Chapter 4
Construction of All Cubic Fields of a Fixed Fundamental Discriminant (Renate Scheidler)

4.1 Introduction

In 1925, Berwick [19] described an approach for generating all cubic fields of a given discriminant Δ. When Δ is fundamental, Berwick's observation, expressed in modern terminology, was that every cubic field of discriminant Δ arises from a 3-*virtual unit* in the quadratic *resolvent field* $\mathbb{L}' = \mathbb{Q}(\sqrt{\Delta'})$ of (also fundamental) discriminant $\Delta' = -3\Delta/\gcd(3,\Delta)^2$. A 3-virtual unit of $\mathbb{L}'$ is defined to be a generator of a principal ideal that is the cube of some ideal in the maximal order $\mathcal{O}_{\mathbb{L}'}$ of $\mathbb{L}'$. Suppose $\lambda = (G+H\sqrt{\Delta'})/2$, with $G,H \in \mathbb{Z}$ non-zero, is a 3-virtual unit that is not itself a cube in $\mathbb{L}'$. Put $\overline{\lambda} = (G-H\sqrt{\Delta'})/2$ and $\lambda\overline{\lambda} = A^3$ with $A \in \mathbb{Z}$. Then $f(x) = x^3 - 3Ax + G$ is the generating polynomial of a cubic field of discriminant Δ or $-27\Delta'$, and every cubic field of discriminant Δ arises in this way. Moreover, two 3-virtual units $\lambda_1, \lambda_2 \in \mathcal{O}_{\mathbb{L}'}$ give rise to the same cubic field up to $\mathbb{Q}$-isomorphism if and only if λ_1/λ_2 or $\lambda_1/\overline{\lambda}_2$ is a cube in $\mathbb{L}'$. In this case, if λ_i is a generator of the $\mathcal{O}_{\mathbb{L}'}$-ideal $\mathfrak{a}_i^3$ for $i = 1,2$, then $\mathfrak{a}_1$ is equivalent to $\mathfrak{a}_2$ or to $\overline{\mathfrak{a}}_2$, i.e., $\mathfrak{a}_1 = (\alpha)\mathfrak{a}_2$ or $\mathfrak{a}_1 = (\alpha)\overline{\mathfrak{a}}_2$ for some non-zero $\alpha \in \mathbb{L}'$. Cubic fields of fundamental discriminant Δ can therefore be obtained from 3-virtual units in the quadratic resolvent field of discriminant Δ', or more exactly, via the cube roots of ideals belonging to 3-torsion classes in the class group of $\mathbb{L}'$. Care must be taken that this construction produces the complete collection of triples of conjugate cubic fields of discriminant Δ, that it yields each such field exactly once, and that any fields of discriminant $-27\Delta'$ are detected and eliminated.

A major problem with Berwick's approach is that the generating polynomials thus obtained can have extremely large coefficients, particularly when $\Delta < 0$, in which case $\mathbb{L}'$ is a real quadratic field. An ingenious solution to this problem was devised by Shanks who proposed a 3-virtual unit construction that produces generating polynomials with remarkably small coefficients. For example, for the 13 triples

S. A. Hambleton, H. C. Williams, *Cubic Fields with Geometry*,
CMS Books in Mathematics, https://doi.org/10.1007/978-3-030-01404-9_4

of conjugate cubic fields of discriminant $\Delta = 44806173$, Shanks' algorithm produces the following generating polynomials:

$$\begin{aligned}
f_1(x) &= x^3 - 61x^2 + 697x - 330,\\
f_2(x) &= x^3 - 279x^2 + 441x - 170,\\
f_3(x) &= x^3 - 63x^2 + 423x - 8,\\
f_4(x) &= x^3 - 69x^2 + 435x - 216,\\
f_5(x) &= x^3 - 63x^2 + 603x - 494,\\
f_6(x) &= x^3 - 83x^2 + 297x - 54,\\
f_7(x) &= x^3 - 63x^2 + 837x - 494,\\
f_8(x) &= x^3 - 257x^2 + 477x - 216,\\
f_9(x) &= x^3 - 87x^2 + 273x - 36,\\
f_{10}(x) &= x^3 - 62x^2 + 546x - 261,\\
f_{11}(x) &= x^3 - 60x^2 + 660x - 97,\\
f_{12}(x) &= x^3 - 165x^2 + 273x - 90,\\
f_{13}(x) &= x^3 - 127x^2 + 185x - 62.
\end{aligned} \tag{4.1}$$

In particular, in the computationally more interesting case of negative cubic discriminants, all computations are conducted in the set of reduced ideals in each 3-torsion ideal class of the class group of $\mathbb{L}'$, known as the *infrastructure* of the class. Shanks therefore assigned his algorithm the six-letter FORTRAN designator CUFFQI, pronounced "cuff-key," an acronym derived from the phrase *Cubic Fields From Quadratic Infrastructure*. Shanks' work is described in his talks [170, 172] and in a manuscript [171] dating back to 1987, but was never published.

In his 1990 doctoral dissertation, Fung [77] presented CUFFQI in a computationally more suitable form and implemented it in FORTRAN on an Amdahl 5870 mainframe computer. Evidence of the efficiency of Fung's version of CUFFQI is provided by his impressive (for the late 1980s) computation of all 364 non-conjugate cubic fields of the 19-digit discriminant $\Delta = -3161659186633662283$ in under 3 CPU minutes. This chapter provides a modern description of the previously unpublished Shanks-Fung CUFFQI algorithm for constructing all cubic fields of a given fundamental discriminant Δ.

4.2 The Quadratic Fields Associated with a Cubic Field

Let $\mathbb{K}$ be a cubic field of discriminant Δ. Recall from §1.6 that there are two fields associated with $\mathbb{K}$, namely $\mathbb{L} = \mathbb{Q}(\sqrt{\Delta})$ and its *dual* (or *mirror*) field $\mathbb{L}' = \mathbb{Q}(\sqrt{-3\Delta})$

which is the resolvent field of $\mathbb{K}$. If D is the (fundamental) discriminant of $\mathbb{L}$, related to Δ via (1.68), then the discriminant of $\mathbb{L}'$, termed the *dual* discriminant, is

$$D' = \frac{-3D}{\gcd(D,3)^2} = \begin{cases} -3D & \text{if } 3 \nmid D, \\ -D/3 & \text{if } 3 \mid D, \end{cases} \tag{4.2}$$

Note that $\{D, D'\} = \{1, -3\}$ if and only if one of $\mathbb{L}$, $\mathbb{L}'$ is $\mathbb{Q}$; otherwise, both $\mathbb{L}$ and $\mathbb{L}'$ are quadratic extensions of $\mathbb{Q}$.

If Δ is a fundamental discriminant, then $D = \Delta$, and the number of cubic fields of discriminant D is related to $\mathbb{L}$ as follows [95, Satz 7, p. 587]:

Theorem 4.1. *Let $\mathbb{L}$ be a quadratic field of discriminant D, and r the 3-rank of the class group of $\mathbb{L}$. Then the number of non-conjugate cubic fields of discriminant D is $(3^r - 1)/2$.*

For example, the class group of the real quadratic field $\mathbb{L} = \mathbb{Q}(\sqrt{44806173})$ has 3-rank 3, so there are $(3^3 - 1)/2 = 13$ non-conjugate cubic fields of that discriminant, generated by the 13 polynomials listed in (4.1). Quer [156] determined that the class group of $\mathbb{L} = \mathbb{Q}(\sqrt{-3161659186633662283})$ has 3-rank 6, so there are 364 non-conjugate cubic fields with this discriminant, for which Fung found generating polynomials in [77].

The 3-ranks of the ideal class groups of $\mathbb{L}$ and its dual field $\mathbb{L}'$ are closely related through a theorem due to [165]:

Theorem 4.2. *Let D and D' be dual fundamental discriminants with $D < 0$, and let r and r' denote the respective 3-ranks of the ideal class groups of the imaginary quadratic field $\mathbb{L} = \mathbb{Q}\sqrt{D})$ and the real quadratic field $\mathbb{L}' = \mathbb{Q}(\sqrt{D'})$. Then $r = r'$ or $r = r' + 1$.*

The first of these two cases is referred to as *non-escalatory*, whereas the second case is labelled *escalatory* [173]. For example, the field $\mathbb{L} = \mathbb{Q}(\sqrt{-14935391})$ and its dual $\mathbb{L}' = \mathbb{Q}(\sqrt{44806173})$ both have class groups of 3-rank 3 and hence belong to the non-escalatory case. Larger examples include the escalatory quadratic field

$$\mathbb{L} = \mathbb{Q}(\sqrt{-35102371403731})$$

of 3-rank 5 and the non-escalatory field

$$\mathbb{L} = \mathbb{Q}(\sqrt{-250930267537731})$$

of 3-rank 4; see Section 5.9 of [77]. More recently, Kishi [111] characterized the escalatory scenario by linking it to the existence of cubic fields with certain properties and to solutions of norm equations in $\mathbb{L}$. Among other criteria, he proved that $r = r' + 1$ if and only if there does not exist a triple $(x, y, z) \in \mathbb{Z}^3$ such that $\gcd(x, y) = 1$, $x^2 \equiv 1$ or $7 \pmod 9$, $y \equiv 1 \pmod 3$, $z \neq 0$, and $x^2 - 3z^2 d = 4y^3$. Here $d > 0$ is the square-free part of $-D$, i.e., $d = -D$ if $D \equiv 1 \pmod 4$ and $d = -\frac{D}{4}$ otherwise.

The resolvent field $\mathbb{L}'$ is further related to the cubic field $\mathbb{K}$ through the roots of a generating polynomial. As seen in §1.4, there exists a generating polynomial of $\mathbb{K}$ of the form

$$f(x) = x^3 - 3Ax + G \tag{4.3}$$

with $A, G \in \mathbb{Z}$. The discriminant of $f(x)$ is $D_f = 27(4A^2 - G^3)$. Recall from (1.52) that the roots β_i, $i = 0, 1, 2$, of $f(x)$ are given by

$$\beta_i = \eta^i \sqrt[3]{\mu} + \eta^{-i} \sqrt[3]{\nu}, \quad i = 0, 1, 2,$$

where η is a primitive cube root of unity and μ, ν are given by (1.51). Put

$$\lambda = -\nu = \frac{G + \sqrt{G^2 - 4A^3}}{2}. \tag{4.4}$$

Then the minimal polynomial of λ over $\mathbb{Q}$ is $R(x) = x^2 - Gx + A^3$ of discriminant $D_R = G^2 - 4A^3 = -D_f/27$. Since D_R/D' is a square, it follows that $\lambda \in \mathbb{L}'$, and we have

$$\beta_i = -\eta^i \kappa - \frac{A}{\eta^i \kappa} \quad \text{with} \quad \kappa^3 = \lambda, \quad i = 0, 1, 2. \tag{4.5}$$

In this way, every cubic field $\mathbb{K}$, through a generating polynomial of the form (4.3), defines an element λ in the maximal order $\mathcal{O}_{\mathbb{L}'}$ of the resolvent field $\mathbb{L}'$ of $\mathbb{K}$. Following the terminology of Berwick [19], we call λ a *(quadratic) generator* of $\mathbb{K}$. Note that both λ and $\bar{\lambda}$ are quadratic generators of each of the three conjugate cubic fields $\mathbb{Q}(\beta_i)$, $i = 0, 1, 2$.

We will make use of the following useful auxiliary result. Recall that the Galois closure of $\mathbb{K}$ is obtained by adjoining any of the three roots β_i, $i = 0, 1, 2$, to $\mathbb{L}$. The analogous construction over $\mathbb{L}'$ yields three different cubic extensions of $\mathbb{L}'$, and we have the following field equalities:

Lemma 4.1. *Let κ and β_i $(i = 0, 1, 2)$ be given by (4.5). Then $\mathbb{L}'(\beta_i) = \mathbb{L}'(\eta^i \kappa)$.*

Proof. By (4.5), $\beta_i \in \mathbb{Q}(\eta^i \kappa) \subset \mathbb{L}'(\eta^i \kappa)$. For the other inclusion, note that the two identities $(\eta^i \kappa)^2 - \beta_i(\eta^i \kappa) + A = 0$ and $(\eta^i \kappa)^3 = \lambda \in \mathbb{L}'$ yield

$$\eta^i \kappa = \frac{\lambda + A\beta_i}{\beta_i^2 - A} \in \mathbb{L}'(\beta_i). \qquad \square$$

Given a fundamental discriminant D, the CUFFQI algorithm produces all non-conjugate cubic fields $\mathbb{K}$ of discriminant either D or $-27D'$ from appropriate elements $\lambda \in \mathbb{L}'$ via the quadratic generator construction. In this context, it is unnecessary to consider the exceptional case $\{D, D'\} = \{1, -3\}$. There are no cubic fields of discriminant $D = -3$ or $-27D' = -27$; in particular, since $\mathbb{L} \neq \mathbb{Q}(\sqrt{-3})$, we only need to consider polynomials of the form (4.3) with $A \neq 0$, i.e., fields that are not pure cubic. There is obviously also no cubic field of discriminant $D = 1$; however, there is one cubic field of discriminant $-27D' = 81$, namely the cyclic cubic field generated by $f(x) = x^3 - 3x - 1$ which is the smallest of the simplest cubic fields.

In the next section, we will investigate which elements of $\mathcal{O}'_{\mathbb{L}'}$ are quadratic generators of some cubic field $\mathbb{K}$, and which of these cubic fields have discriminant D. We restrict to discriminants D with $\{D, D'\} \neq \{1, -3\}$.

4.3 From Quadratic Generators in $\mathcal{O}_{\mathbb{L}'}$ to Cubic Fields

Let $D \in \mathbb{Z} \setminus \{1, -3\}$ be a fundamental discriminant with dual discriminant D' as given in (4.2), and put $\mathbb{L}' = \mathbb{Q}(\sqrt{D'})$. Recall from (1.70) that the maximal order $\mathcal{O}'_{\mathbb{L}'}$ of $\mathbb{L}'$ is a $\mathbb{Z}$-module of rank 2 with basis $\mathcal{B} = \{1, \omega\}$, where $\omega = (s + \sqrt{D'})/2$ and $s \in \{0, 1\}$ is the remainder of D' modulo 4. Hence every element $\lambda \in \mathcal{O}_{\mathbb{L}'}$ can be uniquely expressed in the form

$$\lambda = \frac{G + H\sqrt{D'}}{2},$$

where $G, H \in \mathbb{Z}$, G is even when $D' \equiv 0 \pmod 4$, and $G \equiv H \pmod 2$ when $D' \equiv 1 \pmod 4$. To distinguish conjugation in $\mathbb{L}'$ from conjugation in $\mathbb{K}$, we denote the conjugate of λ by $\overline{\lambda} = (G - H\sqrt{D'})/2 \in \mathcal{O}_{\mathbb{L}'}$. Then $\lambda + \overline{\lambda} = G \in \mathbb{Z}$ and $\lambda\overline{\lambda} = (G^2 - H^2 D')/4 \in \mathbb{Z}$.

Every $\lambda \in \mathcal{O}_{\mathbb{L}'}$ defines a cubic polynomial

$$f_\lambda(x) = x^3 - 3(\lambda\overline{\lambda})^{1/3}x + (\lambda + \overline{\lambda}), \tag{4.6}$$

with real coefficients, where $(\lambda\overline{\lambda})^{1/3}$ is the unique real cube root of $\lambda\overline{\lambda}$. It is clear that $f_\lambda(x)$ has integer coefficients if and only if $\lambda\overline{\lambda}$ is a cube in $\mathbb{Z}$.

For any $\lambda \in \mathcal{O}_{\mathbb{L}'}$, denote by $(\lambda) = \lambda\mathcal{O}_{\mathbb{L}'}$ the principal $\mathcal{O}_{\mathbb{L}'}$-ideal generated by λ. An element $\lambda \in \mathcal{O}_{\mathbb{L}'}$ is said to be a 3-*virtual unit* if $(\lambda) = \mathfrak{a}^3$ for some non-zero ideal $\mathfrak{a}$ of $\mathcal{O}_{\mathbb{L}'}$. Note that λ is a 3-virtual unit if and only if $\overline{\lambda}$ is a 3-virtual unit, since $\overline{\lambda}$ is a generator of $\overline{\mathfrak{a}}^3$ where $\overline{\mathfrak{a}} = \{\overline{\alpha} \mid \alpha \in \mathfrak{a}\}$ is the conjugate ideal of $\mathfrak{a}$. For any $\mathcal{O}_{\mathbb{L}'}$-ideal $\mathfrak{a}$, we have $\mathfrak{a}\overline{\mathfrak{a}} = (\mathfrak{N}(\mathfrak{a}))$ where $\mathfrak{N}(\mathfrak{a}) \in \mathbb{N}$ is the norm of $\mathfrak{a}$, i.e., the index of $\mathfrak{a}$ in $\mathcal{O}_{\mathbb{L}'}$ as an additive subgroup.

Proposition 4.1. *Let $\lambda \in \mathcal{O}_{\mathbb{L}'}$ be non-zero, and let $f_\lambda(x)$ be defined as in (4.6). Then the following hold:*

1. *$f_\lambda(x)$ has integer coefficients if and only if λ is a 3-virtual unit.*
2. *If $\lambda \in \mathcal{O}_{\mathbb{L}'}$ is a 3-virtual unit, then $f_\lambda(x)$ is irreducible over $\mathbb{Q}$ if and only if λ is not a cube in $\mathcal{O}_{\mathbb{L}'}$. In that case, both λ and $\overline{\lambda}$ are quadratic generators of the field $\mathbb{K}$ whose generating polynomial is $f_\lambda(x)$.*

Proof. If λ is a 3-virtual unit, say $(\lambda) = \mathfrak{a}^3$ for some ideal $\mathfrak{a}$ of $\mathcal{O}_{\mathbb{L}'}$, then $(\lambda\overline{\lambda}) = (\mathfrak{N}(\mathfrak{a}))^3$, so $\lambda\overline{\lambda} = \pm\mathfrak{N}(\mathfrak{a})^3$ is a cube in $\mathbb{Z}$. Conversely, by considering the prime ideal factorization of $\mathfrak{b} = (\lambda)$ in $\mathcal{O}_{\mathbb{L}'}$, one sees that $\lambda\overline{\lambda}$ is a cube in $\mathbb{Z}$ only when $\mathfrak{b}$ is an ideal cube. This proves part 1.

For part 2, note that the zeros of $f_\lambda(x)$ are $\beta_0, \beta_1, \beta_2$ as given in (4.5). Now λ is a cube in $\mathcal{O}_{\mathbb{L}'}$ if and only if $\eta^i\kappa \in \mathcal{O}_{\mathbb{L}'}$ for some $i \in \{0,1,2\}$. By Lemma 4.1, this is the case if and only if $\beta_i \in \mathbb{L}'$, which in turn holds if and only if $f_\lambda(x)$ has a quadratic factor with rational coefficients.

Finally, if $f_\lambda(x)$ is irreducible over $\mathbb{Q}$, then it is the generating polynomial of a cubic field $\mathbb{K}$ for which λ is a quadratic generator. Since $f_\lambda(x) = f_{\overline{\lambda}}(x)$, $\overline{\lambda}$ is also quadratic generator of $\mathbb{K}$. □

Corollary 4.1. *If $f_\lambda(x)$ is irreducible, then $\lambda \notin \mathbb{Z}$.*

Proof. If $\lambda \in \mathbb{Z}$, then $\lambda^2 = \lambda\overline{\lambda}$, which is a cube in $\mathbb{Z}$, forcing λ to be a cube in $\mathbb{Z}$. By Proposition 4.1, $f_\lambda(x)$ is reducible. □

Part 2 of Proposition 4.1 shows that every 3-virtual unit $\lambda \in \mathcal{O}_{\mathbb{L}'} \setminus \mathcal{O}_{\mathbb{L}'}^3$ is a quadratic generator of some cubic field $\mathbb{K}$. More exactly, λ and $\overline{\lambda}$ are quadratic generators of the triple of conjugate cubic fields whose generating polynomial is $f_\lambda(x)$. This triple of cubic fields can have many quadratic generators; this is made more precise in the next theorem.

Theorem 4.3. *Two 3-virtual units $\lambda_1, \lambda_2 \in \mathcal{O}_{\mathbb{L}'} \setminus \mathcal{O}_{\mathbb{L}'}^3$ are quadratic generators of the same triple of conjugate cubic fields if and only if $\lambda_1 = \alpha^3\lambda_2$ or $\lambda_1 = \alpha^3\overline{\lambda}_2$ for some non-zero $\alpha \in \mathbb{L}'$.*

Proof. For $j = 1,2$, write $f_{\lambda_j}(x) = x^2 - 3A_jx + G_j$, and let $\beta_{j0}, \beta_{j1}, \beta_{j2}$ be the zeros of $f_{\lambda_j}(x)$. By (4.5), $\beta_{ji} = \eta^i\kappa_j + A_j/\eta^i\kappa_j$ for $i = 0,1,2$ and $j = 1,2$ where $\kappa_j^3 = \lambda_j$.

Suppose first that $\mathbb{Q}(\beta_{10}) = \mathbb{Q}(\beta_{2i})$ for some $i \in \{0,1,2\}$. Then $\mathbb{L}'(\beta_{10}) = \mathbb{L}'(\beta_{2i})$, and hence $\mathbb{L}'(\kappa_1) = \mathbb{L}'(\eta^i\kappa_2)$ by Lemma 4.1. Put $\mathbb{E} = \mathbb{L}'(\eta)$. Then $\mathbb{E}(\kappa_1) = \mathbb{E}(\eta^i\kappa_2) = \mathbb{E}(\kappa_2)$ is a Kummer extension of $\mathbb{E}$. Standard results on generators of Kummer extensions (see, for example, Exercise 7 (c), p. 636, of [68]) imply that $\lambda_1 = \gamma^3\lambda_2$ or $\lambda_1 = \gamma^3\lambda_2^2 = (\gamma\lambda_2/A_2)^3\,\overline{\lambda}_2$ for some $\gamma \in \mathbb{E}$.

It remains to show γ^3 has a cube root in $\mathbb{L}'$. To that end, note that $[\mathbb{L}'(\gamma) : \mathbb{L}'] \le [\mathbb{E}' : \mathbb{L}'] \le 2$ and $\gamma^3 \in \mathbb{L}'$. So the polynomial $x^3 - \gamma^3 \in \mathbb{L}'[x]$ is reducible over $\mathbb{L}'$ and hence must have a root in $\mathbb{L}'$.

Conversely, suppose that $\lambda_1 = \alpha^3\lambda_2$ or $\lambda_1 = \alpha^3\overline{\lambda}_2 = (\alpha A_2)^3/\lambda_2$ for some non-zero $\alpha \in \mathbb{L}'$. Then $\kappa_1 = \eta^i\alpha\kappa_2$ or $\kappa_1 = \alpha A_2/\eta^i\kappa_2$ for some $i \in \{0,1,2\}$. It follows that $\mathbb{L}'(\kappa_1) = \mathbb{L}'(\eta^i\kappa_2)$. By Lemma 4.1, $\mathbb{L}'(\beta_{10}) = \mathbb{L}'(\beta_{2i})$, and hence $\mathbb{Q}(\beta_{10}) \subseteq \mathbb{L}'(\beta_{2i})$. Then

$$6 = [\mathbb{L}'(\beta_{2i}) : \mathbb{Q}] = [\mathbb{L}'(\beta_{2i}) : \mathbb{Q}(\beta_{10})][\mathbb{Q}(\beta_{10}) : \mathbb{Q}] = 3[\mathbb{L}'(\beta_{2i}) : \mathbb{Q}(\beta_{10})],$$

so $[\mathbb{L}'(\beta_{2i}) : \mathbb{Q}(\beta_{10})] = 2$. Since $\mathbb{Q}(\beta_{2i}, \beta_{10})$ is a subfield of $\mathbb{L}'(\beta_{2i})$ that contains $\mathbb{Q}(\beta_{10})$, we have $[\mathbb{Q}(\beta_{2i}, \beta_{10}) : \mathbb{Q}(\beta_{10})] \le 2$. Now β_{2i} is a root of the cubic equation $f_{\lambda_2}(x) = 0$ over $\mathbb{Q}(\beta_{10})$, so $f_{\lambda_2}(x)$ is reducible over $\mathbb{Q}(\beta_{10})$, but not over $\mathbb{Q}$. It follows that $f_{\lambda_2}(x)$ has a root in $\mathbb{Q}(\beta_{10})$. Thus, $\beta_{2j} \in \mathbb{Q}(\beta_{10})$ for some $j \in \{0,1,2\}$, and hence $\mathbb{Q}(\beta_{2j}) = Q(\beta_{10})$. □

4.4 From Primitive 3-Torsion Ideals of $\mathcal{O}_{\mathbb{L}'}$ to Cubic Fields

Analogous to the terminology of §2.3, an ideal $\mathfrak{a}$ of $\mathcal{O}_{\mathbb{L}'}$ is said to be primitive if there exists no rational integer $k \neq \pm 1$ such that every element of $\mathfrak{a}$ is a multiple of k. It is clear that every ideal of $\mathcal{O}_{\mathbb{L}'}$ is equivalent to a primitive ideal. A 3-virtual unit $\lambda \in \mathcal{O}_{\mathbb{L}'}$ is said to be primitive if $(\lambda) = \mathfrak{a}^3$ for some primitive $\mathcal{O}_{\mathbb{L}'}$-ideal $\mathfrak{a}$. The following lemma shows that we may restrict our investigation of cubic fields to primitive 3-virtual units.

Lemma 4.2. *Every cubic field with quadratic resolvent field $\mathbb{L}'$ has a quadratic generator that is a primitive 3-virtual unit.*

Proof. Let $\mathbb{K}$ be a cubic field, $\mu \in \mathcal{O}_{\mathbb{L}'}$ a quadratic generator of $\mathbb{K}$, and $\mathfrak{b}$ the ideal of $\mathcal{O}_{\mathbb{L}'}$ such that $\mathfrak{b}^3 = (\mu)$. Then $\mathfrak{b} = (k)\mathfrak{a}$ where $\mathfrak{a}$ is a primitive ideal of $\mathcal{O}_{\mathbb{L}'}$ and $k \in \mathbb{Z}$. Put $\lambda = \mu/k^3$. Then $(\lambda) = \mathfrak{a}^3$, so $\lambda \in \mathcal{O}_{\mathbb{L}'}$, and λ is also a quadratic generator of $\mathbb{K}$ by Theorem 4.3. □

The next lemma provides a simple necessary condition on primitive 3-virtual units. As before, for any $N \in \mathbb{Z}$ and any rational prime p, let $v_p(N)$ denote the exact power of p dividing N.

Lemma 4.3. *Let $\lambda = (G+H\sqrt{D'})/2 \in \mathcal{O}_{\mathbb{L}'} \setminus \mathcal{O}_{\mathbb{L}'}^3$ be a primitive 3-virtual unit, and $\mathfrak{a}$ the ideal of $\mathcal{O}_{\mathbb{L}'}$ such that $\mathfrak{a}^3 = (\lambda)$. Put $A^3 = \lambda\overline{\lambda}$. Then for all primes $p \in \mathbb{N}$ dividing A, either $p \nmid GHD'$ or $p \mid D'$ and $1 = v_p(A) = v_p(H) < v_p(G)$.*

Proof. Note that $\mathfrak{a}\overline{\mathfrak{a}} = (A)$. Since $\mathfrak{a}$ is primitive, $\overline{\mathfrak{a}}$ is also primitive, so no prime factor p of A can be inert, as otherwise every element in $\mathfrak{a}$ or $\overline{\mathfrak{a}}$ would be a multiple of p.

Suppose p splits in $\mathcal{O}_{\mathbb{L}'}$, and let $\mathfrak{p}$ be a prime ideal above p in $\mathcal{O}_{\mathbb{L}'}$. Then $\mathfrak{p}$ divides exactly one of $\mathfrak{a}$, $\overline{\mathfrak{a}}$, so $\mathfrak{p}$ divides exactly one of the principal ideals (λ), $(\overline{\lambda})$. It follows that $\mathfrak{p}$ does not divide $(\lambda+\overline{\lambda}) = (G)$; similarly, $\mathfrak{p}$ does not divide $(\lambda-\overline{\lambda}) = H\sqrt{D'}$. Thus, $p \nmid GHD'$.

Finally, assume that p is ramified in $\mathcal{O}_{\mathbb{L}'}$, and write $(p) = \mathfrak{p}^2$ where $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_{\mathbb{L}'}$. Then $\mathfrak{p} \mid \mathfrak{a}$, but $\mathfrak{p}^2 = (p) \nmid \mathfrak{a}$ as $\mathfrak{a}$ is primitive. Similarly, $\mathfrak{p} \mid \overline{\mathfrak{a}}$, $\mathfrak{p}^2 \nmid \overline{\mathfrak{a}}$. It follows that $2 = v_{\mathfrak{p}}(A) = 2v_p(A)$, and hence $v_p(A) = 1$.

Now $\mathfrak{p}^3 \mid \mathfrak{a}^3 = (\lambda)$ and $\mathfrak{p}^3 \mid \overline{\mathfrak{a}}^3 = (\overline{\lambda})$, so $\mathfrak{p}^3 \mid (\lambda+\overline{\lambda}) = (G)$. It follows that $p^3 \mid G^2$, and hence $v_p(G) \geq 2$.

Similarly, $p^3 \mid (\lambda-\overline{\lambda})^2 = H^2D'$. We have

$$G^2 - H^2D' = 4A^3. \tag{4.7}$$

Note that $p \mid D'$ as p is ramified in $\mathcal{O}_{\mathbb{L}'}$. If p is odd, then $v_p(D') = 1$, so $v_p(H^2D')$ is odd. Since $v_p(A) = 1$ and $v_p(G) \geq 2$, (4.7) forces $v_p(H^2D') = 3$, so $1 = v_p(A) = v_p(H) < v_p(G)$ as asserted.

For $p = 2$, we have $v_2(4A^3) = 5$ and $v_2(G^2) \geq 4$, so $v_2(H^2D') \geq 4$ by (4.7). Since $v_2(D') \in \{2,3\}$, we have $p \mid H$. If $v_2(G) \geq 3$, then $v_2(H^2D') = v_2(4A^3) = 5$, which forces $v_2(D') = 3$ and $v_2(H) = 1$ as asserted. If $v_2(G) = 2$, then $v_2(H^2D') = v_2(G^2) = 4$, in which case $v_2(D') = 2$ and $v_2(H) = 1$, again as claimed. □

In fact, it can be shown that if $\mathfrak{a}$ as in Lemma 4.3 is primitive, then the elements A and $\lambda / \gcd(G,A)$ form an $\mathcal{O}_{\mathbb{L}'}$-basis of $\mathfrak{a}$. For the case when $\gcd(A,G) = 1$, this is stated in the proof of Theorem 3.3. However, this stronger result is not needed here.

For convenience, we say that a polynomial $f(x) = x^3 - Ex + G \in \mathbb{Z}[x]$ is in *standard form with respect to a prime p* if $p^2 \nmid E$ or $p^3 \nmid G$. So $f(x)$ is in standard form in the sense of Section 1.3 if and only if $f(x)$ is in standard form with respect to every prime $p \in \mathbb{Z}$.

Corollary 4.2. *Let $\lambda \in \mathcal{O}_{\mathbb{L}'} \setminus \mathcal{O}_{\mathbb{L}'}^3$ be a primitive 3-virtual unit. Then the following hold:*

1. *The polynomial $f_\lambda(x)$ of (4.6) is in standard form with respect to every prime $p \neq 3$.*
2. *If the discriminant of the field generated by $f_\lambda(x)$ is divisible by 3, then $f_\lambda(x)$ is in standard form with respect to 3.*
3. *If $f_\lambda(x)$ is not in standard form with respect to 3, then the polynomial*

$$g_\lambda(x) = x^3 - \frac{A}{3}x + \frac{G}{27}$$

has integer coefficients, is in standard form, and generates the same field as $f_\lambda(x)$.

Proof. We have $f_\lambda(x) = x^2 - 3Ax + G$ where $\lambda + \overline{\lambda} = G$ and $\lambda\overline{\lambda} = A^3$. By Lemma 4.3, $v_p(3A) \leq 1$ for all rational primes $p \neq 3$, so $f_\lambda(x)$ is in standard form with respect to every prime $p \neq 3$.

By part 2 of Proposition 4.1, λ is a quadratic generator of some cubic field $\mathbb{K}$. Since $g_\lambda(x) = f_\lambda(3x)/27$, it is clear that $g_\lambda(x)$ is also a generating polynomial of $\mathbb{K}$. If $f_\lambda(x)$ is not in standard form with respect to 3, then $g_\lambda(x)$ has integer coefficients. In that case, $v_3(3A) = 2$ by Lemma 4.3, and hence $v_3(A/3) = 0$. It follows that $g_\lambda(x)$ is in standard form (with respect to all primes). Theorem 2.14 now implies that the discriminant of $\mathbb{K}$ is not divisible by 3. □

Given a 3-virtual unit $\lambda \in \mathcal{O}_{\mathbb{L}'} \setminus \mathcal{O}_{\mathbb{L}'}^3$, it remains to determine the discriminant of the cubic field generated by $f_\lambda(x)$.

Theorem 4.4. *If $\lambda \in \mathcal{O}_{\mathbb{L}'} \setminus \mathcal{O}_{\mathbb{L}'}^3$ is a primitive 3-virtual unit, then the polynomial $f_\lambda(x)$ generates a cubic field $\mathbb{K}$ of discriminant D or $-27D'$.*

Proof. Write $\lambda = (G + H\sqrt{D'})/2$ with $G,H \in \mathbb{Z}$, and put $A^3 = \lambda\overline{\lambda}$. Then the discriminant of $f_\lambda(x)$ is

$$D_{f_\lambda} = 27(4A^3 - G^2) = -27H^2D' = \begin{cases} (9H)^2D & \text{if } 3 \mid D', \\ (3H)^2D & \text{if } 3 \nmid D', \end{cases} \tag{4.8}$$

where D and D' are related via (4.2). So the unique quadratic subfield $\mathbb{L}$ of the Galois closure of $\mathbb{K}$ has discriminant D. By Theorem 2.16, the discriminant of $\mathbb{K}$ is of the form $\Delta = D(3^m g)^2$ where $m \in \{0,1,2\}$, g is square-free, and $\gcd(g, 3D) = 1$. Let p be a prime divisor of Δ. We use Theorem 2.14 to show that $v_p(\Delta) = v_p(D)$ or $v_p(\Delta) = v_p(-27D')$.

For $p \neq 3$, we have $v_p(D) = v_p(-27D')$, and this quantity is equal to $v_p(\Delta)$ if and only if $p \nmid g$. By way of contradiction, suppose some prime divisor $p \neq 3$ of Δ divides g. Then $v_p(\Delta) = 2$. By Theorem 2.14, $1 \leq v_p(G) \leq v_p(3A)$ or, in the case of $p = 2$ only, $D_{f_\lambda}/2^{v_2(D_{f_\lambda})} \equiv 3 \pmod 4$. The first of these two conditions contradicts Lemma 4.3. To see that the second condition is also impossible when $p = 2$, note that $2 \mid g$ and $\gcd(g, 3D) = 1$ together imply that D' is odd. Thus, $D' \equiv 1 \pmod 4$, and $v_2(D_{f_\lambda}) = 2v_2(H)$ by (4.8). It follows that

$$\frac{D_{f_\lambda}}{2^{v_2(D_{f_\lambda})}} = -27D' \left(\frac{H}{2^{v_2(H)}} \right)^2 \equiv 1 \pmod 4.$$

Now consider the case when $p = 3$. Since $3 \mid \Delta$, $f_\lambda(x)$ is in standard form with respect to 3 by Corollary 4.2. As before, Lemma 4.3 precludes $1 \leq v_3(G) < v_3(3A)$ and thus eliminates the case $v_3(\Delta) = 5$. If $v_3(\Delta)$ is odd, then $3 \mid D$, so either $v_3(\Delta) = 1 = v_3(D)$ or $v_3(\Delta) = 3 = v_3(9D) = v_3(-27D')$. If $v_3(\Delta)$ is even, then $3 \nmid D$, in which case $v_3(\Delta) = 4 = v_3(81D) = v_3(-27D')$. This concludes the proof. □

We use Theorem 2.14 to distinguish the cubic fields of discriminant D from those of discriminant $-27D'$.

Theorem 4.5. *Let $\lambda \in \mathcal{O}_{\mathbb{L}'} \setminus \mathcal{O}_{\mathbb{L}'}^3$ be a primitive 3-virtual unit, and let $\mathbb{K}$ be the field generated by $f_\lambda(x) = x^3 - 3Ax + G$ where $\lambda + \overline{\lambda} = G$ and $\lambda\overline{\lambda} = A^3$.*

- *If $f_\lambda(x)$ is not in standard form with respect to 3, then $3 \nmid D$ and $\mathbb{K}$ has discriminant D.*
- *If $f_\lambda(x)$ is in standard form with respect to 3 and $3 \nmid D$, then $\mathbb{K}$ has discriminant D if and only if $A \equiv 1 \pmod 3$ and $G^2 \equiv 3A + 1 \pmod{27}$.*
- *If $f_\lambda(x)$ is in standard form with respect to 3 and $3 \mid D$, then $\mathbb{K}$ has discriminant D if and only if one of the following conditions holds:*

  $3 \nmid A$ and $9 \mid G$ or
  $A \not\equiv 1 \pmod 3$ and $G^2 \equiv 3A + 1 \pmod 9$ or
  $A \equiv 1 \pmod 3$ and $G^2 \equiv 3A + 1 \pmod{27}$.

Proof. Let Δ be the discriminant of $\mathbb{K}$. By Theorem 4.4, $\Delta \in \{D, -27D'\}$. Since $v_3(-27D') \geq 2$, we have $\Delta = D$ if and only if $v_3(\Delta) \leq 1$.

By Lemma 4.3, $v_3(A) \leq 1$, and by Corollary 4.2, $f_\lambda(x)$ is in standard form with respect to all primes $p \neq 3$. Moreover, if $f_\lambda(x)$ is not in standard form with respect to 3, then $v_3(\Delta) = 0$, and hence $v_3(D) = 0$ by Theorem 2.16. In this case, $\Delta = D$.

Suppose now that $f_\lambda(x)$ is in standard form. If $3 \nmid D$, then $\Delta = D$ if and only if $v_3(\Delta) = 0$. Since $3 \mid 3A$, Theorem 2.14 yields that $\Delta = D$ if and only if $3A \equiv 3 \pmod 9$ and $G^2 \equiv 3A+1 \pmod{27}$. If $3 \mid D$, then $\Delta = D$ if and only if $v_3(\Delta) = 1$. Again by Theorem 2.14, $\Delta = D$ if and only if

$1 = v_3(3A) < v_3(G)$ or
$3 \mid 3A$, $3A \not\equiv 3 \pmod 9$ and $G^2 \equiv 3A+1 \pmod 9$ or
$3A \equiv 3 \pmod 9$ and $G^2 \equiv 3A+1 \pmod{27}$. □

Theorem 4.5 is the basis for the following algorithm that converts an input polynomial $f(x) = f_\lambda(x)$ as given in the theorem to standard form if necessary, and detects whether it generates a field of discriminant D or $-27D'$.

Algorithm 4.1 (Detecting the Field Discriminant).
Input: *An irreducible polynomial $g(x) = x^3 - 3Ax + G \in \mathbb{Z}[x]$ that is in standard form except possibly with respect to 3 and generates a field $\mathbb{K}$ of discriminant D or $-27D'$.*
Output: *A pair $(f(x), \texttt{HasDiscD})$ where $f(x)$ is a generating polynomial of $\mathbb{K}$ in standard form and $\texttt{HasDiscD} \in \{0,1\}$ is 1 if $\mathbb{K}$ has discriminant D and 0 otherwise.*
Algorithm:

1. *Put* $\texttt{HasDiscD} = 0$.
2. *If* $3 \nmid D$ *and* $3 \mid A$ *and* $27 \mid G$, *then*
   a. *Replace* $g(x)$ *by* $f(x) = x^3 - (A/3)x + G/27$.
   b. *Put* $\texttt{HasDiscD} = 1$.
   else if $3 \mid D$ *and either* $3 \nmid A$ *and* $9 \mid G$ *or* $A \not\equiv 1 \pmod 3$ *and* $G^2 \equiv 43A+1 \pmod 9$, *then*
   c. *Put* $f(x) = g(x)$.
   d. *Put* $\texttt{HasDiscD} = 1$.
   else if $A \equiv 1 \pmod 3$ *and* $G^2 \equiv 3A+1 \pmod{27}$, *then*
   e. *Put* $f(x) = g(x)$
   f. *Put* $\texttt{HasDiscD} = 1$.
3. *Return* $(f(x), \texttt{HasDiscD})$.

By Corollary 4.2, in all three cases in Step 2, the polynomial $f(x)$ has integer coefficients, is in standard form, and generates $\mathbb{K}$. Moreover, Theorem 4.5 shows that the algorithm sets HasDiscD to 1 if and only if $\mathbb{K}$ has discriminant D.

We remark that in some cases, it is possible to apply transformations to a cubic polynomial $f(x) = x^3 - 3Ax + G$ that decrease the size of the discriminant of $f(x)$. For example, if $A \equiv 1 \pmod 3$ and $G \equiv 3A - 1 \pmod{27}$, put

$$g(x) = \frac{1}{27} f(3x+1) = x^3 + x^2 - Wx + \frac{1}{3}(V - W),$$

where $W = (A-1)/3$ and $V = (G-2)/9$. Then $W \in \mathbb{Z}$ and $(V-W)/3 = (G - 3A + 1)/27 \in \mathbb{Z}$, so $g(x)$ has integer coefficients, and $D_g = D_f/27$. Certain translations of x by integer values can also reduce the size of the discriminant of D_f; see [171] and Theorems 5.8.1 and 5.8.2 of [77]. Our aim, however, is to find cubic polynomials with small coefficients rather than small discriminant.

4.5 From 3-Torsion Ideal Classes of $\mathbb{L}'$ to Cubic Fields

Proposition 4.1 and Theorem 4.4 established that every primitive 3-virtual unit $\lambda \in \mathcal{O}_{\mathbb{L}'} \setminus \mathcal{O}_{\mathbb{L}'}^3$, along with its conjugate $\overline{\lambda}$, is a quadratic generator of a cubic field $\mathbb{K}$ of discriminant D or $-27D'$. Let $\mathfrak{a}$ be the $\mathcal{O}_{\mathbb{L}'}$-ideal such that $\mathfrak{a}^3 = (\lambda)$, $\mathfrak{b}$ an ideal equivalent to $\mathfrak{a}$, and $\alpha \in \mathbb{L}'$ with $\mathfrak{b} = (\alpha)\mathfrak{a}$. Then $\mathfrak{b}^3 = (\alpha^3\lambda)$, so $\alpha^3\lambda$ is also a quadratic generator of $\mathbb{K}$ by Theorem 4.3. It therefore suffices to consider 3-torsion ideal *classes*, paired up with their conjugate (i.e., inverse) classes, for the quadratic generator construction of cubic fields. We will see that each such pair of ideal classes of order exactly 3 gives rise to precisely one cubic field up to conjugation when $D > 1$, and three distinct such fields when $D < -3$. The principal ideal class of $\mathbb{L}'$ produces no cubic field when $D > 1$ and one triple of conjugate cubic fields when $D < -3$.

To that end, we introduce a map that is defined on triples of conjugate cubic fields of discriminant D or -$27D'$ and takes on values consisting of 3-torsion ideal classes, paired with their inverses. This map bears similarities to the exact sequence of Theorem 3.3. For brevity, we define the following sets:

- $\mathcal{K}_\Delta$, the set of triples of conjugate cubic fields $\{\mathbb{K}, \mathbb{K}', \mathbb{K}''\}$ of discriminant Δ;
- $\mathcal{I}_{D'}$, the set of pairs $\{\mathbf{C}, \overline{\mathbf{C}}\}$ where $\mathbf{C}$ is an ideal class of $\mathbb{L}'$ of order 3.

Our goal is to construct generating polynomials of all elements in $\mathcal{K}_D$ via the map

$$\begin{aligned} \Phi : \mathcal{K}_D \cup \mathcal{K}_{-27D'} &\longrightarrow \mathcal{I}_{D'} \cup \{[\mathcal{O}_{\mathbb{L}'}], [\mathcal{O}_{\mathbb{L}'}]\} \\ \{\mathbb{K}, \mathbb{K}', \mathbb{K}''\} &\longmapsto \{[\mathfrak{a}], [\overline{\mathfrak{a}}]\}, \end{aligned} \tag{4.9}$$

where $\mathfrak{a}$ is a primitive ideal of $\mathcal{O}_{\mathbb{L}'}$ such that $\mathfrak{a}^3 = (\lambda)$ for some quadratic generator λ of $\mathbb{K}$.

Proposition 4.2. *The map Φ given in (4.9) is well defined.*

Proof. Firstly, note that every cubic field $\mathbb{K}$ of discriminant D or $-27D'$ has quadratic resolvent field $\mathbb{L}' = \mathbb{Q}(\sqrt{D'})$. So any quadratic generator λ of $\mathbb{K}$ is an element of $\mathcal{O}_{\mathbb{L}'}$ and generates an ideal of the form $\mathfrak{a}^3$ where $\mathfrak{a}$ is an ideal of $\mathcal{O}_{\mathbb{L}'}$. Moreover, by Lemma 4.2, there exists a quadratic generator λ of $\mathbb{K}$ for which $\mathfrak{a}$ is primitive. So the pair $\{[\mathfrak{a}], [\overline{\mathfrak{a}}]\}$ as described above is a valid image of the triple $\{\mathbb{K}, \mathbb{K}', \mathbb{K}''\}$ under Φ.

To establish that this image is unique, let $\{[\mathfrak{a}], [\overline{\mathfrak{a}}]\}$ and $\{[\mathfrak{b}], [\overline{\mathfrak{b}}]\}$ be pairs in $\mathcal{I}_{D'} \cup \{[\mathcal{O}_{\mathbb{L}'}], [\mathcal{O}_{\mathbb{L}'}]\}$ such that $\mathfrak{a}^3 = (\lambda)$, $\mathfrak{b}^3 = (\mu)$ and both λ and μ are quadratic generators of the same triple $\{\mathbb{K}, \mathbb{K}', \mathbb{K}''\} \in \mathcal{K}_D \cup \mathcal{K}_{-27D'}$. By Theorem 4.3, $\lambda = \alpha^3\mu$ or $\lambda = \alpha^3\overline{\mu}$ for some non-zero $\alpha \in \mathbb{L}'$. It follows that $\mathfrak{a} = (\alpha)\mathfrak{b}$ or $\mathfrak{a} = (\alpha)\overline{\mathfrak{b}}$, so $\mathfrak{a}$ is equivalent to $\mathfrak{b}$ or $\overline{\mathfrak{b}}$. Thus, $\{[\mathfrak{a}], [\overline{\mathfrak{a}}]\} = \{[\mathfrak{b}], [\overline{\mathfrak{b}}]\}$. □

We will see that Φ is a bijection onto $\mathcal{I}_{D'}$ when $D' < -3$, while Φ is one-to-one onto the pair $\{[\mathcal{O}_{\mathbb{L}'}], [\mathcal{O}_{\mathbb{L}'}]\}$ and three-to-one onto $\mathcal{I}_{D'}$ when $D' > 1$.

Lemma 4.4. *Every element in $\mathcal{I}_{D'}$ has a non-empty pre-image under Φ.*

Proof. Let $\{\mathbf{C},\overline{\mathbf{C}}\} \in \mathcal{I}_{D'}$. Let $\mathfrak{a} \in \mathbf{C}$ be primitive, and let λ be a generator of $\mathfrak{a}^3$. Since $\mathbf{C}$ is not the principal class, λ is not a cube in $\mathcal{O}_{\mathbb{L}'}$. By part 2 of Proposition 4.1, $f_\lambda(x)$ is the generating polynomial of cubic field $\mathbb{K}$, for which λ is a quadratic generator. By Theorem 4.4, the triple $\{\mathbb{K},\mathbb{K}',\mathbb{K}''\}$ belongs to $\mathcal{K}_D \cup \mathcal{K}_{-27D'}$, and $\Phi(\{\mathbb{K},\mathbb{K}',\mathbb{K}''\}) = \{\mathbf{C},\overline{\mathbf{C}}\}$. □

Note that pre-images of elements in $\mathcal{I}_{D'}$ under Φ may contain more than one triple of fields. Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_{\mathbb{L}'}$ such that $\mathfrak{a}^3$ is principal. If $\mathfrak{a}^3$ has two generators λ_1 and λ_2 such that neither λ_1/λ_2 nor $\lambda_1/\overline{\lambda}_2$ is a cube in $\mathbb{L}'$, then $\Phi^{-1}(\{[\mathfrak{a}],[\overline{\mathfrak{a}}]\})$ contains at least two elements by Theorem 4.3. To obtain the cardinality of each such pre-image, we briefly recall the structure of the unit group $\mathcal{O}^*_{\mathbb{L}'}$ of $\mathcal{O}_{\mathbb{L}'}$.

When $D' < 0$, the only units of $\mathcal{O}_{\mathbb{L}'}$ are roots of unity; these are $\{\pm 1\}$ and, in the case when $D' = -4$, the additional fourth roots of unity $\{\pm i\}$ with $i^2 = -1$. Note that every unit in $\mathbb{L}' = \mathbb{Q}(\sqrt{-4})$ is a cube as $\pm i = \mp i^3$. (There are also roots of unity when $D' = -3$, but recall that we disallow this case here.)

When $D' > 1$, the unit group $\mathcal{O}^*_{\mathbb{L}'}$ is an infinite group of rank 1 with torsion part $\{\pm 1\}$. We denote by $\varepsilon = \varepsilon_{\mathbb{L}'}$ the fundamental unit of $\mathbb{L}'$, i.e., the unique generator of the torsion-free part of $\mathcal{O}^*_{\mathbb{L}'}$ that exceeds 1. Then every coset of $(\mathbb{L}')^*/\mathcal{O}^*_{\mathbb{L}'}$ has a unique *normalized* representative, i.e., a representative λ with $1 \le \lambda < \varepsilon$. Since any two elements of $\mathcal{O}_{\mathbb{L}'}$ generate the same $\mathcal{O}_{\mathbb{L}'}$-ideal if and only if they differ by a factor that is a unit, every non-zero principal ideal has a unique normalized generator.

Theorem 4.6. *Let $D > 1$ be a fundamental discriminant and $D' < -3$ its dual discriminant. Then the pair $\{[\mathcal{O}_{\mathbb{L}'}],[\mathcal{O}_{\mathbb{L}'}]\}$ has no pre-image under Φ, and Φ is a bijection onto $\mathcal{I}_{D'}$.*

Proof. Let $\mathfrak{a}$ be a primitive principal ideal of $\mathcal{O}_{\mathbb{L}'}$ and α a generator of $\mathfrak{a}$. Then every generator λ of $\mathfrak{a}^3$ is of the form $\lambda = \upsilon^3\alpha^3$ for some unit υ, and is hence a cube in $\mathcal{O}_{\mathbb{L}'}$. By part 2 of Proposition 4.1, no triple of fields in $\mathcal{K}_D \cup \mathcal{K}_{-27D'}$ maps to $\{[\mathcal{O}_{\mathbb{L}'}],[\mathcal{O}_{\mathbb{L}'}]\}$ under Φ.

By Lemma 4.4, Φ is surjective onto $\mathcal{I}_{D'}$. To establish injectivity, let $\{\mathbf{C},\overline{\mathbf{C}}\} \in \mathcal{I}_{D'}$, and let $\{\mathbb{K}_1,\mathbb{K}_1',\mathbb{K}_1''\},\{\mathbb{K}_2,\mathbb{K}_2',\mathbb{K}_2''\} \in \mathcal{K}_D \cup \mathcal{K}_{-27D'}$ be pre-images of $\{\mathbf{C},\overline{\mathbf{C}}\}$ under Φ. Let λ_1,λ_2 be quadratic generators of $\mathbb{K}_1,\mathbb{K}_2$, respectively, where $(\lambda_1) = \mathfrak{a}_1^3$ and $\lambda_2 = \mathfrak{a}_2^3$ with primitive ideals $\mathfrak{a}_1,\mathfrak{a}_2$ of $\mathcal{O}_{\mathbb{L}'}$. Then $\{[\mathfrak{a}_1],[\overline{\mathfrak{a}}_1]\} = \{[\mathfrak{a}_2],[\overline{\mathfrak{a}}_2]\} = \{\mathbf{C},\overline{\mathbf{C}}\}$, so $\mathfrak{a}_1$ is equivalent to $\mathfrak{a}_2$ or to $\overline{\mathfrak{a}}_2$. Thus, there exists a non-zero $\alpha \in \mathbb{L}'$ such that $\mathfrak{a}_1 = (\alpha)\mathfrak{a}_2$ or $\mathfrak{a}_1 = (\alpha)\overline{\mathfrak{a}}_2$. It follows that $(\lambda_1) = (\alpha^3\lambda_2)$ or $(\lambda_1) = (\alpha^3\overline{\lambda}_2)$, so $\lambda_1 = \upsilon^3\alpha^3\lambda_2$ or $\lambda_1 = \upsilon^3\alpha^3\overline{\lambda}_2$ for some $\upsilon \in \mathcal{O}^*_{\mathbb{L}'}$. By Theorem 4.3, $\{\mathbb{K}_1,\mathbb{K}_1',\mathbb{K}_1''\} = \{\mathbb{K}_2,\mathbb{K}_2',\mathbb{K}_2''\}$. □

Theorem 4.7. *Let $D < -3$ be a fundamental discriminant and $D' > 1$ its dual discriminant. Then the pair $\{[\mathcal{O}_{\mathbb{L}'}],[\mathcal{O}_{\mathbb{L}'}]\}$ has a unique pre-image under Φ, and Φ is three-to-one onto $\mathcal{I}_{D'}$, i.e., every element in $\mathcal{I}_{D'}$ has three distinct pre-images under Φ.*

Proof. The fundamental unit ε of $\mathbb{L}'$ generates the principal ideal $\mathcal{O}_{\mathbb{L}'}$ and is not a cube in $\mathcal{O}_{\mathbb{L}'}$. So by Theorem 4.4, it is a quadratic generator of some cubic field $\mathbb{K}_0$ of discriminant D or $-27D'$. Thus, $\Phi(\{\mathbb{K}_0,\mathbb{K}_0',\mathbb{K}_0''\}) = \{[\mathcal{O}_{\mathbb{L}'}],[\mathcal{O}_{\mathbb{L}'}]\}$.

To see that $\{\mathbb{K}_0,\mathbb{K}_0',\mathbb{K}_0''\}$ is the unique pre-image of $\{[\mathcal{O}_{\mathbb{L}'}],[\mathcal{O}_{\mathbb{L}'}]\}$ under Φ, let $\mathbb{K}$ be another cubic field of discriminant D or $-27D'$ such that $\Phi(\{\mathbb{K},\mathbb{K}',\mathbb{K}''\}) = \{[\mathcal{O}_{\mathbb{L}'}],[\mathcal{O}_{\mathbb{L}'}]\}$. Then there exists a primitive principal ideal $\mathfrak{b}$ and a generator λ of $\mathfrak{b}^3$ such that λ is a quadratic generator of $\mathbb{K}$. Let β be a generator of $\mathfrak{b}$. Then $\lambda = \pm\varepsilon^m\beta^3$ for some $m \in \mathbb{Z}$. Write $m = 3q + r$ with $|r| \le 1$. Then $\lambda = (\pm\varepsilon^q\beta)^3\varepsilon^r$. Part 2 of Proposition 4.1 forces $r \neq 0$, and Theorem 4.3 yields $\{\mathbb{K},\mathbb{K}',\mathbb{K}''\} = \{\mathbb{K}_0,\mathbb{K}_0',\mathbb{K}_0''\}$ when $r = 1$. Finally, $\varepsilon^{-1} = \overline{\varepsilon}/\varepsilon\overline{\varepsilon} = \pm\overline{\varepsilon}$. So $\lambda = (\pm\varepsilon^q\beta)^3\overline{\varepsilon}$ when $r = -1$, in which case Theorem 4.3 once again establishes that $\{\mathbb{K},\mathbb{K}',\mathbb{K}''\} = \{\mathbb{K}_0,\mathbb{K}_0',\mathbb{K}_0''\}$.

Now let $\{\mathbf{C},\overline{\mathbf{C}}\} \in \mathcal{I}_{D'}$, so $\mathbf{C}$ has order 3. By Proposition 4.4, the pre-image $\Phi^{-1}(\{\mathbf{C},\overline{\mathbf{C}}\})$ contains some triple $\{\mathbb{K},\mathbb{K}',\mathbb{K}''\} \in \mathcal{K}_D \cup \mathcal{K}_{-27D'}$. Let λ be a quadratic generator of $\mathbb{K}$. Then $(\lambda) = \mathfrak{a}^3$ for some primitive ideal $\mathfrak{a}$ that belongs to $\mathbf{C}$ or to $\overline{\mathbf{C}}$. The elements $\varepsilon^i\lambda$ with $-1 \le i \le 1$ are all generators of $\mathfrak{a}$ and are quadratic generators of three distinct cubic fields $\mathbb{K}_i$, $i = -1,0,1$, by Theorem 4.3. So the triples $\{K_i,K_i',K_i''\}$, $i = -1,0,1$, are three distinct pre-images of $\{\mathbf{C},\overline{\mathbf{C}}\}$ under Φ.

To see that $\{\mathbf{C},\overline{\mathbf{C}}\}$ has no other pre-images, let $\mathbb{K}$ be another cubic field of discriminant D or $-27D'$ such that $\Phi(\{\mathbb{K},\mathbb{K}',\mathbb{K}''\}) = \{\mathbf{C},\overline{\mathbf{C}}\}$. Then there exists a primitive ideal $\mathfrak{b}$ in $\mathbf{C}$ or in $\overline{\mathbf{C}}$, and a generator μ of $\mathfrak{b}^3$ such that μ is a quadratic generator of $\mathbb{K}$. Now $\mathfrak{b}$ is equivalent to $\mathfrak{a}$ or to $\overline{\mathfrak{a}}$ so $\mathfrak{b} = (\alpha)\mathfrak{a}$ or $\mathfrak{b} = (\alpha)\overline{\mathfrak{a}}$ for some non-zero $\alpha \in \mathbb{L}'$. It follows that $\mu = \pm\varepsilon^m\alpha^3\lambda$ or $\mu = \pm\varepsilon^m\alpha^3\overline{\lambda}$ for some $m \in \mathbb{Z}$. In the first case, $\mathbb{K} \in \{\mathbb{K}_i,\mathbb{K}_i',\mathbb{K}_i''\}$ where $i \equiv m \pmod 3$ with $|i| \le 1$. Otherwise, we have $\mu = \pm\overline{\varepsilon}^{-m}\alpha^3\overline{\lambda}$, so $\mathbb{K} \in \{\mathbb{K}_i,\mathbb{K}_i',\mathbb{K}_i''\}$ where $i \equiv -m \pmod 3$ with $|i| \le 1$. In either case, $\{\mathbb{K},\mathbb{K}',\mathbb{K}''\} = \{\mathbb{K}_i,\mathbb{K}_i',\mathbb{K}_i''\}$ for some $i \in \{-1,0,1\}$. □

The proofs of Theorems 4.6 and 4.7 provide a road map for finding generating polynomials of all cubic fields of discriminant D or $-27D'$, with $D \notin \{1,-3\}$:

1. Compute primitive representatives $\mathfrak{a}$ of all ideal classes $\mathbf{C}$ with $\{\mathbf{C},\overline{\mathbf{C}}\} \in \mathcal{I}_{D'}$.
2. If $D < -3$, compute the fundamental unit ε of $\mathbb{L}'$ and output $f_\varepsilon(x)$.
3. For each $\mathfrak{a}$ with $\{[\mathfrak{a}],[\overline{\mathfrak{a}}]\} \in \mathcal{I}_{D'}$, do the following:
   a. Compute a generator λ of $\mathfrak{a}^3$.
   b. If $D > 1$, output $f_\lambda(x)$.
   c. If $D < -3$, output $f_\lambda(x)$, $f_{\varepsilon\lambda}(x)$, $f_{\overline{\varepsilon}\lambda}(x)$.

4.6 Small 3-Virtual Units and Reduced Ideals in $\mathcal{O}_{\mathbb{L}'}$

Clearly the method described at the end of the previous section produces all triples of conjugate cubic fields of discriminant D or $-27D'$, and finds exactly one generating polynomial for each such triple. Unfortunately, the quadratic generators obtained in this way can give rise to generating polynomials with very large coefficients, especially when $D < 0$. For example, Step 2 outputs $f_\varepsilon(x) = x^3 \pm 3x + (\varepsilon + \overline{\varepsilon})$. Let

$R = R_{\mathbb{L}'} = \log(\varepsilon)$ be the regulator of $\mathbb{L}'$. Then the analytic class number formula (see Definition 8.32 and Corollary 8.35.1 of [106]) yields

$$2Rh = L(1, \chi_{D'})\sqrt{D'},$$

where h is the class number of $\mathbb{L}'$,

$$L(s, \chi_{D'}) = \sum_{n \in \mathbb{N}} \frac{\chi_{D'}(n)}{n^s}$$

is the Dirichlet L-function of $\mathbb{L}'$, and $\chi_{D'}(n) = (D'/n)$ is the Kronecker symbol (see Definition 1.12 of [106]). By the Cohen-Lenstra heuristic [44], the odd part of h is generally small; e.g., we expect that it is one for approximately 75 percent of all real quadratic fields. Moreover, under the assumption of the generalized Riemann hypothesis for $\mathbb{L}'$, we have $L(1, \chi_{D'}) > C/\log\log(D')$ where $C \approx 0.577$ [131]. Thus, R is frequently of magnitude $\sqrt{D'}$, and since $|\overline{\varepsilon}| = |\varepsilon^{-1}|$ is very small, we have $|\varepsilon + \overline{\varepsilon}| \approx \varepsilon \approx \exp(\sqrt{D'})$. So even for discriminants of modest size, the constant coefficient of $f_\varepsilon(x)$ is far too large to even just write down or store in memory, let alone be computationally suitable.

In general, (4.6) shows that it is computationally desirable to find 3-virtual units λ such that both $\lambda\overline{\lambda}$ and $\lambda + \overline{\lambda}$ are reasonably small in absolute value. To that end, an element $\lambda \in \mathcal{O}_{\mathbb{L}'}$ is defined to be *small* if

$$\begin{aligned} |\lambda| &< (|D'|/3)^{3/4} && \text{when } D' < -3, \\ 1 < \lambda < (D')^{3/2}, \quad |\lambda\overline{\lambda}| &< (D')^{3/2} && \text{when } D' > 1. \end{aligned} \tag{4.10}$$

Lemma 4.5. *Let λ be a small quadratic generator of some cubic field of discriminant D and $f_\lambda(x) = x^3 - 3Ax + G$. Then the following hold:*

$$\begin{aligned} 0 < A < (|D'|/3)^{1/2}, \ |G| &< 2(|D'|/3)^{3/4} && \textit{when } D' < -3, \\ |A| < (D')^{1/2}, \qquad |G| &< (D')^{3/2} && \textit{when } D' > 1. \end{aligned}$$

Proof. The identity $|A| = |\lambda\overline{\lambda}|^{1/3}$ immediately yields the bounds on $|A|$.

Write $\lambda = (G + H\sqrt{D'})/2$. If $D' < 0$, then $A^3 = |\lambda|^2 > 0$, and (4.7) yields

$$G^2 = 4A^3 - H^2|D'| < 4A^3 < 4(|D'|/3)^{3/2}.$$

Now assume $D' > 1$, and note that $|\overline{\lambda}| = |\lambda\overline{\lambda}|/\lambda < (D')^{3/2}$ by (4.10), so

$$|G| + |H|\sqrt{D'} = 2\max\{|\lambda|, |\overline{\lambda}|\} < 2(D')^{3/2}.$$

Suppose $|G| \geq (D')^{3/2}$. Then $|H|\sqrt{D'} < (D')^{3/2} < |G|$, so $G^2 - H^2D' > 0$ and $|H| < |D'|$, which forces $|H| \leq D' - 1$. Also, $H \neq 0$ by Corollary 4.1, and hence

$$4(D')^{3/2} > 4|A|^3 = G^2 - H^2D' > (D')^3 - (D' - 1)^2D' = 2(D')^2 - D'.$$

Solving for D' yields $D' < 5/2 + \sqrt{6} < 5$, which is impossible for a fundamental discriminant D'.

Since the construction of small quadratic generators makes extensive use of ideal arithmetic in $\mathcal{O}_{\mathbb{L}'}$, we briefly summarize some basic results on ideals in $\mathcal{O}_{\mathbb{L}'}$ as described in Sections 4.4–5.3 of Jacobson and Williams Jacobson-Williams [106].

The bounds in (4.10) show that the norm of a principal ideal generated by a small element cannot be too large. The reduced ideals of $\mathcal{O}_{\mathbb{L}'}$ are precisely those ideals that have small norm. A primitive ideal $\mathfrak{a}$ of $\mathcal{O}_{\mathbb{L}'}$ is said to be *reduced* if it does not contain any non-zero element $\alpha \in \mathfrak{a}$ with $|\alpha| < \mathfrak{N}(\mathfrak{a})$ and $|\overline{\alpha}| < \mathfrak{N}(\mathfrak{a})$; when $D' < 0$, we have $|\alpha| = |\overline{\alpha}|$, so these two inequalities condense to one. If $\mathfrak{a}$ is reduced, then

$$\mathfrak{N}(\mathfrak{a}) < \begin{cases} \sqrt{|D'|/3} & \text{when } D' < 0, \\ \sqrt{D'} & \text{when } D' > 1. \end{cases} \tag{4.11}$$

Conversely, if $\mathfrak{N}(\mathfrak{a}) < \sqrt{|D'|}/2$, then $\mathfrak{a}$ is reduced. Every ideal class of $\mathbb{L}'$ contains at least one reduced ideal and at most finitely many reduced ideals. If $D' < 0$, then every ideal class $\mathbf{C}$ contains at most two reduced ideals, and the only scenario where $\mathbf{C}$ contains two distinct reduced ideals is when $\mathbf{C}$ has order 2 and the two reduced ideals in $\mathbf{C}$ are conjugate to each other. When $D' > 1$, in general, every ideal class contains a large number of reduced ideals; this number is bounded below by $2R/\log(D')$.

A 3-virtual unit $\lambda \in \mathcal{O}_{\mathbb{L}'}$ is said to be reduced if $(\lambda) = \mathfrak{a}^3$ where $\mathfrak{a}$ is a reduced ideal. In this case, $|\lambda\overline{\lambda}| = \mathfrak{N}(\mathfrak{a})^3$, so by (4.11), $\lambda\overline{\lambda}$ satisfies the bounds in (4.10). When $D' < 0$, this shows that every reduced 3-virtual unit is small. When $D' > 1$ and $\varepsilon \geq (D')^{3/2}$, every non-trivial ideal $\mathfrak{a}^3$ with $\mathfrak{a}$ reduced has at most one small generator; this small generator, if it exists, is the unique normalized generator of $\mathfrak{a}^3$. Thus, the way to obtain small 3-virtual units is by way of reduced ideals in every 3-torsion ideal class whose cubes have small generators.

Recall that $\mathcal{O}_{\mathbb{L}'} = \mathbb{Z} \oplus \mathbb{Z}\omega$ where $\omega = (s + \sqrt{D'})/2$ and $s \in \{0, 1\}$ is given by $s \equiv D' \pmod 4$. Every ideal $\mathfrak{a}$ of $\mathcal{O}_{\mathbb{L}'}$ is a $\mathbb{Z}$-submodule of $\mathcal{O}_{\mathbb{L}'}$. If $\mathfrak{a}$ is primitive, then $\mathfrak{a}$ has rank 2 over $\mathbb{Z}$ and a $\mathbb{Z}$-basis of the form $\{a, b + \omega\}$ where $a, b \in \mathbb{Z}$ and a divides $(b + \omega)(b + \overline{\omega})$. Here, a is unique up to sign, and b can be chosen so that $|2b + s| \leq |a|$. We write $\mathfrak{a} = [a, b + \omega]$. Since $\mathfrak{a}\overline{\mathfrak{a}} = (a)$, we have $|a| = \mathfrak{N}(\mathfrak{a})$. Given two primitive ideals $\mathfrak{a}_1 = [a_1, b_1 + \omega]$ and $\mathfrak{a}_2 = [a_2, b_2 + \omega]$, integers s, a, b such that $\mathfrak{a}_1\mathfrak{a}_2 = (s)\mathfrak{c}$ with $\mathfrak{c} = [a, b + \omega]$ can be efficiently computed.

Let $\mathfrak{a} = [a, b + \omega]$ be a primitive ideal of $\mathcal{O}_{\mathbb{L}'}$, and let $a', b' \in \mathbb{Z}$ be given by the identity

$$\frac{b' + \omega}{a'} = \frac{1}{\frac{b+\omega}{a} - q},$$

where

$$q = \begin{cases} \lfloor (2b + s)/2a \rceil & \text{when } D' < 0, \\ \lfloor (b + \omega)/a \rfloor & \text{when } D' > 1. \end{cases}$$

Here, $\lfloor r \rfloor$ denotes the largest integer not exceeding $r \in \mathbb{R}$, and $\lceil r \rfloor = \lfloor r + 1/2 \rfloor$ is the nearest integer to r. Note that when $D' > 0$, q is the first partial quotient and $(b' + \omega)/a'$ the subsequent complete quotient of the simple continued fraction expansion of $(b + \omega)/a$ as defined in §1.9. We have

$$b' = qa - b - s, \quad a' = -\frac{(b' + \omega)(b' + \overline{\omega})}{a},$$

and $[a', b' + \omega]$ is a primitive ideal that we denote by $\rho(\mathfrak{a})$. The ideal $\rho(\mathfrak{a})$ is equivalent to $\mathfrak{a}$; specifically

$$\rho(\mathfrak{a}) = (\psi)\mathfrak{a} \quad \text{with} \quad \psi = \frac{b' + \omega}{a} \in \mathbb{L}'.$$

Repeated application of the ρ-operator, starting with some primitive non-reduced ideal $\mathfrak{a} = [a, b + \omega]$, produces a reduced ideal equivalent to $\mathfrak{a}$; this process is referred to as reducing $\mathfrak{a}$. Here, $\mathfrak{N}(\rho^{i+1}(\mathfrak{a})) < \mathfrak{N}(\rho^i(\mathfrak{a}))$ as long as $\rho^i(\mathfrak{a})$ is not reduced. If k is the minimal index i such that $\mathfrak{N}(\rho^{i+1}(\mathfrak{a})) \geq \mathfrak{N}(\rho^i(\mathfrak{a}))$ when $D' < 0$ and $0 < \mathfrak{N}(\rho^i(\mathfrak{a})) < \sqrt{D'}/2$ when $D' > 1$, then $\mathfrak{r} = \rho^k(\mathfrak{a})$ is reduced. In the latter case, we have $\mathfrak{r} = (\theta)\mathfrak{a}$ where $\theta \in \mathbb{L}'$ and $\mathfrak{N}(\mathfrak{a})^{-1} < |\theta| < 2$; the reduction process computes both $\mathfrak{r}$ and θ efficiently and simply entails computing a portion of the simple continued fraction of $(b + \omega)/a$ of appropriate length. For both positive and negative discriminants, the number k of reduction steps required to obtain $\mathfrak{r}$ from $\mathfrak{a}$ is linear in $\log(\mathfrak{N}(\mathfrak{a})/\sqrt{|D'|})$.

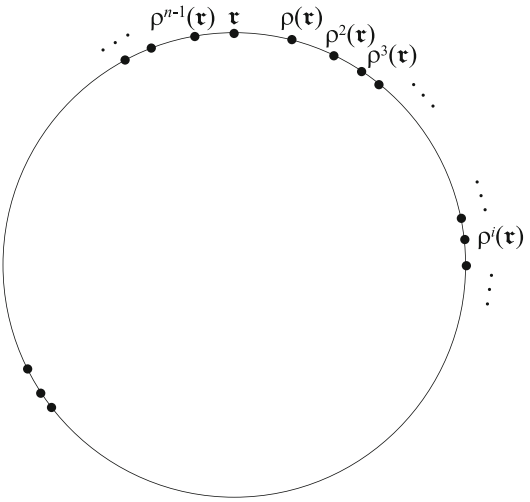

Fig. 4.1 The infrastructure of the ideal class of a reduced ideal $\mathfrak{r}$. The circumference of the circle is the regulator of $\mathbb{L}'$. The length of the arc from $\mathfrak{r}$ to an ideal $\mathfrak{b} = \rho^i(\mathfrak{r})$ is given by $\log(\theta)$ where $\mathfrak{b} = (\theta)\mathfrak{r}$ and $1 \leq \theta < \varepsilon$.

Assume that $D' > 1$ for the remainder of this section. Then continued application of ρ, starting with $\mathfrak{r}$, generates the entire collection of reduced ideals in the class $\mathbf{C} = [\mathfrak{a}]$, known as the *infrastructure* of $\mathbf{C}$ [168]. Here, $\rho^i(\mathfrak{r}) = (\psi_i)\rho^{i-1}(\mathfrak{r})$ with $\psi_i > 1$, $-1 < \overline{\psi}_i < 0$, and $\psi_{i+1}\psi_i > 2$. If n is the number of reduced ideals in $\mathbf{C}$, then $\rho^n(\mathfrak{r}) = \mathfrak{r}$ and $\psi_1\psi_2\cdots\psi_n = \varepsilon$. Hence, the ρ-orbit of $\mathfrak{r}$ is cyclic, and cycle of reduced ideals in the class $\mathbf{C} = [\mathfrak{r}]$ can be considered as a finite set of points on a circle whose circumference is R, the regulator of $\mathbb{L}'$. The location of an ideal $\rho^i(\mathfrak{r})$ on this circle is determined by an arc of length $\log(\psi_1\psi_2\cdots\psi_i)$ from $\mathfrak{r}$ to $\rho^i(\mathfrak{r})$, as depicted in Figure 4.1. Note that if $\mathfrak{b} = [a', b'+\omega] \neq \mathcal{O}_{\mathbb{L}'}$ is reduced, then the ideal $\rho^{-1}(\mathfrak{b})$, i.e., the ideal $\mathfrak{a}$ with $\rho(\mathfrak{a}) = \mathfrak{b}$, is given by $\mathfrak{a} = [a, b+\omega]$ where $a = -(b'+\omega)(b'+\overline{\omega})/a'$ and $b = q'a - b' - t$ with $q' = \lfloor (b'+\omega)/a \rfloor$. The ρ-operator exhibits a symmetry with respect to conjugation of reduced ideals: if $\mathfrak{b} = \rho(\mathfrak{a})$, then $\overline{\mathfrak{a}} = \rho(\overline{\mathfrak{b}})$.

Let R be the regulator of $\mathbb{L}'$, $\mathfrak{r}$ any reduced ideal of $\mathcal{O}_{\mathbb{L}'}$, and $r \in [0, R)$. Then there exists at a unique reduced ideal $\mathfrak{a}$ equivalent to $\mathfrak{r}$ such that if $\mathfrak{a} = (\alpha)\mathfrak{r}$ and $\rho(\mathfrak{a}) = (\alpha')\mathfrak{r}$ with α, α' normalized, then $\log(\alpha) \leq r < \log(\alpha')$. Define the ideal

$$\mathfrak{a}[r, \mathfrak{r}] = \begin{cases} \mathfrak{a} & \text{if } |\log(\alpha) - r| \leq |\log(\alpha') - r|, \\ \rho(\mathfrak{a}) & \text{otherwise.} \end{cases}$$

When $\mathfrak{r} = \mathcal{O}_{\mathbb{L}'}$, we write $\mathfrak{a}[r] = \mathfrak{a}[r, \mathcal{O}_{\mathbb{L}'}]$ for brevity. Thus, $\mathfrak{a}[r]$ is the reduced principal ideal for which the logarithm of the normalized generator δ is closest to r. More generally, $\mathfrak{a}[r, \mathfrak{r}]$ can be thought of as the reduced ideal closest to r relative to $\mathfrak{r}$; see Figure 4.2.

Suppose $\mathfrak{a}[r, \mathfrak{r}] = (\beta)\mathfrak{r}$ with $\beta \in \{\alpha, \alpha'\}$. Since $\alpha' = \psi\alpha$ with $1 < \psi < \sqrt{D'}$, we obtain

$$2|r - \log(\beta)| < (r - \log(\alpha)) + (\log(\alpha') - r) = \log(\psi) < \log(D')/2,$$

and hence $|r - \log(\beta)| < \log(D')/4$.

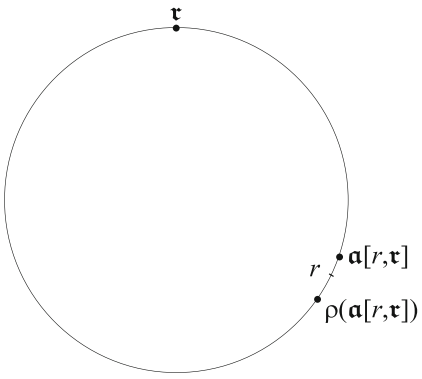

Fig. 4.2 The ideal $\mathfrak{a}[r, \mathfrak{r}]$ closest to r with respect to $\mathfrak{r}$. Note that $\mathfrak{a}[r, \mathfrak{r}]$ is slightly closer to r on the circle that its neighbor $\rho(\mathfrak{a}[r, \mathfrak{r}])$.

Given r, the ideal $\mathfrak{a}[r]$ and a good approximation of $\log(\delta)$, where δ is the normalized generator of $\mathfrak{a}[r]$, can be found efficiently using a technique akin to binary exponentiation (see Algorithm 11.6 of [106]). In general, $\mathfrak{a}[r,\mathfrak{r}]$ can be efficiently computed as follows. First find $\mathfrak{a}[r]$, along with an approximation of $\log(\delta)$, where δ is the normalized generator of $\mathfrak{a}[r]$. Next, obtain the reduction $\mathfrak{b} = (\theta)\mathfrak{r}\mathfrak{a}[r]$ of $\mathfrak{r}\mathfrak{a}[r]$, where $\theta \in \mathbb{L}'$. Then $\mathfrak{b} = (\theta\delta)\mathfrak{r}$, so an appropriate number of applications of ρ or ρ^{-1}, starting with $\mathfrak{b}$, produces the ideal $\mathfrak{a}[r,\mathfrak{r}]$.

The ideals $\mathfrak{r}$ and $\mathfrak{a}[r]$ are both reduced and hence have norm less than $\sqrt{D'}$ by (4.11). So $(D')^{-1} < \mathfrak{N}(\mathfrak{a}[r]\mathfrak{r})^{-1} < |\theta| < 2$ and $|\log(\delta) - r| < \log(D')/4$. It follows that

$$-\frac{5\log(D')}{4} < \log(\delta|\theta|) - r < \frac{\log(D')}{4} + \log(2).$$

Recall that $\rho^2(\mathfrak{a}) = (\alpha)\mathfrak{a}$ with $\alpha > 2$ for any reduced ideal $\mathfrak{a}$; similarly, $\rho^{-2}(\mathfrak{a}) = (\beta)\mathfrak{a}$ with $0 < \beta < 1/2$. Hence the number of applications of ρ or ρ^{-1} to obtain $\mathfrak{a}[r,\mathfrak{r}]$ from $\mathfrak{b}$ is polynomially bounded in $\log(D')$. In summary, the ideal $\mathfrak{a}[r,\mathfrak{r}]$, along with a good approximation of the normalized element β with $\mathfrak{a}[r,\mathfrak{r}] = (\beta)\mathfrak{r}$, can be found efficiently.

4.7 Computing Ideal Cubes with Small Generators

When $D' < 0$, we saw that every reduced 3-virtual unit is small. For the remainder of this section, we therefore assume that $D' > 1$ and solve the problem of finding small 3-virtual units in two stages. First, we compute in each 3-torsion ideal class $\mathbf{C}$ of $\mathbb{L}'$ one reduced ideal when $\mathbf{C}$ is principal and three reduced ideals when $\mathbf{C}$ has order 3 such that the cube of any of these ideals has a small generator. We give explicit expressions for these small generators. However, the quantities in these formulas are far too large to be suitable for computation, so we provide a more efficient way of finding the corresponding small 3-virtual units in the next section.

If $R < 3\log(D')/2$, then the fundamental unit ε is a small generator of $\mathcal{O}_{\mathbb{L}}^3 = \mathcal{O}_{\mathbb{L}'}$ that is not a cube in $\mathcal{O}_{\mathbb{L}'}$ and is hence a small quadratic generator of the triple of conjugate cubic fields in $\Phi^{-1}(\{[\mathcal{O}_{\mathbb{L}'}],[\mathcal{O}_{\mathbb{L}'}]\})$. In this case, ε can easily be found by traversing the infrastructure of principal ideals, starting at $\mathcal{O}_{\mathbb{L}'}$, via the ρ-operator.

When $R \geq 3\log(D')/2$, we compute an ideal $\mathfrak{a}_0$ located approximately one third of the way into the infrastructure cycle of the principal class, close to $R/3$. We also determine in any non-principal class of order 3 three reduced ideals $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3$ that are separated from each other by a distance of approximately $R/3$ and thus correspond to the corners of an equilateral triangle. The cubes of all these ideals have small generators. The locations of these four ideals in their respective infrastructure cycles are depicted in Figure 4.3.

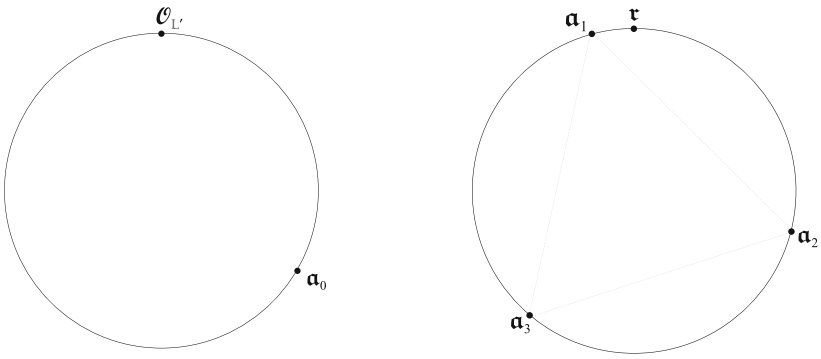

Fig. 4.3 Left: the ideal $\mathfrak{a}_0$ of Theorem 4.8 is located near $R/3$, about one third of the way into the principal infrastructure cycle. Right: the ideals $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3$ of Theorem 4.9 form an equilateral triangle inside the infrastructure cycle of $\mathfrak{r}$. The location of the corners of this triangle on the circle is determined by the size of the generator δ of $\mathfrak{r}^3$.

Theorem 4.8. *Let $D' > 1$, and assume that $R \geq 3\log(D')/2$. Put*

$$\mathfrak{a}_0 = \mathfrak{a}\left[\frac{R}{3} + \frac{\log(D')}{4}\right], \qquad \lambda_0 = \alpha_0^3 \varepsilon^{-1},$$

where α_0 is the normalized generator of $\mathfrak{a}_0$. Then the following hold:

1. *$\mathfrak{a}_0 \neq \mathcal{O}_{\mathbb{L}'}$.*
2. *λ_0 is the unique small generator of $\mathfrak{a}_0^3$ and is hence a small 3-virtual unit.*
3. *λ_0 is a small quadratic generator of the triple of conjugate cubic fields in $\Phi^{-1}(\{[\mathcal{O}_{\mathbb{L}'}], [\mathcal{O}_{\mathbb{L}'}]\})$.*

Proof. Put $r = R/3 + \log(D')/4$ for brevity. Then $r > \log(D')/4 > 0$, and $R \geq 3\log(D')/2$ implies $\log(D')/4 \leq R/6$ and hence $r \leq R/2 < R$. It follows that the ideal $\mathfrak{a}_0 = \mathfrak{a}[r]$ is defined and is distinct from $\mathcal{O}_{\mathbb{L}'}$. Since $\varepsilon \geq (D')^{3/2}$, $\mathfrak{a}_0$ has at most one small generator.

It is clear that λ_0 is a generator of $\mathfrak{a}_0^3$ that is not a cube in $\mathcal{O}_{\mathbb{L}'}$, and is thus a quadratic generator of a triple of conjugate cubic fields in $\Phi^{-1}(\{[\mathcal{O}_{\mathbb{L}'}], [\mathcal{O}_{\mathbb{L}'}]\})$. To see that λ_0 is small, note first that $|\lambda_0 \overline{\lambda}_0| = \mathfrak{N}(\mathfrak{a}_0)^3 < (D')^{3/2}$, since $\mathfrak{a}_0$ is reduced. Moreover, $|\log(\alpha_0) - r| < \log(D')/4$ yields

$$-\frac{\log(D')}{4} < \log(\alpha_0) - r = \log(\alpha_0) - \frac{R}{3} - \frac{\log(D')}{4} < \frac{\log(D')}{4}.$$

Hence $0 < 3\log(\alpha_0) - R < 3\log(D')/2$, which in turn yields $1 < \lambda_0 < (D')^{3/2}$. □

Theorem 4.9. *Let $D' > 1$, $\mathfrak{r}$ a reduced ideal whose class has order 3, and δ a generator of $\mathfrak{r}^3$. Put*

$$k = \left\lfloor \frac{\log((D')^{3/4}/\delta)}{R} \right\rfloor,$$

$$\mathfrak{a}_i = \mathfrak{a}\left[\frac{(i-1-k)R - \log(\delta)}{3} + \frac{\log(D')}{4}, \mathfrak{r} \right] \quad (i = 1,2,3),$$

$$\lambda_i = \alpha_i^3 \delta \varepsilon^{k-i+1} \quad (i = 1,2,3),$$

where $\alpha_i \in \mathbb{L}'$ is normalized such that $\mathfrak{a}_i = (\alpha_i)\mathfrak{r}$. Then the following hold:

1. *The element λ_i is a small generator of $\mathfrak{a}_i^3$ for $i = 1,2,3$ and is hence a small 3-virtual unit.*
2. *λ_1, λ_2, λ_3 are small quadratic generators of the three distinct triples of conjugate cubic fields in $\Phi^{-1}(\{[\mathfrak{r}], [\overline{\mathfrak{r}}]\})$.*

Proof. The definition of k implies that $k \le \log((D')^{3/4}\delta^{-1})/R < k+1$, so

$$0 \le \frac{3\log(D')}{4} - (kR + \log(\delta)) < R.$$

For brevity, put

$$r_i = \frac{(i-1-k)R - \log(\delta)}{3} + \frac{\log(D')}{4} \quad (i = 1,2,3).$$

Then $0 \le 3r_1 < R < 3r_1 + R < 2R < 3r_1 + 2R < 3R$. Since $r_3 = r_2 + R/3 = r_1 + 2R/3$, we obtain

$$0 \le r_1 < \frac{R}{3} \le r_2 < \frac{2R}{3} \le r_3 < R.$$

So the ideals $\mathfrak{a}_1$, $\mathfrak{a}_2$, $\mathfrak{a}_3$ are defined and equivalent to $\mathfrak{r}$. It is also clear that λ_i is a generator of $\mathfrak{a}_i^3$ for $i = 1,2,3$. The argument that λ_i is small proceeds analogous to the proof of Theorem 4.8: we have $|\log(\alpha_i) - r_i| < \log(D')/4$ and hence

$$0 < 3\log(\alpha_i) - (i-1-k)R + \log(\delta) < \frac{3\log(D')}{2},$$

which in turn implies that $1 < \lambda_i < (D')^{3/2}$, for $i = 1,2,3$. Moreover, no λ_i is a cube in $\mathbb{L}'$ as otherwise $\mathfrak{a}_i$ would be principal, contradicting the fact that $\mathfrak{a}_i$ belongs to an ideal class of order 3. So each λ_i is a small quadratic generator of a triple of conjugate cubic fields in $\Phi^{-1}(\{[\mathfrak{r}], [\overline{\mathfrak{r}}]\})$.

To see that the fields thus obtained are distinct up to $\mathbb{Q}$-isomorphism, it suffices to show by Theorem 4.3 that none of the quotients λ_i/λ_j and $\lambda_i/\overline{\lambda}_j$, $1 \le i < j \le 3$, is a cube in $\mathbb{L}'$. We have $\lambda_i/\lambda_j = (\alpha_i/\alpha_j)^3 \varepsilon^{j-i}$ with $0 \le j-i \le 2$, which is a cube if and only if $i = j$. If $\lambda_i/\overline{\lambda}_j$ were a cube, then $\mathfrak{a}_i$ would be equivalent to both $\mathfrak{a}_j$ and $\overline{\mathfrak{a}}_j$, which would force the order of $[\mathfrak{a}_j] = [\mathfrak{r}]$ to be at most 2. □

The computation of the ideals $\mathfrak{a}_i$ $(0 \le i \le 3)$ of Theorems 4.8 and 4.9 requires knowledge of the regulator R of $\mathbb{L}'$ which can be computed using any of the methods

discussed in Sections 7.4 and 10.2 of [106]. In addition, the logarithm of a generator δ of $\mathfrak{r}^3$ is needed which can be obtained as follows. Reduce the ideal $\mathfrak{r}^3$ to obtain a reduced ideal $\mathfrak{c}$ and an element $\theta \in \mathbb{L}'$ such that $\mathfrak{c} = (\theta)\mathfrak{r}^3$. Put $\log(\delta) = \log(\gamma) - \log(|\theta|)$ where γ is the normalized generator of $\mathfrak{c}$. This process for finding $\log(\delta)$ is efficient provided that the logarithm of the normalized generator γ of $\mathfrak{c}$ is given. When R is known, this quantity can be obtained using techniques that are similar to those for computing the regulator; see Section 7.4 and Chapter 13 of [106]. In practice, sufficiently good approximations of R, $\log(\delta)$, and other irrational numbers involved in the computations need to be used.

A note on the quantity k of Theorem 4.9. Since $(D')^{-3/2} < \mathfrak{N}(\mathfrak{r})^{-3} < |\theta| < 2$ and $1 \le \gamma < \varepsilon$, we have $1/2 < \delta < \varepsilon(D')^{3/2}$; in particular, δ need not be normalized. The definition of k and the bounds on δ imply

$$\varepsilon^k \le \frac{(D')^{3/4}}{\delta} < \varepsilon^{k+1}, \qquad \frac{1}{\varepsilon(D')^{3/4}} < \frac{(D')^{3/4}}{\delta} < 2(D')^{3/4}.$$

We thus obtain $\varepsilon^k < 2(D')^{3/4}$ and $\varepsilon^{k+2} > \varepsilon(D')^{3/4}/\delta > (D')^{-3/4}$. If $\varepsilon \ge 2(D')^{3/4}$, which is almost always the case, then this forces $-2 \le k \le 0$. Even when $\varepsilon < 2(D')^{3/4}$, we still obtain the bounds $-3 \le k \le 1$.

In general, ε as well as α_0, α_1, α_2, α_3, and δ are far too large to compute the small 3-virtual units λ_i $(0 \le i \le 3)$ of Theorems 4.8 and 4.9 using the formulas given in these theorems. In the next section, so we describe an algorithm for obtaining small generators of the ideals $\mathfrak{a}_0$, $\mathfrak{a}_1$, $\mathfrak{a}_2$, $\mathfrak{a}_3$ defined in Theorems 4.8 and 4.9 that avoids computing these large quantities.

4.8 Computing Small 3-Virtual Units

When $D' < 0$, every reduced 3-virtual unit is small. In this case, computing small 3-virtual units is straightforward:

Algorithm 4.2 (Small 3-Virtual Units, $D' < -3$).
Input: *A reduced $\mathcal{O}_{\mathbb{L}'}$-ideal $\mathfrak{a}$ whose ideal class has order 3.*
Output: *A small generator λ of $\mathfrak{a}^3$ that is not a cube in $\mathcal{O}_{\mathbb{L}'}$.*
Algorithm:

1. *Compute a primitive ideal $\mathfrak{b}$ and an integer s such that $(s)\mathfrak{b} = \mathfrak{a}^3$.*
2. *Repeatedly apply the ρ-operator, starting with $\mathfrak{b}$, to obtain $\theta \in \mathbb{L}'$ with $\mathfrak{b} = (\theta)$.*
3. *Output $\lambda = s\theta$.*

To see that this algorithm is correct, note that since $\mathcal{O}_{\mathbb{L}'}$ is the only reduced principal ideal, $\mathfrak{a}^3$ is equivalent to $\mathcal{O}_{\mathbb{L}'}$. So θ^{-1} is obtained by reducing the primitive part $\mathfrak{b}$ of $\mathfrak{a}^3$ via repeated application of ρ. Then $\mathfrak{a}^3 = (s)\mathfrak{b} = (s\theta)$, so $\lambda = s\theta$ is a generator of $\mathfrak{a}^3$, which is small since $\mathfrak{a}$ is reduced. Finally, λ is not a cube in $\mathcal{O}_{\mathbb{L}'}$ since $\mathfrak{a}$ is not principal.

We now turn to the case $D' > 1$. The search for small 3-virtual units makes use of the following idea. Suppose $\mathfrak{a} = \mathfrak{a}_i$ for some $i \in \{0,1,2,3\}$ with $\mathfrak{a}_i$ defined in Theorems 4.8 and 4.9, where we preclude the case $R < 3\log(D)/2$, $\mathfrak{a}_0 = \mathcal{O}_{\mathbb{L}'}$ and $\lambda_0 = \varepsilon$ from consideration. Then $\overline{\lambda}$ is a small generator of $\overline{\mathfrak{a}}^3$, so we can search for λ in the infrastructure of the class of $\mathfrak{a}$ and for $\overline{\lambda}$ in the infrastructure of $[\overline{\mathfrak{a}}] = [\mathfrak{a}^2]$ simultaneously as follows. Square $\mathfrak{a}$ and reduce the primitive part of $\overline{\mathfrak{a}}^2$ to obtain a reduced ideal $\mathfrak{c}$ equivalent to $\mathfrak{a}$. Now apply ρ simultaneously to $\mathfrak{c}$ and $\overline{\mathfrak{c}}$ until $\mathfrak{a}$ or $\overline{\mathfrak{a}}$ is found. The process of traversing one or, in some case, both these infrastructures produces a small 3-virtual unit.

Algorithm 4.3 (Small 3-Virtual Units, $D' > 1$).
Input: *An ideal $\mathfrak{a}$ that is one of the ideals $\mathfrak{a}_i$ defined in Theorems 4.8 and 4.9.*
Output: *A small generator λ of the cube of the input ideal such that λ is not a cube in $\mathcal{O}_{\mathbb{L}'}$.*
Algorithm:

1. *Compute a primitive ideal $\mathfrak{b}$ and a positive integer s such that $(s)\mathfrak{b} = \mathfrak{a}^2$.*
2. *Repeatedly apply the ρ-operator, starting with $\overline{\mathfrak{b}}$, to obtain a reduced ideal $\mathfrak{c}$ and an element $\gamma \in \mathbb{L}'$ such that $\mathfrak{c} = (\gamma)\overline{\mathfrak{b}}$ and $\gamma > 0$.*
3. *Put $\phi = s\mathfrak{N}(\mathfrak{b})\gamma$.*
4. *Repeatedly apply the ρ-operator simultaneously, starting with $\mathfrak{c}$ and $\overline{\mathfrak{c}}$, until $\mathfrak{a}$ or $\overline{\mathfrak{a}}$ is found. In the process, compute elements $\theta, \psi \in \mathbb{L}$ such that $\rho^k(\mathfrak{c}) = (\theta)\mathfrak{c}$ and $\rho^k(\overline{\mathfrak{c}}) = (\psi)\overline{\mathfrak{c}}$, where $k \geq 0$ is the number of applications of ρ.*
5. *If $\mathfrak{a}$ was encountered first in Step 4, then*
   a. *if $\phi\theta < (D')^{3/2}$, then*
      i. *Put $\lambda = \phi\theta$*
   else
      ii. *Continue to apply the ρ-operator, starting with $\rho^k(\overline{\mathfrak{c}})$, until $\overline{\mathfrak{a}}$ is found. In the process, update ψ so that $\overline{\mathfrak{a}} = (\psi)\overline{\mathfrak{c}}$.*
      iii. *Put $\lambda = \phi|\overline{\psi}|$.*
   else // *$\overline{\mathfrak{a}}$ was encountered first in Step 4*
   b. *if $\phi|\overline{\psi}| > 1$, then*
      i. *Put $\lambda = \phi|\overline{\psi}|$*
   else
      ii. *Continue to apply the ρ-operator, starting with $\rho^k(\mathfrak{c})$, until $\mathfrak{a}$ is found. In the process, update θ so that $\mathfrak{a} = (\theta)\mathfrak{c}$.*
      iii. *Put $\lambda = \phi\theta$.*
6. *Output λ*

The correctness of this algorithm is established in the next theorem.

Theorem 4.10. *If $\mathfrak{a}$ is the input ideal of Algorithm 4.3, then the output λ is a small generator of $\mathfrak{a}^3$ that is not a cube in $\mathcal{O}_{\mathbb{L}'}$.*

Proof. Note that $\mathfrak{c}$ is equivalent to $\overline{\mathfrak{a}}^2$ and hence to $\mathfrak{a}$ since the class of $\mathfrak{a}$ has order 1 or 3. Similarly, $\overline{\mathfrak{c}}$ is equivalent to $\overline{\mathfrak{a}}$. Hence, the quantities θ and ψ computed in Step 5 satisfy $\mathfrak{a} = (\theta)\mathfrak{c}$, $\overline{\mathfrak{a}} = (\psi)\overline{\mathfrak{c}}$ where either $\theta = 1$ or $\theta > 1$ and $-1 \leq \overline{\theta} < 0$;

similarly, either $\psi = 1$ or $\psi > 1$, and $-1 \leq \overline{\psi} < 0$. Moreover, $\mathfrak{N}(\mathfrak{b})^{-1} < \gamma < 2$, so $s^2\mathfrak{N}(\mathfrak{b}) = \mathfrak{N}(\mathfrak{a})^2$ and $\mathfrak{N}(\mathfrak{a}) < (D')^{1/2}$ yield

$$1 \leq s < s\mathfrak{N}(\mathfrak{b})\gamma = \frac{\mathfrak{N}(\mathfrak{a})^2\gamma}{s} < 2D',$$

and hence $1 < \phi < 2D$.

Put $\mu = \phi\theta$ and $\nu = \phi|\overline{\psi}|$. Then the algorithm outputs either μ or ν. We have $\mathfrak{a} = (\theta)\mathfrak{c} = (\theta\gamma)\overline{\mathfrak{b}}$ and hence

$$\mathfrak{a}^3 = (s)\mathfrak{b}\mathfrak{a} = (s\theta\gamma\mathfrak{N}(\mathfrak{b})) = (\phi\theta) = (\mu).$$

Similarly, $\overline{\mathfrak{a}} = (\psi)\overline{\mathfrak{c}} = (\psi\overline{\gamma})\mathfrak{b}$, so $\mathfrak{a}^3 = (s)\mathfrak{b}\mathfrak{a} = (s\overline{\psi}\gamma\mathfrak{N}(\mathfrak{b})) = (\phi\overline{\psi}) = (\nu)$. It follows that Algorithm 4.3 outputs a generator of $\mathfrak{a}^3$.

We claim that μ or ν is small. To see this, note that $\phi > 1$ and $\theta \geq 1$ together imply $\mu > 1$. Suppose μ is not small. Then $\mu \geq (D')^{3/2}$. If $R \leq 3\log(D')/2$, then this implies $\mu \geq \varepsilon$. If $R > 3\log(D')/2$, then we must also have $\mu \geq \varepsilon$, since the unique normalized generator of $\mathfrak{a}^3$ is known to be small and can hence not be equal to μ. Now $|\overline{\psi}| \leq 1$ and $\phi < 2D'$ yield $\nu \leq 2D' < (D')^{3/2}$, so $\nu \neq \mu$ and hence $\theta \neq |\overline{\psi}|$. By the symmetry property of the ρ-operator with respect to ideal conjugation, we must have $\theta = |\overline{\psi}|\varepsilon$, and hence $\mu = \nu\varepsilon$. Thus, $\nu < (D')^{3/2}$ and $\nu = \mu/\varepsilon > 1$, so ν is small.

Consider the stage when the algorithm reaches Step 5, and suppose first that $\mathfrak{a}$ was encountered first in Step 4. If the *if* clause in Step 5 a is satisfied, then the output is $\lambda = \mu$. Since $1 < \mu < (D')^{3/2}$ in this case, λ is a small generator. If the *if* clause in Step 5 a does not hold, then μ is not small. In his case, the algorithm enters the *else* clause in Step 5 a and outputs ν which is small.

Similarly, consider the situation where $\overline{\mathfrak{a}}$ was encountered first in Step 4. If the *if* portion of Step 5 b is entered, then $\nu > 1$, so ν is small, and the algorithm correctly outputs ν. If the *if* part of Step 5 b is bypassed and the *else* clause holds, then $\nu < 1$ and hence ν is not small. In this case, the algorithm outputs $\lambda = \mu$ which is small.

Finally, we establish that λ is not a cube in $\mathcal{O}_{\mathbb{L}'}$. If $\mathfrak{a}$ is not principal, then no generator of $\mathfrak{a}^3$ is a cube. If $\mathfrak{a}$ is principal, then $R \geq 3\log(D')/2$ by Theorem 4.8. In this case, λ is the unique small generator of $\mathfrak{a}^3$ which by Theorem 4.8 is not a cube in $\mathcal{O}_{\mathbb{L}'}$. □

We now investigate the size of the quantities $\phi, \gamma, \theta, \psi \in \mathbb{L}'$ computed throughout the algorithm. Each of these quantities is of the form $\kappa = (u + v\sqrt{D'})2N$ where $u, v, N \in \mathbb{Z}$ and N is the norm of some appropriate ideal. We have $|u| \leq N(|\kappa| + |\overline{\kappa}|)$ and $|v| \leq N(|\kappa| + |\overline{\kappa}|)/\sqrt{D'}$, so to ascertain the size of κ, we need to find upper bounds on $|\kappa|$, $|\overline{\kappa}|$, and N.

For $\kappa = \phi$, we have $N = 1$, $1 < \phi < 2D'$, and

$$|\overline{\phi}| = \frac{\phi|\overline{\phi}|}{\phi} < \phi|\overline{\phi}| = s^2\mathfrak{N}(\mathfrak{b})^2\gamma) = s^2\mathfrak{N}(\mathfrak{b})\mathfrak{N}(\mathfrak{c}) = \mathfrak{N}(\mathfrak{a})^2\mathfrak{N}(\mathfrak{c}) < (D')^{3/2}.$$

For $\kappa = \gamma$, we have $N = \mathfrak{N}(\mathfrak{b}) < D'$, $\mathfrak{N}(\mathfrak{b})^{-1} < \gamma < 2$, and

$$|\overline{\gamma}| = \frac{|\gamma\overline{\gamma}|}{\gamma} < |\gamma\overline{\gamma}|\mathfrak{N}(\mathfrak{b}) = \mathfrak{N}(\mathfrak{c}) < (D')^{1/2}.$$

For $\kappa = \theta$ and $\kappa = \psi$, we have $N = \mathfrak{N}(\mathfrak{c}) < (D')^{1/2}$ as well as $|\overline{\theta}| \le 1$ and $|\overline{\psi}| \le 1$ throughout Steps 4 and 5. Moreover, $\theta \ge 2^{k/2}$ and $\psi \ge 2^{k/2}$ after Step 4. If μ is small, then $\theta = \mu/\phi < \mu < (D')^{3/2}$. Moreover, $k \le 2\log_2(\theta) < 3\log(D')$, and ψ is a product of k elements in $\mathbb{L}'$ that arise from the repeated application of the ρ-operator. Each of these factors is bounded above by $\sqrt{D'}$. In practice, however, each factor will be much smaller and is in fact bounded by an integer of the form $q+1$ where q is a partial quotient in the simple continued fraction expansion of a reduced quadratic irrational. Every such q is expected to be small by Theorem 1.10. Hence we do not expect ψ to be too large. Similarly, if ν is small, then

$$\psi = \frac{\psi|\overline{\psi}|}{|\overline{\psi}|} = \frac{\mathfrak{N}(\mathfrak{a})}{\mathfrak{N}(\mathfrak{c})}\,\frac{\phi}{\nu} < \mathfrak{N}(\mathfrak{a})\phi < 2(D')^{3/2}.$$

In this case $2^{k/2} \le \psi < 2(D')^{3/2}$, so $k < 3\log_2(D') + 2$, and θ is a product of k elements in $\mathbb{L}'$ that are again expected to be small. Hence, assuming that θ and ψ do not contain too many large factors, all integers computed throughout Algorithm 4.3 are polynomially bounded in D'.

4.9 The CUFFQI Algorithm

We now have all the ingredients for computing small generating polynomials of all cubic fields of a given fundamental discriminant $D \notin \{1, -3\}$ up to $\mathbb{Q}$-isomorphism. Optionally, we can also collect such polynomials for all cubic fields of discriminant $-27D'$. As always, we begin with the easier case of negative fundamental discriminants.

Algorithm 4.4 (Complete Collection of Cubic Fields of Discriminant $D > 1$).
Input: *A fundamental discriminant $D > 1$.*
Output: *A list $\mathcal{K}_D$ of generating polynomials in standard form of triples of conjugate cubic fields of discriminant D.*
*(*Optional: *A list $\mathcal{K}_{-27D'}$ of generating polynomials in standard form of triples of conjugate cubic fields of discriminant $-27D'$.)*
Algorithm:

1. *Put* $D' = -3D/\gcd(3, D)^2$.
2. *Initialize* $\mathcal{K}_D = \emptyset$.
   *(*Optional: *initialize* $\mathcal{K}_{-27D'} = \emptyset$.*)*
3. *Compute a basis* $\mathcal{B} = \{[\mathfrak{r}_1], [\mathfrak{r}_2], \ldots, [\mathfrak{r}_{r'}]\}$ *of the 3-torsion subgroup of the ideal class group of* $\mathbb{L}' = \mathbb{Q}(\sqrt{D'})$*, where* $\mathfrak{r}_i$ *is reduced for* $1 \le i \le r'$.

4. *For $i = 1$ to r' do*
   a. *Compute a small generator λ of $\mathfrak{r}^3$ using Algorithm 4.2.*
   b. *Put $A = (\lambda\overline{\lambda})^{1/3}$ and $G = \lambda + \overline{\lambda}$.*
   c. *Run Algorithm 4.1 on the input polynomial $g(x) = x^3 - 3Ax + G$ to obtain a pair $(f(x), \texttt{HasDiscD})$.*
   d. *If $\texttt{HasDiscD}) = 1$, then append $f(x)$ to $\mathcal{K}_D$.*
   *(*Optional: *else append $f(x)$ to $\mathcal{K}_{-27D'}$.)*
5. *Return $\mathcal{K}_D$. (*Optional: *return $\mathcal{K}_{-27D'}$.)*

By Theorems 4.4 and 4.6, this algorithm computes a complete list, without duplicates, of generating polynomials of all the triples of conjugate cubic fields of discriminant D or $-27D'$. The call to Algorithm 4.1 ensures that all these polynomials are in standard form and are placed in the corrects lists $\mathcal{K}_D$ and $\mathcal{K}_{-27D'}$.

The most time-consuming part of this algorithm is Step 3, the computation of a basis $\mathcal{B}$ of 3-torsion ideal classes. Such a basis can be obtained via Sutherland's method [182] or by computing the entire ideal class group of $\mathbb{L}'$ using one of the algorithms discussed in Section 10.4 of [106].

Next, we turn to the case of negative fundamental discriminants.

Algorithm 4.5 (Complete Collection of Cubic Fields of Discriminant $D < -3$).
Input: *A fundamental discriminant $D < -3$.*
Output: *A list $\mathcal{K}_D$ of generating polynomials in standard form of triples of conjugate cubic fields of discriminant D.*
*(*Optional: *A list $\mathcal{K}_{-27D'}$ of generating polynomials in standard form of triples of conjugate cubic fields of discriminant $-27D'$.)*
Algorithm:

1. *Put $D' = -3D/\gcd(3, D)^2$.*
2. *Initialize $\mathcal{K}_D = \emptyset$.*
   *(*Optional: *initialize $\mathcal{K}_{-27D'} = \emptyset$.)*
3. *Compute the regulator R of $\mathbb{L}' = \mathbb{Q}(\sqrt{D'})$.*

   // *Cubic fields arising from the class of principal ideals*

4. *If $R < 3\log(D')/2$, then*
   a. *Compute the fundamental unit ε of $\mathbb{L}'$.*
   b. *Put $\lambda_0 = \varepsilon$.*
   else
   c. *Compute the ideal $\mathfrak{a}_0$ of Theorem 4.8.*
   d. *Compute a small generator λ_0 of $\mathfrak{a}^3$ using Algorithm 4.3.*
5. *Put $A_0 = (\lambda_0\overline{\lambda}_0)^{1/3}$ and $G_0 = \lambda_0 + \overline{\lambda}_0$.*
6. *Run Algorithm 4.1 on the input polynomial $g(x) = x^3 - 3A_0x + G_0$ to obtain a pair $(f(x), \texttt{HasDiscD})$.*
7. *If $\texttt{HasDiscD} = 1$, then append $f(x)$ to $\mathcal{K}_D$.*
   *(*Optional: *else append $f(x)$ to $\mathcal{K}_{-27D'}$.)*

   // *Cubic fields arising from the ideal classes of order 3*

8. *Compute a basis $\mathcal{B} = \{[\mathfrak{r}_1], [\mathfrak{r}_2], \ldots, [\mathfrak{r}_{r'}]\}$ of the 3-torsion subgroup of the ideal class group of $\mathbb{L}' = \mathbb{Q}(\sqrt{D'})$, where $\mathfrak{r}_i$ is reduced for $1 \le i \le r'$.*

9. *For* $j = 1$ *to* r' *do*
   a. *Compute the logarithm of a generator* δ_j *of* $\mathfrak{r}_j$.
   b. *For* $i = 1,2,3$ *do*
      i. *Compute the ideal* $\mathfrak{a}_i$ *of Theorem 4.9 from* $\mathfrak{r} = \mathfrak{r}_j$ *and* $\log(\delta_j)$.
      ii. *Compute a small generator* λ_i *of* $\mathfrak{a}_i^3$ *using Algorithm 4.3.*
      iii. *Put* $A_i = (\lambda_i\overline{\lambda_i})^{1/3}$ *and* $G_i = \lambda_i + \overline{\lambda}_i$.
      iv. *Run Algorithm 4.1 on the input polynomial* $g(x) = x^3 - 3A_ix + G_i$ *to obtain a pair* $(f(x), \texttt{HasDiscD})$.
      v. *If* $\texttt{HasDiscD}) = 1$, *then append* $f(x)$ *to* $\mathcal{K}_D$.
      (Optional: *else append* $f(x)$ *to* $\mathcal{K}_{-27D'}$).
10. *Return* $\mathcal{K}_D$. (Optional: *return* $\mathcal{K}_{-27D'}$.)

Once again, this algorithm outputs a complete list of generating polynomials, each in standard form, of all the triples of conjugate cubic fields of discriminant D or $-27D'$, with no duplicates. The run time of this algorithm is dominated by Steps 3 (computing the regulator), 8 (computing a basis of the 3-torsion subgroup of the ideal class group of $\mathbb{L}'$), and 9 a (computing the logarithm of a generator of each of the reduced ideas representing the basis ideal classes).

We conclude this section with a brief note on the restriction to fundamental discriminants, an assumption that is crucial for the CUFFQI algorithm. The construction of all cubic fields of an arbitrary, not necessarily fundamental discriminant is significantly more complicated and less efficient. The count for such fields, i.e., a generalization of Theorem 4.1 (Hasse's Theorem), was given by Reichardt (Satz 7 of [157]); see also Theorem 1.1 of Mayer [142]. Algorithms for constructing all cubic fields — and in fact more generally, all fields of prime degree — of a given discriminant are described in Chapter 5 of [42] and make use of class field theory and Kummer theory.

4.10 Detecting Escalatory Versus Non-escalatory from CUFFQI

It is interesting to note that for any fixed fundamental discriminant $D \notin \{1,-3\}$, the CUFFQI construction makes it possible to ascertain whether the field $\mathbb{L} = \mathbb{Q}(\sqrt{D})$ falls under the escalatory or non-escalatory scenario. In fact, this is completely determined by the existence or non-existence of cubic fields of discriminant $-27D'$. To make this more precise, we use the properties of the map Φ described in Theorems 4.6 and 4.7 to compute the cardinalities of the domain and range of Φ, and ultimately, of the set $\mathcal{K}_{-27D'}$.

To obtain the cardinality $|\mathcal{I}_{D'}|$, note that the 3-torsion subgroup of the class group of $\mathbb{L}'$ contains $3^{r'}$ elements, where r' is the 3-rank of the class group. Removing the principal class and pairing up each 3-torsion class $\mathbf{C}$ with its inverse $\mathbf{C}^{-1} = \overline{\mathbf{C}}$ yields a count of

$$|\mathcal{I}_{D'}| = \frac{3^{r'}-1}{2}. \tag{4.12}$$

By Hasse's Theorem (Theorem 4.1), we have $|\mathcal{K}_D| = (3^r - 1)/2$ where r is the 3-rank of the class group of $\mathbb{L}$.

If $D > 1$, then $\Phi : \mathcal{K}_D \cup \mathcal{K}_{-27D'} \to \mathcal{I}_{D'}$ is a bijection by Theorem 4.6, so

$$|\mathcal{K}_{-27D'}| = |\mathcal{I}_{D'}| - |\mathcal{K}_D| = \frac{3^{r'} - 3^r}{2}.$$

By Scholz's Theorem (Theorem 4.2), $r = r'$ or $r = r' - 1$ (note that since $D > 0$, the roles of D and D' in Theorem 4.2 are reversed). In the non-escalatory case, we have $r = r'$, so there are no cubic fields of discriminant $-27D'$, whereas the escalatory case has $r = r' - 1$, and thus there are 3^r non-conjugate cubic fields of discriminant $-27D'$.

If $D < -3$, then Φ is three-to-one onto $\mathcal{I}_{D'}$ and one-to-one onto the pair $\{[\mathcal{O}_{\mathbb{L}'}], [\mathcal{O}_{\mathbb{L}'}]\}$, by Theorem 4.7. So

$$|\mathcal{K}_D \cup \mathcal{K}_{-27D'}| = 3|\mathcal{I}_{D'}| + 1 = \frac{3^{r'+1} - 1}{2},$$

and hence

$$|\mathcal{K}_{-27D'}| = \frac{3^{r'+1} - 1}{2} - |\mathcal{K}_D| = \frac{3^{r'+1} - 3^r}{2}.$$

In the non-escalatory case, there are 3^r non-conjugate cubic fields of discriminant $-27D'$, while in the escalatory case, when $r = r' + 1$, there are no cubic fields of discriminant $-27D'$.

It is worth noting that a special case of Satz 7 of [157]) yields

$$|\mathcal{K}_{3^{2m}D}| = \frac{3^{r'+s'} - 1}{2} - |\mathcal{K}_D|,$$

where D is a fundamental discriminant, m is as described in Theorem 2.16, and s' is the rank of the unit group $\mathcal{O}^*_{\mathbb{L}'}$, i.e., $s' = 0$ when $D > 0$ and $s' = 1$ when $D < 0$. Applied to the CUFFQI situation, this yields $|\mathcal{K}_{-27D'}| = (3^{r'+s'} - 3^r)/2$, in agreement with the counts obtained above.

4.11 Cubic Field Tabulation

Closely related to the construction of all fields of a given discriminant is the problem of field tabulation; that is, producing a table containing generating polynomials of all fields of some fixed degree and discriminant Δ where $|\Delta| \leq X$ for some given bound $X \in \mathbb{N}$. The naive way to accomplish this is to construct for each discriminant Δ with $1 < \pm\Delta \leq X$ all fields of the given degree and discriminant Δ. However, for cubic fields, Belabas [10] presented a far more efficient algorithm based on the Davenport-Heilbronn correspondence (3.10) and reduction theory of integral binary cubic forms as described in §3.2 and §3.3. Here, we must point out that the definition

of the term integral binary cubic form (IBCF) in §1.3 included the requirement of irreducibility over $\mathbb{Z}$, whereas Belabas considered arbitrary integral homogeneous polynomials of degree 3 in two variables which need not be irreducible over $\mathbb{Z}$. Consequently, the definition of a reduced (but not necessarily irreducible) integral bivariate homogeneous cubic polynomial involves more conditions than those stated in §3.2 and §3.3.

Let $N_\pm(X)$ denote the number of cubic fields of discriminant Δ with $1 < \pm\Delta \le X$. Then

$$N_\pm(X) = \frac{C_\pm}{12\zeta(3)}X + \frac{4\sqrt{C_\pm}\zeta(1/3)}{5\Gamma(2/3)^3\zeta(5/3)}X^{5/6} + O\left(X^{7/9+\varepsilon}\right), \tag{4.13}$$

as $X \to \infty$, for any $\varepsilon > 0$. Here, $C_+ = 1$, $C_- = 3$, ζ is the Riemann zeta function and Γ the gamma function. The leading term in (4.13) was established by Davenport and Heilbronn [60]; the approximate values of the corresponding constants are 0.0693 for real cubic fields and $3 \cdot 0.0693 \approx 0.2079$ for complex cubic fields. The secondary term was conjectured by Roberts [159] and implicitly by Datskovsky-Wright [56], and subsequently proved independently by Taniguchi-Thorne [183] (with the asymptotic error term above) and by Bhargava-Shankar-Tsimerman [21] (with an error estimate of $O\left(X^{13/16+\varepsilon}\right)$).

The count in (4.13) shows that the computational effort of any algorithm for producing generating polynomials of all $N_\pm(X)$ cubic fields must be at least proportional to X. Belabas' algorithm achieves this asymptotic run time. For completeness, we outline his technique here; however, since the method is described in detail in [10] and Chapter 8 of [42], we merely provide a brief overview.

Let $\mathcal{W}$ denote the set of all $GL_2(\mathbb{Z})$-equivalence classes of IBCFs, $\mathcal{U} \subset \mathcal{W}$ the subset of all classes of IBCFs that are index forms of some cubic field, and $\mathcal{K}$ the set of all triples of conjugate cubic fields. Then the Davenport-Heilbronn correspondence is a bijection $\varphi : \mathcal{K} \to \mathcal{U}$ that maps a triple $\{\mathbb{K}, \mathbb{K}', \mathbb{K}''\}$ of conjugate cubic fields to the $GL_2(\mathbb{Z})$-equivalence class of an index form $\mathcal{C}(x,y)$ for $\mathbb{K}$. Its inverse is the map $\varphi^{-1} : \mathcal{U} \to \mathcal{K}$ that sends the class of an IBCF $\mathcal{C}(x,y)$ to the triple $\{\mathbb{K}, \mathbb{K}', \mathbb{K}''\} \in \mathcal{K}$ for which $\mathcal{C}(x,y)$ is an index form. Thus, this map is precisely the bijection between $\mathbb{Q}$-isomorphism classes of cubic fields and their reduced index forms (RIF).

Not every IBCF is the index form of some cubic field. For example, we will see in Examples 4.1 and 4.2 below that the class of $\mathcal{C} = (3, 91, 6, -3)$ belongs to $\mathcal{U}$, while the class of $\mathcal{C} = (1, 90, 6, -1)$ does not. In fact, the proportion of classes in $\mathcal{W}$ of discriminant bounded in absolute value by X that belong to $\mathcal{U}$ approaches $\pi^2\zeta(3)/6 \gtrapprox 0.5$ as $X \to \infty$, so roughly half the classes in $\mathcal{W}$ correspond to index forms for cubic fields.

To describe the set $\mathcal{U}$ explicitly, some auxiliary sets need to be defined first. Let

$$\mathcal{V}_2 = \{[\mathcal{C}] \in \mathcal{W} \mid \operatorname{disc}(\mathcal{C}) \equiv 1 \pmod 4 \text{ or } \operatorname{disc}(\mathcal{C}) \equiv 8, 12 \pmod{16}\},$$
$$\mathcal{V}_p = \{[\mathcal{C}] \in \mathcal{W} \mid p^2 \nmid \operatorname{disc}(\mathcal{C})\},$$

where p is any odd prime. Note that $\bigcap_p \mathcal{V}_p$ consists of all classes $[\mathcal{C}] \in \mathcal{W}$ such that $\mathrm{disc}(\mathcal{C})$ is a fundamental discriminant. Now define for any prime p the set $\mathcal{U}_p$ to be the collection of all $[\mathcal{C}] \in \mathcal{W}$ such that either $[\mathcal{C}] \in \mathcal{V}_p$ or there exist $\lambda \in \mathbb{F}_p^*$ and $\alpha, \beta \in \mathbb{F}_p$, not both zero, such that

$$\mathcal{C}(x,y) \equiv \lambda(\alpha x - \beta y)^3 \pmod{p} \quad \text{and} \tag{4.14}$$

$$\mathcal{C}(\beta,\alpha) \not\equiv 0 \pmod{p^2}. \tag{4.15}$$

The image $\mathcal{U}$ of $\mathcal{K}$ under the Davenport-Heilbronn map φ is $\mathcal{U} = \bigcap_p \mathcal{U}_p$. Belabas found the following computationally suitable descriptions of the sets $\mathcal{U}_p$:

Lemma 4.6. *Let $\mathcal{C}(x,y) = ax^3 + bx^2y + cxy^2 + dy^3 \in \mathbb{Z}[x,y]$ with $\gcd(a,b,c,d) = 1$. Let A,B,C be as in (1.40), and let p a prime. Then the following hold:*

1. *$\mathcal{C}$ and p satisfy (4.14) if and only $p \mid \gcd(A,B,C)$.*
2. *Suppose $\mathcal{C}$ and p satisfy (4.14). Then they satisfy (4.15), i.e., $[\mathcal{C}] \in \mathcal{U}_p$, if and only if the following hold:*
   a. *Case $p \neq 3$: $p^3 \nmid \mathrm{disc}(\mathcal{C})$;*
   b. *Case $p = 3$: either $v_3(ad) = 1$ or $v_3(ad) = 0$ and $v_3(a+b+c+d) \geq 2$ when $3 \mid a+d$, $v_3(a-b+c-d) \geq 2$ when $3 \mid a-d$.*

Belabas also established that every class in $\mathcal{U}$ consists of irreducible polynomials only, and hence of IBCFs in the sense of §1.3. This provides the following algorithm for membership in $\mathcal{U}$:

Algorithm 4.6 (Membership in $\mathcal{U}$).
Input: $\mathcal{C}(x,y) = ax^3 + bx^2y + cxy^2 + dy^3 \in \mathbb{Z}[x,y]$ *with* $\gcd(a,b,c,d) = 1$.
Output: `true` *if* $[\mathcal{C}] \in \mathcal{U}$, `false` *otherwise*
Algorithm:

1. *Compute A,B,C as defined in (1.40). Put $t = B^2 - 4AC$ and $s = \gcd(A,B,C)$.*
2. *If $[\mathcal{C}] \notin \mathcal{U}_2$ or $[\mathcal{C}] \notin \mathcal{U}_3$, return* `false`.
3. *If there exists a prime $p \geq 5$ with $p^2 \mid s$, return* `false`.
4. *Replace t by $t/3s^2$ and subsequently by $t/\gcd(t,72)$. If $\gcd(s,t) > 1$, return* `false`.
5. *If t is square-free, return* `true`, *else return* `false`.

Note that $t = -3\,\mathrm{disc}(\mathcal{C})$ in Step 1 by (3.6). Step 2 can easily be verified using Lemma 4.6. To understand Step 3, note that if $p^2 \mid s$ for some prime $p \geq 5$, then $p^4 \mid t$, so $[\mathcal{C}] \notin \mathcal{U}_p$ by Lemma 4.6. In order for $-t/3$ to be the discriminant of a cubic field, Theorem 2.16 forces $v_2(t) \leq 3$, $v_3(t) \leq 5$ and $v_p(t) \leq 2$ for all primes $p \geq 5$. The first two of these conditions hold since $\mathcal{C}$ passed Step 2; moreover, $3 \mid s$. Putting $t' = t/3s^2$, we see that t' is square-free except possibly for powers of 2 and 3, and for these powers we have $v_3(t') \leq 3$ and $v_3(t') \leq 2$. Dividing t' by $\gcd(t',72)$ removes all remaining powers of 2 and 3 from t', leaving only prime factors $p \geq 5$ that do not divide s (possibly as squares of higher powers). The final test in Step 5 ensures that t' is indeed square-free.

Example 4.1. Consider the PIBCF

$$\mathcal{C} = (3, 91, 6, -3).$$

Its Hessian is $\mathcal{Q} = (8227, 627, 855)$, so we have $t = -27743211$ and $s = 19$. Since $t \equiv 1 \pmod 4$, we see that $[\mathcal{C}] \in \mathcal{V}_2$, and since $v_3(t) = 2$, and hence $v_3(\mathrm{disc}(\mathcal{C})) = 1$, we also have $[\mathcal{C}] \in \mathcal{V}_3$. Hence $[\mathcal{C}] \in \mathcal{U}_2$ and $[\mathcal{C}] \in \mathcal{U}_2$. Now $t/3s^2 = 25617$, and $\gcd(25617, 72) = 8539$ which is coprime to 19 and square-free. Hence the class of $\mathcal{C}$ belongs to $\mathcal{U}$.

Example 4.2. Consider the PIBCF

$$\mathcal{C} = (1, 90, 6, -1).$$

Its Hessian is $\mathcal{Q} = (8087, 549, 306)$, so we have $t = -9590967 \equiv 1 \pmod 4$ and $s = 9$. Since $3^4 \mid t$, and hence $3^3 \mid \mathrm{disc}(\mathcal{C})$, we see that $[\mathcal{C}] \notin \mathcal{V}_3$. We have $a = 1$ and $d = -1$, so $3 \mid a + d$. Since $v_3(1 + 90 + 6 - 1) = v_3(6) = 1$, Lemma 4.6 establishes that $[\mathcal{C}] \notin \mathcal{U}_3$, and hence $[\mathcal{C}] \notin \mathcal{U}$. This means that there is no cubic field for which $\mathcal{C}$ is an index form.

Given any $X \in \mathbb{N}$, Belabas' algorithm produces a list $\mathcal{L}$ of generating polynomials of all cubic fields of discriminant Δ with $0 < \Delta \le X$ or $0 > \Delta \ge -X$. The basic idea is to run four nested loops over appropriately bounded integers a, b, c, d. Each 4-tuple (a, b, c, d) defines an IBCF $\mathcal{C}$. The algorithm begins each loop iteration by checking whether $\mathcal{C}$ is primitive and reduced, i.e., is the unique reduced representative of some class in $\mathcal{W}$, and whether the corresponding Hessian has discriminant bounded by $-3X$ in absolute value. If this holds, Algorithm 4.6 is executed to establish membership in $\mathcal{U}$. If all tests are passed, the algorithm stores the cubic polynomial $\mathcal{C}(x, 1)$, along with its discriminant, in $\mathcal{L}$. The potentially costly factorizations of s in Step 3 and t in Step 5 of Algorithm 4.6 can be avoided through a pre-computation, after which square factor testing requires only a small number of trial divisions and a binary search that can be optimized via hashing; for details, see [10].

The bounds on the loops for a, b, c arise from the conditions on the coefficients of a reduced homogeneous cubic polynomial in $\mathbb{Z}[x, y]$. In the case of positive discriminants, they are given by

$$1 \le a \le \frac{2X^{1/4}}{\sqrt{27}}, \quad 0 \le b \le \frac{3a}{2} + \sqrt{\sqrt{X} - \frac{27a^2}{4}}, \quad \frac{b^2 - q}{3a} \le c \le b - 3a,$$

where $q > 0$ is the unique real root of $f(T) = 4T^3 - (3a + 2b)T^2 - 27a^2X$. For negative discriminants, the loop bounds are somewhat simpler:

$$1 \le a \le 2\left(\frac{X}{27}\right)^{1/4}, \quad 0 \le b \le \frac{3a}{2} + \sqrt{\sqrt{\frac{X}{3}} - \frac{3a^2}{4}}, \quad 1 - b \le c \le u + \left(\frac{X}{4a}\right)^{1/3},$$

where $u = b^2/3a$ if $a > 2b/3$ and $u = b - 3a/4$ otherwise.

For any triple (a,b,c), the discriminant of $\mathcal{C}(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$ as given in (1.49) is a quadratic equation in d, yielding the condition $1 < |\operatorname{disc}(\mathcal{C})| \le X$ for looping over d. For positive discriminants, (3.15) yields the additional bounds $|bc - 9ad| \le b^2 - 3ac \le c^2 - 3bd$.

Belabas computed all cubic fields of discriminants bounded by 10^{11} in absolute value; just over 6.7 billion totally real cubic fields and 20 billion complex cubic fields. These numbers are slightly below the expected counts obtained when considering only the leading term in (4.13), due to the fact that the secondary term in (4.13) is negative.

In [12], Belabas described several improvements to his algorithm and provided a detailed complexity analysis. The algorithm requires $O(X)$ integer operations and space $O(X^{3/4})$, and allows for time-memory trade-offs. A variant of the technique, also described in [12], can be used to find quadratic fields whose class group has large 3-rank. Firstly, only a check whether a given discriminant is fundamental, i.e., a test for membership in $\mathcal{V}$, is required. Secondly, instead of writing generating polynomials to a list, all non-fundamental discriminants are discarded, and a counter N_Δ is attached to each fundamental discriminant Δ that keeps track of the number of cubic fields of discriminant Δ. By Theorem 4.1, N_Δ is of the form $(3^{r_\Delta} - 1)/2$ where r_Δ is the 3-rank of the class group of the quadratic resolvent field $\mathbb{Q}(\sqrt{\Delta})$. In this way, large values of N_Δ yield quadratic fields with class groups of large 3-rank.

Belabas' code for enumerating cubic fields, called *cubic*, is available for free download on his research webpage https://www.math.u-bordeaux.fr/~kbelabas/research/ under the heading "Software."