Last time: Hilbert class field of a number field

What about function fields K?

- The image of $U = \prod_v \mathcal{O}_v^\times$ in $\mathbb{A}_K^\times / K^\times$ has ~~finite~~/infinite index in $\mathbb{A}_K^\times / K^\times$.

$$\boxed{\mathbb{A}_K^\times \Big/ \prod_v \mathcal{O}_v^\times \times K^\times \cong \Big(\prod_v{}' \underbrace{K_v^\times / \mathcal{O}_v^\times}_{\mathbb{Z}}\Big) \Big/ K^\times}$$

It is contained in the kernel of the content map

$$c : \mathbb{A}_K^\times / K^\times \longrightarrow \mathbb{R}^{>0}$$
$$(x_v)_v \longmapsto \prod_v |x_v|_v$$

, which has infinite image.

- K has an infinite unramified abelian extension.

$\overline{\mathbb{F}}_q(T) \mid \mathbb{F}_q(T)$ is the max. (abelian) unram. ext.

Pf Unram.: Every irred. $f(T) \in \mathbb{F}_q[T]$ split into distinct (linear) factors over $\overline{\mathbb{F}}_q$.

Same for the place at ∞, replacing T by $\frac{1}{T}$.

Max. unram.: Assume $K' \mid \overline{\mathbb{F}}_q(T)$ is a deg. n unram. ext.

$\rightsquigarrow$ proj. curves $C' \longrightarrow \mathbb{P}^1_{\overline{\mathbb{F}}_q}$ unram. covering of degree n

Riemann-Hurwitz: $\underset{2}{\chi(C)} = n \cdot \underbrace{\chi(\mathbb{P}^1)}_{2} = 2n$

$\Rightarrow n = 1 \Rightarrow K' = \overline{\mathbb{F}}_q(T)$.

5.3. Kummer theory

Thm (Hilbert 90)

Let $L|K$ be a Galois ext. with $Gal(L|K) \cong \mathbb{Z}/n\mathbb{Z}$ generated by σ. Let $a \in L^\times$. Then,

$$Nm_{L|K}(a) = 1 \iff a = \frac{b}{\sigma(b)} \text{ for some } b \in L^\times.$$

Pf "$\Leftarrow$" clear

"$\Rightarrow$" Let $t \in L$

and $b = t + a\sigma(t) + a\sigma(a)\sigma^2(t) + \dots + a\sigma(a)\cdots\sigma^{n-2}(a)\sigma^{n-1}(t)$

$a\sigma(b) = a\sigma(t) + a\sigma(a)\sigma^2(t) + \dots + \dots + \underbrace{a\sigma(a)\cdots\sigma^{n-1}(a)}_{Nm(a)=1}\underbrace{\sigma^n(t)}_{t}$

$\Rightarrow a\sigma(b) = b.$

It remains to choose $t \in L$ so that $b \neq 0$.

But the function $L \longrightarrow L$

$t \longmapsto t + a\sigma(t) + \dots + a\sigma(a)\cdots\sigma^{n-2}(a)\sigma^{n-1}(t)$

is nonzero because the automorphisms $id, \sigma, \dots, \sigma^{n-1}$ of L are linearly independent. $\square$

Cor (Kummer theory)

Let K be a field containing n distinct n-th roots of unity (char $K \nmid n$ and $\zeta_n \in K$). Then, each Gal. ext. $L|K$ with $Gal(L|K) \cong \mathbb{Z}/n\mathbb{Z}$ is of the form

$L = K(\sqrt[n]{c})$ for some $c \in K^\times$.

Ex If char$(K) \neq 2$, the $\mathbb{Z}/2\mathbb{Z}$-ext. are of the form $K(\sqrt{c})$.

Pf $Nm_{L|K}(\zeta_n) = \zeta_n^n = 1$. $\underset{H90}{\Rightarrow} \exists\, b \in L^\times : \zeta_n = \frac{b}{\sigma(b)}$.
$\underset{K}{\wedge}$

$$\Rightarrow 1 = \zeta_n^n = \frac{b^n}{\sigma(b^n)} \Rightarrow \sigma(b^n) = b^n \Rightarrow c := b^n \in K^\times.$$

On the other hand $\sigma^i(b) = \frac{b}{\zeta_n^i} \neq b$ for $i = 1, \dots, n-1$.

$\Rightarrow L = K(b)$. □

5.4. Hilbert symbols

Def Let K be a local field (nonarch. or arch.) containing n distinct n-th roots of unity.

For any $a, b \in K^\times$, define the Hilbert symbol $(a,b)_n \in \mu_n = \{1, \zeta_n, \dots, \zeta_n^{n-1}\} \cong \mathbb{Z}/n\mathbb{Z}$ by

$$\underbrace{\Theta_K(a)}_{\in Gal(K^{ab}|K)}(\sqrt[n]{b}) = (a,b)_n \cdot \sqrt[n]{b}.$$

Rmk $(a,b)_n$ is indep. of the choice of $\sqrt[n]{b}$ because

$$\Theta_K(a)(\zeta_n^i) = \zeta_n^i.$$

Ex $K = \mathbb{R}$, $n = 2 \rightsquigarrow (a,b)_2 = \begin{cases} +1, & a > 0 \text{ or } b > 0 \\ -1, & a < 0 \text{ and } b < 0 \end{cases}$

Ex $K = \mathbb{C}$, any $n \rightsquigarrow (a,b)_n = 1$.

<u>Rmk</u> $(a,b)_n$ is multiplicatively bilinear:

i) $(a_1 a_2, b)_n = (a_1,b)_n \cdot (a_2, b)$

ii) $(a, b_1 b_2)_n = (a,b_1)_n \cdot (a, b_2)$.

<u>Pf</u> Clear from def. $\square$

<u>Rmk</u> $(a,b)_n$ only depends on a, b up to n-th powers in $K^\times$:

i) $(a, b^n)_n = 1$

ii) $(a^n, b)_n = 1$.

<u>Pf</u> $(a,b^n)_n = (a,b)_n^n = 1$

$(a^n,b)_n$ // $\square$

<u>Cor</u> We get a bilinear pairing $(\cdot,\cdot)_n : K^\times/K^{\times n} \times K^\times/K^{\times n} \to \mu_n$.

<u>Rmk</u> $K^\times/K^{\times n}$ is a finite group.

<u>Pf</u> $K^\times \cong \mathcal{O}_K^\times \times \mathbb{Z} \Rightarrow K^\times/K^{\times n} \cong \mathcal{O}_K^\times/\mathcal{O}_K^{\times n} \times \mathbb{Z}/n\mathbb{Z}$

Let $t \in U_K^{(r)} = 1 + \mathfrak{p}_K^r$ for $r \geq 2 v_K(n) + 1$.

$f(X) := X^n - t$.

$v_K(f(1)) = v_K(1-t) \geq r$

$v_K(f'(1)) = v_K(n)$

Hensel (v2) $\Rightarrow$ $f(X)$ has a root in $\mathcal{O}_K^\times$.

$\Rightarrow U_K^{(r)} \subseteq \mathcal{O}_K^{\times n}$.

But $\mathcal{O}_K^\times / U_K^{(r)}$ is finite. $\square$

Rmk $(a,b)_n = 1 \iff a \in \mathrm{Nm}_{L|K}(L^\times)$ where $L = K(\sqrt[n]{b})$.

Pf $(a,b)_n = 1 \iff \Theta_K(a)(\sqrt[n]{b}) = \sqrt[n]{b} \iff \Theta_K(a)|_L = id_L$

$\iff a \in \mathrm{Nm}_{L|K}(L^\times)$.

Prop 1 in section 5.1 : $K^\times / \mathrm{Nm}_{L|K}(L^\times) \xrightarrow[\sim]{\Theta_K} \mathrm{Gal}(L|K)$

□

Cor $(x^n - b, b)_n = 1 \quad \forall x \in K, b \in K^\times$ with $x^n - b \neq 0$.

Pf Let $L = K(\sqrt[n]{b})$.

If $[L:K] = n$, then

$$\mathrm{Nm}_{L|K}(X - \sqrt[n]{b}) = \prod_{i=0}^{n-1} (X - \underbrace{\zeta_n^i \sqrt[n]{b}}_{\text{the conj. of } \sqrt[n]{b}}) = X^n - b.$$

Let $M = K[T]/(T^n - b) = \underbrace{L \times \dots \times L}_{n/[L:K]}$.

$$\mathrm{Nm}_{M|K}(X - T) = X^n - b.$$

Let $X - T = (\alpha_1, \dots, \alpha_r) \in L \times \dots \times L$.

Then, $\mathrm{Nm}_{M|K}(X - T) = \prod_j \mathrm{Nm}_{L|K}(\alpha_j) = \mathrm{Nm}_{L|K}(\prod_j \alpha_j)$.

In other words, if $[L:K] = \frac{n}{r}$, $b = c^r$, then

$$\mathrm{Nm}_{L|K}\left(\prod_{j=0}^{r-1} (X - \zeta_n^j \sqrt[n]{b})\right) = \prod_{j=0}^{r-1} \prod_{k=0}^{\frac{n}{r}-1} (X - \zeta_n^j \zeta_n^{rk} \sqrt[n]{b})$$

$$= \prod_{i=0}^{n} (X - \zeta_n^i \sqrt[n]{b}) = X^n - b.$$

□

Cor i) $(a, 1-a)_n = 1 \quad \forall a \neq 0, 1$

ii) $(a, -a)_n = 1 \quad \forall a \neq 0.$

Pf i) $x = 1, \; b = 1-a$

ii) $x = 0, \; b = -a$ $\square$

Rmk The Hilbert symbol is skew-symmetric:

$$(a,b)_n = (b,a)_n^{-1}.$$

Pf
$$(a,b)_n \cdot (b,a)_n = (a,-a)_n \cdot (a,b)_n \cdot (b,a) \cdot (b,-b)_n$$
$$= (a, -ab)_n \cdot (b, -ab)_n$$
$$= (ab, -ab)_n$$
$$= 1.$$
$\square$

Surprising Cor

$$a \in Nm_{K(\sqrt[n]{b})|K}(K(\sqrt[n]{b})^\times) \iff b \in Nm_{K(\sqrt[n]{a})|K}(K(\sqrt[n]{a})^\times).$$

Rmk The Hilbert symbol $(\cdot,\cdot)_n : K^\times/K^{\times n} \times K^\times/K^{\times n} \to \mu_n$

is nondegenerate:

$$(a,b)_n = 1 \;\; \forall b \in K^\times \iff a \in K^{\times n}$$
$$\Updownarrow$$
$$(b,a)_n = 1 \;\; \forall b \in K^\times$$

Pf "$\Leftarrow$" clear

"$\Rightarrow$" Assume $a \notin K^{\times n}$. $\Rightarrow L = K(\sqrt[n]{a}) \neq K$.

$\Rightarrow \theta_K(b)|_L \neq id_L$ for some $b \in K^\times$

$\Rightarrow (b,a)_n \neq 1$ for some $b \in K^\times$. $\square$

Cor Let $b_1, \dots, b_r \in K^\times$ be representatives of the elements of $K^\times / K^{\times n}$ (or of generators).

Let $L = K(\sqrt[n]{b_1}, \dots, \sqrt[n]{b_r}) = K(\sqrt[n]{K^\times})$ (This is the max. ab. ext. of K s.t. $\sigma^n = id \quad \forall \sigma \in Gal(L|K)$.)

Then, $Nm_{L|K}(L^\times) = K^{\times n}$.

Pf $Gal(K^{ab}|L) = \bigcap_{i=1}^{r} Gal(K^{ab} | K(\sqrt[n]{b_i}))$

$$\underset{\text{Prop 1}}{\Longrightarrow} Nm_{L|K}(L^\times) = \bigcap_i Nm_{K(\sqrt[n]{b_i})|K}(K(\sqrt[n]{b_i})^\times)$$

$$= \bigcap_i \{ a \in K^\times \mid (a, b_i) = 1 \}$$

$$\underset{\text{nondegeneracy}}{=} K^{\times n}. \qquad \square$$

Thm Let K be a nonarch. with residue field $\mathbb{F}_q$.

Assume char $\mathbb{F}_q \nmid n$. ($\Leftrightarrow \mathfrak{p}_K \nmid n$).

Then,
$$(a,b)_n \equiv \left((-1)^{v_K(a) v_K(b)} \cdot \frac{b^{v_K(a)}}{a^{v_K(b)}} \right)^{\frac{q-1}{n}} \mod \mathfrak{p}_K.$$

Rmk Since $\zeta_n \in K$ and char $\mathbb{F}_q \nmid n$,
$\mathbb{F}_q$ contains n distinct n-th roots of unity. $\Rightarrow n \mid q-1$.

The congruence mod $\mathfrak{p}_K$ therefore uniquely determines the n-th root of unity $(a,b) \in K^\times$.