MATH 417, HOMEWORK 13

CHARLES ANCEL

The first few exercises use the following construction: Given R a commutative ring with identity, and an element $u \in R$, let $S := R[\gamma]$ be the set of "formal expressions" $a + b\gamma$ where $a, b \in R$, and γ is a new symbol. (This is just a way of writing ordered pairs (a, b).) We define addition and multiplication operations on S in the "obvious" way, together with the identity $\gamma^2 = u$. Explicitly:

$$(a + b\gamma) + (a' + b'\gamma) := (a + a') + (b + b')\gamma, \qquad (a + b\gamma)(a' + b'\gamma) := (aa' + ubb')(ab' + ba')\gamma$$

Exercise 1. Show that $(S, +, \cdot)$ as defined above is a commutative ring with identity.

Introduction

In this exercise, we will prove that the set $S := R[\gamma]$ with the given operations forms a commutative ring with identity. We will check the ring axioms, which include closure, associativity, distributivity, commutativity, and the presence of identity elements.

Solution

Definition of Addition and Multiplication: For elements $a + b\gamma, a' + b'\gamma \in S$, the operations are defined as:

$$(a + b\gamma) + (a' + b'\gamma) := (a + a') + (b + b')\gamma,$$
$$(a + b\gamma)(a' + b'\gamma) := (aa' + ubb') + (ab' + ba')\gamma,$$

where $\gamma^2 = u$.

Step 1: Closure under Addition and Multiplication.

If $a, b, a', b' \in R,$ then $(a + a') + (b + b')\gamma$ and $(aa' + ubb') + (ab' + ba')\gamma$ are in S.

Step 2: Associativity of Addition and Multiplication.

$$((a + b\gamma) + (a' + b'\gamma)) + (a'' + b''\gamma) = (a + a' + a'') + (b + b' + b'')\gamma,$$
$$((a + b\gamma)(a' + b'\gamma))(a'' + b''\gamma) = (aa' + ubb' + (ab' + ba')\gamma)(a'' + b''\gamma).$$

Expanding the right-hand side and using $\gamma^2 = u$, we get:

$$(aa' + ubb' + (ab' + ba')\gamma)(a'' + b''\gamma) = (aa'a'' + a'ubb' + ab''ab' + ba'b'') + (ab'a'' + ba''ab'')\gamma.$$

This shows that the operation is associative because both sides reduce to the same expression after using $\gamma^2 = u$.

Step 3: Commutativity of Addition and Multiplication.

$$(a + b\gamma) + (a' + b'\gamma) = (a' + b'\gamma) + (a + b\gamma),$$

$$(a + b\gamma)(a' + b'\gamma) = (a' + b'\gamma)(a + b\gamma).$$

Step 4: Existence of Additive Identity. The additive identity is $0 + 0\gamma$, satisfying:

$$(a + b\gamma) + (0 + 0\gamma) = (a + 0) + (b + 0)\gamma = a + b\gamma.$$

Step 5: Existence of Multiplicative Identity. The multiplicative identity is $1 + 0\gamma$, satisfying:

$$(a + b\gamma)(1 + 0\gamma) = a + b\gamma.$$

Therefore, $1 + 0\gamma$ acts as the multiplicative identity for all elements in S.

Conclusion

We have shown that $(S, +, \cdot)$ satisfies all the properties of a commutative ring with identity. Therefore, S is a commutative ring with identity.

Exercise 2. Now suppose $R = \mathbb{Z}_5$ and $u = 2 \in \mathbb{Z}_5$. Show that in this case $S = \mathbb{Z}_5[\gamma]$ is a field.

Introduction

In this exercise, we will demonstrate that $S = \mathbb{Z}_5[\gamma]$ with $\gamma^2 = 2$ forms a field. We will show that every non-zero element in S has a multiplicative inverse, thereby proving that S is a field.

Solution

Step 1: Verify S is a Ring. From Exercise 1, $S = \mathbb{Z}_5[\gamma]$ is a commutative ring with identity.

Step 2: Check Inverses for Non-zero Elements. Let $a + b\gamma \in S$ be a non-zero element. We need to find $c + d\gamma \in S$ such that:

$$(a + b\gamma)(c + d\gamma) = 1.$$

Expanding and equating to 1, we get:

$$ac + 2bd = 1 \quad \text{and} \quad ad + bc = 0.$$

Step 3: Solve the System of Equations. Solving for c and d:

$$c = \frac{a}{a^2 - 2b^2} \quad \text{and} \quad d = \frac{-b}{a^2 - 2b^2}.$$

Since $\mathbb{Z}_5$ is a field, $a^2 - 2b^2 \neq 0$ ensures the denominators are non-zero, and multiplicative inverses exist for all non-zero elements.

Conclusion

We have shown that every non-zero element in $S = \mathbb{Z}_5[\gamma]$ has a multiplicative inverse. Therefore, S is a field.

In the following exercises I'll suppose $u = -1 \in R$, so that it makes sense to write i for $\gamma \in S$. **Exercise 3.** Now suppose $R = \mathbb{Z}_p$ for some prime p, and $u = -1 \in \mathbb{Z}_p$. Show that if there exists $c \in \mathbb{Z}_p$, such that $c^2 = -1$, then $c + i$ is not a unit in $S = \mathbb{Z}_p[i]$, and so $S = \mathbb{Z}_p[i]$ is not a field.

Introduction

We need to show that if $c \in \mathbb{Z}_p$ satisfies $c^2 = -1$, then $c+i$ does not have a multiplicative inverse in $S = \mathbb{Z}_p[i]$. Consequently, S is not a field.

Solution

Let $c \in \mathbb{Z}_p$ be such that $c^2 = -1$. Consider the element $c + i \in S$. Suppose for contradiction that $c + i$ is a unit in S. Then there exists some $a + bi \in S$ such that:

$$(c + i)(a + bi) = 1.$$

Expanding and using $i^2 = -1$, we get:

$$(c + i)(a + bi) = ca + cbi + ai + bi^2 = ca + cbi + ai - b.$$

Equating the real and imaginary parts to 1 and 0, respectively, we obtain:

$$ca - b = 1 \quad \text{and} \quad cb + a = 0.$$

Solving the second equation for a, we get $a = -cb$. Substituting into the first equation:

$$c(-cb) - b = 1 \implies -c^2b - b = 1 \implies -(-1)b - b = 1 \implies b + b = 1 \implies 2b = 1.$$

In $\mathbb{Z}_p$, since p is an odd prime, 2 is invertible. Therefore, $b = \frac{1}{2}$ in $\mathbb{Z}_p$.

Substituting b back into $a = -cb$:

$$a = -c \cdot \frac{1}{2} = -\frac{c}{2}.$$

Thus,

$$a + bi = -\frac{c}{2} + \frac{1}{2}i.$$

Checking the product:

$$(c + i)\left(-\frac{c}{2} + \frac{1}{2}i\right) = -\frac{c^2}{2} + \frac{c}{2}i - \frac{c}{2}i - \frac{1}{2}i^2 = -\frac{-1}{2} - \frac{1}{2} = 1,$$

which contradicts our assumption that $c + i$ is a unit. Thus, $c + i$ is not a unit, and S is not a field.

Conclusion

If there exists $c \in \mathbb{Z}_p$ such that $c^2 = -1$, then $c + i$ is not a unit in $S = \mathbb{Z}_p[i]$. Therefore, $S = \mathbb{Z}_p[i]$ is not a field in this case.

Exercise 4. As in the previous exercise, suppose $R = \mathbb{Z}_p$ for some prime p and $u = -1 \in \mathbb{Z}_p$. Show that if there is no $c \in \mathbb{Z}_p$ such that $c^2 = -1$, then the only solution to the equation $a^2 + b^2 = 0$ with $a, b \in \mathbb{Z}_p$ is $(a, b) = (0, 0)$. Use this to prove that $S = \mathbb{Z}_p[i]$ is a field in this case.

Introduction

We need to show that if there is no $c \in \mathbb{Z}_p$ such that $c^2 = -1$, then the equation $a^2 + b^2 = 0$ only has the trivial solution $(a, b) = (0, 0)$. Using this, we will prove that $S = \mathbb{Z}_p[i]$ is a field.

Solution

Step 1: Show $a^2 + b^2 = 0$ implies $a = b = 0$.

Suppose $a^2 + b^2 = 0$ for some $a, b \in \mathbb{Z}_p$. This implies:

$$a^2 = -b^2.$$

If $b = 0$, then $a^2 = 0$, so $a = 0$. Thus, $(a, b) = (0, 0)$ is a solution. Now suppose $b \neq 0$. Then:

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

Let $c = \frac{a}{b}$. Then $c^2 = -1$, contradicting the assumption that there is no $c \in \mathbb{Z}_p$ such that $c^2 = -1$. Therefore, $b = 0$ and hence $a = 0$. Thus, the only solution to $a^2 + b^2 = 0$ is $(a, b) = (0, 0)$.

Step 2: Show $S = \mathbb{Z}_p[i]$ is a field.

To prove that $S = \mathbb{Z}_p[i]$ is a field, we need to show that every non-zero element in S has a multiplicative inverse.

Consider a non-zero element $a + bi \in S$. We need to find $c + di \in S$ such that:

$$(a + bi)(c + di) = 1.$$

Expanding and using $i^2 = -1$, we get:

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i = 1.$$

Equating the real and imaginary parts to 1 and 0, respectively, we obtain:

$$ac - bd = 1 \quad \text{and} \quad ad + bc = 0.$$

Solving the second equation for d, we get $d = -\frac{bc}{a}$. Substituting into the first equation:

$$ac - b\left(-\frac{bc}{a}\right) = 1 \implies ac + \frac{b^2c}{a} = 1 \implies \frac{a^2c + b^2c}{a} = 1 \implies (a^2 + b^2)c = a.$$

Since $a^2 + b^2 \neq 0$ (as shown above), we have:

$$c = \frac{a}{a^2 + b^2}.$$

Thus,

$$d = -\frac{bc}{a} = -\frac{b}{a^2 + b^2}.$$

Therefore,

$$(a+bi)^{-1} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i.$$

Since every non-zero element $a+bi \in S$ has an inverse, $S = \mathbb{Z}_p[i]$ is a field.

Conclusion

If there is no $c \in \mathbb{Z}_p$ such that $c^2 = -1$, then the only solution to $a^2+b^2 = 0$ with $a, b \in \mathbb{Z}_p$ is $(a,b) = (0,0)$. Using this, we have shown that $S = \mathbb{Z}_p[i]$ is a field in this case.

Exercise 5. Use exercises (3) and (4) together with results from PS6 to show that $\mathbb{Z}_p[i]$ is a field if and only if $p \equiv -1 \pmod 4$.

Introduction

We need to show that $\mathbb{Z}_p[i]$ is a field if and only if $p \equiv -1 \pmod 4$.

Solution

Step 1: Use Exercise 3

From Exercise 3, we know that if there exists $c \in \mathbb{Z}_p$ such that $c^2 = -1$, then $\mathbb{Z}_p[i]$ is not a field.

Step 2: Use Exercise 4

From Exercise 4, we know that if there is no $c \in \mathbb{Z}_p$ such that $c^2 = -1$, then $\mathbb{Z}_p[i]$ is a field.

Step 3: Use Results from PS6

From PS6, Exercise 8, we know that $\mathbb{Z}_p^*$ contains an element of order 4 if and only if $p \equiv 1 \pmod 4$. This is because $\Phi(p)$ contains an element of order 4 if and only if $p \equiv 1 \pmod 4$.

Step 4: Combining the Results

If $p \equiv 1 \pmod 4$, then $\mathbb{Z}_p$ contains an element c such that $c^2 = -1$. Therefore, by Exercise 3, $\mathbb{Z}_p[i]$ is not a field.

If $p \equiv -1 \pmod 4$, then $\mathbb{Z}_p$ does not contain an element c such that $c^2 = -1$. Therefore, by Exercise 4, $\mathbb{Z}_p[i]$ is a field.

Conclusion

We have shown that $\mathbb{Z}_p[i]$ is a field if and only if $p \equiv -1 \pmod 4$.

Exercise 6.2.2. Define a map $\phi : \mathbb{R}[x] \to \mathrm{Mat}_{3\times 3}(\mathbb{R})$ by the formula

$$\phi(\sum a_k x^k) := \begin{bmatrix} a_0 & a_1 & a_2 \\ 0 & a_0 & a_1 \\ 0 & 0 & a_0 \end{bmatrix}$$

Show that ϕ is a unital ring homomorphism. What is $\ker(\phi)$?

Introduction

We need to show that the map $\phi : \mathbb{R}[x] \to \mathrm{Mat}_{3\times 3}(\mathbb{R})$ defined by $\phi(\sum a_k x^k) = \begin{bmatrix} a_0 & a_1 & a_2 \\ 0 & a_0 & a_1 \\ 0 & 0 & a_0 \end{bmatrix}$ is a unital ring homomorphism and determine its kernel.

Solution

Step 1: Show ϕ is a Ring Homomorphism.

Let $f(x) = \sum a_k x^k$ and $g(x) = \sum b_k x^k$ be polynomials in $\mathbb{R}[x]$. We need to show that $\phi(f(x) + g(x)) = \phi(f(x)) + \phi(g(x))$ and $\phi(f(x)g(x)) = \phi(f(x))\phi(g(x))$.

Addition:

$$\phi(f(x) + g(x)) = \phi\left(\sum (a_k + b_k)x^k\right) = \begin{bmatrix} a_0 + b_0 & a_1 + b_1 & a_2 + b_2 \\ 0 & a_0 + b_0 & a_1 + b_1 \\ 0 & 0 & a_0 + b_0 \end{bmatrix}.$$

$$\phi(f(x)) + \phi(g(x)) = \begin{bmatrix} a_0 & a_1 & a_2 \\ 0 & a_0 & a_1 \\ 0 & 0 & a_0 \end{bmatrix} + \begin{bmatrix} b_0 & b_1 & b_2 \\ 0 & b_0 & b_1 \\ 0 & 0 & b_0 \end{bmatrix} = \begin{bmatrix} a_0 + b_0 & a_1 + b_1 & a_2 + b_2 \\ 0 & a_0 + b_0 & a_1 + b_1 \\ 0 & 0 & a_0 + b_0 \end{bmatrix}.$$

Therefore, $\phi(f(x) + g(x)) = \phi(f(x)) + \phi(g(x))$.

Multiplication:

$$\phi(f(x)g(x)) = \phi\left(\sum_{m+n=k} a_m b_n x^k\right) = \begin{bmatrix} \sum_{m+n=0} a_m b_n & \sum_{m+n=1} a_m b_n & \sum_{m+n=2} a_m b_n \\ 0 & \sum_{m+n=0} a_m b_n & \sum_{m+n=1} a_m b_n \\ 0 & 0 & \sum_{m+n=0} a_m b_n \end{bmatrix}.$$

$$\phi(f(x))\phi(g(x)) = \begin{bmatrix} a_0 & a_1 & a_2 \\ 0 & a_0 & a_1 \\ 0 & 0 & a_0 \end{bmatrix} \begin{bmatrix} b_0 & b_1 & b_2 \\ 0 & b_0 & b_1 \\ 0 & 0 & b_0 \end{bmatrix} = \begin{bmatrix} a_0 b_0 & a_0 b_1 + a_1 b_0 & a_0 b_2 + a_1 b_1 + a_2 b_0 \\ 0 & a_0 b_0 & a_0 b_1 + a_1 b_0 \\ 0 & 0 & a_0 b_0 \end{bmatrix}.$$

Therefore, $\phi(f(x)g(x)) = \phi(f(x))\phi(g(x))$.

Step 2: Show ϕ is Unital.

The identity element in $\mathbb{R}[x]$ is the constant polynomial 1, and $\phi(1) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, which is the identity matrix in $\mathrm{Mat}_{3\times 3}(\mathbb{R})$.

Step 3: Determine the Kernel of ϕ.

The kernel of ϕ consists of all polynomials $f(x) = \sum a_k x^k \in \mathbb{R}[x]$ such that:

$$\phi(f(x)) = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

This implies $a_0 = 0$, $a_1 = 0$, and $a_2 = 0$. Therefore, $\ker(\phi) = \{f(x) \in \mathbb{R}[x] \mid f(x) = \sum_{k\geq 3} a_k x^k\}$, which consists of all polynomials with degree at least 3.

Conclusion

We have shown that ϕ is a unital ring homomorphism, and the kernel of ϕ consists of all polynomials in $\mathbb{R}[x]$ with degree at least 3.

Exercise 6.2.4. Show that if $\phi : R \to S$ is a ring homomorphism, then the image $\phi(R)$ is a subring of S.

Introduction

We need to show that if $\phi : R \to S$ is a ring homomorphism, then the image $\phi(R)$ is a subring of S.

Solution

Let $\phi : R \to S$ be a ring homomorphism. The image of ϕ is defined as:

$$\phi(R) = \{\phi(r) \mid r \in R\}.$$

To show that $\phi(R)$ is a subring of S, we need to verify that $\phi(R)$ is closed under addition, multiplication, and contains the identity element of S.

Step 1: Closure under Addition.

Let $a, b \in \phi(R)$. Then there exist $r_1, r_2 \in R$ such that $a = \phi(r_1)$ and $b = \phi(r_2)$. Since ϕ is a ring homomorphism:

$$a + b = \phi(r_1) + \phi(r_2) = \phi(r_1 + r_2).$$

Since $r_1 + r_2 \in R$, we have $a + b \in \phi(R)$. Therefore, $\phi(R)$ is closed under addition.

Step 2: Closure under Multiplication.

Let $a, b \in \phi(R)$. Then there exist $r_1, r_2 \in R$ such that $a = \phi(r_1)$ and $b = \phi(r_2)$. Since ϕ is a ring homomorphism:

$$ab = \phi(r_1)\phi(r_2) = \phi(r_1 r_2).$$

Since $r_1 r_2 \in R$, we have $ab \in \phi(R)$. Therefore, $\phi(R)$ is closed under multiplication.

Step 3: Contains the Identity Element.

Since ϕ is a ring homomorphism, it maps the identity element $1_R \in R$ to the identity element $1_S \in S$:

$$\phi(1_R) = 1_S.$$

Therefore, $\phi(R)$ contains the identity element of S.

Conclusion

We have shown that the image $\phi(R)$ of a ring homomorphism $\phi : R \to S$ is a subring of S.

Exercise 6.2.7. Let R be the ring of 3×3 upper-triangular matrices (a subring of $\mathrm{Mat}_{3\times 3}(\mathbb{R})$). Let $I \subseteq R$ be the subset of upper-triangular matrices which are 0 along the diagonal. Show that I is an ideal in R.

Introduction

We need to show that $I \subseteq R$, the subset of upper-triangular matrices which are 0 along the diagonal, is an ideal in R.

Solution

Let R be the ring of 3×3 upper-triangular matrices, and let $I \subseteq R$ be the subset of upper-triangular matrices with 0 along the diagonal:

$$I = \left\{ \begin{bmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{bmatrix} \mid a, b, c \in \mathbb{R} \right\}.$$

To show that I is an ideal in R, we need to verify that:

1. I is a subring of R.

2. For any $A \in I$ and $B \in R$, both $AB \in I$ and $BA \in I$.

Step 1: I is a Subring of R.

- **Closure under Addition:** Let $A, B \in I$. Then:
$$A = \begin{bmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & d & e \\ 0 & 0 & f \\ 0 & 0 & 0 \end{bmatrix}.$$
$$A + B = \begin{bmatrix} 0 & a+d & b+e \\ 0 & 0 & c+f \\ 0 & 0 & 0 \end{bmatrix}.$$
Since $a+d, b+e, c+f \in \mathbb{R}$, we have $A + B \in I$.

- **Closed under Negation:** Let $A \in I$. Then:
$$-A = \begin{bmatrix} 0 & -a & -b \\ 0 & 0 & -c \\ 0 & 0 & 0 \end{bmatrix}.$$
Since $-a, -b, -c \in \mathbb{R}$, we have $-A \in I$.

- **Contains the Zero Matrix:** The zero matrix $0 \in I$.

- **Closure under Multiplication:** Let $A, B \in I$. Then:
$$AB = \begin{bmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & d & e \\ 0 & 0 & f \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Since the product of any two elements in I is the zero matrix, I is closed under multiplication.

Therefore, I is a subring of R.

Step 2: I is an Ideal in R.

- **For any $A \in I$ and $B \in R$, $AB \in I$:** Let $A \in I$ and $B \in R$. Then:
$$A = \begin{bmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} x & y & z \\ 0 & u & v \\ 0 & 0 & w \end{bmatrix}.$$
$$AB = \begin{bmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} x & y & z \\ 0 & u & v \\ 0 & 0 & w \end{bmatrix} = \begin{bmatrix} 0 & au & aw+bv \\ 0 & 0 & cw \\ 0 & 0 & 0 \end{bmatrix}.$$
Since $au, aw + bv, cw \in \mathbb{R}$, we have $AB \in I$.
- **For any $A \in I$ and $B \in R$, $BA \in I$:** Let $A \in I$ and $B \in R$. Then:
$$A = \begin{bmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} x & y & z \\ 0 & u & v \\ 0 & 0 & w \end{bmatrix}.$$
$$BA = \begin{bmatrix} x & y & z \\ 0 & u & v \\ 0 & 0 & w \end{bmatrix} \begin{bmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & xa & xb+yc \\ 0 & 0 & uc \\ 0 & 0 & 0 \end{bmatrix}.$$
Since $xa, xb + yc, uc \in \mathbb{R}$, we have $BA \in I$.

Therefore, I is an ideal in R.

Conclusion

We have shown that I, the subset of upper-triangular matrices which are 0 along the diagonal, is an ideal in R.

Exercise 6.2.18. Let I and J be two ideals in a ring R. Show that the subset $I + J := \{a + b \mid a \in I, b \in J\}$ is an ideal in R.

Introduction

We need to show that the subset $I + J := \{a + b \mid a \in I, b \in J\}$ is an ideal in R.

Solution

Step 1: Show $I + J$ is a Subring.

- **Closure under Addition:** Let $x_1 = a_1 + b_1$ and $x_2 = a_2 + b_2$ be elements in $I + J$, where $a_1, a_2 \in I$ and $b_1, b_2 \in J$. Then:
$$x_1 + x_2 = (a_1 + b_1) + (a_2 + b_2) = (a_1 + a_2) + (b_1 + b_2).$$
Since I and J are ideals, $a_1 + a_2 \in I$ and $b_1 + b_2 \in J$. Therefore, $x_1 + x_2 \in I + J$.
- **Contains the Zero Element:** The zero element of R can be written as $0 = 0 + 0$, where $0 \in I$ and $0 \in J$. Therefore, $0 \in I + J$.
- **Closed under Negation:** Let $x = a + b \in I + J$, where $a \in I$ and $b \in J$. Then:
$$-x = -a - b.$$
Since I and J are ideals, $-a \in I$ and $-b \in J$. Therefore, $-x \in I + J$.

Therefore, $I + J$ is a subring of R.

Step 2: Show $I + J$ is an Ideal.

Let $r \in R$ and $x = a + b \in I + J$, where $a \in I$ and $b \in J$.

- **Left Ideal:**
$$rx = r(a + b) = ra + rb.$$
Since I and J are ideals, $ra \in I$ and $rb \in J$. Therefore, $rx \in I + J$.
- **Right Ideal:**
$$xr = (a + b)r = ar + br.$$
Since I and J are ideals, $ar \in I$ and $br \in J$. Therefore, $xr \in I + J$.

Therefore, $I + J$ is an ideal in R.

Conclusion

We have shown that the subset $I + J = \{a + b \mid a \in I, b \in J\}$ is an ideal in R.

Exercise 6.2.22. Let R be a ring without identity.

a. Define $\tilde{R} := \mathbb{Z} \times R$, the set of pairs (n, r) with $n \in \mathbb{Z}$ and $r \in R$, which is an abelian group. Define a multiplication on $\tilde{R}$ by the formula

$$(n, r)(m, s) := (nm, ns + mr + rs).$$

Show that this makes $\tilde{R}$ into a ring, with multiplicative identity $(1, 0)$.

b. Show that $r \mapsto (0, r)$ defines an injective ring homomorphism $R \to \tilde{R}$ with image $\{0\} \times R$. Show that $\{0\} \times R$ is an ideal in $\tilde{R}$.

Introduction

We need to show that the set $\tilde{R} = \mathbb{Z} \times R$ with the defined multiplication forms a ring with multiplicative identity $(1, 0)$. Additionally, we need to show that $r \mapsto (0, r)$ defines an injective ring homomorphism and that $\{0\} \times R$ is an ideal in $\tilde{R}$.

Solution

Part (a): Show $\tilde{R}$ is a Ring.

Let $\tilde{R} = \mathbb{Z} \times R$, with multiplication defined by:

$$(n, r)(m, s) = (nm, ns + mr + rs).$$

- **Associativity:** Let $(n_1, r_1), (n_2, r_2), (n_3, r_3) \in \tilde{R}$. We need to show that $((n_1, r_1)(n_2, r_2))(n_3, r_3) = (n_1, r_1)((n_2, r_2)(n_3, r_3))$.

$$\begin{aligned} ((n_1, r_1)(n_2, r_2))(n_3, r_3) &= (n_1n_2, n_1r_2 + r_1n_2 + r_1r_2)(n_3, r_3) \\ &= (n_1n_2n_3, n_1n_2r_3 + n_1r_2n_3 + r_1n_2n_3 + r_1r_2n_3 + n_1r_2r_3 + r_1r_2r_3). \end{aligned}$$

$$\begin{aligned} (n_1, r_1)((n_2, r_2)(n_3, r_3)) &= (n_1, r_1)(n_2n_3, n_2r_3 + r_2n_3 + r_2r_3) \\ &= (n_1n_2n_3, n_1(n_2r_3 + r_2n_3 + r_2r_3) + r_1(n_2n_3 + n_2r_3 + r_2n_3)). \end{aligned}$$

Therefore, $\tilde{R}$ is associative.

- **Distributivity:** Let $(n_1, r_1), (n_2, r_2), (n_3, r_3) \in \tilde{R}$. We need to show that:

$$\begin{aligned} (n_1, r_1)((n_2, r_2)+(n_3, r_3)) = (n_1, r_1)(n_2+n_3, r_2+r_3) &= (n_1(n_2+n_3), n_1(r_2+r_3)+r_1(n_2+n_3)+r_1(r_2+r_3)) \\ &= (n_1n_2 + n_1n_3, n_1r_2 + n_1r_3 + r_1n_2 + r_1n_3 + r_1r_2 + r_1r_3). \end{aligned}$$

$$\begin{aligned} (n_1, r_1)(n_2, r_2) + (n_1, r_1)(n_3, r_3) &= (n_1n_2, n_1r_2 + r_1n_2 + r_1r_2) + (n_1n_3, n_1r_3 + r_1n_3 + r_1r_3) \\ &= (n_1n_2 + n_1n_3, n_1r_2 + n_1r_3 + r_1n_2 + r_1n_3 + r_1r_2 + r_1r_3). \end{aligned}$$

Therefore, $\tilde{R}$ is distributive.

- **Multiplicative Identity:** The multiplicative identity in $\tilde{R}$ is $(1, 0)$ because:

$$(1, 0)(n, r) = (1 \cdot n, 1 \cdot r + 0 \cdot n + 0 \cdot r) = (n, r) = (n, r)(1, 0).$$

Therefore, $\tilde{R}$ is a ring with multiplicative identity $(1, 0)$.

Part (b): Show $r \mapsto (0, r)$ Defines an Injective Ring Homomorphism and that $\{0\} \times R$ is an Ideal in $\tilde{R}$.

Define $\psi : R \to \tilde{R}$ by $\psi(r) = (0, r)$.

- **Injective Ring Homomorphism:** Let $r_1, r_2 \in R$.
$$\psi(r_1 + r_2) = (0, r_1 + r_2) = (0, r_1) + (0, r_2) = \psi(r_1) + \psi(r_2).$$
$$\psi(r_1 r_2) = (0, r_1 r_2) = (0, r_1)(0, r_2) = \psi(r_1)\psi(r_2).$$
Therefore, ψ is a ring homomorphism.
- **Injective:** If $\psi(r_1) = \psi(r_2)$, then $(0, r_1) = (0, r_2)$, which implies $r_1 = r_2$. Therefore, ψ is injective.
- **Ideal:** Let $(n, r) \in \tilde{R}$ and $(0, s) \in \{0\} \times R$.
$$(n, r)(0, s) = (n \cdot 0, ns + r \cdot 0 + rs) = (0, ns + rs) \in \{0\} \times R.$$
$$(0, s)(n, r) = (0 \cdot n, 0s + sn + sr) = (0, sn + sr) \in \{0\} \times R.$$
Therefore, $\{0\} \times R$ is an ideal in $\tilde{R}$.

Conclusion

We have shown that $\tilde{R}$ is a ring with multiplicative identity $(1, 0)$, that $r \mapsto (0, r)$ defines an injective ring homomorphism, and that $\{0\} \times R$ is an ideal in $\tilde{R}$.