Notes on Neukirch–Uchida for nilpotent extensions

Peter Koymans*[1]

[1]University of Michigan

May 31, 2022

1 Introduction

Fix an algebraic closure $\overline{\mathbb{Q}}$. All our number fields will be inside this fixed algebraic closure.

Let $\mathcal{C}$ be a collection of finite groups. If K is a number field, we define

$$K(\mathcal{C}) := K\left(\bigcup_{\substack{K \subseteq L \subseteq \overline{\mathbb{Q}} \\ \mathrm{Gal}(L/K) \cong G \text{ for some } G \in \mathcal{C}}} L\right)$$

and $\mathcal{G}_{K,\mathcal{C}} = \mathrm{Gal}(K(\mathcal{C})/K)$.

Question 1.1. *What information of a number field K can we recover from the isomorphism type of $\mathcal{G}_{K,\mathcal{C}}$ as profinite group?*

2 Known results

Theorem 2.1 (Neukirch, 1969)**.** *One can recover K, up to isomorphism, from $\mathcal{G}_{K,\{\text{fin.}\}}$.*

Theorem 2.2 (Uchida, 1976)**.** *One can recover K, up to isomorphism, from $\mathcal{G}_{K,\{\text{solv.}\}}$.*

Theorem 2.3 (Saïdi–Tamagawa, 2019)**.** *For every integer $m \geq 3$ one can recover K, up to isomorphism, from $\mathcal{G}_{K,\{m-\text{solv.}\}}$.*

Theorem 2.4 (Onabe, 1976)**.** *There are two imaginary quadratic fields K and L with $K \neq L$ but $\mathcal{G}_{K,\{\text{ab}\}} \cong \mathcal{G}_{L,\{\text{ab}\}}$.*

There are also some results that allow one to recover K from $\mathcal{G}_{K,\{\text{ab}\}}$ together with some extra data (CdSLMS).

Theorem 2.5 (K.–Pagano, 2022)**.** *There are two imaginary quadratic fields K and L with $K \neq L$ but $\mathcal{G}_{K,\{2-\text{nil}\}} \cong \mathcal{G}_{L,\{2-\text{nil}\}}$.*

Conjecture 2.6 (K.–Pagano, 2022)**.** *There are two number fields K and L with $\mathcal{G}_{K,\{\text{nil}\}} \cong \mathcal{G}_{L,\{\text{nil}\}}$ and $K \not\cong L$.*

*Department of Mathematics, Ann Arbor, MI 48109, USA, koymans@umich.edu

Theorem 2.7 (K.–Pagano, 2022). *Let K and L be two imaginary quadratic class number 1 fields, not equal to $\mathbb{Q}(\sqrt{-2})$. Then we have $\mathcal{G}_{K,\{C_4,D_4\}} \cong \mathcal{G}_{L,\{C_4,D_4\}}$ if and only if*

- *ζ_4 is in both K and L;*

- *ζ_4 is not in K and not in L. Furthermore, there exists a C_4-extension of K containing $K(\sqrt{-1})$ and a C_4-extension of L containing $L(\sqrt{-1})$;*

- *ζ_4 is not in K and not in L. Furthermore, there does not exist a C_4-extension of K containing $K(\sqrt{-1})$ and there does not exist a C_4-extension of L containing $L(\sqrt{-1})$.*

Remark 2.8. *We have $K(\{C_4, D_4\}) = K(\{D_4\})$.*

3 The Rado graph

Definition 3.1 (Rado graph). *An undirected graph $G = (V, E)$ is Rado if*

- *V is countably infinite;*
- *for all finite disjoint set of vertices U_1 and U_2, there exists a vertex $v \notin U_1 \cup U_2$ that is adjacent to all vertices in U_1 and is not adjacent to all vertices in U_2.*

Theorem 3.2 (Back-and-forth method). *Let $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ be two Rado graphs. Then $G_1 \cong G_2$.*

Proof. Fix enumerations $a_1, a_2, a_3, \ldots$ of V_1 and $b_1, b_2, b_3, \ldots$ of V_2. We will construct a partial graph isomorphism $f_n : V_1 \to V_2$ at each stage $n \in \mathbb{Z}_{\geq 0}$. Initially, f_0 is the empty map.

(1) At odd stages n, take the smallest i such that $a_i \notin \mathrm{dom}(f_n)$. Take $b_j \in V_2 \setminus \mathrm{ran}(f_n)$ such that

$$(b_j, f_n(a)) \in E_2 \Longleftrightarrow (a_i, a) \in E_1$$

for all $a \in \mathrm{dom}(f_n)$. Define f_{n+1} by extending f_n by matching a_i with b_j.

(2) At even stages n, take the smallest j such that $b_j \notin \mathrm{ran}(f_n)$. Take $a_i \in V_1 \setminus \mathrm{dom}(f_n)$ such that

$$(b_j, f_n(a)) \in E_2 \Longleftrightarrow (a_i, a) \in E_1$$

for all $a \in \mathrm{dom}(f_n)$. Define f_{n+1} by extending f_n by matching a_i with b_j.

Now $\bigcup_{n=0}^{\infty} f_n$ is the desired isomorphism. □

So how do we explicitly construct Rado graphs? Here is a classical result due to Erdős.

Theorem 3.3 (Erdős–Rényi model). *Consider a random countably infinite graph G by choosing, independently and with probability $1/2$ for each pair of vertices, whether to connect them by an edge. Then G is Rado with probability 1.*

Proof. For fixed U_1 and U_2

$$\mathbb{P}(\exists v \notin U_1 \cup U_2 \text{ such that } x \text{ is adjacent to } U_1, \text{ but not to } U_2) = 0.$$

Since there are only countably many choices for U_1 and U_2, the result follows. □

For our purposes the following example will be an important source of inspiration.

Example 3.4 (Cameron)**.** *Consider the following graph G. The vertices V are the primes* 1 *modulo* 4*. We connect the vertices p and q by an edge if $(p/q) = 1$. This is well-defined by quadratic reciprocity.*

The resulting graph is Rado thanks to Dirichlet's theorem on primes in arithmetic progressions.

4 Galois cohomology and D_4

Our graphs are now also allowed to have loops.

Definition 4.1. *We attach a graph $G(K) = (V, E)$ to a number field K. Let $V = K^*/K^{*2}$. Then*

$$\begin{aligned}(a, b) \in E &\iff \chi_a \cup \chi_b \text{ is trivial in } H^2(G_K, \mathbb{F}_2)\\ &\iff x^2 = ay^2 + bz^2 \text{ has a non-trivial solution } (x, y, z) \in K^3.\end{aligned}$$

Lemma 4.2. *Let $a, b \in K^*/K^{*2}$ be linearly independent.*

(a) There exists a D_4-extension containing $K(\sqrt{a}, \sqrt{b})$ if and only if $(a, b) \in E$.

(b) There exists a C_4-extension containing $K(\sqrt{a})$ if and only if $(a, a) \in E$.

Proof. Use the inflation–restriction exact sequence and the explicit description of $H^2(\mathbb{F}_2^2, \mathbb{F}_2)$ and $H^2(\mathbb{F}_2, \mathbb{F}_2)$. □

Theorem 4.3. *Let K and L be two number fields. Then we have*

$$\mathcal{G}_{K,\{C_4,D_4\}} \cong \mathcal{G}_{L,\{C_4,D_4\}} \iff G(K) \cong G(L).$$

Proof. One can formally recover the group using cocycles and 1-cochains. □

5 End of proof

Lemma 5.1. *We have*

$$(v, a) \in E \iff (a, a) \in E \text{ for all } a \in V$$

if and only if $v = -1$.

Proof. $\Longleftarrow$: Since $\chi_{-a} \cup \chi_a$ is trivial, it follows that

$$\chi_{-1} \cup \chi_a \text{ is trivial } \iff \chi_a \cup \chi_a \text{ is trivial.}$$

$\Longrightarrow$: Conversely, suppose that $\chi_v \cup \chi_a$ is trivial if and only if $\chi_a \cup \chi_a$ is trivial if and only if $\chi_{-1} \cup \chi_a$ is trivial.

Let $\mathfrak{p}$ be an odd prime ideal of K that is unramified in $K(\sqrt{v}, \sqrt{-1})$. We claim that $\mathfrak{p}$ splits in $K(\sqrt{v})$ if and only if $\mathfrak{p}$ splits in $K(\sqrt{-1})$. Let L be the ray class field of conductor $8\infty\mathfrak{r}$, where $\mathfrak{r}$ is the product of the ramified prime ideals in $K(\sqrt{v})$. By the Chebotarev Density Theorem there exists $\mathfrak{q}$ with $\mathrm{Art}_L(\mathfrak{p}) = -\mathrm{Art}_L(\mathfrak{q})$. Then there exists a totally positive element $a \equiv 1 \bmod 8\mathfrak{r}$ such that $(a) = \mathfrak{p}\mathfrak{q}$, and for such a

$$\chi_{-1} \cup \chi_a \text{ is trivial } \iff \mathfrak{p} \text{ splits in } K(\sqrt{-1})$$

and

$$\chi_v \cup \chi_a \text{ is trivial } \iff \mathfrak{p} \text{ splits in } K(\sqrt{v}).$$

Having established the claim, the lemma follows by another application of the Chebotarev Density Theorem. □

We now construct three isomorphism invariants of the graph $G(K)$.

- we have $(a, a) \in E$ for all $a \in V$;
- there exists $a \in V$ such that $(a, a) \notin E$, and $(-1, -1) \in E$;
- we have $(-1, -1) \notin E$.

Now our main theorem follows from back-and-forth method similar to the case of the Rado graph (need only deal with second case). Differences in the argument:

- we start by matching -1 with -1. Then match 2 with 2;
- list the odd prime elements $\pi_1, \pi_2, \ldots$ of K and the odd prime elements $\rho_1, \rho_2, \ldots$ of L. Observe that 2 is inert in K, $K_2 = \mathbb{Q}_2(\sqrt{5})$ and $K^*/K^{*2} = \langle -1, 2, \pi_1, \pi_2, \ldots \rangle$.

  Lemma 5.2. *Fix some character $\chi : G_{\mathbb{Q}_2(\sqrt{5})} \to \mathbb{F}_2$. Given some odd prime elements $\pi_1, \ldots, \pi_k$ of K and elements $a_1, \ldots, a_k \in \mathbb{Q}/\mathbb{Z}[2]$, there exists a prime element π such that*

  - $\chi_\pi|_{G_{\mathbb{Q}_2(\sqrt{5})}} = \chi$;
  - $\mathrm{inv}_\pi(\chi_\pi \cup \chi_{\pi_i}) = a_i$.