Solutions 05

P5.1. Let K be a field, and let $f, g \in K[x]$ be monic irreducible polynomials. Prove that, when f and g have a common root in some field extension $K \subseteq L$, we have $f = g$.

Solution. Let $\alpha \in L$ be a common root of f and g, meaning that $f(\alpha) = 0$ and $g(\alpha) = 0$. Since f is monic and irreducible over K, it is the minimal polynomial of α over K. Likewise, g is monic and irreducible over K, it is the minimal polynomial of α over K. We deduce that $f = g$, because the minimal polynomial of an algebraic element over a field is unique. □

P5.2. Find the minimal polynomial of the 24th root of unity $\zeta_{24} := \exp(2\pi \mathrm{i}/24)$ as follows.

i. Factor $x^{24} - 1$ over $\mathbb{Q}$.

ii. Determine which of the factors is the minimal polynomial of ζ_{24}.

Solution.

i. Observe that

$$\begin{aligned} x^{24} - 1 &= (x^{12} - 1)(x^{12} + 1) \\ &= (x^6 - 1)(x^6 + 1)(x^4 + 1)(x^8 - x^4 + 1) \\ &= (x^3 - 1)(x^3 + 1)(x^2 + 1)(x^4 - x^2 + 1)(x^4 + 1)(x^8 - x^4 + 1) \\ &= (x - 1)(x^2 + x + 1)(x + 1)(x^2 - x + 1)(x^2 + 1)(x^4 + 1)(x^4 - x^2 + 1)(x^8 - x^4 + 1) \\ &= (x - 1)(x + 1)(x^2 + 1)(x^2 - x + 1)(x^2 + x + 1)(x^4 + 1)(x^4 - x^2 + 1)(x^8 - x^4 + 1)\,. \end{aligned}$$

We claim that all of these factors are irreducible over $\mathbb{Q}$.

The linear factors $x - 1$ and $x + 1$ are obviously irreducible. By having negative discriminants, the quadratic factors $x^2 + 1$, $x^2 - x + 1$, and $x^2 + x + 1$ are all irreducible over $\mathbb{R}$ and $\mathbb{Q}$. Since $(x + 1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2$, the Eisenstein criterion (for the prime 2) implies that $x^4 + 1$ is irreducible.

By the Gauss Lemma, it suffices to prove that $p := x^4 - x^2 + 1$ is irreducible over $\mathbb{Z}$. The image of p in $\mathbb{F}_2[x]$ is $x^4 + x^2 + 1 = (x^2 + x + 1)^2$. Observe that $x^2 + x + 1$ is irreducible over $\mathbb{F}_2$ because $0^2 + 0 + 1 = 1$ and $1^2 + 1 + 1 = 1$. The image of p in $\mathbb{F}_2[x]$ is the square of an irreducible polynomial, so any quadratic factor must be an associate of $x^2 + x + 1$. Lifting such a factorization back to $\mathbb{Z}[x]$ would force p to be the square of a quadratic polynomial. Comparing coefficients, the equation

$$x^4 - x^2 + 1 = (x^2 + ax + b)^2 = x^4 + 2ax^3 + (a^2 + 2b)x + 2abx + b^2\,,$$

gives $2a = 0$, $a^2 + 2b = -1$, $2ab = 0$, and $b^2 = 1$, so $a = 0$, $b = -\frac{1}{2}$, $\frac{1}{4} = 1$ which is absurd. Thus, we see that p is irreducible over $\mathbb{Q}$.

Again by the Gauss Lemma, it suffices to prove that $q := x^8 - x^4 + 1$ is irreducible over $\mathbb{Z}$. The image of q in $\mathbb{F}_2[x]$ is $x^8 + x^4 + 1 = (x^2 + x + 1)^4$. The image of q in $\mathbb{F}_2[x]$ is the fourth power of an irreducible polynomial, so any quadratic factor mush be an associate of $x^2 + x + 1$. Lifting such a factorization back to $\mathbb{Z}[x]$ would force q to be the fourth power of a quadratic polynomial. Comparing coefficients, the equation

$$\begin{aligned} x^8 - x^4 + 1 &= (x^2 + ax + b)^4 \\ &= x^8 + 4ax^7 + (6a^2 + 4b)x^6 + (4a^3 + 12ab)x^5 + (a^4 + 12a^2b + 6b^2)x^4 \\ &\qquad + (4a^3b + 12ab^2)x^3 + (6a^2b^2 + 4b^3)x^2 + 4ab^3x + b^4 \,, \end{aligned}$$

gives $4a = 0$, $6a^2 + 4b = 0$, and $b^4 = 1$, so $a = 0$, $b = 0$, $0 = 1$ which is absurd. Thus, we see that q is irreducible over $\mathbb{Q}$.

ii. For all positive $n \in \mathbb{N}$, let $\zeta_n := \exp(2\pi \mathrm{i}/n) \in \mathbb{C}$ denote a nth root of unity. Since the positive divisors of 24 are $\{1, 2, 3, 4, 6, 8, 12, 24\}$, the elements $\zeta_1, \zeta_2, \zeta_3, \zeta_4, \zeta_6, \zeta_8$, and ζ_{12} are all roots of $x^{24} - 1$. On the other hand, we have

$$\begin{aligned} x^1 - 1 &= x - 1 \,, \\ x^2 - 1 &= (x - 1)(x + 1) \,, \\ x^3 - 1 &= (x - 1)(x^2 + x + 1) \,, \\ x^4 - 1 &= (x^2 - 1)(x^2 + 1) = (x - 1)(x + 1)(x^2 + 1) \,, \\ x^6 - 1 &= (x^3 - 1)(x^3 + 1) = (x - 1)(x^2 + x + 1)(x + 1)(x^2 - x + 1) \,, \\ x^8 - 1 &= (x^4 - 1)(x^4 + 1) = (x - 1)(x + 1)(x^2 + 1)(x^4 + 1) \,, \\ x^{12} - 1 &= (x^6 - 1)(x^6 + 1) = (x - 1)(x^2 + x + 1)(x + 1)(x^2 - x + 1)(x^2 + 1)(x^4 - x^2 + 1) \,. \end{aligned}$$

By comparing the irreducible factors, we deduce that the minimal polynomial of ζ_2 is $x + 1$, the minimal polynomial of ζ_3 is $x^2 + x + 1$, the minimal polynomial of ζ_4 is $x^2 + 1$, the minimal polynomial of ζ_6 is $x^2 - x + 1$, the minimal polynomial of ζ_8 is $x^4 + 1$, the minimal polynomial of ζ_{12} is $x^4 - x^2 + 1$, and the minimal polynomial of ζ_{24} is $x^8 - x^4 + 1$. □

P5.3. Let K be a field

i. Demonstate that the polynomial $x^m - a \in K[x]$ is reducible whenever the positive integer m has a divisor d such that $d > 1$ and

$$a = \begin{cases} b^d & \text{if } b \in K, \\ -4c^4 & \text{if } d = 4 \text{ and } c \in K. \end{cases}$$

ii. Let $L := K(t)$ be the field of rational functions in t with coefficients in K. Consider $f := x^p - t \in L[x]$ where p is a positive prime integer. Prove that f is irreducible.

Solution.

i. Suppose that $a = b^d$ for some $b \in K$. Since $m \in \mathbb{N}$ is divisible by d, there exists $e \in \mathbb{N}$ such that $m = de$. It follows that

$$\begin{aligned} &(x^e - b)(x^{m-e} + bx^{m-2e} + \cdots + b^j x^{m-(j+1)e} + \cdots + b^{d-1}) \\ &\qquad = x^m + bx^{m-e} + \cdots + b^j x^{m-je} + \cdots + b^{d-1}x^e \\ &\qquad\qquad - bx^{m-e} - \cdots - b^j x^{m-je} - \cdots - b^{d-1}x^e - b^d \\ &\qquad = x^m - a \,. \end{aligned}$$

Thus, the polynomial $x^m - a$ is reducible when $a = b^d$.

Suppose that $a = -4c^4$ for some $c \in K$ and $d = 4$. Since $m \in \mathbb{N}$ is divisible by $d = 4$, there exists $e \in \mathbb{N}$ such that $m = 4e$. It follows that

$$\begin{aligned}
&(x^{2e} - 2cx^e + 2c^2)(x^{2e} + 2cx^e + 2c^2) \\
&\quad = x^{4e} + 2cx^{3e} + 2c^2x^{2e} - 2cx^{3e} - 4c^2x^{2e} - 4c^3x^e + 2c^2x^{2e} + 4c^2x^e + 4c^4 \\
&\quad = x^m - a\,.
\end{aligned}$$

Thus, the polynomial $x^m - a$ is reducible when $d = 4$ and $a = -4c^4$.

ii. By Proposition 3.1.5 in the Notes04, it is enough to show that f has no roots in L. Suppose that the rational function $g/h \in L$, where $g, h \in K[t]$ and $g \neq 0$, a root of the polynomial $f \in L[x]$. We may assume that the fraction g/h is in "lowest terms" meaning that $\gcd(g, h) = 1$. Since g/h is a root, it follows that

$$\left(\frac{g}{h}\right)^p = t \quad \iff \quad g^p = t\,h^p\,.$$

Since the polynomial ring $K[t]$ is a unique factorization domain, the linear polynomial t divides g. The numerator g being divisible by t implies that the product g^p is divisible by t^p. As $p \geqslant 2$, the product h^p is thereby divisible by t^{p-1}, so h is also divisible by t. However, this would imply g and h are not relative prime, which is a contradiction. Therefore, the polynomial f has no roots in L. $\square$