The Neukirch-Uchida theorem with restricted ramification

Ryoji Shimizu

RIMS, Kyoto University

This presentation is based on my paper with the same title, whose preprint will be uploaded in a few weeks.

Introduction

Let K be a number field and S a set of primes of K. We write K_S/K for the maximal extension of K unramified outside S and $G_{K,S}$ for its Galois group.

The goal of this talk is to prove the following generalization of the Neukirch-Uchida theorem under as few assumptions as possible:
"For $i = 1, 2$, let K_i be a number field and S_i a set of primes of K_i. If G_{K_1,S_1} and G_{K_2,S_2} are isomorphic, then K_1 and K_2 are isomorphic."

For this, as in the proof of the Neukirch-Uchida theorem, we first characterize group-theoretically the decomposition groups in $G_{K,S}$, and then obtain an isomorphism of fields using them.

Notations

- $G(L/K) \overset{\text{def}}{=} \mathrm{Gal}(L/K)$: the Galois group of a Galois extension L/K
- $\overline{K}$: a separable closure of a field K
- $G_K \overset{\text{def}}{=} G(\overline{K}/K)$
- K : a number field (i.e. a finite extension of the field of rational numbers $\mathbb{Q}$)
- $P = P_K$: the set of primes of K
- $P_\infty = P_{K,\infty}$: the set of archimedean primes of K
- $P_l = P_{K,l}$: the set of primes of K above a prime number l
- S : a subset of P_K
- $S_f \overset{\text{def}}{=} S \setminus P_{K,\infty}$
- $S(L)$: the set of primes of L above the primes in S for an algebraic extension L/K

For convenience, we consider that an algebraic extension L/K is ramified at a complex prime of L if it is above a real prime of K.

Previous works

The Neukirch-Uchida theorem (Uchida, 1976).

Let K_1 and K_2 be number fields. If $G_{K_1} \simeq G_{K_2}$, then $K_1 \simeq K_2$.

This is in the case that $S_i = P_{K_i}$ for i=1,2.

Previous works

Theorem (Ivanov, 2017).

For $i = 1, 2$, let K_i be a number field and S_i a set of primes of K_i. Assume $G_{K_1,S_1} \simeq G_{K_2,S_2}$ and that the following conditions hold:

(a) $K_i/\mathbb{Q}$ is Galois for $i = 1, 2$ and K_1 is totally imaginary.

(b) There exist two odd prime numbers p such that $P_{K_1,p} \subset S_1$.

(c) There exists an odd prime number p such that $P_{K_2,p} \subset S_2$ and S_i is sharply p-stable for $i = 1, 2$.

(d) For $i = 1, 2$, S_i is 2-stable and is sharply p-stable for almost all p.

Then $K_1 \simeq K_2$.

Let K be a number field and S a set of primes of K. We say that S is stable if there are a subset $S_0 \subset S$ and an $\epsilon \in \mathbb{R}_{>0}$ such that for any finite subextension $K_S/L/K$, $S_0(L)$ has Dirichlet density $\delta(S_0(L)) > \epsilon$.

One of main results

Theorem 4.2.

For $i = 1, 2$, let K_i be a number field and S_i a set of primes of K_i with $P_{K_i,\infty} \subset S_i$. Assume $G_{K_1,S_1} \simeq G_{K_2,S_2}$ and that the following conditions hold:

(a) $K_i/\mathbb{Q}$ is Galois for $i = 1, 2$ and K_1 is totally imaginary.

(b) There exist two different prime numbers p such that for $i = 1, 2$, $P_{K_i,p} \subset S_i$.

(c) For one i, there exists a totally real subfield $K_{i,0} \subset K_i$ and a set of nonarchimedean primes $T_{i,0}$ of $K_{i,0}$ such that $\delta(T_{i,0}(K_i)) \neq 0$.[a]

(d) For the other i, $\delta(S_i) \neq 0$.

Then $K_1 \simeq K_2$.

[a] Let K be a number field and S a set of primes of K. We say that $\delta(S) \neq 0$ if S has positive Dirichlet density or does not have Dirichlet density.

Previous works

Theorem (Ivanov, 2013).

Let K be a number field and $P_\infty \subset S$ a finite set of primes of K. Assume that there exist two different prime numbers p such that $P_p \subset S$, and write l for one of them. Assume $(G_{K,S}, l)$ are given. Then the data of the l-adic cyclotomic character of an open subgroup of $G_{K,S}$ is equivalent to the data of the decomposition groups in $G_{K,S}$ at primes in $S_f(K_S)$.

In the proof, the injectivity of

$$H^2(G_{K,S}, \mu_{l^\infty}) \to \bigoplus_{\mathfrak{p} \in S} H^2(D_\mathfrak{p}, \mu_{l^\infty})$$

plays an impotant role.

Even if S is not finite, we can obtain the “bi-anabelian” version of this result. In order to use this, in §1 we recover the l-adic cyclotomic character of an open subgroup of $G_{K,S}$.

Contents

Let K be a number field, and fix a prime number l.

- $\Sigma = \Sigma_K \stackrel{\text{def}}{=} \{l, \infty\}(K) = P_l \cup P_\infty$
- K_∞/K : a $\mathbb{Z}_l$-extension
- $\Gamma = G(K_\infty/K)$
- $K_{\infty,0}/K$: the cyclotomic $\mathbb{Z}_l$-extension
- $\Gamma_0 = \Gamma_{K,0} \stackrel{\text{def}}{=} G(K_{\infty,0}/K)$

Note that K_∞/K is unramified outside Σ.

- $\gamma_{\mathfrak{p}}$: the Frobenius element in Γ at $\mathfrak{p} \in P_K \setminus \Sigma$
- $\Gamma_{\mathfrak{p}} = \langle \gamma_{\mathfrak{p}} \rangle$: the decomposition group in Γ at $\mathfrak{p} \in P_K \setminus \Sigma$
- S : a set of primes of K

In §1, we assume that $\Sigma \subset S$. Then $\mu_{l^\infty} \subset K_S$, and we write $\chi^{(l)} = \chi^{(l)}_K$ for the l-adic cyclotomic character $G_{K,S} \to \mathrm{Aut}(\mu_{l^\infty}) = \mathbb{Z}_l{}^*$.

§1. Recovering the l-adic cyclotomic character (2/7)

We set $\tilde{l} \overset{\text{def}}{=} \begin{cases} 4 \text{ if } l = 2, \\ l \text{ if } l \neq 2. \end{cases}$ We have the following commutative diagram:

$$\begin{array}{ccccc} G_{K,S} & \xrightarrow{\chi^{(l)}} & {\mathbb{Z}_l}^* & = & (1+\tilde{l}\mathbb{Z}_l) \times ({\mathbb{Z}_l}^*)_{tor} \\ \downarrow & & & & \downarrow pr_1 \\ \Gamma_0 & & \xrightarrow{\quad w \quad} & & 1+\tilde{l}\mathbb{Z}_l \end{array}$$

We write $w = w_K : \Gamma_0 \to 1 + \tilde{l}\mathbb{Z}_l$ for the bottom homomorphism.
Note that $\chi^{(l)}|_{G_{K(\mu_{\tilde{l}}),S(K(\mu_{\tilde{l}}))}} = (G_{K,S} \twoheadrightarrow \Gamma_0 \overset{w}{\to} 1 + \tilde{l}\mathbb{Z}_l)|_{G_{K(\mu_{\tilde{l}}),S(K(\mu_{\tilde{l}}))}}$.

The goal of this section is the following.

Theorem 1.7.

Assume that $\delta(S) \neq 0$. Then the surjection $G_{K,S} \twoheadrightarrow \Gamma_0$ and the character $w : \Gamma_0 \to 1 + \tilde{l}\mathbb{Z}_l$ are characterized group-theoretically from $G_{K,S}$ (and l).

We will see the sketch of the proof of Theorem 1.7.

- $\Lambda = \Lambda^{\Gamma} \stackrel{\text{def}}{=} \mathbb{Z}_l[[\Gamma]] = \varprojlim_n \mathbb{Z}_l[\Gamma/\Gamma^{l^n}]$: the complete group ring of Γ
- $X_S = X_S^{\Gamma} \stackrel{\text{def}}{=} (\mathrm{Ker}(G_{K,S} \twoheadrightarrow \Gamma)^{(l)})^{\mathrm{ab}}$

Note that X_S is constructed group-theoretically from $G_{K,S} \twoheadrightarrow \Gamma$ by its very definition, and X_S has a natural structure of Λ-module.

- $(S \setminus \Sigma)^{fd} \stackrel{\text{def}}{=} \{\mathfrak{p} \in S \setminus \Sigma \mid \ \mathfrak{p} \text{ is finitely decomposed in } K_\infty/K\}$
- $(S \setminus \Sigma)^{cd} \stackrel{\text{def}}{=} \{\mathfrak{p} \in S \setminus \Sigma \mid \ \mathfrak{p} \text{ is completely decomposed in } K_\infty/K\}$

Note that $S \setminus \Sigma = (S \setminus \Sigma)^{fd} \coprod (S \setminus \Sigma)^{cd}$.

For $\mathfrak{p} \in (S \setminus \Sigma)^{fd}$ with $\mu_l \subset K_{\mathfrak{p}}$, the local l-adic cyclotomic character $G_{K_{\mathfrak{p}}} \to \mathrm{Aut}(\mu_{l^\infty}) = \mathbb{Z}_l{}^*$ factors as $G_{K_{\mathfrak{p}}} \twoheadrightarrow \Gamma_{\mathfrak{p}} \to \mathbb{Z}_l{}^*$ because $\Gamma_{\mathfrak{p}} = G(K_{\mathfrak{p}}(\mu_{l^\infty})/K_{\mathfrak{p}})$, where we write $\chi_{\mathfrak{p}}^{(l)} : \Gamma_{\mathfrak{p}} \to \mathbb{Z}_l{}^*$ for the second homomorphism. Further, when $\mu_{\tilde{l}} \subset K_{\mathfrak{p}}$ and $\Gamma = \Gamma_0$, we have $w|_{\Gamma_{\mathfrak{p}}} = \chi_{\mathfrak{p}}^{(l)}$.

§1. Recovering the l-adic cyclotomic character (4/7)

We have the following structure theorem for the Λ-module X_S.

Lemma 1.1.

Assume that the weak Leopoldt conjecture holds for K_∞/K. Then there exists an exact sequence of Λ-modules

$$0 \to \prod_{\mathfrak{p}\in S\setminus\Sigma} J_{\mathfrak{p}} \to X_S \to X_\Sigma \to 0,$$

where X_Σ is a finitely generated Λ-module and

$$J_{\mathfrak{p}} = \begin{cases} \Lambda/\langle \gamma_{\mathfrak{p}} - \chi_{\mathfrak{p}}^{(l)}(\gamma_{\mathfrak{p}})\rangle, & \mu_l \subset K_{\mathfrak{p}} \text{ and } \mathfrak{p} \in (S\setminus\Sigma)^{fd}, \\ \Lambda/l^{t_{\mathfrak{p}}}, & \mu_l \subset K_{\mathfrak{p}} \text{ and } \mathfrak{p} \in (S\setminus\Sigma)^{cd}, \\ 0, & \mu_l \not\subset K_{\mathfrak{p}}, \end{cases}$$

where $l^{t_{\mathfrak{p}}} = \#\mu(K_{\mathfrak{p}})[l^\infty]$.

We set $J = J^\Gamma \stackrel{\text{def}}{=} \prod_{\mathfrak{p}\in S\setminus\Sigma} J_{\mathfrak{p}} \subset X_S$.

§1. Recovering the l-adic cyclotomic character (5/7)

Lemma 1.2.

The weak Leopoldt conjecture is true for K_∞/K if and only if $H^2(G(K_S/K_\infty),\ \mathbb{Q}_l/\mathbb{Z}_l) = 0$. Further, the weak Leopoldt conjecture is true for $K_{\infty,0}/K$.

Note that $H^2(G(K_S/K_\infty),\ \mathbb{Q}_l/\mathbb{Z}_l)$ can be reconstructed group-theoretically from $G_{K,S} \twoheadrightarrow \Gamma$ since $G(K_S/K_\infty) = \mathrm{Ker}(G_{K,S} \twoheadrightarrow \Gamma)$ and $\mathbb{Q}_l/\mathbb{Z}_l$ is a trivial $G(K_S/K_\infty)$-module.

Lemma 1.3.

Assume that $\mu_l \subset K$. Then $\#(S \setminus \Sigma)^{cd} < \infty$ if and only if $X_S[l^\infty]$ is a finitely generated Λ-module. Further, $(S \setminus \Sigma)^{cd} = \emptyset$ for $K_{\infty,0}/K$.

Note that $X_S[l^\infty]$ also can be reconstructed group-theoretically from $G_{K,S} \twoheadrightarrow \Gamma$.

Definition 1.4.

Let $M \subset X_S$ be a Λ-submodule whose quotient X_S/M is a finitely generated Λ-module. We set

$$A_M^{\Gamma} \overset{\text{def}}{=} \left\{ \rho : \Gamma \to 1 + \tilde{l}\mathbb{Z}_l \;\middle|\; \begin{array}{l} \text{For } (\gamma, \alpha) \in (\Gamma \times (1 + \tilde{l}\mathbb{Z}_l))^{\text{prim}} \text{ and } x \in M \setminus \{0\} \\ \text{with } \gamma - \alpha \in \mathrm{Ann}_{\Lambda}(x),\ \rho(\gamma) = \alpha \end{array} \right\},$$

where $(\Gamma \times (1 + \tilde{l}\mathbb{Z}_l))^{\text{prim}} \overset{\text{def}}{=} (\Gamma \times (1 + \tilde{l}\mathbb{Z}_l)) \setminus (\Gamma \times (1 + \tilde{l}\mathbb{Z}_l))^l$.

Note that this set is constructed from M and Γ.

Proposition 1.5.

Assume that $\mu_{\tilde{l}} \subset K$, $\Gamma = \Gamma_0$ and $\#S = \infty$. Let $M \subset J$ be a Λ-submodule whose quotient J/M is a finitely generated Λ-module. Then $A_M^{\Gamma_0} = \{w\}$.

Proposition 1.6.

Assume that $\mu_{\tilde{l}} \subset K$, $\Gamma \neq \Gamma_0$, $\delta(S) \neq 0$, the weak Leopoldt conjecture is true for K_∞/K and $\#(S \setminus \Sigma)^{cd} < \infty$. Let $M \subset X_S$ be a Λ-submodule whose quotient X_S/M is a finitely generated Λ-module. Then $A_M^{\Gamma} = \emptyset$.

§1. Recovering the l-adic cyclotomic character (7/7)

We can show the main theorem of §1 using the results obtained so far.

Theorem 1.7.

Assume that $\delta(S) \neq 0$. Then the surjection $G_{K,S} \twoheadrightarrow \Gamma_0$ and the character $w : \Gamma_0 \to 1 + \tilde{l}\mathbb{Z}_l$ are characterized group-theoretically from $G_{K,S}$ (and l).

Proof. Assume that $\mu_{\tilde{l}} \subset K$. (In the other case, the assertion follows from that of this case.) By Lemma 1.2 and Lemma 1.3, we can distinguish purely group-theoretically whether or not a given $\mathbb{Z}_l$-quotient Γ of $G_{K,S}$ satisfies the following conditions:

- The weak Leopoldt conjecture is true for K_∞/K.
- $\#(S \setminus \Sigma)^{cd} < \infty$ (for K_∞/K).

Let Γ be a $\mathbb{Z}_l$-quotient of $G_{K,S}$ satisfying these conditions and $M \subset X_S^\Gamma$ a Λ-submodule whose quotient X_S/M is a finitely generated Λ-module.
If $\Gamma \neq \Gamma_0$, for any $M \subset X_S^\Gamma$, $A_M^\Gamma = \emptyset$ by Proposition 1.6.
If $\Gamma = \Gamma_0$, for sufficiently small $M \subset X_S^\Gamma$, $A_M^\Gamma = \{w\}$ by Proposition 1.5. □

Definition 2.1.

For $i = 1, 2$, let K_i be a number field, S_i a set of primes of K_i, $T_i \subset S_{i,f}$, and $\sigma : G_{K_1,S_1} \xrightarrow{\sim} G_{K_2,S_2}$ an isomorphism. We say that the local correspondence between T_1 and T_2 holds for σ, if the following conditions are satisfied:

- For any $\overline{\mathfrak{p}}_1 \in T_1(K_{1,S_1})$, there is a unique prime $\sigma_*(\overline{\mathfrak{p}}_1) \in T_2(K_{2,S_2})$ with $\sigma(D_{\overline{\mathfrak{p}}_1}) = D_{\sigma_*(\overline{\mathfrak{p}}_1)}$, such that $\sigma_* \colon T_1(K_{1,S_1}) \to T_2(K_{2,S_2})$, $\overline{\mathfrak{p}}_1 \mapsto \sigma_*(\overline{\mathfrak{p}}_1)$ is a bijection.

Then σ_* induces a bijection $\sigma_{*,K_1} \colon T_1 \xrightarrow{\sim} T_2$.

Definition 2.1. (continued)

Moreover, we say that the good local correspondence between T_1 and T_2 holds for σ, if the following conditions are satisfied:

- The local correspondence between T_1 and T_2 holds for σ.
- For any $\overline{\mathfrak{p}}_1 \in T_1(K_{1,S_1})$, the sets of Frobenius lifts[a] correspond to each other under $\sigma|_{D_{\overline{\mathfrak{p}}_1}} : D_{\overline{\mathfrak{p}}_1} \xrightarrow{\sim} D_{\sigma_*(\overline{\mathfrak{p}}_1)}$.
- σ_{*,K_1} preserves the residue characteristics and the residual degrees of all primes in T_1.

[a] For a Galois extension λ/κ of p-adic fields, we say that an element of $G(\lambda/\kappa)$ is a Frobenius lift if its image under $G(\lambda/\kappa) \twoheadrightarrow G(\lambda/\kappa)/I(\lambda/\kappa)$ is equal to the Frobenius element, where $I(\lambda/\kappa)$ is the inertia subgroup of $G(\lambda/\kappa)$.

Lemma 2.2.

For $i = 1, 2$, let p_i be a prime number, κ_i a p_i-adic field and λ_1/κ_1 a Galois extension. Assume that there exists an isomorphism $\sigma : G(\lambda_1/\kappa_1) \xrightarrow{\sim} G_{\kappa_2}$. Then $p_1 = p_2$, the residual degrees of κ_1 and κ_2 coincide and σ induces a bijection between the sets of Frobenius lifts. Further, $[\kappa_1 : \mathbb{Q}_{p_1}] \geq [\kappa_2 : \mathbb{Q}_{p_2}]$.

In the proof,

$$G_{\kappa_i}^{\mathrm{ab}} \simeq \hat{\mathbb{Z}} \times \mathbb{Z}/(q_i - 1)\mathbb{Z} \times \mathbb{Z}/{p_i}^a\mathbb{Z} \times \mathbb{Z}_{p_i}^{[\kappa_i:\mathbb{Q}_{p_i}]}$$

plays an impotant role, where q_i is the order of the residue field of κ_i and $a \in \mathbb{Z}_{\geq 0}$.

Proposition 2.3 (Chenevier-Clozel, 2009).

Let K be a totally real number field and S a set of primes of K. Assume that there exists a prime l with $P_l \cup P_\infty \subset S$. Then the decomposition groups in $G_{K,S}$ at primes in $(S_f \setminus P_l)(K_S)$ are full.[a]

[a] For $\overline{\mathfrak{p}} \in S_f(K_S)$ and $\mathfrak{p} \in S_f$ with $\overline{\mathfrak{p}}|\mathfrak{p}$, we say that $D_{\overline{\mathfrak{p}},K_S/K}$ is full if the canonical surjection $G_{K_\mathfrak{p}} \twoheadrightarrow D_{\overline{\mathfrak{p}},K_S/K}$ is an isomorphism.

We obtain the following using results so far.

Theorem 2.4.

For $i = 1, 2$, let K_i be a number field, S_i a set of primes of K_i with $P_{K_i,\infty} \subset S_i$ and $\sigma : G_{K_1,S_1} \overset{\sim}{\to} G_{K_2,S_2}$ an isomorphism. Assume that the following conditions hold:

- There exist two different prime numbers p such that for $i = 1, 2$, $P_{K_i,p} \subset S_i$.
- For $i = 1, 2$, $\delta(S_i) \neq 0$.

Then the local correspondence between $S_{1,f}$ and $S_{2,f}$ holds for σ. Further, let $T_1 \subset S_{1,f}$ and $T_2 \subset S_{2,f}$ be subsets between which the local correspondence holds for σ and assume that for one i, there exist a totally real subfield $K_{i,0} \subset K_i$ and a set of primes $T_{i,0}$ of $K_{i,0}$ such that $T_{i,0}(K_i) = T_i$. Then the good local correspondence between T_1 and T_2 holds for σ.

§3. The existence of an isomorphism of fields (1/11)

For a number field K and a set of primes S of K, we set

$$\delta_{\sup}(S) \overset{\text{def}}{=} \limsup_{s \to 1+0} \frac{\sum_{\mathfrak{p} \in S_f} \mathfrak{N}(\mathfrak{p})^{-s}}{\log \frac{1}{s-1}}, \delta_{\inf}(S) \overset{\text{def}}{=} \liminf_{s \to 1+0} \frac{\sum_{\mathfrak{p} \in S_f} \mathfrak{N}(\mathfrak{p})^{-s}}{\log \frac{1}{s-1}}.$$

Note that $\delta(S) \neq 0$ if and only if $\delta_{\sup}(S) > 0$.

In §3, for $i = 1, 2$, we set as follows:

- K_i : a number field
- S_i : a set of primes of K_i with $P_{K_i,\infty} \subset S_i$
- $T_i \subset S_{i,f}$: a subset
- $\sigma : G_{K_1,S_1} \xrightarrow{\sim} G_{K_2,S_2}$: an isomorphism

Fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$, and suppose that all number fields and all algebraic extensions of them are subfields of $\overline{\mathbb{Q}}$.

The goal of §3 is to prove the following theorems:

Theorem 3.2.

Assume that the following conditions hold:

(a) $K_i/\mathbb{Q}$ is Galois for $i = 1, 2$.

(b) The good local correspondence between T_1 and T_2 holds for σ.

(c) $\delta_{\sup}(T_i) > 1/2$ for one i.

Then $K_1 \simeq K_2$.

Theorem 3.4.

Assume that the following conditions hold:

(a) $K_i/\mathbb{Q}$ is Galois for $i = 1, 2$ and K_1 is totally imaginary.

(b) The good local correspondence between T_1 and T_2 holds for σ.

(c) $\delta(T_i) \neq 0$ for one i.

(d) There exist two different prime numbers p such that for $i = 1, 2$, $P_{K_i,p} \subset T_i$.

Then $K_1 \simeq K_2$.

Lemma 3.1.

Assume that the following conditions hold:

(a) $K_i/\mathbb{Q}$ is Galois for $i = 1, 2$.

(b) The good local correspondence between T_1 and T_2 holds for σ.

Then the following assertions hold:

(i) $\delta_{\sup}(T_1) = \delta_{\sup}(T_2)$

(ii) For $i = 1, 2$, $\delta_{\sup}(T_i(K_1K_2)) = [K_1K_2 : K_i]\delta_{\sup}(T_i)$.

The similar assertions hold for $\delta_{\inf}$.

Proof. (i): By the good local correspondence between T_1 and T_2, for $s > 1$,

$$\frac{\sum_{\mathfrak{p}_1 \in T_1} \mathfrak{N}(\mathfrak{p}_1)^{-s}}{\log \frac{1}{s-1}} = \frac{\sum_{\mathfrak{p}_2 \in T_2} \mathfrak{N}(\mathfrak{p}_2)^{-s}}{\log \frac{1}{s-1}}.$$

Therefore,

$$\delta_{\sup}(T_1) = \limsup_{s \to 1+0} \frac{\sum_{\mathfrak{p}_1 \in T_1} \mathfrak{N}(\mathfrak{p}_1)^{-s}}{\log \frac{1}{s-1}} = \limsup_{s \to 1+0} \frac{\sum_{\mathfrak{p}_2 \in T_2} \mathfrak{N}(\mathfrak{p}_2)^{-s}}{\log \frac{1}{s-1}} = \delta_{\sup}(T_2).$$

Lemma 3.1.

(ii) For $i = 1, 2$, $\delta_{\mathrm{sup}}(T_i(K_1K_2)) = [K_1K_2 : K_i]\delta_{\mathrm{sup}}(T_i)$.

(ii): We set $\mathrm{cs}(K/\mathbb{Q}) \stackrel{\mathrm{def}}{=} \{p : \text{a prime number} \mid p \text{ splits completely in } K/\mathbb{Q}\}$ for a number field K. We prove the case for $i = 1$. By the good local correspondence between T_1 and T_2, for any prime number p below a prime in T_1 which is unramified in $K_1K_2/\mathbb{Q}$,

$$
\begin{aligned}
\text{“}p \in \mathrm{cs}(K_1/\mathbb{Q})\text{”} &\Leftrightarrow \text{“there exists } \mathfrak{p}_1 \in T_1 \text{ of residual degree 1 such that } \mathfrak{p}_1|p\text{”} \\
&\Leftrightarrow \text{“there exists } \mathfrak{p}_2 \in T_2 \text{ of residual degree 1 such that } \mathfrak{p}_2|p\text{”} \\
&\Leftrightarrow \text{“}p \in \mathrm{cs}(K_2/\mathbb{Q})\text{”} \\
&\Leftrightarrow \text{“}p \in \mathrm{cs}(K_1K_2/\mathbb{Q})\text{”}.
\end{aligned}
$$

Therefore,

$$
\begin{aligned}
\delta_{\mathrm{sup}}(T_1(K_1K_2)) &= \delta_{\mathrm{sup}}(\mathrm{cs}(K_1K_2/\mathbb{Q})(K_1K_2) \cap T_1(K_1K_2)) \\
&= \limsup_{s\to 1+0} \frac{\sum_{\mathfrak{p}\in \mathrm{cs}(K_1K_2/\mathbb{Q})(K_1K_2)\cap T_1(K_1K_2)} \mathfrak{N}(\mathfrak{p})^{-s}}{\log \frac{1}{s-1}} \\
&= \limsup_{s\to 1+0} \frac{\sum_{\mathfrak{p}_1\in \mathrm{cs}(K_1/\mathbb{Q})(K_1)\cap T_1} [K_1K_2 : K_1]\mathfrak{N}(\mathfrak{p}_1)^{-s}}{\log \frac{1}{s-1}} \\
&= [K_1K_2 : K_1]\delta_{\mathrm{sup}}(\mathrm{cs}(K_1/\mathbb{Q})(K_1) \cap T_1) \\
&= [K_1K_2 : K_1]\delta_{\mathrm{sup}}(T_1). \qquad \square
\end{aligned}
$$

§3. The existence of an isomorphism of fields (5/11)

Theorem 3.2.

Assume that the following conditions hold:

(a) $K_i/\mathbb{Q}$ is Galois for $i = 1, 2$.

(b) The good local correspondence between T_1 and T_2 holds for σ.

(c) $\delta_{\mathrm{sup}}(T_i) > 1/2$ for one i.

Then $K_1 \simeq K_2$.

Proof. By Lemma 3.1, we have $\delta_{\mathrm{sup}}(T_1) = \delta_{\mathrm{sup}}(T_2) > 1/2$ and $1 \geq \delta_{\mathrm{sup}}(T_i(K_1K_2)) = [K_1K_2 : K_i]\delta_{\mathrm{sup}}(T_i)$ for $i = 1, 2$. Hence we have $[K_1K_2 : K_i] = 1$ for $i = 1, 2$, so that $K_1 \subset K_2$ and $K_1 \supset K_2$.
Thus, $K_1 = K_2$. □

Lemma 3.3.

Assume that the following conditions hold:

(b) The good local correspondence between T_1 and T_2 holds for σ.

(d) There exist two different prime numbers p such that for $i = 1, 2$, $P_{K_i,p} \subset T_i$.

Then $[K_1 : \mathbb{Q}] = [K_2 : \mathbb{Q}]$.

Proof. The assertion follows from the fact that $[K_i : \mathbb{Q}] = \sum_{\mathfrak{p} \in P_{K_i,p}} [K_{i,\mathfrak{p}} : \mathbb{Q}_p]$. □

The proof of Theorem 3.4 (7/11)

Theorem 3.4.

Assume that the following conditions hold:

(a) $K_i/\mathbb{Q}$ is Galois for $i = 1, 2$ and K_1 is totally imaginary.

(b) The good local correspondence between T_1 and T_2 holds for σ.

(c) $\delta(T_i) \neq 0$ for one i.

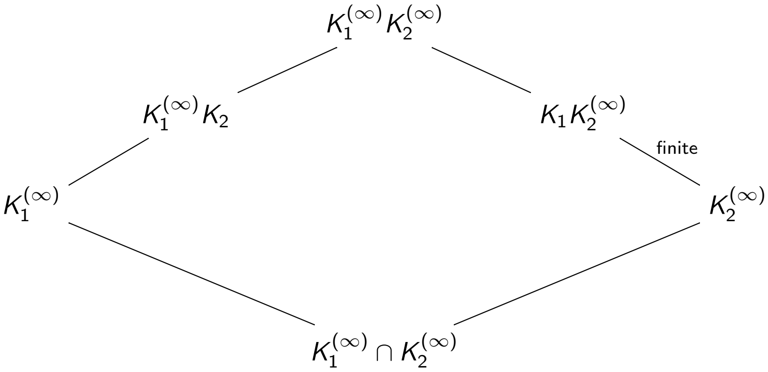
(d) There exist two different prime numbers p such that for $i = 1, 2$, $P_{K_i,p} \subset T_i$.

Then $K_1 \simeq K_2$.

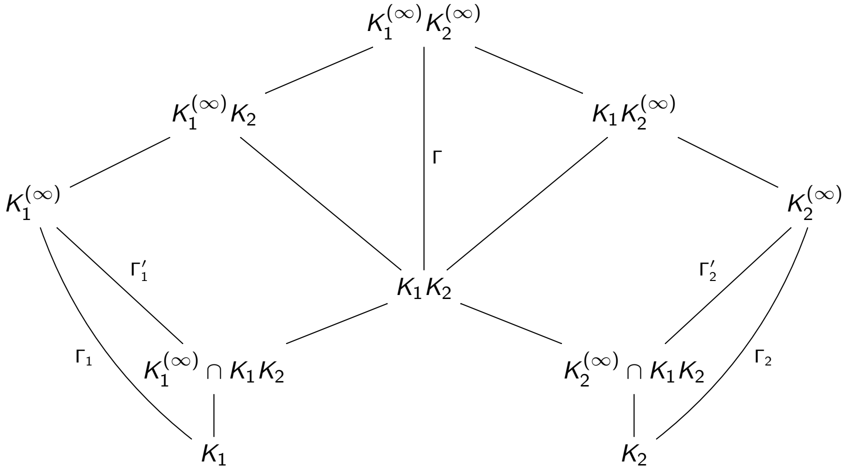
Proof. Take a prime number l such that for $i = 1, 2$, $P_{K_i,l} \subset T_i$. (By (d), we can take at least two different such prime numbers.) For $i = 1, 2$, we set $G_{K_i,S_i} \twoheadrightarrow \Gamma_i \stackrel{\text{def}}{=} G_{K_i,S_i}^{\text{ab},(l),/tor} \simeq \mathbb{Z}_l^{r_i}$ and write $K_i^{(\infty)} = K_i^{(\infty,l)}$ for the corresponding subextension of $K_{i,S_i}/K_i$ with this surjection. Note that $r_{\mathbb{C}}(K_i) + 1 \leq r_i \leq [K_i : \mathbb{Q}]$ by class field theory. σ induces $\overline{\sigma} : \Gamma_1 \xrightarrow{\sim} \Gamma_2$, so that $r_1 = r_2$ for which we write r. Since K_i is Galois over $\mathbb{Q}$ for $i = 1, 2$, $K_i^{(\infty)}$ and $K_1^{(\infty)}K_2^{(\infty)}$ are also.

It suffices to prove that $K_1 \subset K_2^{(\infty)}$. Indeed, then $K_1 \subset \cap_l K_2^{(\infty,l)} = K_2$, so that we obtain $K_1 = K_2$ by $[K_1 : \mathbb{Q}] = [K_2 : \mathbb{Q}]$

The proof of Theorem 3.4 (8/11)

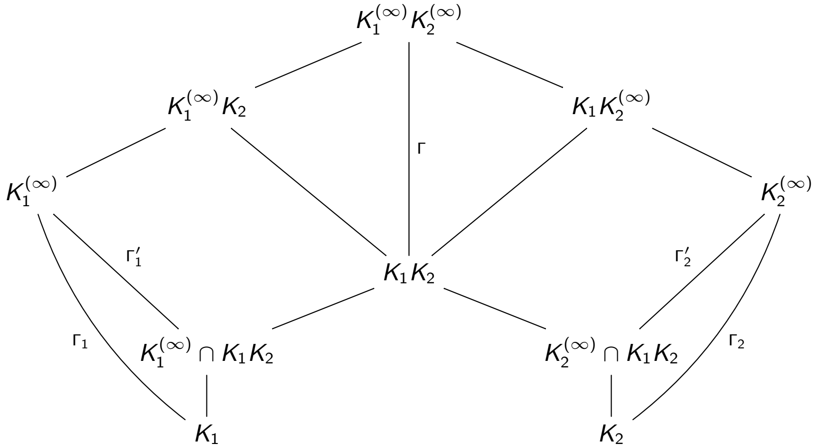


First, we prove $[K_1^{(\infty)} : K_1^{(\infty)} \cap K_2^{(\infty)}] < \infty$.
For this, it suffices to prove $K_1^{(\infty)} K_2^{(\infty)} = K_1 K_2^{(\infty)}$.



We set $\Gamma \overset{\text{def}}{=} G(K_1^{(\infty)}K_2^{(\infty)}/K_1K_2)$ and for $i = 1, 2$, $\Gamma_i' \overset{\text{def}}{=} G(K_i^{(\infty)}/K_i^{(\infty)} \cap K_1K_2)$.

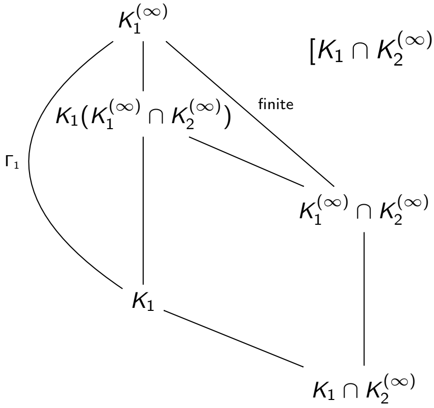
We write π_1 for $\Gamma \twoheadrightarrow G(K_1^{(\infty)}K_2/K_1K_2) \underset{\text{restriction}}{\overset{\sim}{\to}} \Gamma_1' \hookrightarrow \Gamma_1$ and define $\pi_2 : \Gamma \to \Gamma_2$ similarly. It suffices to prove that π_2 is injective. Note that $(\pi_1, \pi_2) : \Gamma \hookrightarrow \Gamma_1 \times \Gamma_2$ is injective.



Since $\delta(T_1(K_1K_2)) \neq 0$, the closed subgroup of Γ generated by Frobenius elements at primes in $T_1(K_1K_2) \setminus P_{K_1K_2,l}$ of degree 1 is open by the Chebotarev density theorem. By the good local correspondence between T_1 and T_2, for $\mathfrak{p} \in T_1(K_1K_2) \setminus P_{K_1K_2,l}$ of degree 1, we have $\overline{\sigma} \circ \pi_1(\mathrm{Frob}_\mathfrak{p}) = \mathrm{Frob}_{\sigma_{*,K_1}(\mathfrak{p}|_{K_1})}$ and $\pi_2(\mathrm{Frob}_\mathfrak{p}) = \mathrm{Frob}_{\mathfrak{p}|_{K_2}}$. Hence $\exists \tau \in G(K_2/\mathbb{Q})$ s.t. $\tau^* \circ \overline{\sigma} \circ \pi_1(\mathrm{Frob}_\mathfrak{p}) = \pi_2(\mathrm{Frob}_\mathfrak{p})$. Therefore, $\exists \tau \in G(K_2/\mathbb{Q})$ s.t. $\tau^* \circ \overline{\sigma} \circ \pi_1 = \pi_2$, so that $\mathrm{Ker}(\pi_2) = \mathrm{Ker}(\tau^* \circ \overline{\sigma} \circ \pi_1) = \mathrm{Ker}(\pi_1)$. Thus, π_1 and π_2 are injective.

The proof of Theorem 3.4 (11/11)

Since $\Gamma_1(\simeq \mathbb{Z}_l^r)$ is torsion free, $K_1^{(\infty)} = K_1(K_1^{(\infty)} \cap K_2^{(\infty)})$. Hence $\Gamma_1 \overset{\text{restriction}}{\overset{\sim}{\to}} G(K_1^{(\infty)} \cap K_2^{(\infty)} / K_1 \cap K_2^{(\infty)})$ is an isomorphism, so that the number r' of independent $\mathbb{Z}_l$-extensions of $K_1 \cap K_2^{(\infty)}$ satisfies that $r \leq r' \leq [K_1 \cap K_2^{(\infty)} : \mathbb{Q}]$.



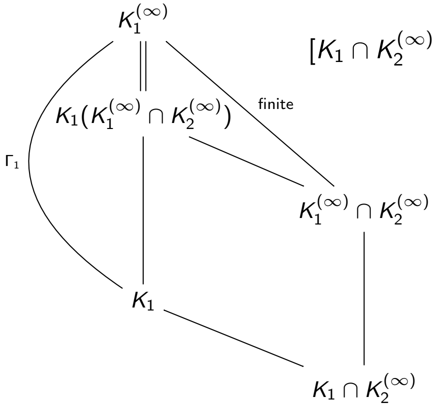
Here, assume that $K_1 \neq K_1 \cap K_2^{(\infty)}$. Then

$$\begin{aligned} [K_1 \cap K_2^{(\infty)} : \mathbb{Q}] &\leq [K_1 : \mathbb{Q}]/2 && \because K_1 \neq K_1 \cap K_2^{(\infty)} \\ &= r_{\mathbb{C}}(K_1) && \because K_1 \text{ is totally imaginary} \\ &< r_{\mathbb{C}}(K_1) + 1 \\ &\leq r \end{aligned}$$

This contradicts the above estimate. Thus, $K_1 = K_1 \cap K_2^{(\infty)}$, so that $K_1 \subset K_2^{(\infty)}$. □

The proof of Theorem 3.4 (11/11)

Since $\Gamma_1 (\simeq \mathbb{Z}_l^r)$ is torsion free, $K_1^{(\infty)} = K_1(K_1^{(\infty)} \cap K_2^{(\infty)})$. Hence $\Gamma_1 \overset{\text{restriction}}{\overset{\sim}{\to}} G(K_1^{(\infty)} \cap K_2^{(\infty)} / K_1 \cap K_2^{(\infty)})$ is an isomorphism, so that the number r' of independent $\mathbb{Z}_l$-extensions of $K_1 \cap K_2^{(\infty)}$ satisfies that $r \leq r' \leq [K_1 \cap K_2^{(\infty)} : \mathbb{Q}]$.



Here, assume that $K_1 \neq K_1 \cap K_2^{(\infty)}$. Then

$$\begin{aligned}[K_1 \cap K_2^{(\infty)} : \mathbb{Q}] &\leq [K_1 : \mathbb{Q}]/2 && \because K_1 \neq K_1 \cap K_2^{(\infty)} \\ &= r_{\mathbb{C}}(K_1) && \because K_1 \text{ is totally imaginary} \\ &< r_{\mathbb{C}}(K_1) + 1 \\ &\leq r\end{aligned}$$

This contradicts the above estimate. Thus, $K_1 = K_1 \cap K_2^{(\infty)}$, so that $K_1 \subset K_2^{(\infty)}$. □

Finally we see the three main results in this talk.

By Theorem 2.4 and Theorem 3.2, we obtain the following theorem.

Theorem 4.1.

For $i = 1, 2$, let K_i be a number field and S_i a set of primes of K_i with $P_{K_i,\infty} \subset S_i$. Assume $G_{K_1,S_1} \simeq G_{K_2,S_2}$ and that the following conditions hold:

(a) $K_i/\mathbb{Q}$ is Galois for $i = 1, 2$.

(b) There exist two different prime numbers p such that for $i = 1, 2$, $P_{K_i,p} \subset S_i$.

(c) For one i, there exist a totally real subfield $K_{i,0} \subset K_i$ and a set of nonarchimedean primes $T_{i,0}$ of $K_{i,0}$ such that $\delta_{\sup}(T_{i,0}(K_i)) > 1/2$.

(d) For the other i, $\delta(S_i) \neq 0$.

Then $K_1 \simeq K_2$.

§4. Main results (2/3)

By Theorem 2.4 and Theorem 3.4, we obtain the following theorem.

Theorem 4.2.

For $i = 1, 2$, let K_i be a number field and S_i a set of primes of K_i with $P_{K_i,\infty} \subset S_i$. Assume $G_{K_1,S_1} \simeq G_{K_2,S_2}$ and that the following conditions hold:

(a) $K_i/\mathbb{Q}$ is Galois for $i = 1, 2$ and K_1 is totally imaginary.

(b) There exist two different prime numbers p such that for $i = 1, 2$, $P_{K_i,p} \subset S_i$.

(c) For one i, there exist a totally real subfield $K_{i,0} \subset K_i$ and a set of nonarchimedean primes $T_{i,0}$ of $K_{i,0}$ such that $\delta(T_{i,0}(K_i)) \neq 0$.

(d) For the other i, $\delta(S_i) \neq 0$.

Then $K_1 \simeq K_2$.

§4. Main results (3/3)

If the Dirichlet densities are large enough, we can omit some assumptions.

Theorem 4.3.

For $i = 1, 2$, let K_i be a number field and S_i a set of primes of K_i with $P_{K_i,\infty} \subset S_i$. Assume $G_{K_1,S_1} \simeq G_{K_2,S_2}$ and that the following conditions hold:

(A) $K_1/\mathbb{Q}$ is Galois.

(B) $\delta_{\sup}(S_1) > 1 - \frac{1}{2[K_1:\mathbb{Q}]}$.

(C) $\delta_{\sup}(S_1) + \delta_{\inf}(S_2)$ or $\delta_{\inf}(S_1) + \delta_{\sup}(S_2)$ is larger than $2 - \frac{1}{[K_1:\mathbb{Q}]([K_2:\mathbb{Q}]!)}$, where $[K_2 : \mathbb{Q}]!$ is the factorial of $[K_2 : \mathbb{Q}]$.

Then $K_1 \simeq K_2$.

In the proof, we show that the conditions in Theorem 4.2 hold.

This theorem is a generalization of Neukirch's original result.

Future perspectives

Future issues are to weaken the assumptions on K_i and S_i.

In particular, we have the following questions:

- To recover the l-adic cyclotomic character from G_{K_i,S_i} when $\delta(S_i) = 0$.
- To study the structures of the decomposition groups in G_{K_i,S_i} in the case where we cannot use the result of [Chenevier-Clozel], and to recover local invariants.
- To prove $K_1 \simeq K_2$ without assuming "Galois over $\mathbb{Q}$".
- To search for counterexamples when $\delta(S_i) = 0$.

References

- Chenevier, G., Clozel, L., Corps de nombres peu ramifiés et formes automorphes autoduales, J. of the AMS, vol. 22 (2009), no. 2, 467-519.
- Ivanov, A., Arithmetic and anabelian theorems for stable sets in number fields, Dissertation, Universität Heidelberg, 2013.
- Ivanov, A., On some anabelian properties of arithmetic curves, Manuscripta Mathematica 144 (2014), no. 3, 545-564.
- Ivanov, A., On a generalization of the Neukirch-Uchida theorem, Moscow Mathematical J. 17 (2017), no. 3, 371-383.
- Neukirch, J., Kennzeichnung der p-adischen und der endlichen algebraischen Zahlkörper, Invent. Math. 6 (1969), 296–314.
- Neukirch, J., Kennzeichnung der endlich-algebraischen Zahlkörper durch die Galoisgruppe der maximal auflösbaren Erweiterungen, J. Reine Angew. Math. 238 (1969), 135–147.
- Neukirch, J., Schmidt, A. and Wingberg, K., Cohomology of number fields, Second edition, Grundlehren der Mathematischen Wissenschaften, 323. Springer-Verlag, Berlin, 2008.

Saïdi, M. and Tamagawa, A., The *m*-step solvable anabelian geometry of number fields, preprint, arXiv:1909.08829.

Serre, J.-P., Abelian *l*-adic representations and elliptic curves, Second edition, Advanced Book Classics, Addison-Wesley, Redwood City, 1989.