Reconstruction of a Number Field from the Absolute Galois Group

Yuichiro Hoshi

RIMS

2014/03/11

§1 Introduction

Naive Question: Can one reconstruct an NF from its absolute Galois group?

Convention

F: an NF $\overset{\text{def}}{\Leftrightarrow}$ $[F : \mathbb{Q}] < \infty$

k: an MLF $\overset{\text{def}}{\Leftrightarrow}$ $[k : \mathbb{Q}_p] < \infty$ for some p

For a profinite group G,

G: of NF-type (resp. of MLF-type)

$\overset{\text{def}}{\Leftrightarrow}$ $G \simeq$ the abs. Gal. gp of an NF (resp. MLF).

Theorem [Neukirch-Uchida]

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

$F_\square$: a global field

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

$G_{F_\square} \overset{\text{def}}{=} \mathrm{Gal}(\overline{F}_\square / F_\square)$

$\Longrightarrow$ The natural map

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

is bijective.

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

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

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

which satisfies certain conditions.

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

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

§2 Review of the Local Theory

k: an MLF

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

$\mathfrak{m}_k \subseteq \mathcal{O}_k$: the maximal ideal

$\mathcal{O}_k^{\triangleright} \stackrel{\mathrm{def}}{=} \mathcal{O}_k \setminus \{0\} \subseteq k^{\times}$ [submonoid]

$\underline{k} \stackrel{\mathrm{def}}{=} \mathcal{O}_k/\mathfrak{m}_k$: the residue field

$\overline{k}$: an algebraic closure of k

$G_k \stackrel{\mathrm{def}}{=} \mathrm{Gal}(\overline{k}/k)$

$P_k \subseteq I_k \subseteq G_k$: the wild inertia, inertia subgps

Proposition

(i) [Local Class Field Theory]

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{Im}(I_k \to G_k^{\mathrm{ab}}) \arrow[r] \arrow[d, "\wr"] & G_k^{\mathrm{ab}} \arrow[r] \arrow[d, "\wr"] & G_k/I_k \arrow[r] \arrow[d, "\wr"] & 1 \\
1 \arrow[r] & \mathcal{O}_k^\times \arrow[r] & (k^\times)^\wedge \arrow[r] & \widehat{\mathbb{Z}} \arrow[r] & 1 \\
1 \arrow[r] & \mathcal{O}_k^\times \arrow[r] \arrow[u, equal] & k^\times \arrow[r] \arrow[u, "\cup"'] & \mathbb{Z} \arrow[r] \arrow[u, "\cup"'] & 1
\end{tikzcd}$$

— where the right-hand upper vertical arrow maps $\mathrm{Frob}_{\underline{k}} \in G_k/I_k$ to $1 \in \widehat{\mathbb{Z}}$.

(ii)
$\{\mathrm{char}(\underline{k})\} = \{\, l : \text{prime} \mid \dim_{\mathbb{Q}_l}(G_k^{\mathrm{ab}} \otimes_{\widehat{\mathbb{Z}}} \mathbb{Q}_l) \geq 2 \,\}$

Write $p \stackrel{\mathrm{def}}{=} \mathrm{char}(\underline{k})$.

(iii) $d_k \stackrel{\mathrm{def}}{=} [k : \mathbb{Q}_p] = \dim_{\mathbb{Q}_p}(G_k^{\mathrm{ab}} \otimes_{\widehat{\mathbb{Z}}} \mathbb{Q}_p) - 1$

(iv) $f_k \stackrel{\mathrm{def}}{=} [\underline{k} : \mathbb{F}_p] = \log_p(\sharp(G_k^{\mathrm{ab}})_{\mathrm{tor}}^{(p')} + 1)$

(v) $I_k = \bigcap_{K/k\text{: fin. s.t. } d_K/f_K = d_k/f_k} G_K$

(vi) $P_k \subseteq I_k$: the unique pro-p-Sylow subgroup

(vii) $\{\, \mathrm{Frob}_{\underline{k}} \in G_k/I_k \,\}$
$= \{\, \gamma \in G_k/I_k \mid \gamma \text{ acts on } I_k/P_k \text{ by } p^{f_k} \,\}$

(viii) $U_k^{(1)} \overset{\mathrm{def}}{=} 1 + \mathfrak{m}_k \subseteq \mathcal{O}_k^\times$: unique pro-$p$-Sylow

(ix) $\overline{k}^\times = \varinjlim_{K/k\text{: fin.}} K^\times$

(x) $\Lambda(\overline{k}) \overset{\mathrm{def}}{=}$ "$\widehat{\mathbb{Z}}(1)$" $= \varprojlim_n \overline{k}^\times[n]$

(xi) $1 \to \overline{k}^\times[n] \to \overline{k}^\times \xrightarrow{n} \overline{k}^\times \to 1 \quad \curvearrowleft \quad G_k$

induces an <u>injection</u>

$$\mathrm{Kmm}_k\colon \; k^\times \hookrightarrow H^1(G_k, \Lambda(\overline{k})).$$

Definition

G: of MLF-type

(i) $p(G)$: [unique] prime l

s.t. $\dim_{\mathbb{Q}_l}(G^{\mathrm{ab}} \otimes_{\widehat{\mathbb{Z}}} \mathbb{Q}_l) \geq 2$

(ii) $d(G) \stackrel{\mathrm{def}}{=} \dim_{\mathbb{Q}_{p(G)}}(G^{\mathrm{ab}} \otimes_{\widehat{\mathbb{Z}}} \mathbb{Q}_{p(G)}) - 1$

(iii) $f(G) \stackrel{\mathrm{def}}{=} \log_{p(G)}(\sharp(G^{\mathrm{ab}})_{\mathrm{tor}}^{(p(G)')} + 1)$

(iv) $I(G) \stackrel{\mathrm{def}}{=} \bigcap_{G^\dagger \subseteq G\text{: open s.t. } \frac{d(G^\dagger)}{f(G^\dagger)} = \frac{d(G)}{f(G)}} G^\dagger$

(v) $P(G) \subseteq I(G)$: [unique] pro-$p(G)$-Sylow

(vi) $\mathrm{Frob}(G) \in G/I(G)$: unique elem't $\in G/I(G)$

which acts on $I(G)/P(G)$ by $p(G)^{f(G)}$

(vii) $k^{\times}(G) \stackrel{\mathrm{def}}{=} G^{\mathrm{ab}} \times_{G/I(G)} \mathrm{Frob}(G)^{\mathbb{Z}} \subseteq G^{\mathrm{ab}}$

(viii) $\mathcal{O}^{\triangleright}(G) \stackrel{\mathrm{def}}{=} G^{\mathrm{ab}} \times_{G/I(G)} \mathrm{Frob}(G)^{\mathbb{N}} \subseteq k^{\times}(G)$

(ix) $\mathcal{O}^{\times}(G) \stackrel{\mathrm{def}}{=} \mathrm{Im}(I(G) \to G^{\mathrm{ab}}) \subseteq \mathcal{O}^{\triangleright}(G)$

(x) $U^{(1)}(G) \subseteq \mathcal{O}^{\times}(G)$: [unique] pro-$p(G)$-Sylow

(xi) $\overline{k}^{\times}(G) \stackrel{\mathrm{def}}{=} \varinjlim_{G^{\dagger} \subseteq G\text{: open}} k^{\times}(G^{\dagger})$

$\overline{k}(G) \stackrel{\mathrm{def}}{=} \overline{k}^{\times}(G) \sqcup \{*_G\}$ [monoid]

$\Lambda(G) \stackrel{\mathrm{def}}{=} \varprojlim_n \overline{k}^{\times}(G)[n] \quad \stackrel{\text{conj.}}{\curvearrowleft} G$

(xii) $\mathrm{Kmm}(G)$: $k^{\times}(G) \hookrightarrow H^1(G, \Lambda(G))$:

<u>injection</u> induced by

$1 \to \overline{k}^{\times}(G)[n] \to \overline{k}^{\times}(G) \xrightarrow{n} \overline{k}^{\times}(G) \to 1 \quad \stackrel{\text{conj.}}{\curvearrowleft} \quad G$

Theorem

$\alpha\colon G_k \xrightarrow{\sim} G$: an isomorphism

(i) $\mathrm{char}(\underline{k}) = p(G)$, $d_k = d(G)$, $f_k = f(G)$.

(ii) α determines a commutative diagram

$$\begin{tikzcd} P_k \arrow[r, "\subset"] \arrow[d, "\wr"'] & I_k \arrow[r, "\subset"] \arrow[d, "\wr"'] & G_k \arrow[d, "\wr"', "\alpha"] \\ P(G) \arrow[r, "\subset"] & I(G) \arrow[r, "\subset"] & G; \end{tikzcd}$$

moreover, $G_k/I_k \xrightarrow{\sim} G/I(G)$ maps

$\mathrm{Frob}_{\underline{k}}$ to $\mathrm{Frob}(G)$.

(iii) α determines a commutative diagram

$$
\begin{tikzcd}
U_k^{(1)} \arrow[r, "\subset"] \arrow[d, "\wr"'] & \mathcal{O}_k^{\times} \arrow[r, "\subset"] \arrow[d, "\wr"'] & \mathcal{O}_k^{\triangleright} \arrow[r, "\subset"] \arrow[d, "\wr"'] & k^{\times} \arrow[d, "\wr"'] \\
U^{(1)}(G) \arrow[r, "\subset"] & \mathcal{O}^{\times}(G) \arrow[r, "\subset"] & \mathcal{O}^{\triangleright}(G) \arrow[r, "\subset"] & k^{\times}(G).
\end{tikzcd}
$$

(iv) α determines (G_k, G)-equiv't isomorphisms

$$\overline{k}^{\times} \xrightarrow{\sim} \overline{k}^{\times}(G), \quad \overline{k} \xrightarrow{\sim} \overline{k}(G),$$

$$\Lambda(\overline{k}) \xrightarrow{\sim} \Lambda(G).$$

(v)
$k^\times \xrightarrow{\sim} k^\times(G)$ of (iii) and $\Lambda(\overline{k}) \xrightarrow{\sim} \Lambda(G)$ of (iv) fit into a commutative diagram

$$\begin{array}{ccc} k^\times & \xrightarrow{\mathrm{Kmm}_k} & H^1(G_k, \Lambda(\overline{k})) \\ \wr\downarrow & & \wr\downarrow \\ k^\times(G) & \xrightarrow{\mathrm{Kmm}(G)} & H^1(G, \Lambda(G)). \end{array}$$

Remark

In general,

$$G_k \not\rightsquigarrow \text{ the field } k.$$

Indeed, $\exists$a pair of MLFs $(k_\circ, k_\bullet)$ s.t.

$$G_{k_\circ} \simeq G_{k_\bullet} \quad \text{but} \quad k_\circ \not\simeq k_\bullet.$$

On the other hand,

$$G_k + \text{ram'n fil'n} \rightsquigarrow \text{ the field } k \quad \text{[Mochizuki]}$$

$$G_k + \text{Hodge-Tate rep's} \rightsquigarrow \text{ the field } k \quad \text{[H]}$$

§3 Global Reconstruction Algorithm

F: an NF

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

$\mathbb{V}(F) \stackrel{\mathrm{def}}{=} \{$ nonarchimedean primes of $F \}$

For $v \in \mathbb{V}(F)$,

$\mathcal{O}_v \subseteq F$: the localization of $\mathcal{O}_F$ at v

$\mathcal{O}_v^{\triangleright} \stackrel{\mathrm{def}}{=} \mathcal{O}_v \setminus \{0\} \subseteq F^{\times}$ [submonoid]

$\mathfrak{m}_v \subseteq \mathcal{O}_v$: the maximal ideal

F_v: the completion of F at v

Uchida's Lemma for NFs

[talked at Waseda on 2013/07/12]

$\exists$A functorial algorithm for reconstructing from [a collection of data which is isomorphic to]

- the multiplicative monoid F,
- the set $\mathbb{V}(F)$, and
- the fam'y of sub's $\left\{1+\mathfrak{m}_v \subseteq \mathcal{O}_v^{\triangleright} \subseteq F\right\}_{v\in\mathbb{V}(F)}$

[the map corresponding to] the additive structure of F

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

Step 1 [Set of Nonarchimedean Primes]

G: of NF-type

- $\widetilde{\mathbb{V}}(G)$

$\stackrel{\mathrm{def}}{=} \{$maximal subgps of G of MLF-type$\} \stackrel{\text{conj.}}{\curvearrowleft} G$

- $\mathbb{V}(G) \stackrel{\mathrm{def}}{=} \widetilde{\mathbb{V}}(G)/G$

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

- $\mathbb{V}(\overline{F}) \stackrel{\mathrm{def}}{=} \{$ nonarch'n primes of $\overline{F}$ $\} \curvearrowleft G_F$
- $\mathbb{V}(F) \stackrel{\mathrm{def}}{=} \{$ nonarch'n primes of F $\}$

by Neukirch's work

Step 2 [Cyclotome]

- $\Lambda(G) \overset{\text{conj.}}{\curvearrowleft} G$ s.t. for $\forall D \in \widetilde{\mathbb{V}}(G)$,

$$(\Lambda(G) \curvearrowleft G \hookleftarrow D) \xrightarrow{\sim} (\Lambda(D) \curvearrowleft D)$$

- $\Lambda(\overline{F}) \overset{\text{def}}{=} \text{``}\widehat{\mathbb{Z}}(1)\text{''} = \varprojlim_n \mu_\infty(\overline{F})[n] \curvearrowleft G_F$

For $\forall \widetilde{v} \in \mathbb{V}(\overline{F})$, $\overline{F}^\times \hookrightarrow \overline{F}_{\widetilde{v}}^\times \Rightarrow \Lambda(\overline{F}) \xrightarrow{\sim} \Lambda(\overline{F}_{\widetilde{v}})$

by Global Class Field Theory

the str'e of the idèle class gp

$$\begin{array}{ccc} \mathcal{H}^{\times}(G) & \xrightarrow{\subset} & \prod_{[D]\in\mathbb{V}(G)} k^{\times}(D) \\ \cap\big\downarrow & & \cap\big\downarrow \mathrm{Kmm}(D)\text{'s} \\ H^1(G,\Lambda(G)) & \xrightarrow{\subset} & \prod_{[D]\in\mathbb{V}(G)} H^1(D,\Lambda(D)) \end{array}$$

$$(F^{\times} \subseteq) \qquad \begin{array}{ccc} \mathcal{H}^{\times}(F) & \xrightarrow{\subset} & \prod_{v\in\mathbb{V}(F)} F_v^{\times} \\ \cap\big\downarrow & & \cap\big\downarrow \mathrm{Kmm}_{F_v}\text{'s} \\ (F^{\times})^{\wedge} & \xrightarrow{\subset} & \prod_{v\in\mathbb{V}(F)} (F_v^{\times})^{\wedge} \end{array}$$

Remark: $$1 \to \mathcal{O}_F^{\times} \to F^{\times} \to F^{\times}/\mathcal{O}_F^{\times} \to 1$$

$$1 \to (\mathcal{O}_F^{\times})^{\wedge} \to \mathcal{H}^{\times}(F) \to F^{\times}/\mathcal{O}_F^{\times} \to 1$$

- $\mathcal{H}(G) \overset{\text{def}}{=} \mathcal{H}^{\times}(G) \sqcup \{*_G\} \subseteq \prod_{[D]\in\mathbb{V}(G)} k(D)$ [submonoid]

Remark: $G^{\dagger} \subseteq G$: open $\Rightarrow$

$$\begin{array}{ccc} \mathcal{H}(G) & \xrightarrow{\subset} & \prod_{[D]\in\mathbb{V}(G)} k(D) \\ \cap\downarrow & & \downarrow\cap \\ \mathcal{H}(G^{\dagger}) & \xrightarrow{\subset} & \prod_{[D^{\dagger}]\in\mathbb{V}(G^{\dagger})} k(D^{\dagger}) \end{array}$$

- $\mathcal{H}(F) \overset{\text{def}}{=} \mathcal{H}^{\times}(F) \sqcup \{0\} \subseteq \prod_{v\in\mathbb{V}(F)} F_v$ [submonoid]

$$F \subseteq \mathcal{H}(F) \subseteq \prod_{v\in\mathbb{V}(F)} F_v$$

Observation

If one knows a "correct sub'd" $F(G) \subseteq \mathcal{H}(G)$
[i.e., "$F \subseteq \mathcal{H}(F)$"],
then, by applying Uchida's Lemma to the $F(G)$
[cf. the diagram below],
one obtains a structure of NF on the $F(G)$,
i.e., an NF $F(G)$ of the desired type!

$$\begin{array}{ccccc}
\mathcal{H}(G) \subseteq \prod_{\mathbb{V}(G)} k(D) & & & & \\
\downarrow & & & & \\
k(D) & \supseteq & \mathcal{O}^{\triangleright}(D) & \supseteq & U^{(1)}(D)
\end{array}$$

Step 3 [Prime Field]

- $G \subseteq C(G)$ [i.e., $G_F \subseteq G_{\mathbb{Q}}$] by Neukirch-Uchida

  $\Rightarrow \mathcal{H}(C(G)) \subseteq \mathcal{H}(G)$ [i.e., $\mathcal{H}(\mathbb{Q}) \subseteq \mathcal{H}(F)$]

- a field str'e on $F(C(G)) \stackrel{\text{def}}{=} \mathcal{H}(C(G))$

  [i.e., the field $\mathbb{Q}$] by $\sharp\mathcal{O}_{\mathbb{Q}}^{\times} < \infty$

Step 4 [Absolutely Solvable Extension Fields]

- Let $G^\dagger \subseteq C(G)$ be s.t. $C(G)/G^\dagger$: fin'e sol'e [i.e., a finite solvable extension $E/\mathbb{Q}$].

Then a submonoid $F(G^\dagger) \subseteq \mathcal{H}(G^\dagger)$,
hence also a field str'e on $F(G^\dagger)$
[i.e., the field E]

by the denseness of $\mathbb{Q}$ in $\mathbb{Q}_p$
Hasse Principle for powers
the simple structure of $E/\mathbb{Q}$

Step 5 [Local Algebraically Closed Fields]

- For $D \in \mathbb{V}(G)$,

a field str'e on $k(D)$ [i.e., the field F_v]

by Grunwald-Wang Theorem

$\Rightarrow$ a field str'e on $\overline{k}(D) \ = \ \varinjlim_{D^\dagger \subseteq D} k(D^\dagger)$

[i.e., the field $\overline{F}_{\widetilde{v}} = \overline{\mathbb{Q}}_p$]

Step 6 [Local Versions of the Global Objects]

- For $D \in \widetilde{\mathbb{V}}(G)$,

  subfields $F(D) \subseteq \overline{F}(D) \subseteq \overline{k}(D)$

- For $\widetilde{v} \in \mathbb{V}(\overline{F})$, subfields $F \subseteq \overline{F} \subseteq \overline{F}_{\widetilde{v}}$

by Čhebotarev's Density Theorem

Step 7 [Global Algebraically Closed Field]

By synchronizing the $F(D)$'s [where $D \in \widetilde{\mathbb{V}}(G)$],

we obtain an NF $F(G)$,

hence also an algebraically closed field

$$\overline{F}(G) \;=\; \varinjlim_{G^\dagger \subseteq G} F(G^\dagger) \quad \overset{\text{conj.}}{\curvearrowleft} \quad G$$

of the desired type!

by Neukirch-Uchida