Math 210B Lecture 24 Notes

Daniel Raban

March 8, 2019

1 Kummer Theory and Solvability by Radicals

1.1 Kummer theory

Definition 1.1. A **Kummer extension** of a field F is an extension generated by roots of elements of $F^\times$

Let F be a field, and let $\mu_n = \mu_n(\overline{F})$ be the n-th roots of unity in an algebraic closure of $\overline{F}$ of F.

Proposition 1.1. *Let $n \geq 1$, and let $a \in F$. Set $E = F(a)$,where $\alpha^n = a$. Let $d \geq 1$ be minimal such that $\alpha^d \in F$.*

1. *E/F is Galois iff $\operatorname{char}(F) \nmid d$ and $\mu_d \subseteq E$.*
2. *If E/F is Galois, and $\mu_d \subseteq F$, then $\chi_a : \operatorname{Gal}(E/F) \to \mu_n$ such that $\chi_a(\sigma) = \sigma(\alpha)/\alpha$ is an isomorphism onto μ_d.*

Definition 1.2. χ_a is the n-th **Kummer character** of a.

Proof. To prove (1), let f be the minimal polynomial of α. Then $f \mid (x^d - \alpha^d)$, but $f \nmid (x^m - \alpha^m)$ for all m property dividing d (by the minimality of d. If $|\mu_d| = d$, then all roots of $x^d - \alpha^d$ are distinct. So f is separable. If $|\mu_d| = m \neq d$, then $x^d - \alpha^d = (x^m - \alpha^m)^{d/m}$. But $f \mid x^d - \alpha^d$ and $f \nmid x^m - \alpha^m$, so f is not separable. So $\operatorname{char}(F) \nmid d$ iff E/F is separable.

Now assume that $\operatorname{char}(F) \nmid d$. Let $\sigma : E \to \overline{F}$ be an embedding fixing F satisfying $\sigma\alpha = \zeta\alpha$ for some $\zeta \in \mu_d$. If $\mu_d \subseteq E$, then $\zeta_\alpha \in E$, so $\sigma(E) \subseteq E$. So E/F is normal and hence Galois. If $\mu_d \not\subseteq E$, then there exists σ such that ζ has order d, since $f \nmid x^m - \alpha^m$ for all m strictly dividing d. Then $\zeta\alpha \notin E$, so $\sigma\alpha \notin E$. So E/F is not normal.

To prove (2), suppose that E/F is Galois and $\mu_d \subseteq F$. Then

$$\chi_a(\sigma\tau) = \frac{\sigma\tau(\alpha)}{\alpha} = \frac{\sigma\tau(\alpha)}{\sigma(\alpha)}\frac{\sigma(\alpha)}{\alpha} = \frac{\sigma\alpha}{\alpha}\sigma\left(\underbrace{\frac{\tau(\alpha)}{\alpha}}_{\in\mu_d\subseteq F}\right) = \chi_a(\sigma)\cdot\sigma(\chi_a(\tau)).$$

Then χ_a is 1 to 1 since it is onto and $[E : F] \leq d$, since $f \mid (x^d - \alpha^d)$. $\square$

Remark 1.1. In general, even if $\mu \not\subseteq F$, we have a map $\chi_a : \mathrm{Gal}(E/F) \to \mu_f$ send ing $\sigma \mapsto \sigma(\alpha)/\alpha$ that is a **1-cocycle**: $\chi_a(\sigma\tau) - \chi_a(\sigma) \cdot \sigma(\chi_a(\tau))$.

Proposition 1.2. *Let* $\mathrm{char}(F) \nmid n$*, and* $\mu_n \subseteq F$*. If* E/F *is a cyclic extension of degree* N*, then* $E = F(\alpha)$ *with* $\alpha^n \in F^\times$*.*

Proof. Let $\mu_n = \langle \zeta \rangle$. Then $N_{E/F}(\zeta) = \zeta^n = 1$. Then Hilbert's theorem 90 gives us that there exists $\alpha \in E$ and $\sigma \in \mathrm{Gal}(E/F)$ of order n such that $\sigma(\alpha)/\alpha = \zeta$.

$$N_{E/F}(\alpha) = \prod_{i=0}^{n-1} \sigma^i(\alpha) = \prod_{i=0}^{n-1} \zeta^i \alpha = \zeta^{n(n-1)/2}\alpha^n = (-1)^{n-1}\alpha^n.$$

Set $a = -N_{E/F}(-\alpha) \in F^\times$. Then

$$\alpha^n = (-1)^{n-1} N_{E/F}(\alpha) = -N_{E/F}(-\alpha) = a \in F^\times. \qquad \square$$

1.2 Perfect pairing

Definition 1.3. An R-bilinear pairing $(\cdot, \cdot) : A \times B \to C$ is **perfect** if the induced maps $A \to \mathrm{Hom}_R(B, C)$ and $B \to \mathrm{Hom}_R(A, C)$ are both isomorphisms. It is **nondegenerate** if these are both injective.

Example 1.1. Let V be an infinite-dimensional vector space over F. Then look at the pairing $V \times V^* \to F$. Then we get an embedding $V \to \mathrm{Hom}(V^*, F) = V^**$, which is not in general an isomorphism. So this pairing is nondegenerate, but it is not perfect.

Theorem 1.1. *Let* $\mathrm{char}(F) \nmid n$ *and* $\mu_n \subseteq F$*. Let* E/F *be (finite) abelian of exponent dividing* n*, and set* $\Delta = F^\times \cap (E^\times)^n$*. Then there is a perfect pairing* $\mathrm{Gal}(E/F) \times \Delta/(F^\times)^n \to \mu_n$ *sending* $(\sigma, \alpha) \mapsto \sigma(a^{1/n})/a^{1/n} = \chi_a(\sigma)$*, and* $E = F(\sqrt[n]{\Delta}) = F(\sqrt[n]{a} : a \in \Delta)$*. In particular we have bijections between (finite) abelian extension of* F *of exponent dividing* n *and subgroups of* $F^\times$ *containing* $(F^\times)^n$ *(with finite index):*

$$E \mapsto F^\times \cap (E^\times)^n,$$

$$F(\sqrt[n]{\Delta}) \leftarrow\!\shortmid \Delta.$$

Proof. We have a map $\Delta/(F^\times)^n \to \mathrm{Hom}(\mathrm{Gal}(E/F), \mu_n)$ sending $a \mapsto \chi_a$. Then $\chi_a = 1$ iff $a \in (F^\times)^n$. So this map is 1 to 1. Given $\chi : \mathrm{Gal}(E/F) \to \mu_n$, the kernel H of χ corresponds to $K = E^H$ with K/F cyclic of degree dividing n. By the previous proposition, there exists some $a = \alpha^n \in \Delta$ such that $K = F(\alpha)$. Then $a \mapsto \chi_a$. Then χ is some power of χ_a. So this map is onto, as well.

We have a map $\mathrm{Gal}(E/F) \to \mathrm{Hom}(\Delta/(F^\times)^n, \mu_n)$ sending $\sigma \mapsto (a \mapsto \chi_a(\sigma))$. Then $\sigma \mapsto 1$ iff $\sigma|_\Delta = \mathrm{id}|_\Delta$, which is equivalent to $\sigma|_K = 1$ for all cyclic K/F in E. This is equivalent to $\sigma = 1$. This is an injective map between groups of the same order, so it is onto. $\square$

1.3 Solvability by radicals

Definition 1.4. A finite field extension is **solvable by radicals** if there exists $s \geq 0$ and fields E_i with $0 \leq i \leq s$ such that

1. $E_0 = F$,
2. $E_{i+1} = E_i(\sqrt[n_i]{a_i})$ $a_i \in E_i^\times$, $n_i \geq 1$
3. $E_s \supseteq E$.

If $E_s = E$, then we call E a **radical extension**.[1]

Theorem 1.2. *If $f \in F[x]$ is nonconstant with splitting gield K of degree prime to* $\mathrm{char}(F)$, *then* $\mathrm{Gal}(K/F)$ *is solvable if and only if K/F is solvable by radicals.*

[1]We do this because E is just so cool.