Problems 07

Due: Friday, 27 February 2026 before 23:59 ET

P7.1. Let K be a field of positive characteristic p, and consider $f := x^p - a \in K[x]$. Assume that f has no roots in K, so the polynomial f is irreducible. Let α be a root of f is some extension of K.

- **i.** Prove that $K(\alpha)$ is the splitting field of f over K and $[K(\alpha) : K] = p$.
- **ii.** Let $\beta \in K(\alpha) \setminus K$. Prove that $\beta^p \in K$.
- **iii.** Prove that the minimal polynomial of β over K is $x^p - \beta^p$.
- **iv.** Prove that no element of $K(\alpha) \setminus K$ is separable over K.

P7.2. Let K be a field of positive characteristic p and let $f \in K[x]$ be irreducible.

- **i.** Assume that the derivative f' is not identically zero. Show that f is separable.
- **ii.** Assume that f' is identically zero. Show that there exists a polynomial $g_1 \in K[x]$ such that $f(x) = g_1(x^p)$.
- **iii.** Show that the polynomial g_1 in part **ii** is irreducible.
- **iv.** Apply parts **i–iii** repeatedly to demonstrate that $f(x) = g(x^{p^e})$ where $e \in \mathbb{N}$ and $g \in K[x]$ is irreducible and separable.

P7.3. Let K be a finite field, and let $K \subseteq L$ be a finite extension. This exercise proves that there exists $\alpha \in L$ such that $L = K(\alpha)$ and α is separable over K.

- **i.** Show that L is a finite field.
- **ii.** The set $L^\times := L \setminus \{0\}$ is a finite group under multiplication. Since group theory (MATH310?) establishes that $L^\times$ is a cyclic group, there exists an element $\alpha \in L^\times$ that generates $L^\times$ as a group. Prove that $L = K(\alpha)$.
- **iii.** Let $m := |L| - 1$. Show that α^j is a root of $x^m - 1 \in K[x]$ for all $0 \leqslant j < m$, and establish that

$$x^m - 1 = (x-1)(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{m-1}) = \prod_{j=0}^{m-1}(x - \alpha^j)\,.$$

- **iv.** Show that α is separable over K.