Solutions 11

P11.1. Consider the subring $\mathbb{Z}[\sqrt{-17}] := \{a + b\sqrt{-17} \mid a, b \in \mathbb{Z}\}$ of the complex numbers.

i. Show that the norm function $\mathrm{N}\colon \mathbb{Z}[\sqrt{-17}] \to \mathbb{Z}$ defined, for any integers a and b, by $\mathrm{N}(a + b\sqrt{-17}) = a^2 + 17\,b^2$ is compatible with multiplication: the norm of a product is equal to the product of the norms of the factors.

ii. Confirm that $3 + \sqrt{-17}$ is an irreducible element in $\mathbb{Z}[\sqrt{-17}]$.

iii. Verify that the ideal $\langle 3 + \sqrt{-17}\rangle$ is not prime in $\mathbb{Z}[\sqrt{-17}]$.

Solution.

i. For any integers a, b, c, and d, we have

$$\begin{aligned}\mathrm{N}\Big((a + b\sqrt{-17})(c + d\sqrt{-17})\Big) &= \mathrm{N}\Big((a\,c - 17\,b\,d) + (a\,d + b\,c)\sqrt{-17}\Big)\\ &= (a\,c - 17\,b\,d)^2 + 17\,(a\,d + b\,c)^2\\ &= a^2\,c^2 - 34\,a\,b\,c\,d + 289\,b^2\,d^2 + 17\,a^2\,d^2 + 34\,a\,b\,c\,d + 17\,b^2\,c^2\\ &= a^2\,(c^2 + 17\,d^2) + 17\,b^2\,(c^2 + 17\,d^2)\\ &= (a^2 + 17\,b^2)(c^2 + 17\,d^2) = \mathrm{N}(a + b\sqrt{-17})\ \mathrm{N}(c + d\sqrt{-17})\,,\end{aligned}$$

so the norm function $\mathrm{N}\colon \mathbb{Z}[\sqrt{-17}] \to \mathbb{Z}$ is compatible with multiplication.

ii. Consider integers a, b, c, and d such that $(a + b\sqrt{-17})(c + d\sqrt{-17}) = 3 + \sqrt{-17}$. Applying the norm function to both sides and using part **i**, we obtain

$$\mathrm{N}(a + b\sqrt{-17})\ \mathrm{N}(c + d\sqrt{-17}) = \mathrm{N}(3 + \sqrt{-17}) = 9 + 17(1) = 26\,.$$

Hence, we deduce that $\mathrm{N}(a + b\sqrt{-17}) = a^2 + 17\,b^2$ is either 1, 2, 13, or 26. As either 2 nor 13 are perfect squares in $\mathbb{Z}$, the equations $a^2 + 17\,b^2 = 2$ and $a^2 + 17\,b^2 = 13$ have no integer solutions. By interchanging factors if necessary, we may assume that $\mathrm{N}(a + b\sqrt{-17}) = a^2 + 17\,b^2 = 1$, which means $a = \pm 1$ and $b = 0$. Since one of the factors is a unit, we conclude that $3 + \sqrt{-17}$ is irreducible.

iii. Since $(a + b\sqrt{-17})(2 + \sqrt{-5}) = (3\,a - 17\,b) + (a + 3\,b)\sqrt{-17}$ and

$$(3 - \sqrt{-17})(3 + \sqrt{-17}) = (3^2 + 17(1^2)) = 26\,,$$

we deduce that $\langle 3 + \sqrt{-17}\rangle \cap \mathbb{Z} = \langle 26\rangle$. Hence, the product $(3)(13)$ belongs to the ideal $\langle 3 + \sqrt{-17}\rangle$, but 3 and 13 do not. Thus, the ideal $\langle 3 + \sqrt{-17}\rangle$ is not prime. □

P11.2. Let R be a unique factorization domain.

i. Consider an element f in R such that $f = q_1\,q_2 \cdots q_k$ where each q_i is irreducible in R. For any g in R that divides f, prove that $g = u\,q_{i_1}\,q_{i_2} \cdots q_{i_\ell}$ for some unit u in R and some subset $\{i_1, i_2, \ldots, i_\ell\} \subseteq \{1, 2, \ldots, k\}$.

ii. Consider elements g and h in R. Since R is a unique factorization domain, there exists units v and w in R, irreducible elements $p_1, p_2, \ldots, p_e$ in R, and nonnegative integers $m_1, m_2, \ldots, m_e, n_1, n_2, \ldots, n_e$ such that

$$g = v\,p_1^{m_1}\,p_2^{m_2} \cdots p_e^{m_e} \qquad \text{and} \qquad h = w\,p_1^{n_1}\,p_2^{n_2} \cdots p_e^{n_e}\,.$$

Demonstrate that $\gcd(g, h) = p_1^{\min(m_1,n_1)}\,p_2^{\min(m_2,n_2)} \cdots p_e^{\min(m_e,n_e)}$.

Solution.

i. As g divides f, there exists an element h in R such that $f = gh$. Since R is a unique factorization domain, there exists units v and w in R, irreducible elements $p_1, p_2, \ldots, p_e$ in R, and nonnegative integers $m_1, m_2, \ldots, m_e, n_1, n_2, \ldots, n_e$ such that

$$g = v\, p_1^{m_1}\, p_2^{m_2} \cdots p_e^{m_e} \qquad \text{and} \qquad h = w\, p_1^{n_1}\, p_2^{n_2} \cdots p_e^{n_e}\,.$$

In particular, we have $v\,w\,p_1^{m_1+n_1}\,p_2^{m_2+n_2}\cdots p_e^{m_e+n_e} = gh = f = q_1\,q_2\cdots q_k$. The uniqueness of factorizations shows that, for any index j satisfying $1 \leqslant j \leqslant e$, there exists a unit c_j in R and an index $i_j \in \{1, 2, \ldots, k\}$ such that $p_j = c_j\, q_{i_j}$. Setting $\{i_1, i_2, \ldots, i_\ell\} = \{i_j \mid m_j > 0 \text{ and } 1 \leqslant j \leqslant e\}$ and $u := v\, c_{i_1}\, c_{i_2} \cdots c_{i_\ell}$, it follows that $g = u\, q_{i_1}\, q_{i_2} \cdots q_{i_\ell}$. The product of units is a units so $u \in R^\times$.

ii. Since

$$\begin{aligned} g &= (v\, p_1^{m_1-\min(m_1,n_1)}\, p_2^{m_2-\min(m_2,n_2)} \cdots p_e^{m_e-\min(m_e,n_e)})(p_1^{\min(m_1,n_1)}\, p_2^{\min(m_2,n_2)} \cdots p_e^{\min(m_e,n_e)}) \\ h &= (w\, p_1^{n_1-\min(m_1,n_1)}\, p_2^{n_2-\min(m_2,n_2)} \cdots p_e^{n_e-\min(m_e,n_e)})(p_1^{\min(m_1,n_1)}\, p_2^{\min(m_2,n_2)} \cdots p_e^{\min(m_e,n_e)}) \end{aligned}$$

the element $p_1^{\min(m_1,n_1)}\, p_2^{\min(m_2,n_2)} \cdots p_e^{\min(m_e,n_e)}$ divides both g and h. Suppose that d divides g and h. Applying part **i**, there exists a unit u in R and nonnegative integers $i_1, i_2, \ldots, i_e$ such that $i_j \leqslant \min(m_j, n_j)$ for all $1 \leqslant j \leqslant e$ and $d = u\, p_1^{i_1}\, p_2^{i_2} \cdots p_e^{i_e}$. It follows that

$$\begin{aligned} &p_1^{\min(m_1,n_1)}\, p_2^{\min(m_2,n_2)} \cdots p_e^{\min(m_e,n_e)} \\ &= (u^{-1}\, p_1^{\min(m_1,n_1)-i_1}\, p_2^{\min(m_2,n_2)-i_2} \cdots p_e^{\min(m_e,n_e)-i_e})(u\, p_1^{i_1}\, p_2^{i_2} \cdots p_e^{i_e})\,, \end{aligned}$$

so d divides $p_1^{\min(m_1,n_1)}\, p_2^{\min(m_2,n_2)} \cdots p_e^{\min(m_e,n_e)}$. We conclude that

$$\gcd(g, h) = p_1^{\min(m_1,n_1)}\, p_2^{\min(m_2,n_2)} \cdots p_e^{\min(m_e,n_e)}\,. \qquad \square$$

P11.3. Let K be a field and consider the subring

$$R := \{a_0 + a_1\, x + a_2\, x^2 + \cdots + a_d\, x^d \in K[x] \mid a_1 = 0\}\,.$$

Observe that $R^\times = (K[x])^\times = K^\times$.

i. Verify that every nonzero nonunit in R is a product of irreducible elements.

ii. Confirm that x^2 is irreducible in R but the principal ideal $\langle x^2 \rangle$ is not prime.

Solution.

i. Suppose that there exists at least one nonzero nonunit in R that is not a product of irreducible elements. By the well-ordering of the nonnegative integers, there would exist an element f in R that has minimal degree among all nonzero nonunits in R that are not a product of irreducible elements. The element f would not being irreducible implies that there would exist nonzero nonunits g and h in R such that $f = gh$. If both g and h were products of irreducible elements, then f would also be. Thus, we may assume that the element g is not a product of irreducible elements. The nonzero elements of degree 0 in R are units, so $\deg(h) > 1$. Since

$\deg(f) = \deg(g)+\deg(h)$, we obtain $\deg(g) < \deg(f)$ which contradicts the choice of f. Therefore, every nonzero nonunit in R is a product of irreducible elements.

ii. By definition, the subring R contains no polynomials of degree 1. Since degree of a product is the sum of the degrees of the factors, it follows that product of elements in R equal to x^2 has a factor of degree 0. As any nonzero element of degree 0 is a unit in R, we see that x^2 is an irreducible element.

The polynomial $(x^3)^2 = x^6 = (x^2)^3$ belongs to the principal ideal $\langle x^2 \rangle$ in R. However, the factor x^3 does not belong to $\langle x^2 \rangle$ because the subring R contains no polynomials of degree 1. Therefore, the principal ideal $\langle x^2 \rangle$ is not prime. □