MATH 25800 (Honors Basic Algebra II) Problem Sets

Steven Labalme

February 5, 2023

Contents

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. $\square$

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. $\square$

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]

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

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.

[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 $\mathbb{R}^2$.

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.

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.

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

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) $\Rightarrow$ (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.

<u>(ii) ⇒ (iii)</u>: 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.

<u>(iii) ⇒ (i)</u>: 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[4]. ☐

(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[5]. ☐

[4]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.

[5]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

$$\begin{aligned} ra + sa &= ar + as \\ (r+s)a &= a(r+s) \end{aligned}$$

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

$$a = 1_R a = a 1_R$$

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 $b_0, b_1, \dots$ 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 $b_0, \dots, b_{n-1}$. 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[6] 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[7] 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

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

[6] From Honors Calculus IBL.
[7] 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. $\square$

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

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

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. $\square$

(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. $\square$

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

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

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.

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

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 linear transformation satisfying $T^{-1} \circ T = \text{id}$). 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 $v \in V$. □

References

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