MA 553 Notes on Separability

Notations • $K \subset L$ an algebraic field extension, char. $p>0$. $L^p = \{x^p \mid x \in L\}$.

Remark (after 1st Prop) If E, F are fields between K and L, then $EF := \{\sum_{i=1}^{n} e_i f_i \mid e_i \in E, f_i \in F, n \geq 0\}$ is a subfield of L. Indeed, if $x \in E(F)$, then $x \in E(F_0)$ for some F_0 such that $[F_0 : K] < \infty$ (why?), so $x \in E(F_0) = E[F_0] \subset EF$. Hence $E(F) = EF$

Definition. A positive-degree irreducible polynomial $f \in K[X]$ is separable if it factors into distinct linear factors over its splitting field.

• $a \in L$ is separable over K if its minimum polyn $Irr(a, K)$ is separable

• L/K is separable if every $a \in L$ is separable.

Example (i) Char 0. (ii) char p: an irred f is inseparable $\Leftrightarrow f = g(X^p)$. PERFECT FIELDS.

Proposition a separable over $K \Leftrightarrow K(a) = K(a^p)$.

Proof; Suppose a separable, $f = Irr(a, K(a^p))$. Since a is root of $X^p - a^p$, $\therefore f \mid X^p - a^p$ (over $K(a^p)$), $\therefore f \mid (X-a)^p$ over L, and so $f = (X-a)^e$ for some e. But f separable $\Rightarrow e = 1 \Rightarrow a \in K(a^p)$.

Conversely if a not separable, say $Irr(a, K) = X^{np} + a_1 X^{p(n-1)} + a_2 X^{p(n-2)} + \cdots$, then a^p is a root of $X^n + a_1 X^{n-1} + a_2 X^{n-2} + \cdots$, $\Rightarrow [K(a):K] = np$, $(K(a^p):K] \leq n \Rightarrow K(a) \neq K(a^p)$.

Remark Since $[K(a):K] = [K(a):K(a^p)][K(a^p):K] \leq p[K(a^p):K]$ we see that if $a \notin K(a^p)$ then $[K(a):K(a^p)] = p$, and $Irr(a, K(a^p)) = X^p - a^p$. Thus:

(because $[K(a^p):K] \leq n$)

Corollary. If $b \notin K^p$, then $X^p - b$ is irreducible in $K[X]$. (Pf Adjoin a root a of $X^p - b$ to K, and apply Remark)

Proposition L/K separable $\Rightarrow L = KL^p$. Converse holds if $[L:K] < \infty$.

Proof L/K separable, $a \in L \Rightarrow a \in K(a^p) \subset KL^p$. Conversely, if $[L:K] < \infty$ and $L = KL^p$, then $[L : K(a)] \underset{①}{=} [L^p : K^p(a^p)] \underset{②}{\geq} [KL^p : K(a^p)] = [L : K(a)][K(a) : K(a^p)] \Rightarrow K(a) = K(a^p)$.

① holds via the isomorphism $x \mapsto x^p$ of L onto L^p (check!)

②: If E, F as above and (ξ_i) is a basis of F/K, then clearly every element of EF is a linear comb'n of the ξ_i with coeff in E; hence $[EF : E] \leq [F : k]$.

Corollary a separable over $K \Rightarrow K(a) = K(a^p) \Rightarrow K(a)$ separable over K.

Corollary $K \subset E \subset L$, E/K sep, L/E sep. $\Rightarrow L/K$ sep.

Pf Let $a \in L$, set $Irr(a, E) = X^n + a_1 X^{n-1} + a_2 X^{n-2} + \cdots$, $E_0 = K(a_1, a_2, \ldots a_n)$, $L_0 = E_0(a)$.

Then E_0/K sep, L_0/E_0 sep, $[L_0 : K] < \infty$ and $L_0 = L_0^p E_0 = L_0^p E_0^p K = L_0^p K \Rightarrow a$ sep over K.

Corollary If $b_1, \cdots b_n \in L$ are sep over K, then $K(b_1, \cdots b_n)/K$ is sep. (Pf. Induction on n)

Corollary K perfect (i.e. $K = K^p$), L/K algebraic $\Rightarrow L$ perfect. (Pf L/K sep $\Rightarrow L = L^p K = L^p K^p = L^p$)

first show L/K separable.

Primitive Element Theorem (any characteristic).

Let $L = K(a, b_1, \dots, b_n)$ with each b_i sep. over K (and a algebraic). Then $\exists \alpha \in L$ such that $L = K(\alpha)$.

Proof If K is finite, then so is L, and can take γ = generator of cyclic group L^*. So assume K infinite. By an obvious induction, reduce to case $n=1$. Look for $c \in K$ s.t. $\alpha = a + cb$ works. $(b := b_1)$. Let f (resp. g) be min poly of a (resp b). b is a root of the polynomials $g(X)$ and $f(\alpha - cX)$ in $K(\alpha)[X]$, so $X-b$ is a common factor. If it's the g.c.d. then it's a linear combination, whence $b \in K(\alpha)$, whence $a = \alpha - cb \in K(\alpha)$, whence $K(a,b) \subset K(\alpha) \subset K(a,b)$, q.e.d.

To make sure there is no other common factor of $g(X)$ and $f(\alpha - cX)$, i.e., that if $b = \beta_1, \beta_2, \cdots \beta_n$ are the roots of g (distinct, by separability) then no β_i with $i \geq 2$ is a root of $f(\alpha - cX)$, we just need that $\alpha - c\beta_i$ ~~is~~ is not one of the roots $a = a_1, a_2, \dots, a_m$ of f, i.e. $a + c(b - \beta_i) \neq a_j$, i.e. $c \neq \dfrac{a_j - a}{b - \beta_i}$. Since K is infinite, such c abound. This completes the proof.

Example (From old qualifier). Let $\zeta_n = e^{2\pi i/n}$. Show that $\mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}(\zeta_n + \zeta_m)$.

Solution In the above proof, take $a = \zeta_n$, $b = \zeta_m$ and show that $c = 1$ works. Since $\zeta_n^n = 1$, $\therefore f(X) \mid X^n - 1$, so any root a_j of f satisfies $a_j^n = 1$, i.e., $a_j = \zeta_n^c$ for some c with $1 \leq c < n$. Similarly $\beta_i = \zeta_m^d$. So need to show

$$\zeta_n + (\zeta_m - \zeta_m^d) \neq \zeta_n^c \quad \text{unless } d = 1, \quad \text{i.e.} \quad \zeta_m - \zeta_m^d \neq \zeta_n^c - \zeta_n$$

Drawing these numbers as points on the unit circle, you see that if $\begin{cases} d \neq \pm 1, \\ c \neq \pm 1 \end{cases}$ then

$$\mathrm{Re}(\zeta_m - \zeta_m^d) < 0 < \mathrm{Re}(\zeta_n^c - \zeta_n)$$

Hence $\{\zeta_m - \zeta_m^d = \zeta_n^c - \zeta \text{ and } d \neq 1\} \Rightarrow \{d = -1 \text{ and } \zeta_m - \zeta_m^{-1} = \zeta_n^{-1} - \zeta_n\}$

But looking at imaginary parts, you see this to be impossible. q.e.d.