MA3202: Algebra II

Satvik Saha, `19MS154` February 3, 2022

Exercise 1 Let R be a unit ring. Consider the map $f\colon \mathbb{Z} \to R$ defined by $f(n) = n \cdot 1$.

(i) Show that f is a homomorphism.

(ii) Show that f is not always injective.

(iii) When is f an embedding (injective homomorphism)?

Solution

(i) It is clear that $f(1) = 1$; for positive m, n, we have $f(m)+f(n) = m\cdot 1+n\cdot 1 = (m+n)\cdot 1 = f(m+n)$, and $f(m)f(n) = (m \cdot 1) \cdot (n \cdot 1) = (mn) \cdot 1 = f(mn)$ by distributing and counting. It is easy to extend this to negative m, n by observing that $f(-n) = -f(n)$.

(ii) Consider $f\colon \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$, $n \mapsto n \cdot 1$. Then, $f(2) = 2 \cdot 1 = 1 + 1 \equiv 0 = f(0)$.

(iii) It is easy to check that f is an embedding precisely when R has characteristic zero. In other words, the elements $n \cdot 1$ are all distinct.

Exercise 2 Let R be a ring and $I \subset R$ be an ideal. Show that if R has identity, so does R/I. What about the converse?

Solution If $1 \in \mathbb{R}$, then $1 + I$ is the multiplicative identity in R/I.

The converse is not true; note that $2\mathbb{Z}/6\mathbb{Z} = \{0, 2, 4\}$ has 4 as the identity, since $4 \cdot 2 = 8 \equiv 2$ and $4 \cdot 4 = 16 \equiv 4$. However, $2\mathbb{Z}$ does not have an identity.

Exercise 3 Let R be a ring and $I \subset R$ be an ideal. Show that if R is commutative, so is R/I. What about the converse?

Solution If $xy = yx$ in R, then $(x + I)(y + I) = xy + I = (y + I)(x + I)$ in R/I.

The converse is not true; note that $R = \mathbb{Z} \times M_2(\mathbb{R})$ is a non-commutative ring, but $I = \{0\} \times M_2(\mathbb{R})$ is an ideal, with $R/I \cong \mathbb{Z}$ being commutative.

Exercise 4 Show that the characteristic of a simple ring is either 0 or p, where p is a prime number.

Solution Suppose that R has characteristic $n = ab > 0$, where $1 < a, b < n$. Then there exists an element $x_0 \in R$ such that $nx_0 = 0$, and $mx_0 \neq 0$ for all $0 < m < n$. Now, consider the elements $aR = \{ax : x \in R\}$. This is clearly an ideal of $\mathbb{R}$; since $ax_0 \neq 0$, $aR \neq \{0\}$. Since R is simple, $aR = R$. Similarly, $bR = R$. Thus, $\{0\} = nR = (ab)R = a(bR) = aR \neq \{0\}$, a contradiction.

Exercise 5 Show that $\mathbb{R}[X]/(X^2 + 1)$ and $\mathbb{C}$ are isomorphic as rings.

Solution By Euclid's Division Lemma, every polynomial in $\mathbb{R}[X]$ can be uniquely expressed as

$$p(x) = u(x)(x^2 + 1) + bx + a.$$

Thus, every polynomial in $\mathbb{R}[X]$ belongs to exactly one equivalence class $[ax + b]$. Define the map

$$\varphi\colon \mathbb{R}[X] \to \mathbb{C}, \qquad u(x)(x^2 + 1) + bx + a \mapsto a + ib.$$

It is clear that $\varphi(1) = 1$, $\varphi(p + q) = \varphi(p) + \varphi(q)$. Now consider

$$p(x) = u(x)(x^2 + 1) + bx + a, \qquad q(x) = v(x)(x^2 + 1) + dx + c.$$

Then,

$$p(x)q(x) = (u(x)v(x) + u(x)(dx + c) + v(x)(bx + a))(x^2 + 1) + bdx^2 + (ad + bc)x + ac.$$

Tweaking this gives

$$p(x)q(x) = (u(x)v(x) + u(x)(dx + c) + v(x)(bx + a) + bd)(x^2 + 1) + (ad + bc)x + ac - bd.$$

In other words,

$$\varphi(pq) = (ac - bd) + i(ad + bc) = \varphi(p)\varphi(q).$$

Thus, φ is a homomorphism, and it is easy to see that it is surjective. Its kernel consists of all the polynomials mapped to 0, i.e. all polynomials of the form $u(x)(x^2+1)$. This is precisely (X^2+1). Thus, the First Isomorphism Theorem guarantees that $R[X]/(X^2+1) \cong \mathbb{C}$.

Exercise 6 Let R be a ring. What are all ideals of $R \times R$?

Solution All ideals of R are of the form $I \times J$, where $I, J \subset R$ are ideals of R.

Exercise 7 Show that $\mathbb{Z}$ and $\mathbb{Z} \times \mathbb{Z}$ are not isomorphic.

Solution Note that $\mathbb{Z}$ is an integral domain, but $\mathbb{Z} \times \mathbb{Z}$ is not since $(1, 0)$ is a zero divisor.

Exercise 8 Are $\mathbb{Z}$ and $\mathbb{Q}$ isomorphic as rings?

Solution No; if $\varphi\colon \mathbb{Q} \to \mathbb{Z}$ were an isomorphism, then set $a = \varphi(1/2)$. We now demand $2a = \varphi(1) = 1$, which is impossible.

Exercise 9 Let $R = C([1, 3])$ and $I(2) = \{f \in R : f(2) = 0\}$. Prove that $I(2)$ is an ideal of R.

Solution It is clear that $I(2)$ is a subring of R; it contains the zero function, and if $f, g \in I(2)$, then $f(2) = g(2) = 0$ hence $(f + g)(2) = 0$, $(-f)(2) = 0$. Furthermore if $h \in R$, then $(hf)(2) = h(2)f(2) = 0$ so $hf \in I(2)$.

Exercise 10 Show that the ring $\mathbb{Z}/14\mathbb{Z}$ is isomorphic to the product of $\mathbb{Z}/7\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$.

Solution Note that $(7\mathbb{Z})(2\mathbb{Z}) = 14\mathbb{Z}$. Furthermore, $7\mathbb{Z} + 2\mathbb{Z} = \mathbb{Z}$, since 7 and 2 are co-prime. The isomorphism $\mathbb{Z}/(7\mathbb{Z} \cdot 2\mathbb{Z}) \cong \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ now follows from the Chinese Remainder Theorem.