$. This combined with the continuity of each f_c implies by Lemma 11.8[7] that to every $c \in [0, 1]$, there corresponds a region $G_c = (c - \delta_c, c + \delta_c)$ such that $f_c > 0$ for all $c \in G_c \cap [0, 1]$.

We now construct the deforming functions. It follows from the above that the set

$$\mathcal{G} = \{G_c \mid c \in [0, 1]\}$$

is an open cover of $[0, 1]$. This combined with the fact that $[0, 1]$ is compact by Theorem 10.14[8] implies that there exists a finite subcover $\mathcal{G}' \subset \mathcal{G}$; in particular, there exists a finite subset $K \subset [0, 1]$ such that

$$\mathcal{G}' = \{G_c \mid c \in K\}$$

[7] From Honors Calculus IBL.
[8] From Honors Calculus IBL.

is an open cover of $[0,1]$. Now for each $c \in K$, define $g_c \in R$ by

$$x \mapsto \begin{cases} 1 - \frac{1}{\delta_c}|x-c| & x \in G_c \cap [0,1] \\ 0 & \text{otherwise} \end{cases}$$

Lastly, we construct h. In particular, let

$$h = \sum_{c \in K} g_c f_c$$

Since M is an ideal of R, each $f_c \in M$, and each $g_c \in R$, it follows from its definition that $h \in M$. We now show that h is positive on $[0,1]$. Let $x \in [0,1]$ be arbitrary. Since $\mathcal{G}'$ covers $[0,1]$, $x \in G_c$ for some $c \in K$. It follows by the above that both $f_c(x), g_c(x) > 0$; hence, $(f_c g_c)(x) > 0$. This combined with the fact that every $f_c g_c : [0,1] \to \mathbb{R}_{\geq 0}$ by definition implies that $h(x) > 0$, as desired.

It follows that $h \in M$ is a unit with inverse $1/h \in M$ (multiply $h \in M$ by $1/h^2 \in R$). Thus, by Proposition 9(1), $M = R$. In particular, $M \subsetneq R$, so M is not a maximal ideal, a contradiction. □

(b) Prove that if b, c are distinct points in $[0,1]$, then $M_b \neq M_c$.

Proof. To prove that $M_b \neq M_c$, it will suffice to find $f \in M_b$ such that $f \notin M_c$. Let $f \in R$ be defined by

$$x \mapsto x - b$$

Since $f(b) = b - b = 0$, $f \in M_b$. However, since $f(c) = c - b \neq 0$, $f \notin M_c$, as desired. □

(c) Prove that M_c is not equal to the principal ideal generated by $x - c$.

Proof. To prove that $M_c \neq R(x-c)$, it will suffice to show that there exists $f \in M_c$ such that $f \notin R(x-c)$. Pick $f = |x-c|$. We have that $f(c) = |c-c| = 0$, so $f \in M_c$. Now suppose for the sake of contradiction that $g \in R$ satisfies $f(x) = g(x) \cdot (x-c)$. Then we must have

$$g(x) = \frac{|x-c|}{x-c} = \begin{cases} -1 & x < c \\ a & x = c \\ 1 & x > c \end{cases}$$

for some $a \in \mathbb{R}$. But no matter which a we pick, g will still be discontinuous and hence not be an element of R, a contradiction. □

(d) Prove that M_c is not a finitely generated ideal.

Proof. The motivation for many of the steps in this argument will not become clear until the very end. Essentially, we wish to construct a function from the generators that is zero only at c. We then modify this function slightly, allowing us to express it in terms of the generators. Lastly, we show that the supposedly continuous left multipliers in R imply the existence of a discontinuous function in R. Let's begin.

Suppose for the sake of contradiction that $M_c = (A)$, where $A = \{a_i \mid 1 \leq i \leq n\}$ for some $a_i : [0,1] \to \mathbb{R}$. Let $f = \sum_{i=1}^n |a_i|$. By the definition of the square root, $\sqrt{f} \in R$ and $\sqrt{f} \in M_c$. It follows from the latter statement that $\sqrt{f} = \sum_{i=1}^n r_i a_i$ for some $r_i \in R$. Let $r = \sum_{i=1}^n |r_i|$. Then

$$\begin{aligned} \sqrt{f(x)} &= \sum_{i=1}^n r_i(x) a_i(x) \\ &\leq \sum_{i=1}^n |r_i(x)| \cdot |a_i(x)| \\ &\leq r(x) f(x) \\ \frac{1}{\sqrt{f(x)}} &\leq r(x) \end{aligned}$$

We know that f is nonzero in the region surrounding (but excluding) c: To guarantee that we can access functions in M_c that are nonzero at every $x \in [0,1]$ not equal to c, we need $a_i(x) \neq 0$ for at least one $i \in [n]$ and for all $x \in [0,1]$. Thus, as $x \to c^+$, the above inequality implies that $r(x) \to +\infty$. But this means that r has a discontinuity at x, contradicting its definition as a necessarily continuous sum of continuous functions. □

The preceding exercise shows that there is a bijection between the *points* of the closed interval $[0,1]$ and the set of *maximal ideals* in the ring R of all continuous functions on $[0,1]$ given by $c \leftrightarrow M_c$. For any subset $X \subset \mathbb{R}$ or, more generally, for any completely regular topological space X, the map $c \mapsto M_c$ is an injection from X to the set of maximal ideals of R, where R is the ring of all bounded, continuous, real-valued functions on X and M_c is the maximal ideal of functions that vanish at c. Let $\beta(X)$ be the set of maximal ideals of R. One can put a topology on $\beta(X)$ in such a way that if we identify X with its image in $\beta(X)$, then X (in its given topology) becomes a subspace of $\beta(X)$. Moreover, $\beta(X)$ is a compact space under this topology and is called the **Stone-Čech compactification** of X.

2.6. Exercise 7.4.34 of Dummit and Foote (2004): Let R be the ring of all continuous functions from $\mathbb{R}$ to $\mathbb{R}$, and for each $c \in \mathbb{R}$, let M_c be the maximal ideal $\{f \in R \mid f(c) = 0\}$.

(a) Let I be the collection of functions $f \in R$ with **compact support** (i.e., $f(x) = 0$ for $|x|$ sufficiently large). Prove that I is an ideal of R that is not a prime ideal.

Proof. To prove that I is an ideal of R, it will suffice to show that $(I,+) \leq (R,+)$ and $aI \subset I$ for all $a \in R$.

Subgroup: Since $0 \in I$, I is nonempty. Adding any two functions with compact support yields a third since the zero values at the extremes add to zero, so I is closed under addition. If f has compact support, then $-f$ will still evaluate to zero at the extremes; hence, I has inverses.

Ideal condition: Let $a \in R$ and $i \in I$ be arbitrary. Since i evaluates to zero for sufficiently large x, so will ai. Therefore, $aI \subset I$ for all $a \in I$, as desired.

Let $a \in R$ be a modification of the triangle wave, specifically one with each triangle spaced apart by a zero gap. Let $b \in R$ be the same wave but offset so that the positive areas of b overlap with the zero areas of a. Formally, let the unit cell of each function be

$$a(x) = \begin{cases} 0.25 - |x - 0.25| & x \in [0, 0.5] \\ 0 & x \in [0.5, 1] \end{cases} \qquad b(x) = \begin{cases} 0 & x \in [0, 0.5] \\ 0.25 - |x - 0.75| & x \in [0.5, 1] \end{cases}$$

and let them satisfy the periodicity relations

$$a(x+1) = a(x) \qquad\qquad b(x+1) = b(x)$$

Then $ab = 0$, which is compactly supported, but neither a nor b is compactly supported in its own right. Therefore, I is not a prime ideal, as desired. □

(b) Let M be a maximal ideal of R containing I (properly, by part (a)). Prove that $M \neq M_c$ for any $c \in \mathbb{R}$ (refer to the preceding exercise).

Proof. Let $c \in \mathbb{R}$ be arbitrary. To prove that $M \neq M_c$, it will suffice to show that there exists $f \in M$ such that $f \notin M_c$. Define f by

$$f(x) = \begin{cases} 1 - |x - c| & x \in [c-1, c+1] \\ 0 & \text{otherwise} \end{cases}$$

Clearly, f has compact support, so $f \in I \subset M$. However, $f(c) = 1 \neq 0$, so $f \notin M_c$, as desired. □

Custom Questions

The first problem below is analogous to Corollary 3 on Dummit and Foote (2004, p. 228), where it is shown that any finite integral domain is a field.

2.7. Let R be a commutative ring, and F be a subring of R that is a field. Then R acquires the structure of a vector space over the field F. Assume now that R is a finite dimensional vector space over F. Show that if R is an integral domain, then R is a field.

Proof. We already know that R is a commutative ring. Thus, to prove that R is a field, it only remains to show that $0_R \neq 1_R$, and $a \in R$ nonzero implies that there exists $b \in R$ such that $ab = 1$. Let's begin.

Since R is an integral domain, $0_R \neq 1_R$, as desired.

Let $a \in R$ nonzero be arbitrary. Consider the map $l_a : R \to R$. Since R is an integral domain, the cancellation law holds, so we may write

$$l_a(r) = l_a(s) \quad \implies \quad ar = as \quad \implies \quad r = s$$

Thus, l_a is injective. It follows that $\ker(l_a) = \{0\}$. Now, viewing R as a finite dimensional vector space over F, we can show that l_a is a linear transformation.

$$\begin{aligned} l_a(r+s) &= a(r+s) \\ &= ar + as \\ &= l_a(r) + l_a(s) \end{aligned} \qquad \begin{aligned} l_a(fr) &= afr \\ &= far \\ &= f l_a(r) \end{aligned}$$

Hence, by fundamental theorem of linear algebra,

$$\begin{aligned} \dim R &= \dim \ker(l_a) + \dim \operatorname{im}(l_a) \\ &= 0 + \dim \operatorname{im}(l_a) \\ &= \dim \operatorname{im}(l_a) \end{aligned}$$

It follows that l_a is surjective. Therefore, we know in particular that there exists b such that $l_a(b) = 1$. By the definition of l_a, this means that $ab = 1$, as desired. □

2.8. Give an example to show that the hypothesis of finite dimensionality cannot be dropped in the previous problem.

Proof. Consider

$$\boxed{R = \mathbb{Q}[X] \text{ and } F = \mathbb{Q}}$$

These objects satisfy all of the necessary hypotheses. However, $\mathbb{Q}[X]$ is still not a field: Consider $X \in \mathbb{Q}[X]$, for instance. We know that $\deg(X) = 1$, $\deg(fg) = \deg(f) + \deg(g)$, and $\deg(1) = 0$, so there is no polynomial $g \in \mathbb{Q}[X]$ such that $gX = 1$. □

2.9. Let V be a finite dimensional vector space over a field F, and let $\operatorname{End}_F(V)$ denote the set of linear transformations $T : V \to V$.

(a) Let $W \subset V$ be a linear subspace. Show that $\{T \in \operatorname{End}_F(V) : T(W) = 0\}$ is a left ideal of the ring $\operatorname{End}_F(V)$.

Proof. Let W^0 denote $\{T \in \operatorname{End}_F(V) : T(W) = 0\}$. To prove that W^0 is a left ideal of $\operatorname{End}_F(V)$, it will suffice to show that $(W^0, +) \leq (\operatorname{End}_F(V), +)$ and $SW^0 \subset W^0$ for all $S \in \operatorname{End}_F(V)$. Let's begin.

The zero map is an element of W^0, so it is nonempty. If $T(W) = 0$ and $T'(W) = 0$, then $(T + T')(W) = 0$, so W^0 is closed under addition. If $T(W) = 0$, then $-T(W) = 0$, so W^0 is closed under inverses. Therefore, $(W^0, +) \leq (\operatorname{End}_F(V), +)$ as desired.

Let $S \in \text{End}_F(V)$ and $T \in W^0$ be arbitrary. By definition, $Tw = 0$ for all $w \in W$. This combined with the fact that linear transformations send zero to zero implies that

$$(S \circ T)(w) = S(Tw) = S(0) = 0$$

for all $w \in W$. Therefore, $(S \circ T)(W) = 0$, so $S \circ T \in W^0$, as desired. □

(b) Let $T : V \to V$ be a linear transformation, and let $W = \ker(T)$. Show that the left ideal generated by T is $\{S \in \text{End}_F(V) : S(W) = 0\}$.

Proof. The left ideal generated by T is $[\text{End}_F(V)]T$. We will prove that

$$[\text{End}_F(V)]T = \{S \in \text{End}_F(V) : S(W) = 0\}$$

via a bidirectional inclusion argument. Suppose first that $R \in [\text{End}_F(V)]T$. Then $R = S \circ T$ for some $S \in \text{End}_F(V)$. It follows as before that since T annihilates W, $R = S \circ T$ annihilates W, so $R \in \{S \in \text{End}_F(V) : S(W) = 0\}$, as desired. Now suppose that $R \in \{S \in \text{End}_F(V) : S(W) = 0\}$. Then R annihilates W, i.e., $\ker(R) \supset W$. Let $S = R \circ T^{-1} \in \text{End}_F(V)$ (T^{-1} denotes a partial left inverse, specifically any linear transformation satisfying $T^{-1} \circ T = \text{id}_{V \setminus W}$). Then $R = S \circ T$, so $R \in [\text{End}_F(V)]T$, as desired. □

(c) Show that $\{T \in \text{End}(V) : T(V) \subset W\}$ is a right ideal of $\text{End}_F(V)$.

Proof. Let W^1 denote $\{T \in \text{End}(V) : T(V) \subset W\}$. To prove that W^1 is a right ideal of $\text{End}_F(V)$, it will suffice to show that $(W^1, +) \leq (\text{End}_F(V), +)$ and $W^1 S \subset W^1$ for all $S \in \text{End}_F(V)$. Let's begin.

The first part proceeds as in part (a).

Let $S \in \text{End}_F(V)$ and $T \in W^1$ be arbitrary. Then since $S(V) \subset V$, $(T \circ S)(V) = T(S(V)) \subset W$. Therefore, $TS \in W^1$, as desired. □

(d) Show that if $\text{im}(T) = W$, then the right ideal of $\text{End}_F(V)$ generated by T is $\{S \in \text{End}_F(V) : S(V) \subset W\}$.

Proof. The right ideal generated by T is $T[\text{End}_F(V)]$. We will prove that

$$T[\text{End}_F(V)] = \{S \in \text{End}_F(V) : S(V) \subset W\}$$

via a bidirectional inclusion argument. Suppose first that $R \in T[\text{End}_F(V)]$. Then $R = T \circ S$ for some $S \in \text{End}_F(V)$. It follows as before that since T maps into W that $R = T \circ S$ maps $S(V) \subset V$ into W, so $R \in \{S \in \text{End}_F(V) : S(V) \subset W\}$, as desired. Now suppose that $R \in \{S \in \text{End}_F(V) : S(V) \subset W\}$. Then R maps into W, i.e., $\text{im}(R) \subset W$. Let $S = T^{-1} \circ R \in \text{End}_F(V)$ (T^{-1} denotes a linear transformation satisfying $T \circ T^{-1} = \text{id}$). Then $R = T \circ S$, so $R \in T[\text{End}_F(V)]$, as desired. □

2.10. Prove that if T is in the center of $\text{End}_F(V)$, then there is some $c \in F$ such that $Tv = cv$ for all $v \in V$.

Proof. Let $\{v_1, v_2, \dots\}$ be a basis of V. Consider v_i. Let S be a linear transformation satisfying $Sv_i = v_i$ and $S(Tv_i) = c_i v_i$ for some $c_i \in F$. Note that if Tv_i, v_i are linearly dependent, then c_i is specified by the ratio of the magnitudes of Tv_i to v_i, and if Tv_i, v_i are linearly independent, any c_i suffices; either way, S is well-defined. It follows that

$$Tv_i = T(Sv_i) = S(Tv_i) = c_i v_i$$

Thus, T scales every basis vector. Now we show that all of the c_i are equal. Let S_i be a linear transformation satisfying $S_i v_1 = v_i$. Then

$$Tv_i = TS_i v_1 = S_i T v_1 = S_i c_1 v_1 = c_1 S_i v_1 = c_1 v_i$$

It follows that $Tv_i = cv_i$ for all basis vectors v_i. Therefore, $Tv = cv$ for all $v \in V$. □

3 Properties of Ideals

When solving a particular problem Y, you may appeal to the result of any problem X that has occurred before Y (earlier problem sheets included) whether or not you submitted a solution of problem X.

1/25: **3.1.** How many maximal ideals does the ring $\mathbb{Z}/a\mathbb{Z}$ possess under the following conditions?

General treatment.
Lemma 1: Let I be a nonzero ideal of $\mathbb{Z}/a\mathbb{Z}$, and let $n = |I|$. Then $n \mid a$ and

$$I = \left\{0, \frac{a}{n}, \frac{2a}{n}, \ldots, \frac{(n-1)a}{n}\right\}$$

Proof: Since I is an ideal of $\mathbb{Z}/a\mathbb{Z}$, $(I, +) \leq (\mathbb{Z}/a\mathbb{Z}, +)$. Thus, by Lagrange's theorem, $n = |I|$ divides $a = |\mathbb{Z}/a\mathbb{Z}|$. As to the other part of the lemma, since I is nonzero, there exists $m \in I$ such that $0 < m < a$. Since I is closed under multiplication, it follows that $0m, 1m, 2m, \ldots, (a-1)m \in I$ (all of these numbers must be taken modulo a). However, some of these numbers may well be the same: If we define n by $\text{lcm}(a, m) = nm$, then we can see that $nm \equiv 0m \bmod a$, $(n+1)m \equiv 1m \bmod a$, and so on. Thus,

$$I = \{0m \bmod a, 1m \bmod a, 2m \bmod a, \ldots, (n-1)m \bmod a\}$$

It follows since $(n-1)m < a$ and $nm \equiv 0 \mod a$ that $nm = a$ and hence $m = a/n$. Substituting this definition of m into the above yields the desired result.

Definition: Suppose that the prime factorization of a is $p_1^{e_1} \cdots p_m^{e_m}$ for some distinct prime numbers $p_1, \ldots, p_m$ and natural numbers $e_1, \ldots, e_m$. Since $n \mid a$ by Lemma 1, $n = p_1^{d_1} \cdots p_m^{d_m}$ where $0 \leq d_i \leq e_i$ $(i = 1, \ldots, m)$. Let $\boldsymbol{I(d_1, \ldots, d_m)}$ denote the ideal of the form given by Lemma 1, where $n = p_1^{d_1} \cdots p_m^{d_m}$.

Lemma 2: If $c_i \leq d_i$ $(i = 1, \ldots, m)$, then $I(c_1, \ldots, c_m) \subset I(d_1, \ldots, d_m)$. If any one of the inequalities is strict, the set inclusion is proper.

Proof: We have that

$$I(c_1, \ldots, c_m) = \left\{\frac{ja}{p_1^{c_1} \cdots p_m^{c_m}}\right\}_{j=0}^{p_1^{c_1} \cdots p_m^{c_m} - 1} \qquad I(d_1, \ldots, d_m) = \left\{\frac{ja}{p_1^{d_1} \cdots p_m^{d_m}}\right\}_{j=0}^{p_1^{d_1} \cdots p_m^{d_m} - 1}$$

Let $r = \frac{p_1^{d_1} \cdots p_m^{d_m}}{p_1^{c_1} \cdots p_m^{c_m}}$. Then

$$I(c_1, \ldots, c_m) = \left\{\frac{jra}{p_1^{d_1} \cdots p_m^{d_m}}\right\}_{j=0}^{p_1^{c_1} \cdots p_m^{c_m} - 1} \subset \left\{\frac{ja}{p_1^{d_1} \cdots p_m^{d_m}}\right\}_{j=0}^{p_1^{d_1} \cdots p_m^{d_m} - 1} = I(d_1, \ldots, d_m)$$

as desired. Any inequality being strict is equivalent to $r > 1$ and hence $I(d_1, \ldots, d_m)$ contains an element (specifically, $ja/p_1^{d_1} \cdots p_m^{d_m}$) that $I(c_1, \ldots, c_m)$ does not, for example.

Theorem: $\mathbb{Z}/a\mathbb{Z}$ has m maximal ideals.

Proof: Consider the m ideals $M_i = I(e_1, \ldots, e_i - 1, \ldots, e_m)$. It follows by Lemma 2 that $M_i \subsetneq I(e_1, \ldots, e_m) = \mathbb{Z}/a\mathbb{Z}$ and that there are no "intermediate" ideals. In particular, suppose that $I(d_1, \ldots, d_m)$ is an ideal that contains M_i properly. Then $e_j \leq d_j \leq e_j$ for all $j \neq i$ and $e_i - 1 \leq d_i \leq e_i$. Moreover, since at least one inequality must be strict and none of the $j \neq i$ ones can be, we must have $d_i = e_i$. Therefore, $I(d_1, \ldots, d_m) = I(e_1, \ldots, e_m) = \mathbb{Z}/a\mathbb{Z}$. Therefore, the M_i are maximal.

Furthermore, any other ideal either has $d_i < e_i - 1$ or some additional $d_j < e_j$, leading to an additional intermediate ideal and negating the possibility of it being maximal. □

(i) $a = 81$.

Answer. $81 = 3^4$, so $\boxed{\text{one}}$. □

(ii) $a = 44$.

Proof. $44 = 2^2 \cdot 11$, so $\boxed{\text{two}}$. □

(iii) $a = 42$.

Proof. $42 = 2 \cdot 3 \cdot 7$, so $\boxed{\text{three}}$. □

3.2. Given ring homomorphisms $f : R \to A$ and $g : R \to B$, check that $h(v) = (f(v), g(v))$ for all $v \in R$ gives a ring homomorphism $h : R \to A \times B$.

Proof. To prove that h is a ring homomorphism, it will suffice to show that h respects addition and multiplication, and that $h(1_R) = 1_{A\times B}$.

Let $a_1, a_2 \in R$ be arbitrary. Then

$$\begin{aligned} h(a_1 + a_2) &= (f(a_1 + a_2), g(a_1 + a_2)) \\ &= (f(a_1) + f(a_2), g(a_1) + g(a_2)) \\ &= (f(a_1), g(a_1)) + (f(a_2), g(a_2)) \\ &= h(a_1) + h(a_2) \end{aligned}$$

and

$$\begin{aligned} h(a_1 \times a_2) &= (f(a_1 \times a_2), g(a_1 \times a_2)) \\ &= (f(a_1) \times f(a_2), g(a_1) \times g(a_2)) \\ &= (f(a_1), g(a_1)) \times (f(a_2), g(a_2)) \\ &= h(a_1) \times h(a_2) \end{aligned}$$

Additionally,

$$\begin{aligned} h(1_R) &= (f(1_R), g(1_R)) \\ &= (1_A, 1_B) \\ &= 1_{A\times B} \end{aligned}$$

These three sets of equations give all of the desired results. □

3.3. In particular, let I_1, I_2 be ideals of a commutative ring R, and let $\pi_i : R \to R/I_i$ $(i = 1, 2)$ be canonical surjections. Consider the ring homomorphism $h : R \to (R/I_1)\times(R/I_2)$ given by $h(a) = (\pi_1(a), \pi_2(a))$ for all $a \in R$.

(i) Describe $\ker(h)$ in terms of I_1, I_2.

Proof. The kernel of h is the set of all $a \in R$ such that

$$(0, 0) = 0 = h(a) = (\pi_1(a), \pi_2(a))$$

i.e., such that $\pi_i(a) = 0$ $(i = 1, 2)$. We know that $0 + I_i = 0 = \pi_i(a) = a + I_i$ when $a \in I_i$. Thus, putting everything back together, $a \in \ker(h)$ implies that $a \in I_i$ $(i = 1, 2)$, i.e., $a \in I_1 \cap I_2$. Additionally, if $a \in I_1 \cap I_2$, then $\pi_1(a) = \pi_2(a) = 0$. Therefore,

$$\boxed{\ker(h) = I_1 \cap I_2}$$

□

(ii) Prove that $A \implies B \implies C \implies A$.

(A) h is a surjection.

(B) $(0,1)$ is in the image of h.

(C) $I_1 + I_2 = R$.

Proof. We tackle the implications one at a time.

(A) $\implies$ (B): Suppose h is a surjection. Then $\operatorname{im} h = (R/I_1) \times (R/I_2)$. Therefore, since $(0,1) \in (R/I_1) \times (R/I_2)$, $(0,1) \in \operatorname{im} h$.

(B) $\implies$ (C): Suppose $(0,1) \in \operatorname{im} h$. Then there exists $a \in R$ such that $h(a) = (0,1)$. Thus, by the definition of h, $a \in 0 + I_1 = I_1$ and $a \in 1 + I_2$. It follows from this latter statement that there exists $x \in I_2$ such that $a = 1 + x$, or $a + (-x) = 1$. Ideals are closed under multiplication by elements of R, so since $-1 \in R$, $-x \in I_2$. This combined with the fact that $a \in I_1$ demonstrates that that $1 = a + (-x) \in I_1 + I_2$. Therefore, since ideals are closed under multiplication, $I_1 + I_2 = R$.

(C) $\implies$ (A): Suppose $I_1 + I_2 = R$. Let $(x + I_1, y + I_2) \in (R/I_1) \times (R/I_2)$ be arbitrary. To prove that h is a surjection, it will suffice to find an $a \in R$ such that $h(a) = (x + I_1, y + I_2)$. Since $x, y \in R$, we know that $x, y \in I_1 + I_2$ by hypothesis. Thus, we may write $x = a_1 + a_2$ and $y = b_1 + b_2$, where $a_1, b_1 \in I_1$ and $a_2, b_2 \in I_2$. It follows that

$$(x+I_1, y+I_2) = ((a_1+a_2)+I_1, (b_1+b_2)+I_2) = (a_2+I_1, b_1+I_2) = ((a_2+b_1)+I_1, (a_2+b_1)+I_2)$$

Therefore, choosing $a = a_2 + b_1$, we have

$$h(a) = (x + I_1, y + I_2)$$

as desired. □

(iii) Assume that $I_1+I_2 = R$. Prove that $I_1I_2 = I_1 \cap I_2$. Deduce that $\phi : R/(I_1I_2) \to (R/I_1) \times (R/I_2)$ is an isomorphism.

Proof. To prove that $I_1I_2 = I_1 \cap I_2$, we will use a bidirectional inclusion proof. Since ideals are closed under multiplication by external elements and addition of internal elements, $I_1I_2 \subset I_1$ and $I_1I_2 \subset I_2$. Therefore, $I_1I_2 \subset I_1 \cap I_2$, as desired. Now let $x \in I_1 \cap I_2$ be arbitrary. Then $x \in I_1$ and $x \in I_2$. Now since $I_1 + I_2 = R$, we may pick $a_1 \in I_1$ and $a_2 \in I_2$ such that $a_1 + a_2 = 1$. Multiplying through this equation by x yields $xa_1 + xa_2 = x$. Moreover, since $x \in I_2$ and $a_1 \in I_1$, $xa_1 \in I_1I_2$. Similarly, $xa_2 \in I_1I_2$. It follows since I_1I_2 is closed under addition that $x = xa_1 + xa_2 \in I_1I_2$, as desired.

Since $h : R \to (R/I_1) \times (R/I_2)$ is a ring homomorphism and, by part (i), $\ker(h) = I_1 \cap I_2$, the NIT implies that h has a unique factorization $h = i \circ \phi \circ \pi$ where $\phi : R/(I_1 \cap I_2) \to (R/I_1) \times (R/I_2)$ is an isomorphism of rings. But since $I_1 \cap I_2 = I_1I_2$ by the above, we have that $\phi : R/(I_1I_2) \to (R/I_1) \times (R/I_2)$ is an isomorphism of rings, as desired. □

3.4. Prove that a nonzero ideal $I \subset F[[X]]$, where F is a field, is the principal ideal generated by X^n for some $n \geq 0$. (This is a continuation of Exercise 7.2.3c of Dummit and Foote (2004), addressed in HW2 Q2.2.)

Proof. Let I be an arbitrary nonzero ideal in $F[[X]]$, let n be the lowest power present in any polynomial in I, and let $f \in I$ be a polynomial with a nonzero X^n term. Since $a_n \neq 0$, f/X^n is a polynomial with nonzero constant term a_n. Additionally, since a_n is a nonzero element of a field, a_n is a unit. It follows by Exercise 7.2.3c that f/X^n is a unit. Thus, there exists $u \in R$ such that $u \times (f/X^n) = 1$. Multiplying through this equation by X^n yields

$$uf = X^n$$

Since $f \in I$ and $u \in F[[X]]$, $uf \in I$, so $X^n = uf \in I$. Multiplying any polynomial in $F[[X]]$ by the monic polynomial X^n can only increase the exponent of every term, so, to reiterate, there are

no polynomials in I having terms with exponents less than n. Moreover, it follows by the Euclidean algorithm that every polynomial h with all terms having powers greater than or equal to n can be expressed as the product of some $q \in F[[X]]$ and X^n. Therefore, $I = (X^n)$. □

3.5. Recall that $R[X,Y] := R[X][Y]$. Regard R as a subring of $R[X,Y]$. Let R be a commutative ring.

The **universal property of $R[X,Y]$** states: Let A be commutative. Given a ring homomorphism $\alpha : R \to A$ and $x, y \in A$, prove that there is a unique ring homomorphism $\beta : R[X,Y] \to A$ that satisfies $\beta(c) = \alpha(c)$ for all $c \in R$, $\beta(X) = x$, and $\beta(Y) = y$.

Deduce this statement from the universal property of $R[X]$.

Proof. Consider the ring homomorphism $\alpha : R \to A$ and the element $x \in A$ provided by the assumptions of the universal property of $R[X,Y]$. By the universal property of $R[X]$, we may link these to a unique ring homomorphism $\tilde{\alpha} : R[X] \to A$ such that $\tilde{\alpha}(a) = \alpha(a)$ for all $a \in R$ and $\tilde{\alpha}(X) = x$. If we now switch perspectives and view $R[X]$ as our ring, $\tilde{\alpha}$ as our coordinate change function on that ring, and y (from the original givens) as our element of interest in A, we can apply the universal property of "$R[X]$"[9] again. This time, it links $\tilde{\alpha}$ and y to a unique ring homomorphism $\beta : R[X][Y] \to A$ such that $\beta(a) = \tilde{\alpha}(a)$ for all $a \in R[X]$ and $\beta(Y) = y$.

Now we show that this β is the β we've been looking for. First off, note that $R[X,Y] = R[X][Y]$, so β has the correct domain and range. Additionally, we already have $\beta(Y) = y$. To show that $\beta(c) = \alpha(c)$ for all $c \in R$, let $c \in R$ be arbitrary. Since $R \subset R[X]$, $c \in R[X]$. Thus, $\beta(c) = \tilde{\alpha}(c)$. Additionally, since $c \in R$, we have from our original definition of $\tilde{\alpha}$ that $\tilde{\alpha}(c) = \alpha(c)$. Therefore, by transitivity, $\beta(c) = \alpha(c)$, as desired. Lastly, we wish to show that $\beta(X) = x$. Since $X \in R[X]$, we know that $\beta(X) = \tilde{\alpha}(X)$. Recall from the original definition of $\tilde{\alpha}$ that $\tilde{\alpha}(X) = x$. Therefore, by transitivity, $\beta(X) = x$, as desired. □

3.6. (i) For any $a \in R$, we may define the ring homomorphism $\phi : R[X] \to R$ by $\phi(f(X)) = f(a)$. Prove that $\ker \phi$ is a principal ideal, and find a generator of this ideal.

Proof. To prove that $\ker \phi$ is a principal ideal and identify its generator in the process, it will suffice to show that $\ker \phi = (X - a)$.

Suppose first that $f \in \ker \phi$. It follows by the definition of the kernel that $f(a) = \phi(f) = 0$. Additionally, recall from class that there exists $q \in R[X]$ such that

$$f(X) - f(a) = q(X)(X - a)$$

But since $f(a) = 0$, we have that

$$f = f - 0 = q \cdot (X - a) \in R[X](X - a) = (X - a)$$

as desired.

Now suppose that $f \in (X - a)$. Then $f = q \cdot (X - a)$ for some $q \in R[X]$. It follows that

$$\phi(f) = f(a) = q(a) \cdot (a - a) = q(a) \cdot 0 = 0$$

so $f \in \ker \phi$, as desired. □

(ii) Let $g \in R[X]$. Define $\phi : R[X,Y] \to R[X]$ by $\phi(f(X,Y)) = f(X, g(X))$. Prove that $\ker \phi$ is a principal ideal, and find a generator of this ideal.

Proof. To prove that $\ker \phi$ is a principal ideal and identify its generator in the process, it will suffice to show that $\ker \phi = (Y - g(X))$.

[9] Perhaps it would be more accurate to say "the universal property of $R[X][Y]$" at this point!

Suppose first that $f \in \ker \phi$. It follows by the definition of the kernel that $f(X, g(X)) = \phi(f) = 0$. Additionally, if we regard f as a polynomial in Y, the Euclidean algorithm asserts that there exist $q, r \in R[X, Y]$ such that

$$f(X, Y) = q(X, Y)(Y - g(X)) + r(X, Y)$$

where $\deg(r) < 1 = \deg(Y - g(X))$. It follows from this last statement that $\deg(r) \in \{0, -\infty\}$, i.e., r is a constant. We may determine its value by evaluating the above at $(X, g(X))$, as follows.

$$\begin{aligned} f(X, g(X)) &= q(X, g(X))(g(X) - g(X)) + r \\ r &= f(X, g(X)) \end{aligned}$$

Therefore,

$$\begin{aligned} f(X, Y) &= f(X, Y) - 0 \\ &= f(X, Y) - f(X, g(X)) \\ &= q(X, Y)(Y - g(X)) \\ &\in R[X, Y](Y - g(X)) \\ &= (Y - g(X)) \end{aligned}$$

as desired.

Now suppose that $f \in (Y - g(X))$. Then $f = q \cdot (Y - g(X))$ for some $q \in R[X, Y]$. It follows that

$$\phi(f) = f(X, g(X)) = q(X, g(X)) \cdot (g(X) - g(X)) = q(X, g(X)) \cdot 0 = 0$$

so $f \in \ker \phi$, as desired. □

3.7. Let a, b be elements of R a commutative ring, and let a be a unit of R. Consider the ring homomorphism $\phi : R[X] \to R[X]$ given by $\phi(f) = f(aX + b)$. Prove that ϕ is an isomorphism. *Hint*: It's inverse can be written down explicitly.

Proof. Let $\alpha : R \to R[X]$ be defined by $\alpha(c) = c$ for all $c \in R$. Given this ring homomorphism $\alpha : R \to R[X]$ as well as $(X - b)/a \in R[X]$, Q3.5 asserts that there is a unique ring homomorphism $\psi : R[X] \to R[X]$ that satisfies $\psi(c) = \alpha(c) = c$ for all $c \in R$ and $\psi(X) = (X - b)/a$. Since $\psi : R[X] \to R[X]$ defined by

$$\psi(f) = f\left(\frac{X - b}{a}\right)$$

satisfies both of these properties, it is the unique ring homomorphism that Q3.5 proved existed.

We now prove that $\phi \circ \psi = \psi \circ \phi = \mathrm{id}$. Let $f \in R[X]$ be arbitrary. Then

$$\begin{aligned} (\phi \circ \psi)(f) &= \phi(\psi(f)) \\ &= \phi\left(f\left(\frac{X - b}{a}\right)\right) \\ &= f\left(\frac{(aX + b) - b}{a}\right) \\ &= f(X) \\ &= \mathrm{id}(f) \end{aligned} \qquad \begin{aligned} (\psi \circ \phi)(f) &= \psi(\phi(f)) \\ &= \psi(f(aX + b)) \\ &= f\left(a \cdot \frac{X - b}{a} + b\right) \\ &= f(X) \\ &= \mathrm{id}(f) \end{aligned}$$

Therefore, ϕ is an isomorphism, as desired. □

3.8. Let R be an integral domain. Prove that every isomorphism $\phi : R[X] \to R[X]$ that satisfies $\phi(c) = c$ for all $c \in R$ is of the type given in Q3.7.

Proof. See the answer to Q3.7. What I did there (and, I guess, what I would need to repeat here) is invoke the universal property of $R[X]$ under an appropriate auxiliary function ($\alpha = \mathrm{id}$). This would then guarantee me existence and uniqueness for a ϕ satisfying $\phi(c) = c$. Additionally, we must have a monomial argument because anything with degree other than 1 would alter the possible degrees we can access in the image, thereby making ϕ *not* an isomorphism. By making the monomial as general as possible, i.e., with the two degrees of freedom a, b in $ax + b$, we can be sure to capture *all* relevant isomorphisms. □

3.9. (i) Exercise 7.1.11 of Dummit and Foote (2004): Prove that if R is an integral domain and $x^2 = 1$ for some $x \in R$, then $x = \pm 1$.

Proof. We have that

$$\begin{aligned} 1 &= x^2 \\ 0 &= x^2 - 1 \\ &= (x+1)(x-1) \end{aligned}$$

Since R is an integral domain, it contains no zero divisors, so either $x + 1 = 0$ (and $x = -1$) or $x - 1 = 0$ (and $x = 1$); either way, $x = \pm 1$, as desired. □

(ii) Deduce that $\{a^2 \mid 0 \neq a \in \mathbb{F}_p\}$ has cardinality $(p-1)/2$. Here, p is an odd prime, and $\mathbb{F}_p$ is the field of cardinality p.

Proof. There are $p - 1$ nonzero elements in $\mathbb{F}_p$. Although we usually think of these elements as $1, \ldots, p-1$, we can divide this list in two and consider instead the congruent elements

$$-\frac{p-1}{2}, \ldots, -1, 1, \ldots, \frac{p-1}{2}$$

Note that it is the fact that $p \geq 3$ is an odd prime that allows us to divide $p - 1$ (necessarily an even number) by 2 and still obtain a (nonzero) integer. Continuing, we can rearrange the list in this way because $a \equiv b \bmod p$ implies $a^2 \equiv b^2 \bmod p$, so it will not affect our operation of choice. Additionally, the boon is that choosing negative elements makes it very easy to see that $a^2 = (-a)^2$ for each $a \in \{1, \ldots, (p-1)/2\}$. Therefore, for the $p - 1$ elements in the above list, there are only $(p-1)/2$ squares: One for each distinct absolute value of an entry in the above list, as desired. □

3.10. Prove that there are exactly four rings of cardinality p^2, where p is a prime ($p = 2$ is included). Identify which of them is a field, which is a product of two fields, and find a nonzero nilpotent in both of the remaining cases.

Hint: First show that there are only two possibilities for the characteristic of such a ring. If the characteristic is an odd prime p, show that there is some θ in the ring with the two properties: (i) $\theta^2 \in \mathbb{F}_p$ and (ii) $1, \theta$ form a basis for the given ring viewed as an $\mathbb{F}_p$ vector space. Now apply the previous problem.

Proof. Tricky??

Yes – by far the hardest question. Show that $X^2 - \theta^2$ is a maximal ideal in the polynomial ring. If f is irreducible, then (f) is maximal. Check that $X^2 - \theta^2$ is irreducible.

Like 5 problems in 1 problem. Takes a bunch of techniques. The case where the square is zero is not hard. Write down four distinct rings and then use this to prove that you can't get any other ones. Keep them all in the quotient form?? One is a product of two cyclic groups; that's a product of fields. You're allowed to multiply differently when they're rings, not groups. 2 groups, but 4 rings. □

4 Applications of Fraction Rings

Throughout this assignment, R will denote a *commutative* ring.

2/1: **4.1.** Let R be a ring, and let $f \in R$ be an element which is not a zero divisor. Recall that we defined $R_f = D^{-1}R$ for $D = \{1, f, f^2, \dots\}$. Prove that

$$R_f \cong R[X]/(fX - 1)$$

using the universal property of the ring of fractions.

Proof. Herein, let $\bar{g}$ denote $g + (fX - 1)$ for any $g \in R[X]$, and let S denote $R[X]/(fX - 1)$.

To prove that $R_f \cong R[X]/(fX-1)$, i.e., that $D^{-1}R \cong S$, it will suffice to construct an isomorphism $\tilde{\varphi} : D^{-1}R \to S$. Per Lecture 2.2, we may define a canonical injection $i : R \to R[X]$ and a canonical surjection $\pi : R[X] \to S$.

We now prove that the restriction $\pi|_R$ of π to $R \cong i(R) \subset R[X]$ is injective. Suppose $\pi|_R(a) = \pi|_R(b)$ for $a, b \in R$. Then $\bar{a} = \bar{b}$, so $a \in \bar{b}$. But since $\deg(a) = 0$ and b is the only element of $\bar{b}$ of degree 0, we must have $a = b$, as desired.

It follows that we may define an injective ring homomorphism $\varphi : R \to S$ by $\varphi = \pi|_R \circ i$. More explicitly, for any $a \in R$, we have that

$$\varphi(a) = (\pi|_R \circ i)(a) = \pi(i(a)) = \pi(a) = \bar{a}$$

We now wish to demonstrate that $\varphi(D) \subset S^\times$. We divide into two cases ($1 \in D$ and $f^n \in D$). Naturally $1 \in D$, which maps to $\bar{1} \in S$ since φ is a ring homomorphism, is a unit. To prove that every f^n maps to a unit in $S^\times$, we induct on n. For the base case $n = 1$, we have that

$$\begin{aligned} \overline{fX - 1} &= \bar{0} \\ \bar{f}\bar{X} - \bar{1} &= \bar{0} \\ \bar{f}\bar{X} &= \bar{1} \\ \varphi(f) \cdot \bar{X} &= \bar{1} \end{aligned}$$

Thus, $\varphi(f) \in S^\times$ by definition, as desired. Now suppose inductively that $\varphi(f^{n-1}) \in S^\times$; we wish to demonstrate that $\varphi(f^n) \in S^\times$. By the induction hypothesis, there exists $\bar{b} \in S$ such that $\varphi(f^{n-1}) \cdot \bar{b} = \bar{1}$. Therefore,

$$\begin{aligned} \varphi(f^n) \cdot \overline{bX} &= \varphi(f)\varphi(f^{n-1})\bar{b}\bar{X} \\ &= \varphi(f)\bar{1}\bar{X} \\ &= \varphi(f)\bar{X} \\ &= \bar{1} \end{aligned}$$

as desired, where we use the base case to get from the next-to-last line to the last line above.

At this point, we have proven that $\varphi : R \to S$ is an injective ring homomorphism such that $\phi(D) \subset S^\times$. Thus, we have by the universal property of rings of fractions that there exists a unique injective ring homomorphism $\tilde{\varphi} : D^{-1}R \to S$ such that $\tilde{\varphi} \circ \iota = \varphi$.

To verify that $\tilde{\varphi}$ is surjective, let $\bar{g} \in S$ be arbitrary, where $g \in R[X]$. Since R is a subring of $D^{-1}R$, we may consider $g \in D^{-1}R[X]$. In particular, we will be interested in $(1/f)g \in D^{-1}R[X]$ and $X - 1/f \in D^{-1}R[X]$. Applying the Euclidean algorithm to the latter monic polynomial generates $q, r \in D^{-1}R[X]$ such that $(1/f)g = q(X - 1/f) + r$ and, since $\deg(r) < \deg(X - 1/f) = 1$, $r \in D^{-1}R$. It follows that $g = q(fX - 1) + rf$, so $\tilde{\varphi}(rf) = \overline{rf} = \bar{g}$ for $rf \in D^{-1}R$.

Let d be the denominator of rf. Then $drf \in R$. It follows that $\tilde{\varphi}(drf) = \tilde{\varphi}(\iota(drf)) = \varphi(drf) = \overline{drf}$ so

$$\begin{aligned} \bar{d} \cdot \overline{rf} &= \tilde{\varphi}(d)\tilde{\varphi}(rf) \\ &= \varphi(d)\tilde{\varphi}(rf) \\ &= \bar{d}\tilde{\varphi}(rf) \\ \overline{rf} &= \tilde{\varphi}(rf) \\ \tilde{\varphi}(rf) &= \bar{g} \end{aligned}$$

as desired. □

4.2. Let $\mathbb{Z}[i] = \mathbb{Z}[X]/(X^2+1)$ denote the ring of **Gaussian integers**. Recall from class that $\mathbb{Z}[i]$ is a Euclidean domain with norm $N : \mathbb{Z}[i] \to \mathbb{Z}_{\geq 0}$ defined by $N(a+bi) = a^2 + b^2$.

(a) Let R be a Euclidean domain with norm N which satisfies $N(xy) = N(x)N(y)$ for all $x, y \in R$. Prove that $a \in R$ is a unit iff $N(a) = 1$. (Hint: Start by computing $N(1)$.)

Proof. Taking the hint, we will begin by computing $N(1)$. Since $1 \neq 0$ and N is a positive norm by assumption, $N(1) > 0$. Additionally, since $\mathbb{Z}$ is an integral domain, we can use the cancellation law between the following equations.

$$\begin{aligned} N(1 \cdot 1) &= N(1) \\ N(1)N(1) &= N(1) \cdot 1 \\ N(1) &= 1 \end{aligned}$$

Having computed $N(1)$, we now begin the argument in earnest.

Suppose first that $a \in R$ is a unit. Then there exists $b \in R$ such that $ab = 1$. It follows that

$$\begin{aligned} N(ab) &= N(1) \\ N(a)N(b) &= 1 \end{aligned}$$

Thus, $N(a) = \pm 1$, but since $N(a) \in \mathbb{Z}_{\geq 0}$, we must have

$$N(a) = 1$$

as desired.

Now suppose that $N(a) = 1$. Since R is an ED and $a \neq 0$, we know that there exist $q, r \in R$ such that $1 = qa + r$ and $N(a) > N(r)$. But since $N(1) = 1$, we must have $N(r) = 0$ or $r = 0$. Therefore, $1 = qa$, so a is a unit, as desired. □

(b) Using part (a), find the units in $\mathbb{Z}[i]$.

Proof. Let $a + bi \in \mathbb{Z}[i]$ be a unit. Then $1 = N(a+bi) = a^2 + b^2$. The four possible solutions over $\mathbb{Z}$ are $(a, b) = (\pm 1, 0)$ and $(a, b) = (0, \pm 1)$. Therefore, the units of $\mathbb{Z}[i]$ are

$$\boxed{\pm 1, \pm i}$$

□

(c) Prove that $\text{Frac}(\mathbb{Z}[i]) = \mathbb{Q}[i]$.

Proof. To prove that $\text{Frac}(\mathbb{Z}[i]) = \mathbb{Q}[i]$, it will suffice to use a bidirectional inclusion argument. Suppose first that

$$\frac{a+bi}{c+di} \in \text{Frac}(\mathbb{Z}[i])$$

Then by the laws of multiplication on the field of fractions and on $\mathbb{Z}[i]$, we have that

$$\frac{a+bi}{c+di} = \frac{a+bi}{c+di}\cdot\frac{c-di}{c-di} = \frac{(a+bi)(c-di)}{(c+di)(c-di)} = \frac{(ac+bd)+(bc-ad)i}{c^2+d^2} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i$$

Since $a+bi, c+di \in \mathbb{Z}[i] = \{\alpha+\beta i \mid \alpha,\beta\in\mathbb{Z}\}$ by the definition of $\mathrm{Frac}(\mathbb{Z}[i])$, we know that $a,b,c,d\in\mathbb{Z}$. Thus,

$$\frac{ac+bd}{c^2+d^2}, \frac{bc-ad}{c^2+d^2} \in \mathbb{Q}$$

and hence

$$\frac{a+bi}{c+di} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i \in \{\alpha+\beta i \mid \alpha,\beta\in\mathbb{Q}\} = \mathbb{Q}[i]$$

as desired.

Now suppose that

$$\frac{a}{b} + \frac{c}{d}i \in \mathbb{Q}[i]$$

Then by the laws of addition and multiplication on $\mathbb{Q}[i]$ and on $\mathbb{Z}[i]$, we have that

$$\frac{a}{b} + \frac{c}{d}i = \frac{a}{b} + \frac{c}{d}\frac{i}{1} = \frac{a}{b} + \frac{ci}{d1} = \frac{a}{b} + \frac{ci}{d} = \frac{ad+bci}{bd} = \frac{ad+bci}{bd+0i}$$

Since $a/b, c/d \in \mathbb{Q}$, $a,b,c,d\in\mathbb{Z}$. Thus, $ad, bc, bd, 0 \in \mathbb{Z}$ so $ad+bci, bd+0i \in \mathbb{Z}[i]$. Additionally, since $b,d\in\mathbb{Z}\setminus\{0\}$ by hypothesis, $bd+0i\neq 0$ as well. Therefore,

$$\frac{a}{b} + \frac{c}{d}i = \frac{ad+bci}{bd+0i} \in \mathrm{Frac}(\mathbb{Z}[i])$$

as desired. □

4.3. (a) For $a,b\in\mathbb{Z}$, prove that $a^2-2b^2=0$ iff $a=b=0$.

Proof. For the forward direction, let that $a,b\in\mathbb{Z}$ satisfy $a^2-2b^2=0$. Suppose for the sake of contradiction that either a or b is nonzero. It follows by the derived equality $a^2=2b^2$ that they are both nonzero. Thus, a/b is a well-defined element of $\mathbb{Q}$. However, we have that

$$\begin{aligned} a^2-2b^2 &= 0 \\ a^2 &= 2b^2 \\ \frac{a^2}{b^2} &= 2 \\ \frac{a}{b} &= \sqrt{2} \end{aligned}$$

i.e., that a rational number equals an irrational number, a contradiction. Therefore, $a=b=0$.

For the reverse direction, let $a=b=0$. Then

$$a^2-2b^2 = 0^2 - 2\cdot 0^2 = 0$$

as desired. □

(b) Prove that $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}[X]/(X^2-2)$ is a field.

Proof. To prove that $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}[X]/(X^2-2)$ is a field, it will suffice to show that its additive and multiplicative identites are distinct and that every element is a unit. Let's begin.

$\mathbb{Q}[X]/(X^2-2)$ inherits addition and multiplication from $\mathbb{Q}[X]$, except now modulo X^2-1. Thus, the additive and multiplicative identities of $\mathbb{Q}[X]/(X^2-2)$ are the (distinct) images of those in $\mathbb{Q}[X]$ under the relevant canonical surjection.

Now let $a+b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ be arbitrary and nonzero. Then a or b is nonzero. It follows by part (a) that $a^2-2b^2 \neq 0$, and hence

$$\frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

is well-defined. By the law of multiplication in $\mathbb{Q}[\sqrt{2}]$, it follows that

$$\left(a+b\sqrt{2}\right)\left(\frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}\right) = \frac{\left(a+b\sqrt{2}\right)\left(a-b\sqrt{2}\right)}{a^2-2b^2} = \frac{a^2-b^2\sqrt{2}^2}{a^2-2b^2} = \frac{a^2-2b^2}{a^2-2b^2} = 1$$

as desired. Note that as in Q4.1, we can prove that $\sqrt{2}$ is the solution to $X^2-2=0$, i.e., an object X such that $X^2=2$. This is what rigorously allows us to simplify the above equation, not any intuitive or notationally implied notion of $\sqrt{2}$. □

4.4. Let D be a multiplicative subset of an integral domain R. Now R is a subring of $D^{-1}R$. Let J be an ideal of $D^{-1}R$. Put $I = R \cap J$.

(a) Is I an ideal of R?

Proof. Yes I is an ideal of R.
Since R, J are both additive subgroups of $D^{-1}R$, $R \cap J$ is an additive subgroup of $D^{-1}R$. Additionally, since $R \cap J \subset R$, $R \cap J$ must be an additive subgroup of R.
Now let $x \in I$ and $r \in R$ be arbitrary. Since $x \in I$, $x \in R$ and $x \in J$. It follows from the former statement and the fact that R is an ideal of R that $rx \in R$. It follows from the latter statement and the fact that J is an ideal of $D^{-1}R$ that $rx \in J$. Therefore, $rx \in R \cap J = I$, as desired. □

(b) Prove that if $I \neq R$, then $I \cap D = \emptyset$.

Proof. Suppose for the sake of contradiction that there exists $x \in I \cap D$. Then $x \in I$ and $x \in D$. It follows from the latter statement that $1/x \in D^{-1}R$. It follows from the former statement that $x \in R$ and $x \in J$. Since J is an ideal of $D^{-1}R$ (hence is closed under multiplication by elements of $D^{-1}R$) and $x \in J$, we have in particular that

$$\frac{1}{x} \cdot x = \frac{x}{x} = 1 \in J$$

It follows that $J = D^{-1}R$. Consequently, since $R \subset D^{-1}R$, we have that $I = R \cap D^{-1}R = R$. This contradicts the hypothesis that $I \neq R$. □

(c) Let $b \in J$. Is it true that $b = d^{-1}a$ for some $d \in D$ and $a \in I$?

Proof. Yes it is true.
Since $b \in J$, we know that $b \in D^{-1}R$. It follows that we may write $b = a/d$ for some $a \in R$ and $d \in D$. Since J is an ideal and $d \in D \subset R \subset D^{-1}R$, we know that $a = db \in J$. Combining the facts that $a \in R$ and $a \in J$, we can determine that $a \in R \cap J = I$, as desired. □

(d) Prove that if I is an ideal in R, then $I^e = \{s^{-1}x \in D^{-1}R \mid s \in D,\ x \in I\}$ is an ideal in $D^{-1}R$.

Proof. To prove that I^e is an ideal, it will suffice to show that $(I^e, +) \leq (D^{-1}R, +)$ and $a/b \cdot x/s \in I^e$ for all $a/b \in D^{-1}R$ and $x/s \in I^e$.
First, we will show that $(I^e, +)$ is a subgroup. By definition, it is a subset of $D^{-1}R$. Since $0 \in I$ and D is nonempty, the identity $0/d \in I^e$. Associativity follows from the containing group. And closure follows from that of I (under multiplication by elements of R and addition) and that of D (under multiplication by elements of D): If $x_1/s_1, x_2/s_2 \in I^e$, then

$$\frac{x_1}{s_1} + \frac{x_2}{s_2} = \frac{x_1s_2 + x_2s_1}{s_1s_2} \in I^e$$

as desired.

Now we show closure under multiplication. Let $x/s \in I^e$ and $a/b \in D^{-1}R$ be arbitrary. Since $x \in I$ and $a \in R$, $xa \in I$. Since $s, b \in D$, $sb \in D$. Therefore,

$$\frac{x}{s} \cdot \frac{a}{b} = \frac{xa}{sb} \in I^e$$

as desired. □

(e) Using part (c), prove that if J is an ideal of $D^{-1}R$, then $J = (R \cap J)^e$. Therefore, we have a surjective map of sets

$$\{\text{Ideals in } R\} \to \{\text{Ideals in } D^{-1}R\}$$

given by $I \mapsto I^e$. Note that the right inverse is given by $J \mapsto R \cap J$. Is this map a bijection?

Proof. To prove that $J = (R \cap J)^e$, we will use a bidirectional inclusion proof. Suppose first that $b \in J$. Then by part (c), $b = d^{-1}a$ for some $d \in D$ and $a \in I$. Therefore, by the definition of $(R \cap J)^e$, $b \in (R \cap J)^e$. Now suppose that $d^{-1}a \in (R \cap J)^e$ Then $a \in R \cap J$, so $a \in J$. It follows since J is an ideal of $D^{-1}R$ and $1/d \in D^{-1}R$ that $a/d = d^{-1}a \in J$, as desired.

No this map is not a bijection. Counterexample: Let R, D be defined as in Q5. Consider (3). Since $3 \in D$, $1 = 3/3 \in (3)^e$. Thus, $(3)^e = D^{-1}R$. It follows that $\mathbb{Z}^e = (3)^e$ even though $\mathbb{Z} \neq (3)$. □

(f) If R is a PID, is $D^{-1}R$ a PID?

Proof. Yes.

Let $J \in D^{-1}R$ be an arbitrary ideal. Per part (e), there exists an ideal $I \subset R$ such that $J = I^e$. Since R is a PID, $I = Ra$ for some $a \in I$. Additionally, as per the definition of the extension map, $a = a/1 \in I^e = J$. We will now prove that $I^e = D^{-1}Ra$. By definition, $D^{-1}Ra \subset I^e$. In the other direction, let $x/s \in I^e$ be arbitrary. Since $x \in I$, $x = ab$ for some $b \in R$. Moreover, $b/s \in D^{-1}R$, so $x/s = (b/s) \cdot a \in D^{-1}Ra$, as desired. □

4.5. (a) Let $D = \{n \in \mathbb{Z} : 2 \nmid n\}$. Recall that we defined

$$\mathbb{Z}_{(2)} = D^{-1}R = \{a/b \in \mathbb{Q} : 2 \nmid b\}$$

Write down all of the ideals in $\mathbb{Z}_{(2)}$. You can use the fact that the ideals in $\mathbb{Z}$ are $(n) = n\mathbb{Z}$ for $n \in \mathbb{Z}$, and the previous question. Which of these ideals are maximal? For each maximal ideal $M \in \mathbb{Z}_{(2)}$, what is the field $\mathbb{Z}_{(2)}/M$?

Proof. Since the ideals in $\mathbb{Z}$ are $(n) = n\mathbb{Z}$ for all $n \in \mathbb{Z}$, Q4.4e implies that the set of ideals of $\mathbb{Z}_{(2)}$ is the image of $\{(n) \mid n \in \mathbb{Z}\}$ under $I \mapsto I^e$. However, many of these are equivalent. In particular, if n is divisible by any numbers other than 2, you will be able to multiply n by the product of those numbers to reduce the magnitude of the generator down to a power of 2. Therefore, the set of all ideals in $\mathbb{Z}_{(2)}$ is

$$\boxed{\{(2^n)^e \mid n \in \mathbb{Z}_{\geq 0}\} \cup \{0\}}$$

Among these ideals,

$$\boxed{\text{Only } (2)^e \text{ is maximal.}}$$

To prove this, we will show that every ideal $(n)^e \in \mathbb{Z}_{(2)}$ is either equal to $\mathbb{Z}_{(2)}$ or is contained in $(2)^e$. Let's begin. Let $(n)^e \subset \mathbb{Z}_{(2)}$ be arbitrary. We divide into two cases ($2 \nmid n$ and $2 \mid n$). If $2 \nmid n$, then $n \in D$. It follows by its definition that $1 = n/n \in (n)^e$. Therefore, $(n)^e = R$. If $2 \mid n$, then $n = 2^m \cdot r$ for some $m \geq 1$ and r coprime to 2. Let $a/d \in (n)^e$ be arbitrary. Then $a \in (n)$ and $d \in D$. It follows that $n \mid a$, i.e., that $2 \mid a$. Thus, $a = 2b \in (2)$. Therefore, $a/d \in (2)^e$, so $(n)^e \subset (2)^e$, as desired.

Finally, we will prove that

$$\boxed{\mathbb{Z}_{(2)}/(2)^e \cong \mathbb{Z}/2\mathbb{Z}}$$

To do so, it will suffice to show that for any $a/d \in \mathbb{Z}_{(2)}$, we either have

$$\frac{a}{d} + (2)^e = 0 + (2)^e \qquad \frac{a}{d} + (2)^e = 1 + (2)^e$$

Since $\mathbb{Z}$ is an ED and $2 \neq 0$, we know that there exist $b, c \in \mathbb{Z}$ such that $a = 2b + c$ and $|c| < |2| = 2$ (i.e., $c \in \{0, \pm 1\}$). We now divide into three cases. If $c = 0$, then $a = 2b$ and hence

$$\frac{a}{d} = \frac{2b}{d} \in (2)^e$$

so $a/d + (2)^e = 0 + (2)^e$. If $c = 1$, then

$$\frac{a}{d} = \frac{1}{d} + \frac{2b}{d}$$

so $a/d \in 1/d + (2)^e$. Additionally, since $2 \nmid d$ by hypothesis, $2 \mid d-1$ and hence $\pm(d-1)/d \in (2)^e$. It follows that

$$\frac{1}{d} = \frac{1}{d} + \frac{d-1}{d} - \frac{d-1}{d} = 1 + -\frac{d-1}{d} \in 1 + (2)^e$$

Therefore, $a/d \in 1 + (2)^e$, as desired. The case $c = -1$ is analogous to the case $c = 1$. □

(b) Let $D = \{2^n \mid n \in \mathbb{Z}_{\geq 0}\}$ and let $R = D^{-1}\mathbb{Z}$. Write down the ideals in R. Which of these ideals are maximal?

Proof. The set of all ideals in R is

$$\boxed{\{(n) : (n, 2) \leq 1\}}$$

By definition, (n) is an ideal in R. Now suppose that I is an arbitrary ideal in R. By Q4.4e and the fact that the ideals of $\mathbb{Z}$ are of the form (n) for some $n \in \mathbb{Z}$, $I = (n)^e$. To verify that $(n)^e = D^{-1}\mathbb{Z}n = (n)$, first let $a/2^m \in (n)^e$. Then since $1/2^m \in R$, $a/2^m = a \cdot (1/2^m) \in (n)$. Now let $na/2^m \in (n)$. Then since $na \in (n)$, $na/2^m \in (n)^e$. Now suppose $(n, 2) > 1$. Then $2 \mid n$ and hence $(n/2)/1 \in (n)$, contradicting the assumption that the generator n is the smallest element of (n).

The maximal ideals in R are the subset of the above consisting of all prime ideals, i.e.,

$$\boxed{\{(n) : n \text{ is prime}\}}$$

We know that every maximal ideal is prime. In the other direction, suppose (n) is a prime ideal. Now suppose for the sake of contradiction that $(n) \subsetneq (m) \subsetneq R$. It follows that $n \in (m)$. Thus, $n = (a/b)m$ for some $a/b \in R$. Consequently, since (n) is a prime ideal, $m \in (n)$ or $a/b \in (n)$. We now divide into two cases. If $m \in (n)$, then $(m) \subset (n)$, a contradiction. If $a/b \in (n)$, then $a/b = n \cdot (c/d)$. Combining this with the result that $n = (a/b)m$, we have that

$$\begin{aligned} n &= \frac{a}{b} \cdot m \\ &= \frac{nc}{d} \cdot m \\ 1 &= \frac{c}{d} \cdot m \end{aligned}$$

But then $1 \in (m)$, and hence $(m) = R$, a contradiction. □

4.6. (a) Define $M_2 : \{\text{commutative rings}\} \to \{\text{sets}\}$ by

$$M_2(R) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in R \right\}$$

Show that for any R, there is a natural bijection between the set $M_2(R)$ and the set S_1 of ring homomorphisms between $\mathbb{Z}[X, Y, Z, W]$ and R. Note that notationally,

$$S_1 = \mathrm{Hom}_{\mathrm{ring}}(\mathbb{Z}[X, Y, Z, W], R)$$

One sometimes says that $\mathbb{Z}[X, Y, Z, W]$ represents the function M_2.

Proof. Define $\psi : M_2(R) \to S_1$ by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \mathrm{ev}_{(a,b,c,d)}$$

We know from class that every evaluation function is a ring homomorphism. Thus, $\mathrm{ev}_{(a,b,c,d)}$ does lie in the correct set.

Injectivity: Suppose

$$\psi \left[\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \right] = \psi \left[\begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \right]$$

Then $\mathrm{ev}_{(a_1,b_1,c_1,d_1)} = \mathrm{ev}_{(a_2,b_2,c_2,d_2)}$. It follows that

$$a_1 = \mathrm{ev}_{(a_1,b_1,c_1,d_1)}(X) = \mathrm{ev}_{(a_2,b_2,c_2,d_2)}(X) = a_2$$

Similar statements hold for b, c, d. Thus, since $x_1 = x_2$ ($x \in \{a, b, c, d\}$), we have that

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}$$

as desired.

Surjectivity: Let $\varphi \in S_1$ be arbitrary. Suppose $\varphi(X) = a$, $\varphi(Y) = b$, $\varphi(Z) = c$, and $\varphi(W) = d$. Since any polynomial in $\mathbb{Z}[X, Y, Z, W]$ is a $\mathbb{Z}$-linear combination of X, Y, Z, W and φ respects these addition and multiplication operations, we have that for any $f \in \mathbb{Z}[X, Y, Z, W]$,

$$\varphi(f) = f(a, b, c, d) = \mathrm{ev}_{(a,b,c,d)}(f)$$

Therefore,

$$\psi \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} \right] = \mathrm{ev}_{(a,b,c,d)} = \varphi$$

as desired. □

(b) (**You do not need to turn in part (b)**, but you are encouraged to think about it.)
Actually, $M_2(R)$ can be naturally given a ring structure: Addition and multiplication are defined using the same procedure as $M_2(\mathbb{R})$ (or with any other field you may have seen). Hence, it makes sense to talk about the units of $M_2(R)$.
Define the set $GL_2(R)$ to be the units of $M_2(R)$, i.e.,

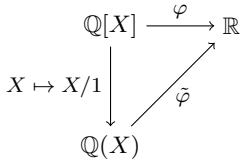
$$GL_2(R) = M_2(R)^\times$$

Show that for any R, there is a natural bijection between $GL_2(R)$ and the set S_2 defined by

$$S_2 = \mathrm{Hom}_{\mathrm{ring}}(\mathbb{Z}[X, Y, Z, W]_{XW-YZ}, R)$$

Note that $\mathbb{Z}[X, Y, Z, W]_{XW-YZ}$ denotes the **localization** of $\mathbb{Z}[X, Y, Z, W]$ by the multiplicative set generated by $XW - YZ$ (that is, the multiplicative set $(1, XW - YZ, (XW - YZ)^2, \dots)$). (Hint: Use the universal property.)
One sometimes says $\mathbb{Z}[X, Y, Z, W]_{XW-YZ}$ represents the function GL_2.

4.7. Let $\mathbb{Q}(X)$ denote the field of fractions of $\mathbb{Q}[X]$. By the universal property of a polynomial ring, we know that giving a ring homomorphism $\varphi : \mathbb{Q}[X] \to \mathbb{R}$ is equivalent to choosing an element $r \in \mathbb{R}$ and setting $\varphi(X) = r$. Which ring homomorphisms $\varphi : \mathbb{Q}[X] \to \mathbb{R}$ extend to ring homomorphisms $\tilde{\varphi} : \mathbb{Q}(X) \to \mathbb{R}$? These ring homomorphisms should satisfy the following commutative diagram.



Proof. We can prove that the set of ring homomorphisms φ which extend to the field of rational functions over $\mathbb{Q}$ is equal to

$$\boxed{\{\varphi : \varphi(X) \text{ is a real transcendental number}\}}$$

Let φ be an element of the above set. Since $\varphi(X) = r$ is transcendental, $\varphi(f) = \mathrm{ev}_r(f) \neq 0$ for any $f \in \mathbb{Q}[X]$. (Note that a similar argument to the surjectivity one used in Q4.6a can justify that $\varphi = \mathrm{ev}_r$.) It follows that if we extend φ to $\mathbb{Q}(X)$ by keeping the evaluation definition (recall that evaluation is always a ring homomorphism), then for any rational function $f/g \in \mathbb{Q}(X)$,

$$\tilde{\varphi}\left(\frac{f}{g}\right) = \left(\frac{f}{g}\right)(r) = \frac{f(r)}{g(r)}$$

where, as established, $g(r)$ is nonzero and hence $\tilde{\varphi}(f/g)$ is well-defined.

Now suppose that $\varphi : \mathbb{Q}[X] \to \mathbb{R}$ is a ring homomorphism that extends to a ring homomorphism $\tilde{\varphi} : \mathbb{Q}(X) \to \mathbb{R}$. Let $\tilde{\varphi}(X) = \varphi(X) = r$. Then as per Q4.6a, $\tilde{\varphi} = \mathrm{ev}_r$. Since $\tilde{\varphi}$ is a ring homomorphism, $\tilde{\varphi}(f/g)$ is well-defined for every $f \in \mathbb{Q}[X]$ and $g \in \mathbb{Q}[X] - \{0\}$. In particular, we must have $0 \neq \tilde{\varphi}(g) = \mathrm{ev}_r(g) = g(r)$ for all such g. It follows by definition that r is a real transcendental number. □

4.8. F is a field. Let R be the smallest subring of $F[X]$ such that (a) $F \subset R$ and (b) both X^2 and X^3 belong to R.

(a) Use the identity $(X^2)^3 = (X^3)^2$ to deduce that R is *not* a UFD.

Proof. Suppose for the sake of contradiction that X^2 is reducible. Then $X^2 = ab$ where $a, b \notin R^\times = F^\times$. It follows since they aren't units that $\deg(a), \deg(b) \geq 1$. But since $\deg(a) + \deg(b) = \deg(ab) = 2$, it must be that $\deg(a) = \deg(b) = 1$. Thus, $a = c_1X + d_1$ and $b = c_2X + d_2$. It follows that

$$X^2 = ab$$
$$1X^2 + 0X + 0 = c_1c_2X^2 + (c_1d_2 + c_2d_1)X + d_1d_2$$

so

$$c_1c_2 = 1 \qquad\qquad d_1d_2 = 0$$

Then $c_1, c_2 \in R^\times = F^\times$ and $d_1 = d_2 = 0$. It follows that $X = c_1c_2X \in R$, and hence $R = F[X]$ by the construction from Lecture 1.2. However, this contradicts the hypothesis that R is the smallest subring of $F[X]$ containing F, X^2, X^3 since $F + (X^2, X^3)$ is an example of a smaller subring of $F[X]$ containing F, X^2, X^3. Therefore, X^2 is irreducible in R.

A similar argument can show that X^3 is irreducible in R.

It follows that two factorizations of X^6 are $(X^2)^3$ and $(X^3)^2$. But since these factorizations have different lengths, they are not equivalent. Therefore, R is not a UFD, as desired. □

(b) Exhibit an ideal I of R that is not a principal ideal.

Proof. Take

$$\boxed{I = (X^2, X^3)}$$

Since both generators are irreducible by part (a), their greatest common divisor is necessarily a unit. Thus, since (X^2, X^3) only consists of polynomials of degree greater than or equal to 2 (i.e., objects that are not units), no element of it can generate both extant generators. Therefore, $(2, X)$ is not principal. □

4.9. Mimic Euclid's proof of the infinitude of primes in $\mathbb{Z}$ to show that $F[X]$ has infinitely many primes for every field F.

Proof. Suppose for the sake of contradiction that $\{f_1, \ldots, f_r\}$ is the set of all primes in $F[X]$. Since $F[X]$ is an ED, it is a PID. Thus, the primes and irreducibles coincide. Likewise, $F[X]$ being an ED makes it a UFD. Thus, the element $f_1 \cdots f_r + 1$ (for example) has a unique factorization in terms of $f_1, \ldots, f_r$. In particular, since each f_i irreducible and hence not a unit, $\deg(f_i) \geq 1$ $(i = 1, \ldots, r)$. This means that $\deg(f_1 \cdots f_r + 1) \geq r$ so $f_1 \cdots f_r + 1$ is not a unit. It follows that there exists at least one f_i such that $f_i \mid f_1 \cdots f_r + 1$. Additionally, $f_i \mid f_1 \cdots f_r$. Thus, $f_i \mid f_1 \cdots f_r + 1 - f_1 \cdots f_r = 1$. Therefore, f_i is a unit, a contradiction. □

4.10. Let R be an integral domain and let d be the degree of a nonzero $f \in R[X]$. Prove that $\{a \in R \mid f(a) = 0\}$ is finite. *Hint*: Case 1 — first prove this when R is a field. Case 2 — reduce to case 1 by looking at the fraction field of R.

Proof. Let $A = \{a \in R \mid f(a) = 0\}$. We induct on d. For the base case $d = 0$, let $f \in R[X]$ be an arbitrary nonzero polynomial having $\deg(f) = d = 0$. It follows that $f(X) = a$ for some nonzero $a \in R$. Thus, since $f(X) \neq 0$ for any X, $|A| = 0$ and we have the desired result. Now suppose inductively that we have proven the claim for $d - 1$; we now wish to prove it for degree d. Once again, let $f \in R[X]$ be an arbitrary nonzero polynomial having $\deg(f) = d$. If f has no roots, then we are done. Otherwise, pick $a \in A$. By the Euclidean algorithm, $f(X) = q(X) \cdot (X - a) + r$ for some $q, r \in R[X]$ with $\deg r < \deg(X - a)$. It follows from the latter constraint that $r \in R$ is a constant. In particular,

$$r = f(a) - q(a) \cdot (a - a) = 0 - q(a) \cdot 0 = 0$$

Thus, $f = q \cdot (X - a)$. It follows that

$$\begin{aligned} \deg(f) &= \deg(q) + \deg(X - a) \\ d &= \deg(q) + 1 \\ \deg(q) &= d - 1 \end{aligned}$$

Thus, by the induction hypothesis, q has finitely many roots. This combined with the fact that $X - a$ has only one root (additive inverses are unique in rings, so only $a + (-a) = 0$) implies that f has at most one more root than q, i.e., f has finitely many roots, as desired. □

5 Misc. Ring Tools

2/10: **5.1.** Let M and m denote the lcm and gcd of natural numbers a, b.

(i) Prove that there is an isomorphism of rings

$$\phi : \mathbb{Z}/(a) \times \mathbb{Z}/(b) \to \mathbb{Z}/(M) \times \mathbb{Z}/(m)$$

Hint: Chinese Remainder Theorem.

Proof. Let $a = p_1^{e_1} \cdots p_n^{e_n}$ and $b = p_1^{f_1} \cdots p_n^{f_n}$, where $e_i, f_i \geq 0$ $(i = 1, \ldots, n)$ and we pick all primes to be greater than zero to obviate the need for multiplication by a unit (1 or -1 in this case). It follows that $ab = p_1^{e_1+f_1} \cdots p_n^{e_n+f_n}$. We know from Proposition 8.13 that we can pick $m = p_1^{\min(e_1,f_1)} \cdots p_n^{\min(e_n,f_n)}$. Additionally, since $ab = mM$, we know that we can pick

$$M = p_1^{e_1+f_1-\min(e_1,f_1)} \cdots p_n^{e_n+f_n-\min(e_n,f_n)} = p_1^{\max(e_1,f_1)} \cdots p_n^{\max(e_n,f_n)}$$

By the Chinese Remainder Theorem (CRT), or more directly Corollary 7.18, we know that

$$\mathbb{Z}/(a) = \mathbb{Z}/(p_1^{e_1}) \times \cdots \times \mathbb{Z}/(p_n^{e_n}) \qquad \mathbb{Z}/(b) = \mathbb{Z}/(p_1^{f_1}) \times \cdots \times \mathbb{Z}/(p_n^{f_n})$$

Thus,

$$\mathbb{Z}/(a) \times \mathbb{Z}/(b) \cong \mathbb{Z}/(p_1^{e_1}) \times \cdots \times \mathbb{Z}/(p_n^{e_n}) \times \mathbb{Z}/(p_1^{f_1}) \times \cdots \times \mathbb{Z}/(p_n^{f_n})$$

Similarly,

$$\mathbb{Z}/(M) \times \mathbb{Z}/(m) \cong \mathbb{Z}/(p_1^{\max(e_1,f_1)}) \times \cdots \times \mathbb{Z}/(p_n^{\max(e_n,f_n)}) \times \mathbb{Z}/(p_1^{\min(e_1,f_1)}) \times \cdots \times \mathbb{Z}/(p_n^{\min(e_n,f_n)})$$

For every $i = 1, \ldots, n$, there are two relevant terms in the above direct product: $\mathbb{Z}/(p_i^{\max(e_i,f_i)})$ and $\mathbb{Z}/(p_i^{\min(e_i,f_i)})$. We divide into two cases ($\min(e_i, f_i) = e_i$ and $\min(e_i, f_i) = f_i$). If $\min(e_i, f_i) = e_i$, then $\max(e_i, f_i) = f_i$ (this holds true even when $e_i = f_i$). Thus,

$$\mathbb{Z}/(p_i^{\min(e_i,f_i)}) = \mathbb{Z}/(p_i^{e_i}) \qquad \mathbb{Z}/(p_i^{\max(e_i,f_i)}) = \mathbb{Z}/(p_i^{f_i})$$

It follows that the i^{th} and $(n+i)^{\text{th}}$ slots in the direct product expansions of $\mathbb{Z}/(a) \times \mathbb{Z}/(b)$ and $\mathbb{Z}/(M) \times \mathbb{Z}/(m)$ above are identical. Now suppose $\min(e_i, f_i) = f_i$. Then for a similar reason to the previous case,

$$\mathbb{Z}/(p_i^{\min(e_i,f_i)}) = \mathbb{Z}/(p_i^{f_i}) \qquad \mathbb{Z}/(p_i^{\max(e_i,f_i)}) = \mathbb{Z}/(p_i^{e_i})$$

Thus, since the direct product operation is commutative,[10] we may flip the entries in the i^{th} and $(n+i)^{\text{th}}$ slots in the direct product expansion of $\mathbb{Z}/(M) \times \mathbb{Z}/(m)$ and still have an isomorphic ring. Doing this for all i proves that

$$\begin{aligned}&\mathbb{Z}/(p_1^{e_1}) \times \cdots \times \mathbb{Z}/(p_n^{e_n}) \times \mathbb{Z}/(p_1^{f_1}) \times \cdots \times \mathbb{Z}/(p_n^{f_n}) \\ &\cong \mathbb{Z}/(p_1^{\max(e_1,f_1)}) \times \cdots \times \mathbb{Z}/(p_n^{\max(e_n,f_n)}) \times \mathbb{Z}/(p_1^{\min(e_1,f_1)}) \times \cdots \times \mathbb{Z}/(p_n^{\min(e_n,f_n)})\end{aligned}$$

and hence by transitivity that

$$\mathbb{Z}/(a) \times \mathbb{Z}/(b) \cong \mathbb{Z}/(M) \times \mathbb{Z}/(m)$$

Stating that two sets are isomorphic as rings is equivalent to stating that there exists an isomorphism of rings

$$\phi : \mathbb{Z}/(a) \times \mathbb{Z}/(b) \to \mathbb{Z}/(M) \times \mathbb{Z}/(m)$$

so we are done. □

[10] Ray said that this assertion need not be justified further.

(ii) Find necessary and sufficient conditions for uniqueness of the ϕ. *Hint*: Do this first when $a = p^c$ and $b = p^d$, where p is prime.

Proof. Let $a = p_1^{e_1} \cdots p_n^{e_n}$ and $b = p_1^{f_1} \cdots p_n^{f_n}$. Then a necessary and sufficient condition for the uniqueness of ϕ is that

$$\boxed{e_i \neq f_i \ \forall \ i = 1, \ldots, n}$$

□

(iii) Prove that the condition you provided for part (ii) is sufficient.

Proof. Taking the hint from part (ii), we first treat the case where $a = p^c$ and $b = p^d$. WLOG, let $c \leq d$, in agreement with part (ii). Suppose that $a \neq b$. Then $c < d$. Since ϕ is a ring homomorphism, we know that $\phi(1,1) = (1,1)$.

Now let's investigate the behavior of $\phi(1,0)$ and $\phi(0,1)$. Let $\phi(1,0) = (\gamma, \delta)$. Since $(1,0)$ is idempotent, i.e., $(1,0)^2 = (1,0)$, we have that

$$\begin{aligned} \phi[(1,0)^2] &= \phi(1,0) \\ (\gamma,\delta)^2 &= (\gamma,\delta) \\ (\gamma^2,\delta^2) &= (\gamma,\delta) \\ (\gamma^2-\gamma,\delta^2-\delta) &= (0,0) \end{aligned}$$

Consider $\gamma(\gamma-1) = 0$. It follows that $\gamma, \gamma-1$ are zero divisors. Hence, at *least* one of $\gamma, \gamma-1$ is a multiple of p. Additionally, since $p \geq 2$ and $\gamma, \gamma-1$ are offset by 1, we know that p divides at *most* one of these. Thus, we divide into two cases ($p \mid \gamma$ and $p \mid \gamma - 1$). Suppose first that $p \mid \gamma$. Then since the units of $\mathbb{Z}/p^n\mathbb{Z}$ are the integers coprime to p, we know that $\gamma - 1$ is a unit. It follows that there exists an element $(\gamma-1)^{-1}$ and thus that

$$\begin{aligned} 0 &= (\gamma-1)^{-1} \cdot \gamma(\gamma-1) \\ 0 &= \gamma \end{aligned}$$

In the case $p \mid \gamma - 1$, we similarly derive that $0 = \gamma - 1$, or $\gamma = 1$. Thus, $\gamma \in \{1, 0\}$. Similarly, $\delta \in \{1, 0\}$.

Now suppose $\gamma = \delta = 1$. Then $\phi(1,1) = (1,1) = \phi(1,0)$ and ϕ is not an isomorphism, a contradiction. Similarly, if $\gamma = \delta = 0$, then $\phi(0,0) = (0,0) = \phi(1,0)$, which is the same contradiction. Therefore, $\phi(1,0) \in \{(1,0),(0,1)\}$.

It follows by a symmetric argument that $\phi(0,1) \in \{(1,0),(0,1)\}$. For the same isomorphism reason, $\phi(1,0)$ and $\phi(0,1)$ must equal distinct elements. Thus, ϕ can be two possible isomorphisms, since the values of $\phi(1,0)$ and $\phi(0,1)$ determine all other values of ϕ.

We now invoke the condition that $c < d$. We know that $(1,0)^{p^c} = (0,0)$. Suppose $\phi(1,0) = (0,1)$. It follows that $\phi[(1,0)^{p^c}] = (0,p^c) \neq (0,0)$, we have a contradiction. Therefore, we must have that ϕ is the identity isomorphism.

Now suppose that a, b have more complex prime factorizations. In particular, let $a = p_1^{e_1} \cdots p_n^{e_n}$ and $b = p_1^{f_1} \cdots p_n^{f_n}$. The existence of ϕ implies the existence of an isomorphism

$$\begin{aligned} \psi : &\mathbb{Z}/(p_1^{e_1}) \times \cdots \times \mathbb{Z}/(p_n^{e_n}) \times \mathbb{Z}/(p_1^{f_1}) \times \cdots \times \mathbb{Z}/(p_n^{f_n}) \\ &\to \mathbb{Z}/(p_1^{\max(e_1,f_1)}) \times \cdots \times \mathbb{Z}/(p_n^{\max(e_n,f_n)}) \times \mathbb{Z}/(p_1^{\min(e_1,f_1)}) \times \cdots \times \mathbb{Z}/(p_n^{\min(e_n,f_n)}) \end{aligned}$$

Defining a restriction isomorphism to the n sets consisting of elements where only the p_i slots are nonzero, ψ induces n isomorphisms of the kind treated above. We know that all of these are unique. Thus, reassembling ψ, we have a unique isomorphism. It follows that ϕ is a unique isomorphism. □

5.2. The Euclidean algorithm for monic polynomials is valid for every commutative ring, but it does not provide a method of obtaining the gcd because the "remainder" may not have a unit as its leading coefficient, so we cannot proceed by induction. But we may get lucky:

(i) Prove that the ideal generated by $X^m - 1$ and $X^n - 1$ in $\mathbb{Z}[X]$ is the principal ideal $(X^d - 1)$, where $d = \gcd(m, n)$.

Proof. We will prove that $(X^m - 1, X^n - 1) = (X^d - 1)$ via a bidirectional inclusion proof. Suppose first that $p \in (X^m - 1, X^n - 1)$. Then there exist polynomials $a, b \in \mathbb{Z}[X]$ such that $p(X) = a(X) \cdot (X^m - 1) + b(X) \cdot (X^n - 1)$. Now since $d = \gcd(m, n)$, there exist s, t such that $m = sd$ and $n = td$. Using s, t, we may write

$$X^m - 1 = (X^d - 1) \cdot \sum_{i=0}^{s-1} X^{di} \qquad X^n - 1 = (X^d - 1) \cdot \sum_{i=0}^{t-1} X^{di}$$

Therefore,

$$\begin{aligned} p(X) &= a(X) \cdot (X^m - 1) + b(X) \cdot (X^n - 1) \\ &= a(X) \cdot (X^d - 1) \cdot \sum_{i=0}^{s-1} X^{di} + b(X) \cdot (X^d - 1) \cdot \sum_{i=0}^{t-1} X^{di} \\ &= \left[a(X) \cdot \sum_{i=0}^{s-1} X^{di} + b(X) \cdot \sum_{i=0}^{t-1} X^{di} \right] \cdot (X^d - 1) \\ &\in (X^d - 1) \end{aligned}$$

as desired.

On the other hand, suppose that $p \in (X^d - 1)$. Then there exists a polynomial $a \in \mathbb{Z}[X]$ such that $p(X) = a(X) \cdot (X^d - 1)$. WLOG let $n \leq m$. Then since

$$X^m - 1 = X^{m-n}(X^n - 1) + (X^{m-n} - 1)$$

we see that we can actually invoke a Euclidean algorithm for monic polynomials here. Thus, continuing, we will eventually reach $X^d - 1$ and thus can rewrite

$$X^d - 1 = b(X) \cdot (X^m - 1) + c(X) \cdot (X^n - 1)$$

Therefore,

$$\begin{aligned} p(X) &= a(X) \cdot (X^d - 1) \\ &= a(X) \cdot [b(X) \cdot (X^m - 1) + c(X) \cdot (X^n - 1)] \\ &= a(X)b(X) \cdot (X^m - 1) + a(X)c(X) \cdot (X^n - 1) \\ &\in (X^m - 1, X^n - 1) \end{aligned}$$

as desired. □

(ii) Deduce that $\gcd(q^m - 1, q^n - 1) = (q^d - 1)$ for every integer q.

Proof. Consider the evaluation homomorphism $\mathrm{ev}_q : \mathbb{Z}[X] \to \mathbb{Z}$. Since every integer $z \in \mathbb{Z}$ is an element of $\mathbb{Z}[X]$, ev_q is surjective. It follows by Exercise 7.3.24(b) of Dummit and Foote (2004) (proven in HW2) that ev_q sends ideals to ideals. Thus, under ev_q,

$$(X^m - 1, X^n - 1) \mapsto (q^n - 1, q^m - 1) \qquad (X^d - 1) \mapsto (q^d - 1)$$

It follows since $(X^m - 1, X^n - 1) = (X^d - 1)$ as per part (i) that $(q^n - 1, q^m - 1) = (q^d - 1)$, and hence $\gcd(q^m - 1, q^n - 1) = (q^d - 1)$, as desired. □

5.3. Let K be the quotient field of a UFD R. If $f \in R[X]$ is a monic polynomial, $c \in K$, and $f(c) = 0$, then $c \in R$.

Proof. Since $f(c) = 0$, it follows that

$$f(X) = q(X) \cdot (X - c)$$

for some $q \in K[X]$. Note that since f is monic, q must have leading coefficient 1. The main takeaway from the above equation is that f is reducible in $K[X]$. Thus, since R is a UFD, $\operatorname{Frac} R = K$, $f \in R[X]$, and f is reducible in $K[X]$, Gauss' Lemma asserts that there exist $r, s \in K$ such that $rq, s(X - c) \in R[X]$ and

$$f(X) = rq(X) \cdot s(X - c)$$

is a factorization of f in $R[X]$. But since $q, (X - c)$ have leading coefficient 1 and f is monic, we must have $rs = 1$. Therefore,

$$f(X) = q(X) \cdot (X - c)$$

is a factorization in $R[X]$. In particular, $X - c \in R[X]$, meaning that $c \in R$, as desired. □

5.4. State whether true or false. If false, give a counterexample.

(i) If R is a UFD, then $D^{-1}R$ is a UFD.

Answer. True. □

(ii) Let K be the field of fractions of a PID R. If $R \subset A \subset K$ is a chain of rings, then $A = D^{-1}R$ for some multiplicative subset D of R.

Answer. True. □

(iii) Same problem as in (ii), except that now R is a UFD.

Answer. True. □

(iv) Let K be the field of fractions of an integral domain R. If D_1, D_2 are multiplicative subsets of R, then $D_1^{-1}R$ and $D_2^{-1}R$ are subrings of K. If $D_1^{-1}R = D_2^{-1}R$, then $D_1 = D_2$.

Answer. False.
Let $R = \mathbb{Z}$. Pick $D_1 = \mathbb{N}$ and $D_2 = \mathbb{Z} - \{0\}$. Then since $D_1 \subset D_2$, any $a/b \in D_1^{-1}R$. If $a/b \in D_2^{-1}R$, then we divide into two cases. If the denominator is positive, we are done. If the denominator is negative, represent the fraction by another member of the equivalence class: $-a/-b \in D_1^{-1}R$. □

5.5. Let $f \in \mathbb{Z}[X]$ be a polynomial with content 1. Let p be prime and let $\bar{f}$ denote the image of f in $\mathbb{F}_p[X]$. If $\deg(f) = \deg(\bar{f})$ and $\bar{f}$ is irreducible, show that f is irreducible in $\mathbb{Z}[X]$.

Proof. To prove that f is irreducible in $\mathbb{Z}[X]$, it will suffice to show that for any factorization $f = qh$ of f, q or h is a unit. Let $f = qh$, let $d = \deg(f)$, and let $\pi : \mathbb{Z}[X] \to \mathbb{F}_p[X]$. We have that

$$\bar{f} = \pi(f) = \pi(qh) = \pi(q)\pi(h) = \bar{q} \cdot \bar{h}$$

Since $\bar{f}$ is irreducible, either $\bar{q}$ or $\bar{h}$ is a unit in $\mathbb{F}_p[X]$. WLOG, let $\bar{h}$ be a unit. Then $\deg(\bar{h}) = 0$. Thus,

$$\deg(\bar{q}) = \deg(\bar{f}) - \deg(\bar{h}) = d - 0 = d$$

It follows since $\deg(q) \geq \deg(\bar{q})$ that $\deg(q) = d$, and hence $\deg(h) = 0$ as well. Consequently, h is an integer. Moreover, since $c(f) = 1$, $h \mid 1$, so $h = \pm 1$, i.e., is a unit. Therefore, f is irreducible in $\mathbb{Z}[X]$. □

5.6. If R is a (commutative) ring of characteristic p, where p is prime, show that $(a+b)^p = a^p + b^p$.

Proof. By the binomial theorem,

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} y^k = \sum_{k=0}^{p} \frac{p!}{k!(p-k)!} a^{p-k} y^k$$

It follows that in all cases except when $k = 0, p$, the coefficient is a multiple of p. In particular, if the coefficient is a multiple of p in a ring of characteristic p, the coefficient is equal to zero. Therefore, all terms save the $k = 0$ and $k = p$ terms disappear, leaving only

$$(a+b)^p = a^p + b^p$$

as desired. □

6 Getting Comfortable With Modules

All modules considered are left modules. Given A-modules M, N, the set of all A-module homomorphisms from $M \to N$ is denoted by $\mathrm{Hom}_A(M, N)$. It is an additive abelian group.

2/17: **6.1.** Let M be an A-module and let $e : M \to M$ be an A-module homomorphism satisfying $e \circ e = e$. We have shown that both $e(M)$ and $\ker(e)$ are submodules of M.

(i) Prove that $\phi : e(M) \oplus \ker(e) \to M$ given by $\phi(v, w) = v + w$ for all $v \in e(M)$, $w \in \ker(e)$ is an isomorphism of A-modules.

(ii) Define $P : e(M) \oplus \ker(e) \to e(M) \oplus \ker(e)$ by $P(v, w) = (v, 0)$ for all $(v, w) \in e(M) \oplus \ker(e)$. Prove that $P = \phi^{-1} \circ e \circ \phi$.

6.2. Let $f : M \to N$ and $g : N \to M$ be A-module homomorphisms such that $g(f(m)) = m$ for all $m \in M$. Prove that $H : M \oplus \ker(g) \to N$ given by $H(m, n) = f(m) + n$ for all $m \in M$, $n \in \ker(g)$ is an isomorphism of A-modules.

Proof. To prove the claim, we will apply Problem 6.1(i). In particular, we will first define a relevant helper function e and show that it satisfies the same properties as the e from Problem 6.1. We will use this e to define an isomorphism $\phi : e(N) \oplus \ker(e) \to N$, in line with Problem 6.1. Lastly, we will show that there is an isomorphism $\psi : M \oplus \ker(g) \to e(N) \oplus \ker(e)$ and define H to be the composition isomorphism $\phi \circ \psi$. Let's begin.

Define $e : N \to N$ by $e = f \circ g$. By Proposition 10.2, e is an A-module homomorphism. Additionally, we can demonstrate that $e \circ e = e$: If we let $n \in N$ be arbitrary, then we have

$$\begin{aligned}(e \circ e)(n) &= (f \circ g \circ f \circ g)(n) \\ &= f((g \circ f)(g(n))) \\ &= f(g(n)) \\ &= (f \circ g)(n) \\ &= e(n)\end{aligned}$$

as desired. Therefore, by Problem 6.1(i), there exists an A-module isomorphism $\phi : e(N) \oplus \ker(e) \to N$ defined by $\phi(v, w) = v + w$ for all $v \in e(N)$, $w \in \ker(e)$.

Moving on, we can show that $M \cong e(N)$. In particular, since $g(f(m)) = m$ for all $m \in M$ by hypothesis, we know that f is injective and g is surjective. It follows from the latter statement that $g(N) = M$. Thus, combining results, we have that

$$M \cong f(M) = f(g(N)) = (f \circ g)(N) = e(N)$$

where the isomorphism is given by $\tilde{f} : M \to e(N)$ defined by $\tilde{f}(m) = f(m)$ for all $m \in M$.

Next, we can show that $\ker(e) = \ker(g)$. Suppose first that $n \in \ker(e)$. Then $e(n) = 0$. It follows by the definition of e that $f(g(n)) = 0$. Additionally, we know that $f(0) = 0$ since f is a group homomorphism (as an A-module homomorphism). Thus, by transitivity, $f(g(n)) = f(0)$. It follows since f is injective (as stated above) that $g(n) = 0$. Therefore, $n \in \ker(g)$ by definition, as desired. Now suppose that $n \in \ker(g)$. Then $g(n) = 0$. It follows for analogous reasons to the other direction (e.g., f is a group homomorphism; definition of e) that $e(n) = f(g(n)) = f(0) = 0$. Therefore, $n \in \ker(e)$ by definition, as desired.

At this point, we may define $\psi : M \oplus \ker(g) \to e(N) \oplus \ker(e)$ by $\psi(m, n) = (\tilde{f}(m), \mathrm{id}(n))$ for all $(m, n) \in M \oplus \ker(g)$. As a componentwise A-module isomorphism, ψ is also an A-module isomorphism, itself (see the analogous justification in Problem 3.2). Thus, we may define the A-module isomorphism $H = \phi \circ \psi$, where the fact that H is an A-module homomorphism is justified by Proposition 10.2 and the fact that it is bijective follows from the bijectivity of both ϕ, ψ. H, as defined, maps the correct sets (i.e., $M \oplus \ker(g) \to N$) and has the correct rule:

$$H(m, n) = (\phi \circ \psi)(m, n) = \phi(\psi(m, n)) = \phi(\tilde{f}(m), n) = \phi(f(m), n) = f(m) + n$$

□

6.3. Let $\phi : A \to B$ be a ring homomorphism, and let M be a B-module. Show that $\cdot : A \times M \to M$ defined by

$$(a, m) \mapsto \phi(a)m$$

for all $a \in A$, $m \in M$ gives M the structure of an A-module.

In particular, every B-module M has the structure of an A module for every subring A of B.

A very important application of this observation ($F[X]$-modules) is discussed on Dummit and Foote (2004, p. 340); it will be all-important later on in this course.

6.4. Let K be the fraction field of an integral domain R. Let V and W be K-modules (i.e., vector spaces over the field K). The preceding problem shows that V and W are also R-modules in a natural manner.

Prove that every R-module homomorphism $f : V \to W$ is also a K-module homomorphism (it has to be shown that $f(av) = af(v)$ for all $a \in K$, $v \in V$).

Proof. Let $a \in K$ and $v \in V$ be arbitrary. Suppose $a = b/c$, where $b, c \in R$. Then

$$af(v) = \frac{b}{c}f(v) = \frac{1}{c}f(bv) = \frac{1}{c}f(acv) = \frac{c}{c}f(av) = 1f(av) = f(av)$$

as desired. □

6.5. With K, R, V, W as in the preceding problem, let M be an R-submodule of V. Assume that for every $v \in V$, there is a nonzero $a \in R$ such that $av \in M$. Let $f : M \to W$ be an R-module homomorphism. Prove that f extends in a unique manner to a K-module homomorphism $F : V \to W$.

Proof. Define $F : V \to W$ by

$$F(v) = \frac{1}{a}f(av)$$

for all $v \in V$, where $a \in R$ satisfies $av \in M$.

To prove that F is well-defined, it will suffice to show that for all $a, b \in R$ satisfying $av, bv \in M$, we have that $f(av)/a = f(bv)/b$. Let a, b be arbitrary elements of R satisfying the desired property. Then

$$\frac{1}{a}f(av) = \frac{ab}{a^2b}f(av) = \frac{1}{a^2b}f(a^2bv) = \frac{a^2}{a^2b}f(bv) = \frac{1}{b}f(bv)$$

as desired.

To prove that F is a homomorphism of abelian groups, it will suffice to show that $F(v_1 + v_2) = F(v_1) + F(v_2)$ for all $v_1, v_2 \in V$. Let $v_1, v_2 \in V$ be arbitrary. Suppose

$$F(v_1 + v_2) = \frac{1}{a}f(a(v_1 + v_2)) \qquad F(v_1) = \frac{1}{b}f(bv_1) \qquad F(v_2) = \frac{1}{c}f(cv_2)$$

for some $a, b, c \in R$. Then

$$\begin{aligned} F(v_1) + F(v_2) &= \frac{1}{b}f(bv_1) + \frac{1}{c}f(cv_2) \\ &= \frac{cf(bv_1) + bf(cv_2)}{bc} \\ &= \frac{1}{bc}f(bc(v_1 + v_2)) \\ &= \frac{1}{a}f(a(v_1 + v_2)) \\ &= F(v_1 + v_2) \end{aligned}$$

as desired, where the fourth equality holds by the above argument used to show that F is well-defined.

To prove that F is a K-module homomorphism, it will suffice to additionally show that $F(kv) = kF(v)$ for all $k \in K$ and $v \in V$. Let $k = l/n \in K$ and $v \in V$ be arbitrary. Then

$$kF(v) = \frac{l}{n} \cdot \frac{1}{a} f(av) = \frac{1}{a} f(a(kv)) = F(kv)$$

as desired.

To prove that F is an extension of f, it will suffice to show that for all $m \in M$, $F(m) = f(m)$. Let $m \in M$ be arbitrary. Then

$$F(m) = \frac{1}{a} f(am) = \frac{a}{a} f(m) = f(m)$$

as desired.

To prove that F is unique, it will suffice to show that if $\tilde{F} : V \to W$ is an extension of f to V, then $F = \tilde{F}$. Let $v \in V$ be arbitrary. Then

$$F(v) = \frac{1}{a} f(av) = \frac{1}{a} \tilde{F}(av) = \frac{a}{a} \tilde{F}(v) = \tilde{F}(v)$$

where the second equality holds because $\tilde{F} = f$ on M by definition and $av \in M$. □

6.6. We have shown in class that every A-module homomorphism $T : A^n \to M$ (where M is an A-module) is given by

$$T(a_1, \ldots, a_n) = a_1 v_1 + \cdots + a_n v_n$$

for all $(a_1, \ldots, a_n) \in A^n$ and some $v_1, \ldots, v_n \in M$. This gives a bijection between $\mathrm{Hom}_A(A^n, M)$ and M^n.

Now let $c = (c_1, \ldots, c_n) \in A^n$. We have the A-submodule $Ac = \{ac : a \in A\}$ of A^n and the quotient module A^n/Ac. Show that there is a bijection from the set of A-module homomorphisms $S : A^n/Ac \to M$ and a certain additive subgroup G of M^n. Describe G explicitly.

Hint: Given S, consider the composite $A^n \to A^n/Ac \xrightarrow{S} M$.

Proof. Let

$$\boxed{G = \{(v_1, \ldots, v_n) \in M^n : c_1 v_1 + \cdots + c_n v_n = 0\}}$$

To confirm that G is an additive subgroup of M^n, Proposition 2.1 tells us that it will suffice to show that $G \neq \emptyset$ and $x, y \in G$ implies $x - y \in G$. Since $c_1 \cdot 0 + \cdots + c_n \cdot 0 = 0$, $(0, \ldots, 0) \in G$ and hence $G \neq \emptyset$, as desired. Now suppose $(v_1, \ldots, v_n), (w_1, \ldots, w_n) \in G$. Then $c_1 v_1 + \cdots + c_n v_n = 0$ and $c_1 w_1 + \cdots + c_n w_n = 0$. It follows that

$$\begin{aligned} 0 &= (c_1 v_1 + \cdots + c_n v_n) - (c_1 w_1 + \cdots + c_n w_n) \\ &= c_1(v_1 - w_1) + \cdots + c_n(v_n - w_n) \end{aligned}$$

and hence $(v_1, \ldots, v_n) - (w_1, \ldots, w_n) = (v_1 - w_1, \ldots, v_n - w_n) \in G$, as desired.

We define $\phi : G \to \mathrm{Hom}_A(A^n/Ac, M)$ by

$$\phi(v_1, \ldots, v_n) = \Big[S : (a_1, \ldots, a_n) + Ac \mapsto a_1 v_1 + \cdots + a_n v_n \Big]$$

We first show that ϕ is injective. Suppose $\phi(v_1, \ldots, v_n) = \phi(w_1, \ldots, w_n)$. Then $S_v = S_w$. In particular,

$$v_i = S_v(e_i + Ac) = S_w(e_i + Ac) = w_i$$

for all $1 \leq i \leq n$. Therefore, since each component is equal, we must have $(v_1, \ldots, v_n) = (w_1, \ldots, w_n)$, as desired.

We now show that ϕ is surjective. Let $S \in \mathrm{Hom}_A(A^n/Ac, M)$ be arbitrary. Consider $\pi : A^n \to A^n/Ac$ and $T = S \circ \pi$. Since $T : A^n \to M$ is an A-module homomorphism, there exist $v_1, \ldots, v_n \in M$ such that for all $(a_1, \ldots, a_n) \in A^n$, $T(a_1, \ldots, a_n) = a_1v_1 + \cdots + a_nv_n$. It follows that

$$\begin{aligned} a_1v_1 + \cdots + a_nv_n &= (S \circ \pi)(a_1, \ldots, a_n) \\ &= S[(a_1, \ldots, a_n) + Ac] \end{aligned}$$

so $S = \phi(v_1, \ldots, v_n)$, as desired.

It follows that $\phi^{-1} : \mathrm{Hom}(A^n/Ac, M) \to G$ is the desired isomorphism. □

6.7. Let $c = (c_1, \ldots, c_n) \in A^n$. Assume that the *right* ideal $c_1A + \cdots + c_nA$ equals A itself.

(i) Prove that there is a left A-module homomorphism $g : A^n \to A$ such that $g(c) = 1$.

Proof. Since $A = c_1A + \cdots + c_nA$ by hypothesis, there exist $v_1, \ldots, v_n \in A$ such that $1 = c_1v_1 + \cdots + c_nv_n$. Define $g : A^n \to A$ by

$$g(a_1, \ldots, a_n) = a_1v_1 + \cdots + a_nv_n$$

Since A is an A-module and g is of the form specified in class (and in the statement of Problem 6.6), we know that g is a left A-module homomorphism. Moreover, we have that

$$g(c) = g(c_1, \ldots, c_n) = c_1v_1 + \cdots + c_nv_n = 1$$

as desired. □

(ii) Deduce that there is an isomorphism $A \oplus \ker(g) \to A^n$ of left A-modules. *Hint*: Problem 6.2.

Proof. Taking the hint, we build up to the point where we can apply Problem 6.2.

Define $f : A \to A^n$ by $f(a) = ac$. Per Lecture 6.1, this instance of left multiplication (like all others) constitutes an A-module homomorphism. Additionally, define $g : A^n \to A$ as in part (i). It follows from part (i) that g is an A-module homomorphism as well. Furthermore, we have for all $a \in A$ that

$$(g \circ f)(a) = g(f(a)) = g(ac) = ag(c) = a \cdot 1 = a$$

Therefore, by Problem 6.2, $A \oplus \ker(g) \cong A^n$, as desired. □

6.8. Assume that A is a commutative ring. Prove that if M is an A-module such that $M \oplus A \cong A^2$, then there is an A-module isomorphism $A \to M$.

Proof.

- Let $\phi : M \oplus A \to A^2$ denote the given isomorphism.
- By definition ($\phi^{-1} = \phi^{-1}$ and $i^{-1} = \pi_2$), the diagram

$$A \xhookrightarrow{i} M \oplus A \xrightarrow{\phi} A^2 \xrightarrow{\phi^{-1}} M \oplus A \xrightarrow{\pi_2} A$$

  commutes. *draw nicely.*
  - Lecture 6.1: i, π_2 are A-module homomorphisms, too.
- To define $\psi : A \to M$, it will suffice to define $\psi(1)$.
- $i(1) = (0, 1)$.
- Let $(a, b) := \phi(0, 1)$.
- Let $(m_1, c) := \phi^{-1}(0, 1)$.
- Let $(m_2, d) := \phi^{-1}(1, 0)$.
- Relating the values a, b, c, d.
  - Since the above diagram commutes, we have that

$$\begin{aligned} 1 &= (\pi_2 \circ \phi^{-1} \circ \phi \circ i)(1) \\ &= \pi_2(\phi^{-1}(\phi(i(1)))) \\ &= \pi_2(\phi^{-1}(\phi(0, 1))) \\ &= \pi_2(\phi^{-1}(a, b)) \\ &= \pi_2(\phi^{-1}[a(1, 0) + b(0, 1)]) \\ &= a\pi_2(\phi^{-1}(1, 0)) + b\pi_2(\phi^{-1}(0, 1)) \\ &= a\pi_2(m_2, d) + b\pi_2(m_1, c) \\ &= ad + bc \end{aligned}$$

- Prove that $T : A \to A^2$ defined by $a \mapsto a(-d, c)$ is an injective A-module homomorphism.
  - A-module homomorphism: It's just right multiplication.
  - Injectivity: Apply the cancellation lemma for nonzero $(-d, c)$.
  - Surjectivity:
    - We start with

$$\{(u, v) \in A^2 : \phi^{-1}(u, v) \in M \oplus 0\} = \{(u, v) \in A^2 : uc + vd = 0\}$$

    - We have

$$ub = -kdb = k(ac - 1) = kac - k = av - k$$

      so $k = av - ub$. Indeed,

$$kc = avc - ubc = v(1 - bd) - ubc = v - bd - bcu = v - bd + vd$$

    - We want to find (u, v) such that $(u, v) = k(-d, c)$. $\phi(m, 0)$.
    - Swap $(-d, c)$ for $(-c, d)$??
- Use the "injectivity" and "surjectivity" of ϕ^{-1}, π_2 to complete the proof.

□

6.9. Let R be a commutative ring. Assume that there are $x, y, z \in R$ such that $x^2 + y^2 + z^2 = 1$. Define $f : R^3 \to R$ by $f(a, b, c) = ax + by + cz$. Let $M = \ker(f)$.

Prove that there is an R-module isomorphism $M \oplus R \to R^3$.

Note: However, M need not be isomorphic to R^2. For example, if $R = \mathbb{R}[X, Y, Z]/(X^2+Y^2+Z^2-1)$ and x, y, z are $\bar{X}, \bar{Y}, \bar{Z}$, respectively, here M is not isomorphic to R^2. This is saying that the tangent bundle of the two-sphere is nontrivial. It is proved using Algebraic Topology, but purely algebraic proofs exist.

Proof. Since $M = \ker(f)$ and $\oplus$ is commutative, $M \oplus R \cong R \oplus \ker(f)$. Thus, we need only prove that there is an isomorphism $R \oplus \ker(f) \to R^3$. To do so, Problem 6.7 tells us that it will suffice to show that $c = (x, y, z) \in R^3$, $xR + yR + zR = R$, and $f : R^3 \to R$ satisfies $f(c) = 1$. Let's begin.

For the first claim, we have by definition that $c \in R^3$.

For the second claim, we have by definition that $xR + yR + zR \subset R$. Now let $r \in R$ be arbitrary. Then

$$r = r \cdot 1 = r \cdot (x^2 + y^2 + z^2) = x \cdot (rx) + y \cdot (ry) + z \cdot (rz) \in xR + yR + zR$$

as desired.

For the third claim, we have that

$$f(c) = f(x, y, z) = xx + yy + zz = x^2 + y^2 + z^2 = 1$$

as desired. □

6.10. Prove that every (left) A-module homomorphism from A to itself is right multiplication by a, denoted by $r_a : A \to A$, for a unique $a \in A$.

6.11. Let R be a commutative ring. Show that if $T : M \to N$ is a homomorphism of R-modules and if $a \in R$, then $S : M \to N$ given by $S(m) = aT(m)$ for all $m \in M$ is also an R-module homomorphism. Deduce that $\mathrm{Hom}_R(M, N)$ has the structure of an R-module.

Proof. For all $m \in M$,

$$S(m) = aT(m) = T(am) = T(ma) = T(r_a(m)) = (T \circ r_a)(m)$$

Note that the second equality holds because T is an R-module homomorphism and the third equality holds because R is commutative (and hence the left and right R-module structures are equivalent). It follows from the above $S = T \circ r_a$. Additionally, by Problem 6.10, $r_a \in \mathrm{Hom}_R(R, R)$. It follows by Proposition 10.2 that S is an R-module homomorphism.

By a similar argument to that used in Problem 1.14, $(\mathrm{Hom}_R(M, N), +)$ is an abelian group, where addition is taken pointwise. By the above $\cdot : A \times \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, N)$ defined by $(a, T) \mapsto a \cdot T$ is closed. Additionally, if $a, b \in R$ and $S, T \in \mathrm{Hom}_R(M, N)$, we can use the fact that M, N are R-modules to confirm that

$$\begin{gathered} a(S+T)(m) = a[S(m) + T(m)] = aS(m) + aT(m) = (aS + aT)(m) \\ a(S+T) = aS + aT \end{gathered} \tag{1}$$

$$\begin{gathered} (a+b)T(m) = aT(m) + bT(m) \\ (a+b)T = aT + bT \end{gathered} \tag{2}$$

$$\begin{gathered} a(bT(m)) = (ab)T(m) \\ a(bT) = (ab)T \end{gathered} \tag{3}$$

$$\begin{gathered} 1_R T(m) = T(m) \\ 1_R T = T \end{gathered} \tag{4}$$

Therefore, $\mathrm{Hom}_R(M, N)$ is an R-module, as desired. □

6.12. Give an example of a PID A and an A-submodule M' of an A-module M such that M and $M' \oplus (M/M')$ are not isomorphic to each other (as A-modules).

Note: If A is a field, then there is an isomorphism $M \to M' \oplus (M/M')$. In class, it was shown that there is such an isomorphism if M/M' is isomorphic to A^n for some $n = 0, 1, 2, \ldots$.

Proof. Pick

$$\boxed{A = \mathbb{Z} \qquad M = \mathbb{Z}/4\mathbb{Z} \qquad M' = (2) \subset M}$$

By Section 8.2 of Dummit and Foote (2004), we know that $A = \mathbb{Z}$ is a PID. Additionally, we know from last quarter that M is an abelian group and M' is a subgroup of M. It follows by Dummit and Foote (2004, p. 339) that these are valid examples of a $\mathbb{Z}$-module and a $\mathbb{Z}$-submodule. Moreover, we know from group theory that $(\mathbb{Z}/4\mathbb{Z})/(2)$ is isomorphic (as a group [or A-module]) to $\mathbb{Z}/2\mathbb{Z}$ and, similarly, $(2) \cong \mathbb{Z}/2\mathbb{Z}$ as a group (or A-module). Therefore,

$$M \oplus (M/M') \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) = K \ncong \mathbb{Z}/4\mathbb{Z} = M$$

as desired, where K denotes the Klein 4-group. □

6.13. Let $f, g \in F[X]$ be polynomials of degrees d and e, respectively, where F is a field. Assume that $\gcd(f, g) = 1$. Prove that there is a unique pair $a, b \in F[X]$ such that

$$af + bg = 1 \qquad \deg(a) < e \qquad \deg(b) < d$$

Hint: One already knows that there exist a, b satisfying $af + bg = 1$, but the a, b satisfying this equation are far from being unique. Given a, b, first find *all* a', b' satisfying $a'f + b'g = 1$. After this, you will see that the problem is easily solved.

Note: There is also a different constructive method of finding the desired a, b that relies on determinants and resultants.

Proof. By hypothesis, there exist polynomials $a_0, b_0 \in F[X]$ such that $a_0 f + b_0 g = 1$. We can easily show that the set of all (a, b) satisfying $af + bg = 1$ is

$$\{(a_0 + gh, b_0 - fh) : h \in F[X]\}$$

In particular, for any element of this set, we have

$$(a_0 + gh)f + (b_0 - fh)g = (a_0 f + b_0 g) + (gfh - fgh) = 1 + 0 = 1$$

and for any (a, b) satisfying the equation, we have

$$\begin{aligned} (af + bg) - (a_0 f + b_0 g) &= 1 - 1 \\ (a - a_0)f + (b - b_0)g &= 0 \\ a &= a_0 + \frac{b - b_0}{f} g \end{aligned}$$

so that $a \in a_0 + (g)$, as desired.

Elaborating on the observation that any a is an element of $a_0 + (g)$: Since $F[X]/(g) \cong \{h \in F[X] : \deg(h) < e\}$ by the corollary from Lecture 3.1, there exists a unique a with $\deg(a) < e$ such that $a \mapsto a_0 + (g)$. It follows by the construction of the isomorphism that $a \in a_0 + (g)$, and hence $a + (g) = a_0 + (g)$. A similar argument holds for b. This yields the desired result. □

7 Modules Over PIDs

2/24: **7.1. Uniqueness of the rational canonical form.** Let $I_1 \subset I_2 \subset \cdots$ be a sequence of ideals in a PID R. Assume that there is some natural number N such that $I_N = R$. Thus, if $I_i = (a_i)$, we have $a_{i+1} \mid a_i$ for all i and $1 = a_N = a_{N+1} = \cdots$. Let $M_i = R/I_i$, and let $M = M_1 \oplus M_2 \oplus \cdots$. For a prime p of R and for $k \geq 0$, we see that $p^k M/p^{k+1}M$ is a module over the *field* $R/(p)$, and is therefore a vector space over $R/(p)$. Denote by $d(p,k)$ its dimension. Define $n_i(p)$ to be the greatest nonnegative integer such that $I_i \subset (p^{n_i})$ — equivalently, $n_i(p)$ is the power of p that occurs in the factorization of a_i. However, $a_i = 0$ (equivalently $I_i = 0$) is a possibility, in which case we put $n_i(p) = \infty$.

(i) Prove that the sequence $d(p,0), d(p,1), \ldots$ determines the sequence $n_1(p), n_2(p), \ldots$.

Proof. We begin with some preliminary results.

We first exhibit an alternate form for M. For all $i \geq N$, we have that $1 = a_i$ and hence

$$M_i = R/I_i = R/(a_i) = R/(1) = R/R \cong 0$$

It follows if we let $\alpha = N - 1$ that

$$M = M_1 \oplus M_2 \oplus \cdots \cong M_1 \oplus \cdots \oplus M_\alpha = R/(a_1) \oplus \cdots \oplus R/(a_\alpha)$$

Since R is a PID (hence a UFD) and $a_1 \in R$, we know that a_1 has a unique factorization

$$a_1 = u p_1^{e_{1,1}} \cdots p_n^{e_{1,n}}$$

It follows by the Chinese Remainder Theorem (CRT) that

$$R/(a_1) \cong R/(p_1^{e_{1,1}}) \oplus \cdots \oplus R/(p_n^{e_{1,n}})$$

Additionally, since $a_\alpha \mid a_{\alpha-1} \mid \cdots \mid a_1$, we know that the unique factorization of *every* a_i will be expressed in terms of the same primes and lesser or equal (and possibly zero) exponents. Essentially, if $i < j$, then

$$a_i = u' p_1^{e_{i,1}} \cdots p_n^{e_{i,n}} \qquad\qquad a_j = u'' p_1^{e_{j,1}} \cdots p_n^{e_{j,n}}$$

where $e_{i,\ell} \geq e_{j,\ell}$ $(\ell = 1, \ldots, n)$. Thus, by combining the last several results, we have that

$$M \cong R/(a_1) \oplus \cdots \oplus R/(a_\alpha) \cong \left(\bigoplus_{\ell=1}^{n} R/(p_\ell^{e_{1,\ell}}) \right) \oplus \cdots \oplus \left(\bigoplus_{\ell=1}^{n} R/(p_\ell^{e_{\alpha,\ell}}) \right)$$

This will be useful later.

Next, we investigate some properties of the individual quotient modules. Let $j \in \{1, \ldots, n\}$ be arbitrary. Consider the ideal $pR/(p_j^{e_{i,j}})$, first where $p = p_j$. In this case, we have that

$$p_j R/(p_j^{e_{i,j}}) \cong R/(p_j^{\max\{0, e_{i,j}-1\}})$$

Now consider the case where $p \neq p_j$. In this case, we can show that

$$pR/(p_j^{e_{i,j}}) \cong R/(p_j^{e_{i,j}})$$

Both of these results will be useful later.

We now begin the proof in earnest.

Let p be an arbitrary prime of R. We divide into two cases ($p \in \{p_1, \ldots, p_n\}$ and $p \notin \{p_1, \ldots, p_n\}$). First, suppose that $p \in \{p_1, \ldots, p_n\}$. For the sake of simplicity, let $p = p_j$. To begin, rewrite the CRT expansion of $R/(a_i)$ to

$$R/(a_i) \cong \bigoplus_{\ell=1}^{n} R/(p_\ell^{e_{i,\ell}}) \cong \underbrace{\left(\bigoplus_{\substack{\ell=1 \\ \ell \neq j}}^{n} R/(p_\ell^{e_{i,\ell}}) \right)}_{N_{i,j}} \oplus R/(p_j^{e_{i,j}}) = N_{i,j} \oplus R/(p_j^{e_{i,j}})$$

for each $i \in \{1, \ldots, \alpha\}$. Thus, we have that

$$M \cong R/(a_1) \oplus \cdots \oplus R/(a_\alpha) \cong [N_{1,j} \oplus R/(p_j^{e_{1,j}})] \oplus \cdots \oplus [N_{\alpha,j} \oplus R/(p_j^{e_{\alpha,j}})]$$

Let $\beta_j = \max\{i \in \{1, \ldots, \alpha\} : e_{i,j} > 0\}$. Then combining several previous results, we have that

$$p^k M \cong [N_{1,j} \oplus R/(p_j^{\max\{0, e_{1,j}-k\}})] \oplus \cdots \oplus [N_{\beta_j,j} \oplus R/(p_j^{\max\{0, e_{\beta_j,j}-k\}})] \oplus N_{\beta_j+1,j} \oplus \cdots \oplus N_{\alpha,j}$$

and similarly for $k+1$. Note that each $N_{i,j}$ is unchanged under left multiplication by p^k because all of its component $R/(p_\ell^{e_{i,\ell}})$'s are unchanged under left multiplication by the coprime element p_j, as discussed above. It follows that

$$p^k M/p^{k+1} M \cong (R/(p_j^{\max\{0, e_{1,j}-k\}}))/(R/(p_j^{\max\{0, e_{1,j}-k-1\}})) \\ \oplus \cdots \oplus (R/(p_j^{\max\{0, e_{\beta_j,j}-k\}}))/(R/(p_j^{\max\{0, e_{\beta_j,j}-k-1\}}))$$

since quotients of identical submodules in a direct sum are equal to zero, and these can be isomorphismed out of the quotient direct sum. Additionally, we have that

$$(R/(p_j^{\max\{0, e_{i,j}-k\}}))/(R/(p_j^{\max\{0, e_{i,j}-k-1\}})) \cong R/(p_j)$$

for $k < e_{i,j}$ and

$$(R/(p_j^{\max\{0, e_{i,j}-k\}}))/(R/(p^{\max\{0, e_{i,j}-k-1\}})) \cong (R/R)/(R/R) \cong 0/0 \cong 0$$

for $k \geq e_{i,j}$ $(i = 1, \ldots, \beta_j)$.

We are now prepared to count dimensions in $p^k M/p^{k+1} M$, i.e., to describe the desired relationship between the d's and n_i's. By the above and the assumption that $e_{i,j} \geq 1$, $p^0 M/p^{0+1} M$ is a β_j-dimensional vector space over the field $R/(p)$. As we increase k, eventually k will equal $e_{\beta_j,j}$. At this point, we will have $d(p, k-1) > d(p, k)$. In particular, suppose $d(p, k) = d(p, k-1) - \gamma$. Then $e_{\beta_j,j} = \cdots = e_{\beta_j-\gamma+1,j}$ and $n_{\beta_j}(p) = \cdots = n_{\beta_j-\gamma+1}(p) = e_{\beta_j,j} = k$. Continuing on, eventually we will get to $k = e_{\beta_j-\gamma,j}$. The change in the dimension d here will reveal the values of $n_{\beta_j-\gamma}(p)$ and possibly some $n_{\beta_j-\gamma-1}(p), n_{\beta_j-\gamma-2}(p), \ldots$. Once we are past $e_{1,j}$, we could raise k infinitely high and still not alter the identity of the vector space any more (specifically as pertains to $i \in \{\beta_j + 1, \ldots, \alpha\}$). Thus, we relate $n_i(p)$ and $d(p, k)$ by stating that

$$\boxed{n_i(p) = \min\{k : d(p, k) < i\}}$$

Note that for $i \in \{\beta_j + 1, \ldots, \alpha\}$, this definition has an interpretation that may still make some sense. If $i > \beta_j$, then $\{k : d(p, k) < i\} = \emptyset$ since $d(p, k) \geq 0$ for all k by definition. In particular, since it would be incorrect to say that such an empty set has minimum equal to any integer, we may as well adopt the convention that $\min \emptyset$ is greater than all of the integers, i.e., $\min \emptyset = \infty$.

Now suppose that $p \notin \{p_1, \ldots, p_n\}$, then we have by the above that

$$pM = \left(\bigoplus_{j=1}^{n} pR/(p_j^{e_{1,j}}) \right) \oplus \cdots \oplus \left(\bigoplus_{j=1}^{n} pR/(p_j^{e_{\alpha,j}}) \right) \cong \left(\bigoplus_{j=1}^{n} R/(p_j^{e_{1,j}}) \right) \oplus \cdots \oplus \left(\bigoplus_{j=1}^{n} R/(p_j^{e_{\alpha,j}}) \right)$$

It follows inductively that

$$p^k M \cong \left(\bigoplus_{j=1}^{n} R/(p_j^{e_{1,j}})\right) \oplus \cdots \oplus \left(\bigoplus_{j=1}^{n} R/(p_j^{e_{\alpha,j}})\right)$$
$$p^{k+1} M \cong \left(\bigoplus_{j=1}^{n} R/(p_j^{e_{1,j}})\right) \oplus \cdots \oplus \left(\bigoplus_{j=1}^{n} R/(p_j^{e_{\alpha,j}})\right)$$

Thus, since $p^k M = p^{k+1} M$, we have that $p^k M / p^{k+1} M = 0$ for all $k \in \mathbb{Z}_{\geq 0}$. Therefore, $d(p,k) = 0$ for all $k \in \mathbb{Z}_{\geq 0}$ and thus, consistent with the above (under the convention $\beta_j = 0$), we may take $n_i(p) = \infty$ $(i = 1, \ldots, \alpha)$. □

(ii) Deduce that if $M \cong N$ where $N = N_1 \oplus N_2 \oplus \cdots$ and $N_i = R/J_i$ for an increasing sequence of ideals $J_1 \subset J_2 \subset \cdots$, then $I_n = J_n$ for all $n \in \mathbb{N}$.

Proof. Since R is a PID, each $J_i = (b_i)$ for some $b_i \in R$. Moreover, the increasing sequence condition implies the divisibility condition $b_2 \mid b_1$, $b_3 \mid b_2$, etc. Since

$$N = R/(b_1) \oplus R/(b_2) \oplus \cdots$$

this divisibility condition implies that b_1 annihilates each $R/(b_i)$ and, hence, N itself. Moreover, any factor of b_1 would miss some part of $R/(b_1)$, so b_1 is minimal. Thus, $\mathrm{Ann}(N) = (b_1)$. We can show in an analogous manner using the analogous conditions on M that $\mathrm{Ann}(M) = (a_1)$. But since $M \cong N$, we have that

$$(b_1) = \mathrm{Ann}(N) = \mathrm{Ann}(M) = (a_1)$$
$$b_1 = a_1$$

In particular, this proves that $I_1 = J_1$. More importantly, however, it pairs with the divisibility condition to demonstrate that the prime factorization of each b_i is a product of the same n primes $p_1, \ldots, p_n$. These primes in the factorizations will be raised to certain powers that are bounded by $e_{1,1}, \ldots, e_{1,n}$, respectively.

We can determine the exact values of the primes' exponents via comparison of the sequences $d(p_j, 0), d(p_j, 1), \ldots$ from part (i) in both M and N. In particular, since $M \cong N$, $p_j^k N / p_j^{k+1} N$ will follow the same dimension sequence $d(p_j, 0), d(p_j, 1), \ldots$ as that generated by $p_j^k M / p_j^{k+1} M$. Note that this observation justifies using a notation for the sequence that does not distinguish between N and M. To conclude, we can apply part (i) to learn that the sequences $d(p_j, 0), d(p_j, 1), \ldots$ as applied to N generate the exponents $e_{1,1}, \ldots, e_{\alpha,n}$. In particular, these exponents that match the corresponding ones in M. □

7.2. Let K be the fraction field of the PID R. We regard K as an R-module and regard $R \subset K$ as an R-submodule.

(i) Show that K/R is a torsion R-module.

Proof. To prove that K/R is a torsion R-module, it will suffice to show that for all $m + R \in K/R$, there exists a nonzero $a \in R$ such that $a(m + R) = 0 + R$. Let $m + R \in K/R$ be arbitrary. Pick any $a \in R$. Then since $am \in Rm \subset R = 0 + R$, $a(m + R) = am + R = 0 + R$, as desired. □

(ii) We have shown that every torsion R-module is the direct sum of its p-primary components. The p-primary component of K/R is S/R, where S is an R-submodule of K. Do you recognize S? *Hint*: You encountered it in fourth week.

Proof. Let $p \in R$ be a prime. By definition, the p-primary component S/R of the R-module K/R is the set of all $a/b + R \in K/R$ such that $p^k(a/b + R) = 0 + R$ for some $k \in \mathbb{Z}_{\geq 0}$. The last expression in the previous sentence is equivalent to $p^k a/b \in R$. But this will be true iff

$b \mid p^k$, i.e., if $b = p^\ell$ for some nonnegative integer $\ell \leq k$. Thus, S/R is equivalently the set of all $a/p^\ell + R \in K/R$ for $\ell \in \mathbb{Z}_{\geq 0}$. Evidently, this is the image of R_p under the canonical surjection, so

$$\boxed{S = R_p}$$

□

7.3. Given subrings A, B of a ring C, it is not true that $A + B$ is a subring in general. But here is an example where it is indeed a subring: Let $C = F(X)$ where F is a field, let $A = F[X]$, let $a \in F$, and let B be the image of the unique ring homomorphism $\phi : F[T] \to F(X)$ such that $\phi(c) = c$ for all $c \in F$ and $\phi(T) = (X - a)^{-1}$. Prove that...

(i) $A \cap B = F$;

Proof. We proceed via a bidirectional inclusion proof.

Suppose first that $c \in F$. Then $c \in F[X] = A$ by definition. Additionally, since $c \in F[T]$ by definition and $\phi(c) = c$ by the definition of ϕ, we have that $c \in \text{im}(\phi) = B$. Therefore, since $c \in A$ and $c \in B$, $c \in A \cap B$, as desired.

Now suppose that $c \in A \cap B$. Since $c \in A$, we know that c is a polynomial in X with coefficients in F. Additionally, by the universal property of the polynomial ring, we know that $\phi = \text{ev}_{(X-a)^{-1}}$. Consequently, $B = \text{im}(\phi) = F[(X - a)^{-1}]$. It follows that if c is the image of any nonconstant polynomial in $F[T]$, a has a nontrivial denominator. But this would contradict our earlier statement that $c \in F[X]$. Thus, c must be the image of some constant. In particular, it follows by the definition of ϕ that $c \in F$, as desired. □

(ii) $A + B$ equals the subring S of the previous problem, where $R = F[X]$ and $p = (X - a)$.

Proof. Analogy to previous: $C = K$ and $A = R$. So $S = R_p = F[X]_{(X-a)}$.
$F[X] + F[(X - a)^{-1}] = F[X]_{(X-a)}$. Invoke the Euclidean algorithm on elements in the right set. Divide by $(X - a)^n$.

The subring S of the previous problem, rephrased in terms of this problem, is

$$S = R_p = F[X]_{(X-a)}$$

Thus, to prove that $A + B = S$, it will suffice to show that $F[X] + F[(X - a)^{-1}] = F[X]_{(X-a)}$. We proceed once again via a bidirectional inclusion proof.

Suppose first that $p/(X - a)^n \in F[X]_{(X-a)}$, where $n \in \mathbb{N}$. By the Euclidean algorithm for monic polynomials, we know that

$$p(X) = q(X) \cdot (X - a)^n + r(X)$$
$$\frac{p(X)}{(X - a)^n} = q(X) + \frac{r(X)}{(X - a)^n}$$

for some $q, r \in F[X]$ with $\deg(r) < n$. From here, we cam resolve $r(X)/(X - a)^n$ into a polynomial in $(X - a)^{-1}$ using the method of partial fractions. Therefore, as the sum of a term in $F[X]$ and a term in $F[(X - a)^{-1}]$, $p/(X - a)^n \in F[X] + F[(X - a)^{-1}]$, as desired.

Now suppose that $p + q \in F[X] + F[(X - a)^{-1}]$. Add all terms together with least common denominator $(X - a)^n$, where n is the degree of $f \in F[T]$ whose image under ϕ is q. This yields a rational function equal to $p + q$ in $F[X]_{(X-a)}$, as desired. □

7.4. Let R be a commutative ring. The **derivative** (of $f = a_0 + a_1X + \cdots + a_nX^n \in R[X]$), denoted by f', is defined by $f'(X) = a_1 + 2a_2X + \cdots + na_nX^{n-1}$. Assume that R is a subring of a commutative ring A. Let M be an A-module. An ***R*-derivation** (of A with values in M) is a function $D : A \to M$ that satisfies...

(1) $D(a + b) = D(a) + D(b)$ for all $a, b \in A$;

(2) $D(ab) = aD(b) + bD(a)$ for all $a, b \in A$;

(3) $D(c) = 0$ for all $c \in R$.

Prove that $D(f) = f'$ is an R-derivation D of $R[X]$ with values in $R[X]$ that satisfies $D(X) = 1$.

Proof. To prove that D is an R-derivation, it will suffice to check Properties 1-3.

Property 1: Let $a, b \in R[X]$ be arbitrary. Suppose $a = a_0 + \cdots + a_n X^n$ and $b = b_0 + \cdots + b_m X^m$. WLOG let $n \leq m$. Then

$$\begin{aligned} D(a+b) &= (a+b)' \\ &= [(a_0 + b_0) + \cdots + (a_n + b_n)X^n + b_{n+1}X^{n+1} + \cdots + b_m X^m]' \\ &= (a_1 + b_1) + \cdots + n(a_n + b_n)X^{n-1} + (n+1)b_{n+1}X^n + \cdots + mb_m X^{m-1} \\ &= (a_1 + \cdots + na_n X^{n-1}) + (b_1 + \cdots + mb_m X^{m-1}) \\ &= a' + b' \\ &= D(a) + D(b) \end{aligned}$$

as desired.

Property 2: Let $a, b \in R[X]$ be arbitrary. Suppose $a = a_0 + \cdots + a_n X^n$ and $b = b_0 + \cdots + b_m X^m$.

WLOG let $n \leq m$. Then

$$\begin{aligned}
aD(b) + bD(a) &= aD(b) + D(a)b \\
&= [a_0 + \cdots + a_n X^n] \cdot [b_0 + \cdots + b_m X^m]' \\
&\quad + [a_0 + \cdots + a_n X^n]' \cdot [b_0 + \cdots + b_m X^m] \\
&= [a_0 + \cdots + a_n X^n] \cdot [b_1 + \cdots + m b_m X^{m-1}] \\
&\quad + [a_1 + \cdots + n a_n X^{n-1}] \cdot [b_0 + \cdots + b_m X^m] \\
&= \sum_{r=0}^{m+n-1} \left(\sum_{p=0}^{r} a_p (r-p+1) b_{r-p+1} \right) X^r + \sum_{r=0}^{m+n-1} \left(\sum_{p=0}^{r} (p+1) a_{p+1} b_{r-p} \right) X^r \\
&= \sum_{r=0}^{m+n-1} \left(\sum_{p=0}^{r} a_p (r-p+1) b_{r-p+1} + \sum_{p=0}^{r} (p+1) a_{p+1} b_{r-p} \right) X^r \\
&= \sum_{r=1}^{m+n} \left(\sum_{p=0}^{r-1} a_p (r-p) b_{r-p} + \sum_{p=0}^{r-1} (p+1) a_{p+1} b_{r-p-1} \right) X^{r-1} \\
&= \sum_{r=1}^{m+n} \left(\sum_{p=0}^{r-1} (r-p) a_p b_{r-p} + \sum_{p=1}^{r} p a_p b_{r-p} \right) X^{r-1} \\
&= \sum_{r=1}^{m+n} \left(r a_0 b_r + \sum_{p=1}^{r-1} (r-p) a_p b_{r-p} + \sum_{p=1}^{r-1} p a_p b_{r-p} + r a_r b_0 \right) X^{r-1} \\
&= \sum_{r=1}^{m+n} \left(r a_0 b_r + \sum_{p=1}^{r-1} r a_p b_{r-p} + r a_r b_0 \right) X^{r-1} \\
&= \sum_{r=1}^{m+n} r \left(a_0 b_r + \sum_{p=1}^{r-1} a_p b_{r-p} + a_r b_0 \right) X^{r-1} \\
&= \sum_{r=1}^{m+n} r \left(\sum_{p=0}^{r} a_p b_{r-p} \right) X^{r-1} \\
&= \left[\sum_{r=0}^{m+n} \left(\sum_{p=0}^{r} a_p b_{r-p} \right) X^r \right]' \\
&= (ab)' \\
&= D(ab)
\end{aligned}$$

as desired.

Property 3: Let $c \in R$ be arbitrary. Then

$$D(c) = c' = 0$$

as desired.

Lastly, we have by that

$$D(X) = X' = 1$$

as desired. □

7.5. (i) Let $a \in R$ and let $f \in R[X]$, where R is a commutative ring. a is said to be a **root** (resp. **repeated root**) of f if f is a multiple of $(X-a)$ (resp. $(X-a)^2$). Prove that $f(a) = f'(a) = 0$ iff f is a multiple of $(X-a)^2$.

Proof. Suppose first that f is a multiple of $(X-a)^2$. Then $f(X) = q(X)\cdot(X-a)^2$ for some $q \in R[X]$. It follows that

$$f(a) = q(a)\cdot(a-a)^2 = q(a)\cdot 0 = 0$$

Additionally, Problem 7.4 tells us that the normal product rule of differentiation applies even when the R in $R[X]$ is an arbitrary commutative ring, not just when $R = \mathbb{R}$. Thus,

$$f'(X) = q'(X)\cdot(X-a)^2 + q(a)\cdot(X^2 - 2aX + a^2)' = q'(X)\cdot(X-a)^2 + q(a)\cdot(2X-2a)$$

It follows that

$$f'(a) = q'(a)\cdot(a-a)^2 + q(a)\cdot(2a-2a) = q'(a)\cdot 0 + q(a)\cdot 0 = 0+0 = 0$$

as desired.

Now suppose that $f(a) = f'(a) = 0$. Since $f(a) = 0$, we have by the application of the Euclidean algorithm in Lecture 3.1 that

$$f(X) = q(X)\cdot(X-a)$$

for some $q \in R[X]$. Similarly, $f'(a) = 0$ implies that

$$f'(X) = \tilde{q}(X)\cdot(X-a)$$

for some $\tilde{q} \in R[X]$. To relate these two equations, we'll differentiate the first one. This yields

$$f'(X) = q(X)\cdot(X-a)' + q'(X)\cdot(X-a) = q(X)\cdot 1 + q'(X)\cdot(X-a) = q(X) + q'(X)\cdot(X-a)$$

This implies that

$$\begin{aligned} q(X) + q'(X)\cdot(X-a) &= \tilde{q}(X)\cdot(X-a) \\ q(X) &= [\tilde{q}(X) - q'(X)]\cdot(X-a) \end{aligned}$$

i.e., that $q(X)$ is a multiple of $X-a$, itself. Define $r(X) = \tilde{q}(X) - q'(X)$. Then

$$f(X) = q(X)\cdot(X-a) = r(X)\cdot(X-a)\cdot(X-a) = r(X)\cdot(X-a)^2$$

Therefore, f is a multiple of $(X-a)^2$, as desired. □

(ii) Let F be a subfield of a field E. Let $a \in E$ and let $f \in F[X]$. Show that if a is a repeated root of f, then there is some $g \in F[X]$ such that...

(1) $\deg(g) > 0$;
(2) Both f and f' are multiples of g in $F[X]$.

Proof. Consider the ring homomorphism $\mathrm{ev}_a : F[X] \to E$. More specifically, consider $\ker(\mathrm{ev}_a)$. Since $F[X]$ is a PID and kernels are ideals, we know that $\ker(\mathrm{ev}_a) = (g)$ for some $g \in F[X]$. Since a is a repeated root of f, part (i) implies that $f(a) = f'(a) = 0$. Thus, $f, f' \in \ker(\mathrm{ev}_a) = (g)$, so both f and f' are multiples of g. Additionally, we know that $\deg(g) > 0$ since the only constant polynomial that "maps" a to 0 is the zero polynomial, and f nonzero an element of (g) implies that 0 is not the generator of the kernel. □

7.6. This is essentially a repetition of the last problem from HW6 but by a slightly different method.

Let $F[X]_{<m}$ be the collection of $a \in F[X]$ such that $\deg(a) < m$. Let $f, g \in F[X]$ be polynomials of degrees d and e, respectively. Define $T : F[X]_{<e} \oplus F[X]_{<d} \to F[X]_{<d+e}$ by $T(a,b) = af + bg$. Note that T is a linear transformation of F-vector spaces, with domain and target of the same dimension.

(i) Deduce that $\gcd(f,g) = 1$ iff every $h \in F[X]$ with $\deg(h) < d+e$ can be expressed as $af + bg$ for some $a, b \in F[X]$ satisfying $\deg(a) < e$ and $\deg(b) < d$.

Proof. Suppose first that $\gcd(f,g)=1$. Then there exist $\tilde{a},\tilde{b}\in F[X]$ such that $\tilde{a}f+\tilde{b}g=1$. Proving the desired claim is equivalent to proving that T is surjective. Since T maps like-dimensional vector spaces, it will suffice to show that T is injective. Suppose $T(a,b)=T(a',b')$. Then $af+bg=a'f+b'g$. Equivalently,

$$\begin{aligned}(a-a')f+(b-b')g&=0\\ a&=a'-\frac{b-b'}{f}g\\ a&\in a'+(g)\end{aligned}$$

Since g has degree e and $F[X]/(g)\cong\{h\in F[X]:\deg(h)<e\}$ by Lecture 3.1, there is a unique $\tilde{a}\in F[X]_{<e}$ such that $\tilde{a}+(g)=a+(g)=a'+(g)$. It follows that we must have $a=\tilde{a}$ and $a'=\tilde{a}$, thereby proving that $a=a'$ by transitivity. An analogous argument can show that $b=b'$. Thus $(a,b)=(a',b')$ as desired.

Now suppose that every $h\in F[X]$ with $\deg(h)<d+e$ can be expressed as $af+bg$ for some $a,b\in F[X]$ satisfying $\deg(a)<e$ and $\deg(b)<d$. Let $h=1$. Clearly $\deg(h)=0<d+e$ in this case. It follows by the supposition that $h=af+bg$ for some $a,b\in F[X]$ satisfying $\deg(a)<e$ and $\deg(b)<d$. Thus, $1=h=af+bg\in(f,g)$, so we must have $\gcd(f,g)=1$, as desired. □

(ii) The **resultant** (of f,g), denoted by $\mathrm{Res}(f,g)$, is the determinant of T. To define the latter, one requires a basis for the source and target. In particular,

$$(1,0),(X,0),\ldots,(X^{e-1},0),(0,1),(0,X),\ldots,(0,X^{d-1})$$

is the basis for $F[X]_{<e}\oplus F[X]_{<d}$ and

$$1,X,\ldots,X^{d+e-1}$$

is the basis for $F[X]_{<d+e}$.
Deduce that $\gcd(f,g)=1$ iff $\mathrm{Res}(f,g)\neq 0$.

Proof. Suppose first that $\gcd(f,g)=1$. Then by part (i), every $h\in F[X]$ with $\deg(h)<d+e$ can be expressed as $af+bg$ for some $a,b\in F[X]$ satisfying $\deg(a)<e$ and $\deg(b)<d$. It follows that T is surjective. Thus, since its domain and range have the same dimension, it is invertible as well. Therefore, it is nonsingular and hence $\mathrm{Res}(f,g)\neq 0$.

Now suppose that $\mathrm{Res}(f,g)\neq 0$. Then T is nonsingular and hence it is invertible. Thus, for the same reason as above, T is surjective. In particular, 1 is in the range of T, so there must exist $a,b\in F[X]$ such that $af+bg=T(a,b)=1$. It follows that $1=af+bg\in(f,g)$. Therefore, $\gcd(f,g)=1$. □

7.7. Given an R-module M and $a\in R$, denote by $a_M:M\to M$ the function $a_M(m)=am$ for all $m\in M$. Now consider $M=R/(p^2)\oplus R/(p)$ where R is a PID and $p\in R$ is a prime. Let N be a submodule of M which has the property that $T(N)\subset N$ for every R-module self-isomorphism $T:M\to M$. Prove that N is one of the following four submodules: $0,M,pM,\ker(p_M)$. *Note*: The above problem is also valid for $(R/(p^2))^m\oplus(R/(p))^n$.

Proof. If $N=0,M$, then the statement obviously holds. Thus, we concern ourselves with the case where $N\notin\{0,M\}$. In this case, we want to show that $N=pM$ or $N=\ker(p_M)$. We know that

$$pM=pR/(p^2)\oplus 0 \qquad\qquad \ker(p_M)=pR/(p^2)\oplus R/(p)$$

$\ker(p_M)$ is a 2D vector space over $R/(p)$. We want to show that $N\cap\ker(p_M)\neq 0$ iff $N\neq 0$. We know that $pN\subset N$ by the definition of N as a submodule. Let $n\in N$ be nonzero. Suppose $n\notin\ker(p_M)$. Then $pn\in\ker(p_M)$. We know that $pn\in N$ as well. Thus, $pn\in N\cap\ker(p_M)$.

$N\cap\ker(p_M)\subset\ker(p_M)$. Thus, $N\cap\ker(p_M)$ is either a 1D or a 2D vector space over $R/(p)$. We want to show that if it's 2D, then it equals $\ker(p_M)$, and if it's 1D, then it equals pM. 2D case: We know that

$N \cap \ker(p_M) \subset \ker(p_M)$. 2D implies that $N \not\subseteq \ker(p_M)$. Thus, either $N = \ker(p_M)$ or $N \supsetneq \ker(p_M)$. In the first case, we are done. In the second case, we can show that this implies that $N = M$. 1D case: We know that $pM \cap \ker(p_M) = p_M$. Assume $N \neq pM$. Then $N \cap \ker(p_M) = \langle (pa, 1) \rangle$. But T exists, where $T : M \to M$ sends $T(1,0) = (1,0)$ and $T(0,1) = (p,1)$. Therefore we must have $N \cap \ker(p_M) = pM$.

Suppose that $N \supsetneq pM$. $N/pM \subset M/pM$. Then use $T(1,0) = (1,1)$ and $T(0,1) = (0,1)$. □

References

Dummit, D. S., & Foote, R. M. (2004). *Abstract algebra* (third). John Wiley and Sons.