ALGEBRA I HOMEWORK IX

HOJIN LEE 2021-11045

Problem 1. *Let K be a field of characteristic $p > 0$. Let α be algebraic over K. Show that α is separable over K if and only if $K(\alpha) = K(\alpha^{p^n})$ for all positive integers n.*

Proof. Suppose α is separable over K. Consider the tower of extensions $K(\alpha)/K(\alpha^{p^n})/K$. Since subextensions are also separable, $K(\alpha)/K(\alpha^{p^n})$ is also separable. But since $\operatorname{irr}(\alpha, K(\alpha^{p^n}), X)$ divides $X^{p^n} - \alpha^{p^n} = (X-\alpha)^{p^n}$, the only possible way for the extension to be separable is the minimal polynomial being $X - \alpha$, i.e. $\alpha \in K(\alpha^{p^n})$. This implies $K(\alpha) = K(\alpha^{p^n})$, which holds for all $n > 0$ since n was arbitrary.

Conversely, suppose $K(\alpha) = K(\alpha^{p^n})$ for all $n > 0$. Suppose α is not separable. Then $\operatorname{irr}(\alpha, K, x) = g(x^p)$ for some $g \in K[x]$. Hence $g(\alpha^p) = 0$, which implies that $\operatorname{irr}(\alpha^p, K, x) | g(x)$. But then $[K(\alpha) : K] = [K(\alpha^p) : K] = \deg(\operatorname{irr}(\alpha^p, K, x)) \leq \deg g(x) < \deg g(x^p) = [K(\alpha) : K]$, which is a contradiction. $\square$

Problem 2. *Let K be a field of characteristic $p > 0$. Let $a \in K$. If a has no pth root in K, show that $X^{p^n} - a$ is irreducible in $K[X]$ for all positive integer n.*

Proof. We show the contrapositive. Assume that $f(X) := X^{p^n} - a$ is not irreducible in $K[X]$ for some $n > 0$. Denote by $\alpha \in \overline{K}$ a root of X^{p^n} in the algebraic closure. Then $\alpha^{p^n} = a$, so $X^{p^n} - a = X^{p^n} - \alpha^{p^n} = (X - \alpha)^{p^n}$. Let $g(X) = \operatorname{irr}(\alpha, K, X)$. Then $g(X)|f(X)$, so we may write $f(X) = g(X)^m$. Since $m \deg g = p^n$, the degree and m must both be powers of p, and $m > 1$ since we assumed f to be non irreducible. Suppose $\deg g = p^r$ and $m = p^s$. Then $g(X) = X^{p^r} - \alpha^{p^r} = (X - \alpha)^{p^r} \in K[X]$, so we have $\alpha^{p^r} \in K$. Since $\alpha^{p^{n-1}} = \alpha^{p^r p^{s-1}} = (\alpha^{p^r})^{p^{s-1}}$ where $s - 1 \geq 0$, this element is in K, and is a pth root of a. $\square$

Problem 3. *Let K be a field of characteristic $p > 0$. Let L/K be a finite extension such that $p \nmid [L : K]$. Show that L is separable over K.*

Proof. Let $\alpha \in L$. Let $f(X) = \operatorname{irr}(\alpha, K, X)$, and $d := \deg f$. Then we have $d|[L : K]$, so $p \nmid d$. Hence $f' \neq 0$, so α is separable over K. Since α was arbitrary, L/K is separable. $\square$

Problem 4. *Show that every element of a finite field can be written as a sum of two squares in that field.*

Proof. For characteristic $p = 2$, the Frobenius automorphism will do the trick. Suppose $p \neq 2$ and denote the finite field as $\mathbb{F}$. Consider the assignment $\varphi : \mathbb{F}^\times \to \mathbb{F}^\times$ given by $x \mapsto x^2$. This is a 2-1 map, since if $\varphi(a) = \varphi(b)$, this implies either $a = b$ or $a = -b$ (since $p \neq 2$). Hence there exists $|\mathbb{F}^\times|/2$ square elements in $\mathbb{F}^\times$, in other words there exists $(|\mathbb{F}| + 1)/2$ square elements in $\mathbb{F}$ (counting zero). Let $S := \{s^2 \mid s \in \mathbb{F}\}$ and $T_x := \{x - t^2 \mid t \in \mathbb{F}\}$ for some $x \in \mathbb{F}$. Both

Date: May 24, 2024.

$|S| = |T| = (|\mathbb{F}| + 1)/2$, so $|S| + |T| = |\mathbb{F}| + 1$. This means that $S \cap T \neq \varnothing$, i.e. there exists some $a, b \in \mathbb{F}$ such that $x = a^2 + b^2$. Since x was arbitrary, we win. $\square$

Problem 5. *Let F be a finite field with q elements. Let $n \geq 1$ be an integer. Let $f(X) \in F[X]$ be irreducible. Show that $f(X)|(X^{q^n} - X)$ if and only if $\deg f|n$. Prove that $X^{q^n} - X$ is the product of all monic irreducible polynomials in $F[X]$ with degree dividing n. Counting degrees, conclude that*

$$q^n = \sum_{d|n} d\psi(d)$$

where $\psi(d)$ is the number of monic irreducible polynomials of degree d in $F[X]$.

Proof. Suppose that $f(X)|(X^{q^n} - X)$. Let $\alpha \in \overline{F}$ be a root of f. Consider the extension E/F by adjoining roots of $X^{q^n} - X$, which is of degree n since $X^q = X$ in F. Since f divides $X^{q^n} - X$, it follows that $E/F(\alpha)$, so we have $[E : F] = n = [E : F(\alpha)][F(\alpha) : F]$, so $[F(\alpha) : F] = \deg f|n$. Conversely, suppose $\deg f|n$. The extension $F(\alpha)/F$ is a field with $q^{\deg f}$ elements. Hence we have $\alpha^{q^{\deg f}} = \alpha$. This implies $\alpha^{q^n} = \alpha$ since $\deg f|n$, so α is also a root of $X^{q^n} - X$. Hence $f(X)|(X^{q^n} - X)$.

The polynomial $X^{q^n} - X$ has no repeated zero in $\overline{F}$ since its derivative is nonzero. Then the fact that it is a product of all monic irreducible polynomials in $F[X]$ follows directly from the fact we have proved above. Thus, the degree q^n must be equal to the sum of the degrees of all monic irreducible polynomials in $F[X]$, with degree dividing n. In other words, $q^n = \sum_{d|n} d\psi(d)$. $\square$