Solutions 03

P3.1. Let K denote a field of characteristic 2.

i. For all $b \in K$, assume that there exists a field L containing K and an element $\beta \in L$ such that $b = \beta^2$. Prove that β is the unique root of $x^2 + b$. As a consequence, we denote β by $\sqrt{b}$.

ii. Suppose that $f := x^2 + ax + b$ is an irreducible quadratic polynomial in $K[x]$ with $a \neq 0$. Assume that there exists a field L containing K and an element $\alpha \in L$ such that α is a root of f. Prove that α cannot be expressed in the form $u + v\sqrt{w}$ where $u, v, w \in K$.

iii. For all $b \in K$, let $R(b)$ denote a root of $x^2 + x + b$ (possibly lying in some larger field). Prove that the roots of $x^2 + x + b$ are $R(b)$ and $R(b) + 1$ and explain why adding 1 to the second root gives the first.

iv. Prove that the roots of $f = x^2 + ax + b$ with $a \neq 0$ are $aR(b/a^2)$ and $aR(b/a^2) + a$.

Solution. Since the characteristic of the field K equals 2, we have $1 + 1 = 0$ in both K and L. Moreover, for all $x, y \in L$, we also have $x = -x$ and $(x + y)^2 = x^2 + y^2$.

i. Suppose that $\beta' \in L$ satisfies $(\beta')^2 = b$. Since K has characteristic 2, it follows that $(\beta + \beta')^2 = \beta^2 + (\beta')^2 = b^2 + b^2 = 0$. We deduce that $\beta + \beta' = 0$ because K is a domain. Hence, we see that $\beta = \beta'$ and there is a unique root of $x^2 + b$.

ii. Suppose that $f = x^2 + ax + b$ has a root of the form $u + v\sqrt{w}$ where $u, v, w \in K$. Observe that $\sqrt{w} \notin K$ because the f is irreducible over K. In particular, we have $u + v\sqrt{w} = 0$ if and only if $u = 0 = v$. It follows that

$$\begin{aligned} 0 &= \big(u + v\sqrt{w}\big)^2 + a(u + v\sqrt{w}) + b \\ &= u^2 + v^2 w + au + av\sqrt{w} + b = (u^2 + v^2 w + au + b) + av\sqrt{w}\,. \end{aligned}$$

The hypothesis that $a \neq 0$ guarantees that $v = 0$, which implies that $u^2 + au + b = 0$. However, this latest equation contradicts the irreducibility of f. We conclude that no root of f can be expressed in the form $u + v\sqrt{w}$ where $u, v, w \in K$.

iii. When $R(b)$ denotes a root of $x^2 + x + b$, it follows that

$$\begin{aligned} \big(x + R(b)\big)\big(x + R(b) + 1\big) &= x^2 + \big(R(b) + R(b) + 1\big)x + R(b)\big(R(b) + 1\big) \\ &= x^2 + x + \big(R(b)^2 + R(b)\big) = x^2 + x + b\,, \end{aligned}$$

and $\big(R(b) + 1\big) + 1 = R(b) + 2 = R(b)$.

iv. Since $R(b)$ is a root of $x^2 + x + b$, the element $R(b/a^2)$ is a root of $x^2 + x + (b/a^2)$ or equivalently $a^2x^2 + a^2x + b$. Hence, we obtain

$$\begin{aligned} \big(x + aR(b/a^2)\big)\big(x + aR(b/a^2) + a\big) &= x^2 + a\big(2R(b/a^2) + 1\big)x + a^2R(b/a^2)\big(R(b/a^2) + 1\big) \\ &= x^2 + ax + \big(a^2R(b/a^2)^2 + a^2R(b/a^2)\big) = x^2 + ax + b\,. \end{aligned}$$

We conclude that $aR(b/a^2)$ and $aR(b/a^2) + a$ are the roots of $x^2 + ax + b$. □

Remark. When K has characteristic 2, the roots of $x^2 + ax + b \in K[x]$ are

$$x = \begin{cases} \sqrt{b} & a = 0\,, \\ aR(b/a^2), a\big(R(b/a^2) + 1\big) & a \neq 0\,. \end{cases}$$

P3.2. Let the roots of $x^3 + 2x^2 - 3x + 5$ be $\alpha, \beta, \gamma \in \mathbb{C}$. Find univariate polynomials with integer coefficients that have the following roots.

i. $\alpha\beta$, $\alpha\gamma$, and $\beta\gamma$.

ii. $\alpha + 1$, $\beta + 1$, and $\gamma + 1$.

iii. α^2, β^2, and γ^2.

Solution. The coefficients of a monic polynomial are signed elementary symmetric functions in its roots, so we deduce that

$$\alpha + \beta + \gamma = -2\,, \qquad \alpha\beta + \alpha\gamma + \beta\gamma = -3\,, \qquad \alpha\beta\gamma = -5\,.$$

i. Since

$$\begin{aligned}(x - \alpha\beta)(x - \alpha\gamma)(x - \beta\gamma) &= x^3 - (\alpha\beta + \alpha\gamma + \beta\gamma)x^2 + (\alpha^2\beta\gamma + \alpha\beta^2\gamma + \alpha\beta\gamma^2)x - \alpha^2\beta^2\gamma^2 \\ &= x^3 - (-3)x^2 + \alpha\beta\gamma(\alpha + \beta + \gamma)x - (-5)^2 \\ &= x^3 + 3x^2 + (-5)(-2)x - 25 = x^3 + 3x^2 + 10x - 25\,,\end{aligned}$$

the roots of the polynomial $x^3 + 3x^2 + 10x - 25$ are $\alpha\beta$, $\alpha\gamma$, and $\beta\gamma$.

ii. Since

$$\begin{aligned}(x-\alpha-1)(x-\beta-1)(x-\gamma-1) &= x^3 - (\alpha+\beta+\gamma+3)x^2 \\ &\qquad + \big((\alpha+1)(\beta+1) + (\alpha+1)(\gamma+1) + (\beta+1)(\gamma+1)\big)x \\ &\qquad\quad - (\alpha+1)(\beta+1)(\gamma+1) \\ &= x^3 - (-2+3)x^2 \\ &\qquad + \big((\alpha\beta + \alpha\gamma + \beta\gamma) + 2(\alpha + \beta + \gamma) + 3\big)x \\ &\qquad\quad - \big((\alpha\beta\gamma) + (\alpha\beta + \alpha\gamma + \beta\gamma) + (\alpha + \beta + \gamma) + 1\big) \\ &= x^3 - x^2 + \big((-3) + 2(-2) + 3\big)x - \big(-5 + (-3) + (-2) + 1\big) \\ &= x^3 - x^2 - 4x + 9\,,\end{aligned}$$

the roots of the polynomial $x^3 - x^2 - 4x + 9$ are $\alpha + 1$, $\beta + 1$, and $\gamma + 1$.

iii. Since

$$\begin{aligned}(x - \alpha^2)(x - \beta^2)(x - \gamma^2) &= x^3 - (\alpha^2 + \beta^2 + \gamma^2)x^2 + \big(\alpha^2\beta^2 + \alpha^2\gamma^2 + \beta^2\gamma^2\big)x - (\alpha^2\beta^2\gamma^2) \\ &= x^3 - \big((\alpha + \beta + \gamma)^2 - 2(\alpha\beta + \alpha\gamma + \beta\gamma)\big)x^2 \\ &\qquad + \big((\alpha\beta + \alpha\gamma + \beta\gamma)^2 - 2(\alpha + \beta + \gamma)(\alpha\beta\gamma)\big)x \\ &\qquad\quad - \big((\alpha\beta\gamma)^2\big) \\ &= x^3 - \big((-2)^2 - 2(-3)\big)x^2 + \big((-3)^2 - 2(-2)(-5)\big)x - \big((-5)^2\big) \\ &= x^3 - 10x^2 - 11x - 25\,,\end{aligned}$$

the roots of the polynomial $x^3 - 10x^2 - 11x - 25$ are α^2, β^2, and γ^2. □

P3.3. The discriminant in $\mathbb{Z}[x_1, x_2, x_3]$ is $\Delta = (x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2$. By analyzing the exponent vectors in the monomial expansion of Δ, one may assume that there exists $c_1, c_2, \ldots, c_5 \in \mathbb{Z}$ such that

$$\Delta = c_1 e_1^2 e_2^2 + c_2 e_2^3 + c_3 e_1^3 e_3 + c_4 e_1 e_2 e_3 + c_5 e_3^2\,.$$

i. The polynomial $f_1 := x^3 - 1$ has roots $1, \omega, \omega^2$. Show that $\Delta(f_1) = -27$ and deduce that $c_5 = -27$.

ii. Use the polynomial $f_2 := x^3 - x$ to show that $c_2 = -4$.
iii. Use the polynomial $f_3 := x^3 - 2x^2 + x$ to show that $c_1 = 1$.
iv. Use the polynomial $f_4 := x^3 - 2x^2 - x + 2$ to show that $c_4 - 4c_3 = 34$.
v. Use the polynomial $f_5 := x^3 - 3x^2 + 3x - 1$ to show that $c_4 + 3c_3 = 6$ and conclude that $c_4 = 18$ and $c_3 = -4$.

Solution.

i. Since $\omega = \frac{1}{2}(-1 + \mathrm{i}\sqrt{3})$, we have

$$\begin{aligned}\Delta(f_1) &= (1-\omega)^2(1-\omega^2)^2(\omega-\omega^2)^2 \\ &= \frac{1}{4^3}\big(3-\mathrm{i}\sqrt{3}\big)^2\big(3+\mathrm{i}\sqrt{3}\big)^2\big(2\mathrm{i}\sqrt{3}\big)^2 = \frac{1}{4^2}(9+3)^2(-3) = -27\,.\end{aligned}$$

From the coefficients of f_1, we deduce that $\mathrm{ev}_{(1,\omega,\omega^2)}(e_1) = 0$, $\mathrm{ev}_{(1,\omega,\omega^2)}(e_2) = 0$, and $\mathrm{ev}_{(1,\omega,\omega^2)}(e_3) = 1$. It follows that

$$-27 = \Delta(f_1) = c_1(0)^2(0)^2 + c_2(0)^3 + c_3(0)^3(1) + c_4(0)(0)(1) + c_5(1)^2 = c_5\,,$$

so we realize that $c_5 = -27$.

ii. Since the roots of $f_2 = x^3 - x = x(x^2-1) = (x+1)x(x-1)$ are $-1, 0, 1$, we have $\Delta(f_2) = (-1-0)^2(-1-1)^2(0-1)^2 = (-1)^2(-2)^2(-1)^2 = 4$. From the coefficients of f_2, we deduce that $\mathrm{ev}_{(-1,0,1)}(e_1) = 0$, $\mathrm{ev}_{(-1,0,1)}(e_2) = -1$, and $\mathrm{ev}_{(-1,0,1)}(e_3) = 0$. It follows that

$$4 = \Delta(f_2) = c_1(0)^2(-1)^2 + c_2(-1)^3 + c_3(0)^3(0) + c_4(0)(-1)(0) + c_5(0)^2 = -c_2\,,$$

so we find that $c_2 = -4$.

iii. The roots of $f_3 = x^3 - 2x^2 + x = x(x^2 - 2x + 1) = x(x-1)^2$ are $0, 1, 1$, so $\Delta(f_3) = 0$. From the coefficients of f_3, we deduce that $\mathrm{ev}_{(0,1,1)}(e_1) = 2$, $\mathrm{ev}_{(0,1,1)}(e_2) = 1$, and $\mathrm{ev}_{(0,1,1)}(e_3) = 0$. Using part **ii**, it follows that

$$0 = \Delta(f_3) = c_1(2)^2(1)^2 - 4(1)^3 + c_3(2)^3(0) + c_4(2)(1)(0) + c_5(0)^2 = 4c_1 - 4\,,$$

so we discover that $c_1 = 1$.

iv. Since the roots of $f_4 = x^3 - 2x^2 - x + 2 = (x+1)(x-1)(x-2)$ are $-1, 1, 2$, we have $\Delta(f_4) = (-1-1)^2(-1-2)^2(1-2)^2 = 36$. From the coefficients of f_4, we deduce that $\mathrm{ev}_{(-1,1,2)}(e_1) = 2$, $\mathrm{ev}_{(-1,1,2)}(e_2) = -1$, and $\mathrm{ev}_{(-1,1,2)}(e_3) = -2$. Using parts **i–iii**, it follows that

$$36 = \Delta(f_4) = (2)^2(-1)^2 - 4(-1)^3 + c_3(2)^3(-2) + c_4(2)(-1)(-2) - 27(-2)^2 = -16c_3 + 4c_4 - 100\,,$$

so we ascertain that $c_4 - 4c_3 = 34$.

v. The roots of $f_5 = x^3 - 3x^2 + 3x - 1 = (x-1)^3$ are $1, 1, 1$, so we have $\Delta(f_5) = 0$. From the coefficients of f_5, we deduce that $\mathrm{ev}_{(1,1,1)}(e_1) = 3$, $\mathrm{ev}_{(1,1,1)}(e_2) = 3$, and $\mathrm{ev}_{(1,1,1)}(e_3) = 1$. Using parts **i–iii**, it follows that

$$0 = \Delta(f_5) = (3)^2(3)^2 - 4(3)^3 + c_3(3)^3(1) + c_4(3)(3)(1) - 27(1)^2 = 27c_3 + 9c_4 - 54\,,$$

so we determine that $c_4 + 3c_3 = 6$. Combined with the equation from part **iv**, we conclude that $c_3 = -4$ and $c_4 = 18$. □