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. ☐

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]. □

[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.