Uchida's theorem for one-dimensional function fields over finite fields

Koichiro Sawada

Research Institute for Mathematical Sciences, Kyoto University

2016/07/18

Theorem (Uchida) (cf. [Uchida] Isomorphisms of Galois groups of algebraic function fields)

Let K: one-dim function field/finite field,
Ω: solvably closed Galois ext. of K
(i.e., Gal. ext. of K which has no nontriv. abelian ext.)

Then K can be reconstructed from $\mathrm{Gal}(\Omega/K)$.

§1 Local theory

In this section, let k: local field of char. $p > 0$.
Write $G_k = \mathrm{Gal}(k^{\mathrm{sep}}/k)$.

Let us reconstruct the multiplicative structure of $k^\times$, together with various objects arising from k.

Notation

$\mathcal{O}_k \subset k$: ring of integers

$\mathcal{O}_k^{\triangleright} := \mathcal{O}_k \setminus \{0\}$: multiplicative monoid of nonzero integers

$U_k^{(1)}$: multiplicative group of principal units

$I_k \subset G_k$: inertia subgroup

$P_k \subset I_k$: wild inertia subgroup

κ: residue field of k

$\mathrm{Frob}_\kappa \in \mathrm{Gal}(\overline{\kappa}/\kappa)$: Frobenius element

- (local class field theory)

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{O}_k^\times & \longrightarrow & (k^\times)^\wedge & \longrightarrow & \hat{\mathbb{Z}} & \longrightarrow & 1 \\ & & \downarrow \wr & & \downarrow \wr & & \downarrow \wr & & \\ 1 & \longrightarrow & \mathrm{Im}(I_k \to G_k^{\mathrm{ab}}) & \longrightarrow & G_k^{\mathrm{ab}} & \longrightarrow & G_k/I_k & \longrightarrow & 1, \end{array}$$

where the right-hand arrow maps

$$\hat{\mathbb{Z}} \ni 1 \mapsto \mathrm{Frob}_\kappa \in \mathrm{Gal}(\overline{\kappa}/\kappa) \overset{\sim}{\leftarrow} G_k/I_k$$

- $k^\times \cong \langle \pi \rangle \times \mathcal{O}_k^\times \cong \langle \pi \rangle \times (k^\times)_{\mathrm{tor}} \times U_k^{(1)}$

Local reconstruction

- p: unique prime number l s.t.

$$l \mid \sharp\kappa = \sharp(k^\times)_{\mathrm{tor}} + 1 = \sharp(G_k^{\mathrm{ab}})_{\mathrm{tor}} + 1$$

- $f_k := [\kappa : \mathbb{F}_p] = \log_p(\sharp(G_k^{\mathrm{ab}})_{\mathrm{tor}} + 1)$
- $I_k = \bigcap_{k' \subset k^{\mathrm{sep}},\ k'/k:\ \mathrm{fin.\ unr.}} G_{k'}$

$$\begin{aligned} k'/k\text{: unr} &\Leftrightarrow [k' : k] = [\kappa' : \kappa] \\ &\Leftrightarrow [G_k : G_{k'}] = f_{k'}/f_k \end{aligned}$$

- P_k: unique Sylow pro-p-subgroup of I_k
- $\mathrm{Frob}_\kappa \in \mathrm{Gal}(\overline{\kappa}/\kappa) \xleftarrow{\sim} G_k/I_k$: unique element of G_k/I_k which acts by conjugation on I_k/P_k by p^{f_k}

- $\mathrm{Im}(\mathcal{O}_k^\times \hookrightarrow k^\times \hookrightarrow G_k^{\mathrm{ab}}) = \mathrm{Im}(I_k \to G_k^{\mathrm{ab}})$
- $\mathrm{Im}(k^\times \hookrightarrow G_k^{\mathrm{ab}})$: subgp of G_k^{ab} gen. by $\mathrm{Im}(\mathcal{O}_k^\times \hookrightarrow G_k^{\mathrm{ab}})$ and (a lifting of) Frob_κ (in G_k^{ab})
- $\mathrm{Im}(\mathcal{O}_k^\triangleright \hookrightarrow k^\times \hookrightarrow G_k^{\mathrm{ab}})$: submonoid of G_k^{ab} gen. by $\mathrm{Im}(\mathcal{O}_k^\times \hookrightarrow G_k^{\mathrm{ab}})$ and (a lifting of) Frob_κ (in G_k^{ab})
- $U_k^{(1)}$: unique Sylow pro-p-subgroup of $\mathcal{O}_k^\times$
- $\mathcal{O}_k^\times \hookrightarrow \mathcal{O}_k \twoheadrightarrow \kappa \supset \kappa^\times$ induce isoms of groups $(\mathcal{O}_k^\times)_{\mathrm{tor}} \xrightarrow{\sim} \mathcal{O}_k^\times / U_k^{(1)} \xrightarrow{\sim} \kappa^\times$ (which determine an isom of fields $(k \supset)$ $(\mathcal{O}_k^\times)_{\mathrm{tor}} \cup \{0\} \xrightarrow{\sim} \kappa$)

§2 Reconstruction of the multiplicative structure (global case)

In the rest of this talk, let

K: one-dim function field/fin. field of char. $p > 0$,

Ω: solvably closed Gal. ext. of K.

Write $G := \mathrm{Gal}(\Omega/K)$.

Local $\Rightarrow$ Global

$\mathcal{V}_\Omega$: set of all (nonarchimedean) places of Ω

$\mathcal{V}_K$: set of all (nonarchimedean) places of K

$\tilde{\mathcal{V}}$: set of all maximal closed subgps of G which are isom to the abs. Gal. group of a local field ($G \overset{\text{conj.}}{\curvearrowright} \tilde{\mathcal{V}}$)

Then

$\mathcal{V}_\Omega \ni w \mapsto D_w \in \tilde{\mathcal{V}}$: bij, $\mathcal{V}_K \to \tilde{\mathcal{V}}/G$: bij

(by Neukirch's work, i.e., by considering local and global Brauer groups "$\approx$" H^2(Gal. group))

$J = \varinjlim_{S \subset \mathcal{V}_K\text{: fin. subset}} (\prod_{v \in S} K_v^\times) \times (\prod_{v \in \mathcal{V}_K \setminus S} \mathcal{O}_{K_v}^\times)$
: idèle group

$J \to G^{\mathrm{ab}}$ is determined by $K_v^\times \hookrightarrow D_v^{\mathrm{ab}} \to G^{\mathrm{ab}}$

$\Rightarrow K^\times = \ker(J \to G^{\mathrm{ab}})$ (global class field theory)

Write $U_v^{(1)},\ \mathcal{O}_v^\times,\ \mathcal{O}_v^\triangleright \subset K^\times$: inv. image of $U_{K_v}^{(1)},\ \mathcal{O}_{K_v}^\times,\ \mathcal{O}_{K_v}^\triangleright \subset K_v^\times$ by $K^\times \hookrightarrow J \to K_v^\times$

Order

$a \in K^\times,\ v \in \mathcal{V}_K,\ n \in \mathbb{Z}$

Write

- $\mathrm{ord}_v(a) := 1$ if $\mathcal{O}_v^{\triangleright}$ is gen. by $\mathcal{O}_v^\times$ and a as monoid
- $\mathrm{ord}_v(a) := n$ if $\exists b \in K^\times$ s.t. $\mathrm{ord}_v(b) = 1$ and
$$a \cdot b^{-n} \in \mathcal{O}_v^\times$$

(well-defined)

Evaluation

$v \in \mathcal{V}_K,\ \ s \in \mathcal{O}_v^{\triangleright}$

$\kappa_v = \kappa_v^{\times} \cup \{0\}$: residue field of K at v

Let us define $s(v) \in \kappa_v$ as follows:

- if $s \in \mathcal{O}_v^{\times}$, then $s(v)$: image of s by $\mathcal{O}_v^{\times} \twoheadrightarrow \mathcal{O}_v^{\times}/U_v^{(1)} \cong \kappa_v^{\times} \hookrightarrow \kappa_v$
- if $s \notin \mathcal{O}_v^{\times}$, then $s(v) := 0$

§3 Additive structure

We want to reconstruct the add. str. of $K = K^\times \cup \{0\}$.

First, we reconstruct the add. str. of residue fields.

Write F: constant field of K

Then

- $F^\times = \bigcap_{v \in \mathcal{V}_K} \mathcal{O}_v^\times$
- p: unique prime number l s.t. $l \mid \sharp F^\times + 1$
- $-1 \in K^\times$: if $p \neq 2$, then -1: unique element
  $a \in K^\times$ s.t. $a^2 = 1$ and $a \neq 1$
  if $p = 2$, then $-1 = 1$

Write $\tilde{K} = K \otimes_F \overline{F}$

$\Rightarrow 1 \to \mathrm{Gal}(\Omega/\tilde{K}) \to G \to G_F \to 1$: exact

Let $H \subset G$: open subgp. Then

$$H \supset \ker(G \twoheadrightarrow G_F) = \mathrm{Gal}(\Omega/\tilde{K}) \Leftrightarrow [G : H] = [F_H : F] = \log_{\sharp F}(\sharp F_H)$$

(in this case, H corresponds to $K \otimes_F F_H$)

By taking limit for such H's, we obtain the following data $(\tilde{K}^\times \cup \{0\},\ \mathcal{V}_{\tilde{K}},\ \{\mathrm{ord}_v\}_{v \in \mathcal{V}_{\tilde{K}}},\ \{\mathcal{O}_v^{\triangleright} \to \kappa_v\}_{v \in \mathcal{V}_{\tilde{K}}})$

(Note: $K = (\tilde{K})^G$)

Divisor

$\mathrm{Div} := \bigoplus_{v \in \mathcal{V}_{\tilde{K}}} \mathbb{Z} \cdot v$

Let $D = \sum_{v \in \mathcal{V}_{\tilde{K}}} n_v \cdot v \in \mathrm{Div}$
($n_v = 0$ for all but finitely many v)

Then

- $H^0(D)$
  $= \{s \in \tilde{K}^\times \mid \mathrm{ord}_v(s) + n_v \geq 0 \ (\forall v \in \mathcal{V}_{\tilde{K}})\} \cup \{0\}$
- $l(D) = \min\{n \in \mathbb{Z}_{\geq 0} \mid \exists v_1, \ldots, v_n \in \mathcal{V}_{\tilde{K}} \text{ s.t. } H^0(D - v_1 - \cdots - v_n) = \{0\}\}$

Additive structure of residue fields

Let us fix $v \in \mathcal{V}_{\tilde{K}}$ and reconstruct the add. str. of κ_v

$\exists D = \sum_{w \in \mathcal{V}_{\tilde{K}}} n_w \cdot w \in \mathrm{Div},\ \exists w_1, w_2 \in \mathcal{V}_{\tilde{K}}$ s.t.
v, w_1, w_2: distinct, $n_v = n_{w_1} = n_{w_2} = 0$, $l(D) = 2$,
$l(D - v - w_1) = l(D - v - w_2) = l(D - w_1 - w_2) = 0$

Let $\zeta, \lambda \in \kappa_v^\times$ s.t. $\zeta \neq (-1) \cdot \lambda$

$\exists!\ s \in H^0(D)$ s.t. $s(v) = \zeta,\ s(w_1) = 0,\ s(w_2) \neq 0$
$\exists!\ t \in H^0(D)$ s.t. $t(v) = \lambda,\ t(w_1) \neq 0,\ t(w_2) = 0$
$\exists!\ u \in H^0(D)$ s.t. $u(w_1) = t(w_1),\ u(w_2) = s(w_2)$

$\Rightarrow \zeta + \lambda = u(v)$ (since u coincides with $s + t$)

Additive structure of $\tilde{K}$

Let $x, y \in \tilde{K}$

- if $x = 0$, then $x + y := y$
- if $y = 0$, then $x + y := x$
- if $x = (-1) \cdot y$, then $x + y := 0$
- if $x \neq 0,\ y \neq 0,\ x \neq (-1) \cdot y$, then
  $x + y$: unique element $z \in \tilde{K}^{\times}$ which satisfies the following condition:
  for infinitely many $v \in \mathcal{V}_{\tilde{K}}$ s.t. $x, y, z \in \mathcal{O}_v^{\times}$,
  it holds that $x(v) + y(v) = z(v)$

Remark

The Frobenius homomorphism $\mathrm{Frob}\colon K \to K$ (which is not an isomorphism!) determines an isomorphism $G_{\mathrm{Frob}}\colon G \xleftarrow{\sim} G$.

$$\begin{array}{ccc} K(G) & \xleftarrow[K(G_{\mathrm{Frob}})]{\sim} & K(G) \\ \uparrow\wr & \not\circlearrowright & \uparrow\wr \\ K & \xrightarrow[\mathrm{Frob}]{\not\sim} & K \end{array}$$