On the degree of Kummer extensions for commutative algebraic groups

Perissinotto, F.

CHAPTER 3

Kummer theory for products of one-dimensional tori

This Chapter is based on the joint work with Antonella Perucca [PP23], and its main focus is to investigate Kummer theory for products of one-dimensional tori defined over number fields. Our main result is the following:

Theorem 3.0.1. *Let T be a finite product of one-dimensional tori defined over a number field K, and fix a finitely generated subgroup G of $T(K)$. If n, N are positive integers such that n divides N, then there is an explicit finite procedure to determine whether T is split over $K(T[N], \frac{1}{n}G)$ and to compute the degree of this field over K and over $K(T[N])$.*

To prove this theorem we fully describe the procedure mentioned in the statement, see Section 3.2 for the case of a single one-dimensional torus and Section 3.3 for the general case. Then in Section 3.4 we prove the following result:

Theorem 3.0.2. *Let T be a finite product of one-dimensional tori defined over $\mathbb{Q}$, and fix a finitely generated subgroup G of $T(\mathbb{Q})$. There exists an explicit finite procedure to compute at once the degree of all extensions $\mathbb{Q}(T[N], \frac{1}{n}G)/\mathbb{Q}(T[N])$, for all n, N positive integers such that n divides N.*

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 Theorem 2.0.1 we have the following:

Remark 3.0.3. In Theorem 3.0.1 we may compute at once the degree of the torsion-Kummer extensions for all n and N if the splitting field of T is multiquadratic.

Finally, in Section 3.5 we present various examples of computations of the degree of torsion-Kummer extensions. Notice that the results about one-dimensional tori from Sections 3.1 and 3.2 may be used to study further arithmetic problems.

The challenge is to study Kummer theory for all tori, and in this Chapter settle a first important case in higher-dimension.

3.1 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 with splitting field L, and call $T(K)$ the group of K-points. Every such torus is defined by the equation $x^2 - dy^2 = 1$ for some $d \in K^\times$ which is not a square and its splitting field is $L = K(\sqrt{d})$, see for example [Vos98, §4.9]. Over L the above equation becomes $(x + \sqrt{d}y)(x - \sqrt{d}y) = 1$ thus for every field $L \subseteq F \subseteq \bar{K}$ the map

$$T(F) \hookrightarrow F^\times \qquad (x, y) \mapsto x + \sqrt{d}y \tag{3.1}$$

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

$$(x_1, y_1) * (x_2, y_2) = (x_1x_2 + dy_1y_2, x_1y_2 + x_2y_1)\,. \tag{3.2}$$

For every positive integer N we let $\zeta_N \in \bar{K}$ be a root of unity of order N and write $\mu_N = \langle \zeta_N \rangle$. Moreover, we call $T[N] \subset T(\bar{K})$ the group of points of order dividing N. By (3.1) we have the following group isomorphism:

$$\mu_N \to T[N] \qquad \zeta \mapsto \Big(\frac{\zeta + \zeta^{-1}}{2}, \frac{\zeta - \zeta^{-1}}{2\sqrt{d}} \Big)\,. \tag{3.3}$$

We set $\mathbb{Q}_N := \mathbb{Q}(\zeta_N)$ and call $\mathbb{Q}_N^+$ the largest totally real subfield of $\mathbb{Q}_N$. Moreover, we use the notation $K_N := K(\zeta_N)$ and $K_N^+ := K \cdot \mathbb{Q}_N^+$. We call $K(T[N])$ the smallest extension of K over which the points of $T[N]$ are defined. We write K_{2^∞}, K_∞ for the union of the fields K_{2^m}, K_N and we similarly define $K(T[2^\infty])$ and $K(T[\infty])$. We clearly have $K(T[1]) = K(T[2]) = K$. If N is odd, then we have $K(T[2N]) = K(T[N])$ hence to study the torsion fields we may suppose that either N is odd or $4 \mid N$.

Proposition 3.1.1. *Let $N, M \geqslant 3$ with $M \mid N$. Then we have*

$$K(T[N]) = K_N^+ \Big(\frac{\zeta_M - \zeta_M^{-1}}{\sqrt{d}} \Big) = K_N^+ \cdot K(T[M])\,. \tag{3.4}$$

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

Proof. By (3.3) we get $K(T[M]) = K_M^+(\frac{\zeta_M - \zeta_M^{-1}}{\sqrt{d}})$ and this implies the second equality in (3.4). We conclude the proof of (3.4) because $(\zeta_N - \zeta_N^{-1})/(\zeta_M - \zeta_M^{-1})$ is a real number contained in $\mathbb{Q}_N$. If $L \not\subseteq K_N^+$, then $L \subseteq K(T[N])$ holds if and only if $\sqrt{d}$ and $\frac{\zeta_N - \zeta_N^{-1}}{\sqrt{d}}$ generate the same quadratic extension over K_N^+, that means $\zeta_N - \zeta_N^{-1} \in K_N^+$ and hence $K_N^+ = K_N$. □

Remark 3.1.2. If $4 \mid N$, then by (3.4) we have

$$K(T[N]) = K_N^+(\sqrt{-d})\,. \tag{3.5}$$

Moreover, if N is odd and w is its squarefree part, then $L \subseteq K(T[N])$ holds if and only if $L \subseteq K(T[w])$ because by (3.4) the degree of $K(T[N])/K(T[w])$ is odd.

Theorem 3.1.3. *Suppose that $\zeta_4 \notin K$ and $4 \mid N$, and write $N = wt2^e$, where wt is odd and w is the squarefree part of wt. Let $r \geqslant 2$ be the largest integer such that $\mathbb{Q}_{2^r}^+ \subseteq K$. If $e \leqslant r$, then $L \subseteq K(T[N])$ holds if and only if $L \subseteq K_{4w}^+$ or $\zeta_4 \in K_{4w}^+$. If $e \geqslant r+1$, then $L \subseteq K(T[N])$ 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 (3.5), and by Remark 3.1.2 we may assume $t = 1$. Notice that we have $\mathbb{Q}_{w2^e}^+ = \mathbb{Q}_{4w}^+ \cdot \mathbb{Q}_{2^e}^+$. If $e \leqslant r$ then $K(T[N]) = K_{4w}^+(\sqrt{-d}) \cdot \mathbb{Q}_{2^e}^+ = K_{4w}^+(\sqrt{-d})$. Therefore if $L \subseteq K_{4w}^+$ or $\zeta_4 \in K_{4w}^+$, then $L \subseteq K(T[N])$, while if $\sqrt{d}, \zeta_4 \notin K_{4w}^+$, then $K_{4w}^+(\sqrt{d}) \neq K_{4w}^+(\sqrt{-d})$ hence $L \not\subseteq K(T[N])$. Now let $e \geqslant r+1$. Notice that 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 $L \not\subseteq K(T[w2^{r+1}])$. To conclude, suppose that $L \not\subseteq K(T[w2^{r+1}])$ and hence $K \cap \mathbb{Q}_{2^\infty} = \mathbb{Q}_{2^r}^+$. Let $K' = K_{4w}^+(\sqrt{-d})$, so we have $K' \cap \mathbb{Q}_{2^\infty} \subseteq \mathbb{Q}_{2^\infty}^+$ because $\zeta_4, \zeta_{2^{r+1}} - \zeta_{2^{r+1}}^{-1} \notin K'$ and $K' \cap \mathbb{Q}_{2^\infty}$ is at most a quadratic extension of $\mathbb{Q}_{2^r}^+$. Therefore $K' \cdot \mathbb{Q}_{2^\infty}^+ \cap \mathbb{Q}_{2^\infty} = \mathbb{Q}_{2^\infty}^+$ and, as $\zeta_4 \in L \cdot K'$, we deduce that $L \not\subseteq K(T[w2^\infty]) = K' \cdot \mathbb{Q}_{2^\infty}^+$.

□

3.2 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 N, n with $n \mid N$, consider the torsion-Kummer extension $K(T[N], \frac{1}{n}G)$ which is obtained by adding to $K(T[N])$ 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 $K(T[N], \frac{1}{n}G)/K$. Notice that for $n = 1$ we are computing the degree of $K(T[N])/K$, thus we can also determine the degree of $K(T[N], \frac{1}{n}G)$ over $K(T[N])$. Also notice that we could remove the assumption that G is torsion-free because, if the torsion subgroup of G has order t, then we can reduce to the torsion-free case replacing N by $\mathrm{lcm}(N, nt)$. We call $G' \subset L^\times$ the image of G under (3.1).

Remark 3.2.1. We have

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

Thus we may reduce to the multiplicative group (and do the computations thanks to [DP16]) provided that we can determine whether $L\subseteq K(T[N],\frac{1}{n}G)$. We may suppose that n is a power of 2 because, if n is odd, then the degree of $K(T[N],\frac{1}{n}G)/K(T[N])$ is odd.

We are left to investigate the following question:

Question 3.2.2. *Given $N\geqslant 1$ and $m\geqslant 0$ with $2^m\mid N$, do we have $L\subseteq K(T[N],\frac{1}{2^m}G)$?*

Notice that we could easily investigate Question 3.2.2 also if G is not torsion-free, reducing to the torsion-free case by replacing N.

Theorem 3.2.3 ([Per17, 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 its image $P'\in L^\times$ by* (3.1)*, 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 P to be a sum of a subset of basis elements.*

Consider $K':=K(T[4])=K(\sqrt{-d})$ and suppose w.l.o.g. that $\zeta_4\notin K'$. We call $L'=L(\zeta_4)$. We let $s\geqslant 2$ be the largest integer satisfying $\mathbb{Q}_{2^s}^+\subseteq K'$. 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 [Per17, 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 $K'\cap\mathbb{Q}_{2^\infty}=\mathbb{Q}_{2^s}^+$ and $L'=K'_{2^s}\not\subseteq K(T[2^\infty])$.

Consider a $\mathbb{Z}$-basis $P_1,\dots,P_r$ for G and its image under (3.1). Up to replacing this basis of G' in a computable way, see [DP16, 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 [Per17, proof of Lemma 3.8].

Theorem 3.2.4 ([Per17, Theorems 3.9 and 3.10])**.** *With the above notation, suppose that $\zeta_4\notin K'$. Consider the property $L'\subseteq K'(T[2^v],\frac{1}{2^m}G)$ for non-negative integers $v\geqslant m$.*

1. *If $L'=K'_{2^{s+1}}=K(T[2^{s+1}])$, then the property holds if and only if $v\geqslant s+1$ or*

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

   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 the property holds if and only if there is some $j\in J$ such that $\delta_j\leqslant m$ and*

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

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 $J \neq \emptyset$.

We conclude this section by answering Question 3.2.2. By (3.5), if $\zeta_4 \in K'$ and $L \not\subseteq K(T[N])$, then $4 \nmid N$ hence $L \subseteq K\big(T[N], \frac{1}{2^m}G\big)$ holds if and only if $m = 1$ and there exists P as in Theorem 3.2.3 with base field $K(T[N])$. Now assume $\zeta_4 \notin K'$: by Theorem 3.2.4 we may determine whether $L \subseteq K(T[2^v], \frac{1}{2^m}G)$ holds for any integer $v \geqslant \max(2, m)$, as this is equivalent to $L' \subseteq K'(T[2^v], \frac{1}{2^m}G)$.

Suppose that $4 \mid N$, and write $N = wt2^v$, where wt is odd and with squarefree part w. By Remark 3.1.2 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 N is a power of 2.

Finally suppose that $4 \nmid N$ hence $m \in \{0, 1\}$. By Proposition 3.1.1 we can determine whether $L \subseteq K(T[N])$. If not, then we consider the largest subfield $F \subseteq K(T[N])$ whose Galois group over K has exponent dividing 2, and we investigate whether $L \subseteq F(\frac{1}{2}G)$ with Theorem 3.2.3.

3.3 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 a number field K, and let $L_i = K(\sqrt{d_i})$ be the splitting field of T_i.

Remark 3.3.1. For $N = 1, 2$ we have $K(T[N]) = K$, while for $N \geqslant 3$ by Proposition 3.1.1 we have

$$K(T[N]) = K^+_N\Big(\sqrt{d_1d_2}, \ldots, \sqrt{d_1d_r}, \frac{\zeta_N - \zeta_N^{-1}}{\sqrt{d_1}}\Big). \tag{3.6}$$

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

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 3.3.2. For $N \geqslant 1$ the extension $K(T[N], \frac{1}{2}G)/K(T[N])$ is generated by square-roots of elements of $K(T[N])$. Indeed, if $P = (x, y) \in G_i \backslash T_i[2]$, then by [Per17, Lemma 3.1] we have $K(\frac{1}{2}P) = K(\sqrt{2(x + 1)})$.

Proof of Theorem 3.0.1. Avoiding trivial cases we may suppose that either $N \geqslant 3$ or $N = n = 2$. By Remark 3.3.3 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

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

For the case $N = n = 2$ see Remark 3.3.2, while for $N \geqslant 3$ we reduce to a single one-dimensional torus over $K(T[N])$ by Remark 3.3.1, and then we refer to Section 3.2. □

Remark 3.3.3. 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

$$K\Big(T_1[\mathrm{lcm}(N, nt_1)], \dots, T_r[\mathrm{lcm}(N, nt_r)]\Big). \tag{3.7}$$

For $N \geqslant 3$ this field is

$$K^+_{\mathrm{lcm}(N, nt_1, \dots, nt_r)}\Big(\sqrt{d_1d_2}, \dots, \sqrt{d_1d_r}, \frac{\zeta_N - \zeta_N^{-1}}{\sqrt{d_1}}\Big)$$

while for $N = n = 2$ 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, similarly to Remark 3.3.1.

Remark 3.3.4. For every i, let n_i be a positive integer dividing N, and call n their least common multiple. Then the compositum of the fields $K(T_i[N], \frac{1}{n_i}G_i)$ equals $K(T[N], \frac{1}{n}G')$, where G' is any finitely generated subgroup of $T(K)$ whose points have coordinates in T_i that form the group $G'_i = \frac{n}{n_i}G_i$.

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

This section is devoted to the proof of Theorem 3.0.2. We write $T = \prod_{i=1}^r T_i$, where T_i is given by the equation $x^2 - d_iy^2 = 1$ for some squarefree $d_i \in \mathbb{Q}$. By Theorem 3.0.1 we can deal with finitely many pairs (N, n) so we may suppose $N \geqslant 3$ and we apply Remark 3.3.1 to work with T_1 over $\mathbb{Q}(T[N])$.

Remark 3.4.1. We may compute at once the degree of $\mathbb{Q}(T[N])$ for all $N \geqslant 1$, where w.l.o.g. N is odd or $4 \mid N$. Indeed, by (3.6) we have

$$\mathbb{Q}(T[N]) = \mathbb{Q}^+_N\Big(\sqrt{-d_1}, \dots, \sqrt{-d_r}\Big) \tag{3.8}$$

if $4 \mid N$ since $(\zeta_N - \zeta_N^{-1}) \cdot \sqrt{-1} \in \mathbb{Q}^+_N$, and

$$\mathbb{Q}(T[N]) = \mathbb{Q}^+_N\Big(\sqrt{-pd_1}, \dots, \sqrt{-pd_r}\Big) \tag{3.9}$$

if N is odd and it has some prime divisor $p \equiv 3 \bmod 4$, since $(\zeta_N - \zeta_N^{-1}) \cdot \sqrt{-p} \in \mathbb{Q}_N^+$. Else, we have

$$[\mathbb{Q}(T[N]) : \mathbb{Q}_N^+] = 2[\mathbb{Q}_N^+(\sqrt{d_1 d_2}, \dots, \sqrt{d_1 d_r}) : \mathbb{Q}_N^+]. \tag{3.10}$$

Indeed, in this last case the field $\mathbb{Q}_N^+(\frac{\zeta_N - \zeta_N^{-1}}{\sqrt{d_1}})$ has degree 2 over the field $\mathbb{Q}_N^+$ and their exponents over $\mathbb{Q}$ differ by a factor 2. Thus the former field is not contained in a compositum of the latter with a multiquadratic field. We conclude by Lemma 3.4.2.

Lemma 3.4.2. *If $c, c_1, \dots, c_n$ are rational numbers, then there is an explicit finite procedure to compute at once the degree of $\mathbb{Q}_N^+(\sqrt{c_1}, \dots, \sqrt{c_n})/\mathbb{Q}_N^+$ for all $N \geqslant 1$ and to determine those $N \geqslant 1$ such that $\sqrt{c} \in \mathbb{Q}_N^+(\sqrt{c_1}, \dots, \sqrt{c_n})$.*

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 N as

$$\frac{2^n}{\#\left\{ I \subseteq \{1, \dots, n\} \ : \ \prod_{i \in I} \sqrt{c_i} \in \mathbb{Q}_N^+ \right\}}. \tag{3.11}$$

Given a squarefree positive integer z, it is a standard fact (see for example [Was97, Ch. 2]) that $\sqrt{z} \in \mathbb{Q}_N$ if and only if $m_z \mid N$, where $m_z = z$ if $z \equiv 1 \pmod 4$ and $m_z = 4z$ otherwise. Therefore we can compute the denominator of (3.11) at once for all N. □

We work now over the base field $K = \mathbb{Q}(\sqrt{d_1 d_2}, \dots, \sqrt{d_1 d_r})$. As each T_i is split over $L = K(\sqrt{d_1}) = \mathbb{Q}(\sqrt{d_1}, \dots, \sqrt{d_n})$, the torus T over the field K is isomorphic to T_1^r and has splitting field L. The image of the group G under this isomorphism is generated by points of the form

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

We may suppose that the image of G is torsion free up to replacing N by $\operatorname{lcm}(N, nt)$, where t is the order of its torsion subgroup (notice that $t \mid 24$ because L is multiquadratic). Calling G' the image of this group in $L_N^\times$, by Theorem 2.0.1 we may compute the degree of all extensions $L_N(\sqrt[n]{G'})/L_N$ at once.

Notice that $K(T_1[N]) = \mathbb{Q}(T[N])$ for $N \geqslant 3$. By the above discussion and by Remark 3.2.1, to conclude the proof of Theorem 3.0.2 it suffices to answer Question 3.2.2 for T_1 over the field K for every N and m at once.

We first determine those $N \geqslant 3$ such that $\sqrt{d_1} \in \mathbb{Q}(T[N])$, where without loss of generality N is odd or $4 \mid N$. By Remark 3.4.1 the suitable N are those for which d_1 is the squarefree part of:

- a subproduct of $(-d_1) \cdots (-d_r)$ times a positive divisor of N (respectively, an odd positive divisor of N) if $8 \mid N$ (respectively, if $4 \mid N$ but $8 \nmid N$);

- a subproduct of $(-pd_1)\cdots(-pd_r)$ times a positive divisor of N congruent to $1 \bmod 4$, if N is odd and $p \mid N$ holds for some prime number $p \equiv 3 \bmod 4$;
- a subproduct of $(d_1d_2)\cdots(d_1d_r)$ times a positive divisor of N, if all primes $p \mid N$ are such that $p \equiv 1 \bmod 4$.

We now determine those $N \geqslant 3$ such that $\sqrt{d_1} \in \mathbb{Q}(T[N], \frac{1}{2}G)$, where w.l.o.g. N is odd or $4 \mid N$. By Remark 3.3.2, this field is the extension of $\mathbb{Q}(T[N])$ 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 3.4.1 we can apply Lemma 3.4.2 to find the suitable N. Notice that, if all prime divisors of N are congruent to $1 \bmod 4$, then the condition is

$$\sqrt{d_1} \in \mathbb{Q}_N^+\Big(\sqrt{d_1d_2}, \ldots, \sqrt{d_1d_r}, \sqrt{2(a_h+1)}\Big).$$

Finally, suppose that $m \geqslant 2$ hence $4 \mid N$. We first determine whether $\sqrt{d_1} \in \mathbb{Q}(T[N])$, and we reduce to the case $\sqrt{d_1} \notin \mathbb{Q}(T[N])$. If $8 \mid N$, then we also have $\sqrt{d_1} \notin \mathbb{Q}(T[2^\infty N])$, as for every positive integer t the maximal field of exponent 2 over $\mathbb{Q}$ contained in $\mathbb{Q}(T[2^tN])$ is the same. If $8 \nmid N$, then $\sqrt{d_1} \in \mathbb{Q}(T[2^\infty N])$ is equivalent to $\sqrt{d_1} \in \mathbb{Q}(T[2N])$ (because $8 \mid 2N$) and hence to $\mathbb{Q}(\sqrt{d_1}, T[N]) = \mathbb{Q}(T[2N])$, so we can determine by Lemma 3.4.2 which N satisfy this condition.

Consider the multiquadratic field $L = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_r})$ and its extensions L_N. We apply Lemma 3.4.3 over L to find, for all N such that $4 \mid N$, appropriate generators for the subgroup of $L^\times$ corresponding to G (we use below the notation of the lemma). Lemma 3.4.3 provides a finite partition of the integers N for which the divisibility parameters of the group G' in L_N stay the same in each subset of the partition. Therefore we need to apply Theorem 3.2.4 over $\mathbb{Q}(T[N])$ only for finitely many N.

Consider the case $\sqrt{d_1} \in \mathbb{Q}(T[2N])$ and hence $8 \nmid N$ and $m = 2$. We can apply Theorem 3.2.4 (1) to T_1 over $\mathbb{Q}(T[N])$, noticing that $s = 2$ because $\sqrt{d_1} \notin \mathbb{Q}(T[N])$. Thus $\sqrt{d_1} \in \mathbb{Q}(T[N], \frac{1}{4}G)$ holds if and only if

$$\min(\{3\} \cup \{3 - h_i : i \in I\} \cup \{\delta_j : j \in J\}) \leqslant 2\,. \tag{3.12}$$

Now consider the remaining case $\sqrt{d_1} \notin \mathbb{Q}(T[2^\infty N])$. Recall that the 2-adic valuation v of N is at least m. Applying Theorem 3.2.4 (2) to T_1 over $\mathbb{Q}(T[N])$ we have $\sqrt{d_1} \in \mathbb{Q}(T[N], \frac{1}{2^m}G)$ if and only if $J \neq \emptyset$ and (v, m) satisfies, for some $j \in J$, the two conditions $\delta_j \leqslant m$ and

$$\begin{aligned} h_j + \delta_j \leqslant \max(\{v\} &\cup \{h_i + \min(m, \delta_i) : i \notin J\} \\ &\cup \{h_i + \min(m, \delta_i - 1) : i \in J\}). \end{aligned}$$

If $m \geqslant \max\{\delta_j\}$, then the second condition does not depend on m and we only need to check it for $v < \max\{h_j + \delta_j\}$. If m 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, m) to be checked.

This concludes the investigation of Question 3.2.2 and also the proof of Theorem 3.0.2.

Lemma 3.4.3. *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 $N \geqslant 1$ such that $4 \mid N$, a $\mathbb{Z}$-basis of H whose elements are of the form $\xi_i a_i^{2^{\delta_i}}$, where $\xi_i \in \mu_8$, $\delta_i \geqslant 0$, and where the elements $a_i \in L_N^\times$ are strongly 2-independent. Moreover, we may suppose that the order of ξ_i equals 2^{h_i} where $h_i = 0$ or $\zeta_{2^{h_i+\delta_i}} \notin L_N$. There is a finite partition of the integers N such that ξ_i, δ_i, a_i are the same for all N in each subset of the partition.*

Proof. As $4 \mid N$, we may suppose w.l.o.g. that $\zeta_4 \in L$. Notice that, up to refining the partition in the end, the condition on the parameters h_i can be easily dealt with: if $\zeta_{2^{h_i+\delta_i}} \in L_N$, 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 N odd because these objects are the same for $2^m N$ (strongly 2-independent elements in L_N are still strongly 2-independent in $L_{2^m N}$ by [DP16, Proposition 9]).

By [DP16, Theorem 14] we may determine the requested basis for $N = 1$, calling $A_1, \dots, A_r$ the involved strongly 2-independent elements. Consider the finite set S consisting of the 2^a-th roots of

$$\zeta_{2^b} \prod_I A_i^{2^{c_i}} \tag{3.13}$$

where $I \subseteq \{1, \dots, r\}$ and a, b, c_i are non-negative integers such that $b \in \{0, 1, 2, 3\}$ and a and c_i satisfy the following restrictions:

- $a \leqslant 3$ and $c_i < a$ for all i, if $b = 0$;
- $a + b \leqslant 6$ and $0 < a - c_i \leqslant 3$ for all i, if $b \neq 0$.

We define a partition of the integers N such that the elements belonging to the same subset of the partition have the same intersection $S \cap L_N$ (we can determine this intersection for all N as seen in Sections 2.4 and 2.5). Notice that $\zeta_{16} \notin L_N$ and that no product $\prod_{i \in J} A_i$ for any non-empty $J \subseteq \{1, \dots, r\}$ has a 16-th root in L_∞ by Theorem 1.0.3. Thus if for some element of the form (3.13) we have $a - c_i > 3$ for some $i \in I$, then its 2^a-th root is not in L_∞. Moreover, if $c_i \geqslant a$ for some i, we can reduce to the product over $I \setminus \{i\}$. If $b = 0$, then increasing a and all c_i by the same amount does not change $S \cap L_N$. If $b \neq 0$, the root of (3.13) is equal to

$$\zeta_{2^{a+b}} \prod_I \sqrt[2^{a-c_i}]{A_i}.$$

If this element belongs to L_N for some N, then $L_N(\prod_I \sqrt[2^{a-c_i}]{A_i}) = L_N(\zeta_{2^{a+b}})$ is an extension of degree at most $2^{\max_i(a-c_i)}$ of L_N, hence $a + b \leqslant 3 + \max_i(a - c_i) \leqslant 6$. Therefore we can lift the restrictions above without changing the defined partition.

In each subset of the partition we may use the same ξ_i, δ_i, a_i, thus we only need to apply [DP16, Theorem 14] over L_N for finitely many N. Indeed, the algorithm from [DP16, Theorem 14] only involves elements of $S \cap L_N$, and it applies with exactly the same steps for N, N' satisfying $S \cap L_N = S \cap L_{N'}$, leading to the same a_i and the same parameters δ_i and h_i. □

3.5 Examples

Example 3.5.1. 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

$$\mathbb{Q}(T[5]) = \mathbb{Q}_5^+\left(\frac{\zeta_5 - \zeta_5^{-1}}{\sqrt{-5}}\right) = \mathbb{Q}\left(\sqrt{5}, \sqrt{\frac{5+\sqrt{5}}{8}}\right).$$

The point $P = (\frac{1}{9}, \frac{4}{9})$ corresponds to $P' = -(\frac{2-\sqrt{-5}}{3})^2 \in L^\times$. Since $\sqrt{P'} \notin L$, Theorem 3.2.3 implies $L \not\subseteq \mathbb{Q}(T[10], \frac{1}{2}P)$ hence by Remark 3.2.1 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 3.3.2 that $\mathbb{Q}(T[10], \frac{1}{2}P) = \mathbb{Q}(T[10], \frac{2}{3}\sqrt{5}) = \mathbb{Q}(T[10])$.

Example 3.5.2. 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 3.2.3 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 3.2.3 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 $N \geqslant 3$ by (3.6) we have

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

Example 3.5.3. If $d_1 = 5$, $d_2 = 13$, and $K = \mathbb{Q}$, then by Remark 3.3.1 the tori T_1 and T_2 are isomorphic and not split over $F = \mathbb{Q}(T[8]) = \mathbb{Q}_8^+(\sqrt{-5}, \sqrt{-13})$. We call L the splitting field of T over F. 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 3.2.4 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 $\delta_2 = 2 \leqslant 3$, $\delta_1 = 4$, and $h_1 = h_2 = 0$, so that $h_2 + \delta_2 \leqslant h_1 + \min(3, \delta_1 - 1)$.

Example 3.5.4. 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 3.3.2. 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 3.5.5. Let $d_1 = -2$, $d_2 = -3$, $K = \mathbb{Q}$, and consider $P = ((-\frac{7}{9}, \frac{4}{9}); (\frac{11}{13}, \frac{4}{13}))$ in $T(\mathbb{Q})$. By Remark 3.3.1 we have $\mathbb{Q}(T[98]) = \mathbb{Q}_{49}^+(\sqrt{14}, \sqrt{6})$ hence by Remark 3.3.2 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 3.4.

Example 3.5.6. 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 N, n such that $L \subseteq \mathbb{Q}(T[N], \frac{1}{n}P)$, with $n \mid N$ and w.l.o.g. $n = 2^m$. Notice first that $L \subseteq \mathbb{Q}(T[N])$ holds if and only if $12 \mid N$. Therefore for $m = 0, 1$ the suitable N are the multiples of 12, as $\mathbb{Q}(T[N]) = \mathbb{Q}(T[N], \frac{1}{2}P)$. If $m \geqslant 2$, we show that the suitable N are the multiples of 12 or of 8. Suppose in fact that $L \not\subseteq \mathbb{Q}(T[N])$ i.e. $12 \nmid N$. The point P corresponds to a^2, where $a = 2 + \sqrt{3} \in L^\times$ is strongly 2-independent in L. If $8 \mid N$, then $a = (\frac{1+\sqrt{3}}{\sqrt{2}})^2 \in L_N$ is the square of an element with norm -1 over $\mathbb{Q}(T[N])$, while a is not a fourth power in L_N for any N by Theorem 1.0.3 because $\zeta_4 \notin L$ and $\sqrt{a} \notin L_4$. As seen in Section 3.4, we must have $L \not\subseteq \mathbb{Q}(T[2^\infty N])$ hence we apply Theorem 3.2.4 (2): if $8 \nmid N$, then $J = \emptyset$ and hence $L \not\subseteq \mathbb{Q}(T[N], \frac{1}{4}P)$; if $8 \mid N$, then m and the 2-adic valuation v of N satisfy the given conditions hence $L \subseteq \mathbb{Q}(T[N], \frac{1}{2^m}P)$.

Example 3.5.7. 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 3.3.1 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 $P_2 = (7, 2\sqrt{6})$. We thus determine the positive integers N, n with $n \mid N$ and w.l.o.g. $n = 2^m$ such that the splitting field $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ is contained in $\mathbb{Q}(T[N], \frac{1}{n}H)$. Clearly $\sqrt{2} \in \mathbb{Q}(T[N])$ holds if and only if $8 \mid N$ or $12 \mid N$, and we have $\sqrt{2} \in \mathbb{Q}(T[N], \frac{1}{2}H) = \mathbb{Q}(T[N], \sqrt{14})$ if and only if $8 \mid N$ or $12 \mid N$ or $28 \mid N$. Now suppose $m \geqslant 2$ and $\sqrt{2} \notin \mathbb{Q}(T[N], \frac{1}{2}H)$. Hence we only need to consider $m = 2$ and N divisible by 4 and not by $8, 12, 28$. The point P_1 corresponds to some $a \in L^\times$ that is not plus or minus a square, and that is a square in L_N if and only if $\sqrt{7} \in L_N$ (i.e. $28 \mid N$ or $21 \mid N$), as $\frac{9}{7} + \frac{4\sqrt{2}}{7} = \frac{(2\sqrt{2}+1)^2}{7}$. The point P_2 corresponds to b^4 for $b = \frac{\sqrt{2}}{2} + \frac{\sqrt{6}}{2} \in L^\times$ that is not a square in $L_N^\times$ by Theorem 1.0.3 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, $ab \in L_N^\times$ is not a square, else (for some possibly larger N) a and ab but not b would be squares. Since $\sqrt{2} \in \mathbb{Q}(T[2N]) \setminus \mathbb{Q}(T[N])$ we only need to check (3.12), which is not satisfied as $I = J = \emptyset$, so we find no further suitable N. We conclude that $L \subseteq \mathbb{Q}(T[N], \frac{1}{n}G)$ holds if and only if $8 \mid N$, or $12 \mid N$, or we have $2 \mid n$ and $28 \mid N$.