ON THE MINKOWSKI CONSTANTS FOR CLASS GROUPS

JACQUES MARTINET

Abstract. We discuss some questions in the geometry of numbers 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).

Introduction

We consider a number field K, of signature (r_1, r_2) and degree $n = r_1 + 2r_2$. We denote by d_K its discriminant, by Cl_K its class group and by h_K the order of Cl_K.

I just want here to briefly discuss the theorem of Minkowski, which asserts the existence of a reasonably small constant $k = k_{r_1,r_2}$, such that

Every class of K contains an integral ideal $\mathfrak{a}$ of norm
$$N := \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a}) \leq k\,\sqrt{|d_K|}\,. \qquad (*)$$

This result is announced first in a letter to Hilbert (December 22nd, 1890; [MBH]), then in a letter to Hermite (January 15th, 1891; [Min1], pp 261–264), that Hermite partially published as a note in *Comptes Read's Acad. Sc. Paris.* The important point for Minkowski is that he can produce for any $n > 1$ a constant $k < 1$, so that the trivial lower bound $N \geq 1$ yields a lower bound $d_K > 1$, giving this way a positive answer to the conjecture of Kronecker, according to which the discriminant of a number field of degree $n \geq 2$ is not equal to ± 1. His proof relies on techniques from geometry of of numbers, a new part of mathematics he had just invented (and christened as *Geometrie der Zahlen*); see Section 2.

1. More on Number Fields

To analyze the theorem of Minkowski quoted above, we must consider general full submodules of K which are finitely generated over $\mathbb{Z}$ (*modules* for short).

Key words and phrases. Euclidean lattices, Minkowski domains
First version: April 28th, 2011; corrected (version 2): May 9th, 2011.

A set of n elements $e_1, \dots, e_n \in K$ has a *discriminant*, namely

$$d_K(e_1, \dots, e_n) = \det(\mathrm{Tr}_{K/\mathbb{Q}}(e_i e_j))\,,$$

which is zero if the e_i are dependent and has otherwise the sign of $(-1)^{r_2}$. A *module M in K* has a discriminant $d_K(M)$, the discriminant of any of its bases. Note that $d_K(M) \bmod \mathbb{Q}^{\times 2}$ *uniquely depends on K*.

An *order $\mathfrak{O}$ in K* is a module which is closed under multiplication and contains the unit element of K. The elements of an order are integral over $\mathbb{Z}$, so that any order is contained in the unique maximal order (with respect to inclusion), namely the *ring of integers $\mathbb{Z}_K$ of K*. What we have denoted by d_K is $d_K(\mathbb{Z}_K)$, and for an order $\mathfrak{O}$ of index f in $\mathbb{Z}_K$, we have $d_K(\mathfrak{O}) = d_K\, f^2$. (This index is sometimes called the *conductor of $\mathfrak{O}$*.)

The usual notion of a fractional ideal extends to orders. We say that a fractional ideal $\mathfrak{a}$ of $\mathfrak{O}$ is *invertible* if there exists $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = \mathfrak{O}$. The invertible ideals of $\mathfrak{O}$ constitute an Abelian group $\mathcal{I}(\mathfrak{O})$ ($\mathcal{I}_K$ if $\mathfrak{O} = \mathbb{Z}_K$), with unit $\mathfrak{O}$. They are locally free $\mathfrak{O}$-modules, so that we can define the norm $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a})$ of an invertible ideal, which is multiplicative on $\mathcal{I}(\mathfrak{O})$. If $\mathfrak{a}$ is integral (i.e., contained in $\mathfrak{O}$), we have $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a}) = |\mathfrak{O}/\mathfrak{a}|$. Using this remark we can define the norm of any fractional ideal, but **warning**: the formula $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a})\,\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{b}) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a}\mathfrak{b})$ may fail for non-invertible $\mathfrak{a}, \mathfrak{b}$. Note that every ideal prime to the conductor is invertible, and that every invertible ideal is equivalent to an ideal prime to the conductor.

A module M has an *associated order* $\mathfrak{O}(M) = \{\lambda \in K \mid \lambda\mathfrak{O} \subset \mathfrak{O}\}$, and M is a fractional ideal of $\mathfrak{O}(M)$. We say that a fractional ideal $\mathfrak{a}$ of an order $\mathfrak{O}$ is *proper* if $\mathfrak{O}(\mathfrak{a}) = \mathfrak{O}$. Hence any module M can be viewed as a proper fractional ideal over some order. An invertible ideal is proper, but a proper ideal need not be invertible. However, this is true for quadratic extensions [1].

The inequality $(*)$ can be deduced from the following result:

Every module M contains a non-zero element x such that

$$|\mathrm{N}_{K/\mathbb{Q}}(x)| \le k\sqrt{|d_K(M)|}\,, \qquad (**)$$

a proof of which is sketched in Section 2 below.

Assertion $(*)$, in the slightly more general form $(*')$ below which applies to all orders, now reads:

Every class of invertible ideals in an order $\mathfrak{O}$
contains an integral ideal $\mathfrak{a}$ of norm

[1] this is proved in Shimura's book *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press (1971); see in particular Proposition 4.11.

$$N := \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a}) \le k\,\sqrt{|d_K(\mathfrak{O})|}\,. \qquad (*')$$

Proof. The proof relies on the "inverse class trick". Let c be a class in $\mathrm{Cl}_{\mathfrak{O}}$ and let $\mathfrak{a}_0$ be a fractional ideal in c^{-1}. For any integral ideal $\mathfrak{a} \in c$, $\mathfrak{a}_0\mathfrak{a}$ is a principal ideal (x) divisible by $\mathfrak{a}_0$, thus $x \in \mathfrak{a}_0$. The discriminant of $\mathfrak{a}_0$ is $d_0 = d_{\mathfrak{O}}\ \mathrm{N}_{K|Q}(\mathfrak{a}_0)^2$. By $(**)$, there exists $x \in \mathfrak{a}_0$ such that $|\mathrm{N}_{K/\mathbb{Q}}(x)| \le k\sqrt{d_0}$. For such an x, $\mathfrak{a} = x\mathfrak{a}_0^{-1}$ is an integral ideal of norm $|\mathrm{N}_{K/\mathbb{Q}}(x)|\,\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a}_0)^{-1}$ which belongs to c.
This completes the proof of $(*')$. □

To find a convenient constant $k = k_{r_1,r_2}$ we use techniques from geometry of numbers, as developed by Minkowski. The result for formula $(**)$ will appear in the form

$$|\mathrm{N}_{K/\mathbb{Q}}(x)| \le \sqrt{\frac{d_K(M)}{\kappa_{r_1,r_2}}}\,, \qquad (**')$$

and the problem is now to find good lower bounds for $\kappa = \kappa_{r_1,r_2}$. Alternatively one could use analytic methods, following Zimmert's 1981 paper [Zi].

2. Geometry of Numbers

2.1. **Basic Definitions.** Geometry of numbers deals with lattices in Euclidean spaces. We denote by E a *Euclidean space of dimension* $n > 0$, equipped with its (positive, definite) *scalar product* (or *dot product*) $x \cdot y$. The choice of an orthonormal basis for E identifies E with $\mathbb{R}^n$, equipped with the dot product $x_1y_1 + \cdots + x_ny_n$.

A *lattice* Λ *in* E is a discrete subgroup of E of maximal rank; this amounts to saying that Λ has a $\mathbb{Z}$-basis $\mathcal{B} = (e_1, \ldots, e_n)$ which is also a basis for E over $\mathbb{R}$.
[**Warning.** In this section, we depart from the traditional notation. On the one hand, we define lattice constants of subsets of E replacing Minkowski's notion of the discriminant of a lattice, as used in the Book [Cas2], by that of the determinant, as used in the recent books [C-S] and [Mar]; on the other hand, we define Minkowski's domain in a non-traditional way, so as to get rid of the factors 2^{r_2} in most of the formulae and obtain natural inclusions between domains having the same dimension.]

Let Λ be a lattice and let $\mathcal{B}$ be a basis for Λ. Denote by M the matrix of $\mathcal{B}$ with respect to an orthonormal basis $\mathcal{B}_o$ for E. Then the determinant of M is well-defined up to sign. Minkowski defined the *discriminant* $\Delta(\Lambda)$ *of* Λ as the absolute value of the determinant of M: $\Delta(\Lambda) = |\det_{\mathcal{B}_o}(\mathcal{B})|$; this is the volume of a fundamental domain of Λ.

Define the *Gram matrix of* $\mathcal{B}$ by $\mathrm{Gram}(\mathcal{B}) = (e_i \cdot e_j)$ and the *determinant of* Λ by $\det(\Lambda) = \det(\mathrm{Gram}(\mathcal{B}))$. We have $\mathrm{Gram}(\mathcal{B}) = {}^tMM$, hence $\det(\Lambda) = \Delta(\Lambda)^2$.

We say that Λ is *admissible for a subset* A *of* E if $\Lambda \cap A = \{0\}$ (or $\emptyset$) and we define the lattice constant of A by

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

($+\infty$ if there are no admissible lattices for A). We say that a lattice Λ is *critical for* A if $\det(\Lambda) = \kappa(A)$. Note that $A \subset B$ implies $\kappa(B) \geq \kappa(A)$.

This very general definition will be applied here only for *open star bodies* (*with respect to the origin*), that is open subsets of E which contain the segment $[0, x]$ for every $x \in A$. Note that if Λ is admissible for A, then so is $\lambda\Lambda$ for any $\lambda \geq 1$. We say that Λ is *minimal-admissible for* A if Λ is admissible for A but $\lambda\Lambda$ is not if $\lambda < 1$. These sets will all be associated with a *distance-function*, that is a continuous map $F : E \to \mathbb{R}_{\geq 0}$ which satisfies a homogeneity condition $F(\lambda x) = |\lambda|^\delta F(x)$ for some $\delta > 0$, setting $A_F = \{x \in E \mid F(x) < 1\}$. Main example:

$$F_{r_1,r_2} = \frac{1}{2^{r_2}} \prod_{1 \leq i \leq r_1} |x_i| \prod_{1 \leq j \leq r_2} (y_i^2 + z_i^2)\,,$$

defined on $E = \mathbb{R}^n$ for any representation $n = r_1 + 2r_2$, writing for short $y_j = x_{r_1+j}$ and $z_j = x_{r_1+r_2+j}$. We shall also consider maps $x \mapsto |q(x)|$ where q is a non-degenerate quadratic form.

Remark 2.1. If $F(x) = 0$ for some $x \neq 0$, then A_F contains the line $\mathbb{R}x$, hence is not bounded. If $F(x)$ is non-zero for $x \neq 0$, then A_F is bounded. In this case, any minimal-admissible Λ for A_F has a point on the boundary of A_F, as one easily sees using the compactness of $\overline{A}_F$. We can prove more: if $\det(\Lambda)$ is locally minimal among the admissible lattices for A_F, then the boundary of A_F contains n-independent points, for if these points span a strict subspace F of E, then for some $\lambda < 1$, the image of Λ by the linear map u_λ which is the identity on F and $x \mapsto \lambda x$ on $F^\perp$ will still be admissible and have a smaller determinant.

The following easy proposition establishes a relation between lattice constants and values taken on lattices by distance-functions:

Proposition 2.2. *Given a distance-function* F *and a lattice* Λ*, set*

$$F(\Lambda) = \inf_{x \in \Lambda \smallsetminus \{0\}} F(x)\,.$$

This function on the set of lattices is related to the lattice constant of A_F by the formula

$$\sup_{\Lambda} \frac{F(\Lambda)^{2n/\delta}}{\det(\Lambda)} = \kappa(A_F)^{-1}\,. \quad \square$$

[Note that the ratio in the formula above is homogeneous of degree zero.]

2.2. **Connection with Number Fields.** We now attach a Euclidean space of dimension n to any number field K of degree n and signature (r_1, r_2) and a lattice to every module $M \subset K$.

Let $\widehat{K}$ be the completion of the $\mathbb{Q}$-algebra K for the usual absolute value on $\mathbb{Q}$. This is an étale $\mathbb{R}$-algebra, canonically isomorphic to $\mathbb{R} \otimes_{\mathbb{Q}} K$, thus non-canonically isomorphic to $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. (The identification relies on the choice of an element of the automorphism group of the $\mathbb{R}$-algebra $\widehat{K}$, of order $r_1!\, r_2!\, 2^{r_2}$.) However, the canonical involution of $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ (the identity on real factors and the complex conjugacy on complex factors) defines a canonical involution $x \mapsto \overline{x}$ on $\widehat{K}$, for which the bilinear form $\mathrm{Tr}(x\overline{y})$ defines a Euclidean structure on $\widehat{K}$. The submodules of K are discrete and closed, hence are invariant under the completion and are consequently lattices in $\widehat{K}$.

On complex factors, one has $\mathrm{Tr}(x\overline{x}) = 2|x|^2$, which produces the factor 2^{2r_2} in the calculations of determinants. To get rid of it in Proposition 2.2, we divide the norm on $\widehat{K}$ by 2^{r_2}, whence the definition above of F_{r_1,r_2}, and identify $\mathbb{C}$ with $\mathbb{R}^2$ sending $y + z\,i$ to $(y+z, y-z)$. Then the image of 1_K is the *all ones vector* $\mathbf{1} = (1, 1, \dots, 1)$, and the condition $|N_{K/\mathbb{Q}}(x)| \geq 1$ on $\mathbb{Z}_k \smallsetminus \{0\}$ now becomes $F_{r_1,r_2}(x) \geq 2^{r_2}$.

Definition 2.3. The *Minkowski domain for signature* (r_1, r_2) is the open star body

$$\begin{aligned} A_{r_1,r_2} &= \{x \in \mathbb{R}^n \mid F_{r_1,r_2}(x) < 1\} \\ &= \{x \in \mathbb{R}^n \mid |x_1 \cdots x_{r_1}| \cdot (y_1^2 + z_1^2) \cdots (y_{r_2}^2 + z_{r_2}^2) < 2^{r_2}\,; \end{aligned}$$

we denote by κ_{r_1,r_2} its *lattice constant.*

The proposition below is one of the motivations for inserting a factor $\frac{1}{2^{r_2}}$ in the definition of F_{r_1,r_2}.

Proposition 2.4. *If* $r_2 \geq 1$ *we have the inclusion* $A_{r_1,r_2} \subset A_{r_1+2,r_2-1}$. *In particular we have* $\kappa_{r_1,r_2} \leq \kappa_{r_1+2,r_2-1}$.

Proof. Just apply the inequality $|x_1 x_2| \leq \frac{x_1^2+x_2^2}{2}$. $\square$

2.3. **Modules in Number Fields.**

Lemma 2.5. *The values taken by the norm on a module belong to a subset of a discrete subgroup $\lambda\mathbb{Z}$ of $\mathbb{R}$. In particular, $|N_{K/\mathbb{Q}}|$ attains a minimum on M.*

Proof. Let M be a module contained in a number field K and let $(e_1,\dots,e_n)$ be a basis for M. There exists $a\in\mathbb{Z}$ such that ae_i is integral over $\mathbb{Z}$ for every i. Then ax is integral for every $x\in M$, which implies that $N_{K/\mathbb{Q}}(ax)\in\mathbb{Z}$, hence that $N_{K/\mathbb{Q}}(x)\in\frac{1}{a^2}\mathbb{Z}$. □

Proof of Formula $(**')$. The determinant of M has the sign of $(-1)^{r_2}$, and replacing $\mathrm{Tr}(x^2)$ by $\mathrm{Tr}(x\overline{x})$ multiplies the determinant by $(-1)^{r_2}$. Thus the determinant of the lattice L associated with M in $\widehat{K}$ is equal to $|d_{K/\mathbb{Q}}(M)|$.

Replacing $\widehat{K}$ by $\mathbb{R}^n$ and $|N_{K/\mathbb{Q}}|$ by F_{r_1,r_2} preserves the value of the ratio $\frac{N_{K/\mathbb{Q}}(M)^2}{\det(M)}$. By Lemma 2.5, the value of $F(\Lambda)$ in Proposition 2.2 is attained on some $x\in\Lambda$, so that the second formula of the proposition bounds $\frac{N_{K/\mathbb{Q}}(M)^2}{\det(M)}$ from above by $\frac{1}{\kappa_{r_1,r_2}}$. □

Definition 2.6. We say that a lattice $\Lambda\subset\mathbb{R}^n$ is *algebraic for a signature* (r_1,r_2) if it is the image of a module in a number field of signature (r_1,r_2). (**Warning.** Lattices constructed using Proposition 2.4 from algebraic lattices with a different signature *are not* considered as algebraic.)

Remark 2.7. It results from Lemma 2.5 that an algebraic lattice can be rescaled so as to have a point on the boundary of A_{r_1,r_2}, and indeed at least r_1+r_2 independent points, as shown by Dirichlet's unit theorem applied to $\mathfrak{O}(M)$. The maximum value n is attained if $r_2=0$, and in various other cases, depending on the number of roots of unity contained in $\mathfrak{O}(M)$.

2.4. **Automorphisms.** An *automorphism of a distance-function* F (or of the corresponding star body) is an element $u\in\mathrm{GL}(E)$ such that $F\circ u=F$. We say that two lattices Λ,Λ' are *equivalent* (with respect to F or to A_F) if $\Lambda'=u(\Lambda)$ for some $u\in\mathrm{Aut}(F)$. The set of automorphism is a closed subgroup $\mathrm{Aut}(F)$ (or $\mathrm{Aut}(A_F)$) of $\mathrm{GL}(E)$, thus a Lie subgroup of $\mathrm{GL}(E)$. We shall construct below a large subgroup of $\mathrm{Aut}(F_{r_1,r_2}$ (indeed the whole group $\mathrm{Aut}(F_{r_1,r_2})$, but we need not this precise result) and prove the following proposition:

Proposition 2.8. *For every $\alpha>0$, the group $\mathrm{Aut}(F_{r_1,r_2})$ acts transitively on the hyper-surface $F_{r_1,r_2}(x)=\alpha$.*

Proof. Consider first r_1+r_2 positive real numbers λ_k, $1\le k\le r_1$, and μ_k, $1\le k\le r_2$, and r_2 real numbers $\theta_\ell \mod 2\pi$, $1\le\ell\le r_2$, submitted

to the condition $\prod \lambda_k \prod \mu_k^2 = 1$. Then multiplications by λ_k of the x_k and by μ_ℓ of (y_ℓ, z_ℓ) followed by rotations of angle θ_ℓ in the plane $\langle y_\ell, z_\ell \rangle$ generate a continuous subgroup of dimension $r_1 + 2r_2 - 1 = n - 1$ of $\mathrm{GL}_n(\mathbb{R})$. The group G generated by these transformations and the orthogonal reflections $x_k \mapsto -x_k$ can be used to map any x with $F(x) = \alpha$ onto the unique element $x' = \lambda\mathbf{1}$ such that $F(x') = \alpha$.
[The whole automorphism group is generated by G and the group of order $r_1!\, r_2!\, 2^{r_2}$ mentioned at the beginning of Subsection 2.2.] □

The following corollary is a consequence of Lemma 2.5:

Corollary 2.9. *A minimal-admissible lattice proportional to an algebraic lattice is equivalent to a lattice containing* $\mathbf{1}$. □

Complements. In general, one cannot assert that the value of $F(\Lambda)$ (a lower bound) is attained, or otherwise stated, that a minimal-admissible lattice has a point on the boundary of A_{r_1,r_2}. However one can prove that *the determinant of any minimal-admissible lattice* Λ *is attained on an admissible lattice containing* $\mathbf{1}$.

Proof (outline). The hypothesis shows that there exists a sequence $x_n \in \Lambda$ such that $\lim F(x_n) = 1$, and Proposition 2.8 shows that there exists for every n an $u_n \in \mathrm{Aut}(A_{r_1,r_2})$ such that $u_n(x_n) = \lambda_n\mathbf{1}$. We have $\lim \lambda_n = 1$. A compactness argument (using "Mahler's compactness lemma") then shows that one can extract from $u_n(\Lambda)$ a convergent sub-sequence. The limit Λ' of this sub-sequence is admissible (because $\complement(A_{r_1,r_2})$ is closed), contains $\mathbf{1} = \lim \lambda_n \mathbf{1}$, and has the same determinant as Λ (because $|\det(u_n)| = 1$). □

3. Lower Bounds for the Minkowski Lattice Constants

Here we list some lower bounds for κ_{r_1,r_2}: results based on volumes of convex bodies, on constants for spheres, and various improvements. Proofs are at best sketched.

3.1. Convex Bodies.

Recall that a subset C of a vector space is *convex* if with every x, y, C contains the whole segment $[x, y]$ (C is a star body with respect to all its points). A very useful way of proving lower bounds for the lattices constants of symmetric convex bodies is the following theorem of Minkowski, first discovered in the case of spheres; the proof, as simplified later by Blichfeldt, can be read in essentially all books dealing with geometry of numbers:

Theorem 3.1. (Minkowski's convex body theorem). *Let $C \subset E$ be a convex, symmetric body (with respect to the origin). Then its lattice constant satisfies the inequality*

$$\sqrt{\kappa(C)} \ge 2^{-n}\,\mathrm{vol}(C)\,.$$

[Since he works with volumes, Minkowski makes use of the discriminant Δ, whence the square root in the formula above.] $\square$

To apply the theorem above to a domain A_{r_1,r_2}, it suffices to find a convex body of large volume contained in it. To this end Minkowski considers the convex body

$$B_{r_1,r_2} = \left\{x \in \mathbb{R}^n \;\middle|\; |x_1| + \cdots + |x_{r_1}| + 2|z_1| + \cdots + 2|z_{r_2}| < 1\right\}.$$

One easily proves the inclusion $n2^{r_2/n}B_{r_1,r_2} \subset A_{r_1,r_2}$ by means of the arithmetico-geometric inequality. There remains to calculate the volume of B_{r_1,r_2}, which is done by induction on r_1 for $r_2 = 0$, and then by induction on r_2 for fixed r_1. The result is

$$\mathrm{vol}(B_{r_1,r_2}) = \left(\frac{\pi}{4}\right)^{r_2}\frac{2^{n-r_2}}{n!}.$$

Putting together the results above, we finally obtain:

Theorem 3.2. *One has* $\sqrt{\kappa_{r_1,r_2}} \geq \left(\frac{\pi}{4}\right)^{r_2}\frac{n^n}{n!}$.

An easy calculation will show that $(\frac{\pi}{4})^{n/2}\frac{n^n}{n!}$ is a strictly increasing function of n, hence greater than 1 for all $n \geq 2$, which solves Kronecker's conjecture. However our domains (except if $(r_1, r_2) = (0, 1)$) are far from being convex (and even the theorem on convex bodies is not optimal except for some specific polyhedral domain, e.g., symmetric hexagons and the limit case of parallelograms in the plane).

For discriminants, we find the optimal values $d_K \leq -3$ if $(r_1, r_2) = (0, 1)$ and $d_k \geq 5$ if $(r_1, r_2) = (2, 0)$, but the bounds are much less satisfactory from $n = 3$ onwards: $d_k \leq -12.49\ldots$ (instead of -23) if $(r_1, r_2) = (1, 1)$ and $d_k \geq 20.25$ (instead of 49) if $(r_1, r_2) = (3, 0)$, ...

3.2. **Spheres.** I should have written "balls", but the use of the word "sphere" rather than "ball" is traditional.

In his 1891 letter to Hermite, Minkowski remarks that his bound for $(r_1, r_2) = (1, 1)$ can be slightly improved if one bounds $\kappa_{1,1}$ from below by the lattice constant of the largest sphere contained in $A_{1,1}$: one then obtains $d_K \leq -\frac{27}{2} = -13.5$. Actually the volume of the largest ball contained in A_{r_1,r_2} is smaller than that of B_{r_1,r_2}, but much effort has been done for obtaining good lower bounds for the lattice constant of the unit ball B_n. The exact value is known up to $n = 8$ (and also for $n = 24$, but this latter dimension is far beyond what we can reasonably consider here). Giving $\kappa(B_0)$ the value 1, one has $\kappa(B_n) = \frac{a_n}{2^n}$ for $0 \leq n \leq 8$, where (a_n) is the palindromic sequence $1, 2, 3, 4, 4, 4, 3, 2, 1$.

Theorem 3.3. *One has* $\kappa_{r_1,r_2} \geq n^n\kappa(B_n)$.

Proof. Applying the arithmetico-geometric inequality to the n numbers x_j^2 $(1 \le j \le r_1)$ and $\frac{y_k^2+z_k^2}{2}$ $(1 \le k \le r_2)$ written twice, we see that A_{r_1,r_2} contains the sphere of radius $\sqrt{n}$, whence the result. $\square$

We know that for fixed n (thus $r_2 = \frac{n-r_1}{2}$), κ_{r_1,r_2} is an increasing function of r_1. The Minkowski bounds are also increasing functions of r_1 whereas those given by spheres only depend on n, so that they must be expected to be especially useful for large values of r_2. In the following table we list for $n \in [2,8]$ the values M of the Minkowski bounds for $r_2 = \lfloor \frac{n}{2} \rfloor$ (thus $r_1 = 0$ or 1) and H (for Hermite) of the bounds given by spheres, rounded to two decimal places. The table shows that H is better than M in these cases; this also holds for $(n, r_1) = (6,2)$, $(7,3)$, and $(8,2)$.

[The results for sphere are often given in terms of the Hermite constant γ_n for dimension n. Given a lattice Λ, its *minimum* is $\min \Lambda = \min_{x \in \Lambda \smallsetminus \{0\}} x \cdot x$, its *Hermite invariant* is $\gamma(\Lambda) = \frac{\min \Lambda}{\det(\Lambda)^{1/n}}$, and the *Hermite constant* is $\gamma_n = \sup_\Lambda \gamma(\Lambda)$. One has $\kappa(B_n) = \gamma_n^{-n}$.]

Table 3.3 a. Lower bounds for M and H.

n	2	3	4	5	6	7	8
M	2.46	12.49	43.29	258.04	985.57	6266.87	25067.89
H	3	13.5	64	390.62	2187	12867.85	65536

3.3. **Some Low-Dimensional Results.** In the table below we display the known lower bounds for κ_{r_1,r_2} up to dimension $n = 4$ and conjectural values for $n = 4$.

Table 3.3 b. Lower bounds for κ_{r_1,r_2}.

(n, r_1)	$(2,0)$	$(2,2)$	$(3,1)$	$(3,3)$	$(4,0)$	$(4,2)$	$(4,4)$
κ_{r_1,r_2}	$= 3$	$= 5$	$= 23$	$= 49$	> 64	> 70.18	> 500
conj.					$= 113$	$= 275$	$= 725$

In dimensions 2 and 3, equality holds exactly for lattices equivalent to the images of the rings of integers of the fields affording the smallest (absolute values of) discriminants. The conjectural values given in the last row of the table also correspond to fields having the smallest possible discriminant.

The results for $n = 2$ come from the theory of binary quadratic forms, and may be considered as going back to Lagrange and Gauss; proofs are given in Section 4 below.

The result in the non-totally real cubic case is due to Davenport ([Dav1]). Mordell found an alternative proof, based on a reduction (using an argument of duality) to the determination of the lattice constant of the plane domain $|x^3 + y^3| < 1$, a problem he himself solved. All proofs are complicated.

The result in the totally real cubic case is due to Davenport, who first produced a complicated proof in 1938, then a much simpler proof in 1941 ([Dav2]). This proof is given in Section 5 below.

The results for $n = 4$ and $r_1 = 0$ or 2 are those of Table 3.3 a; that for $n = r_1 = 4$ is Noordzij's [Noo] ($> M = 113.77...$).

The method of Davenport has been extended by Godwin to totally real domains in dimensions 4 (unpublished) and 5, which reads

$$\kappa_{5,0} \geq 57.02^2 = 3251.2804 \; (> M = 113.77...)\,.$$

Conjectures for the exact values of κ_{r_1,r_2} are obtained using the upper bounds of κ_{r_1,r_2} given by $|d_K|$ for explicit fields K. Probably the minimum of $|d_K|$ among fields of signature (r_1, r_2) coincide in low dimensions with the exact value of κ_{r_1,r_2}. These minima are known in all degrees $n \leq 7$ and in degree 8 for the two extreme signatures. In particular if $n = r_1 = 5$, one has $d_K = 11^4 = 14641$, attained uniquely by the maximal real subfield of the fields of 11-th roots of unity, still much larger than Godwin's lower bound for $\kappa_{5,0}$.

The general method to list fields with discriminant up to some given bound and given signature is to define fields by the minimal polynomial

$$P(X) = X^n - a_1 X^{n-1} + \cdots + (-1)^n a_0 \in \mathbb{Z}[X]$$

of a primitive $\theta \in K$. The a_i are the elementary symmetric functions of the roots $\theta_1, \dots, \theta_n$ of P in $\mathbb{C}$. Let $S = \sum_{i<j} |\theta_j - \theta_i|^2$. One can bound S using techniques from geometry of numbers (see [Mar1]) and choose $a_1 \in [0, \lfloor \frac{n}{2} \rfloor]$ by a transformation $\theta \mapsto \pm\theta + k$, $k \in \mathbb{Z}$. Then all coefficients a_i may be bounded in terms of a_1 and S, so that we find finitely many polynomials, which *theoretically* solves the problem for primitive fields. (To deal with imprimitive fields, one adapts the method to primitive extensions of fields of degrees dividing n having convenient signatures and discriminant; I leave aside this problem.)

There remains the problem of discarding polynomials which are reducible or have not the required signature, calculating the discriminants of the field they define, and testing various fields for isomorphism. In practice one finds a considerable amount of polynomials, which may excess any reasonable running time for a computer, so that one must make use of various tricks to discard *a priori* many polynomials. The extreme signatures are somewhat easier: if $r_1 = 0$ or 1, the small discriminants will have the right signature; if $r_1 = n$, S is explicit in terms of the first two coefficients of P: $S = (n-1)a_1^2 - 2na_2$.

The main ingredient of Davenport's simple determination of $\kappa_{3,0}$ consists in bounding S on the sets (x, y, z) such that the 2-dimensional lattice generated by $(1, 1, 1)$ and (x, y, z) is contained in an admissible lattice for $A_{3,0}$; Godwin's generalization relies on the same idea.

Asymptotic results have been obtained by Rogers ([Rog]) for totally real domains, and by Mulholand ([Mul]) for general signatures. They are not sharp enough to be efficiently applied to problems of algebraic number theory.

4. Quadratic Fields

In this section, after some general remarks, we shall focus on the quadratic A_{r_1,r_2} (thus $(r_1, r_2) = (0, 1)$ or $(2, 0)$).

4.1. **Preliminary Results.**

In this subsection we only consider lattices Λ containing $\mathbf{1}$.

We first notice that the "real" coordinates of a vector X off $\mathbb{R}\,\mathbf{1}$ of an admissible lattice Λ for any Minkowski domain are irrational. Indeed since for $p, q \in \mathbb{Z}$, Λ contains $qX - p\mathbf{1} \in \Lambda$, $x_i = \frac{p}{q}$ would imply $F_{r_1,r_2}(qX - p\mathbf{1}) = 0$. We also remark that $\mathbf{1}$ is primitive in Λ, hence may be enlarged to a basis for Λ.

In dimension 2, writing $X = (x, y)$, we have

$$\det(\langle \mathbf{1}, X\rangle) = \left|\begin{smallmatrix} 1 & x \\ 1 & y \end{smallmatrix}\right|^2 = (x-y)^2\,.$$

The calculation of the determinant using a Gram matrix yields the identity $(x-y)^2 = 2(x^2+y^2) - (x+y)^2$, that we shall use to deal with imaginary quadratic domains. In the real case, we shall write $(x-y)^2 = (x+y)^2 - 4xy$.

When applying geometry of numbers to class groups of orders, we denote for every $c \in \mathrm{Cl}_{\mathfrak{O}}$ by N_c the smallest possible norm of an integral ideal in c and set $N = \max_c N_c$.

4.2. **The Imaginary Quadratic Domain.**

In this subsection we consider the domain $A = A_{0,1}$, i.e., $A = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 < 2\}$.

Theorem 4.1. *One has $\kappa_{0,1} = 3$, and the critical lattices are those which are equivalent to the image of the ring of integers of $\mathbb{Q}(\sqrt{-3})$.*

Proof. Let Λ be a critical lattice for A. Since A is bounded, Λ has a point on ∂A, hence is equivalent to a lattice containing $(1, 1)$, that we extend to a basis $((1, 1), (x, y))$. Replacing (x, y) by $(x + a, y + a)$ for a convenient $a \in \mathbb{Z}$, we may assume that $-1 < x+y \le 1$, and using a symmetry of the domain, that $x \ge y$. We then have

$$\det(\Lambda) = 2(x^2+y^2) - (x+y)^2 \ge 2^2 - 1 = 3\,,$$

and equality holds if and only if $x+y = 1$ and $x-y = \sqrt{3}$. Then Λ has six elements on the boundary of A (namely, $\pm(1,1)$ and $\pm\frac{(1\pm\sqrt{3}}{2})$. This property, which characterizes a hexagonal lattice, is shared by the image of $\mathbb{Z}[\omega]$ where ω is a cubic root of unity. $\square$

Corollary 4.2. *Let $\mathfrak{O}$ be an order in an imaginary quadratic field. Then any class of $\mathfrak{O}$ contains an (invertible) integral ideal $\mathfrak{a}$ such that*

$$\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a}) \le \sqrt{\frac{|d_K(\mathfrak{O})|}{3}}\,.$$

[In other words, N is bounded from above by $\big(d_K(\mathfrak{O})/3\big)^{1/2}$.]

For the minimal norm N (up to $N=5$) on ideal classes of imaginary quadratic fields, we give below the smallest discriminant D, the conductor f, the class number and the discriminant $d = \frac{|D|}{N^2}$ of the corresponding minimal-admissible lattice, rounded to three decimal places.
$N=1 : D=3, f=1, h=1, d=3\,;$
$N=2 : D=-15, f=1, h=2, d=\frac{15}{4}=3.75\,;$
$N=3 : D=-32, f=2, h=2, d=\frac{32}{9}=3.555\,;$
$N=4 : D=-55, f=1, h=4, d=\frac{55}{16}=3.437\,;$
$N=5 : D=-76, f=1, h=4, d=\frac{76}{25}=3.04.$

It is known [2] that $\liminf_{D\to\infty} \frac{D}{N^2} = 3$, so that the denominator 3 cannot be improved in Corollary 4.2,; in particular, the bound in $O(D^{1/2})$ cannot be improved to $o(D^{1/2})$.

4.3. **The Real Quadratic Domain.** This time A is the domain $A_{2,0}$, i.e., $A = \{(x,y) \in \mathbb{R}^2 \mid |xy| < 1\}$.

Theorem 4.3. *One has $\kappa_{2,0} = 5$, and the critical lattices are those which are equivalent to the image of the ring of integers of $\mathbb{Q}(\sqrt{5})$. Moreover, if Λ is a minimal-admissible lattice, then either Λ is critical or* $\det(\Lambda) \ge 8$, *and equality then holds if and only if Λ is equivalent to the image of the ring of integers of $\mathbb{Q}(\sqrt{2})$.*

Proof. We first consider lattices Λ containing $\mathbf{1}$. We shall then sketch a proof of the general characterization of critical lattices, a result which is not needed for applications to algebraic number theory. We thus

[2] but I have no reference for imaginary quadratic fields; for real quadratic fields, see next subsection

consider a lattice Λ admissible for A, equipped with a basis of the form $\big((1,1),(x,y)\big)$.

Using a symmetry of A we may assume that $y \ge x$, and changing (x,y) into $(x+k, y+k)$, that $x \in [-1,0]$, and indeed $x \in (-1,0)$ since x must be irrational. Similarly we have $y \in (m, m+1)$ for some $m \in \mathbb{Z}$, and since $y < 1$ implies $|xy| < 1$, we have $m \ge 1$.

Set $u = x+y$ and $v = xy$, so that x, y are the roots of the polynomial

$$f(X) = X^2 - uX + v\,.$$

The determinant of Λ is $d = u^2 - 4v$, and since the conditions above are invariant under the transformation $(x,y) \mapsto (m-y, m-x)$, we may assume when searching for a lower (resp. an upper) bound for $\det(\Lambda)$ that $u \ge m$ (resp. $u \le m$).

We have $f(t) > 0$ if $t = -1$ or $m+1$ and $f(t) < 0$ if $t = 0$ or m, and since $|(x+k)(y+k)| \ge 1$, we have the four inequalities

$$(a)\, f(-1) \ge 1,\ \ (b)\, f(0) \le -1,\ \ (c)\, f(m) \le -1,\ \ (d)\, f(m+1) \ge 1\,.$$

Explicitly these conditions read

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

Using (b) and choosing $u \ge m$, we obtain the lower bound

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

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

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

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

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

Taking successively $m = 1, 2, 3$, we see that we have

$$d \in \{5\} \cup [8, 12] \cup [13, +\infty)\,,$$

which completes the proof of the theorem for lattices containing $\mathbf{1}$.

To deal with lattices of determinant 5 without using the hypothesis "$\mathbf{1} \in \Lambda$", one must consider the conditions $x \in (-1-\varepsilon, +\varepsilon)$ and $y \in (1-\varepsilon, 2+\varepsilon)$ for every $\varepsilon > 0$. Such an argument is carried out in terms of indefinite binary quadratic forms in [Cas1], Section II.4.

[We say that the lattice Λ corresponding to the ring of integers of $\mathbb{Q}(\sqrt{5})$ is *isolated*, in the sense that a small enough neighbourhood of it contains no admissible lattices except those of the form $\lambda u(\Lambda)$ with $\lambda \ge 1$ and $u \in \mathrm{Aut}(A)$.] $\square$

Corollary 4.4. *Let $\mathfrak{O}$ be an order in a real quadratic field which is not the ring of integers of $\mathbb{Q}(\sqrt{5})$ nor that of $\mathbb{Q}(\sqrt{2})$. Then any class of $\mathfrak{O}$ contains an (invertible) integral ideal $\mathfrak{a}$ such that*

$$\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a}) < \sqrt{\frac{d_K(\mathfrak{O})}{8}}\,. \quad \square$$

[In other words, N is bounded from above by $\big(d_K(\mathfrak{O})/8\big)^{1/2}$.]

To go further one must make use of conditions $|(qx-p)(qy-p)|$ for values of $q>1$ (up to now we only made use of the case $q=1$). Taking $q=2$, we must consider for every $m\ge 2$ the four cases $x\in(-1,-\frac{1}{2})$ or $x\in(-\frac{1}{2},0)$ and similarly $y\in(m,m+\frac{1}{2})$ or $y\in(m+\frac{1}{2},m+1)$, and use the inequalities $|f(-\frac{1}{2})|\ge\frac{1}{4}$ and $|f(m+\frac{1}{2})|\ge\frac{1}{4}$. Carrying out explicitly the calculations for $m=2$ yields a splitting of $[8,12]$ into the three sub-intervals $\{8\}$, $[\frac{221}{25},\frac{480}{49}]$, and $[10,12]$. This shows that denominator 8 in Corollary 4.4 can be replaced by $\frac{221}{25}=8.84$:

Proposition 4.5. *Under the hypothesis of Corollary 4.4, every class in $\mathfrak{O}$ contains an integral ideal $\mathfrak{a}$ such that*

$$\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a}) \le \sqrt{\frac{d_K(\mathfrak{O})}{8.84}}\,. \quad \square$$

The determinants $5,8,\frac{221}{25}$ are the first three terms of an infinite sequence of numbers of the form $9-\frac{4}{m^2}$, where $m=1,2,5,13,29,34,\dots$ is the (rapidly increasing) sequence of *Markoff numbers*, which can be characterized as elements of triplets (m_1,m_2,m_3) which are solutions of the *Markoff diophantine equation* $m_1^2+m_2^2+m_3^2=3m_1m_2m_3$. For a proof (in terms of integral binary quadratic forms) we refer the reader to Chapter II of [Cas1].

Here is an interpretation in the setting of class groups. Given a Markoff number m, let $\mathfrak{O}_m$ be the real quadratic order (let us call it the *Markoff order of index m*) of discriminant $9m^2-4$ if m is odd, and $9(m/2)^2-1$ if m is even. Its discriminant D_m is congruent to 5 modulo 8 if m is odd and to 8 modulo 32 if m is even.[3] With the notation $N=\max N_c$, we have $N=m$ if if m is odd, and $N=\frac{m}{2}$ if m is even, which does give the corresponding lattice the determinant $d=\frac{D}{N^2}$. Note that the existence of the Markoff numbers shows that there is no bound in $o(\sqrt{D})$ for the norm of an integral ideal in a given class.

[3] one has $m\equiv 2 \mod 32$, a congruence recently proved by Y. Zhang, *Congruence and uniqueness of certain Markoff numbers*, Acta Arith. **128** (2007), 295–301.

If $\mathfrak{O}$ is not a Markoff order, we can even replace the denominator 8.84 above by 9, a slight improvement. Now it is easy to prove (by induction) that the m_i in the Markoff equation are pairwise coprime, which proves that m, $3m-2$ and $3m+2$ (writing the equation as $(3m \pm 2) = (m_1 \pm m_2)^2 + m^2$) have no prime divisors $p \equiv 3 \mod 4$, since these numbers divide a sum of two squares with g.c.d 1 or 2. Hence:

Proposition 4.6. *Let $\mathfrak{O}$ be a real quadratic order, the discriminant of which has a prime factor congruent to* 3 *modulo* 4. *Then any class of $\mathfrak{O}$ contains an integral ideal $\mathfrak{a}$ such that*

$$\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a}) < \sqrt{\frac{d_K(\mathfrak{O})}{9}}. \quad \square$$

Question 4.7. Under the hypothesis of Proposition 4.6, can one replace 9 by a larger number? (Certainly at most 12, but 12 is perhaps optimistic.)[4]

5. Totally Real Cubic Fields

This time A is the domain $A_{3,0}$, i.e., $A = \{(x,y,z) \in \mathbb{R}^3 \mid |xyz| < 1\}$. We calculate in a first subsection the lattice constant of A (Theorem 5.5), and then discuss the computational results obtained in 1971 by Swinnerton-Dyer in [SwD]. Due to the progress of computational methods, it would be very interesting to extend his results, using techniques which have been developed during the last forty years.

5.1. **The Lattice Constant for Real Cubic Fields.** A lower bound for the determinant of an admissible lattice for A will be obtained using a lower bound for

$$S = (x-y)^2 + (x-z)^2 + (y-z)^2$$

for any x, y, z belonging to a lattice containing $\mathbf{1} = (1,1,1)$. For the sake of simplicity we leave aside the general case of critical lattice which needs a modification of the proof making use of inequalities "up to an arbitrary small $\varepsilon > 0$".

As in the real quadratic case, we assume that $x \le y \le z$ and consider integers $m_1 \le m_2 \le m_3$ such that $x \in (m_1, m_1+1)$, $y \in (m_2, m_2+1)$ and $z \in (m_3, m_3+1)$, and making use of fact that we may replace (x,y,z) by $(x+k, y+k, z+k)$ for any $k \in \mathbb{Z}$, and use a global change

[4] (added July 13th, 2011) Bill Allombert, in an e-mail of July 9th, 2011, pointed out to me that the idea that 12 could be the right bound is false. Indeed, for the field K of discriminant $d = 924 = 4 \cdot 3 \cdot 7 \cdot 11$, Cl_K is of type $(2,2)$, and representative of classes having the smallest possible norms have norms $1, 2, 5, 10$. One has $\sqrt{(d/12)} = 8.774... << 10$ (or $\sqrt{(d/10)} = 9.612... << 12$)

of signs. In particular we may assume that $m_2 - m_1 \le m_3 - m_2$ and choose arbitrarily one of the m_i.

Lemma 5.1. *We have* $S \ge \frac{3}{2}(z-x)^2$.

Proof. Viewed as a function of y on $[x,z]$, the derivative of S is $2(2y-x-z)$, so that S attains its minimum at $y = \frac{x+z}{2}$. □

Lemma 5.2. *If* $S < 15.44$*, we may assume that* $(m_1, m_2, m_3) = (-1, 0, 2)$.

Proof. We first show that $m_2 > m_1$. Otherwise we might assume that $x, y \in (0,1)$. Then $x(1-x)$ and $y(1-y)$ are bounded from above by $\frac{1}{4}$, which implies $z > \frac{1+\sqrt{65}}{2}$, hence $S \ge 2(z-1)^2 > \frac{49}{2} > 24$.

Next we show that the m_i cannot be consecutive integers. Otherwise we might assume that $-1 < x < 0 < y < 1 < z < 2$. We have $|x| < 1$ and $z < 2$ hence $y > \frac{1}{2}$, and also $|x-1| < 2$ and $z-1 < 1$, hence $1 - y > \frac{1}{2}$, i.e. $y < \frac{1}{2}$, a contradiction.

From now on we fix $m_1 = -1$. If $m_3 \ge 4$, we have $x_3 - x_1 > 4$ hence $S > 16$, so that the possible systems (m_1, m_2, m_3) reduce to $(-1,0,2)$, $(-1,0,3)$, and $(-1,1,3)$, and we must now get rid of the last two. In both cases we have $y < 2$ and $z < 4$, hence $x < -\frac{1}{8}$, and also $|3-x| < 4$ and $3 - y < 3$, hence $z - 3 > \frac{1}{12}$, so that Lemma 5.1 implies

$$S > \tfrac{3}{2}\,(3 + \tfrac{1}{8} + \tfrac{1}{12})^2 = 15.44... \quad \square$$

The result of Lemma 5.2, obtained using crude estimates on x, y, z, could have been improved using the polynomial

$$f(X) := (X-x)(X-y)(X-z) := X^3 - uX^2 + vX - w\,,$$

as we did for real quadratic domains. We then have $S = 2u^2 - 6v$.[5] This we now do in case the m_i are $-1, 0, 2$, which implies the inequalities $f(-1) \le -1$, $f(0) \ge 1$, $f(2) \le -1$ and $f(3) \ge 1$, or explicitly,

$$(a) u+v+w \ge 0, (b) -w \ge 1, (c) 4u-2v+w \ge 9,\ (d) -9u+3v-w \ge -26\,.$$

Proposition 5.3. *Let* (x,y,z) $(x \le y \le z)$ *belong to an admissible lattice* Λ *for* A *which contains* $\mathbf{1}$*. Then we have* $S \ge 14$*, and equality holds if and only if, up to a transformation* $X \mapsto \pm X + k$ *with* $k \in \mathbb{Z}$*,* x, y, z *are the roots of the polynomial* $X^3 - 2X^2 - X + 1$*, of discriminant* 49.

[5] In the general totally real case, we have $S = (n-1)u^2 - 2nv$, and Lemma 5.1 reads $S \le k(n-k)(x_n - x_1)^2$ 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. For non-totally real domains, $S = \sum |\theta_k - \theta_j|^2$ can no longer be expressed in terms of u, v alone.

Proof. We have $2\,(a)+3\,(b)+(c)=6u\ge 12$, hence $u\ge 2$, and then $v\le -1$ by (c). Writing $u=2+h_1$ and $v=-1-h_2$ with $h_1,h_2\ge 0$ we obtain

$$S=2u^2-6v=14+2\big((h_1^2+2h_1)+3h_2\big)\ge 14\,,$$

and equality holds if and only if $h_1=h_2=0$, i.e., $u=2$ and $v=-1$. Then (a) and (b) read $w\ge -1$ and $w\le -1$, i.e. $w=-1$. □

Remark 5.4. We have $f(X+1)=X^3+X^2-2X-1$, a polynomial with roots $\zeta_7^i+\zeta_7^{-i}$, $i=1,2,3$, where ζ_7 stands for a root of unity of order 7.

Before stating the main theorem of this subsection, we recall two elementary facts of Euclidean geometry. Given a vector $e\in E$, of norm $N(e):=e\cdot e>0$, the orthogonal projection to the line $\mathbb{R}e$ is given by $p_e(x)=\frac{x\cdot e}{e\cdot e}\,e$, hence the orthogonal projection to the hyperplane orthogonal to e is given by $p_{e^\perp}(x)=x-\frac{x\cdot e}{N(e)}\,e$, of norm

$$N(p_{e^\perp}(x))=x\cdot x-\frac{(x\cdot e)^2}{N(e)}\,,$$

Also given a basis $\mathcal{B}=(e_1,\dots e_n)$ for E, the determinant of the projection to $e_1^\perp$ of $\mathcal{B}'=(e_2,\dots,e_n)$ is $\frac{\det(\mathcal{B})}{N(e)}$. As a consequence, is e is a primitive vector in a lattice Λ, then the projection Λ' of Λ to $e^\perp$ has determinant

$$\det(\Lambda')=\frac{\det(\Lambda)}{N(e)}\,.$$

Theorem 5.5. *The lattice constant of $A=A_{3,0}$ 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 ring of integers of the maximal real subfield of the cyclotomic field $\mathbb{Q}(\zeta_7)$.*

[The restriction is not necessary, but a proof of this needs an isolation result, which would result from proofs "up to ε" of Lemma 5.2 and Proposition 5.3. Actually, by a theorem of Cassels and Swinnerton-Dyer, all algebraic lattices of signature $(3,0)$ are isolated.]

Proof. We apply the Euclidean formulae above with $e=\mathbf{1}(=(1,1,1))$. Let Λ be an admissible lattice for $A_{3,0}$ containing $\mathbf{1}$, let $X=(x,y,z)\in\Lambda\smallsetminus\mathbb{R}\mathbf{1}$, let p be the orthogonal projection to $e^\perp$, and let $\Lambda'=p(\Lambda)$. We have $N(p(X))=\frac{S}{3}$ and $\det(\Lambda')=\frac{1}{3}\det(\Lambda)$. Proposition 5.3 shows that Λ' is admissible for the disc of square radius $R^2=\frac{14}{3}$, and since the lattice constant of the unit disc $(=\frac{\kappa_{\{0,1\}}}{4})$ is equal to $\frac{3}{4}$, we obtain

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

There remains to characterize the admissible lattices Λ of determinant 49 which contain $\mathbf{1}$. Since equality must hold everywhere in the inequalities above, Λ' 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 $\mathbb{Z}_K$. $\square$

In a 1943 very difficult paper Davenport proved that we may replace the denominator 49 by 81.1 in Theorem 5.5 provided we exclude the cyclic fields of determinants 49 and 81 (the latter one is the maximal real subfield of 9-th roots of unity; $\zeta_9 + \zeta_9^{-1}$ is s root of $X^3 - 3X + 1$, with $S = 18$). The subsection below is devoted to Swinnerton-Dyer's extension of this result.

5.2. **Successive Minima for the Real Cubic Domain.** We give here an account of the results of [SwD] and put forward some conjectures.

The paper [SwD] gives a classification of all minimal-admissible lattices of determinant $d \le 17^2 = 289$ for the domain $A = A_{3,0}$. There are 19 lattices but only 18 determinants ($13^2 = 169$ occurs twice). All lattices are algebraic and isolated, as are all algebraic lattices by a theorem proved by Cassels and Swinnerton-Dyer in [Cas-SwD].

Among these lattices, 6 come from orders, all maximal (those of the fields with discriminant $d = 49 = 7^2$, $81 = 3^4$, $148 = 37 \cdot 2^2$, $169 = 13^2$, 229 and 257. We now consider some of the 12 remaining orders.

At this point, Abelian cubic fields K deserve special comments. Their discriminants are of the form $D = f^2$ where f is a product of t distinct primes $p \equiv 1 \mod 3$ (or $p = 9$). There are 2^{t-1} such fields, the invariant classes of which (under the Galois group) constitute a 3-elementary subgroup of order 3^{t-1} of their class groups (and h_K is prime to 3 if $t = 1$). Several lattices are associated with a module of determinant D/N_c^2 where N_c is the minimal norm of an integral ideal in a class c.

After the discriminants $49, 81, 148$ listed above, one finds a lattice of determinant $d = (\frac{63}{5})^2 = 148.76$ ($f = 63, N_c = 5$), then a second lattice with $d = 13$ ($f = 91, N_c = 7$), and then $196 = 14^2 = 49 \cdot 2^2$, a lattice coming from a module in the field with discriminant 49, but *not from a class* in an order.[6]

Two main questions arise from [SwD]:

1. Does the increasing sequence of determinants of minimal-admissible lattices for $A_{3,0}$ have a limit point (like in the Markoff case), or is it unbounded?
2. Are all minimal-admissible lattices for $A_{3,0}$ equivalent to algebraic lattices?

As was pointed out by Swinnerton-Dyer, if the sequence in the first question in unbounded, there exists an upper bound $N_c = O(d_K(\mathfrak{O}))^{1/2}$ for the norm of an integral ideal in any class c of an order $\mathfrak{O}$.

As for the second question, if we could prove that all minimal-admissible lattices for $A_{3,0}$ are equivalent to algebraic lattices, then we could prove the following long standing conjecture:

Conjecture 5.6. (Littlewood's conjecture.) *Denote by* $\|x\|$ *the distance of the real number* x *to the nearest integer. Then for any two real numbers* α, β*, one has* $\liminf_{n\to\infty} n\,\|n\alpha\|\,\|n\beta\| = 0$.

[Littlewood's conjecture would follow from conjectures of Margulis about approximations in Lie groups. Note that the proof by Margulis of a parent conjecture solved Oppenheim's conjecture, namely that if q is a non-degenerate, indefinite quadratic form in a Euclidean space of dimension $n \geq 5$, then there are no admissible lattices for the domain $|q(x)| \leq 1$.]

My opinion is that it is reasonable to state the following conjecture about the two questions above:

Conjecture 5.7. *All minimal-admissible lattices for* $A_{3,0}$ *are equivalent to algebraic lattices, and the ordered sequence of their discriminants is not bounded.*

In this respect, it would be useful to carry out numerical investigations on admissible lattices for $A_{3,0}$ beyond determinant 289.

6. Varia

In this section we briefly consider various problems related to the questions discussed in the previous five sections.

[6] See Delone-Faddeev, *The Theory of Irrationalities of the Third Degree*, A.M.S. (1964; Russian ed.: 1940), Section 31; actually I could show that if the conductor of an order is divisible by an inert prime p, then it is divisible by p^2

6.1. **Indefinite Quadratic Forms.** After Margulis's work the problem of describing the admissible lattices for a domain $|(q(x)| < 1$ exists for only four types of indefinite quadratic forms q, those of signature $(1,1)$ (which amounts to the problem for $A_{2,0}$ considered in Section 4), $(2,1)$, $(2,2)$ and $(3,1)$. The lattice constants are known, found by Markoff in the 19th century for signature $(2,1)$ and by Oppenheim in the early thirties for the last two; see [Cas2], Appendix. We shall return to signature $(2,2)$ in connection with the class number problem for quaternions, and now restrict ourselves to signature $(2,1)$.

The situation is similar to that of the domain $A_{3,0}$: in both cases, a few first minima are known, found by B.A. Venkov during last world war (the 11 first minima; Oppenheim also found 7 minima (but 8 lattices up to equivalence, listed in [Opp];) for signature $(2,2)$; see again the Appendix to [Cas2]), and isolation theorems are proved in [Cas-SwD], but nobody has been able to guess a Markoff-like rule for the minima.

It would be interesting to carry out extended numerical investigations for both problems.

6.2. **Twin Classes.** Let K be a number field of degree n and signature (r_1, r_2). The (bilinear) trace form $(x,y) \mapsto \mathrm{Tr}(xy)$ defines a duality on K, which maps $\mathbb{Z}_K$ onto the *co-different* $\mathbb{Z}_K^*$ *of* K*, also denoted by* $\mathcal{C}_K$; $\mathcal{D}_K = \mathcal{C}^{-1}$ is the *different of* K, and an ideal $\mathfrak{a}$ onto $\mathfrak{a}^* = \mathcal{C}_K\,\mathfrak{a}^{-1}$. When $\mathfrak{a}$ runs through a class c, $\mathfrak{a}^*$ runs through a class c^*, which we could call the *twin class of* c. However, in Zimmert's work ([Zi]), the twin class is that of $\mathcal{D}_K\,\mathfrak{a}^{-1}$. Any of these dualities can be considered. Zimmert ([Zi]) has given good upper bounds for the minimum of the geometric mean $(\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a})\,\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{b}))^{1/2}$ where $\mathfrak{a}$ and $\mathfrak{b}$ are suitable integral ideals in a given class c and in his twin class. Oesterlé ([Oe]) has given a proof of Zimmert's twin class theorem in the setting of *Weil's explicit formulae*, but he did not publish the case of a single class.

To my knowledge the geometric analogue of the twin class problem has not been studied. Only the analogous question for spheres [7] (to bound the geometric mean of the minima of a lattice and its dual, known as the "Bergé-Martinet invariant") has given rise to various developments. This invariant can be used in the twin class problem as the lattice constants of sphere were used in the single class problem.

[7] A.-M. Bergé, J. Martinet, *Sur un problème de dualité lié aux sphères en géométrie des nombres*, J. Number Theory **32** (1989), 14–42; see also Section 2.8 of [Mar] and its complements in [Marweb]

6.3. **Domains Related to Semi-Simple Algebras.** In this subsection we generalize to the setting of semi-simple algebras the constructions of a Euclidean space and of a "Minkowski domain" made in Section 2. The main algebraic results in the theory of semi-simple algebras are recalled in Appendix 1.

Let L be a semi-simple algebra over $\mathbb{Q}$. Its completion $\widehat{L} = \mathbb{R} \otimes_{\mathbb{Q}} L$ for the infinite place of $\mathbb{Q}$ is a semi-simple algebra over $\mathbb{R}$. It is known (theorem of Frobenius) that any skew-field of finite rank over $\mathbb{R}$ is isomorphic to $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{H}$, the field of Hamilton quaternions, defined by a basis $(1, i, j, k)$ with multiplication

$$i^2 = j^2 = -1,\ ij = -ji = k\,.$$

Hence $\widehat{L}$ is a direct product of matrix rings $\mathcal{M}_m(\mathbb{K})$ where $\mathbb{K}$ is one of the fields $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$.

Each field $\mathbb{K}$ has a canonical involution, which extends to $\mathcal{M}_r(\mathbb{K})$, and one easily verifies that the quadratic form $x \mapsto \mathrm{Trd}(x\overline{x})$ on $\mathcal{M}_r(\mathbb{K})$, where $\mathbb{K}$ is one of the fields $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$, is positive definite. Hence the form $\mathrm{Trd}_{\widehat{L}/\mathbb{R}}(x\overline{x})$ defines on $\widehat{L}$ a Euclidean structure.

As a distance function F we may take $|\mathrm{Nrd}_{\widehat{L}/\mathbb{R}}(x)|$, up to a positive coefficient to be chosen in order that every module M in L should contain an x of reduced norm bounded from above by $(|d_L(M)|/\kappa)^{1/2}$, where κ stands for the lattice constant of the star body associated with F. Here d_L a *reduced discriminant*, defined using the bilinear form $\mathrm{Trd}(xy)$ on L. The case of quaternions is discussed in the next subsection.

[The reduced data are certainly the "good" choice to deal with simple algebras. However the use of ordinary trace, norm, and discriminant may prove simpler in some non-simple cases. For instance the order $\mathbb{Z}[G]$ in the group algebra $\mathbb{Q}[G]$ of a finite group G of order n has discriminant n^n, but the calculation of the reduced discriminant needs a precise knowledge of the representations of G over $\mathbb{Q}$.]

6.4. **Domains for Quaternion Algebras.** Let $H = K_{(a,b)}$ be a quaternion algebra over a number field K of degree m (thus H is of degree $n = 4m$). Given an infinite place v of K, the completion H_v of H is isomorphic to $\mathbb{H}$, $\mathcal{M}_2(\mathbb{R})$ or $\mathcal{M}_2(\mathbb{C})$ according as v is real ramified, real unramified, or complex. The reduced norm takes the form $x^2 + y^2 + z^2 + t^2$ on $\mathbb{H}$, $\det\left|\begin{smallmatrix} x & y \\ z & t \end{smallmatrix}\right| = xt - yz$ on $\mathcal{M}_2(\mathbb{R})$ (a real quadratic form of signature $(2,2)$), and $\mathrm{N}_{\mathbb{C}/\mathbb{R}}(xt - yz) = (xt - yx)(\overline{xt - yz})$ (a real quartic form), respectively. When K is totally real, the *generalized*

Minkowski domain takes up to scale the form

$$A = \{x \in \mathbb{R}^n \mid \prod_{\ell=1}^{m} |q_\ell(x_\ell, y_\ell, z_\ell, t_\ell)| < 1\}\,,$$

where the q_ℓ are ternary quadratic forms of signature $(4,0)$ or $(2,2)$. When H is totally definite, we have more precisely

$$A = \{x \in \mathbb{R}^n \mid \prod_{\ell=1}^{m} (x_\ell^2 + y_\ell^2 + z_\ell^2 + t_\ell^2) < 2^m\}\,.$$

Such domains with $m > 1$ are out of scope of usual techniques from the geometry of numbers. When $m = 1$ the lattice constants are known, and can be compared with the determinant produced by classes of maximal orders.

Over any Dedekind domain R with quotient field K, the (reduced) discriminant of H/K is of the form $\mathfrak{d}^2$ where $\mathfrak{d}$ is a product of distinct prime ideals of R. (In central skew-fields, the ramification is always tame!) Given t, such a ramification occurs exactly in those quaternion algebras in which a number congruent to t modulo 2 of infinite primes ramifies (Hasse's law). The smallest possible discriminants over $\mathbb{Q}$ are thus 2^2 in the definite case and 6^2 in the indefinite case. Over a real quadratic field, there is exactly *one* quaternion field which is unramified at finite primes, of reduced discriminant d_K^2. The smallest discriminant occurs with the "usual" quaternions over $\mathbb{Q}(\sqrt{5})$, and the corresponding lattice is a 5-*modular lattice*, that is an integral lattice Λ which is mapped onto its dual lattice $\Lambda^* = \{x \in \mathbb{R}^8 \mid \forall y \in \Lambda, x \cdot y \in \mathbb{Z}\}$ by a similarity of ratio $\frac{1}{\sqrt{5}}$.

In the definite case over $\mathbb{Q}$, the lattice constant of the domain is that of the sphere of square radius 2, namely 4, exactly the discriminant of the skew-field. The critical lattices are thus equivalent to those defined by a maximal order in the algebra $\mathbb{Q}_{(-1,-1)}$, for instance the *Hurwitz order* $\mathfrak{M}$ with basis $(1, i, j, \omega)$, where $\omega = \frac{-1+i+j+k}{2}$ is a cube root of unity in H.

In the indefinite case, we observe that for $i^2 = -1, j^2 = k^2 = 3$, the quadratic form given by the reduced norm is $x^2 + y^2 - 3(z^2 + t^2)$, which does not represent 0, the Gram matrix is diagonal with entries $2, -2, 3, 3$, the order with basis $(1, i, j, k)$ has discriminant $-2^4 \cdot 3^2$, and replacing k by $\omega = \frac{1+i+j+k}{2}$, we obtain a maximal order, of discriminant -6^2. In Oppenheim's notation, this is his discriminant $\frac{9}{4}$. The form $x^2 + y^2 - 3(z^2 + t^2)$, corresponding to a non-maximal order, appears as the eighth form in Oppenheim's list; it has the same discriminant that the seventh one. The next maximal order, of discriminant -10^2, gives Oppenheim's third form (of discriminant $\frac{25}{4}$), but his forms numbered 2, 4, and 5, the discriminants of which ($\frac{17}{4}$, $\frac{117}{16}$ and $\frac{33}{4}$, respectively) are not squares, do not correspond to any module in an indefinite quaternion algebra.

6.5. **Some possible future work.** (1) About lattice constants and successive minima, it is clearly possible to enlarge Swinnerton-Dyer's calculations for totally real cubic domains, and to deal with totally real quartic domains looks feasible. In a first step one could restrict oneself to lattices containing the image of a given quadratic field. A neighbour problem is to find good lower bounds of $S(X)$ on elements $X \neq \mathbf{1}$ in a minimal-admissible lattice for a Minkowski domain.

Less difficult but capable of giving valuable information would be a numerical estimation of the list of determinants of admissible lattices coming from classes in rings of integers of extensions of degrees 3, 4, and 5, for which extended tables of number fields are available. In degree 4, it would be important to consider separately fields with three quadratic subfields (of signatures $(0, 2)$ and $(4, 0)$), fields containing *one* real quadratic field (of any signature), fields of signature $(0, 2)$ containing *one* imaginary quadratic field, and primitive fields (of any signature).

It would also be interesting to try to extract more information from lattice constants of sphere for domains with $r_1 = 0$ or 1.

7. Appendix: Skew-Fields and Semi-Simple Algebras

7.1. **General Theory.** In our applications, the base field is a number field or a completion of a number field. All algebras are of finite *rank* (= *dimension*).

We say that an algebra L over a field K is *semi-simple* if $\{0\}$ is its only nil-potent two-sided ideal, and that it is *simple* if $\{0\}$ and L are its only two-sided ideals. We state below the two main structure theorems of the theory:

A semi-simple algebra is the direct product of simple algebras

and

A simple algebra is isomorphic to a matrix ring $\mathcal{M}_m(D) \simeq \mathcal{M}_m(K) \otimes D$ *where* D *(well-defined up to isomorphism) is a skew-field* (a *division algebra*; D may be a (commutative) field).

The center of D is a finite extension K_0 of K. We say that L is *central* if its center is K. The center of a semi-simple algebra is thus a direct product of finite extensions of K.

For every extension K'/K one can consider algebra $L_{K'}$ the multiplication law of which is defined by the products of elements of a basis of L but using now linear combinations of the basis elements with coefficients in K'. Intrinsically, $L_{K'} = K' \otimes L$.

We shall also need the following result:

If L/K is central simple then $L_{K'}$ is a central simple K'-algebra.

The study of the structure of $L_{K'}$ in the general case of a semi-simple algebra reduces to the case of finite extensions (the centers of the simple factors). Under a separability condition which is automatic in characteristic zero, $K' \otimes_K K''$ is an étale algebra (a product of (separable) extensions of K') whenever K'' is. Hence over a number field K, $L_{K'}$ is a semi-simple algebra over K' for any extension K' of K. This applies in particular to any completion $\widehat{L} = \widehat{K} \otimes_K L$ induced by a completion $\widehat{K}$ of the base field K.

Note that if $L = \mathcal{M}_m(K)$, the characteristic polynomial of an $x \in L$ (i.e., that of the endomorphism $y \mapsto xy$) is the the m-th power of the characteristic polynomial of the matrix x. Extending the base field K to an algebraic closure, we see that the rank of a central simple algebra L is a square, say m^2, and that the characteristic polynomial of an $x \in L$ is an m-th power of a polynomial, called the *reduced characteristic polynomial*, denoted by $\chi_{red,x}$. It can be proved that $\chi_{red,x}$ is canonically defined by this construction and belongs to $K[X]$. Write $\chi_{red}(x)(X) = X^m - a_1 X^{m-1} + \cdots + (-1)^m a_m$. The coefficient a_1 is called the *reduced trace of* x, denoted by $\mathrm{Trd}_{L/K}(x)$, and a_n is called the *reduced norm of* x, denoted by $\mathrm{Nrd}_{L/K}(x)$; we have $\mathrm{Tr}(x) = m\,\mathrm{Trd}(x)$ and $\mathrm{N}(x) = (\mathrm{Nrd}(x))^m$. Reduced trace and norm are defined on a simple algebra with center an extension K_0 of K by

$$\mathrm{Trd}_{L/K} = \mathrm{Tr}_{K_0/K} \circ \mathrm{Trd}_{L/K_0} \quad \text{and} \quad \mathrm{Nrd}_{L/K} = \mathrm{N}_{K_0/K} \circ \mathrm{Trd}_{L/K_0}\,,$$

and on a semi-simple algebra as the sum of the reduced traces and the product of the reduced norms on each simple factor, respectively.

An *involution on an algebra* L/K is a map $x \mapsto \overline{x}$ of L onto L which satisfies the following four rules: (1) $\overline{\overline{x}} = x$; (2) $\overline{x} = x$ if $x \in K$; (3) $\overline{x+y} = \overline{x} + \overline{y}$; (4) $\overline{(xy)} = \overline{y}\,\overline{x}$.

[**Warning:** the identity *is not* an involution if L is not commutative.]

An involution on an algebra L/K extends canonically to algebras $\mathcal{M}_m(L)$, defining $\overline{M}$ for a matrix $M = (m_{i,j})$ as the transpose of the matrix with entries $\overline{m}_{i,j}$.

7.2. **Example: Quaternion Algebras.** The general definition (over a field of characteristic not 2) of a *quaternion algebra* is an (associative) algebra H equipped with a basis $\mathcal{B} = (1, i, j, k)$ over K, with multiplication law

$$i^2 = a,\ j^2 = b,\ ij = -ji = k\,,$$

where a, b are given non-zero elements of K. This implies

$$k^2 = -ab,\ jk = -kj = i,\ \text{ and } ki = -ik = j\,.$$

We shall sometimes denote this algebra by $K_{(a,b)}$. Note that the commutation relation can be written $jij^{-1} = -i$, defining the conjugacy in $K(i)/K$ when a is not a square.

For $q = x + yi + zj + tk \in H$, set $\overline{q} = q = x - yi - zj - tk$. Then $q \mapsto \overline{q}$ is an involution of H, and we have

$$\mathrm{Trd}(q) = q + \overline{q} = 2x \quad \text{and} \quad \mathrm{Nrd}(q) = q\overline{q} = x^2 - ay^2 - bz^2 + abt^2\,.$$

If the quadratic form $X^2 - aY^2 - bZ^2 + abT^2$ does not represent 0, H is a skew-field (one has $q^{-1} = \frac{q}{\mathrm{Nrd}(q)}$ for every $q \neq 0$). Otherwise, H is isomorphic to $\mathcal{M}_2(K)$ (and one can indeed show that any central simple algebra of rank 4 is a quaternion algebra).

Hasse has classified the central simple algebras over a number field or a completion of a number field. His theorem for quaternions reads as follows, defining *a ramified place in a simple algebra L* as a place at which the completion of L is not a matrix ring (it involves a skew-field):

1. There is up to isomorphism exactly one quaternion skew-field over a $\mathfrak{p}$-adic field or over $\mathbb{R}$ (and none over $\mathbb{C}$).
2. Over a number field, the number of ramified places is even, and conversely, given a set S of an even number of non-complex places of K, there exists up to isomorphism exactly one quaternion algebra ramified exactly at the places of S, which is a skew-field if and only if $S \neq \emptyset$.

[However, to construct a pair (a, b) for a quaternion algebra defined over a number field by its set of ramified places may cause some difficulties.]

We say that a quaternion algebra H over a number field K is *totally definite* if all the infinite places of K are ramified in H, which amounts to saying that K is totally real and that $v(\mathrm{Nrd}(x))$ is strictly positive for all $v : K \to \mathbb{R}$ and all $x \in H^\times$. Totally definite quaternion algebras play a special rôle in the arithmetic theory of semi-simple algebras over number fields.

7.3. **Arithmetic in Semi-Simple algebras.** This is a short overview of a rich theory, first over any field which is the quotient field of a Dedekind domain (modulo a mere condition of separability), then over number fields, where some precise results on class groups have been proved.

Over a Dedekind domain R, there are notions of orders, fractional (left) ideals, invertible fractional ideals, with which we define a *set* of left classes. The set of integers used in the commutative case is no longer a ring, and this notion must be replaced by that of *maximal orders* (for inclusion). In general invertible ideals can be characterized as projective ideals, a local notion, but "locally projective" does not imply "locally free" like in commutative algebras. However this is true for maximal orders, and allows then to develop a theory similar to that we are used to in commutative algebras.

We now restrict ourselves to maximal orders over a number field, taking $R = \mathbb{Z}_K$. The set of left classes is then finite, is in one-to-one correspondence with that of right classes, does not depend on the choice of the maximal order, so that the class number $h = h_L$ of an algebra L is well-defined. Moreover the number t of conjugacy classes of maximal orders in L is bounded from above by h. Any maximal order contains the integers of the center of the algebra, and in particular the central idempotent which split a semi-simple algebra into its simple components. This allows us to restrict ourselves to central simple algebras in which we have chosen a maximal order $\mathfrak{M}$.

Much more is known. First the reduced norm induces a map from the set of (left) classes to a class group in a somewhat narrow sense of the center, namely the group $\mathrm{Cl}'_{L,K}$ of fractional ideals of K modulo the subgroup of principal ideals (α) where α is positive at the places where the reduced norm is positive. The direct sum of ideals $\mathfrak{a}_1, \dots, \mathfrak{a}_k$ can be viewed as an ideal in $\mathfrak{M}_k(L)$. In particular the image of $\mathfrak{a} \oplus \mathfrak{M}_k$ in $\mathrm{Cl}'_{L,K}$ is the same as that of $\mathfrak{a}$ for ever $k \geq 0$.

Say that two left fractional ideals $\mathfrak{a}, \mathfrak{b}$ are *stably equivalent* ($\mathfrak{a} \sim_s \mathfrak{b}$) if $\mathfrak{a} \oplus \mathfrak{M}^k$ and $\mathfrak{b} \oplus \mathfrak{M}^k$ are isomorphic (as $\mathfrak{M}$-modules) for some $k \geq 0$. Left modules M such that $K \otimes_{\mathbb{Z}_K} M$ are free are direct sums of rank 1-modules, so that we may define an addition on the set of stable classes, writing $\mathrm{cl}(\mathfrak{a}) + \mathrm{cl}(\mathfrak{b}) = \mathrm{cl}(\mathfrak{c})$ where $\mathfrak{c}$ is any ideal such that $\mathfrak{a} \oplus \mathfrak{b} \simeq \mathfrak{c} \oplus \mathfrak{M}$. All stably free ideals (those for which $\mathfrak{a} \oplus \mathfrak{M}^k \simeq \mathfrak{M}^{k+1}$) are zero in the stable class group. Results of Eichler, revisited by Swan, read as follows:

1. The reduced norm induces an isomorphism of the stable class group of $\mathfrak{M}$ *onto* $\mathrm{Cl}'_{L,K}$.
2. If L is not *a totally definite quaternion algebra, then stable equivalence on* $\mathfrak{M}$ *amounts to ordinary equivalence.*

Since $\mathcal{M}_2(L)$ is not a totally definite quaternion algebra, the results above imply:

3. Two fractional ideals $\mathfrak{a}, \mathfrak{b}$ *are stably equivalent if and only if* $\mathfrak{a} \oplus \mathfrak{M} \simeq \mathfrak{b} \oplus \mathfrak{M}$.

For instance, when the narrow class number h_K^+ is equal to 1 (e.g., if $K = \mathbb{Q}$ or $\mathbb{Q}(\sqrt{5})$), the *stable class number* h_s *of* $\mathfrak{M}$ is also equal to 1, and thus also the class number if L is not a totally definite quaternion algebra.

In the case of totally definite quaternion algebras, Eichler has given explicit formulae for the number of classes. Over $\mathbb{Q}$, whereas $h = 1$ if L is any indefinite quaternion algebra, in the totally definite case, h tend to infinity with the number of ramified primes, and indeed there are only five fields with class number 1, namely those of discriminant p^2 for $p = 2, 3, 5, 7, 13$.

References

[Cas1] J.W.S. Cassels, *An Introduction to Diophantine Approximation*, Cambridge University Press, Tract **45**, Cambridge, U.K. (1957; second edition: 1965).

[Cas2] J.W.S. Cassels, *An Introduction to the Geometry of Numbers*, Springer-Verlag, Grundlehren **99**, Heidelberg (1959; last reprint: 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, Series A, **248** (1955), 73–96.

[C-S] J.H. Conway, N.J.A. Sloane, *Sphere Packings, Lattices and Groups*, Grundlehren **290**, Springer-Verlag, Heidelberg (1988); third ed.: 1999.

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

[Dav1] H. Davenport, *On the product of three homogeneous linear forms (III)*, Proc. London Math. Soc. **45** (1939), 98–125, =[Dav] I, 34–61.

[Dav2] H. Davenport, *Note on the product of three homogeneous linear forms*, J. London Math. Soc. **15** (1941), 98–101, =[Dav] I, 62–65.

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

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

[Marweb] J. Martinet, http://math.u-bordeaux.fr/~martinet/

[Mar1] J. Martinet, *Méthodes géométriques dans la recherche des petits discriminants*, in Sém. Th. Nombres de Paris 1983–84, Prog. Math. **59**, Birkhäuser, Basel (1985), 1147-179.

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

[Oe] J. Oesterlé, *Le théorème des classes jumelles de Zimmert et les formules explicites de Weil*, in Sém. Th. Nombres de Paris 1983–84, Prog. Math. **59**, Birkhäuser, Basel (1985), 181–197.

[Opp] A. Oppenheim, *The minima of quaternary quadratic forms of signature zero*, Proc. London Math. Soc (2) **37** (1934), 63–81.

[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.

[Zi] R. Zimmert, *Ideale kleiner Norm in Idealklassen und eine Regulator Abschätzung*, Invent. Math. **62** (1981), 367–380.