DEFICIENCY OF p-CLASS TOWER GROUPS AND MINKOWSKI UNITS

by

Farshid Hajir, Christian Maire, Ravi Ramakrishna

Abstract. — The deficiency $\mathrm{Def}(\mathrm{G})$ of a finitely-generated pro-p group G is the difference between its minimal numbers of relations and generators. For a number field K with maximal unramified p-extension $\mathrm{K}_\varnothing$, set $\mathrm{G}_\varnothing = \mathrm{Gal}(\mathrm{K}_\varnothing/\mathrm{K})$. Shafarevich (and independently Koch) showed

$$0 \leqslant \mathrm{Def}(\mathrm{G}_\varnothing) \leqslant \dim(\mathscr{O}_\mathrm{K}^\times/(\mathscr{O}_\mathrm{K}^\times)^p).$$

We explore connections between the relations of $\mathrm{G}_\varnothing$ and the Galois module structure of the units in the tower $\mathrm{K}_\varnothing/\mathrm{K}$. If $\mu_p \not\subset \mathrm{K}$, we give an exact formula for $\mathrm{Def}(\mathrm{G}_\varnothing)$ in terms of the number of independent Minkowski units in the tower. We also study the depth of the relations of $\mathrm{G}_\varnothing$ in the Zassenhaus filtration and provide evidence that the Shafarevich-Koch upper bound is "almost always" sharp. In the other direction, we give the first examples of infinite $\mathrm{G}_\varnothing$ with $\mathrm{Def}(\mathrm{G}_\varnothing) = 0$ and $\dim(\mathscr{O}_\mathrm{K}^\times/(\mathscr{O}_\mathrm{K}^\times)^p)$ large, so that the upper bound is not sharp.

Let p be a prime number, and let K be a number field. For a finite set S of places of K, let K_S be the maximal p-extension of K unramified outside S and $\mathrm{G}_S = \mathrm{Gal}(\mathrm{K}_S/\mathrm{K})$, its Galois group. Note in particular that $\mathrm{K}_\varnothing$ is the maximal pro-p extension of K unramified everywhere and we call $\mathrm{K}_\varnothing/\mathrm{K}$ the p-class field tower of K. Let

$$d(\mathrm{G}_S) = \dim H^1(\mathrm{G}_S) = \dim H^1(\mathrm{G}_S, \mathbb{Z}/p) \text{ and } r(\mathrm{G}_S) = \dim H^2(\mathrm{G}_S) = \dim H^2(\mathrm{G}_S, \mathbb{Z}/p)$$

be, respectively, the minimal number of generators and relations of G_S. Define $\mathrm{Def}(\mathrm{G}_S) := r(\mathrm{G}_S) - d(\mathrm{G}_S)$ as the *deficiency* of G_S. (1)

2000 ***Mathematics Subject Classification.*** — 11R29, 11R37.

Key words and phrases. — Deficiency, Golod-Shafarevich polynomial, p-class field tower, Zassenhaus filtration.

This work started when the second author held a visiting scholar position at Cornell University, funded by the program "Mobilité sortante" of the Région Bourgogne Franche-Comté, during the 2017-18 academic year. It continued during visits to the Harbin Institute of Technology and Cornell University. CM thanks the Department of Mathematics at Cornell University and the Institute for Advanced Study in Mathematics of HIT for providing excellent conditions for conducting research. The second author was partially supported by the ANR project FLAIR (ANR-17-CE40-0012) and by the EIPHI Graduate School (ANR-17-EURE-0002). The third author was supported by Simons Collaboration grant #524863. All three authors were supported by Mathematisches Forschungsinstitut Oberwolfach for a Research in Pairs visit in January, 2019 and by ICERM for a Research in Pairs visit in January, 2020.

We thank the referee for thoroughly reading the paper, making a number of helpful suggestions and asking some interesting questions.

1. In most of the group theory literature the deficiency of G is defined as $d(\mathrm{G}) - r(\mathrm{G})$.

Our goal in this paper is to better understand the pro-p group G_S when S is tame, that is when S does not contain all places above $\{p,\infty\}$. We are particularly interested in the case $S=\varnothing$. In the wild setting, when S contains all places above $\{p,\infty\}$, we have at our disposal a very powerful tool, namely the global duality theorem for G_S, which immediately yields an explicit and easily computable formula for $\mathrm{Def}(\mathrm{G}_S)$. While such a tool is still missing in the tame, and in particular, unramified, case, Theorem A below (see Theorem 2.9) is a step toward refining our understanding of the unramified situation by relating it to the presence of Minkowski units in $\mathrm{K}_\varnothing/\mathrm{K}$.

By class field theory, the maximal abelian quotient of G_S is isomorphic to the p-Sylow subgroup of a ray class group for K, and is therefore finite when S is tame. By the Burnside Basis Theorem, $d(\mathrm{G}_\varnothing)$ is the p-rank of the class group of K and is in particular computable in any given case (at least in theory). In contrast, we do not know an algorithm for computing $r(\mathrm{G}_\varnothing)$. However, thanks to the celebrated work of Shafarevich [**38**] (and, independently, Koch – see for example [**15**, Chapter 11]) we know that

$$0 \leqslant \mathrm{Def}(\mathrm{G}_\varnothing) \leqslant d(\mathscr{O}_\mathrm{K}^\times),$$

where $d(\mathscr{O}_\mathrm{K}^\times) := d(\mathscr{O}_\mathrm{K}^\times/(\mathscr{O}_\mathrm{K}^\times)^p)$ is the p-rank of the unit group $\mathscr{O}_\mathrm{K}^\times$ of the ring of integers $\mathscr{O}_\mathrm{K}$ of K. We recall that if K has r_1 embeddings into $\mathbb{R}$ and r_2 pairs of complex conjugate embeddings into $\mathbb{C}$, then $d(\mathscr{O}_\mathrm{K}^\times)=r_1+r_2-1+\delta$ where δ is 1 or 0 according to whether K contains a primitive pth root of unity ζ_p or not. The number-theoretic work of Shafarevich on the above deficiency bound [**38**] subsequently led to the group-theoretic work of Golod and Shafarevich [**8**]. This pair of papers gave a criterion for the infinitude of $\mathrm{G}_\varnothing$ and produced the first such examples. More historical details can be found in [**37**], [**29**], [**15**], and [**25**].

In this work, we investigate more closely the relationship between units in unramified class field towers and defining relations for their Galois groups. Our main theorem is that the existence of certain types of units along the tower $\mathrm{K}_\varnothing/\mathrm{K}$ provides two types of results: (a) tighter bounds for the deficiency of $\mathrm{G}_\varnothing$, as well as (b) more refined information on the depth of its defining relations. We introduce a constant λ measuring the free-part of the Galois module structure of the units in $\mathrm{K}_\varnothing/\mathrm{K}$ (see §2.3). Here free-part means the following: if F/K is a finite Galois extension in $\mathrm{K}_\varnothing/\mathrm{K}$ with Galois group G, we are interested in the $\mathbb{F}_p[\mathrm{G}]$-structure of $\mathbb{F}_p\otimes\mathscr{O}_\mathrm{F}^\times$, that is the units $\mathscr{O}_\mathrm{F}^\times$ modulo pth powers. Recall that since G is a p-group, the category of $\mathbb{F}_p[\mathrm{G}]$-modules is not semisimple. When the $\mathbb{F}_p[\mathrm{G}]$-free part of $\mathbb{F}_p\otimes\mathscr{O}_\mathrm{F}^\times$ is nontrivial, we say the extension F/K admits a *Minkowski unit* (see §1.3 for further details). It is not difficult to see that the number of independent Minkowski units is non-increasing and stabilizes as we move up the tower $\mathrm{K}_\varnothing/\mathrm{K}$ and therefore after a finite number of steps reaches a constant value we denote $\lambda := \lambda_{\mathrm{K}_\varnothing/\mathrm{K}}$. We also define β to be

$$\beta := \begin{cases} d\left(\frac{\mathscr{O}_\mathrm{K}^\times\cap(\mathscr{O}_{\mathrm{K}_\varnothing}^\times)^p}{(\mathscr{O}_\mathrm{K}^\times)^p}\right) & \zeta_p\in\mathrm{K} \\ 0 & \text{otherwise} \end{cases}.$$

Note that when $\zeta_p\in\mathrm{K}$, if we set $\mathrm{L}=\mathrm{K}_\varnothing\cap\mathrm{K}(\sqrt[p]{\mathscr{O}_\mathrm{K}^\times})$, then $[\mathrm{L}:\mathrm{K}]=p^\beta$. Thus, $0\leqslant\beta\leqslant\min\left(r_1+r_2, d(\mathrm{G}_\varnothing)\right)$. We also note that $\beta>0$ if and only if for some $u\in\mathscr{O}_\mathrm{K}^\times$, $\mathrm{K}(u^{1/p})/\mathrm{K}$ is a $\mathbb{Z}/p$-unramified extension. More generally, the quantity β quantifies the number of such independent extensions of K.

Theorem A. — *Recall* λ *is the number of independent Minkowski units in the* p*-Hilbert class field tower* $\mathrm{K}_\varnothing/\mathrm{K}$*. One has*

$$d(\mathscr{O}_\mathrm{K}^\times) - \lambda - \beta \leqslant \mathrm{Def}(\mathrm{G}_\varnothing) \leqslant d(\mathscr{O}_\mathrm{K}^\times) - \lambda.$$

In particular if $\mathscr{O}_\mathrm{K}^\times \cap (\mathscr{O}_{\mathrm{K}_\varnothing}^\times)^p = (\mathscr{O}_\mathrm{K}^\times)^p$ *or if* K *does not contain a primitive pth root of unity, then* $\mathrm{Def}(\mathrm{G}_\varnothing) = d(\mathscr{O}_\mathrm{K}^\times) - \lambda$.

We give two proofs of this result (see proof of Theorem 2.9). In our second more constructive proof we realize $\mathrm{G}_\varnothing$ as a quotient of some G_S, where S is a well-chosen finite set of tame (coprime to p) prime ideals of $\mathscr{O}_\mathrm{K}$ (see also Notations at the end of this section), and we use the Hochschild-Serre spectral sequence induced by the natural map $\mathrm{G}_S \twoheadrightarrow \mathrm{G}_\varnothing$ to produce $d(\mathrm{G}_\varnothing) + d(\mathscr{O}_\mathrm{K}^\times) - \lambda - \beta$ independent elements of $Ш^2_\varnothing = H^2(\mathrm{G}_\varnothing)$.

In §3.6 we also give examples of infinite $\mathrm{G}_\varnothing$ with as many as seven independent Minkowski units.

Remark. — As mentioned earlier, the non-negativity of $\mathrm{Def}(\mathrm{G}_\varnothing)$ follows from a basic group-theoretical property of $\mathrm{G}_\varnothing$, namely that its maximal abelian quotient is finite. In other words, one knows that $\mathrm{G}_\varnothing$ has at least $d(\mathrm{G}_\varnothing)$ relations. For the group $\mathrm{G}_\varnothing$, one can concretely produce $d(\mathrm{G}_\varnothing)$ relations for $\mathrm{G}_\varnothing$ as follows. In Figure 1, we show a tower of fields $\mathrm{K} \subset \mathrm{K}' \subset \mathrm{L}'_1 \subset \mathrm{L}'_2$ for whose definition, the reader may consult the Notations section at the end of this introduction. For the moment, the key point is that $\mathrm{L}'_2/\mathrm{L}'_1$ is an elementary abelian p-extension of dimension $d(\mathrm{G}_\varnothing)$. By the Chebotarev density theorem, we can choose $d(\mathrm{G}_\varnothing)$ primes of K whose Frobenius automorphisms form a basis of the elementary p-abelian group $\mathrm{Gal}(\mathrm{L}'_2/\mathrm{L}'_1)$. Letting S_1 be the set consisting of these primes, in Section 2.2, we will describe in detail how applying the Gras-Munnier Theorem (Theorem 1.1) and Lemma 1.5 (ii) to the primes in S_1 gives us $d(\mathrm{G}_\varnothing)$ independent elements in $Ш^2_\varnothing = H^2(\mathrm{G}_\varnothing)$, which in turn correspond to $d(\mathrm{G}_\varnothing)$ distinct relations in a minimal presentation of $\mathrm{G}_\varnothing$. We refer to relations constructed in this way as "easily detected" via S_1, or, when the context is clear, simply "easy."

$$\begin{tikzcd}
 & & \mathrm{L}'_2 := \mathrm{K}'\left(\sqrt[p]{\mathrm{V}_\varnothing}\right) \\
 & \mathrm{L}'_1 := \mathrm{K}'\left(\sqrt[p]{\mathscr{O}_\mathrm{K}^\times}\right) \arrow[ur, dash] & \\
\mathrm{K}' := \mathrm{K}(\zeta_p) \arrow[ur, dash] & & \\
\mathrm{K} \arrow[u, dash] & &
\end{tikzcd}$$

Figure 1.

A key observation we make in this work is that aside from the $d(\mathrm{G}_\varnothing)$ relations easily detected via S_1, we can construct $d(\mathscr{O}_\mathrm{K}^\times) - \lambda - \beta$ additional relations via a modification of this construction using a further set S_2 of auxiliary primes whose Frobenius automorphisms span a Galois group in a more complicated tower of governing fields (Figure

2) described in §2.2. The existence of such primes is tied up with the Galois module structure of units in the Hilbert p-class field tower. We refer to the resulting relations as “difficult” relations “detected” by S_2. This set of ideas leads to the lower bound for $\mathrm{Def}(\mathrm{G}_\varnothing)$ in the theorem. The upper bound, on the other hand, is a consequence of a result of Wingberg [**42**]. When $\beta = 0$ (which is always the case if K does not contain a primitive pth root of unity), these upper and lower bounds coincide, in which case all the relations are either easily detected by S_1 or difficult and detected by S_2. But when $\beta > 0$, only $d(\mathscr{O}_{\mathrm{K}}^\times) - \lambda - \beta$ of the relations are constructible in this way. Indeed, in the example below $\beta = 1$ and we find the final relation, which is difficult, by an ad hoc method.

Example. — Take $p = 2$. Our method allows us to show that for $\mathrm{K} = \mathbb{Q}(\sqrt{-5460})$, the example studied extensively by Boston-Wang [**3**], there are 4 easily detected relations and another relation that is difficult. $\mathrm{Def}(\mathrm{G}_\varnothing) = r - d = 5 - 4 = 1$.

Thanks to the work of Labute [**17**], Schmidt [**32**] and others we know that there are special sets S (finite and tame) for which G_S is of cohomological dimension 2; however, their methods do not allow S to be empty. In particular, the question of the computation of the cohomological dimension of $\mathrm{G}_\varnothing$ has only been resolved in a few cases, namely when $\mathrm{G}_\varnothing$ is known to be finite. A consequence of Theorem A is the following (Theorem 3.12):

Corollary. — *Let* K *be a number field such that*
(i) K *contains a primitive pth root of unity;*
(ii) $\mathscr{O}_{\mathrm{K}}^\times \cap (\mathscr{O}_{\mathrm{K}_\varnothing}^\times)^p = (\mathscr{O}_{\mathrm{K}}^\times)^p$.
Then $\dim H^3(\mathrm{G}_\varnothing, \mathbb{F}_p) > 0$. *Moreover:*
- *If* $\dim H^3(\mathrm{G}_\varnothing, \mathbb{F}_p) = 1$*, then* $\mathrm{G}_\varnothing$ *is finite or of cohomological dimension* 3*;*
- *If* $\mathrm{Def}(\mathrm{G}_\varnothing) = 0$ *and* $\mathrm{G}_\varnothing$ *is of cohomological dimension* 3*, then* $\mathrm{G}_\varnothing$ *is a Poincaré duality group.*

We also deduce (Corollary 3.4):

Corollary. — *Let* K *be a number field such that*
(i) K *contains a primitive pth root of unity;*
(ii) $\mathscr{O}_{\mathrm{K}}^\times \cap (\mathscr{O}_{\mathrm{K}_\varnothing}^\times)^p = (\mathscr{O}_{\mathrm{K}}^\times)^p$*;*
(iii) $\mathrm{Def}(\mathrm{G}_\varnothing) = 0$.
Then for every open normal subgroup H *of* $\mathrm{G}_\varnothing$*, one has* $\mathrm{Def}(\mathrm{H}) = 0$.

When $\mathrm{Def}(\mathrm{H}) = 0$ for all open subgroups of G, λ is maximal all along the tower. When $\mathrm{Def}(\mathrm{G}_\varnothing) = 0$ and the tower is finite, it is a standard result from finite group theory that $\mathrm{G}_\varnothing$ is either cyclic or, when $p = 2$, a generalized quaternion group. Observe also that Poincaré groups of dimension 3 have deficiency zero.

When $\mathrm{G}_\varnothing$ is infinite we suspect $\mathrm{Def}(\mathrm{G}_\varnothing)$ is maximal (namely equal to $d(\mathscr{O}_{\mathrm{K}}^\times)$) very often in accordance with the heuristics of Liu-Wood-Zureick–Brown [**20**]. In fact, we elaborate a strategy to investigate maximality of the deficiency by testing for the presence of Minkowski units through computer computation. We further note that if in the first steps of the tower $\mathrm{K}_\varnothing/\mathrm{K}$ there are α Minkowski unit preventing us from concluding that $\mathrm{Def}(\mathrm{G}_\varnothing)$ is maximal, the group $\mathrm{G}_\varnothing$ can be described by at least α relations of high depth in the Zassenhaus filtration. Denote by (K_n) the sequence in $\mathrm{K}_\varnothing/\mathrm{K}$ where $\mathrm{K}_1 := \mathrm{K}$ and K_{n+1} is the maximal elementary abelian p-extension of K_n in $\mathrm{K}_\varnothing/\mathrm{K}$. Put

$\mathrm{H}_n = \mathrm{Gal}(\mathrm{K}_n/\mathrm{K})$. Let $r_{\max} = d(\mathrm{G}_\varnothing)+d(\mathscr{O}_\mathrm{K}^\times)$ be the maximal possible value of $r(\mathrm{G}_\varnothing)$. To each presentation of a pro-p group, there is associated a Golod-Shafarevich polynomial; for the basic facts of these polynomials, see §4.1.2. Golod and Shafarevich proved that if this polynomial vanishes on the open unit interval, then the group must be infinite. In §4, we prove the following result (see Theorem 4.12). See also § 1.3.3.

Theorem B. — *Let λ_n be the number of independent $\mathbb{F}_p[\mathrm{H}_n]$-Minkowski units in K_n. Then $\mathrm{G}_\varnothing$ can be generated by $d(\mathrm{G}_\varnothing)$ generators and r_{max} relations $\{\rho_1, \cdots, \rho_{r_{max}}\}$ such that at least λ_n relations are of depth greater than 2^n. Hence, we can take $1 - d(\mathrm{G}_\varnothing)t + (r_{max} - \lambda_n)t^2 + \lambda_n t^{2n}$ as a Golod-Shafarevich polynomial for $\mathrm{G}_\varnothing$.*

The more familiar Golod-Shafarevich polynomial in this context is $1 - d(\mathrm{G}_\varnothing)t + r_{\max}t^2$, which is *less* likely to have a root and thus indicate $\#\mathrm{G}_\varnothing = \infty$. Also, we will allow the possibility of $n = \infty$, that is there may be fewer than $r_{\max}$ relations.

The imaginary quadratic case is particularly easy to study (here $p = 2$). Indeed when K is an imaginary quadratic field, one has $\mathrm{Def}(\mathrm{G}_\varnothing) \in \{0, 1\}$. Here we show that, almost always, there is no Minkowski unit in any quadratic extension F/K of $\mathrm{K}_\varnothing/\mathrm{K}$, which implies $\mathrm{Def}(\mathrm{G}_\varnothing) = 1$ (see Theorem 5.12). Denote by $\mathscr{F}$ the set of imaginary quadratic fields, and for $X \geqslant 2$, put

$$\mathscr{F}(X) = \{\mathrm{K} \in \mathscr{F},\ |\mathrm{disc}(\mathrm{K})| \leqslant X\},\quad \mathscr{F}_0(X) = \{\mathrm{K} \in \mathscr{F}(X),\ \mathrm{Def}(\mathrm{G}_\varnothing) = 0\}.$$

Theorem C. — *Let K be imaginary quadratic and $p = 2$. One has*

$$\frac{\#\mathscr{F}_0(X)}{\#\mathscr{F}(X)} \leqslant C\frac{\log\log X}{\sqrt{\log X}},$$

where C is an absolute constant and X is large enough. In particular, the proportion of imaginary quadratic fields of discriminant at most X for which $\mathrm{Def}(\mathrm{G}_\varnothing) = 0$ tends to zero as $X \to \infty$.

Notations.
- Let p be a prime number and K be a number field.
- We denote by
  - $\mathscr{O}_\mathrm{K}$ the ring of integers of K, and by $\mathscr{O}_\mathrm{K}^\times$ the group of units of $\mathscr{O}_\mathrm{K}$,
  - $\mathscr{E}_\mathrm{K} = \mathbb{F}_p \otimes \mathscr{O}_\mathrm{K}^\times$, the units modulo the pth-powers,
  - K^H the Hilbert p-class field of K,
  - Cl_K the p-Sylow subgroup of class group of K.
- Let $\zeta_p \in \mathbb{Q}^{alg}$ be a primitive pth root of 1. Put $\delta := \delta_{\mathrm{K},p} := 1$ when $\zeta_p \in \mathrm{K}$, 0 otherwise.
- Let $S = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_s\}$ be a finite set of prime ideals of K. We identify a prime $\mathfrak{p} \in S$ with the place v it defines.
  - We assume each $\mathfrak{p}_i$ is tame (prime to p) and satisfies $|\mathscr{O}_\mathrm{K}/\mathfrak{p}_i| \equiv 1 (\mathrm{mod}\ p)$.
  - We denote by $\mathrm{RCG}_\mathrm{K}(\mathfrak{p}_1, \cdots, \mathfrak{p}_s)$ the p-Sylow subgroup of the ray class group of K of modulus $\mathfrak{p}_1 \cdots \mathfrak{p}_s$. When $S = \varnothing$, one has $\mathrm{RCG}_\mathrm{K}(\varnothing) = \mathrm{Cl}_\mathrm{K}$.
  - Let K_S be the maximal pro-p extension of K unramified outside S, put $\mathrm{G}_S = \mathrm{G}_{\mathrm{K},S} = \mathrm{Gal}(\mathrm{K}_S/\mathrm{K})$.
  - By class field theory, one has $\mathrm{G}_S^{ab} \simeq \mathrm{RCG}_\mathrm{K}(\mathfrak{p}_1, \cdots, \mathfrak{p}_s)$.

– Put $V_S := \{x \in K^\times,\ (x) = I^p$ as a fractional ideal of K; $x \in (K_v^\times)^p, \forall v \in S\}$. Then $V_S \supset (K^\times)^p$ and we have the exact sequence:

$$0 \to \mathscr{O}_K^\times/\mathscr{O}_K^{\times p} \to V_\varnothing/(K^\times)^p \to \mathrm{Cl}_K[p] \to 0.$$

- If M is a $\mathbb{Z}$-module, we set $d(\mathrm{M}) = \dim_{\mathbb{F}_p}(\mathbb{F}_p \otimes \mathrm{M})$.
  – When G is a pro-p group, we denote $d(\mathrm{G}) = d(\mathrm{G}^{ab})$, where $\mathrm{G}^{ab} = \mathrm{G}/[\mathrm{G},\mathrm{G}]$.
  – Let (r_1, r_2) be the signature of K. By Dirichlet's Theorem $d(\mathscr{O}_K^\times) = r_1 + r_2 - 1 + \delta$.
  – From the exact sequence above, $d(V_\varnothing/(K^\times)^p) = d(\mathscr{O}_K^\times) + d(\mathrm{Cl}_K)$.
- Unless otherwise specified, all cohomology groups have $\mathbb{Z}/p$-coefficients.
  – Hence $d(\mathrm{G}_\varnothing) := d(H^1(\mathrm{G}_\varnothing)) = \dim H^1(\mathrm{G}_\varnothing, \mathbb{Z}/p)$ and $r(\mathrm{G}_\varnothing) := \dim H^2(\mathrm{G}_\varnothing, \mathbb{Z}/p)$.
  – The deficiency $\mathrm{Def}(\mathrm{G}_\varnothing)$ of $\mathrm{G}_\varnothing$ is defined to be $r(\mathrm{G}_\varnothing) - d(\mathrm{G}_\varnothing)$.

For the computations in this paper we have used the programs GP-PARI [**27**] and MAGMA [**40**] and have often assumed the GRH to speed up the computations.

1. Preliminaries

In this section we develop the results we need to detect elements of $H^2(\mathrm{G}_\varnothing) = Ш^2_\varnothing$ as described in the Remark in the Introduction. In particular, Lemma 1.5 shows how one can detect elements of $Ш^2_\varnothing$ via ramified extensions of $K_\varnothing$; we illustrate our strategy by finding $Ш^2_\varnothing$ for the field $\mathbb{Q}(\sqrt{-5460})$ with $p = 2$.
In §1.2, we relate $\mathrm{Def}(\mathrm{G}_\varnothing)$ to norms of units from number fields in the tower $K_\varnothing/K$. In §1.3 we develop the basics of the theory of Minkowski units and show, using the Gras-Munnier Theorem 1.1, that the existence of a Minkowski unit in some number field F in the tower $K_\varnothing/K$ follows when $\mathrm{G}^{ab}_{F,\{\mathfrak{p}\}} = \mathrm{G}^{ab}_{F,\varnothing}$ for some prime $\mathfrak{p}$ of K.

1.1. Saturated sets, and a spectral sequence. —

1.1.1. Degree-p cyclic extension with prescribed ramification. — Take p, K and S as in the "Notations". The fields L'_i of Figure 1 are called *governing fields* as the existence of a $\mathbb{Z}/p$-extension of K ramified exactly at a given set of primes depends on their Frobenius automorphisms in these extensions. See Theorem 1.1 below.
For each prime ideal $\mathfrak{p} \in S$, let us choose a prime ideal $\mathfrak{P}|\mathfrak{p}$ of $\mathscr{O}_{L'_2}$, and denote by $\sigma_\mathfrak{p} := \left(\dfrac{L'_2/K'}{\mathfrak{P}}\right)$, the Frobenius at $\mathfrak{P}$ in the governing extension L'_2/K'.
Using that L'_2 is formed by taking pth roots of elements of K (not K′), one can easily show that $\sigma_\mathfrak{p}$ depends, up to a nonzero scalar multiple, only on $\mathfrak{p}$. This serves our purposes. By abuse we also denote by $\sigma_\mathfrak{p}$ its restriction to L'_1. One says that the Frobenius automorphisms $\sigma_\mathfrak{p}$, $\mathfrak{p} \in S$, satisfy a *nontrivial relation* if

$$\prod_{\mathfrak{p}\in S} \sigma_\mathfrak{p}^{a_\mathfrak{p}} = 1,$$

in $\mathrm{Gal}(L'_2/K')$ (or in $\mathrm{Gal}(L'_1/K')$) with the $a_i \in \mathbb{Z}/p$ not all zero. Thus the existence of a nontrivial relation is independent of the ambiguity in the choice of $\sigma_\mathfrak{p}$.

Theorem 1.1 **(Gras-Munnier [11])**. — *Let $S = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_t\}$ be a set of tame prime ideals of* K. *One has:*

(*i*) $d(\mathrm{G}_S) \neq d(\mathrm{G}_\varnothing)$, *if and only if the* $\sigma_\mathfrak{p}$, $\mathfrak{p} \in S$, *satisfy a nontrivial relation in* $\mathrm{Gal}(\mathrm{L}'_2/\mathrm{K}')$.

(*ii*) $|\mathrm{G}_S^{ab}| > |\mathrm{G}_\varnothing^{ab}|$ *if and only if the* $\sigma_\mathfrak{p}$, $\mathfrak{p} \in S$, *satisfy a nontrivial relation in* $\mathrm{Gal}(\mathrm{L}'_1/\mathrm{K}')$.

For a generalization of Theorem 1.1, see [**10**, Chapter V].

Remark 1.2. — 1. The distinction between (i) and (ii) of Theorem 1.1 is that (ii) can occur when $d(\mathrm{G}_S) = d(\mathrm{G}_\varnothing)$. The governing fields for the width and depth of G_S^{ab} are different.

2. The Kummer radical of $\mathrm{L}'_1/\mathrm{K}'$ is $\mathscr{O}_\mathrm{K}^\times(\mathrm{K}'^\times)^p/(\mathrm{K}'^\times)^p$ which is isomorphic to $\mathscr{E}_\mathrm{K}$ since $\mathscr{O}_\mathrm{K}^\times \cap (\mathrm{K}'^\times)^p = (\mathscr{O}_\mathrm{K}^\times)^p$ and $[\mathrm{K}' : \mathrm{K}]$ is coprime to p. For the same reason, $\mathrm{V}_\varnothing/(\mathrm{K}^\times)^p$ is the Kummer radical of $\mathrm{L}'_2/\mathrm{K}'$.

1.1.2. Saturated sets. — For $v \in S$, we denote by G_v the absolute Galois group of the maximal pro-p extension $\overline{\mathrm{K}}_v$ of the completion K_v of K at v. Let $Ш_S^2$ be the kernel of the localization map of $H^2(\mathrm{G}_S)$:

$$Ш_S^2 := \ker\big(H^2(\mathrm{G}_S) \to \oplus_{v\in S} H^2(\mathrm{G}_v)\big).$$

Put $Б_S = \big(\mathrm{V}_S/(\mathrm{K}^\times)^p\big)^\vee$; then one has (see Theorem 11.3 of [**15**]) $Ш_S^2 \hookrightarrow Б_S$. When S contains the places of K above $\{p, \infty\}$ this map is an isomorphism and $Ш_S^2$ is dual to

$$Ш_S^1(\mu_p) := \ker\big(H^1(\mathrm{G}_S, \mu_p) \to \oplus_{v\in S} H^1(\mathrm{G}_v, \mu_p)\big).$$

The failures of the isomorphism and duality in the tame case are reasons it is especially challenging.

Definition 1.3. — The set S of places K is called *saturated* if $\mathrm{V}_S/(\mathrm{K}^\times)^p = \{1\}$.

As consequence of Theorem 1.1, one has (see [**13**, Theorem 1.12])

Theorem 1.4. — *A finite tame set S is saturated if and only if, the Frobenius* $\sigma_\mathfrak{p}$, $\mathfrak{p} \in S$, *span the elementary p-abelian group* $\mathrm{Gal}(\mathrm{K}'(\sqrt[p]{\mathrm{V}_\varnothing})/\mathrm{K}')$.

We recall below the formula of Shafarevich applied in the case where S is tame (see for example [**25**, Chapter X, §7, Corollary 10.7.7]):

$$d(\mathrm{G}_S) = |S| - d(\mathscr{O}_\mathrm{K}^\times) + d(\mathrm{V}_S/(\mathrm{K}^\times)^p). \tag{1}$$

Hence when S is saturated, one has $d(\mathrm{G}_S) = |S| - d(\mathscr{O}_\mathrm{K}^\times)$.

1.1.3. Spectral sequence. — Let us start with the natural exact sequence

$$1 \longrightarrow \mathrm{H}_S \longrightarrow \mathrm{G}_S \longrightarrow \mathrm{G}_\varnothing \longrightarrow 1,$$

where the group H_S is the closed normal subgroup of G_S generated by the tame inertia elements $\tau_\mathfrak{p} \in \mathrm{G}_S$, $\mathfrak{p} \in S$. Set

$$\mathrm{X}_S := \mathrm{H}_S/[\mathrm{H}_S, \mathrm{G}_\varnothing]\mathrm{H}_S^p.$$

Recall as $\mathrm{G}_\varnothing$ is a pro-p group, the compact ring $\mathbb{F}_p[\![\mathrm{G}_\varnothing]\!]$ is local and acts continuously on $\mathrm{H}_S/[\mathrm{H}_S, \mathrm{H}_S]\mathrm{H}_S^p$. We give an easy lemma that can be found in [**13**] (see Lemmas 1.11 and 1.12).

Lemma 1.5. — *Let S be a finite set of tame prime ideals of* $\mathscr{O}_\mathrm{K}$.

(*i*) *The* $\mathbb{F}_p[\![\mathrm{G}_\varnothing]\!]$*-module* $\mathrm{H}_S/[\mathrm{H}_S, \mathrm{H}_S]\mathrm{H}_S^p$ *is topologically finitely generated by at most* $|S|$ *elements.*

(*ii*) *One has the exact sequence*

$$1 \longrightarrow H^1(\mathrm{G}_\varnothing) \longrightarrow H^1(\mathrm{G}_S) \longrightarrow \mathrm{X}_S^\vee \longrightarrow Ш^2_\varnothing \longrightarrow Ш^2_S.$$

In particular, if S is such that $H^1(\mathrm{G}_\varnothing) \simeq H^1(\mathrm{G}_S)$, then $\mathrm{X}_S^\vee \hookrightarrow Ш^2_\varnothing$. If moreover S is also saturated then $\mathrm{X}_S^\vee \simeq Ш^2_\varnothing$.

To conclude this subsection, let us observe the following: Let $\mathrm{F}_0/\mathrm{K}_\varnothing$ be a cyclic extension of degree p in K_S/K such that F_0/K is Galois. Then F_0 comes from a finite level: there exists a finite extension F/K and a cyclic extension F_1/F of degree p, ramified at some places above S, such that $\mathrm{F}_2 = \mathrm{K}_\varnothing \mathrm{F}_1$. The estimate for $\dim H^2(\mathrm{G}_\varnothing)$ can be done by using the previous lemma, typically by seeking the fields F_0: this is the spirit of the method involving the Hochschild-Serre spectral sequence.

***Example 1.6* (The field $\mathbb{Q}(\sqrt{-5460})$).** — Set $p = 2$ and $\mathrm{K} = \mathbb{Q}(\sqrt{-5460})$. The rational primes in $\{43, 53, 101, 149, 157\}$ all split in K. Let $S = \{\mathfrak{p}_{43}, \mathfrak{p}_{53}, \mathfrak{p}_{101}, \mathfrak{p}_{149}, \mathfrak{p}_{157}\}$, the first primes above each of these as MAGMA computes them. We denote the abelian group $\prod_{i=1}^d \mathbb{Z}/a_i$ by $(a_1, \cdots, a_d)$. Computations show that:

(*i*) $\mathrm{RCG}_\mathrm{K}(\varnothing) = (2, 2, 2, 2)$;

(*ii*) $\mathrm{RCG}_\mathrm{K}(\mathfrak{p}_{53}, \mathfrak{p}_{101}, \mathfrak{p}_{149}, \mathfrak{p}_{157}) = (4, 8, 8, 8)$; Furthermore, for each of these primes $\mathfrak{p}$ we compute $\mathrm{RCG}_\mathrm{K}(\mathfrak{p}) = (2, 2, 2, 4)$.

(*iii*) $\mathrm{RCG}_\mathrm{K}(S) = (8, 8, 8, 8)$.

Since $\mathscr{O}_\mathrm{K}^\times = \pm 1$, one easily sees $d(\mathrm{V}_\varnothing/(\mathrm{K}^\times)^2) = 4 + 1 = 5$ hence S is saturated by (*iii*) and equality (1), and (*ii*) implies $d(\mathrm{X}_{\{\mathfrak{p}_{53},\mathfrak{p}_{101},\mathfrak{p}_{149},\mathfrak{p}_{157}\}}) = 4$ and then $\mathrm{d}(\mathrm{X}_S) \geqslant 4$. As $\mathrm{X}_{\{\mathfrak{p}\}}$ is nontrivial for $\mathfrak{p} \in \{\mathfrak{p}_{53}, \mathfrak{p}_{101}, \mathfrak{p}_{149}, \mathfrak{p}_{157}\}$, we see there is a quadratic extension above $\mathrm{K}_\varnothing$ ramified at $\mathfrak{p}$. We have produced four independent elements of $Ш^2_\varnothing$.

Now take $\mathrm{F} = \mathrm{K}(i) \subset \mathrm{K}_\varnothing$; $\mathfrak{p}_{43}$ is inert in F/K. An easy computation shows that $\mathrm{RCG}_\mathrm{F}(\varnothing) = (4, 2, 2, 2)$ and $\mathrm{RCG}_\mathrm{F}(\mathfrak{p}_{43}) = (4, 4, 2, 2)$. As $\mathrm{F}_\varnothing = \mathrm{K}_\varnothing$ we have an extension over $\mathrm{K}_\varnothing$ ramified only at $\mathfrak{p}_{43}$, so $d(\mathrm{X}_S) = 5$, and by Lemma 1.5 we conclude that $r(\mathrm{G}_\varnothing) = 5$.

1.2. Universal norms and relations. — Put $\mathscr{O}_{\mathrm{K}_\varnothing}^\times = \bigcup_\mathrm{F} \mathscr{O}_\mathrm{F}^\times$, where F/K run through the finite Galois extensions in $\mathrm{K}_\varnothing/\mathrm{K}$. Recall the following theorem due to Wingberg [**42**]; see also [**25**, Theorem 8.8.1, Chapter VIII, §8] where we take $S = T = \varnothing$, $\mathfrak{c}$ to be the full class of finite p-groups and $A = \mathbb{Z}$. We have written the results there in our notation.

***Theorem 1.7* (Wingberg).** — *One has $\hat{H}^i(\mathrm{G}_\varnothing, \mathscr{O}_{\mathrm{K}_\varnothing}^\times) \simeq \hat{H}^{3-i}(\mathrm{G}_\varnothing, \mathbb{Z})^\vee$.*

The exact sequence $0 \longrightarrow \mathbb{Z} \xrightarrow{\times p} \mathbb{Z} \longrightarrow \mathbb{Z}/p \longrightarrow 0$ gives:

$$0 \longrightarrow H^2(\mathrm{G}_\varnothing, \mathbb{Z})/p \longrightarrow H^2(\mathrm{G}_\varnothing, \mathbb{Z}/p) \longrightarrow H^3(\mathrm{G}_\varnothing, \mathbb{Z})[p] \longrightarrow 0.$$

Taking the Pontryagin dual, one obtains:

$$(2) \qquad 0 \longrightarrow H^3(\mathrm{G}_\varnothing, \mathbb{Z})^\vee/p \longrightarrow H^2(\mathrm{G}_\varnothing, \mathbb{Z}/p)^\vee \longrightarrow H^2(\mathrm{G}_\varnothing, \mathbb{Z})^\vee[p] \longrightarrow 0.$$

By Theorem 1.7:

$$H^2(\mathrm{G}_\varnothing, \mathbb{Z})^\vee \simeq H^1(\mathrm{G}_\varnothing, \mathscr{O}_{\mathrm{K}_\varnothing}^\times), \text{ and } H^3(\mathrm{G}_\varnothing, \mathbb{Z})^\vee \simeq \hat{H}^0(\mathrm{G}_\varnothing, \mathscr{O}_{\mathrm{K}_\varnothing}^\times).$$

Recall
$$\hat{H}^0(\mathrm{G}_\varnothing, \mathscr{O}_{\mathrm{K}_\varnothing}^\times) \simeq \varprojlim_{\mathrm{F}} \mathscr{O}_{\mathrm{K}}^\times/\mathrm{N}_{\mathrm{F}/\mathrm{K}}\mathscr{O}_{\mathrm{F}}^\times,$$
where F/K run through the finite Galois extensions in $\mathrm{K}_\varnothing/\mathrm{K}$, $\mathrm{N}_{\mathrm{F}/\mathrm{K}}$ is the norm in F/K, and $H^1(\mathrm{G}_\varnothing, \mathscr{O}_{\mathrm{K}_\varnothing}^\times)$ is the p-part of Cl_K (see for example [**25**, Lemma 8.8.4, Chapter VIII, §8]).
This observation associated to Theorem 1.7 allows us to prove:

Corollary 1.8. — *One has* $\mathrm{Def}(\mathrm{G}_\varnothing) = d(\mathscr{E}_\mathrm{K}/\mathrm{N}_{\mathrm{K}_\varnothing/\mathrm{K}}\mathscr{E}_{\mathrm{K}_\varnothing})$, *where* $\mathrm{N}_{\mathrm{K}_\varnothing/\mathrm{K}}\mathscr{E}_{\mathrm{K}_\varnothing} := \bigcap_{\mathrm{F}/\mathrm{K}} \mathrm{N}_{\mathrm{F}/\mathrm{K}}\mathscr{E}_\mathrm{F}$. *In particular when* $[\mathrm{F}:\mathrm{K}]$ *is sufficiently large one has* $\mathrm{Def}(\mathrm{G}_\varnothing) = d(\mathscr{E}_\mathrm{K}/\mathrm{N}_{\mathrm{F}/\mathrm{K}}\mathscr{E}_\mathrm{F})$.

Proof. — If F/K is a finite Galois extension in $\mathrm{K}_\varnothing/\mathrm{K}$ then $(\mathscr{O}_\mathrm{K}^\times)^{[\mathrm{F}:\mathrm{K}]} \subset \mathrm{N}_{\mathrm{F}/\mathrm{K}}\mathscr{O}_F^\times$, hence $\mathscr{O}_\mathrm{K}^\times/\mathrm{N}_{\mathrm{F}/\mathrm{K}}\mathscr{O}_F^\times$ is a finite abelian p-group and $\varprojlim_{\mathrm{F}} \mathscr{O}_\mathrm{K}^\times/\mathrm{N}_{\mathrm{F}/\mathrm{K}}\mathscr{O}_\mathrm{F}^\times$ is an abelian pro-p group (obviously finitely generated). Then $\varprojlim_{\mathrm{F}} \mathscr{O}_\mathrm{K}^\times/\mathrm{N}_{\mathrm{F}/\mathrm{K}}\mathscr{O}_\mathrm{F}^\times \simeq \varprojlim_{\mathrm{F}} \mathbb{Z}_p \otimes \left(\mathscr{O}_\mathrm{K}^\times/\mathrm{N}_{\mathrm{F}/\mathrm{K}}\mathscr{O}_\mathrm{F}^\times\right)$. But as $\mathbb{Z}_p$ is $\mathbb{Z}$-flat, one gets $\mathbb{Z}_p \otimes \left(\mathscr{O}_\mathrm{K}^\times/\mathrm{N}_{\mathrm{F}/\mathrm{K}}\mathscr{O}_\mathrm{F}^\times\right) \simeq E_\mathrm{K}/\left(\mathbb{Z}_p \otimes \mathrm{N}_{\mathrm{F}/\mathrm{K}}\mathscr{O}_\mathrm{F}^\times\right) = E_\mathrm{K}/\overline{\mathrm{N}_{\mathrm{F}/\mathrm{K}}\mathscr{O}_\mathrm{F}^\times}$, where $E_\mathrm{K} = \mathbb{Z}_p \otimes \mathscr{O}_\mathrm{K}^\times$ and $\overline{\mathrm{N}_{\mathrm{F}/\mathrm{K}}\mathscr{O}_\mathrm{F}^\times}$ is the closure of $\mathrm{N}_{\mathrm{F}/\mathrm{K}}\mathscr{O}_\mathrm{F}^\times$ in $\mathbb{Z}_p \otimes \mathscr{O}_\mathrm{K}^\times$. Hence,
$$\varprojlim_{\mathrm{F}} \mathscr{O}_\mathrm{K}^\times/\mathrm{N}_{\mathrm{F}/\mathrm{K}}\mathscr{O}_\mathrm{F}^\times \simeq E_\mathrm{K}/\bigcap_{\mathrm{F}} \overline{\mathrm{N}_{\mathrm{F}/\mathrm{K}}\mathscr{O}_\mathrm{F}^\times}.$$
Thus
$$\mathbb{F}_p \otimes \varprojlim_{\mathrm{F}} \mathscr{O}_\mathrm{K}^\times/\mathrm{N}_{\mathrm{F}/\mathrm{K}}\mathscr{O}_\mathrm{F}^\times \simeq E_\mathrm{K}/E_\mathrm{K}^p \bigcap_{\mathrm{F}} \overline{\mathrm{N}_{\mathrm{F}/\mathrm{K}}\mathscr{O}_\mathrm{F}^\times} \simeq \mathscr{E}_\mathrm{K}/\mathrm{N}_{\mathrm{K}_\varnothing/\mathrm{K}}\mathscr{E}_{\mathrm{K}_\varnothing}.$$
The exact sequence (2) becomes
$$0 \longrightarrow \mathscr{E}_K/\mathrm{N}_{\mathrm{K}_\varnothing/\mathrm{K}}\mathscr{E}_{\mathrm{K}_\varnothing} \longrightarrow H^2(\mathrm{G}_\varnothing, \mathbb{Z}/p)^\vee \longrightarrow \mathrm{Cl}_\mathrm{K}[p] \longrightarrow 0, \tag{3}$$
and computing dimensions gives the result. □

For $\#\mathrm{G}_\varnothing < \infty$ it has been known for a long time that the number of relations of $\mathrm{G}_\varnothing$ is related to the norm of the units in the tower. See for example §2 of [**29**]
As a consequence, one also has

Corollary 1.9. — *Let* F/K *be a finite Galois extension in* $\mathrm{K}_\varnothing/\mathrm{K}$*. Then* $\mathrm{Def}(\mathrm{G}_\varnothing) \geqslant d\left(\mathscr{O}_\mathrm{K}^\times/\mathrm{N}_{\mathrm{F}/\mathrm{K}}\mathscr{O}_\mathrm{F}^\times\right)$, *and one has equality when* F *is sufficiently large.*

Proof. — This is obvious using that $\mathscr{E}_\mathrm{K}/\mathrm{N}_{\mathrm{K}_\varnothing/\mathrm{K}}\mathscr{E}_{\mathrm{K}_\varnothing} \twoheadrightarrow \mathscr{E}_\mathrm{K}/\mathrm{N}_{\mathrm{F}/\mathrm{K}}\mathscr{E}_\mathrm{F}$. For the equality, use the fact that $\mathscr{E}_\mathrm{K}$ is finite. □

When $p=2$, if -1 is not a norm of a unit in a quadratic subextension F/K of $\mathrm{K}_\varnothing/\mathrm{K}$, then $-1 \notin \mathrm{N}_{\mathrm{K}_\varnothing/\mathrm{K}}\mathscr{O}_{\mathrm{K}_\varnothing}^\times$, which implies $\mathrm{Def}(\mathrm{G}_\varnothing) \geqslant 1$. We will see that this condition appears almost all the time when K is an imaginary quadratic extension. We close this subsection with a basic fact.

Fact. — *For* S *a finite set of tame places,* $0 \leqslant \mathrm{Def}(\mathrm{G}_S)$.

Proof. — We refer to [**28**], especially Lemma 6.8.6, for the facts we need concerning the homology of profinite groups. From the exact sequence of compact groups
$$0 \longrightarrow \mathbb{Z}_p \xrightarrow{\times p} \mathbb{Z}_p \longrightarrow \mathbb{Z}/p \longrightarrow 0$$

we obtain the homology sequence

$$\cdots \longrightarrow H_2(\mathrm{G}_S, \mathbb{Z}/p) \twoheadrightarrow H_1(\mathrm{G}_S, \mathbb{Z}_p)[p].$$

As $H_1(\mathrm{G}_S, \mathbb{Z}_p) \simeq \mathrm{G}_S^{ab}$, we have $d(\mathrm{G}_S) = d\big(\mathrm{G}_S^{ab}[p]\big) \leqslant d\big(H_2(\mathrm{G}_S, \mathbb{Z}/p)\big) = r(\mathrm{G}_S)$. $\square$

1.3. Minkowski units. —

1.3.1. — Recall that for a finite group G, the ring $\mathbb{F}_p[\mathrm{G}]$ is a Frobenius algebra (see for example [**4**, §62]): every free submodule of an $\mathbb{F}_p[\mathrm{G}]$-module M is in direct sum so we may write $\mathrm{M} = \mathbb{F}_p[\mathrm{G}]^t \oplus \mathrm{N}$, where N is torsion (for every element $n \in \mathrm{N}$, there exists $0 \neq h \in \mathbb{F}_p[\mathrm{G}]$ such that $h \cdot n = 0$), and $t := t_{\mathrm{G}}(\mathrm{M})$ is uniquely determined (by Krull-Schmidt Theorem). Observe that if $\mathrm{M}^\wedge$ is the Pontryagin dual of M, then $t_{\mathrm{G}}(\mathrm{M}) = t_{\mathrm{G}}(\mathrm{M}^\wedge)$.
We record some useful properties. Let $\mathrm{H} \subset \mathrm{G}$ be a subgroup of G.
(*i*) Recall first that by Mackey's decomposition theorem, one has the isomorphism of $\mathbb{F}_p[\mathrm{H}]$-modules $\mathrm{Res}_{\mathrm{H}}\mathbb{F}_p[\mathrm{G}] \simeq \mathbb{F}_p[\mathrm{H}]^{\oplus[\mathrm{G}:\mathrm{H}]}$.
(*ii*) Suppose moreover $\mathrm{H} \lhd \mathrm{G}$, and denote by $N_{\mathrm{H}} = \sum_{h\in\mathrm{H}} h \in \mathbb{F}_p[\mathrm{G}]$ the norm map from H. For an $\mathbb{F}_p[\mathrm{G}]$-module M let M^H denote the invariants. Then one easily obtains the isomorphism of $\mathbb{F}_p[\mathrm{G}]$-modules

$$\mathbb{F}_p[\mathrm{G}/\mathrm{H}] \simeq \mathbb{F}_p \otimes_{\mathbb{F}_p[\mathrm{H}]} \mathbb{F}_p[\mathrm{G}] \simeq \mathbb{F}_p[\mathrm{G}]^{\mathrm{H}} \tag{4}$$

and $N_{\mathrm{H}}(\mathbb{F}_p[\mathrm{G}]) = \mathbb{F}_p[\mathrm{G}]^{\mathrm{H}}$ so

$$N_{\mathrm{H}}(\mathbb{F}_p[\mathrm{G}]) \simeq \mathbb{F}_p[\mathrm{G}/\mathrm{H}] \tag{5}$$

as $\mathbb{F}_p[\mathrm{G}/\mathrm{H}]$-modules.

1.3.2. — Let F/K be a finite Galois extension of number fields with Galois group G.

Definition 1.10. — Let $\mathscr{E}_{\mathrm{F}} := \mathbb{F}_p \otimes \mathscr{O}_{\mathrm{F}}^\times$. We say that F/K has a Minkowski unit (at p), if $\mathscr{E}_{\mathrm{F}}$ contains a *nontrivial free* $\mathbb{F}_p[\mathrm{G}]$-submodule. In other word, F/K has a Minkowski unit if $t_{\mathrm{G}}(\mathscr{E}_{\mathrm{F}}) \geqslant 1$.

Hence the quantity $t_{\mathrm{G}}(\mathscr{E}_{\mathrm{F}})$ measures "the number" of independent Minkowski units in F/K.

If $(p, |\mathrm{G}|) = 1$ then $\mathscr{E}_{\mathrm{F}}$ is a semisimple $\mathbb{F}_p[\mathrm{G}]$-module. Determining the existence of Minkowski units is more difficult when $(p, |\mathrm{G}|) = p$. When G is a p-group, and F/K is unramified, it is tempting to regard the existence of a Minkowski unit in F/K as rare.

1.3.3. Example. — We want to illustrate the notion of Minkowski units.

Lemma 1.11. — *Let* F/K *be a p-extension with Galois group* G. *Let* $S = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_k\}$ *be a set of tame primes of* K *that split completely in* F/K. *If* $d(\mathrm{G}_{\mathrm{F},S}) = d(\mathrm{G}_{\mathrm{F},\varnothing})$ *then* $t_{\mathrm{G}}(\mathrm{V}_{\mathrm{F},\varnothing}) \geqslant k$, *and if* $|\mathrm{G}_{\mathrm{F},S}^{ab}| = |\mathrm{G}_{\mathrm{F},\varnothing}^{ab}|$ *then* $t_{\mathrm{G}}(\mathscr{E}_{\mathrm{F}}) \geqslant k$.

Proof. — Observe first that G acts on $\mathrm{Gal}(\mathrm{F}'(\sqrt[p]{\mathrm{V}_{\mathrm{F},\varnothing}})/\mathrm{F}')$ (resp. on $\mathrm{Gal}(\mathrm{F}'(\sqrt[p]{\mathscr{O}_{\mathrm{F}}^\times})/\mathrm{F}')$). Then by Remark 1.2, one has

$$t_{\mathrm{G}}\big(\mathrm{V}_{\mathrm{F}}/(\mathrm{F}^\times)^p\big) = t_{\mathrm{G}}\big(\mathrm{Gal}(\mathrm{F}'(\sqrt[p]{\mathrm{V}_{\mathrm{F},\varnothing}})/\mathrm{F}')\big), \tag{6}$$

and

$$t_{\mathrm{G}}(\mathscr{E}_{\mathrm{F}}) = t_{\mathrm{G}}\big((\mathscr{E}_{\mathrm{F}})^\wedge\big) = t_{\mathrm{G}}\big(\mathrm{Gal}(\mathrm{F}'(\sqrt[p]{\mathscr{O}_{\mathrm{F}}^\times}/\mathrm{F}')\big). \tag{7}$$

For all prime ideals $\mathfrak{P}_{ij}|\mathfrak{p}_i$ of $\mathscr{O}_{\mathrm{F}}$ we consider the Frobenius automorphisms $\sigma_{\mathfrak{P}_{ij}}$ in $\mathrm{Gal}(\mathrm{F}'(\sqrt[p]{\mathrm{V}_{\mathrm{F},\varnothing}})/\mathrm{F}')$. Note that we are no longer in an abelian over K situation as just before Theorem 1.1. By Theorem 1.1 (i), the hypothesis $d(\mathrm{G}_{\mathrm{F},S}) = d(\mathrm{G}_{\mathrm{F},\varnothing})$ implies the Frobenius automorphisms $\sigma_{\mathfrak{P}_{ij}}$ in $\mathrm{Gal}(\mathrm{F}'(\sqrt[p]{\mathrm{V}_{\mathrm{F},\varnothing}})/\mathrm{F}')$ are without nontrivial relation. As each $\mathfrak{p}_i$ splits completely in F/K, we have that $\mathrm{Gal}(\mathrm{F}'(\sqrt[p]{\mathrm{V}_{\mathrm{F},\varnothing}})/\mathrm{F}')$ contains k distinct free $\mathbb{F}_p[\mathrm{G}]$-modules, one for each $\mathfrak{p}_i$. The first assertion follows by (6). For the second assertion, use the second part of Theorem 1.1 and (7). □

Recall that we denote the abelian group $\prod_{i=1}^{d} \mathbb{Z}/a_i\mathbb{Z}$ by $(a_1, \cdots, a_d)$. Let $p = 2$ and $\mathrm{K} = \mathbb{Q}(\sqrt{5 \cdot 13 \cdot 17 \cdot 29})$ and let $\mathrm{H} = \mathbb{Q}(\sqrt{5}, \sqrt{13}, \sqrt{17}, \sqrt{29})$ be its Hilbert class field. Here $\mathrm{Cl}_{\mathrm{K}} = (2,2,2)$, and $\mathrm{Cl}_{\mathrm{H}} = (4,4)$. Consider the primes $\ell = 2311$ and $q = 3319$. We easily see $\ell\mathscr{O}_{\mathrm{K}} = \mathfrak{l}_1\mathfrak{l}_2$ and $q\mathscr{O}_{\mathrm{K}} = \mathfrak{q}_1\mathfrak{q}_2$ and these ideals are all principal. In the table below we compute the 2-parts of the ray class groups for K and H of the given conductors. The

Table 1. Ray Class Groups

Conductor	K	H
1	$(2,2,2)$	$(4,4)$
$\mathfrak{l}_i, i \in \{1,2\}$	$(2,2,2)$	$(4,4)$
$\mathfrak{q}_i, i \in \{1,2\}$	$(2,2,2)$	$(4,4)$
$\mathfrak{l}_1\mathfrak{q}_1$	$(2,2,2)$	$(2,2,2,4,4)$
$\mathfrak{l}_1\mathfrak{q}_2$	$(2,2,2,2)$	$(2,2,2,2,2,4,8)$
$\mathfrak{l}_2\mathfrak{q}_1$	$(2,2,2,2)$	$(2,2,2,2,2,4,8)$
$\mathfrak{l}_2\mathfrak{q}_2$	$(2,2,2)$	$(2,2,2,4,4)$

computations were done with MAGMA (see [**40**]) and assume the GRH. Note that in the first three rows, the ray class groups are identical. As the principal ideals $\mathfrak{l}_i$ and $\mathfrak{q}_i$ split completely in H/K, by Lemma 1.11 one sees that $\mathscr{O}_{\mathrm{H}}^{\times} \otimes \mathbb{F}_2$ has a Minkowski unit over K: in other words putting $\mathrm{G} = \mathrm{Gal}(\mathrm{H}/\mathrm{K}) \simeq (\mathbb{Z}/2\mathbb{Z})^3$, one has $t_{\mathrm{G}}(\mathscr{E}_{\mathrm{H}}) \geqslant 1$. Note H is a degree 16 totally real field so $\dim \mathscr{E}_{\mathrm{H}} = 16$ and $\mathscr{E}_{\mathrm{H}} \simeq_{\mathrm{G}} \mathbb{F}_2[\mathrm{G}] \oplus M$ where $\dim M = 8$ so M a priori could be free.

We now show that M is not free. Set $\mathrm{K}_0 = \mathrm{K}$, $\mathrm{K}_1 = \mathbb{Q}(\sqrt{5 \cdot 17})$, and $\mathrm{K}_2 = \mathbb{Q}(\sqrt{13 \cdot 29})$. Let F be the biquadratic field $\mathrm{K}_1\mathrm{K}_2$. Computations show that $\mathrm{Cl}_{\mathrm{K}_1} = (2)$, $\mathrm{Cl}_{\mathrm{K}_2} = (2)$, and $\mathrm{Cl}_{\mathrm{F}} = (2,4)$. Denote by ε_i the fundamental unit of K_i, and put

$$e = \# \left(\mathscr{O}_{\mathrm{F}}^{\times} / \langle -1, \varepsilon_i, i = 0,1,2 \rangle \right).$$

Applying the Brauer class formula in the biquadratic extension $\mathrm{F}/\mathbb{Q}$, *i.e.* $|\mathrm{Cl}_{\mathrm{F}}| = \frac{1}{4}e|\mathrm{Cl}_{\mathrm{K}}||\mathrm{Cl}_{\mathrm{K}_1}||\mathrm{Cl}_{\mathrm{K}_2}|$, to deduce $e = 1$, and then $\mathscr{O}_{\mathrm{F}}^{\times} = \langle -1, \varepsilon_i, i = 0,1,2 \rangle$.
Let σ be a generator of $\mathrm{G} = \mathrm{G}(\mathrm{F}/\mathrm{K})$. We compute:

(i) the norm of ε_2 in F/K is $+1$,

(ii) the norm of ε_1 in F/K is -1,

(iii) σ acts trivially on ε_0,

Hence, as we will observe in Lemma 5.1, one obtains that $\mathscr{E}_{\mathrm{F}} \simeq \mathbb{F}_2[\mathrm{G}'] \oplus \mathbb{F}_2^2$, where $\mathrm{G}' = \mathrm{Gal}(\mathrm{F}/\mathrm{K})$. Finally since $\mathscr{E}_{\mathrm{H}} \twoheadrightarrow \mathscr{E}_{\mathrm{F}}$, and $t_{\mathrm{G}'}(\mathscr{E}_{\mathrm{F}}) \geqslant t_{\mathrm{G}}(\mathscr{E}_{\mathrm{H}})$ we conclude that $t_{\mathrm{G}}(\mathscr{E}_{\mathrm{H}}) = 1$.

2. Detecting the relations along $\mathrm{K}_\varnothing/\mathrm{K}$

As mentioned in the remark in the introduction, we can easily find d elements of $Ш^2_\varnothing$ by constructing ramified extensions at a low level in the tower $\mathrm{K}_\varnothing/\mathrm{K}$. For (G_n) a sequence of open normal subgroups of G with $\bigcap_{n=1}^{\infty} \mathrm{G}_n = \{e\}$, let K_n be the fixed field of G_n and set $\mathrm{H}_n = \mathrm{Gal}(\mathrm{K}_n/\mathrm{K})$. In this section we show that the presence of torsion elements in the $\mathbb{F}_p[\mathrm{H}_n]$-module $\mathrm{Gal}\left(\mathrm{K}'_n\left(\sqrt[p]{\mathscr{O}^\times_{\mathrm{K}_n}}\right)/\mathrm{K}'_n\right)$ can give rise to more relations.

2.1. First observations. — Let p be a prime number and K be a number field.
If F/K is a Galois extension with Galois group G, the norm map N_G sends $\mathscr{E}_\mathrm{F}$ to $\frac{\mathscr{O}^\times_\mathrm{K}}{\mathscr{O}^\times_\mathrm{K} \cap (\mathscr{O}^\times_\mathrm{F})^p} \subset \mathscr{E}_\mathrm{F}$; denote by $N'_\mathrm{G} : \mathscr{E}_\mathrm{F} \to \mathscr{E}_\mathrm{K}$ the map from $\mathscr{E}_\mathrm{F}$ to $\mathscr{E}_\mathrm{K}$ induced by the norm in F/K. The commutative diagram:

$$\begin{tikzcd}
\mathscr{E}_\mathrm{F} \arrow[r, "N_\mathrm{G}"] \arrow[dr, "N'_\mathrm{G}"'] & \frac{\mathscr{O}^\times_\mathrm{K}}{\mathscr{O}^\times_\mathrm{K} \cap (\mathscr{O}^\times_\mathrm{F})^p} \arrow[r, hook] & \mathscr{E}_\mathrm{F} \\
& \mathscr{E}_\mathrm{K} \arrow[u, two heads] &
\end{tikzcd}$$

implies the following easy lemma:

Lemma 2.1. — *One has $N'_\mathrm{G}(\mathscr{E}_\mathrm{F}) \twoheadrightarrow N_\mathrm{G}(\mathscr{E}_\mathrm{F})$. Moreover, $\mathscr{O}^\times_\mathrm{K} \cap (\mathscr{O}^\times_\mathrm{F})^p = (\mathscr{O}^\times_\mathrm{K})^p \implies N'_\mathrm{G}(\mathscr{E}_\mathrm{F}) \simeq N_\mathrm{G}(\mathscr{E}_\mathrm{F})$.*

The study of the norm map N_G is "purely algebraic", i.e. it does not involve number theory. Lemma 2.2 below is proved at the beginning of the proof of [**26**, Lemma 2]). Since that Lemma is stated differently we include a proof that is essentially from [**26**].

Lemma 2.2. — *Let G be a finite p-group and M an $\mathbb{F}_p[\mathrm{G}]$-module. Let $\mathrm{N}_\mathrm{G} : M \to M$ be the norm map. Let $m \in M$. Then $\mathrm{N}_\mathrm{G}(m) = 0$ if and only if m is a torsion element.*

Proof. — Let $0 \neq m \in M$. Recall that the annihilator A_m of a nontrivial element $m \in M$ is an ideal of $\mathbb{F}_p[\mathrm{G}]$ and that m is a torsion element if and only if $A_m \neq 0$.
If $A_m = 0$ then the $\mathbb{F}_p[\mathrm{G}]$-span of m is isomorphic to $\mathbb{F}_p[\mathrm{G}]$ and as $\mathrm{N}_\mathrm{G}(\mathbb{F}_p[\mathrm{G}]) = \mathbb{F}_p$ by (5), we see $\mathrm{N}_\mathrm{G}(m) \neq 0$.
Conversely, suppose that $A_m \neq 0$. Then $A_m^\mathrm{G} \neq 0$ since G is a p-group acting on a nontrivial $\mathbb{F}_p$-vector space. Hence $A_m^\mathrm{G} \subset (\mathbb{F}_p[\mathrm{G}])^\mathrm{G}$ which is in turn the one-dimensional vector space $\mathbb{F}_p \cdot \mathrm{N}_\mathrm{G}$. Thus $\mathbb{F}_p \cdot \mathrm{N}_\mathrm{G} = A_m^\mathrm{G} \subset A_m$ so $\mathrm{N}_\mathrm{G}(m) = 0$. □

More generally, one has

Theorem 2.3. — *Let F/K be a finite p-extension with Galois group G and write $\mathrm{N}'_\mathrm{G}(\mathscr{E}_\mathrm{F}) \simeq \mathbb{F}_p^t$. Then $t_\mathrm{G}(\mathscr{E}_\mathrm{F}) \leqslant t \leqslant t_\mathrm{G}(\mathscr{E}_\mathrm{F}) + d\left(\frac{\mathscr{O}^\times_\mathrm{K} \cap (\mathscr{O}^\times_\mathrm{F})^p}{(\mathscr{O}^\times_\mathrm{K})^p}\right)$. In particular if $\mathscr{O}^\times_\mathrm{K} \cap (\mathscr{O}^\times_\mathrm{F})^p = (\mathscr{O}^\times_\mathrm{K})^p$, then $t = t_\mathrm{G}(\mathscr{E}_\mathrm{F})$.*

Proof. — Write $\mathscr{E}_\mathrm{F} \simeq \mathbb{F}_p[\mathrm{G}]^{t_\mathrm{G}(\mathscr{E}_\mathrm{F})} \oplus \mathrm{N}$, where N is generated by torsion elements as an $\mathbb{F}_p[\mathrm{G}]$-module. By (5) and Lemma 2.2 one has $\mathrm{N}_\mathrm{G}(\mathscr{E}_\mathrm{F}) \simeq \mathbb{F}_p^{t_\mathrm{G}(\mathscr{E}_\mathrm{F})}$. So by Lemma 2.1 we see $\mathrm{N}'_\mathrm{G}(\mathscr{E}_\mathrm{F}) \simeq \mathrm{N}_\mathrm{G}(\mathscr{E}_\mathrm{F}) \simeq \mathbb{F}_p^{t_\mathrm{G}(\mathscr{E}_\mathrm{F})}$, proving the result when $\mathscr{O}^\times_\mathrm{K} \cap (\mathscr{O}^\times_\mathrm{F})^p = (\mathscr{O}^\times_\mathrm{K})^p$.

By noting that the 'difference' between $\mathrm{N}_{\mathrm{G}}(\mathscr{E}_{\mathrm{F}})$ and $\mathrm{N}'_{\mathrm{G}}(\mathscr{E}_{\mathrm{F}})$ is exactly $\frac{\mathrm{N}_{\mathrm{G}}(\mathscr{O}_{\mathrm{F}}^{\times})\cap(\mathscr{O}_{\mathrm{F}}^{\times})^p}{(\mathscr{O}_{\mathrm{K}}^{\times})^p}$ which has p-rank at most $d\left(\frac{\mathscr{O}_{\mathrm{K}}^{\times}\cap(\mathscr{O}_{\mathrm{F}}^{\times})^p}{(\mathscr{O}_{\mathrm{K}}^{\times})^p}\right)$, we obtain the general case. □

2.2. Exhibiting relations via the Hochschild-Serre spectral sequence. — In this subsection, we flesh out the details of the process described in the Remark of the Introduction for explicitly exhibiting $d(\mathrm{G}_\varnothing)$ relations in a minimal presentation of $\mathrm{G}_\varnothing$. It would be helpful to refer to Figure 1 from the introduction. Put $\mathrm{K}' = \mathrm{K}(\zeta_p)$. Let $S = S_1 \cup S_2$ be a set of tame prime ideals of $\mathscr{O}_{\mathrm{K}}$ such that:

- S_1 is a minimal set whose Frobenius automorphisms generate the $d(\mathrm{G}_\varnothing)$-dimensional $\mathbb{F}_p$-vector space $\mathrm{Gal}\left(\mathrm{K}'(\sqrt[p]{\mathrm{V}_\varnothing})/\mathrm{K}'(\sqrt[p]{\mathscr{O}_{\mathrm{K}}^{\times}})\right)$, and
- S_2 is a minimal set whose Frobenius automorphisms generate the $\mathbb{F}_p$-vector space $\mathrm{Gal}\left(\mathrm{K}'(\sqrt[p]{\mathscr{O}_{\mathrm{K}}^{\times}})/\mathrm{K}'\right)$ of dimension $r_1 + r_2 - 1 + \delta$.

Recall the Frobenius automorphisms above are well-defined up to nonzero scalar multiples in the Galois groups, which are vector spaces over $\mathbb{F}_p$. This ambiguity does not affect their spanning properties. One has

Lemma 2.4. — *The set S is saturated, in particular $Ш^2_S = \{0\}$. Moreover $d(\mathrm{G}_S) = d(\mathrm{G}_\varnothing)$, and $r(\mathrm{G}_\varnothing) = d(\mathrm{X}_S)$.*

Proof. — That S is saturated follows immediately from Theorem 1.4. As there is no dependence relation between the Frobenius automorphisms (the set S is minimal), Theorem 1.1 implies $d := d(\mathrm{G}_S) = d(\mathrm{G}_\varnothing)$. That $r(\mathrm{G}_\varnothing) = d(\mathrm{X}_S)$ follows from the second part with Lemma 1.5. □

Lemma 2.5. — *Write $(a_1, \cdots, a_d)$ for the p-part of $\mathrm{RCG}_{\mathrm{K}}(\varnothing)$ and let $S_1 = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_d\}$ as above. Then $\mathrm{RCG}_{\mathrm{K}}(\mathfrak{p}_1, \cdots, \mathfrak{p}_d) \twoheadrightarrow (pa_1, \cdots, pa_d)$.*

Proof. — This is a consequence of Theorem 1.1. As the primes of S_1 split completely in the governing extension $\mathrm{Gal}(\mathrm{K}'(\sqrt[p]{\mathscr{O}_{\mathrm{K}}^{\times}})/\mathrm{K}')$, for each prime ideal $\mathfrak{p} \in S_1$ we have $\#\mathrm{G}^{ab}_{\{\mathfrak{p}\}} \neq \#\mathrm{G}^{ab}_\varnothing$. We conclude by noting that $d(\mathrm{G}_{S_1}) = d(\mathrm{G}_\varnothing)$. □

Lemma 2.5 implies the existence of d independent degree-p cyclic extensions F_i of $\mathrm{K}_\varnothing$, each totally ramified at $\mathfrak{p}_i$, $i = 1, \cdots, d$, and on which $\mathrm{G}_\varnothing$ acts trivially, implying that $d(\mathrm{X}_S) \geqslant d$. *The rest of the relations are difficult and detected via the set S_2.*

2.3. Proof of Theorem A. — Let (G_n) be a sequence of open normal subgroups of $\mathrm{G}_\varnothing$ such that $\mathrm{G}_n \subset \mathrm{G}_{n+1}$ and $\bigcap_n \mathrm{G}_n = \{e\}$. Put $\mathrm{H}_n := \mathrm{G}_\varnothing/\mathrm{G}_n$, $\mathrm{K}_n := \mathrm{K}_\varnothing^{\mathrm{G}_n}$, and write $\mathscr{E}_{\mathrm{K}_n} := \mathbb{F}_p[\mathrm{H}_n]^{t_n} \oplus \mathrm{N}_n$ where N_n is torsion as an $\mathbb{F}_p[\mathrm{H}_n]$-module.

Lemma 2.6. — *The sequence (t_n) is nonincreasing.*

Proof. — Recall from (4) that the norm map from $\mathrm{H}_{n+1,n} := \mathrm{Gal}(\mathrm{K}_{n+1}/\mathrm{K}_n)$ on $\mathbb{F}_p[\mathrm{H}_{n+1}]$ induces the following $\mathbb{F}_p[\mathrm{H}_n]$-isomorphisms:

$$\mathbb{F}_p[\mathrm{H}_n] \simeq \mathbb{F}_p[\mathrm{H}_{n+1}]_{\mathrm{H}_{n+1,n}} \simeq \mathbb{F}_p[\mathrm{H}_{n+1}]^{\mathrm{H}_{n+1,n}}.$$

The norm map $N_{\mathrm{H}_{n+1,n}}$ of $\mathrm{K}_{n+1}/\mathrm{K}_n$ induces a morphism from $\mathscr{E}_{\mathrm{K}_{n+1}}$ to $\mathscr{E}_{\mathrm{K}_{n+1}}$ which allows us to obtain

$$\mathbb{F}_p[\mathrm{H}_n]^{t_{n+1}} \hookrightarrow \frac{\mathscr{O}_{\mathrm{K}_n}^{\times}}{\mathscr{O}_{\mathrm{K}_n}^{\times} \cap (\mathscr{O}_{\mathrm{K}_{n+1}}^{\times})^p} \twoheadleftarrow \mathscr{E}_{\mathrm{K}_n},$$

which implies $t_n \geqslant t_{n+1}$. $\square$

Definition 2.7. — Set $\lambda := \lambda_{\mathrm{K}_\varnothing/\mathrm{K}} = \lim_n t_n$. We call this the *Minkowski-rank* of the units along $\mathrm{K}_\varnothing/\mathrm{K}$.

One easily sees that λ does not depend on the sequence (G_n).

Let us write $p^\beta := [\mathrm{K}'(\sqrt[p]{\mathscr{O}_\mathrm{K}^\times}) \cap \mathrm{K}'\mathrm{K}_\varnothing : \mathrm{K}'] = \left[\mathscr{O}_\mathrm{K}^\times \cap (\mathscr{O}_{\mathrm{K}_\varnothing}^\times)^p : (\mathscr{O}_\mathrm{K}^\times)^p\right]$. Obviously, $\beta \leqslant \min(d(\mathscr{O}_\mathrm{K}^\times), d(\mathrm{G}_\varnothing))$.

Proposition 2.8. — *One has:* $\delta = 0 \Longrightarrow \beta = 0$.

Proof. — Recall $\mathrm{K}' := \mathrm{K}(\zeta_p)$. Let $\Delta = \mathrm{Gal}(\mathrm{K}'/\mathrm{K})$ be the Galois group of K'/K; by hypothesis Δ is of order coprime to p. As Δ acts trivially on $\mathscr{O}_\mathrm{K}^\times$, by Kummer duality the action of Δ over $\mathrm{Gal}(\mathrm{K}'(\sqrt[p]{\mathscr{O}_\mathrm{K}^\times})/\mathrm{K}')$ is given by the cyclotomic character; in particular, there is no nontrivial subspace of $\mathrm{Gal}(\mathrm{K}'(\sqrt[p]{\mathscr{O}_\mathrm{K}^\times})/\mathrm{K}')$ on which Δ acts trivially. As Δ acts trivially on $\mathrm{Gal}(\mathrm{K}'\mathrm{K}_\varnothing/\mathrm{K}')$, the result holds. $\square$

Theorem 2.9. — *We have the estimates:*

$$d(\mathscr{O}_\mathrm{K}^\times) - \lambda - \beta \leqslant \mathrm{Def}(\mathrm{G}_\varnothing) \leqslant d(\mathscr{O}_\mathrm{K}^\times) - \lambda.$$

In particular,

— *if* $\mathscr{O}_\mathrm{K}^\times \cap (\mathscr{O}_{\mathrm{K}_\varnothing}^\times)^p = (\mathscr{O}_\mathrm{K}^\times)^p$ *or if* $\delta = 0$, *then* $\mathrm{Def}(\mathrm{G}_\varnothing) = d(\mathscr{O}_\mathrm{K}^\times) - \lambda$.

— *if* $\lambda = d(\mathscr{O}_\mathrm{K}^\times)$ *then* $\mathrm{Def}(\mathrm{G}_\varnothing) = 0$.

Proof. — We keep the notations of the beginning of the section.
We give two proofs for the lower bound. The first one is 'algebraic' while the second is number-theoretic and is more 'explicit' in how we determine the existence of the relations.

We first establish the upper bound. Denote by N_{H_n} the norm map for the extension K_n/K. Observe that by Corollary 1.9, $\mathrm{Def}(\mathrm{G}_\varnothing) = d(\mathscr{E}_\mathrm{K}) - d(N'_{\mathrm{H}_n}(\mathscr{E}_{\mathrm{K}_n}))$ for $n \gg 0$. Take n sufficiently large such that $t_n = \lambda$. One has $d(N_{\mathrm{H}_n}(\mathscr{E}_{\mathrm{K}_n})) \geqslant \lambda$ (see Theorem 2.3), implying that $d(N'_{\mathrm{H}_n}(\mathscr{E}_{\mathrm{K}_n})) \geqslant \lambda$. Hence one gets:

$$\mathrm{Def}(\mathrm{G}_\varnothing) \leqslant d(\mathscr{O}_\mathrm{K}^\times) - \lambda.$$

Below are the two proofs of the lower bound.
• First proof:
Observe that $\beta = d\left(\frac{\mathscr{O}_\mathrm{K}^\times \cap (\mathscr{O}_{\mathrm{K}_n}^\times)^p}{(\mathscr{O}_\mathrm{K}^\times)^p}\right)$ since $n \gg 0$. By Theorem 2.3 one also has $d(N'_{\mathrm{H}_n}(\mathscr{E}_{\mathrm{K}_n})) \leqslant \lambda + \beta$, and then by Corollary 1.8 we get

$$\mathrm{Def}(\mathrm{G}_\varnothing) \geqslant d(\mathscr{O}_\mathrm{K}^\times) - \lambda - \beta.$$

• Second proof:
Here we show $d(\mathscr{O}_\mathrm{K}^\times) - \lambda - \beta \leqslant \mathrm{Def}(\mathrm{G}_\varnothing)$ using saturated sets and the Hochschild-Serre exact sequence.
First assume that $\zeta_p \in \mathrm{K}$ *i.e.* $\delta = 1$. Choose $n \gg 0$, and write $\mathscr{E}_{\mathrm{K}_n} = \mathbb{F}_p[\mathrm{H}_n]^\lambda \oplus \mathrm{N}_n$, where N_n is a H_n-torsion $\mathbb{F}_p[\mathrm{H}_n]$-module.
Put $\mathscr{E}'_\mathrm{K} := \frac{\mathscr{O}_\mathrm{K}^\times}{\mathscr{O}_\mathrm{K}^\times \cap (\mathscr{O}_{\mathrm{K}_n}^\times)^p} \hookrightarrow \mathscr{E}_{\mathrm{K}_n}$.
Hence $[\mathrm{L}_4 : \mathrm{K}_n] = \#\mathscr{E}'_\mathrm{K}$. Observe that $\mathrm{Gal}(\mathrm{L}_4/\mathrm{K}_n) \simeq \mathbb{F}_p^t$, where $t = d(\mathscr{O}_\mathrm{K}^\times) - \beta$.

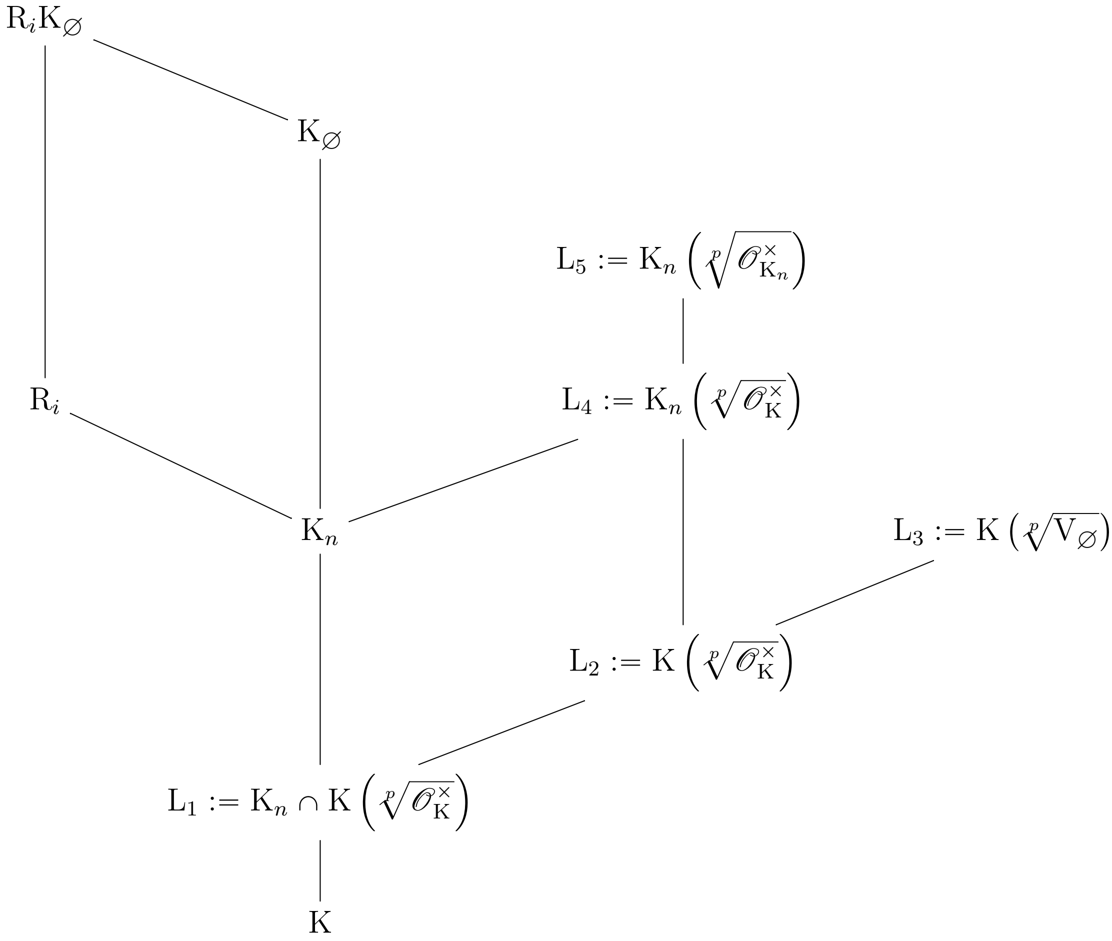

FIGURE 2.

We will find a set of primes of $S = \{\mathfrak{p}_1, \cdots \mathfrak{p}_{t-\lambda}\}$ in K such that:
— $\mathfrak{p}_i$ splits completely in K_n/K,
— Their Frobenius automorphisms span a $(t-\lambda)$-dimensional space in $\mathrm{Gal}(L_2/L_1) \simeq \mathrm{Gal}(L_4/K_n)$,
— For each i, let $\mathfrak{b}_{ij}$ be the primes above $\mathfrak{p}_i$ in K_n. There is a dependence relation on the Frobenius automorphisms of the $\mathfrak{b}_{ij}$ in $\mathrm{Gal}(L_5/K_n)$. By Gras-Munnier (Theorem 1.1) this implies the existence of a $\mathbb{Z}/p$-extension R_i/K_n ramified only at (these primes above) $\mathfrak{p}_i$. Let $\tilde{R}_i$ be the Galois closure over K of R_i. As the p-group $\mathrm{Gal}(K_n/K)$ must act on the $\mathbb{F}_p$-vector space $\mathrm{Gal}(\tilde{R}_i/K_n)$ with a fixed point, by iteration we may assume R_i/K is Galois. The $\mathbb{Z}/p$-extension $R_iK_\varnothing$ is ramified only at $\mathfrak{p}_i$ and gives an element of $Ш^2_\varnothing$. We have produced $t-\lambda$ elements of $Ш^2_\varnothing$ in addition to the d elements of $Ш^2_\varnothing$ we get by choosing primes $\{\mathfrak{q}_1, \cdots, \mathfrak{q}_d\}$ of K whose Frobenius automorphisms form a basis of $\mathrm{Gal}(L_3/L_2)$.

This gives the lower bound. We now construct S.
As L_2/K is abelian ($\zeta_p \in K$), $H_n = \mathrm{Gal}(K_n/K)$ acts trivially on $\mathrm{Gal}(L_2/L_1)$ (and thus on $\mathrm{Gal}(L_4/K_n)$ as well).
After taking the Kummer dual of $\mathscr{E}_{K_n}$, one obtains $\mathrm{Gal}(L_5/K_n) \simeq \mathbb{F}_p[H_n]^\lambda \oplus M_n$, where $M_n = N_n^\vee$ is a H_n-torsion $\mathbb{F}_p[H_n]$-module. The natural surjection $\pi : \mathrm{Gal}(L_5/K_n) \twoheadrightarrow$

$\mathrm{Gal}(\mathrm{L}_4/\mathrm{K}_n)$ induces, upon taking H_n-coinvariants, the map

$$\mathrm{Gal}(\mathrm{L}_5/\mathrm{K}_n)_{\mathrm{H}_n} \simeq \mathbb{F}_p^{\lambda} \oplus (\mathrm{M}_n)_{\mathrm{H}_n} \overset{\pi}{\twoheadrightarrow} \mathrm{Gal}(\mathrm{L}_4/\mathrm{K}_n) \simeq \mathrm{Gal}(\mathrm{L}_2/\mathrm{L}_1) \simeq \mathbb{F}_p^t.$$

Thus

$$d(\pi((\mathrm{M}_n)_{\mathrm{H}_n})) \geqslant t - \lambda = d(\mathscr{O}_{\mathrm{K}}^{\times}) - \beta - \lambda.$$

Take (at least) $t - \lambda$ elements x_i in $\mathrm{Gal}(\mathrm{L}_5/\mathrm{K}_n)$, such that their image under the projection π forms a basis of $\pi((\mathrm{M}_n)_{\mathrm{H}_n}) \subset \mathrm{Gal}(\mathrm{L}_4/\mathrm{K}_n) \simeq \mathrm{Gal}(\mathrm{L}_2/\mathrm{L}_1) \simeq \mathbb{F}_p^t$. We choose $\mathfrak{p}_i$ to split completely in K_n/K and have Frobenius $\pi(x_i) \in \mathrm{Gal}(\mathrm{L}_2/\mathrm{L}_1)$, so clearly $\mathfrak{p}_i$ satisfies the first two points above. We have chosen $\mathfrak{p}_i$ so that the primes above it in K_n have Frobenius automorphisms generating a $\mathbb{F}_p[\mathrm{H}_n]$-torsion module in $\mathrm{Gal}(\mathrm{L}_5/\mathrm{K}_n)$. This settles the third point and the case $\delta = 1$.

Now suppose $\delta = 0$. Replace every field L_i above by $\mathrm{L_i}' := \mathrm{L}_i(\zeta_p)$. The key fact is this: by Proposition 2.8, one has $d(\mathrm{Gal}(\mathrm{L}_2'/\mathrm{L}_1')) = d(\mathscr{O}_{\mathrm{K}}^{\times})$ so $\mathrm{L}_2' \cap \mathrm{K}_n = \mathrm{K}$. This disjointness allows us to apply the Chebotarev density theorem as above. The rest of the proof is word for word the same from this point on.

The last result follows since $\mathrm{Def}(\mathrm{G}_{\varnothing}) \geqslant 0$. □

Remark 2.10. — Observe that

(*i*) the inequality $\mathrm{Def}(\mathrm{G}_{\varnothing}) \leqslant d(\mathscr{O}_{\mathrm{K}}^{\times}) - \lambda$ comes from universal norms of units and is Wingberg's result (Theorem 1.7);

(*ii*) the group $\mathrm{G}_{\varnothing}$ has at least λ *fewer* relations than the maximal possible number, $\dim \mathrm{V}_{\varnothing}/(\mathrm{K}^{\times})^p$.

Corollary 2.11. — *Suppose* $\mathrm{K}_{\varnothing}/\mathrm{K}$ *is finite. Then* $\lambda < d(\mathscr{O}_{\mathrm{K}}^{\times}) - d^2/4 + d$.

Proof. — By the Theorem of Golod-Shafarevich one has $\mathrm{Def}(\mathrm{G}_{\varnothing}) > d^2/4 - d$; then apply Theorem 2.9. □

2.4. Remarks when $\mathrm{G}_{\varnothing}$ is abelian. — • Consider first the case where $\mathrm{G}_{\varnothing}$ is cyclic. Clearly $d(\mathrm{G}) = r(\mathrm{G}) = 1$ so $\mathrm{Def}(\mathrm{G}_{\varnothing}) = 0$. By Theorem 2.3, we get

$$\lambda = t_{\mathrm{G}_{\varnothing}}(\mathscr{E}_{\mathrm{K}_{\varnothing}}) \geqslant d(\mathscr{O}_{\mathrm{K}}^{\times}) - \beta \geqslant d(\mathscr{O}_{\mathrm{K}}^{\times}) - 1,$$

due to the fact that $\beta \leqslant 1$. In particular, this situation forces $\mathrm{K}_{\varnothing}$ to have a Minkowski unit provided K is neither $\mathbb{Q}$ nor imaginary quadratic. We can recover this fact by using the well-known following result: as $\mathrm{G}_{\varnothing}$ is cyclic, every element of $\mathscr{O}_{\mathrm{K}}^{\times}$ is the norm of an element of $\mathscr{O}_{\mathrm{K}_{\varnothing}}^{\times}$. Note this last argument applies in the quadratic imaginary case as well.

As an example, take the imaginary quadratic number field $\mathrm{K} = \mathbb{Q}(\sqrt{-q \cdot \ell})$, with $-q \equiv \ell \equiv 1 (\mathrm{mod}\ 4)$. Here, $p = 2$, $\mathrm{G}_{\varnothing}$ is cyclic, and $\mathscr{O}_{\mathrm{K}}^{\times} \cap \mathscr{O}_{\mathrm{K}_{\varnothing}}^{\times 2} = \mathscr{O}_{\mathrm{K}}^{\times 2}$. We find $\lambda = 1$, and finally that $\mathscr{E}_{\mathrm{K}_{\varnothing}} \simeq \mathbb{F}_2[\mathrm{G}_{\varnothing}]$.

Observe that if $\mathrm{G}_{\varnothing} \simeq \mathbb{Z}/2\mathbb{Z}$, then the fundamental unit of the biquadratic extension $\mathrm{K}(\sqrt{\ell})$ is exactly the fundamental unit of the quadratic field $\mathbb{Q}(\sqrt{\ell})$ and then is of norm -1. We again have $\mathscr{E}_{\mathrm{K}_{\varnothing}} \simeq \mathbb{F}_2[\mathrm{G}_{\varnothing}]$.

• Take $p = 2$, and K such that $\mathrm{G}_{\varnothing} \simeq (\mathbb{Z}/2\mathbb{Z})^2$. Here $d(\mathrm{G}) = 2$ and $r(\mathrm{G}) = 3$ so $\mathrm{Def}(\mathrm{G}_{\varnothing}) = 1$, implying the existence of a difficult relation. By Theorem 2.3, we get

$$\lambda = t_{\mathrm{G}_{\varnothing}}(\mathscr{E}_{\mathrm{K}_{\varnothing}}) \geqslant d(\mathscr{O}_{\mathrm{K}}^{\times}) - 2,$$

due to the fact that $\beta \leqslant 2$.

Let us be more precise: Kisilevsky in [**14**] showed that if $\mathrm{G}_\varnothing \simeq (\mathbb{Z}/2\mathbb{Z})^2$, then for every quadratic subextension F_i/K in $\mathrm{K}_\varnothing/\mathrm{K}$, one has $\big(\mathscr{O}_\mathrm{K}^\times : N_{\mathrm{F}_i/\mathrm{K}}\mathscr{O}_{\mathrm{F}_i}^\times\big) = 2$. We prove

Proposition 2.12. — *Let* $\mathrm{K}/\mathbb{Q}$ *be a quadratic extension such that* $\mathrm{G}_\varnothing \simeq (\mathbb{Z}/2\mathbb{Z})^2$*. Then the difficult relation is detected at one of the three quadratic subextensions* F/K *in* $\mathrm{K}_\varnothing/\mathrm{K}$*.*

Proof. — Suppose first that $\mathrm{K}/\mathbb{Q}$ is an imaginary quadratic extension. By Kisilevsky's result -1 is not a norm of any unit in each of the three subextensions F_i/K of $\mathrm{K}_\varnothing/\mathrm{K}$. Let us choose $\mathrm{F} := \mathrm{F}_i$ such that $\mathrm{F} \neq \mathrm{K}(\sqrt{-1})$; put $\mathrm{G} = \mathrm{Gal}(\mathrm{F}/\mathrm{K})$. By using $N_\mathrm{G}(\mathscr{O}_\mathrm{F}^\times) \subset \{\pm 1\}$, it is then easy to see that, modulo $\mathscr{O}_\mathrm{F}^{\times 2}$, -1 is not a norm of any unit in F/K implying that the norm map $N_\mathrm{G} : \mathscr{E}_\mathrm{F} \to \frac{\mathscr{O}_\mathrm{K}^\times}{\mathscr{O}_\mathrm{K}^\times \cap \mathscr{O}_\mathrm{F}^{\times 2}}$ is not onto.

Recall that $\frac{\mathscr{O}_\mathrm{K}^\times}{\mathscr{O}_\mathrm{K}^\times \cap \mathscr{O}_\mathrm{F}^{\times 2}} \hookrightarrow \mathscr{E}_\mathrm{F}$. As $\dim_{\mathbb{F}_2} \mathscr{E}_\mathrm{F} = 2$, the only possibilities for the $\mathbb{F}_2[\mathrm{G}]$-module $\mathscr{E}_\mathrm{F}$ are $\mathbb{F}_2^2$ and $\mathbb{F}_2[\mathrm{G}]$. As the norm map is onto in the latter case we see $\mathscr{E}_\mathrm{F} \simeq \mathbb{F}_2^2$ and then $t_\mathrm{G}(\mathscr{E}_\mathrm{F}) = 0$ so $\lambda = 0$: the difficult relation is detected by the quadratic extension F/K.

We now settle the case where $\mathrm{K}/\mathbb{Q}$ is real quadratic extension. Denote by ε the positive fundamental unit of K. By Kisilevsky's result, one knows that for every quadratic subextension F_i/K, -1 or ε is not a norm of any unit in F_i/K. Take one such quadratic extension F/K, and put $\mathrm{G} = \mathrm{Gal}(\mathrm{F}/\mathrm{K})$.

Suppose that -1 is not a norm of from F to K of any unit but $-1 \in N_\mathrm{G}(\mathscr{O}_\mathrm{F}^\times)\mathscr{O}_\mathrm{F}^{\times 2}$. First, $N_\mathrm{G}(\mathscr{O}_\mathrm{F}^\times) \subset \{1, \pm\varepsilon\}$ modulo squares. The equations $-1 = z^2$ and $-1 = \varepsilon z^2$ have no solutions with $z \in \mathscr{O}_\mathrm{F}^\times$ for sign reasons. Hence the only possible solution is that $-1 = -\varepsilon z^2$, and then, necessarily $\mathrm{F} = \mathrm{K}(\sqrt{\varepsilon})$.

Suppose now that ε is not a norm of any unit in F/K. As before, if we test the condition $\varepsilon \in N_\mathrm{G}(\mathscr{O}_\mathrm{F}^\times)\mathscr{O}_\mathrm{F}^{\times 2}$, we see the equations $\varepsilon = -z^2$, and $\varepsilon = -\varepsilon^a z^2$ have no solution for sign reasons. Suppose that $\varepsilon = \varepsilon^a z^2$ for some odd integer a with $\varepsilon^a \in N_\mathrm{G}(\mathscr{O}_\mathrm{F}^\times)$. As $N_\mathrm{G}(\varepsilon) = \varepsilon^2$, it is easy to see this implies $\varepsilon \in N_\mathrm{G}(\mathscr{O}_\mathrm{F}^\times)$, which contradicting our assumption. Thus a is even. and we conclude that $\varepsilon \in \mathscr{O}_\mathrm{F}^{\times 2}$, *i.e.* $\mathrm{F} = \mathrm{K}(\sqrt{\varepsilon})$.

Hence, in any quadratic subextension F/K in $\mathrm{K}_\varnothing/\mathrm{K}$ such that $\mathrm{F} \neq \mathrm{K}(\sqrt{\varepsilon})$, one has that the map $N_\mathrm{G} : \mathscr{E}_\mathrm{F} \to \frac{\mathscr{O}_\mathrm{K}^\times}{\mathscr{O}_\mathrm{K}^\times \cap \mathscr{O}_\mathrm{F}^{\times 2}}$ is not onto, and the result follows as in the imaginary case. □

3. Applications

Throughout this section, we explore applications of the previous results, including:

- How λ and deficiency change as we move up the tower $\mathrm{K}_\varnothing/\mathrm{K}$;
- That $\mathrm{Def}(\mathrm{G}_\varnothing) = 0$ implies the same for open subgroups of $\mathrm{G}_\varnothing$ when $\delta = 1$;
- The rapid growth of λ as we move up a p-adic analytic quotient tower of $\mathrm{G}_\varnothing$. The Tame Fontaine-Mazur conjecture predicts that infinite p-adic analytic quotients of $G_\varnothing$ do not exist; thus, proving λ cannot grow rapidly would lend support to the Fontaine-Mazur conjecture;
- Some results in the direction of better understanding the cohomological dimension of $\mathrm{G}_\varnothing$;
- A computable test for maximality of $\mathrm{Def}(\mathrm{G}_\varnothing)$.
- We recall a well-known example of a quadratic imaginary field K where, for $p = 3$, we have $r(\mathrm{G}_{\mathrm{K},\varnothing}) = d(\mathrm{G}_{\mathrm{K},\varnothing}) = 3$ so $\mathrm{Def}(\mathrm{G}_{\mathrm{K},\varnothing}) = 0$ and $|\mathrm{G}_{\mathrm{K},\varnothing}| = \infty$. We give

examples of degree 8 extensions M/K whose 3-Hilbert class field tower is the base change of $G_{K,\varnothing}$, thus providing examples of fields M where $|G_{M,\varnothing}| = \infty$ and $\mathrm{Def}(G_{M,\varnothing}) = 0$. The infinite towers over M have 7 independent Minkowski units.

3.1. Conserving the deficiency along the tower. — Let F be a number field in the tower $K_\varnothing/K$ and recall that $F_\varnothing = K_\varnothing$. We denote by $\lambda_{F_\varnothing/F}$ the asymptotic Minkowski rank in $F_\varnothing/F$.

Proposition 3.1. — *One has* $\lambda_{F_\varnothing/F} \geqslant [F:K]\lambda_{K_\varnothing/K}$.

Proof. — Let $L \supset F \supset K$ in $K_\varnothing/K$ be a large enough number field so that $\lambda_{L/K} = \lambda_{K_\varnothing/K}$ and $\lambda_{L/F} = \lambda_{F_\varnothing/F}$. Set $G = \mathrm{Gal}(L/K)$ and $H = \mathrm{Gal}(L/F)$. Then $\mathscr{E}_L = \mathbb{F}_p[G]^{\lambda_{K_\varnothing/K}} \oplus N$, where N is G-torsion. The result follows by noting that $\mathbb{F}_p[G] \simeq_H \mathbb{F}_p[H]^{[F:K]}$ (see §1.3.1). □

Corollary 3.2. — *For every number field* F *in* $K_\varnothing/K$, *we have*

$$\mathrm{Def}(G_{F,\varnothing}) \leqslant d(\mathscr{O}_F^\times) - [F:K]\lambda_{K_\varnothing/K}.$$

Proof. — This follows immediately from Theorem 2.9 and Proposition 3.1. □

Remark 3.3. — When $\delta = 0$ the above Corollary is a consequence of strictly group-theoretic considerations. Namely, from equations (5.2) and (5.4) of [**15**] one deduces that for an open subgroup H of a pro-p group G, one has

$$\mathrm{Def}(H) + 1 \leqslant (G:H)\big(\mathrm{Def}(G) + 1\big).$$

3.2. When $\mathrm{Def}(G_\varnothing) = 0$**.** —

Corollary 3.4. — *Let* K *be a number field containing* ζ_p. *Suppose that* $\mathscr{O}_K^\times \cap (\mathscr{O}_{K_\varnothing}^\times)^p = (\mathscr{O}_K^\times)^p$, *and that* $\mathrm{Def}(G_\varnothing) = 0$. *Then, for every finite extension* F/K *in* $K_\varnothing/K$, *one has* $\mathrm{Def}(G_{F,\varnothing}) = 0$.

Proof. — Applying Theorem 2.9, we see $\lambda = d(\mathscr{O}_K^\times)$ and is maximal and hence constant in the tower $K_\varnothing/K$, relative to the base field K. By Proposition 3.1 we see

$$\lambda_{F_\varnothing/F} \geqslant [F:K]\lambda = [F:K]d(\mathscr{O}_K^\times) = d(\mathscr{O}_F^\times).$$

The result follows by Theorem 2.9. □

Corollary 3.5. — *Let* G *be a pro-*2 *group such that:*

(*i*) $\mathrm{Def}(G) = 0$,

(*ii*) *there exists a normal open subgroup* H *of* G *such that* $r(H) \neq d(H)$.

Then G *cannot be realized as the* 2*-tower of an imaginary quadratic field* K *of discriminant* $\mathrm{disc}_K \equiv 1 (\mathrm{mod}\ 4)$ *nor* $\mathrm{disc}_K \equiv 0 (\mathrm{mod}\ 8)$.

Proof. — The discriminant hypotheses imply $-1 \notin \mathscr{O}_{K_\varnothing}^{\times 2}$. The result follows from Corollary 3.4. □

The condition that the number of Minkowski units is maximal is very strong [(2)]:

2. We thank Ozaki for bringing this result to our attention.

Proposition 3.6. — *The finite p-groups* G *that have the property* $\mathrm{Def(H)} = 0$ *for every subgroup* H *of* G *are exactly the cyclic groups and generalized quaternion group* $Q_{2^n} = \langle x, y \mid x^{2^{n-1}} = 1, x^{2^{n-2}} = y^2, yxy^{-1} = x^{-1}\rangle$, $n \geqslant 3$.

Proof. — For G with this property, every abelian subgroup H of G is of deficiency 0, forcing H to be cyclic. Then, G is cyclic or the generalized quaternion group Q_{2^n} of order 2^n (see for example [**35**, Theorem 9.7.3]). For the converse, obviously cyclic groups G satisfy $\mathrm{Def(H)} = 0$ for every subgroup H of G. Concerning Q_{2^n}, recall that its subgroups are cyclic or isomorphic to $Q_{2^{n-1}}$, and that the Schur multiplier of the generalized quaternion groups Q_{2^k} are trivial (or in other words that $\mathrm{Def}(Q_{2^k}) = 0$). □

Remark 3.7. — Take $p = 2$, and let K be an imaginary quadratic field. Recall that $\mathrm{Def}(\mathrm{G}_\varnothing) \in \{0, 1\}$. We suspect that when $\mathrm{G}_\varnothing$ is infinite then $\mathrm{Def}(\mathrm{G}_\varnothing)$ is maximal. If this is not the case and the hypothesis of Corollary 3.4 holds ($\mathrm{disc_K} \equiv 1 (\mathrm{mod}\ 4)$ or $\mathrm{disc_K} \equiv 0 (\mathrm{mod}\ 8)$), then $r(\mathrm{H}) = d(\mathrm{H})$ for every open normal subgroup H of $\mathrm{G}_\varnothing$.

Remark 3.8. — Observe that Poincaré pro-p groups of dimension 3 satisfy condition of Corollary 3.4, see for example [**25**, Chapter III, §7].

We close this subsection with an explicit, albeit contrived, example with $p = 2$.

Example 3.9. — Let $\mathrm{K} = \mathbb{Q}(\sqrt{-3 \cdot 5 \cdot 53})$. An easy MAGMA computation gives that the class group of K is $(2, 2)$ and its 2-Hilbert class field tower has degree 8 over K. Straightforward computations show this group has at least three cyclic subgroups of order 4, hence it is the quaternion group of order 8. Here $\mathscr{O}_\mathrm{K}^\times = \{1, -1\}$, and as the discriminant of K is prime to 4, $i^2 = -1 \notin \mathscr{O}_{\mathrm{K}_\varnothing}^{\times 2}$ so $\mathscr{O}_\mathrm{K}^\times \cap \mathscr{O}_{\mathrm{K}_\varnothing}^{\times 2} = \{1\}$ and $\beta = 0$. Then Theorem 2.9 gives $\mathrm{Def}(\mathrm{G}_\varnothing) = 1 - \lambda$. But it is well-known the quaternion group has deficiency 0 so $\lambda = 1$. There is a Minkowski unit in this (short) tower. Indeed, if one computed a basis of the units of the degree 16 field that is the top of the tower and computed norms to K, the elements with norm -1 (which exist!) are Minkowski units.

3.3. In the context of the Fontaine-Mazur conjecture. — The conjecture of Fontaine-Mazur [**6**, Conjecture 5a] asserts that every analytic quotient of $\mathrm{G}_\varnothing$ must be finite. By class field theory, one knows that every infinite analytic quotient of $\mathrm{G}_\varnothing$ must be of analytic dimension at least 3 (see [**22**, Proposition 2.12]).
One knows that $\mathrm{G}_\varnothing$ is not p-analytic when the p-rank $d(\mathrm{Cl_K})$ of the class group $\mathrm{Cl_K}$ of K is large compared to $[\mathrm{K} : \mathbb{Q}]$. See A.3.11 of [**19**]. Alternatively, this is (literally!) an exercise on page 78 of [**36**].

Suppose $\mathrm{G} := \mathrm{G}_\varnothing$ is infinite and analytic. One knows that every infinite analytic pro-p group contains an open *uniform* subgroup. To simplify, assume G is uniform. Denote by (G_n) the p-central descending series of G (it is also the Frattini series), and let $\mathrm{K}_n = \mathrm{K}_\varnothing^{\mathrm{G}_n}$. Put $\mathrm{H}_n = \mathrm{Gal}(\mathrm{K}_n/\mathrm{K})$; recall that $\#\mathrm{H}_n = p^{dn}$, where $d = d(\mathrm{G}_\varnothing)$ is also the dimension of $\mathrm{G}_\varnothing$ as analytic group. For $n \geqslant 1$, denote by λ_n the Minkowski-rank of the units along $\mathrm{K}_\varnothing/\mathrm{K}_n$.
The hypothesis of Corollary 3.10 below is, assuming the Fontaine-Mazur Conjecture, never satisfied. We include the Corollary to indicate a possible strategy to prove $\mathrm{G}_\varnothing$ is not analytic, namely show the number of Minkowski units does not grow so rapidly in the tower.

Corollary 3.10. — *Let* $\mathrm{G}_\varnothing$ *be pro-p analytic of dimension d. Then for m large,*

$$(r_1+r_2)[\mathrm{K}_m:\mathrm{K}]-1+\delta-\frac{d(d-1)}{2}\leqslant\lambda_m\leqslant(r_1+r_2)[\mathrm{K}_m:\mathrm{K}]-1+\delta-\frac{d(d-3)}{2}.$$

Proof. — Theorem 2.9 here, Theorem 4.35 of [**5**], and the assumption that $\mathrm{G}_\varnothing$ is uniform imply $\mathrm{Def}(\mathrm{G}_m)$ is constant and equal to $\mathrm{Def}(\mathrm{G}_\varnothing)=\dfrac{d(d-3)}{2}$. As remarked in the introduction, $\beta_m\leqslant d(\mathrm{G}_m)=d(\mathrm{G})=d$. We immediately see $\lambda_m\sim(r_1+r_2)[\mathrm{K}_m:\mathrm{K}]$, proving the main terms in the estimates.

We now prove the more refined estimates. Let us choose $n\gg m\gg 0$ such that:

$$\mathscr{E}_{\mathrm{K}_n}=\mathbb{F}_p[\mathrm{H}_{n,m}]^{\lambda_m}\oplus\mathrm{N}_{n,m}=\mathbb{F}_p[\mathrm{H}_n]^{\lambda}\oplus\mathrm{N}_n$$

where $\lambda=\lambda_{\mathrm{K}_\varnothing/\mathrm{K}}$, $\lambda_m=\lambda_{\mathrm{K}_\varnothing/\mathrm{K}_m}$, $\mathrm{H}_{n,m}=\mathrm{Gal}(\mathrm{K}_n/\mathrm{K}_m)$, and $\mathrm{N}_{n,m}$ and N_n are torsion modules over $\mathbb{F}_p[\mathrm{H}_{n,m}]$ and $\mathbb{F}_p[\mathrm{H}_n]$ respectively.

Then by Proposition 3.1, we see $\lambda_m=[\mathrm{K}_m:\mathrm{K}]\lambda+\lambda_{m,n}^{new}$; the quantity $\lambda_{m,n}^{new}$ corresponds to the $\mathbb{F}_p[\mathrm{H}_{n,m}]$-free part in N_n. Hence, by Theorem 2.9, one has

$$\mathrm{Def}(\mathrm{G}_m)\geqslant d(\mathscr{O}_{\mathrm{K}_m}^\times)-\lambda_m-\beta_m\geqslant d(\mathscr{O}_{\mathrm{K}_m}^\times)-[\mathrm{K}_m:\mathrm{K}]\lambda-\lambda_{m,n}^{new}-d(\mathrm{G}_m).$$

After noting that $d(\mathscr{O}_{\mathrm{K}_m}^\times)=(r_1+r_2)[\mathrm{K}_m:\mathrm{K}]-1+\delta$, we get

$$\mathrm{Def}(\mathrm{G}_m)\geqslant(r_1+r_2-\lambda)[\mathrm{K}_m:\mathrm{K}]-1+\delta-d-\lambda_{m,n}^{new}\tag{8}$$

But $\mathrm{Def}(\mathrm{G}_m)=\mathrm{Def}(\mathrm{G}_\varnothing)=\dfrac{d(d-3)}{2}$. Hence (8) becomes

$$\lambda_{m,n}^{new}\geqslant(r_1+r_2-\lambda)[\mathrm{K}_m:\mathrm{K}]-1+\delta-\frac{d(d-1)}{2}.\tag{9}$$

and

$$\lambda_m\geqslant(r_1+r_2)[\mathrm{K}_m:\mathrm{K}]-1+\delta-\frac{d(d-1)}{2},\tag{10}$$

proving the first inequality. The upper bound follows as $\mathrm{Def}(\mathrm{G}_m)\leqslant d(\mathscr{O}_{\mathrm{K}_m}^\times)-\lambda_m$ so

$$\lambda_m\leqslant(r_1+r_2)[\mathrm{K}_m:\mathrm{K}]-1+\delta-\frac{d(d-3)}{2}.\tag{11}$$

□

3.4. On the cohomological dimension of $\mathrm{G}_\varnothing$.

— Since the works of Labute [**17**], Labute-Mináč [**18**] and Schmidt [**32**], etc. one knows that in certain cases the groups G_S, for S tame, are of cohomological dimension 2. In all the examples of these papers $S\neq\varnothing$. The question of the computation of cohomological dimension of $\mathrm{G}_\varnothing$ is still an open problem (one can find partial negative answers in [**21**]). To prove Theorem 3.12, we need the following lemma due to Schmidt [**30**, Proposition 1].

Lemma 3.11. — *(Schmidt) Let* G *be an infinite pro-p group such that for a fixed constant* $n\geqslant 0$ *and every open subgroup* H *of* G*, one has*

$$\begin{aligned}-\chi_3(\mathrm{H})+n &:= -1-\mathrm{Def}(\mathrm{H})+\dim H^3(\mathrm{H})+n\\ &\geqslant [\mathrm{G}:\mathrm{H}]\big(-1-\mathrm{Def}(\mathrm{G})+\dim H^3(\mathrm{G})\big)\\ &:= -[\mathrm{G}:\mathrm{H}]\chi_3(\mathrm{G}).\end{aligned}$$

Then $\mathrm{cd}(\mathrm{G})\leqslant 3$*.*

Theorem 3.12. — *Let* K *be a number field such that*

(i) K *contains a primitive pth root of unity;*

(ii) $\mathscr{O}_{\mathrm{K}}^{\times} \cap (\mathscr{O}_{\mathrm{K}_{\varnothing}}^{\times})^p = (\mathscr{O}_{\mathrm{K}}^{\times})^p$.

Then $\dim H^3(\mathrm{G}_{\varnothing}) > 0$. *Moreover:*

- *If* $\dim H^3(\mathrm{G}_{\varnothing}) = 1$, *then* $\mathrm{G}_{\varnothing}$ *is finite or of cohomological dimension* 3*;*
- *If* $\mathrm{Def}(\mathrm{G}_{\varnothing}) = 0$, *and if* $\mathrm{G}_{\varnothing}$ *is of cohomological dimension* 3, *then* $\mathrm{G}_{\varnothing}$ *is a Poincaré duality group.*

Proof. — As $\mathscr{O}_{\mathrm{K}}^{\times} \cap (\mathscr{O}_{\mathrm{K}_{\varnothing}}^{\times})^p = (\mathscr{O}_{\mathrm{K}}^{\times})^p$ and $\delta = 1$, one has, by Theorem 2.9,

$$\mathrm{Def}(\mathrm{G}_{\varnothing}) = d(\mathscr{O}_{\mathrm{K}}^{\times}) - \lambda_{\mathrm{K}_{\varnothing}/\mathrm{K}} = r_1 + r_2 - \lambda_{\mathrm{K}_{\varnothing}/\mathrm{K}}.$$

Let H be an open normal subgroup of $\mathrm{G}_{\varnothing}$ and set $\mathrm{F} = \mathrm{K}_{\varnothing}^{\mathrm{H}}$. Proposition 3.1 implies $\lambda_{\mathrm{F}_{\varnothing}/\mathrm{F}} \geqslant \lambda_{\mathrm{K}_{\varnothing}/\mathrm{K}}[\mathrm{G}_{\varnothing} : \mathrm{H}]$, so Theorem 2.9 implies $\mathrm{Def}(\mathrm{H}) \leqslant [\mathrm{G}_{\varnothing} : \mathrm{H}](r_1 + r_2 - \lambda_{\mathrm{K}_{\varnothing}/\mathrm{K}})$. Recalling that χ_2 is the Euler characteristic truncated at second cohomology,

$$\chi_2(\mathrm{H}) = 1 + \mathrm{Def}(\mathrm{H}) \leqslant 1 + [\mathrm{G}_{\varnothing} : \mathrm{H}](r_1 + r_2 - \lambda_{\mathrm{K}_{\varnothing}/\mathrm{K}}),$$

so $\chi_2(\mathrm{H})$ cannot be equal to $[\mathrm{G}_{\varnothing} : \mathrm{H}]\chi_2(\mathrm{G}_{\varnothing}) = [\mathrm{G}_{\varnothing} : \mathrm{H}](1 + r_1 + r_2 - \lambda_{\mathrm{K}_{\varnothing}/\mathrm{K}})$, a necessary condition, by Theorem 5.4 of [**15**], for $\mathrm{G}_{\varnothing}$ to be of cohomological dimension 2. Hence $\mathrm{G}_{\varnothing}$ is not of cohomological 2 so $\dim H^3(\mathrm{G}_{\varnothing}) > 0$.

Now suppose $\mathrm{G}_{\varnothing}$ is infinite and $\dim H^3(\mathrm{G}_{\varnothing}) = 1$. By Theorem 2.9 and Proposition 3.1, one has

$$\begin{aligned}\big[-1 - \mathrm{Def}(\mathrm{H}) + \dim H^3(\mathrm{H})\big] + 1 &= \lambda_{\mathrm{F}_{\varnothing}/\mathrm{F}} - d(\mathscr{O}_{\mathrm{F}}^{\times}) + \dim H^3(\mathrm{H}) \\ &\geqslant [\mathrm{G}_{\varnothing} : \mathrm{H}]\big(\lambda_{\mathrm{K}_{\varnothing}/\mathrm{K}} - (r_1 + r_2)\big) \\ &= [\mathrm{G}_{\varnothing} : \mathrm{H}]\big(-1 - \mathrm{Def}(\mathrm{G}_{\varnothing}) + \dim H^3(\mathrm{G}_{\varnothing})\big)\end{aligned}$$

where the last equality follows from Theorem 2.9 using that $\beta = 0$ and $\dim H^3(\mathrm{G}_{\varnothing}) = 1$. Now take $n = 1$ in Lemma 3.11 to conclude $\mathrm{cd}(\mathrm{G}_{\varnothing}) = 3$.

Finally, to check that our group is a Poincaré group, following [**25**, Chapter III, §7], we need only verify that $D_i(\mathbb{Z}/p) := \varinjlim_{\mathrm{U}} H^i(\mathrm{U})^\wedge = 0$ for $i = 0, 1, 2$, where the limit is taken over open subgroups U of $\mathrm{G}_{\varnothing}$ and the transition maps are dual to the corestriction. Recall that cohomological dimension is nonincreasing when one restricts to a closed subgroup and that cyclic groups have infinite cohomological dimension, so as $\mathrm{G}_{\varnothing}$ is assumed to be of finite cohomological dimension, it is infinite and thus $D_0(\mathbb{Z}/p) = 0$. Moreover that

$$D_1(\mathbb{Z}/p) = \varinjlim_{\mathrm{U}} \mathrm{U}^{ab}/p = 0$$

follows from the proof of the Principal Ideal Theorem: Namely, for a group G let G' be its (closed) commutator subgroup and let G'' be the (closed) commutator subgroup of G'. The key part of the proof of the Principal Ideal Theorem is that the transfer map

$$\mathrm{Ver} : \mathrm{G}/\mathrm{G}' \to \mathrm{G}'/\mathrm{G}''$$

is the zero map. As the transfer map is the dual of the corestriction map, $D_1(\mathbb{Z}/p) = 0$.

We now show $D_2(\mathbb{Z}/p) = 0$. Let $\mathrm{U} \subset \mathrm{G}_{\varnothing}$ be open. Taking the U -cohomology of the short exact sequence of trivial U-modules

$$0 \to \mathbb{Z}/p \to \mathbb{Q}/\mathbb{Z} \xrightarrow{p} \mathbb{Q}/\mathbb{Z} \to 0$$

gives

$$H^1(\mathrm{U}, \mathbb{Q}/\mathbb{Z}) \xrightarrow{p} H^1(\mathrm{U}, \mathbb{Q}/\mathbb{Z}) \to H^2(\mathrm{U}, \mathbb{Z}/p)$$

which yields $(\mathrm{U}^{ab})^\vee/p \hookrightarrow H^2(\mathrm{U}, \mathbb{Z}/p)$. As $\dim(\mathrm{U}^{ab})^\vee/p = \dim H^1(\mathrm{U})$ and $\mathrm{Def}(\mathrm{U}) = 0$, this injection is an isomorphism and $H^2(\mathrm{U}, \mathbb{Z}/p)^\wedge \simeq \mathrm{U}^{ab}/p \simeq H^1(\mathrm{U}, \mathbb{Z}/p)^\wedge$. Since the duals of the two corestriction maps are induced by the transfer, $D_1(\mathbb{Z}/p) = 0 \implies D_2(\mathbb{Z}/p) = 0$. □

Remark 3.13. — The first part of Theorem 3.12 extends the following observation that can be deduced from the relationship between Galois cohomology and étale cohomology. We use the the formalism of étale cohomology as in [**24**]. Suppose $\mathrm{Def}(\mathrm{G}_\varnothing)$ is maximal. Then the étale version of the Hochschild-Serre spectral sequence with [**31**, Theorem 3.4] shows that $H^i(\mathrm{G}_\varnothing) \simeq H^i_{\acute{e}t}(\mathrm{Spec}\ \mathscr{O}_\mathrm{K})$ for $i = 1, 2$. Moreover, if $\mathrm{G}_\varnothing$ has cohomological dimension 2, then $\mathrm{G}_\varnothing$ is infinite: by [**31**, Lemma 3.7]) and from the Hochschild-Serre spectral sequence we also get $\{0\} = H^3(\mathrm{G}_\varnothing) \simeq H^3_{\acute{e}t}(\mathrm{Spec}\ \mathscr{O}_\mathrm{K}) \simeq \mu_{\mathrm{K},p}$, where here $\mu_{\mathrm{K},p} = \langle \zeta_p \rangle \cap \mathrm{K}$ (by [**31**, Theorem 3.4]). Hence δ *must* be zero.

3.5. Detecting maximality. — The strategy of the Hochschild-Serre spectral sequence allows us to prove Theorem 3.14 below, a computationally feasible method of showing $Ш^2_\varnothing$ is maximal.

Theorem 3.14. — *Suppose there exist two linearly disjoint unramified (and nontrivial) $\mathbb{Z}/p$-extensions F_1/K and F_2/K such that $t_{\mathrm{G}_i}(\mathscr{E}_{\mathrm{F}_i}) = 0$, $i = 1, 2$, where $\mathrm{G}_i = \mathrm{Gal}(\mathrm{F}_i/\mathrm{K})$. Then $\mathrm{Def}(\mathrm{G}_\varnothing) = d(\mathscr{O}_\mathrm{K}^\times)$ is maximal. Only one such extension F_i/K is sufficient if $\mathrm{F}_i \not\subset \mathrm{K}'(\sqrt[p]{\mathscr{O}_\mathrm{K}^\times})$, which is the case when $\delta = 0$.*

Proof. — We use the notations of §2.2. First note that Lemma 2.6 and the fact that $t_{\mathrm{G}_i}(\mathscr{E}_{\mathrm{F}_i}) = 0$ implies $\lambda = 0$.

If $\delta = 0$, Proposition 2.8 implies $\beta = 0$ so $\mathrm{Def}(\mathrm{G}_\varnothing)$ is maximal by Theorem 2.9.

We now address the $\delta = 1$ case. First suppose $\mathrm{F}_1 \not\subset \mathrm{K}(\sqrt[p]{\mathscr{O}_\mathrm{K}^\times})$. Then one can choose $d(\mathscr{O}_\mathrm{K}^\times)$ primes $\mathfrak{p}$ of K that split completely in F_1 and whose Frobenius automorphisms form a basis of $\mathrm{Gal}(\mathrm{K}(\sqrt[p]{\mathscr{O}_\mathrm{K}^\times})/\mathrm{K})$. Since $t_{\mathrm{G}_1}(\mathscr{E}_{\mathrm{F}_1}) = 0$, by Theorem 1.1 we see that for each $\mathfrak{p} \in S_2$ there is a $\mathbb{Z}/p$-extension of F_1, and hence of $\mathrm{K}_\varnothing$, ramified only at (the primes above) $\mathfrak{p}$. Each of these elements gives rise to a relation of $\mathrm{G}_\varnothing$. As usual, one gets the rest of the relations "for free" by choosing primes that split completely in $\mathrm{K}(\sqrt[p]{\mathscr{O}_\mathrm{K}^\times})/\mathrm{K}$ but form a basis of $\mathrm{Gal}\left(\mathrm{K}(\sqrt[p]{\mathrm{V}_{\mathrm{K},\varnothing}})/\mathrm{K}(\sqrt[p]{\mathscr{O}_\mathrm{K}^\times})\right)$. For such primes $\mathfrak{p}$ there is always an abelian extension of K ramified only at $\mathfrak{p}$, also giving rise to a relation of $\mathrm{G}_\varnothing$.
We study the remaining case, namely when $\mathrm{F}_1, \mathrm{F}_2 \subset \mathrm{K}(\sqrt[p]{\mathscr{O}_\mathrm{K}^\times})$. Choose a prime $\mathfrak{q}_1$ of K such that its Frobenius generates $\mathrm{Gal}(\mathrm{F}_1/\mathrm{K})$ *and* $\mathfrak{q}_1$ splits in F_2. Choose $\mathfrak{q}_2$ similarly. Then, as before, when we allow ramification at $\mathfrak{q}_1$ we obtain a ramified extension over $\mathrm{F}_{2,\varnothing}$ and when we allow ramification at $\mathfrak{q}_2$ we obtain a ramified extension over $\mathrm{F}_{1,\varnothing}$. In this case we build S_2 by starting with $S_2 = \{\mathfrak{q}_1, \mathfrak{q}_2\}$ and augmenting it to include primes that split completely in $\mathrm{F}_1\mathrm{F}_2$ and whose Frobenius automorphisms, along with those of $\mathfrak{q}_1$ and $\mathfrak{q}_2$, form a basis of $\mathrm{Gal}(\mathrm{K}(\sqrt[p]{\mathscr{O}_\mathrm{K}^\times})/\mathrm{K})$. For each of these primes when we allow ramification at $\mathfrak{p}$ we obtain a ramified extension over $\mathrm{F}_{i,\varnothing}$ for $i = 1, 2$. Each of these primes gives rise to a relation of $\mathrm{G}_\varnothing$ and along with the "free relations" we get $\mathrm{Def}(\mathrm{G}_\varnothing) = d(\mathscr{O}_\mathrm{K}^\times)$. □

3.6. Infinite towers having Minkowski units. — In this section, as we compare towers of different fields, we include the field in the subscript of G. We produce examples of number fields K for which $G_{K,\varnothing}$ is infinite, $\beta = 0$, and $\mathrm{Def}(G_{K,\varnothing})$ is minimal. By Theorem 2.9 $\lambda > 0$ in these cases.We first need some set up.

3.6.1. Stability of towers. — Let us start with the following context. Let K/k be a Galois extension of order coprime to p. Observe that $K_\varnothing/k$ is Galois. Put $\Delta := \mathrm{Gal}(K/k)$ and $\Gamma = \mathrm{Gal}(K_\varnothing/k)$. By the Schur-Zassenhaus Theorem one has $\Gamma \simeq G_{K,\varnothing} \ltimes \Delta$.
Obviously $\mathrm{Gal}(Kk_\varnothing/K) \simeq G_{k,\varnothing}$ and there is a natural surjective map $G_{K,\varnothing} \twoheadrightarrow G_{k,\varnothing}$. In [**9**] Gras shows:

Theorem 3.15. — *Suppose* K/k *is Galois and of degree prime to p. Then* $G_{K,\varnothing} \simeq G_{k,\varnothing}$ *if and only if* $d(G_K) = d(G_k)$.

We give an alternative proof of this result inspired by Wingberg [**43**], [**41**].
First, let N be the closed normal subgroup of $G_{K,\varnothing}$ generated by the $g^s g^{-1}, g \in G_{K,\varnothing}, s \in \Delta$; put $G^+_{K,\varnothing} := G_{K,\varnothing}/N$. In other words, $G^+_{K,\varnothing}$ is the largest quotient of $G_{K,\varnothing}$ on which Δ acts trivially. Since Δ acts trivially on $G_{k,\varnothing}$, the morphism $\varphi : G_{K,\varnothing} \to G_{k,\varnothing}$ factors through $G^+_{K,\varnothing}$.

Lemma 3.16. — *One has* $H^1(G_{k,\varnothing}) \simeq H^1(G^+_{K,\varnothing})$.

Proof. — By base change from k to K, using that $(\#\Delta, p) = 1$, we have an injection $H^1(G_{k,\varnothing}) \hookrightarrow H^1(G^+_{K,\varnothing})$. As elements of the $H^1(G^+_{K,\varnothing})$ correspond to $\mathbb{Z}/p$-extensions of K on whose Galois group Δ acts trivially, these descend to k, so the injection is a surjection. □

Consider now $\Gamma(p)$ the maximal pro-p quotient of Γ.

Lemma 3.17. — *One has* $\Gamma(p) \simeq G_{k,\varnothing}$.

Proof. — Obviously, $\Gamma(p) \twoheadrightarrow G_{k,\varnothing}$. But it is easy to see that $\Gamma(p)$ corresponds to a pro-p extension of k unramified everywhere. By maximality, we deduce the result. □

We recall now the result of Wingberg (given in [**43**] when $\Delta \simeq \mathbb{Z}/2$, and in general in an unpublished work [**41**]).

***Proposition 3.18* (Wingberg)**. — *If* $d(G_{K,\varnothing}) = d(G_{k,\varnothing})$ *then the natural map* $G^+_{K,\varnothing} \twoheadrightarrow G_{k,\varnothing}$ *is an isomorphism and induces the injection* $H^2(G^+_{K,\varnothing}) \hookrightarrow H^2(G_{K,\varnothing})^\Delta$.

Proof. — The Hochschild-Serre spectral sequence for

$$1 \longrightarrow M \longrightarrow G^+_{K,\varnothing} \longrightarrow G_{k,\varnothing} \longrightarrow 1$$

gives the commutative diagram (by Lemmas 3.16 and 3.17):

$$\begin{tikzcd}
0 \arrow[r] & H^1(M)^{G_{k,\varnothing}} \arrow[r] & H^2(G_{k,\varnothing}) \arrow[r] \arrow[d, "\simeq"] & H^2(G^+_{K,\varnothing}) \arrow[dd, "Inf"] \\
& & H^2(\Gamma(p)) \arrow[d, hook, "Inf"] & \\
& & H^2(\Gamma) \arrow[r, "\simeq"] & H^2(G_{K,\varnothing})^\Delta
\end{tikzcd}$$

We then deduce that $H^1(\mathrm{M})^{\mathrm{G}_{\mathrm{k},\varnothing}} = 0$, or equivalently that $\mathrm{M} = \{e\}$, and $H^2(\mathrm{G}_{\mathrm{k},\varnothing}) \simeq H^2(\mathrm{G}^+_{\mathrm{K},\varnothing}) \hookrightarrow H^2(\mathrm{G}_{\mathrm{K},\varnothing})^\Delta$. $\square$

We can now give an alternative proof of Theorem 3.15.

Proof. — Take the Hochschild-Serre spectral sequence of

$$1 \longrightarrow \mathrm{N} \longrightarrow \mathrm{G}_{\mathrm{K},\varnothing} \longrightarrow \mathrm{G}^+_{\mathrm{K},\varnothing} \longrightarrow 1$$

to obtain

$$0 \to H^1(\mathrm{G}^+_{\mathrm{K},\varnothing}) \to H^1(\mathrm{G}_{\mathrm{K},\varnothing}) \to H^1(\mathrm{N})^{\mathrm{G}_{\mathrm{K},\varnothing}} \to H^2(\mathrm{G}^+_{\mathrm{K},\varnothing}) \to H^2(\mathrm{G}_{\mathrm{K},\varnothing}).$$

By Proposition 3.18, one gets:

$$0 \to H^1(\mathrm{G}^+_{\mathrm{K},\varnothing}) \to H^1(\mathrm{G}_{\mathrm{K},\varnothing}) \to H^1(\mathrm{N})^{\mathrm{G}_{\mathrm{K},\varnothing}} \to 0.$$

Recall that $\mathrm{N} = \{e\}$ if and only if $H^1(\mathrm{N})^{\mathrm{G}_{\mathrm{K},\varnothing}} = 0$. Hence $\mathrm{G}_{\mathrm{K},\varnothing} \simeq \mathrm{G}^+_{\mathrm{K},\varnothing}$ if and only if $d(\mathrm{G}^+_{\mathrm{K},\varnothing}) = d(\mathrm{G}_{\mathrm{K},\varnothing})$, if and only if $d(\mathrm{G}_{\mathrm{k},\varnothing}) = d(\mathrm{G}_{\mathrm{K},\varnothing})$. $\square$

3.6.2. Example. — Let $\mathrm{k} = \mathbb{Q}(\sqrt{-3321607})$ and $p = 3$. It is easy to compute that $d = r = 3$. Furthermore, the $\mathrm{Gal}(\mathrm{k}/\mathbb{Q})$ action on $\mathrm{G}_{\mathrm{k},\varnothing}$ gives that the depth of each relation is at least three so we may take $1 - 3t + 3t^3$ as a Golod-Shafarevich polynomial for G_{k}. As this polynomial has a root in $]0, 1[$ we see $|\mathrm{G}_{\mathrm{k},\varnothing}| = \infty$. This example is well-known (see [**34**]).
We will find explicit multi-quadratic fields $\mathrm{M}/\mathbb{Q}$ such that $d(\mathrm{G}_{\mathrm{Mk},\varnothing}) = d(\mathrm{G}_{\mathrm{k},\varnothing}) = 3$. Theorem 3.15 then gives $(\mathrm{Mk})_\varnothing = \mathrm{M}(\mathrm{k}_\varnothing)$. The largest M we give is degree 8 so Mk is a totally complex field of degree 16 with $r = d = 3$ and $\mathrm{Def}(\mathrm{G}_{\mathrm{Mk},\varnothing}) = 0$. In this case $\lambda = 7$, that is there are 7 independent Minkowski units all the way up the tower $(\mathrm{Mk})_\varnothing/\mathrm{Mk}$.

Lemma 3.19. — *For* $\mathrm{M}/\mathbb{Q}$ *multi-quadratic, to check that* $d(\mathrm{G}_{\mathrm{Mk},\varnothing}) = d(\mathrm{G}_{\mathrm{k},\varnothing}) = 3$*, it is equivalent to check that* $d(\mathrm{G}_{\mathrm{Nk},\varnothing}) = d(\mathrm{G}_{\mathrm{k},\varnothing}) = 3$ *for every quadratic extension* N/k *contained in* Mk*.*

Proof. — Suppose $d(\mathrm{G}_{\mathrm{Mk},\varnothing}) > 3$. The elementary 2-abelian group $\mathrm{Gal}(\mathrm{Mk}/\mathrm{k})$ acts on the $\mathbb{F}_3$-vector space $\mathrm{G}^{3-el,ab}_{\mathrm{Mk},\varnothing}$. Since 2 and 3 are relatively prime and both square roots of unity lie in $\mathbb{F}_3$, $\mathrm{G}^{3-el,ab}_{\mathrm{Mk},\varnothing}$ decomposes as a direct sum of one-dimensional $\mathbb{F}_3[\mathrm{Gal}(\mathrm{Mk}/\mathrm{k})]$ subspaces. The trivial summands descend to k. Since we are assuming $d(\mathrm{G}_{\mathrm{Mk},\varnothing}) > 3$, there is a non-trivial summand. The kernel of the action on this summand is $\mathrm{Gal}(\mathrm{Mk}/\mathrm{N})$ where $[\mathrm{N} : \mathrm{k}] = 2$. Thus any *extra* generators of $\mathrm{G}_{\mathrm{Mk},\varnothing}$ are realized over some N. $\square$

Proposition 3.20. — *For* $\mathrm{M} = \mathbb{Q}(\sqrt{3}, \sqrt{7}, \sqrt{337})$ *we have* $|\mathrm{G}_{\mathrm{Mk},\varnothing}| = \infty$*,* $d(\mathrm{G}_{\mathrm{Mk},\varnothing}) = d(\mathrm{G}_{\mathrm{k},\varnothing}) = 3$ *and* $\mathrm{Def}(\mathrm{G}_{\mathrm{Mk},\varnothing}) = 0$ *is minimal. Assuming the GRH, for* $\mathrm{M} = \mathbb{Q}(\sqrt{3}, \sqrt{7}, \sqrt{r})$ *with* $r = 383$ *or* $r = 461$ *we have* $|\mathrm{G}_{\mathrm{Mk},\varnothing}| = \infty$*,* $d(\mathrm{G}_{\mathrm{Mk},\varnothing}) = d(\mathrm{G}_{\mathrm{k},\varnothing}) = 3$ *and* $\mathrm{Def}(\mathrm{G}_{\mathrm{Mk},\varnothing}) = 0$ *is minimal.*

Proof. — As $|\mathrm{G}_{\mathrm{k},\varnothing}| = \infty$, we immediately have $|\mathrm{G}_{\mathrm{Mk},\varnothing}| = \infty$. We used GP-PARI and MAGMA to check $d(\mathrm{G}_{\mathrm{N},\varnothing}) = 3$ for the seven quadratic extensions N/k inside Mk/k. For the computations with $r = 337$, we did not assume the GRH and these took several days. For $r = 383$ and 461 we assumed the GRH and the computations took several minutes. Theorem 3.15 implies $(\mathrm{Mk})_\varnothing = M(\mathrm{k}_\varnothing)$ so $r\left(\mathrm{Gal}\left((\mathrm{Mk})_\varnothing/\mathrm{Mk}\right)\right) = r\left(\mathrm{Gal}\left(\mathrm{k}_\varnothing/\mathrm{k}\right)\right) = 3$ which in turn gives $\mathrm{Def}(\mathrm{G}_{\mathrm{Mk},\varnothing}) = 7$. $\square$

Remark 3.21. — The fields M above were found by checking all primes q less than 500 such that $d(\mathrm{G}_{\mathrm{k}(\sqrt{q}),\varnothing}) = d(\mathrm{G}_{\mathrm{k},\varnothing}) = 3$. The first such prime was 3. We then searched this list for a second prime q_2 such that for every quadratic extension N/k inside $\mathrm{k}(\sqrt{3}, \sqrt{q_2})$ we had $d(\mathrm{G}_{\mathrm{N},\varnothing})) = 3$. We found the first $q_2 = 7$. Finally, we searched for q_3 such that for every quadratic extension N/k inside $\mathrm{k}(\sqrt{3}, \sqrt{7}, \sqrt{q_3})$ we had $d(\mathrm{G}_{\mathrm{N},\varnothing})) = 3$.
The natural question arises as to whether there are infinitely many fields M with M/k Galois of degree prime to 3 such that $d(\mathrm{G}_{\mathrm{Mk},\varnothing}) = 3$ so $\mathrm{G}_{\mathrm{Mk},\varnothing} = \mathrm{G}_{\mathrm{k},\varnothing}$. One may also ask: Does there exist a number field K such that $|\mathrm{G}_{\mathrm{K},\varnothing}| = \infty$ and $\mathrm{Def}(\mathrm{G}_{\mathrm{K},\varnothing})$ is not maximal, but for every $\mathrm{F} \subset \mathrm{K}$ we have either $|\mathrm{G}_{\mathrm{F},\varnothing}| < \infty$ or $\mathrm{Def}(\mathrm{G}_{\mathrm{F},\varnothing})$ is maximal?

Remark 3.22. — Take $p = 3$. The previous approach does not allow us to produce situations with Minkowski units and such that $\delta = 1$. Indeed, let $k = \mathbb{Q}(\sqrt{n})$ be a quadratic extension, $n \in \mathbb{Z}$, $n \notin \mathbb{Z}^2 \cup -3\mathbb{Z}^2$, such that $d = 3$. By the "Spiegelungssatz" phenomenon of Scholz [**33**], the 3-rank of the class group of $\mathbb{Q}(\sqrt{-3n})$ is at least 2, showing that $\mathrm{k}_\varnothing(\zeta_3) \neq (\mathrm{k}(\zeta_3))_\varnothing$.

4. On the depth of the relations

In this section we show the existence of Minkowski units deep in the Frattini tower imply that some of the relations of $\mathrm{G}_\varnothing$ are very deep. This makes it "more likely" that one can prove $\mathrm{G}_\varnothing$ is infinite using the Golod-Shafarevich series. We also prove a converse, namely the existence of very deep relations implies the existence of Minkowski units along the Frattini tower. One reason we study the Frattini tower as opposed to the Zassenhaus tower is that it is easier to use software for computations along the Frattini tower of $\mathrm{K}_\varnothing/\mathrm{K}$.

4.1. On the Zassenhaus filtration. —

4.1.1. Basic properties. — We refer to Lazard [**19**, Appendice A3]. Given a finitely presented pro-p group G, let us take a minimal presentation of G

$$1 \longrightarrow \mathrm{R} \longrightarrow \mathrm{F} \xrightarrow{\varphi} \mathrm{G} \longrightarrow 1,$$

where F is a free pro-p group on d generators; here $d = d(\mathrm{G})$. Let $\mathrm{I} = \ker(\mathbb{F}_p[\![\mathrm{F}]\!] \to \mathbb{F}_p)$ be the augmentation ideal of $\mathbb{F}_p[\![\mathrm{F}]\!]$, and for $n \geqslant 1$ consider $\mathrm{F}^n = \{x \in \mathrm{F}, x-1 \in \mathrm{I}^n\}$. The sequence (F^n) of open subgroups of F is the Zassenhaus filtration of F.
The depth ω of $x \in \mathrm{F}$ is defined as being $\omega(x) = \max\{n,\ x-1 \in \mathrm{I}^n\}$, with the convention that $\omega(1) = \infty$; the function ω is a valuation following terminology of Lazard. Hence $\mathrm{F}^n = \{g \in \mathrm{F}, \omega(g) \geqslant n\}$. This allows us to define a depth ω_G on G as follows: $\omega_\mathrm{G}(x) = \max\{\omega(g), g \in \mathrm{F}, \varphi(g) = x\}$. Put $\mathrm{G}^n = \{x \in \mathrm{G}, \omega_\mathrm{G}(x) \geqslant n\}$. Observe that $\mathrm{G}^n = \mathrm{F}^n\mathrm{R}/\mathrm{R} \simeq \mathrm{F}^n/(\mathrm{F}^n \cap \mathrm{R})$; the sequence (G^n) is the Zassenhaus series of G, it corresponds to the filtration arising from the augmentation ideal I_G of $\mathbb{F}[\![\mathrm{G}]\!]$, see [**19**, Appendice A3, Theorem 3.5]. One has the following property. If $\pi : \mathrm{G}' \twoheadrightarrow \mathrm{G}$ is surjective, then ω_G is the restriction of $\omega_{\mathrm{G}'}$; in other word, $\omega_\mathrm{G}(x) = \max\{\omega_{\mathrm{G}'}(y), y \in \mathrm{G}',\ \pi(y) = x\}$.
Denote by (G_n) the Frattini filtration of G. Recall the well-known relationship between these two filtrations of G:

Lemma 4.1. — *One has* $\mathrm{G}_n \subset \mathrm{G}^{2^{n-1}}$.

We say a few words about the reverse inclusions. Let H be an open normal subgroup of G. Since the groups (G^n) form a basis of neighborhoods of 1, let $a(\mathrm{H})$ be the smallest integer such that $\mathrm{G}^{a(\mathrm{H})} \subset \mathrm{H}$. We want to give some estimates on $a(\mathrm{H})$ in some special cases.

Definition 4.2. — For a pro-p group Γ, denote by $\mathrm{I}_\Gamma := \ker(\mathbb{F}_p[\![\Gamma]\!] \to \mathbb{F}_p)$, the augmentation ideal of $\mathbb{F}_p[\![\Gamma]\!]$; and denote by $k(\Gamma)$ the smallest integer such that $\mathrm{I}_\Gamma^{k(\Gamma)} = \{0\}$, where we allow $k(\Gamma) = \infty$.

Proposition 4.3. — *(*[**15**, Chapter 7, §7.6, Theorem 7.6]*) Let* $1 \to \mathrm{H} \to \mathrm{G} \to \mathrm{G}/\mathrm{H} \to \mathbf{1}$ *be an exact sequence of pro-p groups. Then* $\mathrm{I}_\mathrm{H} = \ker(\mathbb{F}_p[\![\mathrm{G}]\!] \to \mathbb{F}_p[\![\mathrm{G}/\mathrm{H}]\!])$.

Following Koch's book [**15**, Chapter 7, §7.4], we give some estimates for $a(\mathrm{H})$.

Proposition 4.4. — *One has:*

(i) $a(\mathrm{H}) \leqslant k(\mathrm{G}/\mathrm{H}) \leqslant |\mathrm{G}/\mathrm{H}|$.

(ii) If $\Gamma' \lhd \Gamma$ *are two finite p-groups, then* $k(\Gamma) \leqslant k(\Gamma/\Gamma')k(\Gamma')$.

(iii) $k(\mathrm{G}/\mathrm{G}_2) = p$.

Proof. — *(i)* Take k such that $\mathrm{I}_{\mathrm{G}/\mathrm{H}}^k = \{0\}$. Then by Proposition 4.3 one has $\mathrm{I}_\mathrm{G}^k \subset \mathrm{I}_\mathrm{H}$, which implies $\mathrm{G}^k \subset \mathrm{H}$, and then $a(\mathrm{H}) \leqslant k$. In particular, $a(\mathrm{H}) \leqslant k(\mathrm{G}/\mathrm{H})$. For the second part of the inequality, observe that: for every finite p-group Γ, one has $\mathrm{I}_\Gamma^{|\Gamma|} = \{0\}$ (see the proof of Lemma 7.4 of [**15**, Chapter 7, §7.4]), showing that $k(\Gamma) \leqslant |\Gamma|$.
(ii) By Proposition 4.3, one has $\mathrm{I}_\Gamma^{k(\Gamma/\Gamma')} \subset \mathrm{I}_{\Gamma'}$, and then $\mathrm{I}_\Gamma^{k(\Gamma/\Gamma')k(\Gamma')} \subset \mathrm{I}_{\Gamma'}^{k(\Gamma')} = \{0\}$.
(iii) This follows as G/G_2 is p-elementary abelian. □

For every integer $n \geqslant 1$, put $a_n := a(\mathrm{G}_{n+1})$. Observe that $a_1 = 1$.

Proposition 4.5. — *For* $n \geqslant 2$, *one has* $a_n \leqslant p^n$. *Therefore* $\mathrm{G}_n \subset \mathrm{G}^{2^{n-1}} \subset \mathrm{G}_{(n-1)\log(2)/\log(p)}$.

Proof. — That $a_n \leqslant p^n$ follows from Proposition 4.4 and the fact that $\mathrm{G}_n/\mathrm{G}_{n+1}$ is elementary p-abelian. The second part follows from the first. □

4.1.2. The Golod-Shafarevich polynomial. — Consider a minimal presentation of a finitely generated pro-p group G:

$$1 \longrightarrow \mathrm{R} \longrightarrow \mathrm{F} \xrightarrow{\varphi} \mathrm{G} \longrightarrow 1.$$

Suppose that $\mathrm{R}/\mathrm{R}^p[\mathrm{R},\mathrm{R}]$ is generated as an $\mathbb{F}_p[\![\mathrm{F}]\!]$-module by the family $\mathscr{F} = (\rho_i)$ of elements $\rho_i \in \mathrm{F}$. For $k \geqslant 2$, put $r_k = |\{\rho_i, \omega(\rho_i) = k\}|$; here we assume the r_i's finite.

Definition 4.6. — The series $P(t) = 1 - dt + \sum_{k\geqslant 2} r_k t^k$ is a Golod-Shafarevich series associated to the presentation $\mathscr{F}$ of G.

The theorem of Golod-Shafarevich asserts the following: if for some $t_0 \in (0,1)$ one has $P(t_0) = 0$, then G is infinite (see [**39**] or [**1**]). Observe that when no information on the depth of the ρ_i is available, then one may take $1 - dt + rt^2$ as Golod-Shafarevich series for G, where $r = d(H^2(\mathrm{G}))$.

Remark 4.7. — When $\mathrm{G} = \mathrm{G}_\varnothing$, the p-rank of G_n corresponds to the p-rank of the class group of K_n, where $\mathrm{K}_n = \mathrm{K}_\varnothing^{\mathrm{G}_n}$. Hence by Class Field Theory and with the help of a software package, in a certain sense it is easier to test if an element of G is in G_n than if it is in G^n.

4.2. Minkowski units and the Golod-Shafarevich polynomial of $\mathrm{G}_\varnothing$. —

4.2.1. The principle. — Let S be a finite saturated set of tame places of K as in Lemma 1.5, *i.e.* such that $H^1(\mathrm{G}_\varnothing) \simeq H^1(\mathrm{G}_S)$ and $|S| = d(\mathrm{V}_{\mathrm{K},\varnothing})$. Put $d = d(\mathrm{G}_\varnothing)$. Let F be the free pro-$p$ group on d generators $x_1, \cdots, x_d$. Consider now the minimal presentations of $\mathrm{G}_\varnothing$ and G_S induced by F, and the following diagram

$$\begin{tikzcd} 1 \arrow[r] & \mathrm{R}_S \arrow[r, "i'"] \arrow[d] & \mathrm{F} \arrow[r, "\varphi_S"] \arrow[d, "="] & \mathrm{G}_S \arrow[r] \arrow[d, two heads] & 1 \\ 1 \arrow[r] & \mathrm{R}_\varnothing \arrow[r, "i"] & \mathrm{F} \arrow[r, "\varphi"] & \mathrm{G}_\varnothing \arrow[r] & 1 \end{tikzcd}$$

Put $\mathrm{H}_S = \ker(\mathrm{G}_S \to \mathrm{G}_\varnothing)$; the pro-$p$ group H_S is the normal subgroup of G_S generated by the tame inertia groups $\langle \tau_\mathfrak{p} \rangle_{\mathfrak{p}\in S}$. Hence, this diagram induces the following exact sequence

$$1 \to \mathrm{R}_S \to \mathrm{R}_\varnothing \xrightarrow{\psi'} \mathrm{H}_S \to 1,$$

where $\psi' = \varphi_S \circ i$. The Hochschild-Serre spectral sequences induce the following isomorphisms

$$\begin{tikzcd} & H^2(\mathrm{G}_\varnothing)^\wedge \arrow[dl, "\simeq"'] \arrow[dr, "\simeq"] & \\ \mathrm{R}_\varnothing/\mathrm{R}_\varnothing^p[\mathrm{R}_\varnothing, \mathrm{F}] \arrow[rr, "\psi", "\simeq"'] & & \mathrm{H}_S/\mathrm{H}_S^p[\mathrm{G}_\varnothing, \mathrm{H}_S] \end{tikzcd}$$

where ψ is induced by ψ'. Using ψ we will study the depth of the relations of G: indeed, $\mathrm{R}_\varnothing/\mathrm{R}_\varnothing^p[\mathrm{R}_\varnothing, \mathrm{F}]$ and $\mathrm{H}_S/\mathrm{H}_S^p[\mathrm{G}_\varnothing, \mathrm{H}_S]$ inherit the Zassenhaus valuation from $\mathrm{R}_\varnothing$ and H_S, and thus the Zassenhaus valuation of F. Therefore an element of depth k in $\mathrm{R}_\varnothing/\mathrm{R}_\varnothing^p[\mathrm{R}_\varnothing, \mathrm{F}]$ corresponds to an element of depth k in $\mathrm{H}_S/\mathrm{H}_S^p[\mathrm{G}_\varnothing, \mathrm{H}_S]$.

4.2.2. Minkowski elements. — Here we extend the notion of Minkowski unit to the notion of Minkowski element. Set $\mathscr{V}_\mathrm{K} = \mathrm{V}_{\mathrm{K},\varnothing}/(\mathrm{K}^\times)^p$.

Definition 4.8. — Let L/K be a Galois extension with Galois group G. We denote by $\lambda'_{\mathrm{L/K}} := t_\mathrm{G}(\mathscr{V}_\mathrm{L})$ the $\mathbb{F}_p[\mathrm{G}]$-rank of $\mathscr{V}_\mathrm{L}$. One says that L/K has a Minkowski element if $\lambda'_{\mathrm{L/K}} \geqslant 1$.

Lemma 4.9. — *One has $\lambda'_{\mathrm{L/K}} \geqslant \lambda_{\mathrm{L/K}}$, so the existence of a Minkowski unit implies that of a Minkowski element.*

Proof. — This follows immediately from the exact sequence

$$1 \longrightarrow \mathscr{E}_\mathrm{L} \longrightarrow \mathscr{V}_\mathrm{L} \longrightarrow \mathrm{Cl}_\mathrm{L}[p] \longrightarrow 1. \tag{12}$$

□

When L/K is a subextension of $\mathrm{K}_\varnothing$/K one may give an upper bound for $\lambda'_{\mathrm{L/K}}$:

Proposition 4.10. — *Let* L/K *be a nontrivial finite Galois extension in* $\mathrm{K}_\varnothing$/K*. Then $\lambda'_{\mathrm{L/K}} \leqslant d - 1 + r_1 + r_2$. Moreover, if* $\mathrm{K}_\varnothing$/K *is infinite then there exist infinitely many Galois extensions* L/K *in* $\mathrm{K}_\varnothing$/K *such that $\lambda'_{\mathrm{L/K}} < d - 1 + r_1 + r_2$.*

Proof. — Set $\mathrm{H} = \mathrm{Gal}(\mathrm{K}_\varnothing/\mathrm{L})$. By Schreier's inequality (see [**28**], Corollary 3.6.3), $d(\mathrm{Cl_L}) = d(\mathrm{H}) \leqslant |\mathrm{G/H}|(d-1)+1$. Hence by (12), we get

$$d(\mathscr{V}_\mathrm{L}) \leqslant |\mathrm{G/H}|(d-1+r_1+r_2)+\delta,$$

showing that $\lambda'_{\mathrm{L/K}} \leqslant d-1+r_1+r_2$.
Suppose now that $\mathrm{G}_\varnothing$ is infinite and, except for finitely many Galois extensions L/K in $\mathrm{K}_\varnothing/\mathrm{K}$, one has $\lambda'_{\mathrm{L/K}} = d-1+r_1+r_2$. Then $d(\mathscr{V}_\mathrm{L}) \geqslant |\mathrm{G/H}|(d-1+r_1+r_2)$ and

$$d(\mathrm{Cl_L}) \geqslant 1-\delta+|\mathrm{G/H}|(d-1) \geqslant |\mathrm{G/H}|(d-1),$$

implying

$$-\chi_1(\mathrm{H})+1 \geqslant -|\mathrm{G/H}|\chi_1(\mathrm{G}_\varnothing).$$

By [**30**, Proposition 1], the Galois group $\mathrm{G}_\varnothing$ must be free pro-p, which is impossible. □

The converse below of Lemma 1.11 follows easily from the Cheobatarev density theorem:

Proposition 4.11. — *Let* L/K *be a finite* p*-extension with Galois group* G*.*

(*i*) *If* $t_\mathrm{G}(\mathscr{E}_{\mathrm{L},\varnothing}) \geqslant k$, *then there exist infinitely many sets* $S = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_k\}$ *of tame primes of* K *such that* $\#\mathrm{G}^{ab}_{\mathrm{L},S} = \#\mathrm{G}^{ab}_{\mathrm{L},\varnothing}$.

(*ii*) *If* $t_\mathrm{G}(\mathscr{V}_\mathrm{L}) \geqslant k$, *then there exist infinitely many sets* $S = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_k\}$ *of tame primes of* K *such that* $d(\mathrm{G}_{\mathrm{L},S}) = d(\mathrm{G}_{\mathrm{L},\varnothing})$.

From the computational view point, we will now consider the sequence of fields (K_n) in $\mathrm{K}_\varnothing/\mathrm{K}$ induced by the Frattini filtration (G_n): in other word, $\mathrm{K}_n = \mathrm{K}_\varnothing^{\mathrm{G}_n}$. Put $\mathrm{H}_n = \mathrm{Gal}(\mathrm{K}_n/\mathrm{K})$, and denote by $\lambda'_n := \lambda'_{\mathrm{K}_n}$ the $\mathbb{F}_p[\mathrm{H}_n]$-free rank of $\mathscr{V}_{\mathrm{K}_n}$.
Put $d := d(\mathrm{G}_\varnothing)$, and $r_{\max} := d + d(\mathscr{O}_\mathrm{K}^\times)$.

Theorem 4.12. — *Take* $n \geqslant 2$. *Then* $\mathrm{G}_\varnothing$ *can be generated by* $d(\mathrm{G}_\varnothing)$ *generators and* r_{max} *relations* $\{\rho_1, \cdots, \rho_{r_{max}}\}$ *such that at least* λ'_n *relations are of depth greater than* 2^n.

Proof. — We are assuming that the $\mathbb{F}_p[\mathrm{H}_n]$-module $\mathscr{V}_{\mathrm{K}_n}$ is isomorphic to $\mathbb{F}_p[\mathrm{H}_n]^{\lambda'_n} \oplus N$ where N is torsion. Using Chebotarev's theorem, choose a set $S' = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_{\lambda'_n}\}$ of primes of K such that

— Each $\mathfrak{p}_i$ splits completely from K to K_n,

— The Frobenius at a prime $\mathfrak{P}_{ij}$ of K_n above $\mathfrak{p}_i$ in $\mathrm{Gal}(\mathrm{K}'_n(\sqrt[p]{\mathscr{V}_{\mathrm{K}_n}})/\mathrm{K}'_n)$ lies in the ith copy of $\mathbb{F}_p[\mathrm{H}_n] \subset \mathscr{V}_{\mathrm{K}_n}$ and generates that copy of $\mathbb{F}_p[\mathrm{H}_n]$ under the action of H_n.

We claim $d(\mathrm{G}_{\mathrm{K}_n,S'}) = d(\mathrm{G}_{\mathrm{K}_n,\varnothing})$. Indeed, there are $|\mathrm{H}_n|$ primes $\mathfrak{P}_{ij}$ of K_n above $\mathfrak{p}_i$ and they have independent Frobenius automorphisms in $\mathrm{Gal}(\mathrm{K}'_n(\sqrt[p]{\mathscr{V}_{\mathrm{K}_n}})/\mathrm{K}'_n)$ by choice, even as we take the union over i from 1 to λ'_n. Gras-Munnier (Theorem 1.1) gives the equality. In fact, it gives more: $d(\mathrm{G}_{\mathrm{K}_m,S'}) = d(\mathrm{G}_{\mathrm{K}_m,\varnothing})$ for all $m < n$. If this were false for $m_0 < n$, there would exist a $\mathbb{Z}/p$-extension of $\mathrm{L}/\mathrm{K}_{m_0}$ ramified at primes (above those) of S'. Thus $\mathrm{LK}_n/\mathrm{K}_n$ would be a $\mathbb{Z}/p$-extension ramified only at primes (above those) of S' contradicting the result for n. We have shown that the p-Frattini towers of $\mathrm{G}_{S'}$ and $\mathrm{G}_\varnothing$ agree at the first n levels. Thus the generators $\tau_{\mathfrak{p}_i}$ of the tame inertia groups all have depth 2^n in $\mathrm{G}_{S'}$.
We have

$$0 \to \text{Ш}^2_{S'} \to H^2(\mathrm{G}_{S'}) \stackrel{res}{\to} \oplus_{\mathfrak{p}_i \in S'} H^2(\mathrm{G}_{\mathfrak{p}_i})$$

and $\dim Ш^2_{S'} \leqslant \dim Б_{S'} = r_{\max} - \lambda'_n$. We can say nothing about the depth of the relations coming from $Ш^2_{S'}$, so we assume they have minimal depth two. The local relations are of the form $[\sigma_{\mathfrak{p}_i}, \tau_{\mathfrak{p}_i}]\tau_{\mathfrak{p}_i}^{N(\mathfrak{p}_i)-1}$and are easily seen to have depth at least $2^n + 1$. As

$$G_{S'}/\langle \tau_{\mathfrak{p}_1}, \cdots, \tau_{\mathfrak{p}_{\lambda'_n}} \rangle \simeq \mathrm{G}_\varnothing$$

and taking this quotient trivializes the local relations, the theorem follows. □

Corollary 4.13. — *Assuming the hypothesis of Theorem 4.12, we may take* $1 - dt + (r_{max} - \lambda'_n)t^2 + \lambda'_n t^{2^n}$ *as a Golod-Shafarevich polynomial for* $\mathrm{G}_\varnothing$.

Example 4.14. — Let us return to the field $\mathrm{K} = \mathbb{Q}(\sqrt{5 \cdot 13 \cdot 17 \cdot 19})$ of § 1.3.3. Take $\mathrm{H} = \mathrm{K}_2$, $\mathrm{G} = \mathrm{Gal}(\mathrm{H}/\mathrm{K})$. As seen earlier, $t_{\mathrm{G}}(\mathscr{V}_H) \geqslant 1$. Indeed, the existence of a Minkoswki element follows from that of a Minkowski unit. Here a Golod-Shafarevich polynomial of $\mathrm{G}_\varnothing$ can be taken to be $1 - 3t + 4t^2 + t^4$ instead of the naive choice $1 - 3t + 5t^2$.

4.2.3. The converse. — Theorem 4.12 shows that the presence of Minkowski elements in the tower implies the existence of very deep relations in $\mathrm{G}_\varnothing$. Here we show the converse, that the existence of very deep relations implies the presence of Minkowski elements.
For $n \geqslant 1$, recall that F is a free pro-p group on d generators, F^m and F_m are the Zassenhaus and Frattini filtrations, and a_n is the smallest integer such that $\mathrm{F}^{a_n} \subset \mathrm{F}_{n+1}$. Recall from Lemma 4.1 that $\mathrm{F}_n \subset \mathrm{F}^{2^{n-1}}$. See Section 4.1.1. Put $\mathrm{H}_n = \mathrm{G}_\varnothing/\mathrm{G}_n$ and $\mathrm{K}_n = \mathrm{K}_\varnothing^{\mathrm{G}_n}$.

Theorem 4.15. — *Suppose that all the relations of* $\mathrm{G}_\varnothing$ *are of depth at least* a_n. *Then*
(*i*) *if* $\zeta_p \in \mathrm{K}$, $\lambda'_{\mathrm{K}_n/\mathrm{K}} \geqslant r_1 + r_2$;
(*ii*) *if* $\zeta_p \notin \mathrm{K}$, $\lambda'_{\mathrm{K}_n/\mathrm{K}} = r_1 + r_2 - 1 + d$.

Proof. — Since all the relations of $\mathrm{G}_\varnothing$ have depth a_n, we see that $\mathrm{G}_\varnothing/\mathrm{G}_\varnothing^{a_n} \simeq \mathrm{F}/\mathrm{F}^{a_n}$ has maximal Zassenhaus filtration for the first a_n steps. Thus for *any* set S satisfying $d(\mathrm{G}_S) = d(\mathrm{G}_\varnothing)$ we have

$$\mathrm{F}/\mathrm{F}^{a_n} \simeq \mathrm{G}_\varnothing/\mathrm{G}_\varnothing^{a_n} \simeq \mathrm{G}_S/\mathrm{G}_S^{a_n}$$

and since $\mathrm{F}^{a_n} \subset \mathrm{F}_{n+1}$, we also have

$$\mathrm{F}/\mathrm{F}_{n+1} \simeq \mathrm{G}_\varnothing/\mathrm{G}_{\varnothing,n+1} \simeq \mathrm{G}_S/\mathrm{G}_{S,n+1}$$

so all relations of $\mathrm{G}_\varnothing$ have depth at least $n+1$ in the Frattini filtration.

We first address the case $\zeta_p \in \mathrm{K}$. Consider the p-elementary abelian extensions $\mathrm{K}(\sqrt[p]{\mathrm{V}_{\mathrm{K},\varnothing}})/\mathrm{K}$ and K_2/K, the latter being the maximal unramified p-elementary abelian extension of K. By Kummer theory each is formed by adjoining to K the pth roots of elements $\alpha \in \mathrm{K}$. Since K_2/K is everywhere unramified, (α) is the pth power of an ideal, that is $\alpha \in \mathrm{V}_{\mathrm{K},\varnothing}$ so $\mathrm{K}(\sqrt[p]{\mathrm{V}_{\mathrm{K},\varnothing}}) \supset \mathrm{K}_2$ and $d(\mathrm{Gal}(\mathrm{K}(\sqrt[p]{\mathrm{V}_{\mathrm{K},\varnothing}})/\mathrm{K}_2)) = r_1 + r_2$. Note $\mathrm{K}_n \cap \mathrm{K}(\sqrt[p]{\mathrm{V}_{\mathrm{K},\varnothing}}) = \mathrm{K}_2$ as the intersection is both unramified over K and p-elementary abelian over K. Let $S := \{\mathfrak{p}_1, \cdots, \mathfrak{p}_{r_1+r_2}\}$ consist of primes that split completely from K to K_2 to K_n and whose Frobenius automorphisms form a basis of $\mathrm{Gal}(\mathrm{K}(\sqrt[p]{\mathrm{V}_{\mathrm{K},\varnothing}})/\mathrm{K}_2)$.

$$
\begin{tikzcd}
\mathrm{K}_n \arrow[d, dash] & \mathrm{K}(\sqrt[p]{\mathrm{V}_{\mathrm{K},\varnothing}}) \arrow[dl, dash] \\
\mathrm{K}_2 \arrow[d, dash] & \\
\mathrm{K} &
\end{tikzcd}
$$

By the above discussion

$$
\mathrm{F}/\mathrm{F}_{n+1} \simeq \mathrm{G}_{\varnothing}/\mathrm{G}_{\varnothing,n+1} \simeq \mathrm{G}_S/\mathrm{G}_{S,n+1}. \tag{13}
$$

This will imply $\lambda'_{\mathrm{K}_n/\mathrm{K}} \geqslant r_1 + r_2$. Indeed, above each $\mathfrak{p}_i$ there are $[\mathrm{K}_n : \mathrm{K}]$ primes $\mathfrak{P}_{ij}$ in K_n upon which $\mathrm{Gal}(\mathrm{K}_n/\mathrm{K})$ acts transitively. If for some i the Frobenius automorphisms of the $\mathfrak{P}_{ij}$ did not generate a distinct copy of $\mathbb{F}_p[\mathrm{G}_n]$ in $\mathrm{Gal}(\mathrm{K}_n(\sqrt[p]{\mathrm{V}_{\mathrm{K}_n,\varnothing}})/\mathrm{K}_n)$, then there would be a dependence relation among them and by Gras-Munnier we would have $d(\mathrm{G}_{\mathrm{K}_n,S}) > d(\mathrm{G}_{\mathrm{K}_n,\varnothing})$, contradicting (13). Thus $\lambda'_n \geqslant r_1 + r_2$ completing the proof in the $\delta = 1$ case.

We now consider the case $\zeta_p \notin \mathrm{K}$. As usual, the key fact is that $\mathrm{K}'_n \cap \mathrm{K}'(\sqrt[p]{\mathrm{V}_{\mathrm{K},\varnothing}}) = \mathrm{K}'$ (following the proof of Proposition 2.8) so $d(\mathrm{Gal}(\mathrm{K}'_n(\sqrt[p]{\mathrm{V}_{\mathrm{K},\varnothing}})/\mathrm{K}'_n)) = r_1 + r_2 - 1 + d$.

$$
\begin{tikzcd}
\mathrm{K}'_n \arrow[d, dash] & \mathrm{K}'(\sqrt[p]{\mathrm{V}_{\mathrm{K},\varnothing}}) \arrow[dl, dash] \\
\mathrm{K}' \arrow[d, dash] & \\
\mathrm{K} &
\end{tikzcd}
$$

We choose $S := \{\mathfrak{p}_1, \cdots, \mathfrak{p}_{r_1+r_2-1+d}\}$ to consist of primes of K that split completely from K to K' to K'_n and whose Frobenius automorphisms form a basis of $\mathrm{Gal}(\mathrm{K}(\sqrt[p]{\mathrm{V}_{\mathrm{K},\varnothing}})/\mathrm{K}')$. We complete the proof exactly as in the $\zeta_p \in \mathrm{K}$ case. □

Corollary 4.16. — *If all the relations of $\mathrm{G}_{\varnothing}$ are of depth at least p^2 then K_2 has a Minkowski element.*

Proof. — This follows immediately from Proposition 4.5 and Theorem 4.15. □

4.3. Theorem 2.9 revisited. — There is another way by which we can obtain Theorem 2.9 in the context of Golod-Shafarevich series $P(t)$. Indeed, such a series for a pro-p group G approximates the Hilbert series $H_{\mathrm{G}}(t)$ of the Zassenhaus filtration of G. In particular the Golod-Shafarevich Theorem is a consequence of this inequality: if there is some $t_0 \in]0,1[$ such that $P(t_0) < 0$ then necessarily $H_{\mathrm{G}}(t_0)$ diverges, implying the infiniteness of G.

Retain the notations of Section §2.3, and fix $n \gg 0$. Apply Corollary 4.13 to K_n/K by taking $1 - dt + (r_{\max} - \lambda)t^2 + \lambda t^{2^n}$ as a Golod-Shafarevich polynomial for $\mathrm{G}_{\varnothing}$. Now, as n can be arbitrarily large, we see that $1 - dt + (r_{\max} - \lambda)t^2$ is a Golod-Shafarevich polynomial for $\mathrm{G}_{\varnothing}$.

Of course, the question of determining λ when it is nonzero seems a hard problem, except in the case where at the beginning of the tower, we see $\lambda = 0$. Here is an explicit alternative.

Corollary 4.17. — *Let $n \in \mathbb{Z}_{>1}$. One has:*

(*i*) *if $t_{\mathrm{H}_n}(\mathscr{E}_{\mathrm{K}_n}) = 0$ and $\beta = 0$, then $\mathrm{Def}(\mathrm{G}_\varnothing) = r_1 + r_2 - 1 + \delta$;*

(*ii*) *if $t_{\mathrm{H}_n}(\mathscr{E}_{\mathrm{K}_n}) = \lambda_n > 0$, then one may take $1 - dt + (r_{max} - \lambda_n)t^2 + \lambda_n t^{2n}$ as a Golod-Shafarevich polynomial for $\mathrm{G}_\varnothing$.*

Remark 4.18. — The condition $\beta = 0$ can be relaxed as noted in Theorem 3.14.

5. The case of imaginary quadratic fields

In this section, we take $p = 2$ and let $\mathrm{K} := \mathbb{Q}(\sqrt{D})$ be an imaginary quadratic field of discriminant $D < -7$. Since the unit rank of K is 1, we have $\mathrm{Def}(\mathrm{G}_\varnothing) \in \{0, 1\}$. In this simplest of all non-trivial situations, we will discuss the deficiency of $\mathrm{G}_\varnothing$ and explore the extent to which we can detect relations using the machinery and notation set up in Section 2.2.

5.1. The frame. — Let $d = d(\mathrm{Cl}_\mathrm{K})$ be the 2-rank of the class group of $\mathrm{K} := \mathbb{Q}(\sqrt{D})$. By Gauss's genus theory, we know that D admits a unique (up to reordering) factorization into $d+1$ integers, each of which is a "prime fundamental discriminant" – meaning it is the discriminant of a quadratic field in which a single prime ramifies. For an odd prime q, we define $q^* := (-1)^{(q-1)/2}q$. The prime discriminants are then q^* as q ranges over all odd primes, as well as -4 and ± 8. We write $D = q_1^* \cdots q_{d+1}^*$, with the convention that if D is even, then $q_{d+1}^* \in \{-4, -8, 8\}$.
Put $q_0^* = -1$ and for each i in the range $0 \leqslant i \leqslant d$, put

$$\mathrm{K}_i := \mathrm{K}(\sqrt{q_0^*}, \cdots, \sqrt{q_{i-1}^*}, \sqrt{q_{i+1}^*}, \cdots, \sqrt{q_d'}),$$

where

$$q_d' = \begin{cases} q_d^* & \text{if } D \text{ is odd} \\ q_d^* & \text{if } q_{d+1}^* = \pm 8 \\ 2 & \text{if } q_{d+1}^* = -4. \end{cases}$$

Also define $\mathrm{L}' := \mathrm{K}(\sqrt{q_0^*}, \sqrt{q_1^*}, \cdots, \sqrt{q_{d-1}^*}, \sqrt{q_d'})$. A direct computation shows that the number field L' is the governing field $\mathrm{K}(\sqrt{\mathrm{V}_\varnothing})$ (see Section 2.2). Choose prime numbers $p_0, \cdots, p_d$ that split in K and such that for each i in the range $0 \leqslant i \leqslant d$, the Frobenius automorphisms of the $p_j, j \neq i$ in $\mathrm{L}'/\mathbb{Q}$ generate the Galois group of the quadratic extension L'/K_i. Fix a prime $\mathfrak{p}_i | p_i$ of K and put $S_2 = \{\mathfrak{p}_0\}$, $S_1 = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_d\}$, and $S = S_1 \cup S_2$. Observe that the primes $p_1, \cdots, p_d$ all are congruent to 1 mod 4 and that $p_0 \equiv 3$ mod 4.

As the 2-part of the class group of K has d generators, Lemma 2.5 shows the existence of d independent quadratic extensions F_i above $\mathrm{K}_\varnothing$, totally ramified at $\mathfrak{p}_i$, $i = 1, \cdots, d$, so $d(\mathrm{X}_S) \geqslant d$. This puts us in the situation where the difficult relations are detectable by the set S_2. Now, by studying the Galois module structure of units in imaginary biquadratic number fields, we can specify conditions under which $\mathrm{Def}(\mathrm{G}_\varnothing) = 1$; see Theorem 5.3 below.

Lemma 5.1. — *Let* $\mathrm{K}_0/\mathbb{Q}$ *be a real quadratic field;* $\mathrm{G}_0 = \mathrm{Gal}(\mathrm{K}_0/\mathbb{Q})$. *Then* $\mathscr{E}_{\mathrm{K}_0}$ *is* $\mathbb{F}_2[\mathrm{G}_0]$*-free if and only if, the norm of the fundamental unit* ε *is* -1. *More precisely, as an* $\mathbb{F}_2[\mathrm{G}_0]$*-module,* $\mathscr{E}_{\mathrm{K}} \simeq \left\{ \begin{array}{ll} \mathbb{F}_2 \oplus \mathbb{F}_2 & N(\varepsilon) = 1 \\ \mathbb{F}_2[\mathrm{G}_0] & N(\varepsilon) = -1 \end{array} \right.$.

Proof. — If the norm of ε is $+1$, then modulo $(\mathscr{O}_K^\times)^2$, we get $\varepsilon^\sigma \equiv \varepsilon$. If the norm of ε is -1, then $\mathscr{E}_{\mathrm{K}}$ is generated by $\varepsilon(\mathscr{O}_{\mathrm{K}}^\times)^2$ as G-module, and $\langle \varepsilon(\mathscr{O}_{\mathrm{K}}^\times)^2 \rangle$ is $\mathbb{F}_2[\mathrm{G}_0]$-free. $\square$

Recall this well-known result:

Lemma 5.2. — *Let* $\mathrm{F}/\mathbb{Q}$ *be an imaginary biquadratic field. Let* K_0 *be the real quadratic subfield, and let* ε *be the fundamental unit of* K_0. *Then,* $|\mathscr{O}_{\mathrm{F}}^\times/\langle \mu_{\mathrm{F}}, \varepsilon\rangle| = 1$ *or* 2. *In particular, if* F/K_0 *is ramified at some odd prime, then* $\mathscr{O}_{\mathrm{F}}^\times = \langle \mu_{\mathrm{F}}, \varepsilon \rangle$.

5.2. Main result. — We can now prove:

Theorem 5.3. — *Let* K *be an imaginary quadratic field of discriminant* D. *Assume that we can write* $D = D_1 D_2$*, where* $D_1 > 0$ *and* D_2 *are fundamental discriminants, such that:*

- (i) *the norm of the fundamental unit of* $\mathbb{Q}(\sqrt{D_1})$ *is* $+1$,
- (ii) *some odd prime number divides* D_2.

Then $\mathrm{Def}(\mathrm{G}_\varnothing) = 1$, *and the difficult relation is detected by the quadratic extension* $\mathrm{K}(\sqrt{D_1})/\mathrm{K}$.

Proof. — Put $\mathrm{F} := \mathrm{K}(\sqrt{D_1})$. As D_1 and D_2 are fundamental discriminants, then F/K is unramified. By assumption (ii) and Lemma 5.2, $\mathscr{O}_{\mathrm{F}}^\times = \langle \varepsilon, -1 \rangle$, where ε is the fundamental unit of $\mathbb{Q}(\sqrt{D_1})$. By assumption (i) and Lemma 5.1, $\mathscr{E}_{\mathrm{F}}$ is not $\mathbb{F}_2[\mathrm{G}]$-free, where $\mathrm{G} = \mathrm{Gal}(\mathrm{F}/\mathrm{K})$: in other words $t_{\mathrm{G}}(\mathscr{E}_{\mathrm{F}}) = 0$. The result follows by Theorem 3.14 (here $\sqrt{-1} \notin \mathrm{F}$). $\square$

Remark 5.4. — To elaborate further, observe that p_0 splits in F/K. Indeed, by the choice of p_0 we have, for $i = 1, \cdots, d-1$, $\left(\frac{q_i^*}{p_0}\right) = \left(\frac{q_d'}{p_0}\right) = 1$. Let us study two cases.

(a) Suppose first that $q_d' = q_d^*$. Then by recalling that $\left(\frac{D}{p_0}\right) = 1$, one also gets $\left(\frac{q_{d+1}^*}{p_0}\right) = 1$, and then $\left(\frac{D_1}{p_0}\right) = 1$ (in this case D_1 is the product of some of the q_i^*).

(b) Suppose now that $q_d' = 2$. Since $p_0 \equiv 3 \bmod 4$ and $D = q_1^* \cdots q_{d+1}^*$, we have $\left(\frac{q_d^*}{p_0}\right) = -1$. By assumption, there exists an odd prime p that divides D_2. We may choose $p = q_d$ (before fixing p_0). Then, D_1 is the product of various q_i^*, for $i = 1, \cdots, d-1$ so $\left(\frac{D_1}{p_0}\right) = 1$.

As p_0 splits completely in F/K, we see $\prod_{\mathfrak{P}|\mathfrak{p}_0} \mathscr{U}_{\mathfrak{P}}/\mathscr{U}_{\mathfrak{P}}^2$ is $\mathbb{F}_2[\mathrm{G}]$-free of rank 1. But as $t_{\mathrm{G}}(\mathscr{E}_{\mathrm{F}}) = 0$, the subgroup $I_{\mathfrak{p}_0}$ of $\mathrm{RCG}_{\mathrm{F}}(\mathfrak{p}_0)$ generated by the ramification at $\mathfrak{p}_0$ is not trivial. Put $I := I_{\mathfrak{p}_0}/I_{\mathfrak{p}_0}^2$. By Nakayama's lemma, the coinvariants I_{G} are also not trivial, hence there exists at least one quadratic extension $\mathrm{F}_1/\mathrm{F}_\varnothing$, Galois over K, totally ramified at some $\mathfrak{P}|\mathfrak{p}_0$, such that G acts trivially on $\mathrm{Gal}(\mathrm{F}_1/\mathrm{F}_\varnothing)$. The compositum $\mathrm{F}_1\mathrm{K}_\varnothing/\mathrm{K}_\varnothing$ is ramified at $\mathfrak{p}_0$ and produces a $(d+1)$st relation. This is the formalism of Example 1.6.

Corollary 5.5. — *Let* K *be an imaginary quadratic field of discriminant* D. *Suppose* D *is divisible by at least two odd primes* p_1, p_2 *such that* $p_1 \equiv p_2 \equiv 3$ *mod* 4. *Then* $\mathrm{Def}(\mathrm{G}_\varnothing) = 1$.

Proof. — If there is another odd prime q that divides D, take $D_1 = p_1p_2$.
If $\mathrm{K} = \mathbb{Q}(\sqrt{-p_1p_2})$ (resp. $\mathbb{Q}(\sqrt{-2p_1p_2})$), take $D_1 = 4p_1$ (resp. $D_1 = 8p_1$). □

***Example 5.6* (Martinet [23])**. — Take $\mathrm{K} = \mathbb{Q}(\sqrt{-21})$. Then, by Odlyzko bounds the 2-tower $\mathrm{K}_\varnothing/\mathrm{K}$ is finite, and it is not hard to see $\mathrm{G}_\varnothing \simeq (\mathbb{Z}/2\mathbb{Z})^2$, and $\mathrm{Def}(\mathrm{G}_\varnothing) = 1$.

***Example 5.7* (See Example 1.6)**. — Take $\mathrm{K} = \mathbb{Q}(\sqrt{-5460})$, $D_1 = 21$ and $D_2 = -260$. We then get an difficult relation coming from the extension $\mathrm{K}(\sqrt{21})/\mathrm{K}$, and $\mathrm{Def}(\mathrm{G}_\varnothing) = 1$.

Corollary 5.8. — *Suppose $k \geqslant 2$, and $p_1, \ldots, p_k$ are k distinct odd primes, exactly one of which, say p_1, is $\equiv 3 \bmod 4$. For the imaginary quadratic field $\mathrm{K} = \mathbb{Q}(\sqrt{-2p_1\cdots p_k})$ with discriminant $D = -8p_1\cdots p_k$, we have:* $\mathrm{Def}(\mathrm{G}_\varnothing) = 1$.

Proof. — Take $D_1 = 8p_1$. □

Example 5.9. — Take $\mathrm{K} = \mathbb{Q}(\sqrt{-p_1p_2})$, with primes p_1, p_2 such that $p_1 \equiv 1 \bmod 4$ and $p_2 \equiv 3 \bmod 4$. Here the hypotheses of Theorem 5.3 do not apply and $r = d = 1$ so $\mathrm{Def}(\mathrm{G}_\varnothing) = 0$.

Example 5.10. — The hypotheses of Theorem 5.3 do not apply for $\mathrm{K} = \mathbb{Q}(\sqrt{-130})$. As noted by Martinet [**23**], in that case, $\mathrm{G}_\varnothing$ is the quaternion group so $r = d = 2$.

Example 5.11. — Take $\mathrm{K} = \mathbb{Q}(\sqrt{-5\cdot 13\cdot 41})$. Here $r = d + 1 = 3$; indeed the norm of the fundamental unit of $\mathbb{Q}(\sqrt{5\cdot 41})$ is $+1$.

5.3. $\mathrm{Def}(\mathrm{G}_\varnothing)$ **is maximal almost all the time.** — We easily deduce from Theorem 5.3 that the presence of a Minkowski unit in a quadratic unramified extension F/K is rare, with the consequence that, generically, the deficiency of $\mathrm{G}_\varnothing$ is maximal. Let us say more precisely what we mean by the term "generically" here. Denote by $\mathscr{F}$ the set of imaginary quadratic fields. For $X \geqslant 2$, put

$$\mathscr{F}(X) = \{\mathrm{K} \in \mathscr{F},\ |\mathrm{disc}(\mathrm{K})| \leqslant X\},$$

and

$$\mathscr{F}_0(X) = \{\mathrm{K} \in \mathscr{F}(X),\ \mathrm{Def}(\mathrm{G}_\varnothing) = 0\}.$$

Theorem 5.12. — *There is an absolute constant $C > 0$ such that for all X large enough,*

$$\frac{\#\mathscr{F}_0(X)}{\#\mathscr{F}(X)} \leqslant C\frac{\log\log X}{\sqrt{\log X}}.$$

In particular, when ordered by absolute value of the discriminant, the proportion of imaginary quadratic fields for which $\mathrm{Def}(\mathrm{G}_\varnothing) = 0$*, tends to zero when* $X \to \infty$.

Proof. — We use the analytic number theory tools of [**21**, Theorem 4.6] due to Fouvry. Let K be an imaginary quadratic field. Put

$$B(X) = \{\mathrm{K} \in \mathscr{F}(X), \exists\ 2 \text{ distinct odd primes } p \equiv q \equiv 3 \bmod 4, pq \mid \mathrm{disc}(K)\}.$$

By Corollary 5.5, for every $\mathrm{K} \in B(X)$ one has $\mathrm{Def}(\mathrm{G}_\varnothing) = 1$. Hence $\mathscr{F}_0(X)$ is in the complement $C(X)$ of $B(X)$.
Denote by $A_i(X)$ the set of square-free integers $n \leqslant X$ having exactly i prime factors $\equiv 3 \bmod 4$, put $A(X) = A_0(X) \cup A_1(X)$. Clearly, $|C(X)| = O(|A(X)|)$.

In the proof of Theorem 4.6 of [**21**], it is shown that uniformly for X large enough, one has $|A_0(X)| = O\Big(X/\sqrt{\log X}\Big)$ and $|A_1(X)| = O\Big(X\dfrac{\log\log X}{\sqrt{\log X}}\Big)$. Thus $|C(X)| = O\Big(X\dfrac{\log\log X}{\sqrt{\log X}}\Big)$. We conclude by noting that $|\mathscr{F}(X)| = \dfrac{3}{\pi^2}X + O(\sqrt{\log X})$ (see for example [**7**, §4]). $\square$

The referee asked whether the bulk of the deficiency zero cases for $p = 2$ and imaginary quadratic fields arise with tower group the quaternion group Q_8 of order 8, suggesting a criterion from Table II of [**2**] as a possible method of proving this. Let $\mathscr{F}_{Q_8}(X)$ be the number quadratic imaginary fields having discriminant bounded in absolute value by X with 2-tower group Q_8. While it is not difficult to show, using the GRH versions of the effective Chebotarev Theorem, that

$$c\frac{(\log\log X)^2}{\log(X)} \leqslant \frac{\#\mathscr{F}_{Q_8}(X)}{\#\mathscr{F}(X)}$$

for some $c > 0$ and X large enough, showing that Q_8 towers are 100% of the deficiency zero cases for $p = 2$ seems difficult.

References

[1] I.V. Andožski, *On some classes of closed pro-p-groups*, Math. USSR **9** (1965), no 4, 663-691.

[2] E. Benjamin, F. Lemmermeyer, C. Snyder, *Imaginary quadratic fields k with cyclic $Cl_2(k^1)$*, J. of Number Theory, 67 (1997), no. 2, 229-245.

[3] N. Boston and J. Wang, *The 2-class tower of* $\mathbb{Q}(\sqrt{-5460})$, Geometry, algebra, number theory, and their information technology applications, 71–80, Springer Proc. Math. Stat., 251, Springer, Cham, 2018.

[4] C.W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, John Wiley and Sons, coll. "Pure and Applied Mathematics", no 11, 1988.

[5] J. D. Dixon, M. P. F. Du Sautoy, A. Mann, D. Segal, *Analytic pro-p groups*, 2nd ed. Cambridge University Press, (1999), xviii+ 365 pages.

[6] J.-M. Fontaine and B. Mazur, *Geometric Galois representations*, In Elliptic curves, modular forms, and Fermat's last theorem (Hong Kong, 1993), 41–78, Ser. Number Theory, I, Internat. Press, Cambridge, MA, 1995.

[7] E. Fouvry and J. Klüners, *On the 4-rank of the class groups of quadratic number fields*, Invent. Math. **167** (3) (2007), 455-513.

[8] E. S. Golod, I. R. Shafarevich, *On the class field tower* (Russian) Izv. Akad. Nauk SSSR Ser. Mat. 28 1964 261-272.

[9] G. Gras, *On the T-ramified, S-split p-class field towers over an extension of degree prime to p*, J. Number Theory **129** (2009), no. 11, 2843-2852.

[10] G. Gras, Class Field Theory: from theory to practice, corr. 2nd ed., Springer Monographs in Mathematics, Springer (2005), xiii+507 pages.

[11] G. Gras and A. Munnier, *Extensions cycliques T-totalement ramifiées*, Publ. Math. Besançon, 1997/98.

[12] F. Hajir and C. Maire, *Analytic Lie extensions of number fields with cyclic fixed points and tame ramification*, J. Ramanujan Math. Soc. 37 (2022) 63-85.

[13] F. Hajir, C. Maire, R. Ramakrishna, *On the Shafarevich group of restricted ramification extensions of number fields in the tame case*, Indiana Univ. Math. J. 70 (2021) no. 6, 2693-2710.

[14] H. Kisilevsky, *Number Fields with Class Number congruent to* 4 *mod* 8 *and Hilbert's Theorem 94*, Journal of Number Theory **8** (1976), 271-279.

[15] H. Koch, Galois Theory of p-Extensions, Springer-Verlag. Berlin, 2002.

[16] T. Kubota, *Über den Bizyklischen Biquadratischen Zahlkörper*, Nagoya Math. J. **10** (1956), 65-85.

[17] J. Labute, *Mild pro-p-groups and Galois groups of p-extensions of* $\mathbb{Q}$, J. Reine Angew. Math. **596** (2006), 155-182.

[18] J. Labute, J. Mináč, *Mild pro-2-groups and 2-extensions of* $\mathbb{Q}$ *with restricted ramification*, J. Algebra **332** (2011), 136–158.

[19] M. Lazard, *Groupes analytiques p-adiques*, IHES, Publ. Math. **26** (1965), 389-603.

[20] Y. Liu, M. Matchett Wood, D. Zureick-Brown, *A predicted distribution for Galois groups of maximal unramified extensions*, arXiv:1907.05002, 2019.

[21] C. Maire, *On the quotients of the maximal unramified extensions of a number field*, Documenta Mathematica 23 (2018), 1263-1290.

[22] C. Maire, *Cohomology of number fields and analytic pro-p-groups*, Moscow Mathematical Journal **10** (2010), 399-414.

[23] J. Martinet, *Tours de corps de classes et estimations de discriminants*, Inventiones math. **44** (1978), 65-73.

[24] B. Mazur, *Notes on étale cohomology of number fields*, Annales Sci. Ecole Normale Supérieure **6**, série 4 (1973), 521-553.

[25] J. Neukirch, A. Schmidt and K. Wingberg, Cohomology of Number Fields, second editiion, corrected second printing, GMW 323, Springer-Verlag Berlin Heidelberg, 2013.

[26] M. Ozaki, *Construction of maximal unramified p-extensions with prescribed Galois groups*, Inventiones math. **83** (2011), 649-680.

[27] The PARI Group, PARI/GP version2.9.4, Univ. Bordeaux, 2018, http ://pari.math.u-bordeaux.fr/.

[28] L. Ribes, P. Zalesskii, *Profinite Goups*, 2nd. ed., a series of modern surveys in mathematics, v. 40 (2010).

[29] P. Roquette *On Class Field Towers*, in *Algebraic Number Theory* edited by J. W. S. Cassels and A. Fröhlich, Academic Press 1967.

[30] A. Schmidt, *Bounded defect in partial Euler characteristics*, Bull. London Math. Soc. **28** (1996), 463-464.

[31] A. Schmidt, *Rings of integer of type* $K(\pi, 1)$, Documenta Mathematica **12** (2007), 441-471.

[32] A. Schmidt, *Über Pro-p-Fundamentalgruppen markierter arithmetischer Kurven*, J. reine u. angew. Math. **640** (2010), 203-235.

[33] A. Scholz, *Über die Bezeichung der Klassenzahlen quadratischer Körper zueinander*, J. reine u. angew. Math. **166** (1932), 201-203.

[34] R. Schoof, *Infinite class field towers of quadratic fields*, J. reine u. angew. Math. **372** (1986), 209–220.

[35] W. R. Scott, Group Theory, Dover, New York, 1987.

[36] Serre J.-P. Serre *Cohomologie Galoisienne* Cinquième édition, révisée et complétée, SLNM 5, 1997.

[37] I. Shafarevich, *Algebraic number fields* (Russian), 1963 Proc. Internat. Congr. Mathematicians (Stockholm, 1962) pp. 163-176 Inst. Mittag-Leffler, Djursholm

[38] I. Shafarevich, *Extensions with prescribed ramification points*, Inst. Hautes Études Sci. Publ. Math. 18 (1964), 71 – 95, In Russian ; English translation “Amer. Math. Soc. Transl.,” Vol. 59, pp. 128 149, Amer. Math. Soc., Providence, RI, 1966.

[39] E.B. Vinberg, *On a theorem concerning on infinite dimensionality of an associative algebra*, Izv. Akad. Nauk SSSR Ser. Mat. **29** (1965), 208-214; english transl., Amer. Mat. Soc. Transl. (2) **82** (1969), 237-242.

[40] W. Bosma, J.J. Cannon, C Playoust, *The MAGMA algebra system. I. The user language*, J. Symbolic Computation **24** (1997), 235-265.

[41] K. Wingberg, *Free quotients of Demushkin groups with operators*, preprint 2004.

[42] K. Wingberg, *On the Fontaine-Mazur conjecture for CM-fields*, Compositio Math. **131** (2002), no. 3, 341-354.

[43] K. Wingberg, *On Demushkin groups with involution*, Annales Scientifiques de l’É.N.S. 4ème série **22** (1989), no 4, 555-567.

November 10, 2022

Farshid Hajir, Christian Maire, Ravi Ramakrishna, Department of Mathematics & Statistics, University of Massachusetts, Amherst, MA 01003, USA • FEMTO-ST Institute, Université Bourgogne Franche-Comté, CNRS, 15B avenue des Montboucons, 25000 Besançon, FRANCE • Department of Mathematics, Cornell University, Ithaca, USA • *E-mail :* `hajir@math.umass.edu`, `christian.maire@univ-fcomte.fr`, `ravi@math.cornell.edu`