JOURNAL OF ALGEBRA 171, 113–151 (1995)

The Group of Autoprojectivities of $SL_3(\bar{\mathbf{F}}_p)$ and $PGL_3(\bar{\mathbf{F}}_p)$

MAURO COSTANTINI

Dipartimento di Matematica Pura ed Applicata, Università di Padova, via Belzoni 7, 35131 Padova, Italy

Communicated by Walter Feit

Received January 25, 1993

INTRODUCTION

Given a group G, an *autoprojectivity* of G is an automorphism of the lattice of all subgroups of G. We denote by Aut $L(G)$ the group of all autoprojectivities of G. Every automorphism α of G induces in a natural way the autoprojectivity α^* of G given by $X^{\alpha^*} = X^\alpha$ for every $X \leq G$. We have therefore a homomorphism $*$: Aut $G \to$ Aut $L(G)$ given by $\alpha \mapsto \alpha^*$ for every α in Aut G.

An interesting problem in the study of a given group G, from its subgroup lattice point of view, is whether or not every autoprojectivity of G is induced by an automorphism, that is, if $*$ is surjective or not.

Studying this problem for a simple algebraic group G over the algebraic closure $\bar{\mathbf{F}}_p$ of a finite field, we showed in [5, Corollary 4.9] that $*$ is surjective if and only if the kernel $\Gamma(G)$ of the action of Aut $L(G)$ on the canonical building associated to G coincides with the identity subgroup of Aut $L(G)$ (following Völklein [16] we call the elements of $\Gamma(G)$ *exceptional* autoprojectivities of G). Then we proved in [6, Theorems A, B, C] that this is the case if p is odd and G is not of type A_2. In the present paper we consider the case when G has type A_2, i.e., when G is isomorphic either to $SL_3(\bar{\mathbf{F}}_p)$ or to $PGL_3(\bar{\mathbf{F}}_p)$, with no restriction on p. This kind of problem has been considered already for special linear groups over finite fields F. Metelli proved that $*$ is surjective for all groups $PSL_2(F)$ where F has at least 4 elements and for $PSL_3(3)$ [11, 12]. For $PSL_3(F)$ it is known that $*$ is not in general surjective [16, 2, 4, 3]. In [17], Völklein considered more closely the structure of $\Gamma(G)$ for the groups $SL_n(F)/D$ where D is any central subgroup of $SL_n(F)$ and n is greater than 2, and in particular when n is 3.

We consider in detail the structure of $\Gamma(G)$ for $G = SL_3(K)$ with K any subfield of $\bar{\mathbf{F}}_p$. Here an important role is played by the relation between $\Gamma(G)$ and the group of autoprojectivities of the subgroup H of

0021-8693/95 $6.00

diagonal matrices of G. We first give some necessary conditions for an autoprojectivity of H to be the restriction of an element of $\Gamma(G)$ (Theorem 1.12), and subsequently we prove that these conditions are also sufficient (Theorem 2.7). Thus we get a complete description of $\Gamma(G)$ as an included subgroup of Aut $L(H)$ (Theorem 2.13). We also prove that every autoprojectivity of $PSL_3(K)$ is induced by an autoprojectivity of $SL_3(K)$, and that this correspondence is injective if and only if the 3-component of $K^\times$ is infinite or is the identity or has order 3 (Proposition 2.14, Theorem 2.15).

In the third section we consider more closely the behaviour of certain r-subgroups of H under the action of an exceptional autoprojectivity φ of G, and give arithmetic conditions between the primes p and r able to ensure that each such φ is the identity on the r-component H_r of H (Corollaries 3.4, 3.13). Moreover we prove that the presence of "free" subgroups (Definition 3.14) of H guarantees that $\Gamma(G)$ is not the identity subgroup (Theorem 3.18). This enables us to show that $\Gamma(G)$ is not trivial for a large family of subfields K of $\bar{\mathbf{F}}_p$ (Proposition 3.19). Finally, using exponential congruences, we prove that for every prime p the groups $SL_3(\bar{\mathbf{F}}_p)$ and $PGL_3(\bar{\mathbf{F}}_p)$ have autoprojectivities which are not induced by any automorphism (Theorem 3.20, Corollary 3.21). More precisely we prove that the groups $\Gamma(SL_3(\bar{\mathbf{F}}_p))$ and $\Gamma(PGL_3(\bar{\mathbf{F}}_p))$ are always non-soluble and non-periodic groups. In the last section we give necessary and sufficient conditions on the primes p and r, such that the group of autoprojectivities of $\Omega(H_r)$ induced by $\Gamma(G)$ is trivial, using a result from the theory of elliptic equations (Proposition 4.2, Theorem 4.4). We conclude by giving some examples.

Notation. $\mathbb{N}$ = set of natural numbers $= \{1, 2, \ldots\}$. For every prime r and every natural n, $v_r(n)$ is the maximal power of r dividing n. We also put $\infty = v_r(\infty)$.

Let X be a group. $L(X)$ is the set of all subgroups of X partially ordered by inclusion. $L(X)$ is a complete algebraic lattice.

If X is a group, and x is an element of X, $|x|$ is the order of x. x is an r-element means that the order of x is a power of the *prime* r.

If (X_α), for α is an index set A, is a family of groups, we denote by $\mathrm{Cr}\, X_\alpha$ the cartesian product over A of the groups X_α.

If x, y are elements of a group X, $x^y = y^{-1}xy$. If A, B are subgroups of X, we put $A^B = \langle a^b | a \in A, b \in B \rangle$. If X acts on a set S, for every s in S, s^X is the orbit of s under X and X_s is the stabilizer of s.

For every prime r, C_{r^α} is the cyclic group of order r^α if α lies in $\mathbb{N}$, and the hypercyclic group relative to r if $\alpha = \infty$. If X is an abelian torsion group and r is a prime, X_r is the r-component of X. If X is an abelian r-group, for every n in $\mathbb{N}$, $\Omega_n(X) = \{x \in X | x^{r^n} = 1\}$ and $\Omega(X) = \Omega_1(X)$.

If R is a ring, $R^\times$ denotes the group of units of R.

Let p be a fixed prime. We shall always denote by K a *fixed* subfield of $\bar{\mathbf{F}}_p$ (for a complete description of subfields of $\bar{\mathbf{F}}_p$ see for instance Exercise 6 on page 147 in [9]). Z is the centre of $SL_3(\bar{\mathbf{F}}_p)$, T is the group of diagonal matrices, and U the group of upper unitriangular matrices in $SL_3(\bar{\mathbf{F}}_p)$.

Throughout the paper, by G we shall always denote the group $SL_3(K)$, which is the main concern of our investigation. H is the group of diagonal matrices in G, $N = N_G(H)$, and $W = N/H$. N is therefore the group of monomial matrices in G, W is isomorphic to S_3 and acts on H by permuting the diagonal entries. We shall make W act on $L(H)$ in the obvious way. For every subfield F of K, $H(F)$ is the group of diagonal matrices with entries in F. We denote by $\mathrm{diag}(\lambda_1, \lambda_2, \lambda_3)$ the diagonal 3×3 matrix having λ_i in the (i, i) position.

We consider the vector space K^3 with canonical basis (e_1, e_2, e_3). For every non-zero v in K^3, $\langle v \rangle$ denotes the corresponding point of $\mathbb{P}^2(K)$. G acts naturally on $\mathbb{P}^2(K)$. The canonical building of G is (isomorphic to) the flag complex of $\mathbb{P}^2(K)$. $\Gamma(G)$ denotes the group of exceptional autoprojectivities of G, i.e., the group of autoprojectivities fixing every parabolic subgroup of G.

We choose the algebraic homomorphisms $x_i\colon \bar{\mathbf{F}}_p \to U$ for $i = 1, 2, 3$,

$$x_1(k) = \begin{pmatrix} 1 & k & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad x_2(k) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & k \\ 0 & 0 & 1 \end{pmatrix}$$

$$x_3(k) = \begin{pmatrix} 1 & 0 & -k \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

so that we have the commutator formula $x_2(b)x_1(a) = x_1(a)x_2(b)x_3(ab)$ for every a, b in $\bar{\mathbf{F}}_p$.

1. Some Properties of $\Gamma(SL_3(K))$

We begin recalling some results which were proved for finite fields in [17, 3], and for $\bar{\mathbf{F}}_p$ in [5, 6], and which can be easily extended to our case using local arguments. Every autoprojectivity of G is *index-preserving*, since G is a perfect locally finite group. Using the fundamental theorem of projective geometry, as noticed in [17], one gets the decomposition $\mathrm{Aut}\, L(G) = \Gamma(G) \rtimes \mathrm{Aut}\, G$. Hence every autoprojectivity of G is induced by an automorphism if and only if $\Gamma(G) = \{1\}$. In the next statement we collect some basic results concerning exceptional autoprojectivities of G.

THEOREM 1.1. *Let G be the group $SL_3(K)$. Then every exceptional autoprojectivity φ of G satisfies the following conditions.*

(a) *φ fixes H.*

(b) *For every prime r, φ fixes the groups H_r and $\Omega_n(H_r)$ for each n in $\mathbb{N}$, and $H(F)_r$ for every subfield F of K.*

(c) *φ fixes every subgroup of order 2 and every unipotent subgroup of G.*

(d) *φ commutes with the inner automorphisms of G.*

(e) *For every a in $K^\times$, φ fixes the subgroups $\langle \mathrm{diag}(a, a^{-1}, 1)\rangle$ and $\langle \mathrm{diag}(a, a, a^{-2})\rangle$.*

(f) *φ fixes every subgroup of order 3 of G.*

Moreover, the restriction homomorphism ι from $\Gamma(G)$ to Aut $L(H)$ *is injective.*

Proof. (a) We have $H = G_{\langle e_1\rangle} \wedge G_{\langle e_2\rangle} \wedge G_{\langle e_3\rangle}$ so that $H^\varphi = H$.

(b) This follows from the fact that φ is index-preserving.

(c) and (d) ι is injective. If K is finite, see the theorem and the corollary in [17]. So assume K is infinite.

Let F be a finite subfield of K of order at least 3. We show that φ fixes the subgroup $SL_3(F)$ of G. Let r be a prime divisor of $|F^\times|$. By (b), φ fixes the group $H(F)_r$, and similarly one can show that it fixes the groups $H(F)_r^g$ for every g in $SL_3(F)$. Hence $SL_3(F)^\varphi = SL_3(F)$, since $SL_3(F) = \langle H(F)_r^g | g \in SL_3(F)\rangle$. For each n in $\mathbb{N}$, let F_n be the unique subfield of order $p^{n!}$ of $\bar{\mathbf{F}}_p$, and let $K_n = F_n \wedge K$. We put $G_n = SL_3(K_n)$. G is the set theoretic union of the G_n's. By the previous discussion, there exists an M such that for each $n \geq M$, φ fixes G_n. We denote by φ_n the autoprojectivity of G_n induced by φ. Let σ, u, x, g be elements of G, with σ of order 2 and u unipotent. Let $n \geq M$ be such that σ, u, g, x, h are in G_n. Then, by the theorem and the corollary in [17], we get $\langle\sigma\rangle^{\varphi_n} = \langle\sigma\rangle$, $\langle u\rangle^{\varphi_n} = \langle u\rangle$, $\langle x\rangle^{g\varphi_n} = \langle x\rangle^{\varphi_n g}$, and we are done. Moreover, if the restriction of φ to $L(H)$ is the identity, it follows that the restriction of φ_n to $L(H(K_n))$ is the identity for every $n \geq M$. Hence each φ_n is the identity and $\varphi = 1$.

(e) The group $B = \{\mathrm{diag}(b, b, b^{-2}) | b \in K^\times\}$ coincides with the intersection of $G_{\langle e_3\rangle}$ with the intersection of the family of all G_p for all points P in the line $\langle e_1, e_2\rangle$. Hence $B^\varphi = B$, and $X^\varphi = X$ for every $X \leq B$, since $K^\times$ is a torsion locally cyclic group and φ is index-preserving. Let a be in $K^\times$, and let $s = \mathrm{diag}(a, a^{-1}, 1)$. If s is an involution we are done, by (c). So assume the order of s at least 3. There exists an involution σ in G such that $s^\sigma = s^{-1}$. Then $\langle s\rangle^\varphi = \langle s\rangle$ since $\langle s\rangle$ is the unique cyclic maximal subgroup of the group $\langle s, \sigma\rangle$, which is generated by involutions.

(f) Let x be an element of order 3 of G. If it is unipotent, or semisimple and diagonalizable in G, then we are done by (e), (c), and (d). So assume x semisimple but not diagonalizable in G, and let $n \geq M$ be such that x lies in G_n. Then the result follows from Lemma 8 in [17].

We shall now point out other properties of φ.

LEMMA 1.2. *Let E, F be cyclic subgroups of order r^α of the group $C_{r^\infty} \times C_{r^\infty}$. Then we have $EF = \langle R | E \wedge F \leq R \leq C_{r^\infty} \times C_{r^\infty}$, R cyclic of order $r^\alpha \rangle$.*

Proof. We can get the result by induction on the order of $E \wedge F$. ∎

PROPOSITION 1.3. *Let X be a subgroup of H which is fixed by a non-trivial element of W. Then X is fixed by φ.*

Proof. Suppose first that X is cyclic of order a power of a prime r. If the order of w is 2, there exists σ of order 2 in N such that $w = H\sigma$. If r is odd, then either σ centralizes X or it acts on it as inversion. In both cases we get $X^\varphi = X$ by Theorem 1.1(e). Assume now $r = 2$, and consider the group $\langle X, \sigma \rangle$. If $\langle X, \sigma \rangle$ is abelian or dihedral, then we conclude in the same way as for r odd. If $\langle X\sigma \rangle$ is the modular group, then $\langle X^2, \sigma \rangle$ is abelian, so that $(X^2)^\varphi = X^2$. Let Y be the unique cyclic subgroup of order $|X|$ of H containing X^2 and commuting with σ. Then we have $Y^\varphi = Y$, so that $X^\varphi = X$ as the unique cyclic subgroups of order $|X|$ of H containing X^2 are X and Y. Similarly one proves that $X^\varphi = X$ if $\langle X, \sigma \rangle$ is semidihedral (in this case there exists a unique cyclic subgroup Y of order $|X|$ of H containing X^2 on which σ acts as inversion). Suppose now that w has order 3. Then there exists an element ρ of order 3 in N such that $w = H\rho$. Suppose r is not 3. Then X is the unique r-Sylow subgroup of $\langle X, \rho \rangle$, which is generated by elements of order 3 (ρ and ρx for instance). Hence $X^\varphi = X$ by Theorem 1.1(f). If $r = 3$, then we must have $X = Z$, and we are done.

Now assume X is any subgroup of H. Without loss of generality we may assume X to be a finite r-group, for a certain prime r. We shall have $X \cong C_{r^\alpha} \times C_{r^\beta}$, for some $\alpha \geq \beta$. If $\alpha = \beta$, then we are done by Theorem 1.1(b). So assume $\alpha > \beta$, and let C be a cyclic subgroup of X of order r^α, and M be the subgroup of X isomorphic to $C_{r^\beta} \times C_{r^\beta}$. From $X = \langle C, M \rangle$, it follows that $X^\varphi = X$ if and only if $C^\varphi \leq X$. Let $L = C \wedge C^w$. We have $L^w = L$, as C is cyclic. By Lemma 1.2, $C \cdot C^w = \langle D | L \leq D \leq H$, D cyclic of order $r^\alpha \rangle$, so that $(C \cdot C^w)^\varphi = C \cdot C^w$, as $L^\varphi = L$ by the previous discussion. Hence $C^\varphi \leq C \cdot C^w \leq X$, and we are done. ∎

DEFINITION 1.4. Let $s = \mathrm{diag}(a, b, c)$ be an element of H. We put

$$\alpha_1(s) = ab^{-1}, \qquad \alpha_2(s) = bc^{-1}, \qquad \alpha_3(s) = ac^{-1} \ (= \alpha_1(s)\alpha_2(s)).$$

Also, for $i = 1, 2, 3$, we denote by $\mu_i(s)$ the minimum polynomial of $\alpha_i(s)$ over $\mathbf{F}_p$, and by $F_i(s)$ the field $\mathbf{F}_p(\alpha_i(s))$. We put $F(s) = \mathbf{F}_p(\alpha_1(s), \alpha_2(s))$ and $H(s) = H(\mathbf{F}_p(a, b))$.

DEFINITION 1.5. We say that a diagonal element s satisfies $(*')$ if $\mu_i(s) \neq \mu_j(s)$ for every $i \neq j$. We say that s satisfies $(**')$ if s^w satisfies $(*')$ for every w in W (cf. the definition given in [4]).

From basic facts in field theory, elements u, v in $\bar{\mathbf{F}}_p$ have the same minimum polynomial over $\mathbf{F}_p$ if and only if there exists a non-negative integer m such that $u^{p^m} = v$.

DEFINITION 1.6. Suppose s is an r-element of H not satisfying $(*')$. If r is not 3, we say that s is *determined*. Suppose $r = 3$. We put

$$\mathscr{X}_1(s) = \{m \mid m \geq 0,\ \alpha_2(s)^{p^m} = \alpha_3(s),\ p^m \equiv 1 \bmod 3\}.$$

$$\mathscr{X}_2(s) = \{m \mid m \geq 0,\ \alpha_1(s)^{p^m} = \alpha_3(s),\ p^m \equiv 1 \bmod 3\}.$$

$$\mathscr{X}_3(s) = \{m \mid m \geq 0,\ \alpha_1(s)^{p^m} = \alpha_2(s),\ p^m \equiv 2 \bmod 3\}.$$

We say that s *is almost determined* if each $\mathscr{X}_i(s)$ is empty. Otherwise we say that s is *determined*.

We shall soon prove that if φ is in $\Gamma(G)$, then φ fixes $\langle s \rangle$ if s is determined and it fixes $\langle s^3 \rangle$ if s is almost determined.

PROPOSITION 1.7. *Let $s = \mathrm{diag}(a, b, c)$ be a 3-element of H. If s is almost determined, then $\alpha_1(s)$, $\alpha_2(s)$, and $\alpha_3(s)$ have the same order as s. If s is determined, there exists i such that $\alpha_i(s)$ has order less than the order of s.*

Proof. Let s be almost determined, and let $\alpha_i(s)^{p^m} = \alpha_j(s)$ for some $i < j$ and some nonnegative integer m. In all cases, $\alpha_1(s)$, $\alpha_2(s)$, and $\alpha_3(s)$ have the same order. Let 3^ν be the order of s and 3^λ be the order of the $\alpha_i(s)$'s. Note that for a 3-element t of H we have $|\alpha_i(t)| = |t|$ for every $i = 1, 2, 3$, if and only if $\langle t \rangle \not\cong Z$. If $\lambda < \nu$, it follows that $\langle s \rangle = Z$, so that $\mathscr{X}_1(s)$ is not empty, a contradiction. Hence $\lambda = \nu$.

If s is determined, there exists i such that $\mathscr{X}_i(s)$ is not empty. It then follows that the order of $\alpha_i(s)$ is less than the order of s. ∎

From the previous proposition we get a criterion to see if a 3-element of H not satisfying $(*')$ is determined or almost determined.

COROLLARY 1.8. *Suppose s is a 3-element of H not satisfying $(*')$. Then s is almost determined if and only if $\langle s\rangle \not\geq Z$.*

Proof. Suppose s is almost determined. Then, by Proposition 1.7 we have $|\alpha_i(s)| = |s|$ for every $i = 1, 2, 3$, so that $\langle s\rangle \not\geq Z$. If s is determined, by Proposition 1.7 there exists i such that $|\alpha_i(s)| < |s|$. Hence $\langle s\rangle \geq Z$. ∎

We shall now study the behaviour of subgroups generated by determined or almost determined elements of H, under the action of exceptional autoprojectivities.

LEMMA 1.9. *Let s be an r-element of H not satisfying $(*')$, and let $\alpha = v_r(|(K^\times)_r|)$. Then there exists a subgroup P of U normalized by s and such that $H_r \wedge N_G(P)$ is isomorphic to C_{r^α} if s is determined, and to $C_{3^\alpha} \times C_3$ if s is almost determined.*

Proof. H_r is isomorphic to $C_{r^\alpha} \times C_{r^\alpha}$. Let $\alpha_i(s)^{p^m} = \alpha_j(s)$ for some $i < j$ and some nonnegative integer m. For each case we define a certain subgroup P of U. Suppose first that s is almost determined.

If $(i, j) = (1, 2)$, we put $P = \{x_1(\xi)x_2(\xi^{p^m})x_3(\eta) | \xi, \eta \in K\}$. If $(i, j) = (1, 3)$, we put $P = \{x_1(\xi)x_3(\xi^{p^m}) | \xi \in K\}$. Finally, if $(i, j) = (2, 3)$, we put $P = \{x_2(\xi)x_3(\xi^{p^m}) | \xi \in K\}$. In all cases, s lies in $N_G(P)$ and $N_G(P) \wedge H_3$ is isomorphic to $C_{3^\alpha} \times C_3$.

Suppose now that s is determined. Suppose first $r \neq 3$. If we define P as in the previous cases then $N_G(P) \wedge H_r$ is isomorphic to C_{r^α} and we are done. Finally, if $r = 3$, then at least one of the $\mathscr{X}_k(s)$'s is non-empty. If we define P as in the previous case for the corresponding (i, j), it then follows that $N_G(P) \wedge H(s)_3$ is isomorphic to C_{3^α}, and it contains $\langle s\rangle$. ∎

LEMMA 1.10. *Let s be an almost determined element of H, with $\alpha_i(s)^{p^m} = \alpha_j(s)$ for some $i < j$ and some non-negative integer m. $M = \langle s, \Omega(H_3)\rangle$, s' an element of H of the same order of s. Then the following are equivalent*

(i) $\alpha_i(s')^{p^m} = \alpha_j(s')$.

(ii) *s' lies in M.*

Proof. We observe that from Corollary 1.8 we have $\langle s, \Omega(H_3)\rangle = \langle s\rangle \times Z$. It is then clear that (ii) ⇒ (i). The reverse implication comes from Lemma 1.9: M must be the unique subgroup of $N_G(P) \wedge H(s)_3$ isomorphic to $C_{3^\beta} \times C_3$, where 3^β is the order of s. ∎

PROPOSITION 1.11. *Let s be an r-element of H. Let φ lie in $\Gamma(G)$. If s is determined, then $\langle s\rangle^{\varphi} = \langle s\rangle$. If s is almost determined, then $\langle s^3\rangle^{\varphi} = \langle s^3\rangle$. Moreover, if $\langle s\rangle^{\varphi} = \langle s'\rangle$, then s' is almost determined.*

Proof. In both cases we consider the p-group P of Lemma 1.9. Let $L = H_r \wedge N_G(P)$. We have $L^{\varphi} = L$ as P is the unique maximal p-subgroup of LP, $P^{\varphi} = P$, $(H_r)^{\varphi} = H_r$, and φ is index-preserving (we argue locally). If s is determined we have $\langle s\rangle^{\varphi} = \langle s\rangle$, as L is locally cyclic. So assume s is almost determined, and let 3^r be the order of s. Let M be the unique subgroup of L isomorphic to $C_{3^r} \times C_3$. Then $\langle s^3\rangle^{\varphi} = \langle s^3\rangle$ as $\langle s^3\rangle = \mathrm{Frat}(M)$. Since $\langle s'\rangle \not\geq Z$, s' is almost determined by Lemma 1.10. ∎

It is clear that we still have $\langle s\rangle^{\varphi} = \langle s\rangle$ if there is a cyclic subgroup of $H_3 \wedge N_G(P)$ of order 3^{r+1} containing s.

We summarize the properties satisfied by the elements of the subgroup $\iota(\Gamma(G))$ of Aut $L(H)$ so far obtained.

THEOREM 1.12. *Let G be the group $SL_3(K)$, and let φ be an exceptional autoprojectivity of G. If λ is the autoprojectivity of H induced by φ, then*

(a) *λ commutes with the action of W;*

(b) *λ fixes every subgroup of H which is fixed by a non-trivial element of W;*

(c) *if s is an r-element of H, then λ fixes $\langle s\rangle$ if s is determined, and it fixes $\langle s^3\rangle$ if s is almost determined.*

We shall show in the next section that these conditions are also sufficient. For completeness we prove

COROLLARY 1.13. *Let s be an r-element of H satisfying $(*')$. Let φ lie in $\Gamma(G)$, and $\langle s\rangle^{\varphi} = \langle s'\rangle$. Then s' satisfies $(*')$ and we have $|\alpha_i(s)| = |\alpha_i(s')|$ for every $i = 1, 2, 3$.*

Proof. Suppose that s' does not satisfy $(*')$. If s' is determined, then we get $\langle s\rangle = \langle s'\rangle^{\varphi^{-1}} = \langle s'\rangle$, by Proposition 1.11 and this is a contradiction. If s' is almost determined, then s is almost determined by Proposition 1.11. Again we have a contradiction. Hence s' satisfies $(*')$. Let $|\alpha_1(s)| = r^m$, $|s| = r^n$. Let $t = s^{r^m}$. We have $t = \mathrm{diag}(u, u, u^{-2})$, for a certain u of order r^{n-m}, and $s = \mathrm{diag}(a, b, c)$ with $a^{r^m} = b^{r^m} = u$. Let $s' = \mathrm{diag}(a', b', c')$. We get $a'^{r^m} = b'^{r^m}$ as φ fixes $\langle t\rangle$. Hence $|\alpha_1(s')| \leq |\alpha_1(s)|$. By symmetry we get $|\alpha_1(s')| = |\alpha_1(s)|$. Similarly for $|\alpha_2(s')|$ and $|\alpha_3(s')|$. ∎

2. The Structure of $\Gamma(SL_3(K))$ and $\Gamma(PSL_3(K))$

Our aim is to determine the image of the restriction monomorphism ι: $\Gamma(G) \to \mathrm{Aut}\, L(H)$, i.e., to determine which autoprojectivities λ of H can be extended to exceptional autoprojectivities of G.

Let $s = \mathrm{diag}(\alpha, \beta, \gamma)$ be an r-element of H and let $u = x_1(a)x_2(b)x_3(c)$ be an element of U. For convenience we shall write α_i for $\alpha_i(s)$, F_i for $F_i(s)$, $i = 1, 2, 3$, and F for $F(s)$. We consider the case when s satisfies $(*')$.

Lemma 2.1. *Suppose s satisfies $(*')$. For every A in F_1, B in F_2, C in F_3 there exists k in $\langle F_1, F_2\rangle$ such that $x_1(Aa)x_2(Bb)x_3(Cc + kab)$ is in $\langle u\rangle^{\langle s\rangle}$.*

Proof. See Proposition 2.4 in [4] (note that the proof of Proposition 2.4 in [4] does not make use of the fact that $F_i = F$ for every $i = 1, 2, 3$). ∎

Proposition 2.2. *Suppose s satisfies $(*')$. Then, for every A in F_1, B in F_2, C in F_3 and D in $\langle F_1, F_2\rangle$, $x_1(Aa)x_2(Bb)x_3(Cc + Dab)$ lies in $\langle u\rangle^{\langle s\rangle}$.*

Proof. By Lemma 2.1 we are left to prove the following. For every D in $\langle F_1, F_2\rangle$, $x_3(Dab)$ lies in $\langle u\rangle^{\langle s\rangle}$. So let D be in $\langle F_1, F_2\rangle$. Following the same procedure in the proof of Proposition 2.5 in [4], and by Lemma 2.1, if A, A' are elements of F_1 and B, B' are elements of F_2, one can prove that $x_3((A'B - AB')ab)$ lies in $\langle u\rangle^{\langle s\rangle}$. As at least one of F_1 and F_2 is equal to $\langle F_1, F_2\rangle$, we can always choose A, A', B, B' such that $A'B - AB' = D$, and we are done. ∎

We prove a fact relating elements of H with p-subgroups of G.

Proposition 2.3. *Let s, s' be r-elements of H and let P be a subgroup of U normalized by s. If one of the following condition holds*

(a) *s, s' satisfy $(*')$ and $F_i(s) \geq F_i(s')$ for every $i = 1, 2, 3$;*

(b) *s is almost determined, and s' lies in $\langle s, \Omega(H_3)\rangle$,*

then P is also normalized by s'.

Proof. Suppose (a) holds. If $u = x_1(a)x_2(b)x_3(c)$ is in P, we have $s'us'^{-1} = x_1(\alpha_1(s')a)x_2(\alpha_2(s')b)x_3(\alpha_3(s')c)$. Then $s'us'^{-1}$ is in $\langle u\rangle^{\langle s\rangle}$ by Proposition 2.2. Suppose now (b) holds. Then $s'us'^{-1}$ is in $\langle u\rangle^{\langle s\rangle}$ since $\langle s, \Omega(H_3)\rangle = \langle s\rangle \times Z$. In both cases it follows that s' lies in $N(P)$. ∎

We can now prove two extension criteria in connection with the one proved in [16].

PROPOSITION 2.4. *Let λ be an autoprojectivity of H. Then λ can be extended to an exceptional autoprojectivity of G if the following holds:*

(i) *λ commutes with the action of W;*

(ii) *λ fixes every subgroup of H which is fixed by a non-trivial element of W;*

(iii) *λ fixes every cyclic 3-subgroup C of H such that C^3 fixes pointwise a line of $\mathbb{P}^2(\overline{\mathbf{F}}_p)$;*

(iv) *if s is an r-element of H not satisfying $(*')$, then λ fixes $\langle s\rangle$ if s is determined. If s is almost determined then λ fixes $\langle s^3\rangle$.*

Proof. We follow step by step the proof of Proposition 3 in [16] (taking into account [4]). For brevity, in the following we shall just write [16] to refer to that proof.

(1), (2) If X is a subgroup of H with $X^\lambda \neq X$, then $C_G(X) = H$, as in [16].

(3), (4) If P is a p-subgroup of G normalized by a subgroup X of H, then P is also normalized by X^λ. We may assume X to be a cyclic r-group. Let $X = \langle s\rangle$. If $\langle s\rangle^\lambda = \langle s\rangle$ then we are done. So suppose $\langle s\rangle^\lambda = \langle s'\rangle \neq \langle s\rangle$. As in [16] there exists n in N such that $P^n \leq U$. Let $w = Tn$, and $t = s^w$, $t' = s'^w$. Then $\langle t\rangle^\lambda = \langle s\rangle^{w\lambda} = \langle s\rangle^{\lambda w} = \langle t'\rangle$, and $\langle t\rangle \leq N_G(P^n)$. We prove that $\langle t'\rangle \leq N_G(P^n)$, so that $\langle s'\rangle \leq N_G(P)$.

Suppose t satisfies $(*')$. We prove that t' satisfies $(*')$ and $F_i(t') = F_i(t)$ for every $i = 1, 2, 3$. Suppose t' does not satisfy $(*')$. If t' is determined, we have $\langle t'\rangle^\lambda = \langle t'\rangle$, so that $\langle t\rangle = \langle t'\rangle$ and t does not satisfy $(*')$, which is a contradiction. Hence t' is almost determined, so that $\langle t'^3\rangle^\lambda = \langle t'^3\rangle$. But then t lies in $\langle t'\rangle \times Z$, so that t is almost determined by Lemma 1.10. Again we have a contradiction. Therefore t' satisfies $(*')$. Using the same argument as in the proof of Corollary 1.13, one can show that $|\alpha_i(t')| = |\alpha_i(t)|$ for every $i = 1, 2, 3$, so that $F_i(t') = F_i(t)$ for every $i = 1, 2, 3$. Therefore, by Proposition 2.3 we get $\langle t'\rangle \leq N_G(P^n)$. If t does not satisfy $(*')$, by (iv), t must be almost determined, and t' lies in $\langle t, \Omega(H_3)\rangle$. Again by Proposition 2.3 we get $\langle t'\rangle \leq N_G(P^n)$ and we are done.

As G is locally finite, we first define the map φ on the set $L_f(G)$ of all finite subgroups of G. Later we shall show that φ is inclusion preserving. Similarly one can define ψ starting from λ^{-1}. Then φ and ψ are one the inverse of the other, and they are both inclusion preserving. It is straightforward to prove that φ can then be extended (uniquely) to the required autoprojectivity of G.

(5) We extend the definition of λ to a bijection φ of $L_f(G)$. The extension is defined as in [16]. For the convenience of the reader we recall the procedure. φ is first defined on the set $\mathscr{X}$ of all (finite) subgroups of G

with $X^g \leq H$ for some g in G by $X^\varphi = X^{g\lambda g^{-1}}$. We have a good definition as λ fixes every subgroup of H which is fixed by a non-trivial element of W. Then φ is defined on the set $\mathcal{Y}$ of all (finite) subgroups Y of G which are the semi-direct product of a normal p-subgroup P and some X in $\mathcal{X}$, by $Y^\varphi = P \cdot X^\varphi$. Finally $X^\varphi = X$ for all (finite) subgroups X not in $\mathcal{Y}$.

(6),(7) As in [16], we fix (finite) subgroups E, F of G with $E \leq F$, and we prove that $E^\varphi \leq F^\varphi$. This holds if F belongs to $\mathcal{Y}$.

(8) We assume that E is a cyclic s-subgroup of H for some prime s, with $E^\varphi \neq E$, F is minimal among the subgroups of G containing E and not lying in $\mathcal{Y}$, and suppose for a contradiction that $E^\varphi \not\leq F$.

(9)–(11) $C_G(E) = H$, $F \wedge N_G(E) \leq H$ and if S is an s-Sylow subgroup of F containing E, then S is contained in H and it has a normal complement R in F, as in [16].

(12) R is an r-group for some prime r different from p. As in [16], R cannot be a p-group, and we can choose an r-Sylow subgroup R_1 of R normalized by S, and assume for a contradiction that $R_1 \neq R$. Then R_1S lies in H and $N_R(R_1) \neq C_R(R_1)$. Let K_1 be a complement of R_1 in $N_R(R_1)$ normalized by S, so that $K_1S = (K_1S \wedge H)P$, where P is the unique p-Sylow subgroup of K_1S. Here we modify the proof given in [16]. We prove that $[P, R_1] = 1$. As in the proof of (4) (since P is normalized by E), there exists n in N such that $P^n \leq U$. Hence $[P, R_1]^n = [P^n, R_1^n] \leq [U, H] = U$. Moreover we observe that P must lie in K_1, so that $P \leq N_R(R_1)$, which implies that $[P, R_1] \leq R_1 \leq H$. It follows that $[P, R_1] \leq H \wedge U^{n^{-1}} = 1$. We finally prove that $N_R(R_1) = C_R(R_1)$ to reach a contradiction. From $N_R(R_1) = R_1K_1 \leq R_1(K_1S) = R_1(K_1S \wedge H)P$, it follows that $N_R(R_1) \subseteq HP$. Then $[N_R(R_1), R_1] \leq [HP, R_1] = 1$, and we are done.

(13) R is not abelian. Otherwise R would be diagonalizable over $\bar{\mathbf{F}}_p$. We have 2 possibilities. Either R fixes only 3 points of $\mathbb{P}^2(\bar{\mathbf{F}}_p)$, or it fixes a line γ pointwise and point A not on it. Suppose we are in the second case. Then S must fix both γ and A, so that we get $[R, S] = 1$ as S fixes only 3 points, and this is a contradiction. Hence R fixes only 3 points, A_1, A_2, A_3, say. Then S permutes A_1, A_2, A_3 and we conclude that $[R, S] = 1$ as in [16] if $s \geq 5$. Therefore we have $s = 2$ or 3. Let $E = \langle x \rangle$. Assume $s = 2$. As $[R, S] \neq 1$, without loss of generality we may suppose $S = \langle \tau \rangle S_1$, where S_1 is a subgroup of index 2 in S fixing A_1, A_2, A_3 and τ fixes A_1 and interchanges A_2, A_3, x does not lie in S_1, so that it fixes A_1 and interchanges A_2, A_3. Therefore x^2 fixes pointwise the line $A_2 + A_3$. But then $\langle x^2 \rangle^\varphi = \langle x^2 \rangle$ by (ii). In H, besides E, there is only one cyclic subgroup E_1 of order $|E|$ containing $\langle x^2 \rangle$. E_1 fixes pointwise the line $A_2 + A_3$, so that it is fixed by φ, forcing also E to be fixed by φ. This is

again a contradiction. We are therefore left with the case $s = 3$. In this case x will induce a permutation of order 3 on the points A_1, A_2, A_3, forcing x to have order 3 (as $\det x = 1$). Again by (ii) we get $E^\varphi = E$, which is the final contradiction.

(14) As in [16], we have $\mathrm{Frat}(R) = R' = Z(R)$ (R' = derived subgroup of R), and this group is elementary abelian, $[Z(R), S] = 1$ and S acts irreducibly on $R/Z(R)$, so that $R \wedge H = Z(R)$.

(15) Let us assume that R' lies in Z, so that $R' = Z$, and $r = 3$. $R/Z(R)$ is a vector space of dimension 2 over F_3, and we are done if $s \geq 5$, as in [16]. So now suppose $s = 2$. We have $|R| = 27$. R has 4 maximal subgroups, R_1, R_2, R_3, R_4, say. We then get a homomorphism ε: $S \to S_4$. Also R must be of exponent 3, as in $SL_3(\bar{\mathbf{F}}_p)$ there is no non-abelian subgroup of order 27 and exponent 9. Therefore each R_i lies in a unique maximal torus T_i of $SL_3(\bar{\mathbf{F}}_p)$. We need a description of the T_i's. Just for this purpose we assume $R = X \rtimes \langle \rho \rangle$, where X is the subgroup of the group of diagonal matrices T of $SL_3(\bar{\mathbf{F}}_p)$ isomorphic to $C_3 \times C_3$, and

$$\rho = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

To each torus T_i we associate the triangle whose vertices are the fixed points of T_i. Let θ be a fixed element of $K^\times$ of order 3. We get

$$T_1 = T \leftrightarrow \langle e_1 \rangle, \langle e_2 \rangle, \langle e_3 \rangle;$$

$$T_2 \leftrightarrow \langle e_1 + e_2 + e_3 \rangle, \langle e_1 + \theta e_2 + \theta^2 e_3 \rangle, \langle e_1 + \theta^2 e_2 + \theta e_3 \rangle,$$

$$T_3 \leftrightarrow \langle \theta e_1 + \theta e_2 + e_3 \rangle, \langle \theta e_1 + e_2 + \theta e_3 \rangle, \langle e_1 + \theta e_2 + \theta e_3 \rangle;$$

$$T_4 \leftrightarrow \langle \theta^2 e_1 + \theta^2 e_2 + e_3 \rangle, \langle \theta^2 e_1 + e_2 + \theta^2 e_3 \rangle, \langle e_1 + \theta^2 e_2 + \theta^2 e_3 \rangle.$$

One can show that if A is a vertex of one of the triangles, and B is a vertex of another triangle, then the line through A and B contains a vertex of the third and a vertex of the fourth triangle. It then follows that $N_G(T_1) \wedge N_G(T_2) \wedge N_G(T_3) \wedge N_G(T_4)$ has order 54. Going back to our case, we put $L = N_G(T_1) \wedge N_G(T_2) \wedge N_G(T_3) \wedge N_G(T_4)$. Then $\ker \varepsilon \leq L$, as $C_G(R_i) = T_i$ for every i. In particular $E \wedge \ker \varepsilon$ has order at most 2, from which it follows that E has order at most 8. But the hypotheses on λ then implies that $E^\varphi = E$ (since there exists an involution w in W such that $E^w = E$), which is a contradiction.

(16) As in [16], we are left with the case when $H \subsetneq C_G(R') \subsetneq G$. Hence R' fixes pointwise a line of $\mathbb{P}^2(K)$ so that $C_G(R') \cong GL_2(K)$, $r = 2$, R' has order 2, and R/R' is the Klein group. If $s \geq 5$ we are done.

So now suppose $s = 3$. We have $|R| = 8$. If R is the dihedral group, then it has a characteristic cyclic subgroup C of order 4, which is therefore normalized by S. By minimality of F, C is centralized by E, so that $C \leq H$, which is a contradiction. Hence R is isomorphic to the group of quaternions Q_8. Since $\mathrm{Aut}(Q_8) \cong S_4$, we have $[E\colon E \wedge C_G(R)] = 1$ or 3 (in fact it must be 3), so that E^3 lies in $C_G(R)$. In general, if Q is a subgroup of $SL_3(\bar{\mathbf{F}}_p)$ isomorphic to Q_8, with maximal subgroups Q_1, Q_2, Q_3, then $C_G(Q) = T_1 \wedge T_2 \wedge T_3$, where $T_i = C_G(Q_i)$ is a maximal torus for every i. It turns out that $T_1 \wedge T_2 \wedge T_3$ is a 1-dimensional torus fixing pointwise a line of $\mathbb{P}^2(\bar{\mathbf{F}}_p)$. Hence E^3 fixes pointwise a line of $\mathbb{P}^2(\bar{\mathbf{F}}_p)$, so that $E^\varphi = E$ by (iii). This is the final contradiction for the proof of Proposition 2.4. ∎

We shall now give another criterion of extension, focusing only on the 3-subgroups of H.

PROPOSITION 2.5. *Let λ be an autoprojectivity of H. Then λ can be extended to an exceptional autoprojectivity of G if the following holds*:

(i) *λ commutes with the action of W*;

(ii) *λ fixes every subgroup of H which is fixed by a non-trivial element of W*;

(iii) *λ fixes every r-subgroup of H for every prime r different from* 3;

(iv) *if s is a 3-element of H not satisfying $(*')$, then λ fixes $\langle s \rangle$ if s is determined. If s is almost determined then λ fixes $\langle s^3 \rangle$.*

Proof. If $K^\times$ does not contain elements of order 3, then we have $\lambda = 1$ and we are done (with $\varphi = 1$ of course). So assume $K^\times$ contains elements of order 3.

To define φ to the whole of $L(G)$, we first prove the following

LEMMA 2.6. *If C is a finite subgroup of G whose order is not divisible by* 3 *and $N_G(C)$ contains a finite 3-subgroup X of H, then $N_G(C)$ contains also X^λ.*

Proof. Suppose this is false, and consider the set $\mathscr{E}$ of all the pairs (S, C) with S a finite 3-subgroup of H, $3 \nmid |C|$, $S \leq N_G(C)$, $S^\lambda \not\leq N_G(C)$, In $\mathscr{E}$ we choose a pair (S, C) with minimum $|S|$ and, with this choice of S, with minimum $|C|$. We shall reach a contradiction in several steps.

(a) S is cyclic and $C_G(S) = H$. S is cyclic by minimality of $|S|$. $C_G(S) = H$ as in steps (1), (2) above.

(b) $S \not\leq C_G(C)$. Otherwise $C \leq H$, so that $S^\lambda \leq N_G(C)$.

(c) If P is a p-subgroup of G normalized by S, then P is also normalized by S^λ. The proof is the same as in steps (3), (4) above.

(d) C is an r-group for some prime r different from p. Let $r_1, \ldots, r_m$ be the prime divisors of $|C|$. As in step (12) in [16] for each i we can choose an r_i-Sylow subgroup R_i of C normalized by S. If $S^\lambda \leq N_G(R_i)$ for each i, then we have $S^\lambda \leq N_G(C)$, which is a contradiction. Hence there exists j such that $S^\lambda \not\leq N_G(R_j)$. By minimality of $|C|$, we must have $C = R_j$. We shall just write r for r_j. r is different from p by (c).

(e) C is not abelian. This is as in step (13) above.

(f) $r = 2$ and $Z(C)$ fixes pointwise a line ω of $\mathbb{P}^2(\bar{\mathbf{F}}_p)$. By (d) and (e) we get $r = 2$. Hence $C_G(Z(C)) \neq G$ and $Z(C)$ fixes pointwise a line ω of $\mathbb{P}^2(\bar{\mathbf{F}}_p)$ as $C_G(Z(C))$ is non-abelian (as in step (16) above).

(g) Let A be the unique point of $\mathbb{P}^2(\bar{\mathbf{F}}_p)$ not in ω fixed by $Z(C)$. As S normalizes $Z(C)$, it must fix both A and ω. But S fixes only three points and three lines of $\mathbb{P}^2(\bar{\mathbf{F}}_p)$, so that without loss of generality we may suppose $A = \langle e_1 \rangle$ and $\omega = \langle e_2, e_3 \rangle$, so that $C \leq C_G(Z(C)) = G_A \wedge G_\omega$. The group $B = \langle \mathrm{diag}(\delta^{-2}, \delta, \delta) \rangle$ with δ of the same order of S, then even centralizes C, so that $\langle B, S \rangle \leq N_G(C)$. By Lemma 1.2, $\langle B, S \rangle$ is generated by all the cyclic subgroups of H of order $|S|$ containing $B \wedge S$, which is fixed by λ by (ii). Hence $S^\lambda \leq \langle B, S \rangle^\lambda = \langle B, S \rangle$, which is the final contradiction. ∎

Remark. In fact, as it will be clear later, there are examples of this situation with $X^\lambda \neq X$. For instance with $G = SL_3(109)$, C isomorphic to the group of quaternions Q_8, and $H_3 \wedge N_G(C) \cong C_{27} \times C_3$. In this case one can take $X = \langle \mathrm{diag}(v, v^{10}, v^{16}) \rangle$ and $X^\lambda = \langle \mathrm{diag}(v, v^{19}, v^7) \rangle$, where v is an element of order 27 in $K^\times$.

We can now complete the proof of Proposition 2.5. We extend the definition of λ to $L_f(G)$. Let $\mathscr{X}$ be the set of all (finite) abelian 3-subgroups of G. If X lies in $\mathscr{X}$, then it is diagonalizable, and there exists g in G such that $X^g \leq H$. Then we put $X^\varphi = X^{g\lambda g^{-1}}$. Let $\mathscr{Y}$ be the set of all (finite) subgroups Y of G which are the semi-direct product of a Hall normal subgroup C and some X in $\mathscr{X}$. Let g be an element of G such that $X^g \leq H$. From $X^g \leq N_G(C^g)$, it follows that $X^{g\lambda} \leq N_G(C^g)$ by Lemma 2.6. Hence $X^\varphi = X^{g\lambda g^{-1}} \leq N_G(C)$. We put $Y^\varphi = C \cdot X^\varphi$. This is a good definition as in step (5) above. Finally we put $X^\varphi = X$ for all subgroups X not in $\mathscr{Y}$. To prove that φ can be extended to an autoprojectivity of G, we only have to prove that it is inclusion preserving (as in step (6) above). We first prove the following fact.

Let E, F be 3-subgroups of G such that $E \leq F$. Then we have $E^\varphi \leq F^\varphi$. If E is non-abelian, then we have $E^\varphi = E$, $F^\varphi = F$, and we are done. If F

is abelian, without loss of generality we may suppose $F \leq H$, and we are done. So now suppose E abelian and F non-abelian. Then $F^\varphi = F$ and without loss of generality $E \leq H$. We have to show that $E^\lambda \leq F$. We may assume that is E cyclic and F is minimal among the non-abelian 3-subgroups of G containing E. If $E^\lambda = E$, then we are done. So assume $E^\lambda \neq E$. Then we have $C_G(E) = H$, by (ii). Let M be a maximal subgroup of F containing E. M must be abelian, by minimality of F. Therefore $M \leq C_G(E) = H$, and $C_G(M) = H$. Let ρ be an element of F not centralizing M. Then $\rho \in N_G(C_G(M)) \setminus C_G(M) = N \setminus H$. Let $L = E \wedge E^\rho$. We have $L^\rho = L$, as E is cyclic. By Lemma 1.2, $E \cdot E^\rho = \langle D | L \leq D \leq H, D \text{ cyclic of order } |E| \rangle$, so that $(E \cdot E^\rho)^\lambda = E \cdot E^\rho$, as $L^\lambda = L$ by (ii). Hence $E^\lambda \leq E \cdot E^\rho \leq F$, and we are done.

We now prove that φ is inclusion preserving. Let E_1, E_2 be subgroups of G such that $E_1 \leq E_2$, and let S_1 be a 3-Sylow subgroup of E_1 and S_2 a 3-Sylow subgroup of E_2 containing S_1. By the previous observation we have $S_1^\varphi \leq S_2^\varphi$.

If E_2 belongs to $\mathscr{Y}$, then $E_2 = S_2 C_2$, where C_2 is the unique normal complement of S_2. Hence $C_1 = E_1 \wedge C_2$ is a normal Hall subgroup of E_1 with $E_1 = S_1 C_1$, so that $E_1^\varphi = S_1^\varphi C_1 \leq S_2^\varphi C_2 = E_2^\varphi$, and we are done.

Now assume E_2 does not belong to $\mathscr{Y}$. Hence $E_2^\varphi = E_2$ and $S_2^\varphi = S_2$. If $E_1^\varphi = E_1$, we are done. So assume $E_1^\varphi \neq E_1$, so that E_1 belongs to $\mathscr{Y}$, $E_1 = S_1 C_1$, say. Then $E_1^\varphi = S_1^\varphi C_1 \leq \langle S_2, E_2 \rangle = E_2$ and we are done. ∎

We are now in the position to prove that the conditions given in Theorem 1.12 are also sufficient.

THEOREM 2.7. *Let G be the group $SL_3(K)$. Let λ be an autoprojectivity of the group H of diagonal matrices of G such that*

(a) *λ commutes with the action of W;*

(b) *λ fixes every subgroup of H which is fixed by a non-trivial element of W;*

(c) *let s be an r-element of H not satisfying $(*')$. Then λ fixes $\langle s \rangle$ if s is determined, and it fixes $\langle s^3 \rangle$ otherwise.*

Then there exists a (unique) exceptional autoprojectivity of G inducing λ on H.

Proof. We define the following autoprojectivities of H. We let η be the autoprojectivity inducing λ on H_r for every r different from 3, and inducing the identity on H_3, and we let ρ be the autoprojectivity inducing λ on H_3 and the identity on H_r for every r different from 3.

It follows that η satisfies the hypothesis of Proposition 2.4 and ρ satisfies the hypothesis of Proposition 2.5. We can therefore extend η, ρ

respectively to exceptional autoprojectivities ψ, ω of G. We finally put $\varphi = \psi\omega$ to get the required result. ∎

We can use Theorems 1.12 and 2.7 to give a description of the group $\Gamma(G)$. For this purpose, we first describe the structure of Aut $L(H)$.

For every prime q different from p, let $\nu(q) = v_q(|(K^\times)_q|)$. We have $H = \oplus H_q$, with $H_q \cong C_{q^{\nu(q)}} \times C_{q^{\nu(q)}}$. The determination of the group Aut $L(H)$ is then reduced to the study of the group of autoprojectivities of $C_{q^{\nu(q)}} \times C_{q^{\nu(q)}}$.

So let r be a prime, and let $R = C_{r^\nu} \times C_{r^\nu}$, where $1 \leq \nu \leq \infty$. We introduce the meet-semilattice of a group. For every group X, we define $M(X)$ to be the set of all cyclic subgroups of X. Therefore $M(X)$ is a subset of the lattice $L(X)$ with the property that for every A, B in $M(X)$, $A \wedge B$ lies in $M(X)$ (for a more general definition see [1, p. 22]). A bijection φ of $M(X)$ onto itself will be called an automorphism of $M(X)$ if we have $A \leq B$ if and only if $A^\varphi \leq B^\varphi$. If φ is an autoprojectivity of X, then clearly the restriction of φ to $M(X)$ is an automorphism of $M(X)$. We are interested in the converse, i.e., whether an automorphism of $M(X)$ can be extended (uniquely) to an autoprojectivity of X. This is not in general true, as one can see from the following example. Let X be the group $C_r \times C_r \times C_r$. Then every permutation of $M(X)$ fixing the identity subgroup is an automorphism of $M(X)$, but the automorphism φ interchanging the cyclic subgroups $C_r \times \{1\} \times \{1\}$ and $\{1\} \times \{1\} \times C_r$, and fixing all the other elements of $M(X)$ cannot be extended to an autoprojectivity of X. We show that for the group R every automorphism of $M(R)$ can be extended to an autoprojectivity of R. We state without proof an easy lemma.

LEMMA 2.8. *Let X be a group. Suppose that for every n in $\mathbb{N}$ we have a subgroup X_n of X and an autoprojectivity φ_n of X_n such that $X_n \leq X_{n+1}$ for every n in $\mathbb{N}$, $\bigcup_{n\in\mathbb{N}} X_n = X$, $Y^{\varphi_n} = Y^{\varphi_{n+1}}$ for every n in $\mathbb{N}$ and every subgroup Y of X_n.*
Then there exists a unique autoprojectivity φ of X such that $Y^\varphi = Y^{\varphi_n}$ for every n in $\mathbb{N}$ and every subgroup Y of X_n.

PROPOSITION 2.9. *If φ is an automorphism of $M(R)$, then there exists a unique autoprojectivity ψ of R inducing φ on $M(R)$.*

Proof. For every n, let $R_n = \Omega_n(R)$ and let φ_n be the automorphism of $M(R_n)$ induced by φ. By Lemma 3 in [8], there exists a unique autoprojectivity ψ_n of R_n inducing φ_n on $M(R_n)$. By Lemma 2.8 there exists an autoprojectivity ψ of R such that $Y^\psi = Y^{\psi_n}$ for every n in $\mathbb{N}$ and every subgroup Y of R_n. It is clear that ψ induces φ on $M(R)$. ∎

We can therefore prove

PROPOSITION 2.10. *If for every prime q we have an automorphism φ_q of $M(H_q)$, then there exists a (unique) autoprojectivity φ of H such that $X^{\varphi_q} = X^{\varphi}$ for every q and every cyclic subgroup X of H_q.*

Proof. By Proposition 2.9, we can extend every φ_q to an autoprojectivity $\bar{\varphi}_q$ of H_q. If X is any subgroup of H, we define $X^{\varphi} = \vee X_q^{\bar{\varphi}_q}$. Then φ is an autoprojectivity of H and it induces φ_q on $M(H_q)$. ∎

We actually have $\mathrm{Aut}\, L(H) \cong \mathrm{Cr}\, \mathrm{Aut}\, M(H_q)$, since every autoprojectivity of H is index-preserving. We shall identify $\mathrm{Aut}\, L(H)$ with $\mathrm{Cr}\, \mathrm{Aut}\, M(H_q)$.

LEMMA 2.11. *Let μ be an autoprojectivity of H_r, for a certain prime r. If μ fixes every cyclic subgroup of H_r which is fixed by a non-trivial element of W, then it also fixes every subgroup of H_r which is fixed by a non-trivial element of W. Moreover μ commutes with the action of W if and only if we have $C^{w\mu} = C^{\mu w}$ for every cyclic subgroup C.*

Proof. The second part is obvious. For the first, see the proof of Proposition 1.3. ∎

We are now in the position to describe the group $\Gamma(G)$.

DEFINITION 2.12. *For every prime r different from p we denote by Λ_r the group of automorphisms μ of H_r, satisfying the following conditions.*

(a) *μ commutes with the action of W;*

(b) *μ fixes every cyclic subgroup of H_r which is fixed by a non-trivial element of W;*

(c) *let s be an element of H_r not satisfying $(*')$. Then μ fixes $\langle s \rangle$ if r is not 3. If r is 3, then μ fixes $\langle s \rangle$ if $\langle s \rangle \geq Z$, and it fixes $\langle s^3 \rangle$ otherwise.*

THEOREM 2.13. *Let G be the group $SL_3(K)$. For every element $(\mu_q)_{q \neq p}$ in $\mathrm{Cr}\, \Lambda_q$, there exists a unique exceptional autoprojectivity φ of G inducing μ_q on H_q for each q. The map so obtained is an isomorphism of $\mathrm{Cr}\, \Lambda_q$ onto $\Gamma(G)$.*

Proof. For each q, let Δ_q be the group of automorphisms of $M(H_q)$ induced by $\Gamma(G)$ on $M(H_q)$. By Theorem 1.12 and Corollary 1.8 we have $\Delta_q \leq \Lambda_q$. Let $(\mu_q)_{q \neq p}$ be an element of $\mathrm{Cr}\, \Lambda_q$, and let μ be the unique autoprojectivity of H inducing μ_q on H_q. By Lemma 2.11 and Theorem 2.7, μ lies in $\iota(\Gamma(G))$. Hence, under the identification of $\mathrm{Aut}\, L(H)$ with $\mathrm{Cr}\, \mathrm{Aut}\, M(H_q)$, we get $\iota(\Gamma(G)) \leq \mathrm{Cr}\, \Delta_q \leq \mathrm{Cr}\, \Lambda_q \leq \iota(\Gamma(G))$, so that $\Gamma(G)$ is isomorphic to $\mathrm{Cr}\, \Lambda_q$. ∎

Remark. It also follows that for each r, Λ_r coincides with the group of automorphisms of $M(H_r)$ induced by $\Gamma(G)$ on $M(H_r)$. We describe the structure of Λ_r. For this purpose, let us consider, for each k in $\mathbb{N}$, the restriction maps ρ_k: $\Lambda_r \to \mathrm{Aut}\, M(\Omega_k(H_r))$. We put $\Lambda_{r,k} = \mathrm{Im}\, \rho_k$. Note that if r is not 3, then $\Lambda_{r,k}$ coincides with the group of automorphisms of $M(\Omega_k(H_r))$ satisfying the conditions (a),(b),(c) of Definition 2.12. We define the epimorphism π_k: $\Lambda_{r,k+1} \to \Lambda_{r,k}$ by $\pi_k(\rho_{k+1}(f)) = \rho_k(f)$ for every f in Λ_r. It is then clear that Λ_r is (isomorphic to) the inverse limit of the system $(\Lambda_{r,k}, \pi_k)_{k\in\mathbb{N}}$. We show that for each k, $\Lambda_{r,k+1}$ contains a copy of $\Lambda_{r,k}$, and that $\Lambda_{r,k+1} \cong \Gamma_{r,k+1} \rtimes \Lambda_{r,k}$, where $\Gamma_{r,k+1} = \ker \pi_k$. Let k be in $\mathbb{N}$. We define a map j_k: $\Lambda_{r,k} \to \Lambda_r$. Let $E_1, \ldots, E_s$ be representatives of W-orbits of length 6 of cyclic subgroups of order r^k of H (if there are no such subgroups, we have $\Lambda_{r,k} = \{1\}$). For each $i = 1, \ldots, s$, we put $\mathscr{E}_i = \{X | X \in M(H_r),\ X \geq E_i\}$. Let i_0 be in $\{1, \ldots, s\}$. We denote by $E_{i_0,1}, \ldots, E_{i_0,r}$ the r cyclic subgroups of order r^{k+1} containing E_{i_0}. If X is an element of $\mathscr{E}_i$ of order r^{k+n}, with $n \geq 2$, we write $X = E_{i_0,i_1,\ldots,i_n}$, with $i_1, \ldots, i_n \in \{1, \ldots, r\}$ choosing the indices in order to have $\Omega_{k+n-1}(X) = E_{i_0,i_1,\ldots,i_{n-1}}$. Let φ be in $\Lambda_{r,k}$. We define the bijection $j_k(\varphi)$ of $M(H_r)$ onto itself as follows. Let $X \in M(H_r)$. If X lies in $\Omega_k(H_r)$, we put $X^{j_k(\varphi)} = X^{\varphi}$. Now assume X has order r^{k+n}, with n in $\mathbb{N}$. If $\Omega_k(X)$ has W-orbit of length less than 6, we put $X^{j_k(\varphi)} = X$. Otherwise there exists uniquely i_0 in $\{1, \ldots, s\}$, $i_1, \ldots, i_n$ in $\{1, \ldots, r\}$, and w in W such that $X = E^w_{i_0,i_1,\ldots,i_n}$. Since φ lies in $\Lambda_{r,k}$, the W-orbit of $E^{\varphi}_{i_0}$ has length 6. Hence there exists a unique $\sigma(i_0)$ in $\{1, \ldots, s\}$ and a unique $w(i_0)$ in W, such that $E^{\varphi}_{i_0} = E^{w(i_0)}_{\sigma(i_0)}$. We put $X^{j_k(\varphi)} = E^{w(i_0)w}_{\sigma(i_0),i_1,\ldots,i_n}$. It follows that $j_k(\varphi)$ is an automorphism of $M(H_r)$ satisfying the conditions (a),(b),(c) of Definition 2.12, so that it lies in Λ_r. The map j_k is a monomorphism from $\Lambda_{r,k}$ to Λ_r, and we have $\rho_k(j_k(\varphi)) = \varphi$. In particular Λ_r is isomorphic to $\ker \rho_k \rtimes \Lambda_{r,k}$. Moreover we can get a similar decomposition for all the finite groups $\Lambda_{r,k}$. For every k we define the monomorphism δ_k: $\Lambda_{r,k} \to \Lambda_{r,k+1}$ as the composite of j_k and ρ_{k+1}. Then we have $\Lambda_{r,k+1} = \Gamma_{r,k+1} \rtimes \delta_k(\Lambda_{r,k})$, with $\delta_k(\Lambda_{r,k})$ isomorphic to $\Lambda_{r,k}$, and $\Gamma_{r,k+1} = \ker \pi_k$. We have therefore a recursive way to get all the groups $\Lambda_{r,k}$ starting from $\Lambda_{r,1}$.

So far we dealt with the group $SL_3(K)$. We now describe the relation between the groups $\mathrm{Aut}\, L(SL_3(K))$ and $\mathrm{Aut}\, L(PSL_3(K))$. Every autoprojectivity ψ of G fixes the centre $Z(G)$ of G, so that it induces the autoprojectivity $\bar{\psi}$ of $G/Z(G) = PSL_3(K)$. Hence there is a natural homomorphism π: $\mathrm{Aut}\, L(G) \to \mathrm{Aut}\, L(G/Z(G))$. We shall show that π is always surjective, and that it is injective if and only if the 3-component of $K^{\times}$ is infinite or is the identity or has order 3. For this purpose we make the following observation. The statements are trivial if the 3-component of

$K^\times$ is the identity. So assume $1 \leq \nu \leq \infty$, where $\nu = v_3(|(K^\times)_3|)$, so that $Z(G) = Z$. We observe that all the discussion we have done at the beginning for G can be extended to G/Z, as already proved for finite fields in [17]. In particular we have Aut $L(G/Z) = \Gamma(G/Z) \rtimes \mathrm{Aut}(G/Z)$, and $\Gamma(G/Z)$ embeds into Aut $L(H/Z)$. From the fact that every automorphism of G/Z is induced by a unique automorphism of G (cf. [7, Chap. IV, Sect. 6]), we are left to study the restriction of π (that we still denote by π) from $\Gamma(G)$ to $\Gamma(G/Z)$. To describe $\ker \pi$ we introduce the set $\mathscr{A}$ of all the cyclic subgroups C of H of order 3^ν, with the W-orbit of C of length 6 and $C \not\geq Z$. $\mathscr{A}$ is non-empty if and only if $2 \leq \nu < \infty$, and in this case it has $3^\nu - 3$ elements. Moreover $\mathscr{A}$ is clearly invariant under the action of $\Gamma(G)$.

PROPOSITION 2.14. *π is injective if and only if $\nu = 0, 1, \infty$. In the other cases* $\ker \pi$ *is isomorphic to $C_2 \times (S_3)^m$, where $m = (3^{\nu-2} - 1)/2$.*

Proof. We prove that π is injective if $(K^\times)_3$ is infinite or it has order 3. Let φ be an (exceptional) autoprojectivity of G fixing every subgroup containing Z. To prove that φ is the identity it is enough to show that it fixes every cyclic r-subgroup $\langle s \rangle$ of H. If r is not 3, then $\langle s \rangle$ is the unique r-Sylow subgroup of $\langle s, Z \rangle$ which is fixed by φ, and we are done. Suppose now $r = 3$. If $\nu = 1$, then we have $\langle s \rangle^\varphi = \langle s \rangle$ by Theorem 1.1(f). If $\nu = \infty$, we consider two cases. If $\langle s \rangle \geq Z$, then we are done. Otherwise let y be an element of H such that $y^3 = s$. We have $\mathrm{Frat}(\langle y, Z \rangle) = \langle s \rangle$. Hence $\langle s \rangle^\varphi = \langle s \rangle$, as the Frattini subgroup is clearly an invariant under projectivities.

To complete the proof it is enough to show that if $2 \leq \nu < \infty$, then $\ker \Pi$ is isomorphic to $C_2 \times (S_3)^m$, where $m = (3^{\nu-2} - 1)/2$. So we assume $2 \leq \nu < \infty$.

Let a be an element of order 3^ν in $K^\times$, and let $s = \mathrm{diag}(a, a^{-1}, 1)$. Let X_1, X_2 be the cyclic subgroups of order 3^ν containing s^3 and different from $\langle s \rangle$. Then X_1, X_2 lie in $\mathscr{A}$. Note that if ψ is in $\Gamma(G)$, then $X_1^\psi = X_1$ or X_2. If $\mathscr{A} = X_1^W$ (i.e., if $\nu = 2$), then we are done, since we can define the autoprojectivity μ of H_3, fixing every cyclic subgroup not in $\mathscr{A}$, and such that $X_1^{w\lambda} = X_2^w$ for each w in W (note that there exists an involution σ in W such that $X_1^\sigma = X_2$). We then extend μ to the autoprojectivity λ of H which is the identity on H_q for every $q \neq 3$. By Theorem 2.13, λ can be extended to an element of $\Gamma(G)$, which lies in $\ker \pi$.

Suppose now $\mathscr{A} \neq X_1^W$, and let Y_1 be in $\mathscr{A} \setminus X_1^W$. Let W_1, Z_1 be the cyclic subgroups order 3^ν containing Y_1^3 and different from Y_1. If ψ is in $\ker \pi$, then ψ leaves the set $\{Y_1, W_1, Z_1\}$ invariant. Moreover Y_1^W, W_1^W, Z_1^W are pairwise distinct orbits of length 6, and for each permutation τ of the set $\{Y_1, W_1, Z_1\}$ we can define a (unique) element φ_τ of $\ker \pi$ fixing every

cyclic r-subgroup not in $Y_1^W \cup W_1^W \cup Z_1^W$ and such that $Y_1^{\varphi_\tau} = Y_1^\tau$, $W_1^{\varphi_\tau} = W_1^\tau$, and $Z_1^{\varphi_\tau} = Z_1^\tau$. If $\mathscr{A} = X_1^W \cup Y_1^W \cup W_1^W \cup Z_1^W$, i.e., if $\nu = 3$, then we are done with $m = 1$. Otherwise we keep on with this process till we exhaust $\mathscr{A}$. ∎

THEOREM 2.15. *If $\nu = 0, 1, \infty$, then $\Gamma(G/Z)$ and $\Gamma(G)$ are isomorphic. If $2 \leq \nu < \infty$, then $\Gamma(G)$ is isomorphic to $(C_2 \times (S_3)^m) \rtimes \Gamma(G/Z)$, where $m = (3^{\nu-2} - 1)/2$. π is always surjective.*

Proof. The statement is trivial if $\nu = 0$. So we assume $1 \leq \nu \leq \infty$. Let f be in $\Gamma(G/Z)$, and let μ be the autoprojectivity of H/Z induced by f. Our aim is to define an autoprojectivity λ of H fixing Z, inducing μ on H/Z, and satisfying the hypothesis of Theorem 2.7. By Theorem 2.13, it is enough to define λ on $M(H_r)$, and prove that this restriction lies in Λ_r.

Let s be an r-element of H. If there exists a non-trivial element of W fixing $\langle s \rangle$, we put $\langle s \rangle^\lambda = \langle s \rangle$ (note that in this case μ fixes $\langle sZ \rangle$). So now assume that $\langle s \rangle$ is not fixed by any non-trivial element of W.

Let X be the unique subgroup of H containing Z such that $(\langle s, Z \rangle / Z)^\mu = X/Z$. If r is not 3 we define $\langle s \rangle^\lambda$ to be the unique r-Sylow subgroup of X. If $r = 3$ and $\langle s \rangle \geq Z$, we put $\langle s \rangle^\lambda = X$. We are left with the case $r = 3$ and $\langle s \rangle \not\geq Z$. Here we consider two cases. If there exists y in H such that $y^3 = s$ (and this is always the case if $\nu = \infty$), we put $\langle s \rangle^\lambda = \operatorname{Frat} Y$, where Y is the unique subgroup of H containing Z such that $(\langle y, Z \rangle / Z)^\mu = Y/Z$. Finally suppose there does not exist y in H such that $y^3 = s$. This means $\nu < \infty$, s has order 3^ν, and $\nu \geq 2$, since the W-orbit of $\langle s \rangle$ has length 6. We are therefore left to define λ on the set $\mathscr{A}$ previously defined. We write $\mathscr{A}$ as the disjoint union of W-orbits in the following way. $\mathscr{A} = X_1^W \cup (X_{1,1}^W \cup X_{1,2}^W \cup X_{1,3}^W) \cup \cdots \cup (X_{m,1}^W \cup X_{m,2}^W \cup X_{m,3}^W)$, where $X_1 = \langle \operatorname{diag}(a, a^{-1+3^{\nu-1}}, a^{-3^{\nu-1}}) \rangle$, $m = (3^{\nu-2} - 1)/2$, and $X_{i,1}^3 = X_{i,2}^3 = X_{i,3}^3$ for each $i = 1, \ldots, m$. We denote this last subgroup by Y_i. We define λ on X_1 and the $X_{i,j}$'s, and extend the definition of λ on $\mathscr{A}$, requiring commutativity with the W-action. We put $X_1^\lambda = X_1$. For each i in $\{1, \ldots, m\}$, we note that the W-orbit of Y_i has length 6, and that we have already defined Y_i^λ. Since μ commutes with the W-action (cf. the theorem in [17]), there exists a unique $\sigma(i)$ in $\{1, \ldots, m\}$, and a unique $w(i)$ in W such that $Y_i^\lambda = Y_{\sigma(i)}^{w(i)}$. We put $X_{i,j}^\lambda = X_{\sigma(i),j}^{w(i)}$ for each $j = 1, 2, 3$. Hence we have defined the autoprojectivity λ of H, inducing μ on H/Z, commuting with the W-action and fixing every subgroup of H fixed by a non-trivial element of W. Suppose now that s does not satisfy $(*')$. With a procedure similar to the one used in Lemma 1.10, one can show that $(\langle s, Z \rangle / Z)^\mu = \langle s, Z \rangle / Z$. Hence $\langle s \rangle^\lambda = \langle s \rangle$ if s is determined, and $\langle s^3 \rangle^\lambda = \langle s^3 \rangle$ if s is almost determined.

By Theorem 2.7, there exists a unique element φ in $\Gamma(G)$ inducing λ on H and therefore μ on H/Z. Then the exceptional autoprojectivities $\bar{\varphi}$ and

f of G/Z both induce μ on H/Z, so that they must coincide. We have therefore proved that π is always surjective. We now prove the rest of the assertions. If $\nu = 0, 1, \infty$, then, by Proposition 2.14, π is an isomorphism, and we are done. So suppose $2 \leq \nu < \infty$. To underline the fact that φ depends on f, we write φ_f instead of φ, and we put $M = \{\varphi_f | f \in \Gamma(G/Z)\}$. From a direct calculation it follows that the map $f \mapsto \varphi_f$ is a homomorphism. Since $\pi(\varphi_f) = f$, it follows that $\Gamma(G)$ is the semidirect product of $\ker \pi$ and M, and that M is isomorphic to $\Gamma(G/Z)$. Then we are done by Proposition 2.14. ∎

As a corollary of the proof of Proposition 2.14 we get

COROLLARY 2.16. *For every X in $\mathscr{A}$, there exists φ in $\Gamma(G)$ such that $X^{\varphi} \neq X$.*

3. THE MAIN RESULT

In this section we shall use Theorem 2.13 to construct exceptional autoprojectivities of G for certain families of fields K. We first give some arithmetic conditions between the primes p and r such that every φ in $\Gamma(G)$ induces the identity on H_r.

Let r be a prime different from p, and let n be in $\mathbb{N}$. We denote by $\delta(n)$ the order of p in $(\mathbb{Z}/r^n\mathbb{Z})^{\times}$ (hence $\mathbf{F}_{p^{\delta(n)}}$ is the smallest subfield of $\bar{\mathbf{F}}_p$ containing elements of order r^n). We shall write δ instead of $\delta(1)$.

PROPOSITION 3.1. *Let s be an element of order r^n of H not satisfying $(*')$. Suppose $v_r(|(K^{\times})_r|) \geq n + 1$ and we are in one of the following situations:*

(a) *s is almost determined or s is determined but $r \neq 3$, and $r^{n+1} \nmid p^{\delta(n)} - 1$;*

(b) *$r = 3$, $n \geq 2$, s is determined and $3^n \leq p^{\delta(n-1)} - 1$.*

Then every cyclic subgroup of H of order r^{n+1} containing $\langle s \rangle$ is generated by an element not satisfying $(*')$.

Proof. Let $\alpha_i(s)^{p^m} = \alpha_j(s)$ with $i < j$. Let C be a cyclic subgroup of H of order r^{n+1} containing $\langle s \rangle$. Since $\alpha_i(s)$ and $\alpha_j(s)$ in this case have the same order, this must be the maximal possible order r^f among the orders of $\alpha_1(s), \alpha_2(s), \alpha_3(s)$. If r is not 3, then $f = n$. If $r = 3$, then we have $f = n$ if $\langle s \rangle \not\geq Z$ and $f = n - 1$ if $\langle s \rangle \geq Z$. Suppose we are in case (a), so

that we have $|\alpha_i(s)| = |\alpha_j(s)| = r^n$. We put $m_1 = m$, $m_2 = m + \delta(n), \ldots, m_r = m + (r-1)\delta(n)$. Suppose r is not 3. For each $k = 1, \ldots, r$, there exists an element t_k of order r^{n+1} such that $\alpha_i(t_k)^{p^{m+(k-1)\delta(n)}} = \alpha_j(t_k)$. Since $r^{n+1} \nmid p^{\delta(n)} - 1$, the groups $\langle t_1 \rangle, \ldots, \langle t_r \rangle$ are all distinct, so that there exists k such that $C = \langle t_k \rangle$ and we are done. If r is 3, for each k there are 3 distinct subgroups $\langle t_{k,1} \rangle$, $\langle t_{k,2} \rangle$, and $\langle t_{k,3} \rangle$ such that $\alpha_i(t_{k,l})^{p^{m+(k-1)\delta(n)}} = \alpha_j(t_{k,l})$ for each $l = 1, 2, 3$. Then there exist a unique k and a unique l such that $C = \langle t_{k,l} \rangle$, and we are done.

Suppose now we are in case (b). Here we have $|\alpha_i(s)| = |\alpha_j(s)| = 3^{n-1}$. We put $m_1 = m$, $m_2 = m + \delta(n-1)$, $m_3 = m + 2\delta(n-1)$. For each $k = 1, 2, 3$, let t_k be an element of order 3^{n+1} such that $\alpha_i(t_k)^{p^{m+(k-1)\delta(n-1)}} = \alpha_j(t_k)$. Since $3^n \nmid p^{\delta(n-1)} - 1$, the groups $\langle t_1 \rangle, \ldots, \langle t_3 \rangle$ are all distinct, so that there exists k such that $C = \langle t_k \rangle$ and we are done. ∎

LEMMA 3.2. *If $r > 2$, $a \equiv 1 \bmod r$ or $r = 2$, $a \equiv 1 \bmod 4$ then we have $v_r(a^\beta - 1) = v_r(\beta) + v_r(a - 1)$.*

Proof. See [13, p. 401, Formula (8)]. ∎

THEOREM 3.3. *Let φ be in $\Gamma(G)$, and let s be an element of order r^n of H not satisfying $(*')$. Let $\nu = v_3(|(K^\times)_3|)$. Suppose one of the following condition holds:*

(i) *if r is at least 5, $n = v_r(p^\delta - 1)$;*

(ii) *$r = 2$, $n = v_2(p^{\delta(2)} - 1)$.*

(iii) *$r = 3$, then $n = v_3(p^\delta - 1)$ if $\langle s \rangle \not\geq Z$ and $n - 1 = v_3(p^\delta - 1)$ if $\langle s \rangle \geq Z$.*

Then φ fixes every cyclic r-subgroup of H containing s if s is determined. If s is almost determined, then φ fixes every cyclic subgroup containing s^3 and not containing Z of order less then 3^ν (all of them if $\nu = \infty$).

Proof. Suppose s is determined. If r is not 3, by Lemma 3.2 we have $\delta(n + j) = \delta(n)r^j$, for every j in $\mathbb{N}$. By Proposition 3.1 and induction on j, every cyclic subgroup C of H containing $\langle s \rangle$ is generated by a determined element. Hence φ fixes C by Proposition 1.11. If r is 3, by Lemma 3.2 we get $\delta(n + j - 1) = \delta(n - 1)3^j$, for every j. Then we conclude as in the previous case.

Suppose now that s is almost determined. If $\nu = n$, then we have $\langle s^3 \rangle^\varphi = \langle s^3 \rangle$ by Proposition 1.11 and we are done. So assume $\nu > n$. We prove that φ fixes every cyclic subgroup C of H of order 3^n containing s^3, and not containing Z. Lemma 3.2 and induction will then give the result for every C of order less then 3^ν and for all of them if $\nu = \infty$. Since

$C \leq \langle s \rangle \times Z$, C is generated by an almost determined element. By Proposition 3.1, every cyclic subgroup of H of order 3^{n+1} containing C is generated by an almost determined element. Then by Proposition 1.11, φ fixes C. ∎

COROLLARY 3.4. *Let φ be in $\Gamma(G)$, and let $\nu = v_3(|(K^\times)_3|)$.*

If r is at least 5, $r^2 \nmid p^{r-1} - 1$, and s is an element of order r of H not satisfying $(**')$, then φ fixes every cyclic r-subgroup of H containing s.

If $p \equiv 3$ or $5 \bmod 8$, then φ fixes every 2-subgroup of H.

If $p \equiv 2, 4, 5$, or $7 \bmod 9$, then φ fixes every cyclic 3-subgroup of H not containing Z of order less than 3^ν (all of them if $\nu = \infty$). The same holds if $p \equiv 8, 10, 17$, or $19 \bmod 27$.

If $p \equiv 2, 4, 5$, or $7 \bmod 9$, then φ fixes every cyclic 3-subgroup of H containing Z.

Proof. Suppose $r \geq 5$. Since φ commutes with the inner automorphisms, we may assume that s is determined. The condition $r^2 \nmid p^{r-1} - 1$ implies $v_r(p^\delta - 1) = 1$, so that we are done by Theorem 3.3. Suppose now s is a 2-element of H. We already know that φ fixes every cyclic subgroup of order 2, 4, and 8, since the W-orbits of such groups have length 3. So assume s has order at least 16. Let s' be an element of order 4 in $\langle s \rangle$ if $p \equiv 5 \bmod 8$, and of order 8 if $p \equiv 3 \bmod 8$. Suppose $p \equiv 5 \bmod 8$. Every element of order 4 does not satisfy $(**')$, so we may suppose that s' is determined. We have $\delta(2) = 1$, $v_2(p - 1) = 2$, so that by Theorem 3.3, φ fixes every cyclic 2-subgroup containing s'. Hence φ fixes $\langle s \rangle$. If $p \equiv 3 \bmod 8$, from a direct calculation (see the next Section) it follows that every element of order 8 does not satisfy $(**')$. Then we conclude by Theorem 3.3, as $\delta(2) = 2$, $v_2(p^2 - 1) = 3$.

Suppose finally that s is a 3-element of H. We note that every element of order 3 or of order 9 does not satisfy $(**')$. We first consider the case when $\langle s \rangle \not\geq Z$. If $\nu = 1, 2$, there is nothing to prove, since by Theorem 1.1(f), φ fixes every subgroup of order 3. So we assume $\nu \geq 3$, and s of order $3^{\nu-1}$ if $\nu \neq \infty$, and s of order at least 9 if $\nu = \infty$. Let s', s'' be elements of order respectively 3 and 9 in $\langle s \rangle$. We may suppose s' and s'' are almost determined. If $p \equiv 4, 7 \bmod 9$, we have $\delta = 1$, $v_3(p - 1) = 1$. If $p \equiv 2, 5 \bmod 9$, we have $\delta = 2$, $v_3(p^2 - 1) = 1$. Then we conclude applying Theorem 3.3 to $\langle s' \rangle$. Suppose now that $p \equiv \pm 1 \bmod 9$. If $p \equiv 10, 19 \bmod 27$, we get $\delta = 1$, $v_3(p - 1) = 2$. If $p \equiv 8, 17 \bmod 27$, we get $\delta = 2$, $v_3(p^2 - 1) = 2$. Again we conclude by Theorem 3.3 applied to $\langle s'' \rangle$.

Suppose now $\langle s \rangle \geq Z$. If s has order 3, then $\langle s \rangle = Z$ and we are done. So suppose s has order at least 9, and $p \equiv 2, 4, 5, 7 \bmod 9$. Let s' be an

element of order 9 in $\langle s \rangle$. We may assume s' is determined. Then φ fixes $\langle s \rangle$ by Theorem 3.3 applied to $\langle s' \rangle$. ∎

From the discussion so far developed, it is clear that to construct autoprojectivities of H satisfying the conditions of Theorem 2.13, we need a more explicit description of elements of H satisfying $(**')$. We recall that if r is a prime different from p, and n is in $\mathbb{N}$, we denoted by $\delta(n)$ the order of p in $(\mathbb{Z}/r^n\mathbb{Z})^\times$.

DEFINITION 3.5. Let x, y be integers. We say that x, y are equivalent mod r^n, and we write $x \sim y(r^n)$ (or $x \sim y$ if there is no ambiguity) if there exists an integer γ with $0 \leq \gamma < \delta(n)$ such that $p^\gamma x \equiv y \bmod r^n$.

This is clearly an equivalence relation. Also, if $x, y \not\equiv 0 \bmod r$, then $x \sim y(r^n) \Leftrightarrow y/x$ lies in the subgroup of $(\mathbb{Z}/r^n\mathbb{Z})^\times$ generated by p.

We fix an r-element $s = \operatorname{diag}(a, b, c)$ of H of order r^n. Since s satisfies $(**')$ if and only if wsw^{-1} satisfies $(**')$ for every w in W, we shall assume that a has order r^n. Then $s = \operatorname{diag}(a, a^h, a^{-1-h})$ for a certain integer $h \bmod r^n$. We put $x = h - 1$.

PROPOSITION 3.6. *s does not satisfy $(**')$ if and only if at least one of the following equivalences* mod r^n *holds*:

$$x \sim \varepsilon(x + 3), \qquad x \sim \varepsilon(2x + 3), \qquad x + 3 \sim \varepsilon(2x + 3), \text{ with } \varepsilon = \pm 1.$$

Proof. This follows from a direct calculation. ∎

If x is an integer with $x \neq 0, -3$, we put $a_1(x) = (x + 3)/x$, $a_2(x) = (2x + 3)/x$, $a_3(x) = (2x + 3)/(x + 3)$. Note that $a_1(x)a_3(x) = a_2(x)$. Whenever x and $x + 3$ are invertible in $\mathbb{Z}/r^n\mathbb{Z}$, we shall consider the elements $a_i(x)$ as elements of $\mathbb{Z}/r^n\mathbb{Z}$.

By Proposition 3.6, s does not satisfy $(**')$ if and only if there exists an integer γ with $0 \leq \gamma < \delta(n)$ such that x is a solution of one of the following linear equations mod r^n:

(1) $p^\gamma X = X + 3$, i.e., $(p^\gamma - 1)X = 3$,

(2) $p^\gamma X = -(X + 3)$, i.e., $(p^\gamma + 1)X = -3$,

(3) $p^\gamma X = 2X + 3$, i.e., $(p^\gamma - 2)X = 3$,

(4) $p^\gamma X = -(2X + 3)$, i.e., $(p^\gamma + 2)X = -3$,

(5) $p^\gamma(X + 3) = 2X + 3$, i.e., $(p^\gamma - 2)X = 3(1 - p^\gamma)$,

(6) $p^\gamma(X + 3) = -(2X + 3)$, i.e., $(p^\gamma + 2)X = -3(1 + p^\gamma)$.

The problem is therefore reduced to studying the solutions of the above family $\mathcal{F}_n$ of $6\delta(n)$ equations (if $\delta(n)$ is even and r is odd, then it is enough to study only $3\delta(n)$ equations). It is clear that if r is not 3, each equation has at most one solution.

DEFINITION 3.7. Let y be an integer mod r^n. We denote by $N_n(y)$ the number of equations in $\mathcal{F}_n$ of which y is a solution.

COROLLARY 3.8. *s satisfies $(**')$ if and only if $N_n(x) = 0$.*

We shall make use of the following

LEMMA 3.9. *Let y be an integer* mod r^n, *and let A be a natural number. If for $\delta(n) = A$ we have $N_n(y) = 0$, then whenever $\delta(n)$ divides A, we have $N_n(y) = 0$.*

Proof. This is obvious. ∎

We describe more explicitly the situation when $n = 1$. We just write δ for $\delta(1)$, $\mathcal{F}$ for $\mathcal{F}_1$, and $N(y)$ for $N_n(y)$. H as $r + 1$ subgroups of order r, which are permuted by W. Each of them, except $\langle \mathrm{diag}(1, a, a^{-1})\rangle$, has a generator of the form $t_j = \mathrm{diag}(a, a^j, a^{-1-j})$ for a unique integer j mod r. For convenience we put $t_\infty = \mathrm{diag}(1, a, a^{-1})$, and denote by Ω the set $\mathbb{Z}/r\mathbb{Z} \cup \{\infty\}$. If $r = 2$, there is just one W-orbit of length 3. If $r = 3$, then there is one orbit of length 3 and one orbit of a single element (the center of G). If $r \geq 5$ there are always two orbits of length 3 (the orbits of $\langle t_0\rangle$ and of $\langle t_1\rangle$), and there is one orbit of length 2 if and only if $r \equiv 1 \bmod 3$ (the orbit of $\langle t_\theta\rangle$, where $\theta^3 \equiv 1 \bmod r$, but $\theta \not\equiv 1 \bmod r$). All the other orbits have length six. If $r = 2, 3$, then s does not satisfy $(**')$. We assume $r \geq 5$. Each equation in $\mathcal{F}$ has in particular at most one solution: we denote by $x_i(\gamma)$ the solution of the ith equation corresponding to γ if this equation has a solution. Otherwise we put $x_i(\gamma) = \infty$. We denote by $N(\infty)$ the number of equations with no solution (this notation is in fact consistent, as we could see introducing appropriate homogeneous coordinates for Ω, and rewriting the equations (1)–(6) in terms of these coordinates). We define an action of W on Ω. Let y be in Ω, $Y = \langle t_{y+1}\rangle$, w in W. We put $y^w = y'$, where $Y^w = \langle t_{y'+1}\rangle$ (convention: $\infty = \infty - 1 = \infty + 1$). We get $y^W = \{y, -y - 3, -y/(y + 1), -(2y + 3)/(y + 1), -(y + 3)/(y + 2), -(2y + 3)/(y + 2)\}$. It is clear that the W-orbits of y and Y have the same length, and that $N(y^w) = N(y)$ for every w in W. From the previous discussion, we always have the orbits $\{0, -3, (r - 3)/2\}$ and $\{\infty, -1, -2\}$, and the orbit $\{\theta - 1, \theta^2 - 1\}$ if $r \equiv 1 \bmod 3$. We are interested in the number m of orbits of length six. We have $m = (r - 5)/6$ if $r \not\equiv 1 \bmod 3$ and $m = (r - 7)/6$ if $r \equiv 1 \bmod 3$. Let $y_1, \ldots, y_m$ be repre-

sentatives of each orbit of length six. We get the equations

$$\begin{aligned} 3N(0) + 3N(\infty) & \\ + 6(N(y_1) + \cdots + N(y_m)) &= 6\delta \quad \text{if } r \not\equiv 1 \bmod 3, \qquad (\therefore) \\ 3N(0) + 3N(\infty) + 2N(\theta - 1) & \\ + 6(N(y_1) + \cdots + N(y_m)) &= 6\delta \quad \text{if } r \equiv 1 \bmod 3, \end{aligned}$$

with $N(0), N(\infty) \geq 1$, since $0 = x_5(0)$ and $\infty = x_1(0)$. It is also clear that for every x in $\mathbb{Z}/r\mathbb{Z} \cup \{\infty\}$ we have $N(x) \in \{0, 1, 2, 3, 6\}$, $N(0) \in \{1, 2\}$, and $N(\theta - 1) \in \{0, 3, 6\}$.

Observation 3.10. In practice it is more convenient to study the equations (1)–(6) allowing the coefficients on the left hand side to be any element of a certain subgroup C of $(\mathbb{Z}/r\mathbb{Z})^\times$, and then analyse for which p we have $\langle p \rangle \leq C$ (it is known (Corollary 3 on page 191 in [10]) that the polar density of the set of primes p in C is $|C|/(r - 1)$). It is obvious that the equations $(\therefore)$ will then hold with $|C|$ instead of δ.

We also note that for certain primes p there exists integers x for which at least one of the $\pm a_i(x)$ (as an element of $\mathbb{Q}$) is an integral power of p. For these x it is clear that $N(x) \neq 0$ for each r. The possibilities (besides $x = 0, -1, -2, -3$) are

$x = 3, -6$ for $p = 2$ or 3,

$x = 1, -4$ for $p = 2$ or 5 (note that $-6 \in 3^W$ and $-4 \in 1^W$).

PROPOSITION 3.11. *Let $\delta \leq m$. Then for at least one i we have $N(y_i) = 0$.*

Proof. We have $m \geq 1$. Suppose $N(y_j) > 0$ for each j. From the equations $(\therefore)$ we get $\delta \geq m + 1$, a contradiction. ∎

PROPOSITION 3.12. *Let $r \equiv 1 \bmod 3$. If δ divides $(r - 1)/3$, then there exists y such that $N(y) = 0$.*

Proof. Suppose $\delta = (r - 1)/3$. Then δ is even, so that each $N(z)$ is even. If there exists i such that $N(y_i) = 0$, then we are done. Otherwise we have $N(0), N(\infty), N(y_i) \geq 2$ for each i. But then $3N(0) + 3N(\infty) + 2N(\theta - 1) + 6(N(y_1) + \cdots + N(y_m)) = 6\delta$ implies $N(0) = N(\infty) = N(y_i) = 2$ for each i, and $N(\theta - 1) = 0$, and we are done. By Lemma 3.9 we get the result for each δ dividing $(r - 1)/3$. ∎

On the other hand the equations in $\mathcal{F}$ can be used to prove the following statement.

PROPOSITION 3.13. *Suppose $r \geq 5$. If $\delta = r - 1$ or $(r-1)/2$, then we have $N(x) \neq 0$ for each integer x. The same holds if $\delta = (r-1)/4$, when $r \equiv 5 \bmod 8$. If moreover $r^2 \nmid p^{r-1} - 1$, then $\Lambda_r = \{1\}$.*

Proof. We prove the first part. One is reduced to show that in each case the subgroup $\langle p \rangle$ of $(\mathbb{Z}/r\mathbb{Z})^\times$ contains at least one among $\pm a_1(x)$, $\pm a_2(x)$, $\pm a_3(x)$, for every x in $\mathbb{Z}/r\mathbb{Z}$ different from $0, -3, -3/2$. This is of course the case if $\delta = r - 1$. Also, since $a_1(x)a_3(x) = a_2(x)$, for at least one i we have $a_i(x)^{(r-1)/2} = 1$, so that $a_i(x)$ lies in the subgroup C of index 2 in $(\mathbb{Z}/r\mathbb{Z})^\times$. Hence the result if $\delta = (r-1)/2$. Moreover, if $r \equiv 5 \bmod 8$, then one of $a_i(x)$ and $-a_i(x)$ lies in C^2, and we get the result for $\delta = (r-1)/4$. The second part now comes from Corollary 3.4. ∎

We start now to consider the problem of constructing exceptional autoprojectivities. In the discussion so far developed, we have given a list of conditions that guarantee that a certain cyclic r-subgroup of H is fixed by every element of $\Gamma(G)$. We shall prove that if there exists a cyclic r-subgroup X of H which does not satisfy any of the above mentioned conditions (in the next definition we shall call "free" such a subgroup), then there exists an exceptional autoprojectivity of G not fixing X.

DEFINITION 3.14. Let s be an r-element of H and $X = \langle s \rangle$. We say that X is "free" if the W-orbit of X has length 6 and if one of the following conditions holds:

(i) s satisfies $(**')$,

(ii) $r = 3$, s does not satisfy $(**')$, $X \not\geq Z$, and either X is maximal cyclic in H_3, or at least one (hence all) cyclic subgroup of order $3|X|$ containing X is generated by an element satisfying $(**')$.

We can summarize the results of Section 1 in

PROPOSITION 3.15. *Let X be an r-subgroup of H which is not "free." Then X is fixed by every element of $\Gamma(G)$.*

Observation 3.16. We introduce a standard procedure to construct certain exceptional autoprojectivities of G. Suppose we have "free" subgroups E_0, E_1 of H of order r^k, such that $E_1 \geq E_0^r$ (we do not exclude $E_0 = E_1$). Let $\nu = v_r(|(K^\times)_r|)$.

Let $\mathscr{E}_0$ (respectively $\mathscr{E}_1$) be the set of all cyclic subgroups of H_r containing E_0 (respectively E_1). Let us denote by $E_{0,1}, \ldots, E_{0,r}$ the r cyclic subgroups of order r^{k+1} containing E_0. If X is an element of $\mathscr{E}_0$ of

order r^{k+n}, with $n \geq 2$, we write $X = E_{0,i_1,i_2,\ldots,i_n}$, with $i_1, \ldots, i_n \in \{1, \ldots, r\}$, choosing the indices in order to have $\Omega_{k+n-1}(X) = E_{0,i_1,i_2,\ldots,i_{n-1}}$. Similarly for E_1. Let $X = E_{0,i_1,\ldots,i_n}$ be in $\mathscr{E}_0$, and let $\sigma = (\sigma_i)$ be in $(S_r)^{\mathbb{N}}$. We put $X^\sigma = E_{1,\sigma_1(i_1),\ldots,\sigma_n(i_n)}$. Suppose X, Y are in $\mathscr{E}_0$. Then we have $X^\sigma \leq Y^\sigma$ if and only if $X \leq Y$. Similarly for E_1. We distinguish two cases.

If $E_0^W = E_1^W$, for each σ in $(S_r)^{\mathbb{N}}$ we define the autoprojectivity λ_σ of H to be the identity on H_q if $q \neq r$. Let X be a cyclic subgroup of H_r. We put $X^{\lambda_\sigma} = X$ if $\Omega_k(X)$ does not lie in E_0^W. Otherwise there exists a unique w in W such that $X^w \in \mathscr{E}_0$. We put $X^{\lambda_\sigma} = X^{w\sigma w^{-1}}$.

If $E_0^W \neq E_1^W$, for each σ, τ in $(S_r)^{\mathbb{N}}$ we define the autoprojectivity $\lambda_{\sigma,\tau}$ of H to be the identity on H_q if $q \neq r$. Let X be a cyclic subgroup of H_r. We put $X^{\lambda_{\sigma,\tau}} = X$ if $\Omega_k(X)$ does not lie in $E_0^W \cup E_1^W$. Otherwise there exists a unique w in W such that $X^w \in \mathscr{E}_0 \cup \mathscr{E}_1$. We put $X^{\lambda_{\sigma,\tau}} = X^{w\sigma w^{-1}}$ if $X^w \in \mathscr{E}_0$, and $X^{\lambda_{\sigma,\tau}} = X^{w\tau w^{-1}}$ if $X^w \in \mathscr{E}_1$. In both cases λ_σ or $\lambda_{\sigma,\tau}$ satisfies the hypothesis of Theorem 2.13, so that it can be uniquely extended to an element φ_σ or $\varphi_{\sigma,\tau}$ of $\Gamma(G)$.

We have therefore proved in particular the following things. If $\nu = \infty$, then $\Gamma(G)$ (and $\Gamma(G/Z)$ by Proposition 2.9) contains a copy of $(S_r)^{\mathbb{N}}$: we just need to take $E_0 = E_1$, and consider the subgroup $\{\varphi_\sigma | \sigma \in S_r)\}$ of $\Gamma(G)$. Similarly, if $k < \nu < \infty$, $\Gamma(G)$ contains a copy of $(S_r)^{\nu-k}$.

On the other hand, if $E_0 \neq E_1$, then there exists φ in $\Gamma(G)$ such that $E^\varphi = E_1$ (we just take $\varphi = \varphi_1$ or $\varphi_{1,1}$, and the construction works for every $k \leq \nu \leq \infty$).

LEMMA 3.17. *Let X be a "free" subgroup of H. Then there exists a "free" subgroup Y of the same order of X containing X^r but different from X.*

Proof. Let r^n be the order of X. We put $X^r = C$.

Suppose the W-orbit of C has length less than 6. Then there exists $w \neq 1$ such that $C^w = C$. Then we can take $Y = X^w$ and we are done. Hence we suppose the W-orbit of C has length 6 (in particular $n \geq 2$). We suppose for a contradiction that such a Y does not exist.

Suppose first r is not 3. If C is "free," then every cyclic subgroup containing C is "free," and we may take Y to be any of the cyclic subgroups of order $|X|$ containing C and different from X. Hence C is not "free." We may suppose $C = \langle s \rangle$ with $s = \mathrm{diag}(a, a^h, a^{-1-h})$ with a of order r^{n-1}, and $N_{n-1}(h-1) \neq 0$. If $r^n \nmid p^{\delta(n-1)} - 1$, by Proposition 3.1, X is not "free." Hence $r^n | p^{\delta(n-1)} - 1$. Suppose $r \neq 2$. By Lemma 3.2 we must have $r^n | p^\delta - 1$, so that each equation in $\mathscr{F}_{n-1}$ satisfied by $h-1$ can be lifted only to one equation in $\mathscr{F}_n$. If $N_{n-1}(h-1)$ is 6, we must have $-1 \equiv p^\gamma \bmod r^{n-1}$, for a certain integer γ, so that $N_n(y)$ is even for every integer y. Hence we get $r \leq 4$, which is a contradiction. Therefore

we are left with $N_{n-1}(h-1) \leq 3$, which again gives the contradiction $r \leq 4$. Thus we are done if $r \neq 2$.

Suppose $r = 2$. We must have $n \geq 5$, since the W-orbits of cyclic subgroups of order 2, 4, or 8 have length 3. By Lemma 3.2 we have $2^n | p^{\delta(2)} - 1$. If $\delta(2) = 1$, then C is conjugate either to $\langle \mathrm{diag}(a, a, a^{-2}) \rangle$ or to $\langle \mathrm{diag}(a, 1, a^{-1}) \rangle$. If $\delta(2) = 2$, besides the previous possibilities, C may be conjugate to $\langle \mathrm{diag}(a, a^i, a^{-1-i}) \rangle$ with $i = 2^{n-2} - 1$ or $2^{n-2} + 1$ (i.e., $i^2 \equiv 1 \bmod 2^{n-1}$). In all cases the W-orbit of C would be of length 3, and this is a contradiction.

We are left with the case $r = 3$. Suppose first that X is generated by an element not satisfying $(**')$. We may assume that this element is almost determined. If X is maximal cyclic in H_3, then we can take for Y any of the two cyclic subgroups of order 3^n in $X \times Z$ different from X, and we are done. So assume X is not maximal cyclic, but the cyclic subgroups X_1, X_2, X_3 of order $3|X|$ containing X are generated by elements satisfying $(**')$. By Proposition 3.1 we have $3^{n+1} | p^{\delta(n)} - 1$, so that $3^{n+1} | p^{\delta} - 1$, by Lemma 3.2. Since $\delta = 1$ or 2, the W-orbit of C has length 3, which is a contradiction. Hence X is generated by an element satisfying $(**')$. We have two cases. If $X \geq Z$, we may assume that C is generated by a determined element. By Proposition 3.1 we must have $3^{n-1} | p^{\delta(n-2)} - 1$ (note that $n \geq 3$, since the W-orbit of a cyclic subgroup of order 9 containing Z has order 3). Hence by Lemma 3.2 we must have $3^{n-1} | p^{\delta} - 1$. But $\delta = 1$ or 2, and in both cases we get that C is conjugate to $\langle \mathrm{diag}(u, u, u^{-2}) \rangle$ whose W-orbit has length 3. This is a contradiction. Therefore we must have $X \not\geq Z$. But, if X_1, X_2 are the cyclic subgroups of order 3^n in $X \times Z$ different from X, then both X_1, X_2 are "free." This is the final contradiction. ∎

THEOREM 3.18. *Let X be a "free" subgroup of H. Then there exists φ in $\Gamma(G)$ such that $X^{\varphi} \neq X$. In particular $\Gamma(G) \neq \{1\}$.*

Proof. By Observation 3.16 we only need to prove that there exists a "free" subgroup Y of the same order of X containing X^r but different from X, and this comes from Lemma 3.17. ∎

We give some arithmetic conditions between the primes p and r which ensure that the group Λ_r of automorphisms of $M(H_r)$ induced by $\Gamma(G)$ is not trivial.

PROPOSITION 3.19. *Let $\nu_r = v_r(|(K^{\times})_r|)$. Suppose $\nu_r \geq 1$ and one of the following conditions holds:*

(i) $r = 2$, $\nu_2 \geq 4$, *and* $p \equiv \pm 1 \bmod 8$.

(ii) $r \geq 11$ *and* $r | p^2 - 1$.

(iii) $r \geq 5$ *and* $r^2 | p^{r-1} - 1$.

(iv) $r \equiv 1 \bmod 3$, $r | p^{(r-1)/3} - 1$, *and* $\nu_r \geq 2$.

(v) $r = 3$, $\nu_3 \geq 3$, *and* $p \equiv \pm 1 \bmod 9$.

(vi) $r = 3$ *and* $2 \leq \nu_3 < \infty$.

(vii) $r \equiv 1 \bmod 9$ *and* $r | p^{(r-1)/3} - 1$.

(viii) $r \equiv 4, 7 \bmod 9$, $r | p^{(r-1)/3} - 1$, *and* $2^{(r-1)/3} \equiv 1 \bmod r$.

(ix) $r \equiv 1 \bmod 12$ *and* $\delta = (r-1)/6$.

Then Λ_r *is non-trivial.*

Proof. In all cases, by Lemma 3.17 and Observation 3.16, we only need to prove the existence of a certain r-subgroup which is "free." We recall that if a is an element of order r, and j is an integer, then t_j represents the element $\mathrm{diag}(a, a^j, a^{-1-j})$ of H.

(i) Let u be an element of order 8, and let $s = \mathrm{diag}(u, u^2, u^{-3})$. Then $p \equiv \pm 1 \bmod 8$ implies that $N_3(1) = 0$, so that s satisfies $(**')$. Since the two cyclic subgroups of order 16 containing $\langle s \rangle$ have W-orbit of length 6, they are both "free."

(ii) Since $r \geq 11$, we get $m \geq 1$. Then $\delta = 1$ or 2 implies that $N(y_i) = 0$ for every $i = 1, \ldots, m$. We can take $X = \langle t_{y_1+1} \rangle$, and we are done.

(iii) Since $r^2 | p^{r-1} - 1$, there exists in $K^\times$ an element u of order r^2. Let $s = \mathrm{diag}(u, 1, u^{-1})$. Then at least one among the cyclic subgroups of order r^2 containing s^r is "free." Suppose on the contrary $N_2(x) \neq 0$ for each x in $\mathbb{Z}/r^2\mathbb{Z}$ with $x \equiv -1 \bmod r$. If $N(-1) \neq 6$, we have $N(-1) \leq 3$ so that $r \leq 3$ which is a contradiction. Hence we have $N(-1) = 6$, which means -1 lies in the subgroup of $(\mathbb{Z}/r\mathbb{Z})^\times$ generated by p. Hence $N_2(y)$ is even for every integer y, and $r \leq 3$ which is again a contradiction.

(iv) Since $r | p^{(r-1)/3} - 1$, by Proposition 3.12 there exists y such that $N(y) = 0$. If there exists such a y with W-orbit of length 6, we are done. Otherwise we must have $N(\theta - 1) = 0$, where $\theta^3 \equiv 1 \bmod r$, but $\theta \not\equiv 1 \bmod r$. Then every cyclic subgroup of order r^2 except one containing $\langle t_\theta \rangle$ is "free."

(v) We can take $X = \langle \mathrm{diag}(u, u^{10}, u^{16}) \rangle$ where u has order 27, since $\delta(3) | 6$ implies that $N_3(9) = 0$ (see the next section).

(vi) This follows from Corollary 2.16.

(vii) and (viii) Let $\theta^3 \equiv 1 \bmod r$, but $\theta \not\equiv 1 \bmod r$. We have $a_1(\theta - 1) = \theta^2$, $a_2(\theta - 1) = -\theta$ and $a_3(\theta - 1) = -\theta^2$. Hence we have $N(\theta - 1) \neq 0$ if and only if δ is divisible by 3. Suppose $\delta = (r-1)/3$. If

$r \equiv 1 \bmod 9$, we get $N(\theta - 1) \neq 0$, so that by Proposition 3.12 there exists i with $N(y_i) = 0$, and we are done. Suppose now $r \equiv 4, 7 \bmod 9$. Since $2^{(r-1)/3} \equiv 1 \bmod r$, ± 2 lie in $\langle p \rangle$, so that $N(\infty) = 6$. This implies that there exists i with $N(y_i) = 0$. In both cases, by Lemma 3.9 we have $N(y_i) = 0$ for every δ dividing $(r - 1)/3$, and we are done.

(ix) Since $-1 \in \langle p \rangle$, $N(y)$ is even for every y. Suppose $N(y_i) \neq 0$ for each i (note that $m \geq 1$) we get $r - 1 \geq 12 + 2(r - 7)$, hence $1 \geq r$ which is a contradiction. Therefore there exists i with $N(y_i) = 0$, and we are done. ∎

In the previous section we considered the groups Λ_r, and we showed how each $\Lambda_{r,k}$ decomposes as a certain semidirect product for each k in $\mathbb{N}$. Here we describe the groups $\Lambda_{r,k}$ in a particular situation. First we assume that there are "free" subgroups of order r, and we let s be the number of i's for which $N(y_i) = 0$. Then $\Lambda_{r,1} \cong (S_3)^s \rtimes S_s$ (cf. the description given in Proposition 2 in [17]). Suppose $r \equiv 2 \bmod 3$ and $r^2 \nmid p^{r-1} - 1$. Let $Y_1, \ldots, Y_s$ be representatives of W-orbits of "free" subgroups of order r. We have $\Gamma_{r,2} \cong (S_r)^s$, since every cyclic r-subgroup C for which $\Omega(C) \notin Y_i^W$ for some i in $\{1, \ldots, s\}$, is fixed by every exceptional autoprojectivity by Corollary 3.4. By induction we get $\Gamma_{r,k+1} \cong (S_r)^{sr^{k-1}}$, for each k in $\mathbb{N}$. Since $\Lambda_{r,k+1} \cong \Gamma_{r,k+1} \rtimes \Lambda_{r,k}$ for each k, the groups $\Lambda_{r,k}$ are therefore completely described. Similarly one can deal also with the other cases. In particular, when $v_r(p^{r-1} - 1) \geq 2$, one has to take in account the fact that if for some x in $\mathbb{Z}/r\mathbb{Z}$ we have $N(x) = 3$, then we have one of the following situations. There may exist a unique y in $\mathbb{Z}/r^2\mathbb{Z}$ such that $y \equiv x \bmod r$ and $N_2(y) \neq 0$ (so that $N_2(y) = 3$), or there may exist 3 different $y, z, t \equiv x \bmod r$, for which $N_2 = 1$.

We conclude this section by proving the announced result that every simple algebraic group G of type A_2 over $\bar{\mathbf{F}}_p$ (i.e., G isomorphic either to $SL_3(\bar{\mathbf{F}}_p)$ or to $PGL_3(\bar{\mathbf{F}}_p)$) has autoprojectivities not induced by any automorphism. We shall also consider the behaviour of tori under exceptional autoprojectivities.

We make use of a result of A. Schinzel [14, Theorem 5]. For the convenience of the reader we state this result in the form we shall use it.

THEOREM. *Let $f(t)$ be a polynomial over $\mathbb{Q}$ and a an element of $\mathbb{Q}^\times$. If the congruence*

$$f(a^x) \equiv 0 \mod r$$

has a solution for almost all primes r, then the equation $f(a^x) = 0$ has a solution in $\mathbb{Q}$.

For our purposes we may assume that "almost all" means all but a finite number, even though the statement is true with wider assumptions.

THEOREM 3.20. *For every prime p the group $SL_3(\bar{\mathbf{F}}_p)$ has autoprojectivities not induced by any automorphism.*

Proof. It is equivalent to prove that $\Gamma(\mathrm{SL}_3(\bar{\mathbf{F}}_p))$ is non-trivial.

Let $f(t) = (t + a_1)(t - a_1)(t + a_2)(t - a_2)(t + a_3)(t - a_3)$ with $a_1 = 5/2$, $a_2 = 7/2$, $a_3 = 7/5$, and $a = p$. If the congruence $f(p^x) \equiv 0 \bmod r$ has a solution for al primes r greater than 13, then there exists γ in $\mathbb{Q}$ such that $p^\gamma = \pm a_i$ for some i. In particular γ is an integer, so that a_i is an integral power of p. This is a contradiction. Hence there exists a prime r greater than 13 for which $N(2) = 0$. By Corollary 3.8 the element $s = \mathrm{diag}(u, u^3, u^{-4})$, with u of order r, satisfies $(**')$. The fact that $r > 13$ ensures that $\langle s \rangle$ is not fixed by any nontrivial element of W. Hence $\langle s \rangle$ is "free," and by Theorem 3.18, $\Gamma(SL_3(\bar{\mathbf{F}}_p))$ is non-trivial. ∎

Remark. In fact using Schinzel's theorem we can say much more. Given *any* x in $\mathbb{Z} \setminus \{0, -1, -2, -3, 1, -4, 3, -6\}$ (cf. Observation 3.10) there always exists a prime r (even an infinite family of such primes) for which $\langle \mathrm{diag}(u, u^{x+1}, u^{-x-2}) \rangle$, with u of order r, is "free."

To prove the existence of primes r for which the group Λ_r of automorphisms of $M(H_r)$ induced by $\Gamma(SL_3(\bar{\mathbf{F}}_p))$ is non-trivial, we can follow an alternative way. Let us consider the Galois extension $M = \mathbb{Q}(\xi, p^{1/3})$ of $\mathbb{Q}$, where ξ is a primitive 3-root of 1 in $\mathbb{C}$. It is well known (cf. Exercise 30 on page 91 or Theorem 43 in [10]) that there are infinitely many primes r which completely split over $M/\mathbb{Q}$. (They can be obtained in the following way. Let α be an algebraic integer generating of M over $\mathbb{Q}$, for instance $\alpha = \xi + p^{1/3}$, μ the minimum polynomial of α over $\mathbb{Q}$, and n an integer. Then, excluding the primes 3 and p (Theorems 31, 24, and 34 in [10]), any prime divisor of $\mu(n)$ completely splits over $\mathbb{Q}$, and these are all.) Let r be one of these. Then we must have $r \equiv 1 \bmod 3$, and p is a cube in $\mathbb{Z}/r\mathbb{Z})^\times$. By Proposition 3.19(iv) we get $\Lambda_r \neq \{1\}$ (in the next section we shall consider in more detail this situation).

COROLLARY 3.21. *For every prime p, $PGL_3(\bar{\mathbf{F}}_p)$ has autoprojectivities not induced by any automorphism.*

Proof. Since $\bar{\mathbf{F}}_p$ is algebraically closed, $PGL_3(\bar{\mathbf{F}}_p)$ and $PSL_3(\bar{\mathbf{F}}_p)$ are isomorphic (as abstract groups). Then we are done by Theorem 2.15. ∎

THEOREM 3.22. *$\Gamma(SL_3(\bar{\mathbf{F}}_p))$ and $\Gamma(PGL_3(\bar{\mathbf{F}}_p))$ are infinite and non-soluble.*

Proof. Let r be a prime greater than 13 such that if u is an element of $\bar{\mathbf{F}}_p^\times$ of order r, then $s = \mathrm{diag}(u, u^3, u^{-4})$ satisfies $(**')$. If we apply

Observation 3.16 with $E_0 = E_1 = \langle s \rangle$, we get that $\Gamma(SL_3(\bar{\mathbf{F}}_p))$ (and $\Gamma(PGL_3(\bar{\mathbf{F}}_p))$) contains a copy of $(S_r)^{\mathbb{N}}$, and we are done. ∎

We can also show that $\Gamma(SL_3(\bar{\mathbf{F}}_p))$ and $\Gamma(PGL_3(\bar{\mathbf{F}}_p))$ are *non-periodic* groups. One way to see this is the following. From Schinzel's theorem, we get an infinite sequence of primes $r_1 < r_2 < \ldots$, such that for each i there exists a "free" subgroup $\langle s_i \rangle$ of order r_i. By Observation 3.16 and Theorem 2.13, we can construct an exceptional autoprojectivity φ such that the restriction of φ to H_{r_i} has order r_i. Then φ has infinite order, and the same holds for the autoprojectivity $\bar{\varphi}$ of $\Gamma(PGL_3(\bar{\mathbf{F}}_p))$.

We have another possibility. From the description of Λ_r as an inverse limit of the system $(\Lambda_{r,k}, \pi_k)_{k \in \mathbb{N}}$, and of $\Lambda_{r,k+1}$ as the semidirect product of $\Gamma_{r,k+1}$ and $\Lambda_{r,k}$, whenever H_r is infinite and it contains "free" subgroups, it is possible to show that there exists an element λ in Λ_r of infinite order.

We finally make an observation on the behaviour of *tori* of $SL_3(\bar{\mathbf{F}}_p)$ under exceptional autoprojectivities.

In [5] we proved the following fact. If A is an abelian divisible subgroup of a connected reductive group G over $\bar{\mathbf{F}}_p$, then the closure $\mathrm{cl}(A^\psi)$ of A^ψ is a torus for every autoprojectivity ψ of G (Lemma 2.6). It then follows that the image of a maximal torus is a maximal torus (Proposition 2.7). Here we show that there exists a 1-dimensional torus S and an element φ of $\Gamma(SL_3(\bar{\mathbf{F}}_p))$ such that S^φ is not closed, hence is not a torus.

Let r be a prime bigger than 13 such that if u is an element of $\bar{\mathbf{F}}_p^\times$ of order r, then $s = \mathrm{diag}(u, u^3, u^{-4})$ satisfies $(**')$. We put $u_1 = u$, and for every n in $\mathbb{N}$, we choose an element u_n of $\bar{\mathbf{F}}_p$ such that $u_{n+1}^r = u_n$. Let $z = 3 + a_1 r + a_2 r^2 + \ldots$ be an r-adic integer. To z we associate the following subgroup of H_r. Let $s_n = \mathrm{diag}(u_n, u_n^z, u_n^{-1-z})$, where the meaning of u_n^z, u_n^{-1-z} is the obvious one. We put $X_z = \bigcup \langle s_n \rangle$. X_z is isomorphic to C_{r^∞}, and every such subgroup of T_r containing $\langle s \rangle$ is of that form for a certain z. We take $z = 3$, and for z' any r-adic integer of the form $3 + a_1 r + a_2 r^2 + \ldots$, for which there do not exist coprime integers a, b such that $a = bz'$. Therefore $\mathrm{cl}(X_z) = S$ is a 1-dimensional subtorus of T, while $\mathrm{cl}(X_{z'}) = T$. By Observation 3.16, there exists φ in $\Gamma(SL_3(\bar{\mathbf{F}}_p))$ such that $X_z^\varphi = X_{z'}$. Then S^φ is not closed, otherwise we would have $S^\varphi = T$. Hence S^φ is not a torus of $SL_3(\bar{\mathbf{F}}_p)$. Note that on the other hand the image of a torus under any (abstract) automorphism of $SL_3(\bar{\mathbf{F}}_p)$ is a torus.

4. Final Remarks

In this section we shall give some examples which show how the results obtained so far may be used to describe $\Gamma(G)$ in some concrete cases. We

TABLE I.
$r^n = 27$, C the Subgroup of Order 6 in $(\mathbb{Z}/27\mathbb{Z})^\times$

c	x_1	x_3	x_5
1	—	24	0
10	—	24	0
8	12	5, 14, 23	1, 10, 19
−1	12	−1, 8, 17	−2, 7, 16
−10	12	2, 11, 20	4, 13, 22
−8	—	24	0

TABLE II.
$r^n = 8$, $C = (\mathbb{Z}/8\mathbb{Z})^\times$

c	x_1	x_2	x_3	x_4	x_5	x_6
1	—	—	5	7	0	6
3	—	—	3	1	2	4
5	—	—	1	3	4	2
7	—	—	7	5	6	0

shall also make use of a result from the theory of elliptic curves to give an estimate on the number of "free" r-subgroups of H in a particular situation. We shall therefore obtain necessary and sufficient conditions between the primes p and r such that $\Lambda_{r,1}$ is trivial. First see Tables I and II to justify the assertions given in the proof of Corollary 3.4 and Proposition 3.19 about the behaviour of 2-subgroups and of 3-subgroups of H (cf. Observation 3.10).

From Table I for each element x in the W-orbit $\{3, 6, 9, 15, 18, 21\}$ we have $N_3(x) = 0$. If $p \equiv \pm 1 \bmod 9$, and there is an element v of order 27 in $K^\times$, then there exists φ in $\Gamma(G)$ such that $\langle \mathrm{diag}(v, v^{10}, v^{16})\rangle^\varphi = \langle \mathrm{diag}(v, v^{19}, v^7)\rangle$ (cf. Proposition 3.19(v)).

From Table II, if $p \equiv 3 \bmod 8$, then every element of order 8 does not satisfy $(**')$ (cf. Corollary 3.4). On the other hand, if $p \equiv \pm 1 \bmod 8$, we have $N_3(2) = 0$. Suppose $K^\times$ contains an element v of order 16. There exists φ in $\Gamma(G)$ such that $\langle \mathrm{diag}(v, v^3, v^{12})\rangle^\varphi = \langle \mathrm{diag}(v, v^{11}, v^4)\rangle$ (cf. Proposition 3.19(i)).

As usual, we assume K to be a subfield of $\bar{\mathbf{F}}_p$, and r a prime different from p. We write $\delta = (r-1)/d$, for the order δ of p in $(\mathbb{Z}/r\mathbb{Z})^\times$. In our discussion we shall always assume $r \geq 5$, since we have already described the behaviour of 2- and 3-subgroups of H. We shall describe for which d $\Lambda_{r,1}$ is trivial. When $r \equiv 1 \bmod 3$, we shall also determine for which d we

have $N(x) \neq 0$ for every integer x. We use the notation we introduced in the previous section.

LEMMA 4.1. *Suppose δ is even, and d is different from* $1, 2, 3$. *Then there exists i such that $N(y_i) = 0$.*

Proof. Suppose for a contradiction that $N(y_i) \neq 0$ for each i. Since δ is even, we get $N(y_i) \geq 2$ for each i, so that $\delta \geq 2(1 + m)$ by the equations $(\therefore)$. In both cases $r \equiv \pm 1 \bmod 3$, we get a contradiction. ∎

We are in the position to describe the situation when $r \equiv 2 \bmod 3$.

PROPOSITION 4.2. *Let $r \equiv 2 \bmod 3$, $r \geq 5$. Then $\Lambda_{r,1}$ is trivial if and only if*

$$d \in \{1, 2, 4\} \qquad \text{if } r \equiv 5 \bmod 8,$$
$$d \in \{1, 2\} \qquad \text{if } r \not\equiv 5 \bmod 8.$$

Proof. Suppose $d \in \{1, 2, 4\}$ if $r \equiv 5 \bmod 8$, or $d \in \{1, 2\}$ if $r \not\equiv 5 \bmod 8$. Then we conclude by Proposition 3.13. Now assume $\Lambda_{r,1}$ is trivial. By Proposition 3.11 and Theorem 3.18, we get $\delta \geq m + 1$, so that $d < 6$. Hence $d \in \{1, 2, 4, 5\}$. If $d = 5$, or if $d = 4$ and $r \equiv 1 \bmod 8$, then δ is even, and by Lemma 4.1 we get $\Lambda_{r,1} \neq \{1\}$. ∎

To deal with the case $r \equiv 1 \bmod 3$, we argue as follows. We give an estimate on the number of integers $x \bmod r$ for which $N(x) = 0$. Suppose $\delta = (r - 1)/3$, and let $X = \{x \in \mathbb{Z}/r\mathbb{Z} \mid N(x) = 0\}$.

We fix an element a in $(\mathbb{Z}/r\mathbb{Z})^\times$ which is not a cube and we consider the elliptic curves

$$A: a^2w^3 - az^3 = 1$$
$$B: aw^3 - a^2z^3 = 1$$

over $\mathbb{Z}/r\mathbb{Z}$. Let $S(A), S(B)$ be respectively the set of solutions of A, B. For each (w, z) in $S(A)$ we put $\alpha(w, z) = 3/(az^3 - 1)$, and for each (w, z) in $S(B)$ we put $\beta(w, z) = 3/(a^2z^3 - 1)$. Suppose $x = 3/(az^3 - 1)$ lies in $\alpha(S(A))$. It then follows that

$$(x + 3)/x = az^3, \qquad (2x + 3)/x = a^2w^3, \qquad (2x + 3)/(x + 3) = a(w/z)^3,$$

so that $N(x) = 0$. Similarly one can prove that if x lies in $\beta(S(B))$, then $N(x) = 0$. Moreover the subsets $\alpha(S(A))$ and $\beta(S(B))$ are disjoint subsets of X, and for every x in $\alpha(S(A))$ (respectively in $\beta(S(B))$), $\alpha^{-1}(x)$

(respectively $\beta^{-1}(x)$) consists of 9 elements. We now prove that $X = \alpha(S(A)) \cup \beta(S(B))$. Let x be in X. Then we have $x \neq 0, -3, -3/2$, so that each $a_i(x)$ is defined and non-zero. If C is the set of cubes of $(\mathbb{Z}/r\mathbb{Z})^\times$ (in our case $C = \langle p \rangle$), we have $(\mathbb{Z}/r\mathbb{Z})^\times = C \cup aC \cup a^2C$. Since $a_1(x)a_3(x) = a_2(x)$, we must have either $a_1(x)$ in aC and $a_2(x)$ in a^2C, or $a_1(x)$ in a^2C and $a_2(x)$ in aC. Suppose we are in the first case. Then there exist z, w in $\mathbb{Z}/r\mathbb{Z}$ such that $a_1(x) = az^3$ and $a_2(x) = a^2w^3$. Then (w, z) lies in $S(A)$, and x lies in $\alpha(S(A))$, and similarly for the second case. Hence we get $|X| = 2|S(A)|/9$. By the Gauss–Hasse–Weil theorem (cf. [15, Chap. V, Theorem 1.1]), we have $r + 1 - 2r^{1/2} \leq |S(A)| \leq r + 1 + 2r^{1/2}$, so that

$$2(r + 1 - 2r^{1/2})/9 \leq |X| \leq 2(r + 1 + 2r^{1/2})/9.$$

PROPOSITION 4.3. *Let $r \equiv 1 \bmod 3$, $r \geq 19$. If δ divides $(r - 1)/3$, then $\Lambda_{r,1}$ is non-trivial.*

Proof. Suppose $\delta = (r - 1)/3$. By the above argument, if $r \geq 19$, it follows that there are at least 3 elements x for which $N(x) = 0$. Hence there exists i such that $N(y_i) = 0$. By Lemma 3.9, we have $N(y_i) = 0$ for every δ dividing $(r - 1)/3$, and we are done. ∎

THEOREM 4.4. *Let $r \equiv 1 \bmod 3$. Then $\Lambda_{r,1}$ is trivial if and only if*

$$d \in \{1, 2, 3, 6\} \quad \text{if } r = 7,$$
$$d \in \{1, 2, 3, 4\} \quad \text{if } r = 13.$$
$$d \in \{1, 2, 4\} \quad \text{if } r \equiv 5 \bmod 8,\ r \neq 13,$$
$$d \in \{1, 2\} \quad \text{if } r \not\equiv 5 \bmod 8,\ r \neq 7.$$

Proof. Suppose $\Lambda_{r,1}$ is trivial. By Proposition 3.11 we get $\delta \geq m + 1$, so that $d \leq 6$. By Lemma 4.1, d is not 5. If $r = 7$, we are done. If $r = 13$, then d is not 6 by Proposition 3.19(ix). So we assume $r \geq 19$. By Proposition 4.3 d is not 3 or 6. Moreover, if $r \not\equiv 5 \bmod 8$, d is not 4 by Lemma 4.1. On the other direction, if $r \geq 19$, we are done by Proposition 3.13. If $r = 13$ we note that for $d = 3$ we get $N(1) = 2$, so that there are no "free" subgroups of order 13. Since there are no W-orbits of length 6 in $\Omega(H_7)$, we are done. ∎

When $r \equiv 1 \bmod 3$, it is also useful to know in which cases besides having $N(y_i) \neq 0$ for each i, we also have $N(\theta - 1) \neq 0$. It is only in this situation that if $r^2 \nmid p^{r-1} - 1$ and $\nu_r \geq 2$, we have $\Lambda_r = \{1\}$.

PROPOSITION 4.5. *Let* $r \equiv 1 \bmod 3$. *Then* $N(x) \neq 0$ *for each integer* x *if and only if*

$$d \in \{1, 2, 4\} \quad \text{if } r \equiv 5 \bmod 8,$$
$$d \in \{1, 2\} \quad \text{if } r \not\equiv 5 \bmod 8.$$

Proof. Suppose $N(x) \neq 0$ for each integer x. From $(\therefore)$ we get $d < 6$. By Lemma 4.1, d is not 5, and it is not 4 if $r \not\equiv 5 \bmod 8$. Moreover if $d = 3$ and $N(y_i) \neq 0$ for each i, then we have $N(y_i) \geq 2$ for each i, so that $N(\theta - 1) = 0$, and this is a contradiction. The other implication comes from Proposition 3.13. ∎

One way of analysing the equations $(\therefore)$ is to calculate for a fixed δ, how many x in $\mathbb{Z}/r\mathbb{Z} \cup \{\infty\}$ have $N(x) = 6$. Since $N(x)$ is even if and only if δ is even, we assume δ even (otherwise we consider 2δ). We know that $N(0) = N(-3) = N(-3/2) = 2$. So assume x different from $0, -3, -3/2$. Since $a_1(x)a_3(x) = a_2(x)$, it is equivalent to studying for which x we have $a_1(x)$ and $a_2(x)$ in $\langle p \rangle$. Let $y = 1 + 3/x$. Then $a_1(x) = y$ and $a_2(x) = y + 1$. Therefore the number M of x in $\mathbb{Z}/r\mathbb{Z} \cup \{\infty\}$ for which $N(x) = 6$ equals the cardinality of the set $\langle p \rangle \cap (\langle p \rangle - 1)$ (and this is of course in relation with the number of solutions of the equation $w^d - z^d = 1$). Since we have $N(x^w) = N(x)$ for every x in $\mathbb{Z}/r\mathbb{Z} \cup \{\infty\}$ and every w in W, and $N(\infty) = 6$ if and only if 2 lies in $\langle p \rangle$, we get the following relations $(+)$.

If $r \equiv 2 \bmod 3$, then

$$M \equiv 3 \bmod 6 \quad \text{if } 2 \in \langle p \rangle,$$
$$M \equiv 0 \bmod 6 \quad \text{if } 2 \notin \langle p \rangle.$$

If $r \equiv 1 \bmod 3$, then $N(\theta - 1) = 6$ if and only if $3 | \delta$. Hence

$$M \equiv 0 \bmod 6 \quad \text{if } 2 \notin \langle p \rangle \text{ and } 3 \nmid \delta$$
$$M \equiv 3 \bmod 6 \quad \text{if } 2 \in \langle p \rangle \text{ and } 3 \nmid \delta$$
$$M \equiv 2 \bmod 6 \quad \text{if } 2 \notin \langle p \rangle \text{ and } 3 | \delta$$
$$M \equiv 5 \bmod 6 \quad \text{if } 2 \in \langle p \rangle \text{ and } 3 | \delta.$$

In particular, if $r \equiv 1 \bmod 3$ and $\delta = (r - 1)/3$, we get information on the number of solutions of the elliptic equation $w^3 - z^3 = 1$.

We conclude by giving a list of examples. We consider the prime r rather than p. We give Table III to justify the first example. For the others we just state the results. We always assume $\nu_r \geq 1$.

(1) We consider $r = 5$.

Hence from Table III, $N_2(4) = N_2(19) = 0$. Suppose $p = 7$. We get $\delta = 4$, and $25 | 7^4 - 1$. Since $K^\times$ contains elements of order 5, it contains

TABLE III. $r^n = 25$, C the Subgroup of Order 4 in $(\mathbb{Z}/25\mathbb{Z})^\times$

c	x_1	x_3	x_5
1	—	−3	0
7	13	—	—
−1	11	−1	−2
−7	9	8	14

an element v of order 25. There exists φ in $\Gamma(G)$ such that $\langle \mathrm{diag}(v, v^5, v^{19})\rangle^\varphi = \langle \mathrm{diag}(v, v^{20}, v^4)\rangle$ (cf. Proposition 3.19(iii)). Therefore $\Lambda_{5,1}$ is trivial, while $\Lambda_{5,2}$ is not.

(2) $r = 7$. $\Lambda_{7,1}$ is always trivial. Suppose $\nu_7 \geq 2$ and $7^2 \nmid p^6 - 1$. If $\delta = 3, 6$, then $\Lambda_7 = \{1\}$. If $\delta = 1, 2$, we get $\Lambda_{7,2} \cong (C_3 \times C_3) \rtimes C_2$.

(3) $r = 13$. If $\delta = 3, 6, 12$, we have $\Lambda_{13,1} = \{1\}$. If $\delta = 1, 2$, then $\Lambda_{13,1} \cong S_3$. If $\delta = 4$, we get $N(0) = N(\infty) = N(1) = 2$, $N(\theta - 1) = 0$. Hence $\Lambda_{13,1}$ is trivial, but $\Lambda_{13,2} \geq (C_3)^4 \rtimes S_4$ if $\nu_{13} \geq 2$ ($\Lambda_{13,2} \cong (C_3)^4 \rtimes S_4$ if and only if $13^2 \nmid p^{12} - 1$).

(4) $r = 521$. If $\delta = 260$, we have $N(0) = 2$, $N(\infty) = 6$, $N(y_1) = \cdots = N(y_s) = 6$, $N(y_{s+1}) = \cdots = N(y_{s+t}) = 2$, $s = 21$, $t = 65$. If $\delta = 130$, then $N(0) = 2$, $N(\infty) = 2$, $N(y_1) = \cdots = N(y_s) = 6$, $N(y_{s+1}) = \cdots = N(y_{s+t}) = 2$, $N(y_{s+t+1}) = \cdots = N(y_{s+t+u}) = 0$, where $s = 6$, $t = 46$, $u = 34$. The number of x in $\mathbb{Z}/r\mathbb{Z} \cup \{\infty\}$ for which $N(x) = 6$ is 129 if $\delta = 260$, and 36 if $\delta = 13$ (cf. the list (+)).

(5) $r = 3$, $p = 109$. Let u be an element of order 9 in $K^\times$, and let $s = \langle \mathrm{diag}(u, u^3, u^{-4})\rangle$. Then s is almost determined but every cyclic subgroup of order 27 containing s is generated by an element satisfying (**'). There exists φ in $\Gamma(G)$ such that $\langle \mathrm{diag}(u, u^3, u^{-4})\rangle^\varphi = \langle \mathrm{diag}(u, u^6, u^{-7})\rangle$. We have $\Gamma(SL_3(109)) \cong (S_3 \rtimes C_2) \times C_2 \times C_2$ and $\Gamma(PSL_3(109)) \cong C_2 \times C_2$.

(6) $p = 2$, $r = 31$. Then $\delta = 5$. We already know that $N(1) = N(-4) \neq 0$ and $N(3) = N(-6) \neq 0$. We have $N(0) = 1$, $N(\infty) = 3$, $N(\theta - 1) = 0$, $N(2) = 0$, and $N(1) = N(3) = N(10) = 1$. $\Lambda_{31,1} \cong S_3$.

(7) $p = 3$, $r = 41$. Then $\delta = 8$. We know that $N(3) \neq 0$. We have $N(0) = N(\infty) = 2$, $N(10) = N(3) = N(1) = 2$, $N(11) = N(2) = N(5) = 0$. $\Lambda_{41,1} \cong (S_3)^3 \rtimes S_3$. If $r = 1093$, we get $\delta = 7$, $N(3) = 1$, $N(1) = 0$. There are 6 W-orbits of length 6 for which $N = 1$, and 175 W-orbits of length 6 with $N = 0$.

(8) $p = 5$, $r = 31$. Then $\delta = 3$. We know that $N(1) \neq 0$. We have $N(0) = N(\infty) = 1$, $N(\theta - 1) = 3$, $N(1) = 1$, and $N(2) = N(3) = N(10) = 0$. $\Lambda_{31,1} \cong (S_3)^3 \rtimes S_3$.

(9) $\Gamma(SL_3(17)) \cong C_2 \times C_2$ (cf. [3]). $\Gamma(SL_3(27)) = \{1\}$ (cf. [4]). $\Gamma(SL_3(19)) \cong C_2$ and $\Gamma(PSL_3(19)) = \{1\}$.

(10) We consider the number $M(r)$ of x in $\mathbb{Z}/r\mathbb{Z} \cup \{\infty\}$ for which $N(x) = 6$. Suppose $\delta = (r-1)/3$. We have $M(67) = 6$, $M(31) = 3$, $M(19) = 2$, and $M(109) = 11$.

Acknowledgments

It is a pleasure to acknowledge helpful discussions with A. Schinzel and U. Zannier on exponential congruences. I also express my thanks to the Italian C.N.R. for financial support.

References

1. G. Birkhoff, "Lattice Theory," Amer. Math. Soc. Colloq. Publ., Vol. **25**, Amer. Math. Soc., Providence, RI, 1949.
2. M. Costantini, Sul gruppo delle autoproiettività dei gruppi lineari generale e speciale su un corpo finito, Tesi di laurea, Padova, 1985.
3. M. Costantini, Sul gruppo delle autoproiettività di $PSL(3, q)$, *Riv. Mat. Pura Appl.* **4** (1989), 79–88.
4. M. Costantini, On lattice automorphisms of the special linear group, *Atti Accad. Lincei Rend. Fis. (8)* **83** (1989), 33–38.
5. M. Costantini, Automorphisms and autoprojectivities of certain algebraic groups, *Rend. Accad. Naz. Sci. XL* **110** (1992), 99–114.
6. M. Costantini, On the lattice automorphisms of certain algebraic groups, *Rend. Sem. Mat. Univ. Padova* **90** (1993), 141–157.
7. J. Dieudonné, "Le géométrie des groupes classiques," Ergeb. Math. Grenzgeb., Vol. **5**, Springer-Verlag, New York/Berlin, 1955.
8. C. Holmes, Automorphisms of the lattice of subgroups of $\mathbb{Z}_{p^m} \times \mathbb{Z}_{p^n}$, *Arch. Math.* **51** (1988), 491–495.
9. N. Jacobson, "Lectures in Abstract Algebra, III," Van Nostrand, Princeton, NJ, 1964.
10. D. A. Marcus, "Number Theory," Springer, New York, 1977.
11. C. Metelli, Sugli isomorfismi reticolari di $PSL_2(p^f)$, *Rend. Accad. Naz. Lincei Cl. Sci. (8)* **47**, No. 6 (1969).
12. C. Metelli, Gruppi semplici minimali sono individuati reticolarmente in senso stretto, *Rend. Sem. Mat. Univ. Padova* **45** (1971), 367–378.
13. A. Schinzel, On power residues and exponential congruences, *Acta Arith.* **27** (1975), 397–420.
14. A. Schinzel, Abelian binomials, power residues and exponential congruences, *Acta Arith.* **32** (1977), 245–274.
15. J. H. Silverman, "The Arithmetic of Elliptic Curves," Springer, New York, 1985.
16. H. Völklein, On the lattice automorphisms of the finite Chevalley groups, *Indag. Math.* **89** (1986), 213–228.
17. H. Völklein, On the lattice automorphisms of $SL_n(q)$ and $PSL_n(q)$, *Rend. Sem. Mat. Univ. Padova* **76** (1986), 207–217.