MATH 25800 (Honors Basic Algebra II) Problem Sets

Steven Labalme

January 11, 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. ☐

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]

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

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.

(ii) $\Rightarrow$ (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) $\Rightarrow$ (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. $\square$

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. $\square$

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. $\square$

(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. $\square$

(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. $\square$

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. $\square$

(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]. □

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 $a \in R$.

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 $1 + x + x^2 + \cdots$.

(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.

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.

[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.

(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.

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 $b \in R$.

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 $M = M_c$.

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

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

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

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. 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.

(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).

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.

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

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

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

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

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

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

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

References

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