Homework 8

Kevin Guillen

MATH 202 — Algebra III — Spring 2022

> **Problem 14.9.2** Let p be a prime and let $K = \mathbb{F}_p(x, y)$ with x and y independent transcendentals over $\mathbb{F}_p$.
> Let $F = \mathbb{F}_p(x^p - x, y^p - x)$.
>
> (a) Prove that $[K : F] = p^2$ and the separable degree and inseparable degree of K/F are both equal to p.
>
> (b) Prove that there is a subfield E of K containing F which is purely inseparable over F of degree p (so then K is a separable extension of E of degree p). [Let $s = x^p - x \in F$ and $t = y^p - x \in F$ and consider $s - t$.]

(a) *Proof.* Let us recall from exercises in chapter 14.3 and 14.7 that

$$a^p - t - (x^p - x) \in F[a]$$

is an irreducible polynomial with roots $x + i$ for $i \in \mathbb{Z}_p$. We have then that $F(x)$ is a spearable extension of degree p over F. Which then gives us that y is the unique root of $a^p - y^p \in F(x)[a]$ and $F(x, y) = K$ is a purely inseparable extension of $F(x)$ of degree p $\square$

(b) *Proof.* If we use the hint that is given to us, let us consider,

$$(x - y)^p = x^p - y^p = (x^p - x) - (y^p - x) \in F.$$

Using the equivalence relation found on page 649 of the book, we have that $F(x - y)$ is purely inseparable over F. $\square$

Problem 14.9.3 Let p be an odd prime, let s and t be independent transcendentals over $\mathbb{F}_p$, and let F be the field $\mathbb{F}_p(s,t)$. Let β be a root of $x^2 - sx + t = 0$ and let α be a root of $x^p - \beta = 0$ (in some algebraic closure of F). Set $E = F(\beta)$ and $K = F(\alpha)$.

(a) Prove that E is Galois extension of F of degree 2 and that K is purely inseparable extension of E of degree p.

(b) Prove that K is not a normal extension of F. [If it were, conjugate β over F to show that K would contain a p^{th} root of s and then also a p^{th} root of t, so $[K : F] \geqslant p^2$, a contradiction.]

(c) Prove that there is no field K_0 such that $F \subseteq K_0 \subseteq K$ with K_0/F purely inseparable and K/K_0 separable. [If there were such a field, use exercise 1 and the fact that the composite of two normal extension is again normal to show that K would be the normal extension of F.

(a) *Proof.* Using the quadratic formula on the polynomial $p(x) = x^2 - sx + t$ in $F[x]$ we have that it is irreducible. And we know that a quadratic extension is always Galois over fields of characteristic other than 2, we have that $E = F(\beta)$ is a Galois extension.

Because $\alpha^p = \beta$ it is clear that $E < K$, and because $x^p - \beta$ in $E[x]$ is the minimal polynomial of α in E we have that K is an extension of degree p. We have then that an element k of K is of the form,

$$k = \sum_{i=0}^{p-1} e_i \alpha^i$$

and we have characteristic p and $\alpha^p = \beta$, we have that $k^p \in E$ and its minimal polynomial to be $x^p - k^p$, and using the equivalence relation on page 649, K is purely inseparable over E. □

(b) *Proof.* Let us suppose that K is indeed normal over F. We then have a conjugate $\gamma \in K$ of β such that $\beta + \gamma = s$ and $\beta\gamma = t$. We have that $\sqrt[p]{\beta} = \alpha$ and from part (a), since $\gamma \in K$ we have that $\gamma^{p^n} \in E$ for some n, and so there is some $\alpha' = \sqrt[p]{\gamma} \in K$. We have then that

$$s = \beta + \gamma = \alpha^p + (\alpha')^p = (\alpha + \alpha')^p$$

and

$$t = \beta\gamma = (\alpha\alpha')^p$$

which means that

$$[K : F] \leqslant p^2$$

which is a contradiction. Proving that K is not a normal extension of F. □

(c) *Proof.* Let us suppose that there is a field K_0 satisfy the given statements. We know (using exercise 1 statement) that K_0/F is a normal extension. Then by assumption

K/K_0 and by part (a) this extension must have a prime degree, therefore it is a normal extension, which then implies that K/F is a normal extension which contradicts part (b). Thus no field K_0 can exist satisfying the given statement. □

Problem 14.9.5 Let p be a prime , let t be transcendental over $\mathbb{F}_p$ and let K be obtained by adjoining to $\mathbb{F}_p(t)$ all the $p-$power roots of t. Prove that K has transcendence degree 1 over $\mathbb{F}_p$ and has no separating transcendence base.

Proof. We have by definition that K is the splitting field of $x^p - t$ over $\mathbb{F}_p(t)$. So K is algebraic over $\mathbb{F}_p(t)$ and so we have $\{t\}$ to be a transcendentals base of K over $\mathbb{F}_p$, which means it has transcendence degree 1.

Because K is the splitting field of $x^p - t$ over $\mathbb{F}_p(t)$ and the formal derivative of $x^p - t$ is $px^{p-1} = 0$ we have that K is not separable over $\mathbb{F}_P(t)$. Therefore K has no separating transcendence base over $\mathbb{F}_p$. □

Problem 14.9.6 Show that if t is transcendental over $\mathbb{Q}$ then $\mathbb{Q}(t, \sqrt{t^3 - t})$ is not a purely transcendental extension of $\mathbb{Q}$. (This is an example of what is called an elliptic function field.)

Proof. Note that $\mathbb{Q}(t, \sqrt{t^3 - t})$ has transcendence degree 1, therefore if $\mathbb{Q}(t, \sqrt{t^3 - t})$ was purely transcendental it would be isomorphic to $\mathbb{Q}(x)$. Then there would be non-constant rational functions $f(x), g(x) \in \mathbb{Q}(x)$ such that

$$g(x)^2 = f(x)^2 - f(x).$$

If we derive both sides we obtain,

$$\varphi(x) = \frac{g'(x)}{3f(x)^2 - 1} = \frac{f'(x)}{2g(x)}$$

which must be a polynomial. Because if not the denominators would have factor $x - a$ and so,

$$2g(a) = 3f(a)^2 - 1 = 0$$

and

$$g(a)^2 = f(a)^3 - f(a)$$

which is impossible.

Since both $f(x)$ and $g(x)$ are nonzero we have that φ is a non-zero polynomial. Now, replacing $f(x)$ and $g(x)$ by $f(\frac{1}{x})$ and $f(\frac{1}{x})$ we would get that $\frac{\varphi(1/x)}{x}$ is again a polynomial, which it obviously is not. Therefore we obtain a contradiction, and $\mathbb{Q}(t, \sqrt{t^3 - t})$ is not purely transcendental. □

Problem 14.9.7 Let k be a field with 4 elements, t is a transcendental over k, $F = k(t^4 + t)$ and $K = k(t)$.

(a) Show that $[K : F] = 4$.

(b) Show that K is separable over F.

(c) Show that K is Galois over F.

(d) Describe the lattice of subgroups of the Galois group and the corresponding lattice of subfields of K, giving each subfield in the form $k(r)$, for some rational function r.

(a) *Proof.* Because t is a zero of the irreducible polynomial,

$$x^4 + x + (t^4 + t) \in F[x]$$

we have that,

$$[K : F] = 4.$$

$\square$

(b) *Proof.* Since K is generated by t over F. The minimal polynomial of t is,

$$x^4 + x + (t^4 + t) = (x + t)(x + t + 1)(x + t + \zeta)(x + t + \zeta + 1)$$

which means t is separable over F. We conclude K is separable extension of F. $\square$

(c) *Proof.* We know K is separable algebraic extension of F, so we need to verify it is normal. This follows from the fact that K is the splitting field of

$$x^4 + x + (t^4 + t) = (x + t)(x + t + 1)(x + t + \zeta)(x + t + \zeta + 1).$$

$\square$

(d) We have,

$$Gal(K/F) \cong Z_2 \oplus Z_2$$

with one generator permuting the pairs of roots $(t, t + 1)$ and $(t + \zeta, t + \zeta + 1)$ and the other generator permuting the pairs $(t, t + \zeta)$ and $(t + 1, t + \zeta + 1)$. This group as 3 subgroups and the associated fixed fields are $k(t^2 + t), k(t^2 + \zeta t)$, and $k(t^2 + \zeta t + t)$.

Problem 14.9.10 Prove that a purely transcendental proper extension of a field is never algebraically closed.

Proof. Let E/F be a purely transcendental extension with $E = F(X)$ for some non-empty transcendental base $X = \{t_1, \ldots, t_m\}$. Consider a root of α of the polynomial $x^2 - t_1$. We have that $\alpha \notin F(t_1)$ so if E is algebraically closed then $\alpha \in E$ and so there are $a_{n_1,\ldots,n_m}$ such that,

$$\left(\sum_{(n_1,\ldots,n_m)\in\mathbb{Z}^m} a_{n_1,\ldots,n_m} t_1^{n_1} \ldots t_m^{n_m} \right)^2 = t_1$$

which goes against the independence of the elements in X, therefore E is not algebraically closed. □

Problem 14.9.12 Let K be a subfield of $\mathbb{C}$ maximal with respect to the property "$\sqrt{2} \notin K$"

(a) Show such a field K exists.

(b) Show that $\mathbb{C}$ is algebraic over K

(c) Prove that every finite extension of K in $\mathbb{C}$ is Galois with Galois group a cyclic 2−group.

(d) Deduce that $[\mathbb{C} : K]$ is countable (and not finite).

(a) *Proof.* Now consider the partially ordered set,

$$A = \left\{ L < \mathbb{C} \mid \sqrt{2} \notin L \right\}$$

This set is a non-empty since $\mathbb{Q} \in A$. Every chain of elements in A is bound from above by the union of subfields of the chain, so by Zorn's Lemma, A contained a maximal element K. □

(b) *Proof.* Suppose that $\alpha \in \mathbb{C}$ is transcendental over K, then $\sqrt{2} \notin K(\alpha)$ since if $f(\alpha) \in K(\alpha)$ is such that $f(\alpha)^2 = 2$ then α is algebraic over K, a contradiction. □

(c) *Proof.* Let L be non-trivial finite extension of K. By maximality $\sqrt{2} \in L$. There is some $\sigma \in Gal(L/K)$ that doesn't fix $\sqrt{2}$, so by maximality of K the fixed field of $< \sigma >$ must be K, and so by Galois correspondence $Gal(L/K)$ is cyclic and generated by σ. Again by the maximality of K there is no odd extension of K, so the order of $Gal(L/K)$ must be 2^n for some $n \in \mathbb{N}$. Since every subgroup of a cyclic group is normal L is a Galois extension. □

(d) *Proof.* If $[\mathbb{C} : K]$ was finite by the (c) $[\mathbb{C} : K] = 2^n$. Note though that $\sqrt[n+1]{2} \in \mathbb{C}$ and

$$min(\sqrt[n+1]{2}, K) = x^{n+1} - 2$$

has degree $n + 1$, a contradiction. Therefore $[\mathbb{C} : K]$ is infinite. □

Problem 14.9.13 Let K be a fixed field in $\mathbb{C}$ of an automorphism of $\mathbb{C}$. Prove that every finite extension of K in $\mathbb{C}$ is cyclic.

Proof. Let K be a field of some automorphism σ of $\mathbb{C}$, and let $L < \mathbb{C}$ be some finite some extension of K. Now notice that L/K is separable since

$$\text{char } K = \text{char } \mathbb{C} = 0$$

We then have that the normal closure $\overline{L}$ of L/K is a finite Galois extension. THen σ restricts to a $\overline{\sigma} \in \mathrm{Gal}(\overline{L}/K)$. The fixed field of $\overline{\sigma}$ is K, so by the Galois correspondence,

$$< \overline{\sigma} = \mathrm{Gal}(\overline{L}/K) >$$

is a cyclic group. Since L is an intermediary subfield

$$K < L < \overline{L}$$

by the Galois correspondence we have that $\mathrm{Gal}(L/K)$ is cyclic. $\square$