COMMUNICATIONS IN ALGEBRA, 21(6), 1889-1907 (1993)

# The group $L(2,61)$ embeds in the Lie group of type $E_8$

Arjeh M. Cohen

*Dept. AM*
*CWI*
*Kruislaan 413*
*1098 SJ Amsterdam*
*The Netherlands*

Robert L. Griess, Jr.

*Math. Dept.*
*Angell Hall*
*University of Michigan*
*Ann Arbor, MI 48109-1003*
*USA*

Bert Lisser

*Dept. AM*
*CWI*
*Kruislaan 413*
*1098 SJ Amsterdam*
*The Netherlands*

*Keywords: Lie groups, finite simple groups*

Abstract

In this paper, we prove that the Lie group of type $E_8$ has a unique conjugacy class of subgroups isomorphic to the finite simple group $L(2,61)$ of linear fractional transformations over the field of 61 elements. This result settles the last open case of a conjecture made by B. Kostant in 1983 [Kost] concerning the occurrence of the finite simple group $L(2,2h+1)$ in a complex simple Lie group with Coxeter number $h$. It also settles a case left open in the classification of finite simple subgroups of $E_8(\mathbb{C})$ obtained by the first two authors in 1987.

## 1. Introduction

### 1.1. *The problem*

In 1983, Kostant [Kost] conjectured the existence in $E_8\mathbb{C}$) of a subgroup isomorphic to $L(2,61)$, the group of linear fractional transformations over the finite field $\mathbf{F}_{61}$ of order 61. In fact, he conjectured the more general assertion that, for $h$ the Coxeter number of a simple complex Lie group $G$ such that $2h+1$ is a prime power, there would exist a subgroup of $G$ isomorphic to $L(2,2h+1)$. As remarked in [Kost], for nonexceptional type Lie groups when $2h+1$ is a prime power, there is an embedding of $L(2,2h+1)$, provable using only a short argument with the character table; see also [KR].

For $G$ of exceptional type, the following table summarizes the results known to us:

The status of Kostant's conjecture

| group | $h$ | $L(2,2h+1)$ | reference |
|---|---|---|---|
| $G_2$ | 6 | $L(2,13)$ | [Me], [CW] |
| $F_4$ | 12 | $L(2,25)$ | [CW2] |
| $E_6$ | 12 | $L(2,25)$ | [CW2] |
| $E_7$ | 18 | $L(2,37)$ | [KR] |
| $E_8$ | 30 | $L(2,61)$ | |

This paper solves the only open case left, viz. $G$ of type $E_8$ and $h=30$. The existence result contained in this paper deals with one of the unsettled cases in [CG], Table 1. It also establishes uniqueness of the conjugacy class of subgroups in $E_8(\mathbb{C})$ isomorphic to $L(2,61)$. Except for $G_2$, the conjugacy question is unsettled for the other embeddings listed in the table.

Furthermore, we mention that the embedding of $PSU(3,8)$ in $E_7(\mathbb{C})$ (hence in $E_8(\mathbb{C})$) was recently settled in [GrRy] and the embedding questions for $Sz(8)$, $L(2,31)$ and $L(2,32)$ in $E_8(\mathbb{C})$ remain open.

### 1.2. *The group* $L(2,61)$

Throughout this paper, $L$ stands for $L(2,61)$. It is generated by the elements $u$, $t$, $w$, given by the following matrices, which are identified with pairs of elements of $L$ in the usual way:

$$u = \pm\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\quad t = \pm\begin{pmatrix} 2 & 0 \\ 0 & 1/2 \end{pmatrix},\quad w = \pm\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{1}$$

The elements $u$, $t$, $w$ have order 61, 30, and 2, respectively:

$$u^{61} = t^{30} = w^2 = 1, \tag{2a}$$

and satisfy the following relations

$$w^{-1}t\,w = t^{-1} \tag{2b}$$

$$t^{-1}u\,t = u^{46} \tag{2c}$$

$$wu^{-1}w = u\,w\,u \tag{2d}$$

$$w\,u^2\,w = t^{-1}u^{-2}wu^{30} \tag{2e}$$

Using these relations, it can be seen that $L$ consists of the elements $t^j u^k$ and $t^j u^k w u^l$ for $j = 1, \ldots, 30$; $k, l = 1, \ldots, 61$ (each element uniquely represented). This proves the following result.

1.3. **Lemma.** *The equations (2a–e) provide a full set of defining relations of a presentation for $L$ on the generators $u, t, w$.* □

1.4. *The setup*

Let $G(\cdot)$ be the algebraic group scheme of type $E_8$, so that $G(\mathbb{C})$ is the complex Lie group of this type. In section 2 we give an explicit description of the $\mathbf{Z}$-form $g$ of the Lie algebra of type $E_8$ in terms of a Chevalley basis. Thus, for any field $F$, the group $G(F)$ can be viewed as the set of linear transformations of $g_F = g \otimes F$ leaving invariant the Lie algebra structure.

We construct matrices $\overline{u}, \overline{t}, \overline{w}$ that are elements of the group $G(\mathbf{Z}/1831)$ in such a way that the relations (2a–e) are satisfied upon replacement of $u, t, w$ by $\overline{u}, \overline{t}, \overline{w}$, respectively. Since 1831 does not divide the order of $L$, a lifting argument (cf. Corollary 5.2) allows us to conclude that $G(\mathbb{C})$ has a unique conjugacy class of subgroups isomorphic to $L$.

The procedure for finding $\overline{u}, \overline{t}, \overline{w}$ is organized into three main steps. First, as the Borel subgroup $B = \langle u, t \rangle$ of $L$ is a supersolvable group, it embeds in the normalizer of any Cartan subgroup of $G(\mathbf{Q}(\xi))$, where $\xi$ is a primitive 61st root of unity. In section 3, we explicitly construct elements $\overline{t}_0$ and $\overline{u}_0$ of $G(\mathbf{Z}[\xi])$ for which $t \mapsto \overline{t}_0, u \mapsto \overline{u}_0$ determines such an embedding of $B$ in $G(\mathbf{Z}[\xi]) \leq G(\mathbf{Q}(\xi))$. From these data, we easily extract an involution $\overline{w}_0 \in G(\mathbf{Z})$ inverting $\overline{t}_0$. The elements $\overline{u}_0, \overline{t}_0, \overline{w}_0$ thus obtained satisfy the relations (2a), (2b) and (2c). However, they do not satisfy (2d) and (2e).

The element $\overline{t}_0$ has been extensively studied by Kostant, cf. [Kos]. It is conjugate — over a suitable extension of the base ring — to the diagonal element with respect to the Chevalley basis specified in (14) of section 2. In section 4, we first show how to find an element $a$ of $G(R)$ that conjugates $\overline{t}_0$ to diagonal form, and then specialize to $R = \mathbf{Z}/1831$ and explicitly give an element $a^{-1}$ of $G(\mathbf{Z}/1831)$ whose inverse $a$ conjugates $\overline{t}_0$ to diagonal form. Then $a$ can be explicitly determined by Gauß elimination. We set $\overline{t} = a^{-1}\overline{t}_0 a$ and $\overline{u} = a^{-1}\overline{u}_0 a$. At this stage, for

$R = \mathbf{Z}/1831$, the elements $a$ and $a^{-1}$ of $G(R)$ are both known, and so are $\bar{t}$ and $\bar{u}$. As $C_{G(R)}(\bar{t})$ coincides with the maximal torus $H$ with respect to the Chevalley basis, we then know that the image $\overline{w}$ of $w$ should be of shape $a^{-1}\overline{w}_0 a h(\lambda)$, where $h(\lambda)$ represents an arbitrary element of $H$, defined by the 8-tuple $\lambda = (\lambda_1, \ldots, \lambda_8)$.

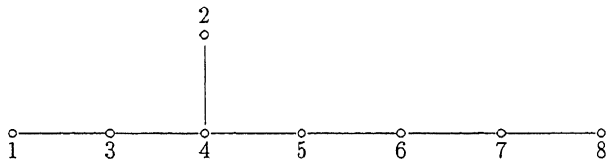
By then the problem of embedding $L$ in $G(R)$ reduces to one of finding the right parameters $\lambda$ for which $\overline{w} = a^{-1}\overline{w}_0 a h$ satisfies (2d) and (2e). Thus, it amounts to solving equations in the 8 unknown $\lambda_1, \ldots, \lambda_8 \in R - \{0\}$. This is a finite problem, but since $|R - \{0\}|^8 = (1830)^8$, we have a domain too large for an exhaustive search, even on the fastest computers. In section 5 we give an explicit solution $\lambda$, describe how it has been found, and argue that it is unique. The main result is stated in Corollary 5.2.

The choice of the prime 1831 for reduction is motivated by the fact that it is the smallest prime $p$ such that $(\mathbf{Z}/p)^*$ contains primitive 30th and 61st roots of unity. When such roots are available, we get a convenient embedding of $B$ in a torus normalizer.

## 2. The Lie algebra $g$

### 2.1. *The root system*

We start with the root system $\Phi$ of type $E_8$, the corresponding root lattice $Q$, and Weyl group $W$. We shall denote by $\alpha_1, \ldots, \alpha_8$ a basis of $Q$ of fundamental roots in $\Phi$. The notation for this root basis is chosen in accordance with [Bou], that is, it corresponds to the labeling of the following diagram




On $Q$ we have a $W$-invariant inner product $(\cdot, \cdot)$ determined by the Cartan matrix. The reflection $s_\gamma$ with root $\gamma \in \Phi$ is given by

$$\alpha s_\gamma = \alpha - (\alpha, \gamma)\gamma \quad (\alpha \in Q). \tag{3}$$

For brevity, we write $s_i = s_{\alpha_i}$. We shall employ the following elements of $W$:

$$\begin{aligned} c_1 &= s_1 s_4 s_6 s_8, \\ c_2 &= s_2 s_3 s_5 s_7, \\ c &= c_1 c_2. \end{aligned} \tag{4}$$

The element $c$ is a so-called Coxeter element (cf. [Bou], also referred to as Coxeter-Killing element, cf. [Kos]) of $W$. It has order 30 and acts semi-regularly on $\Phi$. Each

root $\alpha_i$ $(i = 1, \ldots, 8)$ belongs to a single $\langle c \rangle$-orbit. On the basis $\alpha_1, \ldots, \alpha_8$ of $Q$, the matrix of $c$ is

$$\begin{pmatrix} -1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & -1 & -1 & -1 & -1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 & -1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 \end{pmatrix}. \tag{4a}$$

We use $c$ to label the 240 roots of $\Phi$ as $\beta_\ell$ $(\ell = 1, \ldots, 240)$ as follows:

$$\beta_{30(j-1)+i} = \alpha_j c^{i-1}, \tag{5}$$

where $i \in \{1, \ldots, 30\}$ and $j \in \{1, \ldots, 8\}$.

### 2.2. *The Lie algebra*

As a $\mathbf{Z}$-module, we take the Lie algebra of type $E_8$ to be

$$g = Q \oplus \bigoplus_{\alpha \in \Phi} \mathbf{Z} X_\alpha.$$

Thus, $\operatorname{rk} g = \operatorname{rk} Q + |\Phi| = 248$. Let $\eta : Q \times Q \to \{-1, 1\}$ be the bi-multiplicative map of groups given by the following matrix with respect to $\alpha_1, \ldots, \alpha_8$ :

$$\begin{pmatrix} -1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 \\ -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 \\ -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 \\ -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 1 & -1 & -1 & -1 & 1 \\ 1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix}. \tag{6}$$

Now, multiplication in $g$ is given by the following rules for $\alpha, \beta \in \Phi$.

$$\begin{aligned} [\alpha, \beta] &= 0, \\ [\alpha, X_\beta] &= (\alpha, \beta) X_\beta, \\ [X_\alpha, X_\beta] &= \begin{cases} -\eta(\alpha, \beta) X_{\alpha+\beta} & \text{if } \alpha + \beta \in \Phi, \\ \beta & \text{if } \alpha + \beta = 0, \\ 0 & \text{otherwise.} \end{cases} \end{aligned} \tag{7}$$

By an observation of Frenkel & Kac, cf. [Kac], Exercise 14.5, and G. Segal, cf. [Seg], the product $[\cdot, \cdot]$ defines a Lie algebra structure on $g$. It follows readily from the given Chevalley basis that it is the Lie algebra of type $E_8$. Now let $R$ be any ring. Then the multiplication on $g$ naturally carries over to a multiplication on

$g_R = g \otimes R$. The subalgebra $Q \otimes R$ is commutative; if $R$ is a field, it is a Cartan subalgebra.

### 2.3. *The Lie group*

The group $G(R)$ is defined as the group of all automorphisms of $g_R$, that is, the collection of all linear transformations of the underlying $R$-module preserving the Lie product $[\cdot,\cdot]$. If $R$ is a field, $G(R)$ is the split simple algebraic group of type $E_8$ (in its adjoint representation). In particular, $G(\mathbb{C})$ is the complex Lie group of type $E_8$. We shall indicate some of its elements below.

### 2.4. *Numbering of the basis elements*

In computations, we shall use the following basis for $g$, obtained by use of the root labeling $\beta_\ell$ of (5), which is a Chevalley basis:

$$b_\ell = \begin{cases} X_{\beta_\ell} & \text{if } 1 \le \ell \le 240, \\ \alpha_{\ell-240} & \text{if } \ell \in \{241,\dots,248\}. \end{cases} \tag{8}$$

### 2.5. *The maximal torus H*

Let $R$ be a commutative ring with 1, and denote by $R^*$ its set of invertible elements. For $\lambda_1,\dots,\lambda_8 \in R^*$, let $h(\lambda_1,\dots,\lambda_8)$ be the linear transformation of $g_R$ given by

$$\begin{aligned} \alpha h(\lambda_1,\dots,\lambda_8) &= \alpha, \\ X_\alpha h(\lambda_1,\dots,\lambda_8) &= \prod_{i=1}^{8} \lambda_i^{a_i} X_\alpha \quad \text{if} \quad \alpha = \sum_{i=1}^{8} a_i\alpha_i. \end{aligned} \tag{9}$$

Then $H = \{h(\lambda_1,\dots,\lambda_8) \mid \lambda_1,\dots,\lambda_8 \in R^*\}$ is a commutative subgroup of $G(R)$. Its transformations act diagonally with respect to the basis $(b_\ell)_\ell$. Observe that $h(\lambda_1,\dots,\lambda_8)$ can be characterized as the unique diagonal element of $G(R)$ satisfying

$$X_{\alpha_i} h(\lambda_1,\dots,\lambda_8) = \lambda_i X_{\alpha_i} \text{ for all } i \in \{1,\dots,8\}. \tag{9a}$$

In particular, every diagonal automorphism (with respect to $(b_\ell)_\ell$) of $g_R$ lies in $H$, and, if $R$ is a field, $H$ is a maximal torus of $G(R)$.

### 2.6. *The torus normalizer*

For any $z \in W$, there is a Lie algebra automorphism $\hat{z} \in G(R)$ that is uniquely determined by

$$\hat{z}\,|_Q = z \quad \text{and} \quad X_{\alpha_j}\hat{z} = X_{\alpha_j z} \text{ for all } j \in \{1,\dots,8\}. \tag{10}$$

The group $\widehat{W}$ generated by all $\hat{z}$ for $z \in W$ is the extension of $W$ by an elementary abelian normal subgroup of order $2^8$ contained in $H$. If $R$ is a field, the group $N$ generated by $H$ and $\widehat{W}$ is the full stabilizer in $G(R)$ of the collection of rank 1 $R$-submodules $(Rb_\ell)_\ell$ corresponding to the basis $(b_\ell)_\ell$. It is also the full stabilizer of the Cartan subalgebra $g_R$ and the full normalizer in $G(R)$ of $H$.

## 3. Embedding the Borel subgroup of $L$

We shall denote by $\bar{t}_0$ the extension $\hat{c}$ defined by (10) of the element $c$ given in (4) to an automorphism of $g_R$. Thus

$$\bar{t}_0 = \hat{c}. \tag{11}$$

Up to conjugacy, $\bar{t}_0$ will be the image of $t$ under the embedding of $L$ in $G(R)$ for suitable $R$. Note that (5) and (8) imply $X_\alpha \bar{t}_0^\ell = X_{\alpha c^\ell}$ so that $\bar{t}_0^{30} = 1$. This means that the relevant part of (2a) with $\bar{t}_0$ instead of $t$ is satisfied. The automorphism $\bar{t}_0$ is discussed in [Kos]. It belongs to $N$, has order 30, and induces a Coxeter element in the Weyl group $W$.

We shall exhibit a transformation $\bar{u}_0$ in $H$ such that (2c) and the relevant part of (2a) are satisfied with $\bar{u}_0$ replacing $\bar{u}$ and $\bar{t}_0$ replacing $\bar{t}$. To this end, choose $\xi$ to be a nontrivial 61-st root of 1 in $R$. We ask for integers $a_1, \ldots, a_8$ such that $\bar{u}_0 = h(\xi^{a_1}, \ldots, \xi^{a_8})$ satisfies $\bar{t}_0^{-1} \bar{u}_0 \bar{t}_0 = \bar{u}_0^{46}$. Note that $\bar{u}_0^{61} = 1$ is ensured by the choice of $\xi$. The action of $\bar{t}_0$ on $H$, is given by

$$\bar{t}_0^{-1} h(\xi^{a_1}, \ldots, \xi^{a_8}) \bar{t}_0 = h(\xi_1^{b_1}, \ldots, \xi_1^{b_1}),$$

where $\sum_i b_i \omega_i = (\sum_i a_i \omega_i)c$ (with $(\omega_i)_i$ the basis of $Q$ consisting of the fundamental weights). Thus, (2c) leads to the linear equations

$$\sum_i 46 a_i \omega_i = (\sum_i a_i \omega_i)c,$$

for the $(a_i)_i$ with values in $\mathbf{Z}/61$, which have the unique (up to scalar multiples) nonzero solution $(a_i)_i = (12, 35, 1, 2, 15, 25, 43, 28)$ modulo 61. From this observation, we derive the following uniqueness result for the embedding of $\langle u, t \rangle$ in $G(R)$.

3.1. **Proposition.** *Let $B = \langle u, t \rangle$ be the standard Borel subgroup of $L$ and let $R$ be an algebraically closed field of characteristic 0 or prime to $61 \cdot 30 = 1830$ containing a primitive 61-st root $\xi$ of 1. There is a unique $G(R)$-conjugacy class of subgroups isomorphic to $B$ in $G(R)$ such that the image in $G(R)$ of $\langle u \rangle \leq B$ under such an isomorphism has an 8-dimensional fixed space in $g$. Any such subgroup is conjugate to $\langle \bar{u}_0, \bar{t}_0 \rangle$, where $\bar{t}_0$ is as in (11) and*

$$\bar{u}_0 = h(\xi^{12}, \xi^{35}, \xi, \xi^2, \xi^{15}, \xi^{25}, \xi^{43}, \xi^{28}). \tag{12}$$

PROOF. Let $\bar{t}_1$, $\bar{u}_1$ be the generators of a subgroup of $G(R)$ isomorphic to $B$ corresponding to the elements $t$, $u$, respectively, of $B$. Since the supersolvable group $\langle \bar{t}_1, \bar{u}_1 \rangle$ consists of semisimple elements (due the restrictions on the characteristic of $R$), it stabilizes a Cartan subalgebra (cf. [SpSt]). But all Cartan subalgebras are conjugate, so we may take $\langle \bar{t}_1, \bar{u}_0 \rangle$ to stabilize $Q \otimes R$, that is, to lie in $N$. Since $(61, |W|) = 1$, the structure of $N$ (an extension of $H$ by $W$) implies that $\bar{u}_1$ lies in $H$. Thus, there are $(a_i)_i$ such that $\bar{u}_1 = h(\xi^{a_1}, \ldots, \xi^{a_8})$. Since $B$ is non-commutative, $\bar{t}_1$ induces a nontrivial element of $W = N/H$.

We claim that $\bar{t}_1$ is conjugate to $\bar{t}_0$. By the hypothesis that $\bar{u}_1$ has an 8-dimensional fixed space in $g$, this fixed space must coincide with $Q \otimes R$. Therefore, by the structure of $B$, $\bar{t}_1$ has all of its orbits of length 30 on the eigenspaces $RX_\alpha$ ($\alpha \in \Phi$) of $\bar{u}_1$, whence, viewed as an element of $W$, it has all of its orbits of length 30 on the roots of $W$. Hence, $\bar{t}_1$ induces an element of order 30 in $W$. The orbit lengths imply that $\bar{t}_1$ has determinant 1 on the natural 8-dimensional representation of $W$ since $\bar{t}_1^{15}$ inverts $u_1$ and the Cartan subalgebra fixed by $u_1$. Therefore, in the notation of [Atlas], page 86, $\bar{t}_1$ corresponds to a column headed $15A, 15B$ or $15C$. The latter two classes are interchanged under conjugation by determinant $-1$ elements of $W$, and so fuse to a single class, say $C$ in $W$. Elements of the first class have nontrivial powers with eigenvalue 1 in the natural 8-dimensional representation, so $\bar{t}_1$ corresponds to an element of the class $C$, which must be the conjugacy class of Coxeter elements. So, we may assume $\bar{t}_1 = \bar{t}_0 h$ for some $h \in H$. Since $\bar{t}_1$ induces a regular element (cf. [Spr]), $\bar{t}_1$ is a conjugate of $\bar{t}_0$ for any $h \in H$. Therefore, without loss of generality, we may take $\bar{t}_1 = \bar{t}_0$.

Now, by uniqueness up to scalars of the solution of the above eigenvector equation for $c$, equation (2c) implies that $\bar{u}_1 = \bar{u}_0^\ell$ for some $\ell \in \{1, \ldots, 60\}$. Thus $\langle \bar{u}_1, \bar{t}_1 \rangle = \langle \bar{u}_0, \bar{t}_0 \rangle$, establishing the proposition. □

For later purposes, in order to find the image of $w \in L$ in $G(R)$, we write

$$\bar{w}_0 = h(-1,-1,-1,-1,-1,-1,-1,-1)\,\hat{c}_1, \tag{13}$$

where $\hat{c}_1$ is the automorphism in $G(R)$ defined by (10) using the element $c_1$ given in (4). This defines an involution in $G(R)$.

**3.2. Corollary.** *Let $R$ be field of characteristic 0 or prime to $|L|$ containing a primitive 61-st root of 1. If $L$ embeds in $G(R)$ then, up to conjugacy in $G(R)$ and automorphisms of $L$, we have $u \mapsto \bar{u}_0$ and $t \mapsto \bar{t}_0$, and the image of $w$ in $G(R)$ is contained in $\bar{w}_0 H_0$, where $H_0 = C_{G(R)}(\bar{t}_0)$ is a maximal torus.*

PROOF. Since $g_R$ is a semi-simple $L$-module, analysis as in [CG] shows that $g$ affords a sum of four irreducible characters of $L$, each of degree 62. Consequently, $u$ maps to an element having an 8-dimensional fixed space in $g$.

By the above proposition, the embedding of $L$ in $G(R)$ can be taken so that $t \mapsto \bar{t}_0$ and $u \mapsto \bar{u}_0^b$ for some integer $b \in \{1, \ldots, 60\}$. Composing the morphism with a suitable automorphism (conjugation by a diagonal automorphism) of $L$, we may take $b = 1$.

Since $\bar{t}_0$ corresponds to a regular element of $W$ (cf. [Spr]), the dimension of its centralizer equals the number of orbits on roots, which is 8. Hence, being a semisimple element, its centralizer is a maximal torus. From its action in $W$, cf. (4), it is readily checked that $\overline{w}_0$ inverts $\bar{t}_0$, that is, $\overline{w}_0$ and $\bar{t}_0$ (when replacing $w$ and $t$) satisfy equation (2b).

Denote by $\overline{w}$ the image of $w$ in this embedding. By (2b), $\overline{w}$ inverts $\bar{t}_0$, so $\overline{w}_0\overline{w}$ centralizes $\bar{t}_0$, proving $\overline{w} \in \overline{w}_0 H_0$. □

## 4. Diagonalizing $\bar{t}_0$

Let R be a domain with a primitive $30th$ root of unity. Since the centralizer $H_0$ of section 3.2 is a maximal torus, it is conjugate to $H$. In this section, we shall find an element $a$ of $G(R)$ conjugating $H_0$ into $H$.

From now on, we fix a primitive 30-th root of unity $\epsilon$ in $R$. Thus $\epsilon$ is a zero of the cyclotomic polynomial

$$X^8 + X^7 - X^5 - X^4 - X^3 + X + 1.$$

By [Kos], we know that when $R$ is an algebraically closed field, $\bar{t}_0$ is conjugate in $G(R)$ to the toral element

$$\bar{t} = h(\epsilon, \epsilon, \epsilon, \epsilon, \epsilon, \epsilon, \epsilon, \epsilon). \tag{14}$$

We have:

$$X_\alpha \bar{t} = \epsilon^{ht(\alpha)} X_\alpha, \tag{15}$$

where $ht(\alpha)$ stands for the (usual) height of $\alpha$ with respect to the fundamental basis $\alpha_1, \ldots, \alpha_8$ of roots. Its minimal polynomial on the Cartan subalgebra is the above cyclotomic polynomial.

We shall concentrate on finding an automorphism $a$ of $g_R$ conjugating $\bar{t}_0$ to $\bar{t}$, so that $\bar{t} = a^{-1}\bar{t}_0 a$. Such a transformation $a$ has the following properties: The $\mu$ eigenspace $g(\bar{t}_0, \mu)$ of $\bar{t}_0$ maps onto the $\mu$ eigenspace $g(\bar{t}, \mu)$ of $\bar{t}$; if $\mu = 1$, the latter will be the Cartan subalgebra $Q \otimes R$. Thus, $a^{-1}$ maps $X_\alpha$ to a vector in the eigenspace $g_R(\bar{t}_0, \epsilon^{ht(\alpha)})$. We shall first describe the eigenspaces of $\bar{t}_0$. Denote by $\mu_{30}$ the group of all 30-th roots of unity in $R$. For $\eta \in \mu_{30}$, set

$$S_{9,\eta} = \frac{1}{2} \sum_{l=0}^{29} \eta^{-l} \alpha_1 t^l \quad . \tag{16}$$

Then $S_{9,\eta} = 0$ unless $\eta$ is primitive. If $\eta$ is primitive, the element $S_{9,\eta}$ can be given explicitly as follows:

$$\begin{aligned} S_{9,\eta} = {} & (2 - 2\eta - 2\eta^2 + 2\eta^5 + 4\eta^6 + \eta^7)\alpha_1 \\ & + (-2 - 3\eta + 3\eta^4 + 4\eta^5 + 3\eta^6)\alpha_2 \end{aligned}$$

$$
\begin{aligned}
&+(1-\eta-4\eta^2-\eta^3+\eta^4+3\eta^5+6\eta^6+4\eta^7)\alpha_3\\
&+(-3-3\eta-2\eta^2+\eta^3+5\eta^4+7\eta^5+5\eta^6+2\eta^7)\alpha_4\\
&+(-4-4\eta-\eta^2+2\eta^3+4\eta^4+7\eta^5+3\eta^6+\eta^7)\alpha_5\\
&+(-1-2\eta-\eta^2+\eta^3+2\eta^4+3\eta^5+3\eta^6+3\eta^7)\alpha_6\\
&+(-2\eta-2\eta^2+\eta^3+2\eta^4+\eta^5+3\eta^6+2\eta^7)\alpha_7\\
&+(-1-2\eta+2\eta^3+\eta^4+\eta^5+2\eta^6-\eta^7)\alpha_8.
\end{aligned}
\tag{16a}
$$

Now, the eigenspace $g_R(\bar{t}_0,\eta)$ is spanned by

$$
S_{i,\eta}=\sum_{\ell=0}^{29}\eta^{-\ell}X_{\alpha_i,\epsilon^\ell}=\sum_{\ell=0}^{29}\eta^{-\ell}X_{\alpha_i}\bar{t}_0^{\ell} \tag{17}
$$

for $i\in\{1,\dots,8\}$, and, if $\eta$ is primitive, also $S_{9,\eta}$.

Note that the inverse of the base transformation from $(b_\ell)_\ell$ to $(S_{i,\eta})_{i,\eta}$ is equally straightforward to describe: the $X_\alpha$ ($\alpha\in\Phi$) satisfy

$$
X_{\alpha_i,t^l}=\frac{1}{30}\sum_{\delta\in\mu_{30}}\delta^l S_{i,\delta}\ . \tag{18}
$$

To further pin down $a$, we need a method to determine the $X_\beta a^{-1}$ in terms of the basis $(S(i,\epsilon^{h\iota(\beta)}))_{i,\beta}$. Since $a$ is an automorphism, it suffices to find $X_{\pm\alpha_i}a^{-1}$ for $i=1,\dots,8$. This is done as follows. If $i=1,2,5$, we have

$$
RX_{\alpha_i}a^{-1}=\{X\in g_R(\bar{t}_0,\epsilon)\ \mid\ [X,g_R(\bar{t}_0,\epsilon^j)]=0\} \tag{19}
$$

where $j=15,9,5$ in the respective cases. This yields, up to scalars,

$$
\begin{aligned}
X_{\alpha_1}a^{-1}&=(\epsilon^3-\epsilon^5-\epsilon^6)S_{1,\epsilon}\\
&+(-2+\epsilon+\epsilon^2+\epsilon^4-2\epsilon^6+\epsilon^7)S_{2,\epsilon}\\
&+\epsilon^7 S_{3,\epsilon}\\
&+(2-\epsilon^2-\epsilon^3-2\epsilon^5+2\epsilon^6+\epsilon^7)S_{4,\epsilon}\\
&+(\epsilon-\epsilon^3-\epsilon^6+\epsilon^7)S_{5,\epsilon}\\
&+(-1-\epsilon+\epsilon^2+\epsilon^4+\epsilon^5-\epsilon^7)S_{6,\epsilon}\\
&+(-1-\epsilon+\epsilon^3+\epsilon^4+\epsilon^5+\epsilon^6-\epsilon^7)S_{7,\epsilon}\\
&+(1-\epsilon^2-\epsilon^5+\epsilon^6+\epsilon^7)S_{8,\epsilon}\\
&-S_{9,\epsilon},
\end{aligned}
\tag{19a}
$$

$$
\begin{aligned}
X_{\alpha_2}a^{-1}&=(-1-\epsilon+2\epsilon^2-\epsilon^3+\epsilon^4+\epsilon^5-2\epsilon^7)S_{1,\epsilon}\\
&+(1-\epsilon+\epsilon^3-\epsilon^4-\epsilon^5+\epsilon^6-2\epsilon^7)S_{2,\epsilon}\\
&+(1-\epsilon+\epsilon^3-\epsilon^4-\epsilon^5+\epsilon^6+\epsilon^7)S_{3,\epsilon}
\end{aligned}
$$

$$
\begin{aligned}
&+(1+2\epsilon-\epsilon^2-\epsilon^3-2\epsilon^4+\epsilon^7)S_{4,\epsilon}\\
&+(2+\epsilon-\epsilon^2-2\epsilon^3-\epsilon^4+3\epsilon^7)S_{5,\epsilon}\\
&+(-2-2\epsilon+\epsilon^2+\epsilon^3+2\epsilon^4+2\epsilon^5-\epsilon^7)S_{6,\epsilon}\\
&+(-2+2\epsilon+\epsilon^2-\epsilon^3+\epsilon^4-3\epsilon^6)S_{7,\epsilon}\\
&+(4+2\epsilon-4\epsilon^2-\epsilon^3-2\epsilon^4-3\epsilon^5+3\epsilon^6+4\epsilon^7)S_{8,\epsilon}-2S_{9,\epsilon},
\end{aligned}
\tag{19b}
$$

$$
\begin{aligned}
X_{\alpha_3}a^{-1} = {}&(-3-\epsilon+2\epsilon^2+\epsilon^3+\epsilon^4+3\epsilon^5-2\epsilon^6-2\epsilon^7)S_{1,\epsilon}\\
&+(-1-\epsilon+\epsilon^3+\epsilon^4+\epsilon^5+\epsilon^6-2\epsilon^7)S_{2,\epsilon}\\
&+(-1+\epsilon-\epsilon^3+\epsilon^4+\epsilon^5-\epsilon^6+\epsilon^7)S_{3,\epsilon}\\
&+(-1+\epsilon^2+\epsilon^3-2\epsilon^6-\epsilon^7)S_{4,\epsilon}\\
&+(-2+\epsilon+\epsilon^2+\epsilon^4-2\epsilon^6-\epsilon^7)S_{5,\epsilon}\\
&+(\epsilon^2-\epsilon^3-\epsilon^7)S_{6,\epsilon}\\
&+(2-\epsilon^2-\epsilon^3-\epsilon^4+\epsilon^6)S_{7,\epsilon}\\
&+(-2-2\epsilon+2\epsilon^2+\epsilon^3+2\epsilon^4+\epsilon^5-\epsilon^6-2\epsilon^7)S_{8,\epsilon}-2S_{9,\epsilon}
\end{aligned}
\tag{19c}
$$

Analogously, we can compute $X_{-\alpha_i}a^{-1}$, for these values of $i$ (just replace $\epsilon$ by its inverse). Next for $i=3,4$, we can find $X_{\alpha_i}a^{-1}$ from

$$
RX_{\alpha_i}a^{-1} = [X_{-\alpha_j}a^{-1}, [X_{\alpha_j}a^{-1}, g_R(\bar{t}_0,\epsilon)]] \tag{20}
$$

where $j=1,2$, respectively. For $m=6,7,8$, we obtain $X_{\alpha_m}a^{-1}$ up to scalar multiples by successively computing

$$
\begin{aligned}
&RX_{\alpha_m}a^{-1} =\\
&\quad [X_{-\alpha_{m-1}}a^{-1}, [X_{-\alpha_{m-2}}a^{-1}, [X_{\alpha_{m-2}}a^{-1}, [X_{\alpha_{m-1}}a^{-1}, g_R(\bar{t}_0,\epsilon)]]]].
\end{aligned}
\tag{21}
$$

Finally, for arbitrary $\beta\in\Phi$, the vector $X_\beta a^{-1}$ can be determined by induction on $|ht(\beta)|$ using (7)

$$
X_\beta a^{-1} = -\eta(\gamma,\delta)[X_\gamma a^{-1}, X_\delta a^{-1}] \tag{22}
$$

whenever $\gamma,\delta\in\Phi$ with $\beta=\gamma+\delta$.

Noting that variations of the scalar multiples do not effect the $H$-coset of $a$, we summarize the above as follows:

**4.1. Proposition.** *Let $R$ be an integral domain containing a primitive 30-th root of 1, denoted by $\epsilon$. For $\bar{t}_0$ as in (11) and $\bar{t}$ as in (14), there is an automorphism*

*$a \in G(R)$ such that*

$$\bar{t} = a^{-1}\bar{t}_0 a. \tag{23}$$

*An example of such an element $a$ is determined up to an element of $H$, by (19), (20), (21) and (22), and the corresponding analogues for $-\alpha_j$ instead of $\alpha_j$ with $\epsilon^{-1}$ instead of $\epsilon$.* □

We shall need $a$ and $a^{-1}$ in $G(R)$, where $R = \mathbf{Z}/1831$, the field of prime order 1831.

By Gauß elimination on each of the eigenspaces for $\bar{t}$, and use of (18), it is straightforward to find $a$ from $a^{-1}$.

To find $a^{-1}$, we take $\epsilon = 1604 \in R$. The above equations then lead to the following expressions:

$$\begin{aligned}
X_{\alpha_1}a^{-1} &= 1277S_{1,\epsilon} + 1479S_{2,\epsilon} + 384S_{3,\epsilon} + 1435S_{4,\epsilon} + \\
&\quad 241S_{5,\epsilon} + 1636S_{6,\epsilon} + 1291S_{7,\epsilon} + 1367S_{8,\epsilon} + 1830S_{9,\epsilon} \\
X_{-\alpha_1}a^{-1} &= 554S_{1,\epsilon^{-1}} + 660S_{2,\epsilon^{-1}} + 1111S_{3,\epsilon^{-1}} + 396S_{4,\epsilon^{-1}} + \\
&\quad 1608S_{5,\epsilon^{-1}} + 195S_{6,\epsilon^{-1}} + 97S_{7,\epsilon^{-1}} + 464S_{8,\epsilon^{-1}} + 1830S_{9,\epsilon^{-1}} \\
X_{\alpha_2}a^{-1} &= 337S_{1,\epsilon} + 1505S_{2,\epsilon} + 826S_{3,\epsilon} + 1408S_{4,\epsilon} + \\
&\quad 1602S_{5,\epsilon} + 909S_{6,\epsilon} + 952S_{7,\epsilon} + 16S_{8,\epsilon} + 1829S_{9,\epsilon} \\
X_{-\alpha_2}a^{-1} &= 1494S_{1,\epsilon^{-1}} + 1069S_{2,\epsilon^{-1}} + 740S_{3,\epsilon^{-1}} + 423S_{4,\epsilon^{-1}} + \\
&\quad 1116S_{5,\epsilon^{-1}} + 922S_{6,\epsilon^{-1}} + 46S_{7,\epsilon^{-1}} + 1815S_{8,\epsilon^{-1}} + 1829S_{9,\epsilon^{-1}} \\
X_{\alpha_3}a^{-1} &= 1071S_{1,\epsilon} + 1667S_{2,\epsilon} + 1158S_{3,\epsilon} + 91S_{4,\epsilon} + \\
&\quad 109S_{5,\epsilon} + 189S_{6,\epsilon} + 620S_{7,\epsilon} + 92S_{8,\epsilon} + 605S_{9,\epsilon} \\
X_{-\alpha_3}a^{-1} &= 1071S_{1,\epsilon^{-1}} + 608S_{2,\epsilon^{-1}} + 798S_{3,\epsilon^{-1}} + 91S_{4,\epsilon^{-1}} + \\
&\quad 891S_{5,\epsilon^{-1}} + 189S_{6,\epsilon^{-1}} + 247S_{7,\epsilon^{-1}} + 92S_{8,\epsilon^{-1}} + 605S_{9,\epsilon^{-1}} \\
X_{\alpha_4}a^{-1} &= 631S_{1,\epsilon} + 1310S_{2,\epsilon} + 488S_{3,\epsilon} + 1716S_{4,\epsilon} + \\
&\quad 1175S_{5,\epsilon} + 1403S_{6,\epsilon} + 871S_{7,\epsilon} + 1269S_{8,\epsilon} + 1675S_{9,\epsilon} \\
X_{-\alpha_4}a^{-1} &= 631S_{1,\epsilon^{-1}} + 1083S_{2,\epsilon^{-1}} + 915S_{3,\epsilon^{-1}} + 1716S_{4,\epsilon^{-1}} + \\
&\quad 601S_{5,\epsilon^{-1}} + 1403S_{6,\epsilon^{-1}} + 31S_{7,\epsilon^{-1}} + 1269S_{8,\epsilon^{-1}} + 1675S_{9,\epsilon^{-1}} \\
X_{\alpha_5}a^{-1} &= 201S_{1,\epsilon} + 907S_{2,\epsilon} + 1773S_{3,\epsilon} + 1741S_{4,\epsilon} + \\
&\quad 711S_{5,\epsilon} + 532S_{6,\epsilon} + 593S_{7,\epsilon} + 887S_{8,\epsilon} + 1829S_{9,\epsilon} \\
X_{-\alpha_5}a^{-1} &= 1630S_{1,\epsilon^{-1}} + 817S_{2,\epsilon^{-1}} + 1482S_{3,\epsilon^{-1}} + 90S_{4,\epsilon^{-1}} + \\
&\quad 269S_{5,\epsilon^{-1}} + 1299S_{6,\epsilon^{-1}} + 948S_{7,\epsilon^{-1}} + 944S_{8,\epsilon^{-1}} + 1829S_{9,\epsilon^{-1}}
\end{aligned} \tag{24}$$

$$
\begin{aligned}
X_{\alpha_6}a^{-1} &= 895S_{1,\epsilon} + 1421S_{2,\epsilon} + 1240S_{3,\epsilon} + 720S_{4,\epsilon} + \\
&\quad 1785S_{5,\epsilon} + 161S_{6,\epsilon} + 503S_{7,\epsilon} + 836S_{8,\epsilon} + 1789S_{9,\epsilon} \\
X_{-\alpha_6}a^{-1} &= 895S_{1,\epsilon^{-1}} + 1520S_{2,\epsilon^{-1}} + 494S_{3,\epsilon^{-1}} + 720S_{4,\epsilon^{-1}} + \\
&\quad 1287S_{5,\epsilon^{-1}} + 161S_{6,\epsilon^{-1}} + 1172S_{7,\epsilon^{-1}} + 836S_{8,\epsilon^{-1}} + 1789S_{9,\epsilon^{-1}} \\
X_{\alpha_7}a^{-1} &= 1105S_{1,\epsilon} + 629S_{2,\epsilon} + 1308S_{3,\epsilon} + 1669S_{4,\epsilon} + \\
&\quad 1358S_{5,\epsilon} + 738S_{6,\epsilon} + 528S_{7,\epsilon} + 1280S_{8,\epsilon} + 1693S_{9,\epsilon} \\
X_{-\alpha_7}a^{-1} &= 1105S_{1,\epsilon^{-1}} + 35S_{2,\epsilon^{-1}} + 1537S_{3,\epsilon^{-1}} + 1669S_{4,\epsilon^{-1}} + \\
&\quad 1173S_{5,\epsilon^{-1}} + 738S_{6,\epsilon^{-1}} + 990S_{7,\epsilon^{-1}} + 1280S_{8,\epsilon^{-1}} + 1693S_{9,\epsilon^{-1}} \\
X_{\alpha_8}a^{-1} &= 373S_{1,\epsilon} + 790S_{2,\epsilon} + 200S_{3,\epsilon} + 1362S_{4,\epsilon} + \\
&\quad 560S_{5,\epsilon} + 1494S_{6,\epsilon} + 811S_{7,\epsilon} + 1300S_{8,\epsilon} + 129S_{9,\epsilon} \\
X_{-\alpha_8}a^{-1} &= 373S_{1,\epsilon^{-1}} + 108S_{2,\epsilon^{-1}} + 375S_{3,\epsilon^{-1}} + 1362S_{4,\epsilon^{-1}} + \\
&\quad 1050S_{5,\epsilon^{-1}} + 1494S_{6,\epsilon^{-1}} + 834S_{7,\epsilon^{-1}} + 1300S_{8,\epsilon^{-1}} + 129S_{9,\epsilon^{-1}}
\end{aligned}
$$

## 5. The embedding of $L$ in $G(\mathbf{Z}/1831)$

As before, let $\mathbf{F} = \mathbf{Z}/1831$ and $\epsilon = 1604$. We shall write $\xi = 1287$. Thus $\epsilon$ and $\xi$ are a 30-th and a 61-st root of 1, respectively. Recall the definition of $h(\lambda)$ from (9) and $\overline{w}_0$ from (13). Let $a$ be as determined by (24) and $\overline{t} = a^{-1}\overline{t}_0 a$ as in (23) and (14). Put $\overline{u} = a^{-1}\overline{u}_0 a$, where $\overline{u}_0$ is as in (12).

**5.1. Theorem.** *Let* $\mathbf{F}$ *be the field* $\mathbf{Z}/1831$ *and suppose* $\lambda \in (\mathbf{F}^*)^8$. *The transformations* $\overline{u}$, $\overline{t}$ *and* $\overline{w} = a^{-1}\overline{w}_0 a h(\lambda)$ *satisfy the relations (2a–e) (with* $u, t, w$ *replaced by their barred namesakes) if and only if*

$$\lambda = (1640, 474, 645, 52, 341, 974, 326, 1391).$$

*Consequently, there is a unique conjugacy class of subgroups of* $G(\mathbf{F})$ *isomorphic to* $L$.

PROOF. Recall that (2a), (2b), (2c) are already satisfied for any triple $\overline{u}, \overline{t}, \overline{w}$. We shall concentrate on solving $\lambda$ from equations pertaining to (2d).

Set $\overline{w}_1 = a^{-1}\overline{w}_0 a$ and rewrite (2d) to

$$h(\lambda)\overline{u}\,\overline{w}_1 h(\lambda) = (\overline{u}\,\overline{w}_1)^{-1} h(\lambda)^{-1} (\overline{u}\,\overline{w}_1)^{-1}.$$

Applying both sides to $\alpha_i = b_{240+i}$, using that $\alpha_i h(\lambda) = \alpha_i$ for $i = 1, \ldots, 8$, and taking the $j$-th entry ($1 \le j \le 248$) of the result, we obtain

$$(\overline{u}\,\overline{w}_1)_{240+i,j} x_{j^\tau} = \sum_k ((\overline{u}\,\overline{w}_1)^{-1})_{i,k} ((\overline{u}\,\overline{w}_1)^{-1})_{k,j} x_k, \tag{25}$$

where $x_k = h(\lambda)_{k,k}^{-1}$ and $j^\tau$ is such that $h(\lambda)_{j^\tau,j^\tau} = h(\lambda)_{j,j}^{-1}$. Thus, due to the indexing chosen in (5) and (8), $j^\tau = j$ if $j > 240$ and $j^\tau \equiv j + 15 \bmod 30$ with $30m + 1 \le j^\tau, j \le 30(m+1)$ for some integer $m$ if $1 \le j \le 240$. Observe that $x_{241} = \cdots = x_{248} = 1$, that $\lambda_i = x_{30(i-1)+16}$ are the eight important values ($i = 1, \ldots, 8$)

we wish to determine. Disregarding momentarily that all $x_k$ for $1 \leq k \leq 240$ can be written as quotients of two monomials in the $\lambda_i$ $(i = 1, \ldots, 8)$, we view (25) as a set of $8 \times 248 = 1984$ linear equations in the 240 variables $x_k$ $(k = 1, \ldots, 240)$. Gauß elimination shows that there is a unique solution. The values of the eight important variables are:

$$\lambda = (x_{30(i-1)+16})_{i=1,\ldots,8} = (1640, 474, 645, 52, 341, 974, 326, 1391).$$

Now a direct check shows that, for this solution $\lambda$, the element $\overline{w} = \overline{w}_1 h(\lambda)$ of $G(\mathbf{Z}/1831)$ satisfies both (2d) and (2e). By Lemma 1.3, this establishes the first assertion. The second one follows from the first assertion and Corollary 3.2. □

We now come to the main result of this paper, which, as stated in the introduction, solves one of the open cases of [CG] and proves a conjecture of B. Kostant [Kost].

**5.2. Corollary.** *There is a unique conjugacy class of subgroups of $G(\mathbb{C})$ isomorphic to $L$.*

PROOF. For existence, use Theorem 5.1 and the Lifting Lemma of [Gr], Appendix B.

For uniqueness up to conjugacy, consider a subgroup $L$ of $G(\mathbb{C})$ with $L \cong L(2, 61)$. Let $V = g_{\mathbb{C}}$ be the adjoint module and let $E$ be the field of $|L|$-th roots of unity. Then, there is a representation of $E[L]$ which affords this $L$-representation; let $W$ be the relevant $E[L]$-module. The invariant in $Hom_{\mathbb{C}[L]}(V \otimes V, V)$ which gives the Lie algebra structure is a linear combination of elements of $Hom_{E[L]}(W \otimes W, W)$ involving finitely many complex numbers. Therefore, there are a finitely generated $\mathbf{Q}$-algebra $R$ and an $R$-free $R[L]$-module whose complexification is $V|_{\mathbb{C}[L]}$. Each element of a Chevalley basis for this complex Lie algebra may be written as a complex linear combination of a basis of $W$. Therefore, replacing $R$ by another finitely generated $\mathbf{Q}$-algebra, if necessary, we arrange for this $R[L]$-module to be a Lie algebra with a Chevalley basis. Now factor out a maximal ideal $I$ of $R$ so as to get both the Lie algebra and $L$-module structures written over a field $E'$. By the Hilbert Nullstellensatz, $E'$ is a finite degree field extension of $E$. Clearly, $E'$ can be embedded in $\mathbb{C}$ and the module complexifies to $V|_{\mathbb{C}[L]}$ again. There is therefore a finite extension $K$ of the 1831-adic numbers and an embedding of $K$ into $\mathbb{C}$ whose image contains $E'$. Moreover, the presence of the Chevalley basis guarantees that the Lie algebra structure on the $E'[L]$-module is of type $E_8$. This puts $L$ into $G(K)$.

Let $S$ be the integers of $K$ and let $J$ be the maximal ideal. From the theory of maximal compact subgroups of $p$-adic groups, cf. [BT], [T], we know that $L$ is contained in a subgroup of the form $G_0(S)$, where the functor $G_0$ is associated to a proper subdiagram of the extended Dynkin diagram for $G$. According to the character argument of [CG], 5.2.1, regarding $L$, which works in characteristic

prime to $|L|$, the only functor allowed here is $G$. Therefore, $L$ is in $G(S)$ and so modulo $G(S, J^n)$, the congruence subgroup associated to the ideal $J^n$ of $S$, it reduces to a subgroup of $G(S/J^n) \cong G(S)/G(S, J^n)$. By 5.1, the image of $L$ in $G(S/J)$ is unique up to conjugacy. If two subgroups $L_1$ and $L_2$ of $G(S)$ isomorphic to $L$ are conjugate modulo $G(S, J^n)$, then they are conjugate modulo $G(S, J^{n+1})$ since $G(S, J^n)/G(S, J^{n+1})$ is a finite nilpotent group of order prime to $|L|$. We get an element of $G(S)$ which conjugates $L_1$ to $L_2$ as follows. We may arrange for a sequence of elements $x_n$ in $G(S)$ such that $x_n$ conjugates $L_1 G(S, J^n)$ to $L_2 G(S, J^n)$ and such that $x_n$ and $x_{n+1}$ are congruent modulo $G(S, J^n)$. It follows that this sequence of elements has a limit and so we get a conjugating element of $G(S)$, identified with the inverse limit of the $G(S)/G(S, J^n)$. □

## 6. Remarks

### 6.1. *The field R*

An open problem is to decide for which fields $R$ there is an embedding of $L$ in $G(R)$. It is conceivable that our particular solution might be lifted explicitly to one in $G(R)$ for some subring $R$ of $\mathbb{C}$, possibly even to $\mathbf{Q}(\theta)$, where $\theta$ is a 1830-th root of unity or $\sqrt{61}$. From this, embeddings in $G(F)$ for certain finite fields $F$ would follow.

The g.c.d. over all primes $p$ of $|G(\mathbf{Z}/p)|$ equals

$$2^{30} \cdot 3^{13} \cdot 5^5 \cdot 7^4 \cdot 11^2 \cdot 13^2 \cdot 19 \cdot 31$$

which is not divisible by $|L|$, so $L$ does not embed in every finite Chevalley group of type $E_8$. On the other hand, Lagrange's Theorem does *not* exclude the possibility of an embedding of $L$ in, for example, $G(\mathbf{Z}/11)$, even though $\mathbf{Z}/11$ contains few roots of unity.

### 6.2. *Some history*

The work described in sections 2,3, and 4 was completed about six years ago by the first two authors. At the time, the knowledge that $\overline{w}$ should be found in $\overline{w}_0 H$ led them to produce 57 polynomial equations, in the eight variables $\lambda_1, \ldots, \lambda_8$, each consisting of no more than 9 monomials. These equations had been obtained from a careful analysis of the traces of compositions of restrictions of $\overline{u}$ and $\overline{w}$ to eigenspaces of $\overline{t}$. It has been checked that the above solution $\lambda$ is also a zero of the set of 57 polynomials, but we do not know whether it is the only one. This set of 57 polynomials still provides an interesting test case for procedures solving polynomial equations in several variables.

### 6.3. *Verification of the computations*

All of the computations mentioned in sections 3, 4 and 6.2 were originally performed by the first author using the programming language A68, on a CDC Cyber

computer. Recently, they were redone by the first and third authors, using the computer algebra packages Maple and LiE (cf. [M], [LiE]). The set of 57 polynomials discussed in 6.2 marked the end of the work on the CDC computer. The same 57 polynomials were found by use of Maple.

As a result of the LiE and Maple computations, we have on file $248 \times 248$ matrices such as $a$, $a^{-1}$, $h(\lambda)$, $\bar{t}_0$, $\overline{w}_0$, and $\overline{u}_0$, as well as Maple and LiE routines for performing the various computations needed to verify Theorem 5.1. The nonsparse matrices $a$ and $a^{-1}$ have been stored in the naive way; they require 335 Kb storage. The matrices $h(\lambda)$ and $\overline{u}_0$ are diagonal, the matrices $\bar{t}_0$ and $\overline{w}_0$ are monomial, whence much easier to store and work with on computer. We now discuss the verification of the computations by dividing them into three separate parts.

One part is the verification that the matrices $\overline{u} = a^{-1}\overline{u}_0 a$, $\bar{t} = a^{-1}\bar{t}_0 a$ and $\overline{w} = a^{-1}\overline{u}_0 a h(\lambda)$ , with $\lambda$ as in Theorem 5.1, satisfy the required relations. This requires multiplications of square matrices of dimension 248 over the field of 1831 elements. Such a verification on a work station size computer turned out be hard (but possible) for Mathematica, but an easy matter for LiE.

Another part is the verification that the three matrices $\overline{u}$, $\bar{t}$, $\overline{w}$ preserve the $E_8$ Lie algebra product. This turned out to require too much memory for Maple or Mathematica.

An independent check was performed (and is available on file) with a program written in C in which the Lie algebra product is encoded as a 3-dimensional array of dimension 248 (available on file in Maple format).

Finally, the Gauß elimination proving uniqueness of the solution $\lambda$ was carried out originally in LiE. The space requirements for this are not as great as those of the previous part and so can be checked rather straightforwardly in several packages, however with varying speed performances. It has been succesfully verified in GAP, cf. [GAP].

To finish we provide the LiE code for obtaining the equations (25) from the matrices $\overline{u}$ and $\overline{w}_1$ on file, assuming that $\overline{u}\overline{w}_1$ and $\overline{u}\overline{w}_1^{-1}$ have already been computed. They are called `uw` and `uwi`, respectively.

```
p = 1831 #the prime involved

#preparing the right hand side; here i and j are as in (25)
rhs(int i,j) = { loc ans = null(248);
  for k=1 to 248 do ans[k] = (uwi[240+i,k] * uwi[k,j]) %p
  od; ans
}

tau(int k) = { loc ans = k;
  if k <= 240 then  loc ell =  k%30;  loc m = k-ell;
    if ell == 0 then ell= -15
```

```
      else  ell = (ell+15)%30; if ell == 0 then ell =30 fi;
      fi; ans = m +ell;
    fi; ans
}
#prepare the 1984 x 241 coefficient matrix of the equations
eqstotal = null(0,241)

for i =1 to 8 do   eqs = null(248,248);
  for j=1 to 248 do eqs[j] = rhs(i,j); loc k = tau(j);
    eqs[j,k] = (eqs[j,k] - uw[240+i,j]) %p
  od;
  #now add last 8 columns in 241-th column
  for j=1 to 248 do
    eqs[j, 241] = (
    eqs[j, 241] + eqs[j, 242] + eqs[j, 243] + eqs[j, 244] +
    eqs[j, 245] + eqs[j, 246] + eqs[j, 247] + eqs[j, 248] )%p;
  od;
  #remove the last 7 columns
  eqs= *(*eqs-242-242-242-242-242-242-242);
  #append eqs to eqstotal
  eqstotal = eqstotal^eqs
od;
```

The resulting 1984 × 241 matrix *eqstotal* is the input coefficient matrix for Gauß elimination.

Ample care has been taken to give sufficient details (up to our ordering of basis elements, cf. (8)) so that a reader can repeat the computations independently. Nevertheless, it may be helpful to have copies of the matrices as well as the Lie algebra product referred to above. Requests for electronic copies can be made to the first author.

### 6.4. *Acknowledgments*

We are very grateful to Vermaseren and Faugère for looking at the 57 polynomial equations mentioned in section 6.2. Both used programs of their own that might have led to a solution. It turned out, however that the equations (25), which were found only recently, constitute a much more tractable set for finding the solution $\lambda$.

We thank the referees and editor for their commentary on earlier versions of this article and in particular for suggesting a more elaborate exposition of the computer aspects in this work.

## 7. References

[Atlas] J. Conway, R. Curtis, S. Norton, R. Parker, R. Wilson, *Atlas of Finite Groups*, Clarendon Press, Oxford, 1985.

[Bou] N. Bourbaki, *Groupes et algèbres de Lie, Chap. 4, 5, et 6*, Hermann, Paris, 1968.

[BT] F. Bruhat & J. Tits, "Groupes réductifs sur un corps local", *Inst. Hautes Etudes Sci. Publ. Math.* **41**, (1972). 5–251.

[CG] A.M. Cohen, R.L. Griess, Jr., *On finite simple subgroups of the complex Lie group of type $E_8$*, pp. 367–405 in "Proceedings of Symposia in Pure Math.", 1987.

[CW] A.M. Cohen, D.B. Wales, "Finite subgroups of $G_2(\mathbb{C})$", *Comm. Algebra* **11**, (1983), 441–459.

[CW2] A.M. Cohen, D.B. Wales, *Finite subgroups of $F_4(\mathbb{C})$ and $E_6(\mathbb{C})$*, preprint, (1992).

[GAP] M. Schönert et al., *GAP, Groups, Algorithms and Programming*, Manual, Lehrstuhl D für Mathematik, Aachen, (1992).

[Gr] R.L. Griess, Jr., "Elementary abelian $p$-subgroups of algebraic groups", *Geom. Dedicata* **39**, (1991), 253–305.

[GrRy] R.L. Griess, Jr., A.J.E. Ryba, *Embeddings of $U_3(8)$, $Sz(8)$ and the Rudvalis group in algebraic groups of type $E_7$*, preprint, 1991.

[Kac] V.G. Kac, *Infinite dimensional Lie algebras, 2nd ed.*, Cambridge University Press, 1985.

[Kos] B. Kostant, "The principal three-dimensional subgroups and the Betti numbers of a complex simple Lie group", *Amer. J. Math.* **81**, (1959), 973–1032.

[Kost] B. Kostant, *A tale of two conjugacy classes*, Colloquium lecture of the Amer. Math. Soc., (1983).

[KR] P.B. Kleidman, A.J.E. Ryba, *Kostant's conjecture holds for $E_7$: $L_2(37) < E_7(\mathbb{C})$*, preprint, 1992.

[LiE] M.A.A. van Leeuwen, A.M. Cohen, B. Lisser, *LiE, A package for Lie group computations*, CAN, Amsterdam, 1992.

[Me] A. Meurman, *An embedding of $PSL(2,13)$ in $G_2(\mathbb{C})$*, pp. 157–165 in "article in Lie Algebras and Related Topics, SLN 933", Lecture Notes in Mathematics 933, 1982.

[M] B.W Char, K.O. Geddes, M.B. Monagan, S.M. Watt, *Maple Reference Manual 5th ed.*, WATCOM, Waterloo (Ont.), 1988.

[Seg] G. Segal, "Unitary representations of some infinite dimensional groups", *Communications in Math. Physics* **80**, (1981), 301–342.

[Spr] T.A. Springer, "Regular elements of finite reflection groups", *Invent. Math.* **25**, (1974), 159–198.

[SpSt] T.A. Springer, R. Steinberg, *Conjugacy classes in Classical Groups*, pp. E82–E100 in "Seminar on algebraic groups and related finite groups" (A. Borel, ed.), Lecture Notes in Mathematics 131, Springer-Verlag, 1970.

[T] J. Tits, *Reductive groups over local fields*, pp. 29–69 in "Automorphic forms, representations and L-functions", Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977, Part 1 XXXIII, 1979.

Received: January 1992

Revised: October 1992