EXPLICIT KUMMER THEORY FOR THE RATIONAL NUMBERS

ANTONELLA PERUCCA, PIETRO SGOBBA, SEBASTIANO TRONTO

ABSTRACT. Let G be a finitely generated multiplicative subgroup of $\mathbb{Q}^\times$ having rank r. The ratio between n^r and the Kummer degree $[\mathbb{Q}(\zeta_m, \sqrt[n]{G}) : \mathbb{Q}(\zeta_m)]$, where n divides m, is bounded independently of n and m. We prove that there exist integers m_0, n_0 such that the above ratio depends only on G, $\gcd(m, m_0)$, and $\gcd(n, n_0)$. Our results are very explicit and they yield an algorithm that provides formulas for all the above Kummer degrees (the formulas involve a finite case distinction).

1. INTRODUCTION

The aim of this paper is developing a theory that allows to explicitly compute the degree of Kummer extensions. Let G be a finitely generated multiplicative subgroup of $\mathbb{Q}^\times$ having positive rank r and, without loss of generality, not containing -1. We are interested in the Kummer extension

$$\left[\mathbb{Q}\big(\zeta_M, \sqrt[N]{G}\big) : \mathbb{Q}(\zeta_M)\right] \qquad \text{with } N \mid M\,, \tag{1.1}$$

where ζ_M is a root of unity of order M, and where we are adding the N-th roots of all elements of G. The maximal possible value for the Kummer degree (1.1) is N^r, and in general this degree is a divisor of N^r. It is known (see [4, Theorem 3.1] for a direct proof) that the ratio between N^r and the Kummer degree (1.1) is bounded independently of N and M. We interpret this ratio as the failure of maximality for the Kummer degree.

We prove that there exist explicitly computable integers M_0, N_0 such that the failure of maximality for the Kummer degree only depends on M and N through $\gcd(M, M_0)$ and $\gcd(N, N_0)$. We also present a strategy to provide formulas for the Kummer degree in (1.1): the input is the group G, and the output are formulas for all M, N with a finite case distinction. This algorithm has been implemented in Sagemath by Tronto. Notice that the computation of one single degree (i.e. fixing the parameters M, N and with $M = N$) has also been obtained by Palenstijn in his thesis [2] with a different method (namely with the theory of entanglement groups due to Lenstra).

Let us now illustrate why the Kummer degree fails to be maximal. We may suppose without loss of generality that $N := \ell^e$ for some prime number ℓ. We distinguish two reasons for the failure of maximality for the Kummer degree, namely the *ℓ-adic failure* and the *adelic failure*. The ℓ-adic failure is due to divisibility properties involving the number ℓ. For example, if

2010 *Mathematics Subject Classification.* Primary: 11Y40; Secondary: 11R18, 11R21.
Key words and phrases. Number fields, Kummer theory, Degree, Cyclotomic fields.

$G = \langle 5^\ell \rangle$, then for all $e \geqslant 1$ we have

$$\left[\mathbb{Q}\big(\zeta_{\ell^e}, \sqrt[\ell^e]{5^\ell}\big) : \mathbb{Q}(\zeta_{\ell^e})\right] = \ell^{e-1}\,.$$

The adelic failure is due to the fact that the square root of any rational number is contained in some cyclotomic field. For example, if $G = \langle 5 \rangle$, we need to take into account that $\sqrt{5}$ lies in $\mathbb{Q}(\zeta_5)$:

$$\left[\mathbb{Q}\big(\zeta_M, \sqrt[N]{5}\big) : \mathbb{Q}(\zeta_M)\right] = \begin{cases} N, & \text{if } N \text{ is odd or } 5 \nmid M \\ N/2, & \text{otherwise.} \end{cases}$$

The structure of the paper is as follows. In Section 2 we introduce the notation that is used in the rest of the paper, and in particular we write $A_\ell(N)$ for the *ℓ-adic failure*, and $B(M,N)$ for the *adelic failure*, and we consider the *Kummer failure* $C(M,N)$ (see also Theorem 2.1 and (2.2)), which is

$$C(M,N) := \frac{N^r}{\left[\mathbb{Q}\big(\zeta_M, \sqrt[N]{G}\big) : \mathbb{Q}(\zeta_M)\right]} = B(M,N) \cdot \prod_{\ell \mid N} A_\ell(N)\,.$$

Notice that knowing $C(M,N)$ for every M, N with $N \mid M$ is equivalent to knowing the Kummer degrees that we are interested in. Also notice that the assumption that G is torsion-free is not really necessary (see Remark 2.5).

Section 3 is devoted to studying the ℓ-adic failure $A_\ell(N)$ for all odd prime numbers ℓ (notice that it equals 1 for all but finitely many primes ℓ). The 2-adic failure $A_2(N)$ is studied in Section 4. The adelic failure $B(M,N)$ is more complicated and is studied in the following two sections. Then in Section 7 we prove in particular the following result:

Theorem 1.1. *There are integers M_0 and N_0, depending only on G, such that for all integers N, M with $N \mid M$, the Kummer failure $C(M,N)$ depends only on $\gcd(M, M_0)$ and on $\gcd(N, N_0)$.*

Finally, the last section is devoted to examples that give an insight on the case distinction in our results.

2. The failure of maximality for Kummer extensions

We make use of the following standard notation for any positive integers N, M and any prime number ℓ: we denote by ζ_M a primitive M-th root of unity; $v_\ell(N)$ is the ℓ-adic valuation of N; (N,M) or $\gcd(N,M)$ is the greatest common divisor of N and M, while $[N,M]$ or $\operatorname{lcm}(M,N)$ is the least common multiple; for $n \geqslant 1$ we write $\ell^n \parallel N$ to mean $v_\ell(N) = n$.

Let G be a finitely generated and torsion-free subgroup of $\mathbb{Q}^\times$ of positive rank r. We denote the M-th cyclotomic field by $\mathbb{Q}_M := \mathbb{Q}(\zeta_M)$ and, for $N \mid M$, the N-th Kummer extension of $\mathbb{Q}_M$ related to G by $\mathbb{Q}_{M,N} := \mathbb{Q}_M(\sqrt[N]{G})$.

Theorem 2.1 (see [4, Theorem 3.1] for a direct proof)**.** *Let G be a finitely generated and torsion-free subgroup of $\mathbb{Q}^\times$ of positive rank r. For all integers $M, N \geqslant 1$ with $N \mid M$ the*

Kummer failure

$$C(M,N) := \frac{N^r}{[\mathbb{Q}_{M,N} : \mathbb{Q}_M]}$$

is bounded independently of M, N.

Using arguments of elementary field theory and considering the prime factorization $N = \prod_\ell \ell^n$, where $n = v_\ell(N)$, we can write

$$C(M,N) = \prod_{\ell | N} \frac{\ell^{nr}}{[\mathbb{Q}_{M,\ell^n} : \mathbb{Q}_M]} = \prod_{\ell | N} \frac{\ell^{nr}}{[\mathbb{Q}_{\ell^n,\ell^n} : \mathbb{Q}_{\ell^n}]} \cdot \frac{[\mathbb{Q}_{\ell^n,\ell^n} : \mathbb{Q}_{\ell^n}]}{[\mathbb{Q}_{M,\ell^n} : \mathbb{Q}_M]}.$$

We then decompose the Kummer failure:

Definition 2.2. Let ℓ be a prime number. Let $N \geqslant 1$ with $v_\ell(N) = n$. The *ℓ-adic failure* $A_\ell(N)$ at N is defined as

$$A_\ell(N) := C(\ell^n, \ell^n) = \frac{\ell^{nr}}{[\mathbb{Q}_{\ell^n,\ell^n} : \mathbb{Q}_{\ell^n}]}\,.$$

Notice that the integer $A_\ell(N)$ is a power of ℓ that depends on N only through its ℓ-adic valuation.

Definition 2.3. Let $N \geqslant 1$ with $v_2(N) = n$, and let $M \geqslant 1$ with $N \mid M$. The *adelic failure* at M, N is defined as the ratio

$$B(M,N) := \frac{[\mathbb{Q}_{2^n,2^n} : \mathbb{Q}_{2^n}]}{[\mathbb{Q}_{M,2^n} : \mathbb{Q}_M]}\,.$$

Notice that the integer $B(M,N)$ is a power of 2, and that we have

$$B(M,N) = [\mathbb{Q}_{2^n,2^n} \cap \mathbb{Q}_M : \mathbb{Q}_{2^n}]\,. \tag{2.1}$$

The ratio $[\mathbb{Q}_{\ell^n,\ell^n} : \mathbb{Q}_{\ell^n}]/[\mathbb{Q}_{M,\ell^n} : \mathbb{Q}_M]$ equals 1 if ℓ is odd by [4, Lemma 3.5], so that we have

$$C(M,N) = B(M,N) \cdot \prod_{\ell | N} A_\ell(N)\,. \tag{2.2}$$

Lemma 2.4 (cf. [4, Lemmas 3.2, 3.5])**.** *Let ℓ be a prime number.*

(1) The ℓ-adic failure $A_\ell(N)$ is bounded independently of N. More precisely, there is an integer $n_\ell \geqslant 0$ (which depends only on G and ℓ) such that for every $N \geqslant 1$ we have $A_\ell(N) \mid \ell^{n_\ell}$. The integer n_ℓ equals 0 for all but finitely many primes ℓ.

(2) The adelic failure $B(M,N)$ is bounded independently of M, N. More precisely, for all $M, N \geqslant 1$ with $N \mid M$, we have $B(M,N) \mid 2^r$, where r is the rank of G.

Notice that by Corollary 7.3 we have the following stronger statements:

(1) Let ℓ be a prime number. There is an integer α_ℓ such that $A_\ell(N) = \alpha_\ell$ for all N with $v_\ell(N) \geqslant c_\ell$, where c_ℓ is some integer depending only on ℓ and G. We call α_ℓ the *total ℓ-adic failure*. The integer α_ℓ is a power of ℓ, and we have $\alpha_\ell = 1$ for all but finitely many primes ℓ.

(2) There is an integer β such that $B(M,N)=\beta$ for all M,N with $N \mid M$, $M_0 \mid M$ and $N_0 \mid N$, where M_0 and N_0 are some integers depending only on G. We call β the *total adelic failure*. In particular, β is a power of 2 and we have

$$\beta = [\mathbb{Q}_{2^n,2^n} \cap \mathbb{Q}_\infty : \mathbb{Q}_{2^n}]$$

for all sufficiently large n, where $\mathbb{Q}_\infty$ is the compositum of all cyclotomic fields.

Notice that $A_\ell(\ell^n)$ is non-decreasing in n, and in particular we have $\alpha_\ell = \max_N A_\ell(N)$. Conversely, in general β cannot be expressed as the maximum value of $B(M,N)$ over M,N. For example, taking $G=\langle 2\rangle$ and $M=N=2^n$, the right-hand side of (2.1) is 2 if $n=1,2$, and it is 1 for $n \geqslant 3$ ($\sqrt{2} \in \mathbb{Q}_8$ gives rise to a 2-adic failure instead).

In view of (2.2) we also define the *total Kummer failure* for G by

$$C_0 := \beta \cdot \prod_\ell \alpha_\ell,$$

where the product runs over all prime numbers ℓ. In fact, the integer C_0 is such that $C(M,N)=C_0$ for all M,N with $N \mid M$, $M_0 \mid M$ and $N_0 \mid N$, where M_0 and N_0 depend only on G.

Remark 2.5. *To deal with a finitely generated subgroup G' of $\mathbb{Q}^\times$ which is not torsion-free, write $G'=\langle -1\rangle \times G$, where G is torsion-free. For M,N with $N|M$ we have*

$$\left[\mathbb{Q}_M\left(\sqrt[N]{G'}\right) : \mathbb{Q}_M\right] = \left[\mathbb{Q}_{[M,2N]}\left(\sqrt[N]{G}\right) : \mathbb{Q}_{[M,2N]}\right] \cdot \left[\mathbb{Q}_{[M,2N]} : \mathbb{Q}_M\right] .$$

Therefore, the Kummer degree for G' is the product of a Kummer degree for the torsion-free group G times $\varphi([M,2N])/\varphi(M) \in \{1,2\}$.

3. The ℓ-adic failure for ℓ odd

Let G be a finitely generated and torsion-free subgroup of $\mathbb{Q}^\times$ of rank r and let ℓ be an odd prime number. In order to compute the ℓ-adic failure $A_\ell(N)$, we show how to determine the degrees

$$\left[\mathbb{Q}_{\ell^m}\left(\sqrt[\ell^n]{G}\right) : \mathbb{Q}_{\ell^m}\right]$$

for all integers $m \geqslant n \geqslant 1$ using the results from [1, Section 3.3] which we recall in Proposition 3.1.

An element of $\mathbb{Q}^\times$ is called *strongly ℓ-indivisible* if it is not an ℓ-th power in $\mathbb{Q}^\times$. We call $a_1,\dots,a_r \in \mathbb{Q}^\times$ *strongly ℓ-independent* if $a_1^{e_1}\cdots a_r^{e_r}$ is strongly ℓ-indivisible whenever the integers $e_1,\dots,e_r$ are not all divisible by ℓ. We now specialize results of [1] for the rational numbers.

There is a basis $g_1,\dots,g_r$ of G, which we call an *ℓ-good basis*, such that

$$g_i = b_i^{\ell^{d_i}}$$

holds for some strongly ℓ-independent elements $b_1,\dots,b_r$ of $\mathbb{Q}^\times$, and for some non-negative integers d_i. We refer to the tuple $(d_1,\dots,d_r)$ as the *d-parameters for the ℓ-divisibility* of G. Up to reordering the elements of the basis, we choose the d-parameters to be a non-decreasing sequence: then they are the same for every ℓ-good basis of G.

Proposition 3.1 (cf. [1, Example 21])**.** *Let G be a finitely generated and torsion-free subgroup of $\mathbb{Q}^\times$. Let ℓ be an odd prime, and let $d_1, \dots, d_r$ be the d-parameters for the ℓ-divisibility of G. Then we have*

$$v_\ell\big([\mathbb{Q}_{\ell^m,\ell^n} : \mathbb{Q}_{\ell^m}]\big) = \sum_{i=1}^{r} \max(n - d_i, 0)\,.$$

In particular, the total ℓ-adic failure is $\alpha_\ell = \ell^{\sum_i d_i}$.

Since the d-parameters for the ℓ-divisibility of G are explicitly computable (cf. [1, Section 6.1]) , so is the ℓ-adic failure for each odd prime ℓ. The challenge is here computing the ℓ-adic failure for all primes ℓ at once with a finite procedure. We consider a basis $g_1, \dots, g_r$ of G, and we write the prime factorization of each generator g_i as

$$g_i = \pm \prod_{j=1}^{s} p_j^{e_{ij}}$$

for some integers $e_{ij} \in \mathbb{Z}$, where p_j runs through the finitely many primes appearing in the factorizations of the g_i's. We call (e_{ij}), which is an $r \times s$ matrix with $r \leqslant s$, the *matrix of the exponents*.

Lemma 3.2. *Let ℓ be an odd prime number and let (e_{ij}) be the matrix of the exponents of a basis of G. If that matrix modulo ℓ has maximal rank, then the basis is an ℓ-good basis of G and the d-parameters for the ℓ-divisibility are all zero.*

Proof. The matrix of the exponents has maximal rank r over $\mathbb{Z}/\ell\mathbb{Z}$ if and only if the vectors $v_i = (e_{i,1}, \dots, e_{i,s})$ are linearly independent over $\mathbb{Z}/\ell\mathbb{Z}$. This means that if $\sum_i x_i v_i \equiv 0 \bmod \ell$ for some integers x_i, then $\ell \mid x_i$ for every i. So the linear independence of the vectors v_i is equivalent to the following condition: if there are some integers x_i such that

$$g := \prod_i g_i^{x_i} = \pm \prod_j p_j^{\sum_i x_i e_{ij}}$$

with $\ell \mid \sum_i x_i e_{ij}$ for all j, so that g is an ℓ-th power in $\mathbb{Q}$, then $\ell \mid x_i$ for all i. By definition, this means that the g_i's are strongly ℓ-independent, which implies that the d-parameters are all zero. □

The matrix of the exponents modulo ℓ has maximal rank r for all but finitely many odd primes ℓ, and the set of exceptions is easily computable. In particular, for all but finitely many primes ℓ the d-parameters are all zero, which gives

$$[\mathbb{Q}_{\ell^m,\ell^n} : \mathbb{Q}_{\ell^m}] = \ell^n \qquad \text{for all } m \geqslant n \geqslant 1$$

by Proposition 3.1. Now consider one of the remaining odd primes ℓ. We can apply the algorithm described in [1, Section 6.1] to compute an ℓ-good basis for G and the d-parameters for the ℓ-divisibility. Applying Proposition 3.1 we can then compute $A_\ell(N)$ for every N.

4. THE 2-ADIC FAILURE

Let G be a finitely generated and torsion-free subgroup of $\mathbb{Q}^\times$ of rank r. In this section we show how to compute the degrees

$$\left[\mathbb{Q}_{2^m}\left(\sqrt[2^n]{G}\right) : \mathbb{Q}_{2^m}\right]$$

for all integers $m \geqslant n \geqslant 1$. In Theorem 4.2 we recall from [1, Section 3.3] parametric formulas for these degrees: for $m \geqslant 2$ we can work over $\mathbb{Q}_4$ and apply the formula (4.2), while for $m = n = 1$, we can make use of Eq. (4.3).

Let K be either $\mathbb{Q}^\times$ or $\mathbb{Q}_4^\times$. An element of K is called *strongly* 2*-indivisible in* K if it is not a square in $K^\times$ times a root of unity in K. Elements of $K^\times$ are *strongly* 2*-independent* if the product of any nonempty subset of them is strongly 2-indivisible. We recall results of [1] for K.

We consider a finitely generated and torsion-free subgroup G of $K^\times$ and a basis $g_1, \dots, g_r$ of G. We can write

$$g_i = \zeta_{2^{h_i}} \cdot b_i^{2^{d_i}} \tag{4.1}$$

for some strongly 2-indivisible elements $b_1, \dots, b_r$ of $K^\times$, for some non-negative integers d_i and for some roots of unity $\zeta_{2^{h_i}}$ in K of order 2^{h_i}. We refer to b_i as the *strongly* 2*-indivisible part* of g_i.

(1) We call $g_1, \dots, g_r$ a 2*-good basis* of G if the b_i's are strongly 2-independent. Recall from [1, Theorem 14] that a 2-good basis of G always exists.
(2) For a 2-good basis of G, we refer to the tuple $(d_1, \dots, d_r; h_1, \dots, h_r)$ as the *parameters for the* 2*-divisibility* of G in K. We call $d_1, \dots, d_r$ the d*-parameters* and $h_1, \dots, h_r$ the h*-parameters*. Up to reordering the elements of the basis, we choose the d-parameters to be a non-decreasing sequence. Then the d-parameters are the same for every 2-good basis.
(3) Given a basis of G written as in (4.1), the following are equivalent:
    (a) The strongly 2-indivisible parts $b_1, \dots, b_r$ are strongly 2-independent.
    (b) The sum $\sum_i d_i$ is maximal (among all possible bases for G).
    (c) The strongly 2-indivisible parts $b_1, \dots, b_r$ generate a torsion-free subgroup of $K^\times$ of rank r and whose d-divisibility parameters are all zero.

Notice that the parameters for the 2-divisibility of G are explicitly computable by the algorithm described in [1, Section 6.1].

Remark 4.1. *Let G be a finitely generated and torsion-free subgroup of $\mathbb{Q}^\times$, and suppose that G contains negative elements. Then there is a 2-good basis of G such that exactly one of the generators is negative. Indeed, consider any 2-good basis. If g is one of the negative generators with the highest d-parameter, then we can simply multiply all other negative generators by g (notice that we do not decrease their 2-divisibility).*

Theorem 4.2 ([1, Theorem 18, Lemma 19])**.** *Let G be a finitely generated and torsion-free subgroup of $\mathbb{Q}^\times$ of rank r. Let $m \geqslant n$ be positive integers.*

- *If $m \geqslant 2$, we have*

$$v_2\left(\left[\mathbb{Q}_{2^m}\left(\sqrt[2^n]{G}\right) : \mathbb{Q}_{2^m}\right]\right) = \max\{h_i + n_i : 1 \leqslant i \leqslant r\} \cup \{m\} - m + rn - \sum_{i=1}^{r} n_i\,, \tag{4.2}$$

where $n_i = \min(n, d_i)$ and $(d_1, \dots, d_r; h_1, \dots, h_r)$ are the parameters for the 2-divisibility of G in $\mathbb{Q}_4$.

- *If $m = n = 1$, we have*

$$\left[\mathbb{Q}\big(\sqrt{G}\big) : \mathbb{Q}\right] = e\left[\mathbb{Q}_4\big(\sqrt{G}\big) : \mathbb{Q}_4\right], \tag{4.3}$$

where $e = 2$ if G contains minus a square in $\mathbb{Q}^\times$ and $e = 1$ otherwise.

Notice that to compute the divisibility parameters of G over $\mathbb{Q}_4$ one only needs to take into account that, up to squares in $\mathbb{Q}^\times$, only the elements ± 2 are strongly 2-indivisible over $\mathbb{Q}$ but not over $\mathbb{Q}_4$. Nevertheless, in [5] we show in a more general setting that one can compute the degrees in (4.2) using the parameters over $\mathbb{Q}$ and certain properties of G.

5. The intersection between Kummer extensions and cyclotomic fields

This section is devoted to studying the intersection

$$\mathbb{Q}_{2^m}\left(\sqrt[2^n]{G}\right) \cap \mathbb{Q}_\infty\,,$$

where $n \leqslant m$ are positive integers, and where $\mathbb{Q}_\infty$ denotes the compositum of all cyclotomic fields.

Notation. If $\{g_i\}$ is a basis of G, then we write $g_i = g_{i,d_i}$ to display the d-parameter for the 2-divisibility of g_i in $\mathbb{Q}$.

Firstly we deal with the case $G \subseteq \mathbb{Q}_+^\times$.

Theorem 5.1. *Let G be a finitely generated and torsion-free subgroup of $\mathbb{Q}^\times$ of positive rank. Suppose that G contains only positive elements. Then for every 2-good basis $\{g_{i,d_i}\}$ we have*

$$\mathbb{Q}_{2^m,2^n} \cap \mathbb{Q}_\infty = \mathbb{Q}_{2^m}\left(g_{i,d_i}^{1/2^{d_i+1}} : 0 \leqslant d_i \leqslant n-1\right) \tag{5.1}$$

for all positive integers $m \geqslant n$. Writing $g_{i,d_i} = b_i^{2^{d_i}}$, where the b_i's are strongly 2-independent positive rational numbers, we then have

$$\mathbb{Q}_{2^m,2^n} \cap \mathbb{Q}_\infty = \mathbb{Q}_{2^m}\left(\sqrt{b_i} : 0 \leqslant d_i \leqslant n-1\right). \tag{5.2}$$

Proof. Notice that (5.2) is an immediate consequence of (5.1). The inclusion $\supseteq$ in (5.1) holds because the elements generating the field on the right-hand side lie in $\sqrt[2^n]{G}$, and they can be expressed as the square root of some rational number times a root of unity of order dividing 2^n.

Now we prove the inclusion $\subseteq$ in (5.1). The left-hand side of (5.1) is a finite abelian extension of $\mathbb{Q}_{2^m}$ of exponent dividing 2^n and hence by classical Kummer theory it is of the form $\mathbb{Q}_{2^m}(H^{1/2^n})$, where H is a subgroup of $\mathbb{Q}_{2^m}^\times$ such that $H\mathbb{Q}_{2^m}^{\times 2^n} \subseteq G\mathbb{Q}_{2^m}^{\times 2^n}$. Therefore it is sufficient to determine which 2^n-th roots of elements of G lie in $\mathbb{Q}_\infty$.

The 2^n-th root of a generator g_{i,d_i} with $d_i \geqslant n-1$ lies in the field on the right-hand side, so we may suppose that $n \geqslant 2$ and reduce to study the elements of the form

$$g = \prod_{i \in J_0} g_{i,0}^{f_i} \prod_{i \in J_1} g_{i,1}^{f_i} \cdots \prod_{i \in J_{n-2}} g_{i,n-2}^{f_i},$$

where J_d consists of the indices i such that the generator g_{i,d_i} has divisibility parameter $d_i = d$. Analogously, we may restrict to consider exponents f_i that are positive integers such that $v_2(f_i) + d_i < n-1$. We are left to show that no such element has a 2^n-th root which lies in a cyclotomic field. We may rewrite

$$g = \prod_i b_i^{e_i}$$

such that $v_2(e_i) < n-1$, and we conclude by the following Lemma. □

Lemma 5.2. *Let $b_1, \dots, b_r$ be strongly 2-independent elements of $\mathbb{Q}^\times$. If $n \geqslant 2$, then no 2^n-th root of a product of the form*

$$g = \prod_i b_i^{e_i} \qquad \text{with } v_2(e_i) < n-1 \ \forall i$$

belongs to a cyclotomic field.

Proof. For $n = 2$ we know that the product g, having odd exponents, is strongly 2-indivisible in $\mathbb{Q}^\times$ and hence its fourth root does not lie in a cyclotomic field (which is an abelian extension of $\mathbb{Q}$) by [6, Theorem 2] (see also [4, Theorem 3.3]). Now suppose that $n \geqslant 3$. If $v_2(e_i) = 0$ for some index i we may reason as above, so suppose that all exponents e_i are even and write $\sqrt{g} = \prod_i b_i^{e_i/2}$ where $v_2(e_i/2) < n-2$. The result for $n-1$ applied to $\sqrt{g}$ gives that no 2^{n-1}-th root of this element belongs to a cyclotomic field, so we may conclude by induction. □

Theorem 5.3. *Let G be a finitely generated and torsion-free subgroup of $\mathbb{Q}^\times$ of positive rank. Suppose that G contains negative elements, and consider a 2-good basis $\{g_{i,d_i}\}$ such that exactly one of the generators, say $g_{j,x}$, is negative (cf. Remark 4.1). Then for all positive integers $m \geqslant n$ we have*

$$\mathbb{Q}_{2^m,2^n} \cap \mathbb{Q}_\infty = \mathbb{Q}_{2^v}\left(g_{i,d_i}^{1/2^{d_i+1}} : 0 \leqslant d_i \leqslant n-1\right), \tag{5.3}$$

where $v = m$ if $n \geqslant x+1$, and $v = \max(m, n+1)$ if $n \leqslant x$.

Writing $g_{i,d_i} = \pm b_i^{2^{d_i}}$, where the b_i's are strongly 2-independent positive rational numbers (and where the sign is negative only for $i = j$), we have

$$\mathbb{Q}_{2^m,2^n} \cap \mathbb{Q}_\infty = \mathbb{Q}_{2^v}\left(\sqrt{b_i} : 0 \leqslant d_i \leqslant n-1\right), \tag{5.4}$$

if $n \neq x+1$, while for $n = x+1$ we have

$$\mathbb{Q}_{2^m,2^n} \cap \mathbb{Q}_\infty = \mathbb{Q}_{2^m}\left(\zeta_{2^{x+2}}\sqrt{b_j}, \sqrt{b_i} : 0 \leqslant d_i \leqslant n-1, i \neq j\right). \tag{5.5}$$

Proof. First notice that (5.4) and (5.5) are equivalent to (5.3): for (5.4) with $x \leqslant n$ this is because we take the root of b_j rather than that of g_j, the ratio being a root of unity in $\mathbb{Q}_{2^v}$.

The inclusion $\supseteq$ in (5.3) is similar to Theorem 5.1 and it is clear if one considers that, if $n \leqslant x$, the 2^n-th root of $g_{j,x}$ is a rational number times $\zeta_{2^{n+1}}$.

Now we prove the inclusion $\subseteq$. As in the proof of Theorem 5.1 we are left to detect which 2^n-th roots of the elements of G are contained in a cyclotomic field.

If $n = x+1$, then the 2^n-th root of the negative generator lies in a cyclotomic field and it equals $\zeta_{2^{x+2}}\sqrt{b_j}$. The presence of g_j in the expression of an element of G as a product of generators does not change whether its 2^n-th root lies in a cyclotomic field. So again we may reduce to Theorem 5.1 to prove the inclusion $\subseteq$ in (5.5).

If $n \geqslant x+2$, then the sign of an element of G does not influence whether the 2^n-th root lies in a cyclotomic field and we can proceed as in Theorem 5.1.

If $n \leqslant x$, then the 2^n-th root of the negative generator only contributes by a root of unity $\zeta_{2^{n+1}}$ and hence the presence of the negative generator in an expression for $g \in G$ does not matter. Again we may proceed as in Theorem 5.1. □

Remark 5.4. *Consider the fields in* (5.2)*,* (5.4)*, and* (5.5)*. To study the intersection on the left-hand side we may suppose w.l.o.g. (up to squares in $\mathbb{Q}^\times$) that the b_i's are positive squarefree integers. The smallest cyclotomic field containing $\sqrt{b_i}$ is then $\mathbb{Q}_{b_i}$ if $b_i \equiv 1 \bmod 4$, and $\mathbb{Q}_{4b_i}$ otherwise. Let $M := \operatorname{lcm}\{b_i\}$, where i runs over the indices such that $1 \leqslant d_i \leqslant n-1$ and $g_{i,d_i} > 0$.*

1. *The smallest cyclotomic field containing* (5.2) *is $\mathbb{Q}_{2^m M}$ if $b_i \equiv 1 \bmod 4$ for all $1 \leqslant d_i \leqslant n-1$, and $\mathbb{Q}_{[2^m,4M]}$ otherwise.*
2. *If $n \leqslant x$, then the smallest cyclotomic field containing* (5.4) *is $\mathbb{Q}_{[2^v,M]}$ if $b_i \equiv 1 \bmod 4$ for all $1 \leqslant d_i \leqslant n-1$, and $\mathbb{Q}_{[2^v,4M]}$ otherwise.*
3. *If $n \geqslant x+1$, then the smallest cyclotomic field containing* (5.4) *is $\mathbb{Q}_{[2^m,M,b_j]}$ if $b_i \equiv 1 \bmod 4$ for all $1 \leqslant d_i \leqslant n-1$, and $\mathbb{Q}_{[2^m,4M,b_j]}$ otherwise.*
4. *Now consider the field* (5.5)*, and let $b := \zeta_{2^{x+2}}\sqrt{b_j}$.*
   - *If $x = 0$, then the smallest cyclotomic field containing $b = \sqrt{-b_j}$ is $\mathbb{Q}_{b_j}$ if $-b_j \equiv 1 \bmod 4$, and $\mathbb{Q}_{4b_j}$ otherwise.*
   - *If $x \geqslant 1$ and $2 \nmid b_j$, then the smallest cyclotomic field containing b is $\mathbb{Q}_{2^{x+2}b_j}$.*
   - *If $x = 1$ and $2 \mid b_j$, then the smallest cyclotomic field containing $b = \zeta_8\sqrt{b_j}$ is $\mathbb{Q}_{2b_j}$, as $\zeta_8\sqrt{2} = \zeta_4 + 1$.*
   - *If $x > 1$ and $2 \mid b_j$, then the smallest cyclotomic field containing b is $\mathbb{Q}_{2^{x+1}b_j}$ because $\mathbb{Q}_8(\zeta_{2^{x+2}}\sqrt{2}) = \mathbb{Q}_{2^{x+2}}$ (recall that $\sqrt{2} \in \mathbb{Q}_8$).*

   Hence in each of these cases the smallest cyclotomic field containing the field (5.5) *is given by composing the above cyclotomic fields with $\mathbb{Q}_M$ or $\mathbb{Q}_{4M}$ (according to the other b_i's) and with $\mathbb{Q}_{2^m}$.*

6. THE ADELIC FAILURE

In this section we show how to compute the degrees $B(M,N)$ for M, N with $N \mid M$ (see (2.1)). Set $n := v_2(N)$. We begin with two important remarks whose proof is straight-forward and is left to the reader:

Remark 6.1. *Let G be as in Theorem 5.1. We use the same notation, and in particular each generator of G is written as $g_i = b_i^{2^{d_i}}$. Let $m \geqslant n \geqslant 1$ and $T \geqslant 1$. Let*

$$\mathcal{S} := \{b_i : 0 \leqslant d_i \leqslant n-1\},$$

$$\mathcal{C} := \left\{ y \in \mathbb{Z} : y \equiv \prod_i b_i^{e_i} \bmod \mathbb{Q}^{\times 2}, b_i \in \mathcal{S}, e_i \in \{0,1\}, y \text{ squarefree} \right\},$$

and define H as the following subgroup of $\mathbb{Q}^\times$:

- *if $8 \mid T$, then $H = \langle y \in \mathcal{C} : y \mid T \rangle$,*
- *if $4 \parallel T$, then $H = \langle y \in \mathcal{C} : y \mid T, 2 \nmid y \rangle$,*
- *if $4 \nmid T$, then $H = \langle y \in \mathcal{C} : y \mid T, y \equiv 1 \bmod 4 \rangle$.*

That is, the generators y for H are exactly those $y \in \mathcal{C}$ such that $\sqrt{y} \in \mathbb{Q}_T$. In particular we have that $\mathbb{Q}(\sqrt{H}) \subseteq \mathbb{Q}_T$. We then have

$$\mathbb{Q}_{2^m,2^n} \cap \mathbb{Q}_T = \mathbb{Q}_{2^w}\left(\sqrt{H}\right),$$

where $w := \min(m, v_2(T))$.

Remark 6.2. *Let G be as in Theorem 5.3, and keep the same notation. Let $m \geqslant n \geqslant 1$ and $T \geqslant 1$.*

(1) If $n \leqslant x$, define $\mathcal{S}$, $\mathcal{C}$ and H as in Remark 6.1. Then we have

$$\mathbb{Q}_{2^m,2^n} \cap \mathbb{Q}_T = \mathbb{Q}_{2^w}\left(\sqrt{H}\right),$$

where $w := \min(v, v_2(T))$.

(2) If $n \geqslant x+2$, or if $n = x+1$ and $m \geqslant n+1$, define $\mathcal{S}$, $\mathcal{C}$ and H as in Remark 6.1 (notice that $b_j \in \mathcal{S}$). Then we have

$$\mathbb{Q}_{2^m,2^n} \cap \mathbb{Q}_T = \mathbb{Q}_{2^w}\left(\sqrt{H}\right),$$

where $w := \min(m, v_2(T))$.

(3) If $m = n = x+1$, consider (5.5)*.*

• If $n = 1$, then $\sqrt{-b_j}$ can be treated as the other b_i's. More precisely, we let $\mathcal{S}$ be as in Remark 6.1, but we replace b_j by $-b_j$. Define $\mathcal{C}$ and H as before. Then we have

$$\mathbb{Q}_{2^m,2^n} \cap \mathbb{Q}_T = \mathbb{Q}\left(\sqrt{H}\right).$$

• If $n > 2$ and $2^{n+1} \nmid T$, or if $n = 2$ and $4 \nmid T$, define

$$\mathcal{S} := \{b_i : g_i > 0,\ 0 \leqslant d_i \leqslant n-1\}, \tag{6.1}$$

and $\mathcal{C}$ and H analogously to the previous remark. Then we have

$$\mathbb{Q}_{2^m,2^n} \cap \mathbb{Q}_T = \mathbb{Q}_{2^w}\left(\sqrt{H}\right),$$

where $w := v_2(T)$.

• If $n = 2$ and $4 \parallel T$, define $\mathcal{S}$ as in (6.1)*, and $\mathcal{C}$ and H analogously to Remark 6.1. Set*

$$\mathcal{C}' := \{z \in \mathbb{Z} : z \equiv b_j y \bmod \mathbb{Q}^{\times 2},\ y \in \mathcal{C},\ z \text{ squarefree}\}, \tag{6.2}$$

$$H' := \left\langle \zeta_4 z : z \in \mathcal{C}',\ z \text{ even},\ \frac{z}{2} \mid T \right\rangle.$$

Then we have

$$\mathbb{Q}_{2^m,2^n} \cap \mathbb{Q}_T = \mathbb{Q}_4\big(\sqrt{\langle H, H'\rangle}\big)\,.$$

• *If $n \geqslant 2$ and $2^{n+1} \mid T$, define $\mathcal{S}$ as in* (6.1)*, $\mathcal{C}$ and H as in Remark 6.1, $\mathcal{C}'$ as in* (6.2)*, and set*

$$H' := \big\langle \zeta_{2^n} z : z \in \mathcal{C}',\ z \mid T \big\rangle\,.$$

Then we have

$$\mathbb{Q}_{2^m,2^n} \cap \mathbb{Q}_T = \mathbb{Q}_{2^n}\big(\sqrt{\langle H, H'\rangle}\big)\,.$$

In the computation of the adelic failure $B(M,N)$ we will only need to use Remarks 6.1 and 6.2 with $n = m$ and $v_2(T) \geqslant n$. The case distinction simplifies as follows.

Remark 6.3. *Let M, N be integers with $N \mid M$, and set $n := v_2(N)$. Let G be as in Theorem 5.1 and keep the same notation of Remark 6.1 (here $T = M$). Then we have*

$$B(M,N) = \Big[\mathbb{Q}_{2^n}\big(\sqrt{H}\big) : \mathbb{Q}_{2^n}\Big]\,.$$

Let G be as in Theorem 5.3, and keep the same notation of Remark 6.2 case by case (here $T = M$).

(1) If $n \leqslant x$, then $B(M,N) = [\mathbb{Q}_{2^w}(\sqrt{H}) : \mathbb{Q}_{2^n}]$, where $w = \min(n+1, v_2(M))$.
(2) If $n \geqslant x+2$, then $B(M,N) = [\mathbb{Q}_{2^n}(\sqrt{H}) : \mathbb{Q}_{2^n}]$.
(3) If $n = x+1$, we have:

- *if $n = 1$, then $B(M,N) = [\mathbb{Q}(\sqrt{H}) : \mathbb{Q}]$;*
- *if $n = v_2(M) > 2$, then $B(M,N) = [\mathbb{Q}_{2^n}(\sqrt{H}) : \mathbb{Q}_{2^n}]$;*
- *if $n = v_2(M) = 2$, then $B(M,N) = [\mathbb{Q}_4(\sqrt{\langle H, H'\rangle}) : \mathbb{Q}_4]$;*
- *if $n \geqslant 2$ and $v_2(M) \geqslant n+1$, then $B(M,N) = [\mathbb{Q}_{2^n}(\sqrt{\langle H, H'\rangle}) : \mathbb{Q}_{2^n}]$.*

The next proposition is used to compute the adelic failure.

Proposition 6.4. *Let $H \leqslant \mathbb{Q}^\times$ be a torsion-free and finitely generated subgroup. Assume that H does not contain minus a square in $\mathbb{Q}^\times$. Then we have*

$$\Big[\mathbb{Q}_{2^m}\big(\sqrt{H}\big) : \mathbb{Q}_{2^m}\Big] = \begin{cases} \big|\overline{H}\big|/2 & \text{if } m \geqslant 3 \text{ and } \exists\, b \in H \text{ with } b \equiv \pm 2 \bmod \mathbb{Q}^{\times 2}, \\ \big|\overline{H}\big| & \text{otherwise}, \end{cases}$$

where $\overline{H}$ is a complete set of representatives of $H\mathbb{Q}^{\times 2}$ in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$.

Proof. It is clear that we may replace H by any other subgroup $H' \leqslant \mathbb{Q}^\times$ such that $H\mathbb{Q}^{\times 2} = H'\mathbb{Q}^{\times 2}$. Then we may suppose without loss of generality that H is generated by square-free integers $g_1, \ldots, g_r$, where $\big|\overline{H}\big| = 2^r$ (notice that by hypothesis none of the g_i's can be -1). Moreover, we can also suppose that the g_i's are strongly 2-independent, so that the d-parameters for the 2-divisibility of H are all zero over $\mathbb{Q}$.

Suppose first that $m \geqslant 2$. In this case we can work over $\mathbb{Q}_4$ and apply formula (4.2) from Theorem 4.2. We just need to compute the parameters for the 2-divisibility of H over $\mathbb{Q}_4$. The

only squarefree integers which are not strongly 2-indivisible over $\mathbb{Q}_4$ are ± 2 and in particular we have

$$2 = \zeta_4^{-1}(1+\zeta_4)^2\,. \tag{6.3}$$

A simple computation shows that if H contains an element of the form ± 2 times a square, then we may change the basis to get $g_1 = \pm 2$.

Therefore, if H does not contain ± 2 times a square, we have that $d_i = 0$ and $h_i \in \{0,1\}$ for all i also over $\mathbb{Q}_4$, so that the formula (4.2) yields $[\mathbb{Q}_{2^m}(\sqrt{H}) : \mathbb{Q}_{2^m}] = 2^r$. Otherwise, only the parameters corresponding to $g_1 = \pm 2$ change from $\mathbb{Q}$ to $\mathbb{Q}_4$ (in view of (6.3) we get the new parameters $d_1 = 1$ and $h_1 = 2$). Hence by (4.2) this degree will be 2^r for $m = 2$ and 2^{r-1} for $m \geqslant 3$.

Now let $m = 1$. Since H does not contain minus a square, by (4.3) we get

$$\left[\mathbb{Q}\big(\sqrt{H}\big) : \mathbb{Q}\right] = \left[\mathbb{Q}_4\big(\sqrt{H}\big) : \mathbb{Q}_4\right]$$

which is 2^r by our previous computation. □

Corollary 6.5. *Let G be a finitely generated and torsion-free subgroup of $\mathbb{Q}^\times$ of rank r. Then the total adelic failure β for G is equal to*

$$\beta = \begin{cases} 2^{r-1} & \text{if there is } g \in G \text{ of the form } g = \pm(2a^2)^{2^d} \\ 2^r & \text{otherwise} \end{cases}$$

where $a \in \mathbb{Q}^\times$ and where d is a non-negative integer.

Proof. We know that the adelic failure can only be a power of 2. By Remarks 6.1 and 6.2, for $n \geqslant 2$ large enough, we have

$$\mathbb{Q}_{2^n,2^n} \cap \mathbb{Q}_\infty = \mathbb{Q}_{2^n}\big(\sqrt{H}\big)\,,$$

where $H := \langle b_1, \dots, b_r \rangle$, and the b_i's are the strongly 2-indivisible parts of the elements of the 2-good basis of G chosen in Theorems 5.1 and 5.3. In particular the b_i's are strongly 2-independent over $\mathbb{Q}$ and form a 2-good basis of H. Therefore, $\left|\overline{H}\right| = 2^r$, where $\overline{H}$ is a complete set of representatives of $H\mathbb{Q}^{\times 2}$ modulo $\mathbb{Q}^{\times 2}$. Hence by Proposition 6.4, the degree of $\mathbb{Q}_{2^n}(\sqrt{H})$ over $\mathbb{Q}_{2^n}$ is 2^{r-1} if H contains an element of the form 2 times a square, and 2^r otherwise.

By [5, Proposition 5] (where $f = 2$ in our setup) H contains an element of the form 2 times a square if and only if there is an element in G which is equal to $\pm(2a^2)^{2^d}$. □

7. The Kummer failure

In this section we prove Theorem 1.1 which states that, for a fixed group G, there are integers M_0, N_0 such that the Kummer failure $C(M,N)$ only depends on $\gcd(M, M_0)$ and $\gcd(N, N_0)$.

Proposition 7.1. *Fix a prime number ℓ. There is some integer c_ℓ such that for all $N \geqslant 1$ the ℓ-adic failure $A_\ell(N)$ depends on N only through $\gcd(N, \ell^{c_\ell})$. More precisely, we have*

$$A_\ell(N) = A_\ell\big(\gcd(N, \ell^{c_\ell})\big)\,.$$

If ℓ is odd, then we may take for c_ℓ the maximum of the d-parameters for the ℓ-divisibility of G. If $\ell = 2$, then we may take $c_2 = \max_i(d_i + h_i)$, where the d_i's and the h_i's are the parameters for the 2-divisibility of G over $\mathbb{Q}_4$.

Proof. Set $n = v_\ell(N)$. By definition $A_\ell(N)$ depends only on n and it is 1 if $n = 0$. We only prove that, if c_ℓ is defined as in the statement, $A_\ell(N)$ is constant on $\{N : n \geqslant c_\ell\}$, because it is easy to check from our computations that in this case $A_\ell(N) = A_\ell(\gcd(\ell^{c_\ell}, N))$.

By Proposition 3.1, for ℓ odd we have

$$v_\ell\big([\mathbb{Q}_{\ell^n,\ell^n} : \mathbb{Q}_{\ell^n}]\big) = rn - \sum_{i=1}^{r} \min(d_i, n)\,,$$

where the d_i's are the d-parameters for the ℓ-divisibility of G. Therefore, if $n \geqslant c_\ell$ we obtain

$$v_\ell\big(A_\ell(N)\big) = \sum_{i=1}^{r} d_i\,.$$

For $\ell = 2$ and $n \geqslant 2$, by formula (4.2) from Theorem 4.2, we have

$$v_2\big(A_2(N)\big) = n - \max\{h_i + \min(n, d_i) : 1 \leqslant i \leqslant r\} \cup \{n\} + \sum_{i=1}^{r} \min(d_i, n)\,.$$

If $n \geqslant c_2$, then we clearly have

$$v_2\big(A_2(N)\big) = \sum_{i=1}^{r} d_i\,.$$

Now let $\ell = 2$ and $n = 1$. If $c_2 \geqslant 1$ the formula $A_2(N) = A_2(\gcd(2^{c_2}, N))$ is obvious. If $c_2 = 0$ we have to prove $A_2(2) = A_2(1)$, which means $A_2(2) = 1$.

By Theorem 4.2, Eq. (4.3) we have $[\mathbb{Q}(\sqrt{G}) : \mathbb{Q}] = [\mathbb{Q}_4(\sqrt{G}) : \mathbb{Q}_4]$ if G does not contain minus a square in $\mathbb{Q}^\times$. This is the case because the generators of G are strongly 2-independent ($c_2 = 0$ implies that $d_i = 0$ for all i). By Proposition 6.4 (where $m = 2$) we have $[\mathbb{Q}_4(\sqrt{G}) : \mathbb{Q}_4] = 2^r$. We conclude that $A_2(2) = 1$. □

Proposition 7.2. *There are integers M_0, N_0, with $N_0 \mid M_0$, such that for all integers $M, N \geqslant 1$ with $N \mid M$ the adelic failure $B(M, N)$ depends on M and N only through $\gcd(M, M_0)$ and $\gcd(N, N_0)$. More precisely, we have*

$$B(M, N) = B\big(\gcd(M, M_0), \gcd(N, N_0)\big)\,.$$

In particular, keeping the notation of Sections 4 and 5, we may take:

- $N_0 = 2^{n_0}$, *where*

$$n_0 = \max\{3, x+2, d_1+1, \dots, d_r+1\}$$

where x is the d-parameter for the 2-divisibility of the only negative basis element, or -1 if there is no such element.
- $M_0 = \operatorname{lcm}\{N_0, b_1', \dots, b_r'\}$, *where the b_i''s are positive squarefree integers such that $b_i \equiv b_i' \bmod \mathbb{Q}^{\times 2}$ (recall that the b_i's are positive rational numbers).*

Proof. Let M_0 and N_0 be as above and set $n = v_2(N)$. Suppose first that G contains no negative elements: we are in the setup of Theorem 5.1 and Remark 6.1. Since $G \subseteq \mathbb{Q}_+^\times$, we need to compare

$$B(M,N) = \left[\mathbb{Q}_{2^n}\big(\sqrt{H}\big) : \mathbb{Q}_{2^n}\right] \qquad \text{and}$$

$$B\big(\gcd(M,M_0), \gcd(N,N_0)\big) = \left[\mathbb{Q}_{2^e}\big(\sqrt{H}\big) : \mathbb{Q}_{2^e}\right],$$

where $e := \min(n, n_0)$. Notice that the groups H are the same because we have the same sets $\mathcal{S}$ and $\mathcal{C}$ for both failures, and for every $y \in \mathcal{C}$ we have $\sqrt{y} \in \mathbb{Q}_M$ if and only if $\sqrt{y} \in \mathbb{Q}_{(M,M_0)}$. By Proposition 6.4 we easily deduce that $[\mathbb{Q}_{2^n}(\sqrt{H}) : \mathbb{Q}_{2^n}] = [\mathbb{Q}_{2^e}(\sqrt{H}) : \mathbb{Q}_{2^e}]$.

Now suppose that G contains negative elements: we are in the setup of Theorem 5.3 and Remark 6.2. For $B((M,M_0),(N,N_0))$ we find the same case distinction of Remark 6.3 for $B(M,N)$. Again, the sets $\mathcal{S}$, $\mathcal{C}$, and H (as well as $\mathcal{C}'$ and H') are the same in both cases. Notice that $v_2(M_0) = n_0$.

- If $n \leqslant x$, then we have

$$B(M,N) = \left[\mathbb{Q}_{2^u}\big(\sqrt{H}\big) : \mathbb{Q}_{2^n}\right] \qquad \text{and}$$

$$B\big(\gcd(M,M_0), \gcd(N,N_0)\big) = \left[\mathbb{Q}_{2^w}\big(\sqrt{H}\big) : \mathbb{Q}_{2^n}\right],$$

where $u := \min(n+1, v_2(M))$ and $w := \min(v_2((N,N_0)) + 1, v_2((M,M_0)))$. Since $(N,N_0) = 2^n$ and $n_0 \geqslant x+2 \geqslant n$, we easily see that $w = u$, so that $B((M,M_0),(N,N_0)) = B(M,N)$.
- If $n \geqslant x+2$, then $B((M,M_0),(N,N_0)) = [\mathbb{Q}_{2^e}(\sqrt{H}) : \mathbb{Q}_{2^e}]$, where $e = \min(n,n_0)$, so that we can argue as in the case $G \subseteq \mathbb{Q}_+^\times$.
- If $n = x+1$, for all subcases the equality of the two failures follows directly because $v_2((N,N_0)) = n$ as $n \leqslant n_0$.

□

Corollary 7.3. *Let ℓ be a prime number.*

(1) There is an integer c_ℓ (depending only on G and ℓ) such that for all $N \geqslant 1$ with $v_\ell(N) \geqslant c_\ell$ we have $A_\ell(N) = A_\ell(\ell^{c_\ell})$. We may take c_ℓ as in Proposition 7.1. Then the total ℓ-adic failure is given by $\alpha_\ell = A_\ell(\ell^{c_\ell})$.
(2) There are integers M_0, N_0 with $N_0 \mid M_0$ (depending only on G) such that for all N, M with $N \mid M$, $M_0 \mid M$ and $N_0 \mid N$ we have $B(M,N) = B(M_0,N_0)$. We may take M_0, N_0 as in Proposition 7.2. Then the total adelic failure is given by $\beta = B(M_0,N_0)$.

Remark 7.4. *With the notation of Proposition 7.1, if N_ℓ is a multiple of ℓ^{c_ℓ}, then we have*

$$A_\ell(N) = A_\ell\big(\gcd(N, N_\ell)\big) \qquad \text{for all } N \geqslant 1\,.$$

With the notation of Proposition 7.2, if M_0' and N_0' are multiples of M_0 and N_0, respectively, and satisfy $N_0' \mid M_0'$, then we have

$$B(M, N) = B\big(\gcd(M, M_0'), \gcd(N, N_0')\big) \qquad \text{for all } M, N \geqslant 1 \text{ with } N \mid M\,.$$

Theorem 7.5. *There are integers M_0 and N_0 such that, for all integers N, M with $N \mid M$, the Kummer failure $C(M, N)$ depends on M and N only through $\gcd(M, M_0)$ and $\gcd(N, N_0)$. More precisely, we have*

$$C(M, N) = C\big(\gcd(M, M_0), \gcd(N, N_0)\big)\,.$$

In particular, keeping the notation of the previous sections, we may take:

- *$N_0 = \prod_\ell \ell^{c_\ell}$, where $c_\ell = \max_i d_i$ if $\ell \neq 2$, the d_i's being the d-parameters for the ℓ-divisibility of G (notice that $c_\ell = 0$ for all but finitely many primes ℓ), and*

  $$c_2 = \max\{3, d_1 + h_1 + 1, \ldots, d_r + h_r + 1\}\,,$$

  where d_i and h_i are the parameters for the 2-divisibility of G over $\mathbb{Q}_4$.
- *$M_0 = \operatorname{lcm}\{N_0, b_1', \ldots, b_r'\}$, where the b_i''s are positive squarefree integers such that $b_i \equiv b_i' \bmod \mathbb{Q}^{\times 2}$.*

In particular, the total Kummer failure is given by $C_0 = C(M_0, N_0)$.

Proof. By (2.2) we have $C(M, N) = B(M, N) \prod_\ell A_\ell(N)$. Therefore it suffices to combine Propositions 7.1 and 7.2 and to take into account the previous remark. □

8. Examples

In this last section we work out a few examples to illustrate the procedure described in the rest of the article.

Example 8.1. Let $G = \langle 5^4, 7\rangle$. We compute the ℓ-adic failure for all primes ℓ and the adelic failure. For ℓ odd, the basis $\{5^4, 7\}$ is an ℓ-good basis consisting of strongly ℓ-independent elements. Therefore if $\ell \neq 2$ we have $A_\ell(N) = 1$ for all $N \geqslant 1$. For $\ell = 2$, the basis $\{5^4, 7\}$ is 2-good over $\mathbb{Q}(\zeta_4)$ as $5, 7$ are strongly 2-independent. Therefore G has parameters $d_1 = 2$, $d_2 = h_1 = h_2 = 0$, which by Theorem 4.2 gives

$$\Big[\mathbb{Q}_{2^n}\big(G^{1/2^n}\big) : \mathbb{Q}_{2^n}\Big] = 2^{2n-2} \qquad \text{for all } n \geqslant 2\,,$$

and $[\mathbb{Q}(\sqrt{G}) : \mathbb{Q}] = 2$. Hence the 2-adic failure is given as follows, where $n = v_2(N)$:

$$A_2(N) = \begin{cases} 1, & \text{if } n = 0 \\ 2, & \text{if } n = 1 \\ 4, & \text{if } n \geqslant 2. \end{cases}$$

Next we compute the adelic failure. Let $M, N \geqslant 1$ be integers with $N \mid M$. We apply the method outlined in Remark 6.1, and Proposition 6.4. It is trivial that $B(M, N) = 1$ if $n = 0$.

Suppose that $n = 1$ or $n = 2$, so that $\mathcal{S} = \{7\}$. Then we have $H = \langle 7 \rangle$ and so $B(M, N) = 2$ if $28 \mid M$, and $H = \langle 1 \rangle$ so that $B(M, N) = 1$ otherwise. Suppose that $n \geqslant 3$, so that $8 \mid M$ and $\mathcal{S} = \{5, 7\}$. Then we have

- $H = \langle 1 \rangle$ and $B(M, N) = 1$ if $5 \nmid M$ and $7 \nmid M$,
- $H = \langle 5 \rangle$ and $B(M, N) = 2$ if $5 \mid M$ and $7 \nmid M$,
- $H = \langle 7 \rangle$ and $B(M, N) = 2$ if $5 \nmid M$ and $7 \mid M$,
- $H = \langle 5, 7 \rangle$ and $B(M, N) = 4$ if $35 \mid M$.

Example 8.2. Let us compute the adelic failure for the group $G = \langle -5, 7 \rangle$. Let $M, N \geqslant 1$ be such that $N \mid M$ and $v_2(N) \geqslant 1$. Since the d-parameters for the 2-divisibility are both zero, if $v_2(N) = 1$ we have $\mathcal{S} = \{-5, 7\}$, so that

- $H = \langle 1 \rangle$ and $B(M, N) = 1$ if $20 \nmid M$, $28 \nmid M$, and $35 \nmid M$,
- $H = \langle -5 \rangle$ and $B(M, N) = 2$ if $20 \mid M$ and $28 \nmid M$,
- $H = \langle 7 \rangle$ and $B(M, N) = 2$ if $20 \nmid M$ and $28 \mid M$,
- $H = \langle -35 \rangle$ and $B(M, N) = 2$ if $35 \mid M$ and $4 \nmid M$,
- $H = \langle -5, 7 \rangle$ and $B(M, N) = 4$ if $140 \mid M$.

On the other hand, if $v_2(N) \geqslant 2$, then the fourth root of -5 does not lie in $\mathbb{Q}_\infty$ but $\sqrt{5}$ lies in $\mathbb{Q}(\zeta_5)$. Hence $\mathcal{S} = \{5, 7\}$ and since $4 \mid M$ we obtain exactly the same cases as in the previous example for $v_2(N) \geqslant 3$.

Example 8.3. Let us compute the adelic failure for the group $G = \langle 5, -7^8 \rangle$. Let $M, N \geqslant 1$ be such that $N \mid M$ and $n := v_2(N) \geqslant 1$. The d-parameters for the 2-divisibility are $d_1 = 0$ and $d_2 = 3$. If $n \leqslant 3$ then $\mathcal{S} = \{5\}$ and the 2^n-th root of -7^8 yields a root of unity of order 2^{n+1}. Thus we have

$$\mathbb{Q}_{2^n, 2^n} \cap \mathbb{Q}_M = \mathbb{Q}_{2^w}\left(\sqrt{H}\right)$$

where $w = \min(n + 1, v_2(M))$ and $H = \langle 1 \rangle$ if $5 \nmid M$, $H = \langle 5 \rangle$ otherwise. Hence

- $B(M, N) = 1$ if $5 \nmid M$ and $v_2(M) = n$,
- $B(M, N) = 2$ if $5 \mid M$ and $v_2(M) = n$,
- $B(M, N) = 2$ if $5 \nmid M$ and $v_2(M) \geqslant n + 1$,
- $B(M, N) = 4$ if $5 \mid M$ and $v_2(M) \geqslant n + 1$.

If $n = 4$, then $\mathcal{S} = \{5\}$ and the 16-th root of -7^8 yields $\zeta_{32}\sqrt{7}$. Therefore $v_2(M) = 4$ gives

- $H = \langle 1 \rangle$ and $B(M, N) = 1$ if $5 \nmid M$,
- $H = \langle 5 \rangle$ and $B(M, N) = 2$ if $5 \mid M$.

If $v_2(M) \geqslant 5$, then we obtain

- $\langle H, H' \rangle = \langle 1 \rangle$ and $B(M, N) = 1$ if $5 \nmid M$ and $7 \nmid M$,
- $\langle H, H' \rangle = \langle 5 \rangle$ and $B(M, N) = 2$ if $5 \mid M$ and $7 \nmid M$,
- $\langle H, H' \rangle = \langle \zeta_{16} 7 \rangle$ and $B(M, N) = 2$ if $5 \nmid M$ and $7 \mid M$,
- $\langle H, H' \rangle = \langle 5, \zeta_{16} 7 \rangle$ and $B(M, N) = 4$ if $35 \mid M$.

If $n \geqslant 5$ we obtain again the same cases as in Example 8.1 for $n \geqslant 3$.

Example 8.4. We compute the 2-adic and the adelic failure for the group $G = \langle 2, -7^2 \rangle$. Let $N \geqslant 2$ with $n := v_2(N) \geqslant 1$. The parameters for the 2-divisibility of G over $\mathbb{Q}(\zeta_4)$ are $d_1 = 1$, $h_1 = 2$, $d_2 = h_2 = 1$. Then applying formula (4.2) to compute the 2-adic Kummer degrees over $\mathbb{Q}(\zeta_4)$, we find that $A_2(N) = 1$ if $n = 1$, $A_2(N) = 2$ if $n = 2$, and $A_2(N) = 4$ if $n \geqslant 3$.

Let $M \geqslant 1$ be such that $N \mid M$. The d-parameters for the 2-divisibility of G over $\mathbb{Q}$ are $d_1 = 0$ and $d_2 = 1$. Then for $n = 1$ we have $\mathcal{S} = \{2\}$ and, taking into account that the square root of -7^2 yields ζ_4, we obtain that $B(M, N) = 1$ if $2 \parallel M$, $B(M, N) = 2$ if $4 \parallel M$, and $B(M, N) = 4$ if $8 \mid M$.

If $n = 2$ and $4 \parallel M$, then we need to take into account that $\zeta_8\sqrt{14}$ lies in $\mathbb{Q}(\zeta_{28})$. We have $\mathcal{S} = \{2\}$, $H = \langle 1 \rangle$, and we obtain

- $\langle H, H' \rangle = \langle 1 \rangle$ and $B(M, N) = 1$ if $7 \nmid M$,
- $\langle H, H' \rangle = \langle \zeta_4 \cdot 14 \rangle$ and $B(M, N) = 2$ if $7 \mid M$.

If $n = 2$ and $8 \mid M$, then $\mathcal{S} = \{2\}$, $H = \langle 2 \rangle$, and we have

- $\langle H, H' \rangle = \langle 2 \rangle$ and $B(M, N) = 2$ if $7 \nmid M$,
- $\langle H, H' \rangle = \langle 2, \zeta_4 \cdot 7 \rangle$ and $B(M, N) = 4$ if $7 \mid M$.

If $n \geqslant 3$, then $\mathcal{S} = \{2, 7\}$ and, since $\sqrt{2} \in \mathbb{Q}(\zeta_8)$, we have

- $H = \langle 2 \rangle$ and $B(M, N) = 1$ if $7 \nmid M$,
- $H = \langle 2, 7 \rangle$ and $B(M, N) = 2$ if $7 \mid M$.

All these examples have been tested with the SageMath implementation [7].

REFERENCES

[1] DEBRY, C. - PERUCCA, A., *Reductions of algebraic integers*, J. Number Theory, **167** (2016), 259–283.

[2] PALENSTIJN, W. J., *Radicals in arithmetic*, PhD thesis, University of Leiden (2014), available at `https://openaccess.leidenuniv.nl/handle/1887/25833`.

[3] PERUCCA, A., *The order of the reductions of an algebraic integer*, J. Number Theory, **148** (2015), 121–136.

[4] PERUCCA, A. - SGOBBA, P., *Kummer theory for number fields and the reductions of algebraic numbers*, Int. J. Number Theory, **15** (2019), no. 08, pp. 1617–1633.

[5] PERUCCA, A. - SGOBBA, P. - TRONTO, S., *Addendum to: Reductions of algebraic integers [J. Number Theory 167 (2016) 259–283]*, J. Number Theory, **209** (2020), 391–395.

[6] SCHINZEL, A., *Abelian binomials, power residues and exponential congruences*, Acta Arith. **32**(3) (1977) 245–274. Addendum **36** (1980) 101–104; *Andrzej Schinzel Selecta*, Vol. 2 (European Mathematical Society, 2007), pp. 939–970.

[7] TRONTO, S., *Kummer Degrees*, SageMath implementation and documentation available at `https://github.com/sebastianotronto/kummer-degrees`.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF LUXEMBOURG, 6 AV. DE LA FONTE, 4364 ESCH-SUR-ALZETTE, LUXEMBOURG

Email address: `antonella.perucca@uni.lu, pietro.sgobba@uni.lu, sebastiano.tronto@uni.lu`