MATH 7752 Homework 9

James Harbour

April 8, 2022

Problem 1

Let $K/L/F$ be a tower of algebraic extensions. Show that K/F is separable if and only if K/L and L/F are separable.

Proof.
$\underline{\implies}$: Suppose that K/F is separable. Let $\alpha \in K$. As $\mu_{\alpha,L} | \mu_{\alpha,F}$, it follows that $\mu_{\alpha,L}$ is separable so K/L is separable. As $L \subseteq K$ and every element of K is separable over F, it follows that L/F is also separable.

$\underline{\impliedby}$: Assume that K/L and L/F are separable and suppose, for the sake of contradiction, that $\alpha \in K \setminus L$ is inseparable. As $\mu_{\alpha,L} | \mu_{\alpha,F}$, there exists some $p(x) \in L[x]$ and $k \geq 1$ such that $\mu_{\alpha,F}(x) = (\mu_{\alpha,L}(x))^k p(x)$ and $\gcd(\mu_{\alpha,L}, p) = 1$. As $\mu_{\alpha,F}$ is inseparable,

$$0 = \mu'_{\alpha,F} = \mu_{\alpha,L}^{k-1}(k\mu'_{\alpha,L}p + \mu_{\alpha,L}p') \implies -k\mu'_{\alpha,L}p = \mu'_{\alpha,L}p,$$

contradicting that $\gcd(\mu_{\alpha,L}, p) = 1$. □

Problem 2

Let K/F be a finite separable extension. Show that there is a finite number of fields L such that $F \subseteq L \subseteq K$.

Proof. By the primitive element theorem, there exists an $\alpha \in K$ such that $K = F(\alpha)$. Let $n = \deg(\mu_{\alpha,F})$, so $[K : F] \leq n$. Consider a splitting field E of $\mu_{\alpha,F}$.

By induction over the number of roots of $\mu_{\alpha,F}$, it follows that E/F is finite of degree at most $n!$.

Moreover, E/F is Galois and $|\operatorname{Gal}(E/F)| = [E : F] \leq n!$, and intermediate fields L with $F \subseteq L \subseteq E$ correspond precisely to subgroups of $\operatorname{Gal}(E/F)$, of which there are finitely many, so there are *a fortiori* finitely many intermediate fields L with $F \subseteq L \subseteq F(\alpha) \subseteq E$. □

Problem 3

Let F be a field of $\operatorname{char}(F) = p > 0$. Show that F admits a finite inseparable extension K/F if and only if F is not perfect.

Proof.
$\underline{\impliedby}$: Suppose that F is not perfect. Take $\alpha \in F \setminus \varphi(F)$. We claim first that the polynomial $f(x) = x^p - \alpha \in F[x]$ is irreducible. Fix an algebraic closure $\overline{F}$ of F and identify F with its copy inside $\overline{F}$. Let $\beta \in \overline{F}$ be a

root of f. Then $\beta^p = \alpha$, so $x^p - \alpha = x^p - \beta^p = (x-\beta)^p \in \overline{F}[x]$, so if $f = gh$ for some $g, h \in F[x]$ then $g = (x-\beta)^n$ with $n < p$, whence $(x-\beta)^n = x^n - n \cdot \beta x^{n-1} + \cdots \notin F[x]$ as $\beta \notin F$.

Now, consider the field $K = F[x]/(x^p - \alpha)$ and identify F inside K. Then $[K : F] = p$ and $y^p - \alpha \in F[y]$ has a root $\overline{x} \in K$, whence $y^p - \alpha = y^p - \overline{x}^p = (y - \overline{x})^p$ and is thus not separable.

$\underline{\implies}$: We proceed by contraposition. Suppose that F is perfect. Let K/F be a finite extension and suppose that $\alpha \in K$. Let $f(x) = \mu_{\alpha,F} \in F[x]$. By the argument in problem 5 part (a)'s proof, there exists a separable $g(x) \in F[x]$ and $n \geq 0$ such that $f(x) = g(x^{p^n})$. Consider the polynomial $g(x^{p^{n-1}})$. As φ is surjective, each of its coefficients have p^{th} roots, so let $h(x^{p^{n-1}}) \in F[x]$ be the polynomial obtained by replaceing every coefficient in $g(x^{p^{n-1}})$ with its p^{th} root. Then $f(x) = g(x^{p^n}) = h(x^{p^{n-1}})^p$, whence irreduciblity of f implies that $n = 0$, and thus $f = g$ is separable, so K/F is separable. □

Problem 4

Let F be a field of characteristic $p > 0$ and let K/F be an extension.

(a): Let $E = \{\alpha \in K : \alpha^{p^n} \in F, \text{ for some } n \geq 1\}$. Prove that E is a subfield of K.

Proof. It is clear that $0, 1 \in E$. Suppose that $\alpha, \beta \in E$. Then there exist $n, m \in \mathbb{N}$ such that $\alpha^{p^n}, \beta^{p^m} \in F$, whence

$$(\alpha + \beta)^{p^{mn}} = (\alpha^{p^n})^m + (\beta^{p^m})^n \in F$$

so $\alpha + \beta \in E$. Also $(-\alpha)^{p^n} = (-1)^{p^n}\alpha^{p^n}$, so $-\alpha \in E$, and $(\alpha\beta)^{p^{mn}} = (\alpha^{p^n})^m(\beta^{p^m})^n \in F$ so $\alpha\beta \in F$. Lastly, $(\frac{1}{\alpha})^{p^n} = \frac{1}{\alpha^{p^n}} \in F$, so $\frac{1}{\alpha} \in E$. □

(b): Show that every F-automorphism of K is automatically an E-automorphism.

Proof. Let $\sigma \in \mathrm{Aut}(K/F)$. Suppose that $\alpha \in E$, so there is some $n \in \mathbb{N}$ such that $\alpha^{p^n} \in F$. Then

$$\sigma(\alpha)^{p^n} = \sigma(\alpha^{p^n}) = \alpha^{p^n} \implies (\sigma(\alpha) - \alpha)^{p^n} = 0$$

so $\sigma(\alpha) = \alpha$. □

Problem 5

Let F be a field of characteristic $p > 0$ and let K/F be a finite extension.

(a): Let $\alpha \in K$. Show that either $\alpha^{p^n} \in F$ for some $n \geq 1$, or there exists some $m \geq 1$ such that $\alpha^{p^m} \notin F$ and the element α^{p^m} is separable over F.

Proof. Suppose that $\alpha^{p^n} \notin F$ for all $n \in \mathbb{N}$. Consider $f(x) = \mu_{\alpha,F}(x)$. If f is separable, then we are done. Otherwise, $f' = 0$, so there exists some $h \in F[x]$ with $\deg(h) < \deg(f)$ such that $f = h(x^p)$. Continuing in this way until decreasing degree forces us to stop, we find some $g \in F[x]$ and $n \in \mathbb{N}$ such that $f(x) = g(x^{p^n})$ and such that g is separable, so α^{p^n} is separable. □

(b) Suppose that no element of $K \setminus F$ is separable over F. (Such extensions are called *purely inseparable*). Deduce that for every $\alpha \in K$ there exists some $n \geq 1$ (depending on α) such that $\alpha^{p^n} \in F$.

Proof. Let $\alpha \in K \setminus F$ and suppose for the sake of contradiction that $\alpha^{p^n} \notin F$ for all $n \in \mathbb{N}$. Then by part (a), there is some $m \in \mathbb{N}$ such that $\alpha^{p^m} \notin F$ and α^{p^m} is separable over F, contradicting the assumption that K/F is purely inseparable. □

Problem 6

The purpose of this problem is to show that the primitive element theorem is not true for inseparable extensions. Let p be a prime number. Let t be a transcendental element over $\mathbb{F}_p$ and let $F = \mathbb{F}_p(t)$. Let s be a transcendental element over F and let $K = F(s)$. Consider the polynomial $f(x) = (x^p - t)(x^p - s) \in K[x]$ and let L be its splitting field.

(1): Prove that $[L : K] = p^2$.

Proof. Let $\alpha, \beta \in L$ such that $\alpha^p = t$ and $\beta^p = s$. Then $f(x) = (x - \alpha)^p (x - \beta)^p$, so $L = K(\alpha, \beta)$. By the same argument as in problem 3, these polynomials are irreducible, so $\mu_{\alpha,K} = x^p - t$ and $\mu_{\alpha,K} = x^p - s$. We claim that $\beta \notin K(\alpha)$. Suppose, for the sake of contradiction, that there exist $p(x), q(x) \in K[x]$ such that $\beta = \frac{p(\alpha)}{q(\alpha)}$. Moreover, there exist $\tilde{p}, \tilde{q} \in K[x]$ such that $p(x)^p = \tilde{p}(x^p)$ and $q(x)^p = \tilde{q}(x^p)$. Then,

$$\beta^p = \frac{p(\alpha)^p}{q(\alpha)^p} = \frac{\tilde{p}(t)}{\tilde{q}(t)} \implies s \cdot \tilde{q}(t) - \tilde{p}(t) = 0$$

contradicting that s is transcendental over K. Thus $[K(\alpha, \beta) : K(\alpha)] = p$, so $[L : K] = p^2$. □

(2): Show that for every $\gamma \in L$, it follows that $\gamma^p \in K$.

Proof. Let $\gamma \in L = K(\alpha, \beta)$. Then there exist $p(x, y), q(x, y) \in K[x, y]$ such that $\gamma = \frac{p(\alpha,\beta)}{q(\alpha,\beta)}$. Moreover, there are $u(x, y), v(x, y) \in K[x, y]$ such that $p(x, y)^p = u(x^p, y^p)$ and $q(x, y)^p = v(x^p, y^p)$. Then

$$\gamma^p = \frac{p(\alpha, \beta)^p}{q(\alpha, \beta)^p} = \frac{u(t, s)}{v(t, s)} \in K.$$

□

(3): Show that the extension L/K is not simple.

Proof. Suppose, for the sake of contradiction, that L/K is simple. Then there exists some $\gamma \in L$ such that $L = K(\gamma)$. As $\gamma^p \in K$, it follows that $[L : K] \leq p$, contradicting that $[L : K] = p^2$. □