Lecture # 7 (06/11/2024)

Today: Kummer extensions (Abelian case)

Assuming that the base field has enough roots of unity, we want to characterize Abelian Galois extensions.

Recall that the **exponent** of a group G is the smallest $n \in \mathbb{N}$ such that $g^n = 1_G \ \forall g \in G$.
If G is finite Abelian & of exponent n, then $G \leq (\mathbb{Z}/n\mathbb{Z})^r$ for some r.

is isomorphic to

So, char $K \nmid n$

Definition Let K be a field containing a primitive n-th root of unity. A Galois extension L/K is called n-Kummer if $\mathrm{Gal}(L/K)$ is an Abelian group whose exponent divides n.

- L/K is Kummer if it is n-Kummer for some n

Example (from last time)

- K a field that contains a primitive n-th root of unity
- L a cyclic extension of degree m, $m \mid n$

Then L/K is n-Kummer (it is also m-Kummer).

Example $\left(L = \mathbb{Q}(\sqrt{2}, \sqrt{3}),\ K = \mathbb{Q}\right)$

- Let $f(x) = (x^2-2)(x^2-3)$. Then $L = SF_{\mathbb{Q}}(f)$.
- L/K is Galois and $\underset{\substack{\parallel \\ G}}{\mathrm{Gal}(L/K)} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
- G has exponent 2 and since $-1 \in K = \mathbb{Q}$

  L/K is 2-Kummer

Theorem Let K be a field containing a primitive n-th root of unity and let L/K be a finite extension. Then L/K is n-Kummer iff $L = K(\alpha_1^{1/n}, \ldots, \alpha_r^{1/n})$ for some $\alpha_i \in K$.

proof

($\Leftarrow$) Write $L = K(\beta_1, \dots, \beta_r)$ where $\beta_i^n = \alpha_i \in K$. Let $S = \{ x^n - \alpha_i \,;\, 1 \le i \le r \}$.

and let $\omega \in K$ be a primitive root of unity.

Then $L = SF_K(S)$ and L/K is separable hence Galois

Since $\beta_i, \omega\beta_i, \dots, \omega^{n-1}\beta_i$ are all the roots of $x^n - \alpha_i$ and these all lie in L

Moreover, if $\sigma \in Gal(L/K)$, then $\sigma^n(\beta_i) = \beta_i$ $\forall i = 1, \dots, r$. Thus, the exponent of $Gal(L/K) = G$ divides n.

Finally, G is abelian since given any $\sigma, \tilde{\sigma} \in G$, and any $i = 1, \dots, r$, we know that $\sigma(\beta_i) = \omega^j \beta_i$ and that $\tilde{\sigma}(\beta_i) = \omega^k \beta_i$ for some $j, k \in \{1, \dots, n-1\}$

Thus, $(\sigma\tilde{\sigma})(\beta_i) = (\tilde{\sigma}\sigma)(\beta_i)$. But the β_i generate L ...

$(\Rightarrow)$ Assume that L/K is Galois & that $G = \mathrm{Gal}(L/K)$ is abelian whose exponent divides n. (i.e. L/K is n-Kummer)

Then $G \simeq C_1 \times \cdots \times C_r$ where each C_i is cyclic of order dividing n.

Let H_i be a subgroup of G s.t. $G/H_i \simeq C_i$ and let $L_i := L^{H_i}$.

Then L_i/K is Galois with cyclic Galois group $\simeq C_i$. Let $|C_i| = m_i = [L_i : K]$ and let ω be as in $(\Leftarrow)$ above.

Then $\omega^{n/m_i} \in K$ & by Proposition 3 from Lecture # 6, $L_i = K(a_i^{1/m_i}) = K(\beta_i)$, where $a_i = \beta_i^{m_i} \in K$. Now, under the Galois $K(\beta_1, \ldots, \beta_r)$ corresponds to $\bigcap H_i = \{1_G\}$.

Thus, $L = K(\beta_1, \ldots, \beta_r)$ and since

$$\beta_i^n = a_i^{n/m_i} = \alpha_i \in K,$$

$$L = K(\alpha_1^{1/n}, \ldots, \alpha_r^{1/n}) \quad \blacksquare$$

Question: What is the degree of the extension $L = K(\alpha_1^{1/n}, \dots, \alpha_r^{1/n}) / K$?

(always $\leq n^r$)

Given L/K an n-Kummer extension, consider the following finite abelian group

$$\mathrm{Kum}(L/K) := \{ a \in L^\times ; \ a^n \in K \} / K^\times$$

then there exists a non-degenerate bilinear pairing

$$\mathrm{Gal}(L/K) \times \mathrm{Kum}(L/K) \xrightarrow{B} \mu_n(K) \simeq C_n$$
$$(\sigma, aK^\times) \longmapsto \frac{\sigma(a)}{a}$$

In particular, writing $G = \mathrm{Gal}(L/K)$, we have that the group homomorphism

$$\varphi : \mathrm{Kum}(L/K) \longrightarrow \mathrm{Hom}(G, \mu_n)$$
$$aK^\times \longmapsto \left(\sigma \longmapsto \frac{\sigma(a)}{a} \right)$$

is an isomorphism & $\mathrm{Hom}(G, \mu_n) \simeq G$.

needs more machinery

Therefore, the answer to the question is the size of Kum(L/K).

In general,

<u>Proposition</u>: If L/K is an n-Kummer extension, then there exists an injective group homomorphism $\mathrm{Kum}(L/K) \xrightarrow{f} K^\times / K^{\times n}$ given by $aK^\times \mapsto a^n K^{\times n}$.

<u>proof</u> (injectivity)

$aK^\times \in \mathrm{Ker}(f) \Rightarrow a^n \in K^{\times n}$

$\Rightarrow \exists\, b \in K^\times$ s.t. $a^n = b^n$

$\Rightarrow a/b \in \mu_n \subset K^\times \Rightarrow a \in K^\times$

$\Rightarrow aK^\times = K^\times$ (= id)

∎

This can be used to construct Kummer extensions of a given degree.

Proposition Let K be a field containing a primitive n-th root of unity and let G be a finite abelian subgroup of $K^\times/K^{\times n}$. of exponent n

Consider

$$L_G := F\left(\{\alpha^{1/n} ;\ \alpha K^{\times n} \in G\}\right) \hookrightarrow \overline{K}.$$

Then L_G/K is an n-Kummer extension with $\mathrm{Gal}(L_G/K) \simeq G$.

proof What is left is to show that $G = \mathrm{im}(f)$ where

$$\mathrm{Kum}(L_G/K) \xrightarrow{f} K^\times/K^{\times n} \quad \text{is as before}$$
$$a K^\times \longmapsto a^n K^{\times n}$$

By definition (of L_G),

$$\alpha K^{\times n} \in G \Rightarrow \alpha^{1/n} \in L_G^\times$$
$$\Rightarrow f\left(\alpha^{1/n} K^\times\right) = \alpha K^{\times n}$$
$$\Rightarrow G \subset \mathrm{im}(f)$$

Now, consider the pairing

$$\mathrm{Gal}(L_G/K) \times G \longrightarrow \mu_n$$
$$(\sigma, \alpha K^{\times n}) \longmapsto \frac{\sigma(\alpha^{1/n})}{\alpha^{1/n}}$$

Claim (exercise): This is bilinear & non-degenerate.

$\Rightarrow$ induces an isomorphism $G \simeq \mathrm{Gal}(L_G/K)$

$\Rightarrow |G| = [L_G : K] = |\mathrm{Kum}(L_G/K)|$

On the other hand, f injective $\Rightarrow$

$$|\mathrm{Kum}(L_G/K)| = |\mathrm{im}(f)|$$

and since $G \subset \mathrm{im}(f)$ we deduce that equality holds. $\blacksquare$

Upshot:

$$\left\{ \begin{array}{l} \text{finite abelian} \\ \text{subgroups of } K^{\times}/K^{\times n} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} n\text{-Kummer} \\ \text{extensions } L/K \end{array} \right\}$$

Example Let K/F be cyclic of degree 3 and assume that $\mathrm{char}(K) \neq 2$.

abelian

Let $G \leq K^\times/K^{\times 2}$ be a subgroup of order 4 and assume that $\mathrm{Gal}(K/F) \curvearrowright G$ is free.

Then we obain $\underset{\deg 4}{L_G \supset K} \underset{\deg 3}{\supset F}$ an A_4 Galois extension.

Back to the Kummer pairing Consider

$$\mathrm{Gal}(L/K) \times \mathrm{Kum}(L/K) \xrightarrow{B} \mu_n$$
$$(\sigma, aK^\times) \longmapsto \frac{\sigma(a)}{a}$$

(with L, K & n as before)

Let's check that the following hold.

1. if $\sigma \in \mathrm{Gal}(L/K)$ is such that $B(\sigma, aK^\times) = 1$ $\forall\, aK^\times \in \mathrm{Kum}(L/K)$, then $\sigma = \mathrm{id}$.

2. if $aK^\times \in \mathrm{Kum}(L/K)$ is such that $B(\sigma, aK^\times) = 1$ $\forall\, \sigma \in \mathrm{Gal}(L/K)$, then $aK^\times = K^\times$

① By assumption, $\sigma(a) = a \ \forall a \in L^\times$ s.t. $a^n \in K$. And since these generate L (as a field extension of K), $\sigma = \mathrm{id}$.

② By assumption, $a \in L^{\mathrm{Gal}(L/K)} = K$. Thus, $aK^\times = K^\times$.

Two more examples

Ⓐ $K = \mathbb{Q}(i)$, $i^2 = -1$

$L = K(\sqrt{2}, \sqrt[4]{3})$

- Then L/K is 4-Kummer since $\sqrt{2}\sqrt[4]{3} = \sqrt[4]{12}$
- $[L:K] = 8$ and <u>not</u> $4^2 = 16$

Ⓑ $K = \mathbb{C}(x,y,z)$, $i \in K$

$a := xyz$, $b := y^2 z$, $c := xz^2$

$L = K(a^{1/4}, b^{1/4}, c^{1/4}) \rightsquigarrow L/K$ is 4-Kummer of degree $32 \neq 4^3$