ROLAND BACHER

BORIS VENKOV

Lattices and association schemes: a unimodular example without roots in dimension 28

Annales de l'institut Fourier, tome 45, n° 5 (1995), p. 1163-1176

<http://www.numdam.org/item?id=AIF_1995__45_5_1163_0>

Ann. Inst. Fourier, Grenoble
45, 5 (1995), 1163-1176

LATTICES AND ASSOCIATION SCHEMES: A UNIMODULAR EXAMPLE WITHOUT ROOTS IN DIMENSION 28

by R. BACHER and B. VENKOV

0. Introduction.

In small dimensions, the number of integral unimodular lattices is quite small. The list of such lattices which are indecomposable starts with the trivial lattice $\mathbb{Z}$, the lattice associated to the root system E_8 and a lattice with root system D_{12} in dimension 12. Unimodular lattices are classified up to dimension 25, where there are 665 of them [Bo]. In [Ba], all indecomposable lattices up to dimension 24 are explicitely constructed.

There are even less unimodular lattices without roots. Up to dimension 26, there are exactly four of them, respectively in dimension 23, 24 (Leech), 24 and 26 ([Bo] and [Bo1]).

The main purpose of this paper is to construct a 28-dimensional unimodular lattice without roots and automorphism group the group $\mathrm{Sp}(6, \mathbb{F}_3)\cdot 2$ of all symplectic similitudes of the symplectic space of dimension 6 over $\mathbb{F}_3$. Its order is equal to 18 341 406 720. Pairs of vectors of norm 3 in this lattice are in bijection with the set of Lagrangians in $\mathbb{F}_3^6$. By other constructions, we know several other 28−dimensional unimodular lattices without roots; indeed, we have a complete list of 38 non-isomorphic such lattices, *cf.* [BV].

Key words : Lattice – Association scheme – Symplectic space – Spread.
Math. classification : 05E30 – 11H56.

1. Basic definitions.

Let $\mathbb{E}^n$ denote a real euclidean $n-$dimensional vector space with scalar product $\langle , \rangle$. An *$n-$dimensional lattice* is a discrete cocompact subgroup of $\mathbb{E}^n$. Two lattices $\Lambda, \Lambda' \subset \mathbb{E}^n$ are *isomorphic* if there exists an isometry g of $\mathbb{E}^n$ such that $g\Lambda = \Lambda'$. A lattice $\Lambda \subset \mathbb{E}^n$ is *integral* if all scalar products between lattice elements are integral. The *norm* of a lattice element $\lambda \in \Lambda$ is $\langle \lambda, \lambda \rangle$ (and is hence the square of the euclidean norm of λ). A lattice element of an integral lattice is a *root* if its norm is 1 or 2. The dual lattice $\Lambda^\sharp$ of Λ is the lattice

$$\Lambda^\sharp = \{z \in \mathbb{E}^n \mid \langle z, \lambda \rangle \in \mathbb{Z} \quad \forall \lambda \in \Lambda\}.$$

For an integral lattice Λ we have $\Lambda \subset \Lambda^\sharp$ and the finite group $\Lambda^\sharp / \Lambda$ is the *determinant group* of Λ. Its order is the *determinant* of Λ. An integral lattice is *unimodular* if $\Lambda = \Lambda^\sharp$. The *automorphism group* of Λ is the finite group

$$\mathrm{Aut}(\Lambda) = \{g \in O(\mathbb{E}^n) | g(\Lambda) = \Lambda\}$$

where $O(\mathbb{E}^n)$ denotes the group of linear isometries of $\mathbb{E}^n$. A lattice is *decomposable* if it is the direct sum of two non-trivial sublattices in two orthogonal subspaces of $\mathbb{E}^n$. It is *indecomposable* otherwise.

Let $S = (s_1, \dots, s_k)$ be a finite sequence of elements in $\mathbb{E}^n$. The *Gram matrix* with respect to S is the $k \times k-$matrix G with entries

$$G_{i,j} = \langle s_i, s_j \rangle.$$

A *Gram matrix of a lattice* Λ is the Gram matrix with respect to a $\mathbb{Z}-$basis of Λ.

PROPOSITION 1.1. — *Let Λ be a lattice of $\mathbb{E}^n$. Consider a finite sequence S whose elements generate Λ and the Gram matrix G with respect to S.*

The matrix G is symmetric and of rank n. It has n strictly positive eigenvalues and all the remaining eigenvalues are zero. The matrix G is integral if and only if Λ is an integral lattice.

Conversely, let G be a real symmetric $k \times k-$matrix with n strictly positive eigenvalues and no strictly negative eigenvalues. Then there exists a finite sequence $S = (s_1, \dots, s_k)$ of $\mathbb{E}^n$ such that G is the Gram matrix with respect to S. Moreover, if G is integral, then the set S generates an integral lattice Λ.

The proof of these well-known facts is left to the reader.

Remark 1.2. — The converse statement of Proposition 1.1 is even more striking in the case where the positive symmetric integral matrix G is proportional to an idempotent, i.e. satisfies $G^2 = \lambda G$ for some natural integer λ. Let s_i be the i–th row-vector of the matrix $\frac{1}{\sqrt{\lambda}}G$. We have then

$$\langle s_i, s_j\rangle = \frac{1}{\lambda}\sum_k G_{ik}G_{jk} = \frac{1}{\lambda}\sum_k G_{ik}G_{kj} = G_{i,j}$$

and the finite set S is hence essentially the set of row-vectors of G.

Let X be a finite set. A *symmetric association scheme on X with d classes* is a pair $(X, \mathcal{R})$ such that

(i) $\mathcal{R} = \{R_0, R_1, \ldots, R_d\}$ is a partition of $X \times X$;

(ii) $R_0 = \{(x,x) \mid x \in X\}$;

(iii) $(x,y) \in R_i \Longleftrightarrow (y,x) \in R_i$ (symmetry);

(iv) there are numbers p_{ij}^k such that for any pair $(x,y) \in R_k$ the number of $z \in X$ with $(x,z) \in R_i$ and $(y,z) \in R_j$ equals p_{ij}^k (cf. page 43 in [BCN], or page 52 in [BI]).

The elements of X are the "points" and the elements $R_0, \ldots, R_d$ in $\mathcal{R}$ are the "relations" of the scheme $\mathcal{X} = (X, \mathcal{R})$. The numbers p_{ij}^k are its *intersection numbers.* The number $n_i = p_{ii}^0$ is the *valency* of the relation R_i.

The *automorphism group* of an association scheme $\mathcal{X}$ is the group

$$\mathrm{Aut}(\mathcal{X}) = \{\sigma \in \mathcal{S}_X \mid (\sigma x, \sigma y) \in R_i \text{ for all } (x,y) \in R_i \text{ and for all } i \in \{0, \ldots, d\}\}$$

where $\mathcal{S}_X$ denotes the symmetric group of the set X.

The i–th *adjacency matrix* of $\mathcal{X}$ is the $n \times n$ matrix A_i defined by

$$(A_i)_{x,y} = \begin{cases} 1 & \text{if } (x,y) \in R_i, \\ 0 & \text{otherwise,} \end{cases}$$

where the n points of X index the rows and columns of A_i. The adjacency matrices span a $(d+1)$ dimensional commutative subalgebra $\mathcal{A}$ consisting of symmetric matrices in the algebra of complex $n \times n$ matrices. By definition of the intersection numbers p_{ij}^k, the multiplication in the algebra $\mathcal{A}$ is given by

$$A_i A_j = \sum_k p_{ij}^k A_k.$$

The *intersection matrices* of $\mathcal{X}$ are the $(d+1) \times (d+1)$ matrices $B_0, \dots, B_d$ with entries

$$(B_i)_{k,j} = p_{ij}^k.$$

LEMMA 1.3. — *The linear application*

$$\varphi \left\{ \begin{array}{ccc} \mathcal{A} & \longrightarrow & M_{d+1}(\mathbb{C}) \\ \sum \alpha_i A_i & \longmapsto & \sum \alpha_i B_i \end{array} \right.$$

is an isomorphism of the algebra $\mathcal{A}$ onto a $(d+1)-$dimensional abelian subalgebra of $M_{d+1}(\mathbb{C})$.

Proof. — See Theorem 2.3 chapter II at page 57 in [BI]. □

Remark 1.4. — The underlying vector space of $\mathcal{A}$ carries a second algebra structure given by Hadamard multiplication. The vector space underlying $\mathcal{A}$ equipped with both algebra structures is called the *Bose-Mesner algebra* of the scheme $\mathcal{X}$. We will not need this second algebra structure.

Many symmetric association schemes are described by the following proposition.

PROPOSITION 1.5. — *Let G be a finite group which acts transitively on a set X. Consider the action of $G \times \{\pm 1\}$ on $X \times X$ defined by*

$$(g, +1)(x, y) = (g(x), g(y)),$$
$$(g, -1)(x, y) = (g(y), g(x)).$$

Denote the orbits of $X \times X$ under the action of $G \times \{\pm 1\}$ by $R_0, R_1, \dots, R_d$ where R_0 denotes the diagonal in $X \times X$.

Then $\mathcal{X} = (X, \{R_0, R_1, , \dots, R_d\})$ is a symmetric association scheme on X with d classes.

Proof. — See for instance example 2.1.(1) in [BI]. □

2. Lattices associated to rational idempotents.

Since the algebra $\mathcal{A}$ of a symmetric association scheme with d classes is an abelian, semi-simple, $(d+1)-$dimensional algebra, $\mathcal{A}$ contains $d+1$ minimal idempotents. We denote them by $E_0, E_1, \dots, E_d$ where E_0 is traditionnally the idempotent $E_0 = A_0 + A_1 + \ldots + A_d$ of rank 1. Let $f_0 = 1, f_1, \ldots, f_d$ be the ranks of the idempotents $E_0, \ldots, E_d$. The numbers $f_0, \ldots, f_d$ are the *multiplicities* of the association scheme (and can be recovered from the intersection numbers). An element $M = \sum \mu_i A_i$ of $\mathcal{A}$ is *rational* if the coefficients $\mu_0, \ldots, \mu_d$ are rational numbers. If E_r is a rational minimal idempotent there exists a smallest positive integer λ_r such that $E_r = \frac{1}{\lambda_r} \sum \gamma_{r,i} A_i$ with $\gamma_{r,0}, \ldots, \gamma_{r,d}$ integral. The matrix $G_r = \lambda_r E_r = \sum \gamma_{r,i} A_i$ is hence a symmetric integral matrix.

PROPOSITION 2.1. — *Let $G_r = \lambda_r E_r = \sum \gamma_{r,i} A_i \in \mathcal{A}$ be an integral matrix as above.*

(i) *The vector $(\gamma_{r,0}, \ldots, \gamma_{r,d})$ is a common eigenvector of $B_0, \ldots, B_d$.*

(ii) *The matrix G_r is the Gram matrix with respect to n vectors in $\mathbb{E}^{f_r}$ which span an f_r−dimensional integral lattice Λ_r.*

(iii) *If the rows of G_r are all distinct, then the automorphism group of $\mathcal{A}$ injects into the automorphism group of Λ_r.*

(iv) *If a prime p divides the determinant of Λ_r, then p divides the integer λ_r.*

Proof. — (i) We have by definition $A_i(\lambda_r E_r) = A_i(\sum \gamma_{r,j} A_j) \in \mathbb{C}E_r = \mathbb{C}(\sum \gamma_{r,j} A_j)$. Using Lemma 1.3 this implies that $\mathbb{C}\sum \gamma_{r,j} B_j$ is an ideal of the complex matrix algebra spanned by $B_0, \ldots, B_d$.

(ii) Apply Proposition 1.1 to G_r.

(iii) By Remark 1.2 the lattice Λ_r is the lattice $\frac{1}{\sqrt{\lambda}} \sum \mathbb{Z} s_i$ where $s_1, \ldots, s_n$ are the row-vectors of G_r. The automorphism group of $\mathcal{A}$ permutes $s_1, \ldots, s_n$ and this action extends to a linear isometry of $\mathbb{E}^{f_r} = \Lambda_r \otimes_{\mathbb{Z}} \mathbb{R}$. Since the vectors $s_1, \ldots, s_n$ are all distinct, this defines an injective homomorphism from $\mathrm{Aut}(\mathcal{A})$ into $\mathrm{Aut}(\Lambda_r) \subset O(\mathbb{E}^{f_r})$.

(iv) If p divides $\det(G_r)$ the p−rank of G_r is strictly smaller than f_r. Since the characteristic polynomial of the integral matrix G_r is $(x - \lambda_r)^{f_r} x^{n-f_r}$, the prime p divides λ_r. $\square$

Remark 2.2. — The lattice Λ_r tells something about the position of the r−th subspace V_r of $\mathcal{A}$ in $\frac{1}{\sqrt{\lambda}}\mathbb{Z}^n$. Two natural questions are: What is the finite index of the pair of lattices

$$\left(\frac{1}{\sqrt{\lambda}}\mathbb{Z}^n \cap V_r\right) \subset \Lambda_r = \frac{1}{\sqrt{\lambda}} \sum \mathbb{Z} s_i\,?$$

Is the lattice $\sqrt{\lambda}_r \mathbb{Z}^n$ included in $\Lambda_r = \dfrac{1}{\sqrt{\lambda}} \sum \mathbb{Z} s_i$?

The following proposition gives a partial answer about the set of lattices constructed by using Proposition 2.1.

PROPOSITION 2.3. — *Let Λ be an integral lattice with automorphism group G. Suppose that there exists $\lambda \in \Lambda$ such that the orbit $G.\lambda$ generates Λ. Then there exists an association scheme $\mathcal{A}$ with automorphism group G such that the Gram matrix F with respect to $G.\lambda$ is an element of $\mathcal{A}$. Moreover, if the representation of G on $\Lambda \otimes_{\mathbb{Q}} \mathbb{R}$ is irreducible over the reals, then the matrix F is proportional to a minimal rational idempotent of $\mathcal{A}$.*

Proof. — Construct $\mathcal{A}$ by applying Proposition 1.5 to the permutation representation of G on the set $S = G.\lambda$. The matrix F defined by $F_{x,y} = \langle x, y \rangle$ for $x, y \in S$ belongs then obviously to $\mathcal{A}$. Since the representation of G on $\Lambda \otimes_{\mathbb{Q}} \mathbb{R}$ is irreducible over the reals and since the eigenspaces of F are preserved under this action, the matrix F can have only one non-zero $G-$invariant eigenspace. It is hence proportional to a minimal idempotent of $\mathcal{A}$. □

3. A unimodular lattice in dimension 28.

In this section we construct our basic example: a unimodular lattice in dimension 28.

We consider the finite field $\mathbb{F}_3$ with 3 elements. Let $V = \mathbb{F}_3^6$ be the vector space of dimension 6 over $\mathbb{F}_3$ and let ω denote the standard symplectic form over V, i.e.

$$\omega\left((x_1, x_2, x_3, x_4, x_5, x_6), (y_1, y_2, y_3, y_4, y_5, y_6)\right) = x_1 y_4 + x_2 y_5 + x_3 y_6 - (x_4 y_1 + x_5 y_2 + x_6 y_3).$$

A *Lagrangian* of V is a 3-dimensional isotropic subspace (with respect to ω). There are

$$\frac{(3^6-1)(3^5-3)(3^4-3^2)}{(3^3-1)(3^3-3)(3^3-3^2)} = 2^5 \cdot 5 \cdot 7 = 1120$$

Lagrangians (the numerator counts the number of vectors (l_1, l_2, l_3) which generate a Lagrangian subspace, the denominator counts the number of bases of a given Lagrangian). We consider them oriented, i.e. equipped with an equivalence class of basis. Two bases (l_1, l_2, l_3) and (l'_1, l'_2, l'_3) of a given Lagrangian are equivalent, i.e. define the same orientation, if there exists g in $\mathrm{SL}(3, \mathbb{F}_3)$ (and not just in $\mathrm{GL}(3, \mathbb{F}_3)$) such that $g(l_k) = l'_k$ for $l = 1, 2, 3$. Since every Lagrangian has two possible orientations there are 2240 oriented Lagrangians. The *symplectic group* of V is by definition the group

$$\mathrm{Sp}(6, \mathbb{F}_3) = \{g \in \mathrm{GL}(6, \mathbb{F}_3) \mid \omega(gv, gw) = \omega(v, w) \text{ for all } v, w \in V\}.$$

This group admits an outer automorphism given by $g \longmapsto \tau g \tau$ where $\tau \in \mathrm{GL}(6, \mathbb{F}_3)$ is defined by

$$\tau(x_1, x_2, x_3, x_4, x_5, x_6) = (x_1, x_2, x_3, -x_4, -x_5, -x_6).$$

In particular, τ satisfies $\omega(\tau x, \tau y) = -\omega(x, y)$. We denote by $\mathrm{Sp}(6, \mathbb{F}_3) \cdot 2$ the group generated by $\mathrm{Sp}(6, \mathbb{F}_3)$ and by τ. We have a split exact sequence

$$1 \longrightarrow \mathrm{Sp}(6, \mathbb{F}_3) \longrightarrow \mathrm{Sp}(6, \mathbb{F}_3) \cdot 2 \longrightarrow \{\pm 1\} \longrightarrow 1$$

and the group $\mathrm{Sp}(6, \mathbb{F}_3) \cdot 2$ is the group of all *symplectic similitudes.* Since the group $\mathrm{Sp}(6, \mathbb{F}_3) \cdot 2$ acts transitively on the set of oriented Lagrangians we can apply Proposition 1.5 and we get a symmetric association scheme on five classes defined as ($\mathcal{L}$ and $\mathcal{M}$ denote oriented Lagrangians)

(0) $\mathcal{L} R_0 \mathcal{M} \iff \mathcal{L} = \mathcal{M}$,

(1) $\mathcal{L} R_1 \mathcal{M} \iff \mathcal{L} = (l_1, l_2, l_3)$ and $\mathcal{M} = (-l_1, -l_2, -l_3)$,

(2) $\mathcal{L} R_2 \mathcal{M} \iff \mathcal{L}$ and $\mathcal{M}$ intersect in a subspace of dimension 2,

(3) $\mathcal{L} R_3 \mathcal{M} \iff \mathcal{L} \cap \mathcal{M} = \mathbb{F}_3 v$ for some $v \in V \setminus \{0\}$, $\mathcal{L} = (v, l_2, l_3)$, $\mathcal{M} = (v, m_2, m_3)$ and the determinant of the matrix

$$\begin{pmatrix} \omega(l_2, m_2) & \omega(l_2, m_3) \\ \omega(l_3, m_2) & \omega(l_3, m_3) \end{pmatrix}$$

is 1 in $\mathbb{F}_3$,

(4) $\mathcal{L} R_4 \mathcal{M} \iff \mathcal{L} \cap \mathcal{M} = \mathbb{F}_3 v$ for some $v \in V \setminus \{0\}$, $\mathcal{L} = (v, l_2, l_3)$, $\mathcal{M} = (v, m_2, m_3)$ and the determinant of the matrix

$$\begin{pmatrix} \omega(l_2, m_2) & \omega(l_2, m_3) \\ \omega(l_3, m_2) & \omega(l_3, m_3) \end{pmatrix}$$

is -1 in $\mathbb{F}_3$,

(5) $\mathcal{L} R_5 \mathcal{M} \iff \mathcal{L}$ and $\mathcal{M}$ intersect in a subspace of dimension 0.

LEMMA 3.1. — *The intersection matrix B_3 of this symmetric association scheme is*

$$\begin{pmatrix} 0 & 0 & 0 & 351 & 0 & 0 \\ 0 & 0 & 0 & 0 & 351 & 0 \\ 0 & 0 & 36 & 36 & 36 & 243 \\ 1 & 0 & 8 & 6 & 120 & 216 \\ 0 & 1 & 8 & 120 & 6 & 216 \\ 0 & 0 & 13 & 52 & 52 & 234 \end{pmatrix}.$$

Proof. — Let us check for instance the entries of the row $(B_3)_{4,i}$ indexed by 4 of B_3 (rows and columns of the matrices B_j are indexed by $\{0,\ldots,5\}$).

Let $\mathcal{M}$ and $\mathcal{N}$ be the oriented Lagrangians generated by the rows of the matrices

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

It is easy to check that $\mathcal{M}R_4\mathcal{N}$. By definition of the intersection numbers, the number p_{3i}^4 (which is the entry $(4,i)$ of B_3) is the number of oriented Lagrangians $\mathcal{L}$ such that $\mathcal{L}R_3\mathcal{M}$ and $\mathcal{L}R_i\mathcal{N}$.

Let $\mathcal{L}$ be an oriented Lagrangian such that $\mathcal{L}R_3\mathcal{M}$. We have either $\mathcal{L}\cap\mathcal{M}=\mathcal{M}\cap\mathcal{N}$ or $\mathcal{L}\cap\mathcal{M}\neq\mathcal{M}\cap\mathcal{N}$.

In the first case we can assume that $\mathcal{L}$ is generated by the rows of the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & a & b & 0 & 1 & 0 \\ 0 & b & c & 0 & 0 & 1 \end{pmatrix}.$$

If $a=b=c=0$ we have $\mathcal{L}R_1\mathcal{N}$ and this occurs one time.

If the rank of the matrix $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$ is one we have $\mathcal{L}R_2\mathcal{N}$ and this occurs 8 times.

If the determinant of the matrix $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$ is 1 we have $\mathcal{L}R_3\mathcal{N}$ and this occurs 12 times.

If the determinant of the matrix $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$ is -1 we have $\mathcal{L}R_4\mathcal{N}$ and this occurs 6 times.

We have now to deal with the case where $\mathcal{L} \cap \mathcal{M} \neq \mathcal{M} \cap \mathcal{N}$. There are 12 possibilities for the line $\mathcal{L} \cap \mathcal{M}$. Using a symplectic base change we can assume that $\mathcal{L} \cap \mathcal{M} = \mathbb{F}_3(0,1,0,0,0,0)$ (but we have to keep the factor 12 in the subsequent countings).

We can hence assume that the basis of $\mathcal{L}$ is given by the rows of

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ a & 0 & b & 0 & 0 & 1 \\ c & 0 & a & 1 & 0 & 0 \end{pmatrix}.$$

If $b = 0$ we have $\mathcal{L}R_3\mathcal{N}$ and this occurs $12 \cdot 9$ times.

If $b \neq 0$ we have $\mathcal{L}R_5\mathcal{N}$ and this occurs $12 \cdot 18$ times.

Putting together, we get

$$R_1 + 8R_2 + (12 + 12 \cdot 9)R_3 + 6R_4 + 12 \cdot 18R_5$$

(with a hopefully obvious abuse of notation) and this corresponds to the entries of the row of B_3 indexed by 4. $\square$

The matrices A_3 and B_3 have the same eigenvalues (Lemma 1.3) which are given below together with their multiplicities for the matrix A_3 (which is of order 2240).

The eigenvalues, multiplicities (for A_3) and coordinates $\frac{1}{\lambda_r}(\gamma_{r,0}, \ldots, \gamma_{r,5})$ for the rational idempotents $\frac{1}{\lambda_r}\sum \gamma_{r,i}A_i$ are given in the following table:

eigenvalue	multiplicity	idempotent
351	1	$\frac{1}{2240}$ (1, 1, 1, 1, 1, 1)
39	105	$\frac{1}{576}$ (27, 27, -9, 3, 3, -1)
15	195	$\frac{1}{4032}$ (351, 351, 99, 15, 15, -13)
-9	819	$\frac{1}{2880}$ (1053, 1053, -27, -27, -27, 13)
3	1092	$\frac{1}{240}$ (117, -117, 0, 1, -1, 0)
-117	28	$\frac{1}{240}$ (3 -3, 0, -1, 1, 0)

(the eigenvalues, multiplicities for the adjacency matrix A_3 and idempotents can be computed with a symbolic computer algebra system using the matrix B_3). We have

THEOREM 3.2. — *The matrix $G = 3A_0 - 3A_1 - A_3 + A_4$ is the Gram matrix with respect to the set of all vectors of norm 3 of a 28−dimensional unimodular integral lattice Λ. The lattice Λ is indecomposable and has* *no roots. Its automorphism group is the group* $\mathrm{Sp}(6, \mathbb{F}_3) \cdot 2$ *of order* 18 341 406 720 *of the symplectic space* $\mathbb{F}_3^6$.

In the proof of Theorem 3.2 we will use the following definition. Let V be a symplectic space of dimension $2n$ over a finite field $\mathbb{F}_q$. A *symplectic spread* of V is a set Σ of Lagrangians in V such that every element of $V \setminus \{0\}$ is contained in a unique Lagrangian of Σ. The following construction yields a symplectic spread.

Let $\mathbb{K}$ be the extension of degre n of the field $\mathbb{F}_q$. We consider a symplectic form $\omega' : \mathbb{K}^2 \longrightarrow \mathbb{K}$ and the trace form $\mathrm{tr} : \mathbb{K} \longrightarrow \mathbb{F}_q$. Considering $\mathbb{K}$ as an $n-$dimensional vector space over $\mathbb{F}_q$ provides us with a symplectic form ω of $\mathbb{F}_q^{2n}$ by setting $\omega = \mathrm{tr} \circ \omega'$. The lines (over $\mathbb{K}$) of $\mathbb{K}^2$ can be considered as Lagrangians of $\mathbb{F}_q^{2n}$ and define a spread.

Proof of Theorem 3.2. — Proposition 2.1 shows that Λ is an integral 28−dimensional lattice.

We have to show the unimodularity of Λ. A symplectic spread of $\mathbb{F}_3^6$ provides us with 28 mutually orthogonal vectors of norm 3 in Λ (transverse pairs of oriented Lagrangians are in relation R_5 and represent hence orthogonal vectors of norm 3 in Λ). This shows that Λ contains a sublattice of rank 28 and determinant 3^{28}.

Let us now consider the set of Lagrangians which are preserved by the application τ defined by $\tau(x_1, x_2, x_3, x_4, x_5, x_6) = (x_1, x_2, x_3, -x_4, -x_5, -x_6)$. Such a Lagrangian admits a basis all whose elements are eigenvectors for τ. There are 28 such Lagrangians which we are going to describe. The application τ preserves the orientation of 14 of them and reverses the orientation of the others. The list of the 14 oriented Lagrangians preserved by τ is given by

$$\mathcal{L}_0 = \mathbb{F}_3(1,0,0,0,0,0) + \mathbb{F}_3(0,1,0,0,0,0) + \mathbb{F}_3(0,0,1,0,0,0)$$

(this is the unique Lagrangian on which τ acts as the identity) and

$$\mathcal{L}_v = \mathbb{F}_3(v,0) + \mathbb{F}_3(0,w_1) + \mathbb{F}_3(0,w_2)$$

with $v \in \mathbb{F}_3^3 \setminus \{0\}$ representing a point of $\mathbb{P}^2\mathbb{F}_3$. (The space spanned by $w_1, w_2 \in \mathbb{F}_3^3$ is uniquely determined by the requirement that $\mathcal{L}_v$ is a Lagrangian, i.e.

$$\omega((v,0),(0,w_1)) = \omega((v,0),(0,w_2)) = 0$$

and w_1, w_2 linearly independent.) We can moreover always assume that $\mathcal{L}_v$ is in relation R_4 with L_0.

Let φ be the symplectic application defined by $\varphi(e_i) = e_{i+3}$, $\varphi(e_{i+3}) = -e_i$ for $i = 1,2,3$. Set $\mathcal{L}'_0 = \varphi(\mathcal{L}_0)$ and $\mathcal{L}'_v = \varphi(\mathcal{L}_v)$. The oriented Lagrangians $\mathcal{L}'_0, \mathcal{L}'_v$ are the Lagrangians on which τ reverses the orientation.

We identify now oriented Lagrangians with the corresponding vectors of norm 3 in Λ. Since the isometry of Λ induced by τ fixes the vectors $\mathcal{L}_a$ and reverses the vectors $\mathcal{L}'_a$ (for $a \in \{0\} \cup \mathbb{P}^2\mathbb{F}_3$), they must be orthogonal. A short computation shows that the scalar product of $\mathcal{L}_a$ with $\mathcal{L}_b$ [respectively of $\mathcal{L}'_a$ with $\mathcal{L}'_b$] is equal to 3 if $a = b$ and equal to 1 otherwise $(a, b \in \{0\} \cup \mathbb{P}^2\mathbb{F}_3)$. The lattice generated by the set of vectors $\{\mathcal{L}_a, \mathcal{L}'_a\}_{a\in\{0\}\cup\mathbb{P}^2\mathbb{F}_3}$ is hence isomorphic to the the orthogonal sum of 2 isomorphic lattices M. The lattice M is generated by 14 vectors of norm 3 with scalar product equal to 1 between distinct generators. This lattice has rank 14 and determinant 2^{17}. Since the lattice Λ contains sublattices of finite indices and relatively prime determinants it must be unimodular.

Proposition 2.1 (iii) shows that $\mathrm{Sp}(6,\mathbb{F}_3)\cdot 2$ is contained in the automorphism group of Λ. One checks by computer that the orders $\mathrm{Aut}(\Lambda)$ and of $\mathrm{Sp}(6,\mathbb{F}_3)\cdot 2$ are equal, namely

$$(3^6-1)(3^5-3)(3^4-3^2)3^{3+2+1}2 = 2^{11}\cdot 3^9\cdot 5\cdot 7\cdot 13 = 18\ 341\ 406\ 720$$

(where $(3^6-1)(3^5-3)(3^4-3^2)$ is the number of linearly independent vectors (l_1, l_2, l_3) spanning a Lagrangian and where 3^{3+2+1} is the number of dual bases spanning a Lagrangian transverse to a given fixed Lagrangian, see also pages 110-113 in [Atlas]).

The representation of $\mathrm{Sp}(6,\mathbb{F}_3)\cdot 2$ on $\Lambda\otimes_{\mathbb{Z}}\mathbb{Q}$ is absolutely irreducible (See Section 4 below). Hence Λ is indecomposable. Let us now suppose that Λ contains a non-empty root system R. The irreducibility of the representation of $\mathrm{Aut}(\Lambda)$ implies that R is of rank 28 and that all irreducible components of R are isomorphic to some irreducible root system R_1. The group $\mathrm{Sp}(6,\mathbb{F}_3)$ injects hence into $\mathrm{Aut}(R) = \mathcal{S}_l \ltimes \mathrm{Aut}(R_1)$ where l is the number of irreducible components of R. Since $\mathrm{Sp}(6,\mathbb{F}_3)/\{\pm 1\}$ has no proper subgroup of index less than 364 (see [Atlas], page 113), $\mathrm{Sp}(6,\mathbb{F}_3)$ leaves all components of R invariant. Since the restriction of $\mathrm{Aut}(\Lambda)$ to $\mathrm{Sp}(6,\mathbb{F}_3)$ remains irreducible over $\mathbb{Q}$, the root system R is itself irreducible and is hence of the form A_{28}, B_{28} or D_{28}. We have hence an injective homomorphism of $\mathrm{Sp}(6,\mathbb{F}_3)$ into $\mathrm{Aut}(R)$. This implies the existence of a proper subgroup of index at most 29 in $\mathrm{Sp}(6,\mathbb{F}_3)/\{\pm 1\}$ and this is a contradiction. □

Remarks. — (i) Theorem 3.2 can also be proven by computer. Such a proof is not very enlightening but claims such as the unimodularity of Λ or the fact that Λ has no roots can easily be checked on a Gram matrix. The determination of the automorphism group is more painfull. One can do this by computing the isotropy of some sublattices in Λ and putting the results together.

(ii) The lattice Λ of Theorem 3.2 can be shown to be isomorphic to the lattice

$$\{z \in \mathbb{Z}^{28} \mid \langle z, v\rangle \in \mathbb{Z}\} + \mathbb{Z}v$$

where $v \in \mathbb{Q}^{28}$ is the vector

$$v = \frac{1}{113}(1,2,4,7,8,9,-102,13,14,15,16,18,22,25,\\ 26,28,30,31,32,36,41,44,49,50,51,52,53,56).$$

Moreover the lattice Λ can also be constructed starting from a selfdual code in $\mathbb{F}_3^{28}$. This follows from the fact that Λ contains 28 pairs of vectors of norm 3 which are mutually orthogonal. In fact, it can be shown that every set of 28 such vectors comes from a spread in $\mathbb{F}_3^6$.

(iii) The lattice Λ cannot be endowed with a hermitian structure over the Eisenstein integers. Indeed, Λ would then admit an automorphism of order 3 without non-zero fixed point. The Atlas shows that such an automorphism does not exist.

4. The lattice Λ and the Weil representation of $\mathrm{Sp}(6, \mathbb{F}_3) \cdot 2$.

The group $\mathrm{Aut}(\Lambda) = \mathrm{Sp}(6, \mathbb{F}_3) \cdot 2$ operates linearly on $\mathbb{Q}^{28} = \Lambda \otimes_{\mathbb{Z}} \mathbb{Q}$. This representation is closely related to the Weil representations of $\mathrm{Sp}(6, \mathbb{F}_3)$.

In this section, p is a prime with $p \equiv 3 \pmod 4$ and $n \equiv 1 \pmod 2$. Let A be a non-degenerate symplectic space of dimension $2n$ over the finite field $\mathbb{F}_p$ and let $G = \mathrm{Sp}(A) = \mathrm{Sp}(2n, \mathbb{F}_p)$ be the symplectic group of A. The group $G \cdot 2$, obtained by extending G with the outer automorphism (of order 2) defined by τ can be identified with the subgroup of the symplectic similitudes $\mathrm{CSp}(A)$ satisfying $\omega(\sigma u, \sigma v) = \pm\omega(u, v)$. Fix a splitting $A = B \oplus B'$ with B and B' two Lagrangians of A. For each non-trivial character $\psi : \mathbb{F}_p^* \longrightarrow \mathbb{C}^*$ there exists a representation W_ψ (the Weil representation) of dimension p^n in which G operates on all functions

$B \longrightarrow \mathbb{C}$. This representation W_ψ is the direct sum of two irreducible representations

$$W_\psi = W_\psi^+ + W_\psi^-$$

with dimensions $\dim(W_\psi^+) = \dfrac{p^n+1}{2}$ and $\dim(W_\psi^-) = \dfrac{p^n-1}{2}$. The representations $W_\psi^\pm$ are defined over $\mathbb{Q}(\sqrt{-p})$ (see [Gr], [Ge], [Wa]). A symplectic similitude τ, such that $\omega(\tau u, \tau v) = -\omega(u,v)$ permutes the representations $W_\psi^\pm$ with $W_{\overline{\psi}}^\pm$ (where $\overline{\psi}$ denotes the complex conjugate to ψ) and we get two rational, absolutely irreducible representations $X^\pm = W_\psi^\pm + W_{\overline{\psi}}^\pm$ of $\mathrm{Sp}(A)\cdot 2$ of degrees $p^n \pm 1$. Gross has proved in [Gr] that the representation W^- of $\mathrm{Sp}(A)$ is globally absolutely irreducible (remains irreducible $\pmod q$ for all prime ideals q in $\mathbb{Q}(\sqrt{-p})$) and has developped a theory of lattices in such spaces.

Our lattice Λ lives in X^+ (for $n=3, p=3$). Unfortunately, the representations W^+ and X^+ are not globally absolutely irreducible (at the prime 2 we have $W^+ \equiv 1 + W^- \pmod 2$), so that we cannot apply the general theory of Gross.

Still it seems that the lattice Λ is the beginning of the series of interesting lattices on $X_{n,p}^+$. We hope to return to these lattices latter. Some of these lattices have recently been studied by R. Scharlau and P.H. Tiep, see [ST].

5. Acknowledgements.

We thank Eiichi and Etsuko Bannai, P. de la Harpe and M. Kervaire for discussions and their interest in our work. The authors also thank the "Fonds National Suisse pour la Recherche Scientifique" for support during the period of this work.

BIBLIOGRAPHY

[Ar] E. Artin, Algèbre géométrique, Gauthiers-Villars, 1962.

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

[Ba] R. Bacher, Tables de réseaux entiers unimodulaires construits comme $k-$voisins de $\mathbb{Z}^n$ (Preprint), Genève, 1994.

[BCN] A.E. BROUWER, A.M. COHEN, A. NEUMAIER, Distance-Regular Graphs, Springer, 1989.

[BI] E. BANNAI, T. ITO, Algebraic Combinatorics I: Association schemes, Benjamin, 1984.

[Bo] R.E. BORCHERDS, The Leech lattice and other lattices (Thesis), Trinity College, Cambridge, 1984.

[Bo1] R.E. BORCHERDS, letter (January 1994).

[BV] R. BACHER, B. VENKOV, Réseaux entiers unimodulaires sans racine en dimension 27 et 28, preprint.

[Ge] P. GÉRARDIN, Weil representations associated to finite fields, J. Algebra, 46 (1977), 54-101.

[Gr] B.H. GROSS, Group representations and lattices, J. Amer. Math. Soc., 3 (1990), 929-960.

[ST] R. SCHARLAU, P.H. TIEP, Symplectic groups, symplectic spreads, codes and unimodular lattices, preprint.

[Th] J.G. THOMPSON, Finite groups and even lattices, J. Algebra, 38 (1976), 523-524.

[Wa1] H.N. WARD, Representations of symplectic Groups, J. Algebra, 20 (1972), 182-195.

[Wa2] H.N. WARD, Quadratic Residue Codes and Symplectic Groups, J. Algebra, 29 (1974), 150-171.

Manuscrit reçu le 21 mars 1995,
accepté le 13 juin 1995.

R. BACHER,
Université de Grenoble I
Institut Fourier,
B.P. 74
8402 St Martin d'Hères Cedex (France)

Boris VENKOV,
St. Petersbourg's Department
of the Steklov Mathematical Institute
Fontanka 27
St. Petersbourg (Russia).