Lecture 32: Kummer theory: The cyclic case

Wednesday, March 14, 2018 11:08 AM

Let's go back to the study of a cyclic extension E/F of index n where $\mu_n \subseteq F$. We proved $\exists \alpha \in E$ s.t. $\sigma(\alpha) = \zeta_n \alpha$ where $Gal(E/F) = \langle \sigma \rangle$. This implies

$$m_{\alpha,F}(x) = \prod_{i=0}^{n-1} (x - \sigma^i(\alpha)) = \prod_{i=0}^{n-1} (x - \zeta_n^i \alpha) = x^n - \alpha^n$$

Hence $a = \alpha^n \in F^\times$ and $\alpha^i \notin F$ if $1 \leq i < n$. Therefore $a^i \notin (F^\times)^n$ if $1 \leq i < n$ (otherwise $\underset{\text{for some } b \in F^\times}{\alpha^{in} = b^n} \Rightarrow \alpha^i = \zeta_n^{j} b \in F^\times$ which is a contrad.)

$\Rightarrow |\langle a (F^\times)^n \rangle| = n = |Gal(F[\sqrt[n]{a}]/F)|$; and so

$$Gal(F[\sqrt[n]{a}]/F) \simeq \langle a (F^\times)^n \rangle.$$

Summary:

<u>Lemma</u>. $\left.\begin{array}{l} Gal(E/F) = \langle \sigma \rangle \\ [E:F] = n \\ \mu_n \subseteq F \\ Char(F) \nmid n \end{array}\right\} \Rightarrow \exists\, a \in F^\times$ s.t. $E = F[\sqrt[n]{a}]$ and $Gal(E/F) \simeq \langle a (F^\times)^n \rangle$.

So next we focus on the relation between $F[\sqrt[n]{a}]/F$ and the cyclic subgroup $\langle a (F^\times)^n \rangle$ of $F^\times/(F^\times)^n$.

Theorem. Suppose $\mu_n \subseteq F$, $\mathrm{char}(F) \nmid p$; then

$$F[\sqrt[n]{a_1}] = F[\sqrt[n]{a_2}] \Leftrightarrow a_1 (F^\times)^n = a_2 (F^\times)^n .$$

Pf. We have already proved that $F[\sqrt[n]{a_i}]/F$ is a cyclic extension and

$$\mathrm{Gal}(F[\sqrt[n]{a_1}]/F) \longrightarrow \mathbb{Z}/n\mathbb{Z} \quad \text{where } \sigma(\sqrt[n]{a_1}) = \zeta_n^{j_\sigma} \sqrt[n]{a_1}$$
$$\sigma \longmapsto j_\sigma ,$$

is an injective group homomorphism. (*)

Let $\theta : \mathrm{Gal}(F[\sqrt[n]{a_1}]/F) \longrightarrow \mu_n$, $\theta(\sigma) := \dfrac{\sigma(\sqrt[n]{a_1})}{\sqrt[n]{a_1}} = \zeta_n^{j_\sigma}$

$$\begin{tikzcd} \mathrm{Gal}(F[\sqrt[n]{a_1}]/F) \arrow[rr] \arrow[dr] & & \mu_n \\ & \mathbb{Z}/n\mathbb{Z} \arrow[ur, "\sim"] & \end{tikzcd}$$

By (*), θ is an injective group homomorphism.

Similarly we get $\theta' : \mathrm{Gal}(F[\sqrt[n]{a_2}]/F) \longrightarrow \mu_n$, $\theta'(\sigma) := \dfrac{\sigma(\sqrt[n]{a_2})}{\sqrt[n]{a_2}}$ is an injective group homomorphism. Since μ_n is cyclic, it has a unique subgroup of order $[F[\sqrt[n]{a_1}]:F]$. Therefore

$$\frac{\sigma(\sqrt[n]{a_2})}{\sqrt[n]{a_2}} = \left(\frac{\sigma(\sqrt[n]{a_1})}{\sqrt[n]{a_1}} \right)^{i}$$ for some i. This implies

$\sigma\left(\sqrt[n]{a_1}^{\,i} / \sqrt[n]{a_2} \right) = \sqrt[n]{a_1}^{\,i} / \sqrt[n]{a_2}$; and so $\sqrt[n]{a_1}^{\,i} / \sqrt[n]{a_2} \in \mathrm{Fix}(\sigma) = F$.

And so $a_2 (F^\times)^n = a_1^i (F^\times)^n$, which implies $a_2 (F^\times)^n \in \langle a_1 (F^\times)^n \rangle$.

Lecture 32: Kummer theory: The cyclic case

Wednesday, March 14, 2018 8:50 AM

By symmetry $a_1(F^\times)^n \in \langle a_2(F^\times)^n\rangle$; and claim follows. ∎

<u>Corollary</u>. $\mathrm{char}(F)\nmid n$, $\mu_n \subseteq F$. Then

$$\mathrm{Gal}(F[\sqrt[n]{a}]/F) \simeq \langle a(F^\times)^n\rangle.$$

<u>Pf</u>. We have proved that $\mathrm{Gal}(F[\sqrt[n]{a}]/F) \simeq \mathbb{Z}/m\mathbb{Z}$

for some $m \mid n$. And so $\exists\, b \in F^\times$ s.t. $F[\sqrt[n]{a}] = F[\sqrt[m]{b}]$

and $|\langle b(F^\times)^m\rangle| = m$.

So $F[\sqrt[n]{a}] = F[\sqrt[n]{b^{n/m}}]$; hence, by the previous theorem,

$a(F^\times)^n = (b^{n/m})(F^\times)^n$.

<u>Claim</u>. $o((b^{n/m})(F^\times)^n) = m$.

<u>Pf</u>.. $(b^{n/m})^i \in (F^\times)^n \iff \exists\, c \in F^\times,\ b^{i\,n/m} = c^n$

$$\iff (\sqrt[m]{b})^i = \underbrace{\zeta_n^j\, c}_{\text{in } F^\times} \quad \text{for some } j$$

$$\iff b^i \in (F^\times)^m$$

$$\iff o(b(F^\times)^m) \mid i \text{; and claim follows.}$$

Therefore $|\langle a(F^\times)^n\rangle| = m = |\mathrm{Gal}(F[\sqrt[n]{a}]/F)|$; and as $\langle a(F^\times)^n\rangle$

and $\mathrm{Gal}(F[\sqrt[n]{a}]/F)$ are cyclic, claim follows. ∎

Lecture 32: Kummer theory

Wednesday, March 14, 2018 1:03 PM

<u>Theorem</u>. Suppose $\mathrm{char}(F)\nmid n$ and $\mu_n \subseteq F$. Let $\overline{F}$ be an algebraic closure of F. Then the following is a bijection

$$\{E\subseteq \overline{F} \mid E/F: \text{cyclic of exponent } n\} \longleftarrow \{\text{cyclic subgps of } F^\times/(F^\times)^n\}.$$

(this means $\forall \sigma\in \mathrm{Gal}(E/F), \sigma^n = \mathrm{id}_E$)

$$F[\sqrt[n]{a}] \longleftarrow\!\!\!\shortmid\; a(F^\times)^n$$

where $\sqrt[n]{a}\in\overline{F}$ is a zero of $x^n - a = 0$.

We can extend this bijection to the setting of <u>abelian groups of exponent n</u>.

<u>Theorem</u>. In the above setting, the following are bijections

$$\{E\subseteq \overline{F} \mid E/F: \underset{\text{finite}}{\text{abelian}} \text{ of exponent } n\} \rightleftarrows \{\overset{\text{finite}}{\text{subgroups}} \text{ of } F^\times/(F^\times)^n\}.$$

$$E \longmapsto (E^\times)^n \cap F^\times/(F^\times)^n =: \overline{\Delta}_E$$

$$F[\Delta^{1/n}] \longleftarrow\!\!\!\shortmid\; \overline{\Delta} := \Delta/(F^\times)^n$$

where $\Delta^{1/n} := \{\sqrt[n]{a} \mid a\in\Delta\}$.

($\sqrt[n]{a}\in\overline{F}$ a zero of $x^n - a$).

And $\mathrm{Gal}(E/F) \simeq \mathrm{Hom}(\overline{\Delta}_E, \mu_n)$ if E/F is an abelian extension of exponent n.

(finite is not needed)

Kummer pairing was defined during lecture, but we did not have time to present this pf.

Pf. Let $\Delta_E := (E^\times)^n \cap F^\times$ and $\overline{\Delta}_E := \Delta_E / (F^\times)^n$.

Let $f: \mathrm{Gal}(E/F) \times \Delta_E \to \mu_n$, $f(\sigma, \alpha^n (F^\times)^n) := \frac{\sigma(\alpha)}{\alpha}$ is a well-defined bilinear map. (Known as Kummer pairing.)

Well-defined. $\alpha_1^n (F^\times)^n = \alpha_2^n (F^\times)^n \Leftrightarrow \exists c \in F, \zeta \in \mu_n$ s.t. $\alpha_1 = c\zeta\alpha_2$

$$\Rightarrow \frac{\sigma(\alpha_1)}{\alpha_1} = \frac{\sigma(c\zeta\alpha_2)}{c\zeta\alpha_2} = \frac{c\zeta\,\sigma(\alpha_2)}{c\zeta\,\alpha_2} = \frac{\sigma(\alpha_2)}{\alpha_2}.$$

$$\cdot\ \sigma(\alpha)^n = \sigma(\alpha^n) = \alpha^n \Rightarrow \frac{\sigma(\alpha)}{\alpha} \in \mu_n.$$

linear in 1st factor. $(\sigma_1 \circ \sigma_2)(\alpha) = \sigma_1(\sigma_2(\alpha)) = \sigma_1(f(\sigma_2, \overline{\alpha})\,\alpha)$

$$= f(\sigma_2, \overline{\alpha^n})\ \sigma_1(\alpha) = f(\sigma_2, \overline{\alpha^n})\, f(\sigma_1, \overline{\alpha})\,\alpha$$

$$\Rightarrow f(\sigma_1 \circ \sigma_2, \overline{\alpha^n}) = f(\sigma_1, \overline{\alpha^n})\, f(\sigma_2, \overline{\alpha^n})$$

linear in 2nd factor. $f(\sigma, \overline{\alpha_1^n}\,\overline{\alpha_2^n}) = \frac{\sigma(\alpha_1\alpha_2)}{\alpha_1\alpha_2} = \frac{\sigma(\alpha_1)}{\alpha_1} \cdot \frac{\sigma(\alpha_2)}{\alpha_2}$

$$= f(\sigma, \overline{\alpha_1^n})\, f(\sigma, \overline{\alpha_2^n}).$$

$\boxed{f \text{ is perfect pairing}}$; $\Theta: \overline{\Delta}_E \to \mathrm{Hom}(\mathrm{Gal}(E/F), \mu_n)$

$$(\Theta(\overline{\alpha^n}))(\sigma) := f(\sigma, \overline{\alpha^n}).$$

Since f is bilinear, $\Theta(\sigma) \in \mathrm{Hom}(\overline{\Delta}_E, \mu_n)$ and Θ is a group hom.

Why is Θ injective? $\Theta(\overline{\alpha}^n) = 1$. Then $\forall \sigma \in \mathrm{Gal}(E/F)$, $\sigma(\alpha) = \alpha$.

Lecture 32: Kummer theory

Wednesday, March 14, 2018 4:00 PM

So $\alpha \in F^\times$, and $\bar{\alpha}^n = 1$.

<u>Why is Θ surjective?</u> Let $\xi : Gal(E/F) \to \mu_n$. Let $N := \ker \xi$, and $K := Fix(N)$. Then $Gal(K/F) \simeq Gal(E/F)/Gal(E/K) \simeq \operatorname{Im}\xi$ which is a cyclic group of exponent n. Suppose $\sigma_0 \in Gal(E/F)$ restricted to K generates $Gal(K/F)$. Then, by the cyclic case of Kummer theory, $K = F[\sqrt[n]{a_0}]$, and

$$\left|\left\langle \frac{\sigma_0(\sqrt[n]{a_0})}{\sqrt[n]{a_0}} \right\rangle\right| = |Gal(K/F)| = |\operatorname{Im}\xi| =: m$$

Since $\left\langle \frac{\sigma_0(\sqrt[n]{a_0})}{\sqrt[n]{a_0}} \right\rangle$ and $\operatorname{Im}\xi$ are subgps of μ_n,

$\exists\, i$ s.t. $\gcd(i, m) = 1$ and $\xi(\sigma_0) = \dfrac{\sigma_0(\sqrt[n]{a_0}^{\,i})}{\sqrt[n]{a_0}^{\,i}}$.

So $\xi(\sigma_0) = \Theta(a_0^i (F^\times)^n)(\sigma_0)$; and

$\forall \sigma \in Gal(E/K)$, $\Theta(a_0^i (F^\times)^n)(\sigma) = \dfrac{\sigma(\sqrt[n]{a_0}^{\,i})}{\sqrt[n]{a_0}^{\,i}} = 1 = \xi(\sigma)$.

Therefore $\xi = \Theta(a_0^i (F^\times)^n)$.

$$\operatorname{Hom}\left(\bigoplus_{i=1}^{k} \mathbb{Z}/m_i\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}\right) \simeq \bigoplus \operatorname{Hom}(\mathbb{Z}/m_i\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$$

$$\simeq \bigoplus \mathbb{Z}/\gcd(m_i, n)\mathbb{Z} \simeq \bigoplus \mathbb{Z}/m_i\mathbb{Z}.$$ So

$\operatorname{Hom}(Gal(E/F), \mu_n) \simeq Gal(E/F)$.

Lecture 32: Kummer theory

Wednesday, March 14, 2018 6:27 PM

$\underline{F[\Delta_E^{1/n}] = E}$.

Suppose $\sigma_0|_{F[\Delta_E^{1/n}]} = \mathrm{id}$. Then $(\Theta(\bar{\alpha}^n))(\sigma_0) = 1 \quad \forall \bar{\alpha}^n \in \bar{\Delta}_E$.

So $\forall \xi : \mathrm{Gal}(E/F) \longrightarrow \mu_n$, $\xi(\sigma_0) = 1$. And so $\sigma_0 = \mathrm{id}$.

(See the included notes on dual of abelian gps of exponent n)

- Let $(F^\times)^n \leq \Delta \leq F^\times$, and $E := F[\Delta^{1/n}]$. Then $F[\Delta^{1/n}]$ is a splitting field of $\{x^n - a\}_{a \in \Delta}$. Since $\mathrm{char}(F) \nmid n$, $x^n - a$ is separable. So $F[\Delta^{1/n}]/F$ is Galois. And

$\forall \sigma \in \mathrm{Gal}(F[\Delta^{1/n}]/F)$ and $\alpha \in \Delta^{1/n}$, $\sigma(\alpha^n) = \alpha^n$ implies

$\exists\, \zeta_{\sigma,\alpha} \in \mu_n$ s.t. $\sigma(\alpha) = \zeta_{\sigma,\alpha}\, \alpha$

$$\Rightarrow \begin{cases} \sigma^n(\alpha) = \alpha \\ \sigma_1 \circ \sigma_2(\alpha) = \sigma_1(\zeta_{\sigma_2,\alpha}\, \alpha) = \zeta_{\sigma_2,\alpha} \cdot \zeta_{\sigma_1,\alpha}\, \alpha \\ \sigma_2 \circ \sigma_1(\alpha) = \sigma_2(\zeta_{\sigma_1,\alpha}\, \alpha) = \zeta_{\sigma_1,\alpha} \cdot \zeta_{\sigma_2,\alpha}\, \alpha \end{cases}$$

$\Rightarrow F[\Delta^{1/n}]/F$ is abelian of exponent n.

<u>Claim</u>. $(E^\times)^n \cap F^\times = \Delta$.

<u>Pf</u>. Clearly $\Delta \subseteq \underbrace{(E^\times)^n \cap F^\times}_{\Delta_E}$. Suppose $\Delta \subsetneq \Delta_E$. Then

$\exists\, \eta \in \mathrm{Hom}(\Delta_E, \mu_n)$ s.t. $\Delta \subseteq \ker(\eta) \subsetneq \Delta_E$.

Lecture 32: Kummer theory

Wednesday, March 14, 2018 9:31 PM

Since $f: \mathrm{Gal}(E/F) \times \overline{\Delta}_E \to \mu_n$ is a perfect pairing,

$$\begin{aligned} \mathrm{Gal}(E/F) &\longrightarrow \mathrm{Hom}(\overline{\Delta}_E, \mu_n) \quad \text{is an isomorphism.} \\ \sigma &\longmapsto f(\sigma, \cdot) \end{aligned}$$

And so $\exists\, \sigma_0 \in \mathrm{Gal}(E/F)$ s.t. $\forall\, \overline{\delta} \in \overline{\Delta}_E$, $\eta(\overline{\delta}) = f(\sigma_0, \overline{\delta})$.

In particular, $\forall\, a \in \Delta$, $f(\sigma_0, a) = 1$; and so $\sigma_0(\sqrt[n]{a}) = \sqrt[n]{a}$.

Therefore $\sigma_0|_{F[\Delta^{1/n}]} = \mathrm{id}$; which mean $\sigma_0 = \mathrm{id}$. And so $\eta = 1$, which is a contradiction. ∎

<u>About abelian groups of exponent n and their duals:</u>

For an abelian group A of exponent n, let $\hat{A} := \mathrm{Hom}(A, \mu_n)$.

If $A \xrightarrow{f} B$ is a group hemomorphism, then $\hat{B} \xrightarrow{\hat{f}} \hat{A}$ is a group homomorphism where $\hat{f}(\beta) := \beta \circ f$

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[dr, dashed, "\hat{f}(\beta)"'] & B \arrow[d, "\beta"] \arrow[dl, phantom, "\circlearrowleft"] \\ & \mu_n \end{tikzcd}$$

And $A \xrightarrow{f} B \xrightarrow{g} C$, $\underbrace{A \longrightarrow C}_{g\circ f}$ implies $\widehat{g\circ f} = \hat{f} \circ \hat{g}$

$\hat{C} \xrightarrow{\hat{g}} \hat{B} \xrightarrow{\hat{f}} \hat{A}$, $\underbrace{\hat{C} \longrightarrow \hat{A}}_{\hat{f}\circ\hat{g}}$; and $\widehat{\mathrm{id}_A} = \mathrm{id}_{\hat{A}}$. Therefore if

$f: A \to B$ is an isomorphism, then $\hat{f}: \hat{B} \to \hat{A}$ is an isomorphism.

Lecture 32: Dual of abelian groups of exp n.

Friday, March 16, 2018 8:41 AM

- If $f: A\times B \to \mu_n$ is a bilinear map (called pairing), then

$f_A: A \to \widehat{B}$, $(f_A(a))(b) := f(a,b)$ and

$f_B: B \to \widehat{A}$, $(f_B(b))(a) := f(a,b)$ are group homomorphisms.

- For any A, $\widehat{A}\times A \xrightarrow{f^\circ} \mu_n$ is a pairing. And we have
$(\alpha, a) \mapsto \alpha(a)$

$f^\circ_{\widehat{A}} = \mathrm{id}_{\widehat{A}}$ and $f^\circ_A : A \to \widehat{\widehat{A}}$. Next we study $\widehat{A}$ and f°_A for

<u>finite</u> abelian groups of exponent n.

<u>Lemma</u>. (a) Let A be a <u>finite</u> abelian group of exponent n. Then

$A \simeq \widehat{A}$; in particular $|A| = |\widehat{A}|$.

(b) $f^\circ_A : A \to \widehat{\widehat{A}}$ is an isomorphism,

(c) $\underset{\text{surjective}}{A \xrightarrow{g} B}$ if and only if $\underset{\text{injective}}{\widehat{B} \xrightarrow{\widehat{g}} \widehat{A}}$; and $\underset{\text{inject.}}{A \xrightarrow{g} B} \Leftrightarrow \underset{\text{surj.}}{\widehat{g}}$.

<u>Pf</u> (a) $A \simeq \bigoplus_{i=1}^{\ell} \mathbb{Z}/k_i\mathbb{Z}$ for some $k_i | n$. So $\widehat{A} \simeq \mathrm{Hom}(\bigoplus_{i=1}^{\ell} \mathbb{Z}/k_i\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$

$\simeq \bigoplus_{i=1}^{\ell} \mathrm{Hom}(\mathbb{Z}/k_i\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \simeq \bigoplus_{i=1}^{\ell} \mathbb{Z}/\gcd(k_i,n)\mathbb{Z} \simeq A$.

(b) Let's identify A with $\bigoplus_{i=1}^{\ell} \mu_{k_i}$. And let $p_i : A \to \mu_n$,

Lecture 32: Dual of abelian groups of exp n

Friday, March 16, 2018 11:59 AM

$p_i(x_1,\dots,x_\ell) := x_i \in \mu_{k_i} \subseteq \mu_n$. Then $\forall a \in A$,

$$a = 1 \iff \forall i,\ p_i(a) = 1 \iff \left(f_A^\circ(a)\right)(p_i) = 1.$$

Therefore $f_A^\circ : A \to \hat{\hat{A}}$ is an embedding. By part (a), $|A| = |\hat{A}|$
$= |\hat{\hat{A}}|$.

Hence $f_A^\circ : A \xrightarrow{\sim} \hat{\hat{A}}$.

(c). $\hat{g}(\beta) = 0 \Rightarrow \left(\hat{g}(\beta)\right)(a) = 0$

$$\left.\begin{array}{l} \Rightarrow \beta(g(a)) = 0 \\ \forall a \in A \\ g:\text{ surj.}\end{array}\right\} \Rightarrow \beta = 0.$$

- Suppose $0 \neq a \in \ker(g)$. Then $0 \neq f_A^\circ(a) \in \hat{\hat{A}}$; which means $\exists\, \alpha \in \hat{A}$ s.t. $\left(f_A^\circ(a)\right)(\alpha) \neq 0$; and so $\alpha(a) \neq 0$. Since $\hat{g}$ is surjective, $\hat{g}(\beta) = \alpha$ for some $\beta \in \hat{B}$. And so

$0 \neq \alpha(a) = \hat{g}(\beta) = \beta(g(a)) = 0$ as $a \in \ker(g)$, which is a contra.

Notice that

$$\begin{tikzcd} A \arrow[r, "g"] \arrow[d, "f_A^\circ"', "\wr"] \arrow[dr, phantom, "\circlearrowright"] & B \arrow[d, "f_B^\circ", "\wr"'] \\ \hat{\hat{A}} \arrow[r, "\hat{\hat{g}}"'] & \hat{\hat{B}} \end{tikzcd}$$

$a \mapsto g(a)$, $a \mapsto f_A^\circ(a)$, $g(a) \mapsto f_B^\circ(g(a))$, $f_A^\circ(a) \mapsto \hat{\hat{g}}(f_A^\circ(a))$

$$\left(f_B^\circ(g(a))\right)(\beta) = \beta(g(a))$$

$$\begin{aligned}\left(\hat{\hat{g}}(f_A^\circ(a))\right)(\beta) &= \left(f_A^\circ(a)\circ \hat{g}\right)(\beta) \\ &= \left(f_A^\circ(a)\right)\left(\hat{g}(\beta)\right) \\ &= \left(\hat{g}(\beta)\right)(a) \\ &= \beta(g(a)).\end{aligned}$$

And so g injective $\iff \hat{\hat{g}}$ injective $\iff \hat{g}$ surjective. ∎

<u>Corollary</u>. Suppose $g : A \times B \to \mu_n$ is a pairing. Then g_A is an isomorphism

if and only if g_B is an isomorphism.

Pf. $A \xrightarrow[g_A]{\sim} \hat{B}$ is an isomorphism. And so

$$B \xrightarrow[f_B^\circ]{\sim} \hat{\hat{B}} \xrightarrow[\hat{g}_A]{\sim} \hat{A}$$

$$b \longmapsto f_B^\circ(b) \longmapsto \hat{g}_A(f_B^\circ(b))$$

$$\left(\hat{g}_A(f_B^\circ(b))\right)(a) = \left(f_B^\circ(b) \circ g_A\right)(a) = f_B^\circ(b)\,(g_A(a))$$

$$= \left(g_A(a)\right)(b) = g(a,b) = g_B(b)(a).$$

$\Rightarrow \hat{g}_A \circ f_B^\circ = g_B \Rightarrow g_B$ is an isomorphism. ∎

Def. $g: A \times B \to \mu_n$ is called a perfect pairing if g_A and g_B are isomorphisms.