Math 210B Lecture 7 Notes

Daniel Raban

January 23, 2019

1 Inseparability and Perfect Fields

1.1 Towers of separable extensions

Proposition 1.1. *Let E/F be finite, and let $\mathrm{Emb}_F(E)$ be the set of embeddings $\Phi : E \to \overline{F}$ fixing F. Then $|\mathrm{Emb}_F(E)|$ divides $[E : F]$, with equality iff E/F is separable.*

Proof. Let $e = |\mathrm{Emb}_F(E)|$ and $E = F(\alpha_1, \ldots, \alpha_n)$. Let $E_i = F(\alpha_1, \ldots, \alpha_{i=1}$, and let e_i be the number of embeddings in $\mathrm{Emb}_F(E_{i+1})$ extending an embedding in $\mathrm{Emb}_F(E_i)$. We know that $e_i \mid [E_{i+1} : E_i]$ and we get equality iff E_{i+1}/E_i is separable. This is because this is the number of distinct conjugates of α_i over E_i times the multiplicity (number of conjugates times multiplicity is the degree of the polynomial). Now $e = \prod_{i=1}^n e_i$, so E/F is separable.

If $e = [E : F]$, take $\beta \in E$. The number of conjugates of $\beta \in \overline{F}$ is $d = |\mathrm{Emb}_F(F(\beta))|$, which divides $[F(\beta) : F]$. The number of extensions of any such embedding to $E \to \overline{F}$ divides $c = [E : F(\beta)]$. Now $cd = e = [E : F]$, so $d = [F(\beta) : F]$, since d divides it and $c \mid [E : F(\beta)]$. Then $F(\beta)/F$ is separable. $\square$

Proposition 1.2. *If $K/E/F$ are salgebraic, and K/E and K/F is separable, then K/F is separable.*

Proof. In the case of finite degree, this follows from the previous proposition. In general, any $\alpha \in K$ has minimal polynomial over E which has coefficients in a finite extension E'/F. So $E'(\alpha)/E'/F$ is finite, $E'(\alpha)/E'$ and E'/F are separable. So, by the finite case, α is separable over F. This is true for all $\alpha \in K$, so K/F is separable. $\square$

1.2 Purely inseparable extensions and degrees of separability and inseparability

Definition 1.1. An extension E/F is **purely inseparable** if every $\alpha \in E \setminus F$ is inseparable. Equivalently, E/F is separable it has no nontrivial intermediate separable extensions over F.

Example 1.1. $\mathbb{F}_p(x)/\mathbb{F}_p(x^p)$ is purely inseparable because it has degree p and because the minimal polynomial of x is $t^p - x^p = (t-x)^p$.

Corollary 1.1. *The set of all separable elements in an extension K/F (call it E) is a field, and K/E is purely inseparable.*

Definition 1.2. Suppose K/F is finite, and E is a maximal separable subextension. Then the **degree of separability** of K/F is $[K:F]_s = [E:F]$. The **degree of inseparability** if $[K:F]_i = [K:S]$.

Lemma 1.1. *Let E/F is algebraic, $f \in E[x]$ be monic, and $m \geq 1$ such that $f^m \in F[x]$. Then either $m = 0$ in F or $f \in F[x]$.*

Proof. Let $f = \sum_{i=0}^n a_i x^i$ be monic, and suppose that $f \notin F[x]$. Let $i \leq n-1$ be maximal such that $a_i \notin F$. Let c be the coefficient of $x^{(m-1)n+i}$ in f^m. This is not in F, since c is a sum of terms all in F (involving only a_j with $j > i$ and 1 term coming from $a_i a_n^{m-1} = a_i$). So $c - ma_i \in F$, which means $a_i \in F$ or $m = 0$ in F. But $a_i \notin F$. $\square$

Proposition 1.3. *Let* $\operatorname{char}(F) = p$. *If E/F is purely inseparable and $\alpha \in E$, then there exists a minimal $k \geq 0$ such that $\alpha^{p^k} \in F$, and the minimal polynomial of α is $x^{p^k} - \alpha^{p^k}$.*

Proof. Let $\alpha \in E \setminus F$ have minimal polynomial $f = \prod_{i=1}^d (x-\alpha_i)^m \in \overline{F}[x]$. Of $m > 1$, then $f = g^m$ where $g = \prod_{i=1}^d (x-\alpha_i)$. Then $m = p^k t$, where $p \nmid t$,and $k \geq 1$ by the lemma. Then $f = (g^{p^k})^t \in F[x]$. So the lemma forces $t = 1$ since $p \nmid t$. Letting $a_i = \alpha_i^{p^k}$, we get $f = \prod_{i=1}^d (x^{p^k} - a_i)$. Then $f = h(x^{p^k})$, where $h = \prod_{i=1}^d (x - a_i) \in F[x]$. This is a separable polynomial, so $F(a_i)/F$ is separable for each i. Since E/F is purely inseparable, each $a_i \in F$. Since F is irreducible, we get $d = 1$. So $f = x^{p^k} - \alpha_i^{p^k}$. $\square$

Corollary 1.2. *If E/F is finite and* $\operatorname{char}(F) = p$, *then $[E/F]_i$ is a power of p.*

Proposition 1.4. $[K:F]_s = |\operatorname{Emb}_F(K)|$.

Corollary 1.3. *Degrees of separability and inseparability are multiplicative in extensions.*

1.3 Perfect fields

Definition 1.3. A field is **perfect** if every algebraic extension of it is separable.

Example 1.2. $\mathbb{F}_p$ is perfect. Finite extensions are $\mathbb{F}_{p^n}$, which is generated by the roots of $x^{p^n} - x$, which has p^n distinct roots. So these extensions are separable.

Theorem 1.1. *Every field of characteristic 0 is perfect.*

Proof. Let $\operatorname{char}(F) = 0$. Then every irreducible monic polynomial is $f = \prod_{i=1}^d (x-\alpha_i)^m \in \overline{F}[x]$. Then $f = g^m$, where $g \in \overline{F}[x]$. So $g \in F[x]$ by the lemma. Since f is irreducible, $m = 1$. $\square$

1.4 The primitive element theorem

Definition 1.4. An extension E/F is **simple** if $E = F(\alpha)$ with $\alpha \in E$. Here, α is called a **primitive element** for E/F.

Theorem 1.2 (primitive element theorem)**.** *Every finite separable extension is simple.*

Proof. If $F = \mathbb{F}_q$, then $\mathbb{F}_{q^n}$, where $\mathbb{F}_q(\xi)$, where ξ is the primitive $(q^n - 1)$-th root of 1. Now we may assume that F is an infinite field. It suffices to show that any $F(\alpha, \beta)/F$ (with α, β algebraic) is simple. Look at $\gamma := \alpha + c\beta$ for $c \in F \setminus \{0\}$. Since F is infinite, we can choose $c \neq (\alpha' - \alpha)/(\beta' - \beta)$, where α' is a conjugate of α and same for β. Then $\gamma \neq \alpha' + c\beta'$ for all such α', β'. Let f be the minimal polynomial of α, and let $h(x) = f(\gamma - cx) \in F(\gamma)[x]$. Now $h(\beta) = f(\alpha) = 0$. Then h does not have any other β' as a root. We will finish this next time. $\square$