MATH 417, HOMEWORK 14

CHARLES ANCEL

Exercise 6.3.1. Work out the formula for multiplication in the ring $\mathbb{R}[x]/I$ in terms of canonical forms, where $I = (x^2 - 1)$. Note that canonical forms look like: $a + bx + I$, $a, b \in \mathbb{R}$.

Introduction

In this exercise, we will derive the multiplication formula for the ring $\mathbb{R}[x]/(x^2-1)$ using the canonical forms of elements. The canonical forms are $a + bx + I$ where $a, b \in \mathbb{R}$.

Solution

Let $f(x) = a + bx$ and $g(x) = c + dx$ be elements in $\mathbb{R}[x]$. We need to determine the product $f(x)g(x) \mod (x^2 - 1)$.

Step 1: Compute the Product $f(x)g(x)$

$$f(x)g(x) = (a + bx)(c + dx) = ac + adx + bcx + bdx^2.$$

Step 2: Reduce x^2 **Using the Relation** $x^2 \equiv 1 \mod (x^2-1)$ Since $x^2 \equiv 1 \mod (x^2-1)$, we can replace x^2 with 1 in the expression:

$$bdx^2 \equiv bd \mod (x^2 - 1).$$

Step 3: Substitute and Combine Like Terms Substituting x^2 with 1, we get:

$$f(x)g(x) \equiv ac + adx + bcx + bd \mod (x^2 - 1).$$

Grouping like terms, we obtain:

$$f(x)g(x) \equiv (ac + bd) + (ad + bc)x \mod (x^2 - 1).$$

Canonical Form: Therefore, the multiplication formula in $\mathbb{R}[x]/(x^2 - 1)$ is:

$$(a + bx)(c + dx) \equiv (ac + bd) + (ad + bc)x.$$

Conclusion

In the ring $\mathbb{R}[x]/(x^2 - 1)$, the product of two canonical forms $a + bx$ and $c + dx$ is given by:

$$(a + bx)(c + dx) \equiv (ac + bd) + (ad + bc)x.$$

Exercise 6.3.2. Work out the formula for multiplication in the ring $\mathbb{R}[x]/I$ in terms of canonical forms, where $I = (x^3 - 1)$. Note that canonical forms look like: $a + bx + cx^2 + I$, $a, b, c \in \mathbb{R}$.

Introduction

In this exercise, we will derive the multiplication formula for the ring $\mathbb{R}[x]/(x^3-1)$ using the canonical forms of elements. The canonical forms are $a + bx + cx^2 + I$ where $a, b, c \in \mathbb{R}$.

Solution

Let $f(x) = a + bx + cx^2$ and $g(x) = d + ex + fx^2$ be elements in $\mathbb{R}[x]$. We need to determine the product $f(x)g(x) \mod (x^3 - 1)$.

Step 1: Compute the Product $f(x)g(x)$

$$f(x)g(x) = (a + bx + cx^2)(d + ex + fx^2).$$

Expanding this, we get:

$$f(x)g(x) = ad + aex + afx^2 + bdx + bex^2 + bfx^3 + cdx^2 + cex^3 + cfx^4.$$

Step 2: Reduce Higher Powers of x Using the Relation $x^3 \equiv 1 \mod (x^3 - 1)$ Since $x^3 \equiv 1 \mod (x^3 - 1)$, we can replace higher powers of x:

$$\begin{gathered} bfx^3 \equiv bf \mod (x^3 - 1), \\ cex^3 \equiv ce \mod (x^3 - 1), \\ cfx^4 = cfx \cdot x^3 \equiv cfx \mod (x^3 - 1). \end{gathered}$$

Step 3: Substitute and Combine Like Terms Substituting the reduced terms, we get:

$$f(x)g(x) \equiv ad + bf + aex + afx^2 + bdx + bex^2 + cdx^2 + ce + cfx \mod (x^3 - 1).$$

Grouping like terms, we obtain:

$$f(x)g(x) \equiv (ad + bf + ce) + (ae + bd + cf)x + (af + be + cd)x^2 \mod (x^3 - 1).$$

Canonical Form: Therefore, the multiplication formula in $\mathbb{R}[x]/(x^3 - 1)$ is:

$$(a + bx + cx^2)(d + ex + fx^2) \equiv (ad + bf + ce) + (ae + bd + cf)x + (af + be + cd)x^2.$$

Conclusion

In the ring $\mathbb{R}[x]/(x^3-1)$, the product of two canonical forms $a+bx+cx^2$ and $d+ex+fx^2$ is given by:

$$(a + bx + cx^2)(d + ex + fx^2) \equiv (ad + bf + ce) + (ae + bd + cf)x + (af + be + cd)x^2.$$

Exercise 6.3.10. Let R be any commutative ring. Show that there is an isomorphism $R[x]/(x) \simeq R$.

Introduction

We need to show that there is an isomorphism $R[x]/(x) \simeq R$ for any commutative ring R. We will use the First Isomorphism Theorem for rings.

Solution

Consider the ring homomorphism $\phi : R[x] \to R$ defined by $\phi(f(x)) = f(0)$. This map evaluates the polynomial $f(x)$ at $x = 0$.

Step 1: Homomorphism ϕ Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$. Then,

$$\phi(f(x)) = \phi(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) = a_0.$$

Clearly, ϕ is a ring homomorphism because:

$$\phi(f(x) + g(x)) = (f(x) + g(x))|_{x=0} = f(0) + g(0) = \phi(f(x)) + \phi(g(x)),$$
$$\phi(f(x)g(x)) = (f(x)g(x))|_{x=0} = f(0)g(0) = \phi(f(x))\phi(g(x)).$$

Step 2: Kernel of ϕ The kernel of ϕ is:

$$\ker(\phi) = \{f(x) \in R[x] \mid f(0) = 0\}.$$

This implies that $f(x) \in \ker(\phi)$ can be written as $f(x) = xg(x)$ for some $g(x) \in R[x]$, which means $\ker(\phi) = (x)$.

Step 3: First Isomorphism Theorem By the First Isomorphism Theorem for rings, we have:

$$R[x]/(x) \simeq \mathrm{Im}(\phi).$$

Since $\phi(f(x)) = f(0) \in R$, the image of ϕ is R. Therefore,

$$R[x]/(x) \simeq R.$$

Conclusion

By applying the First Isomorphism Theorem for rings, we have shown that $R[x]/(x) \simeq R$ for any commutative ring R.

Exercise 4. Let R be any commutative ring, and let $c \in R$ be any element. Show that there is an isomorphism $R[x]/(x-c) \simeq R$.

Introduction

We need to show that there is an isomorphism $R[x]/(x-c) \simeq R$ for any commutative ring R and any element $c \in R$. We will use the First Isomorphism Theorem for rings.

Solution

Consider the ring homomorphism $\phi : R[x] \to R$ defined by $\phi(f(x)) = f(c)$. This map evaluates the polynomial $f(x)$ at $x = c$.

Step 1: Homomorphism ϕ Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$. Then,

$$\phi(f(x)) = \phi(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) = a_0 + a_1c + a_2c^2 + \cdots + a_nc^n = f(c).$$

Clearly, ϕ is a ring homomorphism because:

$$\phi(f(x) + g(x)) = (f(x) + g(x))|_{x=c} = f(c) + g(c) = \phi(f(x)) + \phi(g(x)),$$
$$\phi(f(x)g(x)) = (f(x)g(x))|_{x=c} = f(c)g(c) = \phi(f(x))\phi(g(x)).$$

Step 2: Kernel of ϕ The kernel of ϕ is:

$$\ker(\phi) = \{f(x) \in R[x] \mid f(c) = 0\}.$$

This implies that $f(x) \in \ker(\phi)$ can be written as $f(x) = (x-c)g(x)$ for some $g(x) \in R[x]$, which means $\ker(\phi) = (x-c)$.

Step 3: First Isomorphism Theorem By the First Isomorphism Theorem for rings, we have:

$$R[x]/(x-c) \simeq \mathrm{Im}(\phi).$$

Since $\phi(f(x)) = f(c) \in R$, the image of ϕ is R. Therefore,

$$R[x]/(x-c) \simeq R.$$

Conclusion

By applying the First Isomorphism Theorem for rings, we have shown that $R[x]/(x-c) \simeq R$ for any commutative ring R and any element $c \in R$.

Exercise 6.4.9. Let R be a domain, $X = \{(a, b) \mid a, b \in R, b \neq 0\}$, and define a relation $\sim$ on X by $(a, b) \sim (a', b')$ iff $ab' = a'b$. Show that this relation is an equivalence relation. (Hint: Your proof should make use at once of the fact that R is a domain.)
Recall that the group $C(R)$ we defined for any commutative ring R with 1 (it is defined on PS 5, and appears on PS 9 and the optional PS).

Introduction

We need to show that the relation $\sim$ on X defined by $(a, b) \sim (a', b')$ iff $ab' = a'b$ is an equivalence relation. To do this, we will prove that $\sim$ is reflexive, symmetric, and transitive.

Solution

To show that $\sim$ is an equivalence relation, we must prove that it is reflexive, symmetric, and transitive.

Step 1: Reflexivity We need to show that $(a, b) \sim (a, b)$ for all $(a, b) \in X$. This means proving $ab = ab$, which is trivially true. Therefore, $\sim$ is reflexive.

Step 2: Symmetry We need to show that if $(a, b) \sim (a', b')$, then $(a', b') \sim (a, b)$. Suppose $(a, b) \sim (a', b')$. Then $ab' = a'b$. By commutativity of multiplication in R, we have $a'b = ab'$, which shows $(a', b') \sim (a, b)$. Therefore, $\sim$ is symmetric.

Step 3: Transitivity We need to show that if $(a, b) \sim (a', b')$ and $(a', b') \sim (a'', b'')$, then $(a, b) \sim (a'', b'')$. Suppose $(a, b) \sim (a', b')$ and $(a', b') \sim (a'', b'')$. This means $ab' = a'b$ and $a'b'' = a''b'$. We need to show that $ab'' = a''b$.

Starting from $ab' = a'b$, we can multiply both sides by b'' to get:

$$ab'b'' = a'bb''.$$

Using $a'b'' = a''b'$ from the second equivalence, we substitute $a'b''$ with $a''b'$ in the equation above:

$$a(b'b'') = a''b'b.$$

Since R is a domain, we can cancel b' (which is nonzero) from both sides:

$$ab'' = a''b.$$

Therefore, $(a, b) \sim (a'', b'')$, proving that $\sim$ is transitive.

Conclusion

We have shown that the relation $\sim$ on X defined by $(a, b) \sim (a', b')$ iff $ab' = a'b$ is reflexive, symmetric, and transitive. Therefore, $\sim$ is an equivalence relation.

Exercise 7. Let K be a field such that $2 = 0$. Show that every non-identity element of $(x, y) \in C(K)$ has order 2.

Introduction

We need to show that every non-identity element of $(x, y) \in C(K)$ has order 2, given that K is a field such that $2 = 0$.

Solution

Let $(x, y) \in C(K)$ be a non-identity element. This means $(x, y) \neq (1, 0)$. The group operation in $C(K)$ is defined as:

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + y_1x_2).$$

We need to show that $(x, y) \cdot (x, y) = (1, 0)$.

Step 1: Compute the Square of (x, y)

$$(x, y) \cdot (x, y) = (xx - yy, xy + yx).$$

Simplifying the expressions using $2 = 0$ in K, we get:

$$(xx - yy, xy + yx) = (x^2 - y^2, 2xy).$$

Since $2 = 0$, we have $2xy = 0$. Therefore, the expression simplifies to:

$$(x^2 - y^2, 0).$$

Step 2: Non-identity Element Condition Since (x, y) is a non-identity element, we have $(x, y) \neq (1, 0)$. This implies $x \neq 1$ or $y \neq 0$.

Step 3: Solve for $(x, y) \cdot (x, y) = (1, 0)$ We need to show that $(x^2 - y^2, 0) = (1, 0)$:

$$x^2 - y^2 = 1 \quad \text{and} \quad 0 = 0.$$

Therefore, the square of (x, y) is $(1, 0)$, which is the identity element in $C(K)$.

Conclusion

We have shown that every non-identity element of $(x, y) \in C(K)$ has order 2 if K is a field such that $2 = 0$.

Exercise 8. Let K be a field which contains an element $i \in K$ such that $i^2 = -1$. Show that the function

$$\phi : C(K) \to K^\times, \qquad \phi(x, y) := x + iy$$

is a homomorphism of groups.

Introduction

We need to show that the function $\phi : C(K) \to K^\times$ defined by $\phi(x, y) = x + iy$ is a homomorphism of groups, given that K is a field containing an element $i \in K$ such that $i^2 = -1$.

Solution

Let $(x_1, y_1), (x_2, y_2) \in C(K)$. The group operation in $C(K)$ is defined as:

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + y_1x_2).$$

We need to show that $\phi((x_1, y_1) \cdot (x_2, y_2)) = \phi(x_1, y_1)\phi(x_2, y_2)$.

Step 1: Compute $\phi((x_1, y_1) \cdot (x_2, y_2))$

$$\phi((x_1, y_1) \cdot (x_2, y_2)) = \phi(x_1x_2 - y_1y_2, x_1y_2 + y_1x_2).$$

By the definition of ϕ, we have:

$$\phi(x_1x_2 - y_1y_2, x_1y_2 + y_1x_2) = (x_1x_2 - y_1y_2) + i(x_1y_2 + y_1x_2).$$

Step 2: Compute $\phi(x_1, y_1)\phi(x_2, y_2)$

$$\phi(x_1, y_1) = x_1 + iy_1 \quad \text{and} \quad \phi(x_2, y_2) = x_2 + iy_2.$$

Therefore,

$$\phi(x_1, y_1)\phi(x_2, y_2) = (x_1 + iy_1)(x_2 + iy_2).$$

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

$$(x_1 + iy_1)(x_2 + iy_2) = x_1x_2 + ix_1y_2 + iy_1x_2 + i^2y_1y_2 = x_1x_2 + ix_1y_2 + iy_1x_2 - y_1y_2.$$

Simplifying, we get:

$$x_1x_2 - y_1y_2 + i(x_1y_2 + y_1x_2).$$

Step 3: Verify the Homomorphism Property Comparing the results from Steps 1 and 2, we have:

$$\phi((x_1, y_1) \cdot (x_2, y_2)) = (x_1x_2 - y_1y_2) + i(x_1y_2 + y_1x_2) = \phi(x_1, y_1)\phi(x_2, y_2).$$

Therefore, ϕ is a homomorphism.

Conclusion

We have shown that the function $\phi : C(K) \to K^\times$ defined by $\phi(x, y) = x + iy$ is a homomorphism of groups.

Exercise 9. Let K as in the previous problem, and suppose also that $2 \neq 0$ in K. Show that the homomorphism ϕ is injective. Note: on the optional assignment, it is shown that if K is a finite field, then $K^{\times}$ is cyclic. Thus for every finite field K as in (9), $C(K)$ is a subgroup of a cyclic subgroup of a cyclic group and thus cyclic. This includes $\mathbb{Z}_p$ when $p \equiv 1 \pmod 4$. When $p \equiv -1 \pmod 4$, we know that $\mathbb{Z}_p$ is a subfield of $K = \mathbb{Z}_p[i]$, as shown in PS 13, so $C(\mathbb{Z}_p) \leq C(\mathbb{Z}_p[i])$ is also cyclic.

Introduction

We need to show that the homomorphism ϕ defined by $\phi(x, y) = x + iy$ is injective, given that K is a field containing an element $i \in K$ such that $i^2 = -1$ and $2 \neq 0$.

Solution

To show that ϕ is injective, we need to prove that $\phi(x, y) = \phi(x', y')$ implies $(x, y) = (x', y')$ for $(x, y), (x', y') \in C(K)$.

Step 1: Assume $\phi(x, y) = \phi(x', y')$ Suppose $\phi(x, y) = \phi(x', y')$. This means:

$$x + iy = x' + iy'.$$

Step 2: Equate Real and Imaginary Parts Since i is an element in K with $i^2 = -1$, we can equate the real and imaginary parts:

$$x = x' \quad \text{and} \quad iy = iy'.$$

Given that $i \neq 0$ and K is a field (so there are no zero divisors), we can divide by i:

$$y = y'.$$

Step 3: Conclusion Therefore, if $\phi(x, y) = \phi(x', y')$, then $(x, y) = (x', y')$. This shows that ϕ is injective.

Conclusion

We have shown that the homomorphism ϕ defined by $\phi(x, y) = x + iy$ is injective, given that K is a field containing an element $i \in K$ such that $i^2 = -1$ and $2 \neq 0$.