KUMMER THEORY FOR PRODUCTS OF ONE-DIMENSIONAL TORI
LA THÉORIE DE KUMMER POUR LES PRODUITS DE TORES DE DIMENSION UN.

FLAVIO PERISSINOTTO AND ANTONELLA PERUCCA

ABSTRACT. Let T be a finite product of one-dimensional tori defined over a number field K. We consider the torsion-Kummer extension $K(T[nt], \frac{1}{n}G)$, where n, t are positive integers and G is a finitely generated group of K-points on T. We show how to compute the degree of $K(T[nt], \frac{1}{n}G)$ over K and how to determine whether T is split over such an extension. If $K = \mathbb{Q}$, then we may compute at once the degree of the above extensions for all n and t.

ABSTRACT. Soit T un produit fini de tores de dimension un sur un corps de nombres K. Nous considérons l'extension de torsion-Kummer $K(T[nt], \frac{1}{n}G)$, où n, t sont des entiers strictement positifs et G un groupe de type fini engendré par des K-points de T. Nous montrons comment l'on peut calculer le degré de $K(T[nt], \frac{1}{n}G)$ sur K. Nous montrons également comment déterminer si T est déployé sur une telle extension. Lorsque $K = \mathbb{Q}$, nous pouvons calculer les degrés de toutes les extensions ci-dessus pour tous les n et t, d'un coup.

1. INTRODUCTION

Kummer theory is a topic of significant interest in number theory, and in this paper we investigate it for tori defined over a number field. So let T be a torus defined over a number field K, and fix a finitely generated group G of K-points on T. We study the torsion-Kummer extensions related to G, namely the extensions

$$K\Big(T[m], \frac{1}{n}G\Big)$$

where m, n are positive integers and n divides m.

In [5] the second author considered one-dimensional tori and she proved results on the torsion-Kummer extensions supposing that m, n are powers of some given prime number. In this work we remove the assumption on the parameters and consider more generally products of one-dimensional tori. Our main result is the following:

Theorem 1. *Let T be a finite product of one-dimensional tori defined over a number field K, and fix a finitely generated group G of K-points on T. If m, n are positive integers such that n divides m, then there is an explicit finite procedure to determine whether T is split over $K(T[m], \frac{1}{n}G)$ and to compute the degree of this extension over K and over $T[m]$.*

2010 *Mathematics Subject Classification.* Primary: 20G30; Secondary: 11Y40.
Key words and phrases. tori, one-dimensional tori, Kummer theory, number field.

To prove this theorem we fully describe the procedure mentioned in the statement, see Section 3 for the case of a single one-dimensional torus and Section 4 for the general case. Then in Section 5 we prove the following result:

Theorem 2. *Let T be a finite product of one-dimensional tori defined over $\mathbb{Q}$, and fix a finitely generated group G of $\mathbb{Q}$-points on T. It is possible to compute at once the degree of all extensions $\mathbb{Q}(T[m], \frac{1}{n}G)$, where m, n are positive integers such that n divides m.*

The above result is stated over $\mathbb{Q}$ for simplicity, however one may generalize it to those number fields such that the analogous computations are feasible. For example, by the results in [3] we have the following:

Remark 3. *In Theorem 1 we may compute at once the degree of the torsion-Kummer extensions for all m and n if the splitting field of T is multiquadratic.*

Finally, in Section 6 we present various examples of computations of the degree of torsion-Kummer extensions. Notice that the results about one-dimensional tori from Sections 2 and 3 may be used to study further arithmetic problems.

The challenge is to study Kummer theory for all tori, and in this work we have settled a first important case in higher-dimension.

Acknowledgements. We thank Claus Fieker for helpful discussions.

2. Torsion fields of one-dimensional tori

Fix a number field K and some algebraic closure $\bar{K}$. Let T be a non-split one-dimensional torus over K, and call $T(K)$ the group of K-points. So let T be defined by the equation $x^2 - dy^2 = 1$ for some $d \in K^\times$ which is not a square. Over the splitting field $L = K(\sqrt{d})$ the equation becomes $(x + \sqrt{d}y)(x - \sqrt{d}y) = 1$ thus for every field $L \subseteq F \subseteq \bar{K}$ the map

$$T(F) \hookrightarrow F^\times \qquad (x, y) \mapsto x + \sqrt{d}y \tag{1}$$

is a bijection (the image of $T(K)$ consists of the elements of $L^\times$ whose L/K-norm is 1). The multiplication of $\bar{K}^\times$ induces a group law for T, namely we have

$$(x_1, y_1) * (x_2, y_2) = (x_1x_2 + dy_1y_2, x_1y_2 + x_2y_1)\,. \tag{2}$$

For every positive integer m we let $\zeta_m \in \bar{K}$ be a root of unity of order m and write $\mu_m = \langle \zeta_m \rangle$. Moreover, we call $T[m] \subset T(\bar{K})$ the group of points of order dividing m. By (1) we have the following group isomorphism:

$$\mu_m \to T[m] \qquad \zeta \mapsto \left(\frac{\zeta + \zeta^{-1}}{2}, \frac{\zeta - \zeta^{-1}}{2\sqrt{d}}\right). \tag{3}$$

We set $\mathbb{Q}_m = \mathbb{Q}(\zeta_m)$ and call $\mathbb{Q}_m^+$ the largest totally real subfield of $\mathbb{Q}_m$. Moreover, we use the notation $K_m = K(\zeta_m)$ and $K_m^+ = K \cdot \mathbb{Q}_m^+$. We call $K(T[m])$ the smallest extension of K over which the points of $T[m]$ are defined. We write K_{2^∞}, K_∞ for the union of the fields K_{2^m}, K_m and we similarly define $K(T[2^\infty])$ and $K(T[\infty])$. We clearly have $K(T[1]) = K(T[2]) = K$.

If m is odd, then we have $K(T[2m]) = K(T[m])$ hence to study the torsion fields we may suppose that m is odd or $4 \mid m$.

Proposition 4. *Let $m, n \geqslant 3$ with $n \mid m$. Then we have*

$$K(T[m]) = K_m^+\Big(\frac{\zeta_n - \zeta_n^{-1}}{\sqrt{d}}\Big) = K_m^+ \cdot K(T[n])\,. \tag{4}$$

In particular, $K(T[m])$ is at most quadratic over K_m^+ and we have $L(T[m]) = L_m$. Thus $L \subseteq K(T[m])$ holds if and only if $L \subseteq K_m^+$ or $K_m^+ = K_m$ (for example, it holds if $\zeta_4 \in K$).

Proof. The first assertion implies the others (if $L \subseteq K(T[m])$ and $L \nsubseteq K_m^+$, then we have $K_m^+ = K_m$). By (3) we get $K(T[m]) = K_m^+(\frac{\zeta_m - \zeta_m^{-1}}{\sqrt{d}})$ and this implies the second equality in (4). We conclude because $\frac{\zeta_m - \zeta_m^{-1}}{\zeta_n - \zeta_n^{-1}}$ is a real number contained in $\mathbb{Q}_m$. □

Remark 5. *If $4 \mid m$, then by (4) we have*

$$K(T[m]) = K_m^+(\sqrt{-d})\,. \tag{5}$$

Moreover, if m is odd and w is its squarefree part, then $L \subseteq K(T[m])$ holds if and only if $L \subseteq K(T[w])$ because by (4) the degree of $K(T[m])/K(T[w])$ is odd.

Theorem 6. *Suppose that $\zeta_4 \notin K$ and $4 \mid m$, and write $m = wt2^e$, where wt is odd and w is the squarefree part of wt. Let $r \geqslant 2$ be the largest integer such that $\mathbb{Q}_{2^r}^+ \subseteq K_{4w}^+(\sqrt{-d}) \cap \mathbb{Q}_{2^\infty}$. If $e \leqslant r$, then $L \subseteq K(T[m])$ holds if and only if $L \subseteq K_{4w}^+$ or $\zeta_4 \in K_{4w}^+$. If $e \geqslant r+1$, then $L \subseteq K(T[m])$ holds if and only if $L \subseteq K(T[w2^{r+1}])$ if and only if $L \subseteq K_{w2^{r+1}}^+$ or $\zeta_4 \in K_{w2^{r+1}}^+$.*

Proof. We make repeated use of (5), and by Remark 5 we may assume $t = 1$. If $e \leqslant r$, then $K(T[m]) = K_{4w}^+(\sqrt{-d})$ thus $L \subseteq K_{4w}^+$ or $\zeta_4 \in K_{4w}^+$ implies $L \subseteq K(T[m])$, while if $\sqrt{d}, \zeta_4 \notin K_{4w}^+$, then $K_{4w}^+(\sqrt{d}) \neq K_{4w}^+(\sqrt{-d})$ hence $L \nsubseteq K(T[m])$. Now let $e \geqslant r+1$. If $L \subseteq K_{w2^{r+1}}^+$ or $\zeta_4 \in K_{w2^{r+1}}^+$, then $L \subseteq K(T[w2^{r+1}])$, while if $\sqrt{d}, \zeta_4 \notin K_{w2^{r+1}}^+$, then $K_{w2^{r+1}}^+(\sqrt{d}) \neq K_{w2^{r+1}}^+(\sqrt{-d})$ hence $L \nsubseteq K(T[w2^{r+1}])$. To conclude, we suppose that $L \subseteq K(T[w2^e])$ and prove $L \subseteq K(T[w2^{r+1}])$. The extension $K(T[w2^e])/K_{4w}^+(\sqrt{-d})$ is cyclic and by definition of r its quadratic subextension is $K(T[w2^{s+1}])$, so we are done. □

Example 7. We keep the notation of the above theorem. Let $K = \mathbb{Q}(\sqrt{10}, \gamma_{17}(\zeta_{16} + \zeta_{16}^{-1})\zeta_4)$, where γ_{17} is a generator for the quartic subextension of $\mathbb{Q}(\zeta_{17})/\mathbb{Q}$, and let $d = -7$. If $m = 65 \cdot 2^4$, then we have $r = 3$, $e \geqslant r+1$, and $\zeta_4 \in K_{w2^{r+1}}^+$ hence $L \subseteq K(T[w2^{r+1}])$. We cannot replace r by be the largest integer s such that $\mathbb{Q}_{2^s}^+ \subseteq K \cap \mathbb{Q}_{2^\infty}$ because here $s = 2$ and $e \geqslant s+1$ but we have $L \nsubseteq K(T[w2^{s+1}])$ because $\zeta_4 \notin \mathbb{Q}(\sqrt{2}, (\zeta_{16} + \zeta_{16}^{-1})\zeta_4)$.

3. Kummer theory for a non-split one-dimensional torus

Let T be a non-split one-dimensional torus defined over a number field K, and call L the splitting field. Let G be a finitely generated and torsion-free subgroup of $T(K)$. For all positive integers m, n with $n \mid m$, consider the torsion-Kummer extension $K(T[m], \frac{1}{n}G)$ which is obtained by adding to $K(T[m])$ the coordinates of all points $P \in T(\bar{K})$ such that $nP \in G$. We present an explicit finite procedure to compute the degree of the extension $K(T[m], \frac{1}{n}G)/K$. Notice that for $n = 1$ we are computing the degree of $K(T[m])/K$, thus we can also determine the degree of $K(T[m], \frac{1}{n}G)$ over $K(T[m])$. Also notice that we could remove the assumption that G is torsion-free because, if the torsion subgroup has order t, then we can reduce to the torsion-free case replacing m by $\operatorname{lcm}(m, nt)$.

We refer to [2, Section 2] for the definition and properties of strongly 2-indivisible and strongly 2-independent elements of a number field. Calling $G' \subset L^\times$ the image of G under (1), consider a $\mathbb{Z}$-basis $P_1, \dots, P_r$ for G and its image under (1). Up to replacing this basis of G' in a computable way, see [2, Theorem 14], we may suppose that it is of the form $\xi_i a_i^{2^{\delta_i}}$, where the a_i's are strongly 2-independent elements of $L^\times$, the δ_i's are non-negative integers and the ξ_i's are roots of unity in L of order 2^{h_i} for some non-negative integer h_i such that $h_i = 0$ or $\zeta_{2^{h_i+\delta_i}} \notin L$. If $\zeta_4 \notin K$, then we have $N_{L/K}(a_i) \in \{\pm 1\}$ by [5, proof of Lemma 3.8].

Remark 8. *We have*

$$[K\Big(T[m], \frac{1}{n}G\Big) : K] = \begin{cases} 2[L(\zeta_m, \sqrt[n]{G'}) : L] & \text{if } L \subseteq K(T[m], \frac{1}{n}G) \\ [L(\zeta_m, \sqrt[n]{G'}) : L] & \text{otherwise}. \end{cases}$$

Thus we may reduce to the multiplicative group (and do the computations thanks to [2]*) provided that we can determine whether $L \subseteq K(T[m], \frac{1}{n}G)$. We may suppose that n is a power of 2 because, if n is odd, then the degree of $K(T[m], \frac{1}{n}G)/K(T[m])$ is odd.*

We are left to investigate the following question:

Question 9. *Given $m \geqslant 1$ and $f \geqslant 0$ with $2^f \mid m$, do we have $L \subseteq K(T[m], \frac{1}{2^f}G)$?*

Theorem 10 ([5, Lemmas 3.3 and 3.4])**.** *We have $L \subseteq K\big(\frac{1}{2}G\big)$ if and only if there is some $P \in G$ such that $L \subseteq K\big(\frac{1}{2}P\big)$. This means (identifying P with $P' \in L^\times$) that $\sqrt{P'} \in L$ and $N_{L/K}(\sqrt{P'}) \neq 1$. If a basis of G is given and P exists, then we may take it to be a sum of basis elements.*

If $\zeta_4 \notin K$, then we let $s \geqslant 2$ be the largest integer satisfying $\mathbb{Q}_{2^s}^+ \subseteq K \cap \mathbb{Q}_{2^\infty}$. For $s \geqslant 3$ we call $\mathbb{Q}_{2^s}^-$ the subextension of $\mathbb{Q}_{2^s}$ of relative degree 2 which is neither $\mathbb{Q}_{2^s}^+$ nor $\mathbb{Q}_{2^{s-1}}$. By [5, Theorem 2.3] we know that $K(T[2^s]) = K$ and we have either $K \cap \mathbb{Q}_{2^\infty} = \mathbb{Q}_{2^{s+1}}^-$ and $L = K_{2^{s+1}} = K(T[2^{s+1}])$, or $K \cap \mathbb{Q}_{2^\infty} = \mathbb{Q}_{2s}^+$ and $L = K_{2^s} \not\subseteq K(T[2^\infty])$.

Theorem 11 ([5, Theorems 3.9 and 3.10])**.** *Suppose that $\zeta_4 \notin K$.*

(1) If $L = K_{2^{s+1}} = K(T[2^{s+1}])$, then $L \subseteq K(T[2^v], \frac{1}{2^f}G)$ holds if and only if $v \geqslant s+1$ or

$$\min\{s+1\} \cup \{s+1-h_i : i \in I\} \cup \{\delta_j : j \in J\} \leqslant f$$

where I consists of the indices satisfying $h_i \neq 0$ and J of the indices satisfying $h_j = 0$ and $N_{L/K}(a_j) = -1$.

(2) If $L = K_{2^s} \not\subseteq K(T[2^\infty])$, then $L \subseteq K(T[2^v], \frac{1}{2^f}G)$ holds if and only if there is some $j \in J$ such that $\delta_j \leqslant f$ and

$$h_j + \delta_j \leqslant \max\{v\} \cup \{h_i + \min(f, \delta_i) : i \notin J\} \cup \{h_i + \min(f, \delta_i - 1) : i \in J\}$$

where J is the set of indices j satisfying $N_{L/K}(a_j) = -1$. Thus $L \subseteq K(T[2^\infty], \frac{1}{2^\infty}G)$ holds if and only if $J \neq \emptyset$.

Notice that we could easily investigate Question 9 also if G is not torsion-free, reducing to the torsion-free case by replacing m. By (5), if $\zeta_4 \in K$, then $L \subseteq K\big(T[m], \frac{1}{2^f}G\big)$ holds if and only if either $m \geqslant 3$ or we have $m = 2^f = 2$ and there exists P as in Theorem 10. Now assume $\zeta_4 \notin K$: by Theorem 11 we may determine whether $L \subseteq K(T[2^v], \frac{1}{2^f}G)$ for any integer $v \geqslant f$.

Suppose that $4 \mid m$, and write $m = wt2^v$, where wt is odd and with squarefree part w. By Remark 5 we reduce to the case $t = 1$. If $L \subseteq K(T[4w])$, then we are done. Else, we replace K by $K(T[4w]) = K_{4w}^+(\sqrt{-d})$ and, since again $\zeta_4 \notin K$, we have reduced to the known case where m is a power of 2.

Finally suppose that $4 \nmid m$ hence $f \in \{0, 1\}$. By Theorem 4 we can determine whether $L \subseteq K(T[m])$. If not, then we consider the largest subfield $K' \subseteq K(T[m])$ whose Galois group over K has exponent dividing 2, and we investigate whether $L \subseteq K'(\frac{1}{2}G)$ with Theorem 10.

4. Kummer theory for a product of one-dimensional tori

Let $T = \prod_{i=1}^r T_i$ be a finite product of one-dimensional tori defined over K, and let $L_i = K(\sqrt{d_i})$ be the splitting field of T_i.

Remark 12. *For $m = 1, 2$ we have $K(T[m]) = K$, while for $m \geqslant 3$ by Proposition 4 we have*

$$K(T[m]) = K_m^+\Big(\sqrt{d_1 d_2}, \dots, \sqrt{d_1 d_r}, \frac{\zeta_m - \zeta_m^{-1}}{\sqrt{d_1}}\Big) . \tag{6}$$

We may thus compute the degree of $K(T[m])/K$ (this is an extension of K_m^+ obtained by adding square roots). Moreover, all T_i are isomorphic over $K(T[m])$ because they are either all split over $K(T[m])$ or none is, and they are all split over $K(T[m], \sqrt{d_1})$.

We fix a finitely generated subgroup G of $T(K)$ and consider the group G_i consisting of the coordinates in T_i of the points in G.

Remark 13. *For $m \geqslant 1$ the extension $K(T[m], \frac{1}{2}G)/K(T[m])$ is generated by square-roots of elements of $K(T[m])$. Indeed, if $P = (x, y) \in G_i \setminus T_i[2]$, then by* [5, Lemma 3.1] *we have $K(\frac{1}{2}P) = K(\sqrt{2(x+1)})$.*

Proof of Theorem 1. Avoiding trivial cases we may suppose that either $m \geqslant 3$ or $m = n = 2$. By Remark 14 we reduce to the case in which all G_i are torsion-free. We then reduce to the case where the T_i's are pairwise not K-isomorphic (up to replacing G). Indeed, having a point in the power of a torus amounts to having a group of points on the torus, so we may suppose that $T_i \neq T_j$ for $i \neq j$. Moreover, if w.l.o.g. T_1 and T_2 are K-isomorphic, then we may replace T_2 by T_1 because, if $H_1 \subset T_1(K)$ and H_2 denotes its isomorphic image in T_2, then we have

$$K\Big(T_1[m], \frac{1}{n}H_1\Big) = K\Big(T_2[m], \frac{1}{n}H_2\Big) .$$

For the case $m = n = 2$ see Remark 13, while for $m \geqslant 3$ we reduce to a single one-dimensional torus over $K(T[m])$ by Remark 12, and then we refer to Section 3. $\square$

Remark 14. *If G_i has a torsion group of order t_i, then we may reduce to the case where G is torsion-free provided that we work over the torsion field*

$$K\Big(T_1[\mathrm{lcm}(m, nt_1)], \dots, T_r[\mathrm{lcm}(m, nt_r)]\Big)\,. \tag{7}$$

For $m \geqslant 3$ this field is

$$K^+_{\mathrm{lcm}(m,nt_1,\dots,nt_r)}\Big(\sqrt{d_1 d_2}, \dots, \sqrt{d_1 d_r}, \frac{\zeta_m - \zeta_m^{-1}}{\sqrt{d_1}}\Big)$$

while for $m = n = 2$ it is

$$K^+_{\mathrm{lcm}(2t_1,\dots,2t_r)}\Big(\frac{\zeta_{t_1} - \zeta_{t_1}^{-1}}{\sqrt{d_1}}, \dots, \frac{\zeta_{t_r} - \zeta_{t_r}^{-1}}{\sqrt{d_r}}\Big)\,,$$

so the degree of this torsion field is computable, see Remark 12.

5. Products of one-dimensional tori defined over $\mathbb{Q}$

This section is devoted to the proof of Theorem 2. We write $T = \prod_{i=1}^r T_i$, where T_i is given by the equation $x^2 - d_i y^2 = 1$ for some squarefree $d_i \in \mathbb{Q}$. By Theorem 1 we can deal with finitely many pairs (m, n) so we may suppose $m \geqslant 3$ and we apply Remark 12 to work with T_1 over $\mathbb{Q}(T[m])$.

Remark 15. *We may compute at once the degree of $\mathbb{Q}(T[m])$ for all $m \geqslant 1$, where w.l.o.g. m is odd or $4 \nmid m$. Indeed, by* (6) *we have*

$$\mathbb{Q}(T[m]) = \mathbb{Q}^+_m\Big(\sqrt{-d_1}, \dots, \sqrt{-d_r}\Big) \tag{8}$$

if $4 \mid m$, and

$$\mathbb{Q}(T[m]) = \mathbb{Q}^+_m\Big(\sqrt{-pd_1}, \dots, \sqrt{-pd_r}\Big) \tag{9}$$

if m is odd and it has some prime divisor $p \equiv 3 \bmod 4$. Else, we have

$$[\mathbb{Q}(T[m]) : \mathbb{Q}^+_m] = 2[\mathbb{Q}^+_m(\sqrt{d_1 d_2}, \dots, \sqrt{d_1 d_r}) : \mathbb{Q}^+_m] \tag{10}$$

because $\mathbb{Q}^+_m(\frac{\zeta_m - \zeta_m^{-1}}{\sqrt{d_1}})$ has degree 2 over $\mathbb{Q}^+_m$ and these two number fields have the same quadratic subextensions. We conclude by Lemma 16.

Lemma 16. *If $c, c_1, \dots, c_n$ are rational numbers, then there is an explicit finite procedure to compute at once the degree of $\mathbb{Q}^+_m(\sqrt{c_1}, \dots, \sqrt{c_n})/\mathbb{Q}^+_m$ for all $m \geqslant 1$ and to determine those $m \geqslant 1$ such that $\sqrt{c} \in \mathbb{Q}^+_m(\sqrt{c_1}, \dots, \sqrt{c_n})$.*

Proof. The second assertion follows from the first (applied to $c_1, \dots, c_n$ and $c, c_1, \dots, c_n$ respectively). For the first assertion suppose w.l.o.g. that the degree of $\mathbb{Q}(\sqrt{c_1}, \dots, \sqrt{c_n})$ is 2^n. Then we may compute the requested degree for all m as

$$2^n / \# \Big\{ I \subseteq \{1, \dots, n\} \;:\; \prod_{i \in I} \sqrt{c_i} \in \mathbb{Q}^+_m \Big\}\,.$$

□

The group G is now defined over $\mathbb{Q}(\sqrt{d_1d_2},\dots,\sqrt{d_1d_r})$ because it is generated by points of the form

$$\left(x_j, \frac{y_j\sqrt{d_j}}{\sqrt{d_1}}\right) \qquad \text{where} \quad (x_j,y_j)\in T_j(\mathbb{Q}) \quad \text{for some } j\in\{1,\dots,r\}\,.$$

The splitting field is now $L_m=\mathbb{Q}(\sqrt{d_1d_2},\dots,\sqrt{d_1d_r},T_1[m])$, where $L=\mathbb{Q}(\sqrt{d_1},\dots,\sqrt{d_r})$ is multiquadratic. Calling G' the image of G in $L_m^\times$, by [3] we may compute the degree of all extensions $L_m(\sqrt[n]{G'})/L_m$ at once. We may also suppose G to be torsion free up to replacing m by $\operatorname{lcm}(m,nt)$, where t is the order of the torsion subgroup of G (notice that $t\mid 24$ because L is multiquadratic).

By the above discussion and by Remark 8 to conclude the proof of Theorem 2 it suffices to answer Question 9 for T_1 over the field $\mathbb{Q}(\sqrt{d_1d_2},\dots,\sqrt{d_1d_r})$ for every m and f at once.

We determine those $m\geqslant 3$ such that $\sqrt{d_1}\in\mathbb{Q}(T[m])$, where w.l.o.g. m is odd or $4\mid m$. By Remark 15 the suitable m are those satisfying one of the following conditions:
– $4\mid m$ and there is a subproduct of $(-d_1)\cdots(-d_r)$ whose squarefree part is a negative divisor of m and it is odd if $8\nmid m$;
– m is odd and $p\mid m$ for some prime number $p\equiv 3 \bmod 4$ and d_1 is the squarefree part of a subproduct of $(-pd_1)\cdots(-pd_r)$ times a divisor of m congruent to $1 \bmod 4$;
– all primes $p\mid m$ are such that $p\equiv 1 \bmod 4$ and d_1 equals the squarefree part of a subproduct of $(d_1d_2)\cdots(d_1d_r)$ times a divisor of m.

We determine those $m\geqslant 3$ such that $\sqrt{d_1}\in\mathbb{Q}(T[m],\frac{1}{2}G)$, where w.l.o.g. m is odd or $4\mid m$. This field is the extension of $\mathbb{Q}(T[m])$ obtained by adding, for every generator (a_h,b_h) of G, the element $\sqrt{2(a_h+1)}$. Recall that $a_h\in\mathbb{Q}$, so by Remark 15 we apply Lemma 16 to find the suitable m (if all prime divisors of m are congruent to $1 \bmod 4$, then the condition is $\sqrt{d_1}\in\mathbb{Q}_m^+\Big(\sqrt{d_1d_2},\dots,\sqrt{d_1d_r},\sqrt{2(a_h+1)}\Big)$.

Finally, suppose that $f\geqslant 2$ hence $4\mid m$. We first determine whether $\sqrt{d_1}\in\mathbb{Q}(T[m])$, and we reduce to the case $\sqrt{d_1}\notin\mathbb{Q}(T[m])$. If $8\mid m$, then we also have $\sqrt{d_1}\notin\mathbb{Q}(T[2^\infty m])$. If $8\nmid m$, then $\sqrt{d_1}\in\mathbb{Q}(T[2^\infty m])$ is equivalent to $\sqrt{d_1}\in\mathbb{Q}(T[2m])$ (because $8\mid 2m$) and hence to $\mathbb{Q}(\sqrt{d_1},T[m])=\mathbb{Q}(T[2m])$, so we determine by Lemma 16 which m satisfy this condition.

Consider the multiquadratic field $L=\mathbb{Q}(\sqrt{d_1},\dots,\sqrt{d_r})$ and its extensions L_m. We apply Lemma 17 over L to find, for all m such that $4\mid m$, appropriate generators for the subgroup of $L^\times$ corresponding to G (we use below the notation of the lemma).

By Lemma 17 we need to apply Theorem 11 over $\mathbb{Q}(T[m])$ only for finitely many m because the conditions in this result only depend on the divisibility parameters over K_m and these only vary in a finite set.

Consider the case $\sqrt{d_1}\in\mathbb{Q}(T[2m])$, which implies $f=s=2$ because $\sqrt{d_1}\notin\mathbb{Q}(T[m])$, and apply Theorem 11 (1). Thus $\sqrt{d_1}\in\mathbb{Q}(T[m],\frac{1}{4}G)$ holds if and only if

$$\min(\{3\}\cup\{3-h_i : i\in I\}\cup\{\delta_j : j\in J\})\leqslant 2\,. \tag{11}$$

Now consider the remaining case $\sqrt{d_1} \notin \mathbb{Q}(T[2^\infty m])$. Recall that the 2-adic valuation v of m is at least f. Applying Theorem 11 (2) we have $\sqrt{d_1} \in \mathbb{Q}(T[m], \frac{1}{2^f}G)$ if and only if $J \neq \emptyset$ and (v, f) satisfies, for some $j \in J$, the two conditions $\delta_j \leqslant f$ and

$$(12) \quad h_j + \delta_j \leqslant \max(\{v\} \cup \{h_i + \min(f, \delta_i) : i \notin J\} \cup \{h_i + \min(f, \delta_i - 1) : i \in J\}).$$

If $f \geqslant \max\{\delta_j\}$, then the second condition does not depend on f and we only need to check it for $v < \max\{h_j + \delta_j\}$. If f is small and fixed, then for each j we check the first condition, and then we check the second condition for $v < h_j + \delta_j$. This leaves only finitely many pairs (v, f) to be checked.

This concludes the investigation of Question 9 and also the proof of Theorem 2.

Lemma 17. *Let L be a multiquadratic number field, and let H be a torsion-free subgroup of $L^\times$. We may compute at once, for all $m \geqslant 1$ such that $4 \mid m$, a $\mathbb{Z}$-basis of H whose elements are of the form $\xi_i a_i^{2^{\delta_i}}$, where $\xi_i \in \mu_8 \cap L_m$, $\delta_i \geqslant 0$, and where the elements $a_i \in L_m^\times$ are strongly 2-independent. Moreover, we may suppose that the order of ξ_i equals 2^{h_i} where $h_i = 0$ or $\zeta_{2^{h_i+\delta_i}} \notin L_m$. There is a finite partition of the integers m such that ξ_i, δ_i, a_i are the same for all m in each subset of the partition.*

Proof. We may suppose w.l.o.g. that $\zeta_4 \in L$. Notice that the condition on the parameters h_i can be easily dealt with at the end: if $\zeta_{2^{h_i+\delta_i}} \in L_m$, then we can change a_i by a root of unity to ensure $h_i = 0$. It suffices to determine ξ_i, δ_i, a_i for m odd because these objects are the same for $2^f m$ (strongly 2-independent elements in L_m are still strongly 2-independent in $L_{2^f m}$ by [2, Proposition 9]). By [2, Theorem 14] we determine the requested basis for $m = 1$, calling $A_1, \ldots, A_r$ the involved strongly 2-independent elements. Consider the finite set S consisting of the 2^a-th roots of

$$\zeta_{2^b} \prod_I A_i^{2^{c_i}}$$

where $a, b, c_i \in \{0, 1, 2, 3\}$ and $I \subseteq \{1, \ldots, r\}$. We partition the integers m according to $S \cap L_m$ (we can determine this intersection for all m by [3, Sections 5 and 6]).

Notice that A_i has no 16-th root in L_∞ by [6, Theorem 2] and that $\zeta_{16} \notin L_m$. Thus if we had $b \neq 0$ and $a > 3$, or if $a - c_i > 3$ for some element as above, then that root would not be in L_∞. Moreover, if $b = 0$, then increasing a and c_i by the same amount does not change $S \cap L_m$. So we could remove the condition that $a, b, c_i \leqslant 3$ without altering $S \cap L_m$.

In each subset of the partition we may use the same ξ_i, δ_i, a_i, thus we only need to apply [2, Theorem 14] over L_m for finitely many m. Indeed, the algorithm from [2, Theorem 14] only involves elements of $S \cap L_m$, and it applies with exactly the same steps for m, m' satisfying $S \cap L_m = S \cap L_{m'}$, leading to the same a_i and the same parameters δ_i and h_i. $\square$

6. Examples

Example 18. Consider the torus T over $\mathbb{Q}$ given by $x^2 + 5y^2 = 1$. The splitting field $L = \mathbb{Q}(\sqrt{-5})$ is not contained in $\mathbb{Q}(T[5]) = \mathbb{Q}_5^+(\frac{\zeta_5 - \zeta_5^{-1}}{\sqrt{-5}}) = \mathbb{Q}(\sqrt{5}, \sqrt{\frac{5+\sqrt{5}}{8}})$. The point

$P = (\frac{1}{9}, \frac{4}{9})$ corresponds to $P' = -\big(\frac{2-\sqrt{-5}}{3}\big)^2 \in L^\times$. Since $\sqrt{P'} \notin L$, Theorem 10 implies $L \not\subseteq \mathbb{Q}(T[10], \frac{1}{2}P)$ hence by Remark 8 the degree of $\mathbb{Q}(T[10], \frac{1}{2}P)$ is 4. Alternatively, one may compute that $\mathbb{Q}(T[10])$ has degree 4 and notice by Remark 13 that $\mathbb{Q}(T[10], \frac{1}{2}P) = \mathbb{Q}(T[10], \frac{2}{3}\sqrt{5}) = \mathbb{Q}(T[10])$.

Example 19. Let $K = \mathbb{Q}_4$ and consider the torus $x^2 - 2y^2 = 1$ over K whose splitting field is $L = \mathbb{Q}_8$. The point $P = (3, 2)$ corresponds to $P' = (1 + \sqrt{2})^2$ and we have $\sqrt{P'} \in L$ and $N_{L/K}(1 + \sqrt{2}) = -1$ so by Theorem 10 we get $L \subseteq K(\frac{1}{2}P)$. The point $Q = (\frac{9}{7}, \frac{4}{7})$ corresponds to $Q' = \frac{9+4\sqrt{2}}{7}$ and we have $\sqrt{Q'} \notin \mathbb{Q}(\sqrt{2})$ because $63 + 28\sqrt{2}$ is not a square in $\mathbb{Z}(\sqrt{2})$, so by Theorem 10 we get $L \not\subseteq K(\frac{1}{2}Q)$.

In the following examples we consider a torus $T = T_1 \times T_2$ over a number field K, where for $i = 1, 2$ the torus T_i is defined by $x^2 - d_i y^2 = 1$ for some $d_i \in K$. For $m \geqslant 3$ by (6) we have

$$K(T[m]) = K(T_1[m], \sqrt{d_1 d_2})\,.$$

Example 20. If $d_1 = 5$, $d_2 = 13$, and $K = \mathbb{Q}$, then T_1 and T_2 are isomorphic and not split over $F = \mathbb{Q}(T[8]) = \mathbb{Q}_8^+(\sqrt{-5}, \sqrt{-13})$. To study $\mathbb{Q}(T[8], \frac{1}{8}P)$ for the point $P = ((\frac{2207}{2}, \frac{987}{2}); (\frac{497}{81}, \frac{136}{81}))$ in $T(\mathbb{Q})$ we replace P by the group $H \subset T_1(F)$ generated by $P_1 = (\frac{2207}{2}, \frac{987}{2})$ and $P_2 = (\frac{497}{81}, \frac{136\sqrt{13}}{81\sqrt{5}})$. We check with Theorem 11 that T_1 is split over $F(\frac{1}{8}H)$. We have $\zeta_4 \notin F(T_1[2^\infty])$, and the points P_1, P_2 correspond to a_1^{16}, a_2^4, where $a_1 = \frac{1+\sqrt{5}}{2}$, $a_2 = \frac{2+\sqrt{13}}{3}$ are strongly 2-independent over $F(\sqrt{5})$, and $N_{L/F}(a_1) = N_{L/F}(a_2) = -1$: we conclude because $d_2 = 2 \leqslant 3$, $d_1 = 4$, and $h_1 = h_2 = 0$, so that $h_2 + d_2 \leqslant h_1 + \min(3, d_1 - 1)$.

Example 21. Let $d_1 = 3$, $d_2 = 7$, $K = \mathbb{Q}$, and consider the point $P = ((7, 4); (\frac{4}{3}, \frac{1}{3}))$ in $T(\mathbb{Q})$. We have $F = \mathbb{Q}(T[6]) = \mathbb{Q}(\sqrt{-1}, \sqrt{21})$ and $F(\frac{1}{2}P) = F(\sqrt{2})$ by Remark 13. The degree of $F(\frac{1}{3}P)/F$ is the same as that of $L(\sqrt[3]{H})/L$, where $L = F(\sqrt{3})$ and H is generated by $a = 7 + 4\sqrt{3}$ and $b = (4 + \sqrt{7})/3$. The degree is 9 because a, b, ab, ab^2 are not cubes in $L^\times$. We conclude that $\mathbb{Q}(T[6], \frac{1}{6}P)$ is a number field of degree 72.

Example 22. Let $d_1 = -2$, $d_2 = -3$, $K = \mathbb{Q}$, and consider the point $P = ((-\frac{7}{9}, \frac{4}{9}); (\frac{11}{13}, \frac{4}{13}))$ in $T(\mathbb{Q})$. By Remark 12 we have $\mathbb{Q}(T[98]) = \mathbb{Q}_{49}^+(\sqrt{14}, \sqrt{6})$ hence by Remark 13 we get $\mathbb{Q}(T[98], \frac{1}{2}P) = \mathbb{Q}_{49}^+(\sqrt{14}, \sqrt{6}, \sqrt{13/3})$, which is a number field of degree 168.

Finally, we give two examples where we apply the procedure seen in Section 5.

Example 23. Consider the torus T over $\mathbb{Q}$ defined by $x^2 - 3y^2 = 1$ with splitting field $L = \mathbb{Q}(\sqrt{3})$, and the point $P = (7, 4)$. We determine those m, n such that $L \subseteq \mathbb{Q}(T[m], \frac{1}{n}P)$, with $n \mid m$ and w.l.o.g. $n = 2^f$. For $f = 0, 1$ the suitable m are the multiples of 12, as $\mathbb{Q}(T[m]) = \mathbb{Q}(T[m], \frac{1}{2}P)$. If $f \geqslant 2$, then the suitable m are the multiples of 12 or of 8. Now suppose that $L \not\subseteq \mathbb{Q}(T[m])$ i.e. $12 \nmid m$. The point P corresponds to a^2, where $a = 2 + \sqrt{3} \in L^\times$ is strongly 2-independent in L. If $8 \mid m$, then $a = (\frac{1+\sqrt{3}}{\sqrt{2}})^2 \in L_m$ is the square of an element with norm -1 over $\mathbb{Q}(T[m])$, while a is not a fourth power in L_m for any m by [6, Theorem 2] as $\zeta_4 \notin L$ and $\sqrt{a} \notin L_4$. As seen in Section 5, we must have $L \not\subseteq \mathbb{Q}(T[2^\infty m])$ hence we apply Theorem

11 (2): if $8 \nmid m$, then $J = \emptyset$ and hence $L \not\subseteq \mathbb{Q}(T[m], \frac{1}{4}P)$; if $8 \mid m$, then f and the 2-adic valuation v of m satisfy the given conditions hence $L \subseteq \mathbb{Q}(T[m], \frac{1}{2^f}P)$.

Example 24. Consider the torus $T = T_1 \times T_2$ over $\mathbb{Q}$, where T_1 is defined by $x^2 - 2y^2 = 1$ and T_2 by $x^2 - 3y^2 = 1$. Also consider the point $P = ((\frac{9}{7}, \frac{4}{7}); (7, 4))$ in $T(\mathbb{Q})$. By Remark 12 we replace P by the group $H \subset T_1(\mathbb{Q}(\sqrt{6}))$ generated by $P_1 = (\frac{9}{7}, \frac{4}{7})$ and $P_2 = (7, \frac{4\sqrt{6}}{2})$. We thus determine the positive integers m, n with $n \mid m$ and w.l.o.g. $n = 2^f$ such that the splitting field $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ is contained in $\mathbb{Q}(T[m], \frac{1}{n}H)$. Clearly $\sqrt{2} \in \mathbb{Q}(T[m])$ holds if and only if $8 \mid m$ or $12 \mid m$, and we have $\sqrt{2} \in \mathbb{Q}(T[m], \frac{1}{2}H) = \mathbb{Q}(T[m], \sqrt{14})$ if and only if $8 \mid m$ or $12 \mid m$ or $28 \mid m$. Now suppose $f \geqslant 2$ and $\sqrt{2} \notin \mathbb{Q}(T[m], \frac{1}{2}H)$ hence we only need to consider $f = 2$ and m divisible by 4 and not by $8, 12, 28$. The point P_1 corresponds to some $a \in L^\times$ that is not plus/minus a square, and that is a square in L_m if and only if $\sqrt{7} \in L_m$ (i.e. $28 \mid m$ or $21 \mid m$). The point P_2 corresponds to b^4 for some some $b \in L^\times$ that is not a square in $L_m^\times$ by [6, Theorem 2] because $\zeta_4 \notin \mathbb{Q}(\sqrt{3})$, $b^2 \in \mathbb{Q}(\sqrt{3})$ and $b \notin \mathbb{Q}(\zeta_4, \sqrt{3})$. Moreover, $ab \in L_m^\times$ is not a square, else (for some possibly larger m) a and ab but not b would be squares. Since $\sqrt{2} \in \mathbb{Q}(T[2m]) \setminus \mathbb{Q}(T[m])$ we only need to check (11), which is not satisfied as $I = J = \emptyset$, so we find no further suitable m. We conclude that $L \subseteq \mathbb{Q}(T[m], \frac{1}{n}G)$ holds if and only if $8 \mid m$, or $12 \mid m$, or we have $2 \mid n$ and $28 \mid m$.

References

[1] COHEN, H., *Advanced topics in computational number theory.* Graduate Texts in Mathematics, 193. Springer-Verlag, New York, 2000.

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

[3] PERISSINOTTO, F., PERUCCA, A., *Kummer theory for multiquadratic or quartic cyclic number fields*, preprint 2021 (submitted).

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

[5] PERUCCA, A., *Reductions of one-dimensional tori*, Int. J. Number Theory, **13** (2017), no. 1, 1473–1489.

[6] SCHINZEL, A., *Abelian binomials, power residues and exponential congruences*, Acta Arith. **32** (1977), no. 3, 245–274. Addendum, ibid. **36** (1980),101–104. See also Andrzej Schinzel Selecta Vol.II, European Mathematical Society, Zürich, 2007, 939–970.

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

Email address: `flavio.perissinotto@uni.lu, antonella.perucca@uni.lu`