Solutions 06

P6.1. Suppose that the elements α and β are algebraic over the field K having minimal polynomials $f \in K[x]$ and $g \in K[x]$ respectively. Prove that f is irreducible over $K(\beta)$ if and only if g is irreducible over $K(\alpha)$.

Solution. By hypothesis, f is the minimal polynomial of α over K and g is the minimal polynomial of β over K, so $\deg(f) = [K(\alpha) : K]$ and $\deg(g) = [K(\beta) : K]$. Since $K(\alpha, \beta) = \big(K(\beta)\big)(\alpha)$, the polynomial f is irreducible over $K(\beta)$ if and only if it is the minimal polynomial of α over $K(\beta)$, or equivalently, $[K(\alpha,\beta) : K(\beta)] = [K(\alpha) : K]$. Similarly, g is irreducible over $K(\alpha)$ if and only if $[K(\alpha,\beta) : K(\alpha)] = [K(\beta) : K]$. As α and β are algebraic over K, the relevant field extensions are all finite. Hence, the Tower Theorem gives

$$[K(\alpha,\beta) : K] = [K(\alpha,\beta) : K(\alpha)][K(\alpha) : K] = [K(\alpha,\beta) : K(\beta)][K(\beta) : K] .$$

Consequently, we obtain

$$\begin{aligned} [K(\alpha,\beta) : K(\beta)] = [K(\alpha) : K] \quad &\iff \quad [K(\alpha,\beta) : K] = [K(\alpha) : K][K(\beta) : K] , \\ [K(\alpha,\beta) : K(\alpha)] = [K(\beta) : K] \quad &\iff \quad [K(\alpha,\beta) : K] = [K(\alpha) : K][K(\beta) : K] . \end{aligned}$$

Because both irreducibility conditions are equivalent to the same equality of degrees, we conclude that f is irreducible over $K(\beta)$ if and only if g is irreducible over $K(\alpha)$. □

P6.2. **i.** Prove that $\big[\overline{\mathbb{Q}} : \mathbb{Q}\big] = \infty$.

ii. Hermite (1874) establishes that the real number e is transcendental over $\mathbb{Q}$, and Lindermann (1882) shows that the real number π is transcendental over $\mathbb{Q}$. It is unknown whether $\pi + e$ and $\pi - e$ are transcendental. Prove that at least one of these numbers is transcendental over $\mathbb{Q}$.

Solution.

i. For every $n \in \mathbb{Z}$ satisfying $n \geqslant 2$, the Eisenstein criterion (for the prime 2) shows that $x^n - 2$ is irreducible over $\mathbb{Q}$. Setting $\sqrt[n]{2}$ to be the positive real root of the irreducible polynomial $x^n - 2$, it follows that $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$.

Suppose that $\big[\overline{\mathbb{Q}} : \mathbb{Q}\big] = m$ for some $m \in \mathbb{N}$. The Tower Theorem would imply that every intermediate field $\mathbb{Q} \subseteq L \subseteq \overline{\mathbb{Q}}$ would satisfying $[L : \mathbb{Q}] \leqslant m$. However, we have constructed subfields $\mathbb{Q}(\sqrt[n]{2})$ of degree n for all positive integers n, which is a contradiction. Therefore, we have $\big[\overline{\mathbb{Q}} : \mathbb{Q}\big] = \infty$.

ii. Suppose that the real numbers $\pi + e$ and $\pi - e$ are both algebraic over $\mathbb{Q}$. Since the sum of algebraic elements is also algebraic, it would follow that

$$(\pi + e) + (\pi - e) = 2\pi \qquad \text{and} \qquad (\pi + e) - (\pi - e) = 2e$$

are both algebraic over $\mathbb{Q}$. Since the product of algebraic elements is also algebraic and $2 \in \mathbb{Q}$, we would deduce that both π and e are algebraic over $\mathbb{Q}$. However, this contradicts the Hermite (1874) and Lindermann (1882) results. We conclude that at least one of $\pi + e$ and $\pi - e$ is transcendental over $\mathbb{Q}$. □

P6.3. Let $\mathbb{F}_3 := \mathbb{Z}/\langle 3 \rangle$ be the field with three elements and consider $f := x^3 - x + 1 \in \mathbb{F}_3[x]$.

i. Show that f is irreducible over $\mathbb{F}_3$.

ii. Let L be the splitting field of f over $\mathbb{F}_3$. Prove that $[L : \mathbb{F}_3] = 3$.

iii. Explain why L is a field with 27 elements.

Solution.

i. Because $\deg(f) = 3$, the polynomial f is irreducible if and only if it has no roots in $\mathbb{F}_3$. Since

$$f(0) = (0)^3 - (0) + 1 = 1\,, \quad f(1) = (1)^3 - (1) + 1 = 1\,, \quad f(0) = (2)^3 - (2) + 1 = 1\,,$$

we see that the polynomial has not roots in $\mathbb{F}_3$.

ii. Let α be a root of the polynomial $f := x^3 - x + 1 \in \mathbb{F}_3[x]$. Part **i** establishes that f is irreducible, so it is the minimal polynomial of α over $\mathbb{F}_3$. It follows that $[\mathbb{F}_3(\alpha) : \mathbb{F}_3] = 3$. Furthermore, the equation

$$\begin{aligned}(x-\alpha)(x-\alpha+1)(x-\alpha+2) &= \big(x^2 - (2\alpha-1)x + (\alpha^2-\alpha)\big)(x-\alpha+2) \\ &= x^3 - (2\alpha-1)x^2 + (\alpha^2-\alpha)x \\ &\qquad - \alpha x^2 + (2\alpha^2-\alpha)x - (\alpha^3-\alpha^2) \\ &\qquad\qquad + 2x^2 - (\alpha-2)x + (2\alpha^2-2\alpha) \\ &= x^3 - x + (-\alpha^3+\alpha) \\ &= x^3 - x + 1\,,\end{aligned}$$

implies that $L := \mathbb{F}_3(\alpha)$ is a splitting field for f over $\mathbb{F}_3$.

iii. Since the elements $1, \alpha, \alpha^2$ form a $\mathbb{F}_3$-basis for L, every element in the field L can be expressed uniquely in the form $a + b\alpha + c\alpha^2$ for some $a, b, c \in \mathbb{F}_3$. Hence, there are precisely $|\mathbb{F}_3|^3 = 3^3 = 27$ elements in L. □