Solutions 07

P7.1. Let R be a commutative ring and let $R[x]$ be the associated polynomial ring. For every ring S containing R as a subring and every element $s \in S$, prove that there exists a unique ring homomorphism $\varphi\colon R[x] \to S$ that sends x to s and fixes the subring R.

Solution. We treat uniqueness and existence separately.

(*uniqueness*) Suppose that $\varphi\colon R[x] \to S$ is a ring homomorphism such that $\varphi(a) = a$ for all $a \in R$ and $\varphi(x) = s \in S$. For each $f := a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$ where $m \in \mathbb{N}$ and $a_m, a_{m-1}, \ldots, a_0 \in R \subseteq S$, the properties of a ring homomorphism give

$$\begin{aligned}\varphi(f) &= \varphi(a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0)\\ &= \varphi(a_m)(\varphi(x)^m) + \varphi(a_{m-1})(\varphi(x)^{m-1}) + \cdots + \varphi(a_1)\varphi(x) + \varphi(a_0)\\ &= a_m s^m + a_{m-1}s^{m-1} + \cdots + a_1 s + a_0\,.\end{aligned}$$

Hence, fixing the coefficient ring R and sending the indeterminate x to the element $s \in S$ completely determines the output of the ring homomorphism φ. In other words, there is at most one ring homomorphism satisfying the given conditions.

(*existence*) Suppose that

$$\begin{aligned}f &= a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \in R[x]\,,\\ g &= b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 \in R[x]\,,\end{aligned}$$

where $m, n \in \mathbb{N}$, $m \geqslant n$, and $a_m, a_{m-1}, \ldots, a_0, b_n, b_{n-1}, \ldots, b_0 \in R \subseteq S$.

Consider the map $\varphi\colon R[x] \to S$ defined, for each $f \in R[x]$, by

$$\varphi(f) = \varphi(a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0) := a_m s^m + a_{m-1}s^{m-1} + \cdots + a_1 s + a_0\,.$$

This map of sets is well-defined because $a_j \in R \subseteq S$ for all $0 \leqslant j \leqslant m$, $s \in S$, and the ring S is closed under addition and multiplication. By construction, the map φ satisfies $\varphi(a) = a$ for all $a \in R \subseteq S$ and $\varphi(x) = s$. Moreover, we see that

$$\begin{aligned}\varphi(f+g) &= \varphi((a_m + b_m)x^m + (a_{m-1} + b_{m-1})x^{m-1} + \cdots + (a_1 + b_1)x + (a_0 + b_0))\\ &= (a_m + b_m)s^m + (a_{m-1} + b_{m-1})s^{m-1} + \cdots + (a_1 + b_1)s + (a_0 + b_0)\\ &= (a_m s^m + a_{m-1}s^{m-1} + \cdots + a_1 s + a_0) + (b_n s^n + b_{n-1}s^{n-1} + \cdots + b_1 s + b_0)\\ &= \varphi(f) + \varphi(g)\,,\\ \varphi(fg) &= \varphi(a_m b_n x^{m+n} + (a_m b_{n-1} + a_{m-1}b_n)x^{m+n-1} + \cdots + (a_1 b_0 + a_0 b_1)x + (a_0 b_0))\\ &= a_m b_n s^{m+n} + (a_m b_{n-1} + a_{m-1}b_n)s^{m+n-1} + \cdots + (a_1 b_0 + a_0 b_1)s + (a_0 b_0)\\ &= (a_m s^m + a_{m-1}s^{m-1} + \cdots + a_1 s + a_0)(b_n s^n + b_{n-1}s^{n-1} + \cdots + b_1 s + b_0)\\ &= \varphi(f)\varphi(g)\,,\\ \varphi(1) &= 1\,.\end{aligned}$$

Hence, the map φ is a ring homomorphism. □

Remark. This characterization of the ring homomorphisms having a polynomial ring as its source is called the *universal (mapping) property* of a polynomial ring.

CC BY NC ND

P7.2. Let $\mathrm{T}(3,\mathbb{Z})$ be the subset of all lower triangular (3×3)-matrices with integer entries;

$$\mathrm{T}(3,\mathbb{Z}) := \left\{ \begin{bmatrix} a_0 & 0 & 0 \\ a_1 & a_3 & 0 \\ a_2 & a_4 & a_5 \end{bmatrix} \,\middle|\, a_0, a_1, \ldots, a_5 \in \mathbb{Z} \right\}.$$

i. Verify that $\mathrm{T}(3,\mathbb{Z})$ is a subring of the noncommutative ring of all (3×3)-matrices with integer entries.

ii. Given the matrix

$$\mathbf{N} := \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix},$$

let $\eta\colon \mathbb{Z}[x] \to \mathrm{T}(3,\mathbb{Z})$ be the ring homomorphism defined by

$$\eta(a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0) = a_m \mathbf{N}^m + a_{m-1} \mathbf{N}^{m-1} + \cdots + a_1 \mathbf{N} + a_0 \mathbf{I}.$$

Find a polynomial g in $\mathbb{Z}[x]$ such that $\mathrm{Ker}(\eta) = \langle g \rangle$.

Solution.

i. For all matrices

$$\mathbf{A} := \begin{bmatrix} a_0 & 0 & 0 \\ a_1 & a_3 & 0 \\ a_2 & a_4 & a_5 \end{bmatrix} \in \mathrm{T}(3,\mathbb{Z}) \qquad \text{and} \qquad \mathbf{B} := \begin{bmatrix} b_0 & 0 & 0 \\ b_1 & b_3 & 0 \\ b_2 & b_4 & b_5 \end{bmatrix} \in \mathrm{T}(3,\mathbb{Z}),$$

we have

$$\mathbf{A} - \mathbf{B} = \begin{bmatrix} a_0 & 0 & 0 \\ a_1 & a_3 & 0 \\ a_2 & a_4 & a_5 \end{bmatrix} - \begin{bmatrix} b_0 & 0 & 0 \\ b_1 & b_3 & 0 \\ b_2 & b_4 & b_5 \end{bmatrix} = \begin{bmatrix} a_0 - b_0 & 0 & 0 \\ a_1 - b_1 & a_3 - b_3 & 0 \\ a_2 - b_2 & a_4 - b_4 & a_5 - b_5 \end{bmatrix} \in \mathrm{T}(3,\mathbb{Z}),$$

$$\mathbf{A}\,\mathbf{B} = \begin{bmatrix} a_0 & 0 & 0 \\ a_1 & a_3 & 0 \\ a_2 & a_4 & a_5 \end{bmatrix} \begin{bmatrix} b_0 & 0 & 0 \\ b_1 & b_3 & 0 \\ b_2 & b_4 & b_5 \end{bmatrix} = \begin{bmatrix} a_0 b_0 & 0 & 0 \\ a_1 b_0 + a_3 b_1 & a_3 b_3 & 0 \\ a_2 b_0 + a_4 b_1 + a_5 b_2 & a_4 b_3 + a_5 b_4 & a_5 b_5 \end{bmatrix} \in \mathrm{T}(3,\mathbb{Z})$$

$$\mathbf{I} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \in \mathrm{T}(3,\mathbb{Z}).$$

We conclude that $\mathrm{T}(3,\mathbb{Z})$ is a subring.

ii. Observe that

$$\mathbf{N}^2 = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} \quad \text{and} \quad \mathbf{N}^3 = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Hence, for any polynomial $f := a_m x^m + \cdots + a_1 x + a_0$ in $\mathbb{Z}[x]$, we have

$$\begin{aligned} \eta(f) &= a_2 \mathbf{N}^2 + a_1 \mathbf{N} + a_0 \mathbf{I} \\ &= \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ a_2 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 \\ a_1 & 0 & 0 \\ 0 & a_1 & 0 \end{bmatrix} + \begin{bmatrix} a_0 & 0 & 0 \\ 0 & a_0 & 0 \\ 0 & 0 & a_0 \end{bmatrix} = \begin{bmatrix} a_0 & 0 & 0 \\ a_1 & a_0 & 0 \\ a_2 & a_1 & a_0 \end{bmatrix} \end{aligned}$$

It follows that f belongs to $\mathrm{Ker}(\eta)$ if and only if $a_0 = a_1 = a_2 = 0$ or

$$f = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_3 x^3 = (a_m x^{m-3} + a_{m-1} x^{m-4} + \cdots + a_3) x^3.$$

In other words, the polynomial f belongs to $\mathrm{Ker}(\eta)$ if and only if x^3 divides f. We conclude that $\mathrm{Ker}(\eta) = \langle x^3 \rangle$. □

P7.3. Consider the ideal $I := \langle 1 + 2\,\mathrm{i} \rangle$ in the ring $\mathbb{Z}[\mathrm{i}] := \{a + b\,\mathrm{i} \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$ of Gaussian integers. Let $R := \mathbb{Z}[\mathrm{i}]/I$ be the quotient ring.

i. Are the cosets $\mathrm{i} + I$ and $2 + I$ equal in R?

ii. How many elements does R have?

iii. What is the characteristic of R?

iv. Is R a field?

Solution.

i. Since $(\mathrm{i} + I) - (2 + I) = -2 + \mathrm{i} = \mathrm{i}\,(1 + 2\,\mathrm{i})$, the difference $-2 + \mathrm{i}$ belongs to the ideal I. Hence, the cosets $\mathrm{i} + I$ and $2 + I$ are equal in the quotient ring R.

ii. The black dots in Figure 1 correspond to the elements in the ideal I and the grey dots in Figure 1 correspond to the elements in $\mathbb{Z}[\mathrm{i}]$. From Figure 1, we see that one may obtain any Gaussian integer by adding an appropriate element of I to 0, 1, 2, $1 + \mathrm{i}$, or $2 + \mathrm{i}$. Furthermore, the difference between any two of these five Gaussian integers does not belong to I. Therefore, the quotient ring R has five elements: $0 + I$, $1 + I$, $2 + I$, $(1 + \mathrm{i}) + I$, and $(2 + \mathrm{i}) + I$.

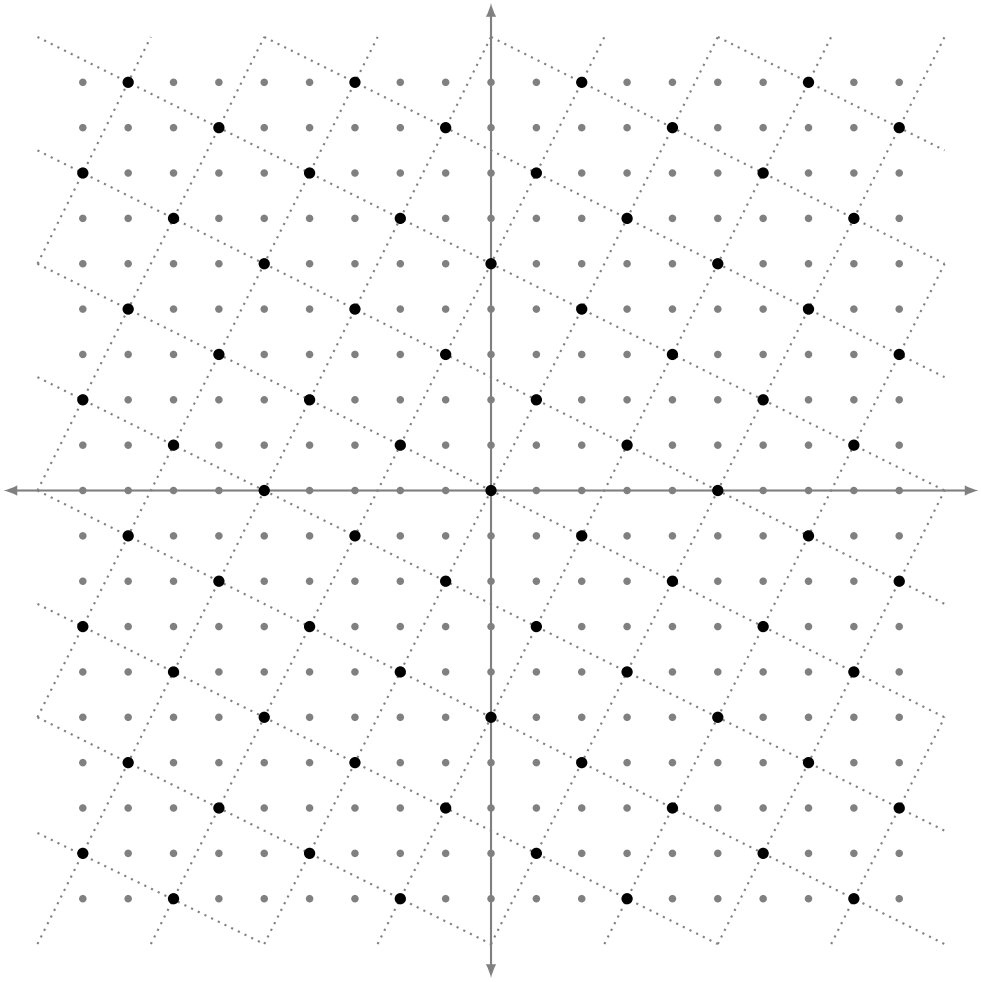


Figure 1. Multiples of the Gaussian integer $1 + 2\,\mathrm{i}$

CC BY NC ND

iii. As $5-(0)=5=(1-2\,\mathrm{i})\,(1+2\,\mathrm{i})$, the difference 5 belongs to the ideal I. Hence, the cosets $5(1+I)=5+I$ and $0+I$ are equal in the quotient ring R. Similarly, we have $3-(1+\mathrm{i})=2-\mathrm{i}=-\mathrm{i}\,(1+2\,\mathrm{i})$ and $4-(2+\mathrm{i})=2-\mathrm{i}=-\mathrm{i}\,(1+2\,\mathrm{i})$, so we have $3(1+I)=3+I=(1+\mathrm{i})+I$ and $4(1+I)=4+I=(2+\mathrm{i})+I$ in R. Thus, the ring R has characteristic 5.

iv. Since

$$\begin{aligned}(1+I)(1+I)&=1+I\\(2+I)\big((1+\mathrm{i})+I\big)&=(2+2\,\mathrm{i})+I=\big(1+(1+2\,\mathrm{i})\big)+I=1+I\\\big((2+\mathrm{i})+I\big)\big((2+\mathrm{i})+I\big)&=(3+4\,\mathrm{i})+I=\big(1+2(1+2\,\mathrm{i})\big)+I=1+I\,,\end{aligned}$$

part **ii** implies that every nonzero element in R is a unit, so R is a field. □

cc BY NC ND