Solutions 04

P4.1. Let K be a field and fix an irreducible polynomial $f \in K[x]$. Consider a nonzero coset $g + \langle f \rangle$ in the quotient ring $L := K[x] \big/ \langle f \rangle$.

i. Show that f and g are relative prime and deduce that there exists $p, q \in K[x]$ such that $pf + qg = 1$.

ii. Show that $q + \langle f \rangle$ is the multiplicative inverse of $g + \langle f \rangle$ in L.

iii. Find a multiplicative inverse for $(1+x)+\langle x^2 + x + 1 \rangle$ in the field $\mathbb{Q}[x]/\langle x^2 + x + 1 \rangle$.

Solution.

i. Since $g + \langle F \rangle \neq 0 + \langle f \rangle$, it follows that $g \notin \langle f \rangle$ or equivalently f does not divide g.

ii. In the field L, part **i** implies that

$$(q + \langle f \rangle)(g + \langle f \rangle) = (qg) + \langle f \rangle = (1 - pf) + \langle f \rangle = 1 + \langle f \rangle \ ,$$

so we conclude that $q + \langle f \rangle$ is the multiplicative inverse of $g + \langle f \rangle$ in L.

iii. Since $(x^2+x+1)-x(x+1) = 1$, we deduce that $x+\langle x^2 + x + 1 \rangle$ is the multiplicative inverse for $(1 + x) + \langle x^2 + x + 1 \rangle$ in the field $\mathbb{Q}[x] \big/ \langle x^2 + x + 1 \rangle$. □

P4.2. Prove that the following are equivalent:

($\mathbb{C}$) Every nonconstact polynomial with coefficients in $\mathbb{C}$ has a root in $\mathbb{C}$.

($\mathbb{R}$) Every nonconstant polynomial with coefficients in $\mathbb{R}$ is a product of linear and quadratics factors with real coefficients.

Solution.

($\mathbb{C}$) ⇒ ($\mathbb{R}$): Let $f \in \mathbb{R}[x]$ have positive degree n. Regarded as a polynomial in $\mathbb{C}[x]$, the Fundamental Theorem of Algebra [which is equivalent to part ($\mathbb{C}$)] implies that f splits completely: there exists $a_0 \in \mathbb{R}$ and $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{C}$ such that

$$f = a_0(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) \,.$$

A real root $r \in \mathbb{R}$ contributes the linear factor $(x - r)$. Since the coefficients of f are real, its nonreal roots occur in conjugate pairs. In particular, if $\alpha_1 = a + \mathrm{i}b$ with $a, b \in \mathbb{R}$ and $b \neq 0$, then $\overline{\alpha_1} = a - \mathrm{i}b$ is also a root. The product of the corresponding linear factors is

$$(x - \alpha_1)(x - \overline{\alpha_1}) = (x - a - \mathrm{i}b)(x - a + \mathrm{i}b) = x^2 - 2ax + (a^2 + b^2)$$

which is a quadratic polynomial with real coefficients. Thus, f can be written as a product of linear factors (from real roots) and real quadratic factors (from conjugate pairs of nonreal roots.

($\mathbb{R}$) ⇒ ($\mathbb{C}$): Let $g \in \mathbb{C}[x]$ be a nonconstant polynomial. By taking real and imaginary parts, there exists unique $u, v \in \mathbb{R}[x]$ such that $g = u + \mathrm{i}\,v$. Consider the real polynomial $h = |g|^2 = g\,\overline{g} = (u + \mathrm{i}\,v)(u - \mathrm{i}\,v) = u^2 + v^2 \in \mathbb{R}[x]$. Since g is nonconstant, h is a nonconstant polynomial in $\mathbb{R}[x]$. By hypothesis, the polynomial h factors in $\mathbb{R}[x]$ as a product of linear and quadratic polynomials. Any real linear factor $(x - r)$ of h implies that $0 = h(r) = |g(r)|^2$, so $g(r) = 0$ and g has a complex root. If h has no linear factors, then it must have a quadratic factor $x^2 + ax + b \in \mathbb{R}[x]$. Over the complex numbers, this quadratic polynomial has roots α and $\overline{\alpha}$. Since

$x^2 + ax + b$ divides h, it follows that $h(\alpha) = 0$, so $|g(\alpha)|^2 = 0$ and $g(\alpha) = 0$. In all cases, g has a root in $\mathbb{C}$. □

P4.3. Let α be a root of the irreducible polynomial $x^3 + 7x + 1 \in \mathbb{Q}[x]$.

i. Find the minimal polynomial for $\alpha + 3$ over $\mathbb{Q}$.
ii. Find the minimal polynomial for $\alpha^2 + 1$ over $\mathbb{Q}$.
iii. Find the minimal polynomial for $\alpha^2 - 2\alpha + 3$ over $\mathbb{Q}$.

Solution.

i. Let $\beta := \alpha + 3$. Since $\alpha = \beta - 3$, it follows that
$$0 = \alpha^3 + 7\alpha + 1 = (\beta - 3)^3 + 7(\beta - 3) + 1 = \beta^3 - 9\beta^2 + 34\beta - 47\,.$$
Set $p_\beta := x^3 - 9x^2 + 34x - 47$. Since 47 is prime, $p_\beta(1) = -21 \neq 0$, $p_\beta(-1) = -91 \neq 0$, $p_\beta(47) = 85483 \neq 0$, and $p_\beta(-47) = -125349 \neq 0$, the polynomial p_β is irreducible over $\mathbb{Q}$. Hence, the minimal polynomial of $\alpha + 3$ over $\mathbb{Q}$ is $x^3 - 9x^2 + 34x - 47$.

ii. Let $\gamma := \alpha^2 + 1$. Since $\alpha^3 = -7\alpha - 1$ and $\alpha^2 = \gamma - 1$, we see that
$$-7\alpha - 1 = \alpha^3 = \alpha(\gamma - 1)$$
so $\alpha(\gamma + 6) + 1 = 0$ or $\alpha = -1/(\gamma + 6)$. Returning to the equation for γ, we obtain
$$0 = \gamma - \left(\frac{-1}{\gamma + 6}\right)^2 - 1$$
$$\Rightarrow \qquad 0 = (\gamma - 1)(\gamma + 6)^2 - 1 = \gamma^3 + 11\gamma^2 + 24\gamma - 37\,.$$
Set $p_\gamma := x^3 + 11x^2 + 24x - 37$. Since 37 is prime, $p_\gamma(1) = -1 \neq 0$, $p_\gamma(-1) = -51 \neq 0$, $p_\gamma(37) = 66563 \neq 0$, and $p_\gamma(-37) = -36519 \neq 0$, the polynomial p_γ is irreducible over $\mathbb{Q}$. Hence, the minimal polynomial of $\alpha^2 + 1$ is $x^3 + 11x^2 + 24x - 37$.

iii. Let $\delta := \alpha^2 - 2\alpha + 3$. Since $\alpha^2 = \delta + 2\alpha - 3$, we see that
$$-7\alpha - 1 = \alpha^3 = \alpha(\delta + 2\alpha - 3) = \alpha\delta + 2(\delta + 2\alpha - 3) - 3\alpha = \alpha\delta + 2\delta + \alpha - 6\,.$$
so $\alpha(\delta + 8) + 2\delta = 5$ or $\alpha = (5 - 2\delta)/(\delta + 8)$. Returning to the equation for δ, we obtain
$$\delta = \left(\frac{5 - 2\delta}{\delta + 8}\right)^2 - 2\left(\frac{5 - 2\delta}{\delta + 8}\right) + 3$$
$$\Rightarrow \qquad 0 = (\delta - 3)(\delta + 8)^2 - (5 - 2\delta)^2 + 2(5 - 2\delta)(\delta + 8) = \delta^3 + 5\delta^2 + 14\delta - 137\,.$$
Set $p_\delta := x^3 + 5x^2 + 14x - 137$. Since 137 is prime,
$$p_\delta(1) = -117 \neq 0\,, \qquad p_\delta(137) = 2666979 \neq 0\,,$$
$$p_\delta(-1) = -147 \neq 0\,, \qquad p_\delta(-137) = -2479563 \neq 0\,.$$
the polynomial p_γ is irreducible over $\mathbb{Q}$. We conclude that the minimal polynomial of $\alpha^2 - 2\alpha + 3$ is $x^3 + 5x^2 + 14x - 137$. □