Solutions 07

P7.1. Both of the subsets

$$R := \mathbb{Q}[\sqrt{2}] = \left\{a + b\sqrt{2} \in \mathbb{R} \;\middle|\; a, b \in \mathbb{Q}\right\}, \quad \text{and} \quad S := \mathbb{Q}[\sqrt{3}] = \left\{a + b\sqrt{3} \in \mathbb{R} \;\middle|\; a, b \in \mathbb{Q}\right\}.$$

are subrings of $\mathbb{R}$. Prove that there does not exist a ring homomorphism $\varphi \colon R \to S$.

Solution. Suppose that the map $\varphi \colon R \to S$ is a ring homomorphism. Hence, there exists rational numbers a and b such that $\varphi(\sqrt{2}) = a + b\sqrt{3}$. It follows that

$$\begin{aligned} 2 = 1 + 1 = \varphi(1+1) = \varphi(2) &= \varphi(\sqrt{2}\sqrt{2}) \\ &= \varphi(\sqrt{2})\,\varphi(\sqrt{2}) = (a + b\sqrt{3})^2 = (a^2 + 3b^2) + 2ab\sqrt{3}\,. \end{aligned}$$

Since $\sqrt{3}$ is an irrational number, we deduce that $ab = 0$. If $a \neq 0$ and $b = 0$, then we would have $2 = a^2$ and $a = \pm\sqrt{2}$. However, the number $\sqrt{2}$ is irrational contradicting the definition of a. Similarly, if $a = 0$ and $b \neq 0$, then we would have $2 = 3b^2$ and $b = \pm\sqrt{2/3}$. However, the number $\sqrt{2/3}$ is irrational contradicting the definition of b. Thus, we see that $a = b = 0$ and $\varphi(\sqrt{2}) = 0$.

Now, the properties of a ring homomorphism give

$$0 = \varphi(0) = \varphi(1-1) = \varphi(1 + (-1)) = \varphi(1) + \varphi(-1) = 1 + \varphi(-1)\,,$$

so $\varphi(-1) = -1$. We thereby obtain

$$\begin{aligned} 1 = \varphi(1) &= \varphi(-1 + \sqrt{2} - \sqrt{2} + 2) \\ &= \varphi((1+\sqrt{2})(-1+\sqrt{2})) \\ &= \varphi(1+\sqrt{2})\,\varphi(-1+\sqrt{2}) \\ &= \big(\varphi(1) + \varphi(\sqrt{2})\big)\big(\varphi(-1) + \varphi(\sqrt{2})\big) = (1)(-1) = -1\,, \end{aligned}$$

which is a contradiction. Thus, no map $\varphi \colon R \to S$ is a ring homomorphism. □

P7.2. Let $\mathrm{U}_4(\mathbb{Z})$ be the subset of all upper triangular (4×4)-matrices with integer entries;

$$\mathrm{U}_4(\mathbb{Z}) := \left\{ \begin{bmatrix} a_0 & a_1 & a_3 & a_6 \\ 0 & a_2 & a_4 & a_7 \\ 0 & 0 & a_5 & a_8 \\ 0 & 0 & 0 & a_9 \end{bmatrix} \;\middle|\; a_0, a_1, \dots, a_9 \in \mathbb{Z} \right\}.$$

i. Verify that $\mathrm{U}_4(\mathbb{Z})$ is a subring of the ring of all (4×4)-matrices with integer entries.

ii. Given the matrix

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

let $\eta \colon \mathbb{Z}[x] \to \mathrm{U}_4(\mathbb{Z})$ 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 $\mathrm{Ker}(\eta) = \langle g \rangle$.

CC BY NC ND

Solution.

i. For any matrices

$$\mathbf{A} := \begin{bmatrix} a_0 & a_1 & a_3 & a_6 \\ 0 & a_2 & a_4 & a_7 \\ 0 & 0 & a_5 & a_8 \\ 0 & 0 & 0 & a_9 \end{bmatrix} \qquad \text{and} \qquad \mathbf{B} := \begin{bmatrix} b_0 & b_1 & b_3 & b_6 \\ 0 & b_2 & b_4 & b_7 \\ 0 & 0 & b_5 & b_8 \\ 0 & 0 & 0 & b_9 \end{bmatrix}$$

in $\mathrm{U}_4(\mathbb{Z})$, we have

$$\mathbf{A} - \mathbf{B} = \begin{bmatrix} a_0 & a_1 & a_3 & a_6 \\ 0 & a_2 & a_4 & a_7 \\ 0 & 0 & a_5 & a_8 \\ 0 & 0 & 0 & a_9 \end{bmatrix} - \begin{bmatrix} b_0 & b_1 & b_3 & b_6 \\ 0 & b_2 & b_4 & b_7 \\ 0 & 0 & b_5 & b_8 \\ 0 & 0 & 0 & b_9 \end{bmatrix} = \begin{bmatrix} a_0 - b_0 & a_1 - b_1 & a_3 - b_3 & a_6 - b_6 \\ 0 & a_2 - b_2 & a_4 - b_4 & a_7 - b_7 \\ 0 & 0 & a_5 - b_5 & a_8 - b_8 \\ 0 & 0 & 0 & a_9 - b_9 \end{bmatrix} \in \mathrm{U}_4(\mathbb{Z})$$

$$\begin{aligned} \mathbf{A}\,\mathbf{B} &= \begin{bmatrix} a_0 & a_1 & a_3 & a_6 \\ 0 & a_2 & a_4 & a_7 \\ 0 & 0 & a_5 & a_8 \\ 0 & 0 & 0 & a_9 \end{bmatrix} \begin{bmatrix} b_0 & b_1 & b_3 & b_6 \\ 0 & b_2 & b_4 & b_7 \\ 0 & 0 & b_5 & b_8 \\ 0 & 0 & 0 & b_9 \end{bmatrix} \\ &= \begin{bmatrix} a_0 b_0 & a_0 b_1 + a_1 b_2 & a_0 b_3 + a_1 b_4 + a_3 b_5 & a_0 b_6 + a_1 b_7 + a_3 b_8 + a_6 b_9 \\ 0 & a_2 b_2 & a_2 b_4 + a_4 b_5 & a_2 b_7 + a_4 b_8 + a_7 b_9 \\ 0 & 0 & a_5 b_5 & a_5 b_8 + a_8 b_9 \\ 0 & 0 & 0 & a_9 b_9 \end{bmatrix} \in \mathrm{U}_4(\mathbb{Z}) \end{aligned}$$

$$\mathbf{I} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \in \mathrm{U}_4(\mathbb{Z})$$

so $\mathrm{U}_4(\mathbb{Z})$ is a subring.

ii. First observe that

$$\begin{aligned} \mathbf{N}^2 &= \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \\ \mathbf{N}^3 &= \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \\ \mathbf{N}^4 &= \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}. \end{aligned}$$

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

$$\begin{aligned} \eta(f) &= a_3\,\mathbf{N}^3 + a_2\,\mathbf{N}^2 + a_1\,\mathbf{N} + a_0\,\mathbf{I} \\ &= \begin{bmatrix} 0 & 0 & 0 & a_3 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 & a_2 & 0 \\ 0 & 0 & 0 & a_2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & a_1 & 0 & 0 \\ 0 & 0 & a_1 & 0 \\ 0 & 0 & 0 & a_1 \\ 0 & 0 & 0 & 0 \end{bmatrix} + \begin{bmatrix} a_0 & 0 & 0 & 0 \\ 0 & a_0 & 0 & 0 \\ 0 & 0 & a_0 & 0 \\ 0 & 0 & 0 & a_0 \end{bmatrix} = \begin{bmatrix} a_0 & a_1 & a_2 & a_3 \\ 0 & a_0 & a_1 & a_2 \\ 0 & 0 & a_0 & a_1 \\ 0 & 0 & 0 & a_0 \end{bmatrix} \end{aligned}$$

CC BY NC ND

It follows that f belongs to $\mathrm{Ker}(\eta)$ if and only if $a_0 = a_1 = a_2 = a_3 = 0$ or

$$f = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_4 x^4 = (a_m x^{m-4} + a_{m-1} x^{m-5} + \cdots + a_4) x^4 .$$

In other words, the polynomial f belong to $\mathrm{Ker}(\eta)$ if and only if x^4 divides f. We conclude that $\mathrm{Ker}(\eta) = \langle x^4 \rangle$. □

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 $-2 + \mathrm{i} = \mathrm{i}\,(1 + 2\,\mathrm{i})$, the difference $-2 + \mathrm{i}$ belongs to the ideal I. Hence, the cosets $\mathrm{i} + I$ and $2 + I$ 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 $(2 + \mathrm{i}) + I$.

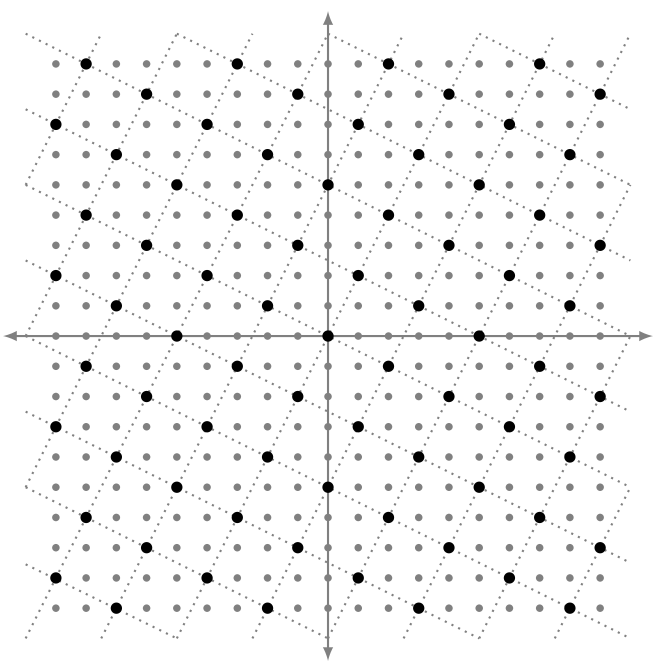

Figure 1. Multiples of the Gaussian integer $1 + 2\,\mathrm{i}$

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

cc BY NC ND

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