Short representation of quadratic integers

Johannes Buchmann
Christoph Thiel
Fachbereich Informatik
Universität des Saarlandes
6600 Saarbrücken
Germany

Hugh Williams
Department of Computer Science
University of Manitoba
Winnipeg, Manitoba
Canada, R3T2N2

August 10, 1993

Abstract

Let $\mathcal{O}$ be a real quadratic order of discriminant Δ. For elements α in $\mathcal{O}$ we develop a compact representation whose binary length is polynomially bounded in $\log\log \mathrm{H}(\alpha)$, $\log \mathrm{N}(\alpha)$ and $\log \Delta$ where $\mathrm{H}(\alpha)$ is the height of α and $\mathrm{N}(\alpha)$ is the norm of α. We show that using compact representations we can in polynomial time compute norms, signs, products, and inverses of numbers in $\mathcal{O}$ and principal ideals generated by numbers in $\mathcal{O}$. We also show how to compare numbers given in compact represention in polynomial time.

1 Introduction

Let $\Delta \in \mathbb{Z}$ be a *quadratic discriminant*, i.e. Δ is not a square in $\mathbb{Z}$ and $\Delta \equiv 0, 1 \bmod 4$. Then $\mathcal{O}_\Delta = \mathbb{Z} + \frac{\Delta+\sqrt{\Delta}}{2}\mathbb{Z}$ is the *quadratic order* of discriminant Δ. Any $\alpha \in \mathcal{O}_\Delta$ can be uniquely represented as

$$\alpha = \frac{x + y\sqrt{\Delta}}{2} \tag{1}$$

where $x, y \in \mathbb{Z}$. This representation will be called the *standard representation* of α in $\mathcal{O}_\Delta$. The *norm* of α is $\mathrm{N}(\alpha) = (x^2 - y^2\Delta)/4$, the *height* of α is $\mathrm{H}(\alpha) = \max\{|x + y\sqrt{\Delta}|, |x - y\sqrt{\Delta}|\}/2$. We also set $\mathrm{C}(\alpha) = \max\{|x|, |y|\}$.

In real quadratic orders there are many integers of small absolute norm and very big height. For example, assuming the extended Riemann hypothesis and that Δ is sufficiently large, the number of bits needed to write down the standard representation of the fundamental unit of $\mathcal{O}_\Delta$ is at least $\sqrt{\Delta}/(9h \log \Delta)$ where h is the class number of $\mathcal{O}$. This will be shown in section 3. Notions like fundamental unit and class number will be explained in section 2 which is a fairly self contained introduction to the algorithmic theory of real quadratic fields as it is used in this paper. Since according to the heuristics of Cohen and Lenstra [3] the odd part of the class number is one with probability at least 75% it is therefore completely impossible to write down the fundamental unit for most of the real quadratic orders. The binary length of its standard representation grows exponentially in $\log \Delta$. Therefore, there cannot be a polynomial time algorithm which on input of Δ determines the standard representation of the fundamental unit of $\mathcal{O}_\Delta$. Similarly, it can be shown under reasonable assumptions that there cannot be a polynomial time algorithm that on input of Δ and the norm of a principal ideal in $\mathcal{O}_\Delta$ computes the standard representation of a generator of such an ideal because the length of this representation is too big.

It is therefore desirable to have a shorter representation for numbers in $\mathcal{O}_\Delta$ of small norm which can be used to perform the same operations that can be performed using the standard representation. In this paper we introduce and study such a representation. It is a generalization of the short representation for units that was introduced in [4]. Also, a similar representation for units is used in the computer algebra system PARI, see [2].

1.1 Definition *Let Δ be a quadratic discriminant and let $\alpha \in \mathcal{O}_\Delta$. A* compact representation *of α (with respect to Δ) is a representation*

$$\alpha = \gamma \prod_{j=1}^{k} \left(\frac{\alpha_j}{d_j}\right)^{2^{k-j}}$$

where

$$k \leq \log\log H(\alpha) + 2$$

and γ, $\alpha_j \in \mathcal{O}_\Delta$, $d_j \in \mathbb{Z}$, $1 \leq j \leq k$ with

$$H(\gamma) \leq |N(\alpha)|,$$

and

$$0 < d_j \leq |\Delta|^{1/2}, \quad H(\alpha_j) \leq |\Delta|^{5/2} \qquad \text{for} \quad 1 \leq j \leq k.$$

Also, for $1 \leq j \leq k$ the number $\gamma_j = \alpha_j \prod_{i=1}^{j-1}(\alpha_i/d_i)^{2^{j-i}}$ belongs to $\mathcal{O}_\Delta$ and its norm is d_j.

For $\Delta < 0$ the standard representation of $\alpha \in \mathcal{O}_\Delta$ is a compact representation of α. So we can restrict our attention to the case where $\Delta > 0$.

We estimate in section 3 of this paper the number of bits necessary to write down compact representations. We show in particular that writing down a compact representation of the fundamental unit of $\mathcal{O}$ only requires $O((\log\Delta)^2)$ bits. We also prove that for any principal ideal A of $\mathcal{O}_\Delta$ there exists a generator which when compactly represented is of binary length $O(\log|\mathrm{N}(\mathrm{A})| + (\log\Delta)^2)$ where $\mathrm{N}(\mathrm{A})$ is the norm of A. Assuming that $\mathcal{O} \subset \mathbb{R}$ we show in section 4 that for any $\alpha \in \mathcal{O}_\Delta$ a standard representation can be computed in polynomial time from the sign of α, the principal ideal $\alpha\mathcal{O}_\Delta$ and a sufficiently precise approximation to $\log\alpha$. In section 5 we show how to perform operations on numbers given in compact representation. We present polynomial time algorithms for computing the sign, the norm, the product, the quotient of numbers in compact representation. We show how to determine in polynomial time the principal ideal generated by those numbers and for a given modulus m the coefficients in the standard representation modulo m. We also describe polynomial time methods for comparing two numbers in compact representation. As an application, we show in section 6 that principal ideal testing belongs to the complexity class NP. In a different context that result can also be found in [1] and [5].

The main tool used in this paper is the infrastructure of the ideal classes of real quadratic orders that was first discovered by Shanks [10] and extensively studied by H.W. Lenstra in [6]. In section 2 we give a short self contained presentation of that theory.

In the remaining sections of this paper we assume that Δ is a quadratic discriminant, $\Delta > 0$. We let $\mathcal{O} = \mathcal{O}_\Delta$ and we let K be the field of fractions of $\mathcal{O}$. By $\mathrm{K} \to \mathbb{R}$, $\alpha \mapsto \alpha^{(i)}$, $i = 1, 2$, we denote the embeddings of K into the field $\mathbb{C}$ of complex numbers. We assume that $K \subset \mathbb{R}$ and that $\alpha = \alpha^{(1)}$ for every $\alpha \in \mathrm{K}$. We also write $\overline{\alpha} = \alpha^{(2)}$. By log we always mean the logarithm to base 2 and by ln we mean the natural logarithm.

2 Algorithmic ideal theory

In this section we review the results of algorithmic ideal theory in $\mathcal{O}$ that are used in this paper. To keep the paper self contained, we present most of the proofs. The presentation is inspired by [6] and [2] but we do not use the language of forms here. We also prove numerous results that are not contained in those descriptions. We start with an algebraic characterization of quadratic orders in K.

2.1 Proposition *A subset $\mathcal{O}'$ of K is a quadratic order, if and only if O' is an unitary subring of K which as a $\mathbb{Z}$-module is free of rank 2. Also, if Δ' is the discriminant of O' then $\mathcal{O}$ is contained in $\mathcal{O}'$ if and only if Δ'/Δ is a square in $\mathbb{Z}$.*

Proof: If $\mathcal{O}'$ is a quadratic order, then according to the definition given in the introduction, $\mathcal{O}'$ is of the form $\mathcal{O}' = \mathbb{Z} + \frac{\Delta'+\sqrt{\Delta'}}{2}\mathbb{Z}$. So $\mathcal{O}'$ is obviously a free $\mathbb{Z}$-module of rank 2 and it is easy to verify that $\mathcal{O}'$ is a unitary ring.

Conversely, assume that $\mathcal{O}'$ is a unitary subring of K which as a $\mathbb{Z}$-module is free of rank 2. Then $\mathcal{O}'$ has a $\mathbb{Z}$-basis $1, \omega = (u + v\sqrt{\Delta})/(2d)$ with $u, v, d \in \mathbb{Z}$, $vd > 0$. Since $\omega^2 \in \mathcal{O}'$ there must be $x, y \in \mathbb{Z}$ with $u^2 + v^2\Delta + 2uv\sqrt{\Delta} = 4d^2x + 2d^2yu + 2d^2yv\sqrt{\Delta}$. This implies that $d^2y = u$ and $v^2\Delta = 4d^2x + u^2$ which means that d^2 divides v^2D. Set $\Delta' = v^2\Delta/d^2$. Then $\Delta' = 4x + y^2$ and $(u + v\sqrt{\Delta})/(2d) = (y + \sqrt{\Delta'})/2$. The first of those equations shows that $y \equiv \Delta \bmod 2$. Therefore it follows from the second equation that $\mathcal{O}' = \mathbb{Z} + \frac{\Delta'+\sqrt{\Delta'}}{2}\mathbb{Z}$.

If $\mathcal{O} \subset \mathcal{O}'$ then $\Delta + \sqrt{\Delta} = 2x + y\Delta' + y\sqrt{D'}$. This means that $v/d = \sqrt{\Delta}/\sqrt{\Delta'} = y \in \mathbb{Z}$ as asserted. □

It is easy to deduce from this statement what the maximal order in K looks like.

2.2 Corollary *Let D be the largest square free divisor of Δ. If $D \equiv 1 \bmod 4$ set $\Delta' = D'$ and otherwise set $\Delta' = 4D'$. Then the quadratic order of discriminant Δ' is with respect to inclusion maximal among all the quadratic orders in K.*

Corollary 2.2 shows that being able to compute maximal orders means being able to determine the square free part of a rational integer. This is considered to be a very hard algorithmic problem. Although the maximal order in K has very nice algebraic properties, it is therefore in general impossible to find that order.

An *(integral) ideal* of $\mathcal{O}$ is an additive subgroup A of $\mathcal{O}$ with $\mathrm{A}\mathcal{O} \subset \mathrm{A}$. In this paper, ideals will always be assumed to be non zero. The *norm* of A is $\mathrm{N}(\mathrm{A}) = |\mathcal{O}/\mathrm{A}|$. A *fractional ideal* of $\mathcal{O}$ is a subset A of K such that $d\mathrm{A}$ is an ideal in $\mathcal{O}$ for some $d \in \mathbb{Z}_{>0}$. The *denominator* $d(\mathrm{A})$ of A is the minimal such d. Also put $\overline{\mathrm{A}} = \{\overline{\alpha} : \alpha \in \mathrm{A}\}$. Two fractional ideals A and B are called *equivalent* if there is a non zero $\alpha \in \mathrm{K}$ such that $\mathrm{A} = \alpha\mathrm{B}$. Equivalence of fractional ideals is an equivalence relation. The eqivalence classes are called *ideal classes* of $\mathcal{O}$. The norm of A is $\mathrm{N}(\mathrm{A}) = \mathrm{N}(d(\mathrm{A})\mathrm{A})/(d(\mathrm{A})^2))$. Unless we talk about compact representations, elements $\alpha \in \mathrm{A}$ will be given as $\alpha = (x + y\sqrt{\Delta})/(2d(\mathrm{A}))$ with $x, y \in \mathbb{Z}$. Let $\alpha \in \mathrm{K}$, $\alpha \neq 0$, the *denominator* $d(\alpha)$ with respect to Δ is the denominator of the *principal ideal* $\alpha\mathcal{O}$ of $\mathcal{O}$. The *height* of α is $\mathrm{H}(\alpha) = \mathrm{H}(d(\alpha)\alpha)/d(\alpha)$.

2.3 Lemma *For any fractional ideal A of $\mathcal{O}$ and any $\alpha \in A$ we have $|N(\alpha)| \geq N(A)$.*

Proof: It suffices to prove the assertion for integral ideals. But then the assertion follows from the fact that $\alpha\mathcal{O}$ is a subgroup of A. □

2.4 Lemma *For $\alpha \in \mathcal{O}$ we have $d(1/\alpha)|N(\alpha)$, $|N(d(1/\alpha)/\alpha)| \leq |d(1/\alpha)|$ and $H(d(\alpha)/\alpha) \leq H(\alpha)$.*

Proof: Clearly, $\mathrm{N}(\alpha)/\alpha = \alpha^{(2)} \in \mathcal{O}$. Therefore, $d(1/\alpha)|\mathrm{N}(\alpha)$. Thus $|\mathrm{N}(d(1/\alpha)/\alpha)| = d(1/\alpha)^2/|\mathrm{N}(\alpha)| \leq d(1/\alpha)$. $\mathrm{H}(d(1/\alpha)/\alpha) \leq \mathrm{H}(\mathrm{N}(\alpha)/\alpha) = \mathrm{H}(\alpha)$. □

For $a, b \in \mathbb{Z}, a \neq 0$, let $\tau(b, a)$ be the unique integer τ such that $\tau \equiv b \bmod 2a$, $-a < \tau \leq a$ if $a > \sqrt{\Delta}$, and $\sqrt{\Delta} - 2a < \tau < \sqrt{\Delta}$ if $a < \sqrt{\Delta}$.

2.5 Proposition *A subset A of K is an ideal of $\mathcal{O}$ if and only if A can be written as*

$$A = m\left(a\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2}\mathbb{Z}\right)$$

where $a, b, m \in \mathbb{Z}$, $a, m > 0$, $b = \tau(b, a)$ and $4a$ divides $\Delta - b^2$. This representation of ideals is unique.

Proof: Let A be an ideal of $\mathcal{O}$. The elements $1, \omega = \frac{\Delta+\sqrt{\Delta}}{2}$ form a $\mathbb{Z}$-basis of $\mathcal{O}$. Hence, there is a $\mathbb{Z}$-basis $u, v + w\omega$ of A with $u, v, w \in \mathbb{Z}$, $w > 0$. The numbers u, w are uniquely determined, and v is unique modulo u. Choose v such that $-u < 2v + w\Delta \leq u$. Since $u\omega$ belongs to A we must have $u\omega = xu + y(v + w\omega) = xu + yv + yw\omega$ with $x, y \in \mathbb{Z}$. This implies that $u = yw$ and $0 = xu + yv = xyw + yv$, thus $v = -xw$. Also, $-y < -2x + \Delta \leq y$. Now let $a = y$, $b' = -2x + \Delta$ and $m = w$. If $a > \sqrt{\Delta}$ or $b' \geq \sqrt{\Delta} - 2a$ then we set $b = b'$, otherwise we set $b = b' + 2a$. Then $m(a, (b + \sqrt{\Delta})/2)$ is a basis of A where $b = \tau(b', a)$. It remains to show that $4a$ divides $\Delta - b^2$. Without loss of generality we may assume that $m = 1$. Since $\omega(b + \sqrt{\Delta})/2 \in$ A we must have $(\Delta(b + 1) + (b + \Delta)\sqrt{\Delta})/4 = xa + y(b + \sqrt{\Delta})/2$ with $x, y \in \mathbb{Z}$. This implies that $2y = b + \Delta$ and $\Delta(b + 1) = 4xa + 2yb = 4xa + b^2 + b\Delta$. Thus we have $4xa = \Delta - b^2$.

Conversely, let A be a subset of K which is of the the form given in the lemma. Without loss of generality we may assume that $m = 1$. We must show that $\omega\alpha \in$ A for $\alpha \in \{a, (b + \sqrt{\Delta})/2\}$. So we must have $\omega a = a\Delta/2 + a\sqrt{\Delta}/2 = xa + y(b + \sqrt{\Delta})/2$ with $x, y \in \mathbb{Z}$. This implies that $y = a$ and $x = (\Delta - b)/2$. Since 4 divides $\Delta - b^2$, either Δ and b are both odd or both even. Therefore, x is an integer. We must also have $\omega(b + \sqrt{\Delta})/2 = (\Delta(b+1) + (b + \Delta)\sqrt{\Delta})/4 = xa + y(b + \sqrt{\Delta})/2$. As shown above this is true for $y = (b + \Delta)/2$ and $x = (\Delta - b^2)/(4a)$. By our assumption both x and y are integers. □

The representation of Proposition 2.5 will be called the *standard representation* of the ideal A. For a fractional ideal A of $\mathcal{O}$ the standard representation is (repfrac)

$$\mathrm{A} = \frac{m}{d(\mathrm{A})}\left(a\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2}\mathbb{Z}\right) \tag{2}$$

where a, b, m satisfy the conditions of Proposition 2.5. By determining a fractional ideal we will mean determining its standard representation.

2.6 Proposition *Let $\alpha, \beta \in K$ be linearly independent over $\mathbb{Z}$ and let $A = \alpha\mathbb{Z} + \beta\mathbb{Z}$. Then $\mathcal{O}_{\mathrm{A}} = \{\gamma \in K : \gamma A \subset A\}$ is an order of K and A is a fractional ideal of $\mathcal{O}_{\mathrm{A}}$.*

Proof: Obviously $\mathcal{O}_{\mathrm{A}}$ is a unitary subring of K. It is also easy to see that there is some $d \in \mathbb{Z}_{>0}$ with $d\mathcal{O} \subset \mathrm{A} \subset (1/d)\mathcal{O}$. This implies that $(1/d^2)\mathcal{O} \subset \mathcal{O}_{\mathrm{A}} \subset d^2\mathcal{O}$ which means that as a $\mathbb{Z}$-module $\mathcal{O}_{\mathrm{A}}$ is free of rank 2. □

The order of Proposition 2.6 is called the *ring of multipliers* of A. As the next statement shows, the ring of multipliers of an ideal of A can be easily computed. When dealing with an ideal A we may therefore assume that the order under consideration is the ring of multipliers of A.

2.7 Proposition *Let $A = a\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2}\mathbb{Z}$ be an ideal of $\mathcal{O}$ in standard representation, let $b^2 - \Delta = 4ac$ and let $s = \gcd(a, b, c)$. Then s^2 divides Δ and the ring of multipliers of A is of discriminant $\Delta_{\mathrm{A}} = \Delta/s^2$. Moreover, if $a' = a/s$ and $b' = b/s$ then $A = s(a'\mathbb{Z} + \frac{b'+\sqrt{\Delta_{\mathrm{A}}}}{2}\mathbb{Z})$ is the standard representation of A with respect to $\mathcal{O}_{\mathrm{A}}$.*

Proof: Clearly, s^2 divides Δ and $\mathrm{A} = s(a'\mathbb{Z} + \frac{b'+\sqrt{\Delta_{\mathrm{A}}}}{2}\mathbb{Z})$ is the standard representation of A with respect to the order $\mathcal{O}' = \mathcal{O}_{\Delta_{\mathrm{A}}}$. This shows that $\mathcal{O}' \subset \mathcal{O}_{\mathrm{A}}$. Conversely, let $\Delta' = \Delta/k^2$ be the discriminant of $\mathcal{O}'$. Then $\mathrm{A} = a\mathbb{Z} + \frac{b+k\sqrt{\Delta'}}{2}\mathbb{Z}$. Then it follows from Proposition 2.5 that k divides a and b and thus k divides c. Hence, it follows from Lemma 2.1 that $\mathcal{O}_{\mathrm{A}} \subset \mathcal{O}'$. $\square$

For two fractional ideals A and B of $\mathcal{O}$ we define $\mathrm{A}+\mathrm{B} = \{\alpha+\beta : (\alpha,\beta) \in \mathrm{A}\times\mathrm{B}\}$ and $\mathrm{AB} = \{\sum_{(a,b)\in S} ab : S \subset \mathrm{A}\times\mathrm{B} \text{ finite}\}$. The *sum* $\mathrm{A}+\mathrm{B}$ and the *product* AB are fractional ideals of $\mathcal{O}$. The set of fractional ideals of $\mathcal{O}$ with this multiplication is a semigroup. The fractional ideal A of $\mathcal{O}$ is called *invertible* if there is a fractional ideal B of $\mathcal{O}$ with $\mathrm{AB} = \mathcal{O}$. The set $\mathcal{I}$ of invertible ideals is an abelian group in which the set $\mathcal{P}$ of principal ideals is a subgroup. The *class group* of $\mathcal{O}$ is the factor group $\mathcal{I}/\mathcal{P}$.

2.8 Lemma *A fractional ideal A of $\mathcal{O}$ is invertible if and only if $\mathcal{O}$ is the ring of multipliers of A. Moreover, if $A = a\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2}\mathbb{Z}$ is invertible then the inverse is $\mathbb{Z} + \frac{-b+\sqrt{\Delta}}{2a}\mathbb{Z}$.*

Proof: Let $\mathcal{O}'$ be the ring of multipliers of A. Clearly $\mathcal{O} \subset \mathcal{O}'$.

If A is invertible then there is a fractional ideal B of $\mathcal{O}$ with $\mathrm{AB} = \mathcal{O}$. Hence, we have for every $\alpha \in \mathrm{K}$ with $\alpha\mathrm{A} \subset \mathrm{A}$ that $\alpha\mathrm{AB} \subset \mathrm{AB}$, i.e. $\alpha \in \mathrm{AB} = \mathcal{O}$. This proves that $\mathcal{O}' \subset \mathcal{O}$.

Conversely, assume that $\mathcal{O}$ is the ring of multipliers of A. Let $\mathrm{B} = \mathbb{Z} + \frac{-b+\sqrt{\Delta}}{2a}\mathbb{Z}$. Also, let $b^2 - \Delta = 4ac$. Then the ideal AB is generated by $a, c, (b+\sqrt{\Delta})/2, (b-\sqrt{\Delta})/2$. Therefore, $\mathrm{AB} \subset \mathcal{O}$ and since a, b, c are contained in AB and since by Proposition 2.7 those numbers are coprime, it follows that $\mathrm{AB} = \mathcal{O}$. $\square$

Now we present a few results concerning ideal arithmetic. By *polynomial time* we mean that the running time is bounded by a polynomial in $\log\Delta$ and the binary length of the input.

2.9 Proposition *For $\alpha \in \mathcal{O}$, $\alpha = \frac{x+y\sqrt{\Delta}}{2}$ where $x, y \in \mathbb{Z}$, the ideal $A = \alpha\mathcal{O}$ can be determined in polynomial time. More prescisely, if we set $m = \gcd(y, (x+y\Delta)/2)$ and choose $k, \ell \in \mathbb{Z}$ such that $ky + \ell(x+y\Delta)/2 = m$ then $A = m(a\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2}\mathbb{Z})$ is the standard representation of A where $a = |N(\alpha)|/m^2$ and $b = \tau((kx + \ell(x+y)\Delta/2)/m, a)$.*

Proof: As a $\mathbb{Z}$-module, A is generated by $(x+y\sqrt{\Delta})/2$ and $(x+y\sqrt{\Delta})(\Delta+\sqrt{\Delta})/4 = ((x+y)\Delta + (x+y\Delta)\sqrt{\Delta})/4$. Let $\mathrm{A} = m(a\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2}\mathbb{Z})$ be the standard representation of A. Since m is the smallest positive coefficient of $\sqrt{\Delta}/2$ in A, we get $m = \gcd(y, (x+y\Delta)/2)$. We also know that $\mathrm{N}(\mathrm{A}) = m^2 a = |\mathrm{N}(\alpha)|$, hence $a = |\mathrm{N}(\alpha)|/(m^2)$. Also, if $ky + \ell(x+y\Delta)/2 = m$ then $b = \tau(kx + \ell(x+y)\Delta/2)/m, a)$. $\square$

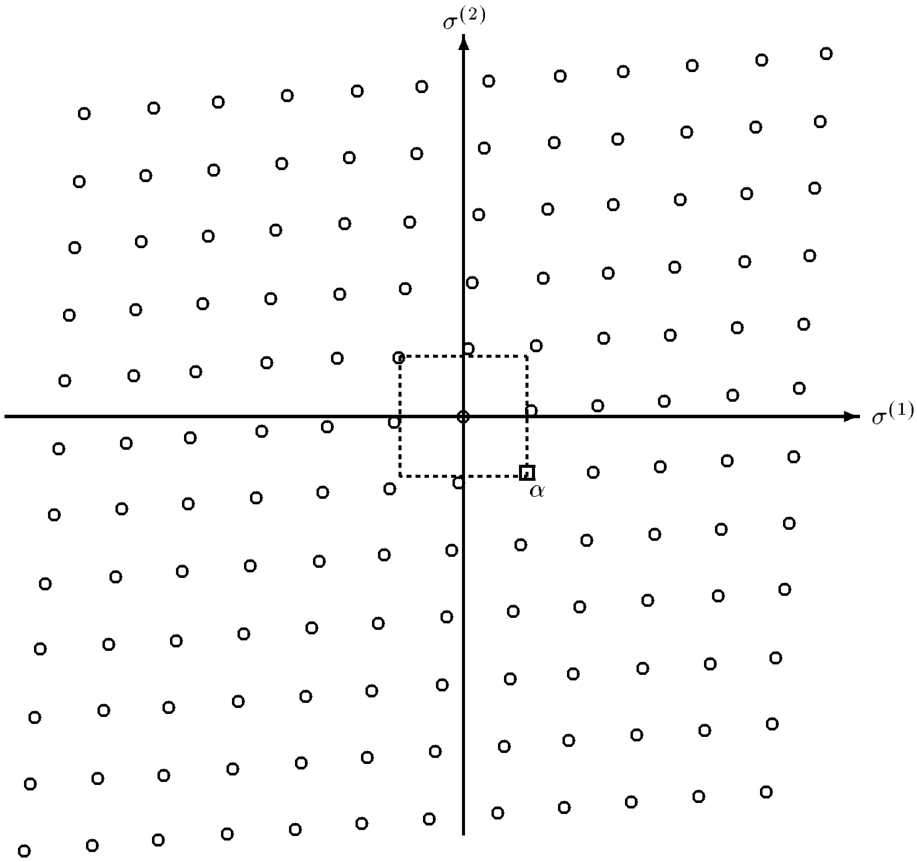
2.10 Proposition *Let A_1 and A_2 be ideals in $\mathcal{O}$ with the standard representations $A_1 = a_1\mathbb{Z} + \frac{b_1+\sqrt{\Delta}}{2}\mathbb{Z}$ and $A_2 = a_2\mathbb{Z} + \frac{b_2+\sqrt{\Delta}}{2}\mathbb{Z}$. Then A_1A_2 can be computed in polynomial time. More precisely, if $m = \gcd(a_1, a_2, (b_1+b_2)/2)$, if $j, k, \ell \in \mathbb{Z}$ are integers such that $ja_1 + ka_2 + \ell(b_1+b_2)/2 = m$ then $A_1A_2 = m(a_3\mathbb{Z} + \frac{b_3+\sqrt{\Delta}}{2}\mathbb{Z})$ is the standard representation of A_1A_2 where $a_3 = a_1a_2/(m^2)$ and $b_3 = \tau((ja_1b_2 + ka_2b_1 + \ell(b_1b_2+\Delta)/2)/m, a_3)$.*

Proof: The ideal $A_3 = \mathrm{A}_1\mathrm{A}_2$ is generated over $\mathbb{Z}$ by a_1a_2, $a_1(b_2+\sqrt{\Delta})/2$, $a_2(b_1+\sqrt{\Delta})/2$ and $(b_1b_2 + (b_1+b+2)\sqrt{\Delta} + \Delta)/4$. If $m(a_3\mathbb{Z} + \frac{b_3+\sqrt{\Delta}}{2}\mathbb{Z})$ is the standard representation of A_3 then we have $m = \gcd(a_1, a_2, (b_1+b_2)/2)$ and $a_3 = a_1a_2/m^2$. If $ja_1 + ka_2 + \ell(b_1+b_2)/2 = m$ then $b_3 = \tau((ja_1b_2 + ka_2b_1 + \ell(b_1b_2+\Delta)/2)/m, a_3)$. $\square$

Next we discuss minima and reduced ideals. We let A be an invertible ideal of $\mathcal{O}$. By Proposition 2.7 and Lemma 2.8 we can determine whether this is true and if it is not true we can easily modify $\mathcal{O}'$ such that it becomes true. A *minimum* of A is an element $\alpha \in A$ such that $\alpha^{(1)} > 0$ and there is no non zero $\beta \in A$ with $|\beta^{(i)}| < |\alpha^{(i)}|$ for $i = 1, 2$. The fractional ideal A is called *reduced* if 1 is a minimum in A. Those notions allow a geometric interpretation. Consider the map

$$\mathrm{K} \to \mathbb{R}^2,\ \alpha \mapsto \underline{\alpha} = (\alpha^{(1)}, \alpha^{(2)}). \tag{3}$$

Then the image $\underline{\mathrm{A}}$ of A under this map is a two dimensional lattice in $\mathbb{R}^2$ of determinant $\mathrm{N(A)}\sqrt{\Delta}$. For $\alpha \in A$ to be a minimum of A means that the open rectangle $\{(x,y) \in \mathbb{R}^2 : |x| < |\alpha^{(1)}|, |y| < |\alpha^{(2)}|$ is free of non zero lattice points.



2.11 Lemma *If A is reduced then its standard representation is of the form $A = \mathbb{Z} + \frac{b+\sqrt{\Delta}}{2a}\mathbb{Z}$, i.e. in (2) we have $m = 1$ and $a = d(A)$.*

Proof: Since 1 belongs to A we must have $1 = m(xa + yb + y\sqrt{\Delta})/d(\mathrm{A})$ with $x, y \in \mathbb{Z}$. This implies that $y = 0$ and $mxa/d(\mathrm{A}) = 1$. Since A is reduced there is no element $\alpha \in A$ with $\mathrm{H}(\alpha) < 1$. Therefore we must have $x = 1$ and $ma = d(\mathrm{A})$. But since m is a divisor of $d(\mathrm{A})$ it follows from the minimality of $d(\mathrm{A})$ that $m = 1$. $\square$

2.12 Corollary *If A is reduced then $N(A) = 1/d(A)$.*

2.13 Lemma *Let $c_i \in \mathbb{R}_{>0}$ with $c_1c_2 > N(A)\sqrt{\Delta}$. Then there exists $\alpha \in A$ with $|\alpha^{(i)}| < c_i$ for $i = 1, 2$.*

Proof: This is a special case of Minkowski's convex body theorem, see [8]. $\square$

2.14 Lemma *Let $A = \mathbb{Z} + \frac{b+\sqrt{\Delta}}{2}\mathbb{Z}$ be a reduced ideal in standard representation. Then $a, |b| < \sqrt{\Delta}$.*

Proof: Since 1 is a minimum in A it follows from Lemma 2.13 and Lemma 2.12 that $1 \le \mathrm{N}(\mathrm{A})\sqrt{\Delta} = \sqrt{\Delta}/d(\mathrm{A})$. □

2.15 Proposition *Let A be a fractional ideal of $\mathcal{O}$ and let $A = \mathbb{Z} + \frac{b+\sqrt{\Delta}}{2a}\mathbb{Z}$ be its standard representation. Then A is reduced if and only if $b \ge 0$ and $b + \sqrt{\Delta} > 2a$.*

Proof: Assume that A is reduced. If $a > \sqrt{\Delta}$ then $|(b+\sqrt{\Delta})/(2a)| < 1$ and $|(b-\sqrt{\Delta})/(2a)| < 1$ which means that A is not reduced. Consequently, we must have $a < \sqrt{\Delta}$. If $b < 0$ then $-2a + \sqrt{\Delta} < b < 0$ which implies that $|b| = -b < 2a - \sqrt{\Delta}$ or $|b| + \sqrt{\Delta} < 2a$ which also contradicts the fact that A is reduced. So $b \ge 0$ and $b + \sqrt{\Delta} > 2a$.

Conversely, assume that $b \ge 0$ and $b + \sqrt{\Delta} > 2a$. The fractional ideal A is reduced if and only if 1 is a minimum in A which, in turn, is true if and only if $\mathrm{H}(2xa + y(b + \sqrt{\Delta})) \ge 2a$ for all $x, y \in \mathbb{Z}$ with $(x, y) \ne (0, 0)$. Then $b + \sqrt{\Delta} > 2a$ implies that $a < \sqrt{\Delta}$. Hence $b - \sqrt{\Delta} < 0$ and $b + \sqrt{\Delta} > 0$ and thus $\mathrm{H}(2xa + y(b + \sqrt{\Delta})) \ge 2|x|a$. If $x \ne 0$ that height clearly exceeds $2a$. So let $x = 0$ and $y \ne 0$. Then the height takes its minimum value for $y = 1$ and for $y = 1$ the height exceeds 1. □

2.16 Corollary *Let A be a fractional ideal of $\mathcal{O}$ and let $A = \mathbb{Z} + \frac{b+\sqrt{\Delta}}{2a}\mathbb{Z}$ be its standard representation. Then A is reduced if $a \le \sqrt{\Delta}/2$.*

Proof: If $a \le \sqrt{\Delta}/2$ then we have $b > 0$ and $2a - b - \sqrt{\Delta} \le \sqrt{\Delta} - b - \sqrt{\Delta} \le 0$ which by Proposition 2.15 means that A is reduced. □

2.17 Lemma *If the extended Riemann hypothesis holds then there is a constant $\Delta_0 \in \mathbb{R}_{>0}$ such that for $\Delta > \Delta_0$ the number of reduced ideals is at least $\sqrt{\Delta}/(3 \ln \Delta)$.*

Proof: It follows from a theorem of Oesterlé [9] that there exists $\Delta_0 \in \mathbb{R}_{>0}$ such that for every $\Delta > \Delta_0$ the number of odd primes $p \le \sqrt{\Delta}/2$ such that Δ is a quadratic residue modulo p is at least $\sqrt{\Delta}/(3 \ln \Delta)$. We show that for any such p there is a reduced ideal of denominator p. Let p be such a prime number and let $b \in \mathbb{Z}$, $0 \le b < p$, with $b^2 \equiv \Delta \bmod p$. If $b - \Delta$ is even then we also have $b^2 \equiv \Delta \bmod 4p$. Otherwise we replace b by $b - p$ which then implies $b^2 \equiv \Delta \bmod 4p$. By Proposition 2.5 and Corollary 2.16 it follows that $\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2p}\mathbb{Z}$ is a reduced ideal of denominator p. □

Assume that $\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2a}\mathbb{Z}$ ist the standard representation of A. We define $\gamma(\mathrm{A}) = \frac{b+\sqrt{\Delta}}{2a}$ and $\rho(\mathrm{A}) = (1/\gamma(\mathrm{A}))\mathrm{A}$. Then the standard representation of $\rho(\mathrm{A})$ is $\mathbb{Z} + \frac{\tau(-b,c)+\sqrt{\Delta}}{2c}$ where $c = |\Delta - b^2|/(4a)$. We now prove that at most $\lceil \log a \rceil + 1$ applications of the *reduction operator* ρ yields a reduced ideal in the equivalence class of A.

2.18 Proposition *Let $A = \mathbb{Z} + \frac{b+\sqrt{\Delta}}{2a}\mathbb{Z}$ be the standard representation of A. Set $A_0 = A$ and for $i > 0$ set $A_i = (1/\gamma(A_{i-1})A_{i-1}$. If A_i is not reduced, then $d(A_i) < d(A_{i-1})/2$ and thus A_i is reduced for some $i \le \lceil \log(a/\sqrt{\Delta}) \rceil + 1$. Let k be the minimal such i. Then $\alpha = \prod_{j=1}^{k-1} \gamma(A_j)$ is a minimum in A, $A_k = (1/\alpha)A$ and $\mathcal{H}(\alpha) \le 1$.*

Proof: For $i \ge 0$ let $\mathbb{Z} + \frac{b_i+\sqrt{\Delta}}{2a_i}\mathbb{Z}$ be the standard representation of A_i. If $a_{i-1} > \sqrt{\Delta}$ we have $|b_{i-1}| < a_{i-1}$ which implies that $a_i = |(b_{i-1}^2 - \Delta)/(4a_{i-1})| < (a_{i-1}^2 + \Delta)/(4a_{i-1}) < a_{i-1}/2$. This means that $a_i < \sqrt{\Delta}$ for some $i \le \lceil \log(a/\sqrt{\Delta}) \rceil$. Assume that $a_i < \sqrt{\Delta}$. If $a_{i+1} \ge a_i$ it follows that $\Delta - b_i^2 \ge 4a_i^2$, hence $\sqrt{\Delta} + |b_i| > 2a_i$ and by Proposition 2.15 this implies that A_i is reduced. If $a_{i+1} < a_i$

then $a_{i+1}^2 < a_i a_{i+1} = a_i|(b_i^2 - \Delta)/(4a_i)| = (\Delta - b_i^2)/4$. Thus $a_{i+1} < \sqrt{(\Delta - b_i^2)}/2 < \sqrt{\Delta}/2$. But then Corollary 2.16 implies that A_{i+1} is reduced.

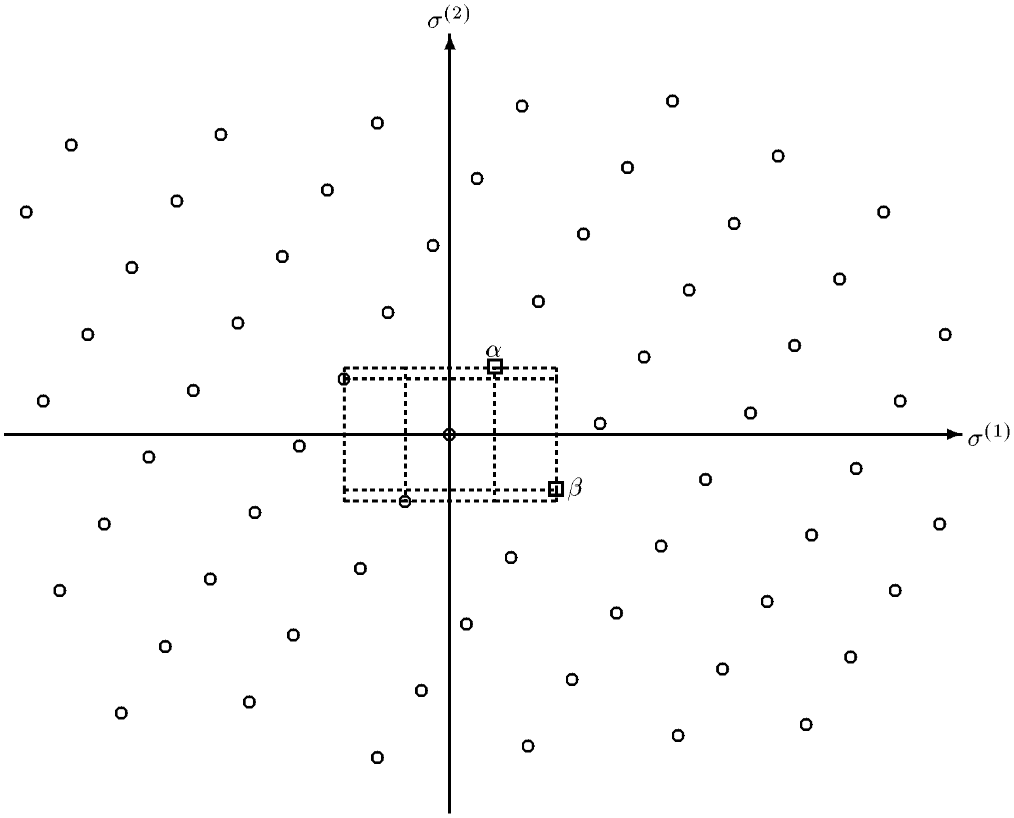
Now we prove the assertions concerning α. Clearly, $\mathrm{A}_k = (1/\alpha)\mathrm{A}$ and since A_k is reduced it follows that α is a minimum in A. As long as A_i is not reduced, we have $\mathrm{H}((b_i + \sqrt{\Delta})/(2a_i)) = (|b_i| + \sqrt{\Delta})/(2a_i) < 1$ which implies that $\mathrm{H}(\alpha) < 1$. □

2.19 Corollary *There is a polynomial time algorithm that on input of the fractional ideal A of $\mathcal{O}$ computes a reduced ideal B in the equivalence class of A and also a minimum α in A with $H(\alpha) \le N(A)$ and $B = (1/\alpha)A$.*

2.20 Corollary *The class group of $\mathcal{O}$ is finite.*

Proof: It follows from Corollary 2.19 that every ideal class of $\mathcal{O}$ contains a reduced ideal. By Proposition 2.15 and Lemma 2.14 the number of reduced ideals of $\mathcal{O}$ is finite. □

The *right neighbor* of a minimum α in A is is the uniquely determined minimum β of A with minimal $\beta^{(1)} > \alpha^{(1)}$. The *left neighbor* of a minimum α in A is the uniquely determined minimum β of A with minimal $|\beta^{(2)}| > |\alpha^{(2)}|$. Again those two notions have a geometric interpretation. The right neighbor β is characterized by the fact that β belongs to A, $\beta > \alpha$ and the open rectangle $\{(x, y) : |x| < |\alpha^{(2)}|, |y| < \beta^{(1)}\}$ is free of non zero points of the lattice $\underline{\mathrm{A}}$. The left neighbor β is characterized by the fact that β belongs to A, $\beta < \alpha$ and the open rectangle $\{(x, y) : |x| < |\beta^{(2)}|, |y| < \alpha^{(1)}\}$ is free of non zero points of the lattice $\underline{\mathrm{A}}$.



If A is reduced, then the *right neighbor* of A is the reduced ideal $(1/\alpha)\mathrm{A}$ where α is the right neighbor of 1 in A and the left neighbor of A is $(1/\beta)\mathrm{A}$ where β is the left neighbor of 1 in A.

The following statement can be easily verified:

2.21 Lemma *Let $\alpha \in K$, $\alpha > 0$. Then the map $A \to \alpha A$, $\beta \mapsto \beta\alpha$ is a bijection which maps minima to minima, right neighbors to right neighbors, and left neighbors to left neighbors.*

2.22 Corollary *The reduced ideals equivalent to A are exactly the ideals $(1/\alpha)A$ where α is a minimum in A.*

The following statement is immediate from the definition of $\gamma(\mathrm{A})$.

2.23 Lemma *If A is reduced then $\gamma(A) > 1$ and $-1 < \overline{\gamma(A)} < 0$.*

2.24 Proposition *Let $A = \mathbb{Z} + \gamma(A)\mathbb{Z}$ be a reduced ideal of $\mathcal{O}$. Then the right neighbor of 1 in A is $\gamma(A)$ and the right neighbor of A is $\rho(A)$.*

Proof: Let $\alpha_r = x + y\gamma(\mathrm{A})$ be the right neighbor of 1 in A. Then it follows from Lemma 2.23 that $y > 0$ and $x \geq 0$. Among all the candidates α_r is minimal for $x = 0$ and $y = 1$. □

Left neighbors can be determined using the following symmetry result:

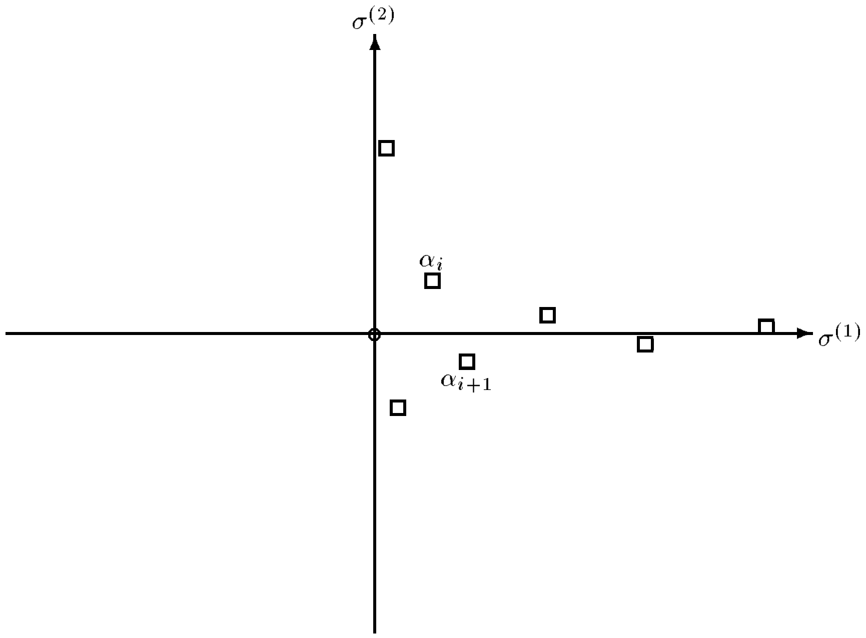
2.25 Proposition *Let $A = \mathbb{Z} + \frac{b+\sqrt{\Delta}}{2a}$ be a reduced ideal in standard representation. Then $\overline{A}$ is a reduced ideal. The standard representation of $\overline{A}$ is $\mathbb{Z} + \frac{\tau(-b,a)+\sqrt{\Delta}}{2a}\mathbb{Z}$. Moreover, let α be a minimum in A with left neighbor β. Then $|\overline{\alpha}|$ is a minimum in $\overline{A}$ with right neighbor $\overline{\beta}$.*

For the left neighbors we also introduce symbols. If A is reduced then we set $\delta(\mathrm{A}) = \frac{-\tau(-b,a)+\sqrt{\Delta}}{2a}$ and $\lambda(\mathrm{A}) = (1/\delta(\alpha))\mathrm{A}$. Then $\delta(\mathrm{A})$ is the left neighbor of 1 in A and $\lambda(\mathrm{A})$ is the left neighbor of A. We remark that when computing sequences of left neighbors of A it is practically useful do this via computing sequences of right neighbors of $\overline{\mathrm{A}}$.

2.26 Corollary *The right and left neighbor of a minimum of A can be computed in polynomial time.*

Proof: Let α be a minimum of A. We determine the reduced ideal $\mathrm{B} = (1/\alpha)\mathrm{A}$. Using Proposition 2.24 and Proposition 2.25 we find the right neighbor β_r and the left neighbor β_l of 1 in B. Then $\alpha\beta_l$ is the left neighbor of α and $\alpha\beta_r$ is the right neighbor of α. □

Let α_0 be a minimum of A and for $i \in \mathbb{Z}$ let α_{i-1} be the left neighbor and α_{i+1} the right neighbor of α_i. Also, let $\mathrm{A}_i = (1/\alpha_i)\mathrm{A}$. Note that by Proposition 2.24 we have $\alpha_{i+1} = \alpha_i\gamma(\mathrm{A}_i)$ and $\mathrm{A}_{i+1} = \rho(\mathrm{A}_i)$ for $i \in \mathbb{Z}$. The lattice points in the sequence $(\underline{\alpha_i})_{i\in\mathbb{Z}}$ lie on some sort of hyperbola as the next figure illustrates.



2.27 Lemma *We have* $0 < \log \alpha_i - \log \alpha_{i-1} \leq \log \sqrt{\Delta}$ *for* $i \in \mathbb{Z}$.

Proof: It follows from Lemma 2.13 that

$$\alpha_i/\alpha_{i-1} = |\alpha_i^{(1)}\alpha_{i-1}^{(2)}|/|\mathrm{N}(\alpha_{i-1})| \leq \mathrm{N}(\mathrm{A})\sqrt{\Delta}/|\mathrm{N}(\alpha_{i-1})| \leq \sqrt{\Delta}.$$

$\square$

2.28 Lemma *We have* $\log \alpha_{i+1} - \log \alpha_{i-1} \geq 1$ *for* $i \in \mathbb{Z}$.

Proof: By Proposition 2.23 we have $\mathrm{sign}(\alpha_i^{(2)}) = -\mathrm{sign}(\alpha_{i+1}^{(2)})$ for $i \in \mathbb{Z}$. This implies that $\mathrm{sign}(\alpha_{i-1}^{(2)}) = \mathrm{sign}(\alpha_{i+1}^{(2)})$. Therefore, we obtain $|\alpha_{i+1}^{(2)} - a_{i-1}^{(2)}| < |\alpha_{i-1}^{(2)}|$. If $\alpha_{i+1}^{(1)}/\alpha_{i-1}^{(1)} < 2$ then we have $\alpha_{i-1}^{(1)} < \alpha_{i+1}^{(1)} < 2\alpha_{i-1}^{(1)}$ which implies that $0 < \alpha_{i+1}^{(1)} - \alpha_{i-1}^{(1)} < \alpha_{i-1}^{(1)}$. This contradicts the minimality of α_{i-1}. $\square$

2.29 Lemma *The sequence* $(\alpha_i)_{i\in\mathbb{Z}}$ *contains all the minima of* A *and the elements of that sequence are pairwise distinct.*

Proof: The elements of $(\alpha_i)_{i\in\mathbb{Z}}$ must be pairwise distinct because the sequence $(\alpha_i)_{i\in\mathbb{Z}}$ is strictly increasing. More precisely, it follows from Lemma 2.28 that $\lim_{i\to\infty} \alpha_i = \infty$ and $\lim_{i\to-\infty} \alpha_i = -\infty$. Let α be any minimum of A. Let $i \in \mathbb{Z}$ with $\alpha_i \leq \alpha^{(1)} < \alpha_{i+1}$. We claim that $\alpha = \alpha_i$. Otherwise we must have $\alpha^{(1)} > \alpha_i^{(1)}$ and since α is a minimum $|\alpha^{(2)}| < |\alpha_i^{(2)}|$ which would contradict the minimality of $\alpha_{i+1}^{(1)}$. $\square$

2.30 Theorem 1. *The sequence* $(A_i)_{i\in\mathbb{Z}}$ *is periodic, i.e. there is* $k \in \mathbb{Z}_{>0}$ *such that* $A_i = A_j$, *if and only if* $i \equiv j \bmod k$ *for any* $i, j \in \mathbb{Z}$. *The number* k *is called the* period length *of the sequence of reduced ideals equivalent to* A, *we write* $k = k(A)$.

2. *The set of reduced ideals equivalent to* A *is* $\{A_i : 0 \leq i < k\}$.

3. *Let* $\epsilon = \alpha_k/\alpha_0$. *Then* ϵ *is a unit of* $\mathcal{O}$, *every unit of* $\mathcal{O}$ *is, up to sign change, a power of* ϵ *and for every* $i, l \in \mathbb{Z}$ *we have* $\alpha_{lk+i}/\alpha_i = \epsilon^l$.

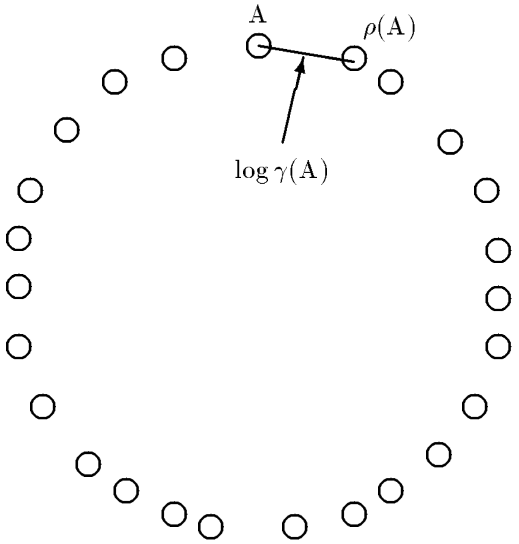
Proof: By Corollary 2.20 the number of reduced ideals in the equivalence class of A is finite. Hence there is $i, k \in \mathbb{Z}$ such that $A_i = A_{i+k}$. This implies that $\alpha_i A = \alpha_{i+k} A$, so $\epsilon = \alpha_{i+k}/\alpha_i$ both ϵ and $1/\epsilon$ belong to the ring of multipliers of A which by assumption is $\mathcal{O}$. Thus ϵ is a unit in $\mathcal{O}$. It follows from Lemma 2.21 that $\alpha_{s+lk} = \epsilon^l \alpha_s$ for every $s, l \in \mathbb{Z}$ and thus $A_s = A_t$ for every $s, t \in \mathbb{Z}$ with $s \equiv t \bmod k$. Choose k minimal with $A_0 = A_k$. Then the A_j, $0 \leq j < k$, are pairwise distinct and as a consequence of Corollary 2.22 and Lemma 2.29 any reduced ideal is equal to one of the A_j.

Let η be any unit in $\mathcal{O}$. We show that $\eta = s\epsilon^l$ with $s = \pm 1$ and $l \in \mathbb{Z}$. Without loss of generality we assume that $\eta^{(1)} > 0$. Then it follows from Lemma 2.29 that $\alpha = \eta\alpha_0 = \alpha_j$ with $j \in \mathbb{Z}$. Since $A_j = A_0$ we must have $j = lk$ with $l \in \mathbb{Z}_{>0}$ and therefore $\eta\alpha_0 = \alpha_{lk} = \epsilon^l \alpha_0$ which implies that $\eta = \epsilon^l$. □

2.31 Corollary *If $k(A) = 1$ then $\log \alpha_i - \log \alpha_{i-1} \geq 1/2$ for $i \in \mathbb{Z}$.*

Theorem 2.30 shows that the factor group $\mathcal{O}^* / < -1 >$ is an infinite cyclic group. The unit ϵ with $\epsilon > 1$ whose canonical image is a generator of that group is called the *fundamental unit* of $\mathcal{O}$. The *regulator* $R = |\ln \epsilon|$ is an invariant of $\mathcal{O}$.

Theorem 2.30 also shows that the finite sequence of reduced ideals can be viewed as lying on a circle with circumpherence R. Reduced ideals that are neighbors are also neighbors on the circle. The distance between some reduced ideal A and its right neighbor $\rho(A)$ is $\log \gamma(A)$.



2.32 Lemma *For $m \in \mathbb{Z}$, $n \in \mathbb{Z}_{>0}$ we have $\lfloor n/2 \rfloor \leq \log \alpha_{m+n} - \log \alpha_m \leq n \log \sqrt{\Delta}$.*

Proof: This statement is an immediate consequence of Lemma 2.28 and Lemma 2.27. □

2.33 Lemma *We have $2R/\ln \Delta \leq k(A) \leq 2R/\ln 2$.*

Proof: Let $k = k(A)$ We have $R = \ln \alpha_k - \ln \alpha_0$. Hence the first assertion follows immediately from Lemma 2.32. It also follows from that Lemma that for every $m \in \mathbb{Z}_{>0}$ we have $(\ln 2)(mk-1)/2 \leq \lfloor (\ln 2)mk/2 \rfloor \leq mR$. This implies the second assertion. □

2.34 Corollary *We have $R \geq \ln 2/2$.*

3 Sizes

We assume that integers are represented in binary. The *binary length* of a rational integer $z \neq 0$ is $\mathrm{size}(z) = \lfloor \log |z| \rfloor + 2$ where log denotes the logarithm to base 2. The extra bit encodes the sign of z. We also set $\mathrm{size}(0) = 2$. The binary length of the standard representation $\alpha = (x + y\sqrt{\Delta})/2$ of a number $\alpha \in \mathcal{O}$ is $\mathrm{size}_s(\alpha) = \mathrm{size}(x) + \mathrm{size}(y) + \mathrm{size}(\Delta)$. The binary length of a compact representation $\alpha = \gamma \prod_{i=1}^{k} (\alpha_i / d_i)^{2^{k-i}}$ is $\mathrm{size}_s(\gamma) + \sum_{i=1}^{k} (\mathrm{size}_s(\alpha_i) + \mathrm{size}(d_i)) + \mathrm{size}(\Delta)$. We define $\mathrm{size}_c(\alpha)$ to be the maximum of that quantity taken over all compact representations.

3.1 Lemma *For $\alpha \in \mathcal{O}$, $\alpha \neq 0$, we have* $\log H(\alpha) \leq \mathrm{size}_s(\alpha) \leq 2\log H(\alpha) + \log \Delta + 8$.

Proof: Let $\alpha = (x + y\sqrt{\Delta})/2$ be the standard representation of α. Since $\mathrm{H}(\alpha) = (|x| + |y|\sqrt{\Delta})/2$, it follows that $|x|, |y|\sqrt{\Delta} \leq 2\mathrm{H}(\alpha)$ which implies that $\mathrm{size}(x) + \mathrm{size}(y) + \mathrm{size}(\Delta) \leq 2\log \mathrm{H}(\alpha) + \log \Delta + 8$. It also follows that $|x| \geq \mathrm{H}(\alpha)$ or $|y|\sqrt{\Delta} \geq \mathrm{H}(\alpha)$ which implies that $\mathrm{size}(x) + \mathrm{size}(y) + \mathrm{size}(\Delta) \geq \log \mathrm{H}(\alpha)$. $\square$

3.2 Corollary *For $\alpha \in \mathcal{O}$ we have* $\mathrm{size}_c(\alpha) \leq 2\log |N(\alpha)| + 2\log \Delta + 10 + (\log\log H(\alpha) + 2)((13 \log \Delta)/2 + 10)$.

3.3 Lemma *We have $hR \leq \sqrt{\Delta} \ln \Delta$.*

Proof: For the proof see [7]. $\square$

3.4 Corollary *For the fundamental unit ϵ of $\mathcal{O}$ we have* $\mathrm{size}_c(\epsilon) = O((\log \Delta)^2)$.

3.5 Lemma *Assume that the extended Riemann hypothesis holds. Then there is $\Delta_0 \in \mathbb{R}_{>0}$ such that for $\Delta > \Delta_0$ we have $hR \geq \sqrt{\Delta}/(6 \log \Delta)$ where R is the regulator and h is the class number of $\mathcal{O}$.*

Proof: For $1 \leq j \leq h$ let k_j be the period length of the jth ideal class. Then it follows from Lemma 2.17 that $\sum_{j=1}^{h} k_j \geq \sqrt{\Delta}/(3 \ln \Delta)$ for $\Delta > \Delta_0$. On the other hand we have by Lemma 2.33 that $k_j \leq R/\ln 2$ for $1 \leq j \leq h$. Hence we have $hR \geq \sqrt{\Delta}/(6 \log \Delta)$ which implies the assertion. $\square$

3.6 Corollary *Assume that the extended Riemann hypothesis holds. Then there is $\Delta_0 \in \mathbb{R}_{>0}$ such that for every $\Delta > \Delta_0$ we have $\mathrm{size}_s(\epsilon) > \sqrt{\Delta}/(9h \log \Delta)$ where ϵ is the fundamental unit and h is the class number of $\mathcal{O}$.*

3.7 Lemma *For any principal ideal A in $\mathcal{O}$ there is a generator α of A with* $\log H(\alpha) \leq \max\{\sqrt{\Delta} \log \Delta, \log N(A)\}$.

Proof: Let β be a generator of A with $\beta^{(1)} \geq 1$ and let ϵ be a fundamental unit of $\mathcal{O}$ with $\log \epsilon^{(1)} = R$. Let $k \in \mathbb{Z}$ such that $0 \leq \log \beta^{(1)} + k \log \epsilon^{(1)} < R$. Then $\alpha = \beta\epsilon^k$ is a generator of A and we have by Lemma 3.3 $0 \leq \log \alpha^{(1)} < R \leq \sqrt{\Delta} \log \Delta$. This implies that $\log |\alpha^{(2)}| \leq \log \mathrm{N}(\mathrm{A})$. $\square$

3.8 Corollary *For any principal ideal A in $\mathcal{O}$ there is a generator α of A with* $\mathrm{size}_c(\alpha) = O(\log |N(\alpha)|) + (\log \Delta)^2)$.

4 Determining compact representations

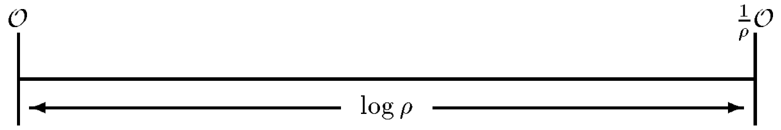
Let c be a complex number and let $q \in \mathbb{Z}_{>0}$. An *approximation of precision* q to c is a number $\hat{c} \in 2^{-q+1}\mathbb{Z}$ such that $|c - \hat{c}| < 2^{-q}$. In this section we prove the following theorem:

4.1 Theorem *There is a polynomial time algorithm that for any $\alpha \in \mathcal{O}$, $\alpha \neq 0$, on input of* $\operatorname{sign}(\alpha)$*, an approximation a of precision* 4 *to* $\log|\alpha|$ *and of the ideal $\alpha\mathcal{O}$ computes a compact representation of α.*

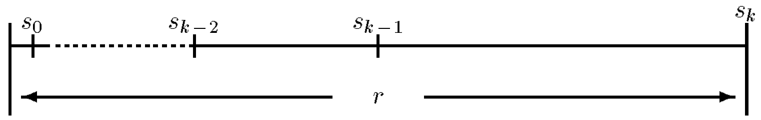
Let $\alpha \in \mathcal{O}$, $\alpha > 0$ and assume that a is an approximation of precision 4 to $\log\alpha$. Compute a minimum $\gamma \in \alpha\mathcal{O}$ with $\mathrm{H}(\gamma) \leq |\mathrm{N}(\alpha)|$. Set $\rho = \gamma/\alpha$. Then ρ is a minimum of $\mathcal{O}$ and $\rho^{(1)} \geq 1$ or $\rho^{(2)} \geq 1$. We assume that $\rho^{(1)} \geq 1$. If $\rho^{(1)} < 1$ then one can use the procedure described below to find a compact representation for $\alpha^{(2)}$ from which we immediately obtain a compact representation for α. We also compute an approximation c of precision 4 to $\log\gamma$ and set $r = c - a$, $\mathrm{A} = (\alpha/\gamma)\mathcal{O}$. Then r is an approximation of precision 3 to $\log\rho$.

Since $1/\rho$ generates the reduced ideal A and since γ satisfies the conditions of Definition 1.1 we have reduced the problem of finding a compact representation for α to finding a compact representation for $1/\rho$.

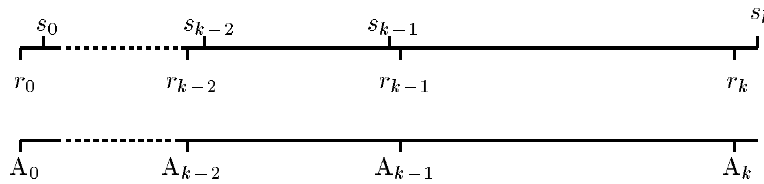
The quantity $r = \log\rho$ can be viewed as the *distance* between those reduced ideals. That distance is uniquely determined up to integer multiples of the regulator R.



We let $k := \min\{j \in \mathbb{Z}_{>0} : r/2^j \leq (\log\Delta)/4 + 1/4\}$ and $s_j := r/2^{k-j}$, $0 \leq j \leq k$.

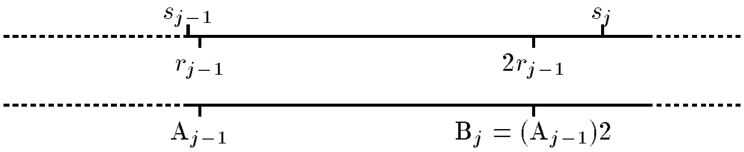


For $0 \leq j \leq k$ we compute a pair (A_j, r_j) where $A_j = (1/\rho_j)\mathrm{A}$ is a reduced principal ideal of $\mathcal{O}$, r_j is an approximation to $\log\rho_j$ and r_j is close to s_j, i.e. $|r_j - s_j| < (\log\Delta + 1)/4$ for $0 \leq j \leq k-1$ and $|r_k - r| < 1/4$. We choose $\mathrm{A}_0 = \mathcal{O}$ and $r_0 = 0$ and we will have $\mathrm{A}_k = \mathrm{A}$.

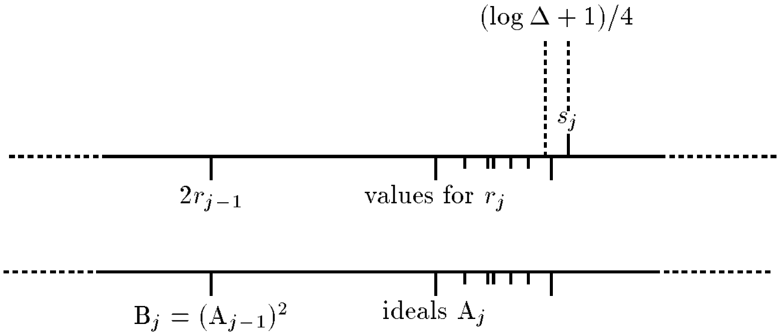


For $1 \leq j \leq k$ we will also have $\mathrm{A}_j = (\alpha_j/d_j)\mathrm{A}_{j-1}^2$ with $\alpha_j \in \mathcal{O}$ and $d_j \in \mathbb{Z}_{>0}$ as specified in Definition 1.1. Moreover, if $\rho_j = \prod_{i=1}^{j}(d_i/\alpha_i)$ then it is easy to verify that $\mathrm{A}_j = (1/\rho_j)\mathcal{O}$ and we will have $|r_j - \log\rho_j| < 1/4$. This implies that $|\log\rho - \log\rho_k| < 1/2$ and we will deduce that this means that $1/\rho = 1/\rho_k = \prod_{j=1}^{k}(\alpha_j/d_j)$ as desired.

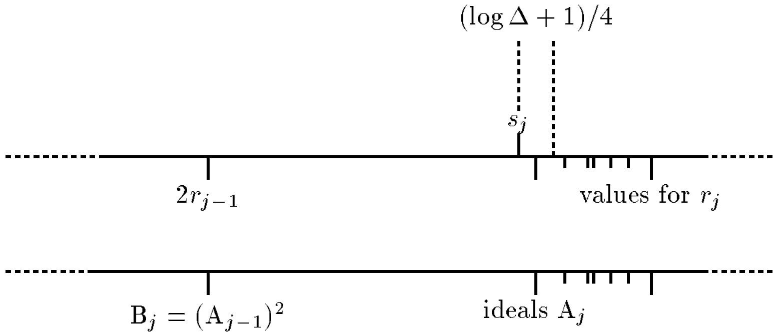
Clearly, $(\mathrm{A}_0 = \mathcal{O}, r_0 = 0)$ is a legal choice for the first pair. Now suppose that we have found the pair $(\mathrm{A}_{j-1}, r_{j-1})$. Then we set $\mathrm{B}_j = \mathrm{A}_{j-1}^2$. Then $\mathrm{B}_j = (1/\rho_{j-1}^2)\mathrm{A}$ is a principal ideal of $\mathcal{O}$ and the approximation $2r_{j-1}$ to the distance $\log\rho_{j-1}^2$ is close to $s_j = 2s_{j-1}$.



There are two reasons for not choosing $A_j = B_j$. The quantity $2r_{j-1}$ might not be close enough to s_j and, more importantly, in general, the ideal B_j is not reduced. So we apply the reduction algorithm from Proposition 2.18 to find β_j such that $(1/\beta_j)B_j$ is reduced. The important point is that $\log \beta_j$ is really small, i.e. of order of magnitude $\log \Delta$. Now we must set $r_j = 2r_{j-1} + b_j$ where b_j is an approximation to $\log \beta_j$. Even though $\log \beta_j$ is very small, r_j might still not be close enough to s_j. But this can be easily repaired by computing neighbors. If r_j is too far on the left, then we replace the reduced ideal $\mathrm{A}_j = (1/\beta_j)B_j$ and the minimum β_j of B_j iteratively by their right neighbors until r_j and s_j are close enough.



If r_j is too far on the right, then we replace the reduced ideal $\mathrm{A}_j = (1/\beta_j)B_j$ and the minimum β_j of B_j iteratively by left right neighbors until r_j and s_j are close enough.



Lemma 2.27 guarantees the success of this procedure. Since $1 \in \mathrm{A}_j$ it follows that $1 \in \mathrm{B}_j$ which implies that $1/\beta_j \in \mathrm{A}_j$. Thus we can write $1/\beta_j = \alpha_j/d_j$ with $d_j = d(\mathrm{A}_j)$ and $\alpha_j \in \mathcal{O}$. The estimate for $\mathrm{H}(\alpha_j)$ will follow from the fact that $\log \beta_j$ was small for the first β_j which we have computed.

We prove that Algorithm 4.2 yields in polynomial time a compact representation for α. In the proof we use the notations introduced in Algorithm 4.2.

4.3 Lemma *We have* $k \leq \log \log H(\alpha) + 2$.

Proof: We first note that $\kappa = (\log \Delta + 1)/4 > 0.8$. Since $k = \max\{0, \lceil \log(r/\kappa) \rceil\}$ we have $k = 0$ for $r \leq 0.8$ So assume that $r > 0.8$. Then $\log \rho > 0.6$ and $(\log \rho + 1/16)/0.8 < 1.5 \log \rho$. We also have

4.2 Algorithm

$k := \min\{j \in \mathbb{Z}_{>0} : r/2^j \leq (\log\Delta)/4 + 1/4\}$;	(1)
FOR $0 \leq j \leq k$	(2)
$s_j := r/2^{k-j}$	(3)
$\alpha_0 := 1$; $r_0 := 0$; $d_0 := 1$; $A_0 := \mathcal{O}$	(4)
FOR $1 \leq j \leq k-1$	(5)

$B_j = (A_{j-1})^2$;
    Compute minimum β_j *in* B_j *with* $H(\beta_j) \leq N(B_j)$.
    Compute approximation b_j *to* $\log\beta_j$ *of precision* $2(k-j)+4$.
    $r_j := 2r_{j-1} + b_j$
	(6)

WHILE $r_j - s_j \leq -(\log\Delta + 1)/4$	(7)
replace β_j *by its right neighbor and* b_j *by an approximation of precision* $2(k-j)+4$ *to* $\log\beta_j$; $r_j := 2r_{j-1} + b_j$	(8)
WHILE $r_j - s_j \geq (\log\Delta + 1)/4$	(9)
replace β_j *by its left neighbor and* b_j *by an approximation of precision* $2(k-j)+4$ *to* $\log\beta_j$; $r_j := 2r_{j-1} + b_j$	(10)
$A_j := (1/\beta_j)B_j$; $d_j := d(A_j)$; $\alpha_j := d_j/\beta_j$	(11)
$B_k := (A_{k-1})^2$ *Compute minimum* β_k *in* B_k *with* $H(\beta_k) \leq N(B_k)$. *Compute approximation* b_k *to* $\log\beta_k$ *of precision* 4; $r_k := 2r_{k-1} + b_k$; $A_k := (1/\beta_k)B_k$;	(12)
WHILE $r_k - r \leq -1/4$ *or* $A_k \neq A$	(13)
replace β_k *by its right neighbor and* b_k *by an approximation of precision* 4 *to* $\log\beta_k$; $r_j := 2r_{j-1} + b_j$; $A_k := (1/\beta_k)B_k$	(14)
WHILE $r_k - r \geq 1/4$ *or* $A_k \neq A$	(15)
replace β_k *by its left neighbor and* b_k *by an approximation of precision* 4 *to* $\log\beta_k$; $r_k := 2r_{k-1} + b_k$; $A_k := (1/\beta_k)B_k$	(16)
$d_k := d(A_k)$; $\alpha_k := d_k/\beta_k$	(17)

$\mathrm{H}(\rho) \leq \mathrm{H}(\gamma)\mathrm{H}(\alpha)/|\mathrm{N}(\alpha)| \leq \mathrm{H}(\alpha)$. This implies

$$\begin{aligned} k &\leq \log(r/\kappa) + 1 \\ &\leq \log((\log\rho + 1/16)/0.8) + 1 \\ &\leq \log(1.5\log\rho) + 1 \\ &\leq \log\log \mathrm{H}(\alpha) + 2. \end{aligned}$$

□

Let $\rho_0 = 1$ and for $1 \leq j \leq k$ define $\rho_j = (\rho_{j-1})^2\beta_j$. Then we have for $0 \leq j \leq k$ (ac)

$$\rho_j = \prod_{i=0}^{j}(d_j/\alpha_j)^{2^{j-i}}, \tag{4}$$

ρ_j is a minimum of O and $\mathrm{A}_j = (1/\rho_j)\mathcal{O}$.

4.4 Lemma *For $0 \leq j \leq k$ we have $|r_j - \log\rho_j| < 2^{-(2(k-j)+3)}$.*

Proof: By definition we have $r_0 = \log\rho_0$. Now suppose that the assertion is true for $j-1$. Then

$$\begin{aligned} |r_j - \log\rho_j| &= |2r_{j-1} + b_j - 2\log\rho_{j-1} - \log\beta_j| \\ &\leq 2\cdot 2^{-(2(k-j+1)+3)} + 2^{-(2(k-j)+4)} \\ &= 2^{-(2(k-j)+3)}. \end{aligned}$$

□

4.5 Lemma *For $1 \leq j \leq k$ Algorithm 4.2 enters at most one of the while loops and terminates after finitely many steps. At the end we have $\rho_k = \rho$.*

Proof: Let $j \leq k-1$. It follows from Lemma 2.27 that there exists a minimum μ with $|s_j - \log\mu| \leq (\log\Delta)/4$. If $r_j - s_j < -(\log\Delta)/4 - 1/4$ then by Lemma 4.4 we have $\log\rho_j - s_j < (\log\Delta)/4$. Hence, μ belongs to the sequence of right neighbors of ρ_j. This implies that in the first while loop we will find a value of r_j such that the conditions of both while loops are violated. If $r_j - s_j > (\log\Delta)/4 + 1/4$ then the existence of μ guarantees that in the second while loop we will find a value of r_j such that the conditions of the first two while loops are violated.

To prove the assertion for $j = k$ we note that $|\log\rho - r| < 1/8$ which implies that either in the third or in the fourth while loop we will find a value of r_k and A_k such that both conditions of the third and the fourth while loop are violated. By Lemma 2.28 this can only happen if $\rho_k = \rho$ or if ρ_k is a neighbor of ρ. If ρ and ρ_k are neighbors then it follows from Theorem 2.30 and from the fact that the second condition in the while loops is violated that there is exactly one reduced ideal in the equivalence class of A. Hence, by Lemma 2.31 we have $|\log\rho - \log\rho_k| \geq 1/2$. But this contradicts the fact that the first condition in both while loops is violated. This means that $\rho_k = \rho$. □

4.6 Lemma *For $1 \leq j \leq k$ we always have $d(B_j) \leq \Delta$, $|\log\beta_j| \leq 3\log\Delta/2$, $H(\beta_j) \leq \Delta^2$, and $H(1/\beta_j) \leq \Delta^2$.*

Proof: Since $d(\mathrm{B}_j)$ divides $d(\mathrm{A}_{j-1})^2$ for $1 \leq j \leq k$, the first assertion holds.

Suppose that we are in step j of the loop. Upon entering the while loop we have $|\mathrm{N}(\beta_j)| \geq \mathrm{N}(\mathrm{B}_j) \geq 1/\Delta$ and $\mathrm{H}(\beta_j) \leq \Delta$ which implies that $-\log\Delta \leq \log b_j \leq 0$. If the algorithm enters the first or the third while loop then $\log\beta_j$ is increased and since $2s_{j-1} = s_j$ we have $\log\beta_j \leq b_j + 1/4 = r_j - 2r_{j-1} + 1/4 =$

$(r_j - s_j) - 2(r_{j-1} - s_{j-1}) + 1/4$. We also have $|r_j - s_j| < (\log\Delta + 1)/4$ and $|r_{j-1} - s_{j-1}| < (\log\Delta + 1)/4$. This implies that $\log\beta_j < 3\log\Delta/4 + 1 < 3\log\Delta/2$. Analogously, one can show that we always have $\log\beta_j \geq -3\log\Delta/2$.

It follows from the second assertion that $1/\Delta \leq |\beta_j^{(1)}| \leq \Delta$. The last two assertions follow from the fact that $\mathrm{N}(\beta_j) \leq \mathrm{N}(\mathrm{B}_j)\sqrt{\Delta} \leq \sqrt{\Delta}$ and $|\mathrm{N}(1/\beta_j)| \geq \mathrm{N}(\mathrm{A}_j) \geq 1/\sqrt{\Delta}$. □

4.7 Lemma *The running time of Algorithm 4.2 is polynomially bounded in* $\log\log H(\alpha)$ *and* $\log\Delta$.

Proof: By Lemma 4.3 the number of iterations of the for loop is bounded by $\log\log \mathrm{H}(\alpha) + 2$.

As shown in the proof of Lemma 4.6 we have upon entering the while loops $|r_j - s_j| = |2(r_{j-1} - s_{j-1}) + b_j| \leq (3\log\Delta)/2 + 3/4$. Since by Lemma 2.28 after any two iterations of the while loop r_j is increased (or decreased) by at least $1 - 1/4$, the number of iterations in the while loops is $O(\log\Delta)$. By Lemma 2.18 the time for determining the first β_j is polynomially bounded in $\log\Delta$. Since by Lemma 4.6 $d(\mathrm{B}_j) \leq \Delta$ and $\mathrm{H}(\beta_j) \leq \Delta^{3/2}$ it follows that the binary length of the standard representation of all the β_j is polynomially bounded in $\log\Delta$ and thus the neighbors and the approximations can be computed in time polynomial in $\log\Delta$. □

4.8 Lemma *For* $0 \leq j \leq k$ *we have* $d_j \leq |\Delta|^{1/2}$ *and* $H(\alpha_j) \leq \Delta^{5/2}$.

Proof: The first inequality follows from Lemma 2.14 the second one from Lemma 4.6. □

4.9 Lemma *For* $0 \leq j \leq k$ *the number* $\gamma_j = \alpha_j \prod_{i=0}^{j-1}(\alpha_i/d_i)^{2^{j-i}}$ *belongs to* $\mathcal{O}_\Delta$ *and its norm is* d_j.

Proof: For $0 \leq j \leq k$ we have $\gamma_j = \alpha_j/\rho_{j-1} = d_j/\rho_j$. Since d_j is the denominator of the reduced ideal $(1/\rho_j)\mathcal{O}$ the assertion follows from Lemma 2.11. □

5 Computing with compact representations

The following theorems deal with the complexity of computations with numbers in $\mathcal{O}$ given in compact representation. By polynomial time we mean that the algorithm is polynomial in $\log\Delta$ and in the binary length of the compact representations and the remaining input.

5.1 Theorem *There is a polynomial time algorithm that given* $\alpha \in \mathcal{O}_\Delta$, $\alpha \neq 0$, *in compact representation and* $q \in \mathbb{Z}_{>0}$ *in unary representation computes an approximation of precision* q *to* $\log|\alpha|$.

Proof: Let $\alpha = \gamma \prod_{j=1}^{k}(\alpha_j/d_j)^{2^{k-j}}$ be a compact representation of α. Set $\beta_0 = \alpha_0/d_0$ and for $1 \leq j \leq k$ define $\beta_j = \beta_{j-1}^2\alpha_j/d_j$. Then $\alpha = \gamma\beta_k$. Determine an approximation b_0 of precision $3k + q + 1$ to β_0 and for $1 \leq j \leq k$ determine an approximation a_j of precision $3(k-j) - 2 + q + 1$ to $\log\alpha_j$ and an approximation l_j of precision $3(k-j) - 1$ to $\log d_j$. Set compute $b_j = 2b_{j-1} + a_j - l_j$. Then b_j is an approximation of precision $3(k-j) + q + 1$ to $\log\beta_j$ for $1 \leq j \leq k$. Finally determine an approximation c of precision $q + 1$ to $\log|\gamma|$ and set $a = b_k + c$. Then a is the approximation we were looking for. This process clearly takes polynomial time. □

5.2 Corollary *Given* $\alpha \in \mathcal{O}$ *in standard representation, one can determine a compact representation of* α *in polynomial time.*

5.3 Theorem *Given* $\alpha \in \mathcal{O}$, $\alpha \neq 0$, *in compact representation, the ideals* $\alpha\mathcal{O}$ *and* $(1/\alpha)\mathcal{O}$ *can be determined in polynomial time.*

Proof: We use the notations of Definition 1.1. We start by computing $\mathrm{A}_0 = (\alpha_0/d_0)\mathcal{O}$. Then we determine recursively $\mathrm{A}_j = (\alpha_j/d_j)(\mathrm{A}_{j-1})^2$ for $1 \leq j \leq k$. Since $\alpha_j(\mathrm{A}_{j-1})^2 = \gamma_j\mathcal{O}$, those ideals can be computed in polynomial time. Finally we calculate $\alpha\mathcal{O} = \gamma\mathrm{A}_k$. The ideal $(1/\alpha)\mathcal{O}$ can be determined similarly. □

5.4 Theorem *Given $\alpha \in \mathcal{O}$ in compact representation* $\mathrm{sign}(\alpha)$ *can be computed in polynomial time.*

Proof: Using the notations of Definition 1.1 we see that $\mathrm{sign}(\alpha) = \mathrm{sign}(\gamma)\,\mathrm{sign}(\alpha_0)$ which clearly can be computed in polnomial time. □

5.5 Theorem *Given $\alpha \in \mathcal{O}$ in compact representation the norm of α can be determined in polynomial time.*

Proof: Using the notations of Definition 1.1 we see that $\mathrm{N}(\alpha) = \mathrm{N}(\gamma)/d_k$. □

5.6 Theorem *Given $\alpha, \beta \in \mathcal{O}$ in compact representation. Then a compact representation of the product $\alpha\beta$ can be computed in polynomial time.*

Proof: From an approximation a to $\log|\alpha|$ and b to $\log|\beta|$ of precision 5 which by Theorem 5.1 can be computed in polynomial time we can determine the approximation $a + b$ of precision 4 to $\log|\alpha\beta|$. By Theorem 5.4 we can also find $\mathrm{sign}(\alpha\beta)$ in polynomial time. So by Theorem 4.1 we can find a compact representation for $\alpha\beta$ in polynomial time. □

5.7 Theorem *Let $\alpha \in \mathcal{O}$ and let $\alpha = (x + y\sqrt{\Delta})/2$ be the standard representation of α. Then given a compact representation of α and $n \in \mathbb{Z}_{>0}$ the values $x \bmod n$ and $y \bmod n$ can be determined in polynomial time.*

Proof: We use the notations of Definition 1.1. For $1 \leq j \leq k$ let $D_j = 2^{2(k-j)+1}\prod_{i=j}^{k} d_j^2$ and let $\gamma_j = (x_j + y_j\sqrt{\Delta})/2$ and $\gamma = (u + v\sqrt{\Delta})/2$ be the standard representations. We start by determining $x_0 \bmod D_0 n$ and $y_0 \bmod D_0 n$. Now suppose that $i \geq 1$ and we know $x_{i-1} \bmod D_{i-1}n$ and $y_{i-1} \bmod D_{i-1}n$. Since $4d_{i-1}^2\gamma_i = (x_{i-1} + y_{i-1}\sqrt{\Delta})^2\alpha_i$ we can determine $4d_{i-1}^2 x_i \bmod D_{i-1}n$ and $4d_{i-1}^2 y_i \bmod D_{i-1}n$ and thus we can find $x_i \bmod D_i n$ and $y_i \bmod D_i n$. So we have finally $x_k \bmod 2d_k^2 n$ and $y_k \bmod 2d_k^2 n$. Since $\alpha = \gamma(x_k + y_k\sqrt{\Delta})/2d_k$ this implies that we can determine $x \bmod n$ and $y \bmod n$. The numbers involved never exceed $\max\{\mathrm{C}(\alpha_j) : 0 \leq j \leq k\} \cup \{\mathrm{C}(\gamma)\} \cup \{2^{2k+1}D_0 n\}$. Their binary length is polynomially bounded in the length of the input. Since we only perform elementary operations with rational integers, the algorithm takes polynomial time. □

5.8 Theorem *Given $\alpha \in \mathcal{O}$, $\alpha \neq 0$, in compact representation we can compute the denominator $d(1/\alpha)$ and a compact representation of $d(1/\alpha)/\alpha$ in polynomial time.*

Proof: The denominator d of $1/\alpha$ is the denominator of $(1/\alpha)\mathcal{O}$ which by Theorem 5.3 can be determined in polynomial time. Since $\log|(d/\alpha)| = \log d - \log|\alpha|$, and since $\mathrm{sign}(d/\alpha) = \mathrm{sign}(\alpha)$ the assertion follows from Theorem 5.1 and Theorem 4.1. □

5.9 Theorem *Given α, β in compact representation with $\beta \neq 0$ we can in polynomial time decide whether β divides α in $\mathcal{O}$ and if the decision is positive, we can in polynomial time determine a compact representation of α/β.*

Proof: We compute $d = d(1/\beta)$ and a compact representation for $\alpha_1 = d/\beta$ which is possible by Theorem 5.8. It follows from Lemma 2.4 that $|\mathrm{N}(\alpha_1)| \leq |\mathrm{N}(\beta)|$ and $\mathrm{H}(\alpha_1) \leq \mathrm{H}(\beta)$. Therefore, by Theorem 5.6 the computation of a compact representation of $\alpha_2 = \alpha\alpha_1$ is possible in polynomial time in the size of the original input data. Also we have $|\mathrm{N}(\alpha_2)| = |\mathrm{N}(\alpha)\mathrm{N}(\alpha_1)|$ and $\mathrm{H}(\alpha_2) \leq \mathrm{H}(\alpha)\mathrm{H}(\alpha_1)$. Let $\alpha_2 = (x + y\sqrt{\Delta})/2$ be the standard representation of α_2. Then we can write $\alpha_2 = z + y\frac{\Delta+\sqrt{\Delta}}{2}$ where $z = (x - \Delta y)/2$. Clearly α/β belongs to $\mathcal{O}$ if d divides y and z which means that $2d$ divides $x - \Delta y$. It therefore suffices to determine x and y modulo $2d$ which by Theorem 5.7 is possible in polynomial time. If we have found that α/β belongs to $\mathcal{O}$ then we must only determine an approximation of precision 5 to $\log|\alpha_2/d| = \log|\alpha_2| - \log d$ which by Theorem 5.1 is possible in polynomial time. Then by Theorem 4.1 we obtain a compact representation of α/β in polynomial time in the size of the original input data. □

5.10 Theorem *Given $\alpha, \beta \in \mathcal{O}$ in compact representation, we can decide in polynomial time whether or not $\alpha = \beta$.*

Proof: First we determine whether or not α and β are of the same norm and sign. If not they cannot be equal. By Theorem 5.5 and Theorem 5.4 this can be done in polynomial time. Then we find out whether not β divides α in $\mathcal{O}$. If so, we compute a compact representation of $\gamma = \alpha/\beta$ which by Theorem 5.9 can be done in polynomial time. Now γ is a unit of $\mathcal{O}$ and by Lemma 2.4 $\mathrm{H}(\gamma) \leq \mathrm{H}(\alpha)\mathrm{H}(\beta)$. We also determine an approximation c of precision 3 to $\log|\gamma|$. By Theorem 5.1 this takes polynomial time. By Lemma 3.5 we have $\gamma = 1$ if and only if $|c| < 1/8$. □

5.11 Theorem *Given $\alpha, \beta \in \mathcal{O}$ in compact representation, we can in polynomial time decide whether or not $|\alpha| > |\beta|$.*

Proof: We have $\alpha = 0$ or $\beta = 0$ if and only if one of the factors in one of the compact representations is zero. So without loss of generality we may assume that $\alpha, \beta \neq 0$. Let $\gamma = d(1/\beta)\alpha/\beta$. Then $|a| > |\beta|$ if and only if $|\gamma| > d(1/\beta)$. We determine approximations c of precision 1 to $\log|\gamma|$ and d to $\log d(1/\beta)$. By Theorems 5.8, 5.6, and 5.1 this is possible in polynomial time. If $c > d+1$ then $\log|\gamma| > \log|d(1/\beta)|$ and this means that $|\alpha| > |\beta|$. Otherwise $\log|\gamma| < \log d(1/\beta) + 2 = \log(4d(1/\beta))$. In that case we compute approximations $\overline{c}$ of precision 1 to $\log|\overline{\gamma}|$ and n to $\log|\mathrm{N}(\gamma)|$. This is possible by Theorem 5.5 and Theorem 5.1 since an application of the non trivial automorphism of $\mathcal{O}$ to the compact representation of γ yields a compact representation of $\overline{\gamma}$. If $n - \overline{c} < d - 3/2$ then $|\mathrm{N}(\gamma)/\overline{\gamma}| < d(1/\beta)$ which implies that $|\alpha| < |\beta|$. Otherwise $\overline{c} \leq 3/2 + n - d$ and therefore $\log|\overline{\gamma}| < 3 + \log|\mathrm{N}(\gamma)| - \log d(1/\beta) = \log(8|\mathrm{N}(\gamma)|/d(1/\beta))$ or $|\overline{\gamma}| < 8|\mathrm{N}(\gamma)|/d(1/\beta) = 8d(1/\beta)|\mathrm{N}(\alpha)/\mathrm{N}(\beta)| \leq 8|\mathrm{N}(\alpha)|$. So we can either decide that $|\alpha| > |\beta|$ or we have $\mathrm{H}(\gamma) < \max\{4|\mathrm{N}(\beta)|, 8|\mathrm{N}(\alpha)|\}$ In the latter case we can determine in polynomial time the standard representation $\gamma = (x + y\sqrt{\Delta})/2$ and using that representation it is an easy matter to tell whether or not $|\gamma| > d(1/\beta)$. □

6 Principal ideal testing is in NP

As an application of the results of the previous sections we solve in this section the following problem: Given a quadratic discriminant Δ and given an ideal $\mathrm{A} = a\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2}\mathbb{Z}$ of $\mathcal{O}_\Delta$. Is there a short proof for the principality of A

We first give a more precise formulation of this question. Integers are always given in binary. Then the set $L = \{(\Delta, a, b) \in \mathbb{Z}^3 : \Delta \text{ is a quadratic discriminant}, a\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2}\mathbb{Z} \text{ is a principal ideal in } \mathcal{O}_\Delta\}$ can be considered as a language over the alphabet $\Sigma = \{0, 1, @\}$. The symbol @ is used as a separator. The class of languages over Σ which in polynomial time are decided by a deterministic Turing machine is denoted by P. The class of languages over Σ which can in polynmial time be accepted by a non deterministic Turing machine is denoted by NP.

6.1 Theorem *The language L belongs to the class NP.*

Proof: Let $(\Delta, a, b) \in L$. Let α be a generator of $\mathrm{A} = a\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2}\mathbb{Z}$ with $\log \mathrm{H}(\alpha) \leq \max\{\sqrt{\Delta}(\log \Delta)^2, \mathrm{N}(\mathrm{A})\}$. By Lemma 3.7 such a generator exists. A compact representation of α as in equality (4) and Lemma 4.8 is a proof for the principality of A which by Theorem 5.3 can be verified in polynomial time. □

References

[1] J. Buchmann, H. C. Williams, *On the existence of a short proof for the value of the class number and regulator of a real quadratic field,* Number Theory and Applications, Nato ASI Series, Kluwer Academic Press, 1989, 327-345.

[2] H. Cohen, *A Course in Computational algebraic number theory,* Springer Verlag, to appear.

[3] H. Cohen, H. W. Lenstra, *Heuristics on class groups of number fields,* Number Theory (Noordwijkerhout, 1983), Lecture Notes in Math. Vol. 1068, Springer-Verlag, Berlin and New York, 1984, 33-62.

[4] G. W. Fung, H. C. Williams, *Compact Representation of the Fundamental Unit in a Complex Cubic Field,* unpublished manuscript, 1991.

[5] J. C. Lagarias, *Succinct certificates for the solvability of binary quadratic polynomials,* Proc. 20th IEEE Conference on Foundations of Computer Science, 1979, 47-54.

[6] H. W. Lenstra, *On the computation of regulators and class numbers of quadratic fields,* Lond. Math. Soc. Lect. Note Ser. **56** (1982), 123-150.

[7] W. Narkiewiecz, *Elementary and Analytic Theory of Algebraic Numbers*, Polish Scientific Publishers, Warszawa, 1974, 400-401.

[8] J. Neukirch, *Algebraische Zahlentheorie*, Springer Verlag, Berlin, 1992, 33-34.

[9] J. Oesterlé, *Versions effectives du théorème de Chebotarev sous l'hypothèse de Riemann généralisée,* Soc. Math. de France Astérisque 61 (1979), 165-167.

[10] D. Shanks, *The infrastructure of a real quadratic field and its applications,* Proc. 1972 Number Theory Conference, Boulder (1972), 217-224.