Radicals in arithmetic

Palenstijn, W.J.

Chapter 4

Computing radical field degrees

4.1 Introduction

One application of entanglement as we defined it in the previous chapter is computing degrees of radical field extensions of the rationals, e.g., the degree of the field $\mathbf{Q}(\zeta_{12}, \sqrt[6]{6}, \sqrt[4]{-9})$ over $\mathbf{Q}$.

Radical expressions like $\mathbf{Q}(\sqrt[16]{-4})$ do not define a unique field: there are multiple choices for roots, and the fields they generate may not be equal. If we add sufficiently many roots of unity, then the generated field *is* uniquely defined, since all choices for each root differ by a root of unity. In this chapter we assume that our radical fields contain enough roots of unity, as made precise in the following Question.

Question 4.1. *Let $c_1, \ldots, c_k$ be non-zero integers, and $a_1, \ldots, a_k$ be integers greater than 1. How do we efficiently compute the degree over $\mathbf{Q}$ of*

$$K = \mathbf{Q}(\mu_{a_1}, \sqrt[a_1]{c_1}, \ldots, \mu_{a_k}, \sqrt[a_k]{c_k})?$$

Unfortunately, this question is (very likely) difficult to answer. Suppose we take only a single root, $\sqrt[d]{2}$, with d the product of two large — and unknown — primes p and q. Then K is $\mathbf{Q}(\mu_d, \sqrt[d]{2})$ with degree $d\varphi(d)$. Then obtaining the value of $d\varphi(d) = d(p-1)(q-1) = d(d+1-(p+q))$ allows us to easily solve p and q from the equations $p+q = d+1-\varphi(d)$ and $pq = d$. Answering Question 4.1 would therefore let us factor d, which is presumed to be hard.

We will instead give an algorithm answering a modified question:

Theorem 4.2. *There is a polynomial time algorithm that given non-zero integers $c_1, \ldots, c_k$, and $a_1, \ldots, a_k$ integers greater than 1, computes the degree of K over $\mathbf{Q}(\mu_d)$, where d is the least common multiple of $a_1, \ldots a_k$, and K is defined as*

$$K = \mathbf{Q}(\mu_{a_1}, \sqrt[a_1]{c_1}, \ldots, \mu_{a_k}, \sqrt[a_k]{c_k}).$$

This algorithm will be stated (proving the theorem) in Section 4.4, combining results from Sections 4.2 and 4.3.

Following Chapter 2, the basic ingredients will consist of computing an index of abelian groups, and the order of an entanglement group.

To this end, define the (Galois) radical extension B of $\mathbf{Q}^*$ as follows:

$$B = \langle \mathbf{Q}^*, \mu_d, \sqrt[a_i]{c_i} : i \in \{1, \ldots, k\} \rangle \subset \bar{\mathbf{Q}}^*.$$

Let $E(B)$ be the entanglement group of B with the action of the absolute Galois group G of $\mathbf{Q}$, as defined by Definition 2.26. In Section 4.4 we will prove and use the following proposition.

Proposition 4.3. *With notation as above, the following equality holds:*

$$[K : \mathbf{Q}(\mu_d)] = \frac{[B : \mathbf{Q}^* \mu_d]}{\#E(B)}$$

The next two sections cover the computation of the factors in this fraction.

4.2 Coprime bases

We start by computing the index $[B : \mathbf{Q}^* \mu_d]$ of abelian groups. This is essentially a matter of $\mathbf{Z}$-linear algebra computation, once we have identified a basis to work with. Factoring all involved numbers into primes would suffice, but is computationally prohibitive. A suitable basis is provided by the following theorem due to D.J. Bernstein.

Theorem 4.4. *(D.J. Bernstein, [3, 4]) There is an algorithm with (up to* log *factors) linear run time that given a finite set $X \subset \mathbf{Z}_{>0}$, computes a set $\mathcal{P} \subset \mathbf{Z}_{>1}$ of pairwise coprime positive integers, none of which are perfect powers, as well as a factorization of each element of X as a product of elements of $\mathcal{P}$.*

We call a set $\mathcal{P}$ that satisfies these properties a *reduced coprime basis* for X. In this chapter, we take $\mathcal{P}$ to be the reduced coprime basis of the set consisting of 2, d, all a_i and all c_i. Define M to be the abelian group

$$M = \langle \mathbf{Q}^*, \zeta_{2d}, \sqrt[d]{p} : p \in \mathcal{P} \rangle / \mathbf{Q}^*.$$

Lemma 4.5. *Let d, $\mathcal{P}$ and M be as above. Then the abelian group M is a free (multiplicative) $\mathbf{Z}/d\mathbf{Z}$-module with basis $\{\zeta_{2d}, \sqrt[d]{p} : p \in \mathcal{P}\}$.*

Proof. The $\mathbf{Z}$-module M has exponent d, so it is a $\mathbf{Z}/d\mathbf{Z}$-module, and the set $\{\zeta_{2d}, \sqrt[d]{p} : p \in \mathcal{P}\}$ is clearly a generating set.

To show they form a basis, suppose a linear combination $\zeta_{2d}^{e_\zeta} \prod_{p \in \mathcal{P}} (\sqrt[d]{p})^{e_p} = x$ is an element of $\mathbf{Q}^*$. Taking the dth power, we find $\prod_{p \in \mathcal{P}} p^{e_p}$ equals $(-1)^{e_\zeta} x^d$.

Since the right-hand side is plus or minus a d-th power, the order of all prime factors of the right-hand side is a multiple of d. Since all $p \in \mathcal{P}$ are pairwise coprime and no perfect powers, this implies the exponents e_p are multiples of d too.

We obtain that $\prod_{p\in\mathcal{P}}(\sqrt[d]{p})^{e_p}$ is an element of $\mathbf{Q}$, so $\zeta_{2d}^{e_\zeta}$ is also in $\mathbf{Q}$, from which we see that e_ζ is also a multiple of d. This shows that the set $\{\zeta_{2d}, \sqrt[d]{p} : p \in \mathcal{P}\}$ is $\mathbf{Z}/d\mathbf{Z}$-linearly independent. □

Determining the index $[B : \mathbf{Q}^*\mu_d]$ can be conveniently done via M if every $|c_i|$ can be factored over $\mathcal{P}$. Specifically, define $s_i \in \{0, 1\}$ and $a_{p,i} \in \mathbf{Z}$ such that $c_i = (-1)^{s_i} \prod_{p\in\mathcal{P}} p^{e_{p,i}}$.

Let $\psi : M \longrightarrow (\mathbf{Z}/d\mathbf{Z})^{1+\#\mathcal{P}}$ be the $\mathbf{Z}/d\mathbf{Z}$-module isomorphism that sends $m \in M$ to its sequence of coordinates on the basis given by the lemma.

The coordinate vectors of the generators of $B/\mathbf{Q}^*$ are given by:

$$\begin{aligned} \psi(\zeta_d) &= (2, (0)_{p\in\mathcal{P}}) \\ \psi(\sqrt[a_i]{c_i}) &= \left(\frac{s_i d}{a_i}, \left(\frac{e_{p,i} d}{a_i}\right)_{p\in\mathcal{P}}\right) \end{aligned} \tag{4.6}$$

Theorem 4.7. *Let $\mathcal{P}$, M and ψ be as above. Then we have*

$$[B : \mathbf{Q}^*\mu_d] = \frac{(2, d)\#\psi(B/\mathbf{Q}^*)}{d}.$$

Proof. This follows from the existence of the isomorphism from Lemma 4.5. The index $[B : \mathbf{Q}^*\mu_d]$ is equal to $[B : \mathbf{Q}^*]/[\mathbf{Q}^*\mu_d : \mathbf{Q}^*]$. The index in the denominator only depends on d, and equals d if d is odd, and $d/2$ if d is even. □

Since we have explicitly written $B/\mathbf{Q}^*$ on a basis of M, we can now compute the index efficiently, using for example the methods from [8].

4.3 Entanglement

For computing the size of the entanglement group $E(B)$, we recall that $E(B)$ is equal to $E(B_{\mathrm{ab}})$ (Corollary 2.27), where B_{ab} is defined as

$$B_{\mathrm{ab}} = \{x \in B : \exists w \in \mathbf{Z}_{>0} : x^w \in B_{\mathrm{tors}}B^G \text{ and } B^G \text{ has an element of order } w\}.$$

Since $B^G = \mathbf{Q}^*$ has exactly two roots of unity, $w = 2$ suffices and this definition reduces to

$$B_{\mathrm{ab}} = \{x \in B : x^2 \in B_{\mathrm{tors}}\mathbf{Q}^*\}. \tag{4.8}$$

If d is odd, then for all $x \in B_{\mathrm{ab}}$, both x^2 and x^d are contained in $B_{\mathrm{tors}}\mathbf{Q}^*$, so B_{ab} is in fact equal to $\mathbf{Q}^*B_{\mathrm{tors}}$. This has no entanglement since every automorphism of $\mathbf{Q}^*B_{\mathrm{tors}}$ over $\mathbf{Q}^*$ extends uniquely to a field automorphism in $\mathrm{Gal}(\mathbf{Q}(B_{\mathrm{tors}})/\mathbf{Q})$.

In the rest of this section, we will therefore assume that d is even.

We turn to Corollary 2.31, which gives an explicit description in the case where B_{ab} is of the form μW where μ consists of roots of unity and W is Kummer. The

group B_{ab} cannot always be written in this form, but as we shall see, that is always possible if we slightly enlarge B by adding the $2d$-th roots of unity:

$$B' = \mu_{2d}B = \langle \mathbf{Q}^*, \mu_{2d}, \sqrt[a_i]{c_i} : i \in \{1, \dots, k\} \rangle \subset \bar{\mathbf{Q}}^*.$$

Since $B'/\mathbf{Q}^*$ has exponent d, the torsion subgroup of B' is contained in μ_{2d} and therefore equal to it. We can now compute B'_{ab}.

Proposition 4.9. *With B' defined as above, B'_{ab} is equal to $\mu_{2d}(\sqrt{\mathbf{Q}^*} \cap B')$, with $\sqrt{\mathbf{Q}^*} = \{x \in \bar{\mathbf{Q}}^* : x^2 \in \mathbf{Q}\}$.*

Proof. Analogously to Equation 4.8, we have

$$B'_{\mathrm{ab}} = \{x \in B' : x^2 \in B'_{\mathrm{tors}}\mathbf{Q}^*\} = \{x \in B' : x^2 \in \mu_{2d}\mathbf{Q}^*\}.$$

It is clear that $\mu_{2d}(\sqrt{\mathbf{Q}^*} \cap B')$ is contained in B'_{ab}. For the opposite inclusion, suppose that x is an element of B'_{ab}. Then we have $x \in B'$ and $x^2 \in \mathbf{Q}^*\mu_{2d}$. Then x^2 can be written as $x^2 = \zeta b$ with $b \in \mathbf{Q}^*$ and $\zeta \in \mu_{2d}$. Taking d-th powers, we get $\zeta^d = \frac{x^{2d}}{b^d} \in (\mathbf{Q}^*)^2$ because d is even. Since ζ^d is now in $(\mathbf{Q}^*)^2$ and in μ_2, we can conclude that ζ^d is 1, so ζ is a d-th root of unity. Since now $x^2 \in \mu_d\mathbf{Q}^*$, we find that $x \in \mu_{2d}\sqrt{\mathbf{Q}^*}$. This proves the claim. □

Following the notation from Corollary 2.31, we will now write $\mu = \mu_{2d}$ and $W = \sqrt{\mathbf{Q}^*} \cap B'$ so that $B'_{\mathrm{ab}} = \mu W$.

Note that Corollary 2.31 allows an amount of freedom in how to distribute elements that are both roots of unity and Kummer roots. In the definition of μ and W above, we have chosen to add these roots of unity to both μ and W.

Proposition 4.10. *With $G_\mu = \ker(G \to \mathrm{Aut}(\mu))$, we have*

$$\begin{aligned} E(\mu) &= 1, \text{ and} \\ E(B') &\cong \mathrm{Aut}_{\mathbf{Q}^* \cdot \langle i \rangle}(W^{G_\mu}). \end{aligned}$$

Proof. Each group automorphism of $\mathrm{Aut}(\mu)$ can be uniquely extended to a field automorphism in $\mathrm{Gal}(\mathbf{Q}(\mu)/\mathbf{Q})$, so $\mathrm{Gal}(\mathbf{Q}(\mu)/\mathbf{Q}) \cong \mathrm{Aut}(\mu)$ and $E(\mu)$ is trivial.

Because of that, Corollary 2.31 leads to

$$E(B') \cong \mathrm{Aut}_{W^G \cdot (\mu \cap W)}(W^{G_\mu}).$$

Since W^G is $\mathbf{Q}^*$ and $\mu \cap W$ is $\langle i \rangle$, the statement follows. □

Using this expression, we can find the order of $E(B')$ by a computation inside $M[2]$, where M (and $\mathcal{P}$) are the objects defined in the previous section. To determine W^{G_μ} we need to look at how G_μ acts on W.

Lemma 4.11. *For a positive integer k that can be factored over $\mathcal{P}$, the intersection $M_k = (\mathbf{Q}(\mu_k)^*/\mathbf{Q}^*) \cap M[2]$ has $\mathbf{F}_2$-basis*

$$\mathcal{B} = \{\sqrt{-1} \text{ if } 4 \mid k\} \cup \{\sqrt{p^*} : p \in \mathcal{P} \text{ with } p^* \mid k\},$$

where $2^* = 8$ and $p^* = \pm p \equiv 1 \bmod 4$ for odd $p \in \mathcal{P}$.

Proof. First of all, note that elements of the reduced coprime basis $\mathcal{P}$ are by definition either 2 or odd, so p^* is properly defined for all $p \in \mathcal{P}$.

For primes q it is well-known that $\sqrt{q^*}$ is an element of $\mathbf{Q}(\mu_{|q^*|})$. On odd integers, both reduction mod 4 and taking square roots (up to the sign of the root) are strictly multiplicative, so for $p = 2$ as well as for p odd, $\sqrt{p^*}$ is an element of $\mathbf{Q}(\mu_{|p^*|})$. Also, $\sqrt{-1}$ is in $\mathbf{Q}(\mu_4)$, so $\mathcal{B}$ is contained in M_k. Since elements of $\mathcal{P}$ are coprime, $\mathcal{B}$ is also $\mathbf{F}_2$-linearly independent.

To see that $\mathcal{B}$ generates M_k, consider an element $\sqrt{x} \in M_k$. We can choose the representative in such a way that x is a product of distinct elements of $\mathcal{P} \cup \{-1\}$. Choose an element $p \in \mathcal{P}$ that divides x, and suppose that p^* does not divide k. Let $l \mid p$ then be a prime number with $\mathrm{ord}_l(p)$ odd. (Such a prime l exists because p is not a perfect power.) Then $\mathbf{Q}(\sqrt{x})$ is ramified at l, while $\mathbf{Q}(\mu_k)$ is not, so $\sqrt{x}$ is not an element of M_k, leading to a contradiction. This shows that $\sqrt{x}$ or $\sqrt{-x}$ (or both) are in $\langle \mathcal{B} \rangle$.

If we have $4 \mid k$, then both $\sqrt{x}$ and $\sqrt{-x}$ are elements of $\langle \mathcal{B} \rangle$, and we are done. If on the other hand we have $4 \nmid k$, then only one of $\sqrt{x}$ and $\sqrt{-x}$ is in M_k, and therefore we conclude $\sqrt{x} \in \langle \mathcal{B} \rangle$. □

Proposition 4.12. *We have* $W^{G_\mu} = W \cap \mathbf{Q}(\mu_{2d})$ *and* $W^{G_\mu}/\mathbf{Q}^* = (W/\mathbf{Q}^*) \cap M_{2d}$.

Proof. By definition, G_μ is the kernel of the map $G \to \mathrm{Aut}(\mu)$, so in this setting it is $\mathrm{Gal}(\mathbf{Q}(B)/\mathbf{Q}(\mu_{2d}))$. The subgroup of W invariant under G_μ is then $W \cap \mathbf{Q}(\mu_{2d})$.

Since $W/\mathbf{Q}^*$ is contained in $M[2]$, we find $(W/\mathbf{Q}^*) \cap \mathbf{Q}(\mu_{2d})/\mathbf{Q}^* = (W/\mathbf{Q}^*) \cap ((\mathbf{Q}(\mu_{2d})/\mathbf{Q}^*) \cap M[2]) = (W/\mathbf{Q}^*) \cap M_{2d}$. □

For the actual explicit computations, we start by taking the intersection of $B'/\mathbf{Q}^*$ and $M[2]$ inside M to get a basis for the $\mathbf{F}_2$-module $(B'/\mathbf{Q}^*) \cap M[2] = ((B'/\mathbf{Q}^*) \cap (\sqrt{\mathbf{Q}^*}/\mathbf{Q}^*)) \cap M[2] = W/\mathbf{Q}^*$. Since we then have an explicit basis for $W/\mathbf{Q}^*$ and M_{2d} inside $M[2]$, we can now compute the order of their intersection, and then also that of $E(B')$.

Theorem 4.13. *The order of the entanglement group of* B' *is given by*

$$\#E(B') = \frac{1}{2}\#\mathrm{Hom}(W^{G_\mu}/\mathbf{Q}^*, \mu_2) = \frac{1}{2}\#(W^{G_\mu}/\mathbf{Q}^*).$$

Proof. Since $\langle \mathbf{Q}^*, \sqrt{\mathcal{P}}, i \rangle$ is a Kummer extension over $\mathbf{Q}^*$, there is an isomorphism $\mathrm{Aut}_{\mathbf{Q}^*}(\langle \mathbf{Q}^*, \sqrt{\mathcal{P}}, i \rangle) \to \mathrm{Hom}(\langle \mathbf{Q}^*, \sqrt{\mathcal{P}}, i \rangle/\mathbf{Q}^*, C_2) = M[2]^\vee$.

This isomorphism induces the three isomorphisms $\mathrm{Aut}_{\mathbf{Q}^*}(W) \cong (W/\mathbf{Q}^*)^\vee$, and $\mathrm{Aut}_{\mathbf{Q}^*}(W^{G_\mu}) \cong (W^{G_\mu}/\mathbf{Q}^*)^\vee$, and $\mathrm{Aut}_{\mathbf{Q}^* \cdot \langle i \rangle}(W^{G_\mu}) \cong (W^{G_\mu}/(\mathbf{Q}^* \cdot \langle i \rangle))^\vee$.

The order of this last dual is half the order of $(W^{G_\mu}/\mathbf{Q}^*)^\vee$, due to the added subgroup $\langle i \rangle$. Proposition 4.10 then gives the desired equality. □

To compute $\#E(B)$, we need to determine if the step from B to B' introduced extra entanglement. The following theorem gives a sufficient and necessary condition for this.

Theorem 4.14. *We have*

$$\#E(B) = \#E(B') \cdot \begin{cases} \frac{1}{2} & \text{if } \mu_{2d} \not\subset B \text{ and } (W^{G_\mu} \cap B)/\mathbf{Q}^* \neq (W/\mathbf{Q}^*) \cap M_d \\ 1 & \text{otherwise.} \end{cases}$$

Proof. If B equals B', we are of course done. So, assume that ζ_{2d} is not in B. Then we have $[B' : B] = 2$ and the kernel of the natural restriction map $\mathrm{Aut}_{\mathbf{Q}^*}(B') \twoheadrightarrow \mathrm{Aut}_{\mathbf{Q}^*}(B)$ equals $\mathrm{Aut}_B(B')$ and therefore contains exactly one non-trivial automorphism σ. The induced surjection $E(B') \twoheadrightarrow E(B)$ has a kernel generated by the image of σ, and it has order at most 2.

We can determine the order of this kernel by checking if σ maps to 1 in $E(B')$. There is no entanglement in extensions generated by roots of unity over $\mathbf{Q}$ (by Proposition 4.10), so we can use Corollary 2.31 for this.

In this corollary we have seen that the entanglement group $E(B')$ is isomorphic to $\mathrm{Aut}_{W^G(\mu \cap W)}(W^{G_\mu})$ and that the corresponding homomorphism from $\mathrm{Aut}_{\mathbf{Q}^*}(B')$ to $\mathrm{Aut}_{W^G(\mu \cap W)}(W^{G_\mu})$ sends σ to $\sigma|_{W^{G_\mu}}(g|_{W^{G_\mu}})^{-1}$ for any $g \in G$ with $\sigma|_\mu = g|_\mu$. To check if σ maps to 1 in $E(B)$ we can therefore check if g and σ have the same restriction to W^{G_μ}.

Since σ has order 2, and $g|_\mu = \sigma|_\mu$, the restriction $g|_{W^{G_\mu}}$ has order at most 2. We then have for all $x \in W^{G_\mu}$ that $gx, \sigma x \in \{\pm 1\}x$. Therefore, the automorphisms $\sigma|_{W^{G_\mu}}$ and $g|_{W^{G_\mu}}$ are equal if and only if they have the same groups of invariants.

The automorphism $\sigma|_{W^{G_\mu}}$ has group of invariants $W^{G_\mu} \cap B$, since we have $B = (B')^{\langle \sigma \rangle}$.

Since we have $g|_\mu = \sigma|_\mu$, the invariant field $\mathbf{Q}(\mu_{2d})^{\langle g \rangle}$ equals $\mathbf{Q}(\mu_d)$. The restriction $g|_{W^{G_\mu}}$ therefore has group of invariants $\mathbf{Q}(\mu_d) \cap W^{G_\mu} = \mathbf{Q}(\mu_d)^* \cap W$.

The image of σ in $E(B)$ therefore equals 1, if and only if the two submodules $(W^{G_\mu} \cap B)/\mathbf{Q}^*$ and $(W/\mathbf{Q}^*) \cap M_d$ of $M[2]$ are equal. The image of σ in $E(B)$ has order 2 otherwise. □

Combining the previous two theorems directly gives the following result for the order of $E(B)$.

Corollary 4.15. *The order of the entanglement group of B is given by*

$$\#E(B) = \#(W^{G_\mu}/\mathbf{Q}^*) \cdot \begin{cases} \frac{1}{4} & \text{if } \mu_{2d} \not\subset B \text{ and } (W^{G_\mu} \cap B)/\mathbf{Q}^* \neq (W/\mathbf{Q}^*) \cap M_d \\ \frac{1}{2} & \text{otherwise.} \end{cases}$$

Since we have already determined explicit bases for all modules in the condition of this corollary, computing the order of $E(B)$ from $\#(W^{G_\mu}/\mathbf{Q}^*)$ is a straightforward $\mathbf{F}_2$-linear algebra computation.

4.4 Field degrees

We will complete the proof of Theorem 4.2 in this section.

We recall the definition of the radical extension B of $\mathbf{Q}^*$:

$$B = \langle \mathbf{Q}^*, \mu_d, \sqrt[a_i]{c_i} : i \in \{1, \ldots, k\} \rangle.$$

Proof of proposition 4.3. Since B is a Galois radical group over $\mathbf{Q}^*$ by construction, Theorem 2.25 shows that B — with the Galois action of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ — has an entanglement group $E(B)$. Recall that in this case, $E(B)$ is the cokernel of the natural embedding of $\mathrm{Gal}(\mathbf{Q}(B)/\mathbf{Q})$ into $\mathrm{Aut}_{\mathbf{Q}^*}(B)$.

We find

$$[\mathbf{Q}(B) : \mathbf{Q}(\mu_d)] = \frac{[\mathbf{Q}(B) : \mathbf{Q}]}{\varphi(d)} = \frac{\#\mathrm{Aut}_{\mathbf{Q}^*}(B)}{\varphi(d)\#E(B)}.$$

Using Theorem 2.19 we conclude

$$\begin{aligned}[\mathbf{Q}(B) : \mathbf{Q}(\mu_d)] &= \frac{[B : \mathbf{Q}^*]}{\varphi(d)\#E(B)} \prod_{\substack{p \text{ prime} \\ B[p] \neq \mathbf{Q}^*[p]}} \frac{p-1}{p} \\ &= \frac{[B : \mathbf{Q}^*\mu_d] \cdot [\mathbf{Q}^*\mu_d : \mathbf{Q}^*]}{(d/2) \cdot \#E(B)} = \frac{[B : \mathbf{Q}^*\mu_d]}{\#E(B)}.\end{aligned}$$

□

Proof of Theorem 4.2. The previous two sections show how to compute the quantities $[B : \mathbf{Q}^*\mu_d]$ and $\#E(B)$ in this fraction in the required time. Combining these statements yields Algorithm 4.16 to compute $[\mathbf{Q}(B) : \mathbf{Q}(\mu_d)]$.

This algorithm runs in time polynomial in the input. The computation and factoring over the co-prime basis is polynomial time due to Theorem 4.4. Computing the intersections and equality inside $M[2]$ is basic linear algebra over $\mathbf{F}_2$ with matrix sizes linear in the input size.

Finally, evaluating the expression from Theorem 4.7 involves computing an order of a $\mathbf{Z}/d\mathbf{Z}$-module D, where the generators of D are written on a basis of the free $\mathbf{Z}/d\mathbf{Z}$-module M of rank, say, r. The computation of this order can be performed by dividing d^r by the index of $((d\mathbf{Z})^r + D)$ inside $\mathbf{Z}^r$. Since both the number of generators of D and the size of each coefficient are linear in the size of the input, this index can be computed in polynomial time, using for example the methods from [8]. □

Algorithm 4.16.

1. Determine a coprime base $\mathcal{P}$ for the set consisting of 2, all a_i, and all c_i and factor all these numbers over $\mathcal{P}$.
2. Compute $d = \operatorname{lcm}\{a_i\}$ using this factorization.
3. Define the $\mathbf{Z}/d\mathbf{Z}$-module M as in Lemma 4.5.
4. Use Equation 4.6 and Theorem 4.7 to compute $[B : \mathbf{Q}^*\mu_d]$.
5. If d is odd, then $\#E(B) = 1$. Proceed with step 10.
6. Use Lemma 4.11 to find $\mathbf{F}_2$-bases of M_d and M_{2d} inside $M[2]$.
7. Use Proposition 4.12 to find $W^{G_\mu}/\mathbf{Q}^*$ by computing $(W/\mathbf{Q}^*) \cap M_{2d}$ inside $M[2]$.
8. Compute the intersections $(W^{G_\mu} \cap B)/\mathbf{Q}^*$ and $(W/\mathbf{Q}^*) \cap M_d$ inside $M[2]$.
9. Use Corollary 4.15 to compute $\#E(B)$.
10. Finally, use Proposition 4.3 to compute $[\mathbf{Q}(B) : \mathbf{Q}(\mu_d)]$.

Example 4.17.

Consider $K = \mathbf{Q}(\mu_{12}, \sqrt[6]{6}, \sqrt[4]{-9})$, or, equivalently

$$K = \mathbf{Q}\left(\mu_{12},\ \sqrt[12]{6^2},\ \sqrt[12]{-3^6}\right).$$

Using the notation from throughout this chapter, we get $d = 12$ and

$$B = \left\langle \mathbf{Q}^*, \mu_{12},\ \sqrt[12]{6^2},\ \sqrt[12]{-3^6} \right\rangle.$$

The coprime base for the numbers involved necessarily consists of actual primes in this case: $\mathcal{P} = \{2, 3\}$. This means that the free $\mathbf{Z}/d\mathbf{Z}$-module M is given by

$$M = \left\langle \mathbf{Q}^*, \mu_{24},\ \sqrt[12]{2},\ \sqrt[12]{3} \right\rangle \Big/ \mathbf{Q}^*.$$

Inside this module, we compute the index $[B : \mu_{12}\mathbf{Q}^*]$. On the (ordered) basis $(\zeta_{24},\ \sqrt[12]{2},\ \sqrt[12]{3})$, the submodule $\mu_{12}\mathbf{Q}^*$ is generated by $\langle(2,0,0)\rangle$ and B by $\langle(2,0,0),(0,2,2),(1,0,6)\rangle$. Adding $3 \cdot (0,2,2)$ to $(1,0,6)$ results in a basis for B in triangular form:

$$B = \langle(2,0,0),(1,6,0),(0,2,2)\rangle.$$

From this we see that $[B : \mu_{12}\mathbf{Q}^*]$ equals $(12/6) \cdot (12/2) = 12$.

We continue with the entanglement group computation, starting with $E(B')$ for $B' = \langle B, \mu_{24} \rangle$. This takes place in the 2-torsion of M:

$$M[2] = \left\langle \sqrt{-1}, \sqrt{2}, \sqrt{3} \right\rangle.$$

Since $\sqrt{-1}$, $\sqrt{2}$ and $\sqrt{3}$ are all contained in $\mathbf{Q}(\mu_{24})$, the intersection $M_{24} = M[2] \cap (\mathbf{Q}(\mu_{24})^*/\mathbf{Q}^*)$ actually equals $M[2]$. The three roots $\sqrt{-1}$, $\sqrt{2}$ and $\sqrt{3}$ are also all contained in B', so $W^{G_\mu}/\mathbf{Q}^* = M_{24} \cap (W/\mathbf{Q}^*) = M_{24} \cap B'$ also equals $M[2]$.

As an aside, according to Theorem 4.13 the order of $E(B')$ is half that of $W^{G_\mu}/\mathbf{Q}^*$, so we have $\#E(B') = 4$. To compute the size of $E(B)$ from this, we need to determine if $(W^{G_\mu} \cap B)/\mathbf{Q}^*$ equals $(W/\mathbf{Q}^*) \cap M_{12}$. Since $\sqrt{3}$ is not in B, it is not in the former module, while it is in the latter, so they are not equal, and $\#E(B) = 8 \cdot \frac{1}{4} = 2$.

This leads us to the conclusion

$$\left[\mathbf{Q}\left(\mu_{12}, \sqrt[6]{6}, \sqrt[4]{-9}\right) : \mathbf{Q}\right] = \varphi(12) \cdot \frac{12}{2} = 24.$$