# Homework 10

Aleck Zhao

April 24, 2017

1. Let $E/F$ be a finite field extension, and let $L/F$ be any field extension. Mimic the proof of § 10.2 Theorem 1 to show that
$$\#\{F\text{-embeddings } E \to L\} \leq [E : F].$$

## Section 10.1: Galois Groups and Separability

30. Le $E \supseteq F$ be a finite extension, where $\operatorname{char} F = p$.

(a) If $u \in E$ has a separable minimal polynomial $q$ over $F$, show that $u \in F(u^p)$. [Hint: If $m$ is the minimal polynomial of $u$ over $F(u^p)$, show $m \mid q$ and $m \mid (x-u)^p$.]

*Proof.* Let $m$ be the minimal polynomial of $u$ over $F(u^p)$. Then since $q \in F(u^p)[x]$ and $q(u) = 0$, we must have $m \mid q$ since it is the minimal polynomial. Since $q$ is separable, it must have distinct roots in $F(u^p)$, and since $m \mid q$, it too must have distinct roots.

Suppose $f = x^p - u^p \in F(u^p)[x]$, but since $\operatorname{char} F = p$, this is $(x-u)^p$. Since $f(u) = 0$, we must have $m \mid (x-u)^p$. But since $m$ must have distinct roots, we must have $m = x - u$, so since $m \in F(u^p)[x]$, we have $u \in F(u^p)$, as desired. □

(b) Define $F(E^p) = \{\, a_1u_1^p + \cdots + a_nu_n^p \mid a_i \in F, u_i \in E, n \geq 1 \,\}$. Show that $F(E^p)$ is a subfield of $E$.

*Proof.* Clearly $1_E \in F(E^p)$. Then if

$$\begin{gathered} a_1u_1^p + \cdots + a_nu_n^p \in F(E^p) \\ b_1v_1^p + \cdots + b_mv_m^p \in F(E^p) \end{gathered}$$

where WLOG $n \leq m$ and $a_i, b_j \in F$ and $u_i, v_j \in E$ for all $i, j$, then

$$\begin{aligned} &(a_1u_1^p + \cdots + a_nu_n^p) - (b_1v_1^p + \cdots + b_mv_m^p) \\ &= (a_1u_1^p - b_1v_1^p) + \cdots + (a_nu_n^p - b_nv_n^p) + b_{n+1}v_{n+1}^p + \cdots + b_mv_m^p \\ &= [a_1u_1^p - a_1v_1^p - (b_1 - a_1)v_1^p] + \cdots + [a_nu_n^p - a_nv_n^p - (b_n - a_n)v_n^p] + \sum_{k=n+1}^m b_kv_k^p \\ &= a_1(u_1^p - v_1^p) + \cdots + a_n(u_n^p - v_n^p) + \sum_{j=1}^n (b_j - a_j)v_j^p + \sum_{k=n+1}^m b_kv_k^p \\ &= \sum_{i=1}^n a_i(u_i - v_i)^p + \sum_{j=1}^n (b_j - a_j)v_j^p + \sum_{k=n+1}^m b_kv_k^p \\ &\in F(E^p) \end{aligned}$$

□

(c) If $E = F(E^p)$ and $\{w_1, \cdots, w_k\} \subseteq E$ is $F$-independent, show that $\{w_1^p, \cdots, w_k^p\}$ is $F$-independent. [Hint: Extend to a basis $\{w_1, \cdots, w_k, \cdots, w_n\}$ of $E$, show that $\{w_1^p, \cdots, w_k^p, \cdots, w_n^p\}$ span $E$, and apply Theorem 7 §6.1.]

*Proof.* Extend $\{w_1, \cdots w_k\}$ to an $F$-basis $\{w_1, \cdots, w_k, \cdots, w_n\}$ of $E$. Now if $v \in E = F(E^p)$, then suppose

$$v = \sum_{i=1}^{m} a_i u_i^p$$

where $a_i \in F$ and $u_i \in E$ for all $i$. Then since $\{w_1, \cdots, w_k, \cdots, w_n\}$ is a basis, there is a unique representation for $u_i$ in terms of these basis elements:

$$v = \sum_{i=1}^{m} a_i u_i^p = \sum_{i=1}^{m} a_i \left( \sum_{j=1}^{n} b_{ij} w_j \right)^p = \sum_{i=1}^{m} \sum_{j=1}^{n} a_i b_{ij}^p w_j^p$$

Thus, the set $\{w_1^p, \cdots, w_k^p, \cdots, w_n^p\}$ spans $E$. Since $\{w_1, \cdots, w_k, \cdots, w_n\}$ was a basis, $\dim E = n$ so $\{w_1^p, \cdots, w_k^p, \cdots, w_n^p\}$ is $F$-independent. □

31. Let $E \supseteq K \supseteq F$ be fields with $[E : F]$ finite. Show that $E \supseteq F$ is separable if and only if both $E \supseteq K$ and $K \supseteq F$ are separable.

32. If $E \supseteq F$ is a finite extension, then $u \in E$ is called a separable element over $F$ if its minimal polynomial in $F[x]$ is separable.

    (a) If $u \in E$ is separable over $F$ and $E \supseteq K \supseteq F$, where $K$ is a field, show that $u$ is separable over $K$. [Hint: Exercise 30(d)]

    *Proof.* If $p \in F[x]$ and $q \in K[x]$ are the minimal polynomials of $u$ over $F$ and $K$, respectively, then since $p \in K[x]$, we must have $q \mid p$. Since $u$ is separable over $F$, that means $p$ is separable so it has distinct roots, and thus $q$ must also have distinct roots, so it is separable. Thus $u$ is separable over $K$. □

    (b) Show that $u \in E$ is separable over $F$ if and only if $F(u) \supseteq F$ is a separable extension.

    (c) Define $S = \{ u \in E \mid u \text{ is separable over } F \}$. Show that $S$ is a subfield of $E$, that $S \supseteq F$ is separable, and that $E \supseteq K \supseteq F$, with $K \supseteq F$ separable, implies that $S \supseteq K$. [Hint: If $u, v \in S$, show that $F(u, v) \supseteq F$ is separable by (a) and Exercise 31.]

    *Proof.* Subfield: Clearly $1_E \in S$ since $1_E \in F$ and $x - 1$ is separable. If $u \in E$, then from (b), we have $F(u) \supseteq F$ is separable. Then if $v \in E$, since $F(u, v) = F(u)(v)$ is separable over $F(u)$, it follows that $F(u, v) \supseteq F$ is separable from Exercise 31. Thus, since $u + v$ and $uv$ are in $F(u, v)$, they are both separable, and thus in $S$. Similarly, $u^{-1} \in F(u, v)$ so $u^{-1}$ is also separable, so $S$ is a subfield, as desired.

    $S \supseteq F$ is separable by its definition, since everything inside is separable over $F$. If $E \supseteq K \supseteq F$ and $K \supseteq F$ is separable, then if $u \in K$ is separable over $F$, since $E \supseteq K$, that means $u \in S$, so $S \supseteq K$. □

## Section 10.2: The Main Theorem of Galois Theory

5. Let $E = F(t)$ be the field of rational forms over a field. In each case, compute $K = E_G$ and find the minimal polynomial $m \in K[x]$ of $t$ over $K$.

    (a) $G = \langle \sigma \rangle$ , where $\sigma$ is that $F$-automorphism of $E$ given by $\sigma(t) = -t$.

    *Solution.* We have $\sigma^2(t) = t$, so it suffices to consider $\sigma$. Let $K \ni f = \frac{p(t)}{q(t)}$ for $p, q \in F[t]$. Then

$$\sigma(f) = f \iff \sigma\left(\frac{p(t)}{q(t)}\right) = \frac{p(-t)}{q(-t)} = \frac{p(t)}{q(t)} \iff p(t)q(-t) = p(-t)q(t)$$

If $\operatorname{char} F = 2$, then $K = E$ because $a = -a \implies at^n = -at^n$ for all $a \in F$. Then the minimal polynomial is $x - t$.

Otherwise, let $g(t) = p(t)q(-t)$, so $g(-t) = p(-t)q(t) = p(t)q(-t) = g(t)$, so $g(t) = h(t^2)$ for some $h \in F[t]$. Now, $f = \frac{p(t)}{q(t)} = \frac{h(t^2)}{q(t)q(-t)}$ and similarly, $q(t)q(-t) = k(t^2)$ for some $k \in F[t]$, so $f = \frac{h(t^2)}{k(t^2)}$, so $K = F(t^2)$. Then the minimal polynomial is $x^2 - t^2$. □

(b) $G = \langle \sigma \rangle$, where $\sigma$ is that $F$-automorphism of $E$ given by $\sigma(t) = 1 - t$.

*Solution.* We have $\sigma^2(t) = t$, so it suffices to consider $\sigma$. Let $K \ni f = \frac{p(t)}{q(t)}$ for $p, q \in F[t]$. Let

$$p(t) = \sum_{i=0}^{m} a_i t^i \implies p(1-t) = \sum_{i=0}^{m} a_i (1-t)^i$$
$$q(t) = \sum_{j=0}^{n} b_j t^j \implies q(1-t) = \sum_{j=0}^{n} b_j (1-t)^j$$

□

10. Let $E \supseteq F$ be fields with $G = \operatorname{Gal}(E/F)$. If $H \subseteq G$ is a subgroup and $H^\circ$ is finite, show that $H$ is closed.

11. If $E \supseteq K \supseteq F$ are fields, show that $E \supseteq K$ is Galois if and only if $K$ is closed as an intermediate field of $E \supseteq F$.