Publ. Math. Debrecen
39 / 1–2 (1991), 19–86

Lattice minima and units in real quadratic number fields

By DANIEL C. MAYER (Graz)

Respectfully dedicated to Professor Alexander Aigner.

Abstract. Using the number geometric concept of lattice minima, it is possible to give a new proof for the fact that one of the generators of ambiguous principal ideals can always be found in the middle of the first primitive period of minimal points in the geometric Minkowski image of the maximal order in a real quadratic number field with normpositive fundamental unit. In particular, the treatment of odd radicands $D \equiv 3 (\bmod 4)$, where the ramification of 2 causes troubles, and $D \equiv 1 (\bmod 4)$, where complications arise from the existence of "half–integers", is considerably easier by this method than by means of continued fractions. Nevertheless, the relations between minimal points in a very general type of lattices and convergents for continued fraction expansions are also examined in detail. Further the distribution of normpositive fundamental units, and of the unit group indices for radicands $D \equiv 5 (\bmod 8)$, is investigated for squarefree positive $D < 10^5$ with the aid of a computer.

§0. Introduction and notation

After some preparatory sections on orders and ramification in § 1, and on lattice minima and chains at the begin of § 2, Theorem 2.3 displays the scale of norms of lattice minima in the various orders of real quadratic fields. In § 3, Theorem 3.2, we state the central result about the connection between minimal points in a rather general type of 2–dimensional lattices and convergents for continued fraction expansions, which is applied to real quadratic number fields in several Corollaries. § 4 deals with the peculiar phenomena, which arise in a comparison of two different orders with respect to their units and lattice minima. Here, Theorem 4.2 establishes the basis for a first version of the unit algorithm, resting upon the determination of minima in a suborder, which are multiples of units in the

1980 Mathematics Subject Classification. 11R11, 11R27, 11D09, 11D57, 11A55, 11Y65.
Keywords. Quadratic fields, lattice minima, principal factors, units, Pellian equations, continued fractions.

maximal order. This version permits a uniform initialization of the unit algorithm for all real quadratic fields, except for one special field, $D = 5$. § 5 starts with preliminaries on generators of ambiguous principal ideals and their norms, and is devoted to the proof of the main results in Theorems 5.11 and 5.12, that one of these generators always appears in the middle of the first primitive period of lattice minima in the maximal order, provided the field has a normpositive fundamental unit, and for certain radicands also in suborders. This fact allows a second version of the unit algorithm, executing very rapidly: the construction of minima, which are radicals of multiples of units, in various orders of a real quadratic field. Thus, as a side result of our investigations into the geometric number theory of real quadratic fields, we obtained special cases of two general methods for the indirect computation of units in arbitrary number fields. Details of these methods, together with similar developments for pure cubic fields, can be found in [21]. As a conclusion, several tables concerning the frequencies and statistics of radicand types, principal factor types, and unit group indices are recorded in § 6 and discussed, in particular pointing out some long period phenomena with influences on the unit calculation.

We use the following notation. If S is a semigroup with unit element, we let $U(S)$ be the group of units (invertible elements) in S, and for an integral domain $R, R^\times = R \setminus \{0\}$ is the multiplication semigroup. Further we denote by $\mathbf{P}$ the set of rational primes. For an algebraic number field K, $\mathbf{P}_K$ is the set of non–zero prime ideals, $\mathcal{I}_K$ (resp. $\mathcal{H}_K$) the group of fractional ideals (resp. principal ideals), $\mathcal{I}_K^0$ (resp. $\mathcal{H}_K^0$) the semigroup of integral ideals (resp. principal ideals), E_K the unit group, and W_K the group of roots of unity in K. Similarly for an order $\mathcal{O}$ in K, $E_\mathcal{O} = U(\mathcal{O}^\times)$ is the unit group in $\mathcal{O}$, and if K is real, $E_\mathcal{O}^+ = \{\varepsilon \in E_\mathcal{O} \mid \varepsilon > 0\}$ is the subgroup of positive units in $\mathcal{O}$. $(v_\mathcal{P})_{\mathcal{P} \in \mathbf{P}_K}$ will be the family of $\mathcal{P}$–adic valuations of $\mathcal{I}_K$ yielding the isomorphism $(\mathcal{I}_K, \times) \simeq (\mathbf{Z}^{(\mathbf{P}_K)}, +)$. If $L \mid k$ is a relative extension of number fields, then $N_{L \mid k} : L \to k$ is the relative norm of numbers, $\mathcal{N}_{L \mid k} : \mathcal{I}_L \to \mathcal{I}_k$ the relative norm of ideals, $E_{L \mid k} = \{E \in E_L \mid N_{L \mid k}(E) = 1\}$ the group of relative units, and for any prime ideal $\mathcal{P} \in \mathbf{P}_k$, $e_{L \mid k}(\mathcal{P})$ will denote the greatest common divisor of all ramification exponents of prime ideals in L lying over $\mathcal{P}$. Finally C_n is the cyclic group of order n, and $\mathbf{F}_q$ is the finite field with q elements.

§1. Orders, discriminants and prime decomposition

In the first theorem, which is well known, we recall some basic properties of quadratic number fields, emphasizing those aspects, concepts and notations, which are vital for the development of the theories in this paper. The classification of real and complex quadratic number fields, according to their maximal orders, discriminants, and the decomposition behaviour of the particular rational prime 2, can be reduced to the characterization by the residue class of the radicand D modulo 4 or modulo 8, and hence leads to the declaration of radicand types or Dedekind types (D–types) of quadratic number fields. Compare also §6, Tables 1,2 for the frequencies and statistics of these types.

Theorem 1.1. (R. Dedekind, 1894; D. Hilbert, 1897.) *Let $D \in \mathbf{Z}$, $D \neq 1$ be a squarefree radicand, that is $\forall p \in \mathbf{P}$ $v_p(D) \leq 1$. Further let $\delta = \sqrt{D}$ be the generating radical, and $\mathcal{O}_K$ the maximal order of the quadratic number field $K = \mathbf{Q}(\delta)$, which is a cyclic extension with C_2–group $Gal(K \mid \mathbf{Q}) = \langle\tau\rangle$, $\tau(\delta) = -\delta$. Finally denote by $\mathcal{O}$ the suborder $\mathbf{Z} \oplus \mathbf{Z}\delta$ of the maximal order $\mathcal{O}_K$, and by $R_{K \mid \mathbf{Q}} = \prod\{r \in \mathbf{P} \mid e_{K \mid \mathbf{Q}}(r) = 2\}$ the ramification quantity of $K \mid \mathbf{Q}$ (the product of all rational prime numbers ramifying in K).*

1. *The discriminant of the suborder $\mathcal{O}$ is discr $(\mathcal{O}) = 2^2 \cdot D = 4D$.*

2. *There are the following Dedekind types or radicand types (D–types) of real and complex quadratic number fields, according to their maximal orders, disriminants, and the decomposition behaviour of the particular rational prime number 2:*

(I) *K is of D–type I, iff one of the following equivalent conditions is satisfied:*

(1) $D \not\equiv 1 (\bmod 4)$.
(2) 2 is ramified in K, $2\mathcal{O}_K = \mathcal{R}^2$ with $\mathcal{R} \in \mathbf{P}_K$, $\mathcal{N}_{K \mid \mathbf{Q}}(\mathcal{R}) = 2$.
(3) $2 \mid R_{K \mid \mathbf{Q}}$, *that is, 2 is an essential discriminant divisor.*
(4) $(\mathcal{O}_K : \mathcal{O}) = 1$, *that is, $\mathcal{O}_K = \mathcal{O}$ with unitary integral basis $(1, \delta)$.*
(5) $discr(K \mid \mathbf{Q}) = discr(\mathcal{O}_K) = discr(\mathcal{O}) = 4D \equiv 0 (\bmod 4)$.

Subclassification for the fields K of D–type I :

(A) *K is of D–type IA, iff one of the following equivalent condtions is satsified:*

(1) $D \equiv 2 (\bmod 4)$, *that is,* $2 \mid D$.
(2) $2\mathcal{O}_K = \mathcal{R}^2$, where $\mathcal{R} = \mathbf{Z}2 \oplus \mathbf{Z}\delta \in \mathbf{P}_K$.
(3) $R_{K \mid \mathbf{Q}} = D$ and $2 \mid D$.

(B) *K is of D–type IB, iff one of the following equivalent conditions is satisfied:*

(1) $D \equiv 3 (\bmod 4)$, *and hence* $2 \nmid D$.
(2) $2\mathcal{O}_K = \mathcal{R}^2$, where $\mathcal{R} = \mathbf{Z}2 \oplus \mathbf{Z}(1 + \delta) \in \mathbf{P}_K$.
(3) $R_{K \mid \mathbf{Q}} = 2D$.

(II) *K is of D–type II, iff one of the following equivalent conditions is satisfied:*

(1) $D \equiv 1(\bmod 4)$, *and hence* $2 \nmid D$.

(2) *2 is unramified in* K.

(3) $R_{K\,|\,\mathbf{Q}} = D$ and $2 \nmid D$.

(4) $(\mathcal{O}_K : \mathcal{O}) = 2$, *and, more detailed,* $\mathcal{O}_K = \mathbf{Z} \oplus \mathbf{Z}\frac{1}{2}(1+\delta)$ *with unitary integral basis* $\left(1, \frac{1}{2}(1+\delta)\right)$. *The conductor of the suborder* $\mathcal{O}$ *in the maximal order* $\mathcal{O}_K$ *is* $\mathcal{F} = cond(\mathcal{O}) = \gcd\{\mathcal{A} \in \mathcal{I}_K^0 \mid \mathcal{A} \subset \mathcal{O}\} = 2\mathcal{O}_K = \mathbf{Z}2 \oplus \mathbf{Z}(1+\delta) \subset \mathcal{O}$.

(5) $discr(K\,|\,\mathbf{Q}) = discr(\mathcal{O}_K) = discr(\mathcal{O})/(\mathcal{O}_K : \mathcal{O})^2 = 4D/4 = D \equiv 1(\bmod 4)$.

Subclassification for the fields K *of* D*–type* II :

(A) K *is of D–type IIA, iff one of the following equivalent conditions is satisfied:*

(1) $D \equiv 1(\bmod 8)$, *and hence* $\left(\frac{D}{2}\right) = 1$.

(2) *2 splits in* K, $2\mathcal{O}_K = \mathcal{L} \cdot \tau(\mathcal{L})$, *where* $\mathcal{L} = \mathbf{Z}2 \oplus \mathbf{Z}\frac{1}{2}(1+\delta) \in \mathbf{P}_K$, $\mathcal{N}_{K\,|\,\mathbf{Q}}(\mathcal{L}) = 2$.

(B) K *is of* D*–type* IIB, *iff one of the following equivalent conditions is satisfied:*

(1) $D \equiv 5(\bmod 8)$, *and hence* $\left(\frac{D}{2}\right) \neq 1$.

(2) *2 remains inert in* K, $2\mathcal{O}_K \in \mathbf{P}_K$, $\mathcal{N}_{K\,|\,\mathbf{Q}}(2\mathcal{O}_K) = 2^2 = 4$.

3. *For prime numbers* $p \in \mathbf{P}$, $p \neq 2$ *the following law of decomposition in* K *is valid:*

a) p *is ramified in* K, *iff* $p \mid D$.
Then $p\mathcal{O}_K = \mathcal{P}^2$, *where* $\mathcal{P} = \mathbf{Z}p \oplus \mathbf{Z}\delta \in \mathbf{P}_K$ *(respectively* $\mathcal{P} = \mathbf{Z}p \oplus \mathbf{Z}\frac{1}{2}(p+\delta)$, *iff* $D \equiv 1(\bmod 4)$), $\mathcal{N}_{K\,|\,\mathbf{Q}}(\mathcal{P}) = p$.

b) p *splits in* K, *iff* $p \nmid D$, $\left(\frac{D}{p}\right) = 1$.
Then $p\mathcal{O}_K = \mathcal{P} \cdot \tau(\mathcal{P})$, *where* $\mathcal{P} = \mathbf{Z}p \oplus \mathbf{Z}(a+\delta) \in \mathbf{P}_K$ *(respectively* $\mathcal{P} = \mathbf{Z}p \oplus \mathbf{Z}\frac{1}{2}(a+\delta)$, *iff* $D \equiv 1(\bmod 4)$), $a \in \mathbf{Z}$, $D \equiv a^2(\bmod p)$ $(a \equiv 1(\bmod 2)$, *if* $D \equiv 1(\bmod 4))$, $\mathcal{N}_{K\,|\,\mathbf{Q}}(\mathcal{P}) = p$.

c) p *remains inert in* K, *iff* $p \nmid D$, $\left(\frac{D}{p}\right) \neq 1$.
Then $p\mathcal{O}_K \in \mathbf{P}_K$, $\mathcal{N}_{K\,|\,\mathbf{Q}}(p\mathcal{O}_K) = p^2$.

4. *Any order in* K, *that is, any integral domain in* $\mathcal{O}_K$ *with quotient field* K, *is* τ*–invariant and of one of the following forms*

a) $\mathcal{O}_f = \mathbf{Z} \oplus \mathbf{Z}f\delta$ *with some* $f \in \mathbf{N}$, *unitary* $\mathbf{Z}$*–basis* $(1, f\delta)$, *conductor* $cond(\mathcal{O}_f) = f\mathcal{O}$, *index* $(\mathcal{O} : \mathcal{O}_f) = f$ *and discriminant* $discr(\mathcal{O}_f) = (\mathcal{O} : \mathcal{O}_f)^2 \cdot discr(\mathcal{O}) = f^2 \cdot 4D = 4f^2D$ *in the case of a* D*–type* I *field,* $D \equiv 2, 3(\bmod 4)$, *with maximal order* $\mathcal{O} = \mathbf{Z} \oplus \mathbf{Z}\delta = \mathcal{O}_1$, *b)* $\mathcal{O}_{K,f} = \mathbf{Z} \oplus \mathbf{Z}\frac{f}{2}(1+\delta)$ *with some* $f \in \mathbf{N}$, *unitary* $\mathbf{Z}$*–basis* $\left(1, \frac{f}{2}(1+\delta)\right)$, *conductor* $cond(\mathcal{O}_{K,f}) = f\mathcal{O}_K$, *index* $(\mathcal{O}_K : \mathcal{O}_{K,f}) = f$ *and discriminant* $discr(\mathcal{O}_{K,f}) = (\mathcal{O}_K : \mathcal{O}_{K,f})^2 \cdot discr(\mathcal{O}_K) = f^2 \cdot D$ *in the case of a* D*–type* II *field,* $D \equiv 1 (\mathrm{mod}\, 4)$, *with maximal order* $\mathcal{O}_K = \mathbf{Z} \oplus \mathbf{Z}\frac{1}{2}(1+\delta) = \mathcal{O}_{K,1}$. *In particular, for even conductors* $2f$ *with* $f \in \mathbf{N}$ *we have formally* $\mathcal{O}_{K,2f} = \mathbf{Z} \oplus \mathbf{Z}\frac{2f}{2}(1+\delta) = \mathbf{Z} \oplus \mathbf{Z}(f + f\delta) = \mathbf{Z} \oplus \mathbf{Z}f\delta = \mathcal{O}_f$ *with another unitary* $\mathbf{Z}$*–basis* $(1, f\delta)$ and $discr(\mathcal{O}_{K,2f}) = (2f)^2 \cdot D = 4f^2 D = discr(\mathcal{O}_f)$.

PROOF. See R. DEDEKIND [8], Supplement XI, §§ 186–187, 634–657, D. HILBERT [15], §§ 59–61, 280–284 and § 88, pag. 322, or H. HASSE [12], § 26, 478–483. □

§2. Lattices, minimal points and chains

1. Let $\binom{\eta_1}{\eta_2}, \binom{\xi_1}{\xi_2} \in \mathbf{R}^2$ be linearly independent over $\mathbf{R}$, then

$$\Lambda = \mathbf{Z}\begin{pmatrix}\eta_1\\ \eta_2\end{pmatrix} \oplus \mathbf{Z}\begin{pmatrix}\xi_1\\ \xi_2\end{pmatrix}$$

is a *complete lattice* in $\mathbf{R}^2$, that is, a free $\mathbf{Z}$–module of rank 2. Λ is symmetric with respect to the origin. Hence it is no loss of information to consider only the right half plane, $x_1 \geq 0$, of $\mathbf{R}^2$.

For $\mathbf{a} = \binom{a_1}{a_2} \in \mathbf{R}^2$ we define the *rectangle* of $\mathbf{a}$,

$$R(\mathbf{a}) = \{\mathbf{x} \in \mathbf{R}^2 \mid 0 \leq x_1 \leq |\, a_1 \,|, |\, x_2 \,| \leq |\, a_2 \,|\},$$

the 1–*strip* of $\mathbf{a}$ (the dilatation region of the rectangle $R(\mathbf{a})$ in 1–direction),

$$S_1(\mathbf{a}) = \{\mathbf{x} \in \mathbf{R}^2 \mid x_1 > |\, a_1 \,|, |\, x_2 \,| < |\, a_2 \,|\},$$

and the 2–*strip* of $\mathbf{a}$ (the dilatation region of the rectangle $R(\mathbf{a})$ in 2–direction),

$$S_2(\mathbf{a}) = \{\mathbf{x} \in \mathbf{R}^2 \mid 0 \leq x_1 < |\, a_1 \,|, |\, x_2 \,| > |\, a_2 \,|\}.$$

For two points $\mathbf{a}, \mathbf{b} \in \mathbf{R}^2$ let their *common rectangle* be

$$R(\mathbf{a}, \mathbf{b}) = \{x \in \mathbf{R}^2 \mid 0 \leq x_1 \mid \max(|\, a_1 \,|, |\, b_1 \,|), |\, x_2 \,| \leq \max(|\, a_2 \,|, |\, b_2 \,|)\}.$$

A lattice point $\mathbf{m} \in \Lambda$ is called a *lattice minimum* or *minimal point* of Λ or also a *best approximation* of the Cartesian coordinate axes by the lattice Λ, iff $int(R(\mathbf{m})) \cap \Lambda = \{0\}$. It should be emphasized that, according to this declaration, a point on the coordinate axes, in particular the origin 0 itself, is not a lattice minimum, but with each minimum $\mathbf{m}$ in the right half plane there is another minimum $-\mathbf{m}$ in the left half plane. We denote by $Min(\Lambda)$ the system of all lattice minima of Λ and by $Min^{+}(\Lambda)$ those in the right half plane. Then simply

$$Min(\Lambda) = \{\pm\mathbf{m} \mid \mathbf{m} \in Min^{+}(\Lambda)\}.$$

If $\mathbf{m} \in Min(\Lambda)$ is a lattice minimum, then it does not lie on the 1–axis, $m_2 \neq 0$, and the 1–strip $S_1(\mathbf{m})$ is not empty. Hence, according to Minkowski's theorem, we find a first lattice point $\mathbf{n} \in S_1(\mathbf{m}) \cap \Lambda$ by dilatation of the rectangle $R(\mathbf{m})$ in 1–direction before the value of the first coordinate exceeds $|\eta_1\xi_2 - \eta_2\xi_1| / |m_2|$, where the determinant $|\eta_1\xi_2 - \eta_2\xi_1|$ is the area of the fundamental lattice mesh. Similar considerations can be made for the 2–direction. Thus it makes sense to define:
If $\mathbf{m} \in Min(\Lambda)$ is a lattice minimum, then a lattice point $\mathbf{n} \in S_1(\mathbf{m}) \cap \Lambda$ (respectively $\mathbf{n} \in S_2(\mathbf{m}) \cap \Lambda$) is called 1–*neighbour* (resp. 2–*neighbour*) of $\mathbf{m}$ or 1–*adjacent* (resp. 2–*adjacent*) to $\mathbf{m}$, iff $int(R(\mathbf{m}, \mathbf{n})) \cap \Lambda = \{0\}$. We write $\nu_1(\mathbf{m}) = \mathbf{n}$ (resp. $\nu_2(\mathbf{m}) = \mathbf{n}$). For general lattices Λ, neighbours need not be minima themselves, because they can lie on an axis.

2. $\mathbf{p} \in \Lambda$ is called a *primary* lattice point, iff $\forall t \in \mathbf{R}\ (0 < t < 1 \Rightarrow t \cdot \mathbf{p} \notin \Lambda)$, that is, iff the "open" line segment from the origin to $\mathbf{p}$ does not contain any lattice points. Notice that the origin is not primary.

Remark. A lattice minimum $\mathbf{m} \in Min(\Lambda)$ is primary.

PROOF. We use contraposition. If $\mathbf{m} \in \Lambda$ is not primary, then either $\mathbf{m} = 0 \notin Min(\Lambda)$, or $\mathbf{m} \neq 0$ but $t \cdot \mathbf{m} \in \Lambda$ for some $t \in \mathbf{R},\ 0 < t < 1$. In the last case either $\mathbf{m}$ lies on a coordinate axis or $int(R(\mathbf{m})) \cap \Lambda$ contains at least two points, 0 and $sgn(m_1) \cdot t \cdot \mathbf{m}$, whence $\mathbf{m} \notin Min(\Lambda)$. □

3. We shall not be concerned with general two dimensional lattices Λ in $\mathbf{R}^2$ but mainly with those, which arise as geometric Minkowski images of orders $\mathcal{O}$ in real quadratic number fields $K = \mathbf{Q}(\sqrt{D})$.

Assume that an arbitrary algebraic number field K has the degree $[K : \mathbf{Q}] = n,\ n \in \mathbf{N}$, and the signature $(r_1, r_2),\ n = r_1 + 2r_2$. We denote the $\mathbf{Q}$–linear *Minkowski embedding* by

$$\psi : K \to \mathbf{R}^2,\ \alpha \to (\ \psi_1(\alpha), \dots, \psi_{r_1}(\alpha), \mathrm{Re}(\psi_{r_1+1}(\alpha)), \mathrm{Im}(\psi_{r_1+1}(\alpha)), \dots, \\ \mathrm{Re}(\psi_{r_1+r_2}(\alpha)), \mathrm{Im}(\psi_{r_1+r_2}(\alpha))\ ),$$

where we suppose that $\psi_1, \dots, \psi_{r_1}, \psi_{r_1+1}, \overline{\psi}_{r_1+1}, \dots, \psi_{r_1+r_2}, \overline{\psi}_{r_1+r_2}$ are the $\mathbf{Q}$–monomorphisms from K into $\mathbf{C}$, i.e., the injective field homomorphisms fixing $\mathbf{Q}$. We always assume that a number field K is an intermediate field of the extension $\mathbf{C} \mid \mathbf{Q}$ and that ψ_1 is the inclusion $K \to \mathbf{C}, \alpha \to \alpha$,

for the sake of simplicity.
If N is the normal field of $K \mid \mathbf{Q}$ and $Gal(N \mid \mathbf{Q}) = \cup_{i=1}^{n} \phi_i \circ Gal(N \mid K)$ is the disjoint left coset decomposition of its group (with $\phi_1 = id_N$), then we can assume that $\psi_i = \psi_{N,1} \circ \phi_i|_K$ for all $1 \leq i \leq n$.

In the special case of a real quadratic field $K = N = \mathbf{Q}(\sqrt{D})(D > 0)$ with C_2–group $Gal(K \mid \mathbf{Q}) = \langle \tau \rangle$, we have $n = r_1 = 2,\ \phi_2 = \tau,\ \psi_2 = \psi_1 \circ \tau$ and $\psi : K \to \mathbf{R}^2,\ \alpha \to \binom{\alpha}{\alpha'}$, where we denote the non–trivial conjugate by $\alpha' = \psi_2(\alpha) = \tau(\alpha)$.

4. The geometric Minkowski image of any free $\mathbf{Z}$–module $\mathcal{M} = \mathbf{Z}\eta \oplus \mathbf{Z}\xi$ in $K = \mathbf{Q}(\sqrt{D})$ with $\mathbf{Z}$–basis (η, ξ), i.e., the discretization of $\mathcal{M}$, is a complete lattice in $\mathbf{R}^2$,

$$\psi(\mathcal{M}) = \mathbf{Z}\begin{pmatrix}\eta\\ \eta'\end{pmatrix} \oplus \mathbf{Z}\begin{pmatrix}\xi\\ \xi'\end{pmatrix}.$$

Algebraic numbers $\alpha \in \mathcal{M}$, whose geometric images $\psi(\alpha)$ are lattice minima of $\psi(\mathcal{M})$, will be called *minima* in $\mathcal{M}$ shortly and we shall write $Min(\mathcal{M}) = \psi^{-1}(Min(\psi(\mathcal{M})))$ for the system of all (respectively $Min^{+}\ (\mathcal{M})$ for all positive) minima in $\mathcal{M}$.

The area of the rectangle $R(\psi(\alpha))$ of the geometric image $\psi(\alpha)$ of an algebraic number $\alpha \in K$ is exactly two times the absolute value of its norm $|\,\alpha\,| \cdot 2\,|\,\alpha'\,| = 2\,|\,N_{K \mid \mathbf{Q}}(\alpha)\,|$. Therefore $R(\psi(\alpha))$ is also called the *norm rectangle* of α. Hence algebraic numbers $\alpha \in \mathcal{M}$ with minimal norms in $\mathcal{M}$ are always minima in $\mathcal{M}$. In particular, in the case of an order $\mathcal{O} = \mathbf{Z} \oplus \mathbf{Z}\xi$ in K, with unitary $\mathbf{Z}$–basis $(1, \xi)$ and geometric Minkowski image

$$\psi(\mathcal{O}) = \mathbf{Z}\begin{pmatrix}1\\ 1\end{pmatrix} \oplus \mathbf{Z}\begin{pmatrix}\xi\\ \xi'\end{pmatrix},$$

numbers with minimal norms are just the units, with norm ±1. Hence $E_{\mathcal{O}} \subset Min(\mathcal{O})$, and in particular, $1 \in Min^{+}(\mathcal{O})$.

5. For the special lattices of type $\psi(\mathcal{O})$ in $\mathbf{R}^2$, arising as geometric Minkowski images of orders, neighbours of minima are uniquely determined and minima again, whence we obtain *neighbour mappings* ν_k : $Min^{+}(\psi(\mathcal{O})) \to Min^{+}(\psi(\mathcal{O}))$, respectively $\nu_k : Min^{+}(\mathcal{O}) \to Min^{+}(\mathcal{O})$, writing for simplicity $\nu_k(\alpha) = \psi^{-1}(\nu_k(\psi(\alpha)))$ for any $\alpha \in Min(\mathcal{O})$, $k = 1, 2$.

By the repetitive construction of neighbours in both coordinate directions, starting with an arbitrary positive minimum $\alpha \in Min^{+}(\mathcal{O})$, all positive minima in $\mathcal{O}$ can be found and arranged in two sequences of successive neighbours of α. For symmetry reasons, the minimum 1 is taken as the starting point in general, in which case these sequences are called the 1–*chain* and the 2–*chain* of minima in $\mathcal{O}, (\nu_1^j(1))_{j\geq 0}$ and $(\nu_2^j(1))_{j\geq 0}$. Here ν_k^j denotes the j–th iterate of the map ν_k for $j \in \mathbf{N}_0$ and $k = 1, 2$. Therefore

$$Min^+(\mathcal{O}) = \{\nu_1^j(1) \mid j \geq 0\} \cup \{\nu_2^j(1) \mid j \geq 0\}.$$

6. The group $E_{\mathcal{O}}^+$ of positive units in $\mathcal{O}$ acts on the system of positive minima $Min^+(\mathcal{O})$ by multiplication, the neighbour mappings are inverse $E_{\mathcal{O}}^+$–isomorphisms, $\nu_2 = \nu_1^{-1}$, and there are only finitely many $E_{\mathcal{O}}^+$–*orbits* in $Min^+(\mathcal{O})$ under this action. If, for some $p \in \mathbf{N}$,

$$Min^+(\mathcal{O}) = \bigcup_{j=0}^{p-1} E_{\mathcal{O}}^+ \nu_1^j(1)$$

is the disjoint orbit decomposition, then $PL(\mathcal{O}) = p$ is called the *primitive period length* of $Min(\mathcal{O})$ and the $(p+1)$–tuple $(\nu_1^j(1))_{0\leq j\leq p}$ is called the *first primitive period* of $Min(\mathcal{O})$ in 1–direction.

The positive units in $\mathcal{O}$ form a distinguished *principal orbit*,

$$E_{\mathcal{O}}^+ = E_{\mathcal{O}}^+ \nu_1^0(1) = \{\nu_1^{jp}(1) \mid j \geq 0\} \cup \{\nu_2^{jp}(1) \mid j \geq 0\} = \{\varepsilon_0^j \mid j \in \mathbf{Z}\},$$

where the unit $\varepsilon_0 = \nu_1^p(1) \in E_{\mathcal{O}}^+$ is called the *fundamental unit* of the order $\mathcal{O}$. Of course, $\varepsilon_0 > 1$.

For proofs of these various properties, most of which remain true with minor modifications for orders in any number field of unit rank 1, see J. Buchmann [5], [6], [7]. For other viewpoints consult A. J. Brentjes [4], H. Minkowski [22], R. Steiner [31], G. F. Voronoi [33] and H. C. Williams [39].

Remark. (Symmetry property of the norms of lattice minima with respect to the primitive period.)

Let $1, \nu_1(1), \nu_1^2(1), \ldots, \nu_1^p(1) = \varepsilon_0$ be the first primitive period of lattice minima in the 1–chain of an order $\mathcal{O}$ with period length $p \in \mathbf{N}$, then

$$\forall 0 \leq j \leq p \quad N_{K\mid\mathbf{Q}}(\nu_1^j(1)) = N_{K\mid\mathbf{Q}}(\nu_1^{p-j}(1)).$$

Proof. This symmetry is due to the influence of the non–trivial automorphism $\tau \in Gal(K \mid \mathbf{Q})$ onto the lattice minima in an order $\mathcal{O}$, which is τ–invariant by Theorem 1.1, 4. The invariance implies $\nu_2^j(1) = |\,\tau(\nu_1^j(1))\,|$ for all $j \geq 0$. Hence $\nu_1^{p-j}(1) = \nu_1^{-j}(\nu_1^p(1)) = \nu_2^j(\varepsilon_0) = \varepsilon_0 \cdot \nu_2^j(1) = \varepsilon_0 \cdot |\,\tau(\nu_1^j(1))\,|$ and thus the norms coincide. □

7. Finally we note that an algebraic integer α in an order $\mathcal{O}$ is called *primitive* in $\mathcal{O}$, iff no rational prime number $p \in \mathbf{P}$ divides α in $\mathcal{O}$, that is, $\alpha \notin p\mathcal{O}$ for every $p \in \mathbf{P}$.

Remark. If the geometric image of an algebraic integer $\alpha \in \mathcal{O}$ is a primary lattice point $\psi(\alpha) \in \psi(\mathcal{O})$, then α is primitive in $\mathcal{O}$.

PROOF. By contraposition: α imprimitive in $\mathcal{O} \Rightarrow \exists p \in \mathbf{P}\ \alpha \in p\mathcal{O}$, i.e., $\alpha/p \in \mathcal{O} \Rightarrow$ either $\alpha = 0$ or $\psi(\alpha)/p = \psi(\alpha/p) \in \psi(\mathcal{O})$ with $0 < 1/p < 1$, and hence $\psi(\alpha)$ is not a primary lattice point of $\psi(\mathcal{O})$. □

The following two Lemmata will be used repeatedly in the proofs of central results about various types of lattice minima in Theorem 2.3 ("small" norms), Theorem 4.2 (norm ±4), and Lemma 5.10 (minimal discriminantal principal factor norms).

Lemma 2.1. (An estimate for the solutions of a system of two binary linear inequalities.)

Let $\gamma \in \mathbf{C}$ be real or purely imaginary and $x, y \in \mathbf{Q}$. If there are bounds $M, N \in \mathbf{R}^+$ such that

$$|\,x + y\gamma\,| < M \text{ and}$$
$$|\,x - y\gamma\,| < N,$$

then the coefficients x, y can be estimated by $|\,x\,|, |\,y\gamma\,| < \frac{1}{2}(M + N)$.

PROOF. The matrix

$$A = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \in M_2(\mathbf{Q}) \text{ is invertible and } A^{-1} = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Let $\alpha, \alpha' \in \mathbf{Q}[\gamma]$ be defined by

$$\begin{pmatrix} \alpha \\ \alpha' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y\gamma \end{pmatrix}. \text{ Then } \begin{pmatrix} x \\ y\gamma \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} \alpha \\ \alpha' \end{pmatrix} \text{ and hence}$$

$|\,x\,| = \frac{1}{2}\,|\,\alpha + \alpha'\,| \le \frac{1}{2}(\,|\,\alpha\,| + |\,\alpha'\,|\,) < \frac{1}{2}(M + N)$,
$|\,y\gamma\,| = \frac{1}{2}\,|\,\alpha - \alpha'\,| \le \frac{1}{2}(\,|\,\alpha\,| + |-1| \cdot |\,\alpha'\,|\,) < \frac{1}{2}(M + N)$. □

Remark. (An estimate for the coefficients of an algebraic number with bounded conjugates in an arbitrary quadratic number field.)

In particular, for a (real or complex) quadratic field $K = \mathbf{Q}(\sqrt{D})$, Lemma 2.1 with the specialization $\gamma = \sqrt{D}$ allows an estimate for the coefficients $x, y \in \mathbf{Q}$ of an algebraic number $\alpha = x + y\sqrt{D} \in K$, if bounds for the absolute values of the conjugates α, α' are known.

Lemma 2.2. (Euklid's lemma for algebraic integers.)

Let K be an algebraic number field and $\mathcal{O}$ an order in K. Further suppose that $n, m \in \mathbf{N}$, and $\alpha \in \mathcal{O}$ is an algebraic integer in the order $\mathcal{O}$.

If n divides $m\alpha$ in $\mathcal{O}$ (that is, $m\alpha \in n\mathcal{O}$), but either α is primitive in $\mathcal{O}$ or $\gcd(\alpha, n) = 1$, then n must divide already m, $n \mid m$.

PROOF. $m\alpha \in n\mathcal{O}$ implies that $m\alpha = n\beta$ for some $\beta \in \mathcal{O}$. Let $M = m/\gcd(m,n)$ and $N = n/\gcd(m,n)$, then $\gcd(M,N) = 1$ and hence $\exists x, y \in \mathbf{Z} \quad xM + yN = 1$. Now $M\alpha = N\beta$ and therefore $\alpha = xM\alpha + yN\alpha = N(x\beta + y\alpha)$, where $x\beta + y\alpha \in \mathcal{O}$ and thus $\alpha \in N\mathcal{O}$, i.e., N divides α in $\mathcal{O}$. But, as either α is primitive in $\mathcal{O}$ or $N\mathcal{O}_K \supset \alpha\mathcal{O}_K + n\mathcal{O}_K = \mathcal{O}_K$, we must have $N = 1$, that is, $\gcd(m,n) = n$, whence $n \mid m$. □

On the basis of these two lemmata we are in the position to prove the following geometric theorem for the Minkowski image of arbitrary orders in real quadratic number fields, displaying the scale of norms of algebraic integers and, in particular, showing that primitive algebraic integers with "sufficiently small" norms are lattice minima.

Theorem 2.3. (Some bounds for norms of lattice minima in the various orders of real quadratic number fields.)

Let $K = \mathbf{Q}(\sqrt{D})$ be a real quadratic field with squarefree radicand $D \in \mathbf{N}$, $D \geq 2$ and $f \in \mathbf{N}$.

1. *Suppose K is of arbitrary D–type and $\alpha \in \mathcal{O}_f = \mathbf{Z} \oplus \mathbf{Z} f\sqrt{D}$ is an alegbraic integer.*
   - **a)** *If α is primitive in $\mathcal{O}_f$ and $|N_{K|\mathbf{Q}}(\alpha)| < f\sqrt{D}$, then $\alpha \in Min(\mathcal{O}_f)$.*
   - **b)** *Conversely, if $\alpha \in Min(\mathcal{O}_f)$, then α is primitive in $\mathcal{O}_f$ and $|N_{K|\mathbf{Q}}(\alpha)| < \sqrt{|discr(\mathcal{O}_f)|} = 2f\sqrt{D}$ (Minkowski bound for norms of lattice minima in $\mathcal{O}_f$).*
   - **c)** *$|N_{K|\mathbf{Q}}(\alpha)| = 1$, if and only if $\alpha \in E_{\mathcal{O}_f}$.*
2. *In the case of a field K of D–type II, $D \equiv 1 (\mathrm{mod}\, 4)$, and $\alpha \in \mathcal{O}_{K,f} = \mathbf{Z} \oplus \mathbf{Z}\frac{f}{2}(1 + \sqrt{D})$, we have additionally:*
   - **a)** *If α is primitive in $\mathcal{O}_{K,f}$ and $|N_{K|\mathbf{Q}}| < \frac{1}{2}f\sqrt{D}$, then $\alpha \in Min(\mathcal{O}_{K,f})$.*
   - **b)** *Conversely, if $\alpha \in Min(\mathcal{O}_{K,f})$, then α is primitive in $\mathcal{O}_{K,f}$ and $|N_{K|\mathbf{Q}}(\alpha)| < \sqrt{|discr(\mathcal{O}_{K,f})|} = f\sqrt{D}$ (Minkowski bound for norms of lattice minima in $\mathcal{O}_{K,f}$).*
   - **c)** *$|N_{K|\mathbf{Q}}(\alpha)| = 1$, if and only if $\alpha \in E_{\mathcal{O}_{K,f}}$.*

PROOF. First compare with Theorem 1.1,4, to see that the above enumeration of orders in K is exhaustive.

1.a) Assume $\alpha \in \mathcal{O}_f$, α primitive in $\mathcal{O}_f$ (hence $\alpha \neq 0$) and $|N_{K|\mathbf{Q}}(\alpha)| < f\delta$. If $\alpha \notin Min(\mathcal{O}_f)$, then $\exists \vartheta \in \mathcal{O}_f \quad 0 < |\vartheta| < |\alpha|$,

$|\vartheta'| < |\alpha'|$. For the number $\xi = |\vartheta| \cdot |\alpha'|$, which belongs to $\mathcal{O}_f$ (because, for $\alpha = u + vf\delta \in \mathcal{O}_f$ with $u, v \in \mathbf{Z}$, also $\alpha' = u - vf\delta \in \mathcal{O}_f$), the conjugates are bounded

$$0 < \xi = |N_{K\,|\,\mathbf{Q}}(\alpha)| \cdot |\vartheta| \,/\, |\alpha| < |N_{K\,|\,\mathbf{Q}}(\alpha)|,$$
$$|\xi'| = |N_{K\,|\,\mathbf{Q}}(\alpha)| \cdot |\vartheta'| \,/\, |\alpha'| < |N_{K\,|\,\mathbf{Q}}(\alpha)|.$$

According to Lemma 2.1, the coefficients $x, y \in \mathbf{Z}$ of $\xi = x + yf\delta$ can be estimated by $|x|, |yf\delta| < |N_{K\,|\,\mathbf{Q}}(\alpha)|$. Therefore immediately $|y| < |N_{K\,|\,\mathbf{Q}}|/f\delta < 1$ and, as $y \in \mathbf{Z}, y = 0$. Further $x = \xi = |\vartheta| \cdot |N_{K\,|\,\mathbf{Q}}(\alpha)|/|\alpha|$ or $x \cdot |\alpha| = |N_{K\,|\,\mathbf{Q}}(\alpha)| \cdot |\vartheta|$ with $|\vartheta| \in \mathcal{O}_f$, i.e., $x \cdot |\alpha| \in |N_{K\,|\,\mathbf{Q}}(\alpha)|\mathcal{O}_f$. From Lemma 2.2 we get $|N_{K\,|\,\mathbf{Q}}(\alpha)| \mid x$, because α is primitive in $\mathcal{O}_f$. But as $x = \xi < |N_{K\,|\,\mathbf{Q}}(\alpha)|$, this implies $x = 0$. Hence $\vartheta = 0$, in contradiction to $0 < |\vartheta|$. Thus we have shown, that α must be a lattice minimum in $\mathcal{O}_f$.

b) This is a special case of a general result for lattice minima α in orders $\mathcal{O}$ of algebraic number fields K with r_2 pairs of conjugate complex embeddings into $\mathbf{C}$: $|N_{K\,|\,\mathbf{Q}}(\alpha)| < (2/\pi)^{r_2} \cdot \sqrt{|\,discr(\mathcal{O})\,|}$. See J. BUCHMANN [6], 181–182. Here $r_2 = 0$ and $discr(\mathcal{O}_f) = 4f^2D$, according to Theorem 1.1, 4.

c) If $|N_{K\,|\,\mathbf{Q}}(\alpha)| = \pm\alpha\alpha' = 1$, then $\alpha^{-1} = \pm\alpha'$ and α' is an algebraic integer in $\mathcal{O}_f$ (compare **1.a**). Hence $\alpha \in E_{\mathcal{O}_f}$. Conversely for $\alpha \in E_{\mathcal{O}_f}$, first $N_{K\,|\,\mathbf{Q}}(\alpha)N_{K\,|\,\mathbf{Q}}(\alpha^{-1}) = N_{K\,|\,\mathbf{Q}}(\alpha \cdot \alpha^{-1}) = N_{K\,|\,\mathbf{Q}}(1) = 1$, and second $N_{K\,|\,\mathbf{Q}}(\alpha), N_{K\,|\,\mathbf{Q}}(\alpha^{-1}) \in \mathbf{Z}$, whence $|N_{K\,|\,\mathbf{Q}}(\alpha)| = 1$.

2.a) Let $\alpha \in \mathcal{O}_{K,f}, \alpha$ primitive in $\mathcal{O}_{K,f}$ (hence $\alpha \neq 0$) and $2|N_{K\,|\,\mathbf{Q}}(\alpha)| < f\delta$. Assume $\alpha \notin Min(\mathcal{O}_{K,f})$, then $\exists\vartheta \in \mathcal{O}_{K,f}\;\; 0 < |\vartheta| < |\alpha|, |\vartheta'| < |\alpha'|$. The number $\xi = |\vartheta| \cdot |\alpha'|$ is contained in $\mathcal{O}_{K,f}$, because if $\alpha = z + w\frac{f}{2}(1 + \delta) \in \mathcal{O}_{K,f}$ with $z, w \in \mathbf{Z}$, then α has yet another representation (which is not necessarily reduced) $\alpha = \frac{1}{2}(u + vf\delta)$ with $u = 2z + fw,\ v = w,\ u \equiv vf \equiv -vf \pmod 2$, and hence also $\alpha' = \frac{1}{2}(u - vf\delta) \in \mathcal{O}_{K,f}$. The conjugates of ξ are bounded by $|N_{K\,|\,\mathbf{Q}}(\alpha)|$, completely similar as in **1.a**. By Lemma 2.1, the coefficients $x/2,\ y/2$ of $\xi = \frac{1}{2}(x + yf\delta)$, where $x, y \in \mathbf{Z},\ x \equiv yf \pmod 2$, can be estimated by $|x/2|, |yf\delta/2| < |N_{K\,|\,\mathbf{Q}}(\alpha)|$. Therefore immediately $|y| < 2|N_{K\,|\,\mathbf{Q}}(\alpha)|/f\delta < 1$ and, as $y \in \mathbf{Z},\ y = 0$. Further $x/2 = \xi = |\vartheta| \cdot |N_{K\,|\,\mathbf{Q}}(\alpha)|/|\alpha| \in \mathbf{Q} \cap \mathcal{O}_{K,f} = \mathbf{Z}$, hence $2|x$ and $|\alpha| \cdot x/2 = |N_{K\,|\,\mathbf{Q}}(\alpha)| \cdot |\vartheta|$ with $|\vartheta| \in \mathcal{O}_{K,f}$, i.e., $|\alpha| \cdot x/2 \in |N_{K\,|\,\mathbf{Q}}(\alpha)|\mathcal{O}_{K,f}$. From Lemma 2.2 we get $|N_{K\,|\,\mathbf{Q}}(\alpha)| \mid (x/2)$, because α is primitive in $\mathcal{O}_{K,f}$. But as $x/2 = \xi < |N_{K\,|\,\mathbf{Q}}(\alpha)|$, this implies $x = 0$. Hence $\vartheta = 0$, in contradiction to $0 < |\vartheta|$. Now we have shown, that α must be a lattice minimum in $\mathcal{O}_{K,f}$.

b) Specialize $r_2 = 0$ and, by Theorem 1.1, 4, $discr(\mathcal{O}_{K,f}) = f^2 D$ in the general inequelity from **1.b**.

c) If $|N_{K\,|\,\mathbf{Q}}(\alpha)| = \pm\alpha\alpha' = 1$, then $\alpha^{-1} = \pm\alpha'$ and α' is an algebraic integer in $\mathcal{O}_{K,f}$ (compare **2.a**). Hence $\alpha \in E_{\mathcal{O}_{K,f}}$.

Conversely for $\alpha \in E_{\mathcal{O}_{K,f}}$ we have $N_{K\,|\,\mathbf{Q}}(\alpha)N_{K\,|\,\mathbf{Q}}(\alpha^{-1}) = 1$ and $N_{K\,|\,\mathbf{Q}}(\alpha)$, $N_{K\,|\,\mathbf{Q}}\ (\alpha^{-1}) \in \mathbf{Z}$, whence $|N_{K\,|\,\mathbf{Q}}(\alpha)| = 1$. □

§3. Minima and continued fractions

For the purpose of the analysis, which properties of a rather general type of lattices give rise to certain influences on the representation of minimal points, we devote this paragraph to the intimate relationship between lattice minima and convergents for ordinary (integer part) continued fraction expansions. Unfortunately these results do not appear in the literature. Only A. J. BRENTJES [4], chap. 1, 12–15, discusses shortly and without proofs the projective geometric interpretation of continued fraction expansions given by F. Klein, but the viewpoint is slightly different from the setting of lattice minima used in this paper, because Brentjes fixes the standard lattice $\mathbf{Z}^2$ and varies the slopes of the coordinate axes, whereas we choose the Cartesian standard axes and vary the lattices.

However, it should be pointed out again that the results concerning generators of ambiguous principal ideals in § 5 will be based on purely number geometric methods and do not depend on the machinery of continued fractions.

Lemma 3.1. (A representation of the total quotients in continued fraction expansions.)

Let $\xi \in \mathbf{R} \setminus \mathbf{Q}$ be an arbitrary irrational real number, $\xi = [a_0, a_1, \dots]$ its continued fraction expansion with total (or complete) quotients ξ_j $(j \geq 0)$, partial quotients a_j $(j \geq 0)$ and with numerators and denominators P_j, Q_j $(j \geq -2)$ of the convergents for this expansion. That is, $P_{-2} = 0$, $Q_{-2} = 1$, $P_{-1} = 1$, $Q_{-1} = 0$, $\xi_0 = \xi$ and $\xi_{j+1} = 1\ /\ (\xi_j - \lfloor \xi_j \rfloor)$, $a_j = \lfloor \xi_j \rfloor$, $P_j = a_j P_{j-1} + P_{j-2}$, $Q_j = a_j Q_{j-1} + Q_{j-2}$ for all $j \geq 0$. The total quotients have representations in the form

$$\xi_j = -\frac{P_{j-2} - Q_{j-2}\xi}{P_{j-1} - Q_{j-1}\xi} \quad \text{for all } j \geq 0.$$

PROOF. By induction with respect to $j \geq 0$. First, for $j = 0$ we have $(P_{-2} - Q_{-2}\xi)/(P_{-1} - Q_{-1}\xi) = (0 - 1 \cdot \xi)/(1 - 0 \cdot \xi) = -\xi = -\xi_0$. Now let $j \geq 0$ and assume $\xi_j = -(P_{j-2} - Q_{j-2}\xi)/(P_{j-1} - Q_{j-1}\xi)$. Then $(P_j - Q_j\xi)/(P_{j-1} - Q_{j-1}\xi) = ((a_j P_{j-1} + P_{j-2}) - (a_j Q_{j-1} + Q_{j-2})\xi)/(P_{j-1} - Q_{j-1}\xi) = (a_j(P_{j-1} - Q_{j-1}\xi) + (P_{j-2} - Q_{j-2}\xi))/(P_{j-1} - Q_{j-1}\xi) = a_j + (P_{j-2} - Q_{j-2}\xi)/(P_{j-1} - Q_{j-1}\xi) = a_j - \xi_j = \lfloor \xi_j \rfloor - \xi_j = -1/\xi_{j+1}$. □

Theorem 3.2. (The relations between lattice minima in a special type of two dimensional lattices and convergents for continued fraction expansions.)

Let $\xi_1, \xi_2 \in \mathbf{R} \setminus \mathbf{Q}$ be two irrational real numbers with the property that either $\xi_1 > 1,\ \xi_2 < 0$ or $\xi_1 > 0,\ \xi_2 < -1$. Further denote by $\Lambda = \mathbf{Z}\binom{1}{1} \oplus \mathbf{Z}\binom{\xi_1}{\xi_2}$ a special type of complete two dimensional lattices in $\mathbf{R}^2$.

1. *$\binom{1}{1}$ is lattice minimum in Λ.*
2. *If $P_j, Q_j \in \mathbf{N}_0$ $(j \geq -2)$ are the numerators and denominators of the convergents for the continued fraction expansion of $-\xi_2$ (> 0), then for all $j \geq 0$*

$$\begin{pmatrix} P_{j-1} + Q_{j-1}\xi_1 \\ P_{j-1} + Q_{j-1}\xi_2 \end{pmatrix} \in Min^+(\Lambda),\ \begin{pmatrix} P_j + Q_j\xi_1 \\ P_j + Q_j\xi_2 \end{pmatrix} = \nu_1 \begin{pmatrix} P_{j-1} + Q_{j-1}\xi_1 \\ P_{j-1} + Q_{j-1}\xi_2 \end{pmatrix}$$

and hence for all $j \geq 0$ the successive minima of the 1–chain in Λ are

$$\nu_1^j \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} P_{j-1} + Q_{j-1}\xi_1 \\ P_{j-1} + Q_{j-1}\xi_2 \end{pmatrix}.$$

3. *If $R_j, S_j \in \mathbf{N}_0$ $(j \geq -2)$ are the numerators and denominators of the convergents for the continued fraction expansion of ξ_1 (> 0), then for all $j \geq 0$*

$$(-1)^j \begin{pmatrix} R_{j-1} - S_{j-1}\xi_1 \\ R_{j-1} - S_{j-1}\xi_2 \end{pmatrix} \in Min^+(\Lambda),$$

$$(-1)^{j+1} \begin{pmatrix} R_j - S_j\xi_1 \\ R_j - S_j\xi_2 \end{pmatrix} = \nu_2 \left((-1)^j \begin{pmatrix} R_{j-1} - S_{j-1}\xi_1 \\ R_{j-1} - S_{j-1}\xi_2 \end{pmatrix} \right)$$

and hence for all $j \geq 0$ the successive minima of the 2–chain in Λ are

$$\nu_2^j \begin{pmatrix} 1 \\ 1 \end{pmatrix} = (-1)^j \begin{pmatrix} R_{j-1} - S_{j-1}\xi_1 \\ R_{j-1} - S_{j-1}\xi_2 \end{pmatrix}.$$

Remark. In particular, Theorem 3.2,2,3 characterizes the cases, where $\binom{\xi_1}{\xi_2} \in Min^+(\Lambda)$:

$$\begin{pmatrix} \xi_1 \\ \xi_2 \end{pmatrix} = \nu_1 \left(\begin{pmatrix} 1 \\ 1 \end{pmatrix} \right) \quad \Leftrightarrow \quad |\xi_2| < 1 < \xi_1, \text{ and } \begin{pmatrix} \xi_1 \\ \xi_2 \end{pmatrix} = \nu_2 \left(\begin{pmatrix} 1 \\ 1 \end{pmatrix} \right)$$

$$\Leftrightarrow \xi_1 < 1 < |\xi_2|\,.$$

Further, a repeated application of Lemma 3.1 yields a representation of the 1–st coordinate of the minima in the 2–chain by means of total quotients of ξ_1,

$$(-1)^j(R_{j-1} - S_{j-1}\xi_1) = (\Pi_{k=1}^{j}(\xi_1)_k)^{-1} \qquad (j \geq 0),$$

and of the 2–st coordinate of the minima in the 1–chain by means of total quotients of $-\xi_2$,

$$P_{j-1} + Q_{j-1}\xi_2 = (-1)^j(\Pi_{k=1}^{j}(-\xi_2)_k)^{-1} \qquad (j \geq 0).$$

PROOF. We set $\mathbf{1} = \binom{1}{1}$ and $\Xi = \binom{\xi_1}{\xi_2}$ for abbreviation. For the proof of **1.** and **2.**, i.e., the construction of the 1–chain of minima in Λ, we use induction with respect to $j \geq 0$.

For the induction start let $j = 0$. Then $P_{j-1} = P_{-1} = 1$ and $Q_{j-1} = Q_{-1} = 0$. We show that $P_{-1}\mathbf{1} + Q_{-1}\Xi = \mathbf{1} \in Min^{+}(\Lambda)$, because $int(R(\mathbf{1})) \cap \Lambda = \{0\}$: for a lattice point $\mathbf{x} = a\mathbf{1} + b\Xi \in \Lambda$ with $a, b \in \mathbf{Z}$ we have the following disjoint distinction of cases

a) in case $b = 0 : x_1 = x_2 = a$ and hence $0 \leq x_1 \leq 1, |x_2| \leq 1 \Leftrightarrow 0 \leq a \leq 1 \Leftrightarrow a \in \{0, 1\}$, corresponding to $\mathbf{0}, \mathbf{1} \in R(\mathbf{1}) \cap \Lambda$,

b) in case $|b| \geq 1$, $sgn(a) = sgn(b)$ (and hence $a \neq 0$) : $|x_1| = |a + b\xi_1| = |sgn(a) \cdot (|a| + |b|\xi_1)| = |a| + |b|\xi_1 \geq 1 + |b|\xi_1 > 1$ and therefore $\mathbf{x} \notin R(\mathbf{1})$,

c) in case $|b| \geq 1$, $sgn(a) = -sgn(b)$ (and hence $a \neq 0$) : $|x_2| = |a + b\xi_2| = |sgn(a) \cdot (|a| - |b|\xi_2)| = |a| + |b| \cdot |\xi_2| \geq 1 + |b| \cdot |\xi_2| > 1$ and therefore $\mathbf{x} \notin R(\mathbf{1})$,

d) in case $|b| \geq 1$, $a = 0$: for the variant $\xi_1 > 1$, $\xi_2 < 0$: $|x_1| = |b\xi_1| = |b|\xi_1 \geq \xi_1 > 1$, and for the variant $\xi_1 > 0$, $\xi_2 < -1$: $|x_2| = |b\xi_2| = |b| \cdot |\xi_2| \geq |\xi_2| > 1$, and thus $\mathbf{x} \notin R(\mathbf{1})$ for both variants.

Together we infer $\mathbf{x} \in R(\mathbf{1}) \Leftrightarrow \mathbf{x} \in \{\mathbf{0}, \mathbf{1}\}$.

It remains to show $P_0\mathbf{1} + Q_0\Xi = \nu_1(P_{-1}\mathbf{1} + Q_{-1}\Xi) = \nu_1(\mathbf{1})$ for the induction start $j = 0$. For this purpose we prove $P_0\mathbf{1} + Q_0\Xi \in S_1(\mathbf{1})$ and $int(R(\mathbf{1}, P_0\mathbf{1} + Q_0\Xi)) \cap \Lambda = \{\mathbf{0}\}$.

First note that the lattice points of Λ in the 1–strip $S_1(\mathbf{1})$ (but not the whole 1–strip, iff $|\xi_2| < \xi_1$) are totally contained in the sector of convex, i.e., non–negative, $\mathbf{R}$–linear combinations $a\mathbf{1} + b\Xi$ with $a, b \in \mathbf{R}_0^{+}$ of the initial lattice basis $(\mathbf{1}, \Xi) = (P_{-1}\mathbf{1} + Q_{-1}\Xi, P_{-2}\mathbf{1} + Q_{-2}\Xi)$: for a lattice point $\mathbf{x} = a\mathbf{1} + b\Xi \in \Lambda$ with $a, b \in \mathbf{Z}$ in the exterior of this sector, that is, with at least one negative coefficient, we have

a) in case $a \geq 1$, $b \leq 0 : |x_2| = |a + b\xi_2| = |a - |b|\xi_2| = a + |b| \cdot |\xi_2| \geq a \geq 1$ and therefore $\mathbf{x} \notin S_1(\mathbf{1})$,

b) in case $a < 1$, $b \leq 0 : x_1 = a + b\xi_1 = a - |b|\xi_1 \leq a < 1$ and hence $\mathbf{x} \notin S_1(\mathbf{1})$,

c) in case $a \le -1,\ b > 0 : |\,x_2\,| = |\,a + b\xi_2\,| = \big| - |\,a\,| - b\,|\,\xi_2\,|\,\big| = |\,a\,| + b\,|\,\xi_2\,| \ge 1 + b\,|\,\xi_2\,| > 1$ and thus $\mathbf{x} \notin S_1(\mathbf{1})$.

The case $a \le -1,\ b \le 0$ is already contained in case b) and together we see that

$$S_1(\mathbf{1}) \cap \Lambda \subset \mathbf{N}_0\mathbf{1} + \mathbf{N}\Xi \subset \mathbf{R}_0^+\mathbf{1} + \mathbf{R}^+\Xi.$$

Next a non–negative $\mathbf{R}$–linear combination $\mathbf{x} = a\mathbf{1} + b\Xi$ with $a \in \mathbf{R}_0^+, b \in \mathbf{R}^+$ of this initial lattice basis is contained in $S_1(\mathbf{1}) \cap \Lambda$, iff

$$\begin{gathered} x_1 = a + b\xi_1 > 1, \\ |\,x_2\,| = |\,a + b\xi_2\,| < 1, \\ \text{and } a \in \mathbf{N}_0,\ b \in \mathbf{N}. \end{gathered}$$

The second condition is equivalent with $|\,a - b(-\xi_2)\,| < 1$ respectively $|\,a - b\xi_0\,| < 1$, where $\xi_0 = -\xi_2$ is the 0–th total quotient in the continued fraction expansion of $-\xi_2$. (We use the notation of Lemma 3.1.) As $b\xi_0 \in \mathbf{R}\setminus\mathbf{Q}$ and $b\xi_0 > 0$, there are exactly two non–negative integers $a \in \mathbf{N}_0$ with the property $|\,a - b\xi_0\,| < 1$, namely $a = \lfloor b\xi_0 \rfloor$ and $a = \lfloor b\xi_0 \rfloor + 1$. But for the 1–st coordinate we have on the one hand $\lfloor b\xi_0 \rfloor + b\xi_1 < \lfloor b\xi_0 \rfloor + 1 + b\xi_1$ and on the other hand for $b \ge 2$ $\lfloor \xi_0 \rfloor < \xi_0,\ b\lfloor \xi_0 \rfloor < b\xi_0, \lfloor \xi_0 \rfloor < 2\lfloor \xi_0 \rfloor \le b\lfloor \xi_0 \rfloor \le \lfloor b\xi_0 \rfloor$ and therefore $\lfloor \xi_0 \rfloor + \xi_1 < \lfloor b\xi_0 \rfloor + b\xi_1$. Hence for the choice of the coefficients a, b of the 1–neighbour $\mathbf{x} = a\mathbf{1} + b\Xi \in \Lambda$ of the lattice minimum $\mathbf{1} = P_{-1}\mathbf{1} + Q_{-1}\Xi \in Min(\Lambda)$ there only remains the unique possibility $b = 1,\ a = \lfloor b\xi_0 \rfloor = \lfloor \xi_0 \rfloor = a_0$. For this choice the last inequalities for the 1–st coordinate show $(R(\mathbf{1}, \mathbf{x}) \setminus R(\mathbf{1})) \cap \Lambda = \{\mathbf{x}\}$, whence $int(R(\mathbf{1}, \mathbf{x})) \cap \Lambda = \{\mathbf{0}\}$ and

$$\begin{aligned} \nu_1(\mathbf{1}) = \mathbf{x} = a_0\mathbf{1} + \Xi &= a_0(P_{-1}\mathbf{1} + Q_{-1}\Xi) + (P_{-2}\mathbf{1} + Q_{-2}\Xi) \\ &= (a_0P_{-1} + P_{-2})\mathbf{1} + (a_0Q_{-1} + Q_{-2})\Xi = P_0\mathbf{1} + Q_0\Xi. \end{aligned}$$

The first condition is satisfied too, because for the variant $\xi_1 > 1, \xi_2 < 0 :$ $x_1 = a + b\xi_1 = a_0 + \xi_1 \ge \xi_1 > 1$, and for the variant $\xi_1 > 0,\ \xi_2 < -1 :$ $a_0 = \lfloor \xi_0 \rfloor \,(= \lfloor -\xi_2 \rfloor) \ge 1$ and hence $x_1 = a + b\xi_1 = a_0 + \xi_1 > a_0 \ge 1$.

Now we assume the induction hypothesis $j \ge 1,\ P_{j-2}\mathbf{1} + Q_{j-2}\Xi \in Min^+(\Lambda),\ P_{j-1}\mathbf{1} + Q_{j-1}\Xi = \nu_1(P_{j-2}\mathbf{1} + Q_{j-2}\Xi)$ and $\nu_1^j(\mathbf{1}) = P_{j-1}\mathbf{1} + Q_{j-1}\Xi$.

For the induction step we show $P_{j-1}\mathbf{1} + Q_{j-1}\Xi \in Min^+(\Lambda)$, $P_j\mathbf{1} + Q_j\Xi = \nu_1(P_{j-1})\mathbf{1} + Q_{j-1}\Xi)$ and $\nu_1^{j+1}(\mathbf{1}) = P_j\mathbf{1} + Q_j\Xi$. From the hypothesis $P_{j-1}\mathbf{1} + Q_{j-1}\Xi = \nu_1(P_{j-2}\mathbf{1} + Q_{j-2}\Xi)$ we get $P_{j-1}\mathbf{1} + Q_{j-1}\Xi \in S_1(P_{j-2}\mathbf{1} + Q_{j-2}\Xi)$ and $int(R(P_{j-1}\mathbf{1} + Q_{j-1}\Xi, P_{j-2}\mathbf{1} + Q_{j-2}\Xi)) \cap \Lambda = \{\mathbf{0}\}$. The second condition implies $int(R(P_{j-1}\mathbf{1} + Q_{j-1}\Xi)) \cap \Lambda = \{\mathbf{0}\}$ i.e., $P_{j-1}\mathbf{1} + Q_{j-1}\Xi \in Min^+(\Lambda)$, as desired. The first condition comprises the following relations: $P_{j-1} + Q_{j-1}\xi_1 > P_{j-2} + Q_{j-2}\xi_1\ (> 0)$,

$|P_{j-1} + Q_{j-1}\xi_2| < |P_{j-2} + Q_{j-2}\xi_2|$. Further, as $P_{j-1} + Q_{j-1}\xi_2 = P_{j-1} - Q_{j-1}(-\xi_2)$ and P_{j-1}, Q_{j-1} are the numerator and denominator of a convergent for the continued fraction expansion of $-\xi_2$, the sign satisfies the rule $sgn(P_{j-1} + Q_{j-1}\xi_2) = (-1)^j$, according to O. PERRON [25], § 6, formula 1, pag. 14. We must look for the 1–neighbour of $P_{j-1}\mathbf{1} + Q_{j-1}\Xi$ in $S_1(P_{j-1}\mathbf{1} + Q_{j-1}\Xi)$, taking into consideration that the whole 1–strip of $P_{j-1}\mathbf{1} + Q_{j-1}\Xi$ (not only the lattice points in it, as for the induction start) is totally contained within the interior of the sector of convex $\mathbf{R}$–linear combinations $a(P_{j-1}\mathbf{1} + Q_{j-1}\Xi) + b(P_{j-2}\mathbf{1} + Q_{j-2}\Xi)$ with $a, b \in \mathbf{R}^+$ of the lattice basis $(P_{j-1}\mathbf{1} + Q_{j-1}\Xi, P_{j-2}\mathbf{1} + Q_{j-2}\Xi)$, which arises from the initial basis $(\mathbf{1}, \Xi) = (P_{-1}\mathbf{1} + Q_{-1}\Xi, P_{-2}\mathbf{1} + Q_{-2}\Xi)$ by an application of the unimodular transformation

$$\begin{pmatrix} P_{j-1} & Q_{j-1} \\ P_{j-2} & Q_{j-2} \end{pmatrix} \in GL_2(\mathbf{Z})$$

with determinant $P_{j-1}Q_{j-2} - P_{j-2}Q_{j-1} = (-1)^j$ (see [25], § 13, pag. 36): for an arbitrary point $\mathbf{x} = a(P_{j-1}\mathbf{1} + Q_{j-1}\Xi) + b(P_{j-2}\mathbf{1} + Q_{j-2}\Xi)$ with $a, b \in \mathbf{R}$ in the exterior of this sector, that is, with at least one negative coefficient, we have

a) in case $a \geq 1,\ b \leq 0 : sgn(P_{j-1} + Q_{j-1}\xi_2) = -sgn(P_{j-2} + Q_{j-2}\xi_2)$, $|x_2| = |a(P_{j-1} + Q_{j-1}\xi_2) + b(P_{j-2} + Q_{j-2}\xi_2)| = |a(P_{j-1} + Q_{j-1}\xi_2) - |b|(P_{j-2} + Q_{j-2}\xi_2)| = a|P_{j-1} + Q_{j-1}\xi_2| + |b| \cdot |P_{j-2} + Q_{j-2}\xi_2| \geq a|P_{j-1} + Q_{j-1}\xi_2| \geq |P_{j-1} + Q_{j-1}\xi_2|$ and therefore $\mathbf{x} \notin S_1(P_{j-1}\mathbf{1} + Q_{j-1}\Xi)$,

b) in case $a < 1,\ b \leq 0 : P_{j-1} + Q_{j-1}\xi_1 > 0,\ P_{j-2} + Q_{j-2}\xi_1 > 0,\ x_1 = a(P_{j-1} + Q_{j-1}\xi_1) + b(P_{j-2} + Q_{j-2}\xi_1) = a(P_{j-1} + Q_{j-1}\xi_1) - |b|(P_{j-2} + Q_{j-2}\xi_1) \leq a(P_{j-1} + Q_{j-1}\xi_1) < P_{j-1} + Q_{j-1}\xi_1$ and hence $\mathbf{x} \notin S_1(P_{j-1}\mathbf{1} + Q_{j-1}\Xi)$,

c) in case $a \leq 0, b \geq 1 : sgn(P_{j-1} + Q_{j-1}\xi_2) = -sgn(P_{j-2} + Q_{j-2}\xi_2)$, $|P_{j-1} + Q_{j-1}\xi_2| < |P_{j-2} + Q_{j-2}\xi_2|$, $|x_2| = |a(P_{j-1} + Q_{j-1}\xi_2) + b(P_{j-2} + Q_{j-2}\xi_2)| = \big| -|a|(P_{j-1} + Q_{j-1}\xi_2) + b(P_{j-2} + Q_{j-2}\xi_2)\big| = |a| \cdot |P_{j-1} + Q_{j-1}\xi_2| + b|P_{j-2} + Q_{j-2}\xi_2| \geq b|P_{j-2} + Q_{j-2}\xi_2| \geq |P_{j-2} + Q_{j-2}\xi_2| > |P_{j-1} + Q_{j-1}\xi_2|$, whence $\mathbf{x} \notin S_1(P_{j-1}\mathbf{1} + Q_{j-1}\Xi)$,

d) in case $a \leq 0,\ b < 1 : P_{j-1} + Q_{j-1}\xi_1 > P_{j-2} + Q_{j-2}\xi_1 > 0,\ x_1 = a(P_{j-1} + Q_{j-1}\xi_1) + b(P_{j-2} + Q_{j-2}\xi_1) = -|a|(P_{j-1} + Q_{j-1}\xi_1) + b(P_{j-2} + Q_{j-2}\xi_1) \leq b(P_{j-2} + Q_{j-2}\xi_1) < P_{j-2} + Q_{j-2}\xi_1 < P_{j-1} + Q_{j-1}\xi_1$ and thus $\mathbf{x} \notin S_1(P_{j-1}\mathbf{1} + Q_{j-1}\Xi)$.

Together we infer $S_1(P_{j-1}\mathbf{1} + Q_{j-1}\Xi) \subset \mathbf{R}^+(P_{j-1}\mathbf{1} + Q_{j-1}\Xi) + \mathbf{R}^+(P_{j-2}\mathbf{1} + Q_{j-2}\Xi)$. Next a positive $\mathbf{R}$–linear combination $\mathbf{x} = a(P_{j-1}\mathbf{1} + Q_{j-1}\Xi) + b(P_{j-2}\mathbf{1} + Q_{j-2}\Xi)$ with $a, b \in \mathbf{R}^+$ of this lattice basis is contained in

$S_1(P_{j-1}\mathbf{1} + Q_{j-1}\Xi) \cap \Lambda$, iff

$$\begin{aligned} x_1 =& a(P_{j-1} + Q_{j-1}\xi_1) + b(P_{j-2} + Q_{j-2}\xi_1) > P_{j-1} + Q_{j-1}\xi_1, \\ |\, x_2 \,| =& |\, a(P_{j-1} + Q_{j-1}\xi_2) + b(P_{j-2} + Q_{j-2}\xi_2) \,| < |\, P_{j-1} + Q_{j-1}\xi_2 \,|, \\ & \text{and } a, b \in \mathbf{N}, \end{aligned}$$

where the first condition is implied by the last one : $a \geq 1 \Rightarrow x_1 = a(P_{j-1}+Q_{j-1}\xi_1)+b(P_{j-2}+Q_{j-2}\xi_1) > a(P_{j-1}+Q_{j-1}\xi_1) \geq P_{j-1}+Q_{j-1}\xi_1$, because $P_{j-1} + Q_{j-1}\xi_1 > 0$, $P_{j-2} + Q_{j-2}\xi_1 > 0$. The second condition is crucial and equivalent with $-\,|\, P_{j-1} + Q_{j-1}\xi_2 \,| < a(P_{j-1} + Q_{j-1}\xi_2) + b(P_{j-2} + Q_{j-2}\xi_2) < |\, P_{j-1} + Q_{j-1}\xi_2 \,|$ respectively

$$-1 < a + b\frac{P_{j-2} + Q_{j-2}\xi_2}{P_{j-1} + Q_{j-1}\xi_2} < 1$$

independently of the sign $sgn(P_{j-1} + Q_{j-1}\xi_2)$. Now, according to Lemma 3.1,

$$\frac{P_{j-2} + Q_{j-2}\xi_2}{P_{j-1} + Q_{j-1}\xi_2} = \frac{P_{j-2} - Q_{j-2}(-\xi_2)}{P_{j-1} - Q_{j-1}(-\xi_2)} = -\xi_j,$$

where ξ_j is the j–th total quotient in the continued fraction expansion of $-\xi_2$. There are exactly two positive integers $a \in \mathbf{N}$ with the property $-1 < a - b\xi_j < 1$ respectively $|\, a - b\xi_j \,| < 1$, because $b\xi_j \in \mathbf{R} \setminus \mathbf{Q}$ and $b\xi_j > 1$. These integers are $a = \lfloor b\xi_j \rfloor$ and $a = \lfloor b\xi_j \rfloor + 1$. But for the 1–st coordinate we have on the one hand $\lfloor b\xi_j \rfloor (P_{j-1} + Q_{j-1}\xi_1) + b(P_{j-2} + Q_{j-2}\xi_1) < (1 + \lfloor b\xi_j \rfloor)(P_{j-1} + Q_{j-1}\xi_1) + b(P_{j-2} + Q_{j-2}\xi_1)$ and on the other hand for $b \geq 2 \quad \lfloor \xi_j \rfloor < \xi_j,\ b\lfloor \xi_j \rfloor < b\xi_j,\ \lfloor \xi_j \rfloor < 2\lfloor \xi_j \rfloor \leq b\lfloor \xi_j \rfloor \leq \lfloor b\xi_j \rfloor$ and therefore $\lfloor \xi_j \rfloor (P_{j-1}+Q_{j-1}\xi_1)+(P_{j-2}+Q_{j-2}\xi_1) < \lfloor b\xi_j \rfloor (P_{j-1}+Q_{j-1}\xi_1)+b(P_{j-2}+Q_{j-2}\xi_1)$. Hence for the choice of the coefficients a, b of the 1–neighbour $\mathbf{x} = a(P_{j-1}\mathbf{1} + Q_{j-1}\Xi) + b(P_{j-2}\mathbf{1} + Q_{j-2}\Xi) \in \Lambda$ of the lattice minimum $P_{j-1}\mathbf{1} + Q_{j-1}\Xi \in Min^+(\Lambda)$ there only remains the unique possibility $b = 1,\ a = \lfloor b\xi_j \rfloor = \lfloor \xi_j \rfloor = a_j$. For this choice the last inequalities for the 1–st coordinate show $(R(P_{j-1}\mathbf{1} + Q_{j-1}\Xi, \mathbf{x}) \setminus\ R(P_{j-1}\mathbf{1} + Q_{j-1}\Xi)) \cap \Lambda = \{\mathbf{x}\}$, $int(R(P_{j-1}\mathbf{1} + Q_{j-1}\Xi, \mathbf{x})) \cap \Lambda = \{\mathbf{0}\}$ and hence

$$\begin{aligned} \nu_1(P_{j-1}\mathbf{1} + Q_{j-1}\Xi) &= \mathbf{x} = a_j(P_{j-1}\mathbf{1} + Q_{j-1}\Xi) + (P_{j-2}\mathbf{1} + Q_{j-2}\Xi) \\ &= (a_jP_{j-1} + P_{j-2})\mathbf{1} + (a_jQ_{j-1} + Q_{j-2})\Xi = P_j\mathbf{1} + Q_j\Xi. \end{aligned}$$

Finally $\nu_1^{j+1}(\mathbf{1}) = \nu_1(\nu_1^j(\mathbf{1})) = \nu_1(P_{j-1}\mathbf{1} + Q_{j-1}\Xi) = P_j\mathbf{1} + Q_j\Xi$, completing the induction.

The proof of **3.**, i.e., the construction of the 2–chain of minima in Λ, is rather simple now, because we must only apply the results in **2.** for an auxiliary lattice

$$\Lambda' = \mathbf{Z}\begin{pmatrix}1\\1\end{pmatrix} \oplus \mathbf{Z}\begin{pmatrix}-\xi_2\\-\xi_1\end{pmatrix}$$

satisfying the same conditions as the lattice Λ. For the variant $\xi_1 > 1$, $\xi_2 < 0 : -\xi_2 > 0,\ -\xi_1 < -1$ and for the variant $\xi_1 > 0,\ \xi_2 < -1 :\ -\xi_2 > 1,\ -\xi_1 < 0$. According to **2.**, we know the 1–chain in the lattice Λ':

$$\binom{R_{j-1}-S_{j-1}\xi_2}{R_{j-1}-S_{j-1}\xi_1} = \binom{R_{j-1}+S_{j-1}(-\xi_2)}{R_{j-1}+S_{j-1}(-\xi_1)} \in Min^+(\Lambda'),$$

$$\nu_1'\binom{R_{j-1}-S_{j-1}\xi_2}{R_{j-1}-S_{j-1}\xi_1} = \nu_1'\binom{R_{j-1}+S_{j-1}(-\xi_2)}{R_{j-1}+S_{j-1}(-\xi_1)} = \binom{R_j+S_j(-\xi_2)}{R_j+S_j(-\xi_1)} = \binom{R_j-S_j\xi_2}{R_j-S_j\xi_1} \text{ and}$$

$$\nu_1'^j(\mathbf{1}) = \binom{R_{j-1}+S_{j-1}(-\xi_2)}{R_{j-1}+S_{j-1}(-\xi_1)} = \binom{R_{j-1}-S_{j-1}\xi_2}{R_{j-1}-S_{j-1}\xi_1} \text{ for all } j \geq 0.$$

Now $\Lambda' = \mathbf{Z}\binom{1}{1} \oplus \mathbf{Z}\binom{-\xi_2}{-\xi_1} = \mathbf{Z}\binom{1}{1} \oplus \binom{\xi_2}{\xi_1}$ can also be viewed as the lattice Λ with twisted coordinates, and hence, twisting the coordinates and taking into consideration that the signs must be chosen so that neighbours are in the right half plane, we obtain the 2–chain in the lattice Λ:

$$(-1)^j\binom{R_{j-1}-S_{j-1}\xi_1}{R_{j-1}-S_{j-1}\xi_2} \in Min^+(\Lambda),$$

$$\nu_2\left((-1)^j\binom{R_{j-1}-S_{j-1}\xi_1}{R_{j-1}-S_{j-1}\xi_2}\right) = (-1)^{j+1}\binom{R_j-S_j\xi_1}{R_j-S_j\xi_2} \text{ and}$$

$$\nu_2^j(\mathbf{1}) = (-1)^j\binom{R_{j-1}-S_{j-1}\xi_1}{R_{j-1}-S_{j-1}\xi_2} \text{ for all } j \geq 0. \quad \square$$

Corollary 3.3. (The representation of minimal points in symmetric lattices.)

Under the hypotheses of Theorem 3.2, and with the additional assumption that $\xi_1 + \xi_2 = f$ for some integer $f \in \mathbf{Z}$, the lattice Λ coincides with the twisted lattice $\Lambda' = \mathbf{Z}\binom{1}{1} \oplus \mathbf{Z}\binom{\xi_2}{\xi_1}$, that is, Λ is symmetric with respect to the line $x_2 = x_1$, and the minimal points of Λ have yet another representation:

$$\nu_1^j\begin{pmatrix}1\\1\end{pmatrix} = \begin{pmatrix}R_{j-1}-S_{j-1}\xi_2\\R_{j-1}-S_{j-1}\xi_1\end{pmatrix},$$

$$\nu_2^j\begin{pmatrix}1\\1\end{pmatrix} = (-1)^j\begin{pmatrix}P_{j-1}+Q_{j-1}\xi_2\\P_{j-1}+Q_{j-1}\xi_1\end{pmatrix} \textit{ for all } j \geq 0.$$

As an additional result the denominators and numerators of the convergents are connected by the relations $S_j = Q_j,\ R_j = P_j + f \cdot Q_j$ for all $j \geq 0$.

PROOF. If $f \in \mathbf{Z}$, then the unimodular transformation

$$\begin{pmatrix} 1 & 0 \\ f & -1 \end{pmatrix} \in GL_2(\mathbf{Z})$$

has the determinant -1 (and is therefore orientation reversing). We obtain another lattice basis $\left(\binom{1}{1}, \binom{f-\xi_1}{f-\xi_2}\right)$ of Λ, applying this matrix to the basis $\left(\binom{1}{1}, \binom{\xi_1}{\xi_2}\right)$. Now we can derive $\Lambda = \mathbf{Z}\binom{1}{1} \oplus \mathbf{Z}\binom{\xi_1}{\xi_2} = \mathbf{Z}\binom{1}{1} \oplus \mathbf{Z}\binom{f-\xi_1}{f-\xi_2} = \mathbf{Z}\binom{1}{1} \oplus \mathbf{Z}\binom{\xi_2}{\xi_1} = \Lambda'$ from $\xi_1 + \xi_2 + f$, that is, both lattices coincide. Thus, as $\Lambda' = \mathbf{Z}\binom{1}{1} \oplus \mathbf{Z}\binom{-\xi_2}{-\xi_1}$, we have for all $j \geq 0$,

$$\nu_1^j \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \nu_1'^j \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} R_{j-1} + S_{j-1}(-\xi_2) \\ R_{j-1} + S_{j-1}(-\xi_1) \end{pmatrix} = \begin{pmatrix} R_{j-1} - S_{j-1}\xi_2 \\ R_{j-1} - S_{j-1}\xi_1 \end{pmatrix}$$

and on the other hand, by an application of the twisting trick in the proof of Theorem 3.2,3

$$\nu_1'^j \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \nu_1^j \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} P_{j-1} + Q_{j-1}\xi_1 \\ P_{j-1} + Q_{j-1}\xi_2 \end{pmatrix}, \text{ whence}$$
$$\nu_2^j \begin{pmatrix} 1 \\ 1 \end{pmatrix} = (-1)^j \begin{pmatrix} P_{j-1} + Q_{j-1}\xi_2 \\ P_{j-1} + Q_{j-1}\xi_1 \end{pmatrix}.$$

Using the $\mathbf{Q}$–linear independence of $(1, \xi_1)$ a comparison of the two representations yields $P_{j-1} + Q_{j-1}\xi_1 = R_{j-1} - S_{j-1}\xi_2 = R_{j-1} - S_{j-1}(f - \xi_1)$ and hence $P_{j-1} = R_{j-1} - f \cdot S_{j-1}$, $Q_{j-1} = S_{j-1}$ for all $j \geq 0$. □

Of course, our main goal is the application of Theorem 3.2 and Corollary 3.3 to the Minkowski image of orders in real quadratic number fields, but nevertheless it was illuminating to see the general background of this application in a fairly broad class of lattices.

Corollary 3.4. (The connection between the lattice minima in arbitrary orders of real quadratic number fields and the convergents for continued fraction expansions of certain quadratic irrationalities.)

Let $D \in \mathbf{N}$, $D \geq 2$ be a squarefree radicand and K the real quadratic number field $\mathbf{Q}(\sqrt{D})$.

1. *In the case of a D–type I field, $D \equiv 2, 3 (\mathrm{mod}\, 4)$, $\mathcal{O} = \mathbf{Z} \oplus \mathbf{Z}\sqrt{D}$ is the maximal order in K. For every $f \in \mathbf{N}$ let $\mathcal{O}_f = \mathbf{Z} \oplus \mathbf{Z}f\sqrt{D}$ be the suborder with conductor $cond(\mathcal{O}_f) = f\mathcal{O}$ in the maximal order $\mathcal{O} = \mathcal{O}_1$. Further assume that $P_j, Q_j \in \mathbf{N}_0$ (with $j \geq -2$) are the*

numerators and denominators of the convergents for the continued fraction expansion of $\xi = \sqrt{f^2D}$. Then

$$Min(\mathcal{O}_f) = \{\pm\nu_1^j(1) \mid j \in \mathbf{N}_0\} \cup \{\pm\nu_2^j(1) \mid j \in \mathbf{N}_0\},$$

where for all $j \geq 0$

$$\nu_1^j(1) = P_{j-1} + Q_{j-1}f\sqrt{D} = (-1)^j \cdot N_{K\mid\mathbf{Q}}(\nu_1^j(1)) \cdot \prod_{k=1}^{j} \xi_k,$$

$$\nu_2^j(1) = (-1)^j(P_{j-1} - Q_{j-1}f\sqrt{D}) = \left(\prod_{k=1}^{j} \xi_k\right)^{-1}.$$

2. *In the case of a D–type II field, $D \equiv 1 (\operatorname{mod} 4)$, the maximal order in K is $\mathcal{O}_K = \mathbf{Z} \oplus \mathbf{Z}\frac{1}{2}(1+\sqrt{D})$. For every $f \in \mathbf{N}$ denote by $\mathcal{O}_{K,f} = \mathbf{Z} \oplus \mathbf{Z}\frac{f}{2}(1+\sqrt{D})$ the suborder with conductor $cond(\mathcal{O}_{K,f}) = f\mathcal{O}_K$ in the maximal order $\mathcal{O}_K = \mathcal{O}_{K,1}$. Further suppose that $P_j, Q_j \in \mathbf{N}_0$ (with $j \geq -2$) are the numerators and denominators of the convergents for the continued fraction expansion of $-\xi_2 = \frac{1}{2}(-f + \sqrt{f^2D}) = -\tau\left(\frac{1}{2}(f + \sqrt{f^2D})\right)$, and $R_j, S_j \in \mathbf{N}_0$ (with $j \geq -2$) are those of $\xi_1 = \frac{1}{2}(f + \sqrt{f^2D})$. Then*

$$Min(\mathcal{O}_{K,f}) = \{\pm\nu_1^j(1) \mid j \in \mathbf{N}_0\} \cup \{\pm\nu_2^j(1) \mid j \in \mathbf{N}_0\},$$

where for all $j \geq 0$ the denominators and numerators are connected by $S_{j-1} = Q_{j-1}$, $R_{j-1} = P_{j-1} + f \cdot Q_{j-1}$ and

$$\begin{aligned}\nu_1^j(1) &= P_{j-1} + Q_{j-1}\frac{f}{2}(1+\sqrt{D}) = (-1)^j \cdot N_{K\mid\mathbf{Q}}(\nu_1^j(1)) \cdot \prod_{k=1}^{j}(-\xi_2)_k \\ &= R_{j-1} + S_{j-1}\frac{f}{2}(-1+\sqrt{D}) = (-1)^j \cdot N_{K\mid\mathbf{Q}}(\nu_1^j(1)) \cdot \prod_{k=1}^{j}(\xi_1)_k,\end{aligned}$$

$$\begin{aligned}\nu_2^j(1) &= (-1)^j(R_{j-1} - S_{j-1}\frac{f}{2}(1+\sqrt{D})) = \left(\prod_{k=1}^{j}(\xi_1)_k\right)^{-1} \\ &= (-1)^j(P_{j-1} - Q_{j-1}\frac{f}{2}(-1+\sqrt{D})) = \left(\prod_{k=1}^{j}(-\xi_2)_k\right)^{-1}.\end{aligned}$$

PROOF. Every order $\mathcal{O}$ in a (real or complex) quadratic field K is of one of the aforementioned types with the conductors $f\mathcal{O}_K,\ f \in \mathbf{N}$, by Theorem 1.1,4. But for the consideration of lattice minima only the case of a real quadratic field is of interest.

1. First $Min(\mathcal{O}_f) = \psi^{-1}(Min(\psi(\mathcal{O}_f)))$ and $\psi(\mathcal{O}_f) = \mathbf{Z}\binom{1}{1} \oplus \mathbf{Z}\binom{\xi_1}{\xi_2}$ with quadratic irrationalities satisfying the necessary conditions, that is $\xi_1 = \sqrt{f^2D} = f\sqrt{D} \geq 1 \cdot \sqrt{2} > 1,\ \xi_2 = -\sqrt{f^2D} = -f\sqrt{D} \leq -1 \cdot \sqrt{2} < -1 < 0$. Hence, according to Theorem 3.2 and as $\xi_1 = -\xi_2$ and therefore $R_{j-1} = P_{j-1},\ S_{j-1} = Q_{j-1} : \nu_1^j(1) = \psi^{-1}(\nu_1^j\binom{1}{1}) = \psi^{-1}\binom{P_{j-1}+Q_{j-1}\xi_1}{P_{j-1}+Q_{j-1}\xi_2} = P_{j-1} + Q_{j-1}\xi_1 = P_{j-1} + Q_{j-1}f\sqrt{D},\ \nu_2^j(1) = \psi^{-1}(\nu_2^j\binom{1}{1}) = \psi^{-1}\left((-1)^j\binom{P_{j-1}-Q_{j-1}\xi_1}{P_{j-1}-Q_{j-1}\xi_2}\right) = (-1)^j(P_{j-1} - Q_{j-1}\xi_1) = (-1)^j(P_{j-1} - Q_{j-1}f\sqrt{D})$ for all $j \geq 0$.

2. Again $Min(\mathcal{O}_{K,f}) = \psi^{-1}(Min(\psi(\mathcal{O}_{K,f})))$ with $\psi(\mathcal{O}_{K,f}) = \mathbf{Z}\binom{1}{1} \oplus \mathbf{Z}\binom{\xi_1}{\xi_2}$ and with quadratic irrationalities satisfying the necessary conditions $\xi_1 = \frac{1}{2}(f + \sqrt{f^2D}) = f \cdot \frac{1}{2}(1 + \sqrt{D}) \geq 1 \cdot \frac{1}{2}(1 + \sqrt{5}) > \frac{1}{2}(1 + 2) > 1,\ \xi_2 = \frac{1}{2}(f - \sqrt{f^2D}) = f \cdot \frac{1}{2}(1 - \sqrt{D}) \leq f \cdot \frac{1}{2}(1 - \sqrt{5}) < f \cdot \frac{1}{2}(1 - 2) = -\frac{f}{2} \leq -\frac{1}{2} < 0$. Hence, according to Theorem 3.2: $\nu_1^j(1) = \psi^{-1}(\nu_1^j\binom{1}{1}) = \psi^{-1}\binom{P_{j-1}+Q_{j-1}\xi_1}{P_{j-1}+Q_{j-1}\xi_2} = P_{j-1} + Q_{j-1}\xi_1 = P_{j-1} + Q_{j-1}\frac{f}{2}(1 + \sqrt{D}),\ \nu_2^j(1) = \psi^{-1}(\nu_2^j\binom{1}{1}) = \psi^{-1}((-1)^j\binom{R_{j-1}-S_{j-1}\xi_1}{R_{j-1}-S_{j-1}\xi_2}) = (-1)^j(R_{j-1} - S_{j-1}\xi_1) = (-1)^j(R_{j-1} - S_{j-1}\frac{f}{2}(1 + \sqrt{D}))$ for all $j \geq 0$. Now these lattices have the additional property that $\xi_1 + \xi_2 = f$ with $f \in \mathbf{N}$, and therefore Corollary 3.3 yields $R_{j-1} = P_{j-1} + f \cdot Q_{j-1}, S_{j-1} = Q_{j-1}$ and yet another representation of the lattice minima: $\nu_1^j(1) = \psi^{-1}(\nu_1^j\binom{1}{1}) = \psi^{-1}\binom{R_{j-1}-S_{j-1}\xi_2}{R_{j-1}-S_{j-1}\xi_1} = R_{j-1} - S_{j-1}\xi_2 = R_{j-1} - S_{j-1}\frac{f}{2}(1 - \sqrt{D}) = R_{j-1} + S_{j-1}\frac{f}{2}(-1 + \sqrt{D}),\ \nu_2^j(1) = \psi^{-1}(\nu_2^j\binom{1}{1}) = \psi^{-1}((-1)^j\binom{P_{j-1}+Q_{j-1}\xi_2}{P_{j-1}+Q_{j-1}\xi_1}) = (-1)^j(P_{j-1} + Q_{j-1}\xi_2) = (-1)^j(P_{j-1} + Q_{j-1}\frac{f}{2}(1 - \sqrt{D})) = (-1)^j(P_{j-1} - Q_{j-1}\frac{f}{2}(-1 + \sqrt{D}))$ for all $j \geq 0$. All the representations by means of total quotients (of $-\xi_2$ resp. ξ_1) can now be obtained from the Remark after Theorem 3.2 and by the utilization of the norms of quadratic irrationalities (which were not yet available in the general context of Theorem 3.2). □

Remark. In Corollary 3.4,1 the statement concerning the system of minimal points and the successive neighbours of 1 remains true for $D \equiv 1 \pmod 4$, if $\mathcal{O}_f$ is replaced by $\mathcal{O}_{K,2f}$ ($= \mathcal{O}_f$ formally).

With the aid of Scheffler's formula (see O. PERRON [25], § 21, formula 18, pag. 71) the norms can be expressed by $N_{K\,|\,\mathbf{Q}}(\nu_1^j(1)) = ((P_{j-1}N_0 - Q_{j-1}M_0)^2 - DQ_{j-1}^2)/N_0^2 = (-1)^jN_j/N_0$, where $(\xi_1)_j = (M_j + \sqrt{f^2D})/N_j$

is the unique representation of the total quotients with integers $M_j, N_j \in \mathbf{Z}$ $(j \geq 0)$.

Finally combining Theorem 2.3 with Corollary 3.4 and changing the frame from algebraic to elementary number theory, we obtain the following Corollary, the first part of which is well known, but not so the second part in this detailed formulation.

Corollary 3.5. (Binary quadratic norm form inequalities characterizing convergents for continued fraction expansions of certain quadratic irrationalities.)

Suppose that $D \in \mathbf{N},\ D \geq 2$ *is squarefree,* $f \in \mathbf{N}$, *and let* $x, y \in \mathbf{Z}$.

1. *If* $P_j, Q_j \in \mathbf{N}_0$ $(j \geq -2)$ *are the numerators and denominators of the convergents for the continued fraction expansion of* $\sqrt{f^2 D}$, *then*

$$|\, x^2 - Df^2y^2 \,| < f\sqrt{D}, \quad \gcd(x,y) = 1 \Rightarrow$$
$$\Rightarrow \exists j \geq 0 \quad |\, x \,| = P_{j-1},\ |\, y \,| = Q_{j-1}.$$

2. *If* $D \equiv 1 (\operatorname{mod} 4)$, *and* $P_j, Q_j \in \mathbf{N}_0$ $(j \geq -2)$ *are the numerators and denominators of the convergents for the continued fraction expansion of* $\frac{1}{2}(-f + \sqrt{f^2D}) = -\tau\left(\frac{1}{2}(f + \sqrt{f^2D})\right)$, and $R_j, S_j \in \mathbf{N}_0$ $(j \geq -2)$ *are those of* $\frac{1}{2}(f + \sqrt{f^2D})$, *then*
   - **a)** $|\, x^2 + fxy - \frac{D-1}{4}f^2y^2 \,| < \frac{1}{2}f\sqrt{D}$, $\gcd(x,y) = 1$, $sgn(x) = sgn(y)$ $\Rightarrow \exists j \geq 0 \quad |\, x \,| = P_{j-1},\ |\, y \,| = Q_{j-1}$,
   - **b)** $|\, x^2 + fxy - \frac{D-1}{4}f^2y^2 \,| < \frac{1}{2}f\sqrt{D}$, $\gcd(x,y) = 1$, $sgn\ (x) \neq sgn(y)$ $\Rightarrow \exists j \geq 0 \quad |\, x \,| = R_{j-1},\ |\, y \,| = S_{j-1}$.

PROOF. **1.** Let an algebraic integer in $K = \mathbf{Q}(\delta)$ be defined by $\alpha = x + yf\delta \in \mathbf{Z} \oplus \mathbf{Z}f\delta = \mathcal{O}_f$ with the given integers $x, y \in \mathbf{Z}$.
(For $D \equiv 1$ (mod 4), α is in the order $\mathcal{O}_{K,2f}$.) By the assumption $\gcd(x,y) = 1$, α is primitive in $\mathcal{O}_f$ and the binary quadratic form $x^2 - Df^2y^2 = (x + yf\delta)(x - yf\delta) = \alpha \cdot \tau(\alpha) = N_{K\,|\,\mathbf{Q}}(\alpha)$ is just the norm of α with respect to the field extension $K\,|\,\mathbf{Q}$. According to Theorem 2.3,1.a, $|\, N_{K\,|\,\mathbf{Q}}(\alpha) \,| < f\delta$ together with the primitivity of α in $\mathcal{O}_f$ implies $\alpha \in Min(\mathcal{O}_f)$. Now by Corollary 3.4,1,

$$Min(\mathcal{O}_f) = \left\{\pm(P_{j-1} + Q_{j-1}f\delta) \;\middle|\; j \geq 0\right\} \cup$$
$$\left\{\pm(-1)^j(P_{j-1} - Q_{j-1}f\delta) \;\middle|\; j \geq 0\right\}$$

and hence $\exists j \geq 0 \quad \alpha = x + yf\delta = \pm(P_{j-1} \pm Q_{j-1}f\delta)$. Finally the $\mathbf{Q}$–linear independence of $(1, f\delta)$ yields $x = \pm P_{j-1},\ y = \pm Q_{j-1}$.

2. Let $D \equiv 1$ (mod 4) and define an algebraic integer in $K = \mathbf{Q}(\delta)$ by $\alpha = x + y\frac{f}{2}(1+\delta) \in \mathbf{Z} \oplus \mathbf{Z}\frac{f}{2}(1+\delta) = \mathcal{O}_{K,f}$ with the given integers $x, y \in \mathbf{Z}$.

The assumption $\gcd(x,y) = 1$ is equivalent with the primitivity of α in $\mathcal{O}_{K,f}$. (In the other representation $\alpha = \frac{1}{2}(z+wf\delta)$, where $z = 2x+fy, w = y$ are rational integers satisfying $z \equiv fw \pmod 2$, the primitivity of α in $\mathcal{O}_{K,f}$ is equivalent with either $\gcd(z,w) = 1$ or $\gcd(z,w) = 2, z/2 \not\equiv fw/2 \pmod 2$.) Further the binary quadratic form $x^2 + fxy - \frac{D-1}{4}f^2y^2 = (x + y\frac{f}{2}(1+\delta)) \cdot (x + y\frac{f}{2}(1-\delta)) = \alpha \cdot \tau(\alpha) = N_{K\,|\,\mathbf{Q}}(\alpha)$ is just the norm of α with respect to the extension $K\,|\,\mathbf{Q}$. According to Theorem 2.3,2.a, $|\,N_{K\,|\,\mathbf{Q}}(\alpha)\,| < \frac{1}{2}f\delta$ together with the primitivity of α in $\mathcal{O}_{K,f}$ implies $\alpha \in Min(\mathcal{O}_{K,f})$. Now by Corollary 3.4,2,

$$Min(\mathcal{O}_{K,f}) = \{\pm(P_{j-1} + Q_{j-1}\frac{f}{2}(1+\delta)) \mid j \geq 0\} \cup \\ \{\pm(-1)^j(R_{j-1} - S_{j-1}\frac{f}{2}(1+\delta)) \mid j \geq 0\}$$

and hence $\exists j \geq 0 \quad \alpha = x + y\frac{f}{2}(1+\delta) = \pm(P_{j-1} + Q_{j-1}\frac{f}{2}(1+\delta))$ or $\alpha = \pm(R_{j-1} - S_{j-1}\frac{f}{2}(1+\delta))$. Finally the $\mathbf{Q}$–linear independence of $(1, \frac{f}{2}(1+\delta))$ yields

a) if $sgn(x) = sgn(y)$, then $|\,x\,| = P_{j-1}$, $|\,y\,| = Q_{j-1}$,
b) if $sgn(x) \neq sgn(y)$, then $|\,x\,| = R_{j-1}$, $|\,y\,| = S_{j-1} = Q_{j-1}$. □

§4. Units in fields with radicand $D \equiv 1 \pmod 4$

In this section the following problems for real quadratic number fields of D–type II will be considered.

I. The possibilities for the index $(E_K : E_{\mathcal{O}})$ of the unit group $E_{\mathcal{O}}$ of the suborder $\mathcal{O} = \mathbf{Z} \oplus \mathbf{Z}\sqrt{D}$ in the unit group E_K of the maximal order $\mathcal{O}_K = \mathbf{Z} \oplus \mathbf{Z}\frac{1}{2}(1+\sqrt{D})$.

In Proposition 4.1 we shall see that these possible values depend on the prime residue class group $U(\mathcal{O}_K/\mathcal{F})$ of the conductor $\mathcal{F} = cond(\mathcal{O})$ of the suborder $\mathcal{O}$ in the maximal order $\mathcal{O}_K$, and that for D–type IIA fields there is only the possibility $(E_K : E_{\mathcal{O}}) = 1$, because $U(\mathcal{O}_K/\mathcal{F}) \simeq C_1$, whereas for D–type IIB fields there are two possible values $(E_K : E_{\mathcal{O}}) \in \{1,3\}$, because $U(\mathcal{O}_K/\mathcal{F}) \simeq C_3$.

II. The indirect computation of the fundamental unit $\varepsilon_0 > 1$ of K by looking for a multiple of the unit in the suborder $\mathcal{O}$.

The continued fraction algorithm finds exactly all the lattice minima among the algebraic integers in an order, as we have seen in Corollary 3.4. Hence the question arises, which conditions must be satisfied by the radicand D, in order that a multiple of the fundamental unit appears as a lattice minimum in the suborder $\mathcal{O}$. According to Proposition 4.1, only in fields of D–type IIB with unit group index $(E_K : E_{\mathcal{O}}) = 3$ a multiple of a unit can be a lattice minimum in the suborder $\mathcal{O}$, because otherwise $E_K = E_{\mathcal{O}} \subset Min(\mathcal{O})$ and a multiple of a minimum is imprimitive and hence cannot be a minimum too. Further, as $\mathcal{F} = cond(\mathcal{O}) = 2\mathcal{O}_K$, the multiple can only be the twofold. Other multiples would not be primitive, because $2\mathcal{O}_K \cap \mathcal{O} = 2\mathcal{O}_K \neq 2\mathcal{O}$, but $p\mathcal{O}_K \cap \mathcal{O} = p\mathcal{O}$ for all $p \in \mathbf{P}, p \neq 2$. The central result, Theorem 4.2 will show that, fortunately, all radicands $D \equiv 5 \pmod 8$, with the single exception $D = 5$, have the property that, in the case $(E_K : E_{\mathcal{O}}) = 3$, the twofold of the fundamental unit, and in fact of any "genuine unit" in $\mathcal{O}_K$, $\varepsilon \in E_K \setminus E_{\mathcal{O}} = \varepsilon_0 E_{\mathcal{O}} \cup \varepsilon_0^2 E_{\mathcal{O}}$, is a minimum in the suborder $\mathcal{O} : 2\varepsilon \in Min(\mathcal{O})$.

III. Arithmetical criteria for the occurrence of unit group index $(E_K : E_{\mathcal{O}}) = 1$ in D–type IIB fields.

Unit group index $(E_K : E_{\mathcal{O}}) = 1$ must be considered as an exceptional event for D–type IIB fields, because in general its occurrence depends on the existence of a certain cubic "auxiliary field" (in D. Hilbert's terminology [15], § 90, pag. 324). This is due to the translation of the problem into the equivalent question, when the 3–ring class field modulo 2 of K is a cubic extension of the Hilbert 3–class field of K, $[F_2^{(3)}(K) : F_1^{(3)}(K)] = 3$. Hence, according to H. Hasse's class field theoretic treatment of non–Galois cubic absolute extensions [13], in the special case that K has a class number h_K coprime to 3, that is, $F_1^{(3)}(K) = K$, another equivalent problem is, when there exists a totally real cubic extension $L \mid \mathbf{Q}$ with discriminant $discr(L \mid \mathbf{Q}) = 2^2 \cdot discr(K \mid \mathbf{Q}) = 4D$, because then $F_2^{(3)}(K) = L \cdot K$ is a cyclic cubic extension of K. This is not the case too often, because cubic discriminants are sown rather thin. See Tables A, B for the smallest radicands of these exceptional fields and also compare the results in § 6, Tables 5, 6 for statistics and frequencies of unit group index $(E_K : E_{\mathcal{O}}) = 3$.

Proposition 4.1. (Unit group indices and "half–units" in real quadratic fields of D–type II.)

Let $K = \mathbf{Q}(\sqrt{D})$ be a quadratic field with radicand $D \equiv 1 (\mathrm{mod}\, 4)$, maximal order $\mathcal{O}_K = \mathbf{Z} \oplus \mathbf{Z}\frac{1}{2}(1 + \sqrt{D})$, and suborder $\mathcal{O} = \mathbf{Z} \oplus \mathbf{Z}\sqrt{D}$ with conductor $\mathcal{F} = cond(\mathcal{O}) = 2\mathcal{O}_K$.

1. *The prime residue class group of the conductor $\mathcal{F} = 2\mathcal{O}_K$ of the suborder $\mathcal{O}$ is $U(\mathcal{O}_K/\mathcal{F}) \simeq C_1$, if $D \equiv 1 \pmod 8$, and $U(\mathcal{O}_K/\mathcal{F}) \simeq C_3$, if $D \equiv 5 \pmod 8$.*

2. *For an algebraic integer $\alpha \in \mathcal{O}_K$ with $\gcd(\alpha, 2) = 1$*

a) *already $\alpha \in \mathcal{O}$, if $D \equiv 1 (\mathrm{mod}\, 8)$,*

b) *either $\alpha \in \mathcal{O}$ or at most the third power $\alpha^3 \in \mathcal{O}$, if $D \equiv 5 (\mathrm{mod}\, 8)$.*

In particular, this result is valid for generators of ambiguous principal ideals in K, $\alpha \in \mathcal{O}_K$ with $N_{K \mid \mathbf{Q}}(\alpha) \mid R_{K \mid \mathbf{Q}}$ (see § 5), and for units $\varepsilon \in E_K$. More detailed:

3. *If $\alpha \in \mathcal{O}_K \setminus \mathcal{O}$ has the reduced representation $\alpha = \frac{1}{2}(x + y\sqrt{D})$ with $x, y \in \mathbf{Z}$, $x \equiv y \equiv 1 \pmod 2$, then $\alpha^2 = \frac{1}{4}((x^2 + Dy^2) + 2xy\sqrt{D}) \in \mathcal{O}_K \setminus \mathcal{O}$, and*

$$\alpha^3 = \frac{1}{8}((x^3 + 3Dxy^2) + (3x^2y + Dy^3)\sqrt{D})$$

$$\in \begin{cases} \mathcal{O}_K \setminus \mathcal{O} & \text{if } D \equiv 1 \pmod 8, \\ \mathcal{O} & \text{if } D \equiv 5 \pmod 8. \end{cases}$$

(Note that $\gcd(\alpha, 2) = 1$ is equivalent with $\alpha \in \mathcal{O}_K \setminus 2\mathcal{O}_K$, if $D \equiv 5 \pmod 8$, but even with $\alpha \in \mathcal{O} \setminus 2\mathcal{O}_K$, if $D \equiv 1 \pmod 8$.)

For the rest of the Proposition assume that K is real quadratic and let $\varepsilon_0 > 1$ be the fundamental unit of $\mathcal{O}_K$ and $\eta_0 > 1$ the fundamental unit of $\mathcal{O}$.

4. *"Half–units" can exist, only if K is of D–type IIB, and if they exist, then $\eta_0 = \varepsilon_0^3$, that is,*

$$E_K \neq E_{\mathcal{O}} \Rightarrow D \equiv 5 (\operatorname{mod} 8),\ (E_K : E_{\mathcal{O}}) = 3.$$

5. *Next we have a closer look at algebraic integers of norm ±4.*
   a) *The twofold of any unit in $\mathcal{O}_K$ lies in the suborder $\mathcal{O}$ and has norm ±4, that is*

$$\varepsilon \in E_K \Rightarrow 2\varepsilon \in \mathcal{O},\ |N_{K|\mathbf{Q}}(2\varepsilon)| = 4.$$

   b) *Conversely, if some algebraic integer in the suborder, $\beta \in \mathcal{O}$, has norm ±4, then 2 divides β in $\mathcal{O}_K$ (that is, β cannot be primitive in $\mathcal{O}_K$), and β is the twofold of a unit:*

$$|N_{K|\mathbf{Q}}(\beta)| = 4 \Rightarrow \beta \in 2\mathcal{O}_K,\ \beta/2 \in E_K.$$

(Furthermore, either 2 divides β even in $\mathcal{O}$, $\beta \in 2\mathcal{O}$, or β is primitive in the suborder $\mathcal{O}$. In any case $\beta/2$ is primitive in $\mathcal{O}_K$.)

   c) *For $\beta \in \mathcal{O}$ the following equivalences hold:*

$$\begin{aligned} |N_{K|\mathbf{Q}}(\beta)| = 4,\ \beta \in 2\mathcal{O} &\quad\Leftrightarrow\quad \beta/2 \in E_{\mathcal{O}},\ \text{and} \\ |N_{K|\mathbf{Q}}(\beta)| = 4,\ \beta \text{ primitive in } \mathcal{O} &\quad\Leftrightarrow\quad \beta/2 \in E_K \setminus E_{\mathcal{O}}, \end{aligned}$$

and thus the following mappings are bijective and order preserving:

$$\{\beta \in \mathcal{O} \mid |N_{K\,|\,\mathbf{Q}}(\beta)| = 4,\ \beta/2 \in \mathcal{O}\} \to E_{\mathcal{O}}, \quad \beta \to \beta/2, \text{ and}$$
$$\{\beta \in \mathcal{O} \mid |N_{K\,|\,\mathbf{Q}}(\beta)| = 4,\ \beta/2 \in \mathcal{O}_K \setminus \mathcal{O}\} \to E_K \setminus E_{\mathcal{O}},\ \beta \to \beta/2.$$

6. *There exist "half–units", exactly if the diophantine quadratic Pellian norm–4–equation has a primitive solution, that is*

$$(E_K : E_{\mathcal{O}}) = 3 \quad \Leftrightarrow \quad \exists \xi \in \mathcal{O} \quad N_{K\,|\,\mathbf{Q}}(\xi) = 4,\ \xi \textit{ primitive in } \mathcal{O}$$
$$\Leftrightarrow \quad \exists x, y \in \mathbf{Z} \quad x^2 - Dy^2 = 4,\ \gcd(x,y) = 1.$$

In particular, if there exists a lattice minimum $\vartheta \in Min(\mathcal{O})$ with the property $|N_{K\,|\,Q}(\vartheta)| = 4$, then $(E_K : E_{\mathcal{O}}) = 3$. (The converse statement is false, if $D = 5$. See Theorem 4.2 and the Remark afterwards.)

For the next two statements, involving principal factor types of real quadratic fields, compare § 5.

7. *If K is of PF–type II, then there exist "half–units", exactly if the period length of the continued fraction expansion of $\sqrt{D}$ is congruent to the period length of the continued fraction expansion of $\frac{1}{2}(1+\sqrt{D})$ modulo 4, that is*

$$N_{K\,|\,\mathbf{Q}}(\varepsilon_0) = -1 \Rightarrow \big((E_K : E_{\mathcal{O}} = 3 \Leftrightarrow PL(\mathcal{O}) \equiv PL(\mathcal{O}_K) (\mathrm{mod}\, 4)\big).$$

8. *If K is of PF–type I, then the period length of the continued fraction expansion of $\sqrt{D}$ is always congruent to the period length of the continued fraction expansion of $\frac{1}{2}(1+\sqrt{D})$ modulo 4, that is,*

$$N_{K\,|\,\mathbf{Q}}(\varepsilon_0) = +1 \quad \Rightarrow \quad PL(\mathcal{O}) \equiv PL(\mathcal{O}_K) (\text{mod } 4).$$

In this case the primitive period lengths do not provide a condition for the existence of "half–units".

PROOF. **1.** For $K = \mathbf{Q}(\sqrt{D})$ with $D \equiv 1$ (mod 4) the conductor of the suborder in the maximal order is $\mathcal{F} = cond(\mathcal{O}) = 2\mathcal{O}_K$, according to Theorem 1.1, 2.

Further, in the case $D \equiv 1$ (mod 8):

2 splits in K, $2\mathcal{O}_K = \mathcal{L}_1 \cdot \mathcal{L}_2$ with distinct prime ideals $\mathcal{L}_1, \mathcal{L}_2 \in \mathbf{P}_K$, $\mathcal{N}_{K\,|\,\mathbf{Q}}(\mathcal{L}_1) = \mathcal{N}_{K\,|\,\mathbf{Q}}(\mathcal{L}_2) = 2$. The generalized Chinese remainder theorem yields $U(\mathcal{O}_K/\mathcal{F}) \simeq U(\mathcal{O}_K/\mathcal{L}_1) \times U(\mathcal{O}_K/\mathcal{L}_2) \simeq U(\mathbf{F}_2) \times U(\mathbf{F}_2) \simeq C_1 \times C_1 \simeq C_1$.

And in the case $D \equiv 5 \pmod 8$):
2 remains inert in K, $2\mathcal{O}_K \in \mathbf{P}_K$, $\mathcal{N}_{K\,|\,\mathbf{Q}}(2\mathcal{O}_K) = 2^2 = 4$, whence $U(\mathcal{O}_K/\mathcal{F}) \simeq U(\mathbf{F}_4) \simeq C_3$.

2. Now for $\alpha \in \mathcal{O}_K : \gcd(\alpha, 2) = 1 \Leftrightarrow \gcd(\alpha\mathcal{O}_K, \mathcal{F}) = \alpha\mathcal{O}_K + \mathcal{F} = \mathcal{O}_K \Leftrightarrow \alpha + \mathcal{F} \in U(\mathcal{O}_K/\mathcal{F})$.
Hence in the case $D \equiv 1 \pmod 8$:
$\gcd(\alpha, 2) = 1 \Rightarrow \alpha + \mathcal{F} \in U(\mathcal{O}_K/\mathcal{F}) \simeq C_1 \Rightarrow \alpha + \mathcal{F} = 1 + \mathcal{F} \Rightarrow \alpha \in 1 + \mathcal{F} = 1 + cond(\mathcal{O}) \subset \mathcal{O}$.
And in the case $D \equiv 5 \pmod 8$:
$\gcd(\alpha, 2) = 1 \Rightarrow \alpha + \mathcal{F} \in U(\mathcal{O}_K/\mathcal{F}) \simeq C_3 \Rightarrow \exists v \in \{1, 3\}\ \alpha^v + \mathcal{F} = 1 + \mathcal{F}$ and therefore $\alpha^v \in 1 + \mathcal{F} = 1 + cond(\mathcal{O}) \subset \mathcal{O}$.
For the specialization to generators of ambiguous principal ideals compare Theorem 5.11 and for units see **4.**

3. An algebraic integer $\alpha \in \mathcal{O}_K \setminus \mathcal{O}$ has the representation $\alpha = \frac{1}{2}(x + y\delta)$ with $x, y \in \mathbf{Z}$ and $x \equiv y \not\equiv 0 \pmod 2$. Hence $x^2 + Dy^2 \equiv x^2 + y^2 \equiv 2 \equiv 2xy \pmod 4$, respectively $\frac{1}{2}(x^2 + Dy^2) \equiv 1 \equiv xy \pmod 2$ and therefore $\alpha^2 = \frac{1}{4}((x^2 + Dy^2) + 2xy\delta) \in \mathcal{O}_K \setminus \mathcal{O}$. Further $x^3 + 3Dxy^2 \equiv x + 3Dx \equiv (3D + 1)x \pmod 8$, $3x^2y + Dy^3 \equiv 3y + Dy \equiv (D + 3)y \pmod 8$, where $3D + 1 \equiv 4 \equiv D + 3 \pmod 8$, if $D \equiv 1 \pmod 8$, and $3D + 1 \equiv 0 \equiv D + 3$ (mod 8), if $D \equiv 5$ (mod8). Thus in case $D \equiv 1 \pmod 8 : \frac{1}{4}(x^3 + 3Dxy^2) \equiv \frac{1}{4}(3D + 1)x \equiv 1 \equiv \frac{1}{4}(D + 3)y \equiv \frac{1}{4}(3x^2y + Dy^3) \pmod 2$, and in case $D \equiv 5 \pmod 8 : \frac{1}{4}(x^3 + 3Dxy^2) \equiv \frac{1}{4}(3D + 1)x \equiv 0 \equiv \frac{1}{4}(D + 3)y \equiv \frac{1}{4}(3x^2y + Dy^3) \pmod 2$, always taking into consideration that $x \equiv y \equiv 1 \pmod 2$. Hence $\alpha^3 = \frac{1}{8}((x^3 + 3Dxy^2) + (3x^2y + Dy^3)\delta) \in \mathcal{O}_K \setminus \mathcal{O}$, if $D \equiv 1 \pmod 8$, and $\alpha^3 \in \mathcal{O}$, if $D \equiv 5 \pmod 8$.

4. For a unit $\varepsilon \in E_K$ we have $\varepsilon\mathcal{O}_K = \mathcal{O}_K$ and hence $\gcd(\varepsilon, 2) = 1$. Thus, according to **2.** and using that $E_K \cap \mathcal{O} = E_{\mathcal{O}}$ (see **5.c**), $W_K = W_{\mathcal{O}} = \{-1, 1\}$, $\varepsilon_0 > 1$ and $\eta_0 > 1$: if $D \equiv 1 \pmod 8$, then $\varepsilon \in \mathcal{O}$, in particular, $\varepsilon_0 \in \mathcal{O}$ and therefore $E_K = E_{\mathcal{O}}$, if $D \equiv 5 \pmod 8$, then $\varepsilon \in \mathcal{O}$ or $\varepsilon^3 \in \mathcal{O}$, and in particular, $\varepsilon_0^3 \in \mathcal{O}$, i.e., $\exists v \in \mathbf{N}\ \ \varepsilon_0^3 = \eta_0^v$. But for $D \equiv 5 \pmod 8$ on the other hand $\eta_0 \in E_K$, i.e., $\exists u \in \mathbf{N}\ \ \eta_0 = \varepsilon_0^u$. Together $\varepsilon_0^3 = \varepsilon_0^{uv}$, i.e., $uv = 3$, and hence either $u = 1, v = 3$ or $u = 3$, $v = 1$. Now, if $E_K \neq E_{\mathcal{O}}$, then $u = 1$ is impossible and $(E_K : E_{\mathcal{O}}) = (\langle -1, \varepsilon_0\rangle : \langle -1, \eta_0\rangle) = ((E_K/W_K) : (E_{\mathcal{O}}/W_{\mathcal{O}})) = (\langle\varepsilon_0\rangle : \langle\eta_0\rangle) = u = 3$.

5. Throughout the proof of this Proposition we always assume $D \equiv 1 \pmod 4$.

a) $\varepsilon \in E_K \Rightarrow N_{K\,|\,\mathbf{Q}}(\varepsilon) = \pm 1 \Rightarrow N_{K\,|\,\mathbf{Q}}(2\varepsilon) = 4N_{K\,|\,\mathbf{Q}}(\varepsilon) = \pm 4$.
Further $2\varepsilon \in \mathcal{O}$, because $2\mathcal{O}_K = cond(\mathcal{O}) \subset \mathcal{O}$.

b) Let $\beta \in \mathcal{O}$, $\beta = x + y\delta$ with $x, y \in \mathbf{Z}$. If $N_{K\,|\,\mathbf{Q}}(\beta) = \pm 4$, then $x^2 - y^2 \equiv x^2 - Dy^2 = \pm 4 \equiv 0 \pmod 4$ and thus $x \equiv y \pmod 2$, i.e., $\beta/2 = \frac{1}{2}(x + y\delta) \in \mathcal{O}_K$, resp., $\beta \in 2\mathcal{O}_K$. But $\beta/2$ is even a unit in E_K, because $N_{K\,|\,\mathbf{Q}}(\beta/2) = \frac{1}{4}N_{K\,|\,\mathbf{Q}}(\beta) = \pm 1$. Further, for a rational prime $p \in \mathbf{P}$ we have : if $\beta \in p\mathcal{O}_K$, i.e., $\beta = p\gamma$ for some $\gamma \in \mathcal{O}_K$, then $N_{K\,|\,\mathbf{Q}}(\beta) = p^2 N_{K\,|\,\mathbf{Q}}(\gamma)$, $N_{K\,|\,\mathbf{Q}}(\gamma) \in \mathbf{Z}$, i.e., $p^2 \,|\, N_{K\,|\,\mathbf{Q}}(\beta)$; by contraposition, if $|\, N_{K\,|\,\mathbf{Q}}(\beta) \,| = 4 = 2^2$, then only the prime 2 can divide β in $\mathcal{O}_K$ and in $\mathcal{O}$. Therefore either β is primitive in $\mathcal{O}$ or 2 divides β in $\mathcal{O}$. But in any case $\beta/2$, as a unit, is primitive in $\mathcal{O}_K$.

c) These are immediate consequences of **a**) and **b**). It only remains to show that $E_K \cap \mathcal{O} = E_\mathcal{O}$. The inclusion $E_\mathcal{O} \subset E_K \cap \mathcal{O}$ is clear and on the other hand $\varepsilon \in E_K \cap \mathcal{O}$ implies $\varepsilon^{-1} = \pm\varepsilon' \in \mathcal{O}$, that is, $\varepsilon \in E_\mathcal{O}$. (In fact, we have proved this for arbitrary orders in Theorem 2.3, 1.c and 2.c already.)

6. From the last bijection in **5.c** we derive: $(E_K : E_\mathcal{O}) = 3 \Leftrightarrow \exists\xi \in \mathcal{O} \quad \xi/2 \in E_K \setminus E_\mathcal{O} \Leftrightarrow \exists\xi \in \mathcal{O} \quad |\, N_{K\,|\,\mathbf{Q}}(\xi) \,| = 4,\ \xi/2 \in \mathcal{O}_K \setminus \mathcal{O} \Leftrightarrow \exists\xi \in \mathcal{O} \quad N_{K\,|\,\mathbf{Q}}(\xi) = 4$, ξ primitive in $\mathcal{O}$. The last step was justified, because in the case $\varepsilon_0 \in E_K \setminus E_\mathcal{O}, N_{K\,|\,\mathbf{Q}}(\varepsilon_0) = -1$ we have $\varepsilon_0^2 \in E_K \setminus E_\mathcal{O}$, by 3., and $N_{K\,|\,\mathbf{Q}}(2\varepsilon_0^2) = +4$. With the aid of the reduced representation $\xi = x + y\delta$ with $x, y \in \mathbf{Z}$, we finally obtain $\exists\xi \in \mathcal{O} \quad N_{K\,|\,\mathbf{Q}}(\xi) = 4 \quad \xi/2 \in \mathcal{O}_K \setminus \mathcal{O} \Leftrightarrow \exists x, y \in \mathbf{Z} \quad x^2 - Dy^2 = 4,\ x \equiv y \not\equiv 0 \pmod 2 \Leftrightarrow \exists x, y \in \mathbf{Z} \quad x^2 - Dy^2 = 4,\ \gcd(x, y) = 1$.
The specialization for a lattice minimum $\vartheta \in Min(\mathcal{O})$ makes use of the primitivity of ϑ in $\mathcal{O}$, discussed in § 2, sections 2, 7, Remarks.

7. For this proof we refer to P. Kaplan and K. S. Williams [16].

8. See § 5, Theorem 5.12. □

By an application of the geometric Theorem 2.3 and a discussion of some exceptional cases, we shall see now that the twofolds of "genuine units" in the maximal order of D–type IIB fields can always be discovered as lattice minima in the geometric Minkowski image of the suborder, except for a single case.

Theorem 4.2. (Twofolds of units among the lattice minima in the suborder $\mathcal{O} = \mathbf{Z} \oplus \mathbf{Z}\sqrt{D}$ of a real quadratic number field of D–type II.)

Let $K = \mathbf{Q}(\sqrt{D})$ *be a real quadratic field with radicand* $D \equiv 1 \pmod 4$, $D \neq 5$. *(For* $D \equiv 1 \pmod 8$ *the statements are also true but "empty".)*

1. *Primitive algebraic integers* $\beta \in \mathcal{O}$ *with norm* ± 4 *are minima in* $\mathcal{O}$:

$$|\, N_{K\,|\,\mathbf{Q}}(\beta) \,| = 4,\ \beta \textit{ primitive in } \mathcal{O} \Rightarrow \beta \in Min(\mathcal{O}).$$

2. *Now we have a new criterion for the existence of "half–units" :*

$$(E_K : E_\mathcal{O}) = 3 \quad \Leftrightarrow \quad \exists\vartheta \in Min(\mathcal{O}) \quad |\, N_{K\,|\,\mathbf{Q}}(\vartheta) \,| = 4.$$

3. *The mapping*

$$\{\vartheta \in Min(\mathcal{O}) \;\mid\; |\, N_{K\,|\,\mathbf{Q}}(\vartheta) \,| = 4\} \to E_K \setminus E_\mathcal{O}, \quad \vartheta \to \vartheta/2$$

is bijective and order preserving.

PROOF. **1.** Assume $\beta \in \mathcal{O} = \mathbf{Z} \oplus \mathbf{Z}\delta$, β primitive in $\mathcal{O}$ (hence in particular $\beta \neq 0$ and $\beta \notin 2\mathcal{O}$) and $|N_{K|\mathbf{Q}}(\beta)| = 4$, whence $\beta \in 2\mathcal{O}_K$, by Proposition 4.1,5.b. If $\beta \notin Min(\mathcal{O})$, then $\exists \vartheta \in \mathcal{O}\;\; 0 < |\vartheta| < |\beta|$, $|\vartheta'| < |\beta'|$. For the number $\xi = |\vartheta| \cdot |\beta'| \in \mathcal{O}$ the conjugates are bounded

$$\begin{aligned} 0 < \xi = |N_{K|\mathbf{Q}}(\beta)| \cdot |\vartheta| / |\beta| < 4, \\ |\xi'| = |N_{K|\mathbf{Q}}(\beta)| \cdot |\vartheta'| / |\beta'| < 4. \end{aligned}$$

Applying Lemma 2.1, the coefficients $x, y \in \mathbf{Z}$ of $\xi = x + y\delta$ can be estimated by $|x|, |y\delta| < 4$, and $\beta/2 \in \mathcal{O}_K$ implies $\beta'/2 = (\beta/2)' \in \mathcal{O}_K$, $\xi/2 = |\vartheta| \cdot |\beta'|/2 \in \mathcal{O}_K$, and thus $x \equiv y \pmod 2$.

If $D \geq 17$, then $\delta > \sqrt{16} = 4$, $|y| < 4/\delta < 1$ and, as $y \in \mathbf{Z}, y = 0$. Now $x = \xi = |\vartheta| \cdot |N_{K|\mathbf{Q}}(\beta)| / |\beta|$ or $x \cdot |\beta| = 4|\vartheta|$ with $|\vartheta| \in \mathcal{O}$, i.e., $x \cdot |\beta| \in 4\mathcal{O}$. But β is primitive in $\mathcal{O}$ and from Lemma 2.2 we get $4 \,|\, x$. Together with $x = \xi < 4$, this implies $x = 0$. Hence $\vartheta = 0$, in contradiction to $0 < |\vartheta|$. Thus we have shown, that β must be a lattice minimum in $\mathcal{O}$. (Of course, for $D > 16$, $\delta > 4 = |N_{K|\mathbf{Q}}(\beta)|$ we could have applied Theorem 2.3, 1.a directly, but we need the preparation above for the following supplementary case.)

If $D = 13$, then $\delta = \sqrt{13} > 3$ and $|y| < 4/\delta < 4/3$, that is, $y \in \{-1, 0, 1\}$. $y = 0$ is impossible for the same reason as in the case $D \geq 17$. $|y| = 1$ implies $x \in \{-3, -1, 1, 3\}$, because $|x| < 4$, $x \equiv y (\mathrm{mod}\, 2)$. Hence there are $2 \cdot 4 = 8$ possibilities for the integer couple (x, y). But
$0 < \xi = x + y\delta \quad \Rightarrow \quad (x,y) \notin \{(-3,-1), (-1,-1), (1,-1), (3,-1)\}$,
$\xi = x + y\delta < 4 \quad \Rightarrow \quad (x,y) \notin \{(3,1), (1,1)\}$, and
$|\xi'| = |x - y\delta| < 4 \quad \Rightarrow \quad (x,y) \notin \{(-3,1), (-1,1)\}$. We see that all possible couples are discouraged by the restrictions for ξ, and thus $\beta \in Min(\mathcal{O})$ also in this supplementary case.

2. By Proposition 4.1,6 we have $(E_K : E_{\mathcal{O}}) = 3$, if and only if there exists $\beta \in \mathcal{O}$, such that $N_{K|\mathbf{Q}}(\beta) = 4$ and β is primitive in $\mathcal{O}$. But then $\beta \in Min(\mathcal{O})$, according to 1. The other implication has been proved already in Proposition 4.1, 6.

3. This is an immediate consequence of Proposition 4.1, 5.c and 1. □

Remark. $D = 5$ really must be excluded, because in this case (using the same notation as in the proof of Theorem 4.2, 1) : $\delta = \sqrt{5} > 2$ and $|y| < 4/\delta < 4/2 = 2$, that is, $y \in \{-1, 0, 1\}$. Similarly as in the case $D = 13$ again $y = 0$ is impossible and $|y| = 1$ implies $x \in \{-3, -1, 1, 3\}$. Now $0 < \xi = x + y\delta \quad \Rightarrow \quad (x,y) \notin \{(-3,-1), (-1,-1), (1,-1)\}$,
$\xi = x + y\delta < 4 \quad \Rightarrow \quad (x,y) \neq (3,1)$, and

$|\xi'| = |x-y\delta| < 4 \quad \Rightarrow \quad (x,y) \notin \{(3,-1),(-3,1)\}$, but the two couples $(x,y) \in \{(1,1),(-1,1)\}$ remain possible. The corresponding lattice points in the norm rectangle of β are $\vartheta = \pm\xi \cdot \beta / N_{K\,|\,\mathbf{Q}}(\beta) = \pm\frac{1}{4}(\pm 1, \pm\delta) \cdot \beta$ with norms $N_{K\,|\,\mathbf{Q}}(\vartheta) = \frac{1}{16} N_{K\,|\,\mathbf{Q}}(\pm 1, +\delta) \cdot N_{K\,|\,\mathbf{Q}}(\beta) = \frac{1}{16}(1-D)\cdot(\pm 4) = \mp 1$, i.e., units. Indeed the fundamental unit of $K = \mathbf{Q}(\sqrt{5})$ is the normnegative $\varepsilon_0 = \frac{1}{2}(1+\delta)$ and $\beta = 2\varepsilon_0 = 1+\delta$ is not a minimum in $\mathcal{O}$, because its norm rectangle contains the unit $\vartheta = \frac{1}{4}(-1+\delta)\cdot(1+\delta) = \frac{1}{4}(D-1) = 1$.

Corollary 4.3. (A first modification of the unit algorithm : the indirect computation of the fundamental unit in fields of D–type IIB with unit group index 3.)

For every real quadratic number field $K = \mathbf{Q}(\sqrt{D})$ with radicand $D \equiv 5 \pmod 8$, $D \neq 5$, i.e., $D \geq 13$, and with unit group index $(E_K : E_{\mathcal{O}}) = 3$, the fundamental unit $\varepsilon_0 > 1$ of K is the half of the smallest lattice minimum ϑ_0 with norm $N_{K\,|\,\mathbf{Q}}(\vartheta) = \pm 4$ in the 1–chain of the suborder $\mathcal{O} = \mathbf{Z} \oplus \mathbf{Z}\sqrt{D}$,

$$\varepsilon_0 = \frac{\vartheta_0}{2} \in E_K \setminus E_{\mathcal{O}},$$

where $\vartheta_0 = \nu_1^j(1) \in Min(\mathcal{O})$ with $j = \min\left\{i \geq 1 \,\middle|\, |N_{K\,|\,\mathbf{Q}}\nu_1^i(1)| = 4\right\}$, and hence ε_0 can be determined indirectly by the investigation of the first half of the first primitive period $1 < \nu_1(1) < \nu_1^2(1) < \ldots < \nu_1^{PL(\mathcal{O})}(1) = \varepsilon_0^3$ in $Min(\mathcal{O})$.

PROOF. As the fundamental unit ε_0 of K, i.e., the first 1–neighbour of 1 with norm ± 1 in $\mathcal{O}_K \setminus \mathcal{O}$, $\varepsilon_0 = \nu_1^{PL(\mathcal{O}_K)}(1) \in Min(\mathcal{O}_K)$, can be characterized metrically by $\varepsilon_0 = \min\{\varepsilon \in E_K \setminus E_{\mathcal{O}} \,|\, \varepsilon > 1\}$, we obtain at first $2\varepsilon_0 = \vartheta_0 = \min\{\vartheta \in Min(\mathcal{O} \mid \vartheta > 2, |N_{K\,|\,\mathbf{Q}}(\vartheta)| = 4\}$, applying the inverse of the bijective order preserving map from Theorem 4.2, 3. But the condition $\vartheta > 2$ can be replaced by $\vartheta > 1$, because the twofold of the inverse fundamental unit ε_0^{-1} cannot be a minimum in the 1–chain of $\mathcal{O}$: though $2\varepsilon_0^{-1} > 1$ is imaginable, surely the conjugate disables minimality, as $\varepsilon_0^{-1} = \nu_2^{PL(\mathcal{O}_K)}(1) \in Min(\mathcal{O}_K)$ and thus $|(2\varepsilon_0^{-1})'| > |(\varepsilon_0^{-1})'| > 1$. Therefore the running parameter j can vary from 1 upwards without restrictions.

Further the periodicity of the norms of minima enforces ϑ_0 to be contained in the first primitive period of $Min(\mathcal{O})$, i.e., $j < PL(\mathcal{O})$.

Finally the symmetry property of the norms of lattice minima with respect to the first primitive period (see § 2, section 6, Remark) implies that ϑ_0 appears even in the first half of the first primitive period already: $j < \frac{1}{2}PL(\mathcal{O})$. □

Remark. This result permits a uniformization of the procedure for computing the fundamental unit in any real quadratic number field, regardless of its D–type, by the successive construction of the lattice minima $(\nu_1^j(1))_{j\geq 1}$ in the 1–chain of the order $\mathcal{O} = \mathbf{Z} \oplus \mathbf{Z}\sqrt{D}$ and the control, if some minimum has either norm ± 4 (in the case $D \equiv 5 \pmod 8$, $(E_K : E_{\mathcal{O}}) = 3$) or ± 1 (in the cases $D \equiv 5 \pmod 8$, $(E_K : E_{\mathcal{O}}) = 1$ or $D \equiv 1 \pmod 8$ or $D \equiv 2, 3 \pmod 4$).

In view of Corollary 3.4 this means that for any field $K = \mathbf{Q}(\sqrt{D})$ some convergent for the continued fraction expansion of $\sqrt{D}$ determines the fundamental unit, more explicitly, either $\varepsilon_0 = \frac{1}{2}\nu_1^j(1) = \frac{1}{2}(P_{j-1} + Q_{j-1}\sqrt{D})$ for some $0 < j < \frac{1}{2}PL(\mathcal{O})$ or $\varepsilon_0 = \nu_1^p(1) = P_{p-1} + Q_{p-1}\sqrt{D}$ with $p = PL(\mathcal{O})$.

The only exception, where the utilization of the principal lattice $\mathcal{O}_K = \mathbf{Z} \oplus \mathbf{Z}\frac{1}{2}(1 + \sqrt{D})$ with the finer meshes and the direct computation of the fundamental unit by expanding $\frac{1}{2}(-1 + \sqrt{D})$ or $\frac{1}{2}(1 + \sqrt{D})$ in a continued fraction cannot be avoided, is the case $D = 5$. Here even the sublattice $\mathcal{O}$ is still so extraordinary fine that its minima leave out algebraic integers with norm ± 4, which must be considered as a "large" norm in this case.

Concerning the position of the smallest minimum $\vartheta_0 \in Min(\mathcal{O})$ with $\vartheta_0 > 1$ and $|N_{K\,|\,\mathbf{Q}}(\vartheta_0)| = 4$ in the first primitive period of $Min(\mathcal{O})$, i.e., the running parameter $j \in \mathbf{N}_0$, $0 < j < \frac{1}{2}PL(\mathcal{O})$ with $\vartheta_0 = \nu_1^j(1)$, compare the detailed discussion at the end of § 6.

In Table A we list the radicands D of the first 37 exceptional D–type IIB fields with unit group index $(E_K : E_{\mathcal{O}}) = 1$, together with the absolute ordinal number of D in the sequence of all squarefree radicands $D \equiv 5 \pmod 8$, the prime factorization of D (if $D \notin \mathbf{P}$), the actual minimal non–trivial discriminantal principal factor (PF, see § 5), the class number h_K, the associated totally real cubic field L with a generating polynomial $p(X) \in \mathbf{Z}[X]$ of minimal index, and the running number of $discr(L\,|\,\mathbf{Q})$ in the sequence of all discriminants of totally real cubic fields. The polynomials have been taken from V. Ennola and R. Turunen [9] (see also [10]).

The table starts with the well–known example $D = 37$, frequently cited for the purpose of illustration that $D \equiv 5 \pmod 8$ alone is (necessary but) not sufficient for the existence of "half–units". A glance at the class numbers of these fields shows that they are not divisible by 3, without exceptions. Indeed, in the next Theorem 4.4, 3 we shall see, that in the special case of $\gcd(h_K, 3) = 1$ the existence of a totally real cubic field extension $L\,|\,\mathbf{Q}$ with discriminant $discr(L\,|\,\mathbf{Q}) = 4{\cdot}discr(K|\mathbf{Q})$ is necessary and sufficient for $(E_K : E_{\mathcal{O}}) = 1$.

But unfortunately not so for D–type IIB fields with positive 3–rank, where this condition still implies $(E_K : E_{\mathcal{O}}) = 1$, but not conversely, as the first examples, starting with $D = 1765$, in Table B reveal, and thus is seems to be difficult to provide a general necessary and sufficient criterion for the existence of "half–units". In those cases of Table B, where the sufficient condition for $(E_K : E_{\mathcal{O}}) = 1$ is satisfied, beginning with $D = 7053$, the associated totally real cubic "auxiliary fields" L arise in triples with the same discriminant, because, together with the field L', they are subfields of a split extension (here always of type $C_3 \times C_3$), according to Theorem 4.4, 2.b. In the remaining cases, however, no cubic extension $L \mid \mathbf{Q}$ with $discr(L \mid \mathbf{Q}) = 4D$ exists and $F_2^{(3)}(K) \mid K$ is a non–split extension (here always with group C_9). Table B immediately continues Table A, but is restricted to fields whose class number is divisible by 3. Additionally we record the associated totally real cubic field L' with discriminant $discr(L' \mid \mathbf{Q}) = discr(K \mid \mathbf{Q})$, a generating polynomial $q(X) \in \mathbf{Z}[X]$ of minimal index, and the running number of $discr(L' \mid \mathbf{Q})$ in the sequence of all discriminants of totally real cubic fields.

Theorem 4.4. (Arithmetical criteria for unit group index $(E_K : E_{\mathcal{O}}) = 1$ in D–type IIB fields.)

Suppose that $D \in \mathbf{N}$, $D \equiv 5 \pmod 8$ is the radicand of a real quadratic number field $K = \mathbf{Q}(\sqrt{D})$ of D–type IIB. (Then $discr(K \mid \mathbf{Q}) = D$.) Further let $\mathcal{C}_K$ denote the (ordinary) ideal class group, $\mathcal{C}_2$ the ring class group modulo 2, F_1 the Hilbert class field, and F_2 the ring class field modulo 2 of K.

1. *The relation between the class number h_K and the ring class number modulo 2 of K, h_2, is expressed by*

$$h_2 = 3 \cdot h_K / (E_K : E_{\mathcal{O}}).$$

Hence $(E_K : E_{\mathcal{O}}) = 1 \Leftrightarrow [F_2 : F_1] = 3$.

2. *The following statements are equivalent.*

a) *There exists a totally real cubic extension $L \mid \mathbf{Q}$ with discriminant $discr(L \mid \mathbf{Q}) = 4 \cdot discr(K \mid \mathbf{Q})$.*

b) *$[F_2 : F_1] = 3$ and $Gal(F_2 \mid K)$ is a split extension of the cyclic group $Gal(F_2 \mid F_1) \simeq C_3$ by $Gal(F_1 \mid K)$.*

c) *The 3–rank of $\mathcal{C}_2$ is strictly greater than the 3–rank of $\mathcal{C}_K$.*

3. *In particular, in the case of a class number h_K coprime with 3, we have the equivalence*

$$(E_K : E_{\mathcal{O}}) = 1 \quad \Leftrightarrow \quad \exists L \mid \mathbf{Q} \quad [L : \mathbf{Q}] = 3,\ discr(L \mid \mathbf{Q}) = 4D.$$

PROOF. Denote by $\mathcal{F} = 2\mathcal{O}_K$ the conductor of the suborder $\mathcal{O}$ in the maximal order $\mathcal{O}_K$ of K. By Proposition 4.1, 1, $\mathcal{F}$ is a prime ideal in K and $U(\mathcal{O}_K/\mathcal{F}) \simeq C_3$, if $D \equiv 5 \pmod 8$.

1. For an arbitrary number field $K \mid \mathbf{Q}$ and an integral ideal $m \in \mathcal{I}_K^0$ let $K^\times(m) \subset K^\times$ (resp. $\mathcal{I}(m) \subset \mathcal{I}_K$, resp. $\mathcal{H}(m) \subset \mathcal{H}_K$) be the group of algebraic numbers (resp. ideals, resp. principal ideals) coprime with

m, $K_m^\times = \{\alpha \in K^\times(m) \,|\, \alpha \equiv 1(\operatorname{mod}{}^\times m)\}$, $i : K^\times \to \mathcal{H}_K$ the map $\alpha \to \alpha\mathcal{O}_K$, $\mathcal{R}_m = i(K_m^\times)$ the ray modulo m, $\mathcal{C}_m = \mathcal{I}(m)/\mathcal{R}_m$ the ray class group modulo m, and $E_m = E_K \cap K_m^\times$ the ray units modulo m in K.

In the special case of an ideal $m = f\mathcal{O}_K$, with $f \in \mathbf{N}$, we also define $\overline{K}_m^\times = \{\alpha \in K^\times(m) \mid \exists r \in \mathbf{Z} \quad (r,f) = 1,\ \alpha \equiv r(\operatorname{mod}{}^\times m)\}$, $\overline{\mathcal{R}}_m = i(\overline{K}_m^\times)$ the ring modulo f, $\overline{\mathcal{C}}_m = \mathcal{I}(m)/\overline{\mathcal{R}}_m$ the ring class group modulo f, and $\overline{E}_m = E_K \cap \overline{K}_m^\times$ the ring units modulo f in K. Compare with H. HASSE [14], § 10, pag. 41–42.

We derive basic connections between the class numbers $h_K = \#\mathcal{C}_K$ and $h_m = \#\mathcal{C}_m$, resp. $\overline{h}_m = \#\overline{\mathcal{C}}_m$. First $\mathcal{I}_K = \mathcal{I}(m) \cdot \mathcal{H}_K$, because any ideal class contains an ideal coprime with m, whence

$$\mathcal{I}(m)/\mathcal{H}(m) = \mathcal{I}(m)/(\mathcal{I}(m) \cap \mathcal{H}_K) \simeq \mathcal{I}(m) \cdot \mathcal{H}_K/\mathcal{H}_K = \mathcal{I}_K/\mathcal{H}_K = \mathcal{C}_K.$$

Next we move the index $(\mathcal{H}(m) : \overline{\mathcal{R}}_m)$ in the relation

$$(\mathcal{I}(m) : \overline{\mathcal{R}}_m) = (\mathcal{I}(m) : \mathcal{H}(m)) \cdot (\mathcal{H}(m) : \overline{\mathcal{R}}_m)$$

from ideals to numbers. The homomorphism i satisfies $i(K^\times(m)) = \mathcal{H}(m)$, $i^{-1}(\overline{\mathcal{R}}_m) = E_K \cdot \overline{K}_m^\times$, and therefore $K^\times(m)/E_K \cdot \overline{K}_m^\times \simeq \mathcal{H}(m)/\overline{\mathcal{R}}_m$. Moreover the index $(E_K \cdot \overline{K}_m^\times : \overline{K}_m^\times)$ in

$$(K^\times(m) : \overline{K}_m^\times) = (K^\times(m) : E_K \cdot \overline{K}_m^\times) \cdot (E_K \cdot \overline{K}_m^\times : \overline{K}_m^\times)$$

can be expressed by means of units : $E_K \cdot \overline{K}_m^\times/\overline{K}_m^\times \simeq E_K/(E_K \cap \overline{K}_m^\times) = E_K/\overline{E}_m$. Combining the isomorphisms and the index relations, which are valid equally well for the groups without bars and arbitrary $m \in \mathcal{I}_K^0$, we obtain the general formulas

$$h_m = h_K \cdot (K^\times(m) : K_m^\times)/(E_K : E_m),$$
$$\overline{h}_m = h_K \cdot (K^\times(m) : \overline{K}_m^\times)/(E_K : \overline{E}_m).$$

Finally from the isomorphism induced by the exact sequence

$$1 \to K_m^\times \to K^\times(m) \to \prod_{\mathcal{P}\in\mathbf{P}_K, \mathcal{P}\,|\,m} U(\mathcal{O}_K/\mathcal{P}^{v_\mathcal{P}(m)}) \to 1,$$

which is the local description of the congruence relation $\operatorname{mod}^\times m$, respectively from

$$1 \to K_m^\times \to \overline{K}_m^\times \to \prod_{p\in\mathbf{P}, p\,|\,f} U(\mathbf{Z}/p^{v_p(f)}\mathbf{Z}) \to 1 \text{ and}$$
$$(K^\times(m) : K_m^\times) = (K^\times(m) : \overline{K}_m^\times) \cdot (\overline{K}_m^\times : K_m^\times),$$

we conclude $(K^\times(m) : K^\times_m) = \varphi_K(m)$, and $(K^\times(m) : \overline{K}^\times_m) = \varphi_K(f\mathcal{O}_K)/\varphi(f)$, in terms of the generalized, respectively the usual Euler function.

Specialization to $K = \mathbf{Q}(\sqrt{D})$, $D \equiv 5(\mathrm{mod}\ 8)$, and $m = \mathcal{F} = 2\mathcal{O}_K$ yields: $h_2 = h_2 = 3 \cdot h_K/(E_K : E_{\mathcal{O}})$, because in this exceptional case the ray and the ring modulo 2 coincide, $\varphi_K(2\mathcal{O}_K) = \#U(\mathcal{O}_K/\mathcal{F}) = 3$, and $E_2 = \overline{E}_2 = E_{\mathcal{O}}$. Here we take into consideration that $E_{\mathcal{O}} = E_K \cap (1+\mathcal{F})$, because for a unit $\varepsilon \in E_K$ with representation $\varepsilon = \frac{1}{2}(x + y\delta)$, $x, y \in \mathbf{Z}$ we have $\varepsilon - 1 = \frac{1}{2}((x-2) + y\delta) \in \mathcal{F} = 2\mathcal{O}_K \Leftrightarrow y \equiv x - 2 \equiv x \equiv 0 \pmod 2$ $\Leftrightarrow \varepsilon \in E_{\mathcal{O}}$. Hence $(E_K : E_{\mathcal{O}}) = 1$ is equivalent with $h_2 = 3 \cdot h_K$, that is, with $[F_2 : F_1] = 3$, by class field theory.

2. According to H. Hasse [13], §§ 2–3, pag. 573–575 and [14], § 10, pag. 41–42, there exists a totally real cubic extension $L \mid \mathbf{Q}$ with discriminant $discr(L \mid \mathbf{Q}) = 2^2 \cdot discr(K \mid \mathbf{Q})$, exactly if the ring class field F_2 modulo 2 of K contains a cyclic cubic extension $N \mid K$, which is not included in the Hilbert class field F_1 of K already, and hence its corresponding idealgroup $\mathcal{R}_2 \subset H \subset \mathcal{I}(2)$ with $Gal(N \mid K) \simeq \mathcal{I}(2)/H$ has really the conductor $\mathcal{F} = 2\mathcal{O}_K$. As we are interested only in the subextensions of 3–power degree, we may restrict ourselves to the Sylow 3–subgroups of all involved groups, and thus also to the 3–class fields. Then, by Galois theory, a further equivalent condition is, that $[F_2^{(3)} : F_1^{(3)}] = 3$ and the exact sequence

$$1 \to Gal(F_2^{(3)} \mid F_1^{(3)}) \to Gal(F_2^{(3)} \mid K) \to Gal(F_1^{(3)} \mid K) \to 1$$

splits (or the same statements for the full class fields), or also, in terms of abelian 3–groups, that the 3–rank of $\mathcal{C}_2$ is strictly greater than the 3–rank of $\mathcal{C}_K$.

3. In the special case of $3 \nmid h_K$ we have $F_1^{(3)} = K$, and therefore the exact sequences in the proof of 2. split trivially. The claimed equivalence then follows from **a)** $\Leftrightarrow$ **b)** in **2.** and from **1.** □

TABLE A. (The radicands D of the first 37 D–type IIB fields with unit group index $(E_K : E_{\mathcal{O}}) = 1$.)

no.	abs.	D	factors	PF	h_K
1	5	37		−1	1
2	12	101		−1	1
3	15	141	$= 3 \cdot 47$	3	1
4	21	197		−1	1
5	28	269		−1	1
6	36	349		−1	1
7	39	373		−1	1
8	40	381	$= 3 \cdot 127$	−3	1
9	41	389		−1	1
10	51	485	$= 5 \cdot 97$	−1	2
11	58	557		−1	1
12	60	573	$= 3 \cdot 191$	3	1
13	70	677		−1	1
14	72	701		−1	1
15	73	709		−1	1
16	78	757		−1	1
17	80	781	$= 11 \cdot 71$	−11	1
18	84	813	$= 3 \cdot 271$	−3	1
19	86	829		−1	1
20	90	877		−1	1
21	91	885	$= 3 \cdot 5 \cdot 59$	15	2
22	93	901	$= 17 \cdot 53$	−1	4
23	95	933	$= 3 \cdot 311$	3	1
24	100	973	$= 7 \cdot 139$	7	1
25	102	997		−1	1
26	118	1149	$= 3 \cdot 383$	3	1
27	119	1157	$= 13 \cdot 89$	−1	2
28	121	1173	$= 3 \cdot 17 \cdot 23$	−17	2
29	125	1213		−1	1
30	134	1293	$= 3 \cdot 431$	3	1
31	135	1301		−1	1
32	144	1389	$= 3 \cdot 463$	−3	1
33	146	1405	$= 5 \cdot 281$	5	2
34	164	1605	$= 3 \cdot 5 \cdot 107$	−5	2
35	165	1613		−1	1
36	176	1717	$= 17 \cdot 101$	17	2
37	180	1757	$= 7 \cdot 251$	7	1

TABLE A. (The radicands D of the first 37 D–type IIB fields with unit group index $(E_K : E_{\mathcal{O}}) = 1$.)

no.	$d(L\|\mathbf{Q})$	$p(X)$	no.
1	148	$X^3 - X^2 - 3X + 1$	3
2	404	$X^3 - X^2 - 5X - 1$	10
3	564	$X^3 - X^2 - 5X + 3$	13
4	788	$X^3 - X^2 - 7X - 3$	21
5	1076	$X^3 - 8X + 6$	29
6	1396	$X^3 - X^2 - 7X + 5$	40
7	1492	$X^3 - X^2 - 9X - 5$	44
8	1524	$X^3 - X^2 - 7X + 1$	46
9	1556	$X^3 - X^2 - 9X + 11$	47
10	1940	$X^3 - 8X + 2$	59
11	2228	$X^3 - X^2 - 13X + 9$	69
12	2292	$X^3 - X^2 - 13X + 1$	72
13	2708	$X^3 - X^2 - 11X - 7$	85
14	2804	$X^3 - X^2 - 9X - 1$	88
15	2836	$X^3 - X^2 - 9X + 7$	90
16	3028	$X^3 - 10X + 6$	98
17	3124	$X^3 - 16X + 12$	99
18	3252	$X^3 - X^2 - 9X + 3$	106
19	3316	$X^3 - 16X + 22$	110
20	3508	$X^3 - X^2 - 11X + 13$	115
21	3540	$X^3 - X^2 - 15X - 15$	116
22	3604	$X^3 - X^2 - 17X + 31$	122
23	3732	$X^3 - X^2 - 13X + 19$	125
24	3892	$X^3 - 10X + 2$	131
25	3988	$X^3 - 16X + 4$	138
26	4596	$X^3 - X^2 - 11X - 3$	154
27	4628	$X^3 - X^2 - 13X - 9$	156
28	4692	$X^3 - X^2 - 17X - 3$	160
29	4852	$X^3 - X^2 - 17X + 13$	168
30	5172	$X^3 - X^2 - 21X + 33$	177
31	5204	$X^3 - X^2 - 17X + 5$	178
32	5556	$X^3 - X^2 - 19X - 23$	196
33	5620	$X^3 - X^2 - 11X + 1$	198
34	6420	$X^3 - X^2 - 21X - 15$	231
35	6452	$X^3 - X^2 - 13X + 15$	232
36	6868	$X^3 - X^2 - 17X - 17$	249
37	7028	$X^3 - 20X + 12$	254

TABLE B. (The radicands D of the first 32 D–type IIB fields with unit group index $(E_K : E_{\mathcal{O}}) = 1$ and with positive 3–rank.)

no.	abs.	D	factors	PF	$q(X)$
38	181	1765	$= 5 \cdot 353$	-1	$X^3 - X^2 - 11X + 16$
42	194	1901		-1	$X^3 - X^2 - 9X - 4$
49	215	2101	$= 11 \cdot 191$	-11	$X^3 - X^2 - 11X - 8$
75	298	2917		-1	$X^3 - X^2 - 13X + 20$
100	394	3877		-1	$X^3 - X^2 - 13X - 10$
126	500	4933		-1	$X^3 - X^2 - 11X - 2$
137	534	5261		-1	$X^3 - X^2 - 19X + 36$
142	556	5477		-1	$X^3 - X^2 - 18X - 4$
154	596	5853	$= 3 \cdot 1951$	-3	$X^3 - X^2 - 13X + 16$
182	702	6901	$= 67 \cdot 103$	-67	$X^3 - X^2 - 25X - 2$
187	717	7053	$= 3 \cdot 2351$	3	$X^3 - X^2 - 23X + 48$
219	852	8373	$= 3 \cdot 2791$	-3	$X^3 - X^2 - 13X - 2$
226	871	8581		-1	$X^3 - 16X + 17$
228	873	8597		-1	$X^3 - X^2 - 22X - 12$
234	893	8789	$= 11 \cdot 17 \cdot 47$	47	$X^3 - 14X + 9$
235	898	8837		-1	$X^3 - X^2 - 27X + 18$
237	905	8909	$= 59 \cdot 151$	59	$X^3 - X^2 - 25X + 54$
249	944	9293		-1	$X^3 - 20X + 29$
250	945	9301	$= 71 \cdot 131$	-71	$X^3 - X^2 - 21X - 26$
272	1023	10069		-1	$X^3 - X^2 - 22X + 20$
278	1050	10333		-1	$X^3 - 25X + 28$
289	1083	10661	$= 7 \cdot 1523$	-7	$X^3 - 26X + 47$
290	1089	10733		-1	$X^3 - 14X + 3$
302	1143	11293	$= 23 \cdot 491$	-23	$X^3 - X^2 - 23X + 46$
320	1213	11965	$= 5 \cdot 2393$	-1	$X^3 - 28X + 53$
363	1373	13549	$= 17 \cdot 797$	-1	$X^3 - X^2 - 31X + 4$
379	1459	14397	$= 3 \cdot 4799$	3	$X^3 - X^2 - 15X + 6$
386	1487	14653		-1	$X^3 - 25X + 12$
410	1573	15501	$= 3 \cdot 5167$	-3	$X^3 - X^2 - 29X + 66$
414	1590	15661		-1	$X^3 - X^2 - 35X + 48$
415	1598	15757	$= 7 \cdot 2251$	-7	$X^3 - X^2 - 26X + 28$
427	1629	16045	$= 5 \cdot 3209$	-5	$X^3 - X^2 - 30X + 52$

TABLE B. (The radicands D of the first 32 D–type IIB fields with unit group index $(E_K : E_{\mathcal{O}}) = 1$ and with positive 3–rank.)

no.	no.	$d(L\|\mathbf{Q})$	$p(X)$	no.
38	52			
42	56			
49	66			
75	92			
100	129			
126	173			
137	179			
142	192			
154	210			
182	251			
187	256	28212	$X^3 - X^2 - 37X - 47$	1214
			$X^3 - X^2 - 53X + 153$	1215
			$X^3 - X^2 - 41X + 93$	1216
219	316			
226	325			
228	326			
234	335			
235	338			
237	341			
249	355			
250	357			
272	385			
278	399	41332	$X^3 - X^2 - 35X - 59$	1842
			$X^3 - X^2 - 53X + 111$	1843
			$X^3 - X^2 - 23X - 11$	1844
289	410			
290	414			
302	442			
320	478	47860	$X^3 - X^2 - 61X - 185$	2156
			$X^3 - X^2 - 51X + 81$	2157
			$X^3 - X^2 - 45X + 97$	2158
363	535			
379	579	57588	$X^3 - 72X + 190$	2647
			$X^3 - X^2 - 71X + 45$	2648
			$X^3 - X^2 - 53X + 75$	2649
386	589			
410	625	62004	$X^3 - X^2 - 57X - 141$	2862
			$X^3 - X^2 - 59X + 189$	2863
			$X^3 - X^2 - 25X + 19$	2864
414	634	62644	$X^3 - X^2 - 37X - 61$	2905
			$X^3 - 46X + 110$	2906
			$X^3 - X^2 - 25X - 1$	2907
415	640	63028	$X^3 - X^2 - 43X + 113$	2919
			$X^3 - 76X + 236$	2920
			$X^3 - 40X + 12$	2921
427	652			

§5. Generators of ambiguous principal ideals

In this paragraph the following problems for real quadratic number fields $K = Q(\sqrt{D})$ with C_2-group $G = Gal(K|Q) = \langle\tau\rangle$ will be discussed.

I. The number a_K (resp. a_K^0) of primitive ambiguous ideals (resp. principal ideals) in K.

The solution of this invariance problem is well known. According to D. Hilbert [15], there is only one possibility $a_K = (\mathcal{I}_K^G : \mathcal{I}_Q) = 2^{t+w}$, where $\mathcal{I}_Q = \mathcal{H}_Q \simeq Q^+$ and $t + w$ is the number of prime divisors of $R_{K|Q}$ ([15], §73, pag. 302-303), and there are two possible values, $a_K^0 = (\mathcal{H}_K^G : \mathcal{H}_Q) \in \{2,4\}$ ([15], §75, pag. 303-305). In Theorem 5.1 we compile a list of necessary and sufficient conditions for each of the two values of a_K^0, leading to a subdivision of real quadratic number fields into two principal factor types (PF-types). See §6, Tables 3,4 for the frequencies and statistics of these types.

More detailed, we are interested in the possibilities for the norms of generators of primitive ambiguous principal ideals in $\mathcal{O}_K$. In the Remark concerning the formalism of discriminantal divisors, immediately after this summary, we shall see that, aside from the trivial couple $\{1, -D\}$, there are on principle $2^{t+w} - 1$ possible couples $\{2^v d_1, -2^v d_2\}$ ($v \in \{0,1\}, d_1|D$, $d_2 = D/d_1$) of non-trivial discriminantal principal factor norms in every real quadratic field and Theorem 5.1 shows that the actual couple in PF-type II fields (where $a_K^0 = 2$) is $\{D, -1\}$, whereas in PF-type I fields (with $a_K^0 = 4$) the actual couple is one of the remaining $2^{t+w} - 2$ possible couples, different from $\{D, -1\}$. Thus there arises the need for

II. Arithmetical criteria for the actual occurrence of any one of the possible couples of non-trivial discriminantal principal factor norms.

The question, which of the $2^{t+w} - 1$ possible couples actually consists of norms of algebraic integers in K, comprises the distinction of PF-types and can be answered by L. Rédei's theory [26], [27], [28], if the structure of the restricted (narrower) 2-class group $\mathcal{C}_K^{(2)+}$ of K is known. For actual computations, handy versions of this theory have developed by P. MORTON [23] and J. C. LAGARIAS [20]. Proposition 5.2 reminds of a simple special case, in view of D-type IB fields.

III. The indirect computation of the fundamental unit $\epsilon_0 > 1$ of K by seeking a radical of a multiple of the unit in the maximal order or also in the suborder, if $D \equiv 1 (\mathrm{mod}\ 4)$.

As the continued fraction algorithm determines exactly all the lattice minima among the algebraic integers in an order, according to Corollary 3.4, the question arises, which conditions must be satisfied by the radicand D, in order that a radical of a multiple of the fundamental unit appears as a lattice minimum in the maximal order $\mathcal{O}_K$. Generally, in arbitrary algebraic number fields, radicals of multiples of units are algebraic integers, composed of certain "highly ramified" prime ideals, more exactly, of prime ideals with non-coprime ramification exponents, as is shown by D. C. MAYER [21], Proposition 4.1 and Theorem 4.3. Like in any cyclic extension of prime degree, in a quadratic field K every ramified prime ideal $\mathcal{P}$ is already totally ramified and has maximal $e_{K|Q}(\mathcal{P}) = 2$, whence $\mathcal{I}_K^G/\mathcal{I}_Q \simeq C_2^{t+w}$, and radicals of multiples Corollary 5.8 only a generator with the minimal (that is, absolutely smaller) norm in the actual couple can be a lattice minimum in $\mathcal{O}_K$. Fortunately, Theorem 5.11 brings the concluding result that in an arbitrary real quadratic field every algebraic integer with minimal discriminantal principal factor norm is a minimal point in the maximal order $\mathcal{O}_K$, and the existence of a non-trivial generator among the minima of the suborder $\mathcal{O}$ in the case of a D-type II field of PF-type I, is warranted by Theorem 5.12.

Remark. Similarly as with the problems in § 4, the relations in an arbitrary order $\mathcal{O}$ of a real quadratic field can be quite different from those in the maximal order $\mathcal{O}_K$ and in the particular suborder $\mathcal{O} = \mathcal{O}_2$, if $D \equiv 1 (\mathrm{mod}\ 4)$. They are heavily dependent on the conductor $cond(\mathcal{O}) = f\mathcal{O}_K$ of the order. The investigation of these phenomena will be the topic of a subsequent paper.

Remark. (The formalishm of discriminantal divisors in real quadratic number fields.)

Let $D \in \mathbf{N}, D \geq 2$ be a squarefree radicand, and $d \in \mathbf{Z}$, $d|D$ a *discriminantal divisor* for the real quadratic number field $K = \mathbf{Q}(\sqrt{D})$, more exactly, a divisor of the ramification quantity $R_{K|\mathbf{Q}}$ of K. In contrast to pure cubic fields, where the sign of norms is inessential because of the antisymmetry of $N_{K|\mathbf{Q}}$ with respect to the origin, $N_{K|\mathbf{Q}}(-\alpha) = -N_{K|\mathbf{Q}}(\alpha)$, the individual norm -1 must be treated as a nontrivial dicriminantal divisor in real quadratic fields because $N_{k|\mathbf{Q}}$ is symmetric, $N_{K|\mathbf{Q}}(-\alpha) = N_{K|\mathbf{Q}}(\alpha)$.

The positive integers

$$d_1 = \prod\{p \in \mathbf{P} \mid v_p(D) = 1,\ v_p(d) = 1\},$$
$$d_2 = \prod\{p \in \mathbf{P} \mid v_p(D) = 1,\ v_p(d) = 0\}$$

are called *canonical factors* of the radicand D with respect to the discriminantal divisor d. By means of these numbers, D and d have representations in the form

$$D = d_1 d_2, \quad d = \pm d_1.$$

Further $R_{K|\mathbf{Q}} = 2^w d_1 d_2$, where $w \in \{0,1\}$ and $w = 1$, iff $D \equiv 3(\mathrm{mod}\ 4)$. (The ramification of the rational prime 2 causes some complications in fields of D-type IB, notationally as well as theoretically.) We declare the *normalized radical* of K with respect to the discriminantal divisor d to be

$$\gamma = \gamma_d = \delta / d_1 (> 0), \quad \text{where } \delta = \sqrt{D}.$$

For a numeration of the possibilities for discriminantal divisors, we need a more explicit description. Let $t = \#\{p \in \mathbf{P} \mid v_p(D) > 0\}$ and suppose that $p_1, \dots, p_t \in \mathbf{P}$ are the prime factors of D, then $R_{K|\mathbf{Q}} = = 2^w p_1 \cdots p_t$, or in uniform notation $R_{K|\mathbf{Q}} = p_1 \cdots p_{t+w}$, where we set $P_{t+1} = 2$.
If we define the multiplicative subgroup $\mathcal{D} = \langle -1 \rangle \times \langle p_1, \dots, p_{t+w} \rangle < \mathbf{Q}^\times$, then, as $(\mathbf{Q}^\times, \times) \simeq ((\mathbf{Z}/2\mathbf{Z}) \times \mathbf{Z}^{(P)}, +)$, we have $\mathcal{D} \simeq (\mathbf{Z}/2\mathbf{Z}) \times \mathbf{Z}^{t+w}$, $\mathcal{D}^2 \simeq (2\mathbf{Z})^{t+w}$, and hence the ***group of discriminantal divisors*** for K,

$$\begin{aligned} \mathcal{D}/\mathcal{D}^2 &\simeq ((\mathbf{Z}/2\mathbf{Z}) \times \mathbf{Z}^{t+w})/(2\mathbf{Z})^{t+w} \simeq \\ &\simeq (\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z})^{t+w} \simeq (\mathbf{Z}/2\mathbf{Z})^{t+w+1}, \end{aligned}$$

is an elementary abelian 2-group of the order $\#(\mathcal{D}/\mathcal{D}^2) = 2^{t+w+1}$. Canonical representatives for $\mathcal{D}/\mathcal{D}^2$ are the 2^{t+w+1} signed divisors of $R_{K|\mathbf{Q}}$.

We call an integer $2^v d$ with $d \in \mathbf{Z}$, $d | D$ and with $v \in \{0,1\}$, where $v = 1$ at most, if $D \equiv 3(\mathrm{mod}\ 4)$, a *discriminantal principal factor* for K, iff $\exists\, \alpha \in \mathcal{O}_K^\times \ N_{K|\mathbf{Q}}(\alpha) = 2^v d$. Because then on the one hand, $2^v d = \pm p_1^{v_1} \cdots p_{t+w}^{v_{t+w}} \mid R_{K|\mathbf{Q}}$ with certain exponents $v_1, \dots, v_t \in \{0,1\}$, $v_{t+1} = v$, and $R_{K|\mathbf{Q}} \mid discr(K|\mathbf{Q})$, and on the other hand α is the generator of an *ambiguous principal ideal* $\alpha\mathcal{O}_K \in \mathcal{H}_K^G$ (invariant under $G = = Gal(K|\mathbf{Q})$), that is, of a *differental principal factor* in K (principal ideal divisor of the absolute different of K), $\alpha\mathcal{O}_K = \mathcal{P}_1^{v_1} \cdots \mathcal{P}_{t+w}^{v_{t+w}} \mid diff(K|\mathbf{Q})$, denoting by $\mathcal{P}_1, \dots, \mathcal{P}_{t+w} \in \mathbf{P}_K$ the prime ideals lying over the ramified primes $p_1, \dots, p_{t+w}$. In particular, the discriminantal principal factor is called *escalatory*, iff $v = v_{t+1} = 1$ (and hence $D \equiv 3(\mathrm{mod}\ 4)$). The *complementary* discriminantal and differental divisors for $\pm 2^v d_1$ and α, respectively, are $\mp 2^v d_2 = \mp p_1^{1-v_1} \cdots p_t^{1-v_1} \cdot p_{t+w}^{v_{t+w}}$ and $(\alpha\delta/d_1)\mathcal{O}_K = = \mathcal{P}_1^{1-v_1} \cdots \mathcal{P}_t^{1-v_t} \cdot \mathcal{P}_{t+w}^{v_t+w}$, respectively, because $\delta\mathcal{O}_K = \mathcal{P}_1 \cdots \mathcal{P}_t$.

Always 1 and $-D$ are the *trivial* discriminantal principal factors, coming from rational units and from radicals: $1 = N_{K|\mathbf{Q}}(1)$, $-D = \sqrt{D} \cdot \cdot (-\sqrt{D}) = \delta \cdot \tau(\delta) = N_{K|\mathbf{Q}}(\delta)$. Therefore we are interested in the factor group $(\mathcal{D}/\mathcal{D}^2)\ /\ \langle -D \rangle$ of $\mathcal{D}/\mathcal{D}^2$ with respect to the subgroup generated by $-D$ (more exactly, by the element $-D \bmod \mathcal{D}^2$ of order 2),

$\langle -D\rangle = \{1, -D\}$. Then $2^v d\langle -D\rangle = \{\pm 2^v d_1, \mp 2^v d_2\}$ is the *coset*, generated by $2^v d$, of $\langle -D\rangle$ in $\mathcal{D}/\mathcal{D}^2$. These cosets of the *trivial couple* $\{1, -D\}$ in $\mathcal{D}/\mathcal{D}^2$ are called the *possible couples* of non-trivial discriminantal principal factors. The total number of cosets of $\langle -D\rangle$ in $\mathcal{D}/\mathcal{D}^2$ is $2^{t+w+1}/2 = 2^{t+w}$ and the number of possible couples of non-trivial discriminantal principal factors is $2^{t+w} - 1 = \frac{1}{2}(2^{t+w+1} - 2)$. Compare also with P. Barrucand and H. Cohn [1], 7-10, and L. Rédei [28], 31-33, for the notation.

In every real quadratic field there exists exactly one *actual couple* of non-trivial discriminantal principal factors, according to the following theorem.

Theorem 5.1. (Classification of real quadratic number fields, according to the number a_K^0 of primitive ambiguous principal ideals in K.)

Let $K = \mathbf{Q}(\sqrt{D})$ be a real quadratic number field with C_2-group $G = Gal(K|\mathbf{Q}) = \langle\tau\rangle$, $\tau(\delta) = -\delta$. Further let $\epsilon_0 \in E_K$ be an arbitrary fundamental unit of K, that is, $E_K = \langle -1, \epsilon_0\rangle$.
There are the following principal factor types or PF-types of real quadratic number fields:

1. *K is of PF-type I, that is, K has non-trivial ambiguous principal ideals, iff one of the following equivalent conditions is satisfied:*
   - *(1) The period length of the continued fraction expansion of $\sqrt{D}$ (and also of $\frac{1}{2}(1+\sqrt{D})$ in the case $D \equiv 1(mod\ 4)$) is even, that is, $PL(\mathcal{O}) \equiv PL(\mathcal{O}_K) \equiv 0(mod\ 2)$.*
   - *(2) $N_{k|\mathbf{Q}}(\epsilon_0) = +1$.*
   - *(3) $\forall \epsilon \in E_K \quad N_{K|\mathbf{Q}}(\epsilon) = +1$, that is, $N_{K|\mathbf{Q}}(E_K) = \{1\}$.*
   - *(4) The group of relative units in K is $E_{K|\mathbf{Q}} = E_K$.*
   - *(5) $E_K = \langle -1, \epsilon_0\rangle_G$ is non-cyclic as a G-module.*
   - *(6) $E_K^{1-\tau} = \langle \epsilon_0^2\rangle$.*
   - *(7) $\exists\, \alpha \in \mathcal{O}_K^\times \quad \epsilon_0 = \alpha^{1-\tau} = \alpha^2 \ /\ N_{K|\mathbf{Q}}(\alpha),\ |N_{K|\mathbf{Q}}(\alpha)| \notin \{1, D\}$.*
   - *(8) $\exists\, m \in \mathbf{Z}^\times\ \exists\, \alpha \in K^\times\ m\cdot\epsilon_0 = \alpha^2$.*
   - *(9) $\exists\, \alpha \in \mathcal{O}_K^\times\ N_{K|\mathbf{Q}}(\alpha)|R_{k|\mathbf{Q}},\ |N_{K|\mathbf{Q}}(\alpha)| \notin \{1, D\}$.*
   - *(10) The actual couple $\{2^v d_1, -2^2 d_2\}$ of non-trivial discriminantal principal factors is different from $\{D, -1\}$.*
   - *(11) The solvable anti-Pellian ("singular") equation is $d_1 X^2 - d_2 Y^2 = 2^v$, resp. $X^2 - DY^2 = 2^v d_1$, resp. $X^2 - DY^2 = -2^v d_2$, where neither $2^v d_1 = 1$ nor $2^v d_2 = 1$.*
   - *(12) $\mathcal{H}_K^G/\mathcal{H}_\mathbf{Q} \simeq E_{K|\mathbf{Q}}/E_K^{1-\tau} \simeq C_2 \times C_2$, that is, $a_K^0 = 4$. More explicitly, aside from the two trivial ambiguous principal ideals, $\mathcal{O}_K$, $\delta\mathcal{O}_K = \mathcal{P}_1 \cdots \mathcal{P}_t$, there are also two non-trivial ambiguous principal ideals, $\alpha\mathcal{O}_K = \mathcal{P}_1^{v_1} \cdots \mathcal{P}_{t+w}^{v_{t+w}}$, $(\alpha\delta/d_1)\mathcal{O}_K = \mathcal{P}_t^{1-v_1} \cdots \cdot\mathcal{P}_t^{1-v_t} \cdot \mathcal{P}_{t+w}^{v_{t+w}}$, where $v_1 \ldots, v_{t+w} \in \{0, 1\}$ and $d_1 = p_1^{v_1} \cdots p_t^{v_t}$.*

2. *K is of PF-type II, that is, K has only the trivial ambiguous principal ideals, iff one of the following equivalent conditions is satisfied:*
   (1) *The period length of the continued fraction expansion of $\sqrt{D}$ (and also of $\frac{1}{2}(1+\sqrt{D})$ in the case $D \equiv 1(\mathit{mod}\ 4)$) is odd, that is, $PL(\mathcal{O}) \equiv PL(\mathcal{O}_K) \equiv 1(\mathit{mod}\ 2)$.*
   (2) $N_{K|\mathbf{Q}}(\epsilon_0) = -1$.
   (3) $\exists\, \epsilon \in E_K \quad N_{K|\mathbf{Q}}(\epsilon) = -1$, *that is,* $N_{K|\mathbf{Q}}(E_K) = \{-1, 1\}$.
   (4) *The group of relative units in K is $E_{K|\mathbf{Q}} = \langle -1, \epsilon_0^2 \rangle$.*
   (5) *$E_K = \langle \epsilon_0 \rangle_G$ is cyclic as a G-module.*
   (6) $E_K^{1-\tau} = \langle -\epsilon_0^2 \rangle$.
   (7) $\forall\, \alpha \in \mathcal{O}_K^\times \quad \epsilon_0 \neq \alpha^{1-\tau} = \alpha^2 \ / \ N_{K|\mathbf{Q}}(\alpha)$.
   (8) $\forall m \in \mathbf{Z}^\times \ \forall \alpha \in K^\times \ m \cdot \epsilon_0 \neq \alpha^2$.
   (9) $\forall\, \alpha \in \mathcal{O}_K^\times \quad (N_{K|\mathbf{Q}}(\alpha) | R_{K|\mathbf{Q}} \Longrightarrow |N_{K|\mathbf{Q}}(\alpha)| \in \{1, D\})$.
   (10) *The actual couple $\{2^v d_1, -2^v d_2\}$ of non-trivial discriminantal principal factors is $\{D, -1\}$.*
   (11) *The solvable anti-Pellian ("singular") equation is $DX^2 - Y^2 = 1$, resp. $X^2 - DY^2 = D$, resp. $X^2 - DY^2 = -1$ (the Pellian minus equation).*
   (12) *$\mathcal{H}_K^G / \mathcal{H}_\mathbf{Q} \simeq E_{K|\mathbf{Q}} / E_K^{1-\tau} \simeq C_2$, that is, $a_K^0 = 2$. More explicitly, there are only the two trivial ambiguous principal ideals $\mathcal{O}_K$ and $\delta\mathcal{O}_K = \mathcal{P}_1 \cdots \mathcal{P}_t$.*

PROOF. See. O.PERRON [25], pag. 93, D. HILBERT [15], §75, 303-305, T. KUBOTA [18], 119-120, [19], pag. 66 and 69-71, P. BARRUCAND and H. COHN [1], 10-12, and H.-J. STENDER [32]. □

Proposition 5.2. (A coarse sufficient condition for PF-type I of a real quadratic field.)

Let $K = \mathbf{Q}(\sqrt{D})$ be a real quadratic field. As -1 is a quadratic non-residue for primes $p \equiv 3(\mathit{mod}\ 4)$, we obtain the following conditions for the PF-type of K:

1. *If K is of PF-type II, then $\forall p \in \mathbf{P} \setminus \{2\} \quad (p|D \Longrightarrow p \equiv 1(\mathit{mod}\ 4))$.*
2. *Hence, if $\exists p \in \mathbf{P}\ p|D,\ p \equiv 3(\mathit{mod}\ 4)$ (in particular, if K is of D-type IB, $D \equiv 3(\mathit{mod}\ 4)$), then K is of PF-type I.*

Proposition 5.3. (Ordering of the symbolic powers $|\alpha^{1-\tau}| = \alpha^2 / \ |N_{K|\mathbf{Q}}(\alpha)|$ with norm 1.)

Let $K = \mathbf{Q}(\sqrt{D})$ be a real quadratic field, $\mathcal{O}$ an order in K, $\alpha \in \mathcal{O}^\times$ and $\varphi, \psi \in Min(\mathcal{O})$.

1. *If $|\alpha| < |\varphi|$, then $\alpha^2 / |N_{K|\mathbf{Q}}(\alpha)| < \varphi^2 / |N_{K|\mathbf{Q}}(\varphi)|$.*
2. $|\psi| < |\varphi| \Longleftrightarrow \psi^2 / N_{K|\mathbf{Q}}(\psi)| < \varphi^2 / |N_{K|\mathbf{Q}}(\varphi)|$.

PROOF. **1.** If $\alpha \in \mathcal{O}$, $\alpha \neq 0$, $\varphi \in Min(\mathcal{O})$ with $|\alpha| < |\varphi|$, then $|\varphi'| < |\alpha'|$ (because otherwise φ could not be a lattice minimum in $\mathcal{O}$). Hence $0 < \alpha^2/|N_{K|\mathbf{Q}}(\alpha)| = |\alpha|/|\alpha'| < |\varphi|/|\alpha'| < \varphi|/|\varphi'| = \varphi^2/N_{K|\mathbf{Q}}(\varphi)|$.

2. The converse can be proved, only if both points are lattice minima. The proof is done by contraposition: if $|\psi| \geq |\varphi|$, then by 1. we get $\psi^2/N_{K|\mathbf{Q}}(\psi)| \geq \varphi^2/|N_{K|\mathbf{Q}}(\varphi)|$. □

Proposition 5.4. (Properties of lattice minima with discriminantal principal factor norms in real quadratic PF-type I fields.)

Let $K = \mathbf{Q}(\sqrt{D})$ be a real quadratic field and suppose that $\mathcal{O}$ is either the maximal order of K or also the suborder $\mathbf{Z} \oplus \mathbf{Z}\sqrt{D}$, if $D \equiv 1 (mod\ 4)$. Further let $\alpha \in \mathcal{O}$ be an algebraic integer, $\vartheta \in Min(\mathcal{O})$ a lattice minimum in $\mathcal{O}$, and $\epsilon_0 \in E_{\mathcal{O}}$, $\epsilon_0 > 1$ the fundamental unit in $\mathcal{O}$.

1. *The norms of primitive algebraic integers, whose symbolic $(1-\tau)$-th powers are units in $\mathcal{O}$, must be discriminantal principal factors for K, that is,*

$$\alpha^{1-\tau} = \alpha^2/N_{K|\mathbf{Q}}(\alpha) \in E_{\mathcal{O}} \text{ and}$$
$$\alpha \text{ is primitive in } \mathcal{O}_K \iff N_{K|\mathbf{Q}}(\alpha) \mid R_{K|\mathbf{Q}}.$$

In particular, for lattice minima (which are primitive, a priori) with discriminantal principal factor norms, we have:

$$N_{K|\mathbf{Q}}(\vartheta) \mid R_{K|\mathbf{Q}} \iff \vartheta^2/N_{K|\mathbf{Q}}(\vartheta) \in E_{\mathcal{O}}.$$

2. *If the lattice minimum additionally belongs to the first primitive period in $\mathcal{O}$, then*

$$N_{K|\mathbf{Q}}(\vartheta) \mid R_{K|\mathbf{Q}}, \quad 1 < \vartheta < \epsilon_0 \iff \vartheta^2/|N_{K|\mathbf{Q}}(\vartheta)| = \epsilon_0, \quad \vartheta > 0.$$

3. Among the lattice minima in the first primitive period of the 1-chain in $\mathcal{O}$ there can be at most one non-unit with discriminantal principal factor norm, that is,

$$\#\{\psi \in Min(\mathcal{O}) \mid N_{K|\mathbf{Q}}(\psi)|R_{K|\mathbf{Q}}, \quad 1 < \psi < \epsilon_0\} \leq 1.$$

4. *If $N_{K|\mathbf{Q}}(\vartheta)|R_{K|\mathbf{Q}}$, and $1 < \vartheta < \epsilon_0$, then $\vartheta^2/|N_{k|\mathbf{Q}}(\vartheta)| = \epsilon_0$, and more generally for arbitrary integers $n \in \mathbf{Z} : (\epsilon_0^n)^2/|N_{K|\mathbf{Q}}(\epsilon_0^n)| = \epsilon_0^{2n}$, $(\epsilon_0^n \cdot \vartheta)^2/|N_{K|\mathbf{Q}}(\epsilon_0^n \cdot \vartheta)| = \epsilon_0^{2n+1}$, that is, the mapping*

$$\{\psi \in Min^+(\mathcal{O}) \mid N_{K|\mathbf{Q}}(\psi)|R_{K|\mathbf{Q}}\} \to E_{\mathcal{O}}^+, \quad \psi \to \frac{\psi^2}{|N_{k|\mathbf{Q}}(\psi)|}$$

is bejective and order preserving.

PROOF. **1.** Here we make use of some general results for arbitrary algebraic number fields in [21], §4: Proposition 1 shows

$$\alpha^2/N_{K|\mathbf{Q}}(\alpha) \in E_K \Longleftrightarrow \alpha\mathcal{O}_K \in \mathcal{H}_K^G,$$

and if additionally α is primitive in $\mathcal{O}_K$, i.e., $\alpha\mathcal{O}_K$ is a primitive ambiguous principal ideal in K, then we obtain, by Theorem 3, that $N_{K|\mathbf{Q}}(\alpha) \mid R_{K|\mathbf{Q}}$, and vice versa. It only remains to show that

$$\alpha^2/N_{K|\mathbf{Q}}(\alpha) \in E_K \Longleftrightarrow \alpha^2/N_{K|\mathbf{Q}}(\alpha) \in E_{\mathcal{O}},$$

in the case of $D \equiv 1 (\mathrm{mod}\ 4)$ and $\alpha \in \mathcal{O}$. For this purpose denote $d = |N_{K|\mathbf{Q}}(\alpha)| \in \mathrm{N}$ and assume $\alpha^2/d \in E_K \subset \mathcal{O}_K$, then, as we know already, $d|R_{K|\mathbf{Q}}$ and $R_{K|\mathbf{Q}} = D$, whence $d \equiv 1(\mathrm{mod}\ 2)$. Thus d is coprime with the conductor 2 of the suborder $\mathcal{O}$, and therefore $\alpha^2 \in \mathcal{O} \cap d\mathcal{O}_K = d\mathcal{O}$, $\alpha^2/d \in \mathcal{O} \cap E_K = E_{\mathcal{O}}$. The inverse implication is trivial.

In particular, if $\vartheta \in Min(\mathcal{O})$, then ϑ is primitive in $\mathcal{O}$, according to §2, sections 2.7, Remarks.

2. If $\vartheta \in Min(\mathcal{O})$, $1 < |\vartheta| < \epsilon_0$ is a lattice minimum in the primitive period of the 1-chain of the point 1 in $\mathcal{O}$ with discriminantal principal factor norm $N_{K|\mathbf{Q}}(\vartheta)|R_{K|\mathbf{Q}}$, then by Proposition 5.3:

$$1 = 1^2/|N_{K|\mathbf{Q}}(1)| < \vartheta^2/|N_{K|\mathbf{Q}}(\vartheta)| < \epsilon_0^2/|N_{K|\mathbf{Q}}(\epsilon_0)| = \epsilon_0^2,$$

and by **1.**: $\vartheta^2/|N_{K|\mathbf{Q}}(\vartheta)| \in E_{\mathcal{O}}$. Hence, as $E_{\mathcal{O}} = \langle -1, \epsilon_0 \rangle$, we get $\exists n \in \mathbf{Z}$ $\vartheta^2/|N_{K|\mathbf{Q}}(\vartheta)| = \pm\epsilon_0^n$, where the minus sign is impossible and $0 < n < 2$, because $1 = \epsilon_0^0 < \epsilon_0^n < \epsilon_0^2$. Therefore $n = 1$, i.e., $\vartheta^2/|N_{K|\mathbf{Q}}(\vartheta)|\epsilon_0$. Conversely, if $\vartheta^2/|N_{K|\mathbf{Q}}(\vartheta)| = \epsilon_0 \in E_{\mathcal{O}}$, then by **1.**: $N_{K|\mathbf{Q}}(\vartheta)|R_{K|\mathbf{Q}}$, and by Proposition 5.3: $1 < |\vartheta| < \epsilon_0$, because if $|\vartheta| \leq 1$ or $|\vartheta| \geq \epsilon_0$, then $\vartheta^2/|N_{K|\mathbf{Q}}(\vartheta)| \leq 1^2/|N_{K|\mathbf{Q}}(1)| = 1$ or $\vartheta^2/|N_{K|\mathbf{Q}}(\vartheta)| \geq \epsilon_0^2/|N_{K|\mathbf{Q}}(\epsilon_0)| = \epsilon_0^2$, in contradiction to $1 < \epsilon_0 < \epsilon_0^2$.

3. If $\vartheta, \varphi \in Min(\mathcal{O})$ with $N_{K|\mathbf{Q}}(\vartheta)|R_{K|\mathbf{Q}}, N_{K|\mathbf{Q}}(\varphi)|R_{K|\mathbf{Q}}$, and $1 < \vartheta < \varphi < \epsilon_0$, then by **2.**: $\vartheta^2/|N_{K|\mathbf{Q}}(\vartheta)| = \varphi^2/|N_{K|\mathbf{Q}}(\varphi)| = \epsilon_0$ and therefore the two units are equal. But, according to Proposition 5.3: $1 < \vartheta^2/|N_{K|\mathbf{Q}}(\vartheta)| < \varphi^2/|N_{K|\mathbf{Q}}(\varphi)| < \epsilon_0^2$, which is a contradiction.

4. If $N_{K|\mathbf{Q}}(\vartheta)|R_{K|\mathbf{Q}}$ and $1 < \vartheta < \epsilon_0$, then we obtain by **2.**: $\vartheta^2/|N_{K|\mathbf{Q}}(\vartheta)| = \epsilon_0$. Finally the relations $(\epsilon^n \cdot \vartheta)^2/|N_{K|\mathbf{Q}}(\epsilon^n \cdot \vartheta)| = \epsilon_0^{2n+1}$ and $(\epsilon^n)^2/|N_{K|\mathbf{Q}}(\epsilon^n)| = \epsilon_0^{2n}$, together with Proposition 5.3,2 and the natural action of $E_{\mathcal{O}}^+$ on $Min^+(\mathcal{O})$, §2, section 6, establish the order preserving bijection. □

Corollary 5.5. (A second version of the unit algorithm: the indirect calculation of the fundamental unit in fields of PF-type I.)

Under the same assumptions as in Proposition 5.4, when there is a non-unit $\alpha \in Min(\mathcal{O}) \setminus E_{\mathcal{O}}$ among the lattice minima in $\mathcal{O}$ with discriminantal principal factor norm $N_{K|\mathbf{Q}}(\alpha) \mid R_{K|\mathbf{Q}}$, then the fundamental unit ϵ_0 of $\mathcal{O}$ has the repsentation

$$\epsilon_0 = \frac{\vartheta_0^2}{|N_{K|\mathbf{Q}}(\vartheta_0)|},$$

where $\vartheta_0 = \nu_1^j(1) \in Min(\mathcal{O})$ with $j = min\{i \geq 1 \mid N_{K|\mathbf{Q}}\nu_1^i(1)|R_{K|\mathbf{Q}}\}$. In fact, the position of ϑ_0 in the first primitive period $1 < \nu_1(1) < \nu_1^2(1) < < \ldots < \nu_1^{PL(\mathcal{O})(1)} = \epsilon_0$ of $Min(\mathcal{O})$ can be specified definitively:

$$\exists\, m \in \mathbf{N} \;\; PL(\mathcal{O}) = 2m \equiv 0 (mod\ 2), \quad \vartheta_0 = \nu_1^m(1),$$

that is, ϑ_0 is situated exactly in the middle of the first primitive period in $\mathcal{O}$.

PROOF. As α is a nonunit, there exists a uniquely determined exponent $n \in \mathbf{Z}$, such that $\epsilon_0^n < |\alpha| < \epsilon_0^{n+1}$, respectively $1 < \vartheta < \epsilon_0$, where we put $\vartheta = |\alpha| \cdot \epsilon_0^{-n}$. The natural operation of $E_{\mathcal{O}}^+$ on $Min^+(\mathcal{O})$ (see. §2, section 6) causes ϑ to be a lattice minimum in $Min^+(\mathcal{O})$ again, and $N_{K|\mathbf{Q}}(\vartheta) = |N_{K|\mathbf{Q}}(\alpha)|$. From this fact, together with $N_{K|\mathbf{Q}}(\vartheta) \mid R_{K|\mathbf{Q}}$, we get $\vartheta^2/|N_{K|\mathbf{Q}}(\vartheta)| = \epsilon_0$ by **4.** Further, the (metrical) minimality of

$$\vartheta_0 = \min\{\psi \in Min(\mathcal{O}) \mid \psi > 1,\ N_{K|\mathbf{Q}}(\psi)|R_{K|\mathbf{Q}}\}$$

implies $1 < \vartheta_0 \leq \vartheta < \epsilon_0$, but, in view of **3.**, $\vartheta_0 < \vartheta$ is impossible and thus we must have $\vartheta_0 = \vartheta$. The rest follows from Theorem 5.1,1.(1), Proposition 5.4,3 and the symmetry property of the norms of lattice minima, §2, section 6, Remark. □

Remark. For fields of PF-type II, the unit algorithm can also be terminated in the middle of the first primitive period, because of the symmetry property of the lattice minima (see H. C. WILLIAMS and J. BROERE [36], pag. 888).

Proposition 5.6. (Conclusions from certain divisibility properties of the norms of algebraic integers.)

Let $K = \mathbf{Q}(\sqrt{D})$ be of arbitrary D-type, *$d \in \mathbf{N}$, $\alpha \in \mathcal{O}_K$ an algebraic integer, and $x, y \in \mathbf{Z}$, $n \in \{1, 2\}$, such that the representation $\alpha = \frac{1}{n}(x + y\sqrt{D})$ is reduced, that is, $gcd(n, x, y) = 1$.*

1. *If d divides α in $\mathcal{O}_K$ (that is, $\alpha \in d\mathcal{O}_K$), then $d^2|N_{K|\mathbf{Q}}(\alpha)$.*

2. *If $d|D$, then d is squarefree and*

$$d|N_{K|\mathbf{Q}}(\alpha) \Longrightarrow d|x.$$

3. *$d|D$, then*

$$d^2|N_{K|\mathbf{Q}}(\alpha) \Longrightarrow \alpha \in d\mathcal{O}_K, \text{ in particular, } d\,|\,gcd(x,y).$$

4. *More generally, if d contains only prime factors which are undecomposed, that is, ramified or inert, in K (in particular, if $d|R_{K|\mathbf{Q}}$), then:*

$$d^2|N_{K|\mathbf{Q}}(\alpha) \Longrightarrow \alpha \in d\mathcal{O}_K.$$

As a special case (cfr. Prop. 4.1,5.b), if $D \equiv 5(mod\ 8)$, then:

$$4|N_{K|\mathbf{Q}}(\alpha) \Longrightarrow \alpha \in 2\mathcal{O}_K.$$

PROOF. **1.** If $\alpha \in d\mathcal{O}_K$, then there exists $\beta \in \mathcal{O}_K$, such that $\alpha = d\beta$ and therefore $N_{K|\mathbf{Q}}(\alpha) = d^2 N_{K|\mathbf{Q}}(\beta)$ with $N_{K|\mathbf{Q}}(\beta) \in \mathbf{Z}$, that is, d^2 divides $N_{K|\mathbf{Q}}(\alpha)$.

2. Suppose $d|D$, then d is squarefree, because D is squarefree.
$N_{K|\mathbf{Q}}(\alpha) = N_{K|\mathbf{Q}}(\frac{1}{n}(x+y\delta)) = \frac{1}{n^2}(x^2 - Dy^2) \in \mathbf{Z}$ and hence
$d|N_{K|\mathbf{Q}}(\alpha) \Longrightarrow d|n^2 N_{K|\mathbf{Q}}(\alpha) \Longrightarrow d|x^2 = (x^2 - Dy^2) + Dy^2 \Longrightarrow d|x$.

3. If even $d^2|N_{K|\mathbf{Q}}(\alpha)$, then $d|N_{K|\mathbf{Q}}(\alpha)$ and, by **2.**, $d|x$, $d^2|x^2$. Therefore, as d is squarefree, $d^2|Dy^2 = -(x^2 - Dy^2) + x^2 \Longrightarrow d|y^2 \Longrightarrow d|y$, whence $d\,|\,\gcd(x,y)$ and $\alpha = d \cdot \frac{1}{n}(x/d + y/d\delta) \in d\mathcal{O}_K$, because, in the case $n = 1 : x/d + y/d\delta \in \mathbf{Z} \oplus \mathbf{Z}\delta = \mathcal{O} \subset \mathcal{O}_K$, and in the case $n = 2$ (and hence $D \equiv 1(\text{mod } 4)$): $x/d \equiv y/d \equiv 1(\text{mod } 2)$ and $\frac{1}{2}(x/d + y/d\delta) \in \mathcal{O}_K$.

4. To realize, that d must not be divisible by splitting primes, suppose generally $d = \Pi_{p\in\mathbf{P}}\, p^{w_p}$, then $d^2 = \Pi_{p\in\mathbf{P}}\, p^{2w_p}$ and $d\mathcal{O}_K = \Pi_{p\in\mathbf{P}}(\Pi_{\mathcal{P}|p}\, \mathcal{P}^{e(\mathcal{P}|p)})^{w_p}$. The statement is trivial for $\alpha = 0$. For $\alpha \in \mathcal{O}_K^\times$ let $\alpha\mathcal{O}_K = \Pi_{\mathcal{P}\in\mathbf{P}_K}\mathcal{P}^{v_\mathcal{P}}$, then $\mathcal{N}_{K|\mathbf{Q}}(\alpha\mathcal{O}_K) = \Pi_{p\in\mathcal{P}}(\Pi_{\mathcal{P}|p} p^{f(\mathcal{P}|p)v_\mathcal{P}})$ and on the other hand $= N_{K|\mathbf{Q}}\ (\alpha)\mathcal{O}_K = \Pi_{p\in\mathbf{P}} p^{\sum_{\mathcal{P}|p} f(\mathcal{P}|p)v_\mathcal{P}}$. Now $\alpha \in d\mathcal{O}_K \Longleftrightarrow \alpha\mathcal{O}_K \subset d\mathcal{O}_K \Longleftrightarrow \exists\, \mathcal{A} \in \mathcal{H}_K^0\ \Pi_{\mathcal{P}\in\mathbf{P}_K}\mathcal{P}^{v_\mathcal{P}} = \mathcal{A} \cdot \Pi_{p\in\mathbf{P}}(\Pi_{\mathcal{P}|p}\mathcal{P}^{e(\mathcal{P}|p)w_p}) \Longleftrightarrow \forall p \in \mathbf{P}\ \forall \mathcal{P}|p\ v_p \geq e(\mathcal{P}|p)w_p$ and $d^2|N_{K|\mathbf{Q}}(\alpha) \Longleftrightarrow \Pi_{p\in\mathbf{P}}\, p^{\sum_{\mathcal{P}|p} f(\mathcal{P}|p)v_p} = = n \cdot \Pi_{p\in\mathbf{P}}\, p^{2w_p} \Longleftrightarrow \forall p \in \mathbf{P} \quad \sum_{\mathcal{P}|p} f(\mathcal{P}|p)v_\mathcal{P} \geq 2w_p$. Finally for $p \in \mathbf{P}$:

a) if p remains (totally) inert, $f(\mathcal{P}|p) = 2$, $e(\mathcal{P}|p) = 1$, then $f(\mathcal{P}|p)v_p = = 2v_p \geq 2w_p$, resp., $v_p \geq w_p \Longrightarrow v_p \geq e(\mathcal{P}|p)w_p$.

b) if p is (totally) ramified, $f(\mathcal{P}|p) = 1$, $e(\mathcal{P}|p) = 2$, then also $f(\mathcal{P}|p)v_p = = v_p \geq 2w_p \Longrightarrow v_\mathcal{P} \geq e(\mathcal{P}|p)w_p$. Hence, if p is not decomposed, i.e.,

$e(\mathcal{P}|p)f(\mathcal{P}|p) = 2$, then the desired implication holds surely:
$f(\mathcal{P}|p)v_{\mathcal{P}} \geq 2w_p \Longrightarrow v_{\mathcal{P}} \geq 2w_p/f(\mathcal{P}|p) = e(\mathcal{P}|p)w_p$.

c) But if p splits, then the implication doesn't hold any longer, in general.

In particular, if K is of D-type IIB, $D \equiv 5(\text{mod } 8)$, then $d = 2$ remains inert in K, and we see once more (cfr. Proposition 4.1,5.b), that $4|N_{K|\mathbf{Q}}(\alpha) \Longrightarrow \alpha \in 2\mathcal{O}_K$. □

Proposition 5.7. (Characterization of the minimal representative in a coset of discriminantal divisors.)

Let $D \in \mathbf{N}$, $D \geq 2$ be the squarefree radicand of a real quadratic number field, $d \in \mathbf{N}$, $d|D$ a positive non-escalatory discriminantal divisor, $\gamma_d = \sqrt{D}/d$ the normalized radical with respect to d, and $c \in \mathbf{N}$, $c \in \{d, D/d\}$ a dicriminantal divisor in the unsigned coset of d.

1. *The following statements are equivalent:*
   a) *c is the minimal (absolutely smaller) represantative in the coset $\{d, D/d\}$, that is,*
   $$c = \min\{d, D/d\}.$$
   b) *$\sqrt{c/d} = \min\{1, \gamma_d\}$ (in particular $\sqrt{c/d} \in \mathbf{Q}(\sqrt{D})$).*
   c) *The discriminantal divisor c is smaller than its complementary discriminantal divisor D/c,*
   $$c < D/c.$$
   d) *The discriminantal divisor c is smaller than the squareroot of the radicand D, $c < \sqrt{D}$.*
   e) *The normalized radical with respect to c is greater than 1, $\gamma_c > 1$.*
2. *Besides the general assumptions above, suppose now additionally that $\alpha \in \mathcal{O}$ is an algebraic integer in the real quadratic field $K = \mathbf{Q}(\sqrt{D})$, where $\mathcal{O}$ denotes either the maximal order of K or also the suborder $\mathbf{Z} \oplus \mathbf{Z}\sqrt{D}$ in the case $D \equiv 1(\text{mod } 4)$.*
   a) *If the norm of α is divisible by the discriminantal divisor d, then the number $\alpha\sqrt{D}/d$ is also an algebraic integer in the order $\mathcal{O}$:*
   $$d|N_{K|\mathbf{Q}}(\alpha) \Longrightarrow \alpha\sqrt{D}/d \in \mathcal{O},$$
   $$N_{K|\mathbf{Q}}(\alpha\sqrt{D}/d) = -(D/d) \cdot N_{K|\mathbf{Q}}(\alpha)/d.$$
   b) *If α has the norm $N_{K|\mathbf{Q}}(\alpha) = \pm 2^v \cdot d$ with $v \in \{0, 1\}$ and $v = 1$ at most, if $D \equiv 3(\text{mod } 4)$ (that is, $\pm 2^v \cdot d$ is a discriminantal principal factor for K), then $\alpha\sqrt{D}/d \in \mathcal{O}$ is an algebraic integer, exactly with the complementary discriminantal principal factor of $N_{K|\mathbf{Q}}(\alpha) = \pm 2^v \cdot d$ as norm, $N_{K|\mathbf{Q}}(\alpha\sqrt{D}/d) = \mp 2^v \cdot D/d$, and*

the following characterization by equivalent statements holds for an algebraic integer $\beta \in \{\alpha, \alpha\sqrt{D}/d\} (\subset \mathcal{O})$ with norm $N_{K|\mathbf{Q}}(\beta) = \pm 2^v \cdot c$:

1) $|N_{K|\mathbf{Q}}(\beta)| = 2^v \cdot \min\{d, D/d\}$, that is, $c = \min\{d, D/d\}$.

2) $|\beta| = |\alpha| \cdot \sqrt{c/d} = \min\{|\alpha|, |\alpha| \cdot \gamma_d\}$.

3) $|\beta| < |\beta| \cdot \gamma_c$.

PROOF. **1.** a) $\Longleftrightarrow$ b):
$c = \min\{d, D/d\} \Longleftrightarrow c/d = \min\{1, D/d^2\} = \min\{1, (\delta/d^2\} \Longleftrightarrow \sqrt{c/d} = = \min\{1, \delta/d\} = \min\{1, \gamma_d\} \in \mathbf{Q}(\sqrt{D})$.

a) $\Longleftrightarrow$ c):
1st case, $c = d : d = \min\{d, D/d\} \Longleftrightarrow d \leq D/d$, but D is squarefree, in particular not a square, whence even $d < D/d$.
2nd case, $c = D/d : D/d = \min\{d, D/d\} \Longleftrightarrow D/d < d$ (strict inequality by the same argument as in the 1st case) and further d can be written in the form $d = D/(D/d)$.

c) $\Longleftrightarrow$ d) $\Longleftrightarrow$ e):
$c < D/c \Longleftrightarrow 1 < D/c^2 = (\delta/c)^2 \Longleftrightarrow 1 < \delta/c = \gamma_c$, resp., $c < \delta$.

2. a) If $d|N_{K|\mathbf{Q}}(\alpha)$, then $N_{K|\mathbf{Q}}(\alpha\delta) = N_{K|\mathbf{Q}}(\alpha)N_{K|\mathbf{Q}}(\delta) = -DN_{K|\mathbf{Q}}(\alpha)$ is divisible by d^2, because $d|D$. Hence, by Proposition 5.6,3, $\alpha\delta \in d\mathcal{O}_K$, i.e., $\alpha\delta/d \in \mathcal{O}_K$. Further $N_{K|\mathbf{Q}}(\alpha\delta/d) = N_{K|\mathbf{Q}}(\alpha)N_{K|\mathbf{Q}}(\delta)/d^2$ $= -(D/d)N_{K|\mathbf{Q}}(\alpha)/d$. Moreover, if $D \equiv 1(\text{mod } 4)$ and $\alpha \in \mathcal{O} = \mathbf{Z} \oplus \mathbf{Z}\delta$, then $d|D \Longrightarrow d \equiv 1(\text{mod } 2)$, i.e., $2 + d$, d is coprime with the conductor $cond(\mathcal{O}) = 2\mathcal{O}_K$, and therefore, as $\delta \in \mathcal{O}$, $\alpha\delta \in \mathcal{O} \cap d\mathcal{O}_K = d\mathcal{O}$, i.e., $\alpha\delta/d$ is an integer in $\mathcal{O}$, not only in $\mathcal{O}_K$.

b) Using **1.**, we obtain $|N_{K|\mathbf{Q}}(\beta)| = 2^v c = 2^v \min\{d, D/d\} \Longleftrightarrow c = = \min\{d, D/d\} \Longleftrightarrow \sqrt{c/d} = \min\{1, \gamma_d\} \Longleftrightarrow |\alpha|\sqrt{c/d} = \min\{|\alpha|, |\alpha|\gamma_d\}$, and furthermore, $\Longleftrightarrow 1 < \gamma_c \Longleftrightarrow |\beta| < |\beta|\gamma_c$.
It only remains to show that $|\beta| = |\alpha|\sqrt{c/d}$.
1st case, $\beta = \alpha$: then $c = d$ and $\alpha\sqrt{c/d} = \alpha = \beta$.
2nd case, $\beta = \alpha\delta/d$: then $c = D/d$ and $\alpha\sqrt{c/d} = \alpha\sqrt{D/d^2} = \alpha\delta/d = \beta$. □

Now it is easy to show, that only a generator α of the differential principal factor with the absolutely smaller (minimal) discriminantal principal factor norm in the actual couple can be a lattice minimum in the geometric Minkowski image of the maximal order $\mathcal{O}_K$, or also of the suborder $\mathcal{O}$, if $D \equiv 1(\text{mod } 4)$ and $\alpha \in \mathcal{O}$.

Corollary 5.8. (A restriction for lattice minima with discriminantal divisor norm.)

Let $K = \mathbf{Q}(\sqrt{D})$ be a real quadratic field. $\mathcal{O}$ denotes the maximal order of K, or also the suborder $\mathbf{Z} \oplus \mathbf{Z}\sqrt{D}$ in the case $D \equiv 1(mod\ 4)$.

Further let $\epsilon_0 \in E_K$, $\epsilon_0 > 1$ be the fundamental unit of $\mathcal{O}$. Finally $d \in \mathbf{N}$, $d|D$ is a discriminantal divisor for K, and $\alpha \in \mathcal{O}$ is supposed to be generator of a differental principal factor in $\mathcal{O}$ with norm $N_{K|\mathbf{Q}}(\alpha) = = \pm 2^v \cdot d$, $v \in \{0,1\}$ ($v = 1 \Longrightarrow D \equiv 3(mod\ 4)$). α can be a lattice minimum in $\mathcal{O}$, at most, if $d = \min\{d, D/d\}$, that is,

$$|\alpha| \neq \min\{|\alpha|, |\alpha| \cdot \gamma_d\} \Longrightarrow \alpha \notin Min(\mathcal{O}).$$

In particular, if $|N_{K|\mathbf{Q}}(\alpha)| = D$, then $\alpha \notin Min(\mathcal{O})$. Further, in this case, $\alpha = \pm\epsilon_0^n \cdot \delta$ for some $n \in \mathbf{Z}$.

PROOF. a) Let $\alpha \in \mathcal{O}$ and $|N_{K|\mathbf{Q}}(\alpha)| = 2^v d$. If $|\alpha| \neq \min\{|\alpha|, |\alpha|\gamma_d\}$, i.e., $|\alpha| > |\alpha|\gamma_d \Longleftrightarrow d > \delta$, then also the conjugate satisfies $|(\alpha\gamma_d)'| = = |\alpha'| \cdot |\gamma_d'| = |\alpha'| \cdot | - \delta/d| = |\alpha'| \cdot \delta/d < |\alpha'|$. The point $\alpha\gamma_d$ in the norm rectangle of α is an algebraic integer in $\mathcal{O}$, by Proposition 5.6, whence $\alpha \notin Min(\mathcal{O})$.

b) In particular, if $d = |N_{K|\mathbf{Q}}(\alpha)| = D$, then $D/d = D/D = 1 < D = = d$ and hence, by a), $\alpha \notin Min(\mathcal{O})$. □

The next theorem transforms a geometric problem into a diophantine problem, showing that for the existence of a nonzero lattice point within the interior of the norm rectangle of an algebraic integer with discriminantal principal factor norm it is necessary and sufficient that a certain system of two binary linear diophantine inequalities (the so called "critical norm rectangle inequalities") with congruential constraints, depending on the residue class of the radicand D modulo 4, has a couple of (rational) integers as a solution.

This is an effectful device for the number geometric treatment of algebraic integers , whose norms are neither constant (as in Theorem 4.2) nor absolutely bounded (as in Theorem 2.3), but increase together with the radicand D and are only relatively bounded by $2\sqrt{D}$.

Theorem 5.9. (A diophantine criterion for the existence of a nontrivial lattice point within the norm rectangle of an algebraic integer with discriminantal principal factor norm.)

Let $K = \mathbf{Q}(\sqrt{D})$ be of arbitrary D-type. Further suppose that $d \in \mathbf{N}$, $d|D$ is a discriminantal divisor for K (not divisible by 2, in the case of D-type IB), with associated normalized radical $\gamma = \gamma_d = \delta/d$.

1. *Assume that*
either K is of D-type I, and $\alpha \in \mathcal{O} (= \mathcal{O}_K)$, $|N_{K|\mathbf{Q}}(\alpha)| = d$ is an algebraic integer with discriminantal principal factor norm, in particular, non-escalatory in the case of D-type IB,
or K is of D-type II, and $\alpha \in \mathcal{O}$ in the suborder is the generator of an ambiguous principal ideal with $|N_{K|\mathbf{Q}}(\alpha)| = d$.
Then $\alpha \notin Min(\mathcal{O})$, exactly if there exists a couple of integers $(k, l) \in \mathbf{Z}^2$ with the properties

(1) $0 < k + l\gamma < 1$,
(2) $|k - l\gamma| < 1$.

2. *Assume that*
either K is of D-type IB, and $\alpha \in \mathcal{O}_K$, $|N_{K|\mathbf{Q}}(\alpha)| = 2d$ is an algebraic integer with escalatory discriminantal principal factor norm (divisible by 2),
or K is of D-type II, and $\alpha \in \mathcal{O}_K$ in the maximal order generates an ambiguous principal ideal with $|N_{K|\mathbf{Q}}(\alpha)| = d$.
Then $\alpha \notin Min(\mathcal{O}_K)$, exactly if there exists a couple of integers $(k, l) \in \mathbf{Z}^2$ with the properties
(1) $0 < k + l\gamma < 2$,
(2) $|k - l\gamma| < 2$,
(3) $k \equiv l (mod\ 2)$.

PROOF. Suppose at first that $\mathcal{O}$ is either the maximal order or the suborder of K. Let $\alpha \in \mathcal{O}$, $|N_{K|\mathbf{Q}}(\alpha)| = 2^v d$ with $v \in \{0,1\}$ ($v = 1 \Longrightarrow D \equiv 3(\mathrm{mod}\ 4)$), and $d \in \mathrm{N}$, $d|D$. Then $\alpha \neq 0$ and generally: $\alpha \notin Min(\mathcal{O})$, iff there exists a point $\vartheta \in \mathcal{O}$ such that $0 < |\vartheta| < |\alpha|$ and $|\vartheta'| < |\alpha'|$, i.e., a non-trivial lattice point within the norm rectangle of α. The number $\xi = |\vartheta| \cdot |N_{K|\mathbf{Q}}(\alpha)/\alpha| = |\vartheta| \cdot |\alpha'| \in \mathcal{O}$ has the metrical properties $0 < \xi = |N_{K|\mathbf{Q}}(\alpha)|.\ |\vartheta|/|\alpha| < |N_{K|\mathbf{Q}}(\alpha)| = 2^v d$, $|\xi'| = |N_{K|\mathbf{Q}}(\alpha)| \cdot |\vartheta'|/|\alpha'| < |N_{K|\mathbf{Q}}(\alpha)| = 2^v d$, and the divisibility property $N_{K|\mathbf{Q}}(\xi) = N_{K|\mathbf{Q}}(|\vartheta|) \cdot N_{K|\mathbf{Q}}(|\alpha'|) = N_{K|\mathbf{Q}}(\alpha) \cdot N_{K|\mathbf{Q}}(\vartheta)$, i.e., $2^v d = |N_{K|\mathbf{Q}}(\alpha)| \mid N_{K|\mathbf{Q}}(\xi)$. Write $\xi = (x + y\delta)/n$ with $x, y \in \mathbf{Z}$, $n \in \{1, 2\}$ ($n = 2 \Longleftrightarrow D \equiv 1(\mathrm{mod}\ 4)$), in not necessarily reduced representation (if $n = 2$). According to Proposition 5.6,2, $d|x$, because $d|N_{K|\mathbf{Q}}(\xi)$ and $d|D$. If we set $k = x/d$, $l = y$, then $k, l \in \mathbf{Z}$ and

$$k + l\gamma = x/d + y\delta/d = (x + y\delta)/d = n\xi/d < 2^v n,$$
$$(k + l\gamma)' = k - l\gamma = n\xi'/d < 2^v n.$$

1. Now let $\mathcal{O}$ be the suborder of K again. In the case $\alpha \in \mathcal{O}$, $|N_{K|\mathbf{Q}}(\alpha)| = d$, we have $v = 0$, $n = 1$ and hence $0 < k + l\gamma < 1$, $|k - l\gamma| < 1$. Conversely assume $(k, l) \in \mathbf{Z}^2$, such that $0 < k + l\gamma < 1$, $|k - l\gamma| < 1$. Then the number $\vartheta = d(k + l\gamma) \cdot |\alpha/N_{K|\mathbf{Q}}(\alpha)| = d(k + l\gamma) \cdot |\alpha|/d = (k + l\gamma) \cdot |\alpha|$ has the desired metrical properties $0 < \vartheta < |\alpha|$ and $|\vartheta'| = |k - l\gamma| \cdot |\alpha'| < |\alpha'|$. It only remains to show that $\vartheta \in \mathcal{O}$. $d(k + l\gamma) = dk + dl\delta/d = x + y\delta \in \mathcal{O}$, if we put $x = dk$, $y = l$, $x, y \in \mathbf{Z}$. Then $N_{K|\mathbf{Q}}(x + y\delta) = x^2 - Dy^2 = d^2k^2 - Dl^2 = d \cdot (dk^2 - l^2 D/d)$, i.e., $d \mid N_{K|\mathbf{Q}}(x + y\delta)$. Now $d^2 \mid N_{K|\mathbf{Q}}((x + y\delta) \cdot |\alpha|)$ and Proposition 5.6,3 shows that $(x + y\delta) \cdot |\alpha| \in d\mathcal{O}_K \cap \mathcal{O} = d\mathcal{O}$, taking into account, that $2 + d$, if $D \equiv 1(\mathrm{mod}\ 4)$. Hence $\vartheta = (x + y\delta) \cdot |\alpha|/d \in \mathcal{O}$.

2. In the case $D \equiv 1(\mathrm{mod}\ 4)$, we have $v = 0$, $n = 2$ and hence $0 < k + l\gamma < 2$, $|k - l\gamma| < 2$. By Theorem 1.1,2, $x \equiv y(\mathrm{mod}\ 2)$ and hence $k \equiv dk = x \equiv y = l(\text{mod } 2)$, because $d \equiv 1(\text{mod } 2)$. In the case $D \equiv 3(\text{mod } 4)$ we have $v = 1$, $n = 1$ and hence $0 < k + l\gamma < 2$, $|k - l\gamma| < 2$. $x^2 - Dy^2 \equiv x^2 - y^2 \equiv x - y(\text{mod } 2)$ shows that $2 \mid N_{K|\mathbf{Q}}(x + y\delta)$, iff $x \equiv y(\text{mod } 2)$, and hence $k \equiv dk = x \equiv y = l(\text{mod } 2)$, because $d \equiv 1(\text{mod } 2)$.

Conversely let $(k, l) \in \mathbf{Z}^2$ such that $0 < k + l\gamma < 2$, $|k - l\gamma| < 2$ and $k \equiv l(\text{mod } 2)$. Then the number $\vartheta = 2^{v-1}d(k + l\gamma) \cdot |\alpha/N_{K|\mathbf{Q}}(\alpha)| = 2^{v-1}d(k + l\gamma) \cdot |\alpha|/(2^v d) = (k + l\gamma) \cdot |\alpha|/2$ has the desired metrical properties $0 < \vartheta < |\alpha|$ and $|\vartheta'| = |k - l\gamma| \cdot |\alpha'|/2 < |\alpha'|$. But we must show that $\vartheta \in \mathcal{O}_K$. If we set $x = dk$, $y = l$, $x, y \in \mathbf{Z}$, then $d(k + l\gamma) = dk + dl\delta/d = x + y\delta \in \mathcal{O} \subset \mathcal{O}_K$, $N_{K|\mathbf{Q}}(x + y\delta) = x^2 - Dy^2 = d^2k^2 - Dl^2 = d \cdot (dk^2 - l^2 D/d)$, i.e., $d | N_{K|\mathbf{Q}}(x + y\delta)$. First consider the case $D \equiv 1(\text{mod } 4)$. Then $v = 0$, $\vartheta = \frac{1}{2}d(k + l\gamma) \cdot |\alpha|/d$, and $x = dk \equiv k \equiv l = y(\text{mod } 2)$, because $d \equiv 1(\text{mod } 2)$. Hence, according to Theorem 1.1,2, $x + y\delta \in 2\mathcal{O}_K$ and therefore $4 \mid N_{K|\mathbf{Q}}(x + y\delta)$. As $2 + d$, also $d \mid \frac{1}{4}N_{K|\mathbf{Q}}(x + y\delta) = N_{K|\mathbf{Q}}((\frac{1}{2}(x + y\delta))$. Now $d^2 | N_{K|\mathbf{Q}}(\frac{1}{2}(x + y\delta) \cdot |\alpha|)$ and Proposition 5.6,3 shows that $\frac{1}{2}(x + y\delta) \cdot |\alpha| \in d\mathcal{O}_K$, i.e., $\vartheta = \frac{1}{2}(x + y\delta) \cdot |\alpha|/d \in \mathcal{O}_K$. Second consider the case $D \equiv 3(\text{mod } 4)$. Then $v = 1$, $\vartheta = d(k + l\gamma) \cdot |\alpha|/(2d)$ and $x = dk \equiv k \equiv l = y(\text{mod } 2)$, because $d \equiv 1(\text{mod } 2)$. Hence, by the above consideration, $x \equiv y(\text{mod } 2) \Longrightarrow 2 | N_{K|\mathbf{Q}}(x + y\delta)$. And, as $2 + d$, also $2d | N_{K|\mathbf{Q}}(x + y\delta)$. Now $(2d)^2 | N_{K|\mathbf{Q}}((x + y\delta) \cdot |\alpha|)$ and Proposition 5.6,4 shows that $(x + y\delta) \cdot |\alpha| \in 2d\mathcal{O}_K$, i.e., $\vartheta = (x + y\delta) \cdot |\alpha|/(2d) \in \mathcal{O}_K$. □

Now we analyze the diophantine criterion for the existence of a nontrivial lattice point within the norm rectangle of an algebraic integer with discriminantal principal factor norm, which is henceforth supposed to be minimal in its coset.

Lemma 5.10. (The solutions of the critical systems of binary linear diophantine inequalities with congruential constraints.)

Let $\gamma \in \mathbf{R}$, $\gamma > 1$.

1. *There are no couples of integers $(k, l) \in \mathbf{Z}^2$ with the properties*
(1) $0 < k + l\gamma < 1$,
(2) $|k - l\gamma| < 1$.

2. *Further there does not exist a couple of integers $(k, l) \in \mathbf{Z}^2$ with the properties*
(1) $0 < k + l\gamma < 2$,
(2) $|k - l\gamma| < 2$,
(3) $k \equiv l(\text{mod } 2)$.

PROOF. **1.** Lemma 2.1 yields the basic restriction for a couple $(k, l) \in \mathbf{Z}^2$ with $|k + l\gamma| < 1$ and $|k - l\gamma| < 1$: $|k|, |l\gamma| < 1$ and hence $|l| < 1/\gamma < 1/1 = 1$. Therefore only the trivial couple (0,0) is a candidate. But, as we demand $0 < k + l\gamma$, no couple remains.

2. The fundamental restriction for a couple $(k,l) \in \mathbf{Z}^2$ with $|k+l\gamma| < 2$ and $|k-l\gamma| < 2$ comes from Lemma 2.1: $|k|, |l\gamma| < 2$ and hence $|l| < 2/\gamma < 2/1 = 2$. Thus there are basically $3^2 = 9$ possibilities for the couple $(k,l) \in \{-1,0,1\}^2$. Next we use condition $k \equiv l (\text{mod } 2)$ to exclude $(k,l) \in \{(-1,0),(0,-1),(0,1),(1,0)\}$, leaving $9-4=5$ possibilities. Further $0 < k+l\gamma$ together with $\gamma > 1$ discourages $(k,l) \in \{(0,0),(-1,-1),(1,-1)\}$ and there remain $5-3=2$ possible couples. Finally $k+l\gamma < 2$, $\gamma > 1$ implies $(k,l) \neq (1,1)$, and from $|k-l\gamma| < 2$, $\gamma > 1$ we infer $k \cdot l \neq -1$ and hence $(k,l) \neq (-1,1)$. Thus even the last two possibilities are culled out. □

Now we have solved the diophantine problem and see that the critical system of norm rectangle inequalities for an algebraic integer with minimal discriminantal principal factor norm is insoluble in any case.

Therefore, as a conclusion, we prove in Theorem 5.11 that an algebraic integer α with minimal discriminantal principal factor norm can always be found among the lattice minima in the geometric Minkowski image as well of the maximal order $\mathcal{O}_K$, as of the suborder $\mathcal{O}$ in the case of D-type II, if $\alpha \in \mathcal{O}$. This result can be obtained by the geometrical Theorem 2.3 only in the cases, when the discriminantal principal factor norm is "sufficiently small", hence not always for odd radicands $D \equiv 3(\text{mod } 4)$ or $D \equiv 1(\text{mod } 4)$.

Theorem 5.11. (Main theorem on algebraic integers, whose norm is a minimal discriminantal principal factor.)

Let $K = \mathbf{Q}(\sqrt{D})$ be a real quadratic field, and $d \in \mathbf{N}$, $d|D$ a minimal discriminantal principal factor for K, that is, $d = \min\{d, D/d\}$, or, in terms of the associated normalized radical, $\gamma = \gamma_d = \sqrt{D}/d > 1$. Further suppose that $\alpha \in \mathcal{O}_K$ is an algebraic integer with norm $|N_{K|\mathbf{Q}}(\alpha)| = 2^v d$, where $v \in \{0,1\}$ and $v = 1$ at most, if K is of D-type IB, $D \equiv 3(\text{mod } 4)$.

1. *If K is of D-type IA, $D \equiv 2(\text{mod } 4)$, then $\alpha \in Min(\mathcal{O}_K)$.*

2. *If K is of D-type IB, $D \equiv 3(\text{mod } 4)$, and $N_{K|\mathbf{Q}}(\alpha)$ is non-escalatory, that is, $v = 0$ resp. $2 + N_{K|\mathbf{Q}}(\alpha)$, then $\alpha \in Min(\mathcal{O}_K)$.*

3. *If K is of D-type II, $D \equiv 1(\text{mod } 4)$, and $\alpha \in \mathcal{O} = \mathbf{Z} \oplus \mathbf{Z}\sqrt{D}$ is contained in the suborder, then $\alpha \in Min(\mathcal{O})$.*

1., 2., 3. *are the easy cases, where $|N_{K|\mathbf{Q}}(\alpha)| = d < \sqrt{D}$, and which therefore could have been treated by Theorem 2.3 directly, too.*

4. *If K is of D-type IB, $D \equiv 3(\text{mod } 4)$, and α has an escalatory norm, that is, $v = 1$ resp. $2|N_{K|\mathbf{Q}}(\alpha)$, then nevertheless $\alpha \in Min(\mathcal{O}_K)$.*

5. *If K is of D-type II, $D \equiv 1(\text{mod } 4)$, and $\alpha \in \mathcal{O}_K = \mathbf{Z} \oplus \mathbf{Z}\frac{1}{2}(1+\sqrt{D})$ is an arbitrary integer in the maximal order, then nevertheless $\alpha \in Min(\mathcal{O}_K)$.*

4., 5. *are the difficult cases, where Theorem 2.3 generally fails, because in*

4. *$|N_{K|\mathbf{Q}}(\alpha)| = 2d$ need not be smaller than $\sqrt{D}$, although $d < \sqrt{D}$, and in* **5.** *$|N_{K|\mathbf{Q}}(\alpha)| = d$ may be greater than $\frac{1}{2}\sqrt{D}$, though $d < \sqrt{D}$.*

Summarized: In real quadratic fields of arbitrary D-type an algebraic integer α with minimal discriminantal principal factor norm is a lattice minimum in the maximal order $\mathcal{O}_K$, and also in the suborder $\mathcal{O}$, if $D \equiv 1 \ (mod\ 4)$ and $\alpha \in \mathcal{O}$.

PROOF. In the cases **1.**, **2.**, **3.** for the algebraic integer $\alpha \in \mathcal{O} = \mathbf{Z} \oplus \mathbf{Z}\delta$ first Theorem 5.9,1 brings a translation of the minimality of $\alpha \in \mathcal{O}$ in a critical system of binary linear diophantine inequalities, and then Lemma 5.10,1 shows the insolubility of this system: $\alpha \in Min(\mathcal{O})$, exactly if there are no couples of integers $(k,l) \in \mathbf{Z}^2$ with the properties $0 < k + l\gamma < 1$, $|k - l\gamma| < 1$, and indeed there are none.

In the cases **4.**,**5.** Theorem 5.9,2 translates the minimality of $\alpha \in \mathcal{O}_K$ in a critical system of binary linear diophantine inequalities, with congruential constraints, and Lemma 5.10,2 shows that these have no solutions either: $\alpha \in Min(\mathcal{O}_K)$, if and only if there is no couple of integers $(k,l) \in \mathbf{Z}^2$ with $0 < k + l\gamma < 2$, $|k - l\gamma| < 2$, $k \equiv l (\text{mod } 2)$, and really there does not exist one. □

Theorem 5.12. (Existence of principal factors in the suborder $\mathcal{O} = \mathbf{Z} \oplus \mathbf{Z}\sqrt{D}$ of a real quadratic D-type II field of PF-type I.)

Let $K = \mathbf{Q}(\sqrt{D})$ be real quadratic with radicand $D \equiv 1 (mod\ 4)$ and with normpositive fundamental unit, $\epsilon_0 \in E_K$, $\epsilon_0 > 1$ and $N_{K|\mathbf{Q}}(\epsilon) = +1$, and suppose that $\eta_0 \in E_{\mathcal{O}}$, $\eta_0 > 1$ is the fundamental unit of the suborder $\mathcal{O}$.

1. *If $\alpha \in \mathcal{O}_K$ is the generator of a non-trivial differental principal factor in K, with norm $N_{K|\mathbf{Q}}(\alpha) = d$, $d \in \mathbf{Z}$, $d|D$, $|d| \notin \{1, D\}$, then either already α itself belongs to the suborder $\mathcal{O}$ (in fact, always, if $D \equiv 1 (mod\ 8)$, or at most the third power α^3 is contained in the suborder $\mathcal{O}$. But $\alpha^3 \in d\mathcal{O}$ is necessarily imprimitive in $\mathcal{O}$, whereas α^3/d is still contained in the suborder $\mathcal{O}$, has norm d, and is generator of a non-trivial primitive ambiguous principal ideal in K.*
2. *There exists a lattice minimum $\varphi \in Min(\mathcal{O})$ in the first primitive period of $\mathcal{O}$, $1 < \varphi < \eta_0$, such that $N_{K|\mathbf{Q}}(\varphi) | R_{K|\mathbf{Q}}$.*
   Further, if $\vartheta \in Min(\mathcal{O}_K)$ is a lattice minimum in the first primitive period of $\mathcal{O}_K$, $1 < \vartheta < \epsilon_0$, such that $N_{K|\mathbf{Q}}(\vartheta) \mid R_{K|\mathbf{Q}}$, then
   a) *$\varphi = \vartheta$ in the case $(E_K : E_{\mathcal{O}}) = 1$,*
   b) *$\varphi = \vartheta^3/|N_{K|\mathbf{Q}}(\vartheta)| = \epsilon_o \cdot \vartheta$ but $\vartheta, \epsilon_0^2 \cdot \vartheta \notin \mathcal{O}$ in the case $(E_K : E_{\mathcal{O}}) = 3$.*
   In any case $N_{K|\mathbf{Q}}(\varphi) = N_{K|\mathbf{Q}}$.

PROOF. **1.** Assume $|N_{K|\mathbf{Q}}(\alpha)| = d$ with $d \in \mathbf{Z}$, $d|D$. As $D \equiv 1 \ (\text{mod } 4)$, D, and hence in particular d, is coprime with 2. But then also $\gcd(\alpha\mathcal{O}_K, 2\mathcal{O}_K)\mathcal{O}_K$, because $\alpha\mathcal{O}_K \supset d\mathcal{O}_K$, $\mathcal{O}_K = d\mathcal{O}_K + 2\mathcal{O}_K \subset \alpha\mathcal{O}_K + 2\mathcal{O}_K \subset \mathcal{O}_K$. Now with the aid of Proposition 4.1: in the case $D \equiv 1(\text{mod } 8)$: $\gcd(\alpha, 2) = 1$ implies $\alpha \in \mathcal{O}$ already, and in the case $D \equiv 5(\text{mod } 8)$: from $\gcd(\alpha, 2) = 1$ follows either $\alpha \in \mathcal{O}$ or $\alpha \notin \mathcal{O}$, $\alpha^3 \in \mathcal{O}$. In the latter case α^3 is imprimitive in $\mathcal{O}$, because $d^2 | N_{K|\mathbf{Q}}(\alpha^3)$, whence $\alpha^3 \in d\mathcal{O}_K$, by Proposition 5.6,3, and thus $\alpha^3 \in \mathcal{O} \cap d\mathcal{O}_K = d\mathcal{O}$, because $d \equiv 1(\text{mod } 2)$. Hence α^3/d is also contained in $\mathcal{O}$ and α^3/d is primitive in $\mathcal{O}$, by Proposition 5.4,1, as $N_{K|\mathbf{Q}}(\alpha^3/d) = N_{K|\mathbf{Q}}(\alpha)^3/d^2$ $= d^3/d^2 = d | R_{K|\mathbf{Q}} = D$.

2. By **1.**, Theorem 5.11,3, and the periodicity of $Min(\mathcal{O})$ (see §2, section 6), there exists $\varphi \in Min(\mathcal{O})$, $1 < \varphi < \eta_0$, $N_{K|\mathbf{Q}}(\varphi) \mid R_{K|\mathbf{Q}}$. In fact also a minimum $\vartheta \in Min(\mathcal{O}_K)$, $1 < \vartheta < \epsilon_0$, $N_{K|\mathbf{Q}}(\vartheta) \mid R_{K|\mathbf{Q}}$ exists by Theorem 5.11,5 and the periodicity of $Min(\mathcal{O}_K)$.

a) If $(E_K : E_{\mathcal{O}}) = 1$, i.e., $\eta_0 = \epsilon_0$, then $1 < \vartheta < \epsilon_0$ and the uniqueness statement in Proposition 5.4,3 for the maximal order $\mathcal{O}_K$ immediately implies $\varphi = \vartheta$.

b) If $(E_K : E_{\mathcal{O}}) = 3$, i.e., $\eta_o = \epsilon_0^3$, then $1 < \vartheta < \epsilon_0$ implies $1 < \vartheta \cdot \epsilon_0 < \epsilon_0^2 < \eta_0$. Now, putting $d = |N_{K|\mathbf{Q}}(\vartheta)|$, $\vartheta^3/d \in \mathcal{O}$ by **1.**, and, as $1 < \vartheta < \epsilon_0$ implies $\vartheta^2/d = \epsilon_0$, by Proposition 5.4,2, we have $\vartheta^3/d = \vartheta \cdot \vartheta^2/d = \vartheta \cdot \epsilon_0 \in \mathcal{O}$. Together with $1 < \varphi < \eta_0$, the uniqueness statement in Proposition 5.4,3 for the suborder $\mathcal{O}$ shows $\varphi = \vartheta \cdot \epsilon_0$. Finally, as $N_{K|\mathbf{Q}}(\epsilon_0) = +1 : N_{K|\mathbf{Q}}(\varphi) = N_{K|\mathbf{Q}}(\epsilon_0) \cdot N_{K|\mathbf{Q}}(\vartheta) = N_{K|\mathbf{Q}}(\vartheta)$. □

Remark. With the aid of Theorem 5.12,2,b we finally obtain a proof for the fact, mentioned in Proposition 4.1,8 already, that under the assumptions of Theorem 5.12

$$PL(\mathcal{O}) \equiv PL(\mathcal{O}_K)(\text{mod } 4).$$

(Compare also with F. HALTER-KOCH [11], pag. 37.) For this purpose we assume $\varphi = \nu_1^m(1) \in Min(\mathcal{O})$, $2m = PL(\mathcal{O})$ and $\vartheta = \nu_1^n(1) \in Min(\mathcal{O}_K)$, $2n = PL(\mathcal{O}_K)$ for some $m, n \in \mathbf{N}$, according to Corollary 5.5. From Theorem 5.12,2.b we know $N_{K|\mathbf{Q}}(\varphi) = N_{K|\mathbf{Q}}(\vartheta)$. Therefore $(-1)^m =$ $= sgn(N_{K|\mathbf{Q}}\nu_1^m(1)) = sgn(N_{K|\mathbf{Q}}\nu_1^n(1)) = (-1)^n$, which implies $m \equiv$ $\equiv n(\text{mod } 2)$, and hence $2m \equiv 2n(\text{mod } 4)$. Here we make use of a weak consequence of Scheffler's formula (see the Remark after Corollary 3.4), concerning the sign of the norm of a lattice minimum: $sgn(N_{K|\mathbf{Q}}\nu_1^j(1)) =$ $(-1)^j$ for all $j \geq 0$.

§6. Tables and recognizable tendencies

The first six tables are associated in successive pairs. Tables 1, 3, 5, 7 list relative intervals of length 10^4 with upper bounds from 10^4 to 10^5

and two samples at $5 \cdot 10^5$ and 10^6. On the other hand in Tables 2, 4, 6 absolute intervals with upper bounds between 50 and 10^5 are recorded.

Table 1 and Table 2 reveal the remarkable constancy of the percentage of squarefree radicands around 60.793%, thus confirming the asymptotic approximation of the absolute percentage of all squarefree numbers by $100 \cdot \frac{6}{\pi^2} \approx 60.792$ (cfr. D. SHANKS [30], pag. 26).

Further the equipartition of squarefree positive integers among the residue classes $\equiv 1, 2, 3 (\mathrm{mod}\ 4)$ and $\equiv 1, 5 (\mathrm{mod}\ 8)$ is striking. Only for very small radicands (at the begin of Table 2) the percentage of D-type I fields is a little bit higher and decreases from about 73% towards 67%. But the latter limit is attained already for $D \approx 10^4$ and so this initial effect does not appear in Table 1.

Table 3 clearly shows an increasing tendency of PF-type I with small fluctuations. This behaviour can be recognized in each of the individual D-types, with the exception of D-type IB, where a priori only PF-type I is possible (100%), because -1 is a quadratic non-residue for all primes $p \equiv 3 (\mathrm{mod}\ 4)$ (see Proposition 5.2). But the relative percentages differ for D-type IA and for D-type II (where the subdivision in types IIA and IIB does not reveal remarkable differences); we have an increase from 82% to 85% for D-type IA, from 57% to 67% for D-type II, and from 80% to 84% for all D-types together. An explanation for the fact that D-type IA shows almost the same values as all D-types together would be the equipartition of squarefree positive integers $D \equiv 2 (\mathrm{mod}4)$ in those with $\frac{D}{2} \equiv 1 (\mathrm{mod}4)$ and the others with $\frac{D}{2} \equiv 3 (\mathrm{mod}4)$.

In Table 4 the oscillations of relative frequencies are smoothened and now PF-type I shows even a monotonic increasing behaviour: an increase from 70% to 84% for D-type IA, from 25% to 62% for D-type II, and from 68% to 82% for all D-types together. The frequencies for the upper bound 15000 coincide with those mentioned by H.C. WILLIAMS [38], pag. 272.

For statistical results concerning the solvability of the Pellian minus equation in arbitrary orders of real quadratic fields compare W. PATZ [24] ($D < 10^4$) or B. D. BEACH and H. C. WILLIAMS [3] ($D < 10^6$). Concerning more special solutions of Pellian equations see H.C. WILLIAMS and C. R. ZARNKE [34] ($D < 10^6$), [35] ($D < 2 \cdot 10^6$).

In Table 5 the percentage of D-type IIB fields with unit group index 3 moves around 70.97% with deviations from -3.61% to $+2.65\%$. The stability seems to be slightly better for PF-type I, showing deviations from -3.31% to $+3.10\%$ around 71.81%, than for PF-type II with deviations from -4.18% to $+3.02\%$ around 69.59%.

Again the relative effects are smoothened in Table 6 and now a slow decrease of unit group index 3 is visible, for PF-type I almost monotonic. This tendency is probably due to the increasing density of discriminants of totally real cubic "auxiliary fields" (see §4, Tables A,B). We have a decrease from 100% to 72% for PF-type I, from 86% to 70% for PF-type II, and from 91% for both PF-types together. Thus the frequency of unit group index 3 for PF-type I fields is obviously a little bit higher than for PF-type II fields.

Table 7 records the increasing maximal period lengths, bounded from above by $C \cdot \sqrt{D} \log\log D\,(C = \text{const.})$. Although the intervals are relative, they are big enough to reveal monotonic increasing behaviour. The values for $PL(\mathcal{O})$, i.e., the period length of the continued fraction expansion of $\sqrt{D}$, agree with those in the table of H. C. WILLIAMS [37] (except for the value 2492, which is only a local maximum, because the interval length 10^4 is already too small here to catch the real hichamp). In [37] the corresponding hichamp radicands D can also be found and the constant C is specified. The listed expression $\lfloor \sqrt{D} \log\log D \rfloor$ is calculated for the upper interval bounds, not for the individual hichamp radicands. The values for $PL(\mathcal{O}_K)$, i.e., the period length of the continued fraction expansion of $\frac{1}{2}(1+\sqrt{D})$, are only considered for $D \equiv 1(\text{mod}4)$. For more details compare R. KORTUM and G. MCNIEL [7] $(D < 5 \cdot 10^4)$, D. SHANKS [29], B. D. BEACH and H. C. WILLIAMS [2] $(D < 1.2 \cdot 10^6)$, or H. C. WILLIAMS [37] $(D < 2 \cdot 10^9)$.

Moreover we have made statistics of the ratios $PL(\mathcal{O})/PL(\mathcal{O}_K)$ in the case of D–type II fields, and also of the position of the twofold $2\epsilon_0$ of the fundamental unit $\epsilon_0 > 1$ of $\mathcal{O}_K$ in the first primitive period of $Min(\mathcal{O})$ in the case of unit group index 3 for radicands $D \equiv 5(\text{mod}8)$, $D \neq 5$.

Except for fluctuations, due to small periods, these considerations detect a very close coincidence of $PL(\mathcal{O})$ and $PL(\mathcal{O}_K)$ in the case of unit group index 1 for radicands $D \equiv 1, 5(\text{mod}8)$, whereas $PL(\mathcal{O}) \approx 3 \cdot PL(\mathcal{O}_K)$ in the case of unit group index 3 for $D \equiv 5(\text{mod}8)$. However, these proportions are distorted for small period lengths and one has to proceed up to rather big radicands in order to achieve long periods and to realize the crystallized phenomena offered by the lattice minima. Possible deviations are $0.33 \leq PL(\mathcal{O})/PL(\mathcal{O}_K) \leq 2.43$ in the case of unit group index 1 for radicands $D \equiv 1, 5(\text{mod}8)$, and on the other hand $1.36 \leq PL(\mathcal{O})/PL(\mathcal{O}_K) \leq 5.00$ in the case of unit group index 3 for $D \equiv 5(\text{mod}8)$.

For fields with radicand $D \equiv 5(\text{mod}8)$, $D \neq 5$ and unit group index 3 the positions $j, k \in \mathbf{N}$ of the twofolds of the fundamental unit $\epsilon_0 > 1$ of $\mathcal{O}_K$ and of its square ϵ_0^2 among the lattice minima in $\mathcal{O}$, that is, $2\epsilon_0 = \nu_1^j(1)$ and $2\epsilon_0^2 = \nu_1^k(1)$ in $Min(\mathcal{O})$, satisfy $j \approx \frac{1}{3} PL(\mathcal{O})$ and $k \approx \frac{2}{3} PL(\mathcal{O})$, but again for small period lengths deviations in the range $0.20 \leq j/PL(\mathcal{O}) \leq 0.42$ are possible. Hence $0.58 \leq k/PL(\mathcal{O}) \leq 0.80$, as a consequence of the symmetry property of norms of lattice minima with respect to the first primitive period in $Min(\mathcal{O})$ (§2, section 6, Remark). This empirical result suggests a further modification of the unit calculation:

Remark. (A third variant of the unit algorithm.)

For large radicands $D \equiv 5(\text{mod}8)$ almost exactly half of the computer time can be saved by the application of the second algorithmic version (Corollary 5.5 and the Remark afterwards) to the maximal order $\mathcal{O}_K$, i.e., the expansion of $\frac{1}{2}(1+\sqrt{D})$) or $\frac{1}{2}(-1+\sqrt{D})$ instead of $\sqrt{D}$ (thus giving up the uniform inialization, according to the first modification, Corollary 4.3), if $(E_K : E_{\mathcal{O}}) = 3$, and if $(E_K : E_{\mathcal{O}}) = 1$, the amount of needed time remains approximately the same.

The typical phenomena for long periods show that the spacing of the minima is then comparable in both orders, and that the magnitude of the i-th lattice minimum $\nu_1^i(1)$ $(i \geq 0)$ is approximately $\nu_1^i(1) \approx \epsilon_0^{i/PL(\mathcal{O}_K)} \approx \eta_0^{i/PL(\mathcal{O})}$ as well in $Min(\mathcal{O}_K)$ as in $Min(\mathcal{O})$, where $\epsilon_0 > 1$ denotes the fundamental unit in $\mathcal{O}_K$, and $\eta_0 > 1$ the fundamental unit in $\mathcal{O}$.

Table 8 contains typical examples of D-type II fileds with large period lengths and various combinations of PF-types and unit group indices. Considered are all radicands $D \equiv 1(\text{mod}4)$, $10^6 < D < 10^6 + 1850$ with $PL(\mathcal{O}_K) > 1500$, if $D \equiv 1(\text{mod}8)$, $PL(\mathcal{O}) > 1490$, if $D \equiv 5(\text{mod}8)$, $(E_K : E_{\mathcal{O}}) = 3$, and $PL(\mathcal{O}) > 400$, if $D \equiv 5(\text{mod}8)$, $(E_K : E_{\mathcal{O}}) = 1$. Similarly as in Tables A,B we denote by PF the actual minimal non-trivial discriminantal principal factor in the field.

All tables have been computed at the EDV-center of the Karl-Franzens-Universität in Graz on a VAX 785 computer. The programs were written in PASCAL.

TABLE 1. (Relative numbers and frequencies of D-types.)

radicands		total		IA		IB
	#	%	#	%	#	%
$0 < D < 10000$	6082	60.82	2027	33.33	2030	33.38
$10000 < D < 20000$	6077	60.77	2029	33.39	2025	33.32
$20000 < D < 30000$	6082	60.82	2025	33.30	2030	33.38
$30000 < D < 40000$	6068	60.68	2023	33.34	2022	33.32
$40000 < D < 50000$	6091	60.91	2030	33.33	2028	33.30
$50000 < D < 60000$	6072	60.72	2027	33.38	2026	33.37
$60000 < D < 70000$	6083	60.83	2024	33.27	2029	33.36
$70000 < D < 80000$	6071	60.71	2021	33.29	2022	33.31
$80000 < D < 90000$	6086	60.86	2035	33.44	2024	33.26
$90000 < D < 100000$	6081	60.81	2026	33.32	2031	33.40
$500000 < D < 510000$	6082	60.82	2027	33.33	2029	33.36
$1000000 < D < 1010000$	6079	60.79	2025	33.31	2027	33.34
radicands		II		IIA		IIB
	#	%	#	%	#	%
$0 < D < 10000$	2025	33.30	1009	16.59	1016	16.71
$10000 < D < 20000$	2023	33.29	1012	16.65	1011	16.64
$20000 < D < 30000$	2027	33.33	1014	16.67	1013	16.66
$30000 < D < 40000$	2023	33.34	1009	16.63	1014	16.71
$40000 < D < 50000$	2033	33.38	1017	16.70	1016	16.68
$50000 < D < 60000$	2019	33.25	1011	16.65	1008	16.60
$60000 < D < 70000$	2030	33.37	1013	16.65	1017	16.72
$70000 < D < 80000$	2028	33.41	1015	16.72	1013	16.69
$80000 < D < 90000$	2027	33.31	1015	16.68	1012	16.63
$90000 < D < 100000$	2024	33.28	1010	16.61	1014	16.68
$500000 < D < 510000$	2026	33.31	1013	16.66	1013	16.66
$1000000 < D < 1010000$	2027	33.34	1015	16.70	1012	16.65

TABLE 2. (Absolute numbers and frequencies of D-types.)

radicands		total		IA		IB
	#	%	#	%	#	%
$2 \leq D < 50$	30	60.00	11	36.67	11	36.67
$2 \leq D < 100$	60	60.00	20	33.33	21	35.00
$2 \leq D < 200$	121	60.50	41	33.88	42	34.71
$2 \leq D < 500$	305	61.00	102	33.44	103	33.77
$2 \leq D < 1000$	607	60.70	204	33.61	204	33.61
$2 \leq D < 2000$	1214	60.70	404	33.28	408	33.61
$2 \leq D < 5000$	3041	60.82	1015	33.38	1018	33.48
$2 \leq D < 10000$	6082	60.82	2027	33.33	2030	33.38
$2 \leq D < 15000$	9119	60.79	3039	33.33	3043	33.37
$2 \leq D < 20000$	12159	60.80	4056	33.36	4055	33.35
$2 \leq D < 50000$	30400	60.80	10134	33.34	10135	33.34
$2 \leq D < 100000$	60793	60.79	20267	33.34	20267	33.34

radicands		II		IIA		IIB
	#	%	#	%	#	%
$2 \leq D < 50$	8	26.67	3	10.00	5	16.67
$2 \leq D < 100$	19	31.67	8	13.33	11	18.33
$2 \leq D < 200$	38	31.41	17	14.05	21	17.36
$2 \leq D < 500$	100	32.79	48	15.73	52	17.05
$2 \leq D < 1000$	199	32.78	97	15.98	102	16.80
$2 \leq D < 2000$	402	33.11	199	16.39	203	16.72
$2 \leq D < 5000$	1008	33.15	502	16.51	506	16.64
$2 \leq D < 10000$	2025	33.30	1009	16.59	1016	16.71
$2 \leq D < 15000$	3037	33.30	1515	16.61	1522	16.69
$2 \leq D < 20000$	4048	33.29	2021	16.62	2027	16.67
$2 \leq D < 50000$	10131	33.33	5061	16.65	5070	16.68
$2 \leq D < 100000$	20259	33.33	10125	16.66	10134	16.67

TABLE 3. (Relative numbers and frequencies of PF-type I in the various D-types.)

radicands	total		IA		IB	
	#	%	#	%	#	%
$0 < D < 10000$	4838	79.55	1658	81.80	2030	100.00
$1000 < D < 2000$	4939	81.27	1689	83.24	2025	100.00
$2000 < D < 3000$	4988	82.01	1710	84.44	2030	100.00
$3000 < D < 4000$	4991	82.25	1704	84.23	2022	100.00
$4000 < D < 5000$	5007	82.20	1711	84.29	2028	100.00
$5000 < D < 6000$	5017	82.63	1714	84.56	2026	100.00
$6000 < D < 7000$	5034	82.76	1707	84.34	2029	100.00
$7000 < D < 8000$	5018	82.66	1713	84.76	2022	100.00
$8000 < D < 9000$	5057	83.09	1720	84.52	2024	100.00
$9000 < D < 100000$	5054	83.11	1722	85.00	2031	100.00
$500000 < D < 510000$	5137	84.46	1737	85.69	2029	100.00
$1000000 < D < 1010000$	5119	84.21	1729	85.38	2027	100.00
radicands	II		IIA		IIB	
	#	%	#	%	#	%
$0 < D < 10000$	1150	56.79	576	57.09	574	56.50
$1000 < D < 2000$	1225	60.55	612	60.47	613	60.63
$2000 < D < 3000$	1248	61.57	620	61.14	628	61.99
$3000 < D < 4000$	1265	62.53	638	63.23	627	61.83
$4000 < D < 5000$	1268	62.37	633	62.24	635	62.50
$5000 < D < 6000$	1277	63.25	639	63.21	638	63.29
$6000 < D < 7000$	1298	63.94	649	64.07	649	63.82
$7000 < D < 8000$	1283	63.26	649	63.94	634	62.59
$8000 < D < 9000$	1313	64.78	654	64.43	659	65.12
$9000 < D < 100000$	1301	64.28	651	64.46	650	64.10
$500000 < D < 510000$	1371	67.67	686	67.72	685	67.62
$1000000 < D < 1010000$	1363	67.24	679	66.90	684	67.59

TABLE 4. (Absolute numbers and frequencies of PF-type I in the various D-types.)

radicands		total		IA		IB
	#	%	#	%	#	%
$2 \le D < 50$	21	70.00	8	72.73	11	100.00
$2 \le D < 100$	41	68.33	14	70.00	21	100.00
$2 \le D < 200$	86	71.07	31	75.61	42	100.00
$2 \le D < 500$	228	74.75	79	77.45	103	100.00
$2 \le D < 1000$	463	76.28	161	78.92	204	100.00
$2 \le D < 2000$	936	77.10	321	79.46	408	100.00
$2 \le D < 5000$	2393	78.69	823	81.08	1018	100.00
$2 \le D < 10000$	4838	79.55	1658	81.80	2030	100.00
$2 \le D < 15000$	7306	80.12	2500	82.26	3043	100.00
$2 \le D < 20000$	9777	80.41	3347	82.52	4055	100.00
$2 \le D < 50000$	24763	81.46	8472	83.60	10135	100.00
$2 \le D < 100000$	49943	82.15	17048	84.12	20267	100.00
radicands		II		IIA		IIB
	#	%	#	%	#	%
$2 \le D < 50$	2	25.00	1	33.33	1	20.00
$2 \le D < 100$	6	31.58	2	25.00	4	36.36
$2 \le D < 200$	13	34.21	6	35.29	7	33.33
$2 \le D < 500$	46	46.00	23	47.92	23	44.23
$2 \le D < 1000$	98	49.25	51	52.58	47	46.08
$2 \le D < 2000$	207	51.49	106	53.27	101	49.75
$2 \le D < 5000$	552	54.76	277	55.18	275	54.35
$2 \le D < 10000$	1150	56.79	576	57.09	574	56.50
$2 \le D < 15000$	1763	58.05	886	58.48	877	57.62
$2 \le D < 20000$	2375	58.67	1188	58.78	1187	58.56
$2 \le D < 50000$	6156	60.76	3079	60.84	3077	60.69
$2 \le D < 100000$	12628	62.33	6321	62.43	6307	62.24

TABLE 5. (Relative numbers and frequencies of unit group index $(E_K : E_{\mathcal{O}}) = 3$ in both PF-types for $D \equiv 5(\mathrm{mod}8)$.)

radicands	total		PF I		PF II	
	#	%	#	%	#	%
$0 < D < 10000$	748	73.62	430	74.91	318	71.95
$10000 < D < 20000$	739	73.10	450	73.41	289	72.61
$20000 < D < 30000$	718	70.88	457	72.77	261	67.79
$30000 < D < 40000$	714	70.41	447	71.29	267	68.99
$40000 < D < 50000$	742	73.03	467	73.54	275	72.18
$50000 < D < 60000$	679	67.36	437	68.50	242	65.41
$60000 < D < 70000$	715	70.31	467	71.96	248	67.39
$70000 < D < 80000$	699	69.00	439	69.24	260	68.60
$80000 < D < 90000$	709	70.06	470	71.32	239	67.71
$90000 < D < 100000$	729	71.89	465	71.54	264	72.53
$500000 < D < 510000$	726	71.67	481	70.22	245	74.70
$1000000 < D < 1010000$	695	68.68	476	69.59	219	66.77

TABLE 6. (Absolute numbers and frequencies of unit group index $(E_K : E_{\mathcal{O}}) = 3$ in both PF-types for $D \equiv 5(\mathrm{mod} 8)$.)

radicands	total		PF I		PF II	
	#	%	#	%	#	%
$2 \leq D < 50$	4	80.00	1	100.00	3	75.00
$2 \leq D < 100$	10	90.91	4	100.00	6	85.71
$2 \leq D < 200$	17	80.95	6	85.71	11	78.57
$2 \leq D < 500$	42	80.77	21	91.30	21	72.41
$2 \leq D < 1000$	77	75.49	39	82.98	38	69.09
$2 \leq D < 2000$	158	77.83	82	81.19	76	74.51
$2 \leq D < 5000$	380	75.10	213	77.46	167	72.29
$2 \leq D < 10000$	748	73.62	430	74.91	318	71.95
$2 \leq D < 15000$	1129	74.18	657	74.92	472	73.18
$2 \leq D < 20000$	1487	73.36	880	74.14	607	72.26
$2 \leq D < 50000$	3661	72.21	2251	73.16	1410	70.75
$2 \leq D < 100000$	7192	70.92	4529	71.81	2663	69.59

TABLE 7. (Maximal primitive period lengths of the chains of lattice minima in the order $\mathcal{O} = \mathbf{Z} \oplus \mathbf{Z}\sqrt{D}$, and for D-type II also in the order $\mathcal{O}_K = \mathbf{Z} \oplus \mathbf{Z}\frac{1}{2}(1 + \sqrt{D})$.)

radicands	$PL(\mathcal{O}_K)_{\max}$	$PL(\mathcal{O})_{\max}$	$\lfloor\sqrt{D} \log\log D\rfloor$
$0 < D < 10000$	173	217	222
$10000 < D < 20000$	261	332	324
$20000 < D < 30000$	326	388	404
$30000 < D < 40000$	378	449	472
$40000 < D < 50000$	443	544	533
$50000 < D < 60000$	487	566	587
$60000 < D < 70000$	537	618	638
$70000 < D < 80000$	564	696	686
$80000 < D < 90000$	626	720	730
$90000 < D < 100000$	648	750	773
$500000 < D < 510000$	1606	1866	1840
$1000000 < D < 1010000$	2353	2492	2640

TABLE 8. (The typical spacing of lattice minima in the first primitive period of the maximal order $\mathcal{O}_K$ and of the suborder $\mathcal{O}$ in D-type II fields.)

D	mod 8	PF	$PL(\mathcal{O}_K)$	$PL(\mathcal{O})$	$PL(\mathcal{O}/PL(\mathcal{O}_K)$
1000101	5	-3	514	1498	2.914
1000141	5	-19	590	1774	3.007
1000189	5	-263	522	1562	2.992
1000261	5	271	588	552	0.939
1000381	5	-1	495	489	0.988
1000429	5	-1	567	1763	3.109
1000437	5	3	400	400	1.000
1000509	5	3	412	432	1.049
1000669	5	-1	503	1503	2.988
1000741	5	-7	674	2006	2.976
1000861	5	-1	825	2409	2.920
1000981	5	-1	593	1769	2.983
1001149	5	-491	606	1786	2.947
1001173	5	-1	403	421	1.045
1001221	5	-1	389	403	1.036
1001269	5	-31	598	1794	3.000
1001389	5	-1	747	2247	3.008
1001509	5	-19	398	414	1.040
1001629	5	-1	429	407	0.949
1000081	1	-1	1693	1687	0.996
1000321	1	7	1820	1824	1.002
1000393	1	-1	1525	1539	1.009
1000609	1	-1	1849	1871	1.012
1000849	1	-1	1779	1725	0.970
1001089	1	-1	1515	1477	0.975
1001209	1	-11	1562	1546	0.990
1001401	1	-1	2139	2117	0.990
1001449	1	-67	2078	2042	0.983
1001569	1	-1	1699	1673	0.985
1001809	1	-1	1841	1807	0.982

TABLE 8. (The typical spacing of lattice minima in the first primitive period of the maximal order $\mathcal{O}_K$ and of the suborder $\mathcal{O}$ in D-type II fields.)

D	j	$j/PL(\mathcal{O})$
1000101	510	0.34
1000141	576	0.32
1000189	518	0.33
1000429	583	0.33
1000669	517	0.34
1000741	666	0.33
1000861	797	0.33
1000981	579	0.33
1001149	590	0.33
1001269	608	0.34
1001389	745	0.33

References

[1] P. Barrucand and H. Cohn, A rational genus, class number divisibility, and unit theory for pure cubic fields, *J. Number Theory* **2** (1970), 7–21.

[2] B. D. Beach and H. C. Williams, Some computer results on periodic continued fractions, Proc. 2nd Louisiana Conf. on Combinatorics Graph Theory and Computing, *Louisiana State Univ., Baton Rouge, Louisiana*, 1971, pp. 133–146.

[3] B. D. Beach and H. C. Williams, A numerical investigation of the diophantine equation $x^2 - dy^2 = -1$, Proc. 3rd Southeastern Conf. on Combinatorics, Graph Theory and Computing, *Florida Atlantic Univ., Boca Raton, Florida*, 1972, pp. 37–68.

[4] A. J. Brentjes, Multi-dimensioanl continued fraction algorithms, *Mathematical centre tracts* **145**, Mathematisch Centrum, Amsterdam, 1981.

[5] J. Buchmann, Zahlengeometrische Kettenbruchalgorithmen zur Einheitenberechnung, *Dissertation, Köln,* 1982.

[6] J. Buchmann, A generalization of Voronoi's unit algorithm I, *J. Number Theory* **20** (1985), 177–191.

[7] J. Buchmann, On the computation of units and class numbers by a generalization of Langrange's algorithm, *J. Number Theory* **26** (1987), 8–30.

[8] R. Dedekind, Vorlesungen über Zahlentheorie von P. G. Lejeune Dirichlet, 4. Auflage, *Vieweg, Braunscheig,* 1894.

[9] V. Ennola and R. Turunen, Tables of totally real cubic fields, *private communication.*

[10] V. Ennola and R. Turunen, On totally real cubic fields, *Math. Comp.* **44** (1985), no. 170, 495–518.

[11] F. Halter-Koch, Über Pell'sche Gleichungen und Kettenbrücke, *Arch. Math.* **49** (1987), 29–37.

[12] H. Hasse, Zahlentheorie, 2. Auflage, *Akademie-Verlag, Berlin,* 1963.

[13] H. Hasse, Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage, *Math. Zeitschrift* **31** (1930), 565–582.

[14] H. HASSE, Bericht über Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Teil I, *Jahresber. der DMV* **35** (1926), 1–55. Teil Ia, *Jahresber. der DMV* **36** (1927), 233–311.

[15] D. HILBERT, Die Theorie der algebraischen Zahlkörper, *Jahresber. der DMV* **4** (1897), 175–546.

[16] P. KAPLAN and K. S. WILLIAMS, Pell's equations $X^2 - mY^2 = -1, -4$ and continued fractions, *J. Number Theory* **23** (1986), 169-182.

[17] R. KORTUM and G. MCNIEL, A table of periodic continued fractions, Lockheed Aircraft Corporation, *Sunnyvale, California,* 1961.

[18] T. KUBOTA, Über die Beziehung der Klassenzahlen der Unterkörper des bizyklischen biquadratischen Zahlkörpers, *Nagoya Math. J.* **6** (1953), 119–127.

[19] T. KUBOTA, Über den bizyklischen biquadratischen Zahlkörper, *Nagoya Math. J.* **10** (1956), 65–85.

[20] J. C. LAGARIAS, On the computational complexity of determining the solvability of the equation $X^2 - DY^2 = -1$, *Trans. Amer. Math. Soc.* **260** (1980), 485–508.

[21] D. C. MAYER, Differential principal factors and units in pure cubic number fields, *to appear.*

[22] H. MINKOWSKI, Zur Geometrie der Zahlen, Gesammelte Abh., *Teubner, Leipzig,* 1911, Bd. 1, 243–371, Bd. 2, 3–100.

[23] P. MORTON, On Rédei's theory of the Pell equation, *J. reine angew. Math* **307/308** (1979), 373–398.

[24] W. PATZ, Tafel der regelmässigen Kettenbrüche und ihrer vollständigen Quotienten für die Quadratwurzeln aus den natürlischen Zahlen von 1–10000, *Akademie-Verlag, Berlin,* 1955.

[25] O. PERRON, Die Lehre von den Kettenbrüchen, Bd. 1, 3. Auflage, *Teubner, Stuttgart,* 1954.

[26] L. RÉDEI, Über die Pellsche Gleichung $t^2 - du^2 = -1$, *J. reine angew. Math.* **173** (1935), 193–211.

[27] L. RÉDEI, Bedingtes Artinsches Symbol mit Anwendung in der Klassenkörpertheorie, *Acta Math. Acad. Sci. Hung.* **4** (1953), 1–29.

[28] L. RÉDEI, Die 2-Ringklassengruppe des quadratischen Zahlkörpers und die Theorie der Pellschen Gleichung, *Acta Math. Acad. Sci. Hung.* **4** (1953), 31–87.

[29] D. SHANKS, Review of [17], *Math. Comp.* **16** (1962), 377–379.

[30] D. SHANKS, A survey of quadratic, cubic and quartic algebraic number fields (from a computational point of view), Proc. 7th Southeastern Conf. on Combinatorics, Graph Theory and Computing, *Florida, Atlantic Univ., Boca Raton, Florida,* 1976, pp. 15–40.

[31] R. STEINER, On the units in algebraic number fields, Proc. 6th Manitoba Conf. on Numerical Math., *Univ. of Manitoba, Winnipeg, Manibota,* 1976, pp. 413–435.

[32] H.-J. STENDER, Zur Parametrisierung reell-quadratischer Zahlkörper, *J. reine angew. Math.* **311/312** (1979), 291–301.

[33] G. F. VORONOI, On a generalization of the algorithm of continued fractions, *Doctoral Dissertation, Warsaw,* 1896, (Russian).

[34] H. C. WILLIAMS and C. R. ZARNKE, Computation of the solutions of the diophantine equation $x^2 - d^4 = 1$, Proc. 3rd Southeastern Conf. on Combinatorics, Graph Theory and Computing, *Florida Atlantic Univ., Boca Raton, Florida,* 1972, pp. 463–483.

[35] H. C. WILLIAMS and C. R. ZARNKE, Computer solution of the diophantine equation $x^2 - dy^4 = -1$, Proc. 2nd Manibota Conf. on Numerical Math., *Univ. of Manibota, Winnipeg, Manibota,* 1972, pp. 405–416.

[36] H. C. WILLIAMS and J. BROERE, A computational technique for evaluating $L(1,\chi)$ and the class number of a real quadratic field, *Math. Comp.* **30** (1976), no. 136, 887–893.

[37] H. C. WILLIAMS, A numerical investigation into the length of the period of the continued fraction expansion of $\sqrt{D}$, *Math. Comp.* **36** (1981), no. 154, 593–601.

[38] H. C. WILLIAMS, Determination of principal factors in $\mathbf{Q}(\sqrt{D})$ and $\mathbf{Q}(\sqrt[3]{D})$, *Math. Comp.* **38** (1982), no. 157, 261–274.

[39] H. C. WILLIAMS, Continued fractions and number-theoretic computations, Proc. Number Theory Conference, Edmonton, 1983, *Rocky Mountain J. Math.* **15** (1985), 621–655.

DANIEL C. MAYER
INSTITUT FÜR MATHEMATIK
KARL-FRANZENS-UNIVERSITÄT
ELISABETHSTRAßE 16
A-8010 GRAZ
AUSTRIA

(Received August 18, 1988)