JOURNAL OF ALGEBRA 63, 56–75 (1980)

Quaternions over $\mathbf{Q}(\sqrt{5})$, Leech's Lattice and the Sporadic Group of Hall–Janko

J. TITS

Collège de France, 11 Place Marcelin-Berthelot, 75231 Paris Cedex 05, France

Communicated by I. N. Herstein

Received April 24, 1979

TO MY FRIEND NATHAN JACOBSON ON HIS 70TH BIRTHDAY

INTRODUCTION

It was observed long ago by J. Thompson that the automorphism group of Leech's lattice Λ—Conway's group $\cdot 0$—contains a subgroup X_9 isomorphic to the double cover $\tilde{\mathfrak{A}}_9$ of the alternating group $\mathfrak{A}_9$. Furthermore, if we denote by $X_8 \supset X_7 \supset \cdots \supset X_2$ the decreasing sequence of subgroups of X_9 characterized up to conjugacy by $X_i \cong \tilde{\mathfrak{A}}_i$, the centralizers $C_i = C_{\cdot 0}(X_i)$ form a remarkable sequence: $C_2 = \cdot 0$ is the double cover of Conway's group $\cdot 1$, C_3 the sextuple cover $\tilde{Suz}$ of Suzuki's sporadic group, C_4 the double cover of $G_2(\mathbf{F}_4)$, C_5 the double cover $\tilde{J}_2$ of the sporadic group of Hall–Janko, ... (cf. [4, p. 242]). This suggests a varicty of interesting ways of looking at Λ, namely, as a module over its endomorphism ring R_i generated by X_i, for $i = 2, 3, 4, \ldots$: indeed, the automorphism group of that module (endowed with a suitable form) is precisely the group C_i. For $i = 2$, $R_i = \mathbf{Z}$ and one simply has Leech's and Conway's original approaches to the lattice [2, 10, 11]. For $i = 3$, $R_i = \mathbf{Z}[\sqrt[3]{1}]$ and Λ appears as the R_3-module of rank 12 investigated by Lindsey [13] (cf. also [4, p. 243; 15, Sect. 3]). The ring R_4 is a maximal order in the quaternion algebra $\mathbf{Q}(i, j, k)$; this case, handled in [16], provides an especially neat analogue of Conway's uniqueness proof [3]. The present paper is concerned with the case $i = 5$, that is, with the study of Λ as a rank 3 module over the ring R_5 (here denoted by R) which is a maximal order in the quaternion algebra $\mathbf{Q}(\sqrt{5})(i, j, k)$.

One way of describing Λ as an R_i-module consists in starting from its R_{i-1}-module structure and giving explicit formulas for a further operator, generating R_i over R_{i-1}; this is done in [4] for $i = 3$. However, there is a more direct and, it appears, more efficient approach: indeed, one can give an essentially uniform description of the R_i-module for $i = 2, 3, 4, 5$ (cf. [17]). In that

0021-8693/80/030056–20$02.00/0

description, the complexity of Λ is, so to speak, divided into two parts: an "arithmetic" part, included in the ring structure of R_i, and a "combinatorial" part, summarized by a certain code (the binary and ternary Golay code for $i = 2, 3$, and a code in $\mathbf{F}_4^6$ for $i = 4$). As i increases, the arithmetic share becomes larger and the combinatorial share decreases to the point of becoming almost nonexistent for $i = 5$ (cf., however, our Section 3). As a result, we are able to give a very simple description of Λ as a free R-module of rank 3, endowed with an explicitly given Hermitian form h. Combining h with a suitably modified "trace map" $\mathbf{Q}(\sqrt{5}) \to \mathbf{Q}$, one gets a quadratic form on Λ which is readily seen to possess the characteristic properties of Leech's form (evenness, unimodularity, no vector of norm 2). That is done in Section 2, where we also point out that the quaternionic reflections with respect to "short vectors," that is, vectors $\mathbf{x} \in \Lambda$ such that $h(\mathbf{x}, \mathbf{x}) = 4$, are automorphisms of (Λ, h). The remainder of the paper is devoted to the study of the group $G = \mathrm{Aut}(\Lambda, h)$, the main goal being to prove that G is a perfect extension of a simple group of order 604,800 (the Hall–Janko group) by a group of order 2. In particular, $G = J_2$ appears most naturally as a group generated by quaternionic reflections, a fact which was first recognized by Conway [2] and Cohen [1]. We note also that the three-dimensional representation of J_2 over $\mathbf{Q}(\sqrt{5})(i, j, k)$ provides in an obvious way the six-dimensional complex representation studied by Lindsey in [12]; more precisely, one sees that J_2 has a six-dimensional representation over any totally imaginary number field containing $\sqrt{5}$.

As will be clear from the above, the point of this paper lies less in the actual results, often well known, than in the approach which I hope to be new, at least in print (I have little doubt that other people have worked out for themselves at least some of the arguments presented here). Considering the relative importance of the methodological aspects, and in contrast to the widespread usage in the present-day literature on finite groups, I have generally tried to give rather explicit proofs of even the most elementary facts, at the risk of appearing lengthy to some.

1. The Order R

1.1. The notation introduced in this section will be used throughout the paper. We set $K = \mathbf{Q}(\sqrt{5})$, $\tau = (1 + \sqrt{5})/2$ and $\mathfrak{o} = \mathbf{Z} + \mathbf{Z}\tau$, thus, $\mathfrak{o}$ is the ring of integers of K. Note the identities

$$\tau^2 = 1 + \tau, \qquad \tau^{-1} = 1 - \tau, \qquad \tau^{-2} = 2 - \tau. \tag{1}$$

We shall often use the $\mathbf{Q}$-linear mapping $\lambda\colon K \to \mathbf{Q}$ defined by

$$\lambda(a + b\tau) = a = \mathrm{Tr}_{K/\mathbf{Q}}\left(\frac{2(a + b\tau)}{5 + \sqrt{5}}\right) \text{ for } a, b \in \mathbf{Q}.$$

Since $5 + \sqrt{5}$ is totally positive, λ takes positive values in the totally positive elements of K. The following observation will be useful:

the only totally positive integers $x \in \mathfrak{o}$ *such that* $\mathrm{Tr}_{K/\mathbf{Q}}\, x \leqslant 4$ *are* $0, 1, 2, (3 + \sqrt{5})/2 = \tau^2$ *and* $(3 - \sqrt{5})/2 = \tau^{-2}$. (2)

1.2. We denote by H the "ordinary" quaternion algebra $K(i, j, k)$, that is, the quaternion algebra over K which is ramified at both infinite places and unramified elsewhere. The standard conjugation in H will be represented by $x \mapsto x'$; thus, $x' + x$ and $x'x$ are the reduced trace and reduced norm of x, which we shall also simply write Trd x and Nrd x.

It is known that H has a single conjugacy class of maximal orders (cf., e.g., [18] for much more general results); we choose one of them and call it R. Actually, the maximality of R as an order of H will not be used explicitly; all we shall need are the properties stated below, in 1.3, 1.4 and 1.5. For a maximal order, those properties are immediate consequences of the general theory of orders in quaternion algebras (cf. [5] and also [19] for 1.4), but the existence of an order R with those properties can also be verified "by hand," as we shall indicate in the Appendix (Section 8) (cf. also 1.4).

1.3. The ring $\bar{R} = R/2R$ is isomorphic with the matrix algebra $\mathbf{M}_2(\mathbf{F}_4)$ and will often be identified with it. We denote by $x \mapsto \bar{x}$ the reduction homomorphism. One has $\bar{K} = \mathbf{F}_4$ and, for $x \in R$,

$$\overline{\mathrm{Nrd}\, x} = \mathrm{Det}\, \bar{x}, \qquad \overline{\mathrm{Trd}\, x} = \mathrm{Tr}\, \bar{x}. \tag{3}$$

For $y \in \mathbf{M}_2(\mathbf{F}_4)$, we set $y' = (\mathrm{Tr}\, y) \cdot 1 + y$; thus we have $y'y = \mathrm{Det}\, y$ and, for $x \in R$, $\overline{x'} = \bar{x}'$.

1.4. We represent by $R^{(1)}$ the group of elements of R of reduced norm one. It is isomorphic with the double covering $\tilde{\mathfrak{A}}_5$ of the alternating group $\mathfrak{A}_5$. (N.B. Conversely, R can be constructed as the ring generated by the binary icosahedral group, naturally embedded in $\mathrm{Spin}_3(\mathbf{R})$ which one identifies with the norm one group in $\mathbf{R}[i, j, k]$; then, all propecties of R we shall need are straightforward consequences of elementary properties of the icosahedron. Cf. also [6, p. 128].) By reduction mod 2, $R^{(1)}$ maps onto $\mathbf{SL}_2(\mathbf{F}_4)$, the kernel being $\{1, -1\}$.

1.5. The algebra H is an eight-dimensional $\mathbf{Q}$-vector space. If we endow it with the quadratic form $2\lambda \circ \mathrm{Nrd}$, associated to the bilinear form $(x, y) \mapsto \lambda(\mathrm{Trd}\, x'y)$, R is an integral, even, unimodular lattice ("the root lattice of E_8": cf., e.g., [14, Chap. V, Exemple 1.4.3]); in particular,

for $x \in H$, *the relations* $x \in R$ *and* $\lambda(\mathrm{Trd}\, x'R) \in \mathbf{Z}$ *are equivalent.* (4)

1.6. As is well known, the above lattice has 240 vectors of norm 2, forming the root system of E_8; here, it is the union $R^{(1)} \cup R^{(1)}\tau$. This remark can be used to deduce the properties stated in 1.4 from 1.5. Other easy consequences of 1.5 are the maximality of R as an order of H and—using the uniqueness of the "form E_8"—the fact that the ring R is *principal*, from which one also deduces the conjugacy of all maximal orders of H. These facts will not be used here.

1.7. LEMMA 1. (i) *Let $x \in R$ be a cubic root of unity in R and set $y = x + \tau$. Then,* $\operatorname{Nrd} y = 2$ *and $\bar{y}$ is a primitive idempotent in* $\mathbf{M}_2(\mathbf{F}_4)$.

(ii) *If $y, z \in R$ are such that* $\operatorname{Nrd} y = \operatorname{Nrd} z = 2$ *and $\bar{y} = \bar{z}$, then $z \in y \cdot R^{(1)}$.*

(i) We have $y'y = x'x + \tau(x' + x) + \tau^2 = 1 - \tau + \tau^2 = 2$, and also $y' + y \equiv x' + x \equiv 1 \pmod 2$, hence $y^2 \equiv (1 - y')\, y \equiv y \pmod 2$.

(ii) Since $z \in 2R + y = yy'R + y = y(y'R + 1)$, the quotient $y^{-1}z$ belongs to R. Furthermore, $\operatorname{Nrd}(y^{-1}z) = \operatorname{Nrd} y^{-1} \cdot \operatorname{Nrd} z = 1$. Hence (ii).

1.8. PROPOSITION 1. *Every invertible element of* $\mathbf{M}_2(\mathbf{F}_4)$ *is the reduction* mod 2 *of exactly two elements of R of reduced norm* 1, τ^2 *or* τ^{-2}, *opposite to each other. Every nonzero singular element of* $\mathbf{M}_2(\mathbf{F}_4)$ *is the reduction* mod 2 *of exactly eight elements of R of reduced norm* 2.

The first assertion is an immediate consequence of 1.4. Let y be an element of R of reduced norm 2 such that $\bar{y}$ is a primitive idempotent of $\mathbf{M}_2(\mathbf{F}_4)$ (cf. Lemma 1(i)). There are exactly four elements s of $\mathbf{SL}_2(\mathbf{F}_4)$ such that $\bar{y}s = \bar{y}$. By Lemma 1(ii) and 1.4, it follows that $\bar{y}$ is the reduction mod 2 of exactly eight elements of R of reduced norm 2. Our assertion ensues (again using 1.4) since, as is readily verified, every nonzero singular element of $\mathbf{M}_2(\mathbf{F}_4)$ belongs to $\mathbf{SL}_2(\mathbf{F}_4) \cdot \bar{y} \cdot \mathbf{SL}_2(\mathbf{F}_4)$.

1.9. *Remark.* The proposition is also clear by localization.

2. THE LATTICE Λ. MAIN RESULTS

2.1. We shall work in the right H-vector-space H^3. Traditionally, its elements are represented by column vectors, but, for obvious typographical reasons, we shall use rows instead; the reader who wishes to make explicit matrix computations should bear that in mind (and imagine, for instance, that throughout the paper, a row (x_1, x_2, x_3) always stands for its transpose). The space H^3 is endowed with the standard Hermitian form

$$h\colon ((x_1, x_2, x_3), (y_1, y_2, y_3)) \mapsto \sum_{i=1}^{3} x_i' y_i .$$

2.2. In R, we choose once and for all an element e such that $\mathrm{Nrd}\, e = 2$ and that $\bar{e}$ is a primitive idempotent of $\bar{R}$ (cf. Lemma 1(i)), and we denote by Λ the (right) sub-R-module of R^3 defined by

$$\Lambda = \left\{(x_1, x_2, x_3) \in R^3 \mid ex_1 \equiv ex_2 \equiv ex_3 \equiv \sum x_i \pmod 2\right\}. \tag{1}$$

Since $e^2 \equiv e \pmod 2$, we also have

$$\Lambda = \left\{(x_1, x_2, x_3) \in R^3 \mid ex_2 \equiv ex_3 \equiv \sum x_i \pmod 2\right\}. \tag{1'}$$

PROPOSITION 2. *Set* $\mathbf{f}_1 = (1, 1, e)$, $\mathbf{f}_2 = (0, e', e')$, $\mathbf{f}_3 = (0, 0, 2)$. *Then,* Λ *is a free module with basis* $(\mathbf{f}_1, \mathbf{f}_2, \mathbf{f}_3)$.

It clearly suffices to show that any element $\mathbf{x} \in \Lambda$ is a linear combination of the $\mathbf{f}_i$'s. Upon adding a multiple of $\mathbf{f}_1$ to $\mathbf{x}$, we may assume that $\mathbf{x} = (0, x_2, x_3)$. By (1), we have $ex_2 \equiv x_2 + x_3 \equiv 0 \pmod 2$. Therefore, there exist $y_2, y_3 \in R$ such that $x_2 = e'y_2$ and $-x_2 + x_3 = 2y_3$. Then $\mathbf{x} = \mathbf{f}_2 y_2 + \mathbf{f}_3 y_3$, and our assertion is proved.

2.3. PROPOSITION 3. (i) *For* $\mathbf{x} \in H^3$, *the relations* $\mathbf{x} \in \Lambda$ *and* $h(\Lambda, \mathbf{x}) \subset 2R$ *are equivalent.*

(ii) *For* $\mathbf{x} \in \Lambda$, *one has* $h(\mathbf{x}, \mathbf{x}) \neq 2$.

(i) Let $\mathbf{x} = (x_1, x_2, x_3) \in H^3$. The relation $h(\mathbf{f}_3, \mathbf{x}) \in 2R$ means that

$$x_3 \in R. \tag{2}$$

The relation $h(\mathbf{f}_2, \mathbf{x}) \in 2R$ can be written $e(x_2 + x_3) \in 2R$; hence, assuming (2),

$$x_2 \in R \qquad \text{and} \qquad ex_2 \equiv ex_3 \pmod 2. \tag{3}$$

Finally, since $e' \equiv e + 1 \pmod 2$ (because $\bar{e}$ is a primitive idempotent of $\bar{R} \cong \mathbf{M}_2(\mathbf{F}_4)$), the relation $h(\mathbf{f}_1, \mathbf{x}) = x_1 + x_2 + e'x_3 \in 2R$ is equivalent to

$$\sum x_i \equiv ex_3 \pmod 2. \tag{4}$$

Since relations (2), (3), and (4) define Λ, by (1'), assertion (i) follows, in view of Proposition 2.

(ii) Now let $\mathbf{x} = (x_1, x_2, x_3)$ be an element of Λ; suppose $h(\mathbf{x}, \mathbf{x}) = 2$ and set $r_i = x_i' x_i$. Thus

$$\sum r_i = 2. \tag{5}$$

Since the integers r_i are totally positive, it follows from 1.1(2) that one of them (hence one of the coordinates x_i) must vanish. Then, (1) implies that $ex_i \in 2R$

for all i, therefore $2r_i = \mathrm{Nrd}(ex_i) \in 4\mathfrak{o}$ and $r_i \in 2\mathfrak{o}$. Again using (5) and 1.1(2), we see that only one r_i (and consequently only one x_i) is not zero. Now, (1) implies that $x_i \in 2R$, therefore $r_i \in 4\mathfrak{o}$, in contradiction to (5). The proposition is proved.

COROLLARY 1. *The rational quadratic form* $\mathbf{x} \mapsto \lambda(h(\mathbf{x}, \mathbf{x}))$ *restricted to* Λ *is integral, even, and unimodular and does not take the value* 2.

The symmetric bilinear form $b\colon \Lambda \times \Lambda \to \mathbf{Q}$ associated with that quadratic form is $\lambda \circ \mathrm{Trd}_{H/K} \circ h$ and, for $\mathbf{x} \in H^3$, we have the following equivalences:

$$\begin{aligned} b(\Lambda, \mathbf{x}) \in 2\mathbf{Z} &\Leftrightarrow \lambda(\mathrm{Trd}_{H/K}(h(\Lambda, \mathbf{x}))) \subset 2\mathbf{Z} \\ &\Leftrightarrow \lambda(\mathrm{Trd}_{H/K}(r' \cdot h(\Lambda, \mathbf{x}))) \subset 2\mathbf{Z} \qquad \text{for all } r \in R \\ &\Leftrightarrow h(\Lambda, \mathbf{x}) \subset 2R \qquad \text{(by 1.5(4))} \\ &\Leftrightarrow \mathbf{x} \in \Lambda \qquad \text{(by Proposition 3),} \end{aligned}$$

proving the evenness and the unimodularity. Suppose $\mathbf{x}$ is an element of Λ for which $\lambda(h(\mathbf{x}, \mathbf{x})) = 2$. By Proposition 3, this equality means that $h(\mathbf{x}, \mathbf{x}) = 2(1 + a\tau)$ for some nonvanishing rational integer a. Since $h(\mathbf{x}, \mathbf{x})$ is totally positive, we have $1 + a\tau > 0$ and $1 - a\tau^{-1} > 0$ (because τ and $-\tau^{-1}$ are conjugate over $\mathbf{Q}$); hence $-\tau^{-1} < a < \tau$, which amounts to $a = 1$. But then, $h(\mathbf{x}, \mathbf{x}) = 2(1 + \tau) = 2\tau^2$, and $h(\mathbf{x}\tau^{-1}, \mathbf{x}\tau^{-1}) = 2$, in contradiction to Proposition 3(ii).

Remark. The above corollary means that the ($\mathbf{Z}$-) lattice Λ endowed with the quadratic form $\mathbf{x} \mapsto \lambda(h(\mathbf{x}, \mathbf{x}))$ is Leech's lattice (cf. [3]). Alternatively, it provides an existence proof of that lattice.

2.4. *Short vectors. Reflections.* If $\mathbf{a}$ is a nonzero element of H^3, we denote by $r_\mathbf{a}$ the *unitary reflection with respect to* $\mathbf{a}$, that is, the linear mapping

$$r_\mathbf{a}\colon \mathbf{x} \mapsto \mathbf{x} - 2\mathbf{a} \cdot h(\mathbf{a}, \mathbf{a})^{-1} \cdot h(\mathbf{a}, \mathbf{x}) \tag{6}$$

of H^3 onto itself. As is well known (and also readily verified), $r_\mathbf{a}$ preserves h and

$$r_\mathbf{a}^2 = 1. \tag{7}$$

The reflection $r_\mathbf{a}$, which depends only on the one-dimensional subspace $\mathbf{a}H$ of H^3, is also called the reflection with respect to that subspace.

We say that an element $\mathbf{a}$ of Λ is *short* (or is a *short vector*) if $h(\mathbf{a}, \mathbf{a}) = 4$.

PROPOSITION 4. *The reflection with respect to a short vector maps* Λ *onto itself.*

That is an immediate consequence of (6), (7), and Proposition 3(i).

2.5. The remaining sections will essentially aim at proving the following result.

THEOREM. *The automorphism group* $\mathrm{Aut}(\Lambda, h)$ *(i.e., the stabilizer of* Λ *in* $U_3(h)$*) is generated by the reflections with respect to short vectors. It is a perfect central extension of a simple group of order* 604,800[1] *by a group of order* 2.

Remark. That the simple group in question is the sporadic group of Hall–Janko follows from the fact that the latter is known to be the only simple group with that order (cf. [7]), but one can also apply Janko's original characterization [8], using the results in 6.3, 6.4 (including the exercise in 6.3).

3. A CODE IN $\mathbf{M}_2(\mathbf{F}_4)^3$

3.1. From now on, we identify $\bar{R}$ with $\mathbf{M}_2(\mathbf{F}_4)$ in such a way that $\bar{e} = \left(\begin{smallmatrix}0 & 0\\ 0 & 1\end{smallmatrix}\right)$ (which is, of course, no restriction). We recall that, for $x \in \mathbf{M}_2(\mathbf{F}_4)$, we set $x' = x + \mathrm{Tr}\, x \cdot 1$.

LEMMA 2. *Let* x *be an element of* $1 + \bar{e}'\bar{R}$ *with determinant zero and set* $y = x + \bar{e}'$. *Then,* $y^2 = 1$, $y\bar{e}' = \bar{e}'$ *and* $yxy = \bar{e}$.

Since $\bar{e}' = \left(\begin{smallmatrix}1 & 0\\ 0 & 0\end{smallmatrix}\right)$, one has $x = \left(\begin{smallmatrix}0 & u\\ 0 & 1\end{smallmatrix}\right)$ for some $u \in \mathbf{F}_4$, hence $y = \left(\begin{smallmatrix}1 & u\\ 0 & 1\end{smallmatrix}\right)$, and the three identities are readily checked. (The reader who does not like matrices will have no difficulty in devising a more intrinsic proof, using only the fact that $\bar{e}$ is a primitive idempotent of $\bar{R}$.)

3.2. We shall presently work in the right $\bar{R}$-module $\bar{R}^3$ (whose elements are again represented by rows instead of columns: cf. 2.1) endowed with its "standard Hermitian form"

$$\bar{h}\colon ((x_1, x_2, x_3), (y_1, y_2, y_2)) \mapsto \sum_{i=1}^{3} x_i' y_i .$$

Relation 2.1(1) defining Λ means that Λ is the inverse image of the submodule

$$\bar{\Lambda} = \left\{(x_1, x_2, x_3) \in \bar{R}^3 \mid \bar{e}x_1 = \bar{e}x_2 = \bar{e}x_3 = \sum x_i\right\} \tag{1}$$

of $\bar{R}^3$ by the mod 2 reduction $R^3 \to \bar{R}^3$. We note two alternative descriptions of $\bar{\Lambda}$:

[1] The number of seconds in a week!

$\bar{\Lambda}$ is the (right) submodule of $\bar{R}^3$ generated by
$\bar{\mathbf{f}}_1 = (1, 1, \bar{e})$ and $\bar{\mathbf{f}}_2 = (0, \bar{e}', \bar{e}')$; (2)

$\bar{\Lambda}$ consists of all vectors (x_1, x_2, x_3) such that the second rows of the matrices x_1, x_2, x_3 are all equal and their first rows add up to zero. (3)

These assertions are most easily verified by checking that, if $\bar{\Lambda}_1, \bar{\Lambda}_2, \bar{\Lambda}_3$ denote the modules defined by (1), (2), (3), one has the inclusions $\bar{\Lambda}_1 \supset \bar{\Lambda}_2 \supset \bar{\Lambda}_3 \supset \bar{\Lambda}_1$ (the equality $\bar{\Lambda}_1 = \bar{\Lambda}_2$ also follows from Proposition 2).

3.3. A more intrinsic characterization of $\bar{\Lambda}$ is provided by the next proposition. We shall use the following notation: E_1, E_2, E_3 are the three "coordinate axes" of $\bar{R}^3$ (i.e., $E_1 = (1, 0, 0) \cdot \bar{R}$, etc.), for any subset X of $\bar{R}^3$ we set $X^\perp = \{\mathbf{x} \in \bar{R}^3 \mid \bar{h}(X, \mathbf{x}) = \{0\}\}$ and $SL_2(\mathbf{F}_4)^3$ stands for the group of automorphisms of $\bar{R}^3$ of the form $\mathrm{Diag}(s_1, s_2, s_3)$ with $s_i \in SL_2(\mathbf{F}_4)$ ("diagonal automorphisms" of $(\bar{R}^3, \bar{h})$).

PROPOSITION 5. *For a submodule M of $\bar{R}^3$, the following properties are equivalent*:

(i) *M is equivalent to $\bar{\Lambda}$ under the action of $SL_2(\mathbf{F}_4)^3$;*

(ii) *$M = M^\perp$ and $M \cap E_i = \{0\}$ for all i.*

To prove that (i) implies (ii), it clearly suffices to show that $\bar{\Lambda}$ has the properties stated in (ii), a fact which readily follows from (1), (2), (3) (the self-orthogonality of $\bar{\Lambda}$ can also be deduced from Proposition 3(i)).

Now let M be a submodule having properties (ii). We want to show that there is an element of $SL_2(\mathbf{F}_4)^3$ which transforms it into $\bar{\Lambda}$. Since M is self-orthogonal, it is six-dimensional as an $\mathbf{F}_4$-vector space. Therefore, the dimension of $M_{23} = M \cap (E_2 + E_3)$ over $\mathbf{F}_4$ is at least 2. But it cannot be 4 because we would then have $M_{23}^\perp = M_{23} + E_1$, hence $M = M_{23} + M \cap E_1 = M_{23}$. Since M_{23} is an $\bar{R}$-module, it follows that $\dim_{\mathbf{F}_4} M_{23} = 2$. This means that M_{23} has a generator of the form $(0, e_1, ae_1)$, where e_1 is a primitive idempotent of $\bar{R}$ and where a, an element of $\bar{R}$, can be chosen in $SL_2(\mathbf{F}_4)$. There exists $b \in SL_2(\mathbf{F}_4)$ such that $be_1b^{-1} = \bar{e}'$ and, upon transforming M by $\mathrm{Diag}(1, b, ba^{-1})$, we may—and shall—assume that M contains $\bar{\mathbf{f}}_2 = (0, \bar{e}', \bar{e}')$. Let M_1 be the submodule of M consisting of all its elements whose last coordinate belongs to $\bar{e}\bar{R}$. Since $\bar{e}\bar{R} + \bar{e}'\bar{R} = \bar{R}$, we have

$$M_1 + \bar{\mathbf{f}}_2\bar{R} = M_1 + M_{23} = M$$

and, by an obvious dimension argument, the canonical projection $M_1 \to E_1$ is surjective (in fact, it is bijective). Therefore, there exists $\mathbf{x} = (1, x_2, x_3) \in M_1$. We have $x_3 \in \bar{e}\bar{R}$, hence $\mathrm{Det}\, x_3 = 0$, and, expressing the self-orthogonality

of $\mathbf{x}$, $1 + \operatorname{Det} x_2 = 0$, which means that x_2 is an element of $SL_2(\mathbf{F}_4)$. But $\mathbf{x}$ is also orthogonal to $\bar{\mathbf{f}}_2$, therefore $\bar{e}(x_2 + x_3) = 0$. Setting $c = x_3 x_2^{-1}$ and $d = c + \bar{e}'$, we have $\bar{e}(1 + c) = 0$, hence $1 + c \in \bar{e}'\bar{R}$, and, by Lemma 2, $d^2 = 1$, $d\bar{e}' = \bar{e}'$ and $dcd = \bar{e}$. As a result, $\operatorname{Diag}(dx_2, d, d)$ transforms $\mathbf{x}x_2^{-1}d$ into $\bar{\mathbf{f}}_1 = (1, 1, \bar{e})$ and $\bar{\mathbf{f}}_2$ into itself. That proves our claim in view of (2) and considering the fact that M and $\bar{A}$ have the same dimension over $\mathbf{F}_4$.

4. Vector Enumeration

4.1. *The Type of a Vector*

We set $\bar{\tau} = \epsilon$ and we denote by δ the function of $\bar{R}$ into the set $\{0, 1, \epsilon, \epsilon^2, 2\}$ defined as follows: $\delta(x) = \operatorname{Det} x$ if $\operatorname{Det} x \neq 0$ or $x = 0$ and $\delta(x) = 2$ if $\operatorname{Det} x = 0$ and $x \neq 0$. We mean by *ordered type* of an element $\mathbf{x} = (x_1, x_2, x_3)$ of $\bar{R}^3$ (resp. R^3) the sequence $(\delta(x_1), \delta(x_2), \delta(x_3))$ (resp. $(\operatorname{Nrd} x_1, \operatorname{Nrd} x_2, \operatorname{Nrd} x_3)$), and by *type* of $\mathbf{x}$ the corresponding unordered sequence—i.e., set with multiplicities—which we write between vertical lines: thus, for instance, the type of $(1, 1, e)$ can be indifferently written $|\, 1, 1, 2 \,|$, or $|\, 2, 1, 1 \,|$, or $|\, 2 \times 1, 2 \,|$, etc. Two elements $\mathbf{x}, \mathbf{y}$ of R^3 are called *equivalent* if there exists $r \in R^{(1)}$ (i.e., $r \in R$ and $\operatorname{Nrd} r = 1$) such that $\mathbf{y} = \mathbf{x}r$; thus, the nonzero equivalence classes consist of $\operatorname{Card} R^{(1)} = 120$ elements.

4.2. Proposition 6. *The module $\bar{A}$ consists of $6 \cdot 4 \cdot 60$ vectors of type $|\, 1, \epsilon, \epsilon^2 \,|$, $3 \cdot 4 \cdot 60$ vectors of each of the types $|\, 1, 1, 2 \,|$, $|\, \epsilon, \epsilon, 2 \,|$, $|\, \epsilon^2, \epsilon^2, 2 \,|$, $3 \cdot 15$ vectors of type $|\, 0, 2, 2 \,|$, 450 vectors of type $|\, 3 \times 2 \,|$ and the vector zero.*

We only sketch the proof, which is a mere exercise. Note first that

(i) among the 16 vectors of $\bar{A}$ of the form $(1, x_2, x_3)$, there are four vectors of each of the ordered types $(1, \epsilon, \epsilon^2)$, $(1, \epsilon^2, \epsilon)$, $(1, 1, 2)$, and $(1, 2, 1)$.

Indeed, by 3.2(3), the matrices x_2 and x_3 have the forms

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 + a & b \\ 0 & 1 \end{pmatrix}$$

and (i) ensues. One shows, in a similar way, that

(ii) the 15 nonzero vectors of $\bar{A}$ of the form $(0, x_2, x_3)$ have the ordered type $(0, 2, 2)$.

Since $\operatorname{Card} SL_2(\mathbf{F}_4) = 60$, it follows from (i) that $\bar{A}$ contains $4 \cdot 60$ elements of each of the ordered types $(1, \epsilon, \epsilon^2)$ and $(1, 1, 2)$, hence, by symmetry, $4 \cdot 6 \cdot 60$ vectors of type $|\, 1, \epsilon, \epsilon^2 \,|$ and $3 \cdot 4 \cdot 60$ vectors of each of the types $|\, 1, 1, 2 \,|$, $|\, \epsilon, \epsilon, 2 \,|$ and $|\, \epsilon^2, \epsilon^2, 2 \,|$. Similarly, by (ii), $\bar{A}$ has $3 \cdot 15$ elements

of type $|\,0, 2, 2\,|$. Since the numbers given by the proposition add up to $4096 = 4^6 = \operatorname{Card} \bar{\Lambda}$, it remains to be shown that

(iii) if $\mathbf{x} = (x_1, x_2, x_3) \in \bar{\Lambda}$ and $\operatorname{Det} x_i \neq 0$ for some i, then $\mathbf{x}$ has one of the types already considered.

For that, we may assume $\operatorname{Det} x_1 \neq 0$. But then, $(1, x_2x_1^{-1}, x_3x_1^{-1}) = \mathbf{x}x_1^{-1} \in \bar{\Lambda}$, and (iii) follows from (i).

COROLLARY 2. *In Λ there are* 315 *equivalence classes of short vectors distributed into* 3 *classes of type* $|\,0, 0, 4\,|$, 24 *classes of type* $|\,0, 2, 2\,|$, 192 *classes of type* $|\,1, 1, 2\,|$, *and* 96 *classes of type* $|\,1, \tau^2, \tau^{-2}\,|$.

Let $|\,r_1, r_2, r_3\,|$ be the type of a short vector, set $t_i = \operatorname{Tr}_{K/\mathbf{Q}} r_i$, and suppose $t_1 \leqslant t_2 \leqslant t_3$. By definition of short vectors, we have $\sum r_i = 4$, hence $\sum t_i = 8$. Assume first $r_1 = 0$. Then, by 2.1(1), r_2, r_3 are divisible by 2 (cf. the proof of Proposition 3(ii)) and, setting $r_i = 2s_i$, we have $\operatorname{Tr}_{K/\mathbf{Q}} s_2 + \operatorname{Tr}_{K/\mathbf{Q}} s_3 = 4$. By 1.1(2), this implies that $s_2 = 0$ and $s_3 = 2$ or $s_2 = s_3 = 1$, hence

$$|\,r_1, r_2, r_3\,| = |\,0, 0, 4\,| \quad \text{or} \quad |\,0, 2, 2\,|.$$

Suppose now $r_1 \neq 0$. Then t_1 and t_2 must be strictly smaller than 4. Again by 1.1(2), we have

$$|\,r_1, r_2, r_3\,| = |\,1, 2, 2\,| \quad \text{or} \quad |\,1, \tau^2, \tau^{-2}\,|.$$

Now, our assertion follows from Proposition 6 since, by Proposition 1, every vector of $\bar{R}^3$ of type $|\,1, \epsilon, \epsilon^2\,|$ (resp. $|\,1, 1, 2\,|$; $|\,0, 2, 2\,|$; $|\,0, 0, 0\,|$) is the reduction mod 2 of exactly 2^3 (resp. $2^2 \cdot 8$; 8^2; $3 \cdot 120$) vectors of R^3 of type $|\,1, \tau^2, \tau^{-2}\,|$ (resp. $|\,1, 1, 2\,|$; $|\,0, 2, 2\,|$; $|\,0, 0, 4\,|$).

4.3. *Remarks.* (a) In a similar way, one easily computes the number of vectors in Λ of any given type. For instance, the $196{,}560 = 1638 \cdot 120$ vectors $\mathbf{x}$ such that $\lambda(h(\mathbf{x}, \mathbf{x})) = 4$ (cf. [3]) are distributed in

576 equivalence classes of type $|\,1, 1 + \tau, 2 + \tau\,|$,

192 classes of each of types $|\,1 + \tau, 1 + \tau, 2\,|$,
$|\,1 + \tau, 1 + \tau, 2 + 2\tau\,|$, $|\,1, 1, 2\,|$, $|\,1, 1, 2 + 2\tau\,|$,

96 classes of each of the types $|\,1, 1 + \tau, 2 - \tau\,|$, $|\,1, 1 + \tau, 2 + 3\tau\,|$,

48 classes of the type $|\,0, 2, 2 + 2\tau\,|$,

24 classes of each of the types $|\,0, 2, 2\,|$, $|\,0, 2 + 2\tau, 2 + 2\tau\,|$,

3 classes of each of the types $|\,0, 0, 4\,|$, $|\,0, 0, 4 + 4\tau\,|$.

(b) J.-P. Serre has provided me with the following formula (analogous to the one used by Conway in [3] and also deduced from the theory of modular

forms but this time over $\mathbf{Q}(\sqrt{5})$ instead of $\mathbf{Q}$) which gives the number $n(a)$ of solutions in Λ of the equation $h(\mathbf{x}, \mathbf{x}) = 2a$, for any given $a \in \mathfrak{o}$. For $d \in \mathbf{N}$ and $x \in \mathfrak{o}$, $x \neq 0$, let $s_d(x)$ denote the sum $\sum (\text{Norm } \mathfrak{x})^d$ over all ideals $\mathfrak{x}$ of $\mathfrak{o}$ dividing x. Then, if a is a nonvanishing totally positive integer, one has

$$n(a) = 14 \cdot \left(3s_5(a) - s_1(a) - 2s_3(a) - 240 \sum s_1(b)\, s_3(c)\right),$$

where the sum extends over all ordered pairs (b, c) of nonvanishing totally positive integers such that $b + c = a$.

5. Axes and Crosses

5.1. We mean by *axis* (of Λ relative to h) a one-dimensional subspace of H^3 containing a short vector, by *ordered cross* a sequence of three mutually orthogonal axes, and by *cross* a system $(A, \{A_1, A_2\})$ consisting of an axis—the *pole* of the cross—and an unordered pair of axes such that the sequence (A, A_1, A_2) is an ordered cross.

From now on, G denotes the group $\mathrm{Aut}(\Lambda, h)$. We set $\mathbf{e}_1 = (2, 0, 0)$, $\mathbf{e}_2 = (0, 2, 0)$, $\mathbf{e}_3 = (0, 0, 2)$, and $H_i = \mathbf{e}_i H$ for $i = 1, 2, 3$. Note that $(H_1, \{H_2, H_3\})$ is a cross.

5.2. Proposition 7. *The group G permutes the ordered crosses transitively.*

Let $\mathbf{u}_i$ $(i = 1, 2, 3)$ denote three mutually orthogonal short vectors and let α be the linear transformation of H^3 mapping $\mathbf{u}_i$ onto $\mathbf{e}_i$ for all i. Clearly, α preserves h. By Proposition 3(ii), it follows that

$$\text{for } \mathbf{x} \in H^3, \text{ the relations } h(\alpha(\Lambda), \mathbf{x}) \subset 2R \text{ and } \mathbf{x} \in \alpha(\Lambda) \text{ are equivalent.} \quad (*)$$

In particular, $\alpha(\Lambda) \subset R^3$ (because $\mathbf{e}_i \in \alpha(\Lambda)$ for all i). Since $\alpha(\Lambda)$ contains $2R^3$, it is the full inverse image of a submodule M of R^3 by the mod 2 reduction. The module M possesses properties (ii) of Proposition 5: that $M = M^\perp$ follows from (*) and the relation $M \cap E_i = \{0\}$ is an immediate consequence of Proposition 3(ii), in view of Proposition 1. Now, Proposition 5(i) and 1.3 imply that there exists an automorphism β of H^3 of the form $\mathrm{Diag}(b_1, b_2, b_3)$ with $b_i' b_i = 1$ such that $\beta(\alpha(\Lambda)) = \Lambda$, hence $\beta \circ \alpha \in G$. Since $\beta \circ \alpha$ maps $(\mathbf{u}_i H)_{i=1,2,3}$ (an arbitrary ordered cross) onto (H_i), our proposition is proved.

5.3. Lemma 3. (i) *Let $\mathbf{x} = (1, x_2, x_3)$ be a short vector and set $\mathbf{y} = \mathbf{e}_1 - \mathbf{x}$. Then, $r_{\mathbf{y}}(\mathbf{e}_1) = \mathbf{x}$ (for the notation $r_{\mathbf{y}}$, cf. 2.4).*

(ii) *Let $\mathbf{x} = (0, x_2, x_3)$ be a short vector, with $x_2 \neq 0$ and $x_3 \neq 0$, and set $\mathbf{y} = (0, x_1, -x_2)$. Then $(H_1, \{\mathbf{x}H, \mathbf{y}H\})$ is a cross.*

(iii) *If* $\mathbf{x}$ *is as in* (ii), *the reflection* $r_{\mathbf{x}}$ *fixes* H_1 *and permutes* H_2 *and* H_3.

All three assertions follow from straightforward computations (for (ii), note that, by Corollary 2, $x_2'x_2 = x_3'x_3 = 2$).

PROPOSITION 8. *The group* G *permutes the axes transitively.*

Let A be an axis. We claim that there is an element of G mapping A onto H_1. In view of Corollary 2 and of the symmetry of the relations 2.2(1) defining Λ, we may assume that A contains a vector $\mathbf{x} = (x_1, x_2, x_3)$ with $x_1 = 1$ or 0. If $x_1 = 1$, our assertion follows from Lemma 3(i). If $x_1 = 0$, Lemma 3(ii) (or 5.1) shows that H_1 and A belong to an ordered cross and we may use Proposition 7.

Remark. The case $x_1 = 0$ could also be handled by observing that there obviously exists a reflection mapping $\mathbf{x}$ onto a vector all three coordinates of which are different from zero. In that way, one sees right away (using also Lemma 3(iii)) that the axes are permuted transitively by the group generated by all reflections.

COROLLARY 3. *If* $\mathbf{a}$ *is a short vector, one has* $\mathbf{a}H \cap \Lambda = \mathbf{a}R$ *and the axis* $\mathbf{a}H$ *contains a single equivalence class* (*cf.* 4.1) *of short vectors.*

This is obvious if one uses the fact that R is principal (cf. 1.6), but one can also observe that the assertion is clear (by 2.2(1)) if $\mathbf{a}H = H_1$, and then invoke Proposition 8.

COROLLARY 4. *Every axis is the pole of exactly five crosses. Every two orthogonal axes are the two first terms of an ordered cross.*

Use Proposition 8 and Corollaries 2 and 3.

From Corollaries 2, 3, and 4, we deduce:

COROLLARY 5. *There are* 315 *axes,* 1575 *crosses, and* 3150 *ordered crosses.*

6. STABILIZERS

6.1. *The Stabilizer of an Ordered Cross. Order of* G

Our next purpose is to determine the stabilizer in G of the ordered cross $(H_i)_{i=1,2,3}$, that is, the group C of all linear transformations $\mathbf{a} = \mathrm{Diag}(a_1, a_2, a_3)$, with $a_i \in R^{(1)}$ $(=\mathrm{Nrd}^{-1}(1) \cap R$: cf. 1.4), such that

$$\mathbf{a}(\Lambda) = \Lambda. \tag{1}$$

In view of Proposition 2, and with the notation used there, condition (1) can be written $\mathbf{a}(\mathbf{f}_i) \in A$ $(i = 1, 2, 3)$ or, more explicitly,

$$ea_1 \equiv ea_2 \equiv ea_3 \equiv a_1 + a_2 + a_3 e \pmod 2, \tag{2}$$

$$ea_2 e' \equiv ea_3 e' \equiv 0 \pmod 2. \tag{3}$$

Those relations are readily translated in terms of the matrices $\bar{a}_i$. For example, (3) clearly means that $\bar{a}_2$ and $\bar{a}_3$ are upper triangular (remember that $\bar{e} = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$: cf. 3.1). Expressing (2) in a similar way, one gets:

PROPOSITION 9. *The stabilizer C of the ordered cross $(H_i)_{i=1,2,3}$ in G consists of all transformations* $\mathrm{Diag}(a_1, a_2, a_3)$ *where $a_i \in R^{(1)}$ and the matrices $\bar{a}_i$ $(\in \mathbf{M}_2(\mathbf{F}_4))$ have the form*

$$\bar{a}_1 = \begin{pmatrix} c & b_1 \\ 0 & c^{-1} \end{pmatrix}, \qquad \bar{a}_2 = \begin{pmatrix} c & b_2 \\ 0 & c^{-1} \end{pmatrix}, \qquad \bar{a}_3 = \begin{pmatrix} c & b_1 + b_2 \\ 0 & c^{-1} \end{pmatrix}, \tag{4}$$

with $c \in \mathbf{F}_4^\times$ and $b_1, b_2 \in \mathbf{F}_4$.

We denote by $\bar{C}$ the "reduction of C mod 2," that is, the group of all linear transformations $\mathrm{Diag}(\bar{a}_1, \bar{a}_2, \bar{a}_3)$ satisfying (4), by $\bar{C}_2$ the subgroup of all such transformations with $c = 1$ and by C_2 the inverse image of $\bar{C}_2$ in C.

LEMMA 4. (i) *The kernel C_0 of the reduction homomorphism $C \to \bar{C}$ is the elementary Abelian group of order 8 generated by the reflections $r_{\mathbf{e}_i}$.*

(ii) *The group C_0 is the derived group and the center of C_2. Moreover, if an element g of C_2 is such that the commutator $[g, C_2]$ is contained in $\{1, -1\}$, then $g \in C_0$.*

Assertion (i) is clear in view of 1.4 and (ii) readily follows from the definition of C_2 and the fact that the inverse image of the group $\{\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \mid b \in \mathbf{F}_4\}$ in $R^{(1)}$ is a quaternion group of order 8 with center $\{1, -1\}$.

Since $\bar{C}_2$ is the derived group of $\bar{C}$, and has order 2^4, Lemma 4 implies:

PROPOSITION 10. *The derived group of C is the group C_2, of order 2^7. The quotient C/C_2 has order 3.*

COROLLARY 6. *The group G has order* $2^8 \cdot 3^3 \cdot 5^2 \cdot 7 = 1{,}209{,}600$.

Indeed, by Corollary 5, $[G : C] = 3150 = 2 \cdot 3^2 \cdot 5^2 \cdot 7$.

6.2. *The Stabilizer of a Cross. Sylow 2-Subgroups and Their Normalizers*

We keep the notation of 6.1 and denote by $\langle X \rangle$, as usual, the group generated by X.

LEMMA 5. (i) *The only one-dimensional subspaces of H^3 stable by C_0 are the H_i's.*

(ii) *If an element g of G is such that the commutator $[g, C_0]$ is contained in $\langle -1\rangle$, then g belongs to C.*

(iii) *The reflection $r_{\mathbf{f}_2}$ (cf. 2.2 and 2.4) normalizes C and C_2, and $C_2 \rtimes \langle r_{\mathbf{f}_2}\rangle$ is a Sylow 2-subgroup of G, normalized by C.*

(i) is evident.

(ii) If $[g, r_{\mathbf{e}_i}]$ is contained in $\langle -1\rangle$, the conjugate of $r_{\mathbf{e}_i}$ by g is $r_{\mathbf{e}_i}$ or $-r_{\mathbf{e}_i}$. The latter being no reflection, g must centralize $r_{\mathbf{e}_i}$, hence stabilize H_i.

(iii) By Lemma 3, $r_{\mathbf{f}_2}$ normalizes C, hence also C_2 which is its only Sylow 2-subgroup. That $S = C_2 \rtimes \langle r_{\mathbf{f}_2}\rangle$ is a Sylow 2-subgroup of G is now clear by Corollaries 5 and 6. Let a_1 be an element of order 3 of $R^{(1)}$ whose reduction mod 2 is diagonal (i.e., of the form $\left(\begin{smallmatrix} c & 0 \\ 0 & c^{-1}\end{smallmatrix}\right)$), and set $\mathbf{a} = \mathrm{Diag}(a_1, a_1, a_1)$. By Proposition 9, $\mathbf{a}$ belongs to C, hence normalizes C_2. On the other hand, $\mathbf{a}(\mathbf{f}_2)$ is proportional to $\mathbf{f}_2$, therefore $\mathbf{a}$ centralizes $r_{\mathbf{f}_2}$. Thus, S is normalized by $\mathbf{a}$, hence by $C = C_2 \rtimes \langle \mathbf{a}\rangle$ (cf. Proposition 10) and the lemma is proved.

PROPOSITION 11. *Every Sylow 2-subgroup of G stabilizes a unique cross and, conversely, every cross is stabilized by a unique Sylow 2-subgroup.*

It is clear, by Lemmas 4(ii) and 5(i), that $(H_1, \{H_2, H_3\})$ is the only cross stable by the Sylow 2-subgroup $S = C_2 \rtimes \langle r_{\mathbf{f}_2}\rangle$. Conversely, by Proposition 9, the stabilizer of that cross is $C \rtimes \langle r_{\mathbf{f}_2}\rangle$, which has S as its only Sylow 2-subgroup, in view of Lemma 5(iii).

PROPOSITION 12. *Let S be a Sylow 2-subgroup of G, $\mathscr{C}$ the unique cross stable by S, A the pole of $\mathscr{C}$, and r_A the reflection with respect to A. Then:*

(i) *the normalizer of S in G coincides with the stabilizer of $\mathscr{C}$ and is the semidirect product of a group of order 3 by S;*

(ii) *the axis A is the only axis stable by S;*

(iii) *the center of S is $\langle -1, r_A\rangle$ and the center of $S/\langle -1\rangle$ is generated by the image of r_A in that quotient.*

We assume, without loss of generality, that $S = C_2 \rtimes \langle r_{\mathbf{f}_2}\rangle$. Now, (i) is clear, in view of Propositions 11 and 10, (ii) follows from Lemma 5(i), and (iii) is a consequence of Lemmas 5(ii) and 4(ii).

6.3. *The Stabilizer of a Short Vector*

PROPOSITION 13. *The stabilizer of a short vector $\mathbf{a}$, that is, the fixator (=pointwise stabilizer) of the axis $\mathbf{a}H$, stabilizes every cross having that axis as its pole.*

By 5.2, it suffices to show that the fixator of H_1 maps $\mathbf{e}_2$ into $H_2 \cup H_3$. Suppose the contrary. Then, there exists an element of G fixing $\mathbf{e}_1$ and mapping $\mathbf{e}_2$ onto a short vector $\mathbf{x} = (0, x_2, x_3)$ with $x_2 \neq 0$ and $x_3 \neq 0$. Since $(\mathbf{e}_1 + \mathbf{e}_2)\, e^{-1}$ belongs to A, so does $(\mathbf{e}_1 + \mathbf{x})\, e^{-1} = (e', x_2 e^{-1}, x_3 e^{-1})$ and we have, by 2.2(1), $2 \equiv e x_2 e^{-1} \equiv e x_3 e^{-1} \pmod 2$. In other words, x_2 and x_3 belong to $e'Re$, which implies that Nrd x_2 and Nrd x_3 are divisible by 4, in contradiction to Corollary 2.

COROLLARY 7. *The stabilizer of a short vector has order* 2^5.

The proof is immediate, using Propositions 8, 9, and 11, and observing that $r_{\mathbf{f}_2}$ fixes H_1 and permutes H_2 and H_3.

COROLLARY 8. *The group G permutes the short vectors transitively.*

Just compare Corollaries 2 (4.2), 6 (6.1) and 7.

EXERCISE. Show, using Proposition 9, that the stabilizer of a short vector $\mathbf{x}$ is an extra-special group of order 2^5 corresponding to a nonsplit quadratic form (i.e., central product of a quaternion group and a dihedral group of order 8), whose 10 involutions are the reflections with respect to the 10 axes orthogonal to $\mathbf{x}$ (cf. Corollary 4).

6.4. *The Stabilizer of an Axis*

PROPOSITION 14. *Let G_1 be the stabilizer of an axis A in G.*

(i) *If we identify $GL(A)$ with $\mathbf{GL}(H) = H^\times$, the subgroup of $GL(A)$ induced by G_1 is the group $R^{(1)}$ $(= \mathfrak{A}_5)$ and G_1 is an extension of that group by the fixator of A, of order 2^5.*

(ii) *The group G_1 is its own derived group.*

(iii) *The five crosses with pole A are permuted by G_1 according to the alternating group $\mathfrak{A}_5$.*

We assume, without loss of generality, that $A = H_1$ (cf. Proposition 8).

(i) It follows from Corollary 8 that the homomorphism $\alpha\colon G_1 \to R^{(1)}$ defined by $g(\mathbf{e}_1) = \mathbf{e}_1 \cdot \alpha(g)$ is surjective; hence (i).

(ii) Let G_1' be the derived group of G_1. By Proposition 10, G_1' contains C_2 and, in particular, the reflection $r_{\mathbf{e}_2}$. From that fact and 5.2, we deduce that G_1' contains $r_{\mathbf{f}_2}$, hence also the Sylow subgroup $S = C_2 \rtimes \langle r_{\mathbf{f}_2} \rangle$ and, in particular, the fixator of H_1. Now, (ii) follows from (i) since $\mathfrak{A}_5$ is its own derived group.

(iii) is an immediate consequence of (ii) and, say, of 5.2.

Remark. In the sequel, the results of 6.3 and 6.4 will be used only through

Proposition 14(ii), which could also be established as follows. Using Proposition 9, one shows that the stabilizer of the cross $(H_1, \{H_2, H_3\})$ permutes the other crosses with pole H_1 according to the alternating group $\mathfrak{A}_4$. From that fact, one readily deduces Proposition 14(iii) and, by a simple argument, Proposition 14(ii).

EXERCISE. Show by direct geometric arguments that the extension in Proposition 14(i) splits.

7. NORMAL SUBGROUPS

7.1. *The Centralizer of a Sylow 7-Subgroup*

PROPOSITION 15. *In G, the centralizer of an element s of order 7 is the cyclic group of order 14 generated by s and -1.*

Let K_1 denote the extension of K by the seventh roots of unity. Since K is contained in the field of fifth roots of unity, we have $[K_1 : K] = 6$ (cf., e.g., [9, p. 204, Theorem 6 and corollary]), hence $K[t]/(t^7 - 1) = K \oplus K_1$. Consequently, the endomorphism algebra H_1 of H^3 generated by s and the algebra H of homothetic transformations is a quotient of $H \oplus K_1 \otimes_K H$. A dimension argument now shows that $H_1 \cong K_1 \otimes_K H \cong \mathbf{M}_2(K_1)$ and that H^3 is a simple H_1-module. The endomorphism algebra of that module is the center K_1 of H_1 and our assertion follows from the fact that the torsion subgroup of $K_1^\times$ is cyclic of order 14 (cf. [9, p. 204, corollary]).

COROLLARY 7. *An element of order 7 in G cannot normalize a nontrivial p-subgroup with $p = 3$ or 5.*

Indeed, if P is a p-subgroup normalized by s and if P' is the centralizer of s in P, 7 divides $[P : P'] - 1$. Since 7 does not divide $3^a - 1$ for $1 \leqslant a \leqslant 3$ nor $5^a - 1$ for $1 \leqslant a \leqslant 2$, we must have $P = P'$, which contradicts Proposition 15.

7.2. *Proof of the Theorem*

LEMMA 6. *The group G is its own derived group.*

By Proposition 14(ii), the derived group G' of G contains the stabilizer of any axis. In particular, it contains the Sylow 2-subgroups of G (cf. 6.2, Proposition 11). Since any two such subgroups are conjugate in G', it follows from Proposition 12(ii) that G' also permutes the axes transitively, hence the lemma.

PROPOSITION 16. *The only normal subgroups of G are $\{1\}$, $\{1, -1\}$ and G.*

Let F be a normal subgroup of G not contained in $\{1, -1\}$. Its maximal normal 2-subgroup $O_2(F)$ stabilizes an axis (Proposition 11), hence all axes (Proposition 8). It follows that $O_2(F) \subset \{1, -1\}$ as one sees easily, using Proposition 9 (or, alternatively, observing that, in view of Proposition 14(i), every element of $O_2(F)$ induces ± 1 on every axis). Let p be an odd prime dividing the order of F and let N be the normalizer in G of a Sylow p-subgroup of F. By the Frattini argument, $G = NF$. In view of Corollary 7, it follows that 7 divides the order of F and we now choose $p = 7$. By Proposition 15, N is solvable. So, therefore, is G/F and Lemma 6 implies that $G = F$.

The theorem of 2.5 is an immediate consequence of the above proposition.

8. Appendix: Explicit Formulas for the Order R

8.1. *Some Identities*

We set $\theta = i + j$, $\zeta = -\frac{1}{2}(1 + i + j + k)$, $\eta = \theta^{-1}(\zeta + \tau)$ and, for $x \in H$, $x^\theta = \theta^{-1}x\theta$. We have

$$i^\theta = j, \qquad j^\theta = i, \qquad k^\theta = -k, \tag{1}$$

hence

$$\zeta^\theta = \zeta' - \theta. \tag{2}$$

Also,

$$\zeta'\zeta = 1, \qquad \zeta' + \zeta = -1, \tag{3}$$

from which one readily deduces, using 1.1(1) and relation (2), above, that

$$\eta'\eta = 1, \qquad \eta' + \eta = -1. \tag{4}$$

Thus, ζ and η are cubic roots of unity, and

$$\zeta^2 - \zeta = \eta^2 - \eta = 1. \tag{5}$$

8.2. *The Order R*

It is well-known—and readily verified—that

$$R_4 = \{\tfrac{1}{2}(a + bi + ci + dk \mid a, b, c, d \in \mathbf{Z};\ a \equiv b \equiv c \equiv d \pmod 2)\}$$

is an order in the quaternion algebra $\mathbf{Q}(i, j, k)$ (in fact, its unique maximal order up to conjugacy: the notation R_4 is motivated by the introduction). By (1), $\theta R_4 = R_4\theta$ is a two-sided ideal in R_4 which we denote by t. One has

$$R_4/\mathrm{t} = \mathbf{F}_4\,. \tag{6}$$

We set

$$R = \{\theta^{-1}(x + \tau y) \mid x, y \in R_4 \,;\, x \equiv \zeta y \pmod{\mathfrak{t}}\}$$
$$= \{(x + \tau y)\,\theta^{-1} \mid x, y \in R_4 \,;\, x \equiv \zeta' y \pmod{\mathfrak{t}}\}$$

(where the second equality follows from (2)). It is clear that R is a lattice in the $\mathbf{Q}$-vector space H and that

$$R' = R, \tag{7}$$

$$R_4 R \text{ and } R R_4 \text{ are contained in } R. \tag{8}$$

In view of (6),

$R_4 + \tau R_4$ is a sublattice of index 4 in R and the four classes are represented by 0, η, $\zeta\eta$ and $\zeta^2\eta$. (9)

In particular, since $\tau = \theta\eta - \zeta$,

$$R = R_4 + R_4\eta. \tag{10}$$

From (5) and (10), we deduce that $R\eta \subset R$, a relation which, together with (8), shows that $RR \subset R$, which means that *R is an order in H.*

8.3. *The Quadratic Form q*

By (7), Nrd R is contained in $\mathfrak{o}$. Therefore, if we denote by q the quadratic form $2\lambda \circ \mathrm{Nrd}$, we have $q(R) \subset 2\mathbf{N}$. The volume of q restricted to $\mathbf{Z} + \mathbf{Z}i + \mathbf{Z}j + \mathbf{Z}k$ is 4. Consequently, the volume of $q\,|_{R_4}$ is 2; the volume of $q\,|_{R_4 + \tau R_4}$ is 4; and, in view of (9), the volume of $q\,|_R$ is 1. This proves the assertions of 1.5.

8.4. *Reduction* mod 2

Let ϵ be a cubic root of unity in $\mathbf{F}_4$. It is an easy matter to verify, using (10), that there is a ring epimorphism $\rho\colon R \to \mathbf{M}_2(\mathbf{F}_4)$ characterized by the following (somewhat redundant) data:

$$\rho(i) = \begin{pmatrix} 1 & \epsilon \\ 0 & 1 \end{pmatrix}, \quad \rho(j) = \begin{pmatrix} 1 & \epsilon^2 \\ 0 & 1 \end{pmatrix}, \quad \rho(k) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

$$\rho(\tau) = \begin{pmatrix} \epsilon & 0 \\ 0 & \epsilon \end{pmatrix}, \quad \rho(\zeta) = \begin{pmatrix} \epsilon^2 & 0 \\ 0 & \epsilon \end{pmatrix}, \quad \rho(\eta) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Furthermore, the kernel of ρ is readily seen to be $2R$; thus, ρ identifies $R/2R$ with $\mathbf{M}_2(\mathbf{F}_4)$. Note that the element $e = \zeta' + \tau$ of R fullfills the requirements of 2.2 and 3.1: Nrd $e = 2$ (cf. Lemma 1(i)) and $\rho(e) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

8.5. *The Group* $R^{(1)}$

Since $\rho(k)$, $\rho(\zeta)$, and $\rho(\eta)$ generate $\mathbf{SL}_2(\mathbf{F}_4)$, we have $\rho(R^{(1)}) = \mathbf{SL}_2(\mathbf{F}_4)$. But it is easily seen that 1 and -1 are the only elements of $R^{(1)}$ congruent to 1 mod 2. Since -1 is also the only element of order 2 in $R^{(1)}$ (in fact, in $H^{\times}!$), it follows that $R^{(1)} = \mathfrak{A}_5$. One may also give the following explicit description of $R^{(1)}$ (cf. [19, p. 269]): its elements are all the elements of H deduced from 1, $(1 + i + j + k)/2$, and $(1 + \tau^{-1}i + \tau j)/2$ by submitting the fundamental units $1, i, j, k$ to an even permutation and arbitrary changes of sign. We leave as an exercise the problem of extracting from $R^{(1)}$ an $\mathfrak{o}$-basis of R.

Acknowledgment

Part of the content of this paper was presented in a lecture at the 1978 Durham conference on finite group theory; I am grateful to George Glauberman who, on that occasion, pointed out several errors in my earlier presentation. I also thank John McKay for conversations which aroused my interest in the subject and Marie-France Vignéras, to whom I owe my information on the order R.

References

1. A. M. Cohen, "Finite Quaternionic Reflection Groups," Technische Hogeschool Twente, Memorandum 229, 1978.
2. J. H. Conway, A perfect group of order 8, 315, 553, 613, 086, 720, 000, *Bull. London Math. Soc.* **1** (1969), 79–88.
3. J. H. Conway, A characterisation of Leech's lattice, *Invent. Math.* **7** (1969), 137–142.
4. J. H. Conway, Three lectures on exceptional groups, *in* "Finite Simple Groups', (M. B. Powell and G. Higman, Eds.), Chap. VII, pp. 215–247 (Proceedings, Conf. London Math. Soc.), Academic Press, New York/London, 1971.
5. M. Eichler, Zur Zahlentheorie der Quaternionenalgebren, *J. Reine Angew. Math.* **195** (1955), 127–151.
6. F. G. Frobenius, "Gesammelte Abhandlungen," Vol. III, Springer–Verlag, Berlin/New York, 1968.
7. M. Hall and D. Wales, The simple group of order 604, 800, *J. Algebra* **9** (1968), 417–450.
8. Z. Janko, Some new finite simple groups of finite order, I. *Ist. Naz. Alta Mat. Symp. Math.* **1** (1969), 25–64.
9. S. Lang, "*Algebra*," Addison–Wesley, Reading, Mass., 1965.
10. J. Leech, Some sphere packings in higher space, *Canad. J. Math.* **16** (1964), 657–682.
11. J. Leech, Notes on sphere packings, *Canad. J. Math.* **19** (1967), 251–267.
12. J. H. Lindsey II, On a six dimensional projective representation of the Hall–Janko group, *Pacific J. Math.* **35** (1970), 175–186.
13. J. H. Lindsey II, A correlation between $PSU_4(3)$, the Suzuki group and the Conway group, *Trans. Amer. Math. Soc.* **157** (1971), 189–204.
14. J.-P. Serre, "Cours d'arithmétique," 2e éd., Presses Univ. Fr., Paris, 1977.
15. J. Tits, Résumé de cours, *in* "Annuaire du Collège de France," 1976–1977, pp. 57–67.

16. J. TITS, Résumé de cours, *in* "Annuaire du Collège de France," 1977–1978, pp. 80–81.
17. J. TITS, Four presentations of Leech's lattice, Conference on Group Theory at Durham, August 1978; preprint, Paris, 1978.
18. M.-F. VIGNÉRAS, Nombre de classes d'un ordre d'Eichler et valeur au point -1 de la fonction zêta d'un corps quadratique réel, *Enseignement Math.* **21** (1975), 69–105.
19. M.-F. VIGNÉRAS, Simplification pour les ordres des corps de quaternions totalement définis, *J. Reine Angew. Math.* **286/287** (1976), 237–277.