ISRAEL JOURNAL OF MATHEMATICS 82 (1993), 45–86

EMBEDDINGS OF THE GROUP $L(2,13)$ IN GROUPS OF LIE TYPE E_6

BY

ARJEH M. COHEN

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

AND

DAVID B. WALES

Caltech, Sloan Lab, Pasadena, CA 91125, USA

Dedicated to John Thompson for his keen interest in broad areas of mathematics and in mathematicians

ABSTRACT

In this paper we show there is exactly one conjugacy class of subgroups of $E_6(\mathbb{C})$ isomorphic to $L(2,13)$ with each of the characters $13+14$ and $1+12+14$ on a 27-dimensional module for E_6. The one with character $13+14$ is a subgroup of the irreducible closed subgroup of type G_2. There is a unique conjugacy class for each of the three algebraic conjugate characters $1+12+14$. Our arguments have applications to fields of characteristic prime to $|L(2,13)|$.

1. Introduction

In this paper we consider embeddings of $L(2,13)$ as a subgroup of F_4 or E_6. These embeddings appear as subgroups of E_6 and F_4 over various fields. Aschbacher [AsI–IV] has given a list of all possible maximal subgroups of the simple group $E_6(k)$ and so has Magaard [Mag] for $F_4(k)$ for large classes of fields k. In each case they left open the possibility of such embeddings. In [CW92] we were also faced with the possible existence of such embeddings over $\mathbb{C}$. The possible embeddings are described by their character on the 27 dimensional space $\mathbf{K}$ acted on by E_6 (see [CW92]) and its restriction to F_4. The explicit actions we consider here on

Received June 11, 1992 and in revised form December 16, 1992

K are $13+14$ for E_6 and $1+12+14$ for F_4. We only deal here with characteristics prime to $|L(2,13)|$ and so the character descriptions apply. Here the integers 1, 12, 13 and 14 refer to the first characters of $L(2,13)$ listed in the Atlas [Atlas] with the corresponding degree. There are two characters of degree 14; three of degree 12. The second character of degree 14 does not occur in any embedding (see [CW92]). The three characters of degree 12 are algebraically conjugate.

In this paper we construct matrices for the action of $L(2,13)$ acting on **K** with character $13 + 14$ and show that this action is unique. It is known that E_6 contains a G_2 which in turn contains an $L(2,13)$ which has this character. This means that any $L(2,13)$ with this character on **K** must be in a G_2 and in turn is contained within a closed proper subgroup of positive dimension. We also develop enough information to show there is a unique conjugacy class of subgroups isomorphic to $L(2,13)$ with character $1 + 12 + 14$.

The Borel subgroup of $L(2,13)$ is a Frobenius group of order 78. The restrictions to such a subgroup of the two $L(2,13)$ characters $1 + 12 + 14$ and $13 + 14$ coincide. In Section 2 we show that there is a unique class of Frobenius groups of order $13 \cdot 6$ with the appropriate character. The rest of the paper is organized as follows. In Section 3 we state the main theorem for the complex numbers, $\mathbb{C}$. In Section 4 we analyze the possibilities for the 14 dimensional subspace common to both embeddings and determine it to within a few possibilities. In Section 5 we determine the action on the 13 dimensional subspace for the embedding with character $13 + 14$ and show it is unique. In section 6 we show there is a unique solution (up to algebraic conjugacy) for the embedding in which the character is $1+12+14$. In Section 7 we find a solution for the each of the cases over the complex numbers and discuss an automorphism which fuses some of the solutions. In Section 8 we discuss fields of characteristic prime to $|L(2,13)|$. In Sections 3 through 7 we are concerned with results over $\mathbb{C}$ which we use in Section 8 with other fields. During the work over $\mathbb{C}$, we use reduction mod 79 for certain 79-local integers as a tool to infer results over $\mathbb{C}$.

We thank Michael Aschbacher for helpful discussions throughout the work.

2. Frobenius groups of order $13 \cdot 6$ in $\widetilde{E}$

We work extensively with a 27-dimensional vector space over a field, k, of characteristic prime to $|L(2,13)|$ containing primitive third and thirteenth roots of unity on which E_6 acts. Let **K** be the vector space whose vectors are the triples

(x_1, x_2, x_3) of 3 by 3 matrices x_i ($i = 1,2,3$), where addition and scalar multiplication are defined coordinatewise, and equip $\mathbf{K}$ with the cubic form $\langle\cdot\rangle$ given by

$$\langle x\rangle = \det x_1 + \det x_2 + \det x_3 - \operatorname{trace} x_1x_2x_3$$

for $x = (x_1, x_2, x_3)$ in $\mathbf{K}$. The symmetric trilinear form corresponding to $\langle\cdot\rangle$ will be denoted by $\langle\cdot,\cdot,\cdot\rangle$. Thus,

$$\langle x,y,z\rangle \;=\; \langle x+y+z\rangle - \langle x+y\rangle - \langle x+z\rangle - \langle y+z\rangle + \langle x\rangle + \langle y\rangle + \langle z\rangle$$

for $x, y, z \in \mathbf{K}$. It is well known that aut $\mathbf{K}$ (i.e., the group of linear transformations of $\mathbf{K}$ preserving $\langle\cdot\rangle$) is the nonsplit central extension $\widetilde{E}$ of $E_6(k)$ by a group of order three. We shall also write $\widetilde{E}_6(k)$ instead of $\widetilde{E}$ to denote the dependency on k. In fact, for an arbitrary ring R, we shall also write $\widetilde{E}_6(R)$ to denote the subgroup of $\mathrm{GL}(R^{27})$ stabilizing $\langle\cdot\rangle$, thereby interpreting R^{27} as the free R-module generated by the natural basis consisting of all triples of matrices $e^i_{j,k}$ ($1 \le i,j,k \le 3$) having 0 at every entry but for the (j,k)-entry of the i-th matrix, which entry equals 1.

This description of the Lie group of type E_6 was first given by [Freu], but other descriptions were known as early as 1901 by [Di].

There are two bases we will use for $\mathbf{K}$. The first is the abovementioned basis $e^i_{j,k}$ ($1 \le i,j,k \le 3$). We shall also use the basis and trilinear form described in [AsI], 3.1. In particular, the 27-dimensional space $\mathbf{K}$ has a basis X_i, $X_{i'}$, X_{jk}, where $1 \le i \le 6$, $1 \le j < k \le 6$. For convenience, we shall adopt the conventions

$$X_{ji} = -X_{ij} \quad (\text{if } j > i) \quad \text{and} \quad X_{-i} = -X_i, \quad X_{-i'} = -X_{i'}.$$

The trilinear form is nonzero only for the triples X_i, $X_{j'}$, X_{ij} if $i \ne j$; and X_{ij}, X_{kl}, X_{mn} where

$$\{i,j,k,l,m,n\} = \{1,2,3,4,5,6\}.$$

The values are all ± 1 as follows: $\langle X_i, X_{j'}, X_{ij}\rangle = 1$ if $i < j$. To determine the sign of $\langle X_{ij}, X_{kl}, X_{mn}\rangle$ identify the triple of (ordered) pairs $\{ij, kl, mn\}$ in the triple below,

triples of pairs		
12 34 56	14 23 56	16 25 34
12 35 64	14 25 63	16 23 45
12 36 45	14 26 35	16 24 53
13 24 65	15 26 43	
13 26 54	15 24 36	
13 25 46	15 23 64	

and then $\langle X_{ij}, X_{kl}, X_{mn}\rangle = 1$ if the triple of pairs is the same as in the table (up to an even number of inversions of pairs) and $\langle X_{ij}, X_{kl}, X_{mn}\rangle = -1$ if one or three of the pairs are inverted.

These bases can be related schematically using the following diagram:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1' & 2' & 3' \\ 23 & 31 & 12 \end{pmatrix}, \quad \begin{pmatrix} 41 & 51 & 61 \\ 42 & 52 & 62 \\ 43 & 53 & 63 \end{pmatrix}, \quad \begin{pmatrix} 4' & -4 & 56 \\ 5' & -5 & 64 \\ 6' & -6 & 45 \end{pmatrix}.$$

Now $e^i_{j,k} = X_y$ if y occurs in the j,k-entry of the i-th matrix of the diagram.

We denote by H the subgroup of $\widetilde{E}$ consisting of all elements which are diagonal with respect to the standard basis $e^i_{j,k}$ $(1 \le i,j,k \le 3)$. An arbitrary element $h \in H$ has the shape

$$h(\alpha,\beta,\gamma,\delta,\epsilon,\zeta) = \begin{pmatrix} \alpha\gamma^{-1}\delta^{-1} & \alpha\beta\gamma & \alpha\delta \\ \alpha^{-1}\beta^{-1}\gamma^{-1}\delta^{-1} & \alpha^{-1}\gamma & \alpha^{-1}\beta^{-1}\delta \\ \gamma^{-1}\delta^{-1} & \beta\gamma & \delta \end{pmatrix},$$
$$\begin{pmatrix} \gamma\delta\zeta^{-1}\epsilon^{-1} & \beta\gamma\delta\epsilon & \gamma\delta\zeta \\ \beta^{-1}\gamma^{-1}\zeta^{-1}\epsilon^{-1} & \gamma^{-1}\epsilon & \beta^{-1}\gamma^{-1}\zeta \\ \delta^{-1}\zeta^{-1}\epsilon^{-1} & \beta\delta^{-1}\epsilon & \delta^{-1}\zeta \end{pmatrix},$$
$$\begin{pmatrix} \alpha^{-1}\zeta\epsilon & \alpha\beta\zeta\epsilon & \epsilon\zeta \\ \alpha^{-1}\beta^{-1}\epsilon^{-1} & \alpha\epsilon^{-1} & \beta^{-1}\epsilon^{-1} \\ \alpha^{-1}\zeta^{-1} & \alpha\beta\zeta^{-1} & \zeta^{-1} \end{pmatrix}.$$

Here, each entry represents the scalar by which the corresponding basis element of $\mathbf{K}$ is multiplied in the action of h. In particular $h(1,1,\omega,\omega,\bar{\omega},\bar{\omega})$, with ω a primitive cube root of unity represents a central element of $\widetilde{E}$ of order 3.

It is easy to see that H is a maximal torus (that is, a connected abelian subgroup consisting of semisimple elements) of $\widetilde{E}$ whose eigenspaces are the 1-dimensional linear subspaces spanned by the standard basis $e^i_{j,k}$ $(1 \le i,j,k \le 3)$.

Recall that the Borel subgroup of $L(2,13)$ is a Frobenius group of order $13 \cdot 6$. We first analyze the possibilities for Frobenius groups of order $13 \cdot 6$ in $\widetilde{E}$. Let ϵ be a fixed primitive 13-th root of 1. The element $\overline{u} = h(\epsilon^3, \epsilon^{11}, \epsilon, \epsilon, \epsilon^8, \epsilon^4)$ is an element of order 13 in $\widetilde{E}_6(k)$. On the basis $X_i, X_{i'}, X_{ij}$, this means $\overline{u}$ has the following eigenvalue pattern:

$X_{3'}$	X_4	X_{34}					
0	0	0					
X_1	X_2	X_5	X_6	X_{13}	X_{23}	X_{35}	X_{36}
1	2	8	10	12	11	5	3
$X_{1'}$	$X_{2'}$	$X_{5'}$	$X_{6'}$	X_{14}	X_{24}	X_{45}	X_{46}
10	11	4	6	3	2	9	7
X_3	$X_{4'}$	X_{12}	X_{15}	X_{16}	X_{25}	X_{26}	X_{56}
4	9	1	8	6	7	5	12

Here the integers below the X_i, $X_{j'}$, X_{ij} are the powers of ϵ to which X_i, $X_{j'}$, X_{ij} are multiplied under the action of $\overline{u}$. Thus, $\overline{u}$ has fixed space $kX_{3'} + kX_4 + kX_{34}$, and each nontrivial eigenvalue occurs with multiplicity 2.

Throughout the paper we assume familiarity with some of the geometry of K given by the trilinear form. In particular the Weyl group acts transitively on the projective points formed by the basis vectors in a rank three manner. Given any two points, there may or may not be another point for which the trilinear form is nonzero on the triple. If so there is a unique such point and the triple spans a special plane. The set $\{X_{3'}, X_4, X_{34}\}$ fixed by $\overline{u}$ is such a triple.

Consider the element $\overline{t} \in \mathrm{GL}(\mathrm{K})$ determined by

$$X_4 \mapsto -X_{3'} \mapsto X_{34} \mapsto X_4$$

$$X_1 \mapsto X_3 \mapsto -X_{14} \mapsto X_{13} \mapsto -X_{4'} \mapsto -X_{1'} \mapsto X_1$$

$$X_2 \mapsto -X_{15} \mapsto X_{6'} \mapsto X_{23} \mapsto -X_{26} \mapsto -X_{46} \mapsto X_2$$

$$X_5 \mapsto -X_{16} \mapsto X_{2'} \mapsto -X_{35} \mapsto X_{25} \mapsto X_{24} \mapsto X_5$$

$$X_6 \mapsto -X_{12} \mapsto X_{5'} \mapsto -X_{36} \mapsto X_{56} \mapsto -X_{45} \mapsto X_6$$

Thus $\overline{t}X_{13} = -X_{4'}$, $\overline{t}X_{1'} = -X_1$, $\overline{t}X_{34} = X_4$. It is straightforward to check that $\overline{t}$ preserves the trilinear form which shows $\langle \overline{u}, \overline{t} \rangle$ is a subgroup of $\widetilde{E}$. Moreover, $\overline{t}\overline{u}\overline{t}^{-1} = \overline{u}^{10}$, so $\langle \overline{u}, \overline{t} \rangle$ is a Frobenius subgroup of $\widetilde{E}$ of order 78.

The signs above have been determined so that the triples of basis vectors for which the form is ± 1 are permuted with the signs preserved. It is sometimes easy to obtain permutations of the lines generated by the basis vectors which preserve the triples but not the signs. By considering representatives in $\mathrm{GL}(27,k)$, it can be shown there is an element in $\widetilde{E}$ which permutes the basis vectors of $\mathbf{K}$ in the same way. In the arguments below we obtain permutations which preserve the signs and infer without further mention that there is an element in $\widetilde{E}$ which permutes the subspaces in the same way.

LEMMA 2.1: *Suppose k is algebraically closed and B is a Frobenius group of order 39 in $\widetilde{E}_6(k)$ and suppose the elements of order 13 and 3 have the same distribution of eigenvalues as $\overline{u}$ and $\overline{t}^2$, respectively, above. Then B is conjugate in $\widetilde{E}_6(k)$ to a subgroup of $\langle \overline{u}, \overline{t}^2, z\rangle$ where z is the central scalar of order 3. Any extension to a Frobenius group of order 78 is conjugate to a subgroup of $\langle \overline{u}, \overline{t}, z\rangle$.*

Proof: As B is supersolvable and consists of semisimple elements, it is conjugate in $\widetilde{E}$ to a subgoup of the normalizer of a torus (cf. [SpSt]). Assume $B = \langle u, s\rangle$ where u of order 13 is diagonal in the basis $\{X_i, X_{i'}, X_{ij}\}$ for $\mathbf{K}$ and suppose s of order three permutes this basis. In the case of a Frobenius group of order 78 let it be $\langle u, t\rangle$ with $s = t^2$, $j = t^3$. We will prove the lemma in a series of steps.

A. THE FIXED VECTORS OF u SPAN A SPECIAL PLANE. In this and the next section we consider the basis vectors to be projective points and consider the permutation action of s on these points. The fixed space of u has dimension 3 and so s (satisfying $\dim(C_{\mathbf{K}}(s)) = 9$ by hypothesis) must permute the three basis vectors fixed by u. The points of a 3-cycle of s either span a special plane or no two of its points are in a special plane. To see this note that if $\{X, sX\}$ is in a special plane, then so are $\{sX, s^2X\}$ and $\{s^2X, X\}$. But given two basis vectors in a special plane, there is a unique third basis vector in the plane with both, and so $\{X, sX, s^2X\}$ spans a special plane. This follows for example because of the rank three action of the Weyl group on the 27 points. In particular each point is in five special planes. The ones for X_1 are $\{X_1, X_{i'}, X_{1i}\}$ for $2 \leq i \leq 6$. None of the points in a special plane with $X_{i'}$ are in a special plane with X_1 except X_{1i} and so the cycle spans a special plane.

The permutation action of the Weyl group is transitive on triples of points which span a special plane and transitive on the triples whose pairs are not in a special plane; the latter triples span a singular plane. A representative which spans a special plane is $\{X_{3'}, X_4, X_{34}\}$. A representative of a triple from a singular plane is $\{X_1, X_2, X_3\}$.

The fixed basis vectors of u are a 3-cycle of s. Suppose they are not in a special plane. After conjugation we can assume they are $\{X_1, X_2, X_3\}$. Let ϵ^i be the eigenvalue of $X_{4'}$. Let ϵ^j be the eigenvalue for X_{14}. Then

$$1 = \langle X_1, X_{4'}, X_{14}\rangle = \langle uX_1, uX_{4'}, uX_{14}\rangle = \epsilon^i\epsilon^j.$$

Consequently X_{14} has eigenvalue ϵ^{-i}. Similarly X_{24} and X_{34} have eigenvalue ϵ^{-i}. However, there are only two eigenvalues ϵ^{-i} for the action of u on $\mathbf{K}$. Here $i \neq 0$ as the three eigenvectors with eigenvalue 1 are X_1, X_2 and X_3. This shows the fixed vectors of u span a special plane.

As the triples which span a special plane are conjugate in $W(E_6)$, we may assume u fixes some specific special plane which we assume to be $X_{3'}, X_4, X_{34}$. The remaining 24 basis vectors for $\mathbf{K}$ are divided into three disjoint sets of eight according to whether they lie on a special plane with $X_{3'}, X_4$, or X_{34}. The action of s permutes these sets of eight. The sets of eight are listed in separate rows in the listing of $\overline{u}$ appearing above. The eight corresponding to $X_{3'}$ are first, the eight corresponding to X_4 second, and the eight corresponding to X_{34} third.

The centralizer of $X_{3'}, X_{34}, X_4$ in $W(E_6)$ (isomorphic to $W(D_4)$) is transitive on any of these sets of eight. Each element in each set of eight is paired with the unique other element with which it forms a special plane. For example the pairs for the first row are $\{X_1, X_{13}\}$, $\{X_2, X_{23}\}$, $\{X_5, X_{35}\}$, $\{X_6, X_{36}\}$. These all form a special plane with X_3'. The automorphisms of $W(E_6)$ which fix $X_{3'}, X_{34}, X_4$ act transitively on the four pairs connected to any given point. The kernel of this action interchanges the elements in an even number of pairs and the kernel of both actions is the identity. By taking a power if necessary we may assume that $X_{3'} \mapsto X_4 \mapsto X_{34}$. As explained above, we are not concerned with signs here.

By taking an appropriate power of u we can assume the eigenvalue associated with u acting on X_1 is ϵ, a primitive 13-th root of 1. We can assume

$$sus^2 = u^3 \quad \text{or} \quad sus^2 = u^9.$$

B. THE 3-CYCLES OF s ON THE BASIS VECTORS ALL SPAN SPECIAL PLANES. Recall s normalizes the element u of order 13 with trace 1. There are two classes of elements of order three in $W(E_6)$ which act fixed point freely on the 27 points.

They are denoted by 3AB and 3D in [Atlas]. For the former, the 3-cycles all span special planes; for the latter, three 3-cycles span special planes and six do not. Let D be the stabilizer in $W(E_6)$ of $X_{3'}, X_4, X_{34}$. Suppose the points in some 3-cycle of s do not span a special plane. As D is transitive on the sets of eight above, we can assume X_1 is the element from its row. Recall from above this means no two points of its orbit are in a special plane. Its image must be in the second row as $X_{3'}$ is taken to X_4. The only elements in this row not in a special plane with X_1 are $X_{1'}, X_{24}, X_{45}, X_{46}$ and so its image must be one of these. Now by transitivity of D_{X_1} on $X_{1'}, X_{24}, X_{45}, X_{46}$, we can assume $X_1 \mapsto X_{1'}$. The only possibilities for the image of $X_{1'}$ are X_{25}, X_{26}, and X_{56}. By transitivity of $D_{X_1, X_{1'}}$ on X_{25}, X_{26}, X_{56}, we can assume $X_{1'} \mapsto X_{25}$, and so $X_{25} \mapsto X_1$.

Because three of the 3-cycles span special planes and $X_{3'}, X_4, X_{34}$ is one of them, the remaining two must include X_2, X_5 or X_6 together with its paired entry in the same row. There is an involution in $D_{X_1, X_{1'}, X_{25}}$ interchanging X_2 and X_5 and so we may assume the 3-cycle containing X_2 does not span a special plane. The possible images of X_2 are $X_{2'}, X_{45}, X_{46}$. Recall X_{13} is paired with X_1 and so its image is X_{14}. But now the image of the special plane spanned by $X_{1'}, X_2, X_{12}$ must be a special plane and so the image of X_2 must be in a special plane with X_{25}. This means X_2 cannot map to X_{25}. Similarly using the special plane spanned by $X_{25}, X_2, X_{5'}$ it cannot map to X_{46}. Consequently $X_2 \mapsto X_{2'}$.

We consider the case

$$sus^2 = u^3$$

first. So far we know $X_1 \mapsto X_{1'} \mapsto X_{25}$ and $X_2 \mapsto X_{2'}$. Now $\{X_{1'}, X_2, X_{12}\} \mapsto \{X_{25}, X_{2'}, X_5\}$ and so $X_{12} \mapsto X_5$. But now $X_1, X_{2'}, X_{12} \mapsto X_{1'}, X_{15}, X_5$ and so $X_{2'} \mapsto X_{15}$. Suppose the power of ϵ for which X_2 is an eigenvalue under u is j, that for X_5 is k, and for X_3 is ℓ. As we are assuming

$$tut^2 = u^3,$$

the powers of ϵ for $X_1, X_{1'}, X_{25}$ are $1, 3, 9$ and for $X_2, X_{2'}, X_{15}$ are $j, 3j, 9j$. As $X_3, X_{2'}, X_{23}$ spans a special plane, the product of the eigenvalues must be 1 and so the value for X_{23} is $-\ell - 3j$. Using the triples $X_{3'}, X_2, X_{23}$ we see the value for X_{23} is $-j$. Similarly the value for X_{13} is -1. Now $\ell + 3j - j = 0$ and so

$$\ell = -2j (\text{mod } 13).$$

Using $X_3, X_{1'}, X_{13}$, the same argument shows that $\ell + 3 - 1 = 0$ and so $j = 1$. Now the triple $X_5, X_{2'}, X_{25}$ gives $3 + k + 9 = 0$ and so $k = 1$ also. Thus, we have 3 eigenvalues ϵ for u, which is one too many. The case

$$sus^2 = u^9$$

gives the same contradiction using the same triples. The only difference is in the eigenvalues under u for images by s. This shows all 3-cycles of s on basis vectors span special planes.

C. UNIQUENESS OF u. The possible s-images of X_1 are $X_{2'}, X_{5'}, X_{6'}, X_{14}$ and by conjugating we may assume $X_1 \mapsto X_{14}$. This forces

$$X_1 \mapsto X_{14} \mapsto X_{4'} \quad \text{and} \quad X_{13} \mapsto X_{1'} \mapsto X_3.$$

Recall that the eigenvalue of u acting on X_1 is ϵ. The possible images of X_2 are $X_{5'}, X_{6'}, X_{24}$. If $X_2 \mapsto X_{24}$, then $X_{24} \mapsto X_{4'}$ which is impossible as $X_{14} \mapsto X_{4'}$. Consequently $X_2 \mapsto X_{5'}$ or $X_2 \mapsto X_{6'}$. We may fix $X_i, X_{i'}, X_{ij}$ with $i, j \leq 4$ and interchange $X_{5'}$ with $X_{6'}$ in $W(E_6)$. Consequently we may assume $X_2 \mapsto X_{6'}$. The remaining values can now be filled in after assuming the eigenvalue of u acting on X_2 is ϵ^i. Assume

$$sus^2 = u^3.$$

Then

$$u = h(\epsilon^{1+i}, \epsilon^{2+11i}, \epsilon^{10+2i}, \epsilon^{3+12i}, \epsilon^{11+5i}, \epsilon^{12+9i}).$$

Written out on the basis vectors this gives for u:

$X_{3'}$	X_4	X_{34}					
0	0	0					
X_1	X_2	X_5	X_6	X_{13}	X_{23}	X_{35}	X_{36}
1	i	$3+9i$	$4+3i$	12	$-i$	$10+4i$	$9+10i$
$X_{1'}$	$X_{2'}$	$X_{5'}$	$X_{6'}$	X_{14}	X_{24}	X_{45}	X_{46}
10	$9+i$	$12+i$	$3i$	3	$4+12i$	$1+4i$	$-3i$
X_3	$X_{4'}$	X_{12}	X_{15}	X_{16}	X_{25}	X_{26}	X_{56}
4	9	$3+12i$	$4i$	$12+10i$	$1+3i$	$9i$	$10+i$

Again the integers below the X_i, $X_{j'}$, X_{ij} are the powers of ϵ to which X_i, $X_{j'}$, X_{ij} are multiplied under the action of u where ϵ is a fixed 13-th root of 1. To see, for instance, how the $12+10i$ below X_{16} was determined, note the triple $X_1, X_{6'}, X_{16}$ spans a special plane and so the eigenvalue for X_{16} is ϵ^{12+10i} as the eigenvalue for X_1 is ϵ, that for $X_{6'}$ is ϵ^{3i} and the product of the eigenvalues is 1.

By routine checking of values it is found that the values $i = 2, 5, 6, 8, 9, 10$ all give the correct eigenvalues. The other values for i do not. In each case the eight values in a given row are distinct and so s is the permutation moving the entry associated with ℓ to the entry associated to 3ℓ in the row below (or the top row for images of the bottom row). In each case, s is uniquely determined as a permutation.

We could have arranged the vectors as follows:

$X_{3'}$	X_4	X_{34}			
0	0	0			
X_1	X_3	X_{14}	X_{13}	$X_{4'}$	$X_{1'}$
1	4	3	12	9	10
X_2	X_{15}	$X_{6'}$	X_{23}	X_{26}	X_{46}
2	8	6	11	5	7
X_5	X_{16}	$X_{2'}$	X_{35}	X_{25}	X_{24}
8	6	11	5	7	2
X_6	X_{12}	$X_{5'}$	X_{36}	X_{56}	X_{45}
10	1	4	3	12	9

An easy check shows that permuting the three bottom rows cyclically is an element of $\widetilde{E}_6(k)$ which commutes with s. The first entries of the bottom three rows are either $\{2,8,10\}$ if i is chosen to be one of these or $\{5,9,6\}$ if i is chosen to be $5, 9$, or 6. After permuting the rows cyclically we can assume the value for i is 2 or 9.

If $i = 2$ the values are those of $\overline{u}$ and so $u = \overline{u}$. The 3-cycle is completely determined as above. The involution j is uniquely determined because it must move each element to the element in the same row with the inverse eigenvalue and it must fix the three points fixed by u. For example X_1 must be moved to X_{13} and X_2 must be moved to X_{23}. In this case, s is $\overline{t}^2$ and j is $\overline{t}^3$.

If the value for i is 9, the linear transformation of $\mathbf{K}$ specified by

$$X_4 \mapsto X_{3'} \mapsto X_{34}$$

$$X_1 \mapsto X_{15} \mapsto X_{24} \mapsto X_{13} \mapsto X_{26} \mapsto X_{2'}$$

$$X_2 \mapsto X_{25} \mapsto X_{14} \mapsto X_{23} \mapsto X_{16} \mapsto X_{1'}$$

$$X_3 \mapsto X_{6'} \mapsto X_5 \mapsto X_{4'} \mapsto X_{46} \mapsto X_{35}$$

$$X_{5'} \mapsto X_{36} \mapsto X_{56} \mapsto X_{45} \mapsto X_6 \mapsto X_{12}$$

is in $\widetilde{E}_6(k)$, centralizes s, and, after conjugating and taking powers, results in $i = 2$. This completes the proof in the case $sus^2 = u^3$.

The following element j' is in $\widetilde{E}_6(k)$ and inverts s.

$$(X_{3'})(X_4, X_{34})(X_1)(X_{13})(X_2, X_{23})(X_5, X_{36})(X_6, X_{35})(X_{1'}, X_3)(X_{2'}, X_{12})$$
$$(X_{5'}, X_{16})(X_{6'}, X_{15})(X_{14}, X_{4'})(X_{24}, X_{56})(X_{45}, X_{25})(X_{46}, X_{26}).$$

The element $u_1 = j'uj'$ is normalized by s and satisfies $su_1s^2 = u_1^9$. This shows that the solutions satisfying this condition are conjugate to those above.

We have now determined s as a permutation. Suppose s and s' are two elements of order three in $\widetilde{E}$ with the same permutation action. Clearly $s's^{-1} = h$ is in the torus. The centralizer of s in the torus is finite as there are nine special planes permuted and the common eigenvalue on any one must be a cube root of unity. The torus is connected and so by Lang's theorem, s and s' are conjugate by an element of the torus.

The proof of Lemma 2.1 is complete. ∎

3. Main theorem

In sections three to seven we use the complex numbers.

THEOREM 3.1: *Let $\overline{u}$ and $\overline{t}$ be as above with k the complex numbers.*

(i) *There is one conjugacy class of subgroups isomorphic to $L(2,13)$ in $\widetilde{E}_6(\mathbb{C})$ with character $13+14$. Each member of this class can be realized within a G_2. There are exactly two such subgroups in $\widetilde{E}_6(\mathbb{C})$ containing $\langle \overline{u}, \overline{t} \rangle$. These are fused under an element in $\widetilde{E}_6(\mathbb{C})$ normalizing $\langle \overline{u}, \overline{t} \rangle$.*

(ii) *There is a unique class of subgroups isomorphic to $L(2,13)$ in $\widetilde{E}_6(\mathbb{C})$ with character $1+12+14$. In particular, there is a unique class of such subgroups isomorphic to $L(2,13)$ in $F_4(\mathbb{C})$ with character $12+14$ on a 26-dimensional irreducible module for F_4. The three algebraic conjugates of the character* *of degree* 12 *give three embeddings conjugate under a field automorphism. Each of these embeddings extends to* PGL(2, 13).

Proof: We know (cf. [CW92]) that there is a G_2 in E_6 and that there is an $L(2,13)$ in G_2 (cf. [CW83]). The character of such an $L(2,13)$ is $13+14$.

Suppose L is a subgroup of $\widetilde{E}_6(\mathbb{C})$ isomorphic to $L(2,13)$. Suppose the character of L acting on $\mathbf{K}$ is either $13+14$ or $1+12+14$. By Lemma 2.1 we may assume L contains $\langle \overline{u}, \overline{t} \rangle$.

We will establish a series of equations which must be satisfied for L to exist with either of the characters and show there are only two possibilities for the $13+14$ character and one for the $1+12+14$ character. Furthermore, we find an element normalizing $\langle \overline{u}, \overline{t} \rangle$ which fuses the two $13+14$ solutions. Because of the existence of $G_2(\mathbb{C})$ as a subgroup of $\widetilde{E}_6(\mathbb{C})$ we infer the $L(2,13)$ in $G_2(\mathbb{C})$ corresponds to the unique solution. We construct a solution for the $1+12+14$ character over $\mathrm{GF}(79^3)$ and use lifting arguments to infer an embedding over $\mathbb{C}$. We do this in a series of sections in which we find out more and more about the possible action of such an $L(2,13)$ on $\mathbf{K}$.

We shall denote the morphism $L(2,13) \to \widetilde{E}$ with image L by $x \mapsto \overline{x}$ $(x \in L)$. In particular, in terms of the presentation $L(2,13) = \langle u, t, w \rangle$ where in matrix form the elements u, t, w are

$$\pm\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \qquad \pm\begin{pmatrix} 2 & 0 \\ 0 & 7 \end{pmatrix}, \qquad \pm\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

we have already determined the images $\overline{u}$ and $\overline{t}$ of u and t, and are out to determine $\overline{w}$.

We shall identify subgroups of $\widetilde{E}$ generated by elements $\overline{u}$, $\overline{t}$, $\overline{w}$ as being isomorphic to $L(2,13)$ by use of the presentation:

$$\overline{u}^{13} = \overline{t}^{6} = I, \quad \overline{t}\,\overline{u}\,\overline{t}^{-1} = \overline{u}^{10},$$

$$\overline{w}^2 = (\overline{u}\,\overline{w})^3 = I, \quad \overline{w}\overline{t}\overline{w} = \overline{t}^5, \quad \overline{w}\,\overline{u}^2\overline{w} = \overline{t}\overline{u}^{11}\,\overline{w}\,\overline{u}^6.$$

4. The fourteen-dimensional invariant subspace V

We begin by finding as much as we can about the action of L on the 14-dimensional L-invariant subspace V of $\mathbf{K}$, for which G restricted to V has character 14.

Let ω be a cube root of unity and let φ be the linear representation of $B = \langle u, t\rangle$ given by $\varphi(t) = \omega$ and $\varphi(u) = 1$. Then $L(2,13)$ restricted to V is the induced character from B to $L(2,13)$ of φ.

There are two bases for V on which the action of G can be conveniently described. Let $w_\infty, w_0, w_1, w_2, \ldots, w_{12}$ be a basis for the monomial action on V for which w_x corresponds to the projective point x over $\mathbb{Z}/13$. The actions are as follows, where the numerical subscripts are taken modulo 13:

$$\overline{u}w_\infty = w_\infty, \qquad \overline{u}w_i = w_{i+1},$$

$$\overline{t}w_\infty = \omega w_\infty, \qquad \overline{t}w_i = \omega^2 w_{10i},$$

$$\overline{w}w_\infty = w_0, \qquad \overline{w}w_0 = w_\infty, \qquad \overline{w}w_{2^i} = \omega^{2^i} w_{-2^{-i}}.$$

Let $v_\infty, v_0, v_1, \ldots, v_{12}$ be a second base for V given by

$$v_\infty = w_\infty, \qquad v_i = \sum_{j=0}^{12} \epsilon^{-ji} w_j$$

for $0 \leq i \leq 12$. In this base

$$\overline{u}v_\infty = v_\infty, \qquad \overline{u}v_i = \epsilon^i v_i,$$

$$\overline{t}v_\infty = \omega v_\infty, \qquad \overline{t}v_i = \omega^2 v_{4i},$$

$$\overline{w}v_\infty = w_0 = \frac{1}{13}\sum_{\ell=0}^{12} v_\ell, \quad \overline{w}v_i = v_\infty + \frac{1}{13}\sum_{\ell=0}^{12} a_{\ell i} v_\ell,$$

where, writing $u^*(2^k \bmod 13) = \omega^{2k}$, we have

$$a_{\ell i} = \sum_{j=1}^{12} u^*(j)\epsilon^{-ij-\ell j^{-1}}.$$

The fixed space of $\overline{u}$ on $\mathbf{K}$ is $\mathbb{C}X_4 + \mathbb{C}X_{3'} + \mathbb{C}X_{34}$. The fixed space of $\overline{u}\,|_V$ has dimension 2 and is spanned by v_∞ and v_0. Within $\mathbb{C}X_4 + \mathbb{C}X_{3'} + \mathbb{C}X_{34}$ there is a unique 1-dimensional subspace of eigenvectors for $\overline{t}$ with eigenvalue ω^2 and so v_0 is a multiple of $X_4 - \omega X_{3'} + \omega^2 X_{34}$ (a vector spanning this 1-space). Similarly v_∞ is a multiple of $X_4 - \omega^2 X_{3'} + \omega X_{34}$. If L has character $1 + 12 + 14$, the vector $v'_* = X_4 - X_{3'} + X_{34}$ must be the fixed vector.

We know that v_0 is a multiple of $X_4 - \omega X_{3'} + \omega^2 X_{34}$ and so we may take v_0 to be $X_4 - \omega X_{3'} + \omega^2 X_{34}$. We may now take $A(X_4 - \omega^2 X_{3'} + \omega X_{34})$ to be v_∞ with A a scalar. Clearly $A \neq 0$. The vector v_1 in V is in the ϵ eigenspace of $\overline{u}$ and we may choose $v_1 = BX_1 - CX_{12}$. The vector v_2 is in the ϵ^2 eigenspace of $\overline{u}$ and we may choose $v_2 = FX_2 + GX_{24}$. With these choices, the vectors $v_i, i \neq 0$, are determined as they are of the form $\overline{t}^j v_1$ or $\overline{t}^j v_2$. For example, $v_4 = \omega\overline{t}v_1 = \omega(\overline{t}BX_1 - \overline{t}CX_{12}) = \omega BX_3 + \omega CX_{5'}$. We tabulate these in Table I.

Table I

v_∞	$=$	$A(X_4 - \omega^2 X_{3'} + \omega X_{34})$	v_7	$=$	$-\omega^2 FX_{46} + \omega^2 GX_{25}$
v_0	$=$	$X_4 - \omega X_{3'} + \omega^2 X_{34}$	v_8	$=$	$-\omega FX_{15} + \omega GX_5$
v_1	$=$	$BX_1 - CX_{12}$	v_9	$=$	$-\omega BX_{4'} - \omega CX_{45}$
v_2	$=$	$FX_2 + GX_{24}$	v_{10}	$=$	$-\omega^2 BX_{1'} + \omega^2 CX_6$
v_3	$=$	$-\omega^2 BX_{14} - \omega^2 CX_{36}$	v_{11}	$=$	$FX_{23} + GX_{2'}$
v_4	$=$	$\omega BX_3 + \omega CX_{5'}$	v_{12}	$=$	$BX_{13} + CX_{56}$
v_5	$=$	$-\omega FX_{26} - \omega GX_{35}$	v'_*	$=$	$X_4 - X_{3'} + X_{34}$
v_6	$=$	$\omega^2 FX_{6'} - \omega^2 GX_{16}$			

There are several calculations which can be checked quickly using the trilinear form. For example

$$\langle v_2, v_3, v_8\rangle = \langle FX_2 + GX_{24}, -\omega^2 BX_{14} - \omega^2 CX_{36}, -\omega FX_{15} + \omega GX_5\rangle = GCF.$$

These are as follows:

Table I.a

$\langle v_\infty, v_1, v_{12}\rangle$	$=$	$-(\omega^2 B^2 + \omega C^2)A$	$\langle v_1, v_3, v_9\rangle$	$=$	$B^3 - C^3$
$\langle v_0, v_1, v_{12}\rangle$	$=$	$-(\omega B^2 + \omega^2 C^2)$	$\langle v_2, v_6, v_5\rangle$	$=$	$-G^3 - F^3$
$\langle v_\infty, v_2, v_{11}\rangle$	$=$	$-(G^2 + \omega^2 F^2)A$	$\langle v_\infty, v_\infty, v_\infty\rangle$	$=$	$6A^3$
$\langle v_0, v_2, v_{11}\rangle$	$=$	$-(G^2 + \omega F^2)$	$\langle v_0, v_0, v_0\rangle$	$=$	6
$\langle v_1, v_2, v_{10}\rangle$	$=$	$-\omega^2 BCF$	$\langle v_\infty, v'_*, v_0\rangle$	$=$	$-3A$
$\langle v_2, v_3, v_8\rangle$	$=$	GCF	$\langle v'_*, v_1, v_{12}\rangle$	$=$	$-(B^2 + C^2)$
$\langle v_1, v_6, v_6\rangle$	$=$	$-2\omega BFG$	$\langle v'_*, v_2, v_{11}\rangle$	$=$	$-(G^2 + F^2)$
$\langle v_1, v_1, v_{11}\rangle$	$=$	$-2BCG$	$\langle v'_*, v'_*, v'_*\rangle$	$=$	6

$\langle v_i, v_j, v_k\rangle = 0$ if $i + j + k \neq 0 \mod 13$ (counting ∞ and $*$ as 0).

The form evaluated on many triples can be seen to be 0 by direct calculation. Triples of vectors which are eigenvectors for $\bar{t}$ or $\bar{u}$ can only have nonzero form if the product of the eigenvalues is 1 as the form is invariant under $\bar{u}$ and $\bar{t}$. For instance $\langle v_\infty, v_\infty, v'_*\rangle = 0$.

We now obtain a series of equations by equating $\langle v_\alpha, v_\beta, v_\gamma\rangle = \langle \overline{w}v_\alpha, \overline{w}v_\beta, \overline{w}v_\gamma\rangle$ for judicious choices of vectors $v_\alpha, v_\beta, v_\gamma$ in V. As $\overline{w}^2 = I$, this is commonly done as

$$\langle \overline{w}v_\alpha, v_\beta, v_\gamma\rangle = \langle v_\alpha, \overline{w}v_\beta, \overline{w}v_\gamma\rangle.$$

These are as follows:

$$\langle w_0, w_0, v_0\rangle = \langle v_\infty, v_\infty, \overline{w}v_0\rangle, \tag{1}$$

$$\langle w_0, v_1, v_{12}\rangle = \langle v_\infty, \overline{w}v_1, \overline{w}v_{12}\rangle, \tag{2}$$

$$\langle w_0, v_2, v_{11}) = \langle v_\infty, \overline{w}v_2, \overline{w}v_{11}), \tag{3}$$

$$\langle w_0, v_3, v_9\rangle = \langle v_\infty, \overline{w}v_3, \overline{w}v_9\rangle, \tag{4}$$

$$\langle w_0, v_5, v_6\rangle = \langle v_\infty, \overline{w}v_5, \overline{w}v_6\rangle, \tag{5}$$

$$\langle w_0, v_2, v_{10}\rangle = \langle v_\infty, \overline{w}v_2, \overline{w}v_{10}\rangle, \tag{6}$$

$$\langle w_0, v_1, v_{11}\rangle = \langle v_\infty, \overline{w}v_1, \overline{w}v_{11}\rangle, \tag{7}$$

$$\langle w_0, v_6, v_6\rangle = \langle v_\infty, \overline{w}v_6, \overline{w}v_6\rangle, \tag{8}$$

$$\langle w_0, v_3, v_8\rangle = \langle v_\infty, \overline{w}v_3, \overline{w}v_8\rangle. \tag{9}$$

The left hand sides can be easily evaluated as $w_0 = (v_0 + v_1 + \cdots + v_{12})/13$. In particular, for (1), we have

$$\begin{aligned}\langle w_0, w_0, v_0\rangle &= \sum_{j,i=0}^{12} \langle v_i, v_j, v_0\rangle/13^2 \\ &= \sum_{i=0}^{12}\langle v_i, v_{-i}, v_0\rangle/13^2 \\ &= \frac{6}{13^2}(\langle v_1, v_{12}, v_0\rangle + \langle v_2, v_{11}, v_0\rangle) + \frac{1}{13^2}\langle v_0, v_0, v_0\rangle \\ &= \frac{-6}{13^2}(\omega B^2 + \omega^2 C^2 + G^2 + \omega F^2) + \frac{6}{13^2}.\end{aligned}$$

As $\langle v_\infty, v_\infty, \overline{w}v_0) = \langle v_\infty, v_\infty, v_\infty\rangle = 6A^3$, equation (1) becomes after multiplying by 13^2

$$-6(\omega B^2 + \omega^2 C^2 + G^2 + \omega F^2) + 6 = 13^2 \cdot 6\, A^3. \tag{1'}$$

For the remaining equations, the left hand sides can be evaluated as follows:

$$(2') \qquad \langle w_0, v_1, v_{12}\rangle = \frac{-1}{13}(\omega B^2 + \omega^2 C^2),$$

$$(3') \qquad \langle w_0, v_2, v_{11}\rangle = \frac{-1}{13}(G^2 + \omega F^2),$$

$$(4') \qquad \langle w_0, v_3, v_9\rangle = \frac{1}{13}(B^3 - C^3),$$

$$(5') \qquad \langle w_0, v_5, v_6\rangle = \frac{1}{13}(-G^3 - F^3),$$

$$(6') \qquad \langle w_0, v_2, v_{10}\rangle = \frac{-1}{13}BCF\omega^2,$$

$$(7') \qquad \langle w_0, v_1, v_{11}\rangle = \frac{-2}{13}BCG,$$

$$(8') \qquad \langle w_0, v_6, v_6\rangle = \frac{-2}{13}BFG\omega,$$

$$(9') \qquad \langle w_0, v_3, v_8\rangle = \frac{1}{13}GCF.$$

The remaining right hand sides can be evaluated also but the terms are difficult to identify as they are sums of terms of the form $\epsilon^i\omega^j$, $0 \le i \le 12$, $0 \le j \le 2$. In general, we have

$$\begin{aligned}\langle v_\infty, \overline{w}v_k, \overline{w}v_\ell\rangle &= \langle v_\infty, v_\infty, v_\infty\rangle + \frac{1}{13^2}\sum_{j+i=0}\langle v_\infty, a_{jk}v_j, a_{i\ell}v_i\rangle \\ &= 6A^3 + \frac{1}{13^2}\sum_{j=-i} a_{jk}a_{i\ell}\langle v_\infty, v_j, v_i\rangle.\end{aligned}$$

Each $\langle v_\infty, v_j, v_i\rangle$ for $j = -i$ is either a multiple of $\langle v_\infty, v_1, v_{12}\rangle = -(\omega^2B^2 + \omega C^2)A$ or a multiple of $\langle v_\infty, v_2, v_{11}\rangle = -(G^2 + \omega^2F^2)A$ depending on whether v_j is a $\bar{t}$-image of a scalar multiple of v_1 or v_2. For the remaining right hand sides we therefore have

$$\langle v_\infty, \overline{w}v_k, \overline{w}v_\ell\rangle = 6A^3 + \alpha_{k,\ell}(\omega^2B^2 + \omega C^2)A + \beta_{k,\ell}(G^2 + \omega^2F^2)A,$$

where

$$\alpha_{k,\ell} = \frac{-1}{169}\sum_{h=0}^{5}\omega^h a_{4^h,k}\, a_{-4^h,\ell},$$

$$\beta_{k,\ell} = \frac{-1}{169}\sum_{h=0}^{5}\omega^h a_{2\cdot 4^h,k}\, a_{-2\cdot 4^h,\ell}.$$

The equations can be evaluated using the basis $\epsilon^i\omega^j$ of $\mathbb{Q}(\epsilon,\omega)$ over $\mathbb{Q}$ for $0 \le i \le 11$, $0 \le j \le 1$. These calculations are done using Mathematica, and checked with Maple. Collecting in terms of this basis gives a method of determining when two expressions are equal.

A miracle occurs with equations (7) and (8), in that their right hand sides turn out to be equal. Thus,

$$\langle v_\infty, \overline{w}v_1, \overline{w}v_{11}\rangle = \langle v_\infty, \overline{w}v_6, \overline{w}v_6\rangle.$$

In terms of left hand sides, this means $-26BG(C-\omega F)=0$, whence we have the three cases:

$$C=\omega F, \qquad B=0, \qquad G=0.$$

The coefficients after multiplying by 13^2 of the equations are all in $\mathbb{Z}[\epsilon,\omega]$ and can be reduced mod $\mathcal{P}$ where $\mathcal{P}$ is a prime ideal in $\mathbb{Z}[\epsilon,\omega]$ for which $79 \in \mathcal{P}$. When this is done, ω may be represented by 23, or 55 and ϵ by 3^6, so $\mathcal{P}=(79,\omega-23,\epsilon-18)$. The equations can all be reduced mod $\mathcal{P}$ by replacing ω by $23=3^{26}$ and ϵ by $18=3^6$ and collecting terms. We use the term "reducing mod 79" for this process. In the remaining sections we will solve sets of equations which have been reduced mod 79 and find they have unique solutions. We are interested in knowing they have unique solutions over $\mathbb{C}$ and our work will show this. We will reduce the existence of solutions to sets of equations to information about the rank of a certain matrix with coefficients in $\mathbb{Z}[\epsilon,\omega]$. The rank over $\mathbb{Z}[\epsilon,\omega]$ is at least the rank over its reduction mod 79. Full rank or corank one mod 79 means at least full or corank one for the original matrix. The reduction mod 79 is done using Mathematica and the results are as follows.

In V, on the basis $v_1,\ldots,v_{12},v_0,v_\infty$,

$$\overline{w}=\frac{1}{13}\begin{pmatrix}
53 & 77 & 37 & 15 & 77 & 75 & 51 & 32 & 13 & 4 & 36 & 5 & 78 & 1\\
48 & 35 & 17 & 22 & 62 & 38 & 71 & 60 & 48 & 40 & 4 & 5 & 24 & 1\\
60 & 17 & 4 & 38 & 48 & 48 & 22 & 5 & 71 & 35 & 40 & 62 & 24 & 1\\
29 & 25 & 36 & 61 & 67 & 38 & 33 & 66 & 13 & 34 & 33 & 62 & 56 & 1\\
77 & 4 & 77 & 51 & 5 & 15 & 13 & 53 & 75 & 36 & 37 & 32 & 78 & 1\\
66 & 36 & 33 & 38 & 29 & 13 & 61 & 62 & 33 & 25 & 34 & 67 & 56 & 1\\
67 & 34 & 25 & 33 & 62 & 61 & 13 & 29 & 38 & 33 & 36 & 66 & 56 & 1\\
32 & 37 & 36 & 75 & 53 & 13 & 15 & 5 & 51 & 77 & 4 & 77 & 78 & 1\\
62 & 33 & 34 & 13 & 66 & 33 & 38 & 67 & 61 & 36 & 25 & 29 & 56 & 1\\
62 & 40 & 35 & 71 & 5 & 22 & 48 & 48 & 38 & 4 & 17 & 60 & 24 & 1\\
5 & 4 & 40 & 48 & 60 & 71 & 38 & 62 & 22 & 17 & 35 & 48 & 24 & 1\\
5 & 36 & 4 & 13 & 32 & 51 & 75 & 77 & 15 & 37 & 77 & 53 & 78 & 1\\
66 & 17 & 17 & 75 & 66 & 75 & 75 & 66 & 75 & 17 & 17 & 66 & 0 & 1\\
13 & 13 & 13 & 13 & 13 & 13 & 13 & 13 & 13 & 13 & 13 & 13 & 13 & 0
\end{pmatrix}.$$

The equations mod 79 are

$$(1)\qquad 73+66A^3+59B^2+14C^2+59F^2+6G^2=0,$$

$$(2)\qquad 66A^3+62B^2+33AB^2+4C^2+77AC^2+32AF^2+25AG^2=0,$$

$$(3)\qquad 66A^3+22AB^2+25AC^2+62F^2+48AF^2+13G^2+77AG^2=0,$$

$$(4)\qquad 66A^3+22AB^2+66B^3+25AC^2+13C^3+59AF^2+14AG^2=0,$$

$$(5)\qquad 66A^3+6AB^2+14AC^2+32AF^2+13F^3+25AG^2+13G^3=0,$$

$$(6)\qquad 66A^3+22AB^2+25AC^2+4BCF+21AF^2+9AG^2=0,$$

$$(7)\qquad 66A^3+33AB^2+77AC^2+48AF^2+77AG^2+26BCG=0,$$

$$(8)\qquad 66A^3+33AB^2+77AC^2+48AF^2+77AG^2+45BFG=0,$$

$$(9)\qquad 66A^3+49AB^2+9AC^2+32AF^2+25AG^2+66CFG=0.$$

The argument now breaks into three cases depending on whether $C=\omega F$, $B=0$, or $G=0$. We begin with the first case.

CASE 1: *($C=\omega F$).* If we set $C=\omega F$ and collect terms, the equations mod 79 become

$$(1)\qquad 73+66A^3+59B^2+39F^2+6G^2=0,$$

$$(2)\qquad 66A^3+62B^2+33AB^2+62F^2+AF^2+25AG^2=0,$$

$$(3)\qquad 66A^3+22AB^2+AF^2+62F^2+13G^2+77AG^2=0,$$

$$(4)\qquad 66A^3+22AB^2+66B^3+12AF^2+13F^3+14AG^2=0,$$

$$(5)\qquad 66A^3+6AB^2+12AF^2+13F^3+25AG^2+13G^3=0,$$

$$(6)\qquad 66A^3+22AB^2+53AF^2+13BF^2+9AG^2=0,$$

$$(7)\qquad 66A^3+33AB^2+17AF^2+77AG^2+45BFG=0,$$

$$(8)\qquad 66A^3+33AB^2+17AF^2+77AG^2+45BFG=0,$$

$$(9)\qquad 66A^3+49AB^2+53AF^2+25AG^2+17F^2G=0.$$

The first three equations give the matrix equation $Z\cdot Y=0$ where

$$Z=\begin{pmatrix}73+66A^3 & 59 & 39 & 6\\ 66A^3 & 62+33A & 62+A & 25A\\ 66A^3 & 22A & 62+A & 13+77A\end{pmatrix}\quad\text{and}\quad Y=\begin{pmatrix}1\\ B^2\\ F^2\\ G^2\end{pmatrix}.$$

Let P_i be the determinant of Z with column i deleted. Now if $P_1 \neq 0$, then Z has rank 3 and Y is proportional to $(\ P_1,\quad -P_2,\quad P_3,\quad -P_4\ )$ and so

$$B^2 = -P_2/P_1, \qquad F^2 = P_3/P_1, \qquad G^2 = -P_4/P_1.$$

However, $P_1 = 61A(20+A)$. If $A = 0$, then Z has rank 3 as $P_2 = 62$. But now Y cannot be proportional to $(\ P_1,\quad -P_2,\quad P_3,\quad -P_4\ )$ as $1 \neq 0$. This shows there is no solution to the equations if $A = 0$. (Of course over $\mathbb{C}$ we know $A \neq 0$ by the geometry but we need to know mod 79 that there is no solution with $A = 0$ because such a solution could correspond to a solution over $\mathbb{C}$ with $A \equiv 0 \pmod{79}$.) If $A = -20$, the second and third equations become the same.

Assuming A is not 0 or -20 we use equations (4) to (9) to give further restrictions. From equation (9), we have $P_1 66A^3 - 49AP_2 + 53AP_3 - 25AP_4 = -17P_3G$. Let LHS be the left hand side of this equation. Then $P_1(LHS)^2 = -(17)^2(P_3)^2P_4$. Factoring the difference of the two sides using Mathematica gives

$$43(20+A)^3(49+38A+A^2)(56+16A+64A^2+A^3)\cdot$$
$$(55+77A+70A^2+78A^3+69A^4+54A^5+31A^6+A^7).$$

From equation (7), we have $P_1 66A^3 - 33AP_2 + 17AP_3 - 77AP_4 = -45BFGP_1$. Again, if LHS is the left hand side of this equation, we obtain $P_1(LHS)^2 = (45)^2P_2P_3P_4$. Factoring the difference of the two sides gives

$$73(6+A)^3(20+A)^3(31+A)(59+A)(56+16A+64A^2+A^3)\cdot$$
$$(39+9A+37A^2+15A^3+14A^4+A^5).$$

The root $A = -20$ is common to both as is the cubic $56+16A+64A^2+A^3$ and no other factors are common. There are therefore two possibilities. Either $A = -20$ or A is a root of $A^3+64A^2+16A+56$, an irreducible cubic over GF(79).

The equations can now be solved when $A = -20$. We claim that there are two solutions:

(a) $A = -20, \quad B = 51, \quad F = 23, \quad C = 55, \quad G = 17;$

(b) $A = -20, \quad B = 4, \quad F = 23, \quad C = 55, \quad G = 39.$

As a start to showing this and for later reference note that 34 times equation (1) minus 59 times equation (2) equals $2+33F^2$, and so $F^2 = 55$, whence $F = \pm 23$.

Solving for G^2 in terms of B^2 in equation (1) and substituting in equation (6) gives a quadratic with two roots, $B = 51$ and $B = 4$. Now G can be found from equation (9) and F from equation (4). We will show later that these two solutions are fused under an automorphism.

Recognizing that $\omega = 23$ leads one to suspect that $F = \pm\omega$ could be a root of the corresponding equations over $\mathbb{C}$. Note $34 = -2 + 5\omega$ and $59 = 6\omega$ for later reference. For now note that everything we have done could have been done over the complex numbers with at most this many solutions.

For the case $A^3 = -(64A^2+16A+56)$ we use the field $\mathrm{GF}(79^3)$. It is convenient to take $\mathrm{GF}(79^3)$ isomorphic to $\mathbb{Z}/79[X]/(X^3+64X^2+16X+56)$ and take A to be the canonical image of X in the latter ring. The values A^3 in the equations can be replaced by $-(64A^2+16A+56)$. The values for B^2, F^2, G^2 can be calculated from P_1, P_2, P_3, P_4 as above. Here $P_1 = 35+61A^2$ and so $P_1^{-1} = 69+8A+60A^2$. Now

$$B^2 = 78 + 66A + 68A^2, \qquad F^2 = 23 + 34A + 16A^2, \qquad G^2 = 56 + 17A + 63A^2.$$

The values of B and G can be found by substituting these values in equations (6) and (9). The value for F can then be found from equation (7). The values must be checked in equations (4) and (5). The unique solution is

$$\text{(c)} \quad \begin{array}{c} A^3 = -(64A^2 + 16A + 56), \\ B = -(6 + 7A + 3A^2), \end{array} \qquad C = \omega F, \qquad \begin{array}{c} F = -(55 + 75A), \\ G = 14 + 69A + 7A^2. \end{array}$$

For these calculations one can check these really are square roots of the values given above and then checking signs is routine. It is also routine to check that these values give solutions to all nine equations. This completes case 1 and we continue with cases 2 and 3. Note first that over the complex numbers there will be no more solutions with these properties than we have found over $\mathrm{GF}(79^3)$. We will show in §7 that the two solutions with $A = -20$ are fused by an element in E_6.

CASES 2 AND 3: *($BG = 0$).* The methods above can be used. The equations if $B = 0$ are

$$(1) \qquad 73 + 66A^3 + 14C^2 + 59F^2 + 6G^2 = 0,$$

$$(2) \qquad 66A^3 + 4C^2 + 77AC^2 + 32AF^2 + 25AG^2 = 0,$$

$$(3) \qquad 66A^3 + 25AC^2 + 62F^2 + 48AF^2 + 13G^2 + 77AG^2 = 0,$$

$$66A^3 + 25AC^2 + 13C^3 + 59AF^2 + 14AG^2 = 0, \tag{4}$$

$$66A^3 + 14AC^2 + 32AF^2 + 13F^3 + 25AG^2 + 13G^3 = 0, \tag{5}$$

$$66A^3 + 25AC^2 + 21AF^2 + 9AG^2 = 0, \tag{6}$$

$$66A^3 + 77AC^2 + 48AF^2 + 77AG^2 = 0, \tag{7}$$

$$66A^3 + 77AC^2 + 48AF^2 + 77AG^2 = 0, \tag{8}$$

$$66A^3 + 9AC^2 + 32AF^2 + 66CFG + 25AG^2 = 0. \tag{9}$$

For example in equations (1), (2), (3), (6), (7) with $B = 0$ only $1, C^2, F^2, G^2$ occur as coefficients. The matrix of coefficients is now a 5×4 matrix which must have rank at most 3. Factoring the determinants of the first four rows and the first three and the fifth gives two polynomials in A with just two common roots, 0 and 20. If $A = 0$, equation (2) gives $C = 0$ and then equations (3) and (5) give $F = G = 0$ but now equation (1) is not satisfied. If $A = 20$, the first 3 rows give unique values for C^2, F^2, G^2. The fourth using these values gives the value for C. Now equations (9) and (5) give the corresponding signs for G and F.

The case $G = 0$ is similar and we omit details as we shall see later that these two solutions are also fused by an element in E_6. The two solutions are

(d) $A = 20, \quad B = 0, \quad C = -22, \quad F = \pm\sqrt{7}, \quad G = \mp\sqrt{7};$

(e) $A = 20, \quad B = C = \pm\sqrt{-10}, \quad F = -25, \quad G = 0.$

In conclusion, we have found five solutions, namely (a),...,(e) for the 14 dimensional irreducible $L(2,13)$-submodule V of $\mathbf{K}$ over $k = GF(79^3)$. The same arguments over the complex numbers give at most this number of solutions. This is all we will say about the action on the 14-dimensional space. We now must consider the two possibilities on the 13-dimensional complement. The possibilities there are 13 and $1 + 12$.

5. The action on the complement in the E_6 case

Let V' be the complement to V and assume the action of $\langle \overline{u}, \overline{t}, \overline{w} \rangle$ has the character 13 which is the permutation character on the projective line minus the identity. If w'_∞, w'_0, $w'_1, \ldots, w'_{12}$ are the permuted vectors, a basis for V' is

$$v'_* = 13w'_\infty - \sum_{i=0}^{12} w'_i, \qquad v'_i = \sum_{j=0}^{12} \epsilon^{-ij} w'_j$$

for $1 \leq i \leq 12$. With this basis the action is as follows:

$$\overline{u}v'_i = \epsilon^i v'_i, \qquad \overline{u}v'_* = v'_*,$$
$$\overline{t}v'_i = v'_{4i}, \qquad \overline{t}v'_* = v'_*,$$
$$\overline{w}v'_* = \frac{1}{13}(-v'_* + 14\sum_{i=1}^{12} v'_i), \qquad \overline{w}v'_i = \frac{1}{13}(v'_* + \sum_{j=1}^{12} b_{ji}v'_j),$$

where

$$b_{ji} = \sum_{\ell=1}^{12} \epsilon^{-i\ell - j\ell^{-1}}.$$

Now we shall identify V' as an L-submodule of $\mathbf{K}$. We know that v'_* is a multiple of any vector fixed by $\overline{u}$ in V' and so we can assume $v'_* = X_4 - X_{3'} + X_{34}$. Now v'_1 is in the ϵ eigenspace for $\overline{u}$ and so $v'_1 = B'X_1 - C'X_{13}$. We can also set $v'_2 = F'X_2 + G'X_{24}$. The remaining v'_i are images under $\overline{t}$ of v'_1 or v'_2. We tabulate these in Table II.

Table II

$$\begin{array}{lcl@{\qquad}lcl}
v'_* & = & X_4 - X_{3'} + X_{34} & v'_7 & = & -F'X_{46} + G'X_{25} \\
v'_1 & = & B'X_1 - C'X_{12} & v'_8 & = & -F'X_{15} + G'X_5 \\
v'_2 & = & F'X_2 + G'X_{24} & v'_9 & = & -B'X_{4'} - C'X_{45} \\
v'_3 & = & -B'X_{14} - C'X_{36} & v'_{10} & = & -B'X_{1'} + C'X_6 \\
v'_4 & = & B'X_3 + C'X_{5'} & v'_{11} & = & F'X_{23} + G'X_{2'} \\
v'_5 & = & -F'X_{26} - G'X_{35} & v'_{12} & = & B'X_{13} + C'X_{56} \\
v'_6 & = & F'X_{6'} - G'X_{16} & & &
\end{array}$$

The matrix for $\overline{w}$ mod 79 on the 13 dimensional space on the basis $v'_1, \ldots, v'_{12}, v'_*$ is

$$\overline{w} = \frac{1}{13}\begin{pmatrix}
33 & 42 & 65 & 33 & 70 & 12 & 2 & 51 & 31 & 21 & 54 & 61 & 14 \\
42 & 33 & 12 & 51 & 21 & 61 & 33 & 65 & 70 & 2 & 31 & 54 & 14 \\
65 & 12 & 31 & 61 & 42 & 70 & 51 & 54 & 33 & 33 & 2 & 21 & 14 \\
33 & 51 & 61 & 65 & 2 & 54 & 42 & 12 & 21 & 33 & 70 & 31 & 14 \\
70 & 21 & 42 & 2 & 61 & 33 & 31 & 33 & 12 & 54 & 65 & 51 & 14 \\
12 & 61 & 70 & 54 & 33 & 21 & 65 & 31 & 42 & 51 & 33 & 2 & 14 \\
2 & 33 & 51 & 42 & 31 & 65 & 21 & 33 & 54 & 70 & 61 & 12 & 14 \\
51 & 65 & 54 & 12 & 33 & 31 & 33 & 61 & 2 & 42 & 21 & 70 & 14 \\
31 & 70 & 33 & 21 & 12 & 42 & 54 & 2 & 65 & 61 & 51 & 33 & 14 \\
21 & 2 & 33 & 33 & 54 & 51 & 70 & 42 & 61 & 31 & 12 & 65 & 14 \\
54 & 31 & 2 & 70 & 65 & 33 & 61 & 21 & 51 & 12 & 33 & 42 & 14 \\
61 & 54 & 21 & 31 & 51 & 2 & 12 & 70 & 33 & 65 & 42 & 33 & 14 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 7
\end{pmatrix}.$$

Here and elsewhere we always check that the matrices satisfy the defining relations for $L(2,13)$ as given in §3.

There are now several equations which must be satisfied similar to the ones for V. By taking two vectors from V and one from V' the terms are linear in B', C', F', G'.

We begin with $\langle v'_*, v_\infty, w_0\rangle$. It is often convenient to act by $13\overline{w}$ rather than with $\overline{w}$. It is straightforward from the definitions that

$$13^2\langle v'_*, v_\infty, w_0\rangle = 13^2\langle v'_*, v_\infty, v_0/13\rangle = -39\cdot A.$$

If we let S be the squares mod 13, we also have

$$\begin{aligned}\langle 13\overline{w}v'_*, 13\overline{w}v_\infty, \overline{w}w_0\rangle &= \langle -v'_* + 14\sum_{i=1}^{12} v'_i, \sum_{i=0}^{12} v_i, v_\infty\rangle \\ &= \langle -v'_*, v_0, v_\infty\rangle + 14\sum_{i=1}^{12}\langle v'_i, v_{-i}, v_\infty\rangle \\ &= 3A + 14\sum_{i\in S}\langle v'_i, v_{-i}, v_\infty\rangle + 14\sum_{i\notin S}\langle v'_i, v_{-i}, v_\infty\rangle \\ &= 3A - 14\cdot 6(\omega^2 BB' + \omega CC')A - 14\cdot 6(GG' + \omega^2 FF')A\end{aligned}$$

and so equating these gives

$$0 = 42A - 84A(\omega^2 BB' + \omega CC' + GG' + \omega^2 FF'). \tag{10}$$

Now $13^2\langle \overline{w}v_\infty, v'_i, v_k\rangle = 13^2\langle w_0, v'_i, v_k\rangle = 13\langle v_{-i-k}, v'_i, v_k\rangle$ and

$$\begin{aligned}\langle v_\infty, 13\overline{w}v'_i, 13\overline{w}v_k\rangle &= \langle v_\infty, v'_* + \sum_{j=1}^{12} b_{ji}v'_j, 13v_\infty + \sum_{j=0}^{12} a_{jk}v_j\rangle \\ &= \langle v_\infty, v'_*, v_0\rangle a_{k0} + \sum_{\ell\in S}\langle v_\infty, v'_\ell, v_{-\ell}\rangle a_{k,-\ell}b_{i\ell} \\ &\quad + \sum_{\ell\notin S}\langle v_\infty, v'_\ell, v_{-\ell}\rangle a_{k,-\ell}b_{i\ell} \\ &= -3Aa_{k0} + (-A)(BB'\omega^2 + CC'\omega)\sum_{\ell\in S} a_{-\ell,k}b_{\ell i} \\ &\quad + (-A)(GG' + FF'\omega^2)\sum_{\ell\notin S} a_{-\ell,k}b_{\ell i}.\end{aligned}$$

By equating the values $13^2\langle \overline{w}v_\infty, v_i', v_k\rangle$ and $\langle v_\infty, 13\overline{w}v_i', 13\overline{w}v_k\rangle$ for various values of i and k, we obtain more equations. We compute $\langle v_{-i-k}, v_i', v_k\rangle$ for several values of i and k using the relations from the previous section:

$$\langle v_0, v_1', v_{12}\rangle = -(\omega BB' + \omega^2 CC'), \tag{11}$$
$$\langle v_0, v_2', v_{11}\rangle = -GG' - \omega FF', \tag{12}$$
$$\langle v_1', v_6, v_6\rangle = -2\omega B'FG, \tag{13}$$
$$\langle v_1', v_3, v_9\rangle = B'B^2 - C'C^2, \tag{14}$$
$$\langle v_2', v_6, v_5\rangle = -G'G^2 - F'F^2, \tag{15}$$
$$\langle v_1', v_1, v_{11}\rangle = -B'CG - C'BG, \tag{16}$$
$$\langle v_2', v_3, v_8\rangle = G'CF, \tag{17}$$
$$\langle v_1', v_2, v_{10}\rangle = -\omega^2 BC'F. \tag{18}$$

Suppose first that solution (a) of §4 is at hand; that is, $A = -20$, $B = 51$, $C = 55$, $F = 23$, $G = 17$. The equations become

$$1 + 78B' + 77F' + 77C' + 45G' = 0, \tag{10}$$
$$10 + 74B' + 70F' + 48C' + 5G' = 0, \tag{11}$$
$$72 + 15B' + 77F' + 30C' + 40G' = 0, \tag{12}$$
$$76 + 35B' + 30F' + 35C' + 36G' = 0, \tag{13}$$
$$72 + 23B' + 42F' + 31C' + 3G' = 0, \tag{14}$$
$$76 + 9B' + 2F' + 18C' + 10G' = 0, \tag{15}$$
$$10 + 31B' + 47F' + 58C' + 9G' = 0, \tag{16}$$
$$72 + 66B' + 67F' + 53C' + 20G' = 0, \tag{17}$$
$$72 + 15B' + 69F' + 61C' + 67G' = 0. \tag{18}$$

This is equivalent to the matrix equation $X \cdot Z = 0$ where

$$X = \begin{pmatrix} 1 & 78 & 77 & 77 & 45 \\ 10 & 74 & 70 & 48 & 5 \\ 72 & 15 & 77 & 30 & 40 \\ 76 & 35 & 30 & 35 & 36 \\ 72 & 23 & 42 & 31 & 3 \\ 76 & 9 & 2 & 18 & 10 \\ 10 & 31 & 47 & 58 & 9 \\ 72 & 66 & 67 & 53 & 20 \\ 72 & 15 & 69 & 61 & 67 \end{pmatrix} \quad \text{and} \quad Z = \begin{pmatrix} 1 \\ B' \\ F' \\ C' \\ G' \end{pmatrix}.$$

There is one solution $B' = -5$, $F' = -25$, $C' = -14$, $G' = 35$, which gives the solution

$$(a.a) \qquad A = -20, \quad \begin{matrix} B = 51, & F = 23, & B' = -5, & C' = -14, \\ C = 55, & G = 17, & F' = -25, & G' = 35. \end{matrix}$$

The solution (b) of §4 leads to the solution

$$(b.a) \qquad A = -20, \quad \begin{matrix} B = 4, & F = 23, & B' = -35, & C' = -25, \\ C = 55, & G = 39, & F' = -14, & G' = 5. \end{matrix}$$

As usual there are at most two solutions over $\mathbb{C}$.

There are two further possibilities when $A = 20$. The first is (d), where $A = 20$, $B = 0$, $C = -22$, $F = \sqrt{7}$, $G = -\sqrt{7}$. Equations (10), (11), (12), (14), (17), (18) lead to the matrix equation $X \cdot Z = 0$ where

$$X = \begin{pmatrix} 1 & 64 & 48 & 2 \\ 69 & 17 & 21 & 70 \\ 7 & 12 & 76 & 60 \\ 7 & 7 & 60 & 42 \\ 7 & 37 & 28 & 37 \\ 7 & 12 & 76 & 69 \end{pmatrix} \quad \text{and} \quad Z = \begin{pmatrix} 1 \\ C' \\ F'\sqrt{7} \\ G'\sqrt{7} \end{pmatrix}.$$

The third and bottom row show $G' = 0$ but the bottom left 3×3 submatrix is nonsingular and there is no solution. The second solution with $A = 20$ is (e), where $G = 0$, $B = C = \pm\sqrt{-10}$, $F = -25$. Equations (12), (13), (15), (16), (18) can be used to show there is no solution. Consequently, there are no solutions over $\mathbb{C}$.

We shall also rule out a solution of equations (10) to (18) for the cubic case (e), where $A^3 = 23 + 63A + 15A^2$. The equations (10) to (14) have no solutions. Indeed the determinant of the matrix of coefficients for equations (10) to (14) is $33 + 50A + 77A^2$ and so is not 0. This shows there is no solution over $\mathrm{GF}(79^3)$ for this value of A. Again, the same is true over $\mathbb{C}$. These arguments show part (i) of Theorem 3.1 has been proved except for the statement about the automorphisms fusing the two subgroups.

6. The action on the complement in the F_4 case

We must also show that there is one possibility for the F_4 case in which the character on V' is $1 + 12$. The fixed space for L would be $\mathbb{C}v'_*$ and so L is a subgroup of the subgroup $\mathbf{F}$ of $\widetilde{E}$ fixing the vector v'_*, which is isomorphic to F_4, as $\langle v'_* \rangle \neq 0$ (see Table I.a). In §4 we have seen that

$$\langle v'_*, v_1, v_{12} \rangle = -B^2 - C^2 \quad \text{and} \quad \langle v'_*, v_2, v_{11} \rangle = -G^2 - F^2.$$

These lead to equations as follows. First, we have

$$\langle \overline{w}v'_*, \overline{w}w_0, \overline{w}w_1 \rangle = \langle v'_*, v_\infty, w_{12} \rangle = \langle v'_*, v_\infty, v_0/13 \rangle = -3A/13,$$

where the latter equality is again from the equations in Table I.a of §4. On the other hand, as

$$\langle v'_*, v_i, v_{-i} \rangle = \langle \bar{t}v'_*, \bar{t}v_i, \bar{t}v_{-i} \rangle = \langle v'_*, \omega^2 v_{4i}, \omega^2 v_{-4i} \rangle = \omega \langle v'_*, v_{4i}, v_{-4i} \rangle$$

and $\langle v'_*, v_0, v_0 \rangle = 0$, we have

$$\begin{aligned} \langle v'_*, w_0, w_1 \rangle &= \langle v'_*, \frac{1}{13}\sum_{i=0}^{12} v_i, \frac{1}{13}\sum_{i=0}^{12} \epsilon^i v_i \rangle \\ &= \frac{1}{13^2}\sum_{i=0}^{12} \epsilon^{-i} \langle v'_*, v_i, v_{-i} \rangle \\ &= \frac{1}{13^2}\langle v'_*, v_1, v_{12} \rangle \Lambda_1^* + \frac{1}{13^2}\langle v'_*, v_2, v_{11} \rangle \Lambda_2^*, \end{aligned}$$

where $\Lambda_i^* = \epsilon^i + \epsilon^{-i} + \omega^2(\epsilon^{4i} + \epsilon^{-4i}) + \omega(\epsilon^{3i} + \epsilon^{-3i})$. Hence, the identity $\langle v'_*, w_0, w_1 \rangle = \langle \overline{w}v'_*, \overline{w}w_0, \overline{w}w_1 \rangle$ gives

$$(B^2 + C^2)\Lambda_1^* + (G^2 + F^2)\Lambda_2^* = 39 \cdot A. \tag{19}$$

The corresponding equation for $\langle v'_*, w_0, w_2 \rangle$ gives

$$(B^2 + C^2)\Lambda_2^* + \omega(G^2 + F^2)\Lambda_1^* = 39 \cdot A\omega^2. \tag{20}$$

We show that the values mod 79 do not satisfy this except for the case (c) of A a root of the cubic in GF(79^3).

The values mod 79 are as follows:

$$\omega = 23, \qquad \omega^2 = 55, \qquad \epsilon = 18, \qquad \Lambda_1^* = 52, \qquad \Lambda_2^* = 8.$$

For each of the four possible solutions (a), (b), (d), (e) for B, C, F, G with $A = \pm 20$, both sides of (19) and (20) can be evaluated and they never coincide.

For instance, in case (e),the left and right hand side of (19) and (20) differ by 20 and 76, respectively. Consequently none of these can lead to embeddings of $L(2,13)$ in F_4.

Next suppose we are in the cubic case (c). Now $B^2+C^2 = 40A$ and $G^2+F^2 = 51A$, so (19) and (20) are satisfied. This shows these values could come from the subgroup $\widetilde{F}$ of $\widetilde{E}$ fixing v'_*. In order to show this is possible we find the action of $\overline{u}$, $\overline{t}$, $\overline{w}$ on the 12-dimensional complement V' to $\langle V, v'_*\rangle$. We use the same vectors $v'_1, v'_2, \dots, v'_{12}$ as above (Table II), as these are the eigenvectors with eigenvalue ϵ^i $(1 \le i \le 12)$ for $\overline{u}$. However, the vectors are determined up to a scalar so if one of B', C', F', G' is nonzero we can assume it is 1.

As the actions of $L(2,13)$ on V and $V' \cap v'^{\perp}_*$ are irreducible and distinct, the $L(2,13)$ invariant pairing $v' \times v \mapsto \langle v'_*, v', v\rangle$ must be trivial, so $\langle v'_*, v', v\rangle = 0$ for $v' \in V'$ and $v \in V$. We calculate exactly as above that

$$\langle v'_*, v'_1, v_{12}\rangle = -(B'B + C'C) \qquad \text{and} \quad \langle v'_*, v'_2, v_{11}\rangle = -(G'G + F'F).$$

These give two equations

$$\begin{aligned} B'(6+7A+3A^2) + C'(23)(55+75A) &= 0, \\ G'(14+69A+7A^2) - F'(55+75A) &= 0. \end{aligned}$$

Noting that $(55+75A)^{-1} = 27+70A+23A^2$, we find

$$C' = (33+72A+7A^2)B' \text{ and } F' = (46+7A+72A^2)G'. \tag{21}$$

Since v'_1 and v'_2 are nonzero vectors, at least one of B', C', and at least one of F', G' is not 0, so we can assume either B' or G' is 1.

The action with respect to the basis $(v'_i)_{1\le i\le 12}$ of $V' \cap v'^{\perp}_*$ is as follows:

$$\begin{aligned} \overline{u}v'_i &= \epsilon^i v'_i, \\ \overline{t}v'_i &= v'_{4i}, \\ \overline{w}v'_i &= \sum_{j=1}^{12} c_{ji} v'_j, \end{aligned}$$

where c_{ji} is defined using the field $\mathrm{GF}(13^2)$ (cf. [NaSh], §II.5.7). This field can be defined as $\{a + b\sqrt{2} \mid a, b \in \mathrm{GF}(13)\}$. The element $q = 2+\sqrt{2}$ is a primitive element as $(2+\sqrt{2})^{14} = (2+\sqrt{2})^{13}(2+\sqrt{2}) = (2-\sqrt{2})(2+\sqrt{2}) = 2$. Write $s = \overline{q} = 2-\sqrt{2}$ and let ζ be a primitive 7-th root of unity. Then

$$c_{ji} = -\frac{1}{13} \sum_{\substack{k=1 \\ 2^k \equiv ji^{-1} \bmod 13}}^{169} \zeta^k \epsilon^{-i(q^k+s^k)}.$$

An alternate definition is

$$c_{ji} = -\frac{1}{13} \sum_{\substack{a \in \mathrm{GF}(169) \\ a\overline{a} = ji^{-1}}} \rho(a)\chi((ia+ja^{-1})(-1))$$

where $\rho(t^k) = \zeta^k$ and $\chi(\alpha) = \epsilon^\alpha$ if $\alpha \in \mathrm{GF}(13)$. Note that if $a\overline{a} = ji^{-1}$, then $ia + ja^{-1} = ia + i\overline{a} = i(a+\overline{a}) \in \mathrm{GF}(13)$.

We now use the equation $\langle v_1', v_\infty, w_0\rangle = \langle \overline{w}v_1', \overline{w}v_\infty, \overline{w}w_0\rangle = \langle \overline{w}v_1', w_0, v_\infty\rangle$ to find the value for B'. In fact

$$\begin{aligned} 13\langle v_i', v_\infty, w_0\rangle &= 13\langle v_i', v_\infty, \sum_{j=0}^{12} v_j\rangle \\ &= \langle v_i', v_\infty, v_{-i}\rangle \\ &= \begin{cases} \langle v_1', v_\infty, v_{12}\rangle & \text{if } i \in S \\ \langle v_2', v_\infty, v_{11}\rangle & \text{if } i \notin S \end{cases} \\ &= \begin{cases} -A(\omega^2 B'B + \omega C'C) & \text{if } i \in S \\ -A(G'G + \omega^2 F'F) & \text{if } i \notin S. \end{cases} \end{aligned}$$

Here S is the set of nonzero squares in GF(13). We also have

$$\begin{aligned} 13\langle \overline{w}v_1', w_0, v_\infty\rangle =& 13\langle \sum_{k=1}^{12} c_{k1}v_k', v_\infty, w_0\rangle \\ =& \left(\sum_{j\in S} c_{j1}\right)(-A)(\omega^2 B'B + \omega C'C) \\ &+ \left(\sum_{j\notin S} c_{j1}\right)(-A)(G'G + \omega^2 F'F) \\ =& A(G'G + \omega^2 F'F) \end{aligned}$$

as

$$\sum_{j\in S} c_{j1} = 0 \qquad \text{and} \qquad \sum_{j\notin S} c_{j1} = -1.$$

This gives the equation

$$-(\omega^2 B'B + \omega C'C) = (G'G + \omega^2 F'F). \tag{22}$$

The equation for $\langle v_2', v_\infty, w_0\rangle$ is the same as

$$\sum_{j\in S} c_{j2} = -1 \qquad \text{and} \qquad \sum_{j\notin S} c_{j2} = 0.$$

Solving (21) and (22) gives $B' = G' = 1$ and we have

$$B' = G' = 1, \qquad C' = 33 + 72A + 7A^2, \qquad F' = 46 + 7A + 72A^2.$$

Notice $C' = -F'$. Incidentally, the full set of roots of $X^3 + 64X^2 + 16X + 56$ is A, $34 + 24A + 73A^2$, $60 + 54A + 6A^2$.

We have one more hurdle to overcome and for this we use the equation

$$\langle v_1', v_{12}', w_0\rangle = \langle \overline{w}v_1', \overline{w}v_{12}', v_\infty\rangle.$$

The left hand side evaluates as

$$\langle v_1', v_{12}', w_0\rangle = -\frac{1}{13}(\omega B'^2 + \omega^2 C'^2).$$

The right hand side evaluates as

$$\begin{aligned}\langle \overline{w}v_1', \overline{w}v_{12}', v_\infty\rangle &= \Big\langle \sum_{j=1}^{12} c_{j1} v_j', \sum_{j=1}^{12} c_{j,12} v_j', v_\infty\Big\rangle \\ &= \sum_{j=1}^{12} c_{j1} c_{-j,12} \langle v_j', v_{-j}', v_\infty\rangle.\end{aligned}$$

As $\langle v_{4i}', v_{-4i}', v_\infty\rangle = \omega^2 \langle v_i', v_{-i}', v_\infty\rangle$, as well as $\langle v_1', v_{-1}', v_\infty\rangle = -A(\omega^2 B'^2 + \omega C'^2)$ and $\langle v_2', v_{-2}', v_\infty\rangle = -A(G'^2 + \omega^2 F'^2)$, this sum is

$$\begin{aligned}\gamma = &\left(\sum_{4^j \bmod 13} c_{4^j,1} c_{-4^j,12}\, \omega^{2j}\right)(\omega^2 B'^2 + \omega C'^2)(-A) \\ &+ \left(\sum_{2\cdot 4^j \bmod 13} c_{2\cdot 4^j,1} c_{-2\cdot 4^j,12}\, \omega^{2j}\right)(\omega^2 F'^2 + G'^2)(-A).\end{aligned}$$

Straightforward computations show

$$\omega^2 B'^2 + \omega C'^2 = 18 + 25A + 28A^2,$$
$$\omega^2 F'^2 + G'^2 = 19 + 22A + 12A^2.$$

In order to evaluate the above sums, we need a value for $\zeta^i + \zeta^{-i}$. The choice of this value is related to the choice of algebraic conjugate from the three 12 dimensional representations of $L(2,13)$. There are three roots in $\mathrm{GF}(79^3)$ to $p(X) = X^3 + X^2 - 2X - 1$, the minimal polynomial of $\zeta^i + \zeta^{-i}$. It is found by searching that the roots are $15 + 40A + 47A^2$, $32 + 72A + 7A^2$ and $31 + 46A + 25A^2$, where in fact $32 + 72A + 7A^2 = (15 + 40A + 47A^2)^{79}$. Each of the three different (but algebraically conjugate) 12 dimensional representations of $L(2,13)$ over $\mathbb{Z}/79[A]$ is obtained by identifying $\zeta^1 + \zeta^{-1}$ with one of these roots.

First, suppose $\zeta^1 + \zeta^{-1} = 32 + 72A + 7A^2$. There are no terms $\zeta^1 + \zeta^{-1}$ in $(c_{ij})_{1\le i,j\le 12}$. Setting

$$\zeta^2 + \zeta^5 = 31 + 46A + 25A^2 \qquad \text{and} \qquad \zeta^3 + \zeta^4 = 15 + 40A + 47A^2,$$

and substituting these values into c_{ji} turns $\overline{w}$ into a matrix of order two. Now,

$$\sum_{4^j \bmod 13} c_{4^j,1} c_{-4^j,12} \omega^{2j} = 6 + 58A + 64A^2,$$
$$\sum_{2\cdot 4^j \bmod 13} c_{2\cdot 4^j,1} c_{-2\cdot 4^j,12} \omega^{2j} = 14 + 13A + 44A^2.$$

Reversing these gives an element not of order two and so the choices above are the correct ones for the representation of $L(2,13)$ in V'. However, substituting the values for these sums in the equations above gives $\gamma = 22 + 54A + 69A^2$ but $-\frac{1}{13}(\omega B'^2 + \omega^2 C'^2) = 9 + 53A + 72A^2$. Consequently, this case is eliminated. Similarly, several other elements such as $\langle v_1', v_{11}', w_0\rangle$, $\langle v_1', v_2', w_0\rangle$ also provide contradictions.

Similarly, the case where $\zeta^1 + \zeta^{-1} = 15 + 40A + 47A^2$ leads to a contradiction.

Thus, we are left with

$$\zeta^1 + \zeta^{-1} = 31 + 46A + 25A^2.$$

Now the matrix $(c_{ij})_{ij}$ for $\overline{w}$ on the 12 dimensional subspace of V' with respect to the basis $v'_1, \ldots, v'_{12}$ is

$$\overline{w} = \begin{pmatrix}
\lambda_1 & \lambda_2 & \lambda_3 & \lambda_4 & \lambda_5 & \lambda_6 & \lambda_7 & \lambda_8 & \lambda_9 & \lambda_{10} & \lambda_{11} & \lambda_{12} \\
\lambda_2 & \lambda_4 & \lambda_6 & \lambda_8 & \lambda_{10} & \lambda_{12} & \lambda_1 & \lambda_3 & \lambda_5 & \lambda_7 & \lambda_9 & \lambda_{11} \\
\lambda_3 & \lambda_6 & \lambda_9 & \lambda_{12} & \lambda_2 & \lambda_5 & \lambda_8 & \lambda_{11} & \lambda_1 & \lambda_4 & \lambda_7 & \lambda_{10} \\
\lambda_4 & \lambda_8 & \lambda_{12} & \lambda_3 & \lambda_7 & \lambda_{11} & \lambda_2 & \lambda_6 & \lambda_{10} & \lambda_1 & \lambda_5 & \lambda_9 \\
\lambda_5 & \lambda_{10} & \lambda_2 & \lambda_7 & \lambda_{12} & \lambda_4 & \lambda_9 & \lambda_1 & \lambda_6 & \lambda_{11} & \lambda_3 & \lambda_8 \\
\lambda_6 & \lambda_{12} & \lambda_5 & \lambda_{11} & \lambda_4 & \lambda_{10} & \lambda_3 & \lambda_9 & \lambda_2 & \lambda_8 & \lambda_1 & \lambda_7 \\
\lambda_7 & \lambda_1 & \lambda_8 & \lambda_2 & \lambda_9 & \lambda_3 & \lambda_{10} & \lambda_4 & \lambda_{11} & \lambda_5 & \lambda_{12} & \lambda_6 \\
\lambda_8 & \lambda_3 & \lambda_{11} & \lambda_6 & \lambda_1 & \lambda_9 & \lambda_4 & \lambda_{12} & \lambda_7 & \lambda_2 & \lambda_{10} & \lambda_5 \\
\lambda_9 & \lambda_5 & \lambda_1 & \lambda_{10} & \lambda_6 & \lambda_2 & \lambda_{11} & \lambda_7 & \lambda_3 & \lambda_{12} & \lambda_8 & \lambda_4 \\
\lambda_{10} & \lambda_7 & \lambda_4 & \lambda_1 & \lambda_{11} & \lambda_8 & \lambda_5 & \lambda_2 & \lambda_{12} & \lambda_9 & \lambda_6 & \lambda_3 \\
\lambda_{11} & \lambda_9 & \lambda_7 & \lambda_5 & \lambda_3 & \lambda_1 & \lambda_{12} & \lambda_{10} & \lambda_8 & \lambda_6 & \lambda_4 & \lambda_2 \\
\lambda_{12} & \lambda_{11} & \lambda_{10} & \lambda_9 & \lambda_8 & \lambda_7 & \lambda_6 & \lambda_5 & \lambda_4 & \lambda_3 & \lambda_2 & \lambda_1
\end{pmatrix}$$

where

$$\begin{aligned}
\lambda_1 &= 3A + 38A^2 + 43, & \lambda_7 &= 62A + 76A^2 + 57,\\
\lambda_2 &= 50A + 2A^2 + 46, & \lambda_8 &= 16A + 6A^2 + 73,\\
\lambda_3 &= 46A + 4A^2, & \lambda_9 &= 54A + 26A^2 + 35,\\
\lambda_4 &= 34A + 15A^2 + 46, & \lambda_{10} &= 33A + 7A^2 + 28,\\
\lambda_5 &= 39A + 29A^2 + 51, & \lambda_{11} &= 42A + 35A^2 + 29,\\
\lambda_6 &= 28A + 10A^2 + 59, & \lambda_{12} &= 67A + 68A^2 + 6.
\end{aligned}$$

A direct check using computer of $\langle \overline{w}x, \overline{w}y, \overline{w}z \rangle = \langle x, y, z \rangle$ for all triples x, y, z from the basis $v_1, \ldots, v_{14}$, $v'_1, \ldots, v'_{12}$, v'_* shows that the resulting element $\overline{w}$ belongs to $\widetilde{E}$, whence to $\widetilde{F}$ as it stabilizes v'_*.

By construction of the representations 12 and 14, the elements $\overline{t}$, $\overline{u}$, $\overline{w}$ generate a subgroup of $\widetilde{F}$ isomorphic to $L(2,13)$. From uniqueness up to conjugacy class of subgroups isomorphic to the Borel subgroup B of $L(2,13)$, cf. Lemma 2.1, and from uniqueness of $\overline{w}$ given solution (c) of §4, we infer that the subgroup is unique up to algebraic conjugacy (from the choice of A as a solution of the cubic $X^3 + 64X^2 + 16X + 56$). But changing to an algebraic conjugate changes the representation, hence uniqueness with given character. The arguments show the same is true over $\mathbb{C}$. As 79 is prime to $|L(2,13)|$, this representation can be lifted to $\mathbb{C}$ by arguments described in [CW92] or [CGL] and also in section eight below. This finishes the proof of part (ii) of Theorem 3.1 except for the statement about the extension to PGL$(2,13)$.

7. The complex cases and the automorphism

There is an element $m \in \widetilde{E}$ which squares to $\bar{t}$ and normalizes $\bar{u}$. The following element is such an element as a check will show.

$$-X_1 \mapsto X_{24} \mapsto -X_3 \mapsto X_5 \mapsto X_{14} \mapsto -X_{16} \mapsto -X_{13} \mapsto X_{2'} \mapsto$$

$$X_{4'} \mapsto -X_{35} \mapsto X_{1'} \mapsto X_{25} \mapsto -X_1,$$

$$X_2 \mapsto X_{5'} \mapsto -X_{15} \mapsto -X_{36} \mapsto X_{6'} \mapsto X_{56} \mapsto X_{23} \mapsto -X_{45} \mapsto$$

$$-X_{26} \mapsto X_6 \mapsto -X_{46} \mapsto -X_{12} \mapsto X_2,$$

$$X_4 \mapsto X_{34} \mapsto -X_{3'} \mapsto X_4.$$

A check also shows $m^{-1}\bar{u}m = \bar{u}^2$.

Of course m normalizes $\langle \bar{u}, \bar{t} \rangle$ and so under conjugation acts on subgroups containing $\langle \bar{u}, \bar{t} \rangle$. In the E_6 case where the character is $13 + 14$, there are exactly two $L(2, 13)$s and so m either fixes one of these $L(2, 13)$s or maps it to the other. However, m could not fix one as PGL(2, 13) is not contained in $\widetilde{E}_6(\mathbb{C})$ as an involution has the wrong trace (see [CW92]) and so m interchanges the two. Consequently there is one conjugacy class of such $L(2, 13)$s in $\widetilde{E}_6(\mathbb{C})$. In the $\mathbf{F}_4$ case where the character is $1 + 12 + 14$, there is a unique $L(2, 13)$ and so m must normalize it. Consequently there is an embedding of PGL(2, 13) in $\widetilde{E}_6(\mathbb{C})$ whose image is contained in a subgroup of type F_4.

To check directly that the four possibilities (a), (b), (d), (e) for A, B, C, D, F, G are fused in pairs to two solutions it is necessary to conjugate by m and evaluate the various constants using the construction above. As $m^2 = \bar{t}$, we must check that $mv_1 = \omega v_2^*$ and $mv_2 = \omega v_1^*$ where v_1, v_2 are as above and v_1^*, v_2^* are the corresponding vectors using $\overline{w}^m$ and $\bar{t}^m = \bar{t}$ instead of $\overline{w}$ and $\bar{t}$. Note $mv_i = \omega v_{2i}^*$. In particular

$$m(51X_1 - 55X_{12}) = -51X_{24} + 55X_2 = \omega(23X_2 + 39X_{24}),$$

$$m(-23\omega^2 X_{46} + \omega^2 17X_{25}) = -23\omega^2 X_{12} - \omega^2 17X_1 = \omega(4X_1 - 55X_{12}),$$

$$22mX_{12} = -22X_2 = \omega(-25X_2),$$

$$\omega^2 m(-\sqrt{7}X_{46} - \sqrt{7}X_{25}) = \omega^2(\sqrt{7}X_{12} + \sqrt{7}X_1) = \omega(-\sqrt{-10}X_1 - \sqrt{-10}X_{12}).$$

This shows the two solutions with $A = -20$ are fused as are the two solutions with $A = 20$. To check directly that m normalizes the $L(2, 13)$ it is sufficicient to check that m preserves the invariant subspaces and this is equivalent to $F=\omega^2 C$, $G=-\omega^2 B$ and $G'=B'$, $F'=-C'$ and these all hold.

By combining this with results from §§5 and 6 we conclude that Theorem 3.1 has been proved. ∎

We were able to find solutions over $\mathbb{C}$ of the equations with $C=\omega F$ using the same method as for GF(79). The two polynomials were difficult to factor and we thank R. Wilson for finding the relevant factors. Because the linear factor has multiplicity three, the linear factor is the greatest common divisor of the polynomial and its second derivative. The cubic is the GCD of the polynomials after the linear factor cubed has been removed. Another way of finding the cubic will be described below. The value for A in the linear term is an element in $Q[\epsilon+\epsilon^{12}+\epsilon^5+\epsilon^8,\omega]$. If

$$\Delta_i=\epsilon^i+\epsilon^{-i}+\epsilon^{5i}+\epsilon^{-5i},$$

$$A=\frac{1}{13}(\omega\Delta_1+\omega^2\Delta_2+\Delta_3).$$

This element A satisfies $13^2A^2=-(4+3\omega)$. Setting A as this value, the equations have a manageable form. Keep in mind that $C=\omega F$.

The equations (1) to (9) become

$$(1)\qquad -30-18\omega+6B^2\omega+12F^2\omega+6G^2=0,$$

$$(2)\qquad -24-18\omega+B^2(-2+5\omega)+F^2(3+12\omega)+G^2(7+2\omega)=0,$$

$$(3)\qquad -24-18\omega+B^2(-2+5\omega)+F^2(3+12\omega)+G^2(7+2\omega)=0,$$

$$(4)\ -24-18\omega+B^2(-2+5\omega)+F^2(3-14\omega)+G^2(7+15\omega)-13B^3+13F^3=0,$$

$$(5)\ -24-18\omega+B^2(-15-\omega)+F^2(3-14\omega)+G^2(7+2\omega)+13F^3+13G^3=0,$$

$$(6)\qquad -24-18\omega+B^2(-2+5\omega)+F^2(-10-\omega)+G^2(-6-11\omega)+13BF^2=0,$$

$$(7)\quad -24-18\omega+B^2(-2-8\omega)+F^2(16+12\omega)+G^2(-6+2\omega)+26BFG\omega=0,$$

$$(8)\quad -24-18\omega+B^2(-2-8\omega)+F^2(16+12\omega)+G^2(-6+2\omega)+26BFG\omega=0,$$

$$(9)\qquad -24-18\omega+B^2(11+5\omega)+F^2(-10-\omega)+G^2(7+2\omega)-13F^2G\omega=0.$$

As in the modular case the first equation times $(-2+5\omega)$ is equal to the second equation times 6ω and so $F^2=-(1+\omega)=\omega^2$ and so $F=\pm\omega$. Substituting the value for G^2 found from equation (1) into equation (4) gives the cubic B^3+

$\omega^2 B^2 + 4$. The root $B = -2\omega$ does not satisfy for example equation (9). The other two roots are $\omega^2(1 \pm \sqrt{-7})/2$.

The case $F = -\omega$ has no solution. This can be shown by substituting the relations from equation (1) into equations (4) and (6).

The solutions with $F = \omega$ are

$$A = \frac{1}{13}(\omega\Delta_1 + \omega^2\Delta_2 + \Delta_3), \qquad B = \frac{1}{2}\omega^2(1 \pm \sqrt{-7}), \quad C = \omega^2, \qquad F = \omega, \quad G = \frac{1}{2}\omega(-1 \pm \sqrt{-7}).$$

The complementary equations are also manageable. The solutions are

$$B' = \frac{1}{28}(-7 \mp \sqrt{-7}), \qquad F' = \frac{1}{28}(7 \pm 3\sqrt{-7}),$$
$$C' = \frac{1}{28}(7 \mp 3\sqrt{-7}), \qquad G' = \frac{1}{28}(7 \mp \sqrt{-7}).$$

These were solved by finding a solution for the first four equations using cofactors and checking the solution worked for all of them.

The solution for the cubic case can also be found using the method of §4 but can be simplified by using some extra conditions. The cubic itself over $Q[\omega, \epsilon]$ has coefficients which are in $Q[\omega, \Delta_i]$. We denote this polynomial by $h(A)$. It is

$$\begin{aligned} h(A) &= -3 - 4\omega + (4 + 2\omega + (6 + 6\omega)\Delta_2 + 6\Delta_4)A \\ &\quad + (-14 - 10\omega - (24 + 6\omega)\Delta_2 - (18 + 24\omega)\Delta_4)A^2 + 169A^3. \end{aligned}$$

The norms of the coefficients of A^0 and A^3 are 13 and 169. There are six algebraic conjugates of the equation. The product of them after dividing by 169 is

$$\mu_0 + \mu_3 A^3 + \mu_6 A^6 + \mu_9 A^9 + \mu_{12} A^{12} + \mu_{15} A^{15} + \mu_{18} A^{18}$$

where

$$\mu_0 = 13, \quad \mu_3 = 1002, \quad \mu_6 = 46527, \quad \mu_9 = 270780,$$
$$\mu_{12} = 102219818, \quad \mu_{15} = 4836462618, \quad \mu_{18} = 13^{10}.$$

This is the minimal polynomial over Q. Notice this is a polynomial in A^3 of degree 6. The equations (1) to (9) can be simplified here because we know the solution is invariant under the automorphism m. This has the consequence that $F = \omega^2 C$, $G = -\omega^2 B$ and $G' = B'$, $F' = -C'$. Substituting these values gives equations in the unknowns A, B, C. Some of the equations become the same. In particular the second and third, the fourth and fifth, the sixth and ninth, and the seventh and eighth are all the same. Recall once we chose $C = \omega F$ the seventh and eighth were the same. Solving as in §4 is easier. The matrix Z from case 1 in §4 can be replaced by a 2 by 3 matrix. The polynomials from equations (7) and (9) are of degree twelve instead of fifteen and have the cubic as greatest common divisor which can be found using the Euclidean algorithm.

However there is an easier way to solve this using the equation (19) or (20) from §6. With these simplifications these equations become

$$(B^2 + C^2)(\Lambda_1^* + \omega\Lambda_2^*) = 39 \cdot A. \tag{23}$$

Equation (1′) becomes

$$-12(\omega B^2 + \omega^2 C^2) + 6 = 13^2 \cdot 6A^3. \tag{24}$$

Using these equations we can form the 2 by 3 matrix of coefficients as in §4 to obtain the matrix equation $X \cdot Y = 0$ where

$$X = \begin{pmatrix} 6 - 1014A^3 & 12\omega & 12\omega^2 \\ -39A & \Lambda_1^* + \omega\Lambda_2^* & \Lambda_1^* + \omega\Lambda_2^* \end{pmatrix} \quad \text{and} \quad Y = \begin{pmatrix} 1 \\ B^2 \\ C^2 \end{pmatrix}.$$

Let R_i be the determinant of X with column i deleted.

As $R_1 \neq 0$, the matrix X has rank 2 and Y is proportional to $(R_1, -R_2, R_3,)$ and so

$$B^2 = -R_2/R_1, \qquad C^2 = R_3/R_1.$$

For purposes in the next section note the norm of R_1 is $2^4 \cdot 3^3 \cdot 13$, a P local unit for all primes P not dividing $|L(2,13)|$. We will also need to know that $h(A)$ has no root in common with $R_2(A)$ or with $R_3(A)$ mod P for such a P. For this we calculate the resultants of $h(A)$ with $R_2(A)$ and $R_3(A)$ and find their norm is $2^{12} \cdot 3^{15} \cdot 13^{13}$. This is done using the computer. The values for B^2 and C^2 are each polynomials of degree 3 divided by R_1.

Now just as in §4, the remaining equations can be used to find the polynomial satisfied by A. Equation (2) gives a quartic equation in A. Then, equations (8) and (9) give polynomials which are of degree nine. The greatest common divisor of any two of these is $h(A)$. After reducing mod 79 it is the cubic of §4 and so is irreducible. The advantage to using this method is the Euclidean algorithm is implemented to find the greatest common divisor of a quartic and a ninth degree polynomial rather than two polynomials of degree twelve. As in §6, the equation $\langle v'_*, v'_1, v_{12}\rangle = -(B'B + C'C) = 0$ holds and so we can take $B' = 1$ and $C' = -B/C$.

The equation for h can be solved by Cardano's formulas. For this we calculate a square root of the discriminant is $\frac{105-42\omega}{13^3}$. If λ is the coefficient of A^2 divided by the coefficient of A^3, the roots are $\frac{1}{3}(-\lambda + \omega^i a + \omega^{-i} b)$ for $i = 0, 1, 2$ and

$$a = \left(\frac{7896 + 11256\omega}{13^4}\right)^{\frac{1}{3}}, \qquad b = \left(\frac{525 + 1428\omega}{13^4}\right)^{\frac{1}{3}}.$$

The cube roots must be chosen appropriately.

These remarks prove the following lemma.

LEMMA 7.1: *Suppose O is the ring of integers in an algebraic number field containing ω and ϵ and containing A in the $1+12+14$ case. Let P be a prime ideal of O satifying $P \cap \mathbb{Z} = (p)$ for an integral prime p other than $\{2, 3, 7, 13\}$. The representations obtained here of $L(2, 13)$ and* PGL(2, 13) *all have coefficients in the P localization of O.*

8. Results for fields of nonzero characteristic

Our results over $\mathbb{C}$ have consequences in $\widetilde{E}_6(k)$ for finite fields of characteristic p prime to $|L(2, 13)|$.

We first discuss some well known facts about lifting representations from characteristic p to characteristic 0. Suppose k is a finite field of characteristic p and suppose that L is a finite subgroup of $\widetilde{E}_6(\overline{k})$ of order prime to p. Here $\overline{k}$ denotes the algebraic closure of k. Consider $\widetilde{E}_6(k)$ as a subgroup of GL(27, k). As L is finite, there is a suitable conjugate of the natural basis such that all matrix coefficients of elements of L are in some finite extension of GF(p), say $k' =$ GF(p^s). Now there is a number field ℓ for which the integers O in ℓ have the property that O/P has order p^s where P is a prime containing p in O. Now let O_P be the completion of the P adic integers and ℓ_P the quotient field. As is well known $k' \cong O/P \cong O_P/PO_P$. Reduction mod PO_P is a homomorphism from $\widetilde{E}_6(O_P)$ onto $\widetilde{E}_6(k')$ where k' is the quotient field O_P/PO_P. The map is onto as $\widetilde{E}_6(k')$ is generated by elements for which there are lifts in $\widetilde{E}_6(O_P)$. For instance by [AsI 3.17], $\widetilde{E}_6(k')$ is generated by the Weyl group which can be chosen monomial with coefficients ± 1 and a group L for which the coefficients are taken from k'. For each of these elements there is an element of $\widetilde{E}_6(O_P)$ which reduces to these mod PO_P. The elements $X(t)$ and $X'(t)$ in [AsI, 3.2] together with the Weyl group can also be used. There are also intermediate maps from $\widetilde{E}_6(O_P/P^nO_P)$ onto $\widetilde{E}_6(k')$. Let L_n be the inverse image in $\widetilde{E}_6(O_P/P^nO_P)$ of L. The kernel of the map from $\widetilde{E}_6(O_P/P^nO_P)$ to $\widetilde{E}_6(k')$ is a finite p-group as the same is true in $\mathrm{GL}(27, O_P/P^nO_P)$. This means that $|L_n| = |L|p^t$ for some t. By the Schur Zassenhaus theorem [Go], there is a subgroup in L_n isomorphic to L and all are conjugate. By taking corresponding subgroups L, for higher and higher powers of P, there is a subgroup of $\widetilde{E}_6(O_P)$ isomorphic to L which maps to L under reduction mod PO_P as O_P is P adically closed. There is an embedding of ℓ_P in $\mathbb{C}$. [We note in passing that this not a topological embedding.] This gives an embedding of L in $\widetilde{E}_6(\mathbb{C})$.

For the remainder of this section, we take $L = L(2,13)$ and O as in Lemma 7.1. We will prove the main theorem about subgroups isomorphic to $L(2,13)$ in $\widetilde{E}_6(k)$ by lifting them to $\widetilde{E}_6(O_P)$, proving a result there, and then reducing mod P for suitable P.

THEOREM 8.1: *Let k be a finite field of characteristic p, and suppose $p \neq \{2,3,7,13\}$ (i.e., p does not divide $|L(2,13)|$). If L is a subgroup of $\widetilde{E}_6(k)$ isomorphic to $L(2,13)$ for which the character on* $\mathbf{K}$ *is $1+12+14$ or $13+14$, then L is conjugate in $\widetilde{E}_6(\overline{k})$ to the reduction mod PO_P of the appropriate group defined in Lemma 7.1. In the $1+12+14$ case L is conjugate within the stabilizer in $\widetilde{E}_6(\overline{k})$ of a fixed 1 space of* $\mathbf{K}$ *(a group of type F_4 over $\overline{k}$) to this reduction. The conjugation can in fact be done in any extension of k which contains primitive 13th and cube roots of unity and a root of x^3+x^2-2x-1 in the F_4 case.*

We prove this by establishing the following result.

THEOREM 8.2: *Let O and P be as in Lemma 7.1. Suppose L is a subgroup of $\widetilde{E}_6(O_P)$ isomorphic to $L(2,13)$ for which the character is $13+14$ or $1+12+14$ and suppose $p \neq \{2,3,7,13\}$ (i.e., p does not divide $|L(2,13)|$). Then L is conjugate in $\widetilde{E}_6(O_P)$ to one of the groups defined in Lemma 7.1. In particular there are unique conjugacy classes of such subgroups in $\widetilde{E}_6(O_P)$.*

Proof: Because O_P contains all 13th and 3rd roots of unity, and $13, 3 \notin P$, we may diagonalize the 27×27 matrix corresponding to u and put the 27×27 matrix corresponding to t in monomial form. Thus, we may assume that the Borel subgroup of L coincides with the one given in §2, and L must be as reviewed in §7.

The coefficients for A, B, C, F, G, B', C', F', G' obtained in Lemma 7.1 in the $13+14$ case have P local coefficients as the only denominators are 2, 13, and 7 and the numerators are all in O. This means the O_P span of the $\{X_i, X_{i'}, X_{ij}\}$ contains the O_P span of $\{v_i, v_i'\}$. But the matrices

$$\begin{pmatrix} A & A\omega & A\omega \\ 1 & \omega^2 & \omega \\ 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} B & C \\ B' & C' \end{pmatrix}, \begin{pmatrix} F & G \\ F' & G' \end{pmatrix}$$

all have determinants which are P local integers not in P. In particular the determinants are $(3+6\omega)A$, $(21+3\sqrt{-7})\omega^2/28$, $(21-3\sqrt{-7})\omega/28$ and A satisfies $13^2A^2 = -(3+4\omega)$. This means that the O_P span of the standard basis $\{X_i, X_{i'}, X_{ij}\}$ is contained in the O_P span of $\{v_i, v_i'\}$ and so they are the same. Denote this span by U. The representation obtained in Lemma 7.1 gives an embedding of $L(2,13)$ in $\widetilde{E}_6(O_P)$ with action on U.

The same ideas work for the $1+12+14$ case. Note first that A is a unit in the P local integers as its minimal polynomial has leading and constant terms which are P local units. The values of B and C are P local integers as that is true for their squares. Recall R_1 is a P local unit as its norm is. Because the resultants of R_2 and R_3 with h are P local units, there can be no common root of R_i and h and so B and C are also P local units. As above we need to know the matrices

$$\begin{pmatrix} A & A\omega & A\omega \\ 1 & \omega^2 & \omega \\ 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} B & C \\ B' & C' \end{pmatrix}$$

have determinants which are P local units. The first does as above. For the second we have chosen $B' = 1$. If we let $B = \lambda C$ the equation (23) implies $1+\lambda^2$ is a unit. But as in §7, the equation $\langle v_*', v_1', v_{12}\rangle = -(B'B + C'C) = 0$ implies $C' = -\lambda B'$, so the second determinant is $-(1+\lambda^2)C$ which is a unit. This means the O_P span of the $\{X_i, X_{i'}, X_{ij}\}$ is the same as the O_P span of $\{v_i, v_i'\}$. Again denote this span by U. As above the representation obtained in Lemma 7.1 gives an embedding of $L(2,13)$ in $\widetilde{E}_6(O_P)$ with action on U fixing v_*'. Let L be this subgroup of $\widetilde{E}_6(O_P)$. Suppose L_1 is a subgroup as in the hypothesis. There is an element in $\widetilde{E}_6(\mathbb{C})$ which conjugates L to L_1 by Theorem 3.1. We will show that the conjugating element in $\widetilde{E}_6(\mathbb{C})$ is in $\widetilde{E}_6(O_P)$. Suppose this element is S. Recall that v_o is one of the unique vectors v fixed by $\overline{u}$ for which $\overline{t}v = \omega^2 v$ and $\langle v,v,v\rangle = 6$. The other such vectors are ωv and $\omega^2 v$. These are permuted by the scalar ωI, an element of $\widetilde{E}$. Once v_0 is determined, all the remaining v_i and v_i' are determined by the $\overline{t}$ and $\overline{w}$ images and the condition $\langle v_o, v_\infty, v_*'\rangle = -3A$. We show that $v_0* = Sv_0$ has coefficients in O_P and not in P. At any rate $\langle v_0*, v_0*, v_0*\rangle = 6$ which is not in P and so the coefficients cannot all be in P. Let $PO_P = \pi O_P$ and let π^s be the highest power of π occurring in the denominators of v_0*. Assume $s \neq 0$. Let $\overline{u}*$ and $\overline{t}*$ be the S conjugates of $\overline{u}$ and $\overline{t}$ which are in $\widetilde{E}_6(O_P)$. Now $v* = \pi^s v_0*$ is an element with coefficients in O_P but not all in P. Further $v*$ is an eigenvalue for $\overline{u}*$ and $\overline{t}*$ with eigenvalues 1 and ω^2. Now reduce $\langle \overline{u}*, \overline{t}*\rangle$ mod PO_P and consider its action in $\widetilde{E}_6(k')$. The vector $v*$ is not the zero vector but satisfies $\langle v*, v*, v*\rangle = 0$. However by Lemma 2.1 there is a vector v' for which $\langle v', v', v'\rangle = 6$ which is not 0 in k' and on which the action of $\langle \overline{u}*, \overline{t}*\rangle$ is the same as on $v*$. Furthermore there is a unique vector with this action to within scalars. This is a contradiction and shows that $s = 0$ and so v_0* has coefficients in O_P. The same argument shows that Sv_*' has coefficients in O_P and not in P. This argument shows that SU is an O_P submodule of U. But the same argument applied to S^{-1} shows that $S^{-1}SU$ is an O_P submodule of SU and so U is a submodule of SU. Now $U = SU$ and all coefficients in S and S^{-1} are in O_P. This proves Theorem 8.2. ∎

Proof of Theorem 8.1: Suppose L is as in the hypotheses. Lift it to $\widetilde{E}_6(O_P)$ as discussed above. Then, by Theorem 8.2, the lifted image is conjugate in $\widetilde{E}_6(O_P)$ to the corresponding group defined in Lemma 7.1. ∎

We now come to the actual implications for finite fields.

THEOREM 8.3: *Let p be a prime other than $\{2,3,7,13\}$ and q a power of p. Then $E_6(q)$ or $E_6(q^3)$ contains subgroups isomorphic to* PGL(2,13) *for which the action on* **K** *is $1+12+14$. The subgroup will be in $E_6(q)$ if and only if* GF(q) *contains the trace of the 12 dimensional character which is a root of x^3+x^2-2x-1. This subgroup is in $F_4(q)$. The group $E_6(q)$ contains a subgroup isomorphic to $L(2,13)$ for which the action on* **K** *is $13+14$ if and only if* GF(q) *contains $\sqrt{-91}$. Otherwise, ${}^2E_6(q)$ contains a subgroup isomorphic to $L(2,13)$ for which the action on* **K** *is $13+14$. By its definition, ${}^2E_6(q)$ is a subgroup of $E_6(q^2)$. Any group in $E_6(q)$ conjugate in E_6 over an extension field to $\langle \bar{u}, \bar{t}\rangle$ in Lemma 2.1 is in a unique conjugacy class of each of these $L(2,13)$s.*

Remark: It is shown in [As87] that the group $G_2(q)$ contains an $L(2,13)$ if and only if $\sqrt{13}$ is in GF(q). It follows from work in [Te] that $G_2(q)$ is in $E_6(q)$ if and only if $\sqrt{-7}$ is in GF(q). Theorem 8.3 shows that $L(2,13)$ is in $E_6(q)$ if and only if either both square roots are in GF(q) or both not in GF(q).

Proof of Theorem 8.3: Let k be the field obtained by adjoining to GF(q) the roots of $x^{13}-1$, x^3-1, x^2+7 and let σ be the Frobenius automorphism whose fixed field is GF(q). The construction in Lemma 7.1 reduced modulo PO_P in the $13+14$ case provides an embedding of $L(2,13)$ in $E_6(k)$. We denote the images of u, t, w in $E_6(k)$ by $\overline{u}$, $\overline{t}$, $\overline{w}$. The field automorphism corresponding to σ fixes $\overline{t}$ and acts on $\overline{u}$ by raising it to a power s. A product of this with conjugation by an element normalizing $\overline{u}$ must centralize $\overline{u}$ and act on $\langle \overline{u}, \overline{t}\,\rangle$. Denote this automorphism by τ. This must normalize or interchange the two $L(2,13)$s which contain $\langle \overline{u}, \overline{t}\,\rangle$. The field automorphism fixes each of the $L(2,13)$s if and only if it fixes $\sqrt{-7}$ from observing the action particularly on the 13 space. But $\sqrt{-7}$ is fixed if and only if $\sqrt{-7}$ is in GF(q). Conjugation by an element normalizing $\overline{u}$ fixes each $L(2,13)$ if and only if the element is in $L(2,13)$ which happens if and only if s is a square mod 13 which happens if and only if GF(q) contains a square root of 13. Now τ fixes each $L(2,13)$ if and only if $\sqrt{-91}$ is in GF(q). If it fixes an $L(2,13)$ it must induce an inner automorphism as no outer automorphism centralizes the element of order 13. Now a conjugate is centralized and so is in $E_6(q)$. A graph automorphism of E_6 which centralized $\overline{u}$ could not fix the $L(2,13)$s or the fixed points would be in F_4 or C_4. Neither is consistent with the action on **K**. [For F_4 fixes a nonzero vector, whereas $L(2,13)$ has no nonzero fixed vectors, and for C_4 the only irreducible $L(2,13)$ representations possible in the natural 8 dimensional representation space N for C_4 are of dimension 7 or 6, while $\mathbf{K} \cong \bigwedge^2 N$ as C_4 modules.] In either case the action on **K** could not be $13+14$. Consequently if $\sqrt{-91}$ is not in GF(q) neither the graph nor τ acts on each $L(2,13)$ and so the product of the two must. Again a conjugate is in ${}^2E_6(q)$.

We may use the same idea for the $1+12+14$ character by adjoining roots of h or x^3+x^2-2x-1 if necessary. There is a PGL(2,13) in $E_6(k)$ with each of the three algebraic conjugates of the character $1+12+14$. If GF(q) contains a root of x^3+x^2-2x-1 the field automorphism normalizes each and so is inner and so fixes a conjugate. This means they are all in $E_6(q)$. Otherwise they are all in $E_6(q^3)$.

The statement about conjugates follows from these arguments and Theorem 8.1 ∎

References

[AsI] M. Aschbacher, *The 27-dimensional module for E_6, I,* Inventiones Math. **89** (1987), 159–195.

[AsII] M. Aschbacher, *The 27-dimensional module for E_6, II,* J. London Math. Soc. **37** (1988), 275–293.

[AsIII] M. Aschbacher, *The 27-dimensional module for E_6, III,* Trans. Amer. Math. Soc. **321** (1990), 45–84.

[AsIV] M. Aschbacher, *The 27-dimensional module for E_6, IV,* J. Algebra **131** (1990), 23–39.

[As87] M. Aschbacher, *Chevalley groups of type G_2 as the group of a trilinear form,* J. Algebra **109** (1987), 131–259.

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

[CGL] A.M. Cohen, R.L. Griess, Jr. and B. Lisser, *The group $L(2,61)$ embeds in the Lie group of type E_8,* Comm. Algebra (1993), to appear.

[CW83] A.M. Cohen and D.B. Wales, *Finite subgroups of $G_2(\mathbb{C})$,* Comm. Algebra **11** (1983), 441–459.

[CW92] A.M. Cohen and D.B. Wales, *Finite subgroups of $E_6(C)$ and $F_4(C)$,* preprint 1992.

[Di] L. Dickson, *A class of groups in the arbitrary realm connected with the configuration of the 27 lines on a cubic surface,* Quarterly J. Pure Appl. Math **33** (1901), 145–173.

[Freu] H. Freudenthal, *Beziehungen der E_7 und E_8 zur Oktavenebene, VIII,* Indagationes Math. (1959), 447–465

[Go] D. Gorenstein, *Finite Groups,* Harper & Row, New York, 1968.

[Mag] K. Magaard, *The Maximal Subgroups of the Chevalley Groups $F_4(F)$ where F is a Finite or Algebraically Closed Field of Characteristic $\neq 2,3$,* PhD Thesis, Caltech (1990).

[NaSh] M.A. Naimark and A.I. Shtern, *Theory of Group Representations,* Grundlehren der Math. Wiss. **246**, Springer, Berlin, 1982

[SpSt] T.A. Springer and R. Steinberg, *Conjugacy classes in classical groups*, in *Seminar on Algebraic Groups and Related Finite Groups* (A. Borel, ed.), Lecture Notes in Math. **131**, Springer-Verlag, Berlin, 1970, pp. E82–E100.

[Te] D. Testerman, *A construction of certain maximal subgroups of the algebraic groups E_6 and F_4*, J. Algebra **122** (1989), 299–322.