SMALL DISCRIMINANTS, CLASS NUMBERS, AND THE GEOMETRY OF NUMBERS

JACQUES MARTINET

Abstract. We discuss some problems related to discriminants and class groups of number fields, in connection with the *Minkowski domains* of dimension $n = r_1 + 2r_2$ attached to number fields of signature (r_1, r_2).

1. Some notation for Geometry of Numbers

First we consider pure geometry of numbers. Let E be a Euclidean space, of dimension n. The scalar product on E is denoted by $x \cdot y$, and the *norm of* $x \in E$ is $N(x) = x \cdot x$, the square of the traditional norm $\|x\|$.

Let Λ be a *lattice in* E, that is a discrete subgroup of E of maximal rank. Thus Λ has a basis $\mathcal{B} = (e_1, \dots, e_n)$ over $\mathbb{Z}$, with which we associate its *Gram matrix* $\mathrm{Gram}(\mathcal{B}) = (e_i \cdot e_j)$, the determinant of which, clearly independent of $\mathcal{B}$, is the *determinant of* Λ: $\det(\Lambda) = \det \mathrm{Gram}(\mathcal{B})$. The traditional notion (Minkowski) is the *discriminant* $\Delta(\Lambda)$ *of* Λ, the absolute value of the determinant of $\mathcal{B}$ with respect to an orthonormal basis for E. We have

$$\det(\Lambda) = \Delta(\Lambda)^2 \quad \text{and} \quad N(x) = \|x\|^2 \,.$$

Introducing these squares simplifies many formulae. Moreover the notion of the determinant fits (up to sign) with that of the discriminant in number fields; see Section 2. Note that our lattice constants to be defined below will be the squares of the usual ones.

Let $A \subset E$. Recall that a lattice Λ is *admissible for* A if $\Lambda \cap A$ is reduced to $\{0\}$ or is empty. We then define the *lattice constant of* A by

$$\kappa(A) = \inf_{\Lambda \text{ admissible}} \det(\Lambda)$$

($\kappa(\Lambda) = +\infty$ if there are no admissible lattices for A). In the cases we shall consider, A will be an open , symmetric *star body* (*with respect to*

Key words and phrases. Euclidean lattices, Minkowski domains
October, 2010 January 2011.

the origin), that is, A is open in E, and for all $x \in A$ and $\lambda \in \mathbb{R}$ with $|\lambda| \le 1$, then $\lambda\, x \in A$; and moreover, our sets A will be of the form

$$A_F = \{x \in E \mid F(x) < 1$$

where F is a *distance-function*, that is F is a continuous, non-negative real function, *"homogeneous" of degree* δ for some $\delta > 0$, i.e., F satisfies the identity

$$\forall\, x \in E, \forall\ \lambda \in \mathbb{R}\,,\ F(\lambda x) = |\lambda|^\delta\, F(x)\,.$$

[Conversely, modulo mild conditions on the boundary, every open star body is of the form A_F for some F.]

The definition of the lattice constant $\kappa(A)$ of an open, symmetric star body A is often used in the following form: if $\det(\Lambda) < \kappa(A)$, then A contains a non-zero point of Λ, and even, for bounded A, if $\det(\Lambda) \le \kappa(A)$, then $\overline{A}$ contains a non-zero point of Λ This last result extends to unbounded domains for which we may apply compactness results, or under some restrictions on Λ. This notably works for lattices related to *modules* inside number fields; see Section 2.

With an F as above we associate the following two functions on the space of lattices:

$$F(\Lambda) = \inf_{x \in \Lambda \smallsetminus \{0\}} F(x) \ \text{ and } \ \gamma_F(\Lambda) = \frac{F(\Lambda)}{\det(\Lambda)^{\delta/2n}}\,.$$

Finally we set $\gamma_{n,F} = \sup_\Lambda\, \gamma_F(\Lambda)\,.$ The relation between κ and $\gamma_{n,F}$ is easy to establish; it reads

$$\kappa(A_F) = \gamma_{n,F}^{-2n/d}\,.$$

An important example of distance-function is the norm, of degree 2. Then $\gamma_N(\Lambda)$, denoted simply by $\gamma(\Lambda)$, is the *Hermite invariant of* Λ, and $\gamma_{n,N}$, denoted simply by γ_n, is the *Hermite constant for dimension* n. We also denote by κ_n the lattice constant of the n-dimension unit ball; we have $\kappa_n = \gamma_n^{-n}$.

2. Connection with number fields

We denote by K a number field, of signature (r_1, r_2) and degree $n = r_1 + 2r_2$, and order the embeddings $\sigma_i : K \to \mathbb{C}$ in such a way that σ_j be real for $j \le r_1$ and (r_j, r_{j+r_2}) be complex conjugates for $r_1 + 1 < j \le r_1 + r_2$. We shall attach to K a Euclidean space $\widehat{K}$ and an open star body in $\widehat{K}$ (a *Minkowski domain*), and to each finitely generated, full submodule of K a lattice in $\widehat{K}$. Proofs for the results stated in this section can be read in the second chapter of [Mar].

Denote by $\widehat{K}$ the completion of K for any infinite norm on K identified with $\mathbb{Q}^n$. This is an étale $\mathbb{R}$-algebra, canonically isomorphic to $\mathbb{R} \otimes_{\mathbb{Q}} K$, thus isomorphic (non-canonically) to$\mathbb{R}^{r_1} \times \mathbb{R}^{r_2}$. Nevertheless the canonical involution of this last algebra (the identity on the real factors and the conjugacy on the complex ones) induces a canonical involution $x \mapsto \overline{x}$ on $\widehat{K}$, for which $\mathrm{Tr}_{\widehat{K}/\mathbb{R}}(x\overline{x})$ is a scalar product. We provisionally define a Minkowski domain inside $\widehat{K}$ by $|N_{\widehat{K}/\mathbb{R}}(x)| < 1$.

To perform explicit calculations we shall identify $\widehat{K}$ with $\mathbb{R}^n$. this is done using coordinates x_j $(j = 1, \ldots, r_1)$ and y_j, z_j $(j = 1, \ldots, r_2)$, and embedding K in $\mathbb{R}^n$ by

$$1_K \mapsto \mathbf{1} := (1, 1, \ldots, 1)\,.$$

For $z = a + bi \in \mathbb{C}$, we have $\mathrm{Tr}_{\mathbb{C}/\mathbb{R}}(z\overline{z}) = 2(a^2 + b^2)$. To take into account these factors 2 attached to all complex components, we define Minkowski domains in $\mathbb{R}^n$ as follows.

Definition 2.1. Let

$$F_{r_1,r_2} = 2^{-r_2} \cdot |x_1| \cdots |x_{r_1}| \cdot (y_1^2 + z_1^2) \cdots (y_{r_2}^2 + z_{r_2}^2)\,.$$

The *Minkowski domain for signature* (r_1, r_2) *(*$r_1 + 2r_2 = n$*) in* $\mathbb{R}^n$ is

$$A_{r_1,r_2} = \{x \in \mathbb{R}^n \mid F_{r_1,r_2}(x) < 1\}\,.$$

Its *lattice constant* is denoted by κ_{r_1,r_2}.

We observe that $\mathbf{1}$ belongs to the boundary of the domain. Moreover, the introduction of the term 2^{r_2} allows us to compare different domains in the same dimension.

Proposition 2.2. *Let* r_1, r_2, r_1', r_2' *such that* $r_1 + 2r_2 = r_1' + 2r_2'$. *If* $r_1' \geq r_1$, *we have the inclusion*

$$A_{r_1,r_2} \subset A_{r_1',r_2'}\,.$$

Proof. This results by induction from the inclusion $A_{r_1-2,r_2+1} \subset A_{r_1,r_2}$ $(r_1 \geq 2)$, which follows from the arithmetico-geometric inequality $|y_1 z_1| \leq \frac{y_1^2+z_1^2}{2}$. □

We now turn to the construction of lattices from submodules of K. By a *module in* K, we mean a finitely generated $\mathbb{Z}$-submodule of K of rank $n = [K : \mathbb{Q}]$. Such a module M has a basis $(\omega_1, \ldots, \omega_n)$ over $\mathbb{Z}$, and a discriminant

$$d_K(M) = \det(\mathrm{Tr}_{K/\mathbb{Q}}(\omega_i \omega_j)) \in \mathbb{Q}^\times$$

(for short, d_K when $M = \mathbb{Z}_K$, the ring of integers of K), which has the sign of $(-1)^{r_2}$. Since M is discrete in K, it is its own closure in

$\widehat{K}$, and may consequently be identified with a lattice in $\widehat{K}$. Since the twist $x \mapsto \overline{x}$ multiplies determinants by $(-1)^{r_2}$, we have

$$\det(M) = |d_K(M)|\,.$$

We now turn to the norm map $N_{K/\mathbb{Q}}$ on $M \smallsetminus \{0\}$. Let q be a positive integer such that $q\,\omega_i \in \mathbb{Z}_K$ for all i. Then we have $q\,M \subset \mathbb{Z}_K$, which shows that the norms of elements of M are integral multiples of q^{-n}. In particular, $|N_{K/\mathbb{Q}}(x)|$ attains a minimum on $M \smallsetminus \{0\}$. Rescaling the image of M in $\widehat{K}$, we obtain a lattice on which the norm function has minimum 1. Its image in $\mathbb{R}^n$ is then an admissible lattice for A_{r_1,r_2} having at least one pair $\pm x$ on its boundary.

Definition 2.3. We say that an admissible lattice for A_{r_1,r_2} is *algebraic* if it is the image in $\mathbb{R}^n$ of a module in some field of signature (r_1, r_2).

Remark 2.4. It results from the discussion above that for all domains A_{r_1,r_2}, there exist admissible lattices which are algebraic, and from Proposition 2.2 that non-algebraic lattices also exist for domains with $r_2 > 0$. It can be shown that non-algebraic lattices also exist in the case of $A_{2,0}$; see Section 5. The status of domains $A_{n,0}$ is not known from $n = 3$ onwards.

Recall that an *order in a number field* K is a subring of K of maximal rank (i.e., containing a basis of $K/\mathbb{Q}$) which is a finitely generated $\mathbb{Z}$-module. (This last condition is equivalent to the fact that all elements of an order are integral over $\mathbb{Z}$. Hence the integral closure $\mathbb{Z}_K$ of $\mathbb{Z}$ in K is the unique maximal order of K.) With every module we attach its *associated order*

$$\mathfrak{O}(M) = \{\lambda \in K \mid \lambda\mathfrak{O} \subset \mathfrak{O}\}\,,$$

the largest subring of K which stabilizes M. Thus modules in K are nothing but fractional ideals over some order, the largest of which is the associated order. (Fractional ideals of an order $\mathfrak{O}$ the associated order of which is $\mathfrak{O}$ itself are called *proper*.) The famous *Dirichlet unit theorem* asserts that the set $\mathfrak{O}^\times$ of invertible elements of $\mathfrak{O}$ is the direct product of the cyclic group $\mu_{\mathfrak{O}}$ of roots of unity which belong to $\mathfrak{O}$ and a free Abelian group of rank $r_1 + r_2 - 1$.

Given an order $\mathfrak{O}$, a *fractional ideal of* $\mathfrak{O}$ is a non-zero sub-$\mathfrak{O}$-module of K which is finitely generated over $\mathfrak{O}$ (or over $\mathbb{Z}$, this amounts to the same). The rule

$$\mathfrak{a}\mathfrak{b} = \{\textstyle\sum x_i y_i \mid x_i \in \mathfrak{a},\, y_i \in \mathfrak{b}\}$$

defines a multiplication on the set of fractional ideals of $\mathfrak{O}$, which is associative and commutative, with neutral element $\mathfrak{O}$. The invertible (fractional) ideals constitute a group, denoted by $\mathcal{I}_{\mathfrak{O}}$, which contains as a subgroup the set of *principal fractional ideals*, denoted by $\mathcal{P}_{\mathfrak{O}}$. The quotient group $\mathrm{Cl}_{\mathfrak{O}}$ is the *class group of* $\mathfrak{O}$. This is a finite group. We also write $\mathcal{I}_K$, $\mathcal{P}_K$ and Cl_K when $\mathfrak{O} = \mathbb{Z}_K$.

An important problem concerning (unbounded) star bodies is that of the rank of points belonging to the boundary (which can be zero). We shall prove (Theorem 4.12 below) that for every minimal-admissible lattice for a Minkowski domain, there exists a minimal-admissible having the same determinant and containing **1**. For algebraic lattices, Dirichlet's units theorem shows that the boundary of the domain contains a set of lattice points of rank at least $r_1 + r_2$, thus the maximal value n in the totally real case. In some cases a better lower bound holds. For $A_{2,0}$, this rank is 1 except when the order $\mathfrak{O}$ is the ring of Eisenstein or of Gaussian integers, which contain roots of unity of order 4 or 6.

The main application of the lattice constants of Minkowski domains is the following theorem (which results from the very definition of lattice constants) and the corollary which follows, proved using the "trick of the inverse class" (thus, the result extends to classes of invertible ideal in orders).

Theorem 2.5. *Let M be a module in a number field K of signature (r_1, r_2). Then there exists non-zero $x \in M$ such that*

$$|N_{K/\mathbb{Q}}(x)| \le \sqrt{\frac{|d_K(M)|}{\kappa_{r_1,r_2}}}. \quad \square$$

Theorem 2.6. *Every ideal class of an order $\mathfrak{O} \subset K$ contains an integral ideal $\mathfrak{a}$ of norm*

$$N_{K/\mathbb{Q}}(\mathfrak{a}) \le \sqrt{\frac{|d_{\mathfrak{O}}|}{\kappa_{r_1,r_2}}}. \quad \square$$

Minkowski, applying his lower bound based on the volume for the lattice constant of a convex set to

$$B_{r_1,r_2} = \left\{x \in \widehat{K} \;\middle|\; |x_1| + \cdots + |x_{r_1}| + 2|z_1| + \cdots + 2|z_{r_2}| < 1\right\}$$

and using the inclusion

$$n2^{r_2/n} B_{r_1,r_2} \subset A_{r_1,r_2}\,,$$

obtained the famous lower bound

$$\sqrt{\kappa_{r_1,r_2}} \ge \left(\frac{\pi}{4}\right)^{r_2} \frac{n^n}{n!}\,,$$

with which he could prove *Kronecker's conjecture*, namely that for any number field of degree $n \ge 2$, one has $|d_K| > 1$. This result was first written in a letter to Hilbert of December 22nd, 1890 ([MBH]), then in a letter to Hermite of January 15th, 1891, partially published by Hermite in C.R. Acad. Sc. Paris. In this last letter, Minkowski remarks that using the ball of largest possible radius inside $A_{1,1}$ yields a slightly better result than using $B_{1,1}$: our pretty good knowledge of the Hermite constants compensate the disadvantage of having a small volume. The optimal radius is easily calculated using the arithmetico-geometric inequality and gives the following lower bound.

Theorem 2.7. *We have*

$$\kappa_{r_1,r_2} \geq n^n \kappa_n = \left(\frac{n}{\gamma_n}\right)^n. \quad \square$$

The improvement on Minkowski's original lower bound for κ_{r_1,r_2} is particularly significant for totally imaginary domains[1] in dimensions 2 (it is then optimal), 4, 6, and 8.

The exact values of κ_{r_1,r_2} and the corresponding *critical lattices* (see Definition 4.4 below) are known for $n = 2$ and 3: $\kappa_{0,1} = 3$, $\kappa_{2,0} = 5$, $\kappa_{1,1} = 23$, and $\kappa_{3,0} = 49$. In all cases the critical lattices correspond to the ring of integers of the fields of minimal discriminant. Such a result conjecturally holds in small dimensions. Thus one conjectures that the lattice constants are 113, 275, and 725 for $n = 4$, and 1609, 4511, and $14641 = 11^4$ for $n = 5$.

The best known results for $A_{4,0}$ and $A_{5,0}$ are those of Noordzij ([Noo], $\kappa_{4,0} \geq 500$) and Godwin ([God], $\kappa_{5,0} > 3251.2\ldots$). Asymptotic lower bounds improving on Minkowski's have been obtained by C. A. Rogers in the totally real case (*The product of n real homogeneous linear forms*, Acta Math. **82** (1950), 185–208) and by H. P. Mullholand in general (*On the product of n complex homogeneous linear forms*, J. London Math. Soc. **35** (1960), 241–250.

3. Small discriminants of number fields

In this section we briefly discuss the following question: what are the first smallest discriminants (in absolute value) in a given signature (r_1, r_2)? That one must take into account not only the degree n but also the signature (r_1, r_2) is clearly shown both by the structure of Minkowski's lower bound and by experimental data. More precisely

[1] I first saw this trick in work of Descombes and Poitou devoted to approximation of complex numbers by elements of imaginary quadratic fields. This problem is related to admissible lattices for $A_{0,2}$ containing the image of an imaginary quadratic field, like approximation of real numbers by rational numbers is related to admissible lattices for the domain $A_{2,0}$.

the aim is, given a real number $B > 0$, to find reasonably small bounds for the coefficients of polynomials that may be used to define all fields of signature (r_1, r_2) with $|d_K| \le B$.

3.1. **Bounds for defining polynomials.** The basic idea to handle a number field K (for which we refer to [Mar1]) consists in using the orthogonal projection in $\widehat{K}$ to $\mathbf{1}^\perp$, and to apply results from geometry of numbers to the projection of $\mathbb{Z}_K$ (or more generally, of any order in K). One then bounds in terms of $|d_K|$ the size of the projection of a convenient element of $\mathbb{Z}_K$, hence of a pull back $\theta \in \mathbb{Z}_K$ *not in* $\mathbb{Q}$. This is the method used in [D-F] for cubic fields,[2] formalized in general by Hunter in [Hun]. In this paper, he obtains a bound in terms of the discriminant d_K for the conjugates of some integer $\theta \in K$ *not in* $\mathbb{Q}$. For a prime degree n, such a θ generates the field. Hunter found this way the smallest discriminants of quintic fields of any of the three signatures.

When n is not a prime, $n' = [\mathbb{Q}(\theta) : \mathbb{Q}]$ may be a a strict divisor of n. One can then either consider successive minima, or prove a relative form of Hunter's theorem, which is more efficient for computation. Such a generalization is proved using this time orthogonal projections in $\widehat{K}$ onto $\widehat{K'}$.

[Given a k-dimensional subspace in a Euclidean space E, equipped with an orthogonal basis $(e_1, \dots, e_k)$, the projection $p_{F^\perp}$ of E to $F^\perp$ is given by the formula

$$p_{F^\perp}(x) = x - \textstyle\sum_{i=1}^k \frac{x \cdot e_k}{e_k \cdot e_k}\, x\,;$$

just observe that $p_{F^\perp}$ maps F to $\{0\}$ and is the identity on $F^\perp$. This implies that the norm of the projection is

$$N\big(p(x)\big) = N(x) - \sum_{i=1}^{k} \frac{(x \cdot e_i)^2}{e_i \cdot e_i}\,.$$

For instance, if $E = \mathbb{R}^n$ and $F = \mathbb{R}\mathbf{1}$, $x = (x_1, \dots, x_n)$ is mapped onto

$$N\big(p(x)\big) = \sum_i x_i^2 - \frac{1}{n}\Big(\sum_i x_i\Big)^2 = \frac{1}{n} \sum_{1 \le i < j \le n} (x_j - x_i)^2\,.]$$

To state this extension of Hunter's theorem, we need some notation. We consider a subfield K' of K, of degree n', and denote by $\mathcal{I}(K')$ the set of embeddings $\sigma : K' \to \mathbb{C}$.

[2] The minimal discriminant of cubic fields in both signatures (namely, -23 and $+49$) were found by Philipp Furtwängler (*Zur Theorie der in Linearfaktoren zerlegbaren ganzzahlingen ternären kubischen Formen*, Dissertation, Göttingen, 1896; advisor: Felix Klein).

Definition 3.1. For $\theta \in K$, let

$$S_{K/K'}(\theta) = \sum_{\sigma \in \mathcal{I}(K')} \sum_{\tau, \tau' | \sigma} |\tau(\theta) - \tau'(\theta)|^2 \,,$$

and let $S_K(\theta) = S_{K/\mathbb{Q}}(\theta)$.
(The notation $\tau \mid \sigma$ means that $\tau \in \mathcal{I}(K)$ extends $\sigma \in \mathcal{I}(K')$.)
In analogy with S_K, given complex numbers $z_1, \dots, z_n$, we set

$$S(z_1, \dots, z_n) = \textstyle\sum_{i<j} |z_j - z_i| \,,$$

and for a polynomial $f \in \mathbb{C}[X]$ of degree n, we set $S_f = S(z_1, \dots, z_n)$ where the z_i are the roots of f.

Remark 3.2. (1) $S_{K/K'}$ is invariant under translations by elements of K'.
(2) If θ belongs to an intermediate field L, we may consider both $S_{L/K'}$ and $S_{K/K'}$. Then $S_{K/K'}(\theta) = [K : L]^2 S_{L/K'}(\theta)$. In particular, $S_K(\theta) = [K : \mathbb{Q}]^2$ if $\theta \in \mathbb{Z}$.
(3) The condition $S_K > 0$ (a *necessary condition* for f to have n distinct real roots) holds if and only if $f^{(n-2)}$ has two distinct real roots.

Proposition 3.3. *With the notation of Definition 3.1, let* $m = \frac{n}{n'}$ *be the relative degree* $[K : K']$*, and for* $\theta \in K$ *and* $\sigma \in \mathcal{I}(K')$*, let* $\mathrm{Tr}_{\sigma,k/K'}(\theta) = \sum_{\tau|\sigma} \tau\theta$. *We have*

$$m \sum_{\tau \in \mathcal{I}(K)} |\tau(\theta)|^2 - \sum_{\sigma \in \mathcal{I}(K')} |\mathrm{Tr}_{\sigma,k/K'}(\theta)|^2 = S_{K/K'}(\theta) \,.$$

Proof. This is an application of the following well known formula in quadratic affine spaces (E, q) involving $n+1$ point $O, M_1, \dots, M_n$:

$$\textstyle\sum_{i<j} q(\overrightarrow{M_i M_j}) = m \sum_i q(\overrightarrow{OM_i}) - q(\sum_i \overrightarrow{OM_i}) \,.$$

□

Theorem 3.4. *Let* K *be a number field of degree* n *and let* K' *be a strict subfield of* K*, of degree* n'*. Then there exists an integer* $\theta \in K$*,* θ *not in* K'*, such that*

$$S_{K/K'}(\theta) \le m\, \gamma_{n-n'} \left| \frac{d_K}{m^{n'} d_{K'}} \right|^{1/(n-n')} .$$

(Recall that $\gamma_{n-n'}$ is the Hermite constant for dimension $n - n'$).

Proof. Just make explicit the projection in $\widehat{K}$ to $\widehat{K'}$; the details can be read in [Mar1]. □

Corollary 3.5. (Hunter) Every number field of degree $n > 1$ contains an element θ not in $\mathbb{Q}$, the conjugates θ_i of which satisfy the condition

$$n\sum_{i=1}^{n}|\theta_i|^2 - \mathrm{Tr}_{K/Q}(\theta)^2 = \sum_{i<j}|\theta_j - \theta_i|^2 \le n\gamma_{n-1}\left(\frac{|d_K|}{n}\right)^{1/(n-1)}.$$

Note that $\gamma_{n-1}^{n-1} = \kappa_{n-1}^{-1}$, a rational number. We may thus write the inequality above as

$$S_K(\theta) \le \left(n^{n-2}\gamma_{n-1}^{n-1}\,|d_K|\right)^{1/(n-1)},$$

say, $S_K(\theta) \le \left(\alpha_n d_K\right)^{1/(n-1)}$, with a rational coefficient α_n.

This inequality is optimal when $n = 2$ ($\gamma_1 = 1$). When $n = 3$, this is optimal if and only if K is cyclic (the projection must be a hexagonal lattice). Optimality is not expected in larger degrees. At any rate, the Hermite constant is not significant for the problem of small discriminants. Other bodies could have been used, but the loss of information mainly comes from the bad quality of the bounds of the elementary symmetric functions of characteristic polynomial.

We now indicate briefly how one can use crude inequalities deduced from theorem 3.4 to prove the following theorem:

Theorem 3.6. (Hermite) *Let $B > 0$. Then there are only finitely number fields (up to isomorphism, or inside a given algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$) such that $|d_K| \le B$.*

Proof. Minkowski's Theorem 2.6 shows that the discriminants of number fields tend to ∞ with the degree. Hence it suffices to consider number fields having a given degree n.[3]

For every non-trivial divisor m of n, one must consider the possibility that K may contain a strict subfield $K' \neq \mathbb{Q}$ with $[K : K'] = m$ (including $m = n$). The transitivity formula of discriminants then shows that $|d_{K'}| \le B^{1/m}$,[4] so that we know by induction that there are only finitely many fields $K' \subset \overline{\mathbb{Q}}$ to consider, and we may moreover assume that K/K' is primitive.

Fix such a field K'. Using the invariance of $S_{K/K'}$ under translations by integers of K', we may choose $\mathrm{Tr}_{\sigma,K/K'}(\theta)$ among $m^{[K':\mathbb{Q}]}$ values

[3] Hermite proved his theorem before geometry of numbers was invented, and used inequalities from the theory of positive definite quadratic forms. Proofs using geometry of numbers are simpler. The same comments apply to Dirichlet's unit theorem.

[4] We have $d_K = d_{K'}^m$ only if K/K' is unramified; otherwise, a "relative Stickelberger congruence" will show that $|d_K/d_{K'}| \ge 3$; one can also bound $|d'_K|$ using inequality 2.12 of [Mar1].

(and indeed less, using the action of roots of unity over $\mathbb{Q}$, it suffices to consider the $\lceil \frac{n+1}{2} \rceil$ values $0, 1, \dots, \lfloor \frac{n}{2} \rfloor$).

Fix now the value $\mathrm{Tr}_{\sigma,K/K'}(\theta)$ for a θ as in Theorem 3.4. Then Theorem 3.4 and Proposition 3.3 bound the absolute values of the conjugate of θ over K', hence the conjugates of the coefficients of the minimal polynomial of θ over K'. There are thus only finitely many possible characteristic polynomials of K over $\mathbb{Q}$. ☐

Notation 3.7. For $\theta \in K$, we denote by $s_1, \dots, s_m$ the elementary symmetric functions of the conjugates of θ over K'. Thus the characteristic polynomial of θ over K' is

$$f(X) = X^m - s_1 X^{m-1} + \cdots + (-1)^m \,.$$

The proof above can hardly be effectively applied to list the small discriminants. In practice, one must use various tricks to bound more efficiently the coefficients of the polynomials. In the case of totally real fields, that we shall illustrate below with various examples, the absolute values which occur in the Theorems above disappear, which allows one to write more precise inequalities. Otherwise it is difficult to take into account the signature, except that one will find naturally the smallest discriminants when there is at most one real place. Actually, the minimal discriminants are known for all signatures up to $n = 7$, but in degree 8, only for fields which are either totally imaginary (Diaz y Diaz)[5]or totally real (Pohst-Martinet-Diaz y Diaz)[6]; and in this last case, the authors had to use *local corrections*; see Appendix *an-geo*.

Remark 3.8. Theorem 3.4 bounds $S_{K/K'}$ in terms of the relative discriminant of some $\theta \in K$. Conversely we can use the arithmetico-geometric inequality to bound this discriminant in terms of $S_{K/K'}$. We obtain

$$|N_{K'/\mathbb{Q}}(d_{K/K'}(\theta))| \leq \left(\frac{S_{K/K'}(\theta)}{n(m-1)/2} \right)^{n(m-1)/2} .$$

3.2. **Some evaluations for totally real fields.** We now restrict ourselves to the case when $K' = \mathbb{Q}$ and K is totally real. and consider an integer $\theta \in K$, with characteristic polynomial

$$f(X) = X^n - s_1 X^{m-1} + s_2 X^{m-2} + \cdots + (-1)^n \,.$$

and conjugates $\theta_1 \leq \theta_2 \leq \cdots \leq \theta_n$. When applying Hunter's theorem, we shall assume that $t_1 \in \{0, 1, \dots, \frac{n}{2}\}$ and that $t_3 > 0$ if $t_1 = 0$.

[5] *Petits discriminants des corps de nombres totalement imaginaires de degré* 8, J. Number Theory **25** (1987), 34–52.

[6] *The minimum discriminant of totally real octic fields*, J. Number Theory **36** (1990), 145–159

We have

$$S_K(\theta) = \sum_{1\le i<j\le n} (\theta_j - \theta_i)^2 = (n-1)\sum_{i=1}^{n} \theta_i^2 - 2 \sum_{1\le i<j\le n} \theta_i\theta_j = (n-1)\, t_1^2 - 2n\, t_2 \,.$$

Example 3.9. Totally real cubic fields.

For real cubic fields, Corollary 3.5 reads $S_K \le \sqrt{4d_K}$, and we have $t_1 = 0$ or $t_1 = 1$. We use the formula $d_g = -4p^3 - 27q^2$ for the discriminant of $g = X^3 + pX + q$, which we apply with $g = f$ if $t_1 = 0$, and after the translation $X \mapsto X + \frac{1}{3}$ if $t_1 = 1$.

Take $B = 169$. By Theorem 3.5, it suffices to consider fields K with $S_K \le 26$. Using the condition $d_f > 0$, getting rid of reducible polynomials, and discarding polynomials having a too large discriminant (*warning*: one must take care of square divisors of d_f which might produce fields for which d_K is a strict divisor of d_f), we find the following results:

- $s_1 = 0$ ($S \equiv 0 \mod 6$). Then $s_2 = 3$, $S = 18$, $s_3 = 1$ ($d_k = 81$); or $s_2 = 4$, $S = 24$, $s_3 = 1$ ($d_K = 229$) or $s_3 = 2$ ($d_K = 148$); or $S \ge 30$.
- $s_1 = 1$ ($S \equiv 2 \mod 6$). Then $s_2 = 2$, $S = 14$, $s_3 = 1$ ($d_k = 49$); or $s_2 = 3$, $S = 20$, $s_3 = 1$ ($d_k = 148$); or $s_2 = 4$, $S = 26$, $s_3 = -1$ ($d_k = 169$), or $s_3 \in \{1,2,3\}$ and $d_K > 169$; or $S \ge 32$.

We note that two polynomials (f, with $S = 20$, and g, with $S = 24$) have discriminant 148. We check that if θ is a root of f, then $\theta^2 - \theta - 2$ is a root of g. We have thus proved:

Proposition 3.10. *The first three values of S_K for a totally real cubic field are $S = 14$, 18, 20, attained exactly on the fields having the smallest three discriminants, namely $d_K = 49$, 81, 148, defined by the polynomials $X^3 - X^2 - 2X + 1$, $X^3 - 3X - 1$, and $X^3 - X^2 - 3X + 1$, respectively. The fourth field has $d_K = 169$ and $S = 24$, and is defined by the polynomial $X^3 - X^2 - 4X - 1$.*

Using a method of Davenport, we shall prove in Section 6 that the lower bounds $S = 14$ and $d = 49$ are attained uniquely among admissible lattices for $A_{3,0}$ on the ring of integers of field with discriminant 49.

Example 3.11. Totally real quartic fields.

In degree 4 the sign of the discriminant does not suffice to decide whether a polynomial has 0 or 4 real roots. We first recall a result which solves this problem. For a proof, see [D-F].[7]

Proposition 3.12. *Let $f = X^4 - aX^3 + bX^2 - cX + d \in \mathbb{R}[X]$. Then f has 4 real roots if and only if the following three conditions are satisfied:*

(1) $d_f > 0$.

---

[7] However in [D-F] condition (2[?]) is written with a wrong sign

(2) $3a^2 - 8b > 0$.
(3) $b^2 - a^2 b + \frac{3}{16}a^4 + ac - 4d > 0$.

We now consider a polynomial $f = X^4 - s_1X^3 + s_2X^2 - s_3X + s_4 \in \mathbb{Q}[X]$. Theorem 3.5 reads $S_K \le (32\,d_K)^{1/3}$. Applied with the two known discriminants obtained as extensions of $K_0 = \mathbb{Q}(\sqrt{5})$, namely $725 = 5^2 \cdot 29$ and $1125 = 3^2 \cdot 5^3$ (corresponding to the maximal real subfield of $\mathbb{Q}(\sigma_{15})$), we obtain for S_K the bounds 28 and 32, respectively.

We have $S_f \equiv 3s_1^2 \bmod 8$, that is $(S_f \bmod 8, s_1) = (0,0)$, $(3,1)$, or $(4,2)$. For each *a priori* possible choice S for S_f, we bound s_4^2 by the arithmetico-geometric inequality between the squares of the roots of f, which gives $|s_4| < \left(\frac{S+s_1^2}{16}\right)^{1/2}$. For s_3, we use the four bounds of type

$$|\theta_1\theta_2\theta_3| < \left(\frac{S + s_1^2 - \theta_4^2}{12}\right)^{3/2} < \left(\frac{S + s_1^2}{12}\right)^{3/2}$$

and observe that the θ_i cannot have the same sign, and thus bound $|s_3|$ by $2\left(\frac{S+s_1^2}{12}\right)^{3/2}$ if $s_4 > 0$ and by $3\left(\frac{S+s_1^2}{12}\right)^{3/2}$ if $s_4 < 0$. These somewhat crude estimates suffice to classify the polynomials associated with fields having $S_K \le 32$; ω stands for the golden ratio $\frac{1+\sqrt{5}}{2}$:

$S_K = 27$: $d_K = 725$, $f = X^4 - X^3 - 3X^2 + X + 1 = N_{K/\mathbb{Q}(\sqrt{5})}(X^2 - \omega X - 1)$.
$S_K = 28$: $d_K = 725$, $f = X^4 - 2X^3 - 2X^2 + 3X + 1 = N_{K/\mathbb{Q}(\sqrt{5})}(X^2 - X - \omega^2)$.
$S_K = 32$: we find three polynomials, with discriminants
1957 ($f = X^4 - 4X^2 + X + 1$), a primitive field;
$2048 = 2^{11}$ ($f = X^4 - 4X^2 + 2$, $K = \mathbb{Q}(\sqrt{2+\sqrt{2}})$);
$2304 = 2^8 \cdot 3^2$ ($f = X^4 - 4X^2 + 1$, $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$).

We observe that we have not found the Abelian field $\mathbb{Q}(\zeta_{15})^+$, of discriminant 1125, which shows the necessity of also classifying the imprimitive fields. This field needs $S_K \ge 35$, and the minimal polynomial of $\zeta_{15} + \zeta_{15}^{-1}$ is actually $f = X^4 - X^3 - 4X^2 + 4X + 1$, for which $S_f = 35$.

Using the bound in Theorem 3.4, or using class field theory, we check that for $d_K < 1400$ (the bound which ensures $S_K < 35$), there are only the two imprimitive fields quoted above. We have thus proved:

Proposition 3.13. *Let K be a totally real field of degree 4. Then:*

(1) *Either K is one of the two fields with discriminants 725 and 1125 quoted above, or we have $d_K \ge 1400$.*
(2) *The three smallest values for S_K are $S_K = 27$, attained on the field with discriminant 725, $S_K = 32$, attained on one of three fields with discriminants 1957, 2048 or 2304, and $S_K = 35$, attained in particular on the field with discriminant 1125.* □

Example 3.14. Totally real quintic fields. Here Corollary 3.5 reads $S_K \le (500|d_K|)^{1/4}$. The maximal real subfield $\mathbb{Q}(\zeta_{11})^+$ of $\mathbb{Q}(\zeta_{11})$ has discriminant $11^4 = 14641$, and may be defined by the polynomial $X^5 - X^4 - 4X^3 + 3X^2 + 3X - 1$, the minimal polynomial of $-(\zeta_{11} + \zeta_{11}^{-1})$, for which $S = 44$.

To complete after a PARI run

4. More on Minkowski's domains

In this section, after having introduced in the first subsection some notions which apply to general distance-functions and open star bodies (always with respect to the origin, and assumed to be symmetric) in a Euclidean space E, we consider the distance-functions $F = F_{r_1,r_2}$ on $\mathbb{R}^n$, $n = r_1 + 2r_2$ (Definition 2.1) and the corresponding Minkowski domains A_{r_1,r_2} defined by $F(x) < 1$, first for any signature, then in the totally real case.

4.1. **Automorphisms and isolation phenomena.**

Definition 4.1. We say that $u \in \mathrm{GL}(E)$ is an *automorphism of a star body* A (resp. of a *distance-functions* F) if $u(A) = A$ (resp. if $F(u(x)) = F(x)$ for all $x \in E$). **Notation**: $\mathrm{Aut}(A)$, $\mathrm{Aut}(F)$.

Clearly, $\mathrm{Aut}(A_F) = \mathrm{Aut}(F)$. These automorphism groups are closed subgroups of $\mathrm{GL}(E)$, hence Lie groups, thus have a well-defined dimension. As in any topological group, their connected components are closed, normal subgroups.

Example 4.2. Quadratic domains.
Let q be a non-degenerate quadratic form. Then the automorphism group of the distance-function $|q|$ is the orthogonal group $\mathrm{O}(q)$ of q. Its connected component has index 2 if q is definite, 4 if q is indefinite.

Proposition 4.3. *Let A be an open star body (with respect to the origin). If there exist admissible lattices for A, then any automorphism of A has determinant ± 1.*

Proof. Assume that Λ is admissible for A, and that there exists $u \in \mathrm{Aut}(A)$ of determinant not ± 1. Changing u into u^{-1} if need be, we may assume that $\det(u) < 1$. Then $\Lambda_n = u^n(\Lambda)$ is admissible for all n, and we have $\lim_{n\to\infty} \det(\Lambda_n) = 0$, which contradicts the existence of a lower bound for the determinant of an admissible lattice of any neighbourhood of 0. $\square$

Definition 4.4. We say that a lattice Λ is *minimal-admissible for an open star body* A if Λ is admissible for A but the lattices λA are not if

$\lambda < 1$, that Λ is *extreme for A* if Λ is admissible for A and its determinant is a local minimum on the set lattices which are admissible for A, and that Λ is *critical* (or *absolutely extreme for A*) if its determinant is the smallest possible among that of all lattices which are admissible for A (that is, if $\det(\Lambda) = \kappa(A)$, the lattice constant of A).

Proposition 4.5. *Let A be an open, symmetric star body (with respect to the origin). Assume that admissible lattices for A exist. Then there also exist critical lattices for A.*

Proof. Since the set of admissible lattices for A is not empty and A is a neighbourhood of the origin, we have $0 < \kappa(A) < +\infty$. For $n > 0$, there exists an admissible lattice Λ_n with $\kappa(A) \leq \det(\Lambda_n) \leq \kappa(A) + \frac{1}{n}$. On this family, the determinants are bounded from above (by $\det(\Lambda_1)$) and the Euclidean distance to 0 is bounded from below (by the radius of a small enough ball centred at the origin). By Mahler's compactness lemma, one can extract from (Λ_n) a sub-sequence which converges to a lattice Λ. We have $\det(\Lambda) = \kappa(A)$, and $A \cap (\Lambda \smallsetminus \{0\})$ is empty since $\complement A$ is closed. $\square$

It is easy to prove that if A is a bounded star body, then admissible, hence also critical lattices exist, and that extreme lattices have n independent points on the boundary of A; see [Cas2], V.6. (If A is convex, extreme lattices even have at least $\frac{n(n+1)}{2}$ points on the boundary of A; theorem of Swinnerton-Dyer; see [Cas2], V.8).

Nothing similar holds for unbounded star bodies. First, it may happen that no admissible lattice exist (by Proposition 4.3, this is the case for the set $A = \{(x,y) \in \mathbb{R}^2 \mid x^2|y| < 1\}$). A less trivial example is provided by the indefinite quadratic domains of dimension $n \geq 5$ (*conjecture of Oppenheim, now a theorem of Margulis*).[8]

The notion we introduce below will allow us to prove in some cases the existence of points on the boundary.

Definition 4.6. We say that a distance-function F or its corresponding star body A_F is of *compact type* (Mahler said *automorphic*) if the following property holds: for every $B > 0$, there exists a compact subset C_B of E such that for every $x \in E$ with $F(x) < B$, there exists $u \in \mathrm{Aut}(F)$ which maps x into K_B.

[8]This results from the more precise statement: *every non-degenerate, indefinite real quadratic form of dimension $n \geq 3$ which* is not *proportional to an integral form takes on $\mathbb{Z}^n$ arbitrary small values of each sign*, since by the Hasse-Minkowski theorem, indefinite integral quadratic forms of dimension $n \geq 5$ represent zero.

Proposition 4.7. *Let F be a distance-function of compact type. Then for every minimal-admissible lattice Λ for A_F, there exists a sequence u_k of automorphisms of F such that the sequence $u_k(\Lambda)$ converges to a lattice having a a point on the boundary of A_F.*
[This lattice is minimal-admissible and has the same determinant as Λ.]

Proof. Since Λ is minimal-admissible, it contains for all $n > 0$ a point x_n such that $F(x_n) < \det(\Lambda) + \frac{1}{n}$. Let $B = \det(\Lambda) + 1$. There exists a compact set $K_B \subset E$ and for every n, an automorphism u_k of F such that $u_k(x_n) \in K_B$. By successive extractions of sequences, we construct a map $\varphi : \mathbb{N} \to \mathbb{N}$ such that $u_{\varphi(k)}(\Lambda)$ tends to a lattice Λ' and $u_{\varphi(k)}(x_n)$ tends to a point $x \in E$. Then Λ' is admissible for A_F and x belongs to $\partial A \cap \Lambda'$. $\square$

Corollary 4.8. *If A_F possesses admissible lattices, then it possesses critical lattices having at least one pair $\pm x$ of points on its boundary.* $\square$

Proposition 4.7 does not suffice to prove that every lattice Λ which is extreme for a domain A of compact type has points on ∂A. All we can say is that such a lattice exists in the closure of the set $\{u(\Lambda) \mid u \in \mathrm{Aut}(F)\}$. The notion we introduce in the definition below will allow us to conclude in some situations.

Definition 4.9. We say that an admissible lattice Λ for an open star body A is *isolated* if there exists a neighbourhood of A on which every admissible lattice is of the form $\lambda u(\Lambda)$ for some $\lambda \geq 1$ and some $u \in \mathrm{Aut}(A)$.
[Clearly, "isolated" $\Longrightarrow$ "extreme" $\Longrightarrow$ "minimal-admissible".]

It may happen that we are able to show that the sequence $u_k(\Lambda)$ in Proposition 4.7 converges to an isolated lattice. Then the sequence must be stationary, and consequently, the initial lattice Λ itself does have a point on the boundary of A.

4.2. **The automorphism groups of Minkowski's domains.** We construct automorphisms of the Minkowski domain A_{r_1,r_2}, that we write in the form

$$\prod_{k\leq r_1} |x_k| \prod_{k\leq r_2} (y_k^2 + z_k^2) \ \big(= \prod_{k\leq r_1} |x_k| \prod_{k\leq r_2} |y_k + iz_k|^2 \,, i^2 = -1\big) < 2^{r_2} \,.$$

Definition 4.10. Let λ_k ($k \leq r_1$) and μ_k ($k \leq r_2$) be $r_1 + r_2$ strictly positive real numbers, and let ω_k ($k \leq r_2$) be r_2 real numbers $\mod 2\pi$, submitted to the condition $\prod \lambda_k \prod \mu_k^2 = 1$. Let $G^\circ \subset \mathrm{GL}_n(\mathbb{R})$ be the group of transformations $x_k \mapsto \lambda_k x_k$, $y_k + iz_k \mapsto \mu_k e^{i\omega_k}(y_k + iz_k)$, and let

$G \subset \mathrm{GL}_n(\mathbb{R})$ be the group generated by G°, the change of signs of the x_k and the z_k, the $r_1!$ permutations of the x_k, and the $r_2!$ permutations of the $y_k + iz_k$.

It is clear that G is a group of automorphisms of A_{r_1,r_2} and that $G^\circ \simeq \mathbb{R}^{r_1+r_2-1} \times (R/2\pi\mathbb{Z})^{r_2}$, of dimension $n-1$, is its connected component. This information suffices for what we need in the sequel. For the sake of completeness, we nevertheless state the following result, leaving its proof to the reader.

Proposition 4.11. *The group G of Definition 4.10 is the group of all automorphisms of A_{r_1,r_2}.* $\square$

We observe that the Abelian group G°, modulo its maximal compact subgroup, has dimension $r_1 + r_2 - 1$, the *Dirichlet number* of fields K of signature (r_1, r_2), which is the rank of the unit group of any order $\mathfrak{O} \subset K$. Taking into account the unit 1, we see that an algebraic lattice will have at least $r_1 + r_2$ independent points on the boundary of A_{r_1,r_2}. In the totally real case, this is the maximal value. Otherwise, the maximal value will be $r_1 + r_2$, except if the order $\mathfrak{O}(M) = \{\lambda \mid \lambda M \subset M\}$ contains roots of unity distinct from ± 1.

In the easy case of $A_{0,1}$ (the disc of radius $\sqrt{2}$), minimal-admissible lattices are isometric to a lattice having a basis (e_1, e_2) with $N(e_2) \geq N(e_1) = 2$. The boundary of $A_{0,1}$ generally contains only the pair $\pm e_1$, except on the close subset $N(e_1) = N(e_2)$. Then we may assume that $\angle(e_1, e_2) \in [\frac{\pi}{3}, \frac{\pi}{2}]$. The endpoints of this interval correspond to algebraic lattices (Eisenstein and Gaussian integers). Lattices corresponding to angles in the open interval $(\frac{\pi}{3}, \frac{\pi}{2})$ are not algebraic.

We now use the automorphisms constructed above to prove in a precise form that Minkowski's domains are of compact type (see Subsection 4.1).

Theorem 4.12. (1) *Let $B > 0$ and $x \in \mathbb{R}^n$ with $0 < F_{r_1,r_2}(x) \leq B$. Then there exists an automorphism of A_{r_1,r_2} which maps x into the compact interval $\{\lambda \mathbf{1}\}$, $0 \leq \lambda \leq 2^{-r_2/n} B^{1/n}$ of $\mathbb{R}\,\mathbf{1}$.*

(2) *If Λ is a minimal-admissible lattice for A_{r_1,r_2}, there exists a sequence u_k of automorphisms of A_{r_1,r_2} such that $u_k(\Lambda)$ tends to a lattice Λ' containing $\mathbf{1}$.*

Proof. (1) Let $x \in \mathbb{R}^n$ such that $F_{r_1,r_2}(x) \leq B$, and let x_i, y_j, z_j be the components of x (notation Definition 4.10). We may assume by changing signs that the components are non-negative, hence strictly positive, and using plane rotations in the r_2 planes $\langle y_j, z_j \rangle$, that $y_j = z_j$

for $j = 1, \dots, r_2$. Set

$$\lambda_i = \frac{F(x)^{1/n}}{x_i} \text{ for } i = 1, \dots, r_1 \text{ and } \mu_j = \frac{F(x)^{1/n}}{\sqrt{y_j^2 + z_j^2}} \text{ for } j = 1, \dots, r_2 \,.$$

Then $x_i \mapsto \lambda_i x_i$, $(y_j, z_j) \mapsto \mu_j(y_j, z_j)$ is an automorphism of A_{r_1,r_2}, which transforms x into a vector with equal components x_i and equal components y_j, z_j. If $r_1 = 0$ or $r_2 = 0$, we are done. Otherwise, we perform the transformation $x_i \mapsto \lambda x_i$, $(y_j, z_j) \mapsto \mu(y_j, z_j)$ with $\lambda = (y_1 x_1^{-1})$ and $\mu = \frac{x_1}{y_1}\,\lambda$.

(2) For $k = 1.2, \dots$, there exists $x^{(k)} \in \Lambda$ with $F(x^{(k)}) \leq 2^{r_2}(1 + \frac{1}{k})$. By (1), there exists $u_k \in \mathrm{Aut}(A_{r_1,r_2}$ which maps $x^{(k)}$ to an $y_k \in 2^{r_2/n}[1, \varepsilon_k]\,\mathbf{1}$ with $\varepsilon_k = O(\frac{1}{k})$. We can extract from the sequence $u_k(\Lambda)$ a converging sub-sequence, the limit of which contains an y which belongs to $\cap_k 2^{r_2}[1, \varepsilon_k]\,\mathbf{1} = \{2^{r_2}\,\mathbf{1}\}$. □

4.3. **The function S for totally real Minkowski domains.** Let $x = (x_1, \dots, x_n) \in \mathbb{R}^n$. We assume that the components of x satisfy $x_1 \leq x_2 \leq \cdots \leq x_n$. In Definition 3.1 we introduced the function

$$S(x) = \sum_{1 \leq i < j \leq n} (x_j - x_i)^2 \,.$$

We shall need later, in particular in section 6, to estimate the size of S for a given difference $x_n - x_1$. (Note that S is invariant under translations.) This is the aim of the proposition below.

Proposition 4.13. *We have*

$$\frac{n}{2}\,(x_n - x_1)^2 \leq S \leq k(n-k)(x_n - x_1)^2$$

with $k = \frac{n}{2}$ if n is even and $k = \frac{n-1}{2}$ or $k = \frac{n+1}{2}$ if n is odd.

The minimum is attained exactly when $x_i = \frac{x_1 + x_n}{2}$ for $1 < i < n$, and the maximum when x_i takes k times the value x_1 and $n - k$ times the value x_n.

Proof. One can write $S - (x_n - x_1)^2$ as a sum of non-negative terms $(x_i - x_j)^2(1 < i < j < n$ and of $n - 2$ terms $(x_i - x_1)^2 + (x_n - x_i)^2$ which are minimum exactly when $x_i = \frac{x_1 + x_n}{2}$, and the other terms are then zero.

The minimum is attained at the only point where all partial derivatives vanish, so that the maximum is attained on the boundary of the domain $[x_1, x_n]^n$. By induction, we see that all x_i are equal to x_1 or x_n, so that the maximum is of the form $k(n-k)(x_n - x_1)^2$, and $k(n-k)$ is maximum exactly for $k \in [\frac{k-1}{2}, \frac{k+1}{2}]$. □

In practice, the x_i will never take many equal values, so that the bounds in the proposition above will be strict. We shall prove some better estimates when x belongs to a lattice Λ which is admissible for $A_{n,0}$ and contains 1.

4.4. **Totally real Minkowski domains.** In this subsection, we consider 2-dimensional lattices in $\mathbb{R}^n$ having a basis of the form $(\mathbf{1}, x)$ and no points in $A_{n,0}$; otherwise stated, we have $F_{n,0}(y) \geq 1$ for all $\mathbb{Z}$-linear combination of $\mathbf{1}$ and x. We write $(x_1, \dots, x_n)$, and assume that $x_1 \leq x_2 \leq \cdots \leq x_n$. (We can reduce ourselves to this case since permutations of the coordinates are automorphisms of $A_{n,0}$ which preserve $\mathbf{1}$.) We observe that the x_k are not integral, so that each x_k lies in some interval $\mathcal{J}_k = (m_k, m_k + 1)$, and even that x_k cannot be too close to an endpoint of $\mathcal{J}_k$. This we now give a precise form.

Fix an index i. We observe that we have $x_j - m_i \leq m_j - m_1 + 1$ if $x_j \geq m_i$, and $m_i - x_j \leq m_i - m_j$ if $x_j < m_i$, and similar upper bounds for $|m_i + 1 - x_j|$. Since the products of the $|x_j - m_i|$ and $|m_i + 1 - x_j|$ are ≥ 1, we obtain this way upper bounds for $x_i - mi$ and $m_i + 1 - x_i$. We state the result in the proposition below.

Proposition 4.14. *Set*

$$a_{i,j} = m_j - m_i + 1 \textit{ if } x_j \geq m_i \textit{ and } a_{i,j} = m_i - m_j \textit{ if } x_j < m_i\,,$$

and

$$b_{i,j} = m_j - m_i \textit{ if } x_j > m_i \textit{ and } b_{i,j} = m_i - m_j + 1 \textit{ if } x_j \leq m_i$$

(thus $a_{i,i} = b_{i,i} = 1$). Then we have

$$0 < x_i - m_i < \prod_j a_{i,j}^{-1} \quad \textit{and} \quad 0 < m_i + 1 - x_i < \prod_j b_{i,j}^{-1}\,. \quad \square$$

Proposition 4.14 gives us upper bounds for all differences $x_j - m_j$ and $m_j + 1 - x_j$, that can then be used in the proof above. This "round 2" calculations produce improvements on the result above. We produce this way two families $(a_i^{(k)})$ and $(b_i^{(k)})$, $k \in \mathbb{N}$, of increasing sequences contained in $(0, 1)$, such that, for all i, one has $m_i + a_i^{(k)} < x_i < m_i + 1 - (b_i^{(k)}$. These sequences have limits a_i, b_i, and we have $a_i \leq x_i \leq b_i$ for $i = 1, \dots, n$. One can even use infinitely many inequalities, those we obtain by calculating as above $|pm_j - qx_j|$ and $|p(m_i + 1) - qx_j|$ for convenient integers p, q (depending on i and j). The difficulty is to guess what "convenient" means. The *Markoff chain* for $A_{2,0}$, described in Section 5 below, is one of the few cases for which this difficult problem was solved. Examples of calculations of these limits are displayed in Subsection 5.1.

Remark 4.15. When classifying the possible values of $S(x)$ (always assuming that $\langle \mathbf{1}, x\rangle \cap A_{n,0} = \emptyset$), we may replace x by $x+k$ for any $k \in \mathbb{Z}$, and thus fix the integral part of one x_k, say, assume that $0 < x_1 < 1$. Moreover, using the symmetry $x \mapsto -x$, we may assume one more restriction, for instance, $x_n - x_{n-1} > x_2 - x_1$.

If we fix an upper bound for S, then $x_n - x_1$ is bounded, and choosing x_1 in $(0,1)$, we see that the x_k must be chosen in only finitely many intervals (m_k, m_{k+1}).

Proposition 4.16. *Still under the hypothesis $\langle \mathbf{1}, x\rangle \cap A_{n,0} = \emptyset$, we have:*

(1) *The components of x do not lie in the union of two consecutive intervals $\mathcal{J}_k$.*
(2) *If $n-1$ components of x lie in a same interval $\mathcal{J}_k$, then $S > \frac{n-1}{4}(2^n-1)^2$.*
(3) *If the components of x lie in the union of three consecutive intervals $\mathcal{J}_k$, no $(n-1)$ of them lying in the same interval, then one of the following properties holds:*
(a) $n=4$, $m_1 = m_2$, and $m_3 = m_4 = m_2 + 2$.
(b) $n=5$, $m_1 = m_2$, $m_3 = m_2 + 1$, and $m_4 = m_5 = m_1 + 2$.
(c) $n \geq 6$.

Proof. (1) By translation, we may assume that all x_i belong to $(-1,+1)$, which contradicts the lower bound $\prod_i x_i \geq 1$.

(2) By translation and symmetry $x \mapsto -x$, we may assume that $x_i \in (0,1)$ for $i < n$, which implies $x_i(1-x_i) \leq \frac{1}{4}$, hence $x_n(x_n-1) > 4^{n-1}$, thus $x_n > \frac{1+\sqrt{1+4^n}}{2} > \frac{2^n+1}{2}$, whence the result, since $x_n - x_i > \frac{2^n-1}{2}$ for $i < n$.

(3) If $n=3$ we may assume that $-1 < x_1 < 0 < x_2 < 1 < x_3 < 2$. We then have $x_2(1-x_2) \leq \frac{1}{4}$ and $x_i|1-x_i| < 2$ for $i = 1,3$, hence $\prod_i x_i \prod_i |1-x_i| < 1$, a contradiction. We may now assume that $n \geq 4$.

Suppose that $n-2$ components of x lie in the same interval, say, $(0,1)$, a hypothesis which holds for $n=4$. Then the product $\prod_i x_i \prod_i (1-x_i)$ on these components is bounded from above by $\frac{1}{4^{n-1}}$. Using the symmetry $x \mapsto 1-x$, we may assume that the remaining two components are not negative, so that one of the three cases holds: (1) $x_1 \in (0,1), x_n \in (1,2)$; (2) $x_{n-1} \in (1,2), x_n \in (2,3)$; (3) $x_{n-1}, x_n \in (2,3)$. Bounding the products of the $x_i|1-x_i|$ for the remaining two components, we obtain the inequalities $4^{n-2} \leq 4$, $4^{n-2} \leq 12$, and $4^{n-2} \leq 26$, respectively. The first two are impossible, and the third one holds only if $n=4$ and if $x{,}x_2 \in (0,1)$ and $x_3, x_4 \in (2,3)$.

[Such systems exist: take (x,y) such that $\langle (1,1),(x,y)\rangle$ is admissible for

$A_{2,0}$, e.g., a lattice coming from the ring of integers of a quadratic subfield of a quartic field; then we may take $x_1 = x_2 = x$ and $x_3 = x_4 = y$.]

A similar proof applies in dimension 5: there must be clearly two pairs of components in the same interval, and we find as above that these pairs must be contained in the extreme intervals. □

Remark 4.17. An other way for bounding the x_i is to use the polynomial

$$f = \prod_i (X - x_i) = X^n - t_1 X^{n-1} t_2 X^{n-2} + \cdots + (-1)^n t_n\,.$$

For all $m \in \mathbb{Z}$, we have $|f(m)| = |\prod_i (X - m_i)| \geq 1$, and $f(m)$ has the sign of $(-1)^{n-n_m}$ where n_m is the number of roots of f which are smaller than m. An example occurs in Subsection 6.1. Amazingly, the quality of the inequalities obtained by this method is not invariant under integral translations. One should center the set $\{x_i\}$ close to small integers $(0, \pm 1, \dots)$.

More generally, for any vector $x = (x_1, \dots, x_n) \in \Lambda$, $x \notin \mathbb{R}\mathbf{1}$, we must have $\prod_{i=1}^n |(qx_i + p)| \geq 1$ for all $p, q \in \mathbb{Z}$, $q \neq 0$ (and indeed, $q > 0$ suffices), so that we have $|f(\frac{p}{q})| \geq \frac{1}{q^n}$ for all pairs of integers p and $q > 1$.

Definition 4.18. For $q \geq 1$, let

$$\mathcal{E}'_q = \{x \in \mathbb{R}^n \mid \forall\, p \in \mathbb{Z}, \prod_{i=1}^n |(qx_i + p)| \geq 1\} \quad \text{and} \quad \mathcal{E}_q = \cap_{k \leq q} \mathcal{E}'_k\,.$$

We moreover identify $x \in \mathcal{E}'_q$ with the relative lattice $\Lambda = \langle \mathbf{1}, x \rangle$.

If Λ is admissible for $A_{n,0}$, every $x \in \Lambda \smallsetminus \mathbb{Z}\mathbf{1}$ belongs to the intersection of the $\mathcal{E}_q$. In particular the set of admissible lattices for $A_{2,0}$ is the intersection of the $\mathcal{E}_q$.

Note that if $x \in \mathcal{E}'_q$, the components of x are not rational numbers, the denominator of which divides q. This proves:

Proposition 4.19. *If Λ is admissible for $A_{n,0}$, then every $x \in \Lambda \smallsetminus \mathbb{Z}\mathbf{1}$ has irrational components.* □

5. A glance at dimension 2

To classify the possible values of the determinants d of minimal-admissible lattices Λ for $A_{n,0}$ we may restrict ourselves to lattices Λ containing the point $\mathbf{1} = (1, \dots, 1)$; if moreover we can prove an isolation theorem for such lattices, we then obtain a classification of minimal-admissible lattices such that $\det(\Lambda) = d$.

The remaining of this section is devoted to $A_{2,0}$. Then a lattice Λ containing $\mathbf{1}$, say, $\Lambda = \langle \mathbf{1}, x \rangle$, is admissible for $A_{2,0}$ if and only if $x \in \cap_{q \geq 1} \mathcal{E}_q$.

In a first subsection, we prove that the first two minima of admissible lattices are attained on the lattices which are equivalent to the algebraic lattices associated with $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ and $\mathbb{Z}[\sqrt{2}]$, with determinants 5 and 8, respectively. This is a small part of Markoff's theorem, which describes all admissible lattices of determinant $d < 9$, that we state in a second subsection.

5.1. The first two minima for $\mathbf{A_{2,0}}$.

Lemma 5.1. *Let* $\Lambda \in \mathcal{E}_1$.

(1) Λ *has a basis* $(\mathbf{1}, x)$, *where* $x = (x_1, x_2)$ *satisfies the conditions*
$$-1 < x_1 < 0 \text{ and } m < x_2 < m + 1$$
for some integer $m \geq 1$.

(2) *Set* $u = x_1 + x_2$ *and* $v = x_1 x_2$, *so that* x_1 *and* x_2 *are the roots of* $f(X) = X^2 - uX + v$. *Then either* f *defines* x *uniquely, and then* $u = m$, *or there are two choices for* x, *one with* $u < m$ *and one with* $u > m$.

Proof. There exists $x \in \Lambda$ such that $(\mathbf{1}, x)$ is a basis for Λ, and such an x is unique up to a transformation $x \mapsto \pm x + k\,\mathbf{1}$ for some $k \in \mathbb{Z}$. Replacing x by $x + k\,\mathbf{1}$ for a convenient $k \in \mathbb{Z}$, we may assume that $-1 < x_1 \leq 0$ and $x_2 \geq x_1$. Set $m = \lfloor x_2 \rfloor$. Then we have $m \leq x_2 < m + 1$, but the cases $x_1 = 0$ and $x_2 = m$ must be excluded (if e.g., $x_2 = m$, then $x - m\mathbf{1}$ has a zero component), so that we have $-1 < x_1 < 0$ and $m < x_2 < m + 1$, and moreover $m \geq 1$ by Proposition 4.16. Then x is unique up to its replacement by $m\mathbf{1} - x$.

Finally if $x_1 + x_2 > m$, then $(m - x_1) + (m - x_2) < m$. $\square$

We now investigate the set $\mathcal{E}_1$, choosing $x \in \mathcal{E}_1$ satisfying the hypotheses of Lemma 5.1.

Theorem 5.2. (1) *Let* m *and* $x = (x_1, x_2)$ *be as in Lemma 5.1. Then the set of determinants* d *of lattices* $\Lambda = \langle \mathbf{1}, x \rangle$ *with* $x \in \mathcal{E}_1$ *fills the interval* $[m^2 + 4, m^2 + 4m]$.

(2) *The endpoints of the intervals above are obtained exactly on the lattices associated with the order of discriminant* d.

(3) *The set of values of* d *for* $x \in \mathcal{E}_1$ *is*
$$\{5\} \cup [8, 12] \cup [13, \infty)\,.$$

Proof. Recall that the determinant of Λ is
$$d = (x_2 - x_1)^2 = (x_1 + x_2)^2 - 4x_1 x_2 = u^2 - 4v\,.$$
The conditions $x_1 \in (-1, 0)$ and $x_2 \in (m, m + 1)$ are equivalent to the four inequalities
$$f(-1) > 0,\ f(0) < 0,\ f(m) < 0,\ f(m + 1) > 0\,,$$

and the condition $x \in \mathcal{E}_1$ to

$$\forall\, k \in \mathbb{Z},\ |f(k)| \geq 1\,.$$

Hence the conditions

$$f(-1) \geq 1,\ f(0) \leq -1,\ f(m) \leq -1,\ f(m+1) \geq 1$$

are necessary for Λ to belong to $\mathcal{E}_1$, and they are indeed also sufficient, since we have $f(x) > f(-1)$ on $(-\infty, -1)$, $f(x) < \max(f(1), f(m))$ on $(0, m)$ and $f(x) > f(m+1)$ on $(m+1, \infty)$. These conditions read

(a): $u + v \geq 0$; (b): $v \leq -1$; (c): $u \geq \frac{v+m^2+1}{m}$; (d): $u \leq \frac{v+m^2+2m}{m+1}$.

Using (a) and choosing $u \leq m$, we obtain the upper bound

$$d = u^2 - 4v \leq u^2 + 4u \leq m^2 + 4m = (m+2)^2 - 4\,,$$

which is attained uniquely if $u = m$ and $v = -m$, and then Λ is associated with the order of discriminant $d = m^2 + 4m$.

Similarly, using (b) and choosing $u \geq m$, we obtain the lower bound

$$d = u^2 - 4v \geq u^2 + 4 \geq m^2 + 4\,,$$

attained uniquely if $u = m$ and $v = -1$, and then Λ is associated with the order of discriminant $d = m^2 + 4$.

Taking $u = m$ and letting v run through $[-m, -1]$, we obtain polynomials taking convenient values at -1, 0, m, $m+1$, with determinants running through the whole interval $I_m = [m^2 + 4, m^2 + 4m]$. This proves (1) and (2).

To prove (3), just observe that $I_1 = [5, 5]$, $I_2 = [10, 12]$ and $I_3 = [13, 21]$, and that I_m and I_{m+1} overlap for $m \geq 3$ ($I_4 = [20, 32]$, etc.). □

Since the lattice $L = \langle \mathbf{1}, (\frac{1-\sqrt{5}}{2}, \frac{1+\sqrt{5}}{2}) \rangle$ is isolated among lattices of determinant $d \leq 8$, we have:

Corollary 5.3. *The lattice constant of $A_{2,0}$ is $\kappa_{2,0} = 5$, and is attained only on lattices equivalent to the lattice of $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$. Other minimal-admissible lattices have a determinant $d \geq 8$.* □

Remark 5.4.
(1) The end points of the intervals I_m above are quadratic surds having a purely periodic continued fraction, namely $[\,\overline{m}\,]$ on the left and $[\,\overline{m\,1}\,]$ on the right. ($[\,\overline{m\,1}\,] = [\,\overline{1}\,]$ if $m = 1$!)
(2) The orders defined by these endpoints need not be maximal. An example is provided by I_4, the endpoints of which both have conductor 2.

The next step in the study of admissible lattices for $A_{2,0}$ consists in analyzing $\mathcal{E}_q$ for $q = 2, 3, \dots$. To this end we consider conditions $x_1 \in (-1 + \frac{i}{q}, -1 + \frac{i+1}{q})$ and $x_2 \in (m + \frac{i}{q}, m + \frac{i+1}{q})$ for $i = 0, \dots, q-1$, that is, q^2 pairs of intervals, among which q are fixed and $\frac{q(q-1)}{2}$ are exchanged by $x \mapsto m\mathbf{1} - x$, and by Theorem 5.2, we may assume that $m \geq 2$.

This we now do for $q = 2$, dividing $I = (-1, 0)$ and $J = (m, m+1)$ (now for $m \geq 2$) into sub-intervals $I' = (-\frac{1}{2}, 0)$, $I'' = (-1, -\frac{1}{2})$, and $J' = (m, m+\frac{1}{2})$, $J'' = (m+\frac{1}{2}, m+1)$, and making use of the conditions $|f(-\frac{1}{2})| \geq \frac{1}{4}$ and $|f(m+\frac{1}{2})| \geq \frac{1}{4}$ besides conditions (a) to (d) introduced in the proof of Theorem 5.2.

Theorem 5.5. *Let Λ be a lattice having a basis of the form $(\mathbf{1}, x)$, $x = (x_1, x_2)$, with $-1 < x_1 < 0 < x_2$ and $x \in \mathcal{E}_2$. Then up to a symmetry, one of the following conditions holds:*

(1) $1 < x_2 < 2$, *and then* $(x_1, x_2) = \left(\frac{1-\sqrt{5}}{2}, \frac{1+\sqrt{5}}{2}\right)$ *and* $\det(\Lambda) = 5$ *;*
(2) $-\frac{1}{2} < x_1 < 0$ *and* $2 < x_2 < \frac{5}{2}$, *and then* $(x_1, x_2) = (1 - \sqrt{2}, 1 + \sqrt{2})$ *and* $\det(\Lambda) = 8$ *;*
(3) $-1 < x_1 < -\frac{1}{2}$ *and* $2 < x_2 < \frac{5}{2}$, *or* $-\frac{1}{2} < x_1 < 0$ *and* $\frac{5}{2} < x_2 < 3$, *and then the set of values taken by* $\det(\Lambda)$ *is the interval* $[\frac{221}{25}, \frac{480}{49}]$ $(= [8.84, 9.7959\dots])$ *;*
(4) $-1 < x_1 < -\frac{1}{2}$ *and* $\frac{5}{2} < x_2 < 3$, *and then the set of values taken by* $\det(\Lambda)$ *is the interval* $[10, 12]$.
(5) $x_2 > 3$, *and then* $\det(\Lambda) \geq 13$.

In particular we have

$$\{\det(\mathcal{E}_2)\} \cap (0, 13) = \{5\} \cup \{8\} \cup \left[\frac{221}{25}, \frac{480}{49}\right] \cup [10, 12]\,.$$

Proof. We keep the notation $u = x_1 + x_2$, $v = x_1 x_2$. The first and last assertions result from Theorem 5.2, so that we may restrict ourselves to the case when $m = 2$, and we moreover know that we then have $8 \leq d \leq 12$.

(2) The lower bounds $f(-\frac{1}{2}) \geq \frac{1}{4}$ and $f(\frac{5}{2}) \geq \frac{1}{4}$ read

$$(a')\colon\ u + 2v \geq 0\,;\ (d')\colon\ 5u - 2v \leq 12\,;$$

together with (b), they imply $u = 2$ and $v = -1$, which proves (2).

(3) Using the transformation $x \mapsto m\mathbf{1} - x$ we may assume that $-\frac{1}{2} < x_1 < 0$ and $\frac{5}{2} < x_2 < 3$, which implies the four conditions

$$(a')\colon\ -u - 2v \leq 0\,;\ (b)\colon\ v \leq -1\,;\ (c')\colon\ -5u + 2v \leq -13\,;\ (d)\colon\ 3u - v \leq 8.$$

We now consider the six pairs of values of (u, v) obtained by replacing inequalities by equalities in two systems (a'), (b), (c'), (d). We must excludes $(a') + (b)$, for which $(u, v) = (2, -1)$ implies $x_2 = 1 + \sqrt{2} < \frac{5}{2}$, and $(c') + (d)$, for which $(u, v) = (3, 1)$ implies $x_2 = \frac{3+\sqrt{13}}{2} > 3$. The remaining four cases are listed below together with the corresponding value of $d = u^2 - 4v$, a function of (u, v) with non-vanishing partial

derivatives in the domain we consider, so that the extremal values are attained on one of the four pairs (u, v) below:
$(\frac{13}{6}, -\frac{13}{12})$, $d = \frac{325}{36} = 9.0277\ldots$; $(\frac{11}{5}, -1)$, $d = \frac{221}{25} = 8.84$;
$(\frac{16}{7}, -\frac{8}{7})$, $d = \frac{480}{49} = 9.7959\ldots$; $(\frac{7}{3}, -1)$, $d = \frac{85}{9} = 9.4444\ldots$.
These four values of (u, v) are the vertices of a closed convex set in the plane $\langle u, v\rangle$, all points of which produce an admissible determinant for $\mathcal{E}_2'$. As a consequence, the values of d fill the interval $[\frac{221}{25}, \frac{480}{49}]$. This proves (3), since this interval is included in $\mathcal{E}_1$.

(4) There remains to consider the case when $-1 < x_1 < -\frac{1}{2}$ and $\frac{5}{2} < x_2 < 3$. The conditions are now

(a): $-u - v \le 0$; (b'): $u + 2v \le -1$; (c'): $-5u + 2v \le -13$; (d): $3u - v \le 8$.

Using $(a) + (d)$ and $(b') + (c')$, we prove that $-2 \le v \le -\frac{3}{2}$. Since the domain we consider is invariant under $x \mapsto 2\mathbf{1} - x$, we may assume that $u \le 2$ (resp. $u \ge 2$) to obtain an upper (resp. a lower) bound for d. Hence we have $10 \le d \le 12$, and $2^2 - 4v$ runs through the whole interval $[10, 12]$ when v. runs through $[-2, -\frac{3}{2}]$. This proves (4) and completes the proof of the theorem. □

Various values of d which appear in Theorem 5.5 (5, 8, $\frac{221}{25}$, $\frac{4}{80}49$, 10, 12, 13) or in its proof ($\frac{85}{9}$) are indeed the determinants of admissible lattices for $A_{2,0}$. This we prove in the next subsection, in connection with the arithmetic of real quadratic orders.

Consideration of $\mathcal{E}_2$ beyond $m = 2$ does not throw much light on the Markoff spectrum. So we now sketch the study of $\mathcal{E}_3$, first in the range $d \in (0, 13)$, for which we must choose $m = 2$, then for $d \in [13, 20]$, where we must choose $m = 3$.

If $-\frac{1}{3} < x_1 < 0$, we have $f(-\frac{1}{3}) \ge \frac{1}{9}$ and $f(0) \le -1$, that is $u+3b \ge 0$ and $v \le -1$, hence $d = u^2 - 4v \ge 9v^2 - 4v \ge 13$, which contradicts Theorem 5.2. Similarly, using the transformation $x \mapsto 2\mathbf{1} - x$, we see that we must exclude the range $2 < x_2 < \frac{7}{3}$. We are thus left with four pairs of intervals, which reduce to three using the transformation above: $(-\frac{2}{3}, -\frac{1}{3}) \times (\frac{7}{3}, \frac{8}{3})$ and $(-1, -\frac{2}{3}) \times (\frac{8}{3}, 3)$, which are invariant, and $(-\frac{2}{3}, -\frac{1}{3}) \times (\frac{8}{3}, 3)$, which is not.

5.2. **Quadratic orders and the Markoff spectrum.**

Definition 5.6. The set S of determinants of minimal-admissible lattices for $A_{2,0}$ is called the *Markoff spectrum.*
[The usual definition is the square roots of these determinants d, which appear in diophantine approximations in the form $|\theta - \frac{p}{q}| \le \frac{1}{\sqrt{d}\,q^2}$.]

The results of Markoff stated in the next subsection will show that $S \cap [0,9]$ consists of a discrete subset of $(5,9)$ together with its unique limit point 9. Theorem 5.2 shows that $(12,13)$ is a gap in the Markoff spectrum, and indeed a maximal gap, since both 12 and 13 are determinants of algebraic lattices coming from quadratic orders. Besides the infinite series of gaps produced by the Markoff chain, other gaps exist, both in $(9,13)$ and in $(13,+\infty)$. We have proved above that $[\frac{480}{49},10]$ is a gap, and it can be shown that 13 is isolated in the Markoff spectrum (the maximal gap at the right of 13 is $(13, \frac{9\sqrt{3}+65}{22} = 13.418\ldots)$; see [C-F], Ch. 1, Lemma 9).

However a theorem of Marshall Hall asserts that every large enough real number belongs to S. It has been proved independently by Freiman and by Schecker[9] that the *Hall's ray* contains $[21,+\infty)$. Finally Freiman[10] proved that the Hall ray is

$$[\mu^2,+\infty) \;\text{ for }\; a = \frac{2221564096 + 283748\sqrt{462}}{491993569} \quad (\mu^2 = 20.389...)\,.$$

Proposition 5.7. *The Markoff spectrum is closed.*

Proof. Let (d_n) be a convergent sequence of elements of the Markoff spectrum and let d be its limit. Every n is of the form $d_n = \det(\Lambda_n)$ for some minimal admissible lattice Λ_n. By Mahler's compactness lemma, we can extract from (Λ_n) a sub-sequence converging to a lattice Λ. This lattice is minimal-admissible and has determinant d.
[Other viewpoint: the sets $\mathcal{E}_q$ are closed, and so is $\cap_q \mathcal{E}_q$.] $\square$

Let us now give some complements on orders in a quadratic field (real or not, this does not matter at this stage). Let K be a quadratic field, and let $om \in K$ such that $(1,\omega)$ is a $\mathbb{Z}$-basis for the ring of integers $\mathbb{Z}_K$ of K. In practice, if K has discriminant d_0, we take $\omega = \frac{1+\sqrt{d_0}}{2}$ if d_0 is odd, and $\omega = \sqrt{d_0}$ if d_0 is even. For every integer $f \geq 1$, $(1, f\omega)$ is a $\mathbb{Z}$-basis for an order $\mathfrak{O}_f \subset \mathbb{Z}_K$, and the assignment $f \mapsto \mathfrak{O}_f$ is one-to-one. The integer f is called the *conductor* of $\mathfrak{O}_f$, the discriminant of which is $d = d_0 f^2$.

A basic property of quadratic orders is that every proper fractional ideal $\mathfrak{a}$ of a quadratic order $\mathfrak{O}$ is *invertible*, that is, there exists a fractional ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = \mathfrak{O}$. Thus every module in K can be

[9] see H. Schecker, *Über die menge der Zahlen, die als Minima quadratischer Formen auftreten*, J. Number T. **9** (1977), 121–141

[10] In the unpublished Russian paper *Approximations and the geometry of numbers*, Moscow (1975), cited by Conway and Guy; in [C-F], p. 55, one must replace μ by $\mu + 4$.

viewed as an invertible fractional ideal of an order, a property which fails in higher degrees.
[In the general theory of orders in a separable algebra K/K_0 relatively to a Dedekind domain R with quotient field K_0, "invertible" amounts to "projective", and in a few important cases, "projective" implies "locally free" (these orders are called *clean*). This last property holds when K is commutative (by standard techniques of commutative algebra) and when the order is maximal (theorem of Auslander-Goldman); this also holds when for group rings $R[G]$ (theorem of Swan). Given an order $\mathfrak{O}$ of R in K and a maximal order $\mathfrak{M}$ containing $\mathfrak{O}$, the annihilator of $\mathfrak{M}/\mathfrak{O}$ is an ideal in $\mathfrak{O}$ *and* in $\mathfrak{M}$, 'the *conductor* $\mathfrak{f}$ *of* $\mathfrak{O}$ *in* $\mathfrak{M}$. Every integral ideal prime to $\mathfrak{f}$ is invertible, and every locally free ideal is equivalent to an ideal prime to $\mathfrak{f}$.]

For any order $\mathfrak{O}$ in any number field K of signature (r_1, r_2), the class group (group of invertible fractional ideals modulo Principal fractional ideals) is finite. This can be proved using Theorem 2.6:
Every class of $\mathfrak{O}$ contains an integral ideal of norm bounded from above by $\sqrt{\frac{d_\mathfrak{O}}{\kappa_{r_1,r_2}}}$.
More precisely, for any class $c \in \mathrm{Cl}_\mathfrak{O}$, denote by N_c the minimum of the norms of integral ideals in c (which depends only on the pair $\{c, c^{-1}\}$). The theorem above bounds $N = \max_c N_c$, but the collections of all N_c is useful to construct modules.

Given an invertible fractional ideal $\mathfrak{a}$ in $\mathfrak{O}$, we have

$$\min_{x \in \mathfrak{a} \smallsetminus \{0\}} |\mathrm{N}_{K/\mathbb{Q}}(x)| = \mathrm{N}(\mathfrak{a})$$

and $d_\mathfrak{a} = d_\mathfrak{O}\,\mathrm{N}(\mathfrak{a})^2$, and replacing $\mathfrak{a}$ by an equivalent ideal $\mathfrak{b} = \alpha\,\mathfrak{a}$ multiplies the norm form on $\mathfrak{a}$ by $\mathrm{N}_{K/\mathbb{Q}}(\alpha)$, so that once rescaled to minimum 1, the algebraic lattices deduced from $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent. In this scaling, taking $\mathfrak{a} \in c$ of norm N_c, we obtain a lattice of determinant

$$d_c = \frac{d_\mathfrak{O}}{N_c^2}\,,$$

and since all modules in a quadratic field arise from invertible ideals in orders, we obtain:

Proposition 5.8. *The discriminants of algebraic, minimal-admissible lattices for $A_{2,0}$ are the rational numbers $d_c = \frac{d_\mathfrak{O}}{N_c^2}$ where $\mathfrak{O}$ runs through the set of orders in a real quadratic field, c runs through the set of classes of $\mathfrak{O}$, and N_c is the smallest norm of an integral ideal in c.* $\square$

The discriminants of quadratic orders are easy to characterize: these are the integers d which are not a square and are congruent to 0 or 1 modulo 4. Among these discriminants, those of maximal orders are those which are square-free except for a divisor 4 when d is congruent to 8 or 12 modulo 4.

Since $\kappa_{2,0} = 5$, we can use the bound $\max N_c \le \sqrt{\frac{d}{5}}$ to evaluate the N_c. However, Theorem 5.5 shows that if we exclude the first two discriminants $5, 8$ of real quadratic orders, we can use the better bound

$$\max N_c \le \sqrt{\frac{d}{221/25}} = \sqrt{\frac{d}{8.84}}\,.$$

We now give some elements of the spectrum obtained using class groups. Given a prime p , we adopt the notation $(p) = \mathfrak{p}_p^2$ if p ramifies in $\mathfrak{O}$ and $(p) = \mathfrak{p}_p\mathfrak{p}_p'$ if p splits in $\mathfrak{O}$.
[*Warning*: if p divides the conductor, then there is in $\mathfrak{O}$ *one* maximal ideal $\mathfrak{p}_p$ above p, and this ideal is not invertible. For instance, in $\mathfrak{O} = \mathbb{Z}[\sqrt{5}]$, we have $\mathfrak{p}_2 = (2, 1+\sqrt{5})$, hence $\mathfrak{p}_2^2 = (2)\mathfrak{p}_2$ though $\mathfrak{p}_2 \ne (2)$. The norm of an integral ideal $\mathfrak{a}$ can be defined as the cardinality of the residue ring $\mathfrak{O}/\mathfrak{a}$, but the norm *need not be multiplicative* when primes dividing the conductor are involved.]

• There are 30 orders of discriminant $D < 100$, among which 25 have class number $h = 1$ and 5 have $h = 2$, namely those of discriminant 40, 60, 65, 85 (maximal) and 96 (with $f = 2$). The values of N_c for the unique non-trivial class are 2 for the first three and 3 for the last two, which produces lattices of determinant 10, 15, $\frac{65}{4} = 16.25$, $\frac{85}{9} = 9.44\dots$ and $\frac{32}{3} = 10.66\dots$; we met the determinants 10 and $\frac{85}{9}$ in Theorem 5.5.
• The first determinant for which $\max N_c \ge 4$ is $D = 145 = 5 \cdot 29$, the discriminant of a field K in which 2 and 3 split. The class group is cyclic of order 4, generated by $c = \mathrm{cl}(\mathfrak{p}_2)$. Since $\mathrm{N}(\frac{13+\sqrt{145}}{2}) = 6$, we have $\mathrm{cl}(\mathfrak{p}_3) = c^{\pm 1}$, so that norm 4 is needed to represent c^2. We construct this way a lattice of determinant $d = \frac{145}{16} = 9.0625$, fairly close to the Markoff limit 9.
• The first determinant for which $\max N_c \ge 5$ is $D = 221 = 13 \cdot 17$. We have $h = 2$, and since 2 and 3 are inert, we need consider an ideal above 5 to generate the class group. We construct this way a lattice of determinant $d = \frac{221}{25} = 8.84$. We showed in Theorem 5.5 that this is the third element of the Markoff spectrum (after 5 and 8).
• Let $K = \mathbb{Q}(\sqrt{30})$, of discriminant $d_K = 120$, and let $\mathfrak{O}$ be the order of discriminant $D = 480 = d_K \cdot 2^2$. We have $h_K = 2$ (we need consider ideals of norm $N \le 3$, and since $\mathrm{N}(6+\sqrt{30}) = 6$, the ramified ideals $\mathfrak{p}_2$ and $\mathfrak{p}_3$ are equivalent). For further use we note that the fundamental unit of K, namely $\varepsilon = 11 + 2\sqrt{30}$, belongs to $\mathfrak{O}$, and that $\mathfrak{p}_5$ is principal (we have $\mathrm{N}(5+\sqrt{30}) = -5$).

In $\mathfrak{O}$, $\mathfrak{p}_2$ disappears, so that we must discard norms 2, 4 and 6, and since $\varepsilon \in \mathfrak{O}$, $\mathfrak{p}_5$ is no longer principal. We have $\mathrm{Cl}_{\mathfrak{O}} = \{1, \mathrm{cl}(\mathfrak{p}_3), \mathrm{cl}(\mathfrak{p}_5), \mathrm{cl}(\mathfrak{p}_3\mathfrak{p}_5)\}$, so that norm 7 is needed to represent $\mathrm{cl}(\mathfrak{p}_3\,\mathfrak{p}_5)$. We construct this way the lattice of determinant $d = \frac{480}{49} = 9.7959\ldots$ which appears in Theorem 5.5. [Check: $\mathrm{N}(13+2\sqrt{30}) = 7^2$, $\mathrm{N}(15+2\sqrt{30}) = 3\cdot 5\cdot 7$.]

5.3. **The Markoff chain.** The description below of the admissible lattices for $A_{2,0}$ of low determinant relies on the second chapter of Cassels's book [Cas], where a chain of indefinite binary quadratic forms is constructed, a method which is easily translated into the language of lattices. This makes his book more suitable for our purpose than for instance that by Cusick and Flahive ([C-F]), in which only approximation theory is considered. Actually Cassels's motivation is mainly the theory of diophantine approximations, but he establishes a dictionary which relies indefinite, binary quadratic forms and approximations of real numbers by rational numbers.

The quadratic forms we shall consider do not represent zero, and will be written in the following two ways:

$$f(x,y) = ax^2 + bxy + cy^2 = a(x-\theta y)\,(x-\theta' y)$$

with real, irrational θ, θ', and discriminant $D = b^2 - 4ac > 0$; we have $|a(\theta'-\theta)| = \sqrt{D}$. The *minimum of* f (not necessarily attained) is $m = \inf_{(x,y)\neq(0,0)} |f(x,y)| \geq 0$.

In a crude form, Markoff's theorem reads as follows:

Theorem 5.9. (Markoff) *There exists a sequence* (Λ_n) *of algebraic lattices and an increasing sequence* (m_n) *of positive integers* (the Markoff numbers) *such that:*

(1) $\lim_{n\to\infty} m_n = +\infty$.
(2) $\det(\Lambda_n) = 9 - \frac{4}{m_n^2}$.
(3) *Every admissible lattice* Λ *for* $A_{n,0}$ *of determinant* $d < 9$ *is of the form* $\Lambda = \lambda\, u(\Lambda_n)$ *for some* $\lambda \geq 1$ *and some* $u \in \mathrm{Aut}(A_{n,0})$.

One has $d_1 = 5$, $d_2 = 8$, *and the lattices* Λ_1, Λ_2 *are the images of* $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ *and* $\mathbb{Z}[\sqrt{2}]$, *respectively.*
[Whether the sequence (m_n) is strictly increasing is not known.]

The translation in terms of approximations runs as follows. We say that two irrational numbers θ, θ' are *equivalent* if $\theta' = \frac{a\theta+b}{c\theta+c}$ for some $a,b,c,d \in \mathbb{Z}$ with $ad-bc = \pm 1$. Then for any irrational number θ, the inequality $|\theta - \frac{p}{q}| < \frac{1}{\sqrt{5}\,q^2}$ has infinitely many solutions, and the constant $\frac{1}{\sqrt{5}}$ is optimal if θ is equivalent to $\frac{1+\sqrt{5}}{2}$; otherwise, the inequality $|\theta - \frac{p}{q}| < \frac{1}{\sqrt{8}\,q^2}$ has infinitely many solutions, and the constant $\frac{1}{\sqrt{8}}$ is optimal if θ is equivalent to $\sqrt{2}$; otherwise, the inequality $|\theta - \frac{p}{q}| < \frac{1}{\sqrt{d_3}\,q^2}$ has infinitely many solutions, etc.

If m is not attained uniquely at $(1,0)$ and is non-zero, so that we may rescale f to minimum 1, we obtain inequalities $|\theta - \frac{x}{y}|\,|\theta' - \frac{x}{y}| \le \frac{1+\varepsilon}{|a|}\,\frac{1}{y^2}$. If $\frac{x}{y}$ can be made arbitrarily close to θ, we obtain inequalities of the form $|\theta - \frac{x}{y}| \le \frac{1+\varepsilon}{\sqrt{d}\,y^2}$. To obtain the sharper inequalities stated above, we shall have to restrict to forms for which θ, θ' are conjugate quadratic irrational numbers and having moreover a minimum f attained on both positive and negative sides.

The construction of the sequence m_n needs the consideration of the diophantine equation (*the Markoff equation*)

$$m_1^2 + m_2^2 + m_3^2 = 3m_1m_2m_3$$

in positive integers m_1, m_2, m_3. Any m_i is called a *Markoff number*. In practice we shall consider solutions (m, m_2, m_1) with $m \ge m_2 \ge m_1$ (and indeed $m > m_2 > m_1$ except for the two *singular solutions* $(1,1,1)$ and $(2,1,1)$) and attach to each solution (m, m_2, m_1) an integral, indefinite, binary quadratic form f_m of minimum m attained on both sides (that is, f represents both m and $-m$), Then $\frac{1}{m}\,f$ has minimum 1, and we can associate with f an admissible lattice for $A_{2,0}$ containing $\mathbf{1}$. [The notation should be f_{m,m_1,m_2}, but see Conjecture 5.10 below.]

Given a non-singular solution (m, m_2, m_1), we can view m as a root of the quadratic $X^2 - 3m_1m_2X + m_1^2 + m_2^2$. Then the other root

$$m' = 3m_1m_2 - m = \frac{m_1^2+m_2^2}{m}$$

is smaller than $\min(m_1, m_2)$, so that all solutions of the Markoff equation stem from a singular solution by applying successively the inverse procedure, which yields to solutions (m_2', m, m_1) and (m_1', m, m_2) such that $m_i' \ge m \ge m_j$. Note that given a Markoff number m, there may *a priori* exist several pairs (m_1, m_2) with $m \ge m_2 \ge m_1$. Extensive calculations did not produce any such example, which supports the conjecture below, which apparently appeared for the first time in a 1913 paper of Frobenius:

Conjecture 5.10. *For every Markoff number m, there exists only one solution (m, m_2, m_1) with $m \ge m_2 \ge m_1$ to the Markoff equation.*

We now define a form f_m attached to (m, m_1, m_2). Let $k \equiv \frac{m_1}{m_2}$ mod m chosen in $(0, m)$. Exchanging m_1 and $-m_2$ changes k into $m - k$. We chose $k \equiv \frac{m_1}{m_2}$ or $-\frac{m_2}{m_1}$ such that $1 \le k \le \frac{m}{2}$. Clearly m divides $k^2 + 1$, so that setting $k^2 + 1 = m\,\ell$, we define an integer ℓ. Finally let

$$f_m(x,y) = mx^2 + (3m - 2k)xy + (\ell - 3k)y^2\,.$$

The key result in the theory of the Markoff chain is the following theorem, for a proof of which we refer to Chapter 2 of [Cas].

Theorem 5.11. (Markoff) *The minimum of the form f_m is equal to m and is attained both by f and $-f$. The discriminant of f_m is*

$$D = 9m^2 - 4\,.$$

The sequence (m_n) in Theorem 5.9 is the sequence of Markoff numbers organized in increasing order. □

Remark 5.12. The gcd of the first two coefficients of f_m is $(2, m)$, and if m is even, then k and ℓ are odd. Hence for m odd (resp. even), the primitive form associated with f_m is $g_m = f_m$ (resp. $g_m = \frac{1}{2} f_m$). For even m, setting $m' = \frac{m}{2}$, g_m reads

$$g_m = m'x^2 + (3m' - k)xy + \tfrac{\ell-3k}{2}y^2\,.$$

Its discriminant is $D' = 9m'^2 - 1 = \frac{D'}{4}$. In both cases, the discriminant of the lattice Λ attached to f_m is $d = \frac{D}{m^2} = 9 - \frac{4}{m^2}$ ($d = 5, 8, \frac{221}{25} = 8.84, \dots$).

We now attach to a Markoff number m (more precisely, to a Markoff triple (m, m_1, m_2) with $m \ge m_2 \ge m_1$) the monic polynomial $h(X)$ canonically associated with the primitive form g_m, namely $m\, g_m(\frac{X}{m}, 1)$ or $m' g_m(\frac{X}{m'}, 1)$, that is

$$h(X) = X^2 + (3m - 2k)X + m(\ell - 3k) \text{ or } h(X) = X^2 + (3m' - k)X + \frac{m'(\ell - 3k)}{2}$$

according as m is odd or even, and we denote by $\mathfrak{O}_m$, or simply $\mathfrak{O}$ the order generated by a root of h in the splitting field K of h. To prove various properties of the discriminant $d_{\mathfrak{O}}$ of $\mathfrak{O}$, we need some more results on the Markoff numbers, including a congruence recently proved by Zhang[11].

Lemma 5.13. *Let (m, m_1, m_2) be a Markoff triple with $m \ge m_2 \ge m_1$.*

1. *m, m_1, m_2 are pairwise coprime.*
2. *m and $m_1 \pm m_2$ are coprime except for a common divisor 2 when m is even.*
3. (Frobenius) *The odd prime divisors of m, $3m - 2$ and $3m + 2$ are congruent to 1 modulo 4.*
4. (Zhang) *m is congruent to 1 modulo 4 or to 2 modulo 32.*

Proof. (1) If (m, m_1, m_2) is not singular, it has a neighbour (m_2, m_1, m') with $m' < m_1$. By induction we reduce ourselves to the obvious case of a singular triple.

(2) The Markoff equation may be written in the form $m^2 + (m_2 \pm m_1)^2 = m_1 m_2 (3m \pm 2)$, which shows that the gcd of m and $(m_2 \pm m_1)$, since it is coprime with $m_1 m_2$, must divide $3m \pm 2$, hence 2.

[11] Ying Zhang, *Congruence and uniqueness of certain Markoff numbers*, Acta Arith. **128** (2007), 295–301; arXiv:math/0612620v2 [math.NT] 29 Dec 2006

(3) The equation above shows that $3m \pm 2$ or $\frac{3m\pm 2}{4}$ divides the sum of two coprime integers, hence both $3m+2$ and $3m-2$ have no divisor $p \equiv 3 \mod 4$. The same proof works for m, writing the Markoff equation as $m(3m_1m_2 - m) = m_1^2 + m_2^2$.

(4) Only the second congruence needs a proof. Since m is even, m_1 and m_2 are odd, so that $m_1^2 + m_2^2 \equiv 2 \mod 8$, hence $m \equiv 2 \mod 4$ because m divides this sum, and since $m_1 \equiv m_2 \equiv 1 \mod 4$, the Markoff equation modulo 8 reads $3m \equiv m^2 + 2 \equiv 6$, i.e. $m \equiv 2 \mod 8$. Then $\frac{3m-2}{4}$, which is an odd divisor of $m^2 + (m_2 - m_1)^2$ by (2), is congruent to 1 modulo 4. This shows first that $m \equiv 2 \mod 16$ and then that $3m + 2 \equiv 8 \mod 16$, i.e. that $\frac{3m+2}{8}$ is odd. Writing finally the Markoff equation in the form $\left(\frac{m_1+m_2}{2}\right)^2 + \left(\frac{m}{2}\right)^2 = 2m_1m_2\left(\frac{3m+2}{8}\right)$, we see that we have $\frac{3m+2}{8} \equiv 1 \mod 4$, i.e. $m \equiv 2 \mod 32$. □

Proposition 5.14. *The discriminant $d_{\mathfrak{O}}$ of an order $\mathfrak{O}$ attached to a Markoff triple is a product of primes $p \equiv 1 \mod 4$ (or $p = 8$), and is congruent to 1 modulo 4 or to 8 modulo 16. Its conductor is odd.*

Proof. The assertions on odd numbers are consequences of Lemma 5.13, (3). If d_O is even, it is of the form $D' = m'^2 - 1$ with $m' = \frac{m}{2}$. By Lemma 5.13, (4). one has $m' \equiv 1 \mod 16$, hence $D' \equiv 8 \mod 16$. Write $d_{\mathfrak{O}} = d_0 f^2$ where d_0 is a fundamental discriminant. Then d_0 is even, hence must be congruent to 8 or 12 modulo 16. This shows that the first congruence holds, which implies $f \equiv 1 \mod 2$. □

Proposition 5.15. *The fundamental unit of the Markoff orders, except those of the first two, have norm +1.*

Proof. The fundamental units of the first two orders, namely $\frac{1+\sqrt{5}}{2}$ and $1+\sqrt{2}$ are of norm -1. Let now $\mathfrak{O}$ be a Markoff order of discriminant $\Delta > 8$.

Recall the following well known and easy to prove result: consider an order in a real quadratic field $K = \mathbb{Q}(\sqrt{\mu})$, $\mu > 1$. with fundamental unit $\varepsilon = u + v\sqrt{\mu}$, $u, v > 0$, $u, v \in \mathbb{Z}$ or $\frac{1}{2} + \mathbb{Z}$. For $k > 1$, let $\varepsilon^k = u_k + v_k\sqrt{\mu}$. Then we have $v_k > v$ except if $\mu = 5$ and $k = 2$, where $\left(\frac{1+\sqrt{5}}{2}\right)^2 = \left(\frac{3+\sqrt{5}}{2}\right)$.

If $d_{\mathfrak{O}}$ is odd, then $\eta = \frac{3m+\sqrt{9m^2-4}}{2}$ is a unit of $\mathfrak{O}$, and since $d_{\mathfrak{O}} = 9m^2 - 4$, the result above shows that η is the fundamental unit of the order except if $9m^2 - 4 = 5$.

If $d_{\mathfrak{O}}$ is even, we consider the unit $\eta = 3m' + 2\sqrt{(m'^2 - 1)}/4$. This time this is of the form $u + v\sqrt{\mu}$ with $v = 2$. One easily checks that η is a k-th power for some $k \geq 2$ if and only if $\mu = 2$ and $k = 2$, where $(1+\sqrt{2})^2 = 3+2\sqrt{2}$, or $k = 3$ and $\mu = 5$, where $\left(\frac{1+\sqrt{5}}{2}\right)^3 = 2+\sqrt{5}$. □

Remark 5.16. The conductor of $\mathfrak{O}$ may be non-trivial. The first occurrence is produced by $m=34$, thus $m'=12$ and $d_{\mathfrak{O}}=(8\cdot13)\cdot5^2$. In this case, the fundamental unit of the order, namely $\eta=51+10\sqrt{26}$, is the square of the fundamental unit $\varepsilon=5+\sqrt{26}$ of the maximal order, of norm -1.

6. Dimension 3

In a first subsection, we determine following Davenport the lattice constant of $A_{3,0}$, then describe the extension due to Swinnerton-Dyer of Davenport's results in a second subsection. Finally we state some conjectures on totally real Minkowski's domain of dimension $n\geq 3$.

6.1. **The lattice constant of $\mathbf{A_{3,0}}$ (after Davenport).** In this subsection, following Davenport's [Dav1], we consider a 2-dimensional lattice L generated by $\mathbf{1}=(1,1,1)$ and a second vector $x=(x_1,x_2,x_3)$, and set $S=S(x)$ (Definition 3.1).

Lemma 6.1. *Assume that $L\cap A_{3,0}=\{0\}$. Then either L or its image under an orthogonal automorphism of $A_{3,0}$ has a basis $(\mathbf{1},x)$ with $-1<x_1<0<x_2<1<2<x_3<3$, or $S>15.84$.*

Proof. Using permutations of the coordinates and base changes $x\mapsto \pm x+k$, $k\in\mathbb{Z}$, we may assume that $x_1<x_2<x_3$ and $0<x_2<1$. If x_1 or x_3 belongs to $(0,1)$, we have $S\geq\frac{49}{2}>24$ by Proposition 4.16, (2). Hence we may assume that $x_1<0$ and $x_3>1$, and by Proposition 4.16, (3), we have $x_3>2$ or $x_1<-1$. Changing x into $1-x$, we may assume that $x_3>2$.

If $x_1<-2$, or $x_1<-1$ and $x_3>3$, or $x_3>4$, we have $S>\frac{3}{2}\,4^2=24$ by Proposition 4.13. We are thus left with three possible cases:
(a) $-1<x_1<0$ and $2<x_3<3$;
(b) $-1<x_1<0$ and $3<x_3<4$;
(c) $-2<x_1<-1$ and $2<x_3<3$,
and we bound S from below in the last two cases, using Proposition 4.14.

In case (b), we have $x_1<-\frac{1}{4}$, $x_3>3+\frac{1}{12}$, hence $S>\frac{3}{2}\left(\frac{10}{3}\right)^2=\frac{50}{3}=16.666\ldots$.

In case (c), we have $x_1<-1-\frac{1}{8}$, $x_3>2+\frac{1}{8}$, hence $S>\frac{3}{2}\left(\frac{13}{4}\right)^2=\frac{507}{32}=15.84375$.
[Using four times Proposition 4.14, we obtain $S>16.13$.] □

Remark 6.2. The smallest two values of S for integers of cubic fields (14 and 18) occur using an x of the form (a) above. Polynomials having roots in the intervals described above are obtained by translation from those given in Example 3.9: there is in each case a unique choice, namely X^3-2X^2-X+1 and X^3-3X^2+1. The next value ($S=20$) needs $\lceil x_3\rceil-\lfloor x_1\rfloor>4$.

Proposition 6.3. *Under the hypotheses of Lemma 6.1, and assuming that $x_1 < x_2 < x_3$, we have $S \geq 14$, and equality holds if and only if (x_1, x_2, x_3) is the image under a transformation $x \mapsto \pm\mathbf{1} + kx$ $(k \in \mathbb{Z})$ of the roots of the polynomial $f = X^3 - X^2 - 2X + 1$.*
[The roots of f are $\theta_1 = -2\cos\frac{2\pi}{7} < \theta_2 = -2\cos\frac{4\pi}{7} < \theta_3 = -2\cos\frac{6\pi}{7}$.]

Proof. After having performed the translation $x \mapsto x - \mathbf{1}$, Lemma 6.1 shows that we may assume that we have

$$-2 < x_1 < -1 < x_2 < 0 < 1 < x_3 < 2\,.$$

Set $f(X) = (X - x_1)(X - x_2)(X - x_3) = X^3 - t_1X^2 + t_2X - t_3$. Calculating f at $-1, 0, 1$, we obtain the inequalities

(1) $1 + t_1 + t_2 + t_3 \leq -1$; (2) $-t_3 \leq -1$; (3) $1 - t_1 + t_2 - t_3 \leq -1$.

The combinations (1)+(3) and (1)+(2) then read $t_2 \leq -2$ and $-t_1 \geq t_2 + 3$, that we may write $t_2 = -2 - h$ and $t_1 = -1 + h - h'$ with $h, h' \geq 0$. This implies

$$S = 14 + 2(h + 2h' + (h - h')^2) \geq 14\,,$$

which shows that $S \geq 14$, and that equality holds if and only if $h = h' = 0$, i.e. $t_2 = -2, t_1 = 1$. Then (2) and (3) show that $t_3 = 1$ (the inequalities above now read $\max(1, 1 - 2h + h') \leq t_3 \leq 1 + h'$), and $f(-X)$ is the polynomial of the proposition. □

Theorem 6.4. *The lattice constant of $A_{3,0}$ is $\kappa_{3,0} = 49$, attained uniquely (among lattices on which $x_1x_2x_3$ attains the value 1) on lattices equivalent to the image of $\mathbb{Z}[\zeta_7 + \zeta_7^{-1}]$.*
[The restriction is not necessary, but a proof of this needs an isolation result.]

Proof. Let Λ be an admissible lattice for $A_{3,0}$ containing $\mathbf{1}$, and let p be the orthogonal projection to $F = \mathbb{R}\,\mathbf{1}^\perp$. Since $N(\mathbf{1}) = 3$, we have $\det(p(\Lambda)) = \frac{1}{3}\det(\Lambda)$. By the results of Subsection 3.1, the projection of $x = (x_1, x_2, x_3) \in E$ has norm $\frac{S(x)}{3}$. By Proposition 6.3, $p(\Lambda)$ is admissible for the sphere of square radius $R^2 = \frac{14}{3}$. Since the lattice constant κ_2 of the unit disc is equal to $\frac{3}{4}$, we obtain

$$\det(\Lambda) \geq 3 \cdot \frac{3}{4} \cdot \left(\frac{S}{3}\right)^2 = \left(\frac{S}{2}\right)^2 \geq 49\,.$$

There remains to characterize the admissible lattices Λ of determinant 49 which contain $\mathbf{1}$. Since equality must hold everywhere in the inequalities above, $p(\Lambda)$ must be critical for the disc of square radius $\frac{14}{3}$. Hence there are in Λ three vectors v_1, v_2, v_3 the components x_1, x_2, x_3 of which are permutations of the roots $\theta_1, \theta_2, \theta_3$ of f, and moreover there exists relation $\sum \pm p(v_i) = 0$ between their projections which lifts to a relation $\sum \pm v_i = \lambda \mathbf{1}$ for some $\lambda \in \mathbb{Z}$. There cannot be a transposition among the permutations, for if, say, $v_1 = (\theta_1, \theta_2, \theta_3)$ and $v_2 = (\theta_1, \theta_3, \theta_2)$, no combination $\sum \pm v_i$ belongs to $\mathbb{R}\mathbf{1}$. Hence the three permutations are the three possible circular permutations, the v_i add to -1, and v_1, v_2, v_3 constitute a basis for the lattice which represents $\mathbb{Z}_K$. □

6.2. **The next minima of $\mathbf{A_{3,0}}$ (after Swinnerton-Dyer).** This subsection relies on Swinnerton-Dyer's paper [SwD]; see also [SwD2].

6.3. **Conjectures on totally real Minkowski's domains.** The behaviour of the first eighteen minima for $A_{3,0}$ found by Swinnerton-Dyer suggests the following conjecture:

Conjecture 6.5. *Let $n \geq 3$ odd. There exists a sequence $M_1, \dots, M_n$ of modules in totally real number fields of degree n such that the sequence Λ_n of lattices in $\mathbb{R}^n$ associated with m_n has the following properties:*

(1) *Every admissible lattice for $A_{n,0}$ is of the form $\lambda\, u(\Lambda_n)$ for some $n \geq 1$, $\lambda \geq 1$, and $u \in \mathrm{Aut}(A_{n,0})$.*
(2) *The determinants of the Λ_n constitute an increasing sequence which tends to infinity.*

The conjecture is false for $n = 2$, and similarly, its analogue for relative quadratic extensions might well be false: we cannot exclude the existence of some "Markoff-like chain". This is the reason for the hypothesis "n odd".

Note that the comments made by Swinnerton-Dyer in [SwD] indicate that he believed the conjecture above is true in dimension $n = 3$, though he does not state it explicitly. Note also that part (1) implies part (2) thanks to Cassels and Swinnerton-Dyer's paper [Cas-SwD].

7. Dimension 4

Difficulties related to the possible existence of several components of an $x \notin \mathbb{R}\mathbf{1}$ belonging to a same interval $(m, m+1)$ occur from dimension 4 onwards. As was noted by Godwin in [God], we can obtain lower bounds for S by assuming that such components are equal. A precise statement is given in the next proposition, the easy proof of which is left to the reader.

We thus consider $x = (x_1, \dots, x_n)$ and assume that p components x_i lie in some interval $(m, m+1)$, and more precisely in some interval $[\alpha, \beta] \subset (m, m+1)$ (which can be constructed using Proposition 4.14 under the hypothesis that x lies outside $A_{n,0}$), and the remaining

$q = n - p$ components are off this interval. Let $a = \frac{1}{q} \sum_{x_i \notin (m,m+1)} x_i$ be the average of the x_i off $(m, m+1)$.

Proposition 7.1. *Under the hypotheses above, $S = \sum_{i<j} (x_j - x_i)^2$, viewed as a function of the x_i belonging to $(m, m+1)$ attains its minimum when these x_i are equal, to α, to a or to β according to whether $a < \alpha$, $\alpha \leq a \leq \beta$ or $a > \beta$.* □

References

[Cas] J.W.S. Cassels, *An Introduction to Diophantine Approximation*, Cambridge University Press, Tract **45**, Cambridge, U.K. (1965; first edition: 1957).

[Cas2] J.W.S. Cassels, *An Introduction to the Geometry of Numbers*, Springer-Verlag, Grundlehren **99**, Heidelberg (1959; second edition: 1997).

[Cas-SwD] J.W.S. Cassels, H.P.F. Swinnerton-Dyer, *On the product of three homogeneous linear forms and the indefinite ternary quadratic forms*, Philos. Trans. Roy. Soc. London **248** (1955), 73-96.

[C-F] T.W. Cusick, M.E. Flahive, *The Markoff and Lagrange spectra*, A.M.S. Math. Surveys **10**, Providence, Rhode Island (1989).

[Dav] H. Davenport, *collected works*. Academic Press, London (1977).

[Dav1] H. Davenport, *Note on the product of three homogeneous linear forms*, J. London Math. Soc. **15** (1941), 98–101, =[Dav] I, 62–65.

[D-F] B.N. Delone, D.K. Fadeev, *The Theory of Irrationalities of the Third Degree*, Translations Amer. Math. Soc. **10**, Providence, R.I (1964; Russian original: Moscow, 1940).

[God] H.J. Godwin, *Note on the product of five homogeneous linear forms*, J. London Math. Soc. **25** (1950), 331–339.

[Hun] J. Hunter, *The minimum discriminant of quintic fields*, Proc. Glasgow Math. Ass. **3** (1957), 57–67.

[Mar] J. Martinet, *Perfect Lattices in Euclidean Spaces*, Springer-Verlag, Grundlehren **327**, Heidelberg (2003). Especially Chapter 2.]

[Mar1] J. Martinet, *Méthodes géométriques dans la recherche des petits discriminants*, Séminaire de Théorie des Nombres de Paris 1983–84, Birkhäuser, Basel (1985), 147–179.

[Min1] H. Minkowski (Hilbert ed.), *Gesammelte Abhandlungen*, Chelsea, New York (1967; first edition: Leipzig, 1911).

[Min2] H. Minkowski, *Geometrie der Zahlen*, Johnson reprint Co., New York (1968; first two editions: Teubner, Leipzig, 1896 & 1910, edited by Hilbert and Speiser).

[MBH] H. Minkowski (L. Rüdenberg, H. Zassenhaus, ed.), *Briefe an David Hilbert*, Springer-Verlag (1973).

[Mul] .P. Mulholand, *On the product of n complex homogeneous linear forms*, J. London Math. Soc. **35** (1960), 241-–250.

[Noo] P. Noordzij, *Über das Produkt von vier, reellen, homogenen, linear Formen*, Monatshefte Math. **71** (1967), 436–445.

[Rog] C.A. Rogers, *The product of n real homogeneous linear forms*, Acta Math. **82** (1950), 185-–208.

[SwD] H.P.F. Swinnerton-Dyer, *On the product of three homogeneous linear forms*, Acta Arith. **18** (1971), 371–385.

[SwD2] H.P.F. Swinnerton-Dyer, The Products of Three and of Four Linear Forms, in "Computers in number theory", edited by A.O.L. Atkin and B.J. Birch, Academic Press, Oxford (1971), 231–236.