GENERATION OF LOCAL INTEGRAL ORTHOGONAL GROUPS IN CHARACTERISTIC 2

BARTH POLLAK

In two previous papers (see **4**; **5**) O. T. O'Meara and I investigated the problem of generating the integral orthogonal group of a quadratic form by symmetries in the case where the underlying ring of integers was the integers of a dyadic local field of characteristic not 2. In this paper, the investigation is concerned with a local field of characteristic 2. As in (**5**), only the unimodular case is treated. As in (**4**) and (**5**), groups $\mathbf{S}(L)$, $\mathbf{X}_h(L)$, and $\mathbf{O}(L)$ are introduced for a unimodular lattice L and the relationship between $\mathbf{S}(L)$ and $\mathbf{O}(L)$ studied. As in the previously cited papers, generation by symmetries means that $\mathbf{S}(L) = \mathbf{O}(L)$. The following result is obtained.

THEOREM. *Let L be a unimodular lattice over a local field of characteristic* 2. *Then $\mathbf{X}_h(L) = \mathbf{O}(L)$. If the residue class field has more than two elements, then $\mathbf{S}(L) = \mathbf{O}(L)$. If the residue class field has exactly two elements, then $\mathbf{S}(L) = \mathbf{O}(L)$ except in* 4 *and* 6 *dimensions with L's of the following form*:

if $\dim L = 4$: $H \perp H$ *or* $H \perp M$,

if $\dim L = 6$: $H \perp H \perp M$,

with H a hyperbolic plane and M a binary unimodular lattice which does not represent a unit. In these exceptional cases, $(\mathbf{O}(L):\mathbf{S}(L)) = 2$.

1. Preliminaries. F will always denote a local field of characteristic 2. Thus F is complete with respect to a non-archimedean valuation with finite residue class field $\mathscr{F}$ (necessarily of characteristic 2). Let $\mathfrak{o}$ denote the valuation ring of F, $\mathfrak{u}$ the units of $\mathfrak{o}$, and $\mathfrak{p}$ the maximal ideal of $\mathfrak{o}$. We shall let π denote a fixed prime element of $\mathfrak{o}$ (thus $\mathfrak{p} = \pi\mathfrak{o}$). If $\gamma \in F$, $|\gamma| = |\pi|^\nu$ for some integer ν. Set $\nu = \operatorname{ord}\gamma$. If $\alpha, \beta \in \mathfrak{o}$, then $\alpha \sim \beta$ will mean $\operatorname{ord}\alpha \equiv \operatorname{ord}\beta \pmod 2$. The mapping $\wp\colon F \to F$ given by $\wp(\alpha) = \alpha^2 + \alpha$ is a homomorphism of additive groups with kernel $\{0, 1\}$. Hence $(\mathscr{F}\colon \wp(\mathscr{F})) = 2$ and we let 0 and ρ denote representatives of $\mathscr{F} \bmod \wp(\mathscr{F})$ in $\mathscr{F}$.

Let V be a finite-dimensional vector space over F with quadratic map $Q\colon V \to F$ and associated bilinear form B. We assume familiarity with the theory of quadratic spaces over fields of characteristic 2 as developed in (**1**; **2**; **3**). In particular, we assume familiarity with the concepts of isometry, orthogonality, non-degeneracy, defect, isotropy, etc. A vector x is called *singular* if $Q(x) = 0$. Recall that V^α is obtained from V by scaling: its

Received January 13, 1967. This work was supported in part by the National Science Foundation under grant GP-3986.

quadratic map $Q^\alpha = \alpha Q$. Then $B^\alpha = \alpha B$. Let $\mathbf{O}(V)$ denote the orthogonal group of V. Use $V = U \perp W$ for an orthogonal splitting. Use $V \cong V'$ to denote an isometry of V onto a quadratic space V'. We call vectors x, y a *hyperbolic pair* if $Q(x) = Q(y) = 0$ and $B(x, y) = 1$.

We shall consider lattices J, K, L, ... with respect to $\mathfrak{o}$ in V. Here we need the concepts developed in (**6**) and (**7**). In particular, we assume familiarity with the concepts of isometry, orthogonality, defect, non-degeneracy, modularity, etc., for lattices. The subspace of V that is spanned by L will be written FL and we say that L is *on* V if $V = FL$. A vector x in L is called *maximal* if $x \notin \pi L$. Since $\mathfrak{o}$ is a principal ideal domain, L must be free. Recall that L^α is obtained from L by scaling B. Let $\mathbf{O}(L)$ denote the group of units of L, $\mathfrak{s}L$ the scale, $\mathfrak{n}L$ the norm and $\mathfrak{g}L$ the norm group of L. As in (**6**), we have $\mathfrak{g}L = a\mathfrak{o}^2 + b\mathfrak{o}$, where a is a norm generator of L and b is a base generator of L. Use $L = J \perp K$ for an orthogonal splitting; call J a component of L and say that it splits L. Write $L \cong L'$ to denote an isometry of L onto a lattice L'. If L is non-defective, define the Arf invariant of L as in (**6**) and use the notation $\Delta(L)$.

1.1 *If* $\Delta(L) \neq 0$, *then* ord $\Delta(L)$ *is zero or a negative odd integer.*

Proof. See (**7**, Lemma 1.1).

2. Unimodular lattices. A unimodular lattice is an $\mathfrak{o}$-modular lattice. Necessarily, it is non-defective and, consequently, L unimodular implies dim L is even.

We let $A(\alpha, \beta)$ denote the binary lattice $\mathfrak{o}x + \mathfrak{o}y$, where $Q(x) = \alpha$, $Q(y) = \beta$, and $B(x, y) = 1$. Write $L \cong A(\alpha, \beta)$ in x, y to describe this situation. More generally, we write $L \cong A(\alpha_1, \beta_1) \perp \ldots \perp A(\alpha_n, \beta_n)$ in

$$\{x_1, y_1\} \cup \ldots \cup \{x_n, y_n\}.$$

We let H denote the generic lattice $A(0, 0)$ and we call any such H a *hyperbolic plane.*

The following result is due to Sah (**7**).

2.1. THEOREM. *The following assertions are valid.*

(1) L *unimodular and* dim $L \geqq 6$ *implies* L *is split by a hyperbolic plane.*

(2) H *a hyperbolic plane and* $H \perp J \cong H \perp K$ *implies* $J \cong K$ (*this will be referred to as the cancellation of hyperbolic planes*).

(3) *If* J *is binary unimodular,* $\Delta(J) = 0$, *and* $\mathfrak{n}J \subseteq \mathfrak{o}$, *then* J *is a hyperbolic plane.*

(4) *Let* J *be a unimodular sublattice of a non-degenerate lattice* L. *Then* J *splits* L, *i.e.,* $L = J \perp K$, *if and only if* $B(J, L) \subseteq \mathfrak{o}$.

3. Various subgroups of the orthogonal group. Let L be a lattice on a non-defective quadratic space V. We define several groups.

https://doi.org/10.4153/CJM-1968-112-9 Published online by Cambridge University Press

$$\mathbf{O}(L) = \{\sigma \in \mathbf{O}(FL) \mid \sigma L \subseteq L\}.$$

If J is a sublattice of L, then

$$\mathbf{O}(L, J) = \{\sigma \in \mathbf{O}(L) \mid \sigma x = x \text{ for } x \in J\}.$$

If J splits L, $L = J \perp K$, we identify $\mathbf{O}(L, J)$ and $\mathbf{O}(K)$. Note that $\mathbf{O}(L) = \mathbf{O}(L^\alpha)$ and $\mathbf{O}(L, J) = \mathbf{O}(L^\alpha, J^\alpha)$ for all non-zero α in F.

A *symmetry* τ_y: $V \to V$, y not singular, is defined by the equation

$$\tau_y x = x + \frac{B(x, y)}{Q(y)} y.$$

Thus $\tau_y \in \mathbf{O}(V)$. And $\mathbf{O}(V)$ is generated by these isometries. (See (**2** or **3**), noting that our field is not the finite field of two elements.) We let $\mathbf{S}(L)$ denote the subgroup of $\mathbf{O}(L)$ that is generated by all symmetries τ_y in $\mathbf{O}(L)$. $\mathbf{S}(L) = \mathbf{S}(L^\alpha)$ for any non-zero α in F.

Suppose that i is a non-zero singular vector of V. Let $w \in V$ satisfy $B(i, w) = 0$. Define a map $E_w{}^i$: $V \to V$ as follows: for $x \in V$,

$$E_w{}^i x = x + B(x, i)w + B(x, w)i + Q(w)B(x, i)i;$$

then $E_w{}^i \in \mathbf{O}(V)$. Also, $E^i_{w_1+w_2} = E_{w_1}{}^i E_{w_2}{}^i$ and, if $Q(w) \neq 0$, then $E_w{}^i = \tau_{w+Q(w)i}\tau_w$. Let $\mathbf{X}(L)$ denote the subgroup of $\mathbf{O}(L)$ that is generated by $\mathbf{S}(L)$ and those $E_w{}^i$, if any, in $\mathbf{O}(L)$.

If L has scale $\mathfrak{o}$ we define another group $\mathbf{X}_h(L)$, as in (**4**). Thus, if $\dim L \leqq 2$, then $\mathbf{X}_h(L) = \mathbf{S}(L)$. If $\dim L > 2$, we define $\mathbf{X}_h(L)$ as the subgroup of $\mathbf{X}(L)$ generated by $\mathbf{S}(L)$ and those $E_w{}^i \in \mathbf{X}(L)$ for which there exists a splitting $L = H \perp M$ with H a hyperbolic plane, $i \in H$, and $w \in M$. If L is a lattice of scale $\mathfrak{o}$ that is not split by a hyperbolic plane, then $\mathbf{X}_h(L) = \mathbf{S}(L)$, trivially.

As in (**4**), if A and B are subsets of a group G, then by AB we mean the set of all elements of G of the form ab, where $a \in A$ and $b \in B$.

As an initial step we have the following.

3.1. *Let L be a non-defective lattice and suppose that* $\dim L \leqq 2$. *Then* $\mathbf{O}(L) = \mathbf{S}(L)$.

Proof. The hypothesis immediately implies that $\dim L = 2$. Write $L = \mathfrak{o}x + \mathfrak{o}y$. Then $B(x, y) \neq 0$. By scaling we may assume that $B(x, y) = 1$. Then L is binary unimodular. By (**6**, Lemma 1.20) we may suppose that $L = A(a, c)$ in x, y, where $a \in Q(L)$ is a norm generator of $\mathfrak{g}L$ and $|ac| = |\Delta(L)|$. Since $\mathfrak{o} = \mathfrak{s}L \subseteq \mathfrak{n}L = a\mathfrak{o}$ we have that $|a| \geqq 1$.

Now let $\sigma \in \mathbf{O}(L)$ and set $\sigma x = \alpha x + \beta y$, where $\alpha, \beta \in \mathfrak{o}$. Then $\tau_{\sigma x + x} \in \mathbf{O}(L)$ if and only if

$$\frac{B(\sigma x + x, L)}{Q(\sigma x + x)} (\sigma x + x) \subseteq L. \tag{1}$$

https://doi.org/10.4153/CJM-1968-112-9 Published online by Cambridge University Press

Now $Q(\sigma x + x) = \beta$, $B(\sigma x + x, x) = \beta$, and $B(\sigma x + x, y) = \alpha - 1$. It immediately follows that (1) holds if and only if $(\alpha + 1)^2 \in \beta\mathfrak{o}$. But

$$a = Q(\sigma x) = \alpha^2 a + \alpha\beta + \beta^2 c,$$

whence $(\alpha + 1)^2 a = \beta(\alpha + \beta c)$ and therefore $(\alpha + 1)^2 = \beta(\alpha a^{-1} + \beta c a^{-1})$. Since a is a norm generator and $c \in Q(L)$, $ca^{-1} \in \mathfrak{o}$. Thus $(\alpha + 1)^2 \in \beta\mathfrak{o}$, whence $\tau_{\sigma x + x} \in \mathbf{O}(L)$. Set $\lambda = \tau_{\sigma x + x}\sigma$. Then $\lambda x = x$. Let $\lambda y = \gamma x + \delta y$, where $\gamma, \delta \in \mathfrak{o}$. Then $1 = B(\lambda x, \lambda y) = B(x, \lambda y) = \delta$. Thus $\lambda y = \gamma x + y$. Hence $c = Q(\lambda y) = \gamma^2 a + \gamma + c$, whence $\gamma(\gamma a + 1) = 0$. If $\gamma = 0$, then $\lambda y = y$ and λ is the identity map. Thus $\sigma = \tau_{\sigma x - x} \in \mathbf{S}(L)$. Thus we may assume that $\gamma a + 1 = 0$. Then $a \in \mathfrak{u}$ and $\gamma = a^{-1}$. Thus $Q(\lambda y + y) = B(\lambda y, y) = a^{-1}$ and $\tau_{\lambda y + y} \in \mathbf{O}(L)$. Now $\tau_{\lambda y + y}\lambda y = y$ and $\tau_{\lambda y + y}\lambda x = x$. Thus $\tau_{\lambda y + y}\lambda$ is the identity map. Thus $\lambda = \tau_{\lambda y + y}$ and $\sigma = \tau_{\sigma x + x}\,\tau_{\lambda y + y} \in \mathbf{S}(L)$.

4. Generalities. In this section we assume that L is a non-defective lattice of scale $\mathfrak{o}$ and dimension greater than 2.

4.1. *Suppose that i, j, and k are maximal singular vectors of L with $B(i, k) = B(j, k) = 1$. Write $L = (\mathfrak{o}i + \mathfrak{o}k) \perp M$. Then there exists $w \in M$ such that $E_w{}^k \in \mathbf{X}_h(L)$ and $E_w{}^k i = j$.*

Proof. See (**4**, §6.1).

4.2. *Let i, k and j, l be two hyperbolic pairs in L. Then there is a σ in $\mathbf{X}_h(L)$ such that $\sigma i = \epsilon j$ for some unit ϵ.*

Proof. Write $L = (\mathfrak{o}i + \mathfrak{o}k) \perp M$. If $B(i, j) \in \mathfrak{u}$, then $\tau_{i+j} \in \mathbf{X}_h(L)$ and $\tau_{i+j} i = j$. Thus suppose that $B(i, j) \in \mathfrak{p}$ and write $j = \alpha i + \beta k + w$ with $\alpha, \beta \in \mathfrak{o}$ and $w \in M$. Then $B(i, j) = \beta$ implies $\beta \in \mathfrak{p}$. If $\alpha \in \mathfrak{u}$, then

$$E^k_{\alpha^{-1}w} i = \alpha^{-1} j \quad \text{and} \quad E^k_{\alpha^{-1}w} \in \mathbf{X}_h(L).$$

Thus suppose that $\alpha \in \mathfrak{p}$. Now $l = \gamma i + \delta k + t$, where $\gamma, \delta \in \mathfrak{o}$ and $t \in M$. And $B(j, l) = 1$ implies $B(w, t) \in \mathfrak{u}$. Also, $Q(w) = \alpha\beta \in \mathfrak{p}^2$ and $Q(t) = \gamma\delta \in \mathfrak{o}$. Thus $J = \mathfrak{o}w + \mathfrak{o}t$ is binary unimodular with $\mathfrak{n}J \subseteq \mathfrak{o}$. And $\Delta(J) \in \mathfrak{p}^2$, whence $\Delta(J) = 0$ by §1.1. By (3) of §2.1, J is a hyperbolic plane. Hence, there is a singular z in M with $B(j, z) = 1$. Then

$$B(i, k + z) = B((\alpha + 1)^{-1} j, k + z) = 1$$

and $(\alpha + 1) \in \mathfrak{u}$. Invoke §4.1.

4.3. *Suppose that $L = H_\nu \perp M_\nu$ with H_ν a hyperbolic plane spanned by the hyperbolic pair i_ν, k_ν for $\nu = 1, 2$. Then there exists $\lambda \in \mathbf{X}_h(L)$ such that $\lambda i_1 = i_2$ and $\lambda k_1 = k_2$.*

Proof. See (**4**, §6.3).

4.4. *If $L = H \perp M$, where H is a hyperbolic plane, then $\mathbf{O}(L) = \mathbf{X}_h(L)\mathbf{O}(L, H)$.*

Proof. See (**4**, §6.4).

4.4a. COROLLARY. *If, in the notation of* §4.4, dim $M = 2$, *then* $\mathbf{O}(L) = \mathbf{X}_h(L)$.

Proof. Immediate by §§3.1 and 4.4.

5. The 4-dimensional case, part 1. In this section we assume that L is a 4-dimensional unimodular lattice which is split by a hyperbolic plane. By §4.4a, $\mathbf{O}(L) = \mathbf{X}_h(L)$. We wish to see when $\mathbf{O}(L) = \mathbf{S}(L)$. Hence we need only consider a splitting $L = H \perp M$ with H a hyperbolic plane and prove that any $E_w{}^i \in \mathbf{O}(L)$, with i a singular vector in H and with $w \in M$, is also in $\mathbf{S}(L)$. Now $E_w{}^i \in \mathbf{O}(L)$ immediately implies that $Q(w) \in \mathfrak{o}$. If $Q(w) \in \mathfrak{u}$, then the equation $E_w{}^i = \tau_{w+Q(w)i}\tau_w$ immediately shows that $E_w{}^i \in \mathbf{S}(L)$ hence, for the remainder of the paper, we may assume that $Q(w) \in \mathfrak{p}$. By (**6**, Lemma 1.20), we may write

$$M \cong A(a, c) \text{ in } x, y,$$

where $a \in Q(M)$ is a norm generator of $\mathfrak{g}M$ and $ac = \Delta(M)$. Note that $\mathfrak{o} = \mathfrak{s}M \subseteq \mathfrak{n}M = a\mathfrak{o}$ implies that $|a| \geqq 1$.

5.1. *Suppose that* $Q(M) \cap \mathfrak{u} = \emptyset$. *Then* ord a *is odd and* $|c| < 1$.

Proof. That ord a is odd is trivial since $|a| \geqq 1$. If $|c| \geqq 1$, then

$$|\Delta(M)| = |ac| > 1.$$

But then ord $\Delta(M)$ is odd by §1.1. Hence ord c is even. But then $Q(\lambda y) \in \mathfrak{u}$ for some $\lambda \in \mathfrak{o}$.

5.2. *Suppose that* $Q(M) \cap \mathfrak{u} \neq \emptyset$ *and that* M *is not a hyperbolic plane. Then* $\mathbf{O}(L) = \mathbf{S}(L)$.

Proof. By §5.1, either ord a is even or $|c| \geqq 1$.

(1) ord a *even and* $|a| > 1$. Then there exists $\lambda \in \mathfrak{p}$ such that $Q(\lambda x) \in \mathfrak{u}$. Also, $Q(w + \lambda x) \in \mathfrak{u}$. Thus $E_{\lambda x}{}^i$ and $E^i_{w+\lambda x} \in \mathbf{S}(L)$. Hence $E_w{}^i = E_{\lambda x}{}^i E^i_{w+\lambda x}$ is in $\mathbf{S}(L)$.

(2) $a \in \mathfrak{u}$ *or* ord a *odd and* $|c| \geqq 1$. Write $w = \alpha x + \beta y$ for some $\alpha, \beta \in \mathfrak{o}$. By (**6**, Lemma 1.5) it is easy to see that $Q(w) \in \mathfrak{p}$ implies $Q(\alpha x)$ and $Q(\beta y) \in \mathfrak{o}$. Thus both $E_{\alpha x}{}^i$ and $E_{\beta y}{}^i \in \mathbf{O}(L)$. But $E_{\alpha x}{}^i = \tau_{\alpha x+Q(\alpha x)i}\tau_{\alpha x} = \tau_{\alpha x+Q(\alpha x)i}\tau_x$. Since $\tau_x \in \mathbf{S}(L)$, we have that $\tau_{\alpha x+Q(\alpha x)i} \in \mathbf{S}(L)$. Thus $E_{\alpha x}{}^i \in \mathbf{S}(L)$. Similarly, $E_{\beta y}{}^i \in \mathbf{S}(L)$. Hence $E_w{}^i = E_{\alpha x}{}^i E_{\beta y}{}^i \in \mathbf{S}(L)$.

5.3. *Suppose that either* $Q(M) \cap \mathfrak{u} = \emptyset$ *or* M *is a hyperbolic plane. Assume that* $\mathscr{F} \neq \mathbf{F}_2$, *the field of two elements. Then* $\mathbf{O}(L) = \mathbf{S}(L)$.

Proof. If M is not a hyperbolic plane, §5.1 implies that ord a is odd and $|c| < 1$. If M is a hyperbolic plane we may take $a = 1$ and $c = 0$. Write $w = \alpha x + \beta y$ for some $\alpha, \beta \in \mathfrak{o}$. Then $Q(w) \in \mathfrak{o}$ implies $Q(\alpha x) \in \mathfrak{o}$. Hence

$E_{\alpha x}{}^i$ and $E_{\beta y}{}^i \in \mathbf{O}(L)$ and $E_w{}^i = E_{\alpha x}{}^i E_{\beta y}{}^i$. As in the proof of the previous proposition, we show that $E_{\alpha x}{}^i \in \mathbf{S}(L)$. Thus we must show that $E_{\beta y}{}^i \in \mathbf{S}(L)$.

(1) $\beta \in \mathfrak{u}$. Now $E_{\beta y}{}^i = E_y{}^{\beta i}$. Clearly, there exists $\lambda \in \mathbf{O}(H)$ such that $\lambda i = \beta i$. Hence $E_y{}^{\beta i} = E_{\lambda y}{}^{\lambda i} = \lambda E_y{}^i \lambda^{-1}$ whence $E_{\beta y}{}^i = [\lambda E_y{}^i \lambda^{-1} (E_y{}^i)^{-1}] E_y{}^i$. Now $\lambda \in \mathbf{O}(H) = \mathbf{S}(H)$ by §3.1. Thus $\lambda \in \mathbf{S}(L)$, whence

$$\lambda E_y{}^i \lambda^{-1} (E_y{}^i)^{-1} \in \mathbf{S}(L).$$

Thus we have shown that

(2) $\beta \in \mathfrak{u}$ implies that $E_{\beta y}{}^i = \sigma E_y{}^i$ for some $\sigma \in \mathbf{S}(L)$.

Now the hypothesis implies that there exists a unit ϵ such that $\epsilon + 1$ is also a unit. Then $E_y{}^i = E^i_{(\epsilon+1)y} E_{\epsilon y}{}^i$ and by repeated application of (2) we obtain $E_y{}^i = \rho E_{2y}{}^i$ for some $\rho \in \mathbf{S}(L)$. But $E_{2y}{}^i = E_0{}^i$ is the identity map. Thus $E_y{}^i = \rho \in \mathbf{S}(L)$.

(2) $\beta \in \mathfrak{p}$. Then $E_{\beta y}{}^i = E^i_{(\beta+1)y} E_y{}^i$ and $\beta + 1 \in \mathfrak{u}$. By case (1), $E_{\beta y}{}^i \in \mathbf{S}(L)$.

5.4. *Let L be a 4-dimensional unimodular lattice which is split by a hyperbolic plane H. Then $\mathbf{O}(L) = \mathbf{X}_h(L)$. If $\mathscr{F} \neq \mathbf{F}_2$, then $\mathbf{O}(L) = \mathbf{S}(L)$. Finally, suppose that $\mathscr{F} = \mathbf{F}_2$. Write $L = H \perp M$. Then $\mathbf{O}(L) = \mathbf{S}(L)$ if M is not a hyperbolic plane and $Q(M) \cap \mathfrak{u} \neq \emptyset$.*

Proof. Immediate by §§5.2 and 5.3.

6. The 4-dimensional case, part 2. In this section we assume that L is a 4-dimensional unimodular lattice that is not split by a hyperbolic plane. We shall ultimately prove that $\mathbf{O}(L) = \mathbf{S}(L)$.

6.1. *Write $\mathfrak{g}L = a\mathfrak{o}^2 + b\mathfrak{o}$. Then $b \notin \mathfrak{p}$ and $L \cong A(a, c) \perp A(b, \omega b^{-1})$ in x, y, z, w say, where $\omega = 0$ or ρ, $\Delta A(a, c) = ac$ and $|c| < |b|$.*

Proof. All that has to be shown is that $|c| < |b|$, as the other assertions follow immediately from (**6**, Lemma 1.26). Assume that $|c| \geqq |b|$. Then $|c| \geqq 1$ and $|ac| \geqq |a| > |b| \geqq 1$. As $\Delta A(a, c) = ac$, ord ac is negative and odd. Thus ord $c \equiv$ ord $b \pmod 2$. It follows from the perfectness of the residue class field that there exists $\lambda \in \mathfrak{o}$ such that $\lambda^2 b \equiv c \pmod{\mathfrak{p}}$. Now

$$J = \mathfrak{o}(z + \lambda y) + \mathfrak{o}w$$

splits L by (4) of §2.1 and since $\mathfrak{n}J \subseteq \mathfrak{o}$. Since $Q(z + \lambda y) \in \mathfrak{p}$, we have that $\Delta(J) = 0$ by §1.1. By §2.1 (3), J is a hyperbolic plane. This contradiction shows that $|c| < |b|$.

As a consequence of §6.1 we shall assume for the remainder of this section that our lattice L has the shape

$$L \cong A(a, c) \perp A(b, \omega b^{-1})$$

in x, y, z, w with $\mathfrak{g}L = a\mathfrak{o}^2 + b\mathfrak{o}$, $b \notin \mathfrak{p}$, and $|c| < |b|$.

6.2. $\mathbf{O}(L) = \mathbf{S}(L)\mathbf{O}(L, \mathfrak{o}z)$.

Proof. Let $\sigma \in \mathbf{O}(L)$. Write

$$\sigma z = \alpha x + \beta y + \gamma z + \delta w$$

with $\alpha, \beta, \gamma, \delta \in \mathfrak{o}$. Then $Q(\sigma z + z) = B(\sigma z, z) = \delta$.

(1) $\delta \in \mathfrak{u}$. Then $\tau_{\sigma z+z} \in \mathbf{O}(L)$ and $\tau_{\sigma z+z}\sigma \in \mathbf{O}(L, \mathfrak{o}z)$, whence

$$\sigma \in \mathbf{S}(L)\mathbf{O}(L, \mathfrak{o}z),$$

as desired.

(2) $\delta \in \mathfrak{p}$. $b = Q(\sigma z)$ implies that

$$Q(\alpha x + \beta y) = (\gamma + 1)^2 b + \gamma\delta + \delta^2 b^{-1}\omega. \tag{3}$$

We assert that $\gamma \equiv 1 \pmod{\mathfrak{p}}$. Suppose the contrary. Then $\gamma + 1 \in \mathfrak{u}$, whence $|(\gamma + 1)^2 b| = |b| > |\gamma\delta|$ and $|\delta^2 b^{-1}\omega|$. Hence the absolute value of the right-hand side of (3) is $|b|$. If $c = 0$, then $Q(\alpha x + \beta y) = \alpha^2 a + \alpha\beta$, whence $|\alpha^2 a + \alpha\beta| = |b|$. If $|\alpha^2 a| \leqq |\alpha\beta|$, then $|b| \leqq |\alpha\beta| \leqq 1$, whence

$$|b| = |\alpha| = |\beta| = 1.$$

But then $|\alpha^2 a| = |a| > |b| = |\alpha\beta|$, a contradiction. Hence $|\alpha^2 a| > |\alpha\beta|$. But then $|\alpha^2 a| = |b|$, a contradiction of the definition of b. Thus the assertion is proved if $c = 0$. If $c \neq 0$ then, by (**6**, Lemma 1.5),

$$|Q(\alpha x + \beta y)| = \max\{|\alpha^2 a|, |\beta^2 c|\}.$$

Hence, by (3), $\max\{|\alpha^2 a|, |\beta^2 c|\} = |b|$. But, as before, $|\alpha^2 a| = |b|$ is impossible. Thus $|\beta^2 c| = |b|$. But then $|c| \geqq |b|$ which is also impossible. Thus we must have $\gamma \equiv 1 \pmod{\mathfrak{p}}$.

(i) Suppose that ord b is even. If $b \in \mathfrak{u}$, then $\omega \neq 0$ since $\omega = 0$ would imply that $A(b, 0)$ is a hyperbolic plane. Thus $\tau_w \in \mathbf{O}(L)$. The coefficient of w in $\tau_w\sigma z$ is $\gamma + \delta \in \mathfrak{u}$. We may proceed as in case (1). Therefore we may assume that $|b| > 1$. Then there exists $\lambda \in \mathfrak{p}$ such that $|\lambda^2 b| = 1$. Then $Q(\lambda z + w) \in \mathfrak{u}$. Thus $\tau_{\lambda z+w} \in \mathbf{S}(L)$. And the coefficient of w in $\tau_{\lambda z+w}\sigma z$ is a unit. We may proceed as in case (1).

(ii) Suppose ord b is odd. Then there exists $\lambda \in \mathfrak{p}$ such that $|\lambda^2 a| = 1$ since ord a + ord b is odd. Then $Q(\lambda x + w) \in \mathfrak{u}$, whence $\tau_{\lambda x+w} \in \mathbf{S}(L)$. The coefficient of w in $\tau_{\lambda x+w}\sigma z$ is a unit. Again we proceed as in case (1).

6.3. $\mathbf{O}(L, \mathfrak{o}z) \subseteq \mathbf{S}(L)\mathbf{O}(L, \mathfrak{o}x + \mathfrak{o}w)$.

Proof. Let $\lambda \in \mathbf{O}(L, \mathfrak{o}z)$. If we can show that $\tau_{\lambda x+x} \in \mathbf{O}(L)$, our proof would be complete since then, $\tau_{\lambda x+x}\lambda \in \mathbf{O}(L, \mathfrak{o}x + \mathfrak{o}z)$. Write

$$\lambda x = \alpha x + \beta y + \gamma z + \delta w$$

with $\alpha, \beta, \gamma, \delta \in \mathfrak{o}$. Now $B(\lambda x, z) = B(\lambda x, \lambda z) = 0$, whence $\delta = 0$. Also, $Q(\lambda x + x) = B(\lambda x, x) = \beta$. Thus $\tau_{\lambda x+x} \in \mathbf{O}(L)$ if and only if

$$B(\lambda x + x, L)(\lambda x + x) \subseteq \beta L.$$

https://doi.org/10.4153/CJM-1968-112-9 Published online by Cambridge University Press

By various obvious computations one easily finds that it is sufficient to establish that

$$|(\alpha+1)^2| \leqq |\beta| \quad \text{and} \quad |\gamma^2| \leqq |\beta|. \tag{4}$$

Now $\beta = Q(\lambda x + x)$ implies that

$$Q((\alpha+1)x + \beta y) = \beta + \gamma^2 b. \tag{5}$$

(i) Suppose that $|\beta| \geqq |\gamma^2 b|$. Then $|\beta| \geqq |\gamma^2|$ and we have $(4)_2$. If $c \neq 0$, using (**6**, Lemma 1.5), we have that

$$\max\{|(\alpha+1)^2 a|, |\beta^2 c|\} \leqq |\beta|$$

by (5). Thus $|(\alpha+1)^2 a| \leqq |\beta|$. But $|a| > |b| \geqq 1$. Hence we have $(4)_1$. If $c = 0$, then $(\alpha+1)^2 a + (\alpha+1)\beta = \beta + \gamma^2 b$. If $|(\alpha+1)^2 a| > |(\alpha+1)\beta|$, then $|(\alpha+1)^2 a| = |\beta + \gamma^2 b| \leqq |\beta|$ and we obtain $(4)_1$. If

$$|(\alpha+1)^2 a| < |(\alpha+1)\beta|,$$

then $|(\alpha+1)^2 a| < |\beta + \gamma^2 b| \leqq |\beta|$ and again we obtain $(4)_1$. We are left with $|(\alpha+1)^2 a| = |(\alpha+1)\beta|$. But then $|\alpha+1| = |\beta a^{-1}|$, whence

$$|(\alpha+1)^2| = |\beta a^{-2}|\,|\beta|$$

and, since $|\beta a^{-2}| < 1$, we again obtain $(4)_1$. This settles case (i).

(ii) Suppose that $|\beta| < |\gamma^2 b|$. If $c \neq 0$, then (5) implies

$$\max\{|(\alpha+1)^2 a|, |\beta^2 c|\} = |\gamma^2 b|.$$

Thus $|(\alpha+1)^2 a| \leqq |\gamma^2 b|$, whence $|(\alpha+1)^2| \leqq |ba^{-1}|\,|\gamma^2| \leqq |\gamma^2|$. Hence it will be enough to prove $(4)_2$. By definition of b, $|(\alpha+1)^2 a| = |\gamma^2 b|$ is impossible. Thus we must have that $|\beta^2 c| = |\gamma^2 b|$. Thus $|\beta^2|\,|cb^{-1}| = |\gamma^2|$. Hence $|\beta^2| > |\gamma^2|$. But $|\beta| \leqq 1$, whence $|\beta^2| \leqq |\beta|$. Thus $|\gamma^2| \leqq |\beta|$ and we have $(4)_2$. Thus we may suppose that $c = 0$. Then (5) yields

$$(\alpha+1)^2 a + (\alpha+1)\beta = \beta + \gamma^2 b.$$

If $|(\alpha+1)^2 a| > |(\alpha+1)\beta|$ we would obtain $|(\alpha+1)^2 a| = |\gamma^2 b|$, an impossibility. Thus $|(\alpha+1)^2 a| \leqq |(\alpha+1)\beta|$. Hence

$$|(\alpha+1)^2| < |(\alpha+1)^2 a| \leqq |(\alpha+1)\beta| \leqq |\beta|$$

and we have $(4)_1$. Also we have that $|\gamma^2 b| \leqq |(\alpha+1)\beta|$ by (5). Hence

$$|\gamma^2| \leqq |\alpha+1|\,|b^{-1}|\,|\beta| \leqq |\beta|$$

and we obtain $(4)_2$. This exhausts all cases and our proof is complete.

6.4. $\mathbf{O}(L, \mathfrak{o}x + \mathfrak{o}z) \subseteq \mathbf{S}(L)\mathbf{O}(L, \mathfrak{o}z + \mathfrak{o}w)$.

Proof. Let $\sigma \in \mathbf{O}(L, \mathfrak{o}x + \mathfrak{o}z)$. If we can establish that $\tau_{\sigma w + w} \in \mathbf{O}(L)$ our proof would be complete since $\tau_{\sigma w + w}\sigma$ is easily seen to be in $\mathbf{O}(L, \mathfrak{o}z + \mathfrak{o}w)$.

https://doi.org/10.4153/CJM-1968-112-9 Published online by Cambridge University Press

Let

$$\sigma w = \alpha x + \beta y + \gamma z + \delta w$$

with $\alpha, \beta, \gamma, \delta \in \mathfrak{o}$. Now $\sigma x = x$ and $\sigma z = z$ immediately imply that $\beta = 0$ and $\delta = 1$. And $Q(\sigma w + w) = \gamma$. Hence $\tau_{\sigma w + w} \in \mathbf{O}(L)$ if and only if

$$B(\sigma w + w, L)(\sigma w + w) \subseteq \gamma L.$$

By several obvious computations we see that it suffices to prove that $\alpha^2 \in \gamma\mathfrak{o}$. Now, $\omega b^{-1} = Q(\sigma w)$ implies that $\alpha^2 a = \gamma^2 b + \gamma$ whence $\alpha^2 = \gamma(\gamma b a^{-1} + a^{-1})$. But clearly, $\gamma b a^{-1} + a^{-1} \in \mathfrak{o}$ and our proof is complete.

We can now prove the following.

6.5. $\mathbf{O}(L) = \mathbf{S}(L)$.

Proof. Immediate by §§6.2, 6.3, and 6.4.

7. The group $\mathbf{X}_h(L)$. In this section we assume that L is an arbitrary unimodular lattice. The case $\dim L = 2$ was discussed in §3.1, thus we may assume that $\dim L \geqq 4$.

7.1. *Suppose that $L = J \perp M$ and consider an $E_w{}^i \in \mathbf{O}(L)$ with $i \in J$ and $w \in M$. Suppose that either* (1) $Q(w) \in \mathfrak{u}$ *or* (2) $w \in \pi M$ *and* $Q(M) \cap \mathfrak{u} \neq \emptyset$. *Then* $E_w{}^i \in \mathbf{S}(L)$.

Proof. (1) $Q(w) \in \mathfrak{u}$. Then $\tau_w \in \mathbf{O}(L)$. As $E_w{}^i \in \mathbf{O}(L)$ and $E_w{}^i = \tau_{w+Q(w)i}\tau_w$, $\tau_{w+Q(w)i} \in \mathbf{O}(L)$. Thus $E_w{}^i \in \mathbf{S}(L)$.

(2) Fix $w_1 \in M$ with $Q(w_1) \in \mathfrak{u}$. Clearly, $Q(w + w_1) \in \mathfrak{u}$. Thus $E_{w_1}{}^i$ and $E^i_{w+w_1}$ are in $\mathbf{S}(L)$. Thus $E_w{}^i = E_{w_1}{}^i E^i_{w+w_1} \in \mathbf{S}(L)$.

7.2. *Suppose that* $\dim L \neq 4$ *or* 6 *if the residue class field* $\mathfrak{F} = \mathbf{F}_2$. *Then* $\mathbf{X}_h(L) = \mathbf{S}(L)$.

Proof. By §3.1 we may assume that $\dim L \geqq 4$. If $\dim L = 4$, the hypothesis implies that $\mathfrak{F} \neq \mathbf{F}_2$. By §§5.4 and 6.5, $\mathbf{O}(L) = \mathbf{S}(L)$, whence $\mathbf{X}_h(L) = \mathbf{S}(L)$. Thus, we may assume that $\dim L \geqq 6$. We have to consider a splitting $L = H \perp M$ with H a hyperbolic plane and prove that any $E_w{}^i \in \mathbf{O}(L)$, with i a singular vector in H and $w \in M$, is also in $\mathbf{S}(L)$. Note that $\dim M \geqq 4$. Thus, $Q(M) \cap \mathfrak{u} \neq \emptyset$. (See, e.g., **6**, Lemma 1.26.) We may therefore assume, by §7.1, that w is maximal in M and $Q(w) \in \mathfrak{p}$. Now pick $t \in M$ with $B(w, t) = 1$ and obtain a splitting $M = (\mathfrak{o}w + \mathfrak{o}t) \perp N$. Suppose that $\mathfrak{F} \neq \mathbf{F}_2$. Set $K = H \perp (\mathfrak{o}w + \mathfrak{o}t)$. Then $L = K \perp N$ and $\mathbf{O}(K) = \mathbf{S}(K)$ by §5.4. Hence $E_w{}^i \in \mathbf{O}(L, N) \subseteq \mathbf{S}(L)$. Therefore we may suppose that $\mathfrak{F} = \mathbf{F}_2$. Here we have $\dim N \geqq 4$ and, again by (**6**, Lemma 1.26), there exists $w_1 \in N$ with $Q(w_1) \in \mathfrak{u}$. Then $Q(w + w_1) \in \mathfrak{u}$. Thus $E_{w_1}{}^i$ and $E^i_{w+w_1}$ are in $\mathbf{S}(L)$ by §7.1. Thus $E_w{}^i \in \mathbf{S}(L)$.

7.3. THEOREM. *If L is unimodular, then $\mathbf{O}(L) = \mathbf{X}_h(L)$. If $\mathfrak{F} \neq \mathbf{F}_2$, then $\mathbf{O}(L) = \mathbf{S}(L)$. If $\mathfrak{F} = \mathbf{F}_2$ and $\dim L \neq 4$ or 6, then $\mathbf{O}(L) = \mathbf{S}(L)$.*

https://doi.org/10.4153/CJM-1968-112-9 Published online by Cambridge University Press

Proof. The proof is by induction on dim L. If dim $L = 2$, the result follows from §3.1. If dim $L = 4$, then invoke §§5.4 and 6.5. Thus we may assume that dim $L \geqq 6$. But then, by (1) of §2.1, L is split by a hyperbolic plane H. By §4.4, $\mathbf{O}(L) = \mathbf{X}_h(L)\mathbf{O}(L, H)$. By the induction hypothesis,

$$\mathbf{O}(L, H) \subseteq \mathbf{X}_h(L).$$

Thus $\mathbf{O}(L) = \mathbf{X}_h(L)$. The result now follows from §7.2.

8. The exceptional dimensions, part 1. The only cases where the validity of the equation $\mathbf{O}(L) = \mathbf{S}(L)$, L unimodular, is still in doubt occur in dimensions 4 and 6 when $\mathfrak{F} = \mathbf{F}_2$. We have already studied the case dim $L = 4$ and found that $\mathbf{O}(L) = \mathbf{S}(L)$ with the possible exception of the following cases:

$$L \cong \begin{cases} H \perp H, \\ H \perp M, \text{ where } Q(M) \cap \mathfrak{u} = \emptyset. \end{cases}$$

We shall prove in the next section that $(\mathbf{O}(L) : \mathbf{S}(L)) = 2$ in these cases. We now wish to investigate the 6-dimensional cases for which $\mathbf{O}(L) = \mathbf{S}(L)$ holds.

TABLE I

I	$A(0, 0) \perp A(0, 0) \perp J$
II	$A(0, 0) \perp A(0, 0) \perp K$
III	$A(0, 0) \perp N$

8.1. *Let L be 6-dimensional unimodular. Then there is a base for L such that L has exactly one of the forms* I, II, *or* III *of Table* 1. *In case* I, *J is binary unimodular such that $Q(J) \cap \mathfrak{u} = \emptyset$. In case* II, *$K$ is binary unimodular such that $Q(K) \cap \mathfrak{u} \neq \emptyset$. In case* III, *$N$ is 4-dimensional unimodular and is not split by a hyperbolic plane.*

Proof. Immediate by (1) of §2.1.

8.2. *Let L be 6-dimensional unimodular of type* II *or* III. *Then* $\mathbf{O}(L) = \mathbf{S}(L)$.

Proof. As $\mathbf{O}(L) = \mathbf{X}_h(L)$ we need only prove that an $E_w{}^i \in \mathbf{O}(L)$ which is determined by a splitting $L = H \perp M$, H a hyperbolic plane, $i \in H$, $w \in M$, is in $\mathbf{S}(L)$. By cancelling hyperbolic planes we may suppose that

$$M \cong \begin{cases} A(0, 0) \perp K, \text{ or} \\ N. \end{cases}$$

If $Q(w) \in \mathfrak{u}$, then $E_w{}^i \in \mathbf{S}(L)$ trivially, therefore we may assume that $Q(w) \in \mathfrak{p}$.

Case 1. $M \cong A(0, 0) \perp K$. Write $w = w_1 + w_2$, where $w_1 \in A(0, 0)$ and $w_2 \in K$. Now $Q(w) = Q(w_1) + Q(w_2)$. There are two possibilities:

(i) both $Q(w_1)$ and $Q(w_2) \in \mathfrak{p}$,

https://doi.org/10.4153/CJM-1968-112-9 Published online by Cambridge University Press

(ii) both $Q(w_1)$ and $Q(w_2) \in \mathfrak{u}$.

Now $E_w{}^i = E_{w_1}{}^i E_{w_2}{}^i$. In Case 1 (i), choose $x_1 \in K$ such that $Q(x_1) \in \mathfrak{u}$. Then $Q(w_1 + x_1) = Q(w_1) + Q(x_1) \in \mathfrak{u}$ whence $E_{w_1}{}^i = E_{x_1}{}^i E^i_{w_1+x_1} \in S(L)$. There exists $x_2 \in A(0,0)$ such that $Q(x_2) \in \mathfrak{u}$. Then $Q(w_2 + x_2) \in \mathfrak{u}$ and $E_{w_2}{}^i = E_{x_2}{}^i E^i_{w_2+x_2} \in \mathbf{S}(L)$. Thus $E_w{}^i \in \mathbf{S}(L)$.

In Case 1 (ii), $E_{w_1}{}^i$ and $E_{w_2}{}^i$ are trivially in $\mathbf{S}(L)$. Thus $E_w{}^i \in \mathbf{S}(L)$.

Case 2. $M \cong N$.

(i) Suppose that $b \in \mathfrak{u}$. Then

$$N \cong A(a, c) \perp A(b, \rho b^{-1})$$

in k, l, m, n, say, and we must have that $c \in \mathfrak{p}$ by §6.1. Write $w = w_1 + w_2$ with $w_1 \in A(a, c)$, $w_2 \in A(b, \rho b^{-1})$. Now $E_w{}^i = E_{w_1}{}^i E_{w_2}{}^i$ and by an analysis similar to the preceding case, we may suppose both $Q(w_1)$ and $Q(w_2) \in \mathfrak{p}$. We note that this implies that w_2 is not maximal; cf. (**6**, Lemma 1.5). Hence $|Q(m)| = |Q(w_1 + m)| = |Q(w_2 + m)| = 1$. Thus $E_{w_1}{}^i = E_m{}^i E^i_{w_1+m} \in \mathbf{S}(L)$ and $E_{w_2}{}^i = E_m{}^i E^i_{w_2+m} \in \mathbf{S}(L)$. Thus $E_w{}^i \in \mathbf{S}(L)$.

(ii) Suppose that $|b| > 1$. By §6.1, we may write

$$N \cong A(a, c) \perp A(b, \omega b^{-1}),$$

$w = w_1 + w_2$ with $w_1 \in A(a, c)$, $w_2 \in A(b, \omega b^{-1})$. We may suppose both $Q(w_1)$ and $Q(w_2) \in \mathfrak{p}$. If ord b is even, there exists a non-maximal vector $x \in A(b, \omega b^{-1})$ such that $Q(x) \in \mathfrak{u}$. Then both $Q(w_1 + x)$ and $Q(w_2 + x)$ are in $\mathfrak{u}$ and hence both $E_{w_1}{}^i = E_x{}^i E^i_{w_1+x}$ and $E_{w_2}{}^i = E_x{}^i E^i_{w_2+x}$ are in $\mathbf{S}(L)$. Then $E_w{}^i = E_{w_1}{}^i E_{w_2}{}^i \in \mathbf{S}(L)$. Finally, if ord b is odd, then ord a is even and there exists a non-maximal vector $x \in A(a, c)$ such that $Q(x) \in \mathfrak{u}$. By a similar argument we see that $E_w{}^i \in \mathbf{S}(L)$.

9. The exceptional dimensions, part 2. We continue in this section with our assumptions that L is unimodular of dimension 4 or 6 and $\mathscr{F} = \mathbf{F}_2$. The only cases which remain to be discussed are listed below:

dim $L = 4$	I	$A(0,0) \perp A(0,0)$	in i, j, k, l
	II	$A(0,0) \perp A(a, c)$	
dim $L = 6$	III	$A(0,0) \perp A(0,0) \perp A(a, c)$	in i, j, k, l, m, n

Furthermore, for the binary lattice $A(a, c)$, we have $Q(A(a, c)) \cap \mathfrak{u} = \emptyset$. By §5.1, we must have ord a odd and $c \in \mathfrak{p}$.

Lattices of types I, II, and III will be referred to as *exceptional* lattices.

9.1. *Let L be an exceptional lattice. Suppose that i and r are maximal singular vectors both of which lie in hyperbolic planes. Then there exists $\phi \in \mathbf{S}(L)$ such that $\phi i = r$.*

https://doi.org/10.4153/CJM-1968-112-9 Published online by Cambridge University Press

Proof. Let i, j be a hyperbolic pair and write $L = (\mathfrak{o}i + \mathfrak{o}j) \perp K$. Then we have $r = \alpha i + \beta j + z$ for some $\alpha, \beta \in \mathfrak{o}$ and $z \in K$. If $\beta \in \mathfrak{u}$, then $B(i, r) \in \mathfrak{u}$ whence $\tau_{r+i} \in \mathbf{S}(L)$ and $r = \tau_{r+i} i$. If $\alpha \in \mathfrak{u}$, then $B(j, r) \in \mathfrak{u}$ and $\tau_{r+j} \in \mathbf{S}(L)$. Then $\phi = \tau_{r+j}\tau_{i+j} \in \mathbf{S}(L)$ and $\phi i = r$. Thus we may assume that both α and β lie in $\mathfrak{p}$. Hence z is maximal in K. Therefore there exists $t \in K$ such that $B(z, t) = 1$; and $Q(r) = 0$ implies $Q(z) \in \mathfrak{p}$. We may write

$$L = (\mathfrak{o}i + \mathfrak{o}j) \perp (\mathfrak{o}z + \mathfrak{o}t)$$

if $\dim L = 4$ or $(\mathfrak{o}i + \mathfrak{o}j) \perp (\mathfrak{o}z + \mathfrak{o}t) \perp R$ if $\dim L = 6$.

Case 1. Suppose that $L \cong A(0, 0) \perp A(a, c)$. By cancellation of hyperbolic planes, we may suppose that $\mathfrak{o}z + \mathfrak{o}t \cong A(a, c)$ in k, l. Write $z = \gamma k + \delta l$ for some $\gamma, \delta \in \mathfrak{o}$. Thus $r = \alpha i + \beta j + \gamma k + \delta l$ and $Q(r) = 0$ implies $\gamma \in \mathfrak{p}$. Let r, s be a hyperbolic pair. Write $s = \alpha_1 i + \beta_1 j + \gamma_1 k + \delta_1 l$. Then $B(r, s) = 1$ implies $\gamma_1 \in \mathfrak{u}$. But then $|Q(s)| = |a|$, contradicting $Q(s) = 0$. Thus, not both of α and β can lie in $\mathfrak{p}$ and this case is settled.

Case 2. Suppose that $L \cong A(0, 0) \perp A(0, 0)$. By cancellation of hyperbolic planes, we may suppose that $\mathfrak{o}z + \mathfrak{o}t \cong A(0, 0)$ in k, l. Write $z = \gamma k + \delta l$ for some $\gamma, \delta \in \mathfrak{o}$. Thus $r = \alpha i + \beta j + \gamma k + \delta l$ and r maximal implies at least one of γ and δ is a unit. Suppose, temporarily, that $\gamma \in \mathfrak{u}$. Then $Q(r) = 0$ implies $\delta \in \mathfrak{p}$. Then $B(r, i + j + k + l) \in \mathfrak{u}$ whence $\tau_{r+i+j+k+l} \in \mathbf{S}(L)$. Also, $\tau_{j+k+l} \in \mathbf{S}(L)$. Set $\phi = \tau_{r+i+j+k+l}\tau_{j+k+l}$. Then $\phi \in \mathbf{S}(L)$ and $\phi i = r$. If $\delta \in \mathfrak{u}$ we proceed in an analogous fashion.

Case 3. $\dim L = 6$. If $Q(t)$ is a norm generator of L, then

$$L_1 = (\mathfrak{o}i + \mathfrak{o}j) \perp (\mathfrak{o}z + \mathfrak{o}t)$$

is a lattice of the type considered in Case 1 and both $i, r \in L_1$. We may invoke Case 1 to complete the proof. If $Q(t)$ is not a norm generator, then R must contain a norm generator. Noting that 1 is a base generator for L, we conclude that $\operatorname{ord} Q(t) + \operatorname{ord} a$ is even if $|Q(t)| > 1$. By amalgamating a suitable vector of R with t if necessary, we may assume that $Q(t) \in \mathfrak{o}$. But then $\mathfrak{o}z + \mathfrak{o}t$ is a hyperbolic plane, both $i, r \in L_1$, and we may invoke Case 2.

9.2. *Let L be an exceptional lattice. Suppose that $\sigma \in \mathbf{O}(L)$. Then either $\sigma \in \mathbf{S}(L)$ or σ is of the form $\lambda E_l{}^i$ for some $\lambda \in \mathbf{S}(L)$. Hence $(\mathbf{O}(L) : \mathbf{S}(L)) \leqq 2$.*

Proof. By §7.3, $\mathbf{O}(L) = \mathbf{X}_h(L)$. Suppose that $E_v{}^r$ occurs in the expression for σ as an element of $\mathbf{X}_h(L)$. The equation $E_w{}^{\alpha i} = E_{\alpha w}{}^i$ allows us to assume that r is maximal. Invoking §9.1, we may write $E_v{}^r = E_{\phi w}{}^{\phi i}$, $\phi \in \mathbf{S}(L)$. Thus $E_v{}^r = \phi E_w{}^i \phi^{-1}$ and, ultimately, we may express σ in the form $\psi E_w{}^i$, where $\psi \in \mathbf{S}(L)$ and w, of course, lies in $(\mathfrak{o}i + \mathfrak{o}j)^*$, the orthogonal complement of $\mathfrak{o}i + \mathfrak{o}j$ in L. Now $E_w{}^i \in \mathbf{O}(L)$ implies that $Q(w) \in \mathfrak{o}$. If $Q(w) \in \mathfrak{u}$, then, trivially, $\sigma \in \mathbf{S}(L)$, thus we may assume that $Q(w) \in \mathfrak{p}$.

Case 1. $\dim L = 4$. We may write $w = \alpha k + \beta l$ for some $\alpha, \beta \in \mathfrak{o}$. As $Q(w) \in \mathfrak{p}$ we have both $Q(\alpha k)$ and $Q(\beta k)$ in $\mathfrak{p}$. Then both $E_{\alpha k}{}^i$ and $E_{\beta l}{}^i$ are in $\mathbf{O}(L)$ and, of course, $E_w{}^i = E_{\alpha k}{}^i E_{\beta l}{}^i$.

(i) Suppose that $(\mathfrak{v}i + \mathfrak{v}j)^* = A(0, 0)$ in k, l. If $\alpha \in \mathfrak{u}$, then

$$E_{\alpha k}{}^i = E_k{}^{\alpha i} = E_{\tau l}{}^{\tau i} = \tau E_l{}^i \tau^{-1},$$

where $\tau \in \mathbf{S}(L)$ sends $i \to \alpha i$, $j \to \alpha^{-1} j$, $k \to l$, and $l \to k$. As in the proof of §5.3 we obtain $E_{\alpha k}{}^i = \phi E_l{}^i$ for some $\phi \in \mathbf{S}(L)$. If $\alpha \in \mathfrak{p}$ write $E_{\alpha k}{}^i = E^i_{(\alpha+1)k} E_k{}^i$ and, by the preceding observation, we have

$$E_{\alpha k}{}^i = \psi E_{2l}{}^i = \psi E_0{}^i = \psi \quad \text{for some } \psi \in \mathbf{S}(L).$$

(ii) Suppose that $(\mathfrak{v}i + \mathfrak{v}j)^* = A(a, c)$ in k, l. Then $E_{\alpha k}{}^i = \tau_{\alpha k + Q(\alpha k)\, i} \tau_{\alpha k}$. As $\tau_{\alpha k} = \tau_k \in \mathbf{O}(L)$, it follows that $\tau_{\alpha k + Q(\alpha k)\, i} \in \mathbf{O}(L)$, whence $E_{\alpha k}{}^i \in \mathbf{S}(L)$.

(iii) $E_{\beta l}{}^i$ has either the form ϕ or $\phi E_l{}^i$ for some $\phi \in \mathbf{S}(L)$. This follows exactly as in the proof of §5.3.

(iv) By (i), (ii), and (iii) we see that σ has one of the forms λ or $\lambda E_l{}^i$ for some $\lambda \in \mathbf{S}(L)$ and Case 1 is complete.

Case 2. $\dim L = 6$. Write $w = x + y$, where $x \in A(0, 0)$ and $y \in A(a, c)$. Now $Q(w) = Q(x) + Q(y) \in \mathfrak{p}$ implies either both $Q(x)$, $Q(y) \in \mathfrak{u}$ or both $Q(x)$, $Q(y) \in \mathfrak{p}$. As $Q(A(a, c)) \cap \mathfrak{u} = \emptyset$, only the latter case can occur. Now $|Q(k + l)| = |Q(y + k + l)| = 1$. Thus $E_y{}^i = E^i_{k+l} E^i_{y+k+l} \in \mathbf{S}(L)$. Since $E_w{}^i = E_y{}^i E_x{}^i$ and $x \in A(0, 0)$ we may invoke Case 1.

10. The exceptional behaviour, part 3. In this section, L will denote an exceptional lattice. Thus $\mathscr{F} = \mathbf{F}_2$ and L has one of the shapes I, II, or III given at the beginning of the preceding section and we shall continue to use the notation introduced at that time. We will ultimately prove that $E_l{}^i \notin \mathbf{S}(L)$ whence, by §9.2, $(\mathbf{O}(L) : \mathbf{S}(L)) = 2$.

Now πL is an additive subgroup of L. As in (**4**, §10) we can endow $\bar{V} = L/\pi L$ with the structure of a vector space over the finite field of two elements. And we can put a symmetric bilinear form $\bar{B}$ on $\bar{V}$ and construct a homomorphism

$$f\colon \mathbf{O}(L) \to \mathbf{GL}(\bar{V}).$$

10.1. *Let L be an exceptional lattice. Then $E_l{}^i \notin \mathbf{S}(L)$ and hence $(\mathbf{O}(L) : \mathbf{S}(L)) = 2$.*

Proof. Using the bar notation of (**4**, §10) we shall prove that

$$f(E_l{}^i) \notin f(\mathbf{S}(L)).$$

By considerations analogous to those of (**4**, §10), we can list a set of generators $\bar{\tau}_s$ for $f(\mathbf{S}(L))$.

Type of L	Generators for $f(\mathbf{S}(L))$
I	$\bar{\tau}_{i+j}$, $\bar{\tau}_{i+j+k}$, $\bar{\tau}_{i+j+l}$ $\bar{\tau}_{k+l}$, $\bar{\tau}_{i+k+l}$, $\bar{\tau}_{j+k+l}$
II	$\bar{\tau}_{i+j}$, $\bar{\tau}_{i+j+l}$
III	$\bar{\tau}_x$ or $\bar{\tau}_{x+n}$, where $\bar{\tau}_x$ is one of the generators for type I.

https://doi.org/10.4153/CJM-1968-112-9 Published online by Cambridge University Press

Case 1. Suppose that L is of type I or II. Note that the set of generators in type II is contained in the set of generators in type I. Note also that $f(E_l{}^i)$ is the same element of $\mathbf{GL}(\bar{V})$ in both types I and II. Hence it will suffice to prove that $f(E_l{}^i) \notin f(\mathbf{S}(L))$ for L of type I.

Now in the case of type I we can give $\bar{V}$ the structure of a non-defective quadratic space over $\mathbf{F}_2$ by defining a quadratic map $\bar{Q}$ on $\bar{V}$ by

$$\bar{Q}(\bar{x}) = \overline{Q(x)} \quad \text{for } x \in L.$$

Then $\bar{Q}$ is well-defined, $\bar{B}$ becomes the associated bilinear form and f clearly becomes a homomorphism

$$f\colon \mathbf{O}(L) \to \mathbf{O}(\bar{V}).$$

Since F contains a copy of $\mathbf{F}_2$, f is surjective. Hence, if $E_l{}^i \in \mathbf{S}(L)$, then, by §9.2, $\mathbf{O}(L) = \mathbf{S}(L)$ and it would follow that $\mathbf{O}(\bar{V})$ is generated by symmetries. But the Witt index of the space $\bar{V}$ is clearly 2. This gives a contradiction to (**2**, I.5.1). (Alternatively, see **3**, Proposition 14.)

Case 2. Suppose that L is of type III. The argument in this situation is completely analogous to the argument of Case 4 of §8.3 given in (**5**).

References

1. C. Arf, *Untersuchungen über quadratischen Formen in Körpern der Charakteristik* 2, J. Reine Angew. Math. *183* (1940), 148–167.
2. C. Chevalley, *The algebraic theory of spinors* (Columbia Univ. Press, New York, 1954).
3. J. Dieudonné, *Sur les groupes classiques* (Hermann, Paris, 1948).
4. O. T. O'Meara and Barth Pollak, *Generation of local integral orthogonal groups*, Math. Z. *87* (1965), 385–400.
5. ——— *Generation of local integral orthogonal groups*. II, Math. Z. *93* (1966), 171–188.
6. C. R. Riehm, *Integral representations of quadratic forms in characteristic* 2, Amer. J. Math. *87* (1965), 32–64.
7. Chih-Han Sah, *Quadratic forms over fields of characteristic* 2, Amer. J. Math. *82* (1960), 812–830.

University of Notre Dame,
Notre Dame, Indiana