Cubic rings and the exceptional Jordan algebra

N.D. Elkies
Benedict H. Gross

In a previous paper [EG], we described an integral structure (J, E) on the exceptional cone in $\mathbf{R}^{27}$, and studied the integral, even lattice $J_0 = (\mathbf{Z}E)^{\perp}$ of rank 26 and discriminant 3. In this paper, we will study ring embeddings $f:\ A \to J$ of totally real cubic rings A into J, mapping the identity element 1 of A to the polarization $E = f(1)$ of J.

We first show how such an embedding gives rise to an integral, even lattice $L = A^{\perp}$ of rank 24, as well as to a holomorphic Hilbert modular form $F(\underline{\tau})$ of weight (4,4,4) for the discrete group $\mathrm{SL}_2(A) \subset \mathrm{SL}_2(\mathbf{R})^3$. We then establish some general results on the lattice L and the form $F(\underline{\tau})$. In particular, when the discriminant of A is a square, we show there is a Niemeier lattice M between L and its dual lattice $L^{\vee}$, which is determined by the embedding $f:\ A \to J$.

We then give some examples. In particular, when $A = \mathbf{Z}[\cos(2\pi/7)] = \mathbf{Z}[\alpha]/(\alpha^3 + \alpha^2 - 2\alpha - 1)$ is the Dedekind domain of discriminant $D = 49$, and when $A = \{(a, b, c) \in \mathbf{Z}^3 : a \equiv b \equiv c \pmod 2\} = \mathbf{Z} + 2\mathbf{Z}^3$ has discriminant $D = 16$, the embedding f is unique up to conjugation by the finite group $\mathrm{Aut}(J, E)$. In these cases, we determine the lattices L and M, and the Hilbert modular form $F(\underline{\tau})$.

In chapter 5.7 of his thesis [B], Borcherds proved that J_0 is characterized by the following properties: it is an even integral lattice of rank 26, discriminant 3, and minimal norm 4. His proof requires detailed knowledge of the Lorentzian lattice $\mathrm{II}_{25,1}$. But one can also prove this uniqueness result using only theta functions and elementary Euclidean arguments, somewhat in the spirit of Conway's characterization [C] of the Leech lattice by its rank, discriminant, and minimal norm. Starting from any even lattice $L \subset \mathbf{R}^{26}$ of discriminant 3 and minimal norm 4, the proof examines the configuration of minimal vectors of L and its dual, showing that L shares further combinatorial properties with J_0 until L is forced to coincide with J_0. Most of these properties are also needed in our investigation of the algebra J; in particular, the Niemeier lattice for $D = 16$ arises naturally in the course of the uniqueness proof. Thus several steps in that proof also provide alternative explanations for facts about J and J_0 that we used to analyze embeddings of cubic rings. In the final section of our paper we indicate these steps of the proof; a fuller treatment of that uniqueness proof will appear elsewhere.

It is a pleasure to thank Wee Teck Gan for his help, and Richard E. Borcherds for a copy and discussion of his thesis. The work of the first-named author is supported in part by the Packard Foundation.

Table of Contents

1. The integral structure (J, E)

In this section, we recall the results from [EG] which we will need. Let $R \subset \mathbf{O}$ be the Coxeter order in Cayley's octonion algebra [EG, (5.1)] and let β in R be defined by

$$\beta = -\frac{1}{2} + \frac{1}{2}(e_1 + e_2 + \cdots + e_7). \tag{1.1}$$

Let J be the $\mathbf{Z}$-lattice, of rank 27, consisting of the 3×3 Hermitian symmetric matrices over R. (This lattice was denoted L in [EG], where J was used for the real vector space containing the lattice, here denoted $J \otimes \mathbf{R}$.) An element B of J has the form

$$B = \begin{pmatrix} a & z & \overline{y} \\ \overline{z} & b & x \\ y & \overline{x} & c \end{pmatrix}$$

with a, b, c in $\mathbf{Z}$ and x, y, z in R. In particular, we define the element E in J by [EG, (5.4)]:

$$E = \begin{pmatrix} 2 & \beta & \overline{\beta} \\ \overline{\beta} & 2 & \beta \\ \beta & \overline{\beta} & 2 \end{pmatrix}. \tag{1.2}$$

The function [EG, (1.7)]

$$d(B) = abc + \mathrm{Tr}(xyz) - ax\overline{x} - by\overline{y} - cz\overline{z} \tag{1.3}$$

defines a cubic form

$$d: \ J \to \mathbf{Z}.$$

This gives a symmetric trilinear form (B, B', B'') with $(B, B, B) = 6d(B)$. Since $\beta\overline{\beta} = 2$ and $\mathrm{Tr}(\beta^3) = 5$, we find that $d(E) = 1$. Since E is also positive definite [EG, (1.12)], it defines a polarization of J. The finite group $\mathrm{Aut}(J, d, E)$ has order $2^{12}3^5 7^2 13$, and is isomorphic to ${}^3D_4(2).3$ [EG, (7.7)].

From E and the cubic form, we obtain a linear form on J:

$$T(B) = \frac{1}{2}(E, E, B) = 2(a + b + c) + \mathrm{Tr}(x\beta) + \mathrm{Tr}(y\beta) + \mathrm{Tr}(z\beta) \tag{1.3}$$

We also obtain two symmetric bilinear forms on J:

$$\begin{aligned}(B,B') &= (E,B,B')\\ \langle B,B'\rangle &= -(B,B')+T(B)T(B').\end{aligned}$$

The first is even, of signature (1, 26) and discriminant 2. The second is positive definite and unimodular [EG, (7.2)]. We have

$$\langle B,B\rangle \equiv \langle E,B\rangle = T(B) \pmod 2.$$

On the lattice of rank 26:

$$\begin{aligned}J_0 &= \{B\in J : T(B)=0\}\\ &= \{B\in J : \langle B,E\rangle = 0\}\\ &= \{B\in J : (B,E)=0\}\end{aligned}$$

we have the formula

$$(B,B') = -\langle B,B'\rangle.$$

(This lattice was denoted L_0 in [EG, §8].) It is even, of discriminant 3, and has no roots [EG, (8.4)]. Its theta function was determined in [EG, (8.7)].

Recall that the Jordan roots S in J are the matrices of rank 1 [EG, (1.8)] which satisfy $T(S)=2$. There are $819 = 3^2\,7\cdot 13$ Jordan roots, permuted transitively by the group $\mathrm{Aut}(J,d,E)$ [EG, (7.8)]. If S is a fixed Jordan root, then

$\langle S,S'\rangle =$	4	2	1	0
for precisely	1	288	144	18

Jordan roots S' [EG, (8.9)]. Moreover, the 18 roots S' orthogonal to S come in 9 pairs (S',S''), with $\langle S',S''\rangle = 0$ and

$$2E = S + S' + S''.$$

These are the "root triples" containing S [EG, (7.8)]. If S' and T' are orthogonal to S, with $S'\neq T'$ and $\langle S',T'\rangle \neq 0$, then $\langle S',T'\rangle = 2$. Indeed,

$$4 = \langle 2E,T'\rangle = 0 + \langle S',T'\rangle + \langle S'',T'\rangle,$$

so $\langle S',T'\rangle = \langle S'',T'\rangle = 2$.

In [EG, §8], we showed that the short vectors v in $J_0^\vee$ have the form

$$v = \pm\left(S - \frac{2}{3}E\right)$$

where S is a Jordan root. From this, we shall determine all elements B in J with $\langle B, B\rangle \le 4$.

Proposition 1.4. *If $\langle B, B\rangle = 0$, then $B = 0$. There are no B in J with $\langle B, B\rangle = 1$ or $\langle B, B\rangle = 2$. If $\langle B, B\rangle = 3$, then either*

$$B = \pm E \quad \textit{and} \quad T(B) = \pm 3,$$

or

$$B = \pm(E - S) \quad \textit{and} \quad T(B) = \pm 1$$

for a unique Jordan root S. If $\langle B, B\rangle = 4$, then either

$$B = \pm S \quad \textit{and} \quad T(B) = \pm 2$$

for a unique Jordan root S, or

$$B = S_1 - S_2 \quad \textit{and} \quad T(B) = 0$$

for a pair (S_1, S_2) of Jordan roots with $\langle S_1, S_2\rangle = 2$. There are precisely 2 representations of B as a difference of Jordan roots.

Proof. The first statement is clear, as $\langle\cdot,\cdot\rangle$ is a positive definite pairing. Since

$$\mathbf{Z}E \oplus J_0 \underset{3}{\subsetneq} J \underset{3}{\subsetneq} \frac{1}{3}\mathbf{Z}E \oplus J_0^\vee$$

we may write

$$B = \frac{a}{3}E + v$$

with v in $J_0^\vee$, and a an integer. The class of $a \bmod 3$ is determined by the class of v in $J_0^\vee/J_0$. Since $\langle E, E\rangle = 3$,

$$\langle B, B\rangle = \frac{a^2}{3} + \langle v, v\rangle.$$

If $v = 0$, then $a = 3b$ and $B = bE$. Then $\langle B, B\rangle \ge 3$, with equality iff $b = \pm 1$. Otherwise, $\langle B, B\rangle \ge 12$.

If $v \neq 0$, we have $\langle v, v \rangle \geq \frac{8}{3}$, with equality iff $v = \mp\left(S - \frac{2}{3}E\right)$ for a unique Jordan root S [EG, (8.4)]. Taking $a = \pm 1$, we obtain the elements

$$B = \pm(E - S),$$

with

$$\langle B, B \rangle = 3, \qquad T(B) = \pm 1.$$

Taking $a = \mp 2$, we obtain the elements

$$B = \mp S,$$

with

$$\langle B, B \rangle = 4, \qquad T(B) = \mp 2.$$

If $\langle v, v \rangle > \frac{8}{3}$, then $\langle v, v \rangle \geq 4$, with equality implying that v lies in J_0. We conclude the proof by showing that:

$$v = S_1 - S_2, \quad \langle S_1, S_2 \rangle = 2$$

in precisely two distinct ways. Since there are $144 \cdot 819$ short vectors v in J_0 [EG, (8.7)], and $288 \cdot 819$ ordered pairs (S_1, S_2) of Jordan roots with $\langle S_1, S_2 \rangle = 2$, we will get all the short vectors provided that we show each $S_1 - S_2$ has precisely one further representation as $T_1 - T_2$.

If $S_1 - S_2 = T_1 - T_2$ with $S_i \neq T_i$, we have

$$2 = \langle S_1, T_1 - T_2 \rangle = \langle S_1, T_1 \rangle - \langle S_1, T_2 \rangle.$$

Hence $\langle S_1, T_2 \rangle = 2$ and $\langle S_1, T_2 \rangle = 0$. Similarly, $\langle T_1, S_2 \rangle = 0$ so we have

$$S_1 + T_2 + R = 2E$$

$$T_1 + S_2 + R' = 2E$$

for Jordan roots R (orthogonal to S_1 and T_1) and R' (orthogonal to T_1 and S_2). But $S_1 + T_2 = T_1 + S_2$, so $R = R'$ is orthogonal to both (S_1, S_2) and (T_1, T_2). Conversely, such an R orthogonal to (S_1, S_2) gives us another pair (T_1, T_2). We conclude the proof, by proving the following.

Lemma 1.6. *If S_1 and S_2 are Jordan roots with $\langle S_1, S_2 \rangle = 2$, there is a unique Jordan root R orthogonal to S_1 and S_2.*

Proof. As we noted in [EG, (8,9)] (by invoking the ATLAS [A]), $\mathrm{Aut}(J_0)$ acts transitively on pairs (S_1, S_2) of Jordan roots such that $\langle S_1, S_2 \rangle = 2$. Thus the number of Jordan roots orthogonal to both S_1, S_2 is a constant independent of the choice of S_1, S_2; call this constant n. We determine n by counting in two ways the triples (S_1, S_2, R) of Jordan roots with the above inner products.

On the one hand, there are 819 choices for S_1, then 288 choices for S_2, then n choices for R, so a total of $819 \cdot 288 \cdot n$ triples.

On the other hand, there are 819 choices for R, then 18 choices for S_2, then 16 choices for S_1, so $819 \cdot 18 \cdot 16 = 819 \cdot 288$ triples.

Hence $n = 1$ as claimed.

2. Embeddings of cubic rings

Let A be a *cubic ring*, by which we mean a commutative ring with unit which is isomorphic as an additive group with $\mathbf{Z}^3$. Assume that A is *totally real*, i.e. that $A \otimes \mathbf{R} \simeq \mathbf{R}^3$. Let $\mathbf{N} : A \to \mathbf{Z}$ be the norm, which is a cubic form. Let $f : A \to J$ be a homomorphism of abelian groups. We say f is an *embedding* provided the following three conditions hold:

$$d(f(a)) = \mathbf{N}a \quad \text{for all } a \in A \tag{2.1}$$

$$f(1) = E \tag{2.2}$$

$$\text{the abelian group } J/f(A) \text{ is torsion-free} \tag{2.3}$$

The first two conditions imply that f is a ring homomorphism [GG, Lemma 2]:

$$f(a \cdot b) = f(a) \circ_E f(b) \tag{2.4}$$

where $B \circ_E B'$ is the Jordan product on $J \otimes \mathbf{Z}[1/2]$ defined in [EG, (2.15)]. The condition (2.3) implies that the embedding f does not extend to a larger order $A' \supset A$ in the étale algebra $A \otimes \mathbf{Q}$. Since only maximal orders were considered in [GG], this condition was unnecessary there.

By (2.1) and (2.2), we have

$$d(xE - f(a)) = \mathbf{N}(x - a)$$

as cubic polynomials over $\mathbf{Z}$. Hence

$$\begin{aligned} T(f(a)) &= \mathrm{Tr}(a) \\ \langle f(a), f(b) \rangle &= T(f(a) \circ_E f(b)) \\ &= \mathrm{Tr}(a \cdot b). \end{aligned}$$

Let $A^\vee \subset A \otimes \mathbf{Q}$ be the lattice dual to A under the form $\langle a, b \rangle = \mathrm{Tr}(a \cdot b)$; the finite A-module $A^\vee/A$ has order $D = \mathrm{disc}(A)$.

Let $L = f(A)^\perp$ be the subgroup, of rank 24, of elements B of J which are orthogonal to the image of A. Then $L \subset J_0$ is an even lattice, and $L^\perp = f(A)$, by (2.3).

We have inclusions

$$A \oplus L \subset J \subset A^\vee \oplus L^\vee. \tag{2.5}$$

Proposition 2.6. *The projections onto the first and second components define isomorphisms of finite abelian groups*

$$\alpha: \ J/A \oplus L \simeq A^\vee/A$$

$$\beta: \ J/A \oplus L \simeq L^\vee/L.$$

If $\beta \circ \alpha^{-1} = \gamma: \ A^\vee/A \simeq L^\vee/L$, *then for all* a, b *in* $A^\vee$, *we have*

$$\langle \gamma a, \gamma b \rangle \equiv -\langle a, b \rangle \pmod{\mathbf{Z}}.$$

Proof. We have $(A \oplus L)^\vee = A^\vee \oplus L^\vee$. Since J is unimodular, the index d of $A \oplus L$ in J is equal to the index d of J in $A^\vee \oplus L^\vee$. Since the maps α and β are both injective, we have $d \leq \#(A^\vee/A)$ and $d \leq \#(L^\vee/L)$. But by the above remark, $d^2 = \#(A^\vee/A) \cdot \#(L^\vee/L)$. Hence the maps α and β are both isomorphisms, and we have $d = \#(L^\vee/L) = \#(A^\vee/A) = D$.

Define $t_A : J \to A^\vee$ as follows: $t_A(B)$ is the first component of B in the decomposition $J \subset A^\vee + L^\vee$. Then

$$\mathrm{Tr}(t_A(B)) = \langle 1, t_A(B) \rangle = \langle E, B \rangle = T(B) \in \mathbf{Z}. \tag{2.7}$$

3. The A-module structure on L

The lattice J_0 is even, so $q(v) = \frac{1}{2}\langle v, v\rangle$ defines a positive definite quadratic form $q: \ J_0 \to \mathbf{Z}$. In this section, we will define an A-module structure on the lattice $L = f(A)^\perp \subset J_0$, and a positive definite quadratic map of A-modules

$$(3.1) \qquad q_A: \ L \to A^\vee$$

such that $\mathrm{Tr}(q_A) = q$ on L.

The A-module structure on L is due to Springer (cf. [KMRT]). It comes from the E-adjoint map $B \mapsto B^\#$ on J (cf. [EG, (2.21)] where $B^\#$ was denoted B_E^*). This is a quadratic map, which satisfies [EG, (2.22)]:

$$\begin{aligned} B \circ_E B^\# = B^\# \circ_E B &= d(B) \cdot Eq(v) \\ &= -\langle v^\#, E\rangle \qquad v \in J_0 \ . \end{aligned}$$

There is a similar map $a \mapsto a^\#$ on A, with $a \cdot a^\# = \mathbf{N}(a)$, and if $f: A \to J$ is an embedding we have $f(a^\#) = f(a)^\#$.

The Freudenthal product $B \times C$ is the symmetric bilinear map $J \times J \to J$ defined by the formulas

$$\begin{aligned} B \times C &= (B + C)^\# - B^\# - C^\# \\ &= 2(B \circ_E C) - T(B)C - T(C)B + (B, C)E \ . \end{aligned}$$

Note that $E \times C = -C$. A key identity, which can be verified using [EG, (2.15)] is the inner product formula

$$\langle B \times C, D\rangle = \langle B, C \times D\rangle.$$

For $a \in A$ and $v \in L$, we define $a \cdot v$ in L by the formula

$$a \cdot v = -(f(a) \times v).$$

This lies in $L = f(A)^\perp$, as for any $b \in A$

$$\begin{aligned} \langle f(b), a \cdot v\rangle &= -\langle f(b), f(a) \times v\rangle \\ &= -\langle f(b) \times f(a), v\rangle \\ &= -\langle f(b \times a), v\rangle \\ &= 0. \end{aligned}$$

It endows L with an A-module structure (the relevant identities can be checked for the action of $A \otimes \mathbf{R}$ on $L \otimes \mathbf{R}$, as in [EG, §1–3]).

Now for $v \in L \subset J \subset A^\vee + L^\vee$, write

$$\left\{ \begin{array}{c} v^\# = -q_A(v) + \beta(v), \quad \text{with} \\ q_A : L \to A^\vee \\ \beta : L \to L^\vee \end{array} \right. \tag{3.3}$$

Again, by extending scalars to $\mathbf{R}$, one can check that q_A is a quadratic form: $q_A(a \cdot v) = a^2 \cdot q_A(v)$, and $\langle v, w \rangle_A = q_A(v+w) - q_A(v) - q_A(w)$ is a bilinear form with values in $A^\vee$. Moreover,

$$\mathrm{Tr}\, q_A(v) = -T(v^\#) = -\langle v^\#, E \rangle = q(v).$$

From this it follows that $L^\vee$ is also an A-module inside $L \otimes \mathbf{Q}$. Indeed $L^\vee = \mathrm{Hom}(L, \mathbf{Z})$ under $\langle \cdot, \cdot \rangle$, so

$$L^\vee = \mathrm{Hom}_A(L, A^\vee) \tag{3.4}$$

under the bilinear form $\langle \cdot, \cdot \rangle_A$. Some further identities include [KMRT, 522–523]

$$\beta(a \cdot v) = a^\# \cdot \beta(v) \qquad \text{in } L^\vee \ ,$$

as well as the formula for the cubic form on L:

$$d(v) = \langle v, \beta(v) \rangle_A.$$

The right-hand side miraculously takes values in the subring $\mathbf{Z}$ of A. In particular, for $a \in A$,

$$d(a \cdot v) = \mathbf{N}a \cdot d(v).$$

Even though the quotient $L^\vee/L$ has the structure of a finite A-module, the isomorphism $\gamma : A^\vee/A \simeq L^\vee/L$ of finite abelian groups in Proposition 2.6 is *not* an A-module homomorphism, as the action of A on $A^\vee + L^\vee$ does not stabilize the sublattice J.

4. A Hilbert modular form

Let A be a totally real cubic ring. An element of $A \otimes \mathbf{R} \simeq \mathbf{R}^3$ is said to be *totally positive* if each of its three $\mathbf{R}^3$ coordinates is nonnegative. We denote by $(A \otimes \mathbf{R})_+$ the self-dual cone of such elements. Fix an embedding $f : A \to J$. Since $(A \otimes \mathbf{R})_+ = (A \otimes \mathbf{R})^2$ and $(J \otimes \mathbf{R})^2$ is the cone of positive semi-definite matrices B in $J \otimes \mathbf{R}$, f maps totally positive α in A to positive semi-definite $B = f(\alpha)$ in J.

Conversely, if $B \geq 0$ in J, then $\alpha = t_A(B)$ lies in $A_+^\vee$. To verify this, it suffices to check that $\mathrm{Tr}(\alpha\alpha') \geq 0$ for all $\alpha' \in A_+$. But

$$\mathrm{Tr}(\alpha\alpha') = \langle t_A(B), f(\alpha')\rangle = \langle B, f(a')\rangle \geq 0$$

as $f(\alpha') \geq 0$ in J.

Let $\mathcal{H}$ be the upper half-plane.

Proposition 4.1. *The holomorphic function $f : \mathcal{H}^3 \to \mathbf{C}$, defined by the convergent Fourier expansion*

$$F(\underline{\tau}) = f(\tau_1, \tau_2, \tau_3) = \sum_{\alpha \in A_+^\vee} c(\alpha) e^{2\pi i(\alpha_1\tau_1 + \alpha_2\tau_2 + \alpha_3\tau_3)}$$

with $c(0) = 1$ and

$$c(\alpha) = 240 \sum_{\substack{S \text{ in } J \\ \mathrm{rank}(S)=1 \\ t_A(S)=\alpha}} \left(\sum_{d \mid c(S)} d^3 \right) \tag{4.2}$$

is a Hilbert modular form of weight $(4,4,4)$ for $SL_2(A)$. That is:

$$F\left(\frac{a\underline{\tau} + b}{c\underline{\tau} + d}\right) = \mathbf{N}(c\underline{\tau} + d)^4 F(\underline{\tau}) \tag{4.3}$$

for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $SL_2(A)$.

In the proposition, $c(S)$ is the largest positive integer dividing S in J. If α is primitive in $A^\vee$, then $c(S) = 1$ and

$$c(a) = 240 \cdot \#\{S : \mathrm{rank}\ S = 1, t_A(S) = 2\}.$$

Writing

$$S = \alpha + v \qquad \text{in} \quad J \subset A^\vee + L^\vee$$

with $\alpha = t_A(S)$, we find

$$S^\# = (\alpha^\# - q_A(v)) + (\beta(v) - \alpha \cdot v).$$

The condition that $\operatorname{rank}(S) = 1$ is equivalent to the fact that $S^\# = 0$ [EG, (1.11)], so

$$\left\{ \begin{array}{ll} q_A(v) = \alpha^\# \text{ in} & A^\vee \otimes A^\vee \\ \beta(v) = \alpha \cdot v \text{ in} & A^\vee \otimes L^\vee \end{array} \right. \tag{4.4}$$

To prove the proposition, we begin with a description of Kim's singular form $F(Z)$ on the exceptional tube domain

$$\mathcal{D} = \{Z = X + iY, \text{ with } X \in J \otimes \mathbf{R} \text{ and } Y \in (J \otimes \mathbf{R})_+\}.$$

This is a holomorphic function $F : \mathcal{D} \to \mathbf{C}$ which satisfies

$$F(Z + B) = F(Z) \qquad B \in J$$

$$F(gZ) = F(Z) \qquad g \in \operatorname{Aut}(J, d)$$
$$F(-Z^\#/d(Z)) = d(Z)^4 F(Z).$$

It has Fourier expansion

$$F(Z) = 1 + 240 \sum_{\substack{S \geq 0 \\ \operatorname{rank}(S)=1}} \left(\sum_{d | c(S)} d^3 \right) e^{2\pi i \langle A, Z \rangle} \ . \tag{4.5}$$

These facts were established by Kim [K, p. 146] using the identity I to polarize J; in fact, any polarization E determines an isomorphic discrete subgroup of automorphisms of the exceptional domain.

The form $F(\underline{\tau})$ is simply the restriction of $F(Z)$ to the sub-tube-domain:

$$\mathcal{H}^3 = (A \otimes \mathbf{R}) + i(A \otimes \mathbf{R})_+ \underset{f}{\hookrightarrow} (J \otimes \mathbf{R}) + i(J \otimes \mathbf{R})_+ = \mathcal{D}.$$

This satisfies:

$$\begin{array}{rcll} F(\underline{\tau}+b) & = & F(\underline{\tau}) & \qquad b\in A \\ F(\alpha^2\cdot\underline{\tau}) & = & F(\underline{\tau}) & \qquad \alpha\in A^* \\ F(-1/\underline{\tau}) & = & (\mathbf{N}\underline{\tau})^4 F(\underline{\tau}). & \end{array}$$

The matrices $\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix}$, $\begin{pmatrix}\alpha & 0\\ 0 & \alpha^{-1}\end{pmatrix}$, $\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$ generate $\mathrm{SL}_2(A)$, so $F(\underline{\tau})$ has weight (4,4,4) for this discrete group acting on $\mathcal{H}^3$. Its Fourier expansion is given by

$$\begin{aligned} F(\underline{\tau}) &= 1+240\sum_{\substack{S\geq 0\\ \mathrm{rank}(S)=1}}\left(\sum_{d|c(S)} d^3\right) e^{2\pi i\ \mathrm{Tr}(t_A(S)\cdot\underline{\tau})} \\ &= 1+240\sum_{\substack{\alpha\in A_+^\vee\\ \alpha\neq 0}}\left(\sum_{\substack{\mathrm{rank}(S)=1\\ t_A(S)=\alpha}}\left(\sum_{d|c(S)} d^3\right)\right) e^{2\pi i\ \mathrm{Tr}(\alpha\cdot\underline{\tau})} \end{aligned}$$

as claimed.

5. The case $D = p^2$

In this section, we consider the case when the cubic ring A is maximal, and has discriminant $D = p^2$. Then $p \equiv 1 \pmod 3$, and A is the ring of integers in the cubic subfield of the p-th cyclotomic field. Thus p is tamely ramified in A, and lies under a unique prime $\mathfrak{p}$ of A; we have

$$(5.1) \qquad \begin{cases} pA = \mathfrak{p}^3, \\ A^\vee = \mathfrak{p}^{-2}A, \\ A^\vee/A \simeq (\mathbf{Z}/p\mathbf{Z})^2. \end{cases}$$

The quadratic space $A^\vee/A$ with form $p \cdot \mathrm{Tr}(xy) \pmod p$ is split over $\mathbf{Z}/p\mathbf{Z}$, with one of its isotropic lines the sub-A-module:

$$(5.2) \qquad \overline{N} = \mathfrak{p}^{-1}A/A.$$

Let $\overline{N}'$ be the other isotropic line in $A^\vee/A$, and let N and N' be the corresponding unimodular lattices contained in $A^\vee$. Since $\mathrm{rank}(N) = \mathrm{rank}(N') = 3$, both are isomorphic to the lattice $\mathbf{Z}^3$ [MH, p. 19]. Thus N has six short vectors $\pm e_1, \pm e_2, \pm e_3$ which satisfy $\langle e_i, e_j \rangle = \mathrm{Tr}(e_i e_j) = \delta_{ij}$, and likewise N' has six short vectors $\pm e_1', \pm e_2', \pm e_3'$ with $\mathrm{Tr}(e_i' e_j') = \delta_{ij}$ Both N and N' contain the element 1 of A, with $\langle 1, 1 \rangle = 3$. We may normalize the signs of the e_i so that $e_1 + e_2 + e_3 = 1$, as the only v with $\langle v, v \rangle = 3$ have the form $v = \pm e_1 \pm e_2 \pm e_3$.

We next determine the cubic equations satisfied by the e_i, e_i', and in the process obtain a novel proof of the existence of integers s, t such that $4p = s^2 + 27t^2$. Let σ generate the cyclic group (of order 3) of automorphisms of A. Then $\sigma(A^\vee) = A^\vee$, $\sigma(N) = N$, and $\sigma(N') = N'$. Since $\langle e_i^\sigma, e_i^\sigma \rangle = 1$, e_i^σ is a short vector not equal to $\pm e_i$. Since

$$e_1^\sigma + e_2^\sigma + e_3^\sigma = 1^\sigma = 1 ,$$

we see that σ cyclically permutes the set $\{e_1, e_2, e_3\}$. Hence $\mathrm{Tr}(e_i) = 1$. Since $\mathrm{Tr}(e_i^2) = 1$, the e_i are the three roots of a cubic equation of the form

$$(5.3) \qquad f_m(x) = x^3 - x^2 - m = 0$$

with $m = \mathbf{N}(e_i)$. The same argument shows that the e_i' are roots of a cubic equation $f_{m'}(x) = 0$ with $m' = \mathbf{N}(e_i')$. These norms m, m' are rational numbers of p-valuation -1 and -2 respectively. Now the discriminant d_μ of $f_\mu(x)$ is given by

$$d_\mu = -4\mu - 27\mu^2 = -\mu(4 + 27\mu).$$

Since A has square discriminant, d_μ must be a rational square for both $\mu = m$ and $\mu = m'$. Thus if we write $m = -m_1/p$, $m' = -m_2/p^2$ then both $m_1(4p - 27m_1)$ and $m_2(4p^2 - 27m_2)$ are squares. Now $\gcd(m_i, 4p - 27m_i)|4$ for $i = 1, 2$, since the m_i are integers not divisible by p. Thus each m_i must be either a square or twice a square. But the latter is impossible because then $4p^i - 27m_i$ would also be twice a square, yet $4p^i - 27m_i \equiv 1 \bmod 3$. Therefore each m_i is a square. Writing $m_1 = t^2$ we find that $4p - 27t^2 = s^2$ for some integer s, and have thus solved $4p = s^2 + 27t^2$; hence

$$m = -\frac{t^2}{p}, \qquad d_m = \frac{s^2t^2}{p^2}\ . \tag{5.4}$$

Next, if $m_2 = t'^2$ then $4p^2 - 27t'^2 = s'^2$ for some integer s'. Having solved $4p = s^2 + 27t^2$, we have represented p as a norm of the algebraic integer $(s+t\sqrt{-27})/2$ in the quadratic imaginary ring $\mathbf{Z}+\mathbf{Z}(1+\sqrt{-27})/2$; squaring, we obtain the representation of p^2, and conclude that $s' = st$, so

$$m' = -\frac{s^2t^2}{p^2}, \qquad d_{m'} = \frac{s^2t^2\left(\frac{s^2-27t^2}{2}\right)^2}{p^4}\ . \tag{5.5}$$

Fix an embedding $f : A \to J$, and let $L = f(A)^\perp$ as in §2. By Proposition 2.6, the map $\gamma : A^\vee/A \simeq L^\vee/L$ identifies the isotropic lines in these rank 2 quadratic spaces over $\mathbf{Z}/p\mathbf{Z}$. We let M/L be the line corresponding to N/A, and M'/L be the line corresponding to N'/A. Then M and M' are two even, integral, unimodular lattices of rank 24, which lie between L and $L^\vee$.

The abelian group $L^\vee/L$ has the structure of a finite A-module, by the results of §3.

Proposition 5.6. *The A-module $L^\vee/L$ is cyclic, and isomorphic to $A/\mathfrak{p}^2$. It has a unique non-trivial A-submodule $\mathfrak{p}(L^\vee/L)$, which is equal to the isotropic line M/L. The quadratic form q_A on M takes values in $A^\vee$, and the A-bilinear map $\langle\cdot,\cdot\rangle_A : M \times M \to A^\vee$ identifies the A-module M with $\mathrm{Hom}_A(M, A^\vee)$.*

Proof. Since $L^\vee/L$ has order p^2, it is isomorphic to either the cyclic A-module $A/\mathfrak{p}^2$, or to the A-module $(A/\mathfrak{p})^2$. In the latter case, $\mathfrak{p}L^\vee \subset L$, which we will use to derive a contradiction.

Indeed $\langle L, L^\vee\rangle_A \subset A^\vee$, so if $\mathfrak{p}L^\vee \subset L$, we have $\langle L^\vee, L^\vee\rangle_A \subset \mathfrak{p}^{-1}A^\vee$. Since $p > 2$, this means that for any $y \in L^\vee$, we would have

$$\mathrm{ord}_{\mathfrak{p}}\, q_A(y) = \mathrm{ord}_{\mathfrak{p}} \left(\frac{1}{2}\langle y, y\rangle_A\right) \geq -3.$$

On the other hand, take a in $A^\vee$ with $\mathrm{ord}_{\mathfrak{p}}(a) = -2$ and find y in $L^\vee$ such that $v = a + y$ is in J. Then $v^\# = (a^\# - q_A(y)) + (\beta(y) - a \cdot y)$ is also in J, so it has first component $a^\# - q_A(y)$ in $A^\vee$. Since $\mathrm{ord}_{\mathfrak{p}}(a^\#) = -4$, this forces $\mathrm{ord}_{\mathfrak{p}}(q_A(y)) = -4$, a contradiction.

Hence $L^\vee/L$ is cyclic, and its unique A-submodule is $\mathfrak{p}(L^\vee/L)$. We show this submodule is isotropic for the quadratic form $p \cdot q(y) : L^\vee/L \to \mathbf{Z}/p\mathbf{Z}$.

Let π be a uniformizing element at $\mathfrak{p}$ in A, and write a basis of $\mathfrak{p}(L^\vee/L)$ as $e = \pi \cdot \lambda$, with $\lambda \in L^\vee$. Then

$$p \cdot q(e) = p \cdot \mathrm{Tr}\; q_A(e) = p \cdot \mathrm{Tr}(\pi^2 q_A(y)).$$

It suffices to show that $\pi^2 q_A(\lambda)$ lies in $A^\vee$. Since $L^\vee = \mathrm{Hom}_A(L, A^\vee\rangle$ and $\mathfrak{p}^2(L^\vee) \subset L$, the quadratic form q_A takes elements of $L^\vee$ to elements in $\mathfrak{p}^{-2}A^\vee = (A^\vee)^{\otimes 2}$. Hence $\pi^2 q_A(\lambda) \in A^\vee$.

Since $\mathfrak{p}(L^\vee/L)$ is isotropic, it is equal to the line M/L or the line M'/L in $L^\vee/L$. If it is equal to M/L, then M is an A-module, $q_A : M \to A^\vee$, and $\langle , \rangle_A$ identifies M with the A-module $\mathrm{Hom}_A(M, A^\vee)$. If not, $\mathfrak{p}(L^\vee/L) = M'/L$ and $q_A : M' \to A^\vee$. From this we will derive a contradiction. Indeed, M' corresponds to the unimodular lattice $A \subset N' \subset A^\vee$, and if $a \in N' - A$ then $\mathrm{ord}_{\mathfrak{p}}(a) = -2$, $\mathrm{ord}_{\mathfrak{p}}(a^\#) = -4$. By the definition of M', we may find an element m' in M' with $a + m'$ in J. Then

$$(a + m')^\# = (a^\# - q_A(m')) + (\beta(m') - a \cdot m')$$

also lies in J. Hence its first component

$$a^\# - q_A(m')$$

lies in $A^\vee = \mathfrak{p}^{-2}A$. This contradicts the fact that $\mathrm{ord}_{\mathfrak{p}}(a^\#) = -4$ and $\mathrm{ord}_{\mathfrak{p}}(q_A(m')) \geq -2$.

Note 5.7. The results in this section extend, with minor modifications, to all cubic A of square discriminant. There is always a canonical A-module M with $L \subset M \subset L^\vee$ which is unimodular for $\langle \cdot, \cdot \rangle$ and on which $\langle \cdot, \cdot \rangle_A$ takes values in $A^\vee$.

6. The case $D = 49$

We now study the case when A is the Dedekind domain $\mathbf{Z}[\cos(2\pi/7)] = \mathbf{Z}[\alpha]/(\alpha^3+\alpha^2-2\alpha-1)$ of discriminant $D = 49$. In this case, there are $2^9 3^4 13$ embeddings $f : A \to J$, all conjugate under the finite group $\mathrm{Aut}(J, E) = {}^3D_4(2).3$ of order $2^{12}3^5 7^2 13$ [GG, §8]. The stabilizer of a fixed embedding is the subgroup $7^2 : 2A_4$ of order $2^3 3 \cdot 7^2$, and the normalizer of this subgroup is the maximal subgroup $7^2 : 2A_4 \times 3$. The quotient is the cyclic group $\mathrm{Aut}(A)$ of order 3. In particular, Galois conjugate embeddings are conjugate under $\mathrm{Aut}(J, E)$.

We may specify one embedding by taking

$$f(\alpha) = \begin{pmatrix} -1 & 1 & -\overline{\beta} \\ 1 & -1 & -\beta \\ -\beta & -\overline{\beta} & -1 \end{pmatrix}, \tag{6.1}$$

where we recall that

$$f(1) = E = \begin{pmatrix} 2 & \beta & \overline{\beta} \\ \overline{\beta} & 2 & \beta \\ \beta & \overline{\beta} & 2 \end{pmatrix},$$

and $\beta^2 + \beta + 2 = 0$. The image $f(A)$ consists of the $\mathbf{Z}$-module:

$$\begin{pmatrix} f+p+r & p-r+p\beta & f-r-r\beta \\ p-r+p\overline{\beta} & f+p+r & f+r\beta \\ f-r-r\overline{\beta} & f+r\overline{\beta} & f+p+r \end{pmatrix}$$

with (f, p, r) all integers. The element E corresponds to the triple $(0, 1, 1)$ and the element $f(\alpha)$ corresponds to the triple $(0, 0, -1)$. The trace form is $4f + 2p + r$, so $f(A^\vee)$ consists of matrices with f, p, r in $\frac{1}{7}\mathbf{Z}$ and $4f + 2p + r$ in $\mathbf{Z}$.

Since the trace form $\mathrm{Tr}(x^2)$ on A takes the values $0, 3, 5, 6, \ldots$, the six nontrivial cosets of $N/A = \mathfrak{p}^{-1}A/A$ are represented uniquely by the six short vectors n in N with $\mathrm{Tr}(n^2) = 1$. Let $L \subset M \subset L^\vee$ be the even unimodular lattice of rank 24 corresponding to the lattice N. If $\lambda \in M$ is a root, we may find a unique short vector $n \in N$ which satisfies $\mathrm{Tr}(n) = 1$ and a unique choice of sign $\pm$ such that

$$S = E \pm \lambda - n$$

is a Jordan root in J. Indeed, choose n and the sign uniquely so that the sum

$$v = n \pm \lambda \qquad \text{in} \quad A^\vee + L^\vee \tag{6.3}$$

lies in J. Since

$$\langle v, v\rangle = \langle n, n\rangle + \langle \lambda, \lambda\rangle = 1 + 2 = 3,$$

and $T(v) = \mathrm{Tr}(n) = 1$, we have

$$v = E - S$$

for a Jordan root S by Proposition 1.4. Consequently, we have shown the following

Proposition 6.4. *The number of roots λ in the Niemeier lattice M is equal to twice the number of Jordan roots S in J which satisfy $t_A(S) = 1 - n$ in $A^\vee_+$, where n is any short vector in N with* $\mathrm{Tr}(n) = 1$.

Since the three short vectors in N with $\mathrm{Tr}(n) = 1$ are Galois conjugate, and Galois conjugate embeddings of A are conjugate by $\mathrm{Aut}(J, E)$, the number of S with $t_A(S) = 1 - n$ is equal to the number of S with $t_A(S) = 1 - n^\sigma$. Hence we obtain the following.

Corollary 6.5. *Fix a short vector n in N with* $\mathrm{Tr}(n) = 1$*, and let $a = 1 - n$ be the corresponding (totally positive) element in $A^\vee_+$. Then*

$$\#\{\text{roots } \lambda \text{ in } M\} = 6 \cdot \#\{\text{Jordan roots } S \text{ in } J \text{ with } t_A(S) = a\}.$$

A similar argument works for the lattices M' and N'. Fix a short vector n' in N' with $\mathrm{Tr}(n') = 1$, and let $a' = 1 - n'$. Then

$$\#\{\text{roots } \lambda' \text{ in } M\} = 6 \cdot \#\{\text{Jordan roots } S \text{ with } t_A(S) = a'\}. \tag{6.6}$$

We can calculate these numbers by a determination of the Hilbert modular form $F(\underline{\tau})$. This has weight (4,4,4) for $\mathrm{SL}_2(A)$, and since the Galois conjugate embeddings are conjugate, is invariant under the action of $\mathrm{Aut}(A)$. One can show, using the trace formula, that the space of such forms is 2-dimensional, and is spanned by the forms E_2^2 and E_4. Here E_k is the weight

(k,k,k) Eisenstein series studied by Siegel, with the Fourier expansion [vdG, pp. 19–20]

$$E_k = \frac{1}{2^3}\zeta_A(1-k) + \sum_{\substack{a>0 \\ \text{in } A^\vee}} \left(\sum_{c|(a)\mathfrak{p}^2} (\mathbf{N}c)^{k-1} \right) q^a. \tag{6.7}$$

From the values

$$\begin{aligned} \zeta_A(-1) &= -\tfrac{1}{3\cdot 7} \\ \zeta_A(-3) &= \tfrac{79}{2\cdot 3\cdot 5\cdot 7}\ , \end{aligned}$$

we find:

$$\begin{aligned} E_2 &= -\frac{1}{2^3 3\cdot 7} + \sum_{\substack{a>0 \\ \text{in } A^\vee}} \left(\sum_{c|(a)\mathfrak{p}^2} \mathbf{N}c \right) q^a \\ E_4 &= -\frac{79}{2^4 3\cdot 5\cdot 7} + \sum_{\substack{a>0 \\ \text{in } A^\vee}} \left(\sum_{c|(a)\mathfrak{p}^2} (\mathbf{N}c)^3 \right) q^a. \end{aligned}$$

There is a unique $\mathrm{Aut}(A)$ orbit of elements $a > 0$ in $A^\vee$ with $\mathrm{Tr}(a) = 1$, represented by the squares n^2 of short vectors in N. Since the space of modular forms is two-dimensional, there is a unique form $F(\underline{\tau})$ with constant Fourier coefficient $c(0) = 1$ and coefficient $c(n^2) = 0$. Some calculation shows that this is the linear combination

$$F(\underline{\tau}) = 2^4 3\cdot 5\cdot 7\ E_2(\underline{\tau})^2 + 2^2 5\ E_4(\underline{\tau}). \tag{6.8}$$

There are five orbits of $\mathrm{Aut}(A)$ on elements $a > 0$ in $A^\vee$ with $\mathrm{Tr}(a) = 2$, and we tabulate the Fourier coefficients $c(a)$ of $F(\underline{\tau})$ on these orbits. As before, n is a short vector in N with $\mathrm{Tr}(n) = 1$, and n' is a short vector in N' with $\mathrm{Tr}(n') = 1$. We have $n^3 - n^2 + \frac{1}{7} = 0$, and $(n')^3 - (n')^2 + \frac{1}{49} = 0$ by (5.4) and (5.5). Indeed, for $p = 7$, $s^2 = t^2 = 1$.

$a > 0$ in $A^\vee$ $\mathrm{Tr}(a) = 2$	$(a)\mathfrak{p}^2$	$c(a)$ of $F(\underline{\tau})$
$2.n^2$	(2)	$240 \cdot 49$
$1 - n$	$\mathfrak{p}$	$240 \cdot 28$
$1 - n'$	1	0
$1 - n^2$	a prime of norm 13	$240 \cdot 196$
$1 - 2n + n^2$	1	0

The form $F(\underline{\tau})$ we have determined is the one that appears in §4, as that satisfies $c(0) = 1$, $c(n^2) = 0$. Hence, for $\mathrm{Tr}(a) = 2$ we have

$$c(a) = 240\#\{S = \text{Jordan roots of } J \text{ with } t_A(S) = a\}.$$

In particular, this shows that the lattice N has $6 \cdot 28 = 168$ roots, and that the lattice N' has $6 \cdot 0 = 0$ roots. Hence, as Niemeier lattices,

$$\begin{cases} N & \simeq A_6^4 \\ N' & \simeq \text{Leech lattice} \end{cases} \tag{6.9}$$

as claimed in [GG, §8]. Indeed A_6^4 is the unique Niemeier lattice with 168 roots (and Coxeter number $h = 7$), and the Leech lattice is the unique Niemeier lattice with no roots ([N], see also [V]).

7. The case $D = 16$

We treat another case, when A is the subring of index 4 in $\mathbf{Z}^3$ consisting of the triples (a, b, c) with $a \equiv b \equiv c \pmod 2$. This ring has discriminant $D = 16$, and admits an embedding $f : A \to J$ which is unique up to conjugacy by $\mathrm{Aut}(J, d, E)$. Indeed, an embedding of A is given by the images

$$(7.1) \qquad \begin{cases} f(2,0,0) = S_1 \\ f(0,2,0) = S_2 \\ f(0,0,2) = S_3 \end{cases},$$

which satisfy:

$$S_i^2 = 2S_i$$

$$S_i S_j = 0$$

$$S_1 + S_2 + S_3 = 2E.$$

Thus (S_1, S_2, S_3) forms a root triple, in the sense of [EG, §3], and by [EG, Prop. 7.8] the group $\mathrm{Aut}(J, d, E) = {}^3D_4(2).3$ of order $2^{12}3^5 7^2 13$ acts transitively on root triples, with fixer the subgroup $2^{2+3+6}.7.3$. Hence there are $2 \cdot 3^4 \cdot 7 \cdot 13 = 14742$ distinct embeddings $f : A \to J$.

Fix an embedding, and let $L = A^\perp$. Then $L^\vee/L \simeq A^\vee/A$. Since $A^\vee$ is the subgroup of $(\frac{1}{2}\mathbf{Z})^3$ consisting of triples (a, b, c) with $a + b + c$ in $\mathbf{Z}$, we find $A^\vee/A \simeq (\mathbf{Z}/4\mathbf{Z})^2$. The unimodular lattice $A \subset \mathbf{Z}^3 \subset A^\vee$ corresponds to the subgroup $(2\mathbf{Z}/4\mathbf{Z})^2$ killed by 2, and in turn yields a Niemeier lattice M between L and $L^\vee$. We will show that M is isomorphic to the Niemeier lattice whose root system is A_1^{24}, by showing that M contains precisely 48 roots.

To do this, we first determine the modular form $F(\underline{\tau})$ of weight $(4, 4, 4)$ for $\mathrm{SL}_2(A)$, defined in §4. Let $\Gamma(2) \triangleleft \mathrm{SL}_2(\mathbf{Z})$ be the subgroup of integral matrices which reduce to the identity mod 2. Then $\mathrm{SL}_2(A) \triangleleft \Gamma(2)^3$, so $F(\underline{\tau})$ has weight $(4, 4, 4)$ for $\Gamma(2)^3$, and enjoys some additional invariance properties.

Let W be the complex vector space of holomorphic modular forms of weight 4 for $\Gamma(2)$. This has dimension 3, and is spanned by the Eisenstein series at the three cusps [R, 232–235]:

$$\begin{aligned} f_1 &= \frac{1}{16} - q + 7q^2 + \dots \\ f_2 &= -q^{1/2} + 8q - 28q^{3/2} + 64q^2 + \dots \\ f_3 &= q^{1/2} + 8q + 28q^{3/2} + 64q^2 + \dots \end{aligned}$$

Here $q^{1/2} = e^{\pi i \tau}$. The form f_1 is a power series in $q = e^{2\pi i\tau}$, as is $f_2 + f_3$. The general Fourier coefficient a_n of $q^{n/2}$ is given by [R, Thm. 7.3.1]

$$\begin{aligned}
a_n &= \sum_{\substack{d|n \\ n|d \text{ even}}} (-1)^d d^3 \qquad \text{for} \quad f_1, \\
a_n &= \sum_{\substack{d|n \\ n|d \text{ odd}}} (-1)^d d^3 \qquad \text{for} \quad f_2, \\
a_n &= \sum_{\substack{d|n \\ n|d \text{ odd}}} d^3 \qquad \text{for} \quad f_3.
\end{aligned}$$

The group $\mathrm{SL}_2(\mathbf{Z})/\Gamma(2) \simeq S_3$ acts on this space by permuting the forms f_1, f_2, f_3. The unique invariant is the sum

$$\begin{aligned}
f_1 + f_2 + f_3 &= \frac{1}{16} + 15q + 135q^2 + \ldots \\
&= \frac{1}{16} E_4, \quad \text{of weight 4 for } \mathrm{SL}_2(\mathbf{Z}).
\end{aligned}$$

The space of forms of weight $(4,4,4)$ for $\Gamma(2)^3$ is isomorphic to $W \otimes W \otimes W$. This has dimension 27, and basis $f_i \otimes f_j \otimes f_k$. The group $\mathrm{SL}_2(\mathbf{Z})/\Gamma(2)$ acts diagonally, and has invariant subspace of dimension 5. A basis for the invariants is given by:

$$\begin{aligned}
g_1 &= f_1 \otimes f_1 \otimes f_1 + f_2 \otimes f_2 \otimes f_2 + f_3 \otimes f_3 \otimes f_3 \\
g_2 &= f_1 \otimes f_1 \otimes f_2 + f_1 \otimes f_1 \otimes f_3 + f_2 \otimes f_2 \otimes f_1 + f_2 \otimes f_2 \otimes f_3 \\
&\qquad + f_3 \otimes f_3 \otimes f_1 + f_3 \otimes f_3 \otimes f_2 \\
g_3 &= f_1 \otimes f_2 \otimes f_1 + f_1 \otimes f_3 \otimes f_1 + f_2 \otimes f_1 \otimes f_2 + f_2 \otimes f_3 \otimes f_2 \\
&\qquad + f_3 \otimes f_1 \otimes f_3 + f_3 \otimes f_2 \otimes f_3 \\
g_4 &= f_2 \otimes f_1 \otimes f_1 + f_3 \otimes f_1 \otimes f_1 + f_1 \otimes f_2 \otimes f_2 + f_3 \otimes f_2 \otimes f_2 \\
&\qquad + f_1 \otimes f_3 \otimes f_3 + f_2 \otimes f_3 \otimes f_3 \\
g_5 &= f_1 \otimes f_2 \otimes f_3 + f_1 \otimes f_3 \otimes f_2 + f_2 \otimes f_1 \otimes f_3 + f_2 \otimes f_3 \otimes f_1 \\
&\qquad + f_3 \otimes f_1 \otimes f_2 + f_3 \otimes f_2 \otimes f_1
\end{aligned}$$

This is precisely the space of forms of weight $(4,4,4)$ on $\mathrm{SL}_2(A)$, as $\mathrm{SL}_2(A)$ is the subgroup of $\mathrm{SL}_2(\mathbf{Z})^3$ consisting of triples of matrices with the *same* reduction mod 2.

The form $F(\underline{\tau})$ has an additional invariance property. Since the $\mathrm{Aut}(A) = S_3$ conjugate embeddings $f : A \to J$ are conjugate under $\mathrm{Aut}(J, d, E)$, the number of rank 1 S in J with $t_A(S) = a$ is equal to the number with $t_A(S) = a^\sigma$, for all $\sigma \in S_3 = \mathrm{Aut}(A)$. Hence the Fourier coefficient $c(a)$ of $F(\underline{\tau})$ is equal to $c(a^\sigma)$, for all $\sigma \in S_3$ and $a \in A_+^\vee$, and

$$F(\tau_{\sigma 1}, \tau_{\sigma 2}, \tau_{\sigma 3}) = F(\tau_1, \tau_2, \tau_3).$$

The subspace of forms of weight $(4, 4, 4)$ for $\mathrm{SL}_2(A)$ with this extra invariance property has dimension 3. As basis, we may take

$h_1 = 2^{12} g_1$	with	$c(0,0,0) = 1$
$h_2 = 2^4(g_2 + g_3 + g_4)$	with	$c(0,0,0) = 0$ $c(1,0,0) = 1$
$h_3 = -2^3 g_5$	with	$c(0,0,0) = 0$ $c(1,0,0) = 0$ $c(1/2,1/2,0) = 1$

We tabulate the coefficients of the basis elements h_i, at orbits of $\mathrm{Aut}(A)$ on $A_+^\vee$ with $\mathrm{Tr}(a) \leq 2$.

$a =$	(0,0,0)	(1,0,0)	$(\frac{1}{2},\frac{1}{2},0)$	(2,0,0)	(1,1,0)	$(\frac{1}{2},\frac{3}{2},0)$	$(\frac{1}{2},\frac{1}{2},1)$
h_1	1	-16	0	112	256	0	65536
h_2	0	1	2	8	96	56	-288
h_3	0	0	1	0	-64	28	-16

The form $F(\underline{\tau})$ has Fourier coefficients:

$$c(0,0,0) = 1$$

$$c(1,0,0) = 0$$

$$c\left(\frac{1}{2}, \frac{1}{2}, 0\right) = 0.$$

Hence, we must have

$$f = h_1 + 16h_2 - 32h_3. \tag{7.2}$$

The coefficients of F at elements a in $A_+^\vee$ with $\mathrm{Tr}(a) = 2$ are:

$$\begin{aligned} c(2,0,0) &= 240 \\ c(1,1,0) &= 16 \cdot 240 \\ c\left(\frac{1}{2}, \frac{3}{2}, 0\right) &= 0 \\ c\left(\frac{1}{2}, \frac{1}{2}, 1\right) &= 256 \cdot 240 \end{aligned}$$

Hence, there are 16 Jordan roots S with $t_A(S) = (1,1,0)$, 16 roots with $t_A(S) = (0,1,1)$, and 16 roots with $t_A(S) = (1,0,1)$.

The three nontrivial cosets of $\mathbf{Z}^3/A$ are represented by short vectors n with $\langle n, n\rangle = 1$ and $\mathrm{Tr}\, n = 1$. An argument similar to that in §6 shows that, if n is such a short vector,

$$\#\{\text{roots } \lambda \text{ in } M\} = 3\#\{\text{Jordan roots with } t_A(S) = 1 - n\} = 3 \cdot 16 = 48 .$$

This completes the proof that $N \simeq A_1^{24}$, as that is the unique Niemeier lattice with 48 roots (and Coxeter number $h = 2$; again see [N, V]).

8. The case $D = 32$

Another interesting case, which merits further study, is the cubic ring

$$A = \{(b, c + d\sqrt{2}) : b \equiv c \pmod 2\},$$

which has index 2 in the maximal order

$$A' = \mathbf{Z} + \mathbf{Z}[\sqrt{2}] \quad \text{of discriminant 8.}$$

Hence, A has discriminant $D = 32$. The embeddings $f : A \to J$ are all conjugate. To construct one, choose a triple of Jordan roots (S_1, S_2, S) with $\langle S_1, S_2 \rangle = 2$ and S orthogonal to S_1 and S_2, as in the proof of Lemma 1.6. We embed A into J by mapping

$$f(1,1) = E$$

$$f(2,0) = S$$

$$f(0, 2 + \sqrt{2}) = S_1 + S_2.$$

Since $B = S_1 + S_2$ satisfies

$$B^3 - 4B^2 + 2B = 0 \quad \text{in } J,$$

and $S \cdot B = B \cdot S = 0$, this a ring embedding.

The abelian group $A^\vee / A$ is isomorphic to $\mathbf{Z}/8 + \mathbf{Z}/4$. Indeed

$$A^\vee = \left\{ \left(\frac{b}{2}, \frac{c + d\sqrt{2}}{4} \right) : b \equiv c \pmod 2 \right\}.$$

Hence the exponent of $A^\vee / A$ is 8. The 2-torsion in $A^\vee / A$ is given by the image of the lattice

$$N = \left\{ \left(b, \frac{c}{\sqrt{2}} + d \right) \right\},$$

and $N/A \simeq \mathbf{Z}/2 + \mathbf{Z}/2$. The subgroup N/A is also isotropic for the induced pairing

$$A^\vee / A \times A^\vee / A \to \mathbf{Q}/\mathbf{Z},$$

as $\mathrm{Tr}(n^2) = \mathrm{Tr}\left(b^2, \frac{c^2}{2} + d^2 + \sqrt{2}cd\right) = b^2 + c^2 + 2d^2$ is integral, for $n \in N$.

We have $N \underset{2}{\supset} A' \underset{2}{\supset} A$. The lattice N has discriminant 2, and is isomorphic to $\mathbf{Z} + \mathbf{Z} + \mathbf{Z}(2)$. By the results of §2, the lattice $L = f(A)^{\perp}$ has index 32 in $L^{\vee}$, and contains the intermediate integral lattices

$$L \underset{2}{\subsetneq} L' \underset{2}{\subsetneq} M \subset L^{\vee}$$

corresponding to A' and N, respectively. The discriminant of M is 2. Can one determine these lattices explicitly, and identify the Hilbert modular form $F(\underline{\tau})$ inside the space of forms of weight $(4, 4, 4)$ for $\Gamma(2) \times \Gamma(\sqrt{2})$, where $\Gamma(\sqrt{2})$ is the normal subgroup of $\mathrm{SL}_2(\mathbf{Z}[\sqrt{2}])$ consisting of matrices reducing to the identity (mod $\sqrt{2}$)?

9. The uniqueness of J_0

We outline here how J_0 can be proved unique without using the Lorentzian lattice $\mathrm{II}_{25,1}$. We remark that this uniqueness result was recently used [BV] in the classification of rootless lattices in dimensions 27 and 28. We postpone to a future paper some details of the spaces of modular forms that can arise as weighted theta functions and of the reconstruction of J_0 from the Niemeier lattice with root system A_1^{24}.

Let Λ be a positive-definite even integral lattice of rank 26, discriminant 3, and minimal norm 4. To prove that Λ is isometric with J_0, we show:

Proposition 9.1 *i) Every vector of the dual lattice $\Lambda^\vee$ is either in Λ or has norm congruent to $2/3$ mod $2\mathbf{Z}$.*

ii) No vector of $\Lambda^\vee$ has norm $2/3$.

iii) The theta series of $\Lambda, \Lambda^\vee$ coincide with those of $J_0, J_0^\vee$. In particular, each of the two nontrivial cosets of Λ in $\Lambda^\vee$ has 819 vectors of minimal norm $8/3$.

iv) Those 819 vectors constitute a spherical 2-design Δ, and the $2 \cdot 819$ minimal vectors of $\Lambda^\vee$ constitute a spherical 4-design $\Delta \cup (-\Delta)$.

v) The inner product of any $w_1, w_2 \in \Delta$ is one of $8/3$, $2/3$, $-1/3$, $-4/3$. For each w_1, these inner products occur respectively for 1, 288, 512, 18 of the 819 choices of w_2.

vi) For each $i, j, k \in \{8/3, 2/3, -1/3, -4/3\}$ there exists an integer $n_{i,j}^k$, independent of Λ, such that for any $w_1, w_2 \in \Delta$ with $(a,b) = k$ the number of $w \in K$ with $(w_1, w) = i$ and $(w_2, w) = j$ is $n_{i,j}^k$.

[For part (iv), recall that a nonempty finite subset S of a sphere in $\mathbf{R}^n$ is a "spherical t-design" if, for every polynomial P on $\mathbf{R}^n$ of degree at most t, $|S|^{-1} \sum_{x \in S} P(x)$ equals the average of P over the sphere. Part (vi) is the statement that Δ is a 4-class association scheme indexed by $\{8/3, 2/3, -1/3, -4/3\}$, with parameters $n_{i,j}^k$ independent of Λ. That Δ is such an association scheme when $\Lambda = J_0$ follows from the fact that $\mathrm{Aut}(J_0)$ acts distance-transitively on Δ; but of course this argument, which we have used earlier in this paper, is not yet available to us for arbitrary Λ.]

Proof. (i) This is known to be true for any positive-definite even integral lattice Λ of discriminant 3 and rank $8n+2$. Since $[\Lambda^\vee : \Lambda] = \det(\Lambda) = 3$, we have either $v^* - w^* \in \Lambda$ or $v^* + w^* \in \Lambda$ for any $v^*, w^* \in \Lambda^\vee - \Lambda$. Thus $\langle v^*, v^* \rangle \cong \langle w^*, w^* \rangle$ mod $\mathbf{Z}$. Moreover, $3v^* \in \Lambda$, so $3\langle v^*, v^* \rangle = \langle 3v^*, v^* \rangle \in \mathbf{Z}$, and $9\langle v^*, v^* \rangle = \langle 3v^*, 3v^* \rangle \in 2\mathbf{Z}$. Thus there exists an integer c such that $\langle v^*, v^* \rangle \equiv 2c/3$ mod $2\mathbf{Z}$ for all $v^* \in \Lambda^\vee - \Lambda$. If we had $c = 0$ then $\Lambda^\vee$ would be an integral lattice, which is impossible because $\det\Lambda^\vee = 1/3 \notin \mathbf{Z}$. If $c = 2$ then we could glue $\Lambda^\vee$ to the A_2 lattice, obtaining a positive-definite even unimodular lattice of rank $8n + 4$, which is impossible. Thus $c = 1$ as claimed.

(ii) Assume on the contrary that $\langle v^*, v^*\rangle = 2/3$ for some $v^* \in \Lambda^\vee$. Let $\Lambda_1 = \Lambda \cap (\mathbf{Z}v^*)^\perp$. This is a positive-definite even integral lattice of rank 25 and discriminant $\langle v^*, v^*\rangle(\det\Lambda) = 2$ containing no vectors of norm 2. But no such lattice exists. As with J_0, but more simply, the nonexistence of Λ_1 was proved by Borcherds via $\mathrm{II}_{25,1}$ [B, Lemma 4.3.1], and can also be established using theta series without invoking hyperbolic lattices. To do this, first show as in (i) that all vectors in $\Lambda_1^\vee - \Lambda_1$ would have norm $\equiv 1/2 \bmod 2\mathbf{Z}$, and note that $\Lambda_1^\vee$ has minimal norm at least $5/2$ because if $w^* \in \Lambda_1^\vee$ has norm $1/2$ then $2w^* \in \Lambda_1$ has norm 2. Then show, as we shall do for Λ in (iii) and (iv), that $\Lambda_1^\vee$ has minimal norm $5/2$ and that its minimal vectors constitute a spherical 2-design. Thus, for any minimal vector $w_0^* \in \Lambda_1^\vee$, the average of $\langle w^*, w_0^*\rangle^2$ over all minimal vectors w^* is $(5/2)^2/25 = 1/4$. But $\langle w^*, w_0^*\rangle \in \mathbf{Z} + 1/2$ for all $w^* \in \Lambda_1^\vee$, and $\langle w_0^*, w_0^*\rangle = 5/2$. Thus each $\langle w^*, w_0^*\rangle^2 \geq 1/4$, and the inequality is strict at least for $w^* = w_0^*$. Therefore the average of $\langle w, w_0\rangle^2$ exceeds $1/4$. This contradiction proves that Λ_1 cannot exist, and thus that $\Lambda^\vee$ has no vectors of norm $2/3$.

(iii) This is in effect already proved in [EG, Prop. 8.6], in which the theta series of $J_0, J_0^\vee$ were determined using only the facts about J_0 that we assumed for Λ or proved in (i) and (ii). Since the two nontrivial cosets of Λ in $\Lambda^\vee$ are each other's image under $x \leftrightarrow -x$, each has the same number of minimal vectors; thus the theta series of $\Lambda^\vee$ also determines the number of minimal vectors in each nontrivial coset.

(iv) We use the fact that S is a t-design if and only if $\sum_{x\in S} P(x) = 0$ whenever P is a spherical harmonic of positive degree at most t. Let C be one of the nontrivial cosets of Λ in $\Lambda^\vee$, and consider the weighted theta series $\sum_{x\in C} P(x) q^{\frac{1}{2}\langle x,x\rangle}$. This is a modular form of weight $13 + \deg(P)$ for $\Gamma(3)$. Because $\Lambda^\vee$ has minimal norm $8/3$, this form vanishes at each cusp at least to the same order as $\eta(z)^{32}$, a form of weight 16. Thus if $13 + \deg(P) < 16$ then the form is identically zero. In particular, its $q^{4/3}$ coefficient vanishes; since this coefficient is the sum of $P(x)$ over the 819 minimal vectors of C, we confirm that these vectors constitute a spherical 2-design. (This is the argument we suggested in [EG, p.693]; see also the second part of (v) below.) As for the minimal vectors of $\Lambda^\vee$, the same construction yields a modular form $\vartheta(z) := \sum_{x\in\Lambda^\vee} P(x) q(z)^{\frac{1}{2}\langle x,x\rangle}$ of weight $13+\deg(P)$ for $\Gamma_0(3)$. It still vanishes at least as η^{32} at each cusp, but at the cusp $z=0$ we have $\vartheta(z) = O(q(-1/z)^2)$, not just $O(q(-1/z)^{4/3})$, because $\vartheta(-1/z)$ is proportional to $\sum_{x\in\Lambda} P(x) q(z)^{\frac{1}{2}\langle x,x\rangle}$, and Λ has minimal norm 4. This lets us conclude $\vartheta \equiv 0$ if $13+\deg(P) < 18$, and thus that $\Delta \cup (-\Delta)$, the set of minimal vectors of $\Lambda^\vee$, is a spherical 4-design as claimed. (Since this design is symmetric about the origin, it is thus automatically a 5-design as well, but we do not use this.)

v) Since $w_2 \equiv w_1 \bmod \Lambda$ we have $\langle w_1, w_2\rangle \equiv \langle w_1, w_1\rangle = 8/3 \equiv 2/3 \bmod \mathbf{Z}$. By Cauchy-Schwarz $|\langle w_1, w_2\rangle| \le 8/3$, with equality unless w_1, w_2 are proportional. Since $w_1, w_2 \in \Delta$, this equality condition is equivalent to $w_1 = w_2$. If $w_1 \ne w_2$ then $w_1 - w_2 \in \Lambda - \{0\}$, so $w_1 - w_2$ has norm at least 4, whence $\langle w_1, w_2\rangle = (|w_1|^2 + |w_1|^2 - |w_1 - w_2|^2)/2 \le (16/3 - 4)/2 = 2/3$. Likewise $w_1 + w_2$, a nonzero vector in $\Lambda^\vee$, has norm at least $8/3$, whence $\langle w_1, w_2\rangle \ge -4/3$. Thus the only possibilities for $\langle w_1, w_2\rangle$ are $-4/3$, $-1/3$, $2/3$, and $8/3$, the last occurring if and only if $w_2 = w_1$.

Now fix w_1 and apply (iv) with $P(x) = \langle w_1, x\rangle$ and $P(x) = \langle w_1, x\rangle^2$. This yields two linear equations on the four counts $n_i := \#\{w_2 \in \Delta : \langle w_1, x\rangle = i\}$ ($i = 8/3, 2/3, -1/3, -4/3$). These are already known to satisfy the two linear conditions $n_{8/3} = 1$ and $\sum_i n_i = 819$. Solving these simultaneous linear equations yields $(n_{2/3}, n_{-1/3}, n_{-4/3}) = (288, 512, 18)$ as claimed. For a check on the computation we may verify that $\sum_i i^4 n_i = 512/3$ is consistent with $\Delta \cup (-\Delta)$ being a spherical 4-design.

vi) (sketch) We may assume that $k \ne 8/3$. For each of the remaining three values of k, and $w_1, w_2 \in \Delta$ such that $\langle w_1, w_2\rangle = k$, let

$$n_{i,j} := \#\{w \in \Delta : \langle w_1, w\rangle = i, \langle w_2, w\rangle = j\}.$$

We know $\sum_i n_{i,j}$ for each j, and $\sum_j n_{i,j}$ for each i, from (v). We can also calculate $\sum_{i,j} ij\, n_{i,j}$ and $\sum_{i,j} (ij)^2 n_{i,j}$ using the fact that $\Delta \cup (-\Delta)$ is a 4-design. In each case this gives us enough independent linear equations to determine all the $n_{i,j}$, and in particular to show that they depend only on k, and not on the choice of w_1, w_2.

This completes the proof of the Proposition.

We can now obtain the uniqueness of J_0 in two ways. The first is to use a combinatorial characterizations of a regular graph G of order 819 and degree 18 obtained from Δ. This graph has vertex set Δ and an edge connecting any $w_1, w_2 \in \Delta$ if and only if $\langle w_1, w_2\rangle = -4/3$. It turns out that the

$n_{i,j}^k$ of our Proposition are equivalent to the condition that G be a "generalized hexagon of order $(2,8)$". Cohen and Tits showed [CT] that every such generalized hexagon is isomorphic to the graph obtained from the norm-$(8/3)$ vectors of $J_0^\vee$. [They actually reduced this result in turn to Ronan's characterization [R1,R2] of this graph, and offered an alternative proof by showing that for each vertex of such a graph there is a graph involution fixing only the vertex and its neighbors and then citing Timmesfeld's group-theoretic characterization [T,(3,3)] of ${}^3D_4(2)$.] But G determines the inner products of all pairs of vectors in Δ: two vertices at distance d on the graph correspond to vectors in Δ with inner product $(-1)^d 2^{3-d}/3$. Thus Δ is isometric with the configuration of minimal vectors of $J_0^\vee$, and since these vectors generate $J_0^\vee$ it follows that $\Lambda^\vee \cong J_0^\vee$, and thus that $L \cong J_0$, as claimed.

In the second approach we use the counts $n_{i,j}^k$ for $k = -4/3$ to find a copy of the A_1^{24} Niemeier lattice in Λ. Fix $w_1, w_2 \in \Delta$ such that $\langle w_1, w_2 \rangle = -4/3$, and let $w_3 = -(w_1 + w_2)$. Then $w_3 \in \Delta$ also, and w_1, w_2, w_3 form an equilateral triangle. When $\Lambda = J_0$ such triangles are precisely the projections to J_0 of "root triples" in J. Let L be the 24-dimensional slice of Λ orthogonal to w_1, w_2, w_3. As in §7 we show that this is an even lattice of discriminant 16 with $L^\vee/L \cong (\mathbf{Z}/4\mathbf{Z})^2$, and thus that the preimage of $(2\mathbf{Z}/4\mathbf{Z})^2$ in $L^\vee$ is a self-dual lattice M. This lattice can also be described as the projection to $L \otimes \mathbf{R}$ of all vectors of Λ whose inner product with each w_i is even. The norm of such a projection must be even; thus M is a Niemeier lattice.

The next step is to show that M contains 48 roots. We cannot use the methods of §7 to count the roots, so instead we reduce the problem to the results of Prop. 9.1. If $r \in M$ has norm 2, then since $r \notin \Lambda$ we must have $r + 3w_i/2 \in \Lambda$ for exactly one of $i = 1, 2, 3$. Thus $w := r - w_i/2 \in \Lambda^\vee$. Then w has norm $8/3$, and being congruent to w_i mod Λ it must be contained in Δ. Since $\langle r, w_i \rangle = 0$ for each i, the projection of w to the (w_1, w_2, w_3) plane is $-w_i/2$. Conversely, given $w \in \Delta$ with that projection, we can reconstruct the root $r = w + w_i/2$. Enumerating the roots thus reduces to enumerating the w's. But this is done in part (vi) of our proposition (actually in this case part (v) would suffice); the multiplicities of the projections of Δ to that plane are given by the following diagram:

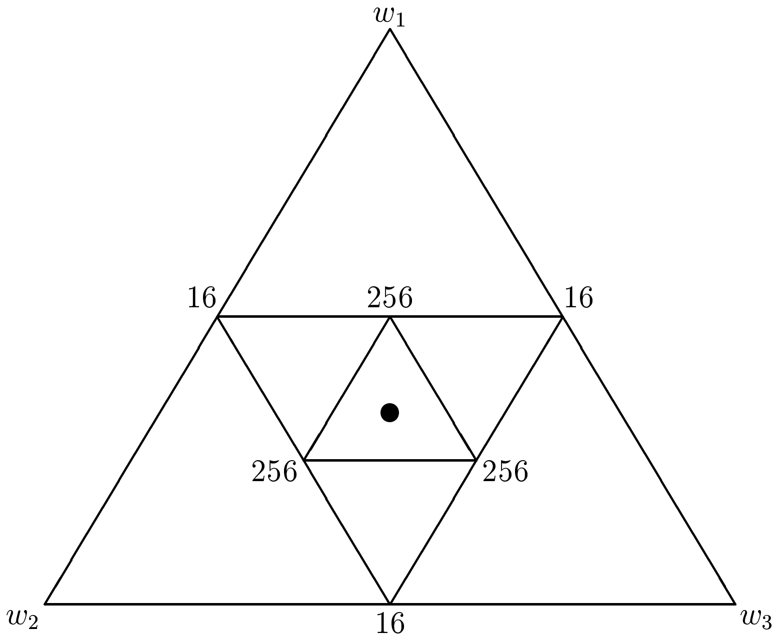

Figure 1

In particular, the number of roots is $16 + 16 + 16 = 48$ as claimed.

We finish this proof of the uniqueness of J_0 by showing that, up to the automorphisms of M, there is a unique suitable choice for its index-4 sublattice L, from which we recover Λ and thus identify it with J_0. We can even obtain the size, if not the structure, of $\mathrm{Aut}(J_0)$ by multiplying $\#\mathrm{Aut}(L)$ by the number of choices we have made along the way. This analysis, too, we relegate to a future paper.

References

[A] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, and R.A. Wilson. *ATLAS of finite groups.* Oxford, 1985.

[B] Richard E. Borcherds. *The Leech lattice and other lattices.* Ph. D. thesis, Trinity College, Cambridge, 1984.

[BV] Roland Bacher and Boris Venkov. Réseaux entiers unimodulaires sans racine en dimension 27 et 28. Preprint, 2000.

[C] John H. Conway. A characterisation of Leech's lattice. *Inventiones Math.* **7** (1969), 137–142.

[CS] John H. Conway and Neil J. A. Sloane. *Sphere packings, lattices, and groups.* Springer Grundlehren 290 (1993).

[CT] Arjeh M. Cohen and Jacques Tits. On generalized hexagons and a near octagon whose lines have three points. *European J. Combinatorics* **6** (1985) #1, 13–27.

[EG] Noam D. Elkies and Benedict H. Gross. The exceptional cone and the Leech lattice. IMRN 14 (1996) 665–698.

[vdG] Gerard van der Geer. *Hilbert modular surfaces.* Springer Ergebnisse 16 (1988).

[GG] Benedict H. Gross and Wee Teck Gan. Commutative subrings of certain non-associative rings. *Math. Annalen* **314** (1999), 265–283.

[KMRT] M.-A. Knus, A. Merkurjev, M. Rost, and J. Tignol. *The book of involutions.* AMS Colloq. Publ. 44 (1998).

[K] Henry Kim. Exceptional modular form of weight 4 on an exceptional tube domain contained in $\mathbf{C}^{27}$. *Rev. Math. Iberoamericana* **9** (1983), 139–200.

[MH] John Milnor and Dale Husemoller. *Symmetric bilinear forms.* Springer Ergebnisse 73 (1973).

[N] Hans-Volker Niemeier. Definite quadratische Formen der Dimension 24 und Diskriminante 1. *Jour. Number Th.* **5** (1973), 142–178.

[R] Robert Rankin. *Modular forms and functions.* Cambridge University Press 1977.

[R1] Mark A. Ronan. A note on the ${}^3D_4(q)$ generalized hexagons. *J. Comb. Theory Ser. A* **29** (1980) #2, 249–250.

[R2] Mark A. Ronan. A combinatorial characterization of the dual Moufang hexagons. *Geom. Dedicata* **11** (1981) #1, 61–67.

[T] Franz G. Timmesfeld. A characterization of the Chevalley- and Steinberg-groups over F_2. *Geom. Dedicata* **1** (1973) #3, 269–321.

[V] Boris B. Venkov. Even Unimodular 24-Dimensional Lattices (trans. G.A. Kendall), Chapter 18 of [CS].