MATHEMATICS OF COMPUTATION, VOLUME 31, NUMBER 139
JULY 1977, PAGES 754–770

An Effective Number Geometric Method of Computing the Fundamental Units of an Algebraic Number Field

By Michael Pohst and Hans Zassenhaus

Abstract. The Minkowski method of unit search is applied to particular types of parallelotopes permitting to discover algebraic integers of bounded norm in a given algebraic number field of degree n at will by solving successively $2n$ linear inequalities for one unknown each. Application is made to the unit search for all totally real number fields of minimal discriminant for $n \leqslant 7$.

Introduction. Many methods have been devised for producing maximal sets of independent units of an integral domain $\mathfrak{O}$ with a finite basis $\omega_1, \ldots, \omega_n$ over the rational integer ring, $\mathbf{Z}$. The number geometric methods devised so far always lead to a large number of linear inequalities for n unknowns simultaneously. It is the purpose of this note to reduce the application of number geometric methods to sequences of n pairs of linear inequalities, each only for one unknown.

1. Parallelotopes of Bounded Norm. Denoting by r_1 the number of distinct isomorphisms of $\mathfrak{O}$ into the real number field, $\mathbf{R}$, say

$$\mathfrak{O} \longrightarrow \mathbf{R}\colon \theta_i \qquad (1 \leqslant i \leqslant r_1)$$

and denoting by $2r_2$ the number of the remaining isomorphisms of $\mathfrak{O}$ into the complex number field, $\mathbf{C}$, say

$$\mathfrak{O} \longrightarrow \mathbf{C}\colon \theta_{r_1+i} \qquad (1 \leqslant i \leqslant 2r_2),$$

where

$$\alpha\theta_{r_1+r_2+i} = (\alpha\theta_{r_1+i})^* \qquad (1 \leqslant i \leqslant r_2), \tag{1}$$

it follows from Dirichlet's unit theorem that every set of independent units of $\mathfrak{O}$ can be extended to a set of

$$r = r_1 + r_2 - 1 \tag{2}$$

independent units and that any set of r independent units is a maximal independent set of units.

Moreover,

Received March 18, 1976; revised September 9, 1976.
AMS (MOS) subject classifications (1970). Primary 12A45.

* $\alpha^* = R\alpha - I\alpha j$ denotes the complex conjugate of the complex number $\alpha = \mathrm{R}\alpha + I\alpha j$ with real part $R\alpha$ and imaginary part $I\alpha$ both contained in R and $j^2 = -1$, the imaginary unit.

(3) $$n = r_1 + 2r_2.$$

The applications of number geometric methods to the task of determining maximal independent unit sets of $\mathcal{O}$ hinge on the possibility of an additive homomorphism ι of $\mathcal{O}$ into the n-dimensional vector space $\mathbf{C}^{1\times n}$ over the complex number field $\mathbf{C}$ with the property that the norm of an element ω is equal to the value of a certain homogeneous polynomial N_ι of degree n on $\omega\iota$.

It can be shown easily that ι is monomorphic, that the embedding ι is unique up to a nonsingular linear transformation over $\mathbf{C}$, that $\mathcal{O}\iota$ is a discrete subset of $\mathbf{C}^{1\times n}$ in the customary sequential topology and that the linear space $\mathbf{R}\mathcal{O}\iota$ is of dimension n over $\mathbf{R}$. In other words ι maps $\mathcal{O}$ one-to-one on an n-dimensional lattice. (H. Hasse, *Zahlentheorie,* 3. Auflage, Akademie Verlag, Berlin, 1969, pp. 516–520.)

The usual choice of ι is the Minkowski coordinatization

$$\mathcal{O} \longrightarrow \mathbf{R}^{1\times n}\colon \iota_1,$$

(4a) $$\omega\iota_1 = (\omega\theta_1, \ldots, \omega\theta_{r_1}, R(\omega\theta_{r_1+1})/\sqrt{2},$$
$$I(\omega\theta_{r_1+1})/\sqrt{2}, \ldots, R(\omega\theta_{r_1+r_2})/\sqrt{2}, I(\omega\theta_{r_1+r_2})/\sqrt{2}),$$

which has the advantage of employing only real coordinates with norm form

(5a) $$N_{\iota_1}(x_1, \ldots, x_n) = 2^{-r_2} \prod_{i=1}^{r_1} x_i \prod_{j=1}^{r_2} (x_{r_1+2j-1}^2 + x_{r_1+2j}^2).$$

More satisfactory from the theoretical vantage point is the coordinatization

(4b) $$\mathcal{O} \longrightarrow \mathbf{C}^{1\times n}\colon \iota_2, \qquad \omega\iota_2 = (\omega\theta_1, \omega\theta_2, \ldots, \omega\theta_n) \qquad (\omega \in \mathcal{O}),$$

with norm form

(5b) $$N_{\iota_2}(x_1, x_2, \ldots, x_n) = \prod_{i=1}^{n} x_i.$$

For practical purposes we shall use the coordinatization

$$\mathcal{O} \longrightarrow \mathbf{R}^{1\times n}\colon \iota_3,$$

(4c) $$\omega\iota_3 = \left(\sum_{i=1}^{n} \lambda_i\omega_i\right)\iota_3 = (\lambda_1, \lambda_2, \ldots, \lambda_n) \qquad (\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbf{Z}),$$

with norm form

(5c) $$N_{\iota_3}(\omega) = \det(\omega\Delta),$$

where Δ denotes the right regular matrix representation

(6) $$\mathcal{O} \longrightarrow \mathbf{Z}^{n\times n}\colon \Delta, \qquad \omega\Delta = (\lambda_{ik}(\omega)), \qquad \omega_i\omega = \sum_{k=1}^{n} \lambda_{ik}(\omega)\omega_k,$$

of $\mathcal{O}$ with respect to the $\mathbf{Z}$-basis $\omega_1, \ldots, \omega_n$.

Any ρ elements $v_1, \ldots, v_\rho$ of $\mathbf{C}^{1\times n}$ that are linearly independent over $\mathbf{R}$

generate the discrete submodule $\vec{L} = \dot{\Sigma}_{i=1}^{\rho} \mathbf{Z}v_i$, also called a *$\rho$-vector lattice*. It determines the *basic parallelotope*

$$\Pi(v_1, \ldots, v_\rho) = \left\{ \sum_{i=1}^{\rho} \xi_i v_i \mid \xi_i \in \mathbf{R}, -\tfrac{1}{2} \leqslant \xi \leqslant \tfrac{1}{2}, 1 \leqslant i \leqslant \rho \right\} \tag{7}$$

of $\vec{L}$ with the property that its translates under the translations by vectors belonging to $\vec{L}$ provide a packing of the ρ-dimensional space $\mathbf{R}\vec{L}$ over $\mathbf{R}$ by convex closed parallelotopes centered at the members of $\vec{L}$.

The linear space $\mathbf{C}^{1\times n}$ of dimension n over $\mathbf{C}$ is metricized by standard unitary distance:

$$d(x, y) = |((x - y)\,(x - y)^t)^{1/2}|^{**} \tag{8a}$$

giving rise to the ρ-volume measurement

$$V_\rho(v_1, \ldots, v_\rho) = |\det((v_i v_k^t))^{1/2}| \qquad (i = 1, 2, \ldots, \rho), \tag{8b}$$

which turns out to be invariant under the unitary subgroup

$$U(n) = \{x \mid x \in \mathbf{C}^{n\times n} \;\&\; xx^t = I_n\}, \tag{8c}$$

of the general linear group of degree n over $\mathbf{C}$ applied to $v_1, v_2, \ldots, v_\rho$ on the right. The application of a matrix X of degree ρ over $\mathbf{C}$ to the $\rho \times n$-matrix V with ρ rows $v_1, \ldots, v_\rho$ yields the matrix XV with ρ rows $w_1, w_2, \ldots, w_\rho$ such that $V_\rho(w_1, w_2, \ldots, w_\rho) = |\det X| V_\rho(v_1, \ldots, v_\rho)$. It yields a positive measure in case $v_1, \ldots, v_\rho$ are linearly independent over $\mathbf{R}$, but zero in case $v_1, \ldots, v_\rho$ are linearly dependent over $\mathbf{R}$.

The number

$$|\vec{L}| = \left| \dot{\Sigma}_{i=1}^{\rho} \mathbf{Z}v_i \right| = V_\rho(v_1, \ldots, v_\rho) \tag{8d}$$

is independent of the choice of the lattice basis $v_1, \ldots, v_\rho$ of the ρ-vector lattice $\vec{L}$. It is called the *mesh* of $\vec{L}$ due to the fact that its value gives an idea of the space about each lattice point. For example, if $\vec{L}_1$ is a ρ-sublattice of $\vec{L}$, i.e. $\vec{L}_1$ is a submodule of the discrete module $\vec{L}$ of $\mathbf{R}$-dimension ρ, then the group theoretic index of $\vec{L}_1$ in $\vec{L}$, i.e. the number $\vec{L} : \vec{L}_1$ counting the cosets of $\vec{L}$ over $\vec{L}_1$ is equal to the mesh quotient:

$$|\vec{L}_1|/|\vec{L}| = \vec{L} : \vec{L}_1. \tag{8}$$

For our coordinatizations we find that

$$|\mathfrak{O}\iota_1| = |\mathfrak{O}\iota_2| = |d(\mathfrak{O}\iota/\mathbf{Z})^{1/2}|, \tag{9a}$$

$$|\mathfrak{O}\iota_3| = 1, \tag{9b}$$

where

**where $(\alpha_{ki}^*) = (\alpha_{ik})^t$ denotes the hermitian transpose of the rectangular matrix $(\alpha_{ik}) \in \mathbf{C}^{p\times q}$ $(\alpha_{ik} \in \mathbf{C};\ 1 \leqslant i \leqslant p,\ 1 \leqslant k \leqslant q;\ p, q \in \mathbf{Z}^{>0})$.

(10) $$d(\mathcal{O}/\mathbf{Z}) = \det(\mathrm{tr}((\omega_i\Delta)(\omega_k\Delta)))$$

is the discriminant of the order $\mathcal{O}$ over $\mathbf{Z}$ which by (10) is defined as a nonzero rational integer independent of the choice of the $\mathbf{Z}$-basis $\omega_1, \ldots, \omega_n$.

According to the first fundamental theorem of Minkowski's Geometry of Numbers, any convex body of $\mathbf{R}\mathcal{O}\iota$ centered at the origin contains a nonzero lattice vector of $\mathcal{O}\iota$ in case its volume is not smaller than 2^n times the mesh of the n-lattice $\mathcal{O}\iota$. In particular, the parallelotope

$$\hat{\Pi}(1) = 2\Pi(\omega_1\iota, \ldots, \omega_n\iota) = \left\{ \sum_{i=1}^{n} \xi_i\omega_i\iota \mid \xi_i \in \mathbf{R}, -1 \leqslant \xi_i \leqslant 1, 1 \leqslant i \leqslant n \right\}$$

and the parallelotopes derived from it by a linear transformation of $\omega_1\iota, \ldots, \omega_n\iota$ of degree n and determinant 1 over $\mathbf{R}$ always contain a nonzero member of $\mathcal{O}\iota$.

Evidently, the estimate obtained above is sharp in many instances.

In his initial applications to the task of unit search H. Minkowski formed parallelotopes which in his coordinatization were rectangular and parallel to the coordinate axes. This application has the effect that one has to consider irrational coordinates of the lattice points subject to $2n$ linear inequalities involving all of the unknowns at once.

Apply the fundamental theorem to those parallelotopes

$$\hat{\Pi}(\omega) = 2|N_{\iota_3}(\omega)^{-1/n}|\Pi((\omega_1\omega)\iota_3, (\omega_2\omega)\iota_3, \ldots, (\omega_n\omega)\iota_3)$$

obtained upon transition from the $n \times n$ matrix V with row vectors $2\omega_1\iota_3$, $2\omega_2\iota_3$, $\ldots$, $2\omega_n\iota_3$ to the matrix

$$V\omega\Delta/|N_{\iota_3}(\omega)^{1/n}|$$

of the same determinant using some nonzero element ω of $\mathcal{O}$.

This application will have the effect that we will work with integral rational coordinates of the lattice points subject only to two linear inequalities for each of the unknown coordinates in sequence.

We observe that the norm function on $\mathcal{O}$ defined by setting

(11a) $$N(\omega) = \det(\omega\Delta) \qquad (\omega \in \mathcal{O})$$

is independent of the choice of the $\mathbf{Z}$-basis $\omega_1, \ldots, \omega_n$ and coincides with the norm function N_ι referred to above. It is by definition a multiplicative homomorphism of $\mathcal{O}$ in $\mathbf{Z}$ such that

(11b) $$N(\alpha\beta) = N(\alpha)N(\beta) \qquad (\alpha, \beta \in \mathcal{O}),$$

(11c) $$N(\lambda) = \lambda^n \qquad (\lambda \in \mathbf{Z}).$$

It is easily computed for any element ω of $\mathcal{O}$ with given right regular representation $\omega\Delta$ upon forming the Hermitian column reduced matrix

$$(\omega\Delta)U(\omega) = (\alpha_{ik}(\omega)) \tag{11d}$$

$$(U(\omega) \in SL(n, \mathbf{Z});\ \alpha_{ik}(\omega) \in \mathbf{Z},\ \alpha_{ik}(\omega) = 0 \text{ if } 1 \leqslant i < k \leqslant n).$$

Simply:

$$N(\omega) = \prod_{i=1}^{n} \alpha_{ii}(\omega). \tag{11e}$$

It is convenient to determine the integral matrix $(\beta_{ik}(\omega))$ solving the matrix equation

$$(\alpha_{ik}(\omega))(\beta_{ik}(\omega)) = N(\omega)I_n \tag{11f}$$

by the recursive sequence of equations

$$\beta_{ik}(\omega) = 0 \qquad \text{if } 1 \leqslant i < k \leqslant n, \tag{11g}$$

$$\beta_{ii}(\omega) = N(\omega)/\alpha_{ii}(\omega) \quad \text{if } 1 \leqslant i \leqslant n, \tag{11h}$$

$$\sum_{j=1}^{i} \alpha_{ij}(\omega)\beta_{jk}(\omega) = 0 \quad \text{if } 1 \leqslant k < i \leqslant n. \tag{11i}$$

It follows that the inequalities

$$-1 \leqslant \xi_i \leqslant 1 \qquad (1 \leqslant i \leqslant n)$$

for the lattice points

$$\eta = (\eta_1, \eta_2, \ldots, \eta_n) \in \mathbf{Z}^{1\times n} \cap \hat{\Pi}(\omega) \tag{11j}$$

with

$$\eta = \xi(\omega\Delta)|N(\omega)^{-1/n}|, \tag{11k}$$

$$\xi = (\xi_1, \xi_2, \ldots, \xi_n), \tag{11l}$$

after the unimodular substitutions

$$\zeta = \eta U(\omega) = (\zeta_1, \zeta_2, \ldots, \zeta_n), \tag{11m}$$

amount to the triangular set of inequalities

$$\begin{aligned}
&-|N(\omega)^{(n-1)/n}| \leqslant \zeta_n\beta_{nn}(\omega) \leqslant |N(\omega)^{(n-1)/n}| \\
&-|N(\omega)^{(n-1)/n}| \leqslant \zeta_{n-1}\beta_{n-1,n-1}(\omega) + \zeta_n\beta_{n,n-1}(\omega) \leqslant |N(\omega)^{(n-1)/n}| \\
&\qquad\qquad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
&-|N(\omega)^{(n-1)/n}| \leqslant \zeta_1\beta_{11}(\omega) + \cdots + \zeta_{n-1}\beta_{n-1,1}(\omega) + \zeta_n\beta_{n1}(\omega) \\
&\qquad\qquad \leqslant |N(\omega)^{(n-1)/n}|.
\end{aligned} \tag{11n}$$

They are solved recursively one after another yielding a finite number of lattice points

$$\eta = \zeta U^{-1}(\omega) \in \mathbf{Z}^{1\times n}. \tag{11o}$$

By construction the corresponding elements, $\eta\iota_3^{-1}$ of $\mathcal{O}$ have absolute norms bounded by the maximum of the norm function on $\hat{\Pi}(1)$.

Upon choosing ω randomly in $\mathcal{O}$ in several ways so that never any one of them is a rational multiple of another, we get as many elements of bounded absolute norm as we like by the number geometric method explained above. The principles of an efficient choice of ω partially depend on mathematical intuition. It is of course desirable that scientific principles guiding our direction be developed. This aim underlies the investigations of a forthcoming paper.

2. Unit Search I. According to Dirichlet's Theorem (see [1], [6]) the logarithmic mapping

$$\mathbf{Q}\mathcal{O}\setminus\{0\} \longrightarrow \mathbf{R}^{1\times n}\colon \operatorname{Log},\ \epsilon\ \operatorname{Log} = (\log|\epsilon\theta_1|, \ldots, \log|\epsilon\theta_n|) \qquad (0 \neq \epsilon \in \mathbf{Q}\mathcal{O}) \tag{12a}$$

is a multiplicative to additive homomorphism of the multiplicative group of $\mathbf{Q}\mathcal{O}$ in $\mathbf{R}^{1\times n}$. The kernel of its restriction to the unit group $U(\mathcal{O})$ is the torsion subgroup $TU(\mathcal{O})$ of $U(\mathcal{O})$, a cyclic group of finite order $w(\mathcal{O})$. The image of $U(\mathcal{O})$ is an r-dimensional lattice spanning the linear subspace

$$\mathbf{R}(U(\mathcal{O})\operatorname{Log}) = \left\{(x_1, \ldots, x_n) \mid x_i \in \mathbf{R},\ 1 \leqslant i \leqslant n\ \&\ \sum_{i=1}^{n} x_i = 0 \right. \tag{12b}$$
$$\left. \&\ x_{r_1+j} = x_{r_1+r_2+j},\ 1 \leqslant j \leqslant r_2 \right\}.$$

In order to determine $TU(\mathcal{O})$ remember that the generators of $TU(\mathcal{O})$ are the roots of the cyclotomic polynomial

$$\varphi_{w(\mathcal{O})}(t) = \prod_{1\leqslant d \mid w(\mathcal{O})} (t^d - 1)^{\mu(w(\mathcal{O})/d)} \tag{12c}$$

of degree $\varphi(w(\mathcal{O}))$ over $\mathbf{Z}$. Hence

$$\varphi(w(\mathcal{O})) \mid n, \tag{12d}$$

and there exist only finitely many possibilities for $w(\mathcal{O})$, given n, say

$$w_1 > w_2 > \cdots > w_{\kappa(n)-1} > w_{\kappa(n)} = 1.$$

Following the method given in [5], we test whether the polynomial φ_{w_j} has a root ζ in $\mathbf{Q}\mathcal{O}$ for $i = 1, 2, \ldots, j$, until the answer is affirmative for the first time, say $\varphi_{w_j}(\xi) = 0$.

It follows that every unit root of $\mathbf{Q}\mathcal{O}$ is a power of φ.

The first power of ζ belonging to $\mathcal{O}$ generates $TU(\mathcal{O})\operatorname{Log}$; its order is $w(\mathcal{O})$.

Since -1 always is a torsion unit of $\mathcal{O}$, it follows that

$$2 \mid w(\mathcal{O}). \tag{12e}$$

We want to find a set of r fundamental vectors $\eta_1\operatorname{Log}, \ldots, \eta_r\operatorname{Log}$ which form a basis of the unit lattice $U(\mathcal{O})\operatorname{Log}$, i.e. $\eta_1, \eta_2, \ldots, \eta_r$ generate a free abelian subgroup of

$$U(\mathcal{O}) = \ker \operatorname{Log} \times \langle\eta_1\rangle \times \langle\eta_2\rangle \times \cdots \times \langle\eta_r\rangle. \tag{12f}$$

In the course of the search we shall find finitely many units $\epsilon_1, \ldots, \epsilon_\rho$ of $\mathcal{O}$ generating the sublattice $\Sigma_{j=1}^{\rho} \mathbf{Z}\epsilon_j\mathrm{Log}$ of the unit lattice. It will be required to find a $\mathbf{Z}$-basis of that sublattice and to express the generators $\epsilon_j\mathrm{Log}$ as integral linear combinations of the lattice vectors. This will be achieved by means of the Minkowski reduction expounded in Minkowski [3], or simply by Hermite's row reduction, applied to the $\rho \times n$-matrix of the ρ vectors $\epsilon_i\mathrm{Log}$ $(1 \leqslant i \leqslant \rho)$.

The first task is to find r independent units of $\mathcal{O}$, i.e. units $\epsilon_1, \epsilon_2, \ldots, \epsilon_r$ of $\mathcal{O}$ for which the n-rows $\epsilon_1\mathrm{Log}, \epsilon_2\mathrm{Log}, \ldots, \epsilon_r\mathrm{Log}$ are linearly independent.

For this purpose we give two methods, the first one simply carrying out the Dirichlet-Minkowski ideas in a new setting, the second one implementing additional economies obtained by using the action of the automorphism group of the minimal splitting field of $\mathbf{Q}\mathcal{O}$ over $\mathbf{Q}$ and the ideal theory of $\mathcal{O}$.

If $r = 0$, then $TU(\mathcal{O}) = U(\mathcal{O})$; and we are done. Let $r > 0$.

Method I. Suppose we have found already ρ independent units $\epsilon_1, \ldots, \epsilon_\rho$ of $\mathcal{O}$ and $\alpha(\rho)$ nonequivalent elements $\xi_1, \ldots, \xi_{\alpha(\rho)}$ of $\mathcal{O}$ with the properties

$$0 \leqslant \rho < r, \qquad \alpha(\rho) \geqslant 0; \tag{13a}$$

the absolute value of each ξ_i is not larger than

$$\mathrm{lub}\,|N_{\iota_3}(x)|, \qquad x \in 2\Pi(\omega_1\iota_3, \ldots, \omega_n\iota_3). \tag{13b}$$

Proceed as follows.

Choose some nonzero element ω of $\mathcal{O}$ and find the nonzero lattice points of $\hat{\Pi}(\omega)$, say $\pm\varphi_1, \ldots, \pm\varphi_\kappa$.

(a) If one of the quotients φ_j/ξ_i is a unit, then we seek independent units $\epsilon_1', \ldots, \epsilon_{\rho'}'$ of $\mathcal{O}$ generating the same subgroup of $U(\mathcal{O})$ as $\epsilon_1, \epsilon_2, \ldots, \epsilon_\rho, \varphi_j/\xi_i$, taken together with $TU(\mathcal{O})$.

Eliminate $\pm\varphi_j$.

Replace $\epsilon_1, \ldots, \epsilon_\rho$ by $\epsilon_1', \ldots, \epsilon_\rho'$. If $\rho' = r$ then we are done.

(b) If none of the φ_j/ξ_i is a unit, then set $\xi_{\alpha(\rho)+1} = \varphi_j$, $\alpha(\rho) + 1$ to $\alpha(\rho)$ and go on. If all of the φ_j's are run through, then choose another ω. It was shown in [5] that the method will come to a halt as desired after finitely many steps.

Method II requires $\mathcal{O}$ to be a maximal order.

Using the methods of [5], we form the minimal splitting field E generated by the conjugate subfields $\mathbf{Q}\mathcal{O}\theta_j$ $(1 \leqslant j \leqslant n)$ and its automorphism group G, a transitive permutation group on the conjugates of any primitive element Ψ of $\mathbf{Q}\mathcal{O}$ such that the stabilizer of $\mathbf{Q}\mathcal{O}\theta_1 = \mathbf{Q}\mathcal{O}$ is the subgroup H of all automorphisms of E fixing $\mathbf{Q}\mathcal{O}$ elementwise.

Hence,

$$G = \bigcup_{j=1}^{n} H\sigma_j$$

such that

$$\alpha\theta_j = \alpha\sigma_j \qquad (1 \leqslant j \leqslant n), \qquad \sigma_1 = \mathbf{1}.$$

Suppose we have found already ρ independent units $\epsilon_1, \ldots, \epsilon_\rho$ of $\mathcal{O}$, and $\beta(\rho)$ ideals $\mathfrak{A}_1, \ldots, \mathfrak{A}_{\beta(\rho)}$ of $\mathcal{O}$ as well as their inverses $\mathfrak{A}_1^{-1}, \ldots, \mathfrak{A}_{\beta(\rho)}^{-1}$ and $\alpha(\rho)$ elements $\xi_1, \xi_2, \ldots, \xi_{\alpha(\rho)}$ of $\mathcal{O}$ of absolute norm not larger than

$$\operatorname{lub}|N_{\iota_3}(x)|, \qquad x \in 2\Pi(\omega_1\iota_3, \ldots, \omega_n\iota_3)$$

and some $\alpha(\rho) \times \beta(\rho)$-integral matrix $A = (\alpha_{ik})$ such that

(14a) $$0 \leqslant \rho < r, \quad \alpha(\rho) \geqslant 0, \quad \beta(\rho) \geqslant 0,$$

(14b) $$\mathcal{O} \supset \mathfrak{A}_i \qquad (1 \leqslant i \leqslant \beta(\rho)),$$

(14c) $$\mathfrak{A}_i + \mathfrak{A}_k = \mathcal{O} \qquad (1 \leqslant i < k \leqslant \beta(\rho)),$$

(14d) $$0 \neq \xi_i\mathcal{O} = \prod_{k=1}^{\beta(\rho)} \mathfrak{A}_k^{\alpha_{ik}};$$

(14e) the rank of A is equal to $\alpha(\rho)$.

Choose some nonzero element ω of $\mathcal{O}$ and find the nonzero lattice points of $\hat{\Pi}(\omega)$, say $\pm\varphi_1, \pm\varphi_2, \ldots, \pm\varphi_\kappa$.

(a) If $\varphi_j\mathcal{O} = \Pi_{k=1}^{\beta(\rho)}\mathfrak{A}_k^{\nu_k}$ $(0 \leqslant \nu_k \in \mathbf{Z}, 1 \leqslant k \leqslant \beta(\rho))$ and if there is a rational $\alpha(\rho)$-row $\mu_0^{-1}\mu = (\mu_1, \ldots, \mu_{\alpha(\rho)})/\mu_0$ such that $0 \neq \mu_0 \in \mathbf{Z}$ and

(14f) $$\nu\mathbf{Z} + \sum_{i=0}^{\alpha(\rho)} \mathbf{Z}\mu_i = \mathbf{Z},$$

(14g) $$\mu_0^{-1}\mu A = \nu = (\nu_1, \ldots, \nu_{\beta(\rho)}),$$

then because of (14e)–(14g), the rational integers $\mu_0, \mu_1, \ldots, \mu_{\alpha(\rho)}$ are uniquely determined by φ_j and $\mathfrak{A}_1, \ldots, \mathfrak{A}_{\beta(\rho)}$. Furthermore, the quotient

$$\epsilon = \varphi_j^{\mu_0} \Big/ \prod_{i=1}^{\alpha(\rho)} \xi_i^{\mu_i}$$

is a unit of $\mathcal{O}$.

We find independent units $\epsilon_1', \ldots, \epsilon_{\rho'}'$ of $\mathcal{O}$ generating the same subgroup of $U(\mathcal{O})$ as $\epsilon_1, \epsilon_2, \ldots, \epsilon_\rho$ and the units

$$\epsilon, \prod_{\sigma \in H} \epsilon\theta_k\sigma \qquad (1 < k \leqslant n),$$

taken together with $TU(\mathcal{O})$.

Eliminate $\pm\varphi_j$.

Replace $\epsilon_1, \ldots, \epsilon_\rho$ by $\epsilon_1', \ldots, \epsilon_{\rho'}'$.

If $\rho' = r$, then we are done.

Otherwise, rename ρ' to ρ, go on increasing j by 1 if $j < \kappa$.

(b) If

$$\varphi_j 0 = \prod_{k=1}^{\beta(\rho)} \mathfrak{A}_k^{\nu_k} \qquad (0 \leqslant \nu_k \in \mathbf{Z},\ 1 \leqslant k \leqslant \beta(\rho))$$

and if the rank of the matrix $\bar{A}$ obtained by adjoining the $\beta(\rho)$-row $(\nu_1, \ldots, \nu_{\beta(\rho)})$ as $(\alpha(\rho)+1)$st row to A is equal to $\alpha(\rho)+1$, then rename φ_j to $\xi_{\alpha(\rho)+1}$, $\alpha(\rho)+1$ to $\alpha(\rho)$, $\bar{A}$ to A and go on increasing j by 1 if $j < \kappa$. .

(c) If $\varphi_j 0 = \mathfrak{R}\prod_{k=1}^{\beta(\rho)} \mathfrak{A}_k^{\nu_k}$ ($\mathfrak{R} \subset 0$; $\mathfrak{R} \not\subseteq \mathfrak{A}_k$, $0 \leqslant \nu_k \in \mathbf{Z}$, $1 \leqslant k \leqslant \beta(\rho)$), then we replace the ideals $\mathfrak{A}_1, \ldots, \mathfrak{A}_{\beta(\rho)-1}, \mathfrak{A}_{\beta(\rho)}$ as follows:

By several applications of ideal addition and quotient formation of ideals one of which is contained in the other let us form the divisor cascade (see [5, Part II]) determined by $\mathfrak{A}_1, \ldots, \mathfrak{A}_{\beta(\rho)}, \mathfrak{R}$ resulting in ideals $\mathfrak{A}'_1, \ldots, \mathfrak{A}'_{\beta(\rho)'}$ with the properties

$$0 < \beta(\rho)' \in \mathbf{Z}, \tag{15a}$$

$$\mathfrak{A}'_k \subset 0 \qquad (1 \leqslant k \leqslant \beta(\rho)'), \tag{15b}$$

$$\mathfrak{A}'_i + \mathfrak{A}'_k = 0 \qquad (1 \leqslant i < k \leqslant \beta(\rho)'), \tag{15c}$$

$$\mathfrak{A}_i = \prod_{k=1}^{\beta(\rho)'} \mathfrak{A}_i'^{\gamma_{ik}} \qquad (\gamma_{ik} \in \mathbf{Z}^{\geqslant 0},\ 1 \leqslant i \leqslant \beta(\rho),\ 1 \leqslant k \leqslant \alpha(\rho)'), \tag{15d}$$

$$= \prod_{k=1}^{\beta(\rho)'} \mathfrak{A}_i'^{\gamma_{0k}} \qquad (\gamma_{0k} \in \mathbf{Z}^{\geqslant 0},\ 1 \leqslant k \leqslant \beta(\rho)'). \tag{15e}$$

We form the $(\alpha(\rho)+1) \times \beta(\rho)'$-matrix $\bar{A} = (\alpha_{ik})$ determined by

$$\alpha'_{ik} = \sum_{\nu=1}^{\beta(\rho)} \alpha_{i\nu}\gamma_{\nu k} \qquad (1 \leqslant i \leqslant \alpha(\rho)),$$

$$\alpha'_{\alpha(\rho)+1,k} = \left(\sum_{h=1}^{\beta(\rho)} \nu_h \gamma_{hk}\right) + \gamma_{0k} \qquad (1 \leqslant k \leqslant \beta(\rho)'),$$

rename φ_j to $\xi_{\alpha(\rho)+1}$, α'_{ik} to α_{ik}, $\bar{A}$ to A, $\alpha(\rho)+1$ to $\alpha(\rho)$ and $\mathfrak{A}'_1, \ldots, \mathfrak{A}'_{\beta(\rho)'}$ to $\mathfrak{A}_1, \ldots, \mathfrak{A}_{\beta(\rho)}$, $\beta(\rho)'$ to $\beta(\rho)$, and go on increasing j by 1 if $j < \kappa$.

If all of the φ_j's are run through, then choose another ω. It was shown in [6] that this method will come to a halt as desired after finitely many steps.

3. Unit Search II. Suppose $\epsilon_1, \ldots, \epsilon_\rho$ are ρ independent units and $p_1, \ldots, p_\sigma$ are distinct prime numbers. Then all units ϵ of 0 with the property that some power ϵ^h with exponent of the form $h = p_1^{\nu_1} p_2^{\nu_2} \cdots p_\sigma^{\nu_\sigma}$ belong to the subgroup generated by $TU(0)$, $\epsilon_1, \ldots, \epsilon_\rho$ form a subgroup $S(\epsilon_1, \ldots, \epsilon_\rho; p_1, \ldots, p_\sigma)$ of $U(0)$ such that

$$S(\epsilon_1, \ldots, \epsilon_\rho; p_1, \ldots, p_\sigma) = TU(0) \times \langle \epsilon'_1 \rangle \times \cdots \times \langle \epsilon'_\rho \rangle. \tag{16a}$$

We want to find a set of ρ units $\epsilon'_1, \ldots, \epsilon'_\rho$ of $U(0)$ satisfying (16a). Firstly, let $\rho = 1$, $\epsilon = \epsilon_1$. Supposing there holds an equation

(16b) $$\epsilon u = \xi^m \qquad (u \in TU(\mathcal{O}),\ \xi \in \mathcal{O},\ m \geqslant 2),$$

then

(16c) $$|\xi\theta_k| \leqslant x_k \quad \text{and} \quad x_k = \begin{cases} |\epsilon\theta_k^{1/2}| & \text{if } |\epsilon\theta_k| > 1, \\ 1 & \text{if } |\epsilon\theta_k| \leqslant 1, \end{cases} \qquad (1 \leqslant k \leqslant n),$$

$$\xi = \sum_{k=1}^{n} \xi_k \omega_k \qquad (\xi_k \in \mathbf{Z}),$$

(16d) $$\xi\theta_i = \sum_{k=1}^{n} \xi_k \omega_k \theta_i,$$

(16e) $$\xi_k = \sum_{i=1}^{n} A_{ik} d(\mathcal{O}/\mathbf{Z})^{1/2} \xi\theta_i,$$

when A_{ik} is the algebraic complement of $\omega_k\theta_i$ in the matrix $(\omega_k\theta_i)$ and

(16f) $$\det(\omega_k\theta_i) = d(\mathcal{O}/\mathbf{Z})^{1/2}.$$

Hence,

(16g) $$|\xi_k| \leqslant \sum_{i=1}^{n} |A_{ik}(x_i/d(\mathcal{O}/\mathbf{Z}))^{1/2}|.$$

There is a natural number p satisfying

(16h) $$p \geqslant \sum_{i=1}^{n} |A_{ik}(x_i/d(\mathcal{O}/\mathbf{Z}))^{1/2}| \qquad (1 \leqslant k \leqslant n).$$

Each solution of the congruence

(16i) $$\eta^h \equiv \epsilon u \pmod{p\mathcal{O}} \qquad \left(\eta \in TU(\mathcal{O}),\ h = \prod_{i=1}^{\sigma} p_i^{\nu_i}\right)$$

is congruent to

(16j) $$\eta = \sum_{k=1}^{n} \eta_k \omega_k$$

modulo $p\mathcal{O}$ where the rational integer η_k is a least residue modulo p. Because of (16g) any solution of (16b) is equal to one of the congruence solutions (16j). If none of them satisfies (16b), then (16b) has no solution. If some of the η's of (16j) satisfy (16b), then pick one with maximum value of m. That one will serve as ϵ_1'.

Now let $\rho > 1$. Using the method above, we determine $S(\epsilon_1; p_1, \ldots, p_\sigma) = TU(\mathcal{O}) \times \langle \epsilon_1' \rangle = S(\epsilon_1'; p_1, \ldots, p_\sigma)$. We replace ϵ_1 by ϵ_1'.

Without loss of generality we may assume that

(16k) $$S(\epsilon_1; p_1, \ldots, p_\sigma) = TU(\mathcal{O}) \times \langle \epsilon_1 \rangle.$$

Hence

$$\mathbf{Q}\mathcal{O}\,[\sqrt[p_j]{\epsilon_1}] \supset \mathbf{Q}\mathcal{O},$$

the polynomial $t^{p_j} - \epsilon_1$ of $\mathbf{Q}(\mathcal{O})[t]$ is irreducible. By Čebotarev (*Math. Ann.*, v. 95, 1926, pp. 191–229) there is a prime ideal $\mathfrak{p}_j \not\supseteq d(\mathcal{O})$ so that the polynomial $t^{p_j} - \epsilon_1$ remains irreducible mod $\mathfrak{p}_j$. Hence, $p_j | (N(\mathfrak{p}_j) - 1)$.

Hence for every unit ϵ_i for which $1 < i \leqslant \rho$ there is precisely one rational integer ν_i for which

$$0 \leqslant \nu_i < p_j, \qquad \epsilon_1^{\nu_i} \epsilon_i \text{ is congruent a } p_j\text{th power modulo } \mathfrak{p}_j.$$

Hence, by an application of the Chinese remainder theorem we obtain units $\hat{\epsilon}_2, \ldots, \hat{\epsilon}_\rho$ such that

$$\langle \epsilon_1 \rangle \times \langle \epsilon_2 \rangle \times \cdots \times \langle \epsilon_\rho \rangle = \langle \epsilon_1 \rangle \times \langle \hat{\epsilon}_2 \rangle \times \cdots \times \langle \hat{\epsilon}_\rho \rangle;$$

and every element of $\langle \hat{\epsilon}_2 \rangle \times \cdots \times \langle \hat{\epsilon}_\rho \rangle$ is a p_jth power modulo $\mathfrak{p}_j$ for $j = 1, 2, \ldots, \sigma$.

Hence, any element ξ of $\mathcal{O}$ for which ξ^{p_j} belongs to $TU(\mathcal{O}) \times \langle \epsilon_1 \rangle \times \cdots \times \langle \epsilon_\rho \rangle$ must itself belong to $TU(\mathcal{O}) \times \langle \epsilon_1 \rangle \times S(\hat{\epsilon}_2, \ldots, \hat{\epsilon}_\rho; p_j)$. Applying mathematical induction over ρ, we assume that we have already constructed units $\hat{\epsilon}_2', \ldots, \hat{\epsilon}_\rho'$ of $\mathcal{O}$ for which

$$S(\hat{\epsilon}_2, \ldots, \hat{\epsilon}_\rho; p_1, \ldots, p_\sigma) = TU(\mathcal{O}) \times \langle \hat{\epsilon}_2' \rangle \times \cdots \times \langle \hat{\epsilon}_\rho' \rangle. \tag{16l}$$

It follows that

$$S(\epsilon_1, \ldots, \epsilon_\rho; p_1, \ldots, p_\sigma) = S(\epsilon_1, \hat{\epsilon}_2, \ldots, \hat{\epsilon}_\rho; p_1, \ldots, p_\sigma). \tag{16m}$$

and that

$$S(\epsilon_1, \ldots, \epsilon_\rho; p_1, \ldots, p_\sigma) = TU(\mathcal{O}) \times \langle \epsilon_1 \rangle \times \langle \hat{\epsilon}_2 \rangle \times \cdots \times \langle \hat{\epsilon}_\rho \rangle \tag{16n}$$

in case

$$S(\hat{\epsilon}_2, \ldots, \hat{\epsilon}_\rho; p_1, \ldots, p_\sigma) = TU(\mathcal{O}) \times \langle \hat{\epsilon}_2 \rangle \times \cdots \times \langle \hat{\epsilon}_\rho \rangle. \tag{16o}$$

Hence, upon repeated replacement of $\epsilon_1, \ldots, \epsilon_\rho$ by $\epsilon_1, \hat{\epsilon}_2', \ldots, \hat{\epsilon}_\rho'$ until one arrives at (16o), the last ρ-tuple obtained will serve in the capacity of $\epsilon_1', \ldots, \epsilon_\rho'$.

In the event p and s are not too large one can employ with advantage a 'non p-adic method' based on the inspection of the possible candidates $\epsilon = \epsilon_1^{l_1} \cdots \epsilon_{s-1}^{l_{s-1}} \epsilon_s^{l_s}$ $(0 \leqslant l_i < p,\ 1 \leqslant i \leqslant s)$ and their conjugates. Using a dual $\mathbf{Q}$-basis $\overline{\omega}_1, \ldots, \overline{\omega}_n$ of $\mathbf{Q}\mathcal{O}$ characterized by the equation $\mathrm{tr}(\omega_i \overline{\omega}_k) = \delta_{ik}$, it follows for $\epsilon = \xi^p$ $(\xi = \Sigma_{i=1}^n a_i \omega_i,\ a_i \in \mathbf{Z},\ 1 \leqslant i \leqslant n)$ that $a_i = \mathrm{tr}(\overline{\omega}_i \xi) = \Sigma_{\nu=1}^n \overline{\omega}_i^{(\nu)} \sqrt[p]{\epsilon^{(\nu)}}$. If this a_i (double precision!) is 'not integral', then $\epsilon = \xi^p$ is impossible. Otherwise, upon taking for a_i the pertinent rational integer, one obtains a solution.

For computerization of the algorithm and complete numerical examples see the article by Michael Pohst on '*A Program for Determining Fundamental Units*' in SYMSAC 76, pp. 177–182 and also a forthcoming paper by the authors.

4. Unit Search III. Using methods of Zassenhaus [5], [6], we determine the algebraic number fields $F_1, \ldots, F_\tau$ satisfying

$$\mathbf{Q} \subset F_j \subset \mathbf{Q}\mathcal{O} \qquad (1 \leqslant j \leqslant \tau).$$

Note if n is a prime number, then $\tau = 0$.

Applying an inductive argument, we assume that we have found already a generator set of the unit group of each of the integral domains $F_j \cap \mathcal{O}$ and that the independent units $\epsilon_1, \ldots, \epsilon_r$ of $\mathcal{O}$ together with $TU(\mathcal{O})$ generate a subgroup of the unit group of $\mathcal{O}$ that contains all those generators. As a result, we know that any unit ϵ of $\mathcal{O}$ that is not already contained in the subgroup $TU(\mathcal{O}) \times \langle \epsilon_1 \rangle \times \cdots \times \langle \epsilon_r \rangle$ is a primitive element of $\mathbf{Q}\mathcal{O}$, i.e. $\mathbf{Q}\mathcal{O} = \mathcal{O}(\epsilon)$. Hence, any n consecutive powers of ϵ like

$$\epsilon^{1+[n/2]-n}, \ldots, \epsilon^{-1}, 1, \epsilon, \ldots, \epsilon^{[n/2]}$$

are linearly independent over $\mathbf{Q}$ which implies the linear independence of $\epsilon^{1+[n/2]-n}\iota, \ldots, \epsilon^{[n/2]}\iota$ over $\mathbf{R}$.

We apply this remark to the $(n-1)$-dimensional linear $\mathbf{R}$-space $M = \Sigma_{i=1}^{n-1} \mathbf{R}\mu_i$ determined by the first $n-1$ successive minima of the lattice or relative to the Cartesian distance function on the n-dimensional linear space $\mathbf{R}\mathcal{O}\iota$ over $\mathbf{R}$. For this purpose we determine n linearly independent lattice vectors μ_j of $\mathcal{O}\iota$ with the property that any lattice vector which is linearly independent of $\mu_1, \ldots, \mu_j$ is of a Cartesian length not less than the Cartesian length of μ_{j+1} $(j = 1, 2, \ldots, n-1)$. In particular, μ_1 is a lattice vector of shortest positive length. Clearly, 1ι is of shortest length. We choose μ_1 to be equal to 1ι. For an algorithm to find $\mu_1, \mu_2, \ldots, \mu_r$ see [3] or [8].

Of the n vectors

$$\epsilon^{1+[n/2]-n}\iota, \ldots, 1\iota, \ldots, \epsilon^{[n/2]}\iota$$

at least one is not contained in the $(n-1)$-dimensional linear $\mathbf{R}$-space spanned by $\mu_1, \ldots, \mu_{n-1}$. It follows that $|\epsilon^j \iota| \geqslant |\mu_n|$ for some exponent j satisfying $1 + [n/2] - n \leqslant j \leqslant [n/2]$, and $j \neq 0$ because $1\iota = \mu_1$. Hence

$$|\epsilon\iota| \geqslant |\mu_n|^{[n/2]^{-1}}. \tag{20}$$

According to the Hadamard inequality, we have

$$|\mathcal{O}\iota| = |d(\mathcal{O}/\mathbf{Z})^{1/2}| \leqslant \prod_{i=1}^{n} |\mu_i| \leqslant \sqrt{n}\,|\mu_n|^{n-1}, \tag{21a}$$

$$|\mu_n| \geqslant |(d(\mathcal{O}/\mathbf{Z})/n)^{1/(2(n-1))}|, \tag{21b}$$

$$|\epsilon\iota| \geqslant |(d(\mathcal{O}/\mathbf{Z})/n)^{(2[n/2](n-1))^{-1}} \tag{21c}$$

In any case we obtain an estimate of the form

$$|\epsilon\iota| \geqslant \mu > 0 \tag{21d}$$

leading to an estimate of the form

$$|\epsilon \operatorname{Log}| = \left| \left(\sum_{i=1}^{n} (\log|\epsilon\theta_i|)^2 \right)^{1/2} \right| \geqslant g(\mu) > 0 \tag{22}$$

according to the

LEMMA. *Let $\sigma_1, \ldots, \sigma_n, \mu$ be real positive numbers subject to the conditions*

(23a) $$\sum_{i=1}^{n} \sigma_i^2 \geqslant \mu^2 > n, \quad \prod_{i=1}^{n} \sigma_i = 1,$$

then

(23b) $$\sum_{i=1}^{n} (\log \sigma_i)^2 \geqslant g(\mu)^2,$$

where $g(\mu) > 0$ *and* $g(\mu)^2$ *is the minimum of the finitely many positive numbers*

$$\beta^2 n\alpha/(n-\alpha) \qquad (\alpha \in \mathbf{Z},\ 0 < \alpha < n;\ \beta > 0,$$

$$\alpha \exp(2\beta) + (n-\alpha)\exp(-2\beta\alpha/(n-\alpha)) = \mu^2).^{***}$$

Proof. Apply the Lagrange multiplier method to the function $\Sigma_{i=1}^{n}(\log \sigma_i)^2$ with the side conditions (23a) and $\sigma_i > 0$ for $i = 1, 2, \ldots, n$.

Supposing we know already that for some natural number $\rho < r$ every unit of $\mathcal{O}$ a power of which belongs to the subgroup $S = TU(\mathcal{O}) \times \langle \epsilon_1 \rangle \times \cdots \times \langle \epsilon_\rho \rangle$ of the unit group of $\mathcal{O}$ is contained in that subgroup S. In other words $\epsilon_1, \epsilon_2, \ldots, \epsilon_\rho$ are known to be part of a system of fundamental units of $\mathcal{O}$. It is our task to find a unit η of $\mathcal{O}$ a power of which belongs to $S \times \langle \epsilon_{\rho+1} \rangle$ such that even $\epsilon_1, \epsilon_2, \ldots, \epsilon_\rho$, η are part of a system of fundamental units. This implies of course that $S \times \langle \epsilon_{\rho+1} \rangle$ is a subgroup of finite index of $S \times \langle \eta \rangle$. Since we know from the general theory that there is an η, it is appropriate to employ the method expounded in Section 3 (Unit Search II) in order to find it *provided that we have an upper estimate for the index of* $S \times \langle \epsilon_{\rho+1} \rangle$ in $S \times \langle \eta \rangle$.

It remains to give an estimate of the form

(24) $$\kappa = (S \times \langle \eta \rangle) : (S \times \langle \epsilon_{\rho+1} \rangle) \leqslant \gamma.$$

We denote by

$$R(\delta_1, \ldots, \delta_\sigma) = |\det((\delta_i \mathrm{Log})(\delta_k \mathrm{Log}))^{1/2}| \quad (i, k = 1, 2, \ldots, \sigma)$$

the mesh of the sublattice $\Sigma_{i=1}^{\sigma} \mathbf{Z}\delta_i \mathrm{Log}$ of $U(\mathcal{O})\mathrm{Log}$ corresponding to σ independent units $\delta_1, \ldots, \delta_\sigma$ of $U(\mathcal{O})$. By the second fundamental theorem of the geometry of numbers

$$R(\epsilon_1, \ldots, \epsilon_\rho, \eta) \geqslant \gamma_{\rho+1} |\nu_1|\, |\nu_2| \cdots |\nu_{\rho+1}|,$$

where $\nu_1, \nu_2, \ldots, \nu_{\rho+1}$ are successive minima of the lattice

$$L = \left(\sum_{i=1}^{\rho} \mathbf{Z}\epsilon_i \mathrm{Log} \right) + \mathbf{Z}\eta \mathrm{Log}$$

and $\gamma_{\rho+1}$ is the Hermite constant indicating the critical mesh for Cartesian distance in $\rho + 1$ dimensions.

Denoting by $\nu_1', \nu_2', \ldots, \nu_{\rho+1}'$ a $(\rho+1)$-tuple of successive minima of the

***An estimate (22) remains valid even for $\mu^2 \leqslant n$ because of the inequality $|N(\epsilon^2 - 1)| \geqslant 1$ (see forthcoming paper by the authors).

sublattice $L' = \Sigma_{i=1}^{\rho+1} \mathbf{Z}\epsilon_i$Log of L, it follows that $|\nu_i| \leqslant |\nu_i'|$ and either $\nu_i \notin L'$, $|\nu_i| \geqslant g(\mu)$ or $\nu_i \in L'$, $|\nu_i| = |\nu_i'|$ thus

$$R(\epsilon_1, \ldots, \epsilon_\rho, \eta) \geqslant \gamma_{\rho+1} |\nu_1'| \cdots |\nu_j'| g(\mu)^{\rho+1-j},$$

$$0 < |\nu_1'| \leqslant |\nu_2'| \leqslant \cdots \leqslant |\nu_j'| < g(\mu),$$

$$\kappa = \frac{R(\epsilon_1, \ldots, \epsilon_\rho, \epsilon_{\rho+1})}{R(\epsilon_1, \ldots, \epsilon_\rho, \eta)} \leqslant \frac{R(\epsilon_1, \ldots, \epsilon_{\rho+1})}{\gamma_{\rho+1} |\nu_1'| \cdots |\nu_j'| g(\mu)^{\rho+1-j}},$$

where the successive minima $|\nu_1'|, \ldots, |\nu_j'|$ may be calculated (or estimated from below) by the methods of [5] or [8]. Note that $j = 0$ if $\tau = 0$!

The method given here works very well in all cases. However, it requires r number geometric estimates, as indicated above.

We can reduce the number of estimates in case $\mathcal{O}$ is the maximal order of $\mathbf{Q}\mathcal{O}$ and a minimal splitting field E of $\mathbf{Q}\mathcal{O}$ over $\mathbf{Q}$ and its automorphism group G over $\mathbf{Q}$ are known, say G is a permutation group of the algebraic conjugates of a primitive element ω of $\mathbf{Q}\mathcal{O}$ over $\mathcal{O}$, *provided G is not doubly transitive.* In that case we determine first of all by the method of Section 3 the subgroup S of $U(\mathcal{O})$ consisting of all units ϵ of $\mathcal{O}$ for which some power ϵ^h with h divisible only by the prime divisors of $|G||TU(\mathcal{O})|$ belongs to $TU(\mathcal{O}) \times \langle\epsilon_1\rangle \times \cdots \times \langle\epsilon_r\rangle$. Having done that, we may assume without loss of generality that for every prime number p dividing the order of G or $TU(\mathcal{O})$ the relation

$$\epsilon^p \in TU(\mathcal{O}) \times \langle\epsilon_1\rangle \times \cdots \times \langle\epsilon_r\rangle$$

always implies that

$$\epsilon \in TU(\mathcal{O}) \times \langle\epsilon_1\rangle \times \cdots \times \langle\epsilon_r\rangle.$$

Let G_1 be the stabilizer of ω in G. Set $\delta_1 = \epsilon_1$. Assuming that (after suitable renumbering of the ϵ_i's $(1 \leqslant i \leqslant r)$) the units $\epsilon_1, \ldots, \epsilon_\nu$ have the property that $\epsilon_{\mu+1}$ is independent of the finite set of units

$$U_\mu = \left\{ N_{E/\mathbf{Q}\mathcal{O}}\, \epsilon_i \theta_j = \prod_{\sigma \in G_1} \epsilon_i \theta_j \sigma \mid 1 \leqslant i \leqslant \mu,\ 1 \leqslant j \leqslant n \right\}$$

for $\mu = 1, 2, \ldots, \nu$, then we replace ν by $\nu + 1$. After a finite number of steps, we arrive at a subset $\{\epsilon_1, \ldots, \epsilon_\nu\}$ of $\{\epsilon_1, \ldots, \epsilon_r\}$ such that every unit of ρ is dependent on U_ν but that $\epsilon_{\mu+1}$ is independent of U_μ for $\mu = 1, 2, \ldots, \nu - 1$.

It follows from the integral representation theory of G that for any prime number p not dividing the order of G or of $TU(\mathcal{O})$, the relations

$$\epsilon^p \in TU(\mathcal{O}) \times \langle\epsilon_1\rangle \times \cdots \times \langle\epsilon_r\rangle, \qquad \epsilon \in U(\mathcal{O}),$$

either imply that ϵ itself belongs to $TU(\mathcal{O}) \times \langle\epsilon_1\rangle \times \cdots \times \langle\epsilon_\nu\rangle$, or else there is a unit δ of $U(\mathcal{O})$ that is not contained in $\langle\epsilon_1\rangle \times \cdots \times \langle\epsilon_\nu\rangle$ such that δ belongs to $\langle\epsilon_1\rangle \times \cdots \times \langle\epsilon_\nu\rangle$.

Applying the method given above, we obtain number geometric estimates of p depending only on $\epsilon_1, \ldots, \epsilon_\nu$.

Using these estimates, either we determine right away a system of fundamental units as above, or else we first determine ν fundamental units $\eta_1, \ldots, \eta_\nu$ such that

$$\epsilon_i \in \langle \eta_1 \rangle \times \langle \eta_2 \rangle \times \cdots \times \langle \eta_\nu \rangle \qquad (1 \leqslant i \leqslant \nu)$$

and then extend $TU(0), \eta_1, \ldots, \eta_\nu$ to a generator set $TU(0), \eta_1, \ldots, \eta_r$ of the group generated by U_ν and $\epsilon_{\nu+1}, \ldots, \epsilon_r$. As the theory shows, the units $\eta_1, \ldots, \eta_r$ form the desired system of fundamental units.

5. Applications and Examples. To show the effectiveness of our method we compute the fundamental units of all known totally real algebraic number fields F with minimum discriminants, i.e. of the degrees $n = 2, \ldots, 7$ ([4], [2]). At first we determine independent units as described in Section 1. There is no difficulty in writing a computer program for this procedure. In fact, most of the necessary computations are so simple that in case $n = 2, 3, 4$ we need not even use a computer.

In each case we obtain $n - 1$ independent units $\eta_1, \ldots, \eta_{n-1}$. But it is useful to carry on the procedure. Every time a new unit η will be found we examine whether it is already contained in the group generated by $-1, \eta_1, \ldots, \eta_{n-1}$. If not, we determine a new system of generators $\eta_1', \ldots, \eta_{n-1}'$, for which $\langle -1, \eta_1, \ldots, \eta_{n-1}, \eta \rangle = \langle -1, \eta_1', \ldots, \eta_{n-1}' \rangle$ holds. If the system of generators does not change any longer, we expect that we have already found $n - 1$ fundamental units. Then we compute an upper bound for the index x of our system in a system of fundamental units as shown in Section 4 or by using a lower bound for the regulator of F. For all prime numbers $p \leqslant x$ we try to solve the equation $\epsilon = \xi^p$ as described in Section 3. If there is no solution for the test units ϵ generated by our system, we have determined a system of fundamental units.

$n = 2$. (a) Let $F = \mathbf{Q}(\sqrt{5})$. The elements $\omega_1 = 1, \omega_2 = (1 + \sqrt{5})/2$ form an integral basis, and the lattice point $(0, 1)$ of the basic parallelotope $2\Pi(\omega_1 \iota, \omega_2 \iota)$ is already a fundamental unit of F.

(b) In $F = \mathbf{Q}(\sqrt{6})$ things are slightly more complicated. We have $\omega_1 = 1, \omega_2 = \sqrt{6}$ as an integral basis, but the parallelotope $2\Pi(\omega_1 \iota, \omega_2 \iota)$ does not contain a unit different from ± 1. To transform the parallelotope we choose an element $\omega = a + b\sqrt{6}$ $(a, b \in \mathbf{Z})$ of F, for example $\omega = 1 + \sqrt{6}$. Transforming the basic parallelotope with this element ω does not yield anything new. But after the transformation by ω^2, ω^3 we find lattice points $\beta_1 = 2 + \sqrt{6}$ and $\beta_2 = 3 + \sqrt{6}$ of norms $-2, 3$, respectively. On the other hand $2\Pi(\omega_1 \iota, \omega_2 \iota)$ contains $\sqrt{6}$; and therefore, $\epsilon = \beta_1 \beta_2 / \sqrt{6}$ should be a unit, in our case it is even a fundamental unit.

Remark. It seems that transformations of the basic parallelotope by elements $\omega \in F$ give better results (i.e. more new lattice points), if $|N(\omega)|$ is large.

$n = 3$. We determine a pair of fundamental units of $F_3 = \mathbf{Q}(\beta)$, where β is a root of the polynomial $f(x) = x^3 + x^2 - 2x - 1$ of discriminant $d_3 = 49$. In this and all following examples an integral basis $\omega_1, \ldots, \omega_n$ of the field F under consideration is given by the successive powers $1, \beta, \ldots, \beta^{n-1}$.

The basic parallelotope $2\Pi(\omega_1\iota, \omega_2\iota, \omega_3\iota)$ contains $\epsilon_1 = \beta$, $\epsilon_2 = \beta + 1$. These two units are obviously independent. They already form a system of fundamental units as is shown by an easy index computation.

$n = 4$. We have $F_4 = \mathbf{Q}(\beta)$, $\beta^4 + \beta^3 - 3\beta^2 - \beta + 1 = 0$, $d_4 = 725$. The units $\epsilon_1 = \beta$, $\epsilon_2 = \beta + 1$, $\epsilon_3 = \beta - 1$ are independent. By an index computation we find that they are either fundamental units or that they are of index 2 in a system of fundamental units. But the latter is shown to be impossible by considering the signs of the pertinent conjugates.

$n = 5$. $F_5 = \mathbf{Q}(\beta)$, β a zero of $x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1 = 0$, $d_5 = 14641$. By means of electronic computation we find four independent units

$$\epsilon_1 = \beta^3 + \beta^2 - 3\beta - 1, \quad \epsilon_2 = \beta, \quad \epsilon_3 = \beta + 1, \quad \epsilon_4 = \beta^4 + \beta^3 - 1.$$

They turn out to be fundamental units.

$n = 6$. $F_6 = \mathbf{Q}(\beta)$, β a zero of $x^6 + x^5 - 7x^4 - 2x^3 + 7x^2 + 2x - 1 = 0$, $d_6 = 300\,125$. A system of fundamental units is given by

$$\epsilon_1 = \beta^5 + \beta^4 - 6\beta^3 + 3\beta - 1, \quad \epsilon_2 = \beta^4 + \beta^3 - 6\beta^2 - \beta + 1,$$

$$\epsilon_3 = \beta + 1, \quad \epsilon_4 = \beta, \quad \epsilon_5 = \beta^4 - \beta^2 + \beta + 1.$$

$n = 7$. $F_7 = \mathbf{Q}(\beta)$, β a zero of $x^7 + x^6 - 6x^5 - 5x^4 + 8x^3 + 5x^2 - 2x - 1 = 0$, $d_7 = 20\,134\,393$. A system of fundamental units is given by

$$\epsilon_1 = \beta^6 + 2\beta^5 - 5\beta^4 - 10\beta^3 + 3\beta^2 + 8\beta + 2,$$

$$\epsilon_2 = \beta^6 + \beta^5 - 6\beta^4 - 5\beta^3 + 8\beta^2 + 5\beta - 1,$$

$$\epsilon_3 = \beta^5 + \beta^4 - 5\beta^3 - 4\beta^2 + 3\beta + 1, \quad \epsilon_4 = \beta,$$

$$\epsilon_5 = 4\beta^6 + \beta^5 - 25\beta^4 - 2\beta^3 + 35\beta^2 - 3\beta - 6,$$

$$\epsilon_6 = 5\beta^6 - \beta^5 - 36\beta^4 + 8\beta^3 + 63\beta^2 - 9\beta - 12.$$

Mathematisches Institut
Universität zu Köln
Cologne, Germany

Department of Mathematics
The Ohio State University
Columbus, Ohio 43210

1. P. G. L. DIRICHLET, "Zur Theorie der complexen Einheiten," *Mathematische Werke*, Band II, reprint, Chelsea, New York, 1969, pp. 642–644. MR **40** #2514.

2. W. NARKIEWICZ, *Elementary and Analytic Theory of Algebraic Numbers*, PWN, Warsaw, 1974. MR **50** #268.

3. H. MINKOWSKI, "Diskontinuitätsbereich für arithmetische Äquivalenz," *J. Reine Angew. Math.*, v. 129, 1905, pp. 220–274.

4. M. POHST, "The minimum discriminant of seventh degree totally real algebraic number fields," *Algebra and Number Theory*. Special volume, Academic Press.

5. HANS ZASSENHAUS, "On Hensel factorization. I," *J. Number Theory*, v. 1, 1969, pp. 291–311; "On Hensel factorization. II," *Symposia Mathematica*, vol. 15, Academic Press, London, 1975, pp. 499–513. MR **39** #4120; **52** #10700.

6. HANS ZASSENHAUS, "On the units of orders," *J. Algebra*, v. 20, 1972, pp. 368–395. MR **44** #6659.

7. HANS ZASSENHAUS, "On the second round of the maximal order program," *Applications of Number Theory to Numerical Analysis* (Proc. Sympos., Quebec, 1971), Academic Press, New York, 1972, pp. 389–431. MR **51** #8079.

8. HANS ZASSENHAUS, "Gauss theory of ternary quadratic forms, an example of the theory of homogeneous forms in many variables, with applications," *Number Theory Seminar Lecture Notes*, Calif. Inst. Tech.