

# 1. Lattices

Objektyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **48 (2002)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **23.05.2024**

## **Nutzungsbedingungen**

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

## **Haftungsausschluss**

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

The purpose of this article is to provide an indepth study of the fanning method. To do so, Venkov's fanning method is generalized to the isofan, a special isomorphism between rational bilinear form modules associated to root lattices. Some examples are given illustrating the construction of new complete even unimodular lattices from already known ones using isofans. In particular, an easy construction for a lattice that Conway and Pless found using "several processes including divination" is given. A classification of isofans concludes the paper.

The author is indebted to Helmut Koch for the hints and suggestions he has provided. Special thanks are due to Boris Venkov for the many helpful discussions concerning even unimodular lattices and to the referee for suggesting many improvements to the original version of this paper.

## 1. LATTICES

Let  $\mathbf{R}^n$  be  $n$ -dimensional euclidean space equipped with the standard scalar product

$$x \cdot y = \sum_{i=1}^n x_i y_i \text{ for all } x = (x_1, \dots, x_n), y = (y_1, \dots, y_n) \in \mathbf{R}^n.$$

A free  $\mathbf{Z}$ -module  $\Lambda \subset \mathbf{R}^n$  of rank  $k := \dim_{\mathbf{R}} \mathbf{R} \otimes_{\mathbf{Z}} \Lambda$  is called a *lattice of rank  $k$* . A *basis* of a rank  $k$  lattice  $\Lambda$  is a subset  $\{\lambda_1, \dots, \lambda_k\} \subset \Lambda$  that generates  $\Lambda$  over  $\mathbf{Z}$ .

Let  $\Lambda \subset \mathbf{R}^n$  be a lattice.  $\Lambda$  is said to be *integral* if  $\lambda_i \cdot \lambda_j \in \mathbf{Z}$  for all  $\lambda_i, \lambda_j \in \Lambda$ . It is an *even* lattice if, in addition to being integral,  $\lambda^2 := \lambda \cdot \lambda \in 2\mathbf{Z}$  for all  $\lambda \in \Lambda$ . Let  $\Lambda^\# = \{x \in \mathbf{R}^n \mid x \cdot \lambda \in \mathbf{Z} \text{ for all } \lambda \in \Lambda\}$  denote the *dual lattice*. Clearly,  $\Lambda$  is integral if and only if  $\Lambda \subseteq \Lambda^\#$ .  $\Lambda$  is called *unimodular* if in fact  $\Lambda = \Lambda^\#$ . Thus, an even unimodular lattice is a self-dual lattice such that  $\lambda^2 \in 2\mathbf{Z}$  for all  $\lambda \in \Lambda$ .

Let  $\Lambda_1, \dots, \Lambda_m$  be nontrivial sublattices of the integral lattice  $\Lambda$  whose direct sum is equal to  $\Lambda$ . If  $x \cdot y = 0$  for all  $x \in \Lambda_i, y \in \Lambda_j, i \neq j$ , then  $\Lambda$  is called the orthogonal direct sum of the sublattices  $\Lambda_1, \dots, \Lambda_m$  and denoted by  $\Lambda = \Lambda_1 \oplus \dots \oplus \Lambda_m$ .  $\Lambda$  is called *decomposable* if there exists such an orthogonal direct sum with  $m > 1$ , otherwise  $\Lambda$  is said to be *indecomposable*.

The *root system* of an even lattice  $\Lambda$  is the set

$$\Lambda_{\text{rt}} := \{\lambda \in \Lambda \mid \lambda^2 = 2\},$$

the elements of which are called *roots*.  $\Lambda$  is called a *root lattice* if  $\Lambda$  is

generated by its roots. Let  $\{e_1, \dots, e_n\}$  denote the standard basis of  $\mathbf{R}^n$ . The root system of an even lattice is the orthogonal direct sum of root systems of the following type, corresponding to the indecomposable root lattices [W1]:

$$A_n := \{\pm(e_i - e_j) \mid 1 \leq i < j \leq n+1, n \geq 1\},$$

$$D_m := \{\pm(e_i \pm e_j) \mid 1 \leq i < j \leq m, m \geq 3\},$$

$$E_8 := \{\pm(e_i \pm e_j), \frac{1}{2} \sum_{k=1}^8 \epsilon_k e_k \mid \epsilon_k = \pm 1, \prod_{k=1}^8 \epsilon_k = 1, 1 \leq i < j \leq 8\},$$

$$E_7 := \{v \in E_8 \mid \langle v, e_7 - e_8 \rangle = 0\},$$

$$E_6 := \{v \in E_8 \mid \langle v, e_7 - e_8 \rangle = 0 \text{ and } \langle v, e_6 - e_7 \rangle = 0\}.$$

The root system of an even lattice is said to be *complete* (in  $\Lambda$ ) if the lattice generated by  $\Lambda_{\text{rt}}$  has finite index in  $\Lambda$ . In this case, we will call  $\Lambda$  a *complete lattice*.

In general, one wants to determine the finitely many isometry classes of even unimodular lattices of a given rank. These isometry classes have been determined for ranks up to 24. Since the rank of even unimodular lattices is known to be divisible by 8, the next rank of interest is 32. There are millions of isometry classes of rank 32 even unimodular lattices. Instead of classifying all isometry classes, several authors have restricted their attention to the isometry classes of *complete* even unimodular lattices of rank 32.

When dealing with complete even unimodular lattices, it is convenient to classify the lattices according to their root systems. Beginning with a candidate root system  $R$ , the goal is to construct all isometry classes of even unimodular lattices  $\Lambda$  such that  $\Lambda_{\text{rt}} = R$ . To do that, it is helpful to associate a code to the lattice generated by  $\Lambda_{\text{rt}}$ , which can be achieved in the following manner.

Assume that  $\Lambda$  is a complete integral lattice in  $\mathbf{R}^n$ . Let  $R = \Lambda_{\text{rt}}$ , and let  $\mathbf{R}$  denote the lattice generated by  $R$ . By definition,  $\mathbf{R} \subseteq \Lambda$  is a sublattice of finite index and  $\mathbf{R} \subseteq \Lambda \subseteq \Lambda^\# \subseteq \mathbf{R}^\#$ . Let  $\pi: \mathbf{R}^\# \rightarrow \mathbf{R}^\#/\mathbf{R}$  be the natural projection of  $\mathbf{R}^\#$  onto the *discriminant group*  $G(R) := \mathbf{R}^\#/\mathbf{R}$ , also known as the *word group*. It is a finite abelian group that inherits a nondegenerate, bilinear form

$$b_R: \mathbf{R}^\#/\mathbf{R} \times \mathbf{R}^\#/\mathbf{R} \rightarrow \mathbf{Q}/\mathbf{Z}; \quad b_R(\pi(\xi_1), \pi(\xi_2)) = \xi_1 \cdot \xi_2 \bmod \mathbf{Z}$$

for  $\xi_1, \xi_2 \in \mathbf{R}^\#$ . Thus, the discriminant group is a bilinear form module, which will be denoted by  $(G(R), b_R)$  or simply  $G(R)$  if no confusion arises.

Next, define a norm

$$\mathbf{n}_R: G(R) \rightarrow \mathbf{Q}; \quad \mathbf{n}_R(g) = \min_{\xi \in \mathbf{R}^\#} \{\xi^2 \mid \xi = \pi^{-1}(g)\}.$$

An *admissible representative system*  $\{r_1, \dots, r_k\}$  of  $G(R)$  is any representative system of  $G(R)$  such that  $r_i^2 = \mathbf{n}_R(\pi(r_i))$ ,  $1 \leq i \leq k$ . The following chart gives the discriminant groups associated to the indecomposable root lattices given earlier. It also provides an admissible representative system for each and includes information on norms.

TABLE 1

$R$	$G(R) \simeq$	admissible representative system	norm
$A_\ell$ ( $\ell \geq 1$ )	$\mathbf{Z}/(\ell+1)\mathbf{Z}$	$a_{\ell,r} = \frac{r}{\ell+1} \sum_{i=0}^{\ell-r} e_i - \frac{\ell+1-r}{\ell+1} \sum_{j=\ell-r+1}^{\ell} e_j$	$\frac{\ell(\ell-r+1)}{\ell+1}$
$D_\ell$ ( $\ell \geq 3$ )	$\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ ( $\ell$ even) $\mathbf{Z}/4\mathbf{Z}$ ( $\ell$ odd)	$d_{\ell,0} = 0$ $d_{\ell,1} = \frac{1}{2} \sum_{i=1}^{\ell} e_i$ $d_{\ell,2} = e_\ell$ $d_{\ell,3} = \frac{1}{2} \sum_{i=1}^{\ell-1} e_i - \frac{1}{2} e_\ell$	0 $\ell/4$ 1 $\ell/4$
$E_8$	0	$e_{8,0} = 0$	0
$E_7$	$\mathbf{Z}/2\mathbf{Z}$	$e_{7,0} = 0$ $e_{7,1} = \frac{1}{4}(e_1 + \dots + e_6 - 3(e_7 + e_8))$	0 $3/2$
$E_6$	$\mathbf{Z}/3\mathbf{Z}$	$e_{6,0} = 0$ $e_{6,1} = \frac{1}{3}(e_1 + \dots + e_4 - 2(e_5 + e_6))$ $e_{6,2} = -e_{6,1}$	0 $4/3$ $4/3$

The nontrivial bilinear forms are as follows:

$$b_{A_\ell}(a_{\ell,j}, a_{\ell,k}) \equiv \frac{j(\ell+1-k)}{\ell+1} \pmod{\mathbf{Z}}, \quad 0 \leq j \leq k \leq \ell;$$

$$b_{D_\ell}(d_{\ell,j}, d_{\ell,0}) \equiv 0 \pmod{\mathbf{Z}}, \quad 0 \leq j \leq 3, \quad b_{D_\ell}(d_{\ell,k}, d_{\ell,2}) \equiv \frac{1}{2} \pmod{\mathbf{Z}}, \quad k = 1, 3,$$

$$b_{D_\ell}(d_{\ell,2}, d_{\ell,2}) \equiv 0 \pmod{\mathbf{Z}}, \quad b_{D_\ell}(d_{\ell,1}, d_{\ell,3}) \equiv \frac{\ell-2}{4} \pmod{\mathbf{Z}},$$

$$b_{D_\ell}(d_{\ell,k}, d_{\ell,k}) \equiv \frac{\ell}{4} \pmod{\mathbf{Z}}, \quad k = 1, 3;$$

$$b_{E_7}(e_{7,j}, e_{7,0}) \equiv 0 \pmod{\mathbf{Z}}, \quad j = 0, 1, \quad b_{E_7}(e_{7,1}, e_{7,1}) \equiv \frac{1}{2} \pmod{\mathbf{Z}};$$

$$b_{E_6}(e_{6,j}, e_{6,0}) \equiv 0 \pmod{\mathbf{Z}}, \quad j = 0, 1, 2, \quad b_{E_6}(e_{6,k}, e_{6,k}) \equiv \frac{1}{3} \pmod{\mathbf{Z}}, \quad k = 1, 2,$$

$$b_{E_6}(e_{6,1}, e_{6,2}) \equiv \frac{2}{3} \pmod{\mathbf{Z}}.$$

Note that the index of each root system  $R$  in the chart indicates the rank of the indecomposable root lattice  $\mathbf{R}$ . (To simplify the terminology, set  $\text{rk } R := \text{rk } \mathbf{R}$ .) It is easy to verify that  $(G(D_3), b_{D_3}) \simeq (G(A_3), b_{A_3})$ , so that these two bilinear form modules can be identified with one another. Note also that  $G(2A_1) \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \simeq G(D_{2k})$ . The norms of the elements in  $G(2A_1)$  are  $0, \frac{1}{2}, 1, \frac{1}{2}$ . These would be the norms of the elements of  $G(D_2)$  if  $D_2$  existed as a root system. Let  $a_{1,1}^1$  denote the nontrivial representative of the first copy of  $G(A_1)$  and  $a_{1,1}^2$  that of the second copy. Set  $d_{2,1} := a_{1,1}^1$ ,  $d_{2,2} := a_{1,1}^1 + a_{1,1}^2$ ,  $d_{2,3} := a_{1,1}^2$ . It is now easy to check that the bilinear form  $b = b_{2A_1}$  for  $2A_1$  has the same values as a bilinear form for  $D_2$  would under this identification. Thus,  $D_2$  will often be used to denote  $2A_1$  when it is convenient.

If  $\Lambda_1, \Lambda_2 \subset \mathbf{R}^n$  are mutually orthogonal, finitely generated  $\mathbf{Z}$ -submodules of  $\mathbf{R}^n$ , then  $(\Lambda_1 \oplus \Lambda_2)^\# = \Lambda_1^\# \oplus \Lambda_2^\#$ , where  $\oplus$  denotes the orthogonal direct sum. Thus, the discriminant groups are just orthogonal direct sums of the discriminant groups described above. In particular, if we restrict ourselves to the case of root systems of the form  $R = \alpha_1 A_1 + \sum_{i=1}^k \delta_{2k} D_{2k} + \varepsilon_7 E_7$ , resp.  $R = \alpha_2 A_2 + \varepsilon_6 E_6$ , then  $G(R)$  is isomorphic to  $\mathbf{F}_2^n$ , resp.  $\mathbf{F}_3^n$ .

Let  $\Lambda$  be a complete integral lattice, set  $H = \pi(\Lambda)$ ,  $H^\perp = \pi(\Lambda^\#)$ . Note that

$$H^\perp = \{x \in G(\Lambda_{\text{rt}}) \mid b_{\Lambda_{\text{rt}}}(x, h) = 0 \text{ for all } h \in H\}.$$

Because  $\Lambda$  is integral,  $H \subseteq H^\perp$ . Thus,  $H$  is self-orthogonal with respect to the bilinear form  $b$  of  $G := G(\Lambda_{\text{rt}})$ . Furthermore,  $H = H^\perp$  if and only if  $\Lambda = \Lambda^\#$  (i.e.,  $\Lambda$  is unimodular), and in this case  $H$  is referred to as an *isotropic subgroup* of  $G$  with respect to  $b$ , otherwise known as a *metabolizer*.  $\Lambda$  will be an even unimodular lattice if and only if  $H = H^\perp$  and  $\mathbf{n}(g)$  is an even integer for all  $g \in G$ .

Beginning with the root system  $R$ , each isotropic subgroup  $H \subset G(R)$  leads to the even unimodular lattice  $\Lambda = \pi^{-1}(H)$ . It is not necessary that  $\Lambda_{\text{rt}} = R$  because an additional root arises if the norm of some element of  $H$  is 2. Since the objective is to construct the even unimodular lattices with a given root system, it is sufficient to consider only those isotropic subgroups  $H$  for which  $\mathbf{n}(h)$  is an even integer  $\neq 2$  for all  $h \in H$ . Such isotropic subgroups will be called *admissible isotropic subgroups*.

An observation aids in determining the isometry classes of complete even unimodular lattices. Let  $\Lambda$  be a complete even lattice in  $\mathbf{R}^n$  and  $R = \Lambda_{\text{rt}}$  its root system. Let  $\Gamma(R)$  be the subgroup of  $\text{Aut } G(R)$  induced by the isometry group of  $\mathbf{R}$ . There is a one-to-one correspondence between equivalence classes

of even lattices in  $\mathbf{R}^n$  with root system  $R$  and  $\Gamma(R)$ -orbits of subgroups  $H$  in  $G(R)$  with  $\mathbf{n}(h) \in 2\mathbf{Z} \setminus \{2\}$  for all  $h \in H$ . Unimodular lattices correspond to isotropic subgroups.

## 2. ISOFOLDS AND ISOFANS

Given any root system  $R$ , we want to determine whether or not a complete even unimodular lattice  $\Lambda$  exists such that  $\Lambda_{\text{rt}} = R$ . This is equivalent to determining whether or not  $(G(R), b_R)$  has an admissible isotropic subgroup. Suppose  $R'$  is another root system such that the bilinear form modules  $(G(R'), b_{R'})$ ,  $(G(R), b_R)$  are isomorphic. Let  $\varphi$  denote such an isomorphism. As  $\varphi$  is a bilinear form module isomorphism,  $b_{R'}(g'_1, g'_2) = b_R(\varphi(g'_1), \varphi(g'_2))$  for all  $g'_1, g'_2 \in G(R')$ . Recall that the bilinear forms have values in  $\mathbf{Q}/\mathbf{Z}$ , so that

$$\mathbf{n}(g') \equiv \mathbf{n}(\varphi(g')) \pmod{\mathbf{Z}} \text{ for all } g' \in G(R').$$

If  $(G(R'), b_{R'})$  has an isotropic subgroup  $H'$ , it may be possible to use  $H'$  to construct an admissible isotropic subgroup  $H$  for  $(G(R), b_R)$ .

DEFINITION. In the notation above, let

$$\varphi: (G(R'), b_{R'}) \rightarrow (G(R), b_R)$$

be an isomorphism of bilinear form modules, where  $\text{rk } R' < \text{rk } R$ . The isomorphism  $\varphi$  is called an *isofan* if

$$\begin{aligned} \mathbf{n}(g') &\equiv \mathbf{n}(\varphi(g')) \pmod{2\mathbf{Z}}, \\ \mathbf{n}(g') &\leq \mathbf{n}(\varphi(g')) \end{aligned}$$

for all  $g' \in G(R')$ . The inverse  $\varphi^{-1}$  of the isofan  $\varphi$  is called an *isofold*.

EXAMPLE 1. The simplest example of an isofan was given by Venkov [V]. Consider the root system  $D_k$ ,  $k \geq 2$ , where  $D_2$  is identified with  $2A_1$ . Recall that an admissible representative system for  $(G(D_k), b_{D_k})$  can be given by  $d_{k,0}, d_{k,1}, d_{k,2}, d_{k,3}$ , the norms of the representatives being  $0, \frac{k}{4}, 1, \frac{k}{4}$ , respectively. Thus, for any integer  $k_1$  satisfying  $k_1 \equiv k \pmod{8}$ , the norms of  $d_{k_1,i}$  and  $d_{k,i}$  differ by an integral multiple of 2 for  $0 \leq i \leq 3$ .

Let  $\varphi_{D_k}$  be the group isomorphism given by

$$\varphi_{D_k}: G(D_k) \rightarrow G(D_{k+8}); \quad d_{k,i} \mapsto d_{k+8,i} \quad (0 \leq i \leq 3).$$