Solutions 07

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.

Solution.

i. Since f is irreducible of degree p, it is the minimal polynomial of α over K. It follows that $[K(\alpha) : K] = p$. In characteristic p, we have $(x-\alpha)^p = x^p - \alpha^p = x^p - a$. Hence, the polynomial f has a single root α with multiplicity p. In particular, f splits completely over $K(\alpha)$ and no smaller field can contain a root. Therefore, $K(\alpha)$ is the splitting field of f over K.

ii. Since α is algebraic over K, we have $K(\alpha) = K[\alpha]$. Hence, every element $\beta \in K(\alpha)$ can be written uniquely as

$$\beta = c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{p-1}\alpha^{p-1} = \sum_{j=0}^{p-1} c_j \alpha^j \,,$$

where $c_0, c_1, \ldots, c_{p-1} \in K$. In characteristic p, we obtain

$$\beta^p = \left(\sum_{j=0}^{p-1} c_j \alpha^j \right)^p = \sum_{j=0}^{p-1} c_j^p \alpha^{jp} \,.$$

Since $c_j^p \in K$ and $\alpha^p = a \in K$, it follows that

$$\beta^p = \sum_{j=0}^{p-1} c_j^p a^j \in K \,.$$

Thus, every element of $K(\alpha)$ has its pth power in K.

iii. Part **ii** establishes that $\beta^p \in K$, so β is a root of $g := x^p - \beta^p \in K[x]$. As in part **i**, we observe that $x^p - \beta^p = (x - \beta)^p$, so this polynomial has only one root in any field extension. As $\beta \notin K$, its minimal polynomial of β over K has degree greater than 1. Since p is a prime integer and the minimal polynomial of β over K divides g, we deduce that this minimal polynomial must be g.

iv. By part **iii**, the minimal polynomial of $\beta \in K(\alpha) \setminus K$ is $x^p - \beta^p = (x - \beta)^p$. Since this polynomial has a single root β of multiplicity p, the element β is inseparable 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.

Solution.

i. Since f is irreducible in $K[x]$, any nonconstant common divisor of f and f' must be f itself (up to a constant multiple). However, $\deg(f') < \deg(f)$, so f cannot divide f' unless $f' = 0$. Hence, we deduce that $\gcd(f, f') = 1$ and the derivative criteria for separablity establishes that f is separable.

ii. Suppose that

$$f := a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = \sum_{j=0}^{n} a_j x^{n-j}$$

where $n \in \mathbb{N}$ and $a_n, a_{n-1}, \ldots, a_0 \in K$. It follows that

$$f' = n a_0 x^{n-1} + (n-1) a_1 x^{n-2} + \cdots + a_{n-1} = \sum_{j=1}^{n} (n-j) a_j x^{n-j-1} = \sum_{k=1}^{n} k a_{n-k} x^{k-1}.$$

Since the characteristic of K is $p > 0$, the derivative f' is identically zero if and only if $k a_{n-k} = 0$ for all $1 \leqslant k \leqslant n$. This means that $a_{n-k} = 0$ whenever p does not divide k. Hence, all exponents appearing in f are multiples of p, so we obtain

$$f = \sum_{k=0}^{\lfloor n/p \rfloor} a_{n-pk} x^{pk}.$$

Setting $g_1 := \sum_{k=0}^{\lfloor n/p \rfloor} a_{n-pk} x^k$ gives $f(x) = g_1(x^p)$.

iii. Suppose that the polynomial $g_1 \in K[x]$ factors as $g_1 = uv$ for some nonconstant $u, v \in K[x]$. It would follow that $f(x) = g_1(x^p) = u(x^p)v(x^p)$ which would give a nontrivial factorization of f. However, this contradicts the irreducibility of f. Thus, the polynomial $g_1 \in K[x]$ is irreducible.

iv. When the derivative g_1' is not identically zero, part **i** implies that g_1 is separable and we are done. If g_1' is identically zero, then part **ii** produces $g_2 \in K[x]$ such that $g_1(x) = g_2(x^p)$ and part **iii** shows that g_2 is irreducible. Hence, we obtain $f(x) = g_2(x^{p^2})$. Repeating this process, we obtain $f(x) = g_e(x^{p^e})$ for some $e \in \mathbb{N}$ where $g_e \in K[x]$ is irreducible and $g_e' \neq 0$. Again, part **i** implies that g_e is separable. Since the degree strictly decrease at each step, the process terminates after finitely many iterations. □

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.

Solution.

i. Since K is a finite field, let $q := |K|$ be its cardinality. There exists a positive $n \in \mathbb{Z}$ such that $n := [L : K] < \infty$, because L is a finite field extension of K. From the K-vector space structure of L, we deduce that $|L| = q^n$, so L is a finite field.

ii. The multiplicative group $L^\times := L \setminus \{0\}$ is a finite abelian group. A theorem from group theory asserts that the multiplicative group of a finite field is cyclic. Hence, there exists $\alpha \in L^\times$ such that $L^\times = \{1, \alpha, \alpha^2, \ldots, \alpha^{m-1}\}$ for some positive integer m, so every element of L lies in the subfield $K(\alpha)$. We deduce that $L = K(\alpha)$.

iii. Since the cyclic group $L^\times$ has order m, every nonzero element of L satisfies $x^m = 1$, because the order of every element in a group divides the order of the group. In particular, the element α^j is a root of $x^m - 1$ for all $0 \leqslant j < m$. Because the distinct elements $1, \alpha, \alpha^2, \ldots, \alpha^{m-1}$ are exactly the elements of $L^\times$, we obtain the factorization

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

Since $x^m - 1 \in K[x]$, we see that this polynomial splits completely over L.

iv. Part **iii** established

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

where $m := |L| - 1$ and the roots $1, \alpha, \alpha^2, \ldots, \alpha^{m-1}$ are distinct because α generates the cyclic group $L^\times$. Since there are exactly m distinct roots and the polynomial has degree m, it follows that the polynomial $x^m - 1$ has not repeated roots. The minimal polynomial $p \in K[x]$ of α over K divides $x^m - 1$. Since a divisor of a separable polynomial is again separable, the polynomial p has no repeatd roots, so α is separable over K. □