ON SUCCESSIVE MINIMA OF RINGS OF ALGEBRAIC INTEGERS (EXTENDED ABSTRACT AND COMMENTS)

par JACQUES MARTINET[1]

The article appeared under the reference

On Successive Minima of Rings of Algebraic Integers, J.P. Buhler (Ed.), Lectures Notes in Computer Science **1423**, Springer-Verlag, Heidelberg, 1998, pp. 424–432.

The aim of the paper was to draw attention upon the possibility of using Minkowski's theorem on successive minima to obtain nice reductions of rings of algebraic integers.

Let K be a number field of degree n and signature (r_1, r_2) $(r_1 + 2r_2 = n)$. We order the embeddings $\sigma_k : K \to \mathbb{C}$ in the usual way: σ_k is real for $1 \le k \le r_1$ and $\sigma_{k+r_2} = \overline{\sigma}_k$ for $r_1 + 1 \le k \le r_1 + r_2$. We consider on K the standard positive definite quadratic form (the *"twisted" trace form*) defined by

$$q(x) = \sum_{k=1}^{n} \sigma_k(x)\overline{\sigma}_k(x)\,.$$

The completion of K for the real embedding of $\mathbb{Q}$ yields the real algebra with involution $E = \mathbb{R} \bigotimes_{\mathbb{Q}} K$. It is a Euclidean space for the form $\mathrm{Tr}_{E/\mathbb{R}}(x\overline{x})$, whose restriction to K is the form q considered above, and the ring $\mathbb{Z}_K$ of integers of K is a lattice Λ in E, whose successive minima $m_1, \dots, m_k$ are defined in the usual way : m_k is the smallest real number λ such that the set of elements $x \in \mathbb{Z}_K$ with $q(x) \le \lambda$ spans a subspace of E of dimension at least k.

Two problems were considered, and stated as conjectures (but conjecture 1, page 429, is not true, see below).

1. The first problem consists of the following two questions:
Do (arbitrary) representatives of the successive minima consstitute a $\mathbb{Z}$-basis of $\mathbb{Z}_K$? If not, what can be the index in $\mathbb{Z}_K$ of the sublattice Λ' generated by such representatives ?

The general upper bound $[\Lambda : \Lambda'] \le \gamma_n^{n/2}$ where γ_n is the *Hermite constant for dimension* n, which is sharp for $n \le 8$, is improved in case $\Lambda = \mathbb{Z}_K$ and $n = 4, 6, 7, 8$. For instance, one finds the upper bound $[\Lambda : \Lambda'] \le 2$ for $n = 6$ whereas $[\mathbb{Z}_K : \Lambda'] = 4$ could hold for the root lattice $\Lambda = \mathbb{D}_6$.

Key words and phrases. Number fields, lattices, successive minima.

[1]laboratoire associé au C.N.R.S. – Université Bordeaux 1

However, examples due to H.W. Lenstra and Bart de Smit show that for $n = 6$ (and indeed probably for all $n \geq 6$), the index 2 may occur, as well as larger indices for larger values of n.

The idea of their counterexamples, as explained to me by F. Diaz y Diaz, is as follows: consider a polynomial $f \in \mathbb{Z}[X]$ of the form

$$aX^n + a_1X^{n-1} + \cdots + a_{n-1}X + b$$

with large a, b and small $a - b, a_1, \ldots, a_{n-1}$, in some sense close to a Kummer polynomial. Then, modulo some restrictions (in particular on the behaviour of $f(X) \mod 2$), the index $[\mathbb{Z}_K : \Lambda']$ is at least 2. The example with the smallest known discriminant in degree 6 is provided by Diaz y Diaz's polynomial

$$7X^6 + X^5 - X^4 + 3X^3 + X^2 - 7\,,$$

with discriminant

$$d_K = 3\,731\,647\,088\,561 \# 3.7\,10^{12}\,,$$

a value which lies far beyond the existing tables of sixth degree fields.

Consequently, for algorithmic purposes, to use representatives of the successive minima as a basis of $\mathbb{Z}_K$ often works and provides the best possible reduction. This is an important practical remark: all those who make use of packages such as *KANT* or *PARI* to compute units and class groups know the importance of reduction to make the calculations faster. The same remark applies to the calculation of relative extensions.

2. The second problem, of a less computational nature, concerns Abelian fields and the Kronecker-Weber theorem, at least for fields of prime degree.

Let thus K be cyclic over $\mathbb{Q}$ of odd prime degree ℓ (the case $\ell = 2$ is trivial), with conductor f, and hence discriminant $d_K = f^{\ell-1}$. It is clear that the successive minima are $m_1 = \ell$ (represented by $1 \in \mathbb{Z}_K$) and that $m_2 = \cdots = m_\ell > m_1$ (because of the Galois action on $\mathbb{Z}_K$). Let $\zeta \in \overline{\mathbb{Q}}$ be a root of unity of order f, and let $\theta = \mathrm{Tr}_{\mathbb{Q}(\zeta)/K}(\zeta)$. Then, θ is an element of $\mathbb{Z}_K$ which generates K over $\mathbb{Q}$.
Does θ represent m_2 ?

The answer is positive for $\ell = 3$ (use "quasi-normal" integral bases). Calculations for $\ell = 5, 7, 11$ to be found in Huguette NAPIAS's thesis (Bordeaux, 1996) suggest that the answer could be positive for all ℓ.

J. MARTINET
A2X, INSTITUT DE MATHÉMATIQUES
UNIVERSITÉ BORDEAUX 1
351, COURS DE LA LIBÉRATION
F–33405 TALENCE CEDEX

E-mail : martinet@math.u-bordeaux.fr