Mono-anabelian Reconstruction of Number Fields

Yuichiro Hoshi

RIMS

2014/07/09

§1 Mono-anabelian Reconstruction of Number Fields

Question: Can one reconstruct a number field [i.e., a finite extension of $\mathbb{Q}$] from the associated absolute Galois group?

Definition

For a topological group G,

G: of NF-type

$\stackrel{\text{def}}{\Leftrightarrow}$ $G \cong$ the abs. Gal. gp of a number field

Theorem [Neukirch-Uchida]

$\Box \in \{\circ, \bullet\}$

$F_\Box$: a global field [i.e., a fin. ext. of $\mathbb{Q}$ or $\mathbb{F}_p(t)$]

$\overline{F}_\Box$: a separable closure of $F_\Box$

$G_{F_\Box} \stackrel{\mathrm{def}}{=} \mathrm{Gal}(\overline{F}_\Box / F_\Box)$

$\Longrightarrow$ The natural map

$$\mathrm{Isom}(\overline{F}_\circ / F_\circ, \overline{F}_\bullet / F_\bullet) \longrightarrow \mathrm{Isom}(G_{F_\bullet}, G_{F_\circ})$$

is bijective.

In particular, $F_\circ \cong F_\bullet \Longleftrightarrow G_{F_\circ} \cong G_{F_\bullet}$.

Mochizuki's Mono-anabelian Philosophy

Give a(n) [functorial "group-theoretic"] algorithm

$$G_F \quad \rightsquigarrow \quad \overline{F}/F.$$

A "reconstruction" as in Theorem [N-U] is called "<u>bi-anabelian reconstruction</u>".

In the case where

- $\mathrm{char}(F_\square) > 0$, the proof $\Rightarrow$ mono-anab'n rec'n,
- $\mathrm{char}(F_\square) = 0$, the proof $\not\Rightarrow$ mono-anab'n rec'n.

Rough Statement of Main Theorem

$\exists$A functorial "group-theoretic" algorithm

G : of NF-type

$\rightsquigarrow \quad \overline{F}(G)$: an algebraically closed field $\curvearrowleft \quad G$

which satisfies certain conditions.

E.g., every $G \xrightarrow{\sim} \mathrm{Gal}(\overline{F}/F)$ determines

$$(\overline{F}(G) \curvearrowleft G) \xrightarrow{\sim} (\overline{F} \curvearrowleft \mathrm{Gal}(\overline{F}/F)).$$

Notation

F: a number field

$\mathcal{O}_F \subseteq F$: the ring of integers of F

$\mathcal{V}_F$: the set of nonarchimedean primes of F

If $v \in \mathcal{V}_F$, then

$\mathcal{O}_{(v)} \subseteq F$: the localization of $\mathcal{O}_F$ at v

$\mathfrak{m}_{(v)} \subseteq \mathcal{O}_{(v)}$: the maximal ideal of $\mathcal{O}_{(v)}$

$\kappa(v) \stackrel{\mathrm{def}}{=} \mathcal{O}_{(v)}/\mathfrak{m}_{(v)}$: the residue field at v

$U_{(v)} \stackrel{\mathrm{def}}{=} 1 + \mathfrak{m}_{(v)} \subseteq \mathcal{O}_{(v)}^{\times}$

$\mathrm{ord}_v \colon F^{\times} \twoheadrightarrow \mathbb{Z}$: the surjective valuation at v

"Outline" of the Proof

$G_F \stackrel{\mathrm{def}}{=} \mathrm{Gal}(\overline{F}/F)$

(a) By Neukirch's work,

$$G_F \rightsquigarrow G_F \curvearrowright \mathcal{V}_{\overline{F}} \stackrel{\mathrm{def}}{=} \{\,\text{nonarch. primes of } \overline{F}\,\}$$
$$\rightsquigarrow \mathcal{V}_F \cong \mathcal{V}_{\overline{F}}/G_F.$$

(b) By Class Field Theory + Local Rec'n Results, the multiplicative groups $F^{\times} \subseteq \prod_{v \in \mathcal{V}_F} F_v^{\times}$, where F_v is the completion of F at v.

$\rightsquigarrow \ \mathcal{M}_F \stackrel{\mathrm{def}}{=} (F, \mathcal{O}_F, \mathcal{V}_F, \{U_{(v)}\}_{v \in \mathcal{V}_F})$, where

- the monoid F with respect to "$\times$",
- the submonoid $\mathcal{O}_F \subseteq F$,
- the set $\mathcal{V}_F$, and
- the subgroups $U_{(v)} \subseteq F$ for $v \in \mathcal{V}_F$.

(c) $\mathcal{M}_F \stackrel{\S 2}{\rightsquigarrow}$ "$+$" of F,

i.e., the field structure of F. $\square$

§2 Mono-anabelian Reconstruction of the Additive Structures of Number Fields

Theorem (= Uchida's Lemma for Number Fields)

$\exists$A functorial algorithm for reconstructing from

[a collection of data which is isomorphic to]

$$\mathcal{M}_F \stackrel{\mathrm{def}}{=} (F, \mathcal{O}_F, \mathcal{V}_F, \{U_{(v)}\}_{v \in \mathcal{V}_F})$$

[the map corresponding to]

the additive structure of F

$$F \times F \longrightarrow F; \quad (a, b) \mapsto a + b.$$

§2.1 The General Case I

(1) $0 \in F$: the unique $a \in F$ s.t. $ax = a$ $(\forall x \in F)$

$\Rightarrow$ $F^{\times} = F \setminus \{0\}$, $\mathcal{O}_F^{\triangleright} = \mathcal{O}_F \setminus \{0\}$

(2) $1 \in F$: the unique $a \in F$ s.t. $ax = x$ $(\forall x \in F)$

(3) $-1 \in F$: the unique $a \in F$ s.t. $a \neq 1$ but $a^2 = 1$

$v \in \mathcal{V}_F$

$$
\begin{tikzcd}
 & & 1 \arrow[d] & 1 \arrow[d] & \\
1 \arrow[r] & U_{(v)} \arrow[r] \arrow[d, equal] & \mathcal{O}_{(v)}^{\times} \arrow[r] \arrow[d] & \kappa(v)^{\times} \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & U_{(v)} \arrow[r] & F^{\times} \arrow[r] \arrow[d, "\mathrm{ord}_v"'] & F^{\times}/U_{(v)} \arrow[r] \arrow[d] & 1 \\
 & & \mathbb{Z} \arrow[r, equal] \arrow[d] & \mathbb{Z} \arrow[d] & \\
 & & 1 & 1 &
\end{tikzcd}
$$

(4) $\kappa(v)^\times = (F^\times / U_{(v)})_{\mathrm{tor}}$
$\Rightarrow \ \kappa(v) = \kappa(v)^\times \sqcup \{0\}$

(5) $\mathrm{char}(\kappa(v))$: the unique prime p s.t. $p | \sharp\kappa(v)$

(6) the $\{\pm 1\}$-orbit of ord_v

$$= \left\{ F^\times \twoheadrightarrow F^\times / U_{(v)} \twoheadrightarrow (F^\times / U_{(v)})/\kappa(v)^\times \overset{\pm 1}{\cong} \mathbb{Z} \right\}$$

(7) ord_v: the unique element of this orbit which maps $\mathcal{O}_F^\triangleright \subseteq F^\times$ to $\mathbb{Z}_{\geq 0} \subseteq \mathbb{Z}$

(8) For $a \in F^{\times}$,

$$\mathrm{Supp}(a) \stackrel{\mathrm{def}}{=} \{ v \in \mathcal{V}_F \mid \mathrm{ord}_v(a) \neq 0 \} \subseteq \mathcal{V}_F$$

(9) $\mathcal{O}_{(v)}^{\times} = \mathrm{Ker}(\mathrm{ord}_v)$

(10) $\mathcal{O}_{(v)}^{\times} \twoheadrightarrow \kappa(v)^{\times}$ as $\mathcal{O}_{(v)}^{\times} \twoheadrightarrow \mathcal{O}_{(v)}^{\times}/U_{(v)}$

$(\subseteq F^{\times}/U_{(v)})$

§2.2 In the Case of $\mathbb{Q}$

Suppose that $F = \mathbb{Q}$.

(11) $2\mathbb{Z}$ (resp. $3\mathbb{Z}$; $5\mathbb{Z}$) $\in \mathcal{V}_F$: the unique $v \in \mathcal{V}_F$ s.t. $\mathrm{char}(\kappa(v)) = 2$ (resp. 3; 5)

(12) $2 \in \mathcal{O}_F^{\triangleright}$: the unique $a \in \mathcal{O}_F^{\triangleright}$ s.t. $\mathrm{Supp}(a) = \{2\mathbb{Z}\}$, $\mathrm{ord}_{2\mathbb{Z}}(a) = 1$, $a \notin U_{(3\mathbb{Z})}$

(13) $-2 = (-1) \cdot 2 \in \mathcal{O}_F^{\triangleright}$

(14) $3 \in \mathcal{O}_F^{\triangleright}$: the unique $a \in \mathcal{O}_F^{\triangleright}$ s.t.

$$\mathrm{Supp}(a) = \{3\mathbb{Z}\},\ \mathrm{ord}_{3\mathbb{Z}}(a) = 1,\ 2 \cdot a \in U_{(5\mathbb{Z})}$$

$$a \in \mathcal{O}_F \setminus \{-2, -1, 0, 1, 2\}$$

(15) $\{a-1, a+1\}$

$$= \{\, b \in \mathcal{O}_F^{\triangleright} \mid \mathrm{Supp}(a) \cap \mathrm{Supp}(b) = \emptyset,\ a \cdot b^{-1} \notin U_{(v)}\ (\forall v \in \mathcal{V}_F) \,\} \subseteq \mathcal{O}_F^{\triangleright}$$

Note: $a \cdot b^{-1} \in U_{(p\mathbb{Z})}$ "$\Leftrightarrow$" $a \cdot b^{-1} \equiv 1 \bmod p$ "$\Leftrightarrow$" $a \equiv b \bmod p$ "$\Leftrightarrow$" $p | a - b$

(16) Suppose: $\mathrm{Supp}(a) \not\subseteq \{2\mathbb{Z}\}$

$a + 1 \in \mathcal{O}_F^{\triangleright}$: the unique $b \in \{a-1, a+1\}$

s.t. $b \in U_{(v)}$ $(\forall v \in \mathrm{Supp}(a))$

(17) Suppose: $\mathrm{Supp}(a) \subseteq \{2\mathbb{Z}\}$

$(\Rightarrow a$: even $\Rightarrow \mathrm{Supp}(a \pm 1) \not\subseteq \{2\mathbb{Z}\})$

$a + 1 \in \mathcal{O}_F^{\triangleright}$: the unique $b \in \{a-1, a+1\}$

s.t. $a \neq b + 1$

(18) $a \in \mathcal{O}_F$

$$\mathrm{Next}(a) \stackrel{\mathrm{def}}{=} \begin{cases} -1 & a = -2 \\ 0 & a = -1 \\ 1 & a = 0 \\ 2 & a = 1 \\ 3 & a = 2 \\ a+1 & a \notin \{-2, -1, 0, 1, 2\} \end{cases}$$

$\Rightarrow$ $\mathrm{Next}\colon \mathcal{O}_F \to \mathcal{O}_F$: a bijection

(19) The map $\mathcal{O}_F \times \mathcal{O}_F \to \mathcal{O}_F$; $(a, b) \mapsto a + b$ by the bijection Next

(We omit the proof.)

(20) For $v \in \mathcal{V}_F$,
the map $\kappa(v) \times \kappa(v) \to \kappa(v)$; $(\overline{a}, \overline{b}) \mapsto \overline{a} + \overline{b}$ by

$$\overline{a} + \overline{b} = \overline{a + b}$$

§2.3 The General Case II

(21) $$\mathbb{Q}^\times = \{\, a \in F^\times \mid a^{\mathrm{char}(\kappa(v))-1} \in U_{(v)} \text{ for all but finitely many } v \in \mathcal{V}_F \,\}$$

(by Chebotarev's density theorem)

(22) $\mathbb{Q} = \mathbb{Q}^\times \sqcup \{0\}, \ \mathbb{Z} = \mathbb{Q} \cap \mathcal{O}_F$

(23) $\mathcal{V}_\mathbb{Q} = \mathcal{V}_F / \sim,$

where $v \sim w \overset{\mathrm{def}}{\Leftrightarrow} \mathrm{char}(\kappa(v)) = \mathrm{char}(\kappa(w))$

(24) For $\overline{v} \in \mathcal{V}_\mathbb{Q}$, $U_{(\overline{v})} = \mathbb{Q} \cap U_{(v)}$

$$\Rightarrow \mathcal{M}_{\mathbb{Q}} = (\mathbb{Q},\ \mathbb{Z},\ \mathcal{V}_{\mathbb{Q}},\ \{U_{(\overline{v})}\}_{\overline{v} \in \mathcal{V}_{\mathbb{Q}}})$$

$\overset{\S 2.2}{\Rightarrow}$ The add. str. of $\kappa(\overline{v})$ ($\forall \overline{v} \in \mathcal{V}_{\mathbb{Q}}$),
i.e., the add. str. of $\kappa(v)$ for $\forall v \in \mathcal{V}_F$
s.t. $\sharp\kappa(v) = \mathrm{char}(\kappa(v))$

Recall: $\exists\infty\ v \in \mathcal{V}_F$ s.t. $\sharp\kappa(v) = \mathrm{char}(\kappa(v))$
(by Chebotarev's density theorem)

(25) $a,\ b \in F$

- $a = 0 \ \Rightarrow \ a + b = b$
- $b = 0 \ \Rightarrow \ a + b = a$
- $a \cdot b^{-1} = -1 \ \Rightarrow \ a + b = 0$
- otherwise $\ \Rightarrow \ a + b \in F^{\times}$:

the unique $c \in F^{\times}$ which satisfies the following:
For infinitely many $v \in \mathcal{V}_F$

s.t. $\sharp\kappa(v) = \mathrm{char}(\kappa(v))$; $a,\ b,\ c \in \mathcal{O}^{\times}_{(v)}$,

$\overline{a} + \overline{b} = \overline{c}$ in $\kappa(v)$