ALGEBRAIC CONSTRUCTIONS OF LATTICES; ISODUAL LATTICES

by JACQUES MARTINET[1]

Introduction. Let Λ be a lattice (discrete subgroup of maximal rank) in some n-dimensional Euclidean space E. The *dual-lattice of* Λ is $\Lambda^* = \{x \in E \mid \forall y \in \Lambda, x.y \in \mathbb{Z}\}$.

The most important invariant of Λ is certainly the *Hermite invariant* $\gamma(\Lambda)$, which measures the density of the sphere packing canonically attached to Λ. However, invariants taking into account both Λ and Λ^* appeared during the last ten years, in connection with various domains of mathematics (for instance, algebraic number theory or abelian varieties). In this survey, which follows closely my talk in Eger, I shall focus on arithmetical problems involving duality.

§ **1. Basic questions.** Let E be a Euclidean space, of dimension n, and let Λ be a lattice in E. Let $x.y$ denote the scalar product of $x, y \in E$. The *norm* of a vector $x \in E$ is $N(x) = x.x\,(=\|x\|^2)$, and the *norm* (or minimum) *of* Λ is $N(\Lambda) = \min_{x \in \Lambda \smallsetminus \{0\}} N(x)$.

Les $\mathcal{B} = (e_1, \dots, e_n)$ be a basis of Λ; its *Gram matrix* is

$$\mathrm{Gram}(\mathcal{B}) = (e_i.e_j) = Mat(\mathrm{Id}, \mathcal{B}, \mathcal{B}^*)\,,$$

whose determinant, which does not depend on the choice of $\mathcal{B}$, is the *determinant* $\det(\Lambda)$ *of* Λ. The *Hermite invariant of* Λ is

$$\gamma(\Lambda) = \frac{N(\Lambda)}{\det(\Lambda)^{1/n}}\,,$$

and the *Hermite constant* (known only for $n \le 8$) is then $\gamma_n = \sup_\Lambda \gamma(\Lambda)$. Note that the density of the sphere packing attached to a lattice Λ is proportional to $\gamma(\Lambda)^{n/2}$.

An other important invariant is the *kissing number* $2s$ *of* Λ, where

$$s = \frac{1}{2}|S| \quad \text{for} \quad S = S(\Lambda) = \{x \in \Lambda \mid N(x) = N(\Lambda)\}\,.$$

By analogy with the Hermite invariant, we define its dual version

$$\gamma'(\Lambda) = \big(N(\Lambda)N(\Lambda^*)\big)^{1/2} = \big(\gamma(\Lambda)\gamma(\Lambda^*)\big)^{1/2}$$

(the second inequality holds because of the equality $\det(\Lambda^*) = \det(\Lambda)^{-1}$). The dual version of γ_n is then $\gamma'_n = \sup_\Lambda \gamma'(\Lambda)$.

Key words and phrases. Lattices, duality, density, minimal vectors.
[1]Laboratoire A2X, U.M.R. 9936 C.N.R.S. – Université Bordeaux 1

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

The constant γ'_n was introduced in [B-M1] as a geometric counterpart to Zimmert's analytic study of *twin-classes* in number fields. (For Zimmert's theory, see [Oe], [Zi].)

This constant was considered again by Conway et Sloane in [C-S1] (under the name of "Bergé-Martinet"), motivated by the paper [B-S] by Buser and Sarnak, where *symplectic lattices* occur in connection with the theory of abelian varieties; Conway and Sloane consider more generally *isodual lattices*, those for which there exists an isometry σ of Λ^* onto Λ; symplectic lattices correspond to $\sigma^2 = -\operatorname{Id}$. The invariants γ' and γ are equal for lattices which are similar to their dual lattice. Note that such a lattice can be rescaled so as to become isodual. We shall often call *isodual* those lattices which are merely similar to their dual lattice.

The value of γ_n, as well as the corresponding *critical lattices*, is known for $n \le 8$. Since these critical lattices (the root lattices $\mathbb{Z}$, $\mathbb{A}_2$, $\mathbb{A}_3$, $\mathbb{D}_4$, $\mathbb{D}_5$, $\mathbb{E}_6$, $\mathbb{E}_7$, $\mathbb{E}_8$) are isodual for $n = 1, 2, 4, 8$, one has $\gamma'_n = \gamma_n$ for these four dimensions. The constant γ'_n is also known in dimension 3. One conjectures that the lattices which realize γ'_n are the critical lattices and their dual lattices for all $n \le 8$ (plus an extra pair (Λ, Λ^*) in dimension 5). To find the exact value of γ_n or γ'_n for other values of n looks very difficult. The following problems are more tractable :

Problems.

(1) To construct lattices with a large γ' invariant.
(2) Same question for isodual lattices, and more precisely for σ-isodual lattices, where σ is a given "interesting" orthogonal transformation of E.
(3) Same question for *modular lattices.*
(One says after Quebbemann that Λ is *ℓ-modular* for some integer ℓ if Λ is integral, and if there exists a similarity of modulus $\sqrt{\ell}$ which maps Λ^* onto Λ.)

[There is no reason not to look at the Hermite constant itself. The recent constructions by Bacher ([Bc], 1996) of dense lattices in dimensions $27, 28, 29$ show that progress can still be made in comparatively low dimensions.]

We now come to the first part of the title. A great many of the famous even-dimensional lattices can be constructed over maximal orders in algebras with involutions, especially C.M. fields or totally definite quaternion algebras; examples are A_2, D_4, E_8, Coxeter-Todd's K_{12}, Barnes-Wall's Λ_{16}, the Leech lattice Λ_{24}, some 2-modular lattices of dimension 32 (Quebbemann, Bachoc), ... The algebras involved are cyclotomic fields and/or various quaternion skew-fields, in particular those with center $\mathbb{Q}$ ramified at ∞ and 2 or 3.

All these lattices are modular and (when conveniently rescaled) symplectic. In all cases, multiplication by a convenient purely imaginary element of the order yields a similarity from Λ^* onto Λ. Thus, algebraic methods appear to be suitable for constructing interesting symplectic lattices. Other interesting examples are the *Craig lattices* $\mathbb{A}_{p-1}^{(r)} = (\mathfrak{P}^r, \frac{1}{p}\operatorname{Tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(x\overline{y}))$, where p is an odd prime, ζ_p is a primitive p^{th}-root of unity and $\mathfrak{P}$ is the prime ideal above p in $\mathbb{Q}(\zeta_p)$; $\mathbb{A}_{p-1}^{(1)}$ is the root lattice $\mathbb{A}_{p-1}$.

§ **2. Isodualities.** We still denote by Λ a lattice in some n-dimensional Euclidean space E. An *isoduality* is an isometry σ which maps Λ onto Λ^* (or Λ^* onto Λ, it amounts to the same thing). Then, σ^2 is an automorphism of Λ.

To σ is attached the bilinear form $b : (x, y,) \mapsto x.\sigma y$, which is *unimodular*, i.e. integral on Λ, of determinant 1. We say that σ is *orthogonal* (resp. *symplectic*) if b is symmetric (resp. alternating). This is equivalent to $\sigma^2 = \mathrm{Id}$ (resp. $\sigma^2 = -\mathrm{Id}$), and also to the fact that the eigenvalues of σ are ± 1 (resp. $\pm i$). In the orthogonal case, if $+1$ and -1 have respective multiplicities p and q, then (p, q) is the signature of b.

By looking at Gram matrices, or by making use of a convenient Lie group to be defined later, one shows that, up to similarity, these families are of respective dimensions pq and m^2+m (we put $n = 2m$ in the symplectic case). The case when b is orthogonal of signature $(n, 0)$ or $(0, n)$ is somewhat special : the 0-dimensional corresponding families are those of unimodular lattices. Put $\mathrm{Aut}^{\#}(\Lambda) = \{\tau \in \mathrm{O}(E) \mid \tau(\Lambda) \subset \Lambda \text{ or } \tau(\Lambda) \subset \Lambda^*\}$. Then, the index $[\mathrm{Aut}^{\#}(\Lambda) : \mathrm{Aut}(\Lambda)]$ is 2 when Λ is isodual non-unimodular, and 1 otherwise.

There are only finitely many unimodular lattices in each given dimension, whose classification is known up to dimension 25, cf. [C-S], ch. 17. Their various orthogonal or symplectic structures can be detected by inspection of the conjugacy classes of order 2 or 4 of their automorphism groups.

§ **3. Connection with Abelian varieties.**

Given a complex vector space V of dimension g (thus of real dimension $n = 2g$), and a lattice $L \subset V$, consider the complex torus $T = V/L$; T is an analytic manifold. We say that T is an *Abelian variety* if it is an algebraic variety. Abelian varieties possess various characterizations (see e.g. [L-B]), among which we quote the existence of a *Riemann form*, i.e. of a positive definite Hermitian form H, whose imaginary part $\Im(H)$ takes integral values on L. Such a form is also called a *polarization*.

By making use of the elementary divisors theorem, one easily shows that, with respect to $\Im(H)$, V is an orthogonal sum of planes possessing a basis for which $\Im(H)$ has a matrix of form $\begin{pmatrix} 0 & -b_k \\ b_k & 0 \end{pmatrix}$, $k = 1, 2, \dots, g$. When all b_k are equal to 1, we say that H is a *principal polarization*.

Let us now come back to the notation of the previous two sections.

Let $\Lambda \subset E$ be a lattice with a symplectic isoduality $\sigma : \Lambda \to \Lambda^*$. One defines a complex structure on E by puting $ix = \sigma(x)$. Then, $H(x, y) = x.y + i\sigma(x).y$ is a principal polarization on E: one has $H(x, x) = x.x > 0$ for $x \in E \setminus \{0\}$, and $\Lambda/\sigma(\Lambda^*)$ is trivial. Conversely, for any pair (L, H) of a lattice L and a polarization H, the real part $\Re(H)$ of H is a scalar product on V, and, when H is principal, L is symplectic for the isometry $x \mapsto ix$.

To any curve C of genus g, one can attach its Jacobian $J(C)$. It is an Abelian variety of complex dimension g, which possesses a canonical principal polarization, and thus defines an isometry class of symplectic lattices. However, for $n = 2g \geq 8$, such constructions cannot produce the examples we gave above: Hurwitz's theorem asserts that one has

$|\operatorname{Aut}(C)| \leq 84(g-1)$, and Torelli's theorem that the centralizer of σ is of order at most $2 \times |\operatorname{Aut}(C)|$; for $\mathbb{E}_8$ or Λ_{24}, this order is much bigger than $168(g-1)$.

It would be interesting to derive from algebraic geometry canonical constructions of lattices such as $\mathbb{E}_8$ or the Leech lattice.

§ **4. Local theory.** We study in this section the local maxima of density of lattices belonging to various important families. We indeed consider families $\mathcal{F}$ of lattices which are orbits of one lattice in $\mathcal{F}$ under the action of a closed subgroup $\mathcal{G}$ of $\operatorname{GL}(E)$, invariant under transposition. One can moreover without loss of generality replace $\mathcal{G}$ by its connected component. We refer the reader to [M], ch. X and XI for the proofs.

Here are some examples:

4.1. Example. (G-lattices.) Let G be a finite rational subgroup of $\operatorname{O}(E)$. (This means that the natural representation of G comes from a rational representation.) Let

$$\mathcal{F} = \{\Lambda \mid \operatorname{Aut}(\Lambda) \supset G\}\,.$$

Then, we can take

$$\mathcal{G} = \{u \in \operatorname{GL}(E) \mid \forall s \in G,\ su = us\}\,.$$

4.2. Example. Let $G^\#$ be a finite subgroup of the orthogonal group $\operatorname{O}(E)$, and let G be a subgroup of index 2 of $G^\#$. Let

$$\mathcal{F} = \{\Lambda \mid \forall \sigma \in G^\# \smallsetminus G,\ \sigma(\Lambda) = \Lambda^*\}\,.$$

Then, we can take

$$\mathcal{G} = \{u \in \operatorname{GL}(E) \mid \forall \sigma \in G^\#,\ \sigma u = {}^t u^{-1} \sigma^{-1}\}\,.$$

Note that lattices in $\mathcal{F}$ are in particular G-lattices, and that we recover the notion of a σ-isodual lattice by taking for $G^\#$ a cyclic group with generator σ.

4.3. Example. In this example, we replace E by $E \times E$, and consider

$$\mathcal{F} = \{(\Lambda, \Lambda^*) \mid \Lambda \subset E\}\,.$$

Then, we can take

$$\mathcal{G} = \{(u, {}^t u^{-1}) \mid u \in \operatorname{GL}(E) \subset \operatorname{GL}(E \times E)\}\,.$$

Let $\mathcal{F}$ be such a family. Then we say that a lattice Λ is *$\mathcal{F}$-extreme* (or *$\mathcal{G}$-extreme)* if γ attains a local maximum at Λ among lattices $\Lambda \in \mathcal{F}$, and that Λ is *strictly $\mathcal{F}$-* (or *$\mathcal{G}$-)extreme* if there exists a neighbourhood $\mathcal{V}$ of Λ in the set of lattices of E such that $\Lambda' \in \mathcal{V} \cap \mathcal{F}$ and $\gamma(\Lambda') \geq \gamma(\Lambda)$ is possible only if Λ' is similar to Λ.

To characterize extreme lattices, we must introduce a few more definitions. Let $\mathcal{T}_0$ be the tangent space of $\mathcal{G}$ at $1_{\mathcal{G}}$, and let

$$\mathcal{T} = \{u + {}^t u \mid u \in \mathcal{T}_0\}\,.$$

For $x \in S(\Lambda)$, let φ_x be the restriction to $\mathcal{T}$ of the linear form

$$x \mapsto x.u(x)$$

defined on the space $\mathrm{End}^s(E)$ of symmetric endomorphisms of E.

We say that Λ is *$\mathcal{G}$-perfect* if the φ_x generate $\mathrm{Hom}(\mathcal{T}, \mathbb{R})$, and that Λ is *$\mathcal{G}$-eutactic* if there is in $\mathrm{Hom}(\mathcal{T}, \mathbb{R})$ a relation

$$\mathrm{Tr}_{|\mathcal{T}} = \sum \rho_x \varphi_x$$

with strictly positive coefficients ρ_x.

4.4. Theorem ([B-M3]).

(1) *Λ is strictly extreme if and only if it is $\mathcal{G}$-perfect and $\mathcal{G}$-eutactic.*
(2) *If Λ is extreme, but not strictly extreme, there is a path*

$$t \mapsto \Lambda_t,\ \ t \in [0,1]$$

such that $\Lambda_0 = \Lambda$, rank$(S(\Lambda_t)) < n$ for $t > 0$, and $\gamma(\Lambda_t) = \gamma(\Lambda)$ on $[0,1]$.

This theorem leaves open the following
Question. When does

$$\text{“extreme”} \implies \text{“strictly extreme”}\ ?$$

The answer is positive in the case of example 4.1 ([B-M2]; if $G = \{\mathrm{Id}\}$, this is an old theorem of Voronoi ([Vor]) (partially proved previously in 1873 by Korkine and Zolotareff in [K-Z]). The answer is also positive in the case of example 4.3 ([B-M1]; the $\mathcal{G}$-extreme lattices correspond to the local maxima of γ'). In the case of example 2, the answer depends on the representation of G afforded by the inclusion $G^{\#} \subset \mathrm{O}(E)$; it is positive for orthogonal or symplectic lattices.

This problem was recently revisited by Bavard ([Bv]) in the setting of Riemannian geometry. Let X be a compact non simply connected Riemannian manifold. Consider the *systole of X*, i.e. the minimal length of a homotopically non-trivial closed curve C on X, then the ratio $\dfrac{\text{length}\,(C)}{\text{vol}\,(X)^{1/\dim X}}$, and finally the supremum of this ratio over some family of Riemannian metrics on X. This supremum on the set of flat tori is precisely the Hermite constant. A characterization à la Voronoi of local maxima, involving convenient notions of perfection and eutaxy, is proved in [Bv].

§ 5. Isodual lattices and the Voronoi algorithm. Voronoi developped at the beginning of the century an algorithm which yields (theoretically) a classification of all perfect lattices in a given dimension. He applied it to recover the results of [K-Z] in dimensions $n \le 5$, and only began shortly before his death the classification in dimension 6, which was completed half a century later by Barnes ([Brn]). Such an algorithm was extended in [B-M-S] to the case of G-lattices. No general result is known for the families of examples 4.2 and 4.3, and this is an important open problem of the theory. (However, some families of symplectic lattices have been recently dealt with by Bavard, using methods of differential geometry; it would be interesting to study other examples, e.g. those arising from example 4.3.)

Let us explain briefly (in terms of lattices, though the consideration of positive definite quadratic forms would be more suitable) how the generalized Voronoi algorithm works for example 4.1.

Thus, let G be a finite subgroup of $\mathrm{O}(E)$, and let $\mathcal{G}$ be as in the example. One easily checks that $\mathcal{T}$ is the space

$$\mathrm{End}^s_G(E) = \{u \in \mathrm{End}^s(E) \mid \forall s \in G, su = us\}\,.$$

Let Λ be a G-perfect (i.e., a $\mathcal{G}$-perfect) lattice. For $x \in S(\Lambda)$, let $p_x \in \mathrm{End}^s(E)$ be the orthogonal projection on the line $\mathbb{R}x$, and consider the average

$$\omega_x = \frac{1}{|G|}\sum_{s\in G} p_{sx} \in \mathrm{End}^s_G(E)\,.$$

The *Voronoi domain of* Λ is the convex hull $\mathcal{D}_\Lambda$ in $\mathcal{T}$ of the rays $\mathbb{R}\omega_x$. Choose a vector $F \in \mathcal{T}$ orthogonal to some face of codimension 1 of this polyedral cone, with orientation towards the interior of $\mathcal{D}_\Lambda$. Then, for θ positive and not too large, $\Lambda_\theta = (\mathrm{Id} + \theta F)^{1/2}(\Lambda)$ is a non-perfect G-lattice with the same norm as Λ. Let ρ be the upper bound of such θ's. If ρ is finite (this is always the case for the original Voronoi algortihm, for which $G = \{\mathrm{Id}\}$), then Λ_ρ is again a G-perfect lattice with the same norm as Λ. Such a lattice Λ_ρ is called a *Voronoi neighbour of* Λ, and the path $\theta \mapsto \Lambda_\theta$ from $[0,\rho]$ to the topological space of G-lattices is called a *(G-)Voronoi path.* It is shown in [B-M-S] that the neighbouring graph is connected when one restricts oneself to lattices belonging to a fixed class of integral representations of G.

If Λ and Λ' are Voronoi neighbours, and if Λ' is similar to Λ^*, then one can reasonnably expect to find an isodual lattice on the Voronoi path which connects them. In practice, there is an involution $t \mapsto t^*$ of $[0,\rho]$ such that Λ_t^* is similar to Λ_{t^*}, and the isodual lattice Λ_{isod} is its fixed point.

Most of the isodual lattices of high density found by Conway and Sloane in [C-S1] by means of their gluing theory can also be found by the above procedure. One can use S_5-lattices in dimension 5, with $\Lambda \sim \mathbb{D}_5$ ([M], ch. XIII, § 4). The usual Voronoi algorithm works in dimensions 6 and 7, with paths $\mathbb{E}_6 - \mathbb{E}_6^*$ and $\mathbb{E}_7 - \mathbb{E}_7^*$ ([Brl]).

The case of dimension 6 is of great interest. The above lattice $\Lambda_{\rm isod}$ is symplectic, with Hermite invariant $\gamma(\Lambda_{\rm isod}) = 1 + \frac{1}{\sqrt{3}}$. It has been proved by Quine in [Qi] (and independently, by Bavard – private communication), and that it corresponds to the curve $y^3z = x^4 - z^4$ (known as the *Picard* or the *exceptional Wiman curve*); it is denser than the perfect symplectic lattice $\mathbb{A}_6^{(2)}$, which corresponds to the Klein quartic $y^3z+z^3x+x^3y = 0$.

These two lattices are extreme among the family of symplectic lattices ([Q-Z]; $\mathbb{A}_6^{(2)}$ was known to Barnes ([Brn]) to be extreme in the usual sense). Note that the Fermat curve $x^4 + y^4 = z^4$ does not correspond to an extreme lattice.

The problem of the local maxima of the systole of principally polarized abelian varieties is equivalent to the corresponding problem for the Hermite invariant of symplectic lattices. The relations which might exist between the systole of a Riemann surface and that of its Jacobian are not clear.

§ **6. Modular lattices.** Let ℓ be a positive integer. Recall that an integral lattice Λ is *ℓ-modular* if there exists a similarity $\sigma : \Lambda^* \to \Lambda$ of modulus $\sqrt{\ell}$. Thus, modular lattices are isodual.

Following Quebbemann, we restrict ourselves to even lattices. The theta series of such a lattice is then a modular form for the *Fricke group of level ℓ*, a group which contains $\Gamma_0(\ell)$ with the index 2, except for $\ell = 1$, where this group is simply the full modular group $\mathrm{SL}_2(\mathbb{Z})$. Note that 1-modular lattices are just unimodular lattices.

We are as usual interested in finding the densest possible lattices for given ℓ and n (if any). Upper bounds of the Hermite constant yield upper bounds for the minimal norms of ℓ-modular lattices, but better bounds can often be derived from the theory of modular forms. Indeed, if Λ has (even) minimum m, then its theta series takes the form $\vartheta_\Lambda(q) = 1 + \sum_{k\geq m} a_k q^k$ (with $q = e^{2\pi i z}$ as usual), where a_k is the number of vectors $x \in \Lambda$ with $x.x = k$. For m large enough (in practice, the dimension of the corresponding space of modular forms), the $\lfloor \frac{m}{2} \rfloor$ conditions $a_0 = 1$ and $a_2 = \cdots = a_{m-2} = 0$ determine ϑ_Λ uniquely. Actually, one can say much more, and, by calculating the dimensions of the corresponding spaces of modular forms, derive strong constraints for the maximal possible value for m. For instance, Hecke proved that for $\ell = 1$, even unimodular lattices exist if and only if $n \equiv 0 \mod 8$, and that one must have $m \leq 2 + 2\lfloor \frac{n}{24} \rfloor$. This result has been generalized to other levels. In particular, Quebbemann proved that, for

$$\ell \text{ prime and } \ell + 1 \mid 24 \quad \Longleftrightarrow \quad \ell \in \{1, 2, 3, 5, 7, 11, 23\},$$

ℓ-modular lattices can exist only if $\ell \equiv 3 \mod 4$ or $n \equiv 0 \mod 4$, and obained the upper bound

$$m \leq 2 + 2\left\lfloor \frac{(1+\ell)n}{48} \right\rfloor, \qquad \textbf{(6.1)}$$

which reduces to Hecke's for $\ell = 1$.

A fundamental problem is to find the largest possible value $m(n,\ell)$ for m. It is customary to call *extremal* those lattices for which equality holds in 6.1, though, in my opinion, it does not deserve a name. Actually, there are other methods to obtain upper bounds of m, for instance:

- Nebe and Venkov proved by making use of Siegel modular forms that extremal lattices for $n=12$, $\ell=11,13$ do not exist ([Ne-Ve]);
- Scharlau and Hemkemeier proved the impossibility of $(n,\ell)=(12,7)$ by classifying all lattices in the genus which would be that of such a lattice. (They found 395 lattices!)

Dimensions for which there is a jump in 6.1 are of particular interest, for the corresponding lattices (if any) often yield the best known values of the Hermite invariant. Here are some examples (disregarding the 0-dimensional lattice):

- $\ell=1$. $n=8$: $\mathbb{E}_8$; $n=24$: the Leech lattice Λ_{24} ; $n=48$: 3 known lattices.
- $\ell=2$. $n=4$: $\mathbb{D}_4$; $n=16$: the Barnes-Wall lattice Λ_{16} ; $n=32$: 3 known lattices. Extremal lattices also exist for $n=48$ (thus, $m=8$), but are less dense that the extremal unimodular lattices (with $m=6$).
- $\ell=3$. $n=2$: $\mathbb{A}_2$; $n=12$: the Coxeter-Todd lattice K_{12}.

For $\ell=1$, extremal lattices are known to exist for $n=8,16,24,32,40,48,56,64,80$. The case of dimension 80 (with $m=8$) was recently settled by Bachoc and Nebe who gave two examples in [Ba-Ne], solving simultaneously the problem for $(n,\ell)=(20,7)$ and $(40,3)$. The idea is to start with a $(20,7)$-extremal lattice constructed as a module for the ring $\mathfrak{O}=\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ (such an example can be found in [ATLAS], in relation with the Mathieu group M_{22}), then to show that extending the scalars from $\mathfrak{O}$ to a maximal order $\mathfrak{M}_3$ of the quaternion algebra with center $\mathbb{Q}$ ramified at 3 and at $\{\infty\}$ (the corresponding lattice is $\mathbb{A}_2\perp\mathbb{A}_2$) preserves the minimum 8, yielding a $(40,3)$ extremal lattice, and finally to extend the scalars over $\mathfrak{M}_3$ by E_8 (or a Cayley order). They used coding theory to prove the inequality $m\ge 8$.

Coulangeon (private communication) gave an alternative proof involving general properties of tensor products, which would apply to the sequence $(n,\ell)=(18,7)-(36,3)-(72,1)$ if any $(18,7)$-extremal lattice were to exist on $\mathfrak{O}$, thus solving positively the fundamental problem of the existence of 72-dimensional unimodular lattices. However, no 18-dimensional 7-extremal lattice is known.

Note that the existence of such lattices would establish new records of density in dimensions 18, 36, 72. My guess is that such extremal lattices do not exist.

§ 7. Some algebraic constructions. We consider a (skew) field K of one of the following three types:

(1) A totally real number field.
(2) A C.M. field.
(3) A totally definite quaternion algebra.

The field K contains a largest totally real number field K_0 (with $[K:K_0]=1,2,4$ respectively). Let $x\mapsto\overline{x}$ be the standard conjugacy of K (the identity map in case 1), and let $\mathrm{Tr} = \mathrm{Tr}_{K/\mathbb{Q}}$ be the (reduced) trace. Put $n = [K : \mathbb{Q}]$ and $n_0 = [K_0 : \mathbb{Q}]$. For any totally positive $\alpha \in K_0$, $(x, y) \mapsto \mathrm{Tr}(\alpha x \overline{y})$ is a positive definite $\mathbb{Q}$-bilinear form on K, which extends to a scalar product on the completion $\widehat{K} = \mathbb{R} \bigotimes_{\mathbb{Q}} K \simeq \mathbb{K}^{n_0}$ of K, where $\mathbb{K} = \mathbb{R}, \mathbb{C}, \mathbb{H}$ respectively.

We now construct lattices in $\widehat{K}$. To this end, we consider a maximal order $\mathfrak{M}$ in K (the ring $\mathbb{Z}_K$ of the integers of K in the first two cases), and a (left) fractional ideal I of $\mathfrak{M}$. (This means that I is a finitely generated non-zero $\mathfrak{M}$-submodule of K.) One has $\mathfrak{M}I = I$. Hence, I is a finitely generated $\mathbb{Z}$-module of rank n, and thus a lattice in $\widehat{K}$.

For $\beta \in K^\times$, the map $x \mapsto x\beta$ is an isomorphism of $\mathfrak{M}$-modules of I onto the equivalent ideal $I\beta$. For $x, y \in K$, one has $\mathrm{Tr}((x\beta)(\overline{y\beta})) = \mathrm{Tr}((\beta\overline{\beta})(x\overline{y}))$, and one easily sees that this map is a similarity if and only if $\beta\overline{\beta} \in \mathbb{Q}$.

Let $\mathcal{D}$ be the (reduced) different of $K/\mathbb{Q}$. For I as above, the dual module of I is

$$I^* = \alpha^{-1}\mathcal{D}^{-1}\overline{I}^{-1}\,.$$

As a consequence, we see that, if I is isodual by an isometry $x \mapsto x\beta$, then $\alpha\overline{I}\mathcal{D}I$ is the principal ideal generated by β^{-1}. Conversely, if this condition is satisfied with some generator β_0, then I is isodual provided there exists some unit ε in $\mathfrak{M}$ with $\varepsilon\overline{\varepsilon}\beta_0\overline{\beta_0} \in \mathbb{Q}$. To determine the nature of the isoduality (e.g., symplectic or orthogonal) reduces to a calculation of eigenvalues.

In the case of the Craig lattices defined in section 1, one has $K = \mathbb{Q}(\zeta_p)$, $K_0 = \mathbb{Q}(\zeta_p + \overline{\zeta}_p)$, $I = \mathfrak{P}^r$, $\alpha = \dfrac{1}{p}$ and $\mathcal{D} = \mathfrak{P}^{p-2}$, hence $\alpha\mathcal{D}I\overline{I} = \mathfrak{P}^{2r-1}$. For $p \equiv -1 \mod 4$ and $r = \frac{p+1}{4}$, one can take $\beta = \sqrt{-p}$, and $x \mapsto x\beta$ yields a symplectic isoduality.
[For r not too large, the minimum of $\mathbb{A}_{p-1}^{(r)}$ is at least $2r$, cf. [C-S], ch. 8, § 6, th. 7; equality holds for small values of r, and moreover for $r = \frac{p+1}{4}$ (Elkies) and also whenever r divides $p-1$ (Bachoc and Batut); these authors conjecture that equality holds for $r \le \frac{p+1}{4}$.]

More generally, one may consider (left) K-vector spaces of dimension $m > 1$. Then, many of the most famous lattices have been contructed as modules of small rank over an order of one of the above three types. We refer the reader to [Bay] for the case of cyclotomic fields and to the recent papers [Bt-Q-S], [Bay-M], [M1] for other examples; see also [M], ch. VIII. This kind of construction often provides obvious symplectic isomorphisms. For instance, consider a lattice Λ constructed over a maximal order $\mathfrak{M}$ of the quaternion field H with center $\mathbb{Q}$, with ramified places $2, \infty$ (resp. $3, \infty$), so that H may be defined by elements i, j with $i^2 = j^2 = -1, ij = -ji$ (resp. with $i^2 = -1, j^2 = -3, ij = -ji$). Then, right multiplication by $j - i$ (resp. j) is a similarity of square -2 (resp. -3). In this way, one obtains a nice definition of the Barnes-Wall lattice Λ_{16} (resp. of the Coxeter-Todd lattice K_{12}), which immediately shows that it is 2-modular (resp. 3-modular) of symplectic type.

ACKNOWLEDGEMENTS. I would like to thank Christophe Bavard with whom I had several discussions when writing this survey, and also Anne-Marie Bergé for the help I found in listening to the talk she delivered at the Luminy meeting of October, 1996.

References

[ATLAS] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, R.A. Wilson, *ATLAS of Finite Groups*, Oxford Univ. Press, Oxford, 1985.

[Bc] R. Bacher, *Dense lattices in dimensions* 27*,* 28 *and* 29, Invent. Math., to appear.

[Ba-Ne] C. Bachoc, G. Nebe, *Extremal lattices of minimum* 8 *related to the Mathieu group* M_{22}, to appear.

[Brl] J.-L. Baril, *Thèse, Bordeaux*, 1996.

[Brn] E.S. Barnes, *The complete enumeration of extreme senary forms*, Phil. Trans. Roy. Soc. London **(A), 249** (1957), 461–506.

[Bt-Q-S] C. Batut, H-G. Quebbemann, R. Scharlau, *Computations of Cyclotomic Lattices*, Exp. Math. **4** (1995), 175–179.

[Bv] C. Bavard, *Systole et invariant d'Hermite*, J. reine Angew. Math. (1997), to appear.

[Bay] E. Bayer-Fluckiger, *Definite unimodular lattices having an automorphism of given characteristic polynomial*, Comm. Math. Helvet. **59** (1984), 509–538.

[Bay-M] E. Bayer-Fluckiger, J. Martinet, *Formes quadratiques liées aux algèbres semi-simples*, J. reine angew. Math. **451** (1994), 51–69.

[B-M1] A.-M. Bergé, J. Martinet, *Sur un problème de dualité lié aux sphères en géométrie des nombres*, J. Number Theory **32** (1989), 14–42.

[B-M2] A.-M. Bergé, J. Martinet, *Réseaux extrêmes pour un groupe d'automorphismes*, Astérisque **198–200** (1992), 41–66.

[B-M3] A.-M. Bergé, J. Martinet, *Densité dans des familles de réseaux. Application aux réseaux isodu-aux*, L'Enseignement Mathématique **41** (1995), 335–365.

[B-M-S] A.-M. Bergé, J. Martinet, F. Sigrist, *Une généralisation de l'algorithme de Voronoï*, Astérisque **209** (1992), 137–158.

[B-S] P. Buser, P. Sarnak, *On the period matrix of a Riemann surface of large genus (with an Appendix by J.H. Conway and N.J.A. Sloane)*, Invent. Math. **117** (1994), 27–56.

[C-S] J.H. Conway, N.J.A. Sloane, *Sphere Packings, Lattices and Groups*, Springer-Verlag, Grundlehren n°290, Heidelberg, 1988.

[C-S1] J.H. Conway, N.J.A Sloane, *On Lattices Equivalent to Their Duals*, J. Number Theory **48** (1994), 373–382.

[C-S2] J.H. Conway, N.J.A. Sloane, Appendix to [B-S].

[K-Z] A. Korkine, G. Zolotareff, *Sur les formes quadratiques positives*, Math. Ann. **11** (1877), 242–292.

[L-B] H. Lange, Ch. Birkenhake, *Complex Abelian Varieties*, Springer-Verlag, Grundlehren n° 302, Heidelberg, 1992.

[M] J. Martinet, *Les réseaux parfaits des espaces euclidiens*, Masson, Paris, 1996.

[M1] J. Martinet, *Structures algébriques sur les réseaux*, Number Theory, S. David éd. (Séminaire de Théorie des Nombres de Paris, 1992-93), Cambridge University Press, Cambridge, 1995, pp. 167–186.

[Ne-V] G. Nebe, B.B. Venkov, *Nonexistence of Extremal Lattices in Certain Genera of Modular Lattices*, J. Number Theory **60** (1996), 310–317.

[Oe] J. Oesterlé, *Séminaire de Théorie des Nombres de Paris, 1983-84*, Birkhäuser, Prog. Math. n°59, Bâle, 1985.

[Q] H.-G. Quebbemann, *Modular Lattices in Euclidean Spaces*, J. Number Theory **54** (1995), 190–202.

[Qi] J.R. Quine, *Jacobian of the Picard Curve*, preprint, Florida State University, 1995.

[Qi-Z] J.R. Quine, P. L. Zhang, *Extremal Symplectic Lattices*, preprint, Florida State University, 1995.

[S-H] R. Scharlau, B. Hemkemeier., *Classification of integral lattices with large class numbers*, Math. Comp., to appear.

[Vo1] G. Voronoï, *Nouvelles applications des paramètres continus à la théorie des formes quadratiques : 1 Sur quelques propriétés des formes quadratiques positives parfaites*, J. reine angew. Math **133** (1908), 97–178.

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

J. Martinet
Laboratoire d'Algorithmique Arithmétique
Université Bordeaux I
351, cours de la Libération
33405 TALENCE cedex
E-mail : martinet@math.u-bordeaux.fr