

Mathematics 100C

Kummer theory handout

In this document, we give an overview of some results from Kummer theory.

We will use the following result, which will be a homework problem.

Theorem: Suppose V is a finite dimensional F vector space and $T \in \text{End}_F(V)$. Suppose $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in F[x]$, and

- $p(T) = 0$ on V ;
- $p(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ with the $\alpha_j \in F$ distinct.

Then $V = \bigoplus_j V_{\alpha_j}$, where $V_{\alpha} = \{v \in V : Tv = \alpha v\}$ is the α -eigenspace.

As mentioned, this will be a homework problem; an application of the CRT. An immediate corollary is:

Corollary: If $\mu_r \subseteq F$ and $T^r = 1$ on V , then $V = \bigoplus_{\zeta \in \mu_r} V_{\zeta}$.

Theorem: Suppose F is characteristic 0, $\mu_n \subseteq F$.

1. Suppose L/F is finite Galois with Galois group cyclic of order n . Then $L = F(\beta)$ where $\beta \in L^{\times}$ satisfies $\beta^n \in F^{\times}$, and $\beta^d \notin F^{\times}$ for all $d|n, d \neq n$.
2. Conversely, if $\beta \in L^{\times}$, and satisfies $\beta^n \in F^{\times}$, and $\beta^d \notin F^{\times}$ for all $d|n, d \neq n$, then L/F is Galois with Galois group cyclic of order n .

Proof. We prove the second part first. For this, first note that L is the splitting field of $x^n - \beta^n \in F[x]$, so L/F is Galois. From a homework question, you know the map $\Phi : \text{Gal}(L/F) \rightarrow \mu_n$, $\Phi(\sigma) = \sigma(\beta)/\beta$ is an injective group homomorphism. To see that it is surjective, note that if not, then its image is $\mu_m \subseteq \mu_n$, where $m|n, m \neq n$. Thus $\Phi(\sigma)^m = 1$ for all $\sigma \in \text{Gal}(L/F)$, so $\sigma(\beta^m) = \beta^m$ for all σ , so $\beta^m \in F^{\times}$ contradicting our assumption on β . Thus Φ is surjective, so an isomorphism, proving $\text{Gal}(L/F)$ is cyclic of order n .

Now we prove the first part. Let σ be a generator for $\text{Gal}(L/F)$. If $\zeta \in \mu_n$, let L_{ζ} denote the ζ -eigenspace of the F vector space L for the linear map $\sigma : L \rightarrow L$.

Claim: There exists a primitive n^{th} root of unity ζ such that $L_{\zeta} \neq 0$.

Proof of Claim. Let $H = \{\delta \in \mu_n : L_{\delta} \neq 0\}$. One sees easily that H is a subgroup of μ_n , because if $x \in L_{\zeta_1}, y \in L_{\zeta_2}$ then $xy \in L_{\zeta_1\zeta_2}$. Thus $H = \mu_m$, some $m|n$. One thus has $\sigma^m = 1$ on L . But σ has order n , so $H = \mu_n$ and the claim is proved. $\square$

Continuing with the proof of the first part, we have a $\beta \in L^{\times}$ so that $\sigma(\beta) = \zeta\beta$ with ζ a primitive n^{th} root of unity. Now $L \supseteq F(\beta) \supseteq F$. But now it is easy to see that $\text{Gal}(F(\beta)/F) \simeq \mu_n$ via the map Φ , because ζ is primitive. Thus $L = F(\beta)$. Additionally, we cannot have $\beta^m \in F^{\times}$ for $m|n, m \neq n$, again because ζ is primitive.

This completes the proof. $\square$

Definition: For an abelian group A , set $\widehat{A} = \text{Hom}(A, S^1)$, where $S^1 = \{z \in \mathbf{C}^{\times} : |z| = 1\}$ is the unit circle. Note that, if A has exponent n , then $\widehat{A} = \text{Hom}(A, \mu_n)$.

It is a fact that if A is a finite abelian group, then $\widehat{\widehat{A}}$ is a finite abelian group of the same size as A . Actually, in this case, A and $\widehat{\widehat{A}}$ are abstractly isomorphic as groups, although not canonically.

Definition: For a finite extension of fields L/F , set $\Delta(L/F) = ((L^{\times})^n \cap F^{\times})/(F^{\times})^n$.

We can generalize the above result via the following two theorems. For both of these theorems, we suppose $\text{char}(F) = 0$ and $\mu_n \subseteq F$.

Theorem: Suppose L/F is finite Galois with group $G = \text{Gal}(L/F)$, and G is abelian of exponent n . Define

$$\Phi : \Delta(L/F) \rightarrow \widehat{\text{Gal}(L/F)}$$

as $t \mapsto \Phi_t$, where $\Phi_t(\sigma) = \sigma(t^{1/n})/t^{1/n}$. Then Φ is an isomorphism.

Proof. Note that Φ_t is well-defined (independent of the choice of n^{th} root $t^{1/n}$, because $\mu_n \subseteq F$.) One easily checks that Φ is a group homomorphism.

To see that Φ is injective, suppose $t \in \Delta(L/F)$, and $\Phi_t \equiv 1$. Then $\sigma(t^{1/n}) = t^{1/n}$ for all $\sigma \in \text{Gal}(L/F)$, so $t^{1/n} \in F^\times$ and thus $t \in (F^\times)^n$, so $t \equiv 1 \in \Delta(L/F)$.

The surjectivity uses what we've already proved. Thus suppose $\chi : \text{Gal}(L/F) \rightarrow \mu_n$. Let $H = \ker(\chi)$ and $K = L^H$. Then χ induces

$$\bar{\chi} : \text{Gal}(K/F) \simeq \mu_m \subseteq \mu_n$$

for some $m|n$. Thus K/F is Galois with group the cyclic group of order m , so by Theorem above, $K = F(v^{1/m})$ for some $v \in F^\times$. Moreover, if σ generates the Galois group and $\bar{\chi}(\sigma) = \zeta$, then the proof above shows we may select v so that $\sigma(v^{1/m})/v^{1/m} = \zeta$. Indeed, simply take $\beta \neq 0$ to be in K_ζ (which we verified is nonzero), and $v = \beta^m$. Now if $u = v^{n/m} \in F^\times$, one has $u^{1/n} = v^{1/m} \in K^\times \subseteq L^\times$, and $\Phi_u = \chi$ on $\text{Gal}(L/F)$. This proves surjectivity. $\square$

Here is the second theorem.

Theorem: The association $L/F \mapsto \Delta(L/F)$ induces a bijection between finite Galois extensions L/F with $\text{Gal}(L/F)$ abelian of exponent n and finite subgroups of $F^\times/(F^\times)^n$. The inverse map is $\Delta \mapsto F(\Delta^{1/n}) = F(t^{1/n} : t \in \Delta)$.

Proof. We first check that both maps of the bijection have the correct image.

1. If L/F is finite Galois abelian with exponent n , then $\Delta(L/F)$ is finite: Indeed, by the previous theorem, $|\Delta(L/F)| = |\text{Gal}(L/F)|$.
2. If $\Delta \subseteq F^\times/(F^\times)^n$ is finite, then $F(\Delta^{1/n})/F$ is finite Galois with Galois group abelian of exponent n : Indeed, $F(\Delta^{1/n})$ is a splitting field over F , so is finite Galois. Let G be the Galois group. Then $\Psi : G \rightarrow \widehat{\Delta}$ via $\Psi_\sigma(t) = \sigma(t^{1/n})/t^{1/n}$. The map Ψ is easily seen to be a well-defined group homomorphism. It is injective, because if $\sigma(t^{1/n}) = t^{1/n}$ for all $t \in \Delta$, then σ acts trivially on $F(\Delta^{1/n})$ so $\sigma = 1$. Thus, G is abelian with exponent n , because Δ and thus $\widehat{\Delta}$ are.

We now take care of the bijectivity.

1. $\Delta \mapsto L = F(\Delta^{1/n}) \mapsto \Delta(L/F)$: Clearly $\Delta \subseteq \Delta(L/F)$. But $\text{Gal}(L/F) \hookrightarrow \widehat{\Delta}$ via the map Ψ above, and $\text{Gal}(L/F) \simeq \widehat{\Delta(L/F)}$ by the previous theorem. By counting, $\Delta = \Delta(L/F)$.
2. $L \mapsto \Delta(L/F) \mapsto F(\Delta^{1/n})$: Clearly $F(\Delta^{1/n}) \subseteq L$. But $\text{Gal}(L/F) \simeq \widehat{\Delta(L/F)}$ by the previous theorem; and $\text{Gal}(F(\Delta^{1/n})/F) = \widehat{\Delta(L/F)}$ by just proved. Thus $F(\Delta^{1/n}) = L$ by counting.

$\square$