Illinois Journal of Mathematics
Volume 47, Number 1/2, Spring/Summer 2003, Pages 395–418
S 0019-2082

ON THE EXISTENCE OF A COMPLEMENT FOR A FINITE SIMPLE GROUP IN ITS AUTOMORPHISM GROUP

A. LUCCHINI, F. MENEGAZZO, AND M. MORIGI

ABSTRACT. In this paper we determine all finite simple groups G for which the automorphism group $\operatorname{Aut} G$ splits over $G = \operatorname{Inn} G$.

The theory of group extensions, and, in particular, the study of conditions which force the splitting of a given extension or class of extensions, is one of the themes with which the name of Reinhold Baer is associated. The present article gives a concrete, very special instance of this type of study: we examine the automorphism groups of the finite non abelian simple groups to determine those groups G for which $\operatorname{Aut} G$ splits over G, where we identify G with the inner automorphism group $\operatorname{Inn} G$. For such groups, the structure of the complement for $\operatorname{Inn} G$ in the automorphism group $\operatorname{Aut} G$ is of course well known: the complement is isomorphic to the outer automorphism group $\operatorname{Out} G$ (see [2]).

The question we are considering is very natural and easily stated; yet, it seems that only very partial results are known (see [6], [7]).

In fact, this is a problem on simple groups of Lie type, since the remaining cases are easily dealt with. Indeed, if $n \geq 5$, $n \neq 6$, $\operatorname{Sym}(n) = \operatorname{Aut}(\operatorname{Alt}(n))$ always splits over $\operatorname{Alt}(n)$, while $\operatorname{Alt}(6) \cong \operatorname{PSL}(2,9)$ has no complement in $\operatorname{Aut}(\operatorname{Alt}(6))$. Similarly, all automorphism groups of the sporadic simple groups split over their socle: if G is a sporadic group, then either $\operatorname{Aut} G = \operatorname{Inn} G$ or $\operatorname{Inn} G$ has index 2 in $\operatorname{Aut} G$, and in each case there exists a conjugacy class of non-inner involutions in $\operatorname{Aut} G$ (see [2]).

On the other hand, the behaviour of groups of Lie type is not so uniform; it depends on the type of the group and on some arithmetical conditions involving the cardinality of the field and the rank of the group. The following theorem collects our results.

Received March 8, 2002.

2000 *Mathematics Subject Classification.* 20E32, 20D06, 20F28.

This research was supported by MIUR, project Teoria dei gruppi e applicazioni. The third author was supported by the University of Bologna, funds for selected research topics.

Theorem. *Let G be a simple group of Lie type over a finite field with $q = p^m$ elements, p prime, and denote by d the order of the abelian group $\hat{H}/H$, where $\hat{H}$ is the group of diagonal automorphisms of G and H is the subgroup of $\hat{H}$ consisting of those diagonal automorphisms which are inner. (The values of d for untwisted and twisted groups are given in the tables in Sections 3 and 4.) Then $\operatorname{Aut} G$ splits over G if and only if one of the following conditions holds:*

(1) *G is untwisted, not of type $D_l(q)$, and $(\frac{q-1}{d}, d, m) = 1$;*
(2) *$G = D_l(q)$ and $(\frac{q^l-1}{d}, d, m) = 1$;*
(3) *G is twisted, not of type ${}^2D_l(q)$, and $\left(\frac{q+1}{d}, d, m\right) = 1$;*
(4) *$G = {}^2D_l(q)$ and either l is odd or $p = 2$.*

The paper is divided into four sections. In Sections 1 and 2 we study the groups $A_n(q)$ and ${}^2A_n(q)$, respectively, using their natural projective representations; in Sections 3 and 4 we consider the remaining untwisted (respectively twisted) groups of Lie type.

1. The special linear groups

Let $\mathrm{F} = \mathrm{F}_q$ be the finite field with q elements, where $q = p^m$ for some prime number p. We fix a generator λ of the multiplicative group of the field F^*. As usual, $\mathrm{GL}(n, q)$ (resp. $\mathrm{SL}(n, q)$) will denote the general (resp. special) linear group of degree n over the field F_q. In the following we will identify F^* with the subgroup of $\mathrm{GL}(n, q)$ consisting of scalar matrices, and let $\mathrm{PGL}(n, q) = \mathrm{GL}(n, q)/\mathrm{F}^*$, $\mathrm{PSL}(n, q) = \mathrm{SL}(n, q)\,\mathrm{F}^*/\mathrm{F}^*$. For an element $g \in \mathrm{GL}(n, q)$ its image in $\mathrm{PGL}(n, q)$ will be denoted with $\bar{g}$. Also, as usual, $\det(g)$ will denote the determinant of a matrix g.

Throughout this section, we will consider $G = A_{n-1}(q) = \mathrm{PSL}(n, q)$, for n and q fixed. Let ϕ be the Frobenius automorphism of F, defined by $a^\phi = a^p$ (using the exponential notation for automorphisms). Then ϕ induces an automorphism of $\mathrm{GL}(n, q)$ of order m, which will also be denoted by ϕ, given by $(a_{ij})^\phi = (a_{ij}^p)$ for $i, j = 1, \ldots, n$.

Let $\iota : \mathrm{GL}(n, q) \to \mathrm{GL}(n, q)$ be the automorphism defined by $g^\iota = (g^\top)^{-1}$, where $g^\top$ denotes the transpose matrix of g.

Both ϕ and ι induce automorphisms $\bar{\phi}$ and $\bar{\iota}$ of $\mathrm{PGL}(n, q)$. $\bar{\phi}$ generates the group of field automorphisms, $\bar{\iota}$ is the product of the graph automorphism and an inner automorphism if $n \geq 3$, and it is an inner automorphism if $n = 2$. As G is simple, we may also identify G with $\operatorname{Inn} G \leq \operatorname{Aut} G$.

We have the sequence of normal subgroups

$$\mathrm{SL}(n, q) \leq \mathrm{GL}(n, q) \leq \Gamma\mathrm{L}(n, q) = \mathrm{GL}(n, q)\langle\phi\rangle \leq \Gamma\mathrm{L}(n, q)\langle\iota\rangle.$$

Taking quotients modulo the scalar matrices we obtain

$$G \leq \mathrm{PGL}(n, q) \leq \mathrm{P}\Gamma\mathrm{L}(n, q) = \mathrm{PGL}(n, q)\langle\bar{\phi}\rangle \leq \operatorname{Aut} G = \mathrm{P}\Gamma\mathrm{L}(n, q)\langle\bar{\iota}\rangle.$$

Also, $\mathrm{PGL}(n,q)/G$ is cyclic of order $d=(n,q-1)$ and $\bar{\phi}$ acts on it as the p-th power. We want to prove that G has a complement in $\mathrm{Aut}\,G$ if and only if $\left(\frac{q-1}{d},d,m\right)=1$. Letting t be the product of all prime factors of d dividing $\frac{q-1}{d}$, counting multiplicities, this is equivalent to proving that G has a complement in $\mathrm{Aut}\,G$ if and only if $(t,m)=1$.

Lemma 1.1.

(i) *$\langle\bar{g}\rangle$ is a complement for $\mathrm{PSL}(n,q)$ in $\mathrm{PGL}(n,q)$ if and only if $\det(g)=\lambda^u$, with $(u,d)=1$ and $g^d\in \mathrm{F}^*$.*

(ii) *Assume that G has a complement $\bar{C}$ in $\mathrm{P\Gamma L}(n,q)$. Then it is possible to choose $g\in \mathrm{GL}(n,q)$ and $h\in \mathrm{SL}(n,q)$ such that $\bar{C}=\langle\bar{g},\bar{\phi}\bar{h}\rangle$, $\det(g)=\lambda$, $|\bar{g}|=d$ and $\bar{g}^{\bar{\phi}\bar{h}}=\bar{g}^p$.*

Proof. (i) Suppose that $\det(g)=\lambda^u$. Then $\bar{g}$ generates $\mathrm{PGL}(n,q)$ modulo $\mathrm{PSL}(n,q)$ if and only if λ^u generates F^* modulo $(\mathrm{F}^*)^n$, that is, if and only if $(u,d)=1$. Therefore $\langle\bar{g}\rangle$ is a complement if and only if we have that $\bar{g}^d=1$, that is, $g^d\in\mathrm{F}^*$.

(ii) Choose g such that $\langle\bar{g}\rangle=\bar{C}\cap G$. As $\bar{g}$ generates $\mathrm{PGL}(n,q)$ modulo $\mathrm{PSL}(n,q)$, we have that $\det(g)=\lambda^u$ with $(u,d)=(u,n,q-1)=1$. Let $r,s,v\in\mathbb{Z}$ be such that $ru+sn+v(q-1)=1$. Then $\det(\lambda^s g^r)=\lambda$ and we may replace g by $\lambda^s g^r$. The remaining statements follow from the fact that the projection $\pi:\bar{C}\to\langle\bar{g},\bar{\phi}\rangle G/G$ is an isomorphism. □

Lemma 1.2. *Assume that G has a complement in $\mathrm{P\Gamma L}(n,q)$. Then $(m,t)=1$.*

Proof. Let g,h be as in Lemma 1.1 (ii), so that $g^d=\lambda^\alpha\in\mathrm{F}^*$. Taking the determinant of both sides we have that $\lambda^d=\det(g)^d=(\lambda^\alpha)^n$. So $d\equiv\alpha n \bmod q-1$, that is, $1\equiv\alpha(n/d)\bmod (q-1)/d$ and thus $(\alpha,\frac{q-1}{d})=1$. It follows that $(\alpha,t)=1$.

We may view ϕh as a ring automorphism of the ring $\mathrm{Mat}(n,q)$ of $n\times n$ matrices with entries in F. As $\bar{g}^{\bar{\phi}\bar{h}}=\bar{g}^p$, we have that $g^{\phi h}=(gz)^p$ for some $z\in\mathrm{F}^*$, so ϕh normalizes the subring $\mathrm{F}[g]$ of $\mathrm{Mat}(n,q)$ (where, as usual, F is identified with the ring of scalar matrices). Now the map $\pi:\mathrm{F}[g]\to\mathrm{F}[g]$, defined by $v^\pi=v^p$ is also a ring automorphism of $\mathrm{F}[g]$, and $\phi h\pi^{-1}$ is a ring automorphism which centralizes F. So $\lambda^\alpha=g^d=(g^d)^{\phi h\pi^{-1}}=(g^{\phi h\pi^{-1}})^d=(gz)^d=\lambda^\alpha z^d$ and $z^d=1$. Thus we may assume that $z=\lambda^{\beta(q-1)/d}$ for some integer β. It is easy to see that $g^{(\phi h)^i}=g^{p^i}z^{ip^i}$ for each natural number i. As $(\phi h)^m$ is a scalar matrix, we obtain that $g=g^{(\phi h)^m}=g^{p^m}z^{mp^m}=g^q z^{mq}=g^q z^m$, so $g^{q-1}=z^{-m}$. As $g^{q-1}=g^{d\frac{q-1}{d}}=\lambda^{\alpha\frac{q-1}{d}}$, we have that $\alpha\frac{q-1}{d}\equiv -(m\beta)\frac{(q-1)}{d}\bmod q-1$. It follows that $\alpha\equiv-\beta m\bmod d$, so $(m,t)\mid(\alpha,t)=1$, as we wanted to prove. □

We now seek a complement for G in $\mathrm{P\Gamma L}(n,q)$. If $n=2$, we find $g\in \mathrm{GL}(n,q)$ such that $\det(g)=\lambda$, $g^d\in \mathrm{F}^*$, and $\langle g\rangle$ is normalized by ϕ; if $n\geq 3$, we find a matrix g with the above properties and such that $\langle g\rangle$ is normalized by ιu, for a suitable matrix $u\in \mathrm{GL}(n,q)$ such that $(\iota u)^2=1$ and ιu commutes with ϕ.

Lemma 1.3. *Let $d=tl$, $d_1|d$, $d_1=t_1l_1$, where $t_1=(d_1,t)$. There exist $v_1,\dots,v_{n/t_1}\in \mathrm{F}$ and $u\in\mathbb{Z}$ such that $(u,t_1)=1$, $v_j^{l_1}=1$ for $j=1,\dots,n/t_1$, and*

$$\prod_{j=1}^{n/t_1}(-1)^{t_1-1}\lambda^u v_j=\lambda^{d/d_1}.$$

Proof. Assume that a prime r divides $\frac{q-1}{l}=\frac{q-1}{d}\frac{d}{l}=\frac{q-1}{d}t$. Then r divides $\frac{q-1}{d}$, so r divides neither l, as $\left(\frac{q-1}{d},l\right)=1$, nor $\frac{n}{d}$, as $\left(\frac{n}{d},\frac{q-1}{d}\right)=1$. It follows that $\left(\frac{q-1}{l},\frac{n}{t}\right)=\left(\frac{q-1}{l},l\frac{n}{d}\right)=1$. Thus we have $\left(\frac{q-1}{l_1},\frac{n}{t_1}\right)=\left(\frac{q-1}{l}\frac{l}{l_1},\frac{n}{t}\frac{t}{t_1}\right)\mid\left(\frac{q-1}{l},\frac{n}{t}\right)\frac{l}{l_1}\frac{t}{t_1}=\frac{d}{d_1}$.

We now distinguish two cases. If t_1 is odd or $\frac{n}{t_1}$ is even, we take $u,y\in\mathbb{Z}$ such that $y\frac{q-1}{l_1}+u\frac{n}{t_1}=\frac{d}{d_1}$. Note that, by dividing both sides by $\frac{d}{d_1}$, we get $y\frac{q-1}{d}t_1+u\frac{n}{d}l_1=1$, so $(u,t_1)=1$.

If t_1 is even and $\frac{n}{t_1}$ is odd, then $\frac{d}{d_1}\mid\frac{q-1}{2}$, so we may take $u,y\in\mathbb{Z}$ such that $y\frac{q-1}{l_1}+u\frac{n}{t_1}=\frac{d}{d_1}+\frac{q-1}{2}$. Again, dividing by $\frac{d}{d_1}$, we get $y\frac{q-1}{d}t_1+u\frac{n}{d}l_1=1+\frac{q-1}{d}\frac{d_1}{2}$, so $(u,t_1)=1$, because every prime dividing t_1 divides also $\frac{q-1}{d}$.

In both cases u has the desired properties, and taking $v_1=\lambda^{y\frac{q-1}{l_1}}$, $v_j=1$ for $j\neq 1$, we have

$$\prod_{j=1}^{n/t_1}(-1)^{t_1-1}\lambda^u v_j=(-1)^{(t_1-1)n/t_1}\lambda^{u\frac{n}{t_1}+y\frac{q-1}{l_1}}=\lambda^{d/d_1}. \qquad \square$$

We now describe a construction which will be used in the sequel.

Lemma 1.4. *Let $d_1=t_1l_1$ be as above. Take $u\in\mathbb{Z}$ and $v_1,\dots,v_{n/t_1}\in\mathrm{F}$ such that $v_j^{l_1}=1$ for every $j=1,\dots,n/t_1$, and $\prod_{j=1}^{n/t_1}(-1)^{t_1-1}\lambda^u v_j=\lambda^{d/d_1}$. Then there exists a matrix $g\in\mathrm{GL}(n,q)$ such that $g^{d_1}\in\mathrm{F}^*$ and $\det(g)=\lambda^{d/d_1}$.*

Proof. Note that Lemma 1.3 ensures the existence of u and $v_1,\dots,v_{n/t_1}$ with the required properties. Let $j\in\{1,\dots,n/t_1\}$, $c=\lambda^u$ and $c_j=cv_j$. Consider the commutative ring $V_j=\mathrm{F}[w_j]$, where w_j has minimal polynomial $x^{t_1}-c_j$ over F, that is, $\mathrm{F}[w_j]$ is isomorphic to the quotient of the polynomial ring $\mathrm{F}[x]$ over the ideal $(x^{t_1}-c_j)$. Then V_j is a vector space of dimension t_1 over F and a basis is $\{1,w_j,w_j^2,\dots,w_j^{t_1-1}\}$. We have that w_j acts on V_j via right multiplication, and the matrix associated to this endomorphism with respect to the fixed basis is

$$g_j = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & & 0 \\ \vdots & & & \ddots & 0 \\ 0 & 0 & 0 & & 1 \\ c_j & 0 & \dots & 0 & 0 \end{pmatrix}.$$

Note that $\det(g_j) = (-1)^{t_1-1}\lambda^u v_j$.

Also $g_j^{d_1} = (g_j^{t_1})^{l_1} = (c_j)^{l_1} = (cv_j)^{l_1} = c^{l_1}$. Let $V = \oplus_{j=1}^{n/t_1} V_j$ and let g be the matrix

$$g = \begin{pmatrix} g_1 & & \\ & \ddots & \\ & & g_{n/t_1} \end{pmatrix};$$

then $g^{d_1} = c^{l_1} \in \mathrm{F}^*$ and $\det(g) = \prod_{j=1}^{n/t_1}(-1)^{t_1-1}\lambda^u v_j = \lambda^{d/d_1}$, as required. □

Proposition 1.5. $\mathrm{PSL}(n,q)$ *is complemented in* $\mathrm{PGL}(n,q)$.

Proof. Take $v_1,\dots,v_{n/t} \in \mathrm{F}$ and $u \in \mathbb{Z}$ as in Lemma 1.3, with $d_1 = d$, and let g be the matrix constructed in Lemma 1.4. Then $\langle \bar{g} \rangle$ is the required complement. □

We will also need the following observation:

Observation 1.6. *Consider the polynomial* $x^s - c$*, where* $c \in \mathrm{F}$ *and* $s|q-1$. *If* $c = \lambda^u$*, where* $(u,s) = 1$*, then* $x^s - c$ *is irreducible in* $\mathrm{F}[x]$.

Lemma 1.7. *Let* $\mathrm{F}[w]$ *be a field, where* w *has minimal polynomial* $x^s - c$ *over* F *and* $s|q-1$. *Assume also that* $(s,m) = 1$ *and let* $k \in \mathbb{N}$ *be such that* $mk \equiv -1 \bmod s$. *Let* $\pi : \mathrm{F}[w] \to \mathrm{F}[w]$ *be the map defined by* $v^\pi = v^p$. *Then* $\psi = \pi^{mk+1}$ *is an automorphism of* $\mathrm{F}[w]$ *of order* m *such that* $a^\psi = a^p$ *for every* $a \in \mathrm{F}$ *and* $w^\psi = (wz)^p$*, where* $z = c^{(q^k-1)/s} \in \langle w \rangle \cap \mathrm{F}^*$.

Proof. $\mathrm{F}[w]$ is a field of order $q^s = p^{ms}$. Also, $\psi = \pi^{mk+1}$ induces ϕ on F, so m divides the order of ψ. Note that the order of π is sm, so if $mk+1 = sh$ we have that $\psi^m = \pi^{(mk+1)m} = \pi^{shm} = 1$. Hence ψ has order m. Also, $w^\psi = w^{\pi^{mk+1}} = (ww^{q^k-1})^p = (wc^{(q^k-1)/s})^p$, and $z = c^{(q^k-1)/s} \in \langle w \rangle$. □

Next, we recall some well-known facts about symmetric bilinear forms. Let K be a field and let $\beta : V \times V \to K$ be a symmetric non-degenerate bilinear form over a K-vector space V of dimension s. If $f \in \mathrm{End}(V)$ is a linear map, then there exists a unique linear map $f' \in \mathrm{End}(V)$ such that $\beta(uf, v) = \beta(u, vf')$ for every $u, v \in V$. The map f' is called the adjoint map of f with respect to β, and f is said to be self-adjoint if $f' = f$. Take a basis $\{e_1, e_2, \dots, e_s\}$ of V and let A, A' and B be the matrices associated to f, f' and β with respect to this basis. Then $A' = B^\top A^\top (B^\top)^{-1}$. The following lemma is an exercise in [5, p. 367]:

Lemma 1.8. *Let V be a vector space of dimension s over the field K, and let $f \in \mathrm{End}(V)$ be a linear map. Then there exists a symmetric non-degenerate bilinear form β with discriminant $\delta \in \{\pm 1(K^*)^2\}$ such that f is self-adjoint with respect to β.*

Lemma 1.9. *Let V be a vector space of dimension s over the field K, and let β be a symmetric non-degenerate bilinear form on V with discriminant δ. If p is odd and $\delta = (K^*)^2$ or if $p = 2$ and s is odd, then there exists a basis E of V such that the matrix associated to β with respect to E is the identity matrix. If p is odd, -1 is not a square in F and $\delta = -1(K^*)^2$, then there exists a basis E of V such that the matrix associated to β with respect to E is the diagonal matrix $B = \mathrm{diag}(-1, 1, \dots, 1)$.*

Proof. See [3, pp. 16,20]. □

In the sequel, if R is an algebra and $w \in R$, the linear map given by right multiplication by w will be denoted by r_w.

Lemma 1.10. *With the hypotheses and notations of Lemma 1.7, let $V = \mathrm{F}[w]$. There exists a basis $E = \{e_1, \dots, e_s\}$ of V and a matrix $B \in \mathrm{GL}(s, p)$ such that the following hold:*

(i) *$\iota B \in Aut(\mathrm{SL}(n, q))$ has order 2, and it commutes with ϕ.*
(ii) *The matrix g associated to r_w with respect to E is such that $g^{\iota B} = g^{-1}$ and $g^\phi = (gz)^p$, where $z = c^{(q^k-1)/s} \in \langle g \rangle$. Also, $g^s = c$ and $\det(g) = (-1)^{s-1}c$.*

Proof. We have that $\mathrm{F}[w]$ is a field of order $q^s = p^{ms}$. The field F' of fixed points of the automorphism ψ has order p^s and we have $\mathrm{F} \cap \mathrm{F}' = \mathrm{F}_p$, as $(m, s) = 1$.

Let $\mathrm{F}' = \mathrm{F}_p[v]$ and note that $\mathrm{F}[w] = \mathrm{F}[v]$ and that every basis of F' over F_p is also a basis of $\mathrm{F}[w]$ over F. We may view F' as a vector space over F_p and consider the linear map $r_v \in \mathrm{End}_{\mathrm{F}_p}(\mathrm{F}')$. By Lemma 1.8 there exists a symmetric non-degenerate bilinear form β on F' over F_p with discriminant $\delta \in \{\pm 1(\mathrm{F}_p^*)^2\}$ such that r_v is self-adjoint with respect to β. Note that if $p = 2$, then s is odd. By Lemma 1.9 we may choose a basis $E = \{e_1, \dots, e_s\}$ of F' such that the matrix B associated to β is of the form $B = \mathrm{diag}(\epsilon, 1, \dots, 1)$, where $\epsilon \in \{\pm 1\}$. Then the matrix A of r_v with respect to this basis satisfies $A^{\top B} = A$.

Now consider $V = \mathrm{F}[v] = \mathrm{F}[w]$. We have that E is a basis for V over F. Also, as $w \in \mathrm{F}[v]$, w is a linear combination of powers of v, so the matrix g

associated to r_w with respect to E is such that $g^{\top B} = g$, that is, $g^{\iota B} = g^{-1}$, as required. Moreover, $B \in \mathrm{GL}(s, \mathrm{F}_p)$, $B = B^{\top} = B^{-1}$, so that (i) holds.

Next, let $x = \lambda_1 + \lambda_2 v + \ldots + \lambda_s v^{s-1} \in V$, with $\lambda_1, \ldots, \lambda_s \in \mathrm{F}$. As ψ acts trivially on $E \subseteq \mathrm{F}'$, we have $x^{\psi} = \lambda_1^p + \lambda_2^p v \ldots + \lambda_s^p v^{s-1}$, that is, ψ is the semi-linear map associated to the identity matrix and the automorphism ϕ with respect to the basis E. As $w^{\psi} = (zw)^p$, the matrix associated to $r_{w^{\psi}}$ is $g^{\phi} = c^{p(q^k-1)/s} g^p$, as we wanted to show.

Note that r_{w^s} is right multiplication by the scalar c, so $g^s = c$ and $x^s - c$ is both the minimal polynomial and the characteristic polynomial of g. It follows that $\det(g) = (-1)^{s-1}c$. □

Proposition 1.11. *Let $d_1 | d$, $d_1 = t_1 l_1$, where $t_1 = (d_1, t)$. Assume that $D \leq \mathrm{PGL}(n,q)$ is such that $G \leq D$ and D/G has order d_1. If $(m, t_1) = 1$, then G has a complement in $\langle D, \bar{\phi}, \bar{\iota} \rangle$.*

Proof. Take $v_1, \ldots, v_{n/t_1} \in \mathrm{F}$ and $u \in \mathbb{Z}$ as in Lemma 1.3, and let $c = \lambda^u$ and $c_j = cv_j$. Note that $c_j = \lambda^{u + \alpha_j (q-1)/l_1}$ for some integer α_j, and as $(u, t_1) = 1$ we have that $(u + \alpha_j \frac{q-1}{l_1}, t_1) = 1$, so by Observation 1.6 the polynomials $x^{t_1} - c_j$ are irreducible. Now we may apply Lemma 1.10 and find matrices g_j and B_j such that B_j satisfies (i) of Lemma 1.10, $g_j^{\iota B_j} = g_j^{-1}$, $g_j^{\phi} = (cv_j)^{p(q^k-1)/t_1} g_j^p$ and $g_j^{t_1} = cv_j$ for $j = 1, \ldots, n/t_1$. As $l_1 | \frac{q^k-1}{t_1}$, it follows that $v_j^{(q^k-1)/t_1} = 1$, so $g_j^{\phi} = c^{p(q^k-1)/t_1} g^p$. Also, $g_j^{d_1} = g_j^{t_1 l_1} = (cv_j)^{l_1} = c^{l_1}$. Now consider the matrices

$$g = \begin{pmatrix} g_1 & & \\ & \ddots & \\ & & g_{n/t_1} \end{pmatrix}, \qquad B = \begin{pmatrix} B_1 & & \\ & \ddots & \\ & & B_{n/t_1} \end{pmatrix}.$$

We have that ιB has order 2 and commutes with ϕ, $g^{\iota B} = g^{-1}$ and $g^{\phi} = (gz)^p$, where $z = c^{(q^k-1)/t_1} \in \mathrm{F}$. Also, $g^{d_1} = c^{l_1}$ and

$$\det(g) = \prod_{j=1}^{n/t_1} \det(g_j) = \prod_{j=1}^{n/t_1} (-1)^{t_1 - 1} \lambda^u v_j = \lambda^{d/d_1}.$$

Then $\bar{C} = \langle \bar{g}, \bar{\phi}, \bar{\iota}\bar{B} \rangle$ is the required complement. □

Combining Lemma 1.2 with the special case $d_1 = d$ of Proposition 1.11 we get:

Theorem 1.12. $\mathrm{PSL}(n,q)$ *has a complement in* $\mathrm{Aut}(\mathrm{PSL}(n,q))$ *if and only if* $(\frac{q-1}{d}, d, m) = 1$.

2. The unitary groups

In this section, we will consider the group $G = {}^2A_{n-1}(q) = \mathrm{PSU}(n,q)$, for n and q fixed.

Let $\mathrm{F} = \mathrm{F}_{q^2}$ be the finite field with q^2 elements, where $q = p^m$ for some prime number p. We fix a generator λ of the multiplicative group of the field F^*. Then $\mathrm{U}(n,q)$ (resp. $\mathrm{SU}(n,q)$) will denote the general (resp. special) unitary group of degree n, that is, $\mathrm{U}(n,q) = \{g \in \mathrm{GL}(n,q^2) \mid g(g^\top)^\sigma = 1\}$, where $\sigma = \phi^m \in \mathrm{Aut}(\mathrm{GL}(n,q^2))$, and $\mathrm{SU}(n,q) = \{g \in \mathrm{U}(n,q) \mid \det(g) = 1\}$. All other notations, unless otherwise specified, are as in the previous section, and as usual F^* is identified with the subgroup of $\mathrm{GL}(n,q^2)$ consisting of scalar matrices.

We have the sequence of normal subgroups

$$\mathrm{SU}(n,q) \leq \mathrm{U}(n,q) \leq \mathrm{U}(n,q)\langle\phi\rangle,$$

from which, taking images in $\mathrm{U}(n,q)\langle\phi\rangle\,\mathrm{F}^*\,/\,\mathrm{F}^*$, we obtain the sequence

$$\mathrm{PSU}(n,q) \leq \mathrm{PU}(n,q) \leq \mathrm{U}(n,q)\langle\phi\rangle\,\mathrm{F}^*\,/\,\mathrm{F}^* = \mathrm{Aut}(\mathrm{PSU}(n,q)).$$

Also, $\mathrm{PU}(n,q)/G$ is cyclic of order $d = (n, q+1)$ and $\bar{\phi}$ acts on it as the p-th power. We want to prove that G has a complement in $\mathrm{Aut}\,G$ if and only if $\left(\frac{q+1}{d}, d, m\right) = 1$. Letting t be the product of all prime factors of d dividing $\frac{q+1}{d}$, counting multiplicities, this is equivalent to proving that G has a complement in $\mathrm{Aut}\,G$ if and only if $(t,m) = 1$.

Lemma 2.1.

(i) *If* $g \in \mathrm{U}(n,q)$, *then* $\det(g)^{q+1} = 1$.
(ii) $\mathrm{U}(n,q) \cap \mathrm{F}^* = \{a \in \mathrm{F}^* \mid a^{q+1} = 1\}$.
(iii) $\langle\bar{g}\rangle$ *is a complement for* $\mathrm{PSU}(n,q)$ *in* $\mathrm{PU}(n,q)$ *if and only if* $\det(g) = \lambda^{(q-1)u}$, *with* $(u,d) = 1$, *and* $g^d \in \mathrm{F}^*$.
(iv) *Assume that* G *has a complement* $\bar{C}$ *in* $\mathrm{Aut}\,G$. *Then it is possible to choose* $g \in \mathrm{U}(n,q)$ *and* $h \in \mathrm{SU}(n,q)$ *such that* $\bar{C} = \langle\bar{g}, \bar{\phi}\bar{h}\rangle$, $\bar{g}^{\bar{\phi}\bar{h}} = \bar{g}^p$, $\det(g) = \lambda^{(q-1)u}$, *with* $(u,d) = 1$, *and* $g^d, (\phi h)^{2m} \in \mathrm{F}^*$.

Proof. (i) and (ii) follow directly form the definition of $\mathrm{U}(n,q)$. To obtain (iii) and (iv), we note that, by (i), $\det(g)$ is of the form $\lambda^{(q-1)u}$. The proofs are now analogous to those of Lemma 1.1. □

Lemma 2.2. *Assume that* G *has a complement in* $\mathrm{Aut}\,G$. *Then* $(m,t) = 1$.

Proof. Let g, h be as in Lemma 2.1 (iv), so that $\det(g) = \lambda^{(q-1)u}$, with $(u,d) = 1$, and $g^d = \lambda^{\alpha(q-1)} \in \mathrm{U}(n,q) \cap \mathrm{F}^*$ for some natural number α (see Lemma 2.1 (ii)). Taking the determinant on both sides, we obtain $\lambda^{du(q-1)} = \lambda^{\alpha n(q-1)}$, that is, $du(q-1) \equiv d\alpha\frac{n}{d}(q-1) \bmod (q^2-1)$, and so $u \equiv \alpha\frac{n}{d} \bmod \frac{q+1}{d}$. If r is a prime such that $r|t$, then $r|\frac{q+1}{d}$ and $r \nmid u$, so $r \nmid \alpha$. It follows that $(\alpha, t) = 1$.

We may view ϕh as a ring automorphism of the ring $\mathrm{Mat}(n, q^2)$. As $\bar{g}^{\bar{\phi}\bar{h}} = \bar{g}^p$, we have that $g^{\phi h} = (gz)^p$ for some $z \in \mathrm{F}^*$, so ϕh normalizes the subring $\mathrm{F}[g]$ of $\mathrm{Mat}(n, q^2)$. Now the map $\pi : \mathrm{F}[g] \to \mathrm{F}[g]$, defined by $v^\pi = v^p$, is also a ring automorphism of $\mathrm{F}[g]$, and $\phi h \pi^{-1}$ is ring automorphism which centralizes F. So $\lambda^{\alpha(q-1)} = g^d = (g^d)^{\phi h \pi^{-1}} = (g^{\phi h \pi^{-1}})^d = (gz)^d = \lambda^{\alpha(q-1)} z^d$ and $z^d = 1$. Hence we may assume that $z = \lambda^{\beta(q^2-1)/d}$ for some integer β. As $(\phi h)^{2m}$ is a scalar matrix and $g^{(\phi h)^i} = g^{p^i} z^{ip^i}$ for each natural number i, we obtain that $g = g^{(\phi h)^{2m}} = g^{q^2} z^{2m}$, so $g^{q^2-1} = z^{-2m}$. Moreover, $g^{q^2-1} = g^{d(q^2-1)/d} = \lambda^{\alpha(q-1)(q^2-1)/d}$, so we have $\alpha(q-1)\frac{q^2-1}{d} \equiv -(2m\beta)\frac{q^2-1}{d} \bmod q^2-1$. It follows that $\alpha(q-1) \equiv -2\beta m \bmod d$.

Let r be a prime which divides t. If $r = 2$, then $p \neq 2$. Both $\frac{q+1}{d}$ and d are even, so $q+1 = p^m + 1 \equiv 0 \bmod 4$ and m is odd. If $r \neq 2$, then $r | d, r | q+1, r \nmid q-1$, and $r \nmid \alpha$ (by what we have just proved), so $r \nmid m$. It follows that $(m, t) = 1$, as we wanted to prove. □

We now seek a complement for G in $\mathrm{Aut}\, G$. We find $g, h \in \mathrm{U}(n, q)$ such that $\det(g) = \lambda^{q-1}$, $g^d \in \mathrm{F}^*$, $(\phi h)^{2m} \in \mathrm{F}^*$ and $\langle g \rangle$ is normalized by ϕh.

LEMMA 2.3. *Assume that $d = tl$, $d_1 | d$, $d_1 = t_1 l_1$, where $t_1 = (d_1, t)$. Then there exist $v_1, \ldots, v_{n/t_1} \in (\mathrm{F}^*)^{q-1}$ and $u \in \mathbb{Z}$ such that $v_j^{l_1} = 1$ for $j = 1, \ldots, n/t_1$ and*

$$\prod_{j=1}^{n/t_1} (-1)^{t_1 - 1} \lambda^{u(q-1)} v_j = \lambda^{(q-1)d/d_1}.$$

Proof. The proof is analogous to that of Lemma 1.3. □

LEMMA 2.4. *Let $d_1 = t_1 l_1$ as above. Take $u \in \mathbb{Z}$ and $v_1, \ldots, v_{n/t_1} \in \mathrm{F}$ such that $v_j^{l_1} = 1$ for every $j = 1, \ldots, n/t_1$, and $\prod_{j=1}^{n/t_1} (-1)^{t_1-1} \lambda^{u(q-1)} v_j = \lambda^{(q-1)d/d_1}$. Then there exists a matrix $g \in \mathrm{U}(n, q)$ such that $g^{d_1} \in \mathrm{F}^*$ and $\det(g) = \lambda^{(q-1)d/d_1}$.*

Proof. Note that Lemma 2.3 ensures the existence of u and $v_1, \ldots, v_{n/t_1}$ with the required properties. Then construct the matrix g as in Lemma 1.4, using $c = \lambda^{u(q-1)}$ in place of $c = \lambda^u$. It is easy to see that $g_j (g_j^\top)^\sigma = \mathrm{diag}(1, \ldots, 1, c_j^{q+1}) = 1$, as $c_j^{q+1} = (\lambda^{u(q-1)} v_j)^{q+1} = 1$, because $l_1 | q+1$. It follows that $g(g^\top)^\sigma = 1$, so $g \in \mathrm{U}(n, q)$. □

PROPOSITION 2.5. $\mathrm{PSU}(n, q)$ *is complemented in* $\mathrm{PU}(n, q)$.

Proof. Take $v_1, \ldots, v_{n/t} \in \mathrm{F}$ and $u \in \mathbb{Z}$ as in Lemma 2.3, with $d_1 = d$ and let g be the matrix constructed in Lemma 2.4. Then $\langle \bar{g} \rangle$ is the required complement. □

Lemma 2.6. *Let* $\mathrm{F}[w]$ *be a commutative ring, where* w *has minimal polynomial* $x^{t_1} - c$ *over* F *(where* t_1 *is as in Lemma 2.3), that is,* $\mathrm{F}[w]$ *is isomorphic to the quotient of the polynomial ring* $\mathrm{F}[x]$ *over the ideal* $(x^{t_1} - c)$*. Let* $c = \lambda^{u(q-1)}$ *and assume also that* $(t_1, u) = (t_1, m) = 1$*. Then* $\mathrm{F}[w]$ *has a ring automorphism* ψ *of order* $2m$ *such that* $a^\psi = a^p$ *for every* $a \in \mathrm{F}$ *and* $w^\psi = (wz)^p$*, with* $z \in \langle c \rangle$*. More specifically, we have:*

(i) *If* t_1 *is odd, let* $k \in \mathbb{N}$ *be such that* $2mk \equiv -1 \bmod t_1$*. Then* $z = c^{(q^{2k}-1)/t_1} \in \langle w \rangle$*.*
(ii) *If* t_1 *is even let* $k \in \mathbb{N}$ *be such that* k *is odd and* $mk \equiv -1 \bmod t_1/2$*. Then* $z = c^{(q^{2k}-1)/(2t_1)} \in \langle w \rangle$*.*

Proof. (i) In this case $(t_1, 2m) = 1$. Note that, as $t_1 | q+1$, we have that $(t_1, q-1) = 1$, so by Observation 1.6 the polynomial $x^{t_1} - \lambda^{u(q-1)}$ is irreducible. Then the map $\psi = \pi^{2mk+1}$ constructed in Lemma 1.7 with $s = t_1$ and $2m$ in place of m has the required properties.

(ii) As $(m, \frac{t_1}{2}) = 1$, there exist an odd $k \in \mathbb{N}$ and $s \in \mathbb{Z}$ such that $mk + s\frac{t_1}{2} + 1 = 0$.

Let $\epsilon = c^{(q^{2k}-1)/(2t_1)}$. As $q^2 \equiv 1 \bmod t$, it follows that $1 + q^2 + \cdots + q^{2(k-1)} \equiv k \bmod t$. Also, it is clear that $\left(\frac{q-1}{2}, t_1\right) = 1$, so if $\alpha = u\frac{q-1}{2}(1 + q^2 + \cdots + q^{2(k-1)})$ we have that $(\alpha, t_1) = 1$. It follows that $\epsilon = \lambda^{(q-1)u(q^{2k}-1)/(2t_1)} = \lambda^{\alpha(q^2-1)/t_1}$ has order t_1, so $\epsilon^{t_1/2} = -1$.

Let $b = \lambda^{u(q-1)/2}$, so that $b^2 = c$. Then $x_1^t - c = (x^{t_1/2} - b)(x^{t_1/2} + b)$. Consider the ring $K[w_1]$, where w_1 has minimal polynomial $x^{t_1/2} - b$. Note that, as $\left(u\frac{q-1}{2}, \frac{t_1}{2}\right) = 1$ and $\frac{t_1}{2} | \frac{q^2-1}{2}$, the polynomials $x^{t_1/2} - b$ and $x^{t_1/2} + b$ are irreducible.

We have that $(w_1\epsilon)^{t_1/2} = -b$ and we may assume that $\mathrm{F}[w]$ is the direct product $\mathrm{F}[w_1] \times \mathrm{F}[w_1\epsilon] = \mathrm{F}[w_1] \times \mathrm{F}[w_1]$, as $\epsilon \in \mathrm{F}$. Moreover, we may assume that $w = (w_1, w_1\epsilon)$ and that $\mathrm{F} \leq \mathrm{F}[w]$ is identified with the subfield $\tilde{\mathrm{F}} = \{(a, a) \mid a \in \mathrm{F}\}$ of the direct product.

Define $\psi : \mathrm{F}[w] \to \mathrm{F}[w]$ by $(a_1, a_2)^\psi = (a_2^p, a_1^{p^{2mk+1}})$. For every $a \in \mathrm{F}$ we have that $(a, a)^\psi = (a^p, a^{p^{2mk+1}}) = (a^p, a^p) = (a, a)^p$, so that ψ acts on $\tilde{\mathrm{F}}$ as the p-th power π. In particular, the order of ψ is at least $2m$.

We also have that $(a_1, a_2)^{\psi^2} = (a_1^{p^{2mk+2}}, a_2^{p^{2mk+2}})$, so ψ^2 stabilizes $\mathrm{F}[w_1]$. Moreover, $\psi^{2m} = \pi^{(2mk+2)m} = \pi^{-2smt_1/2}$. But $\pi^{2mt_1/2}$ acts trivially on $\mathrm{F}[w_1]$, so ψ has order $2m$. Note that

$$w^\psi w^{-p} = (w_1, w_1\epsilon)^\psi (w_1, w_1\epsilon)^{-p} = (\epsilon^p, w_1^{p^{2mk+1}-p}\epsilon^{-p}) = (\epsilon, w_1^{p^{2mk}-1}\epsilon^{-1})^p$$

and

$$w_1^{p^{2mk}-1} = w_1^{q^{2k}-1} = w_1^{t_1(q^{2k}-1)/t_1} = c^{(q^{2k}-1)/t_1} = \epsilon^2.$$

Therefore $w^\psi w^{-p} = (\epsilon,\epsilon)^p$, that is,

$$w^\psi = (gz)^p, \quad z = (c^{(q^{2k}-1)/(2t_1)}, c^{(q^{2k}-1)/(2t_1)}) \in \tilde{\mathrm{F}} \cap \langle w\rangle. \qquad \square$$

Lemma 2.7. *With the hypotheses and notation of Lemma 2.6, there exist two matrices $g, h \in \mathrm{U}(t_1, q)$ such that $g^{t_1} = c$, $\det(g) = (-1)^{t_1-1}c$, $g^{\phi h} = (gz)^p$, where $z = c^{(q^{2k}-1)/t_1} \in \langle g\rangle$ if t_1 is odd, and $z = c^{(q^{2k}-1)/(2t_1)} \in \langle g\rangle$ if t_1 is even. Also, $(\phi h)^{2m} = 1$.*

Proof. We have that $E = \{1, w, w^2, \dots, w^{t_1-1}\}$ is a basis of $V = \mathrm{F}[w]$ as a vector space over F. The matrix g associated to r_w with respect to E is

$$g = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & & 0 \\ \vdots & & & \ddots & 0 \\ 0 & 0 & 0 & & 1 \\ c & 0 & & 0 & 0 \end{pmatrix}.$$

We have that $g \in \mathrm{U}(t_1, q)$, by the same argument as in Lemma 2.4. Also, $g^{t_1} = c$ and $\det(g) = (-1)^{t_1-1}c$. Note that ψ is a semilinear map associated with the automorphism ϕ of F. We have that $(w^i)^\psi = c^{\alpha_i}(w)^{i\sigma}$, where $\sigma \in \mathrm{Sym}(t_1)$. So ψ permutes the subspaces $\mathrm{F}\,w^i$. Let h be the matrix associated to the linear map which acts in the same way as ψ on the given basis. Then h is monomial. Also, $h(h^\top)^\sigma$ is a diagonal matrix with all non-zero entries of the form $c^{\alpha_i(q+1)} = \lambda^{\alpha_i u(q-1)(q+1)} = 1$, so $h \in \mathrm{U}(t_1, q)$.

Next, note that the group $\Gamma\mathrm{L}(V)$ of semilinear maps is isomorphic to $\Gamma\mathrm{L}(n, q)$ and, with respect to the chosen basis E, we have that ψ corresponds to ϕh, so $(\phi h)^{2m} = 1$. Also, $\langle \phi h\rangle \cap \mathrm{F}^* = 1$.

Finally, right multiplication by w^ψ is right multiplication by $(wz)^p$, so $g^{\phi h} = (gz)^p$. $\square$

Proposition 2.8. *Let $d_1 | d$, $d_1 = t_1 l_1$, where $t_1 = (d_1, t)$. Let $D \le \mathrm{PU}(n, q)$ be such that $G \le D$ and D/G has order d_1. If $(m, t_1) = 1$, then G has a complement in $\langle D, \bar{\phi}\rangle$.*

Proof. Take $v_1, \dots, v_{n/t_1} \in \mathrm{F}$ and $u \in \mathbb{Z}$ as in Lemma 2.3, and let $c = \lambda^{u(q-1)}$ and $c_j = cv_j$. Note that $c_j = \lambda^{u(q-1)+\alpha_j(q^2-1)/l_1}$ for some integer α_j, and as $(u, t_1) = 1$ and $t_1 | \frac{q^2-1}{l_1}$, we have that $(u + \alpha_j \frac{q^2-1}{l_1}, t_1) = 1$, so the hypotheses of Lemma 2.6 are satisfied. Now we may apply Lemma 2.7 and find matrices $g_j, h_j \in \mathrm{U}(t_1, q)$ such that $(\phi h_j)^{2m} = 1$, $g_j^{\phi h_j} = (g_j z_j)^p$, with $z_j \in \langle g_j\rangle$. If t_1 is odd, we have

$$z_j = c_j^{(q^{2k}-1)/t_1} = (cv_j)^{(q^{2k}-1)/t_1} = c^{(q^{2k}-1)/t_1}$$

for every $j = 1, \dots n/t_1$, as $l_1 \mid \frac{q^2-1}{t_1}$. If t_1 is even, we have

$$z_j = c_j^{(q^{2k}-1)/(2t_1)} = (cv_j)^{(q^{2k}-1)/(2t_1)} = c^{(q^{2k}-1)/(2t_1)}$$

for every $j = 1, \dots n/t_1$, as $l_1 \mid \frac{q^2-1}{2t_1}$ (where l_1 is odd). Also, $g_j^{d_1} = g_j^{t_1 l_1} = (cv_j)^{l_1} = c^{l_1}$.

Now consider the matrices

$$g = \begin{pmatrix} g_1 & & \\ & \ddots & \\ & & g_{n/t_1} \end{pmatrix}, \qquad h = \begin{pmatrix} h_1 & & \\ & \ddots & \\ & & h_{n/t_1} \end{pmatrix}.$$

We have that $g, h \in \mathrm{U}(n,q)$, $(\phi h)^{2m} = 1$ and $g^{\phi h} = (gz)^p$, where $z \in \mathrm{F} \cap \langle g \rangle$. Also, $g^{d_1} = c^{l_1}$ and

$$\det(g) = \prod_{j=1}^{n/t_1} \det(g_j) = \prod_{j=1}^{n/t_1} (-1)^{t_1-1} \lambda^{u(q-1)} v_j = \lambda^{(q-1)d/d_1}.$$

Then $\bar{C} = \langle \bar{g}, \bar{\phi}\bar{h} \rangle$ is the required complement. □

Combining Lemma 2.2 with the special case $d_1 = d$ of Proposition 2.8 we get:

THEOREM 2.9. $\mathrm{PSU}(n,q)$ *has a complement in* $\mathrm{Aut}(\mathrm{PSU}(n,q))$ *if and only if* $(\frac{q+1}{d}, d, m) = 1$.

3. Untwisted groups of Lie type

In the following, we denote by F_q the finite field of order $q = p^m$, with p a prime and m a positive integer. Moreover, we denote by λ a generator of the multiplicative group of F_q. Let Φ be a root system corresponding to a simple Lie algebra L over the complex field $\mathbb{C}$, and let us consider a fundamental system $\Pi = \{a_1, \dots, a_l\}$ in Φ. For any choice of Π and for any finite field F_q, we let $L(q)$ denote the corresponding finite group (where L denotes the type of the group; i.e., $L = A_l, B_l, C_l, D_l, E_6, E_7, E_8, F_4, G_2$).

We assume that for the various possible root systems the elements of Π are labelled in such a way that $(a,a) = 2$ and $(a,b) = 0$ for each pair of roots in

Π, with the following exceptions:

A_l : $(a_i, a_{i+1}) = -1$ for $1 \leq i \leq l-1$;
B_l : $(a_1, a_1) = 1$, $(a_i, a_{i+1}) = -1$ for $1 \leq i \leq l-1$;
C_l : $(a_i, a_i)=1, (a_i, a_{i+1}) = -1/2$ for $1 \leq i \leq l-2$,
$(a_{l-1}, a_{l-1}) = -(a_{l-1}, a_l) = 1$;
D_l : $(a_1, a_3) = (a_i, a_{i+1}) = -1$ for $2 \leq i \leq l-1$;
E_l : $(a_i, a_{i+1}) = (a_{l-3}, a_l) = -1$ for $1 \leq i \leq l-2$;
F_4 : $(a_1, a_1) = (a_2, a_2) = 1$, $(a_1, a_2) = -1/2$,
$(a_2, a_3) = (a_3, a_4) = -1$;
G_2 : $(a_1, a_1) = 2/3$, $(a_1, a_2) = -1$.

The Chevalley group $L(q)$, viewed as a group of automorphisms of a Lie algebra L_K over the field $K = \mathrm{F}_q$, obtained from a simple Lie algebra L over the complex field $\mathbb{C}$, is the group generated by certain automorphisms $x_r(t)$, where t runs over F_q and r runs over the root system Φ associated to L. For each $r \in \Phi$, $X_r = \{x_r(t) \mid t \in \mathrm{F}_q\}$ is a subgroup of $L(q)$ isomorphic to the additive group of the field. X_r is called a *root subgroup*, and the group $L(q)$ is generated by the root-subgroups X_r, $\pm r \in \Pi$. In the following we will use the notations and the terminology introduced in [1].

Let us recall some facts about the automorphism group of $L(q)$.

Any automorphism σ of the field F_q induces a *field automorphism* (also denoted by σ) of $L(q)$, defined by

$$(x_r(t))^\sigma = x_r(t^\sigma).$$

The set of the field automorphisms of $L(q)$ is a cyclic group of order m generated by the Frobenius automorphism ϕ.

We recall that a symmetry of the Dynkin diagram of $L(q)$ is a permutation ρ of the nodes of the diagram, such that the number of bonds joining nodes i, j is the same as the number of bonds joining nodes $i\rho, j\rho$, for any $i \neq j$. A non trivial symmetry ρ of the Dynkin diagram can be extended to a map of the space $\langle\Phi\rangle$ into itself, which we also denote by ρ. This map yields an outer automorphism ϵ of $L(q)$; ϵ is said to be a *graph automorphism* of $L(q)$. If $L(q)$ is $A_l(q)$, $l \geq 2$, $D_l(q)$ or $E_6(q)$, then $(x_r(t))^\epsilon = x_{r\rho}(\gamma_r t)$, where $r \in \Phi$, $t \in \mathrm{F}_q$, $\gamma_r \in \mathbb{Z}$. Moreover, the γ_r can be chosen so that $\gamma_r = 1$ if $r \in \Pi$, and $\gamma_r = -1$ if $-r \in \Pi$.

Let $P = \mathbb{Z}\Phi$ be the additive group generated by the roots in Φ; a homomorphism from P into the multiplicative group F_q^* will be called an F_q-character of P. From each F_q-character χ of P arises a *diagonal automorphism* $h(\chi)$ of $L(q)$ which maps $x_r(t)$ to $x_r(\chi(r)t)$. The automorphisms of the form $h(\chi)$ form an abelian subgroup $\hat{H}$ of the full automorphism group of $L(q)$. Now consider the additive group Q generated by the fundamental weights $\lambda_1, \ldots, \lambda_l$.

Any element of P is an integral combination of $\lambda_1, \dots, \lambda_l$. (More precisely, $a_i = \sum_{1 \le j \le l} A_{ji}\lambda_j$, where (A_{ij}) is the Cartan matrix of L.) Thus P is a subgroup of Q. Every F_q-character of Q gives rise to an F_q-character of P by restriction. However, an F_q-character of P need not be the restriction of some F_q-character of Q. More precisely, if an F_q-character of P, say χ, can be extended to an F_q-character of Q, then the automorphism $h(\chi)$ is inner, and vice versa. In the following we will often apply the above criterion to decide whether a diagonal automorphism $h(\chi)$ is inner; this will be done using the information coming from the Cartan matrix. Namely, if $\chi(a_i) = \lambda^{\alpha_i}$, $1 \le i \le l$, then χ can be extended to a F_q-character of Q by setting $\chi(\lambda_i) = \lambda^{\beta_i}$ for $1 \le i \le l$ if and only the integers $\beta_1, \dots, \beta_l$ satisfy the conditions $\alpha_i \equiv \sum_{1 \le j \le l} A_{ji}\beta_j \mod q-1$ for $1 \le i \le l$.

We denote by H the group of the diagonal automorphisms that are inner and by d the order of the abelian group $\hat{H}/H$. The value of d is given by the following table.

$L(q)$	d
$A_l(q)$	$(l+1, q-1)$
$B_l(q)$	$(2, q-1)$
$C_l(q)$	$(2, q-1)$
$D_l(q)$	$(4, q^l-1)$
$E_6(q)$	$(3, q-1)$
$E_7(q)$	$(2, q-1)$
$E_8(q)$	1
$G_2(q)$	1
$F_4(q)$	1

The main result about the automorphism group of $L(q)$ is as follows:

For each automorphism $\theta \in \mathrm{Aut}\, L(q)$ there exist an inner automorphism i, a diagonal automorphism h, a field automorphism f and a graph automorphism ϵ, such that $\theta = ihf\epsilon$; moreover,

$$L(q) \trianglelefteq \langle L(q), \hat{H} \rangle \trianglelefteq \langle L(q), \hat{H}, \phi \rangle \trianglelefteq \mathrm{Aut}\, L(q).$$

We will prove the following result:

THEOREM 3.1. *Suppose that $q = p^m$ and let $L(q)$ be an untwisted group of Lie type. Define $\tilde{q} = q^l$ if $L = D_l$, and $\tilde{q} = q$ otherwise. Then $L(q)$ has a complement in $\mathrm{Aut}\, L(q)$ if and only if the following condition is satisfied:*

$$(*) \qquad \left(\frac{\tilde{q}-1}{d}, d, m \right) = 1.$$

We have already proved that this is true for $A_l(q) \cong \mathrm{PSL}(l+1, q)$. In this section we discuss the remaining cases.

The subgroup $\langle L(q), \hat{H}\rangle$ of inner-diagonal automorphisms is always complemented in $\mathrm{Aut}\, L(q)$, so we only have to deal with the cases when $d \neq 1$.

We first prove that the condition $(*)$ is necessary in order for $L(q)$ to have a complement.

As had already been noticed by Pandya [6, Lemma 3.5], Lang's Theorem implies the following result.

Lemma 3.2. *Suppose that $L(q)$ has a complement X in $\mathrm{Aut}\, L(q)$. Then there exists $g \in L(q)$ such that the Frobenius automorphism ϕ belongs to X^g.*

Thus, if $L(q)$ has a complement X in $\mathrm{Aut}\, L(q)$, we may assume without loss of generality that $\phi \in X$. In particular, $Y = \langle L(q), \hat{H}\rangle \cap X$ is a subgroup of X isomorphic to $\hat{H}/H$ and normalized by ϕ. We will show that this is possible only if $(\tilde{q}-1/d, d, m) = 1$. To this end we use the Bruhat Decomposition. As is well known, if N is the normalizer of H in $L(q)$, then there exists a homomorphism from N onto the Weyl group W of L, with kernel H. For each $w \in W$ we fix an element $n_w \in N$ which maps to w under this homomorphism and such that $[n_w, \phi] = 1$. Let $U = \langle X_r \mid r \in \Pi\rangle$ and let U_w be the subgroup generated by those root subgroups X_r for which r is positive and rw is negative. Each element x of $\langle L(q), \hat{H}\rangle$ has a unique representation in the form $x = u_1 h(\chi) n_w u$, where $u_1 \in U$, $h(\chi) \in \hat{H}$, $w \in W$, $u \in U_w$.

Lemma 3.3. *Suppose that $L(q) = B_l(q), C_l(q)$, or $E_7(q)$ and that there exists a complement Y of $L(q)$ in $\langle L(q), \hat{H}\rangle$ normalized by the Frobenius automorphism ϕ. Then $(*)$ is satisfied.*

Proof. We may assume $d \neq 1$. Hence $d = (q-1, 2) = 2$ and $q = p^m$ with p an odd prime. In this case $Y = \langle x\rangle$, with $|x| = 2$. Using the Bruhat Decomposition we may write x in the form $x = u_1 h(\chi) n_w u$ with $u_1 \in U$ and $u \in U_w$. Then

$$x = x^\phi = u_1^\phi h(\chi)^\phi n_w^\phi u^\phi = u_1^\phi h(\chi)^\phi n_w u^\phi.$$

Note that $u_1^\phi \in U$ and $u^\phi \in U_w$, so by the uniqueness of the representation of x we deduce $h(\chi)^\phi = h(\chi)$, and this implies $\chi^p = \chi$. Since $x \notin L(q)$, we have $h(\chi) \in \hat{H} \setminus H$, which implies that there exists $1 \leq i \leq l$ with $\chi(a_i) = \lambda^s$ for an odd integer s. Therefore $sp \equiv s \bmod q-1$. Hence $(q-1)_2 \leq (p-1)_2$, and this is possible only if m is odd. To conclude the proof, it is enough to notice that if $d = 2$, then $(q-1/d, d, m) = 1$ if and only if m is odd. □

Lemma 3.4. *Suppose that $L(q) = D_l(q)$ with l even and that there exists a complement Y of $L(q)$ in $\langle L(q), \hat{H}\rangle$ normalized by the Frobenius automorphism ϕ. Then $(*)$ is satisfied.*

Proof. Again we may assume $d \neq 1$. In this case $d = 4$, $\hat{H}/H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ and ϕ centralizes $\hat{H}/H$. In particular, Y contains an element x of order 2 centralized by ϕ. Arguing as in Lemma 3.3, we deduce that m is odd, and this is equivalent to the condition that $(q^l - 1/4, 4, m) = 1$. □

LEMMA 3.5. *Suppose that $L(q) = D_l(q)$ with l odd and that there exists a complement Y of $L(q)$ in $\langle L(q), \hat{H}\rangle$ normalized by the Frobenius automorphism ϕ. Then $(*)$ is satisfied.*

Proof. Again it is enough to prove that either $d = 1$ or m is odd. Assume $d \neq 1$. Then $\hat{H}/H$ is cyclic of order $d \in \{2, 4\}$. Let x be a generator of Y. If $[\phi, x] = 1$ we may repeat the argument of Lemma 3.3 to deduce that m is odd. So assume that ϕ does not centralize x. This occurs only if $d = 4$, $p \equiv 3 \bmod 4$, and m is even. In this case we take an element $y \in Y$ of order 2 and write y in the form $y = u_1 h(\chi) n_w u$ with $u_1 \in U$ and $u \in U_w$. As ϕ centralizes y, using the uniqueness of this representation, we deduce $\chi^p = \chi$. Since $y \notin L(q)$, we have $h(\chi) \in \hat{H} \setminus H$, which implies that there exists $1 \leq i \leq l$ with $\chi(a_i) = \lambda^s$, for some integer s not divisible by 4. Therefore $sp \equiv s \bmod q - 1$. Hence $(q-1)_2 \leq (s(p-1))_2 \leq 4$, but this is impossible, since if $p \equiv 3 \bmod 4$ and m is even, then $q \equiv 1 \bmod 8$. □

LEMMA 3.6. *Suppose that $L(q) = E_6(q)$ and that there exists a complement Y of $L(q)$ in $\langle L(q), \hat{H}\rangle$ normalized by the Frobenius automorphism ϕ. Then $(*)$ is satisfied.*

Proof. In this case $d = (3, q-1)$ and $(*)$ is equivalent to the condition that either $d = 1$ or $(3, m) = 1$. Suppose that $d \neq 1$. $\hat{H}/H$ is cyclic of order 3. Let x be a generator of Y and write x in the form $x = u_1 h(\chi) n_w u$ with $u_1 \in U$ and $u \in U_w$. Since ϕ^2 centralizes x, arguing as in the proof of Lemma 3.3 we deduce $h(\chi)^{\phi^2} = h(\chi)$, and this implies $\chi^{p^2} = \chi$. Since $x \notin L(q)$, we have $h(\chi) \in \hat{H} \setminus H$, which implies that there exists $1 \leq i \leq 6$ with $\chi(a_i) = \lambda^s$ for an integer s not divisible by 3. Therefore $sp^2 \equiv s \bmod q - 1$. Hence $(q-1)_3 \leq (p^2 - 1)_3$, which implies $(3, m) = 1$. □

It remains to prove that if $(*)$ is satisfied, then $L(q)$ has a complement in $\operatorname{Aut} L(q)$. As we have already noticed, $\langle L(q), \hat{H}\rangle$ is always complemented in $\operatorname{Aut} L(q)$, so we only have to consider the case when $d \neq 1$.

We first recall the following useful result (see [1, Theorem 7.2.2]):

LEMMA 3.7. *If $n \in N$ and n maps to w under the natural homomorphism from N onto W, then $h(\chi)^n = h(\chi^w)$, where $\chi^w(r) = \chi(rw)$ for each $r \in \Phi$.*

For any $r \in \Phi$ let w_r be the reflection in the hyperplane orthogonal to r and let $n_r = x_r(1)x_{-r}(-1)x_r(1)$. Then $n_r \in N$ and n_r maps to w_r under the natural homomorphism from N onto W. In the following we write w_i, n_i in place of w_{a_i}, n_{a_i}, for any $a_i \in \Pi$.

LEMMA 3.8. *If $L(q) = B_l(q)$ and $(*)$ is satisfied, then there is a complement X of $L(q)$ in* $\operatorname{Aut} L(q)$.

Proof. We may assume $d = 2$ (in which case $L(q)$ has no graph automorphism). Let μ be a generator of the 2-Sylow subgroup of F_q^* and define χ by $\chi(a_1) = \mu$, $\chi(a_2) = \mu^{-1}$, and $\chi(a_i) = 1$ for $i > 2$. Consider the element $x = h(\chi)n_1$. We have $n_1^2 = h_1(-1) = 1$ (see [4, p. 20]), $\chi^{w_1}(a_1) = \chi(a_1 w_1) = \chi(-a_1) = \mu^{-1}$ and $\chi^{w_1}(a_2) = \chi(a_1 w_1) = \chi(2a_1 + a_2) = \mu$. Hence $x^2 = h(\chi)h(\chi)^{n_1} = h(\chi)h(\chi^{w_1}) = 1$. Moreover, since $(*)$ is satisfied, we have $(q-1)_2 = (p-1)_2$, so $\mu^p = \mu$ and $[x, \phi] = 1$. We claim that $x \notin L(q)$. Indeed, if $x \in L(q)$, then $h(\chi) \in H$, and χ could be extended to an F_q-character of Q; as $2\lambda_1 = la_1 + (l-1)a_2 + \cdots + a_l$, we would then have $\chi(\lambda_1)^2 = \chi(la_1 + (l-1)a_2) = \mu \in \mathrm{F}_q^2$, a contradiction. But then $X = \langle x, \phi\rangle$ is a complement for $L(q)$ in $\operatorname{Aut} L(q)$. □

LEMMA 3.9. *If $L(q) = C_l(q)$ and $(*)$ is satisfied, then there is a complement X of $L(q)$ in* $\operatorname{Aut} L(q)$.

Proof. We may assume $d = 2$. Let μ be a generator of the 2-Sylow subgroup of F_q^* and define χ by $\chi(a_i) = \mu$ if $i \equiv 1 \bmod 4$, $\chi(a_i) = \mu^{-1}$ if $i \equiv 3 \bmod 4$, $\chi(a_i) = 1$ if i is even and $i \neq l$, and $\chi(a_l) = \chi(a_{l-1})^{-1}$ if l is even. Let $n = n_1 n_3 \ldots n_k$ with $k = 2\left[\frac{l-1}{2}\right] + 1$ and consider the element $x = h(\chi)n$. Let $w = w_1 w_3 \ldots w_k$. Then $\chi^w(a_i) = \chi(a_i w) = \chi(-a_i)$ if i is odd, $\chi^w(a_i) = \chi(a_i w) = \chi(a_{i-1} + a_i + a_{i+1}) = 1$ if i is even and $i \neq l$, and $\chi^w(a_l) = \chi(a_l w) = \chi(2a_{l-1} + a_l) = \chi(a_l)^{-1}$ if l is even. Since $n^2 = h_1(-1)h_3(-1)\ldots h_k(-1) = 1$ (see [4, p. 20]), we have $x^2 = h(\chi)h(\chi)^n = h(\chi)h(\chi^w) = 1$. Moreover, since $(*)$ is satisfied, $(q-1)_2 = (p-1)_2$, so $\mu^p = \mu$ and $[x, \phi] = 1$. We claim that $x \notin L(q)$. Indeed, if $x \in L(q)$, then $h(\chi) \in H$, and χ could be extended to an F_q-character of Q; as $2\lambda_1 - a_l \in \langle 2a_1, 2a_2, \ldots, 2a_{l-1}\rangle$ we would then have $\chi(a_l) \equiv \chi(\lambda_1)^2 \bmod \mathrm{F}_q^2$, and hence $\chi(a_l) \in \mathrm{F}_q^2$, a contradiction. But then $X = \langle x, \phi\rangle$ is a complement for $L(q)$ in $\operatorname{Aut} L(q)$. □

LEMMA 3.10. *If $L(q) = E_7(q)$ and $(*)$ is satisfied, then there is a complement X of $L(q)$ in* $\operatorname{Aut} L(q)$.

Proof. We may assume $d = 2$. Let μ be a generator of the 2-Sylow subgroup of F_q^* and define χ by $\chi(a_1) = \chi(a_7) = \mu$, $\chi(a_3) = \mu^{-1}$, and $\chi(a_i) = 1$ otherwise. Let $n = n_1 n_3 n_7$ and consider the element $x = h(\chi)n$. Let $w = w_1 w_3 w_7$. Then $\chi^w(a_i) = \chi(a_i w) = \chi(-a_i)$ if $i \in \{1, 3, 7\}$, $\chi^w(a_i) = \chi(a_i w) = \chi(a_i) = 1$ if $i \in \{5, 6\}$, $\chi^w(a_2) = \chi(a_2 w) = \chi(a_1 + a_2 + a_3) = 1$, and $\chi^w(a_4) = \chi(a_4 w) = \chi(a_3 + a_4 + a_7) = 1$. Since $n^2 = h_1(-1)h_3(-1)h_7(-1) = 1$ (see

[4, p. 20]), we have $x^2 = h(\chi)h(\chi)^n = h(\chi)h(\chi^w) = 1$. Moreover, since $(*)$ is satisfied, $(q-1)_2 = (p-1)_2$, so $\mu^p = \mu$ and $[x, \phi] = 1$. We claim that $x \notin L(q)$. Indeed, if $x \in L(q)$, then $h(\chi) \in H$, and χ could be extended to an F_q-character of Q; as $2\lambda_1 = 3a_1 + 4a_2 + 5a_3 + 6a_4 + 4a_5 + 2a_6 + 3a_7$, we would then have $\chi(\lambda_1)^2 = \chi(3a_1 + 5a_3 + 3a_7) = \mu \in \mathrm{F}_q^2$, a contradiction. But then $X = \langle x, \phi \rangle$ is a complement for $L(q)$ in $\mathrm{Aut}\, L(q)$. ☐

LEMMA 3.11. *If $L(q) = E_6(q)$ and $(*)$ is satisfied, then there is a complement X of $L(q)$ in* $\mathrm{Aut}\, L(q)$.

Proof. We may assume $d = 3$. Consider the subgroup $S = \langle X_{a_i}, X_{-a_i} \mid 1 \leq i \leq 5 \rangle$ of $E_6(q)$ and let T be the subgroup of $\mathrm{Aut}\, E_6(q)$ consisting of the elements of the form $sh(\chi)$ with $s \in S$ and $\chi(a_6) = 1$. Let $Z = Z(S)$. Then Z is cyclic of order 2, generated by $z = h_{a_1}(-1)h_{a_3}(-1)h_{a_5}(-1)$. Moreover, $S \cong \mathrm{SL}(6, q)/\langle \omega \rangle$ with ω a primitive 3rd root of unity in F_q, $S/Z \cong A_5(q) \cong \mathrm{PSL}(6, q)$, T normalizes S and acts by conjugation on $S/Z \cong A_5(q)$ as the group of the inner-diagonal automorphism of $A_5(q)$. We have proved in Proposition 1.11 that if $(*)$ is satisfied, then there exist $g_1 \in \mathrm{GL}(6, q) \setminus \mathrm{SL}(6, q)$ and $g_2 \in \mathrm{SL}(6, q)$ such that $(\iota g_2)^2 = 1$, $[\iota g_2, \phi] = 1$, ϕ and ιg_2 normalize $\langle g_1 \rangle$ and $g_1^3 \in Z(\mathrm{SL}(6, q))$. Thus there exist an element $y \in S$, centralized by ϕ and such that $y\epsilon$ has order 2 (where ϵ is the graph automorphism of $L(q)$), and an element $x = sh(\chi) \in T$ such that $x \notin S$, $x^3 \in Z$, and $\langle x \rangle$ is normalized by ϕ and by $y\epsilon$. We claim that $X = \langle x^2, \phi, y\epsilon \rangle$ is a complement for $L(q)$ in $\mathrm{Aut}\, L(q)$. We only have to prove that $x^2 \notin L(q)$. Since $x \notin S$, we have $\chi(a_1)\chi(a_2)^{-1}\chi(a_4)\chi(a_5)^{-1} \notin \mathrm{F}_q^3$. If $x^2 \in L(q)$, then $h(\chi^2) \in H$, and χ^2 could be extended to a F_q-character $\bar{\chi}$ of Q; as $3\lambda_1 = 4a_1 + 5a_2 + 6a_3 + 4a_4 + 2a_5 + 3a_6$, we would then have $(\chi(a_1)\chi(a_2)^{-1}\chi(a_4)\chi(a_5)^{-1})^2 \equiv \bar{\chi}(\lambda_1)^3 \bmod \mathrm{F}_q^3$, a contradiction. ☐

LEMMA 3.12. *If $L(q) = D_l(q)$ with l even and $(*)$ is satisfied, then there is a complement X of $L(q)$ in $\langle L(q), \hat{H} \rangle$, which is normalized by the Frobenius and the graph automorphisms.*

Proof. We may assume $d \neq 1$. In this case $\hat{H}/H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Moreover, if χ is an F_q-character of P with $\chi(a_i) = 1$ for $i > 4$ then $h(\chi) \in H$ only if $\chi(a_i)\chi(a_j) \in \mathrm{F}_q^2$ for each $(i, j) \in \{(1, 2, 4)\}^2$. Let μ be a generator of the Sylow 2-subgroup of the multiplicative group of the field F_q. For $i \in \{1, 2, 4\}$ let χ_i be the F_q-character of P defined by $\chi_i(a_3) = \mu^{-1}$, $\chi_i(a_i) = 1$, and $\chi_i(a_j) = \mu$ if $j \notin \{i, 3\}$. Consider the elements $x_1 = h(\chi_1)n_2n_4$, $x_2 = h(\chi_2)n_1n_4$, and $x_4 = h(\chi_4)n_1n_2$, It can be easily verified that x_1, x_2, x_4 generate a complement X of $L(q)$ in $\langle L(q), \hat{H} \rangle$. Since $(q - 1/2, 2, m) = 1$, $(q-1)/(p-1)$ is odd and $\mu^\phi = \mu$. This implies that X is centralized by the field automorphisms. Any graph automorphism ϵ of $D_l(q)$ arises from a permutation of the roots a_1, a_2 when $l \neq 4$, and from a permutation of the roots a_1, a_2, a_4 when $l = 4$. This automorphism ϵ permutes in the same way the three generators x_1, x_2, x_4 of X, so X is normalized by the graph automorphisms. □

LEMMA 3.13. *If $L(q) = D_l(q)$ with l odd and $(*)$ is satisfied, then there is a complement X of $L(q)$ in* $\operatorname{Aut} L(q)$.

Proof. We may assume $d = (4, q-1) \neq 1$. We first deal with the case $d = 2$. Consider the subgroup $S = \langle X_{a_i}, X_{-a_i} \mid 1 \leq i \leq 3\rangle$ of $D_l(q)$ and let T be the subgroup of $\operatorname{Aut} D_l(q)$ consisting of the elements of the form $sh(\chi)$ with $s \in S$ and $\chi(a_i) = 1$ for $i \geq 4$. Then $S \cong A_3(q) \cong \mathrm{PSL}(4, q)$ and T acts by conjugation on S as the group of the inner-diagonal automorphism of S. We have proved in Theorem 1.12 that if $(*)$ is satisfied, then there exists a complement $\langle x\rangle$ of $\mathrm{PSL}(4, q)$ in $\mathrm{PGL}(4, q)$, normalized by ϕ and ι. When we identify $\mathrm{PSL}(4, q)$ with $A_3(q)$, the automorphism ι can be written as the product of an inner automorphism centralized by ϕ with the graph automorphism. Note that the graph automorphism ϵ of $D_l(q)$ centralizes the root subgroup $X_{a_i}, 3 \leq i \leq l$, and acts on T as the graph automorphism of $A_3(q)$. Thus there exist an element $y \in S$, centralized by ϕ and such that $y\epsilon$ has order 2, and an element $x = sh(\chi) \in T$ of order d modulo S, which generate a subgroup normalized by $y\epsilon$ and ϕ. We claim that $X = \langle x, \phi, y\epsilon\rangle$ is a complement for $L(q)$ in $\operatorname{Aut} L(q)$. We only have to prove that $x \notin L(q)$. Since $x \notin S$, we have $\chi(a_1)\chi(a_2) \notin \mathrm{F}_q^2$. If $x \in L(q)$, then χ could be extended to a F_q-character $\bar\chi$ of Q; as $4\lambda_1 \in a_1 + a_2 + 2\langle a_1, a_2, a_3, a_4, \ldots, a_l\rangle$, we would then have $\chi(a_1)\chi(a_2) \equiv \bar\chi(\lambda_1)^4 \bmod \mathrm{F}_q^2$, which implies $\chi(a_1)\chi(a_2) \in \mathrm{F}_q^2$, a contradiction.

Now assume $d = (q-1, 4) = 4$. Let μ be a generator of the 2-Sylow subgroup of F_q^* and define χ by $\chi(a_2) = \mu$, $\chi(a_1) = \chi(a_3) = 1$, $\chi(a_i) = 1$ if i is even and $i \neq 2$, $\chi(a_i) = -\mu^{-1}$ if i is odd, $i > 3$ and $i \equiv 1 \bmod 4$, and $\chi(a_i) = -\mu$ if i is odd, $i > 3$ and $i \equiv 3 \bmod 4$. Let $n = n_1n_3n_2n_5n_7\ldots n_l$ and consider the element $x = h(\chi)n$. Since $n^4 = 1$, we have $x^4 = (h(\chi)n)^4 = h(\chi)h(\chi)^n h(\chi)^{n^2} h(\chi)^{n^3} = h(\chi\chi^w\chi^{w^2}\chi^{w^3})$, where $w = w_1w_3w_2w_5w_7\ldots w_l$. But $a_i(1 + w + w^2 + w^3) = 0$ if i is odd or $i = 2$, $a_4(1 + w + w^2 + w^3) = 2(a_1 + a_2 + 2a_3 + 2a_4 + a_5)$ and $a_i(1 + w + w^2 + w^3) = 2(a_{i-1} + 2a_i + a_{i+1})$ if i is even and $i > 4$. Hence $\chi\chi^w\chi^{w^2}\chi^{w^3} = 1$ and $x^4 = 1$. Moreover, $x^\epsilon x = h(\chi)^\epsilon n^\epsilon h(\chi)n = h(\chi)^\epsilon h_5(-1)h_7(-1)\ldots h_l(-1)h(\chi)^n = h(\bar\chi\psi\chi^w)$, where $\bar\chi(a_1) = \chi(a_2)$, $\bar\chi(a_2) = \chi(a_1)$, and $\bar\chi(a_i) = \chi(a_i)$ otherwise, $\psi(a_4) = -1$, and $\psi(a_i) = 1$ otherwise. Now,

$$\bar\chi\psi\chi(a_1) = \chi(a_2)\chi(a_1w) = \chi(a_2)\chi(-a_1 - a_2 - a_3) = 1,$$
$$\bar\chi\psi\chi(a_2) = \chi(a_1)\chi(a_2w) = \chi(a_3) = 1,$$
$$\bar\chi\psi\chi(a_3) = \chi(a_3)\chi(a_3w) = \chi(a_1) = 1,$$
$$\bar\chi\psi\chi(a_4) = \chi(a_4)\chi(a_4w) = -\chi(a_2 + a_3 + a_4 + a_5) = 1,$$
$$\bar\chi\psi\chi(a_i) = \chi(a_i)\chi(a_iw) = \chi(a_i)\chi(-a_i) = 1 \text{ if } i \text{ is odd, } i \geq 5,$$

$$\bar{\chi}\psi\chi(a_i) = \chi(a_i)\chi(a_i w) = \chi(a_i)\chi(a_{i-1} + a_i + a_{i+1}) = 1 \quad \text{if } i \text{ is even, } i \geq 6.$$

Hence we conclude $x^\epsilon = x^{-1}$. Moreover, since $(*)$ is satisfied, we have $(q-1)_2 = (p-1)_2$, so $\mu^p = \mu$ and $[x, \phi] = 1$. We claim that $x^2 \notin L(q)$. Since $x^2 \notin S$, we have $\chi(a_1)\chi(a_2) \notin \mathrm{F}_q^2$. If $x^2 \in L(q)$, then χ^2 could be extended to a F_q-character $\bar{\chi}$ of Q; as $4\lambda_1 \in a_1 + a_2 + 2\langle a_1, a_2, a_3, a_4, \ldots, a_l\rangle$, we would then have $\mu^2 = \chi(a_1)^2\chi(a_2)^2 \equiv \bar{\chi}(\lambda_1)^4 \bmod \mathrm{F}_q^4$, a contradiction. But then $X = \langle x, \phi, \epsilon\rangle$ is a complement for $L(q)$ in $\operatorname{Aut} L(q)$. □

4. Twisted groups of Lie type

We begin with a short description of the twisted groups. Let $G = L(q^s)$ be a group of Lie type whose Dynkin diagram has a non trivial symmetry ρ of order s. If ϵ is the graph automorphism corresponding to ρ, let us suppose that $L(q^s)$ admits a non trivial field automorphism α such that the automorphism $\sigma = \epsilon\alpha$ satisfies $\sigma^s = 1$. If such an automorphism σ does exist, the twisted group ${}^sL(q)$ is defined as the subgroup of the group $L(q^s)$ which is fixed elementwise by σ. The structure of ${}^sL(q)$ is very similar to that of a Chevalley group: if Φ is the root-system fixed in $L(q^s)$, the automorphism σ determines a partition of $\Phi = \cup S_i$. If R is an element of the partition, we denote by X_R the subgroup $\langle X_r \mid r \in R\rangle$ of $L(q^s)$, and by X_R^1 the subgroup $\{x \in X_R, \mid x^\sigma = x\}$ of ${}^sL(q)$. The group ${}^sL(q)$ is generated by the groups $X_{S_i}^1$, $\Phi = \cup S_i$; in fact, the subgroups X_R^1 play the role of the root-subgroups. An element R of the partition which contains a simple root is said to be a *simple set*. We have $\operatorname{Aut}({}^sL(q)) = \langle {}^sL(q), \hat{H}^1, \phi\rangle$, where ϕ is the Frobenius automorphism and $\hat{H}^1 = N_{\hat{H}}({}^sL(q))$. Note that $h(\chi) \in \hat{H}^1$ if and only if $\chi(r\rho) = \chi(r)^\alpha$ for any $s \in \Phi$. Moreover, a diagonal automorphism $h \in \hat{H}^1$ is inner if and only if $h \in H^1 = H \cap {}^sL(q)$. Let d be the order of $\hat{H}^1/H^1$. Then $d = 1$ except in the following cases:

${}^sL(q)$	d
${}^2A_l(q)$	$(l+1, q+1)$
${}^2D_l(q)$	$(4, q^l+1)$
${}^2E_6(q)$	$(3, q+1)$

We will prove the following result:

Theorem 4.1. *Suppose that $q = p^m$ and let ${}^sL(q)$ a twisted group of Lie type.*

1. *If ${}^sL(q) \neq {}^2D_l(q)$, then ${}^sL(q)$ has a complement in* $\operatorname{Aut}{}^sL(q)$ *if and only if $\left(\frac{q+1}{d}, d, m\right) = 1$.*
2. *If l is odd, then ${}^2D_l(q)$ has a complement in* $\operatorname{Aut}{}^2D_l(q)$ *for any choice of q.*

(3) *If l is even, then ${}^2D_l(q)$ has a complement in* $\mathrm{Aut}\,{}^2D_l(q)$ *if and only if* $d = 1$.

We have already shown that this is true for ${}^2A_l(q) \cong \mathrm{PSU}(l+1, q)$. When $d = 1$, $\langle\phi\rangle$ is a complement for ${}^sL(q)$ in $\mathrm{Aut}^s L(q)$, so we only have to deal with the cases ${}^2D_l(q)$ and ${}^2E_6(q)$.

Lemma 4.2. *If l is odd, there exists a complement X of ${}^2D_l(q)$ in* $\mathrm{Aut}\,{}^2D_l(q)$.

Proof. We may assume $d \neq 1$. First suppose $d = (q^l + 1, 4) = 2$ and note that this implies $(\frac{q+1}{2}, 2, m) = 1$. Consider the simple sets $R_1 = \{a_1, a_2\}$, $R_2 = \{-a_1, -a_2\}$, $R_3 = \{a_3\}$, $R_4 = \{-a_3\}$. Let $S = \langle X^1_{R_1}, X^1_{R_2}, X^1_{R_3}, X^1_{R_4}\rangle \leq {}^2D_l(q)$ and let T be the subgroup of $\mathrm{Aut}\,{}^2D_l(q)$ consisting of the elements of the form $sh(\chi)$ with $s \in S$, $h(\chi) \in \hat{H}^1$ and $\chi(a_i) = 1$ for $i \geq 4$. Then $S \cong {}^2A_3(q) \cong \mathrm{PSU}(4, q)$ and T acts by conjugation on S as the group of the inner-diagonal automorphism of S. Since $(\frac{q+1}{2}, 2, m) = 1$, by Theorem 2.9 $\mathrm{PSU}(4, q)$ has a complement in $\mathrm{Aut}(\mathrm{PSU}(4, q))$. Therefore there exist $t = s_1 h(\chi) \in T$ and $s_2 \in S$ such that $\langle t\rangle$ is a complement for S in T normalized by $s_2\phi$ and $|s_2\phi| = |\phi|$. We claim that $X = \langle t, s_2\phi\rangle$ is a complement for ${}^2D_l(q)$ in $\mathrm{Aut}\,{}^2D_l(q)$. We only have to prove that $t \notin {}^2D_l(q)$. Since $t \notin S$, we have $\chi(a_1) \notin (\mathrm{F}_{q^2})^2$. If $t \in {}^2D_l(q)$, then χ could be extended to an F_{q^2}-character $\bar{\chi}$ of Q satisfying $\bar{\chi}(\lambda_2) = \bar{\chi}(\lambda_1)^q$. As $2(\lambda_1 - \lambda_2) = a_1 - a_2$, we would then have $\bar{\chi}(\lambda_1)^{2(q-1)} = \chi(a_1)^{q-1}$, which implies $\chi(a_1) \in (\mathrm{F}_{q^2})^2$, a contradiction.

Now assume $d = (q^l + 1, 4) = 4$. Let μ be a generator of the 2-Sylow subgroup of $\mathrm{F}^*_{q^2}$ and define χ by $\chi(a_1) = \mu$, $\chi(a_2) = \mu^q$, $\chi(a_3) = -1$, and $\chi(a_i) = 1$ otherwise. Let $n = n_3 n_1 n_2 n_5 n_7 \ldots n_l$ and consider the element $x = h(\chi)n$. Since $[n, \phi] = [n, \epsilon] = 1$, we have $x \in {}^2D_l(q)$. Arguing as in the proof of Lemma 3.13 it can be shown that $x^4 = 1$. Now let $y = n_1 n_2 \phi$. We claim that $x^y = x^{-1}$. Indeed, $x^y x = (h(\chi)n)^y h(\chi)n = h(\chi)^{n_1 n_2 \phi} n^{n_1 n_2} h(\chi)n = h(\chi^\phi)^{n_1 n_2} h_3(-1)h_5(-1)\ldots h_l(-1)h(\chi)^n = h((\chi^\phi)^{w_1 w_2}\psi\chi^n)$, where $\psi(a_1) = \psi(a_2) = -1$, and $\psi(a_i) = 1$ otherwise, and $w = w_3 w_1 w_2 w_5 w_7 \ldots w_l$. Let $\bar{\chi} = (\chi^\phi)^{w_1 w_2}\psi\chi^n$. Then

$$\bar{\chi}(a_1) = -\chi(a_1 w_1 w_2)^p \chi(a_1 w) = -\chi(-a_1)^p \chi(a_2 + a_3) = \mu^{q-p} = 1,$$
$$\bar{\chi}(a_2) = -\chi(a_2 w_1 w_2)^p \chi(a_2 w) = -\chi(-a_2)^p \chi(a_1 + a_3) = \mu^{1-pq} = 1,$$
$$\bar{\chi}(a_3) = \chi(a_3 w_1 w_2)^p \chi(a_3 w) = \chi(a_1 + a_2 + a_3)^p \chi(-a_1 - a_2 - a_3) = \mu^{(q+1)(p-1)} = 1,$$
$$\bar{\chi}(a_4) = \chi(a_4 w_1 w_2)^p \chi(a_4 w) = \chi(a_4)^p \chi(a_1 + a_2 + a_3 + a_4 + a_5) = -\mu^{q+1} = 1,$$
$$\bar{\chi}(a_i) = \chi(a_i w_1 w_2)^p \chi(a_i w) = \chi(a_i)^p \chi(-a_i) = 1 \text{ if } i \text{ is odd, } i \geq 5,$$

$$\bar{\chi}(a_i) = \chi(a_i w_1 w_2)^p \chi(a_i w) = \chi(a_i)^p \chi(a_{i-1} + a_i + a_{i+1}) = 1 \quad \text{if } i \text{ is even, } i > 4.$$

We claim that $\langle x, n_1 n_2 \phi\rangle$ is a complement for ${}^2D_l(q)$ in $\mathrm{Aut}\,{}^2D_l(q)$. We only have to prove that $x^2 \notin {}^2D_l(q)$. If $x^2 \in {}^2D_l(q)$, then χ^2 could be extended to a F_{q^2}-character $\bar{\chi}$ of Q satisfying $\bar{\chi}(\lambda_2) = \bar{\chi}(\lambda_1)^q$. As $2(\lambda_1 - \lambda_2) = a_1 - a_2$, we have $\bar{\chi}(\lambda_1)^{2(q-1)} = \mu^{2(q-1)}$. Moreover, from $\lambda_1 + \lambda_2 = \frac{l-1}{2}(a_1 + a_2) + (l-2)a_3 + \cdots + a_l$ we deduce $\bar{\chi}(\lambda_1)^{q+1} \in (\mathrm{F}_{q^2})^{2(q+1)}$, so

$$\mu^{\frac{q^2-1}{2}} = \mu^{2(q-1)\frac{q+1}{4}} = \bar{\chi}(\lambda_1)^{2(q-1)\frac{q+1}{4}} = 1,$$

which is again a contradiction. □

Lemma 4.3. *If l is even and q is odd, then ${}^2D_l(q)$ has no complement in* $\mathrm{Aut}\,{}^2D_l(q)$.

Proof. Assume that X is a complement of ${}^2D_l(q)$ in $\mathrm{Aut}\,{}^2D_l(q)$. We may assume $X = \langle x, \phi y\rangle$, where $y \in {}^2D_l(q)$ and x is an inner-diagonal automorphism of ${}^2D_l(q)$ of order 2, centralized by ϕy. We may write $x = h(\chi)z$, with $z \in {}^2D_l(q)$, $\chi(a_1) = \lambda$, $\chi(a_2) = \lambda^q$, and $\chi(a_i) = 1$ for $i \geq 3$ (where λ is a generator of $\mathrm{F}^*_{q^2}$). The inner diagonal automorphism group $\langle {}^2D_l(q), \hat{H}^1\rangle$ can be viewed as a subgroup of $\langle D_l(q^2), \hat{H}\rangle$. We claim that $h(\chi) \notin H$. Indeed, if $h(\chi) \in H$, then χ could be extended to an F_{q^2}-character of Q; as $2\lambda_1 \in a_1 + \langle a_1 + a_2, a_3, \ldots, a_l\rangle$ we would then have $\lambda = \chi(a_1) \in (\mathrm{F}_{q^2})^2$, a contradiction. This implies that $x \notin D_l(q^2)$. By Lang's Theorem there exists $g \in D_l(q^2)$ with $(\phi y)^g = \phi$. In particular, $x^g \in \langle D_l(q^2), \hat{H}\rangle \setminus D_l(q^2)$ and is centralized by ϕ. Using the Bruhat Decomposition in $D_l(q^2)$ we may write x^g in the form $x^g = u_1 h(\chi_1) n_w u$ with $u_1 \in U$ and $u \in U_w$. Then

$$x^g = (x^g)^\phi = u_1^\phi h(\chi_1)^\phi n_w^\phi u^\phi = u_1^\phi h(\chi_1)^\phi n_w u^\phi.$$

Note that $u_1^\phi \in U$ and $u^\phi \in U_w$, so, by the uniqueness of the representation of x^g, we deduce $h(\chi_1)^\phi = h(\chi_1)$, and this implies $\chi_1^p = \chi_1$. Since $x^g \notin D_l(q^2)$, we have $h(\chi_1) \in \hat{H} \setminus H$, which implies that there exists $1 \leq i \leq l$ with $\chi(a_i) = \lambda^s$, for an odd integer s. Therefore $sp \equiv s \bmod q^2 - 1$. Hence $(q^2-1)_2 \leq (p-1)_2$, but this is impossible. □

Lemma 4.4. *If ${}^2E_6(q)$ has a complement in* $\mathrm{Aut}\,{}^2E_6(q)$*, then* $\left(\frac{q+1}{d}, d, m\right) = 1$.

Proof. In this case $d = (3, q+1)$ and $\left(\frac{q+1}{d}, d, m\right) = 1$ is equivalent to the condition that either $d = 1$ or $(3, m) = 1$. Suppose that $d \neq 1$. Assume that X is a complement of ${}^2E_6(q)$ in $\mathrm{Aut}\,{}^2E_6(q)$. We may assume $X = \langle x, \phi y\rangle$, where $y \in {}^2E_6(q)$ and x is an inner-diagonal automorphism of ${}^2E_6(q)$ of order 3, centralized by $(\phi y)^2$. We may write $x = \chi(h)z$, with $z \in {}^2E_6(q)$, $\chi(a_1) = \lambda$,

$\chi(a_5)=\lambda^q$, and $\chi(a_i)=1$ otherwise (where λ is a generator of $\mathrm{F}_{q^2}^*$). The inner diagonal automorphism group $\langle {}^2E_6(q), \hat{H}^1\rangle$ can be viewed as a subgroup of $\langle E_6(q^2), \hat{H}\rangle$. We claim that $h(\chi)\notin H$. Indeed, if $h(\chi)\in H$, then χ could be extended to an F_{q^2}-character of Q; as $3\lambda_1 = 4a_1+5a_2+6a_3+4a_4+2a_5+3a_6$, we would then have $\chi(\lambda_1)^3=\lambda^{4+2q}$, which implies $\lambda\in(\mathrm{F}_{q^2})^3$, a contradiction. This implies that $x\notin E_6(q^2)$. By Lang's Theorem there exists $g\in E_6(q^2)$ with $(\phi y)^g=\phi$. In particular, $x^g\in\langle E_6(q^2),\hat{H}\rangle\setminus E_6(q^2)$ and is centralized by ϕ^2. Using the Bruhat Decomposition in $E_6(q^2)$ we may write x^g in the form $x^g=u_1h(\chi_1)n_w u$ with $u_1\in U$ and $u\in U_w$. Arguing as in the previous lemma we deduce that $h(\chi_1)^{\phi^2}=h(\chi_1)$, and this implies $\chi_1^{p^2}=\chi_1$. Since $x^g\notin E_6(q^2)$, we have $h(\chi_1)\in\hat{H}\setminus H$, which implies that there exists $1\le i\le 6$ with $\chi(a_i)=\lambda^s$ for some integer s not divisible by 3. Therefore $sp^2\equiv s \bmod q^2-1$. Hence $(q^2-1)_3\le(p^2-1)_3$, which implies $(m,3)=1$ (for otherwise $(q^2-1)_3 = (q+1)_3=(p+1)_3(1-p+\cdots+p^{m-1})_3>(p+1)_3=(p^2-1)_3$). □

Lemma 4.5. *If* $\left(\frac{q+1}{d},d,m\right)=1$, *then there is a complement of* ${}^2E_6(q)$ *in* $\mathrm{Aut}\,{}^2E_6(q)$.

Proof. We may assume $d=3$. Consider the simple sets $R_1=\{a_1,a_5\}$, $R_2=\{-a_1,-a_5\}$, $R_3=\{a_2,a_4\}$, $R_4=\{-a_2,-a_4\}$, $R_5=\{a_3\}$, $R_6=\{-a_3\}$. Let $S=\langle X^1_{R_i}\mid 1\le i\le 6\rangle\le {}^2E_6(q)$ and let T be the subgroup of $\mathrm{Aut}\,{}^2E_6(q)$ consisting of the elements of form $sh(\chi)$ with $s\in S$, $h(\chi)\in\hat{H}^1$ and $\chi(a_6)=1$. Let $Z=Z(S)$. Then Z is cyclic of order 2, generated by $z=h_{a_1}(-1)h_{a_3}(-1)h_{a_5}(-1)$. Moreover, $S\cong \mathrm{SU}(6,q)/\langle\omega\rangle$ with ω a primitive 3rd root of unity in F_{q^2}, $S/Z\cong {}^2A_5(q)\cong \mathrm{PSU}(6,q)$, T normalizes S and acts by conjugation on $S/Z\cong A_5(q)$ as the group of the inner-diagonal automorphism of $A_5(q)$. We have proved in Proposition 2.8 that if $\left(\frac{q+1}{d},d,m\right)=1$, then there exist $g_1\in \mathrm{U}(6,q)\setminus\mathrm{SU}(6,q)$ and $g_2\in\mathrm{SU}(6,q)$ such that $|\phi g_2|=|\phi|=2m$, ϕg_2 normalizes $\langle g_1\rangle$ and $g_1^3\in Z(\mathrm{SL}(6,q))$. Thus there exist an element $y\in S$ and an element $x=sh(\chi)\in T$ such that $x\notin S$, $x^3\in Z$, $\langle x\rangle$ is normalized by ϕy and $|\phi y|=|\phi|=2m$. We claim that $X=\langle x^2,\phi y\rangle$ is a complement for ${}^2E_6(q)$ in $\mathrm{Aut}\,{}^2E_6(q)$. We only have to prove that $x^2\notin L(q)$. Since $x\notin S$, we have $\chi(a_1)\chi(a_2)^{-1}\notin \mathrm{F}_q^3$. If $x^2\in L(q)$, then $h(\chi^2)\in\hat{H}$, and χ^2 could be extended to an F_q-character $\bar{\chi}$ of Q; as $3\lambda_1=4a_1+5a_2+6a_3+4a_4+2a_5+3a_6$, we would then have $(\chi^2(a_1)\chi^2(a_2)^{-1})^{q-1}\equiv\bar{\chi}(\lambda_1)^3 \bmod \mathrm{F}_q^3$, a contradiction. □

References

[1] R.W. Carter, *Simple groups of Lie type*, Pure and Applied Mathematics, vol. 28, John Wiley & Sons, London-New York-Sydney, 1972.

[2] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, and R.A. Wilson, *Atlas of finite groups. Maximal subgroups and ordinary characters for simple groups*, Oxford University Press, Eynsham, 1985.

[3] J. Dieudonné *La géométrie des groupes classiques*, Second edition, Springer-Verlag, Berlin-Göttingen-Heidelberg, 1963.

[4] D. Gorenstein, R. Lyons, and R. Solomon, *The classification of the finite simple groups. Number 3. Part I. Chapter A. Almost simple K-groups*, Mathematical Surveys and Monographs, vol. 40.3, American Mathematical Society, Providence, RI, 1998.

[5] N. Jacobson, *Basic algebra I*, Second edition, W. H. Freeman and Company, New York, 1985.

[6] G.N. Pandya, *Algebraic groups and automorphisms of finite simple Chevalley groups*, J. Number Theory **6** (1974), 239–247.

[7] ———, *On automorphisms of finite simple Chevalley groups*, J. Number Theory **6** (1974), 171–184.

A. Lucchini, Dipartimento di Matematica, Università degli Studi di Brescia, Via Valotti 9, 25133 Brescia, Italy

E-mail address: `lucchini@bsing.ing.unibs.it`

F. Menegazzo, Dipartimento di Matematica Pura e Applicata, Università di Padova, via Belzoni 7, 35131 Padova, Italy

E-mail address: `federico@math.unipd.it`

M. Morigi, Dipartimento di Matematica, Università di Bologna, Piazza di Porta S.Donato 5, 40127 Bologna, Italy

E-mail address: `mmorigi@dm.unibo.it`