Splitting fields for Jordan subgroups

Citation for published version (APA):

Cohen, A. M., & Tiep, P. H. (1997). Splitting fields for Jordan subgroups. In M. Cabanes (Ed.), *Proceedings of Finite Reductive Groups, Related structures and Representations* (pp. 165-183). Birkhäuser Verlag.

Document status and date:

Published: 01/01/1997

Document Version:

Publisher's PDF, also known as Version of Record (includes final page, issue and volume numbers)

Please check the document version of this publication:

- A submitted manuscript is the version of the article upon submission and before peer-review. There can be important differences between the submitted version and the official published version of record. People interested in the research are advised to contact the author for the final version of the publication, or visit the DOI to the publisher's website.
- The final author version and the galley proof are versions of the publication after peer review.
- The final published version features the final layout of the paper including the volume, issue and page numbers.

[Link to publication](#)

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal.

If the publication is distributed under the terms of Article 25fa of the Dutch Copyright Act, indicated by the "Taverne" license above, please follow below link for the End User Agreement:

www.tue.nl/taverne

Take down policy

If you believe that this document breaches copyright please contact us at:

openaccess@tue.nl

providing details and we will investigate your claim.

Splitting Fields for Jordan Subgroups

Arjeh M. Cohen and Pham Huu Tiep*

Abstract

Let J be a Jordan subgroup of a simple complex adjoint Lie group $\mathcal{G}$. Then $N = N_{\mathcal{G}}(J)$ is a Lie primitive subgroup of $\mathcal{G}$. In this paper, the minimal field k for which there exists a k -form of $\mathcal{G}$ containing N is determined.

1. Introduction

Let $\mathcal{G}$ be a simple complex Lie group. An elementary abelian finite subgroup J of $\mathcal{G}$ is said to be a *Jordan subgroup* if the following conditions hold:

- (i) $N = N_{\mathcal{G}}(J)$ is a finite group;
- (ii) J is a minimal normal subgroup of N ;
- (iii) if J' is another finite subgroup of $\mathcal{G}$ with properties (i), (ii) and such that $J \subseteq J'$, $N \subseteq N_{\mathcal{G}}(J')$, then $N = N_{\mathcal{G}}(J')$.

This notion was introduced by A. V. Alekseevskii, who classified all Jordan subgroups of simple complex Lie groups in [Ale]. For the reader's convenience we reproduce this nice result in Table 1.

The interrelation between Jordan subgroups of Lie groups $\mathcal{G}$ and the so-called *orthogonal decompositions* of corresponding Lie algebras $\mathcal{L}$ has been investigated in detail by A. V. Borovik, V. P. Burichenko, A. I. Kostrikin and P. H. Tiep; for more about this, see [KoT].

The definition of Jordan subgroups can be carried over to algebraic groups over fields of characteristic $p > 0$ without any change. As shown by Borovik [Bor 1], the classification of Jordan subgroups then remains unaltered, except for the natural restriction $\exp(J) \neq p$. Thus, the group J together with its normalizer N embeds in finite groups $\mathcal{G}_q$ of Lie type corresponding to $\mathcal{G}$ (under some conditions regarding the fields of definition $\mathbb{F}_q$). Furthermore, if we take the definition field $\mathbb{F}_q$ to be minimal with respect to containing J , then $N_{\mathcal{G}_q}(J)$ usually turns out to be a local maximal subgroup of $\mathcal{G}_q$ (see [CLSS]).

*Supported by the Alexander von Humboldt Foundation.

As can be seen from [Asch], [Bor 2], and [CLSS], Jordan subgroups play a role in the classification of

- finite Lie primitive subgroups of complex Lie groups (here Lie primitive means that the subgroup is maximal among all proper closed Lie subgroups);
- (local) maximal subgroups of groups of Lie type, algebraic or finite.

Namely, the normalizers of Jordan subgroups represent a subclass of the class of maximal (closed) finite subgroups with abelian socle. The two other classes are those with non-abelian simple socle and with the socle equal to $A_5 \times A_6$ (in the latter case, the group must be of type E_8 , see [Bor 2]).

Table 1. Jordan subgroups of simple complex Lie groups

$\mathcal{G}$	J	$C_{\mathcal{G}}(J)/J$	$N_{\mathcal{G}}(J)/C_{\mathcal{G}}(J)$	cf. §
A_{p^n-1} , p a prime	$\mathbb{Z}_p^{2n}$	1	$Sp_{2n}(p)$	2.1, 3
B_n , $n \geq 3$	$\mathbb{Z}_2^{2n}$	1	S_{2n+1}	2.3
C_{2^n-1} , $n \geq 2$	$\mathbb{Z}_2^{2n}$	1	$O_{2n}^-(2)$	2.2
D_{2^n-1} , $n \geq 3$	$\mathbb{Z}_2^{2n}$	1	$O_{2n}^+(2)$	2.2
D_{n+1} , $n \geq 4$	$\mathbb{Z}_2^{2n}$	1	S_{2n+2}	2.3
G_2	$\mathbb{Z}_3^3$	1	$SL_3(2)$	2.4
F_4	$\mathbb{Z}_3^3$	1	$SL_3(3)$	4
E_6	$\mathbb{Z}_3^3$	$\mathbb{Z}_3^3$	$SL_3(3)$	4
E_8	$\mathbb{Z}_5^3$	1	$SL_3(5)$	4
E_8	$\mathbb{Z}_2^5$	$\mathbb{Z}_2^{10}$	$SL_5(2)$	2.5
$D_4 \cdot \mathbb{Z}_3$ ($\mathcal{G}$ is not simple)	$\mathbb{Z}_2^3$	$\mathbb{Z}_2^6 \cdot \mathbb{Z}_3$	$SL_3(2)$	2.4

The aforementioned activity on classifying maximal finite subgroups of complex Lie groups is now believed to be nearly complete, due to work of A. M. Cohen, R. L. Griess Jr., P. B. Kleidmann, A. J. E. Ryba, J.-P. Serre, D. B. Wales, R. A. Wilson and others (cf. [CoW2]). One of the open questions left is to determine the *minimal splitting field* for a given maximal finite subgroup G of $\mathcal{G}$. We shall be concerned with the situation where $\mathcal{G}$ is interpreted as the automorphism group $\text{Aut}(\mathcal{L})$ of a given complex simple Lie algebra $\mathcal{L}$. Often the subgroup $\text{Inn}(\mathcal{L})$ of $\text{Aut}(\mathcal{L})$ consisting of all inner automorphisms of $\mathcal{L}$ will suffice for defining J .

Definitions. Given a complex algebraic group $\mathcal{G}$ containing G , a $\mathbb{K}$ -form of $\mathcal{G}$ for G is a $\mathbb{K}$ -form $\mathcal{G}_{\mathbb{K}}$ of $\mathcal{G}$ such that G is contained in $\mathcal{G}_{\mathbb{K}}(\mathbb{K})$, the group of $\mathbb{K}$ -rational points of $\mathcal{G}_{\mathbb{K}}$.

Let $\mathcal{L}$ be a complex simple Lie algebra, $\mathcal{G} = \text{Aut}(\mathcal{L})$, and G a finite subgroup of $\mathcal{G}$. A subfield $\mathbb{K}$ of $\mathbb{C}$ is said to be a *splitting field* for G in $\mathcal{L}$, if there exists a $\mathbb{K}$ -subspace V of $\mathcal{L}$ (viewed as $\mathbb{K}$ -space) with the following properties:

- (i) V is invariant under G ;
- (ii) $V \otimes_{\mathbb{K}} \mathbb{C} = \mathcal{L}$; and
- (iii) V is closed under the Lie multiplication of $\mathcal{L}$.

The resulting Lie algebra V over $\mathbb{K}$ is called a $\mathbb{K}$ -form of $\mathcal{L}$ for G .

According to a result of T. A. Springer ([Spr]), there is a unique minimal (with respect to inclusion) splitting field $\mathbb{K}$ for each Lie primitive finite subgroup G of $\mathcal{G}$ (to be more precise: for each finite subgroup G whose centralizer in $\mathcal{G}$ is contained in $Z(\mathcal{G})$). The elegant proof of this result does not tell us what the minimal splitting field is, nor what the corresponding $\mathbb{K}$ -form $\mathcal{G}_{\mathbb{K}}$ is.

The different $\mathbb{K}$ -forms of $\mathcal{L}$ and those of $\mathcal{G}$ are in bijective correspondence; since $\text{Aut } \mathcal{G} \cong \mathcal{G}$ and the (pointed) first order Galois cohomology set $H^1(\text{Gal}(\overline{\mathbb{K}}, \mathbb{K}), \mathcal{G})$, where $\text{Gal}(\overline{\mathbb{K}}, \mathbb{K})$ denotes the Galois group of the algebraic closure $\overline{\mathbb{K}}$ of $\mathbb{K}$ over $\mathbb{K}$, describes the different $\mathbb{K}$ -forms of $\mathcal{L}$, cf. [Ser]. Therefore, we can study the $\mathbb{K}$ -forms of $\mathcal{L}$ to determine the minimal splitting field and the corresponding $\mathbb{K}$ -form of $\mathcal{G}$ for a given subgroup G .

For the various finite Lie primitive subgroups of $\mathcal{G}$ of type G_2 , the minimal splitting fields have been fully determined (see [CoW] and [CNP]). In this paper we determine them for all Jordan subgroups of simple complex Lie groups.

Theorem. *Let $\mathcal{L}$ be a complex simple Lie algebra, $\mathcal{G} = \text{Aut}(\mathcal{L})$, J a Jordan subgroup of $\mathcal{G}$, and let $p = \exp(J)$. Then $\mathbb{Q}(\cos(2\pi/p))$ is the unique minimal splitting field for $N_{\mathcal{G}}(J)$ in $\mathcal{G}$.*

2. The case $p = 2$

The aim of this section is to prove the theorem stated in the introduction for the case where $p = 2$. Thus, we establish that $\mathbb{Q}$ is a splitting field for the normalizer $N_{\mathcal{G}}(J)$ of any Jordan 2-subgroup J of $\mathcal{G} = \text{Aut}(\mathcal{L})$. We distinguish cases according to Alekseevskii's classification (see Table 1).

2.1 $\mathcal{L}$ is of type A_{2m-1} , $m \geq 1$. First we recall the construction of the Jordan subgroup J for the case where $\mathcal{L}$ is of type A_{p^m-1} with p

an arbitrary prime, cf. [KoT]. Let $q = p^m$, $W = \mathbb{F}_q^2$ viewed as a $2m$ -dimensional vector space over $\mathbb{F}_p$ with the symplectic form

$$(u, v) = \text{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(ad - bc)$$

for $u = (a, b)$, $v = (c, d)$, $a, b, c, d \in \mathbb{F}_q$. For such vectors u, v we also set $B(u, v) = \text{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(-bc)$. Put $\varepsilon = \exp(2\pi i/p)$ and write

$$D = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & \varepsilon & 0 & \dots & 0 \\ 0 & 0 & \varepsilon^2 & \dots & 0 \\ & & & \ddots & \\ 0 & 0 & 0 & \dots & \varepsilon^{p-1} \end{pmatrix}, \quad P = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ & & \ddots & & \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}.$$

Choosing a basis $\{e_1, \dots, e_m, f_1, \dots, f_m\}$ of W , one can set

$$J_u = D^{a_1} P^{b_1} \otimes \dots \otimes D^{a_m} P^{b_m}$$

for $u = \sum_{i=1}^m (a_i e_i + b_i f_i)$. It is shown in §1.1 of [KoT] that, for an appropriate choice of the basis $\{e_1, \dots, f_m\}$, one has

$$J_u \cdot J_v = \varepsilon^{B(u,v)} J_{u+v}. \quad (1)$$

Furthermore, the set $\{J_u \mid u \in W \setminus \{0\}\}$ forms a basis for the Lie algebra $\mathcal{L}$.

If $p > 2$, then the required Jordan subgroup $J \simeq \mathbb{Z}_p^{2m}$ has inverse image

$$\hat{J} = \{\varepsilon^a J_u \mid a \in \mathbb{F}_p, u \in W\} \simeq p_+^{1+2m}$$

in $\hat{\mathcal{G}}^0 = SL_q(\mathbb{C})$ (here and below, $\mathcal{G}^0 = \text{Inn}(\mathcal{L})$). Moreover, $C_{\mathcal{G}}(J) = J$ and $G = N_{\mathcal{G}}(J) \simeq J \cdot (Sp(W) \cdot \mathbb{Z}_2)$. The additional factor $\mathbb{Z}_2$ is generated by the outer automorphism $T : X \mapsto -^t X$ of $\mathcal{L}$.

Now we return to the case $p = 2$. For a fixed square root i of -1 and $a \in \mathbb{F}_2$ we set

$$i^a = \begin{cases} 1 & a = 0, \\ i & a = 1. \end{cases}$$

In particular, $i^a \cdot i^b = (-1)^{ab} i^{a+b}$. The Jordan subgroup $J \simeq \mathbb{Z}_2^{2m}$ has inverse image

$$\hat{J} = \{\pm i^{a_1+b_1} J_u \mid u = \sum_{j=1}^m (a_j e_j + b_j f_j) \in W\} \simeq 2_-^{1+2m}$$

in $\hat{\mathcal{G}}^0 = SL_q(\mathbb{C})$. Furthermore, $C_{\mathcal{G}}(J) = J \times \mathbb{Z}_2$ and $G = N_{\mathcal{G}}(J) \simeq (J \times \mathbb{Z}_2) \cdot Sp(W)$. Again, the additional factor $\mathbb{Z}_2$ is generated by the

outer automorphism $T : X \mapsto -^tX$ of $\mathcal{L}$. It is more convenient to work with the following basis of $\mathcal{L}$:

$$I_u = (-1)^{B(u,u)} i^{B(u,u)+1} J_u, \quad u \in W \setminus \{0\}.$$

In what follows we shall often write $W^\#$ instead of $W \setminus \{0\}$. It can be verified (see e.g. §1.3 of [KoT]) that each automorphism $g \in N$ of $\mathcal{L}$ acts rationally in the basis $\{I_u \mid u \in W^\#\}$, namely,

$$g(I_u) = (-1)^{h(u)} I_{\varphi(u)},$$

where the maps $h : W \rightarrow \mathbb{F}_2$ and $\varphi \in Sp(W)$ satisfy the condition

$$h(u+v) = h(u) + h(v) + C(u, v) + C(\varphi(u), \varphi(v)).$$

Here we are denoting, for $u, v \in W$,

$$C(u, v) = B(u, u)B(v, v) + B(v, u) + (u, v)(B(u, u) + B(v, v)).$$

The outer automorphism T also acts rationally in the basis $\{I_u \mid u \in W^\#\}$, namely, $T(I_u) = (-1)^{B(u,u)+1} I_u$.

For $x \in \text{End}(\mathcal{L})$ and $\mathcal{M}$ an x -invariant subspace of $\mathcal{L}$, we denote by $\text{Spec}(\mathcal{M}, x)$ the set of eigenvalues of x in its action on $\mathcal{M}$. Observe that, for any $u \in W$,

$$\text{Spec}(\mathcal{L}, I_u) \subseteq \mathbb{Q}i. \quad (2)$$

Furthermore, from (1) it follows that

$$[I_u, I_v] := I_u I_v - I_v I_u = \begin{cases} 0 & \text{if } (u, v) = 0, \\ 2(-1)^{D(u,v)+B(u,v)} I_{u+v} & \text{if } (u, v) = 1, \end{cases}$$

where

$$D(u, v) = B(u, u)B(v, v) + B(u+v, u+v) \cdot \{1 + B(u, u) + B(v, v)\} + 1.$$

Our computations show that the $\mathbb{Q}$ -subspace $\langle I_u \mid u \in W^\# \rangle_{\mathbb{Q}}$ is a $\mathbb{Q}$ -form for G . Consequently, $\mathbb{Q}$ is the unique minimal splitting field for G .

2.2 $\mathcal{L}$ is of type C_{2m-1} or D_{2m-1} , $m \geq 3$. Let $W, (\cdot, \cdot), I_u$ be as in §2.1. One can embed $\mathcal{L}$ in the Lie algebra $\hat{\mathcal{L}}$ of type A_{2m-1} ,

$$\hat{\mathcal{L}} = \langle I_u \mid u \in W^\# \rangle_{\mathbb{C}},$$

in such a way that

$$\mathcal{L} = \langle I_u \mid u \in W, q(u) = 1 \rangle_{\mathbb{C}}$$

(see §2.1 of [KoT]). Here q is a quadratic form on W associated with $(\cdot, \cdot)$, i.e.,

$$q(u) + q(v) + q(u+v) = (u, v)$$

for any $u, v \in W$. The corresponding Jordan subgroup J remains the same as in §2.1: $J \simeq \mathbb{Z}_2^{2m}$. Furthermore, q is of type $-$ if $\mathcal{L}$ is of type C_{2m-1} , and $+$ if $\mathcal{L}$ is of type D_{2m-1} . Finally,

$$N_{\text{Aut}(\mathcal{L})}(J) = N_{\text{Inn}(\mathcal{L})}(J) \cap \text{Aut}(\mathcal{L}) \simeq J \cdot O(q).$$

(Remark that if $\mathcal{L}$ is of type D_4 , then its triality outer automorphisms do not normalize the Jordan subgroup J of order 2^6 .) Therefore, the $\mathbb{Q}$ -subspace $\langle I_u \mid u \in W, q(u) = 1 \rangle_{\mathbb{Q}}$ is a $\mathbb{Q}$ -form, and $\mathbb{Q}$ is the unique minimal splitting field for $N_{\text{Aut}(\mathcal{L})}(J)$.

2.3 $\mathcal{L}$ is of type B_n ($n \geq 2$) or D_{n+1} ($n \geq 4$), and $J = \mathbb{Z}_2^{2n}$. Here we realize $\mathcal{L}$ as the Lie algebra of skew-symmetric matrices of order m , where $m = 2n + 1$ or $m = 2n + 2$ according as $\mathcal{L}$ is of type B_n or D_{n+1} . If $E_{ij} = (\delta_{i,k}\delta_{j,l})_{1 \leq k,l \leq m}$, $1 \leq i, j \leq m$, are the "standard matrix basis", and $E(i, j) = E_{ij} - E_{ji}$, then

$$\mathcal{L} = \langle E(i, j) \mid 1 \leq i, j \leq m \rangle_{\mathbb{C}}.$$

As shown in §2.2 of [KoT], each automorphism $g \in N_{\mathcal{G}}(J)$ acts rationally in the basis $\{E(i, j) \mid 1 \leq i < j \leq m\}$ of $\mathcal{L}$. Namely, there exist maps $f : \{1, 2, \dots, m\} \rightarrow \mathbb{F}_2$ and $\varphi \in \text{Sym}(\{1, 2, \dots, m\})$ such that

$$g(E(i, j)) = (-1)^{f(i)+f(j)} E(\varphi(i), \varphi(j)).$$

Furthermore,

$$[E(i, j), E(k, l)] = \begin{cases} 0 & \text{if } |\{i, j\} \cap \{k, l\}| = 0 \text{ or } 2, \\ E(i, l) & \text{if } i \neq j = k \neq l \neq i. \end{cases}$$

Hence the $\mathbb{Q}$ -subspace $\langle E(i, j) \mid 1 \leq i < j \leq m \rangle_{\mathbb{Q}}$ is a $\mathbb{Q}$ -form, and $\mathbb{Q}$ is the unique minimal splitting field for $N_{\mathcal{G}}(J)$ in $\mathcal{G}$.

2.4 $\mathcal{L}$ is of type G_2 or D_4 , and $J \simeq \mathbb{Z}_2^3$. If $\mathcal{L} = D_4$, one has to take $\mathcal{G}$ containing not only $\text{Inn}(\mathcal{L})$, but also a triality automorphism of $\mathcal{L}$. For more about the Jordan subgroup J and its normalizer in $\mathcal{G}$ see [Gri].

Recall (see §3.1 of [KoT]) that, if $J \simeq \mathbb{Z}_p^3$ is a Jordan subgroup of $\mathcal{G}$, a Lie group of type G_2 , D_4 , F_4 , E_6 or E_8 , one can associate to J the following orthogonal decomposition

$$\mathcal{L} = \oplus_{k=1}^{p^2+p+1} \mathcal{H}_k \quad (3)$$

of $\mathcal{L}$. Each component $\mathcal{H}_k$ is a Cartan subalgebra of $\mathcal{L}$ and coincides with the fixed point subalgebra

$$C_{\mathcal{L}}(J') = \{x \in \mathcal{L} \mid \forall g \in J', g(x) = x\}$$

for a unique maximal subgroup J' of J . If we again set $G = N_G(J)$, then one easily sees that G is just the group of all elements from $\mathcal{G}$ that preserve decomposition (3).

We shall need the following assertion:

Lemma 1. *Let p be a prime and $J \simeq \mathbb{Z}_p^3$ be a Jordan subgroup of the Lie group $\mathcal{G} = \text{Aut}(\mathcal{L})$ of type G_2 , D_4 , F_4 , E_6 or E_8 , respectively. Then, for any non-identity element g from J , the fixed point subalgebra*

$$C_{\mathcal{L}}(g) = \{x \in \mathcal{L} \mid g(x) = x\}$$

is a semisimple Lie algebra of type $2A_1$, $4A_1$, $2A_2$, $3A_2$ or $2A_4$, respectively.

Proof. For E_8 , the element g must have class 5A in the notation of [CoG], and so the result can be read off from the table 4 in [CoG]. Although a similar proof can be given for the other cases, we shall give a less case dependent proof here.

Set $\mathcal{C} = C_{\mathcal{L}}(g)$. From the definition of $\mathcal{C}$ one can show that the kernel of the Killing form $\kappa_{\mathcal{C}}$ corresponding to $\mathcal{C}$ is contained in the kernel of the Killing form κ associated with $\mathcal{L}$. But κ is non-degenerate, so $\kappa_{\mathcal{C}}$ is also non-degenerate. This means that $\mathcal{C}$ is a semisimple Lie algebra. Considering decomposition (3) corresponding to J one sees that $\mathcal{C}$ contains at least one component $\mathcal{H}_k$ of (3), which is a Cartan subalgebra of $\mathcal{L}$. Because $\mathcal{H}_k$ is also a Cartan subalgebra of $\mathcal{C}$, the ranks of $\mathcal{C}$ and $\mathcal{L}$ coincide. Furthermore, standard computations with the characters of J show that the dimension of $\mathcal{C}$ is equal to

$$(p+1) \cdot \text{rank}(\mathcal{L}) = \frac{p+1}{p^2+p+1} \dim(\mathcal{L}).$$

Finally, the simple components of the Lie algebra $\mathcal{C}$ are isomorphic to each other, since $\mathcal{C}$ is acted on irreducibly by $N_G(\langle g \rangle)$. These data regarding $\mathcal{C}$ suffice to determine its type. $\square$

Now we suppose that $J \simeq \mathbb{Z}_2^3$ and $\mathcal{L}$ is of type G_2 or D_4 . Note that, if $\mathcal{L}$ is of type D_4 , some triality automorphism of $\mathcal{L}$ centralizes the Jordan subgroup J of order 2^3 (compare with §2.2). We show that $\mathcal{Q}$ is the unique

minimal splitting field for G . Observation (2) suggests considering the $\mathbb{Q}$ -subspace $V = \bigoplus_{k=1}^7 V_k$ of $\mathcal{L}$, where

$$V_k = \{x \in \mathcal{H}_k \mid \text{Spec}(\mathcal{L}, \text{ad } x) \subseteq \mathbb{Q}i\}.$$

The fact that V is a G -invariant $\mathbb{Q}$ -subspace follows from the following simple observation:

Lemma 2. *Let $\mathcal{L}$ be a semisimple Lie algebra over $\mathbb{C}$ with Cartan subalgebra $\mathcal{H}$. If $\mathbb{K}$ is a subfield of $\mathbb{C}$ and $\lambda \in \mathbb{C}$, $\lambda \neq 0$, then the set*

$$U = \{x \in \mathcal{H} \mid \text{Spec}(\mathcal{L}, \text{ad } x) \subseteq \lambda\mathbb{K}\}$$

is an $N_{\text{Aut}(\mathcal{L})}(\mathcal{H})$ -invariant $\mathbb{K}$ -subspace of dimension equal to $\dim \mathcal{H}$.

Proof. The commutativity of $\mathcal{H}$ implies that U is a $\mathbb{K}$ -subspace. Let R denote the root system corresponding to $\mathcal{H}$. Then, for $x \in \mathcal{H}$,

$$x \in U \iff \forall \alpha \in R \quad \alpha(x) \in \lambda\mathbb{K}. \quad (4)$$

This equivalence shows that U is invariant under $N_{\text{Aut}(\mathcal{L})}(\mathcal{H})$. But R spans a $\mathbb{Q}$ -space of dimension $\dim \mathcal{H}$ in $\mathcal{H}^*$. So $\dim U = \dim \mathcal{H}$. $\square$

It remains to check that V is multiplicatively closed: $[V, V] \subseteq V$, or equivalently, $[V_k, V_l] \subseteq V$ for all k, l . If $k = l$, then $[V_k, V_l] = 0$. Suppose that $k \neq l$. Then there exists a non-identity element $g \in J$ such that $\mathcal{H}_k$ and $\mathcal{H}_l$ both are contained in the subalgebra $\mathcal{C} = C_{\mathcal{L}}(g)$. By Lemma 1, $\mathcal{C}$ is a semisimple Lie algebra of type rA_1 , where $r = 2$ or $r = 4$. One has a decomposition of $\mathcal{C}$ into a sum of simple components $\mathcal{C} = \sum_{s=1}^r \mathcal{C}^s$, each of them being a Lie algebra of type A_1 invariant under J . On the other hand, $\mathcal{C}$ is a sum of three Cartan subalgebras, namely $\mathcal{H}_k$, $\mathcal{H}_l$ and some other $\mathcal{H}_m$. Without loss of generality we suppose $k = 1$, $l = 2$, $m = 3$. Because of (3), we also get an orthogonal decomposition

$$\mathcal{C}^s = \bigoplus_{t=1}^3 \mathcal{H}_t^s$$

for each $\mathcal{C}^s$, $s = 1, \dots, r$. Moreover, $\mathcal{H}_t = \bigoplus_{s=1}^r \mathcal{H}_t^s$, $t = 1, 2, 3$. Now we set

$$V_t^s = \{x \in \mathcal{H}_t^s \mid \text{Spec}(\mathcal{C}^s, \text{ad } x) \subseteq \mathbb{Q}i\}.$$

The root systems corresponding to $\mathcal{H}_t^s$, $s = 1, \dots, r$, together span the same $\mathbb{Q}$ -space as the root system corresponding to $\mathcal{H}_t$. This remark and (4) show that

$$V_t = \bigoplus_{s=1}^r V_t^s.$$

By §2.1, $\oplus_{t=1}^3 V_t^s$ is a $\mathbb{Q}$ -form. In particular, $[V_t^s, V_{t'}^s] \subseteq V$. Furthermore, it is obvious that $[V_t^s, V_{t'}^{s'}] = 0$ whenever $s \neq s'$. Now we have

$$[V_1, V_2] = [\oplus_{s=1}^r V_1^s, \oplus_{s'=1}^r V_2^{s'}] \subseteq \sum_{s,s'=1}^r [V_1^s, V_2^{s'}] \subseteq V,$$

as required.

2.5 $\mathcal{L}$ is of type E_8 and $J \simeq \mathbb{Z}_2^5$. The fact that $\mathbb{Q}$ is the unique minimal splitting field for $N_G(J)$ has been established by J. G. Thompson [Tho]. Another way to see it is to follow the scheme of arguments of §2.4 by

- considering the orthogonal decomposition $\mathcal{L} = \oplus_{k=1}^{31} \mathcal{H}_k$ corresponding to J , and
- the $\mathbb{Q}$ -space $V = \oplus_{k=1}^{31} V_k$, $V_k = \{x \in \mathcal{H}_k \mid \text{Spec}(\mathcal{L}, \text{ad } x) \subseteq \mathbb{Q}i\}$; then observing that
- the sum of each pair of Cartan subalgebras $\mathcal{H}_k, \mathcal{H}_l$ is contained in the Lie algebra $C_{\mathcal{L}}(g)$ of type D_8 , $1 \neq g \in J$ (in the Lie algebra $C_{\mathcal{L}}(g, g', g'')$ of type $8A_1$, $1 \neq g, g', g'' \in J$, if you like the Lie algebra A_1 more!), and that
- $\mathbb{Q}$ is the unique minimal splitting field for D_8 by §2.2 (for $8A_1$ by §2.1).

3. The case A_{p^m-1} for p odd

Here we are concerned with the Jordan subgroup $J \simeq \mathbb{Z}_p^{2m}$ of $\mathcal{G} = \text{Aut}(\mathcal{L})$ of the Lie algebra $\mathcal{L} = sl_q(\mathbb{C})$, $q = p^m$, p an odd prime. We also use the notation of the beginning of §2.1. The normalizer $G = N_G(J) \simeq J \cdot (Sp(W) \cdot \mathbb{Z}_2)$ is in fact split; namely, one can identify J with the subgroup $\{\hat{w} \in \text{Aut}(\mathcal{L}) \mid w \in W\}$, where

$$\hat{w}(J_u) = \varepsilon^{(w,u)} J_u, \quad u, w \in W,$$

and

$$Sp(W) \cdot \mathbb{Z}_2 =$$

$$\{\varphi \in GL(W) \mid \exists \mu_\varphi = \pm 1, \forall u, v \in W, (\varphi(u), \varphi(v)) = \mu_\varphi(u, v)\}$$

with the subgroup $\{\hat{\varphi} \in \text{Aut}(\mathcal{L}) \mid \varphi \in Sp(W) \cdot \mathbb{Z}_2\}$, where

$$\hat{\varphi}(J_u) = \mu_\varphi \varepsilon^{\{B(\varphi(u), \varphi(u)) - B(u, u)\}/2} J_{\varphi(u)}.$$

First we replace the basis $\{J_u\}$ by $\{I_u \mid u \in W^\#\}$ with $I_u = \varepsilon^{B(u,u)/2} J_u$. Then, in view of (1), one has:

$$I_u \cdot I_v = \varepsilon^{(u,v)/2} I_{u+v}, \quad \hat{w}(I_u) = \varepsilon^{(w,u)} I_u, \quad \hat{\varphi}(I_u) = \mu_\varphi I_{\varphi(u)}. \quad (5)$$

Taking $\vartheta = \varepsilon - \varepsilon^{-1} = 2i \sin(2\pi/p)$, we set, for $u \in W$,

$$K_u = \vartheta \sum_{v \in W^\#} \varepsilon^{(u,v)} I_v.$$

Since $\sum_{u \in W} \varepsilon^{(u,v)} = \delta_{v,0} q^2$, we find $\sum_{u \in W} K_u = 0$. Furthermore, for $w \in W$,

$$\hat{w}K_u = \vartheta \sum_{v \in W^\#} \varepsilon^{(w+u,v)} I_v = K_{w+u},$$

and, for $\varphi \in Sp(W) \cdot \mathbb{Z}_2$,

$$\begin{aligned} \hat{\varphi}(K_u) &= \mu_\varphi \vartheta \sum_{v \in W^\#} \varepsilon^{(u,v)} I_{\varphi(v)} = \mu_\varphi \vartheta \sum_{v \in W^\#} \varepsilon^{(\mu_\varphi \varphi(u), \varphi(v))} I_{\varphi(v)} \\ &= \mu_\varphi K_{\mu_\varphi \varphi(u)}. \end{aligned} \quad (6)$$

Finally, for $u, v \in W$ we have:

$$K_u \cdot K_v = \vartheta^2 \left(-I_0 + q^2 \varepsilon^{2(v,u)} I_{2(u-v)} \right) - \vartheta (K_u + K_v),$$

from which we obtain,

$$[K_u, K_v] = \sum_{x \in W^\#} A_{u,v}(x) K_x,$$

where

$$A_{u,v}(x) = \vartheta (\varepsilon^{2(v,u)+2(u-v,x)} - \varepsilon^{2(u,v)+2(v-u,x)} - \varepsilon^{2(v,u)} + \varepsilon^{2(u,v)}). \quad (7)$$

Indeed,

$$\begin{aligned} [K_u, K_v] &= q^2 \vartheta^2 \left(\varepsilon^{2(v,u)} I_{2(u-v)} - \varepsilon^{2(u,v)} I_{2(v-u)} \right) \\ &= \vartheta \left(\varepsilon^{2(v,u)} \sum_{x \in W} \varepsilon^{(2(u-v),x)} K_x - \varepsilon^{2(u,v)} \sum_{x \in W} \varepsilon^{(2(v-u),x)} K_x \right) \\ &= \sum_{x \in W^\#} A_{u,v}(x) K_x. \end{aligned}$$

As $A_{u,v}(x) \in \mathbb{Q}(\varepsilon)$ and $\overline{A_{u,v}(x)} = A_{u,v}(x)$, we obtain that $A_{u,v}(x)$ belongs to the field $\mathbb{K}_0 = \mathbb{Q}(\cos(2\pi/p)) = \mathbb{Q}(\varepsilon) \cap \mathbb{R}$. We have shown that $\mathbb{K}_0$ is a splitting field for G .

We can actually show that $\mathbb{K}_0$ is the minimal splitting field for any subgroup H of G with the property: $J \triangleleft H$ and H/J is a subgroup of $Sp(W) \cdot \mathbb{Z}_2$ acting transitively on $W^\#$. (Note that this condition on H is equivalent to saying that H is a subgroup of G containing J which is irreducible on $\mathcal{L}$.)

In order to prove this assertion, consider any such subgroup H and suppose that V is a $\mathbb{K}$ -form for H , where $\mathbb{K}$ is a subfield of $\mathbb{K}_0$. As G splits over J , the subgroup H splits over J and one may suppose that $H = J \cdot S$ for some subgroup S of $Sp(W) \cdot \mathbb{Z}_2$. Denote by χ the character of H afforded by $\mathcal{L}$. From (6) it follows that S leaves the pair $\pm K_0$ fixed. Hence

$$1 \leq (\chi_S, \mu)_S = (\chi, \mu_S^H)_H.$$

Here μ stands for the character $\varphi \mapsto \mu_\varphi$. But $\deg \mu_S^H = q^2 = \deg \chi + 1$, so $(\chi_S, \mu)_S = 1$. In other words, the subspace

$$\mathcal{L}_1 = \{x \in \mathcal{L} \mid \forall s \in S, s(x) = \mu(s)x\}$$

is spanned by the vector K_0 . We shall need the following simple statement:

Lemma 3. *Let $\mathbb{K} \subseteq \mathbb{L}$ be fields of characteristic 0, G a finite group, V a $\mathbb{K}G$ -module of finite rank. Assume that $V^\mathbb{L} = V \otimes_\mathbb{K} \mathbb{L}$ has a composition factor U which is realizable over $\mathbb{K}$. Then V has a direct summand, which is isomorphic to U .*

Proof. Any G -module over $\mathbb{K}$ and $\mathbb{L}$ is completely reducible. So $V = V_1 \oplus \cdots \oplus V_n$ for some simple $\mathbb{K}G$ -modules $V_1, \dots, V_n$. Furthermore, $V_i^\mathbb{L} = W_{i1} \oplus \cdots \oplus W_{it_i}$ for some simple $\mathbb{L}G$ -modules W_{ij} , $1 \leq i \leq n$, $1 \leq j \leq t_i$. One may suppose that $W_{11} \simeq U^\mathbb{L}$ and U is a $\mathbb{K}G$ -module. We come to the situation in which V_1 and U are simple $\mathbb{K}G$ -modules and $V_1^\mathbb{L}$ and $U^\mathbb{L}$ have a common composition factor (namely W_{11}). By Corollary 9.7 [Isa], $V_1 \simeq U$. $\square$

By Lemma 3, the $\mathbb{K}S$ -module V has a direct summand, which affords the character μ . But $\dim \mathcal{L}_1 = 1$, so this summand is spanned over $\mathbb{K}$ by λK_0 for some $\lambda \in \mathbb{C}^*$. This means that V contains λK_0 . Hence V contains $\hat{u}(\lambda K_0) = \lambda K_u$ for any $u \in W$. Since the elements K_u , $u \in W^\#$, are linearly independent over $\mathbb{C}$, one has $V = \langle \lambda K_u \mid u \in W^\# \rangle_\mathbb{K}$. Furthermore, $[V, V] \subseteq V$ and $[\lambda K_u, \lambda K_v] = \sum_{x \in W^\#} \lambda A_{u,v}(x) \cdot \lambda K_x$, where $A_{u,v}(x)$ is defined in (7). Consequently, $\mathbb{K}$ contains all the coefficients $\lambda A_{u,v}(x)$, $u, v, x \in W^\#$. In particular,

$$\mathbb{K} \ni \lambda A_{u,-u}(x) = \lambda \vartheta(\varepsilon^{4(u,x)} - \varepsilon^{-4(u,x)})$$

for all $u, x \neq 0$. Choosing u such that $(u, x) = 1/4$ and $(u, x) = 1/2$, respectively, one finds $\lambda\vartheta(\varepsilon - \varepsilon^{-1}), \lambda\vartheta(\varepsilon^2 - \varepsilon^{-2}) \in \mathbb{K}$. We arrive at the conclusion that $\mathbb{K}$ contains

$$\frac{\lambda\vartheta(\varepsilon^2 - \varepsilon^{-2})}{\lambda\vartheta(\varepsilon - \varepsilon^{-1})} = \varepsilon + \varepsilon^{-1},$$

i.e., $\mathbb{K}$ contains $\mathbb{K}_0$, as claimed.

All the above computations are done with respect to a specific embedding of the finite group $G = \mathbb{Z}_p^{2m} \cdot (Sp_{2m}(p) \cdot \mathbb{Z}_2)$ in $PSL_p(\mathbb{C}) \cdot \mathbb{Z}_2$. However, in case $m = 1$ the following statement holds:

Proposition 4. *Let p be an odd prime and assume that $G = \mathbb{Z}_p^2 \cdot SL_2(p)$ has a faithful action on a complex Lie algebra $\mathcal{L}$ of dimension $p^2 - 1$ with nontrivial multiplication. Then $\mathcal{L}$ is a simple Lie algebra of type A_{p-1} and $\mathbb{K}_0 = \mathbb{Q}(\cos(2\pi/p))$ is the unique minimal splitting field for G .*

Proof. 1) First we show that $\mathcal{L} \simeq A_{p-1}$. From the faithfulness of the action of G on $\mathcal{L}$ and the equation $\dim \mathcal{L} = p^2 - 1$ it follows that this action is absolutely irreducible. But $0 \neq [\mathcal{L}, \mathcal{L}]$ is a G -submodule of $\mathcal{L}$, so $[\mathcal{L}, \mathcal{L}] = \mathcal{L}$. In particular, the Killing form κ of $\mathcal{L}$ is nonzero. As the kernel of κ is also a G -submodule of $\mathcal{L}$, the form κ is in fact non-degenerate. Hence, $\mathcal{L}$ is semisimple. Decompose $\mathcal{L}$ into a sum of simple components: $\mathcal{L} = \mathcal{L}_1 \oplus \cdots \oplus \mathcal{L}_m$. As the action of G on $\mathcal{L}$ is irreducible, G permutes the m components $\mathcal{L}_i$ transitively. Observe that $\dim \mathcal{L}_i \geq 3$, so $m \leq (p^2 - 1)/3$. In particular, the subgroup $J \simeq \mathbb{Z}_p^2$ of G leaves each component $\mathcal{L}_i$ fixed.

If $p = 3$, then obviously $\mathcal{L} \simeq A_2$. Assume that $p \geq 5$. Observe then that the simple Lie algebra $\mathcal{L}_i$ admits no outer automorphisms of order p . Hence J consists of only inner automorphisms of $\mathcal{L}$. In particular, for a fixed element $x \in J \setminus \{1\}$ the fixed point subalgebra $C_{\mathcal{L}}(x)$ contains a Cartan subalgebra $\mathcal{H}$ of $\mathcal{L}$. Note that J acts fixed-point-freely on $\mathcal{L}$. Thus, if we choose $y \in J$ such that $J = \langle x, y \rangle$, then y acts fixed-point-freely on $C_{\mathcal{L}}(x)$. This implies that the Lie algebra $C_{\mathcal{L}}(x)$ is nilpotent. Therefore $C_{\mathcal{L}}(x) = \mathcal{H}$ and $\text{rank}(\mathcal{L}) = \dim C_{\mathcal{L}}(x) = p - 1$. As a consequence, we get $m = \text{rank}(\mathcal{L})/\text{rank}(\mathcal{L}_i) \leq p - 1$. If $m \geq 2$, then $G/J \simeq SL_2(p)$ has no subgroups of index m , a contradiction. So $m = 1$, $\mathcal{L}$ is a simple Lie algebra of rank $p - 1$ and dimension $p^2 - 1$. In other words, $\mathcal{L} \simeq A_{p-1}$.

2) Denote by χ the G -character afforded by $\mathcal{L}$. Then $\chi(x) = -1$ for all $x \in J$. It is shown in Proposition 4.3.10 of [KoT] that there exists a unique subgroup $J \subset \mathcal{G} = \text{Inn}(\mathcal{L}) \simeq PSL_p(\mathbb{C})$ acting on $\mathcal{L}$ with such a character. Furthermore, due to [Sah], we have $H^1(SL_2(p), W) = 0$,

where $W = \mathbb{F}_p^2$ denotes the natural module for $SL_2(p)$. Therefore, one can choose a basis $\{I_u \mid u \in W^\# \}$ and define a G -invariant Lie structure $\{X, Y\} = X \cdot Y - Y \cdot X$ such that (5) holds. Here $(\cdot, \cdot)$ is some non-degenerate symplectic structure on W , and we identify J with $\{\hat{w} \mid w \in W\}$ and $SL_2(p)$ with $\{\hat{\varphi} \mid \varphi \in Sp(W)\}$. In particular, with respect to $\{\cdot, \cdot\}$, the group G has $\mathbb{K}_0$ as the unique minimal splitting field, as we have shown above. We would like to show that the initial Lie bracket $[\cdot, \cdot]$ on $\mathcal{L}$ is defined in the same way as $\{\cdot, \cdot\}$, and so $\mathbb{K}_0$ is also the unique minimal splitting field for G under the Lie multiplication $[\cdot, \cdot]$ (but the multiplications $[\cdot, \cdot]$ and $\{\cdot, \cdot\}$ need not coincide).

We shall reconstruct the initial Lie structure $[\cdot, \cdot]$ using the basis $\{I_u \mid u \in W^\# \}$. Since G consists of only inner automorphisms of $\mathcal{L}$, $[X, Y] = X \cdot Y - Y \cdot X$ for some G -invariant associative structure $X \cdot Y$ on $\mathcal{L} \oplus \langle E \rangle$ with

$$E \cdot X = X \cdot E = X, \quad \text{and} \quad \forall g \in G \quad g(E) = E.$$

Recall that the action of G on $\{I_u\}$ is given by (5). Our goal is to show that there exists a non-degenerate symplectic structure $(\cdot | \cdot)$ on W and a rescaling of the matrices I_u such that, for all $u, v \in W$,

$$I_u \cdot I_v = \varepsilon^{(u|v)/2} I_{u+v}.$$

From (5) it follows that

$$\hat{w}(I_u \cdot I_v) = \hat{w}(I_u) \cdot \hat{w}(I_v) = \varepsilon^{(w, u+v)} I_u \cdot I_v$$

for any $w \in W$, so $I_u \cdot I_v = \alpha_{u,v} I_{u+v}$ for some $\alpha_{u,v} \in \mathbb{C}$. Similarly,

$$\hat{w}((I_u)^p) = (\hat{w}(I_u))^p = (I_u)^p,$$

hence $(I_u)^p = \beta_u E$ for some $\beta_u \in \mathbb{C}$. But for any $\varphi \in SL_2(p)$ we have

$$\beta_{\varphi(u)} E = (I_{\varphi(u)})^p = (\hat{\varphi}(I_u))^p = \hat{\varphi}((I_u)^p) = \beta_u E,$$

therefore $\beta_u = \beta$ for all $u \in W^\#$. Suppose that $\beta = 0$. Then I_u is an ad-nilpotent element in $\mathcal{L}$. On the other hand, if we choose $x \in W^\#$ such that $(u, x) = 0$, then I_u belongs to the Cartan subalgebra $C_{\mathcal{L}}(\hat{x})$, a contradiction. So $\beta \neq 0$. Replacing I_u by $\beta^{-1/p} I_u$, one gets $(I_u)^p = E$ for any $u \in W$.

Now we may suppose that $I_{ku} = \alpha_k (I_u)^k$ for $1 \leq k \leq p$ and $\alpha_k \in \mathbb{C}^*$, $\alpha_1 = \alpha_p = 1$. Here, the coefficients α_k are the same for all $u \in W^\#$, as $SL_2(p)$ acts transitively on the set $\{I_u \mid u \in W^\# \}$. Furthermore,

$$I_{ku} \cdot I_{lu} = \alpha_k \alpha_l (I_u)^{k+l} = \alpha_k \alpha_l \alpha_{k+l}^{-1} I_{(k+l)u}.$$

Applying the automorphism $\hat{\varphi}$ with $\varphi = \begin{pmatrix} s & 0 \\ 0 & s^{-1} \end{pmatrix}$, $\varphi(u) = su$, $s \in \mathbb{F}_p^*$, one gets

$$\alpha_{ks}\alpha_{ls}\alpha_{ks+ls}^{-1} = \alpha_k\alpha_l\alpha_{k+l}^{-1}. \quad (8)$$

Setting $l = 1$ in (8) we have $\alpha_k/\alpha_{k+1} = \alpha_s\alpha_{ks}/\alpha_{(k+1)s}$. Hence

$$1 = \alpha_1/\alpha_p = \prod_{k=1}^{p-1} \frac{\alpha_k}{\alpha_{k+1}} = \alpha_s^{p-1} \prod_{k=1}^{p-1} \frac{\alpha_{ks}}{\alpha_{(k+1)s}} = (\alpha_s)^p,$$

i.e., $(\alpha_s)^p = 1$ for any $s \in \mathbb{F}_p$. Replacing each I_u by $\alpha_2 I_u$, we still have $(I_u)^p = E$, but the collection $\alpha_1, \alpha_2, \dots, \alpha_p$ will possess the property $\alpha_1 = \alpha_2 = \alpha_p = 1$. Now taking $k = l = 1$ in (8) we obtain $\alpha_{2s} = \alpha_s^2$. Finally, with setting $l = 1$ and $s = 2$ in (8) we get

$$\alpha_k/\alpha_{k+1} = \alpha_{2k}/\alpha_{2k+2} = (\alpha_k/\alpha_{k+1})^2,$$

that is, $\alpha_k = \alpha_{k+1}$. This means that $\alpha_k = 1$ and so $(I_u)^k = I_{ku}$ for all k .

Next we choose $u, v \in W$ such that $W = \langle u, v \rangle$ and write down $I_{ku} \cdot I_v = \gamma_k I_{ku+v}$ for $k = 1, 2, \dots, p$, $\gamma_k \in \mathbb{C}$, $\gamma_p = 1$. Then

$$\gamma_{k+1} I_{(k+1)u+v} = I_{(k+1)u} \cdot I_v = (I_{ku} \cdot I_u) \cdot I_v = \gamma_1 I_{ku} \cdot I_{u+v}.$$

On the other hand, applying $\hat{\varphi}$ with $\varphi : u \mapsto u, v \mapsto u + v$ to the identity $I_{ku} \cdot I_v = \gamma_k I_{ku+v}$, one finds $I_{ku} \cdot I_{u+v} = \gamma_k I_{(k+1)u+v}$. Therefore, $\gamma_{k+1} = \gamma_k \gamma_1$, $\gamma_k = \gamma_1^k$ and $\gamma_1^p = 1$. If $\gamma_1 = 1$, then $\gamma_k = 1$ for all k , and so $I_x \cdot I_y = I_{x+y}$ for any $x, y \in W$. The last identity means that the Lie multiplication on $\mathcal{L}$ is trivial, a contradiction. Hence, $\gamma_1 \neq 1$. In this case one can define an $SL_2(p)$ -invariant symplectic form $(\cdot | \cdot)$ on W such that $C_1 = \varepsilon^{(u|v)/2}$. Then for any k one has $I_{ku} \cdot I_v = \varepsilon^{(ku|v)/2} I_{ku+v}$. From this it is not difficult to derive that $I_x \cdot I_y = \varepsilon^{(x|y)/2} I_{x+y}$, as required. This settles Proposition 4. $\square$

Remark. The proof of Proposition 4 shows that the number of conjugacy classes of embeddings of $G = \mathbb{Z}_p^2 \cdot SL_2(p)$ in $\text{Inn}(\mathcal{L}) = PSL_p(\mathbb{C})$ is equal to the number of $SL_2(p)$ -invariant nontrivial symplectic structures on $W = \mathbb{F}_p^2$, i.e., equal to $p - 1$. (It is clear that the nontrivial symplectic forms on W are all scalar multiples of each other.) All these embeddings afford the same character, as G has a unique absolutely irreducible real character of degree $p^2 - 1$. Moreover, they are algebraically conjugate. Namely, let ε' be another p th primitive root of 1. Then one can use ε' instead of ε in the definition of the matrices D, P (cf. §2.1), and in the definition of the action of G (see the beginning of §3). In this way,

we arrive at the associative structure $I_u \bullet I_v = \varepsilon^{(u,v)/2} I_{u+v}$. Thus, these $p-1$ embeddings are in bijective correspondence with the elements of $\text{Gal}(\mathbb{Q}(\varepsilon)/\mathbb{Q})$. Remark also that there are $(p-1)/2$ $\text{Aut}(\mathcal{L})$ -conjugacy classes of embeddings of G in $\text{Aut}(\mathcal{L}) \simeq \text{PSL}_p(\mathbb{C}) \cdot \mathbb{Z}_2$. Indeed, the complex conjugation $\varepsilon \mapsto \varepsilon^{-1}$ leaves all the coefficients $A_{u,v}(x)$ (see (7)) fixed. Therefore, these $\text{Aut}(\mathcal{L})$ -conjugacy classes are in bijective correspondence with the elements of $\text{Gal}(\mathbb{K}_0/\mathbb{Q})$.

4. The case of exceptional types and p odd

To conclude the proof of our theorem, it remains to consider Jordan subgroups $J \simeq \mathbb{Z}_p^3$ of $\mathcal{G} = \text{Aut}(\mathcal{L})$, where $\mathcal{L}$ is of type F_4 , E_6 or E_8 , with $p = 3, 3, 5$ in the respective cases (cf. Table 1). Our arguments will follow the same scheme, so below we shall treat only the case $J \simeq \mathbb{Z}_5^3$, $\mathcal{L} = E_8$.

We shall write $\varepsilon = \exp(2\pi i/5)$, $\vartheta = \varepsilon - \varepsilon^{-1}$, $\mathbb{K}_0 = \mathbb{Q}(\varepsilon + \varepsilon^{-1}) = \mathbb{Q}(\sqrt{5})$. It is known that $G = N_{\mathcal{G}}(J)$ is a split extension of J by $SL_3(5)$. Following the proof of Proposition 4, one can establish

Lemma 5. *Assume that $G \simeq \mathbb{Z}_5^3 \cdot SL_3(5)$ is a subgroup of $\text{Aut}(\mathcal{L})$, where $\mathcal{L}$ is a complex Lie algebra $\mathcal{L}$ of dimension 248 with nonzero multiplication. If G has an absolutely irreducible action on $\mathcal{L}$, then $\mathcal{L}$ is a simple Lie algebra of type E_8 , $J = O_5(G)$ is a Jordan subgroup of $\mathcal{G} = \text{Inn}(\mathcal{L})$, and G coincides with $N_{\mathcal{G}}(J)$. $\square$*

Unlike the case of Proposition 4, here the group G has just two irreducible characters of degree 248, and both of them can be realized by embeddings of G in $\mathcal{G}$, see [Tiep]. Consider one of these embeddings and the orthogonal decomposition (3) corresponding to J . Fix a non-identity element $g \in J$. Then by Lemma 1 the fixed point subalgebra $\mathcal{C} = \mathcal{C}_{\mathcal{L}}(g)$ is a semisimple Lie algebra of type $2A_4$. So $\mathcal{C} = \mathcal{C}^1 \oplus \mathcal{C}^2$, where $\mathcal{C}^s$, $s = 1, 2$, are simple Lie algebras of type A_4 . On the other hand, by (3), $\mathcal{C}$ is a direct sum of six Cartan subalgebras of $\mathcal{L}$, say $\mathcal{H}_j$, $j = 1, \dots, 6$, of (3). The proof of the following assertion will be omitted:

Lemma 6. *The normalizer $N_G(\langle g \rangle)$ acts on $\mathcal{C}$ as a subgroup of type $(\mathbb{Z}_5^2 \times \mathbb{Z}_5^2) \cdot GL_2(5)$ of $\text{Aut}(\mathcal{C}) \simeq (\text{PSL}_5(\mathbb{C}) \cdot \mathbb{Z}_2) \wr \mathbb{Z}_2$. This action induces a subgroup $H \simeq \mathbb{Z}_5^2 \cdot SL_2(5)$ such that $\langle O_5(H), g \rangle = J$, and H acts faithfully and irreducibly on each component $\mathcal{C}^s$, $s = 1, 2$. In particular, $O_5(H)$ is a Jordan subgroup of $\mathcal{G}^s = \text{Inn}(\mathcal{C}^s)$, and H coincides with $N_{\mathcal{G}^s}(O_5(H))$. $\square$*

First we claim that $\mathbb{K}_0$ is a splitting field for G . For, consider the

$\mathbb{K}_0$ -subspace $V = \bigoplus_{j=1}^{31} V_j$ of $\mathcal{L}$, where

$$V_j = \{x \in \mathcal{H}_j \mid \text{Spec}(\mathcal{L}, \text{ad } x) \subseteq \vartheta \mathbb{K}_0\}.$$

Then V is G -invariant. It remains to check that V is multiplicatively closed: $[V, V] \subseteq V$, or equivalently, $[V_k, V_l] \subseteq V$ for all k, l . If $k = l$, then $[V_k, V_l] = 0$. Suppose that $k \neq l$. Without loss of generality, one can suppose that $k = 1$ and $l = 2$. Because of (3), we also have an orthogonal decomposition

$$\mathcal{C}^s = \bigoplus_{t=1}^6 \mathcal{H}_t^s$$

for each $\mathcal{C}^s$, $s = 1, 2$. This decomposition is nothing else but the orthogonal decomposition (3) corresponding to the Jordan subgroup $O_5(H)$ of $\mathcal{G}^s$. Moreover, $\mathcal{H}_t = \bigoplus_{s=1}^2 \mathcal{H}_t^s$ for $t = 1, \dots, 6$. Now we set

$$V_t^s = \{x \in \mathcal{H}_t^s \mid \text{Spec}(\mathcal{C}^s, \text{ad } x) \in \vartheta \mathbb{K}_0\}.$$

Remark that the root systems (of type A_4) corresponding to $\mathcal{H}_t^s$, $s = 1, 2$, together span the same $\mathbb{Q}$ -space as the root system (of type E_8) corresponding to $\mathcal{H}_t$. This remark and the equivalence (4) show that

$$V_t = \bigoplus_{s=1}^2 V_t^s.$$

By the results of §3, $\bigoplus_{t=1}^6 V_t^s$ is a $\mathbb{K}_0$ -form. In particular, $[V_t^s, V_{t'}^s] \subseteq V$. Furthermore, it is obvious that $[V_t^s, V_{t'}^{s'}] = 0$ whenever $s \neq s'$. Now we have

$$[V_1, V_2] = [\bigoplus_{s=1}^2 V_1^s, \bigoplus_{s'=1}^2 V_2^{s'}] \subseteq \sum_{s, s'=1}^2 [V_1^s, V_2^{s'}] \subseteq V,$$

as required.

Finally, in order to show that $\mathbb{K}_0$ is a minimal splitting field, suppose that $\mathbb{K}$ is a splitting field for G in $\mathcal{L}$ and that V is a $\mathbb{K}$ -form for G . We shall need the following simple statement:

Lemma 7. *Assume that a finite group A acts irreducibly on a complex vector space V of dimension n . Let $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{C}$ and suppose A fixes two nonzero $\mathbb{K}$ -subspaces U, U' in V . Then $U' = \lambda U$ for some $\lambda \in \mathbb{C}^*$.*

Proof. We know that $\mathbb{K}$ -representations of A on U and U' are equivalent over $\mathbb{C}$. So by the Deuring-Noether theorem they are equivalent over $\mathbb{K}$. This means that there exist a basis $\{e_1, \dots, e_n\}$ of U and a basis $\{f_1, \dots, f_n\}$ of U' such that the action of any $a \in A$ is written by the same matrix $\Phi(a)$ in $\{e_i\}$ and $\{f_i\}$. Write

$$\{f_1, \dots, f_n\} = \{e_1, \dots, e_n\}X$$

for $X \in GL_n(\mathbb{C})$. Then $X\Phi(a)X^{-1} = \Phi(a)$ for all $a \in A$. By Schur's lemma, the matrix X is a scalar: $X = \lambda E$ for some $\lambda \in \mathbb{C}^*$. In particular, $U' = \lambda U$. $\square$

Consider the Cartan subalgebra $\mathcal{H} = \mathcal{H}_1$ contained in $\mathcal{C}$ and set

$$U = \{x \in \mathcal{H} \mid \text{Spec}(\mathcal{L}, \text{ad } x) \subseteq \mathbb{K}\}.$$

Then U is obviously a $\mathbb{K}M$ -module, where $M = N_G(\mathcal{H})$. By Lemma 3 applied to the subgroup $\langle g, h \rangle \simeq \mathbb{Z}_5^2$ of J which acts trivially on $\mathcal{H}$, we see that $V \cap \mathcal{H}$ is another nonzero $\mathbb{K}M$ -module in $\mathcal{H}$. Furthermore, M acts irreducibly on $\mathcal{H}$. Therefore, by Lemma 7 there exists $\lambda \in \mathbb{C}^*$ such that $V \cap \mathcal{H} = \lambda U$. Put $\mathcal{H}^s = \mathcal{H} \cap \mathcal{C}^s$ and

$$U^s = \{x \in \mathcal{H}^s \mid \text{Spec}(\mathcal{C}^s, \text{ad } x) \subseteq \mathbb{K}\},$$

$s = 1, 2$. As above, one has $U = U^1 \oplus U^2$. Hence,

$$\lambda U^1 = \lambda U \cap \mathcal{C}^1 = (V \cap \mathcal{H}) \cap \mathcal{C}^1,$$

in particular, $V \cap \mathcal{C}^1 \neq 0$. It is now obvious that $V \cap \mathcal{C}^1$ is a $\mathbb{K}$ -form for the group $H = \mathbb{Z}_5^2 \cdot SL_2(5)$ distinguished by Lemma 6. Applying Proposition 4, we arrive at the conclusion that $\mathbb{K} \supseteq \mathbb{K}_0$.

Our theorem is completely proved.

Acknowledgments. Part of this work has been done during the Canadian Mathematical Society Annual Seminar "Representations of Groups: Lie, Finite, Quantum" held at Banff, June 1994. The authors' thanks go to the organizers of the Seminar for their support. The second author is also grateful to Prof. Dr. G. O. Michler and the Volkswagen Foundation for supporting his participation in the CMS Annual Seminar 1994.

References

- [Ale] A. V. Alekseevskii, *Jordan finite commutative subgroups of simple complex Lie groups*, Funktsional Anal. i Prilozhen. 8 (1974), no. 4, 1 – 4; English transl. in Functional Anal. Appl. 8 (1974), 277 – 279.
- [Asch] M. Aschbacher, *On the maximal subgroups of the finite classical groups*, Invent. Math. 76 (1984), 469 – 514.
- [Bor 1] A. V. Borovik, *Jordan subgroups of simple algebraic groups*, Algebra i logika 28 (1989), no. 2, 144 – 159; English transl. in Algebra and Logic 28 (1989), no. 2, 97 – 108.

- [Bor 2] A. V. Borovik, *The structure of finite subgroups of simple algebraic groups*, Algebra i logika 28 (1989), no. 3, 249 – 279; English transl. in Algebra and Logic 28 (1989), no. 3, 163 – 183.
- [CLSS] A. M. Cohen, M. W. Liebeck, J. Saxl and G. M. Seitz, *The local maximal subgroups of exceptional groups of Lie type, finite and algebraic*, Proc. London Math. Soc. (3) 64 (1992), no. 1, 21 – 48.
- [CNP] A. M. Cohen, G. Nebe and W. Plesken, *Cayley Orders*, to appear in Compositio Math., 1995.
- [CoG] A. M. Cohen and R. L. Griess, *On finite simple subgroups of the complex Lie group of type E_8* , Proc. Symp. Pure Math. 47 (1987), Pt. 2, 367 – 405.
- [CoW] A. M. Cohen and D. B. Wales, *Finite subgroups of $G_2(\mathbb{C})$* , Comm. Algebra, 11 (1983), 441 – 459.
- [CoW2] A. M. Cohen and D. B. Wales, *Finite simple subgroups of semisimple complex Lie groups – a survey*, pp. 77–96 in “Groups of Lie Type and their Geometries”, eds. W.M. Kantor and L. Di Martino, LMS Lecture Notes, no. 207, Cambridge University Press, 1995.
- [Gri] R. L. Griess, *Code loops and a large finite group containing triality for D_4* , Rend. Circ. Mat. Palermo (2) Suppl. no. 19 (1988), 79 – 98.
- [Isa] I. M. Isaacs, *‘Character Theory of Finite Groups’*, Academic Press, London, 1976, 303 pp.
- [KoT] A. I. Kostrikin and Pham Huu Tiep, *‘Orthogonal Decompositions and Integral Lattices’*, Walter de Gruyter, Berlin a.o., 1994, 535 pp.
- [Sah] C.-H. Sah, *Cohomology of split group extensions*, J. Algebra 29 (1974), 255 – 302.
- [Ser] J.-P. Serre, *Cohomologie Galoisienne*, Lecture Notes in Math., 5, Springer-Verlag, Berlin, 1964.
- [Spr] T. A. Springer, private communication, Zeist, 1994.
- [Tho] J. G. Thompson, *A simple subgroup of $E_8(3)$* , Finite Groups Symposium, N. Iwahori, Japan Soc. for Promotion of Science, 1976, pp. 113 – 116.

[Tiep] Pham Huu Tiep, *Invariant lattices of type E_8 and their automorphism groups*, Algebra i Analiz, 4 (1992), no. 5, 227 – 256; English transl. in St. Petersburg Math. J. 4 (1993), no. 5, 1029 – 1054.

Arjeh M. Cohen

Fak. Wisk. & Inf., Eindhoven University of Technology

Postbox 513, 5600 MB Eindhoven, The Netherlands

email:amc@win.tue.nl

Pham Huu Tiep

Institut für Experimentelle Mathematik, Universität Essen

Ellernstr. 29, 45326 Essen, Germany

Received February 1995