ON THE $\mathbb{Z}_l$-RANK OF ABELIAN EXTENSIONS WITH RESTRICTED RAMIFICATION

CHRISTIAN MAIRE

ABSTRACT. For a prime number ℓ, we consider ℓ-extensions k_S of number fields k unramified outside a finite set $S \subset S_\ell$ of places of k and, we study the $\mathbb{Z}_\ell$-rank of the abelian part of k_S/k and the number of relations of the Galois group $G_S := \mathrm{Gal}(k_S/k)$.

INTRODUCTION

Let k be a number field. In class field theory, the study of ℓ-extension of k with restricted ramification at a finite set S is very classical. Many authors have contributed to unterstand the invariants of k attached to such extensions (e.g Shafarevich [18], Koch [7], [8], Haberland [5] ...). However in the wild ramification case, the standard results are essentially with the assumption that S contains the set S_ℓ of all places of k above ℓ. This case is related to the famous Leopoldt's Conjecture. Let us explain now this conjecture more precisely: The Galois group over k of the maximal abelian ℓ-extension of k unramified outside S_ℓ has a $\mathbb{Z}_\ell$-rank equals to $r_2 + 1 + \delta$ where r_2 is the number of complex places of k, and δ is an non-negative integer, which is zero under Leopoldt's Conjecture. In particular for all number fields k, there exists at least one $\mathbb{Z}_\ell$-extension : namely the cyclotomic extension k^∞. Here we ought to mention Brumer's Theorem [1] (which is a ℓ-adic version of a Theorem of Baker) that proves Leopoldt's Conjecture for abelian fields and a result of Waldschmidt [19] which proves "one half" of Leopoldt's Conjecture. A nice description of all these facts can be found, for instance, in the book of Neukirch-Schmidt-Wingberg [12] and the book of Gras [3].
Let G_S be the Galois group of k_S/k, and let G_S^{ab} be its abelianization. Now concerning the $\mathbb{Z}_\ell$-rank of G_S^{ab} few results have been proved when S is a proper, nonempty subset of S_ℓ. One of our main results (Theorem 1) shows that for a number field k, the choice of S is very important for the $\mathbb{Z}_\ell$-rank. In particular, it is possible to find examples with S small and G_S^{ab} *infinite* and on the other hand for the same field k and prime ℓ, one can find S very large such that G_S^{ab} is *finite*. To make this statement precise, we have to introduce some definitions. For a prime ℓ and a number field k, let $\mathrm{i}_\ell(k)$ be the smallest value of $|S|/|S_\ell|$ such that G_S^{ab} is infinite, and define $\mathrm{I}_\ell(k)$ to be the smallet rational number c, such that for all $|S|$ with $|S|/|S_\ell| \geq c$, G_S^{ab} is infinite.

Theorem 1. *For all prime ℓ,*

$$\sup_{\text{number fields } k} I_\ell(k) - i_\ell(k) = 1.$$

Date: December 12, 2000.
2000 *Mathematics Subject Classification.* Primary: 11R37, 11S37. *Key words and phrases.* S-ramification, $\mathbb{Z}_\ell$-rank, Schanuel ℓ-adic Conjecture.

An other quantity of interest is the cohomological dimension of the Galois groups of the extensions which appear. For example it is well-known that $\overline{k}(\ell)/k^{\infty}$ is free (for $\ell > 2$), where $\overline{k}(\ell)$ is the maximal ℓ-extension of k. Denote by $\widetilde{k_S}$ be the compositum of all $\mathbb{Z}_\ell$-extensions of k contained in k_S. Before giving some examples with $S \subsetneqq S_\ell$ for which $\overline{k}(\ell)/\widetilde{k_S}$ is free, we give a definition:

Definition 2. *Let k/N be a finite Galois extension of number fields with Galois group G. Let $\mathfrak{p}$ be a prime of N. Define $S_{\overline{\mathfrak{p}}} = \{\mathfrak{P} \subset \mathcal{O}_k, \mathfrak{P} \cap \mathcal{O}_N = \mathfrak{p}\} = \{\mathfrak{P}^g, g \in G\}$.*

First let us give a result for extensions of quadratic imaginary fields:

Theorem 3. *Let N be an imaginary quadratic field, $\mathfrak{p}$ be a prime of N and k/N be a finite Galois extension. Let $k_{S_{\overline{\mathfrak{p}}}}$ be the maximal ℓ-extension of k unramified outside $S_{\overline{\mathfrak{p}}}$. Then $\mathrm{Gal}(\overline{k}(\ell)/\widetilde{k_{S_{\overline{\mathfrak{p}}}}})$ is free.*

For the real quadratic case, we prove:

Theorem 4 (Under Schanuel ℓ-adic Conjecture (see §2.3.1))**.** *Let $f(x) \in \mathbb{Z}[x]$ be an irreducible polynomial of degree 4, such that:*

1. *The discriminant d of f is a fundamental discriminant of a real quadratic field; $N = \mathbb{Q}(\sqrt{d})$;*
2. *The roots of f are not real.*

It is well-known that the Galois closure k of f over $\mathbb{Q}$ is of degree 24, and $\mathrm{Gal}(k/N) \simeq \mathrm{A}_4$ (see [9]). Choose a prime number ℓ such that $\left(\frac{d}{\ell}\right) = 1$, and fix a prime $\mathfrak{p}$ of N dividing ℓ.
Let $k_{S_{\overline{\mathfrak{p}}}}$ be the maximal ℓ-extension of k unramified outside $S_{\overline{\mathfrak{p}}}$. Then $\mathrm{Gal}(\overline{k}(\ell)/\widetilde{k_{S_{\overline{\mathfrak{p}}}}})$ is free.

The organization of this paper is as follows. After a preliminary section, in the second section we study the $\mathbb{Z}_\ell$-rank of G_S^{ab} by using techniques based on linear representations inspired by [6]. In the next section, the nice situation where $\mathfrak{p}$ is of degree 1 ($[N_{\mathfrak{p}} : \mathbb{Q}_\ell] = 1$) is studied in detail, and many examples are given. The section 2 finishes with the proof of Theorems 1, 3 and 4. In the last section, we are interested in the group G_S, in particular we consider the situation in which it is possible to give the exact value of the minimal number of the relations of G_S. The case where $\mathrm{cd}(G_S) = 1$ is studied. The results are in connection with the chapter 3 of the book of Gras [3].
This work was supported by a Postdoctoral fellowship position in *Mathematical Sciences Research Institute*[1] at Berkeley and, by *CNRS* and *department A2X of Bordeaux I*.
I thank G. Gras and J.-F. Jaulent for discussions in this topic, F. Hajir and N. Yui for their comments and remarks.

1. Preliminaries

1.1. **Notations.** We fix a prime number ℓ and an algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$.
For a number field k, S_ℓ denotes the set of places of k above ℓ, S is a non-empty subset of S_ℓ, and $\mathfrak{p}$ is a prime ideal of the ring of integers $\mathcal{O}_k$ of k.
Some standard notations are as follows:

[1] Research at MSRI is supported in part by NSF grant DMS-9701755

- $k_\mathfrak{p}$ the completion of k in $\mathfrak{p}$; $N\mathfrak{p}$ the absolute norm, $e_\mathfrak{p}$ and $f_\mathfrak{p}$ the ramification index and the residue degree of $\mathfrak{p}$ in $k/\mathbb{Q}$ respectively;
- $[k_\mathfrak{p} : \mathbb{Q}_\ell] = e_\mathfrak{p} \cdot f_\mathfrak{p}$ be the degree of $\mathfrak{p}$;
- $\mathcal{O}_\mathfrak{p}$ the completion at $\mathfrak{p}$ of the ring of the integers $\mathcal{O}_k$ of k;
- $U_\mathfrak{p}$ the units group of $\mathcal{O}_\mathfrak{p}$;
- $U_\mathfrak{p}^i$ the units of $U_\mathfrak{p}$ congruent to 1 modulo $\mathfrak{p}^i$;
- $\mathcal{G}_\mathfrak{p}$ the pro-ℓ-absolute Galois group of $k_\mathfrak{p}$.
- E_k the units group of k;
- E_k^T the T-units group of k (in the classical sense), where T is a finite set of places of k;
- $k_S^1 = \{x \in k^\times,\ \forall \mathfrak{p} \in S, v_\mathfrak{p}(x-1) \geq 1\}$;
- $E_S^T = k_S^1 \cap E_k^T$ and $E_S = k_S^1 \cap E_k$;
- $\mathbf{\Delta}_S = \{x \in k^\times, (x) = \mathcal{Q}^\ell, x \in k_\mathfrak{p}^\ell, \forall \mathfrak{p} \in S\}/k^{\times\ell}$
- k^∞ the $\mathbb{Z}_\ell$ cyclotomic extension of k;
- k_S the maximal ℓ-extension of k unramified outside S (archimedean places are decomposed);
- k_S^T the maximal subextension of k_S in which all places of T split totally;
- $G_S = \mathrm{Gal}(k_S/k)$ and $G_S{}^{ab} = G_S/[G_S, G_S]$;
- $\overline{k} = \bar{\mathbb{Q}}$, and $\overline{k}(\ell)$ the maximal ℓ-extension of k contained in $\overline{k}$;
- $G_{\overline{k}} = \mathrm{Gal}(\overline{k}/k)$ the absolute Galois group of k.

If A is a $\mathbb{Z}_\ell$ (resp. $\mathbb{Z}$) module of finite type:

- $\mathrm{Tor}(A)$ the $\mathbb{Z}_\ell$-torsion part of A (resp. $\mathbb{Z}$);
- $d_\ell(A) = d(A)$ the $\mathbb{F}_\ell$-rank of A;
- $\mathrm{rk}_{\mathbb{Z}_\ell}$ (resp. $\mathrm{rk}_\mathbb{Z}$), the $\mathbb{Z}_\ell$-rank of A (resp. $\mathbb{Z}$-rank).

1.2. **Leopoldt's Conjecture.** Fix now an algebraic closure $\overline{\mathbb{Q}_\ell}$ of $\mathbb{Q}_\ell$, and for each place $\mathfrak{p}_i$ $(i = 1, \cdots, s)$ of S, we fix σ_i an imbedding of $\mathbb{Q}$ in $k_{\mathfrak{p}_i} \subset \overline{\mathbb{Q}_\ell}$.
Now consider the following homomorphism Θ_S of groups:

$$\begin{array}{rcl} \Theta_S : k_S^1 & \to & \prod_{\mathfrak{p}\in S} \overline{\mathbb{Q}_\ell} \\ x & \mapsto & (\sigma_1(x), \cdots, \sigma_s(x)) \end{array}$$

and let L_S be the Logarithmic map:

$$\begin{array}{rcl} \mathrm{L}_S : \prod_{\mathfrak{p}\in S} U_\mathfrak{p}^1 & \to & \prod_{\mathfrak{p}\in S} k_\mathfrak{p} \simeq \mathbb{Q}_\ell{}^{\sum_\mathfrak{p} e_\mathfrak{p} f_\mathfrak{p}} \\ (x_1, \cdots, x_s) & \mapsto & (\log_\ell(x_1), \cdots, \log_\ell(x_s)) \end{array}$$

Note that the kernel of the logarithmic map is finite.
We can now present Leopoldt's Conjecture:

Conjecture 1. If $S = S_\ell$, then

$$\mathrm{rk}_\mathbb{Z} E_k = \mathrm{rk}_{\mathbb{Z}_\ell} \overline{\Theta_S(E_S)}.$$

Or equivalently $(\mathrm{L}_S(\overline{\Theta_S(E_S)}))$ is a $\mathbb{Z}_\ell$-lattice of $\mathbb{Q}_\ell^n$ with rank $r_1 + r_2 - 1$.
If ℓ splits totally in $k/\mathbb{Q}$, then $\mathrm{L}_S(\Theta_S(E_S)))$ is in the hyperplane of $\mathbb{Q}_\ell^n$ defined by the equation: $x_1 + \cdots + x_n = 0$.

1.3. **On the $\mathbb{Z}_\ell$-rank of G_S^{ab}.** In order to prove Theorem 1, we need to consider subextensions where places split completely.

Theorem 5. *Let T and S be two finite sets of finite places of k ($S \subset S_\ell$). Let k_S^T be the maximal ℓ-extension of k unramified outside S in which all places of T split.*

Put $G_S^T = \mathrm{Gal}(k_S^T/k)$. Then we have the following isomorphism of $\mathbb{Z}_\ell$-modules:

$$G_S^{T^{ab}} \simeq \mathbb{Z}_\ell^t \times \mathrm{Tor}(G_S^{T^{ab}}),$$

where $t = \sum_{\mathfrak{p}\in S}[k_\mathfrak{p} : \mathbb{Q}_\ell] - \mathrm{rk}_{\mathbb{Z}_\ell}\overline{\Theta_S(E_S^T)} = \sum_{\mathfrak{p}\in S}[k_\mathfrak{p} : \mathbb{Q}_\ell] - \mathrm{rk}_{\mathbb{Z}_\ell}L_S(\overline{\Theta_S(E_S^T)})$.

Proof. We want to determine t. By Class field theory $k_S^{T^{ab}}$ is associated to the following sub-group of ideles:

$$k^\times \prod_{\mathfrak{p}\notin S\cup T} U_\mathfrak{p} \prod_{\mathfrak{p}\in T} k_\mathfrak{p}^\times.$$

Remark that archimedean places play no role for the determination of t.
Let $n \geq 1$ be an integer and consider the following exact sequence:

$$1 \longrightarrow \frac{k^\times \prod_{\mathfrak{p}\notin S\cup T} U_p \prod_{\mathfrak{p}\in S} U_\mathfrak{p}^1 \prod_{\mathfrak{p}\in T} k_\mathfrak{p}^\times}{k^\times \prod_{\mathfrak{p}\notin S\cup T} U_\mathfrak{p} \prod_{\mathfrak{p}\in S} U_\mathfrak{p}^n \prod_{\mathfrak{p}\in T} k_\mathfrak{p}^\times} \longrightarrow \frac{J_k}{k^\times \prod_{\mathfrak{p}\notin S\cup T} U_\mathfrak{p} \prod_{\mathfrak{p}\in S} U_\mathfrak{p}^n \prod_{\mathfrak{p}\in T} k_\mathfrak{p}^\times}$$
$$\longrightarrow \frac{J_k}{k^\times \prod_{\mathfrak{p}\notin S\cup T} U_p \prod_{\mathfrak{p}\in S} U_\mathfrak{p}^1 \prod_{\mathfrak{p}\in T} k_\mathfrak{p}^\times} \longrightarrow 1$$

Now $\dfrac{J_k}{k^\times \prod_{\mathfrak{p}\notin S\cup T} U_p \prod_{\mathfrak{p}\in S} U_\mathfrak{p}^1 \prod_{\mathfrak{p}\in T} k_\mathfrak{p}^\times}$ corresponds to the maximal abelian extension $k_S^{T^{tame}}$ of k, unramified outside S, tamely ramified for all places of S and totally decomposed for places of T; it is finite and does not depend on n.
Now $k_S^{T^{ab}}$ is the inductive limit of extensions k_n of k associated to : $k^\times \prod_{\mathfrak{p}\notin S\cup T} U_\mathfrak{p} \prod_{\mathfrak{p}\in S} U_\mathfrak{p}^n \prod_{\mathfrak{p}\in T} k_\mathfrak{p}^\times$.
So we have:

$$1 \longrightarrow \varprojlim_n A_n \longrightarrow \mathrm{Gal}(k_S^{T^{ab}}/k) \longrightarrow \mathrm{Gal}(k_S^{T^{tame}}/k) \longrightarrow 1,$$

where $A_n = \dfrac{k^\times \prod_{\mathfrak{p}\notin S\cup T} U_p \prod_{\mathfrak{p}\in S} U_\mathfrak{p}^1 \prod_{\mathfrak{p}\in T} k_\mathfrak{p}^\times}{k^\times \prod_{\mathfrak{p}\notin S\cup T} U_\mathfrak{p} \prod_{\mathfrak{p}\in S} U_\mathfrak{p}^n \prod_{\mathfrak{p}\in T} k_\mathfrak{p}^\times}$, and so $t = \mathrm{rk}_{\mathbb{Z}_\ell} \varprojlim_n A_n$.
It is easy to see that we have the following continuous isomorphism of groups:

$$A_n \simeq \frac{\prod_{\mathfrak{p}\in S} U_\mathfrak{p}^1}{\Theta_S(E_S^T)\prod_{\mathfrak{p}\in S} U_p^n}, \tag{1}$$

where restrictions are compatible. So

$$\varprojlim_n A_n \simeq \varprojlim_n \frac{\prod_{\mathfrak{p}\in S} U_\mathfrak{p}^1}{\Theta_S(E_S^T)\prod_{\mathfrak{p}\in S} U_p^n}.$$

Now for each integer n, $\Theta_S(E_S^T)\prod_{\mathfrak{p}\in S} U_\mathfrak{p}^n$ is of finite index in $\prod_{\mathfrak{p}\in s} U_\mathfrak{p}^1$, which is a pro-$\ell$-group, and so these sub-groups are closed and we obtain (see for example [16] lemma 1 page 3)

$$\varprojlim_n \frac{\prod_{\mathfrak{p}\in S} U_\mathfrak{p}^1}{\Theta_S(E_S^T)\prod_{\mathfrak{p}\in S} U_p^n} \simeq \frac{\prod_{\mathfrak{p}\in S} U_\mathfrak{p}^1}{\bigcap_n(\Theta_S(E_S^T)\prod_{\mathfrak{p}\in S} U_\mathfrak{p}^n)}.$$

The conclusion comes from the observation that

$$\bigcap_n \Theta_S(E_S^T)\prod_{\mathfrak{p}\in S} U_\mathfrak{p}^n = \overline{\Theta_S(E_S)}.$$

$\square$

1.4. **On the rank and relations of G_S.** We recall the following result:

Proposition 6. *Let k be a number field, ℓ be a prime number and $S \subset S_\ell$. Let k_S be the maximal ℓ-extension of k unramified outside S, $G_S = \mathrm{Gal}(k_S/k)$, and let $d(G_S)$ be the ℓ-rank of G_S and $r(G_S)$ be the minimal number of relations of G_S. Then*

1. $d(G_S) = d_\ell \mathbf{\Delta}_S + \sum_{\mathfrak{p}\in S} U^1_{\mathfrak{p}} - d_\ell E_k$.
2. $$r(G_S) - d(G_S) \leq d_\ell E_k - \delta_k + \delta_S - \sum_{\mathfrak{p}\in S}[k_{\mathfrak{p}} : \mathbb{Q}_\ell],$$
   where $\delta_S = 1$ if k contains μ_ℓ and S is empty, 0 otherwise.
3. *There exists the following surjective homomorphism:*
   $$\mathbf{\Delta}_S \twoheadrightarrow \left(\ker(H^2(G_S, \mathbb{F}_\ell) \to \oplus_{\mathfrak{p}\in S^*} H^2(\mathcal{G}_{\mathfrak{p}}, \mathbb{F}_\ell))\right)^*,$$
   where S^* is S minus one place if k contains μ_ℓ.
4. $r(G_{S_\ell}) - d(G_{S_\ell}) = -(r_2 + 1)$.

Proof. cf. [5], [7], [8]. For $\ell = 2$ in the point 4), see [14]. □

1.5. **First examples.**

Theorem 7. *1) The group G_S^{ab} is finite in the following cases:*

(i) *k is totally real, S does not contain all places above ℓ and Leopoldt's Conjecture is true for k and ℓ.*
(ii) *k is not an imaginary quadratic field, ℓ splits in $k/\mathbb{Q}$ and $S = \{\mathfrak{p}\}$, where $\mathfrak{p}$ is a prime of k above ℓ.*

2) Let k be a totally imaginary field of degree n over $\mathbb{Q}$; $n = 2r_2$. Let ℓ be a prime which splits completely in $k/\mathbb{Q}$: $\ell\mathcal{O}_k = \mathfrak{p}_1 \cdots \mathfrak{p}_n$. Put $S = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_i\}$. If $i \geq r_2$, G_S^{ab} is infinite.
3) Consider $k = \mathbb{Q}(\sqrt{17})$, $S = \{\mathfrak{p}\}$, where $\mathfrak{p}$ is a prime above 2. Then G_S is trivial.

Proof. 1 i) As k is totally real, k has exactly one $\mathbb{Z}_\ell$-extension (by Leopoldt's Conjecture): it is the cyclotomic extension k^∞ of k. In this extension, all places above ℓ are infinitely ramified. So $k_S \cap k^\infty$ is finite over k, and the same is for G_S^{ab}.
1 ii) We use Theorem 5 to note that the abelian part is finite.
2) The number of $\mathbb{Z}_\ell$-extensions contained in G_S^{ab} is $i - r$, where $r \leq r_2 - 1$. So here $i - r \geq 1$.
3) By computation, we find $d(G_S) = 0$. □

2. On the group G_S^{ab}

Before to precise the situation, we recall some facts about linear representations of finite groups.

2.1. **Linear representations.** Let G be a finite group and let M be a $\mathbb{Q}[G]$-module. We will identify the following modules:

1. the $\mathbb{Q}[G]$-module M
2. the $\mathbb{Q}_\ell[G]$ module $\mathbb{Q}_\ell \otimes_{\mathbb{Q}} M$
3. the $\mathbb{C}_\ell[G]$-module $\mathbb{C}_\ell \otimes_{\mathbb{Q}} M$.

Let χ be a $\mathbb{Q}_\ell$-irreducible character of G. One knows that χ is equal to a sum of $\mathbb{C}_\ell$-irreducible characters ψ. More precisely recall the definition of the Schur index m_ψ of a $\mathbb{C}_\ell$-irreducible character ψ : $m_\psi = \min_k[k : \mathbb{Q}_\ell(\psi)]$, the minimum being over all fields k realizing ψ and where $\mathbb{Q}_\ell(\psi)$ is the extension of $\mathbb{Q}_\ell$ generated by the values of ψ. We know some properties of m_ψ, e.g. m_ψ divides the degree n_ψ of ψ. For more details see [2] or [17]. So if χ is a $\mathbb{Q}_\ell$-irreducible character, one has

$$\chi = m_\chi\,(\psi_1 + \cdots + \psi_n)$$

where the characters ψ_i are $\mathbb{C}_\ell$-irreducible conjugates (with the same degree n_χ), and moreover $m_\chi = m_{\psi_1} = \cdots = m_{\psi_n}$ and where finally $n = [\mathbb{Q}_\ell(\chi) : \mathbb{Q}_\ell]$. The character χ is of degree $m_\chi n_\chi[\mathbb{Q}_\ell(\chi) : \mathbb{Q}_\ell]$. If G is abelian then $m_\psi n_\psi = 1$, for all $\mathbb{C}_\ell$-irreducible characters ψ.

Definition 8. *For a finite group G, $\mathrm{Irr}(\mathbb{C}_\ell)$ denotes the set of $\mathbb{C}_\ell$-irreducible characters of G.*

2.1.1. *Regular representation.* The regular representation of G is the representation of G acting on itself by translation. The character χ_{reg} of this representation is known:

$$\chi_{\mathrm{reg}} = \sum_{\psi \in \mathrm{Irr}(\mathbb{C}_\ell)} n_\psi \psi = \mathrm{Ind}_{\{1\}}^G \mathbf{1},$$

where $\mathbf{1}$ is the character of the unit (or trivial) representation of G (Here $\mathrm{Ind}_{\{1\}}^G \mathbf{1}$ means the character of the induced representation from $\{1\}$ to G of the trivial representation).
Now if H is a subgroup of G, then $\mathrm{Ind}_H^G \mathbf{1}$ is contained in χ_{reg}: this can be seen by transitivity formula of induction:

$$\begin{aligned}
\mathrm{Ind}_{\{1\}}^G \mathbf{1} &= \mathrm{Ind}_H^G(\mathrm{Ind}_{\{1\}}^H \mathbf{1}) \\
&= \mathrm{Ind}_H^G(\chi_{\mathrm{reg}}(H)) \\
&= \mathrm{Ind}_H^G(\mathbf{1} + \cdots) \\
&= \mathrm{Ind}_H^G(\mathbf{1}) + \cdots
\end{aligned}$$

To conclude this part, let us give :

Lemma 9. *Let G be a finite group. Let H and H' be two subgroups of G with the same order. Let $I = \mathrm{Ind}_H^G \mathbf{1}$ and $I' = \mathrm{Ind}_{H'}^G \mathbf{1}$. Consider now the decomposition of I and I' as a sum of $\mathbb{C}_\ell$-irreducible characters ψ: $I = \sum_\psi a_\psi \psi$, and $I' = \sum_\psi a'_\psi \psi$. As I and I' appear in χ_{reg}, one has: $a_\psi, a'_\psi \le n_\psi$.*
Then

1. *$H \lhd G$ if and only if $a_\psi = n_\psi$, $\forall \psi \in \mathrm{Irr}(\mathbb{C}_\ell)$;*
2. *If $H \lhd G$, then $I = I'$ if and only if $H = H'$.*

Proof. Let us calculate the scalar product $< I, I' >$ in G: To do this we use [17]. Let S be a representing system on the double coset $H/G\backslash H'$:

$$G = \dot{\bigcup_{s \in S}} HsH'.$$

For $s \in S$, denote ${H_s}' = sH's^{-1} \cap H$, and consider the following representation $\mathbf{1}_s$ of ${H_s}'$:

$$\forall x \in {H_s}',\ \mathbf{1}_s(x) = \mathbf{1}_{H'}(s^{-1}xs),$$

where $\mathbf{1}_{H'}$ is the unit representation of H'. One has in fact $\mathbf{1}_s = \mathbf{1}_{H_s{}'}$. We get:

$$\mathrm{Res}_H(\mathrm{Ind}_{H'}^G \mathbf{1}) = \sum_{s\in S} \mathrm{Ind}_{H_s{}'}^H(\mathbf{1}_s) \tag{2}$$

where Res_H is the restriction to H. By using the Frobenius formula, one has:

$$\begin{array}{rcl} < I, I' > & = & < \mathbf{1}_H, \mathrm{Res}_H(\mathrm{Ind}_{H'}^G \mathbf{1}) >_H \\ & = & < \mathbf{1}_H, \sum_{s\in S} \mathrm{Ind}_{H_s{}'}^H(\mathbf{1}_s) >_H \\ & = & \sum_{s\in S} < \mathbf{1}_H, \mathrm{Ind}_{H_s{}'}^H(\mathbf{1}_s) >_H \\ & = & \sum_{s\in S} < \mathrm{Res}_{H_s{}'}(\mathbf{1}_H), \mathbf{1}_s >_{H_s{}'} \\ & = & |S| \end{array}$$

By a similary computation: $< I, I >= |H/G\backslash H|$.
We can now prove the first point:
1) One knows that $H \lhd G$ if and only if $|G/H| = |H/G\backslash H|$. But $|G/H|$ is of order $\deg(I)$, i.e

$$|G/H| = \sum_\psi a_\psi n_\psi.$$

But we have also the identity:

$$|H/G\backslash H| =< I, I >= \sum_\psi a_\psi^2.$$

The first result follows.
2) By looking at the scalar products $< I, I >$, $< I, I' >$ and $< I', I' >$, one obtains $I = I'$ if and only if

$$\sum_\psi a_\psi^2 = \sum_\psi a_\psi a'_\psi = \sum_\psi (a'_\psi)^2 = |S|.$$

It suffices then to show that for $H \neq H'$, $|S| \neq \sum_\psi a_\psi^2$.
Suppose $H \neq H'$. There exists $h' \in H$ and $\notin H$; a representing system of G/H could be written $\{1, h', \cdots\}$.
Now two elements of G which are in the same class in G/H are in the same class in $H/G\backslash H'$. Moreover 1 and h' are also in the same class in $H/G\backslash H'$. So $|S| \leq |G|/|H| - 1$. To conclude our proof it suffices to note that (by using the fact that $H \lhd G$)

$$\sum_\psi a_\psi^2 = \sum_\psi a_\psi n_\psi = \deg(I) = |G|/|H|.$$

□

2.2. **Presentation of the situation.** Let N be a number field and let k/N be a finite Galois extension with group G. Let S_N be a set of places of N above ℓ and let S be the set of places of k above S_N: $S = \{\mathfrak{P} \subset \mathcal{O}_k, \mathfrak{P} \cap \mathcal{O}_N \in S_N\}$. Then G acts on $U_S^1 := \prod_{\mathfrak{p}\in S} U_\mathfrak{p}^1$ and, Θ_S and $\mathrm{L}_S \circ \Theta_S$ are homomorphisms of $\mathbb{Q}_\ell[G]$-modules. With these facts, we can give some informations on the character of $\Theta_S(E_S)$ and so on the $\mathbb{Z}_\ell$-rank of G_S^{ab}.

Definition 10. *Denote by χ_S the character of $\Theta_S(E_S)$.*

2.2.1. *Character of units.* Let $\mathfrak{p}_{\infty_1}, \cdots, \mathfrak{p}_{\infty_n}$ be the archimedean places of N; $n = r_1(N) + r_2(N)$.
We recall Dirichlet's Theorem for representations (whose proof can be found in [4]):

Proposition 11. *Let k/N be a finite Galois extension of number fields with group G. Let T and S be two finite sets of primes of k on which G acts respectively. The group of T-units of k tensored by $\mathbb{Q}$ is a $\mathbb{Q}[G]$-module with character:*

$$\chi(E_k^T) = \chi(E_S^T) = \sum_{i=1,\cdots,n} \mathrm{Ind}_{D_{\mathfrak{p}_{\infty_i}}}^G(\mathbf{1}) + \sum_{\mathfrak{p}\in T} \mathrm{Ind}_{D_\mathfrak{p}}^G \mathbf{1} - \mathbf{1},$$

where $D_\mathfrak{p}$ is the decomposition group of $\mathfrak{p}$ in k/N.

2.2.2. *Character of U_S^1.*

Lemma 12.

$$\chi(U_S^1) = \sum_{\mathfrak{p}\in S_N} [N_\mathfrak{p} : \mathbb{Q}_\ell]\chi reg.$$

Proof. Fix $\mathfrak{p} \in S_N$. Let $\mathfrak{P}|\mathfrak{p}$. Note first that for $i \geq 1$ the two modules $\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} U_{k_\mathfrak{P}}^1$ and $\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} U_{k_\mathfrak{P}}^i$ are isomorphic because $U_{k_\mathfrak{P}}^1 / U_{k_\mathfrak{P}}^i$ is finite. Moreover for large i, one has the isomorphsim of $\mathbb{Z}_\ell[G]$-modules via the logarithm : $U_{k_\mathfrak{P}}^i \simeq \mathcal{O}_{k_\mathfrak{P}}$. Thus for large i, we get:

$$\prod_{\mathfrak{P}\in S} U_\mathfrak{P}^i \simeq \prod_{\mathfrak{P}\in S} \mathcal{O}_{k_\mathfrak{P}}.$$

One then has the following isomorphisms of G-modules:

$$\begin{array}{rcl}
\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} \prod_{\mathfrak{P}|\mathfrak{p}} U_{k_\mathfrak{P}}^1 & \simeq & \mathbb{Q}_\ell \otimes \prod_{\mathfrak{P}|\mathfrak{p}} U_{k_\mathfrak{P}}^i \\
& \simeq & \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} \prod_{\mathfrak{P}|\mathfrak{p}} \mathcal{O}_{k_\mathfrak{P}} \\
& \simeq & \prod_{\mathfrak{P}|\mathfrak{p}} \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} k_\mathfrak{P} \\
& \simeq & \prod_{\mathfrak{P}|\mathfrak{p}} k_\mathfrak{P} \\
& = & N_\mathfrak{p} \otimes_N k \\
& \simeq & N_\mathfrak{p} \otimes_N N[G] \\
& \simeq & N_\mathfrak{p}[G] \\
& \simeq & \mathbb{Q}_\ell[G] \oplus \cdots \otimes \mathbb{Q}_\ell[G] = [N_\mathfrak{p} : \mathbb{Q}_\ell]\mathbb{Q}_\ell[G].
\end{array}$$

□

2.2.3. *Upper bound for χ_S.* It comes immediately the following:

Proposition 13. *One has for the character χ_S of the $\mathbb{Q}_\ell[G]$-module $\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} \Theta_S(E_S)$:*

$$\chi_S \leq \sum_{\mathfrak{p}\in S_N} [N_\mathfrak{p} : \mathbb{Q}_\ell]\chi reg \wedge \left(\sum_{i=1,\cdots,r(N)} \mathrm{Ind}_{D_{\infty_i}}^G(\mathbf{1}) - \mathbf{1} \right).$$

2.3. Lower bound for χ_S and Schanuel ℓ-adic Conjecture.

2.3.1. *Conjectural results.* The ℓ-adic independance conjecture of Schanuel is at the center of the problem:
Schanuel ℓ-adic Conjecture. Let $x_1, \cdots, x_r \in \overline{\mathbb{Q}_\ell}$ be a family of algebraic numbers, such that the family $\log(x_i)_{i=1,\cdots,r}$ is independent over $\mathbb{Q}$. Then the transcendance degree over $\mathbb{Q}$ of $\mathbb{Q}(\log_\ell(x_1), \cdots, \log_\ell(x_r))$ is r.
Under this Conjecture we can prove the following result which can be found, for example, in [6]:

Proposition 14. *Let M_0 be a $\mathbb{Q}[G]$-module of finite type included in k_S^1. Let $m = \dim_{\mathbb{Q}_\ell}(\chi reg \wedge \chi(M_0))$. With Schanuel's Conjecture one has:*

$$\mathrm{rk}_{\mathbb{Z}_\ell}(L_S(\Theta_S(M_0))) \geq m.$$

Remark 2.1. Proposition 14 shows that Schanuel's Conjecture implies Leopoldt's Conjecture.

To prove the Proposition 14 we need a Lemma:

Lemma 15 ([6]). *Let $\varepsilon \in M_0$. There exists a $\mathbb{Q}[G]$-submodule M of k_S^1 with $\chi(M) = \chi reg$ and such that the principal $\mathbb{Q}[G]$-module $\mathbb{Q}[G] \cdot \varepsilon$ is a submodule of M.*

Proof. Let $\mathfrak{q}$ be a prime of N which splits completely in k/N. Take T to be the set of primes of k above $\mathfrak{q}$ and consider E_S^T. The character of $\mathbb{Q} \otimes E_S^T$ contains χ_{reg}. Let M be the maximal principal submodule of $\mathbb{Q} \otimes (E_S^T + M_0)$ containing ε. Then the character of M is $\chi(E_S^T + M_0) \wedge \chi_{\text{reg}} = \chi_{\text{reg}}$. □

Proof. (Proposition 14)
It suffices to prove it for $S_N = \{\mathfrak{p}\}$. Let $S = \{\mathfrak{P}_1, \cdots, \mathfrak{P}_s\}$ be the primes of k above $\mathfrak{p}$.
Recall that a $\mathbb{Q}[G]$-module is principal if and only if its character appears in χ_{reg}. Let $\chi = \chi_{\text{reg}} \wedge \chi(M_0)$. It is the character of a $\mathbb{Q}[G]$-principal module M_1, thus there exists $\varepsilon \in M_0$ such that $M_1 = \mathbb{Q}[G] \cdot \varepsilon$. By Lemma 15, there exists a $\mathbb{Q}[G]$-module M containing M_1 and with representation χ_{reg}. We will show that $\overline{\Theta_S(M)}$ has maximal $\mathbb{Q}_\ell$-rank $|G|$, and this would imply that $\overline{\Theta_S(M_1)}$ has $\mathbb{Q}_\ell$-rank m.
Let $(x_1, \cdots, x_n)$ be a $\mathbb{Q}$-basis of M such that $x_i = x^{g_i}$, with $g_i \in G$.
Suppose the existence of a linear relation on $\mathbb{Z}_\ell$ between the images of x_i by $\mathrm{L}_S \circ \Theta_S$. We may write such a linear relation by:

$$\sum_{i=1,\cdots,m} a_i \mathrm{L}_S(\Theta_S(x_i)) = 0,$$

with $a_i \in \mathbb{Z}_\ell$. Then one has:

$$\forall \sigma_j, \sum_{i=1,\cdots,m} a_i \log_\ell(\sigma_j(x_i)) = 0.$$

Therefore we obtain:

Lemma 16.
$$\forall g \in G, \sum_{i=1,\cdots,m} a_i \log_\ell(\sigma_1({x_i}^g)) = 0.$$

Proof. Let $g \in G$. If g is in the decomposition group of $\mathfrak{P}_1$ in N/k, then there exists $g' \in \mathrm{Gal}(k_{\mathfrak{P}_1}/N_{\mathfrak{p}})$ such that $\sigma_1(y^g) = \sigma_1(y)^{g'}, \forall y \in k$.
Then

$$\begin{array}{rcl}\sum_i a_i \log_\ell(\sigma_1({x_i}^g)) & = & \sum_i a_i \log_\ell(\sigma_1(x_i))^{g'} \\ & = & \sum_i a_i (\log_\ell(\sigma_1(x_i)))^{g'} \\ & = & (\sum_i a_i (\log_\ell(\sigma_1(x_i)))^{g'} \\ & = & 0\end{array}$$

Now as $|S_N| = 1$, G acts transitively on S. Consequently $\sigma_1(y^g) = g' \cdot \sigma_{i(g)}(y)$ where g' is in $\mathrm{Gal}(k_{\mathfrak{P}_{i(g)}}/N_{\mathfrak{p}})$, and we conclude our proof as before.

□

Now consider the square matrix $\mathcal{M}$ of size $|G| \times |G|$: $(\log(\sigma_1(x_i{}^g)))_{g\in G, i=1,\cdots,|G|}$. The determinant of this matrix is zero (by Lemma 16). It is a polynomial on ℓ-adic logarithms of independent algebraic numbers. If we show that this polynomial is not the zero polynomial then we obtain a contradiction to Schanuel's Conjecture.

Lemma 17. *Put $X_g = x^g$, for $g \in G$. Let $\mathcal{M}'$ be the matrix $(X_{g\cdot g'})_{g,g'\in G}$ and let $P((X_g)_{g\in G})$ be the determinant of this matrix. One has: $\det(\mathcal{M}) = P((x^g)_g)$. Then P is not the zero polynomial.*

We can assume that $\mathcal{M}'$ can be written:

$$\begin{pmatrix} X_1 & X_\sigma & \cdots & X_\tau \\ X_{\sigma^{-1}} & X_1 & \cdots & X_{\sigma^{-1}\tau} \\ \cdots & \cdots & \cdots & \cdots \\ X_{\tau^{-1}} & \cdots & \cdots & X_1 \end{pmatrix}$$

Then the determinant of $\mathcal{M}$ is a monic polynomial in X_1 of degree $|G|$.

$\square$

2.3.2. *Unconditionnal results.* First recall the ℓ-adic version of Baker's Theorem proved by Brumer [1] on the independance of logarithms:

Proposition 18. *Let $(\alpha_i)_{i=1,\cdots,r}$ be a family of non zero algebraic numbers such that there are linearely multiplicatively independent. Look at these elements in $\overline{\mathbb{Q}_\ell}$. Then the family $(\log_\ell \alpha_i)_{i=1,\cdots,r}$ is $\overline{\mathbb{Q}}$-independent.*

As noted in [6], we have:

Proposition 19. *For all noetherian $\mathbb{Z}[G]$-module M of k_S^1, the character of the $\mathbb{Q}_\ell[G]$-module $\mathbb{Q}_\ell \otimes_\mathbb{Z} \Theta_S(M)$ contains all $\mathbb{Q}_\ell$-irreducible character χ represented in $\chi(M)$. More precisely:*

$$\begin{aligned} \chi(\Theta_S(M)) &\geq \sum_{\chi \leq \chi(M)} \chi \\ &\geq \sum_{\substack{\psi \leq \chi(M) \\ \psi \in \mathrm{Irr}(\mathbb{C}_\ell)}} m_\psi \psi \end{aligned}$$

Proof. Let M_0 be a principal $\mathbb{Q}[G]$-sub module of M with character $\chi(M_0)$: $M_0 = \mathbb{Q}_\ell[G] \cdot x$, with $x \in M_0$. Let χ be a $\mathbb{Q}_\ell$-irreducible character dividing $\chi(M_0)$. The values of χ are in $\bar{\mathbb{Q}}$. One has

$$\sum_{g\in G} \chi(g^{-1}) g \cdot x \neq 1. \tag{3}$$

Let $(x_1, \cdots, x_r)$ be a $\mathbb{Q}$-basis of M_0. Look at the projection on χ of the image of x by $\mathrm{L}_S(\Theta_S)$: If it is trivial, it implies that

$$\mathrm{L}_S(\Theta_S(\sum_{g\in G} \chi(g^{-1}) g \cdot x)) = 0.$$

Look at this vector equality on the first component to obtain:

$$\log_\ell(\sigma_1(\sum_{g\in G} \chi(g^{-1}) g \cdot x)) = 0.$$

Now we write $g \cdot x$ in the $\mathbb{Q}$-basis $(x_1, \cdots, x_r)$ to obtain

$$\sum_{i=1,\cdots,r} a_i \log_\ell(\sigma_1(x_i)) = 0,$$

where a_i are algebraic over $\mathbb{Q}$. Moreover this relation is not trivial by (3). Then Theorem of Baker-Brumer yields a contradiction. So the character χ appears in χ_S. ☐

To finish, in our case we can apply a ℓ-adic version of Theorem 1.16 of Chapter 1 of [20] (I thank M. Waldschmidt for telling me the existence of this version):

Proposition 20. *Let $(x_{i,j})_{\substack{i=1,\cdots,d\\ j=1,\cdots,l}}$ be a family of algebraic numbers. Let $l(\cdot) = L_S(\sigma_1(\cdot))$ be the logarithmic on $\overline{\mathbb{Q}_\ell}$. Assume that for all $(t_i)_{i=1,\cdots,d} \in \mathbb{Z}^d \backslash \{0\}$ and $(s_i)_{i=1,\cdots,l} \in \mathbb{Z}^l \backslash \{0\}$ we have:*

$$\sum_{i,j} t_i s_j x_{i,j} \neq 0.$$

Then the rank of the matrix $(l(x_{i,j})))_{\substack{i=1,\cdots,d\\ j=1,\cdots,l}}$ is at least $\dfrac{ld}{l+d}$.

As consequence of Proposition 20, we have:

Theorem 21. *Let M be a $\mathbb{Q}[G]$-module of finite type included in k_S^1. Let χ be a $\mathbb{Q}$-character of $\mathbb{Q}[G]$-module such that $\chi \leq \chi_{reg}$. If $m \cdot \chi \leq \chi(M)$, then*

$$\mathrm{rk}_{\mathbb{Z}_\ell} L_S(\Theta_S(M)) \geq \frac{m \cdot n_\chi}{m + n_\chi}.$$

Proof. As $m \cdot \chi \leq Reg$, there exists $x_1, \cdots, x_m$ in M such that:

1. $\chi(\mathbb{Q}[G] \cdot x_i) = \chi$;
2. $\mathbb{Q}[G] \cdot x_i = \mathbb{Q} < x_i^{(1)}, \cdots, x_i^{(d)} >$, where $d = n_\chi$.
3. The elements $x_i^{(j)}$ can be chosen as to be the Galois conjugates of x_i: There exists $s_1, \cdots, s_d \in G$ such that
$$\forall i, j\ ,\ x_i^{(j)} = s_j \cdot x_i = x_i{}^{s_j}.$$
4. The family $(x_i^{(j)})_{\substack{i=1,\cdots,m\\ j=1,\cdots,d}}$ is linearly $\mathbb{Q}$-independants.

Put $X_i = \mathrm{L}_S(\Theta_S(x_i))$. We will prove that the $\mathbb{Q}_\ell$-rank of $\{X_1, \cdots, X_m\}$ is at least $r = \dfrac{m \cdot n_\chi}{m + n_\chi}$.
Suppose that the rank is less than $r - 1$. That means that for all sub-families $\{X_{i_1}, \cdots, X_{i_s}\}$ with $s \leq r-1$, there exists $(a_j)_j \in \mathbb{Q}_\ell^{r-1}$ such that

$$\sum_{j=1}^{r-1} a_j X_{i_j} = 0.$$

Using the same method as for the proof of Lemma 16, one obtains:

$$\forall g \in G,\ \sum_{j=1}^{r-1} a_j \log_\ell(\sigma_1(g \cdot x_{i_j})) = 0. \tag{4}$$

Now look at the matrix $\widetilde{\mathcal{M}}$ of size $d\times m$ defined by: $\widetilde{\mathcal{M}}_{j,i} = (\log_\ell(\sigma_1(x_i^{(j)})))_{\substack{j=1,\cdots,d \\ i=1,\cdots,m}}$: its rank is at least r by Proposition 20. Moreover $\widetilde{\mathcal{M}}$ is a sub-matrix of $\mathcal{M} = (\log_\ell(\sigma_1(g\cdot x_i)))_{\substack{g\in G \\ i=1,\cdots,d}}$ (of size $|G|\times m$) with rank at most $r-1$ by (4). And so we obtain a contradiction. □

3. The degree one case

In all this section, k/N is a finite Galois extension and $\mathfrak{p}$ a prime of N of degree 1. We recall:

Definition 22. *Let k/N be a Galois extension of number fields with group G and $\mathfrak{p}\subset\mathcal{O}_k$. Define $S_{\bar{\mathfrak{p}}} = \{\mathfrak{p}^g, g\in G\}$.*

We first will show what Schanuel Conjecture, Baker-Brumer Theorem and Theorem 21 imply for the $\mathbb{Z}_\ell$-rank of $G^{ab}_{S_{\bar{\mathfrak{p}}}}$. After this, we will give some examples (§3.3 and 3.4) and conclude by the proof of Theorem 1 (§3.5).

3.1. With Schanuel's Conjecture.

Proposition 23. *Let k/N be a Galois extension of number fields with group G, $\mathfrak{p}$ be a prime of N of degree 1. Let M_0 be a $\mathbb{Q}[G]$-module of finite type included in $k^1_{S_{\bar{\mathfrak{p}}}}$. Then Schanuel's conjecture implies: $\chi(\Theta_{S_{\bar{\mathfrak{p}}}}(M_0)) = \chi_{reg}\wedge\chi(M_0)$.*

Proof. Consequence of Proposition 14. □

Theorem 24. *Let k/N be a Galois extension of number fields, $\mathfrak{p}$ be a prime of N of degree 1. Assume $[N:\mathbb{Q}]>2$ and $r_2(N)>0$. Then Schanuel's Conjecture implies that $G^{ab}_{S_{\bar{\mathfrak{p}}}}$ is finite.*

Proof. Application of Proposition 23 and Theorem 5. □

3.2. Unconditional results.

Theorem 25. *Let k/N be an* **abelian** *extension of number fields with group G. Let ℓ be a prime such that there exists $\mathfrak{p}\in N$ above ℓ of degree 1. Then*

$$G^{ab}_{S_{\bar{\mathfrak{p}}}} \simeq \mathbb{Z}_\ell^t \times \mathrm{Tor}(G^{ab}_{S_{\bar{\mathfrak{p}}}}),$$

where $t = |G| - |\psi\in\mathrm{Irr}(\mathbb{C}_\ell), \psi\leq\chi(E_k)|$. In particular if N is totally real, k is totally complex and if all groups of decomposition of archimedean places are equals, then $t=|H|/2$. But if $[N:\mathbb{Q}]>2$ and if $r_2(N)>0$, then $t=0$.

Proof. This is a direct application of Propositions 13 and 19. □

To finish, we give some applications of Theorem 21:

Theorem 26. *Let N be a number field k/N be a finite Galois extension with group G. Put $n=r_1(N)+r_2(N)$. Assume that $n\geq 2$ and that all decomposition groups for archimedean places are trivial in k/N. Let $\mathfrak{p}$ be a prime of $\mathcal{O}_N$ with degree 1. Then $|G| < \dfrac{1+\sqrt{3+4n}}{2}$ implies $G^{ab}_{S_{\bar{\mathfrak{p}}}}$ finite.*

Proof. By hypothesis, in the extension k/N the character of the units contains $(n_1-1)\chi_{\mathrm{reg}}$. By Theorem 21, one has:

$$\mathrm{rk}_{\mathbb{Z}_\ell}\mathrm{L}_S(\Theta_S(E_S)) \geq \frac{|G|(n-1)}{|G|+n-1}.$$

Now by Theorem 5, the $\mathbb{Z}_\ell$-rank of $G^{ab}_{S_{\bar{\mathfrak{p}}}}$ is trivial if and only if

$$|G| - \mathrm{rk}_{\mathbb{Z}_\ell}\mathrm{L}_S(\Theta_S(E_S)) < 1.$$

And in particular this is the case, if $|G| < \dfrac{1+\sqrt{3+4n}}{2}$.

□

3.3. **Compositum of $\mathbb{Z}_\ell$-extensions.**

Definition 27. *Let K/k be a pro-ℓ-extension of a number field k. We denote by $\widetilde{K}$ the compositum of $\mathbb{Z}_\ell$-extensions of k contained in K and by $\widetilde{\mathrm{Gal}(K/k)}$ the Galois group $\mathrm{Gal}(\widetilde{K}/k)$. In particular $\widetilde{\mathrm{Gal}(K/k)} \simeq \mathbb{Z}_\ell^t$.*

We have immediately these properties:

Proposition 28. *1) If $S \cap S' = \emptyset$, then $\mathrm{rk}_{\mathbb{Z}_\ell}\mathrm{Gal}(\widetilde{k_S k_{S'}}/k) = \mathrm{rk}_{\mathbb{Z}_\ell}\mathrm{Gal}(\widetilde{k_S}/k) + \mathrm{rk}_{\mathbb{Z}_\ell}\mathrm{Gal}(\widetilde{k_{S'}}/k)$.*
2) If $S \neq S_\ell$, then $\mathrm{rk}_{\mathbb{Z}_\ell}\mathrm{Gal}(\widetilde{k^\infty k_S}/k) = 1 + \mathrm{rk}_{\mathbb{Z}_\ell}\mathrm{Gal}(\widetilde{k_S}/k)$.

We can present:

Theorem 29. *Let k/N be a Galois extension of number fields with group G. Let ℓ be a prime number totally decomposed in $N/\mathbb{Q}$. Assume that Schanuel Conjecture is true.*
Then $\widetilde{k_{S_\ell}} = k^\infty \cdot \prod_{\mathfrak{p}\in S_\ell} \widetilde{k_{S_{\bar{\mathfrak{p}}}}}$ if and only if:
(i) k is totally real.
Or,
(ii) N is totally real, k is totally imaginary and for all i,j, $\mathrm{Ind}^G_{D_{\mathfrak{p}_{\infty i}}}(\mathbf{1}) = \mathrm{Ind}^G_{D_{\mathfrak{p}_{\infty j}}}(\mathbf{1})$.
Moreover if for every $\mathbb{C}_\ell$-irreducible characters ψ dividing $\mathrm{Ind}^G_{D_{\mathfrak{p}_\infty}}(\mathbf{1})$, ψ divises it $\deg(\psi)$ times (which is equivalent to $D_{\mathfrak{p}_\infty}$ is distinguished in G for an archimedean place $\mathfrak{p}_\infty$ cf. lemma 9) then k is a CM-field.
Or,
(iii) N is a imaginary quadratic field and $[k:N]=2$.

Proof. By Leopoldt's Conjecture (which is a consequence of Schanuel's Conjecture) the $\mathbb{Z}_\ell$-rank of $G^{ab}_{S_\ell}$ is r_2+1.
By Schanuel's Conjecture (Proposition 23), Proposition 28 and Theorem 5, the number of $\mathbb{Z}_\ell$-extensions coming from the compositum of the fields $k_{S_{\bar{\mathfrak{p}}}}$ with the cyclotomic extension k^∞, is:

$$r_1 + 2r_2 - [N:\mathbb{Q}]\cdot \dim_{\mathbb{Q}_\ell}\left((-\mathbf{1} + \sum_i \mathrm{Ind}^G_{D_{\mathfrak{p}_{\infty i}}}(\mathbf{1})) \wedge \chi\mathrm{reg}\right) + 1.$$

So we want:

$$r_1 + r_2 = [N:\mathbb{Q}]\cdot \dim_{\mathbb{Q}_\ell}\left((-\mathbf{1} + \sum_i \mathrm{Ind}^G_{D_{\mathfrak{p}_{\infty i}}}(\mathbf{1})) \wedge \chi\mathrm{reg}\right). \tag{5}$$

1) The first case is trivial.
2) Let (r_1, r_2) be the signature of k. Assume that $r_2 > 0$ and that $r_1(N)+r_2(N) \geq 2$. That means in particular that N is not an imaginary quadratic field. Suppose

moreover that at least one archimedean place $\mathfrak{p}_{\infty_i}$ of N splits in k/N. As $\mathrm{Ind}_{D_{\mathfrak{p}_\infty}}^G(\mathbf{1})$ contains the unit representation $\mathbf{1}$ and that $r_1(N)+r_2(N)\geq 2$, we have

$$\dim_{\mathbb{Q}_\ell}\left((-\mathbf{1}+\sum \mathrm{Ind}_{D_{\mathfrak{p}_{\infty_i}}}^G(\mathbf{1}))\wedge \chi\mathrm{reg}\right)=|G|.$$

So (5) becomes:

$$\begin{array}{rcl} r_1+r_2 & = & [N:\mathbb{Q}]\cdot|G| \\ & = & [k:\mathbb{Q}]=r_1+2r_2 \end{array}$$

and this is a contradiction. So N is totally real and k totally complex. The equality (5) now becomes:

$$\begin{array}{rcl} \dfrac{|G|\cdot[N:\mathbb{Q}]}{2} & = & r_2 \\ & = & [N:\mathbb{Q}]\cdot\dim_{\mathbb{Q}_\ell}\left(\chi(E_S)\wedge\chi\mathrm{reg}\right). \end{array}$$

Now, as N has at least two archimedean places,

$$(-\mathbf{1}+\sum \mathrm{Ind}_{D_{\mathfrak{p}_{\infty_i}}}^G(\mathbf{1}))\wedge\chi\mathrm{reg}=(\sum \mathrm{Ind}_{D_{\mathfrak{p}_{\infty_i}}}^G(\mathbf{1}))\wedge\chi\mathrm{reg}.$$

Recall that $\mathrm{Ind}_{D_{\infty_i}}^G(\mathbf{1}))$ is in $\chi\mathrm{reg}$ and is of dimension $|G|/2$. Suppose that there exist i and j, such that

$$\mathrm{Ind}_{D_{\mathfrak{p}_{\infty_i}}}^G(\mathbf{1}))\neq \mathrm{Ind}_{D_{\mathfrak{p}_{\infty_j}}}^G(\mathbf{1});$$

One would have

$$\dim_{\mathbb{Q}_\ell}\left((\sum \mathrm{Ind}_{D_{\mathfrak{p}_{\infty_i}}}^G(\mathbf{1}))\wedge\chi\mathrm{reg}\right)>|G|/2,$$

and so a contradiction.
If all irreducible characters ψ dividing $\mathrm{Ind}_{D_{\mathfrak{p}_\infty}}^G(\mathbf{1})$, occur with multiplicity $\deg(\psi)$, by Lemma 9, one has $D_{\mathfrak{p}_{\infty_i}}=D_{\mathfrak{p}_{\infty_j}}$ $\forall i,j$. And so k is a CM field with $k^+=k^{D_{\mathfrak{p}_{\infty_i}}}$, for one i.
3) Now if N an imaginary quadratic field, the equality (5) becomes

$$r_2=[N:\mathbb{Q}](|G|-1),$$

and the last case occurs.

□

3.4. **Behavior of the $\mathbb{Z}_\ell$-rank of G_S^{ab} in a $\mathbb{Z}_\ell$-extension.** We will look at the following situation. Let us fixe k be a number field such that $r_1+r_2\geq 2$, and let K be a $\mathbb{Z}_\ell$-extension of k; $\Gamma=\mathrm{Gal}(K/k)$. Let $S\subset S_\ell$ be a set of places of k. Denote by k_S^{ab} the maximal abelian ℓ-extension of k unramified outside S ; $\mathrm{X}_S=G_S^{ab}=\mathrm{Gal}(k_S^{ab}/k)$.
More generally put $\mathrm{X}_{n,S}=\mathrm{Gal}(k_{n,S_n}^{ab}/k_n)$ where $\cup_n k_n=K$ with $[k_n:k]=\ell^n$, and $S_n=\{\mathfrak{P}\subset\mathcal{O}_{k_n},\mathfrak{P}\cap\mathcal{O}_k\in S\}$. Also put $\mathrm{X}_{\infty,S}=\varprojlim_n \mathrm{X}_{n,S}$ (the restriction map is the norm).
Let $\Lambda=\mathbb{Z}_\ell[[T]]$. We know that $\mathrm{X}_{\infty,S}$ is a finitely generated Λ-module pseudo-isomorphic to

$$\Lambda^r\oplus(\oplus_i\Lambda/\ell^{n_i})\oplus(\oplus_i\Lambda/f_i),$$

f_i being polynomials of $\mathbb{Z}_\ell[T]$. For more details see, for example, [21].
We will determine r in three cases:

3.4.1. Consider the following case: $S = \{\mathfrak{p}\}$ with $\mathfrak{p}$ of degree 1.
We look at the action of $G_n = \mathrm{Gal}(k_n/k)$. As in a $\mathbb{Z}_\ell$-extension, archimedean places are decomposed, one has $\chi(E_{k_n}) = (r_1 + r_2)\chi_{\mathrm{reg}}(G_n) - \mathbf{1}$ and so by Theorem 25, for all n the $\mathbb{Z}_\ell$-rank of $\mathrm{X}_{n,S}$ is trivial. The group $\mathrm{X}_{n,S}$ is then finite and so $r = 0$.

3.4.2. Assume that k is a CM field. Denote by k^+ the maximal real subfield of k. Take $\mathfrak{p}$ in k^+ of degree 1. Take for S all the places of k above $\mathfrak{p}$, and $K = k^\infty$ be the cyclotomic $\mathbb{Z}_\ell$-extension of k. Then for all n, $\mathrm{Gal}(k_n/k^+) \simeq \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. By using Theorem 25, one obtains

$$\mathrm{X}_{n,S} \simeq \mathbb{Z}_\ell^{\ell^n} \times (\text{finite}).$$

So in this case $r = 1$.

3.4.3. Take $\ell > 2$. Assume that k is a CM field (non quadratic). Denote by k^+ the maximal real subfield of k. Let $\mathfrak{p}$ in k^+ of degree 1, and for S all the places of k above $\mathfrak{p}$. Here we have $\mathrm{X}_S \simeq \mathbb{Z}_\ell \times (\text{finite})$. Take then K as being the $\mathbb{Z}_\ell$-extension unramified outside S.
The extensions k_n/k^+ are Galois (because $\mathrm{rk}_{\mathbb{Z}_\ell}\mathrm{X}_S = 1$) with a non abelian group (because k^+ is totally real and so $G_{\{\mathfrak{p}\}}^{ab}(k^+)$ is finite) isomorphic to the diedral group $D_{2\ell^n} = \langle x, y, x^{l^n} = 1, y^2 = 1, yxy = x^{-1}\rangle$. This group has $(\ell^n - 1)/2 + 2$ $\mathbb{C}_\ell$-irreducible representations. Two of them are of degree 1: $\mathbf{1}$ and $\psi_0(x) = 1$ $\psi_0(y) = -1$, and $(\ell^n - 1)/2$ representations ρ_h are of degree 2 (for $h = 1, \cdots, (\ell^n - 1)/2$) :

$$\rho_h(x) = \begin{pmatrix} \zeta^{-h} & 0 \\ 0 & \zeta^h \end{pmatrix}, \ \rho_h(y) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

where ζ is a ℓ^n-primitive root of 1.
Now we can note that $\sum_h \rho_h$ is a $\mathbb{Q}_\ell$-irreducible character of degree $\ell^n - 1$ (The Schur index of ρ_h is 1).
For an archimedean place $\mathfrak{p}_\infty$ of k^+ the decomposition group $D_{\mathfrak{p}_\infty} = \langle x^a y\rangle$ in $\mathrm{Gal}(k_n/k^+)$ is of order 2. As ℓ is odd, the subgroups of order 2 of $D_{2\ell^n}$ are conjugated and so:

$$\chi(E_{k_n}) = [k^+ : \mathbb{Q}]\left(\sum_h \rho_h + \mathbf{1}\right) - \mathbf{1}.$$

One then has $\chi(\Theta_{S_n}(E_{k_n})) = \mathbf{1} + \sum_h \rho_h$ or $\chi(\Theta_{S_n}(E_{k_n})) = \mathbf{1} + 2\sum_h \rho_h$. In the first case $\mathrm{X}_{n,S} = \mathbb{Z}_\ell^{\ell^n} \times (\text{finite})$ and in the second $\mathrm{X}_{n,S} = \mathbb{Z}_\ell \times (\text{finite})$.
Thus $\mathrm{Gal}(k_{n,S_n}^{ab}/k_\infty) \simeq \mathbb{Z}_\ell^{\ell^n - 1} \times (\text{finite})$ in the first case, and $\mathrm{Gal}(k_{n,S_n}^{ab}/k_\infty)$ is finite in the second case.
Now we have to remark that $\mathrm{Gal}(k_{n,S_n}^{ab}/k_\infty) \simeq \mathrm{X}_{\infty,S}/\omega_n$ where $\omega_n = (1+T)^{\ell^n} - 1$ (cf. [21] for example) and this implies:

$$\mathrm{rk}_{\mathbb{Z}_\ell}\mathrm{Gal}(k_{n,S_n}^{ab}/k_\infty) = r \cdot \ell^n + a,$$

with $a \in \mathbb{N}$. Only the second case is possible.
In conclusion we have for all n, $\chi(\Theta_{S_n}(E_{k_n})) = \mathbf{1} + 2\sum_h \rho_h$ and $r = 0$.

Remark 3.1. Schanuel's Conjecture implies in the last example that $\chi(\Theta_{S_n}(E_{k_n})) = \mathbf{1} + 2\sum_h \rho_h$.

3.5. **Proof of Theorem 1.** We recall the definition of $\mathrm{i}_\ell(k)$ and $\mathrm{I}_\ell(k)$:

Definition 30. (i) $i_\ell(k) = \min_{S\subset S_\ell}\{\frac{|S|}{|S_\ell|}, G_S^{ab}$ *is infinite*$\}$;

(ii) $I_\ell(k) = \min c$, *such that* $\forall S \subset S_\ell$, $\frac{|S|}{|S_\ell|} \geq c \Longrightarrow G_S^{ab}$ *is infinite.*

In the previous sections, we have gathered much data concerning these quantities.
a) First assume $\ell > 2$.
Consider the polynomial $f(x) = x^{\ell+1} - x^2 + x + \ell$.
We can note that all the roots of f are complex. Moreover, if we look at f modulo ℓ, we find

$$f(x) = x(x^\ell - x + 1) \ \in \mathbb{F}_\ell[x] \tag{6}$$

which is the decomposition into irreducible polynomials in $\mathbb{F}_\ell[x]$. And this guarantees the irreducibility of f in $\mathbb{Q}(x)$.
Let $N = \mathbb{Q}(\delta)$, where
theta is a root of f. Then N is of degree $\ell + 1$ on $\mathbb{Q}$ and totally imaginary.
The factorization (6) also gives us the factorization of $\ell\mathcal{O}_N$:

$$\ell\mathcal{O}_N = \mathfrak{p}_1\mathfrak{p}_2,$$

where $\mathfrak{p}_1$ is of degree 1, and $\mathfrak{p}_2$ of degree ℓ.
Put $T = \{\mathfrak{p}_1\}$ and $S = \{\mathfrak{p}_2\}$. Consider now, the maximal ℓ-extension k_S^T, S-ramified and T-decomposed of k; $G_S^T = \mathrm{Gal}(k_S^T/k)$. Then the $\mathbb{Z}_\ell$-rank of ${G_S^T}^{ab}$ is at least (by Theorem 5)

$$[N_{\mathfrak{p}_2}/\mathbb{Q}_\ell] - (r_1(k) + r_2(k) - 1 + |T|) = \ell - (\ell+1)/2 \geq 1.$$

Then let K be a $\mathbb{Z}_\ell$-extension of N included in k_S^T.
Denote now by k_n the subfield of K defined by $[k_n : N] = \ell^n$. As the class group of N is finite, there exists n_0, such that $\mathfrak{p}_2$ is totally ramified in K/k_{n_0}.
Now we consider $n \geq n_0$. For a field k_n, we have: $|T(k_n)| = \ell^n$, $|S(k_n)| \leq \ell^{n_0}$, and

$$\ell^n + 1 \leq |S_\ell(k_n)| = |T(k_n)| + |S(k_n)| \leq \ell^n + \ell^{n_0}.$$

The field k_n admits K/k_n as a $\mathbb{Z}_\ell$-extension which is ramified only at $S(k_n)$, and so

$$\mathrm{i}_\ell(k_n) \leq \frac{\ell^{n_0}}{\ell^n + 1}.$$

Now we apply Proposition 25 in the extension k_n/N with $S_N = T = \{\mathfrak{p}_1\}$. The $\mathbb{Z}_\ell$-rank of ${k_n^{ab}}_{S_{\bar{\mathfrak{p}}_1}}/k_n$ is trivial, and so

$$\mathrm{I}_\ell(k_n) > \frac{\ell^n}{|S_\ell(k_n)|} \geq \frac{\ell^n}{\ell^n + \ell^{n_0}}.$$

Letting $n \to \infty$, we have the result.
b) For $\ell = 2$ we can apply the same argument as above by taking for example $f(x) = x^4 + x^2 + x + 2$.

3.6. **Proof of Theorems 3 and 4.** We first prove:

Theorem 31. *Let k be a number field (for $\ell > 2$, assume that k is totally complex) and $S \subset S_\ell$ such that:*

1. *For all $\mathfrak{p} \notin S$, $\mathrm{rk}_{\mathbb{Z}_\ell} {G_S^{\{\mathfrak{p}\}}}^{ab} < \mathrm{rk}_{\mathbb{Z}_\ell} G_S^{ab}$ ($\Leftrightarrow \mathrm{rk}_{\mathbb{Z}_\ell}\Theta_S(E_S^{\{\mathfrak{p}\}}) > \mathrm{rk}_{\mathbb{Z}_\ell}\Theta_S(E_S)$);*
2. *For all $S' \subsetneq S$, $\mathrm{rk}_{\mathbb{Z}_\ell} G_S^{ab} > \mathrm{rk}_{\mathbb{Z}_\ell} {G_{S'}}^{ab}$.*

Then $\mathrm{Gal}(\overline{k}(\ell)/\widetilde{k_S})$ *is free.*

Proof. Let $\widetilde{k_S}$ (resp. $\widetilde{k_S^T}$, for a finite set T of places of k) be the compositum of all $\mathbb{Z}_\ell$-extensions of k contained in k_S (resp. in k_S^T).

Lemma 32. *With the conditions 1 and 2 of Theorem 31, one has for all finite places* $\mathfrak{p}$ *of* k, $[\widetilde{k_S}_{\mathfrak{p}} : k_{\mathfrak{p}}] = \ell^\infty$.

Proof. For a finite place $\mathfrak{p}$ of k, denote by $D_{\mathfrak{p}}$ the decomposition group of $\mathfrak{p}$ in $\mathrm{Gal}(\widetilde{k_S}/k) \simeq Z_\ell^t$. As $D_{\mathfrak{p}}$ is a closed subgroup of $\mathbb{Z}_\ell^t$, it is trivial, or contains a subgroup isomorphic to $\mathbb{Z}_\ell$. We will show that $D_{\mathfrak{p}}$ can not be trivial. Denote by $\widetilde{k_S}^{D_{\mathfrak{p}}}$ the subfield of $\widetilde{k_S}$ fixed by $D_{\mathfrak{p}}$. Note that $\widetilde{k_S}^{D_{\mathfrak{p}}}$ is included in $k_S^{\{\mathfrak{p}\}}$ and $\widetilde{k_S^{\{\mathfrak{p}\}}} \subset \widetilde{k_S}$.

Now assume that for $\mathfrak{p} \notin S$, $D_{\mathfrak{p}}$ is trivial. Then $\widetilde{k_S} = \widetilde{k_S}^{D_{\mathfrak{p}}} \subset k_S^{\{\mathfrak{p}\}}$. Also $\widetilde{k_S} \subset \widetilde{k_S^{\{\mathfrak{p}\}}}$ and the equality $\widetilde{k_S} = \widetilde{k_S^{\{\mathfrak{p}\}}}$ yealds. This implies that for $\mathfrak{p} \notin S$, $\mathrm{rk}_{\mathbb{Z}_\ell} {G_S^{\{\mathfrak{p}\}}}^{ab} = \mathrm{rk}_{\mathbb{Z}_\ell} G_S^{ab}$ which contradicts the condition 1. Now for $\mathfrak{p} \in S$, as we have:

$$k \subset \widetilde{k_S^{\{\mathfrak{p}\}}} \subset \widetilde{k_{S\backslash\{\mathfrak{p}\}}} \subset \widetilde{k_S},$$

the conclusion is the same as for $\mathfrak{p} \notin S$. □

Now we will apply a result which can be found in [16]: the ℓ-cohomological dimension $\mathrm{Gal}(\overline{k}/\widetilde{k_S})$ is less than 1. In consequence, we can now apply Proposition 2 page 85 of [16] and so $\mathrm{cd}_\ell(\mathrm{Gal}(\overline{k}(\ell)/\widetilde{k_S})) = 1$. □

3.6.1. *Proof of Theorem 3.* If $S_{\overline{\mathfrak{p}}} = S_\ell$ this is well-known.
Let K be the maximal abelian ℓ-extension of N unramified outside $\mathfrak{p}$, and for a prime $\mathfrak{p}'$ different from $\mathfrak{p}$, let $K^{\{\mathfrak{p}'\}}$ be the maximal abelian ℓ-extension of N contained in K and in which $\mathfrak{p}'$ splits completely. By Theorem 5, we have $\mathrm{rk}_{\mathbb{Z}_\ell}\mathrm{Gal}(K/N) = 1$, and for $\mathfrak{p}' \neq \mathfrak{p}$, $\mathrm{rk}_{\mathbb{Z}_\ell}\mathrm{Gal}(K^{\{\mathfrak{p}'\}}/N) = 0$. Then for all $\mathfrak{p} \in \mathcal{O}_N$, $[K_{\mathfrak{p}} : N_{\mathfrak{p}}] = \infty$. By base change, the same is true for $k_{S_{\overline{\mathfrak{p}}}}/k$. Then the end of the proof of Theorem 31 can be applied.

3.6.2. *Proof of Theorem 4.* Let $f(x) \in \mathbb{Z}[x]$ be an irreducible polynomial of degree 4, such that the discriminant d of f is a fundamental discriminant of a real quadratic field: for example $f(x) = x^4 - x + 1$ with $d = 229$.
It is well know that the Galois closure k of f is of degree 24 over $\mathbb{Q}$ with Galois group S_4, and moreover, $k/\mathbb{Q}(\sqrt{d})$ is unramified everywhere, with Galois group $G = \mathrm{A}_4$.
Let $\mathfrak{p}|\ell$ be a prime of $N := \mathbb{Q}(\sqrt{d})$ which is of degree one. Put $S_N = \{\mathfrak{p}\}$ and $S = S_{\overline{\mathfrak{p}}} = \{\mathfrak{P} \in \mathcal{O}_k, \mathfrak{P} \cap \mathcal{O}_N = \mathfrak{p}\}$.
We will study the action of A_4.
The group A_4 has three irreducible characters of degree one $(\mathbf{1}, \psi_1, \psi_2)$ plus one irreducible character ψ of degree 3.
As the archimedean places are unramified in k/N, we have:

$$\chi(E_k) = 2(\mathbf{1} + \psi_1 + \psi_2 + \psi) - \mathbf{1} = \mathbf{1} + 2\psi_1 + 2\psi_2 + 2\psi.$$

Now by Proposition 14, one has:

$$\chi_S = \mathbf{1} + \psi_1 + \psi_2 + 2\psi,$$

and so

$$\mathrm{rk}_{\mathbb{Z}_\ell} G_S^{ab} = 3.$$

Now we prove that conditions 1 and 2 of Theorem 31 are satisfied.
1) First a lemma:

Lemma 33. *Let $\mathfrak{q}$ be a prime of k prime to S. Let $T = \{\mathfrak{q}\}$ and $\overline{T} = \{\mathfrak{q}^s, s \in G\}$. Then $\mathrm{rk}_{\mathbb{Z}_\ell} G_S^{\overline{T}^{ab}} < \mathrm{rk}_{\mathbb{Z}_\ell} G_S^{ab}$ if and only if $\mathrm{rk}_{\mathbb{Z}_\ell} G_S^{T^{ab}} < \mathrm{rk}_{\mathbb{Z}_\ell} G_S^{ab}$.*

Proof. For a finite place $\mathfrak{q}$ of k, denote by $D_\mathfrak{q}$ the decomposition group of $\mathfrak{q}$ in $\widetilde{k_S}/k$. First we have :

$$\mathbb{Q} \subset N \subset k \subset \widetilde{k_S^{\overline{T}}} \subset \widetilde{k_S^T} \subset \widetilde{k_S}^{D_\mathfrak{q}} \subset \widetilde{k_S}.$$

Note that $\widetilde{k_S}/N$ is a Galois extension.
It is clear that $\mathrm{rk}_{\mathbb{Z}_\ell} G_S^{T^{ab}} < \mathrm{rk}_{\mathbb{Z}_\ell} G_S^{ab}$ implies $\mathrm{rk}_{\mathbb{Z}_\ell} G_S^{\overline{T}^{ab}} < \mathrm{rk}_{\mathbb{Z}_\ell} G_S^{ab}$. We have only to prove the reciprocity: Assume that $\mathrm{rk}_{\mathbb{Z}_\ell} G_S^{T^{ab}} = \mathrm{rk}_{\mathbb{Z}_\ell} G_S^{ab}$. Then $\widetilde{k_S} = \widetilde{k_S^T}$. The decomposition group of $\mathfrak{q}$ in $\widetilde{k_S}/k$ is then trivial and so the decomposition group of all conjugate of $\mathfrak{p}$ by G are trivial. Consequently, $\widetilde{k_S} \subset k_S^{\overline{T}}$ and so $\widetilde{k_S} \subset \widetilde{k_S^{\overline{T}}}$, giving $\widetilde{k_S} = \widetilde{k_S^{\overline{T}}}$. ∎

For a finite place $\mathfrak{p}$ of N, the decomposition group $D_\mathfrak{p}$ in k/N is cyclic, because $\mathfrak{p}$ is unramified. So the order of $D_\mathfrak{p}$ is 1, 2 or 3, which implies that the degree of $\mathrm{Ind}_{D_\mathfrak{p}}^G \mathbf{1}$ is 12, 6 or 4. Moreover $\mathrm{Ind}_{D_\mathfrak{p}}^G \mathbf{1} \le \chi\mathrm{reg}$, implying $\psi \le \mathrm{Ind}_{D_\mathfrak{p}}^G$. And so for all prime $\mathfrak{p}$ of N, we have (by using Proposition 11):

$$\chi(E_S^{\bar{T}}) \ge \chi\mathrm{reg}.$$

By Proposition 14,

$$\Theta_S(E_S^{\overline{T}}) = \chi\mathrm{reg},$$

and so by Theorem 5

$$\mathrm{rk}_{\mathbb{Z}_\ell} G_S^{\overline{T}^{ab}} = 0.$$

By Lemma 33, one has the first condition of Theorem 31.
2) To prove the second condition, we use a method similar to that of Lemma 33. For a prime $\mathfrak{q}$ in S, denote by $k_{S\backslash\{\mathfrak{q}\}}$ the maximal ℓ-extension of k, unramified outside $S\backslash\{\mathfrak{q}\}$ and let $\widetilde{k_{S\backslash\{\mathfrak{q}\}}}$ be the compositum of $\mathbb{Z}_\ell$-extension included in $k_{S\backslash\{\mathfrak{q}\}}$. We have

$$\mathbb{Q} \subset N \subset k \subset \widetilde{k_{S\backslash\{\mathfrak{q}\}}} \subset \widetilde{k_S}^{I_\mathfrak{q}} \subset \widetilde{k_S},$$

where $I_\mathfrak{q}$ is the ramification group of $\mathfrak{q}$ in $\widetilde{k_S}/k$. Now $I_\mathfrak{q}$ is a closed subgroup of $\mathrm{Gal}(K_S/k) \simeq \mathbb{Z}_\ell^3$: it is trivial, or it contains a subgroup isomorphic to $\mathbb{Z}_\ell$. As before, if $I_\mathfrak{q}$ is trivial then for all conjugates $\mathfrak{q}^s$, $s \in G$, $I_{\mathfrak{q}^s}$ is also trivial, and so $\widetilde{k_S}/k$ is unramified everywhere which is impossible. The second condition of Theorem 31 is then verified.

4. On the group G_S

4.1. The exact value of the number of relations of G_S.

4.1.1. *Relations and torsion.* Leopoldt's conjecture says that for $S = S_\ell$, the $\mathbb{Z}_\ell$-rank of $\overline{\Theta_S(E_S)}$ is exactly the $\mathbb{Z}$-rank of the group of units of k. As noted in [11], this result has a link with the Schur multiplicator of G_S:

Proposition 34. *Leopoldt's Conjecture is true for (ℓ, k) if and only if $H_2(G_{S_\ell}, \mathbb{Z}_\ell)$ is trivial.*

Proof. Proposition 34 is a direct consequence of the following Lemma:

Lemma 35 (see [13] for example)**.** *Let G be a pro-ℓ-group. Then*

$$d(H_2(G, \mathbb{Z}_\ell)) = r(G) - d(\mathrm{Tor}(G)) = r(G) - d(G) + \mathrm{rk}_{\mathbb{Z}_\ell} G^{ab}.$$

The difference $r(G_{S_\ell}) - d(G_{S_\ell})$ is well-known and is equal to $-(r_2 + 1)$. But Leopoldt's Conjecture is true if and only if $\mathrm{rk}_{\mathbb{Z}_\ell} G^{ab} = r_2 + 1$, i.e. if and only if $H_2(G, \mathbb{Z}_\ell)$ is trivial. □

The triviality of this cohomology group, allows us to see $d(\mathrm{Tor}(G_{S_\ell}))$ as the number of relations of G_{S_ℓ}:

Theorem 36. *Leopoldt's Conjecture is equivalent to*

$$r(G_{S_\ell}) = d(\mathrm{Tor}(G_{S_\ell})).$$

4.1.2. *General case.*

Theorem 37. *Assume $S \subset S_\ell$ (not empty). If $\mathrm{rk}_{\mathbb{Z}_\ell}\overline{\Theta_S(E_S)} = \mathrm{rk}_{\mathbb{Z}} E_k$, one has:*

1. $r(G_S) = d(G_S) - \sum_{\mathfrak{p}\in S}[k_\mathfrak{p} : \mathbb{Q}_\ell] + r_1 + r_2 - 1 = d(\mathrm{Tor}(G_S))$;
2. $H_2(G_S, \mathbb{Q}_\ell/\mathbb{Z}_\ell) \simeq \mathrm{Tor}(G_S)$.

Proof. By Propositions 35 and 6, one has:

(7) $0 \leq d(H_2(G_S, \mathbb{Z}_\ell)) \leq r(G_S) - d(G_S) + \mathrm{rk}_{\mathbb{Z}_\ell} G_S^{ab} \leq \mathrm{rk}_{\mathbb{Z}} E_k - \mathrm{rk}_{\mathbb{Z}_\ell}\overline{\Theta_S(E_S)}$.

The first assertion is then proved. For the second assertion, we use a result of Nguyen [11]. First by the inequality (7), $H^2(G_S, \mathbb{Q}_\ell/\mathbb{Z}_\ell) = H_2(G_S, \mathbb{Z}_\ell)^* = 0$.
So the exact sequence

$$1 \longrightarrow \mathbb{Z}_\ell \xrightarrow{\ell^m} \mathbb{Z}_\ell \longrightarrow \mathbb{Z}/\ell^m\mathbb{Z} \longrightarrow 1,$$

gives for large m

$$H_2(G_S, \mathbb{Z}/\ell^m\mathbb{Z}) \simeq \mathrm{Tor}(G_S).$$

By passing to inductive limit, we have the result. □

We can now give some examples.

4.1.3. *Examples.* 1) Let k be a quadratic field and $S \subset S_\ell$ (S not empty). Then $r(G_S) = d(\mathrm{Tor}(G_S))$.
2) Consider the two following situations:
i) Let N be an imaginary quadratic field, let $\mathfrak{p}$ be a prime of N above ℓ and let k/N be a finite Galois extension. Assume Schanuel's Conjecture.
ii) Let N be a real quadratic field and $\mathfrak{p}$ be a prime of N. Let σ_1 and σ_2 be the two archimedean places of N. Suppose $\alpha \in N\backslash N^2$ and $\beta \in N\backslash N^2$ have negative absolute norm satisfying $\sigma_1(\alpha) > 0$, $\sigma_2(\beta) > 0$. Put $k = N(\sqrt{\alpha}, \sqrt{\beta})$; k is a totally complex biquadratic extension over N.
Put for the two cases $S = \{\mathfrak{P} \in k, \mathfrak{P}|\mathfrak{p}\}$. Then one has:

$$r(G_S)=d(\mathrm{Tor}(G_S))=\begin{cases} d(G_S)-(r_2+1), & \text{if } S=S_\ell \\ d(G_S)-1, & \text{else}\end{cases}$$

In the two cases, G_S^{ab} is infinite.

Proof. 1) Direct application of Theorem 37.
2) If $S=S_\ell$ this is well-known.
Let us show the second equality. To do this we use the action of $G=\mathrm{Gal}(k/N)$.
i) We are exactly in the same context as in Proposition 23. So we have:

$$\chi_S=\chi\mathrm{reg}\wedge\chi(E_S)=\chi(E_S)=\chi\mathrm{reg}-\mathbf{1}.$$

ii) Denote $N_0=N$, $N_1=N(\sqrt{\alpha})$, $N_2=N(\sqrt{\beta})$ and $N_3=N(\sqrt{\alpha\cdot\beta})$. Let φ_i be the $\mathbb{C}_\ell$-irreducible character of $G=\mathrm{Gal}(k/N)$ such that the kernel of φ_i defined N_i. Then

$$\chi(E_S)=\varphi_0+\varphi_1+\varphi_2.$$

And so $\chi_S=\chi(E_S)$, by Proposition 19.
In the two cases, Theorem 37 can be applied. □

4.2. **Free pro-ℓ-groups.**

4.2.1. *Classical results.*

Proposition 38. *The pro-ℓ-group G_{S_ℓ} is free if and only if one of the following is satisfied:*

1. *There exists a place $\mathfrak{p}$ of S_ℓ such that $\mu_\ell\subset k_\mathfrak{p}$, then $\mu_\ell\subset k$, $\mathbf{\Delta}_{S_\ell}=0$ and $|S_\ell|=1$.*
2. *For all places $\mathfrak{p}$ of S_ℓ, $k_\mathfrak{p}$ does not contain μ_ℓ, and $\mathbf{\Delta}_{S_\ell}=0$.*

In this case, G_{S_ℓ} is the free pro-ℓ-group with r_2+1 generators.

Proof. One has $r(G_{S_\ell})-d(G_{S_\ell})=-(r_2+1)$. Moreover $d(G_{S_\ell})=r_2+1+\sum_{\mathfrak{p}\in S_\ell}\delta_\mathfrak{p}+d(\mathbf{\Delta}_{S_\ell})-\delta_k$. So $r(G_{S_\ell})=0$ if and only if $\delta_k=\sum_{\mathfrak{p}\in S_\ell}\delta_\mathfrak{p}+d(\mathbf{\Delta}_{S_\ell})$. □

4.2.2. *General case.* We have:

Theorem 39. *Let $S\subset S_\ell$. Then G_S is pro-ℓ-free in the following situations:*

1. *$\mu_\ell\subset k$, $S=\{\mathfrak{p}\}$ and $\mathbf{\Delta}_S=0$.*
2. *For all places $\mathfrak{p}$ of S, $k_\mathfrak{p}$ does not contain μ_ℓ and $\mathbf{\Delta}_S=0$.*

In the two cases G_S is the free pro-ℓ-group with $\sum_{\mathfrak{p}\in S}[k_\mathfrak{p}:\mathbb{Q}_\ell]+1-(r_2+r_1)$ generators.

Proof. Recall the surjective map of Proposition 6 :

$$\mathbf{\Delta}_S\twoheadrightarrow\ker\left(H^2(G_S,\mathbb{F}_\ell)\to\bigoplus_{\mathfrak{p}\in S^*}H^2(\mathcal{G}_\mathfrak{p},\mathbb{F}_\ell)\right)^*.$$

Now $\ker\left(H^2(G_S,\mathbb{F}_\ell)\to\bigoplus_\mathfrak{p}H^2(\mathcal{G}_\mathfrak{p},\mathbb{F}_\ell)\right)=H^2(G_S,\mathbb{F}_\ell)$ in one of the following:

1. $|S|=1$, if $\mu_\ell\in k$;
2. $k_\mathfrak{p}$ does not contain μ_ℓ for all places $\mathfrak{p}$ of S (in this case, $H^2(\mathcal{G}_\mathfrak{p},\mathbb{F}_\ell)=0$).

These conditions plus triviality of $\mathbf{\Delta}_S$ imply $H^2(G_S,\mathbb{F}_\ell)=1$. □

References

[1] A. Brumer, On the units of algebraic number fields, Mathematika **14** (1967), 121-124.

[2] W. Curtis and I. Reiner, Representation theory of finite groups and associative algebras, Intersc. Publ., New York, 1962.

[3] G. Gras, Pratique du corps de Classes, in preparation.

[4] G. Gras, Théorèmes de réflexion, J. Théorie des Nombres de Bordeaux **10** (1998), 399-499.

[5] Haberland, Galois cohomology of algebraic number fields, V.E.B. Deutscher Verlag der Wissenschaften 1970.

[6] J.-F. Jaulent, Sur l'indépendance ℓ-adique de nombres algébriques, J. Number Theory **20** (1985), 149-158.

[7] H. Koch, On p-extension with given ramification, Appendix 1 to Haberland, 1978, 89-126.

[8] H. Koch, Galoissche Theorie der p-Erweiterungen, VFB Deutscher Verlag der Wissenschaften, Berlin 1970.

[9] T. Kondo, Algebraic number fields with the discriminant equal to that of quadratic field, J. Math. Soc. Japan **47** (1995), 31-36.

[10] S. Lang, Cyclotomic fields I and II, G.T.M. 121, Springer-Verlag, 1990.

[11] T. Nguyen Quang Do, Sur la $\mathbb{Z}_p$-torsion de certains modules galoisiens, Ann. Inst. Fourier, Grenoble **36**, 2 (1986), 27-46.

[12] J. Neukirch, A. Schmidt and K. Wingberg, Cohomology of number fields, Grund. der Math. Wissenschaften 323, Springer-Verlag, Berlin 2000.

[13] P. Roquette, On class field towers, in Algebraic Number Theory, ed. J. Cassels, A. Fröhlich, Academic Press 1980.

[14] A. Schmidt, On the relation between 2 and ∞ in Galois cohomology of number fields, preprint 2000.

[15] J.-P. Serre, Corps locaux, Hermann, Paris, 1962.

[16] J.-P. Serre, Cohomologie galoisienne, Springer-Verlag, 1994.

[17] J.-P. Serre, Représentations linéaires des groupes finis, coll. Méthodes, Hermann, Paris, 1978.

[18] I.-R. Shafarevich, Extensions with given ramification points, Publ. Math. IHES **18** (1964), 71-95 [In russian]; English transl. in Amer. Math. Soc. Transl., vol. 59, 128-149, American Math. Soc., Providence, R.I. 1966.

[19] M. Waldschimdt, Transcendance et exponentielles en plusieurs variables, Invent. Math **63** (1981), 97-127.

[20] M. Waldschimdt, Approximation on linear algebraic groups, Grundlehren der Math. Wissenschaften 326, Springer-Verlag, 2000.

[21] L. Washington, Introduction to cyclotomic fields, G.T.M. 83, Springer-Verlag, 1982.

Christian Maire
Laboratoire A2X
Université Bordeaux I
Cours de la Libération
33405 Talence Cedex France
maire@math.u-bordeaux.fr

Current address:
Mathematical Sciences Research Institute
1000 Centennial Drive
Berkeley, Califoria 94720
USA
maire@msri.org