JOURNAL OF ALGEBRA 57, 522–543 (1979)

On Abstract Monomorphisms of k-Forms of $PGL(2)$

B. WEISFEILER*

Department of Mathematics, Pennsylvania State University, University Park 16802

Communicated by J. Dieudonné

Received June 20, 1978

Abstract monomorphisms of the group of rational points of forms of $PGL(2)$ are described. This result is obtained as an application of an algebro-geometric structure of a projective plane on the set of connected one-dimensional subgroups of $PGL(2)$. Another application is a characterization of the groups of rational points of k-forms of $PGL(2)$ in characteristic $\neq 2$.

0. INTRODUCTION

0.1. We refer to the Introduction of [6] and 5.8 of [10] for a survey of the history of the subject; more information is contained in the references given there. As far as the present paper is concerned, we indicate only two points.

First, A. Borel and J. Tits [6] described in 1973 abstract *homomorphisms* of "big" subgroups of isotropic almost simple algebraic groups into other semi-simple algebraic groups. By the nature of their "big" subgroups the homomorphisms they consider can have only finite central kernels. So they actually are almost monomorphisms.

Second, O. T. O'Meara introduced in 1968 his method of residual spaces which permits one to deal with some anisotropic groups and even "sufficiently big" subgroups of these.

The present paper studies monomorphisms of forms of $PGL(2)$. So the class of homomorphisms we consider is close to that of Borel and Tits. However, we do consider anisotropic forms to which the methods of Borel and Tits are not applicable. On the other hand, our result does not apply to proper subgroups (cf. 4.4 below) so in this sense it is much more restricted than results of both O'Meara and Borel and Tits.

Our interest in this special case is two-fold. First, this case is a paradigm for a series of different developments (however, in each of them only some sides of our case are generalizable). Second, the case of groups of rank one can be used as a basis for induction to larger groups.

* Supported by NSF grant.

0021-8693/79/040522-22$2.00/0
Copyright © 1979 by Academic Press, Inc.
All rights of reproduction in any form reserved.

0.2. Our main result is Theorem 2.1.1. It says that on the set of connected one-dimensional subgroups of a group of type A_1 there is a natural structure of projective plane. In essence, this is an algebro-geometric version of O'Meara's method of residual spaces. The combinatorial structure of the projective plane is easily describable in abstract group terms and this leads to our main applications, which are Theorems 3.2 and 4.1. Theorem 3.2 gives an abstract group-theoretic characterization of groups of rational points of forms of $PGL(2)$ in characteristic $\neq 2$. Another characterization was given by R. Baer [3]. Theorem 4.1(i) says that if an almost simple algebraic group G' contains a dense homomorphic image of a form of $PGL(2)$, then G' is of type A_1. Note that here a homomorphism does not need to be injective. Theorem 4.1(ii) is about monomorphisms and shows that they have the usual decomposition into a field homomorphism and an isomorphism of algebraic groups. In the case of isomorphisms and in char $k \neq 2$ Theorem 4.1(ii) was proved by R. Baer in [3]. Actually, we establish a more general statement than 4.1(ii) in 4.3.3. We plan to use this more general statement in the study of monomorphisms of orthogonal groups in characteristic 2.

Some other statements are not always strictly necessary for the immediate purposes of the present paper. They were included to avoid repetitions and references to proofs in subsequent papers.

0.3. *Conventions and notations.*

We denote by $M(k)$ the set of rational points of an algebraic variety M defined over a field k. Sometimes we write M_k to indicate that M is defined over k (for example, $\mathbb{P}_k^2$ is a projective plane defined over k). If $\varphi: k \to k'$ is a homomorphism of fields, then ${}^{\varphi}M$ denotes the algebraic variety over k' obtained from M by base change φ. We denote by φ^0 the corresponding mapping $\varphi^0: M(k) \to {}^{\varphi}M(k')$. All this applies also to such objects as algebras and vector spaces, although occassionally we use the more classical view.

For an algebraic (resp. abstract) group G and an algebraic (resp. abstract) subset $M \subseteq G$, we denote by $Z_G(M)$, $N_G(M)$ the algebraic (resp. abstract) subgroup of G which is the centralizer or, respectively, the normalizer of M in G. If G is an algebraic (resp. abstract) group and $H_1, H_2, \ldots$, are its algebraic (resp. abstract) subgroups then D^iG and $\langle H_1, H_2, \ldots \rangle$ denote respectively the algebraic (resp. abstract) i-th derived group of G and the algebraic (resp. abstract) subgroup of G generated by $H_1, H_2, \ldots$. For an algebraic group G we denote by G^0 its connected component and by Lie G its Lie algebra.

The full matrix algebra of 2×2-matrices is denoted Mat_2. Its forms are the quaternion algebras [1]. If D is a quaternion algebra then Tr and Nrd denote its trace and reduced norm. Forms of $PGL(2)$ are in natural one-to-one correspondence [13] with forms of Mat_2. The form of $PGL(2)$ corresponding to a quaternion algebra D is denoted G^D.

Finally, $|S|$ denotes the cardinality of S.

1. Forms of PGL(2): Recollections and Preliminaries

1.1. *Realizations.*

1.1.1. Let k be a field and let G be a k-form of $PGL(2)$. It is known (cf. for example, [13]) that G corresponds to a (unique) associative simple algebra D of dimension 4 over k. This correspondence is such that $G(k') \simeq D^*(k')/k'^*$ for every field $k' \supseteq k$. Given D we denote by G^D the corresponding form of $PGL(2)$ and given a form G of $PGL(2)$ we denote by D^G the corresponding algebra. Recall that four-dimensional simple associative algebras are called algebras of quaternions.

1.1.2. It is convenient to remember that the group G has also realization as a group of orthogonal transformations of a three-dimensional space V, $G \simeq SO(V, f)$, for an appropriate quadratic form f on V. The connection of our previous realization with the present one is as follows. We make D^* operate on $V = \{d \in D \mid \operatorname{Tr} d = 0\}$ by $d \to gdg^{-1}$, $g \in D^*$. Clearly the center of D^* is the kernel of this action, so actually we get an action of D^* modulo center, i.e., the action of G^D. This action clearly preserves reduced norm Nrd (cf. 1.2.7 below) on D and the restriction of Nrd to V gives us a quadratic form. Since G^D is connected and 3-dimensional, it must coincide with $SO(V, Nrd)$.

1.2. *Subalgabras of quaternions and their splitting properties.*

1.2.1. An algebra D of quaternions is called *split* if it is isomorphic over k to the algebra Mat_2 of 2×2-matrices. The corresponding group G^D is then the group $PGL(2)$ itself. If $k' \supseteq k$ then we say that k' splits D if $D \simeq \mathrm{Mat}_2$ over k'. If D is not split over k then $D(k)$ is a division algebra.

1.2.2. (cf. [1], 4.27, 7.21) A quadratic extension field $K \supset k$ splits D if and only if K is isomorphic to a subfield of $D(k)$. In particular, if $D \simeq \mathrm{Mat}_2$ over k then every quadratic extension of k is isomorphic to a subfield of $D(k)$. If char $k = 2$ then D is always split by some inseparable quadratic extension.

1.2.3. (cf. [9] Ch. 6, Th. 15). If A_1, A_2 are two k-subalgebras of D and $\varphi: A_1 \to A_2$ is a k-isomorphism then there exists $d \in D(k)^*$ such that $dad^{-1} = \varphi(a)$ for any $a \in A_1$. In particular, if K is a separable commutative k-subalgebra of D of dimension 2 then there exists $d \in D(k)^*$ such that $dKd^{-1} = K$ and d induces on K the non-trivial automorphism of order 2.

1.2.4. If K is a separable commutative k-subalgebra of D of dimension 2, then $K \supset k$ and either $K \simeq k \otimes k$ or K is a quadratic extension of k (which splits D by 1.2.2).

1.2.5. If K is an inseparable commutative k-subalgebra of D of dimension 2 then either $K \simeq k[u]/(u^2)$ (and then D is split over k) or char $k = 2$ and K is a field $K \simeq k[u]/(u^2 - a)$, $a \notin k^2$.

1.2.6. If K is a separable commutative k-subalgebra of D of dimension 2 and $x \to \bar{x}$, $x \in K$, the (unique) non-trivial automorphism of K over k, then we can write $K = k(b)$ with $\bar{b} = 1 - b$ and we can identify $D(K)$ with the subalgebra $D_a(k)$ of $\mathrm{Mat}_2(K)$ consisting of matrices

$$A_{x,y} = \begin{pmatrix} x & y \\ a\bar{y} & \bar{x} \end{pmatrix}, \qquad x, y \in K, \quad a \in k^*.$$

The algebras D_a and D_c are isomorphic over k if and only if $a \in c \cdot N_{K/k}(K^*)$. In particular, $D_a \simeq \mathrm{Mat}_2$ if and only if $a \in N_{K/k}(K^*)$ (cf. [1], 7.5, 7.7).

1.2.7. For $A_{x,y} \in D_a(k)$ the reduced norm is given by

$$\mathrm{Nrd}\, A_{x,y} = \det A_{x,y} = x\bar{x} - ay\bar{y}.$$

We have $\mathrm{Nrd}(d_1 \cdot d_2) = \mathrm{Nrd}(d_1) \cdot \mathrm{Nrd}(d_2)$ and $D(k)$ is a division algebra if and only if $\mathrm{Nrd}\, d = 0$ for $d \in D(k)$ implies that $d = 0$.

Recall that for a commutative k-subalgebra K of D of dimension 2 we have $\mathrm{Nrd} \mid K = N_{K/k}$.

1.3. *Subtori of G.*

Let $G = G^D$ for some algebra D of quaternions over k.

1.3.1. Subtori of G are one-dimensional and they are in one-to-one correspondence with commutative separable subalgebras of dimension 2 of D. To such a subalgebra K there corresponds the torus T^K such that $T^K(k') = K(k')^*/k'^*$. The subalgebra corresponding to torus T will be denoted K^T.

1.3.2. A torus T is defined over k if and only if K^T is a k-subalgebra. If T is defined over k but not k-split, then K^T is the minimal splitting field of T.

1.3.3. If char $k \neq 2$ then any subtorus T of G contains a non-trivial element of order 2; if char $k = 2$, no torus has elements of order 2.

1.3.4. If k is infinite and T is defined over k then $T(k)$ is not periodic and any infinite subset of $T(k)$ is Zariski-dense in T. Moreover, any torsion subgroup of $T(k)$ is contained in the group of roots of unity, contained in the minimal splitting field of T.

1.3.5. It follows from 1.2.3 that two k-tori of G are conjugate over k if and only if they have the same minimal splitting field. It also follows from 1.2.3 that $N_{G(k)}(T(k))/T(k) \simeq \mathbb{Z}/2$, the group of two elements, if T is a k-torus of G, and $N_{G(k)}(T(k)) - T(k)$ consists of elements of order 2.

1.3.6. It is interesting to note the following fact. The above statement describes the action of $G(k)$ on the set of k-tori which are split by a given quadratic (separable) extension. However a slightly stronger statement is true. Set $q = 0$ if $D(k)$ is a division algebra and $q = 1$ if $D \simeq \mathrm{Mat}_2$ over k.

CLAIM. *Let K be a quadratic (separable) extension field of k which splits D. Let B be a Borel K-subgroup of G. Then $G(k)$ has $q+1$ orbits on $(G/B)(K)$.*

Proof. Indeed, $(G/B)(k)$ forms q orbits under $G(k)$. Set $X = (G/B)(K) - (G/B)(k)$ and take $B_1, B_2 \in X$. Let $\sigma \in \mathrm{Gal}(K/k)$, $\sigma \neq 1$. Then $T_1 = B_1 \cap B_1^\sigma$ and $T_2 = B_2 \cap B_2^\sigma$ are two k-subtori of G which are split by K (and not by k). By 1.3.5 there exists $g \in G(k)$ such that $gT_1g^{-1} = T_2$. Therefore either $gB_1g^{-1} = B_2$ (and we are done) or $gB_1g^{-1} = B_2$ (and then we have to apply an element from $N_G(T_2)(k) - T_2(k)$ to B_2^σ to get B_2).

1.4. *Unipotent subgroups of G.*

Let $G = G^D$ for some k-algebra D of quaternions. We denote by ω the canonical projection from the universal cover $\tilde{G}$ of G to G (it is defined over k).

1.4.1. Every unipotent element of $\omega(\tilde{G}(k))$ is contained in a Borel k-subgroup.

Proof. $\tilde{G}(k)$ is a subgroup of $D(k)^*$ (consisting of elements of reduced norm 1). Therefore $\tilde{G}(k)$ does not have unipotents if $D(k)$ is a division algebra. Then $\omega(\tilde{G}(k))$ also does not have them. If $D(k) \simeq \mathrm{Mat}_2(k)$ then every unipotent can be brought into a triangular form by an element of $D(k)^*$ and therefore it is contained in a k-algebra of all triangular matrices. Hence its image in $G(k)$ is contained in a Borel k-subgroup.

1.4.2. If char $k \neq 2$ then every unipotent element of $G(k)$ is contained in a Borel k-subgroup.

Proof. Take a unipotent $u \in G(k)$, $u \neq 1$. Consider a preimage $\tilde{u}$ of u in $D(k)$ under the canonical projection. Then $K = Z_D(\tilde{u})$ is a commutative subalgebra of D of dimension 2. It can not be separable. Therefore $K \simeq k[v]/v^2$ (cf. 1.2.5.). Then D is split and $1+v$ can be brought into a triangular form. The argument as in 1.4.1 concludes the proof.

1.4.3. If char $k = 2$ and $1 \neq u \in G(k)$ is unipotent then either u is contained in a Borel k-subgroup or there exists an inseparable subfield K of $D(k)$ such that $u \in K^*/k^*$. In this latter case $U = Z_G(u)$ is a unipotent k-subgroup of G which is isomorphic to $\mathbb{G}_a$ over K (but not over k); we have $U(k) = K^*/k^*$ (in particular, it is infinite) and $N_G(U)$ is not defined over k.

Proof. As in 1.4.2 we lift u to $\tilde{u} \in D(k)$ and set $K = Z_{D(k)}(\tilde{u})$. If $K \simeq K[v]/v^2$ then as in 1.4.2 we get that u lies in some Borel k-subgroup. If $K \simeq K[v]/v^2 - a$, $a \notin k^2$, then there is no Borel k-subgroup, containing u, since otherwise $U = Z_G(u)$ would be k-isomorphic to $\mathbb{G}_a$ (because of $\mathbb{G}_m$-action induced by a Borel subgroup), i.e., $K \simeq K[v]/v^2$, a contradiction. It remains to show that U is defined over k. But K is given by linear equation with coefficients in k (since it is a k-subspace of D). Therefore U is given by the same equations (plus condition: determinant $\neq 0$). So U is defined over k.

1.4.4. *Remark.* Cf. [7] for a general study of the above phenomenon.

1.4.5. If char $k \neq 0$ then any unipotent subgroup of G has period char k. If char $k = 0$ then any unipotent subgroup of G has no torsion.

1.4.6. If U is a unipotent k-subgroup of G then $U(k)$ is infinite and either $N_{G(k)}(U(k))/U(k) \simeq k^*$ (and then U is contained in a Borel k-subgroup) or $N_{G(k)}(U(k)) = U(k)$.

Proof. Only the last statement is not completely clear. Suppose that $N_{G(k)}(U(k)) \neq U(k)$. Then any $h \in N_{G(k)}(U(k)) - U(k)$ is semi-simple. Then $Z_G(h)^0$ normalizes U (it is clear over $\bar{k}$). But $Z_G(h)^0$ is a k-torus (cf. [5], 10.3) and therefore U is defined over k (cf. [4], 8.2), a contradiction.

1.5. *Centralizers.*

Let $G = G^D$ where D is an algebra of quaternions over k.

1.5.1. LEMMA. *Let $h \in G(k)$, $h \neq 1$, be a semi-simple element of G. Then*

(i) *$Z_G(h)^0$ is a k-subtorus of G,*

(ii) *$Z_G(h) = Z_G(h)^0$ if $h^2 \neq 1$,*

(iii) *$Z_G(h) = N_G(Z_G(h)^0)$ if $h^2 = 1$ (this case is possible only if* char $k \neq 2$, cf. 1.3.3),

(iv) *$Z_G(h)(k) = Z_{G(k)}(h)$.*

Proof. The first assertion follows from ([5], 10.3). The rest is easy and can be derived from 1.3.3, 1.3.5.

1.5.2. COROLLARY. *If T is a k-subtorus of G then $T(k) = \bigcap_{t \in T(k)} Z_{G(k)}(t)$.*

Proof. By 1.3.4 and 1.5.1(ii), (iv) there exists $h \in T(k)$ such that $T(k) = Z_{G(k)}(h)$.

1.5.3. LEMMA. *Let $u \in G(k)$, $u \neq 1$, be a unipotent element of G. Suppose that* char $k \neq 2$.

(i) *$Z_G(u)$ is a (connected) one-dimensional unipotent k-subgroup of G;*

(ii) *$Z_{G(k)}(u) = Z_G(u)(k)$;*

(iii) *$N_G(Z_G(u))$ is a Borel k-subgroup of G; in particular $N_{G(k)}(Z_G(u)(k))/Z_G(U)(k) \simeq k^*$.*

Proof follows directly from 1.4.2 and 1.4.6.

1.5.4. LEMMA. *Let $u \in G(k)$, $u \neq 1$, be a unipotent element of G. Suppose that* char $k = 2$.

(i) *$Z_G(u)$ is a (connected) one-dimensional unipotent k-subgroup of G;*

(ii) *$Z_G(u)$ has period* 2;

(iii) $Z_{G(k)}(u) = Z_G(u)(k)$;

(iv) $N_{G(k)}(Z_{G(k)}(u))/Z_{G(k)}(u) \simeq k^*$ *or* $\{1\}$; *the first case occurs if and only if $Z_G(u)$ is k-isomorphic to $\mathbb{G}_a$.*

Proof follows directly from 1.4.3, 1.4.5, 1.4.6.

1.5.5. COROLLARY. *Let $u \in G(k)$ be unipotent and $U = Z_G(u)$. Then $Z_{G(k)}(v) = U(k)$ for any $v \in U(k)$, $v \neq 1$.*

1.5.6. COROLLARY. *Let $g \in G(k)$, $g \neq 1$. Suppose that k is infinite.*

(i) *g is semi-simple if and only if $N_{G(k)}(Z_{G(k)}(H))/Z_{G(k)}(H) \simeq \mathbb{Z}/2$ where H is the group generated by squares of elements of $Z_{G(k)}(h)$,*

(ii) *g is unipotent if and only if either $N_{G(k)}(Z_{G(k)}(g))/Z_{G(k)}(g)$ is infinite or $N_{G(k)}(Z_{G(k)}(g)) = Z_{G(k)}(g)$ and $Z_{G(k)}(g)$ has period* 2.

Remark. Of course, a characterization of semi-simple elements gives a characterization of unipotent ones (since in adjoint groups of type A_1 every element is either semi-simple or unipotent).

Proof of Corollary. Let $Z = Z_G(g)^0$. If g is semi-simple then $Z(k)$ is not periodic by 1.3.4 and 1.5.1(i). Therefore H is infinite. Since in all cases $[Z_G(g): Z] \leqslant 2$ (by 1.3.5), we have that squares of elements of $Z_G(g)$ are contained in $Z(k)$. Now 1.5.2 together with 1.3.5 concludes the proof of (i). If g is unipotent we are done by 1.5.3, 1.5.4.

1.5.7. DEFINITION. Let H be a group and let $M = Z_H(m)$ be a centralizer in H. We say that M is a *minimal centralizer* in H if $M = \bigcap_{h \in M} Z_H(h)$. We denote by $S(H)$ the set of minimal centralizers contained in H.

Remark. Clearly, every minimal centralizer is commutative and $\neq \{1\}$.

1.5.8. COROLLARY.

(i) *Zariski-closure of every minimal centralizer in $G(k)$ is a connected one-dimensional k-subgroup of G;*

(ii) *Every element $h \neq 1$ of $G(k)$ belongs to a unique minimal centralizer denoted $Z_{G(k)}(h)^0$;*

(iii) *The Zariski-closure of $Z_{G(k)}(h)^0$ is $Z_G(h)^0$; it is a unipotent subgroup or a torus depending on whether h is unipotent or semi-simple.*

Proof. All assertions of the corollary will follow from equality $Z_{G(k)}(h)^0 = Z_G(h)^0(k)$. This follows from 1.5.3(i) and 1.5.4(i) if h is unipotent. If h is semi-simple and $h^2 \neq 1$, it follows from 1.5.1(i). So assume that h is semi-simple and

$h^2 = 1$. Of course, h is contained in a unique torus (otherwise h will be central) and this torus is $Z_G(h)^0$. By 1.5.2 $Z_G(h)^0(k)$ is a minimal centralizer.

1.6. *Relative position of connected one-dimensional subgroups.*

Let $G = G^D$ where D is an algebra of quaternions over k. Assume that k is infinite.

1.6.1. LEMMA. *Let H_1, H_2 be two different connected one-dimensional subgroups of G. Then one (and only one) of the following statements holds:*

(i) *$\langle H_1, H_2\rangle$ is a Borel subgroup; in this case $D(\langle H_1, H_2\rangle)$ is a (connected one-dimensional) unipotent subgroup of G and $\langle H_1, H_2\rangle = N_G(D(\langle H_1, H_2\rangle))$; in particular, $D^2(\langle H_1, H_2\rangle) = \{1\}$ in this case.*

(ii) *$\langle H_1, H_2\rangle = G$; in this case $D^n(\langle H_1, H_2\rangle) \neq \{1\}$ for any $n \geqslant 0$.*

Proof is evident since $\dim\langle H_1, H_2\rangle \geqslant 2$ and Borel subgroups are the only proper subgroups of G of dimension $\geqslant 2$.

1.6.2. COROLLARY. *Let H_1, H_2 be two different connected one-dimensional subgroups of G such that $H_i(k)$ is infinite. Then one (and only one) of the following statements holds.*

(i) *$D^2(\langle H_1(k), H_2(k)\rangle) = 1$; in this case H_1 and H_2 are defined over k and $Z_{G(k)}(D(\langle H_1(k), H_2(k)\rangle))$ is the set of rational points of a unipotent k-subgroup of G.*

(ii) *$D^n(\langle H_1(k), H_2(k)\rangle) \neq 1$ for any n.*

Proof. It is easy to see either by using general theory or by specific properties of our case that $\langle H_1(k), H_2(k)\rangle$ is dense in $\langle H_1, H_2\rangle$. Therefore $D^n(\langle H_1(k), H_2(k)\rangle)$ is dense in $D^n(\langle H_1, H_2\rangle)$ and our assertion follows from 1.6.1.

Let us record the following

1.6.3. *Remark.* In case (i) of 1.6.1 (or 1.6.2) at least one of the groups H_1 or H_2 must be a torus.

1.6.4. PROPOSITION. *Let H_1, H_2 be two different connected one-dimensional k-subgroups of G such that $\langle H_1, H_2\rangle = G$. Then there exists a unique $h \in G(k) \cap N_G(H_1) \cap N_G(H_2)$ such that $h^2 = 1$ and $hmh^{-1} = m^{-1}$ for every $m \in H_1 \cup H_2$.*

Proof. Suppose first that both H_1 and H_2 are unipotent. Then $B_i = N_G(H_i)$ is a Borel subgroup. Therefore $T = B_1 \cap B_2$ is a torus. If char $k = 2$ then $1 \in T$ acts as required on $H_1 \cup H_2$ (since $m = m^{-1}$ in this case) but no other element of T will do (cf. 1.3.3). Clearly, $1 \in G(k)$. Assume therefore that char $k \neq 2$. Then both B_1 and B_2 are defined over k (by 1.5.3(iii)) and therefore T is defined over k. Then $T(k)$ contains exactly 2 elements of order 2, namely 1 and, say, h. The identity will not satisfy $hmh^{-1} = m^{-1}$ because of 1.4.5. But h acts

as -1 on every unipotent subgroup normalized by T (it is easy to see because h is the image of $\left(\begin{smallmatrix}-1 & 0\\ 0 & 1\end{smallmatrix}\right)$).

So we can now assume that one of our groups, say H_1, is a torus. Then H_1 is defined over k (since $H_1(k)$ is infinite and by [5], 10.3). Let K be the minimal splitting field of H_1. We can assume over K that H_1 is diagonalized, i.e., $H_1 = \omega\{\left(\begin{smallmatrix}a & 0\\ 0 & b\end{smallmatrix}\right)\}$ where ω is the canonical projection $GL(2) \to PGL(2)$. Take $\tilde{m} = \omega\left(\begin{smallmatrix}p & q\\ r & s\end{smallmatrix}\right) \in H_2(k)$ such that $Z_G(\tilde{m}) = H_2$ (cf. 1.5.5 and 1.5.1(ii)). Since $\langle H_1, H_2\rangle = G$ we can assume that $r \neq 0$, $q \neq 0$. We search for h of the form $h = \omega\left(\begin{smallmatrix}0 & x\\ 1 & 0\end{smallmatrix}\right) \in N_G(H_1) - H_1$. We have to solve the equation $h\tilde{m}h^{-1} = \tilde{m}^{-1}$. It can be rewritten as

$$\begin{pmatrix}0 & x\\ 1 & 0\end{pmatrix}\begin{pmatrix}p & q\\ r & s\end{pmatrix} = \begin{pmatrix}cs & -cq\\ -cr & cp\end{pmatrix}\begin{pmatrix}0 & x\\ 1 & 0\end{pmatrix}$$

with $c \in k^*$. This gives us

$$xr = -cq, \qquad xs = csx, \qquad p = cp, \qquad q = -crx,$$

whence $c = 1$, $x = -q/r$. So our problem has an unique solution $h \in G(K)$ such that $h^2 = 1$, $hth^{-1} = t$, $\forall t \in T(k)$ and $h\tilde{m}h^{-1} = \tilde{m}^{-1}$. It is clear from our choice of $\tilde{m}$ (i.e. from $Z_G(\tilde{m}) = H_2$) that $hH_2h^{-1} = H_2$. Since h acts on a "generic" element $\tilde{m}$ as required it also acts on the whole of H_2 as inversion. So we solved our problem with $h \in G(K)$. If $K = k$ then we are done, so assume that $K \neq k$. Then K is quadratic separable over k. Let $\sigma \in \mathrm{Gal}(K/k)$, $\sigma \neq 1$. Clearly $\sigma(h)$ has the same properties as h (since it acts on $H_1(k)$ and $H_2(k)$ as inversion). By unicity of h we have $\sigma(h) = h$, that is $h \in G(k)$, which proves the last conclusion of our proposition.

1.6.5. The above discussion justifies the following definitions.

Definition. A subset L of one-dimensional connected subgroups of G is called a *line* if at least one of the following holds:

(i) L is the set of all one-dimensional connected subgroups of G contained in some Borel subgroup B of G; we write $L = L(B)$; in this case $B = B(L) = \langle H; H \in L\rangle$; we say that $L(B)$ is a *parabolic line*.

(ii) There exists $h \in G$ such that $h^2 = 1$ and L consists of all one dimensional connected subgroups H of G such that $hmh^{-1} = m^{-1}$ for all $m \in H$; we write $L = L(h)$; in this case $h = h(L)$ is uniquely determined by L (cf. 1.6.4); we say that $L(h)$ is an *involutorial line*.

1.6.6. Definition. Let H be a group and $S(H)$ the set of minimal centralizers of H (cf. 1.5.7). A subset L of $S(H)$ is called a *line* if $|L| > 2$ and if at least one of the following holds

(i) L is the set of all minimal centralizers contained in $N_H(M)$ for some $M \in S(H)$; in this case L is called a *parabolic line*.

(ii) There exists $h \in H$, $h^2 = 1$, such that L consists of all $M \in S(H)$ such that $hmh^{-1} = m^{-1}$ for all $m \in M$. In this case L is called an *involutorial line.*

2. A Structure of $\mathbb{P}^2$ on the Set of Connected One-Dimensional Subgroups

Throughout this section $G = G^D$ where D is a quaternion algebra over an infinite field k. We denote by $S(G)$ the set of connected one-dimensional subgroups of G.

2.1. *Algebraic structure on $S(G)$.*

2.1.1. Theorem.

(i) *The set $S(G)$ has a natural structure of an algebraic manifold defined over k and isomorphic over k to the projective plane $\mathbb{P}^2$.*

(ii) *The natural action of G on $S(G)$ is algebraic and defined over k.*

(iii) *The points of $S(G)(k)$ are k-subgroups $H \in S(G)$; or (what is the same by* 1.5.1(i), 1.5.3(i), 1.5.4(i)) *they are connected centralizers of elements $x \in G(k)$, $x \neq 1$.*

Proof. Let us start with the case $G = PGL(2)$, i.e., $D = \mathrm{Mat}_2$.

2.1.2. Lemma, *If $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL(2)$ then $Z_{GL(2)}(A)$ consists of matrices $\left(\begin{smallmatrix} x & y \\ u & v \end{smallmatrix}\right)$ such that*

$$xv - uy \neq 0$$
$$yc = bu$$
$$(a - d)u = c(x - v)$$

Proof by direct verification.

2.1.3. *Proof of Theorem continued.* We identify the set of one-dimensional connected subgroups of G with the set of connected centralizers of non-identity elements of G and those latter with the set of centralizers of non-central elements of $GL(2)$. Let us put into correspondence to the centralizer of A from 2.1.2 the set of triples $(my, mu, m(x - v))$, where $m \in k^*$. By 2.1.2 this set of triples completely describes $Z_{GL(2)}(A)$. On the other hand for any $(y, u, x - v)$ we can find x and v such that $xv - uy \neq 0$. The triple $(0, 0, 0)$ corresponds to the centralizers of central elements. So the set of centralizers of non-central elements is identified with $(\mathbb{A}^3 - (0, 0, 0))/\mathbb{G}_m$, where $\mathbb{G}_m$ acts scalarly, i.e., it is identified with $\mathbb{P}^2$. Clearly, this structure of algebraic manifold on $S(G)$ is defined over k and the action of $PGL(2)$ on $\mathbb{P}^2$ obtained in this cay is algebraic. This proves (i) and (ii) for $PGL(2)$.

Consider now the case of anisotropic G. Then G is split over a quadratic separable extension K. Then by standard and easy argument $S(G)$ gets a struc-

ture of an algebraic manifold defined over k and the action of G is also defined over k. Let us show that $S(G)$ is isomorphic to $\mathbb{P}^2$ over k. Forms of $\mathbb{P}^2$ correspond to algebras of degree three (Brauer-Severi varieties) which therefore are either $\mathbb{P}^2$ or are split only by extensions of degrees divisible by 3. Since G is split over a quadratic extension we must have that our manifold is $\mathbb{P}_k{}^2$.

Remark. The assertion proved in the last paragraph follows (independently) also from either of 2.1.5 or 2.1.6 below. We establish the isomorphism claimed in these statements for $PGL(2)$ and get one over k by Galois descent.

2.1.4. It remains to establish (iii). Again it can be deduced from 2.1.5 or 2.1.6. But also it can be deduced for $PGL(2)$ explicitly and then for any G by Galois descent. For $PGL(2)$ let us take $H \in S(G)(K)$ corresponding to coordinates $(y, u, x - v)$ (cf. 2.1.3). We may assume that $y \neq 0$. Then the condition that $H \in S(G)(K)$ means that $s_1 = u/y \in K$ and $s_2 = (x - v)/y \in K$. If $u \neq 0$ then $H = \alpha(Z_{GL(2)}\left(\begin{smallmatrix} s_2 & 1 \\ s_1 & 0 \end{smallmatrix}\right))$ and if $u = 0$ then $H = (Z_{GL(2)}\left(\begin{smallmatrix} s_2+s & 1 \\ 0 & s \end{smallmatrix}\right))$ where $s \in K$ is chosen so that $s_2 + s \neq 0$, $s \neq 0$. So in all cases H in the centralizer of an element from $G(K)$ and we are done by 1.5.1(i), 1.5.2(i), 1.5.3(i).

2.1.5. Let Lie G be the Lie algebra of G. Let $\mathbb{P}$ (Lie G) be the associated projective space. Since the group G is adjoint (it is false for $SL(2)$) the map φ: $S(G) \to \mathbb{P}$ (Lie G) which maps $H \in S(G)$ to Lie $H \subset$ Lie G is bijective.

PROPOSITION. *φ is a k-isomorphism of $S(G)$ onto $\mathbb{P}$ (Lie G).*

Proof. For $PGL(2)$ one can use the fact that the same equations (cf. 2.1.2) define centralizers in $PGL(2)$ and one-dimensional subalgebras in Lie $PGL(2)$. Then one can use Galois descent.

2.1.6. Let B be a Borel subgroup of G. Then G/B is defined over k and isomorphic over some extension to $\mathbb{P}^1$. Let $S^2(G/B)$ be the symmetric square of G/B. Then $S^2(G/B) \simeq \mathbb{P}^2$ (it is known). We define a map φ: $S(G) \to S^2(G/B)$ by $\varphi(H) = \{$set of Borel subgroups, containing $H\}$ for $H \in S(G)$. Let Δ: $G/B \to S^2(G/B)$ be the diagonal.

PROPOSITION.

(i) *φ is a k-isomorphism of $S(G)$ and $S^2(G/B)$.*

(ii) *$\varphi^{-1}(\Delta(G/B))$ is the set of unipotent subgroups $H \in S(G)$.*

Proof. Of course, φ commutes with action of G. Clearly φ is an isomorphism on an open set of tori of G. Therefore φ can be extended to an equivariant (and defined over k) map of $\mathbb{P}^2$ to $\mathbb{P}^2$.

This proves (i). To prove (ii) it is sufficient to note that unipotent subgroups and only they are contained in exactly one Borel subgroup. So the set of unipotent subgroups is the set where the map $G/B \times G/B \to S(G)$ obtained by

composition of the canonical projection $G/B \times G/B \to S^2(G/B)$ and φ^{-1} is ramified. On the other hand $\Delta(G/B)$ is the set where projection is ramified.

2.1.7. *Remark.* We call the set $\varphi^{-1}(\Delta(G/B))$ the *unipotent curve.* This curve is a conic (non-singular curve of degree 2) if char $k \neq 2$. If char $k = 2$ then it is a double line. In this case we call it also *unipotent line.* Let us see how it is related with 2.1.5. The set of nil-subalgebras in Lie G consists of isotropic lines for the Killing form, which means that this set is given by a quadratic form if char $k \neq 2$. So we once again see that it is a conic. If char $k = 2$ then the all nil-subalgebras are contained in [Lie G, Lie G] which is a two-dimensional subspace of Lie G. Moreover, any line contained in [Lie G, Lie G] is a nil-subalgebra of Lie G. So we see that $\varphi^{-1}(\Delta(G/B)) = \mathbb{P}([\text{Lie } G, \text{Lie } G]) \subset \mathbb{P}(\text{Lie } G)$, so we again see that it is a line.

2.2. *Lines of $S(G)$.*

We say that an algebraic curve on $S(G)$ is a projective line if it is a projective line of $\mathbb{P}^2$ after our identification of $\mathbb{P}^2$ with $S(G)$ (cf. 2.1.1).

2.2.1. THEOREM.

(i) *Parabolic lines and involutorial lines of $S(G)$* (cf. 1.6.5) *are projective lines.*

(ii) *Every projective line of $S(G)$ is either a parabolic line or an involutorial line.*

Proof. Let us take homogeneous coordinates $(y, u, x - v)$ (cf. 2.1.3) on $S(G)$. One parabolic line is given by (linear) equation $y = 0$ and so it is a projective line. Since G acts transitively on parabolic lines we get that all parabolic lines are projective lines.

If char $k = 2$ then $L(1)$ is clearly a projective line (cf. 2.1.7). So we can assume that our infolutorial line $L(h)$ contains a torus. We can assume that this torus is diagonalized and that $h = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Then h maps a point with homogeneous coordinates $(y, u, x - v)$ to the point $(u, y, v - x) = (-u, \ -y, \ x - v)$. Therefore the equation of the line of fixed points is $u = -y$ which is again linear. This proves (i).

Remark. There is also a fixed point given by $u = y, x - v = 0$. It lies off $L(h)$ iff char $k \neq 2$. Cf. 2.3 below for more details.

Now (ii) follows immediately because for any two distinct $H_1, H_2 \in S(G)$ we have either $\langle H_1, H_2 \rangle$ is a Borel subgroup and then H_1, H_2 belong to a parabolic line which by (i) is the unique projective line passing through H_1, H_2; or $\langle H_1, H_2 \rangle = G$ and then H_1, H_2 belong to an involutorial line (by 1.6.4) which is by (i) the unique projective line passing through H_1, H_2.

2.2.2. COROLLARY.

(i) *A parabolic line $L(B)$ is defined over k if and only if B is defined over k.*

(ii) *An involutorial line $L(h)$ is defined over k if and only if $h \in G(k)$.*

Proof. If $L(B)$ is defined over k it contains two distinct subgroups H_1, $H_2 \in S(G)(k)$. Then H_1, H_2 are defined over k (cf. 2.1.1(iii)) and therefore $B = \langle H_1, H_2 \rangle$ is defined over k. The converse is clear.

If $L(h)$ is defined over k then there exist two distinct points H_1, $H_2 \in S(G)(k)$ lying on $L(h)$. Then $\langle H_1, H_2 \rangle = G$ and by 2.1.1(iii) H_1 and H_2 are defined over k. Then $h \in G(k)$ by 1.6.4. Converse, that is that if $h \in G(k)$ then $L(h)$ is defined over k, follows for example from the explicit description of involutorial lines in the proof of 2.2.1.

2.2.3. *Remark.* In terms of identification of $S(G)$ with $\mathbb{P}$ (Lie G), cf. 2.1.5, the projective lines are of course of the form $\mathbb{P}(V)$ where $V \subset$ Lie G, dim $V = 2$.

2.2.4. Let $S(G(k))$ be the set of minimal centralizers of $G(k)$ (cf. 1.5.7) with lines defined as in 1.6.6. Define incidence relation on $S(G(k))$: a point belongs to a line.

THEOREM. *$S(G(k))$ with the above incidence relation is a Pappian projective plane.*

Proof. By 1.5.8 we can identify $S(G(k))$ with $S(G)(k)$. Then the lines of one become the lines of another by 2.2.1, 1.6.4, 1.6.2. The fact that $S(G(k))$ is a Pappian projective plane follows from 2.2.1 since $\mathbb{P}^2$ is one.

2.3. *Polarity of $S(G)$.*

Assume that char $k \neq 2$.

Denote by $S(G)^*$ the dual projective plane of $S(G)$). We can also identify $S(G)^*$ with $\mathbb{P}((\text{Lie } G)^*)$, the projectivization of a dual space of Lie G.

Let us define $F\colon S(G)^* \to S(G)$ by the following rules. If $L = L(B)$ is a parabolic line then $F(L) = [B, B] \in S(G)$. If $L = L(h)$ is an involutorial line then $F(L) = (Z_G(h)^0) \in S(G)$ (cf. 1.6.5). Let us also define $F^*\colon S(G) \to S(G)^*$ by the following rule. If $H \in S(G)$ is a torus then take a unique $h \in H$, $h \neq 1$, $h^2 = 1$ and set $F^*(H) = L(h)$. If $H \in S(G)$ is unipotent then set $F^*(H) = L(N_G(H))$.

2.3.1. THEOREM. (*recall*: char $k \neq 2$)

(i) $F \circ F^* = F^* \circ F = \mathrm{Id}$.

(ii) *F and F^* commute with the action of G.*

(iii) *F and F^* are correlations of respective planes.*

(iv) *F and F^* are defined over k.*

Proof is simple and is omitted.

2.3.2. PROPOSITION. *In terms of the identification of $S(G)$ with $\mathbb{P}$ (Lie G)* (cf. 2.1.5) *the map F is identified with the Killing form of Lie G. Namely, $F(H) =$* (Lie $H)^\perp$ *where $\perp$ denotes orthogonal complement with respect to Killing form.*

Proof. Since char $k \neq 2$ the Killing form is non-degenerate and the action of G on $\mathbb{P}^2 = \mathbb{P}(\text{Lie } G) = S(G)$ is irreducible. Therefore there exists at most one G-invariant polarity, namely F. Since the Killing form also defines a polarity given by $V \to V^\perp$ for dim $V = 1$, we see that both must coincide, as claimed.

2.3.3. COROLLARY. *The maps F and F^* define polarities of $S(G(k))$ and $S(G(k))^*$.*

Proof. Direct corollary of 2.2.4.

2.3.4. *Remark.* If char $k = 2$ then F is defined for all but the unipotent line. And it maps all non-unipotent lines into the points of the unipotent line.

3. A CHARACTERIZATION OF GROUPS G(k), G A FORM OF PGL(2) IN CHAR $k \neq 2$

3.1. Let H be a group. We take for H the definitions of 1.5.7 and 1.6.6. Let us impose the following conditions on $S(H)$.

(p1) The incidence structure on $S(H)$ given by intersection of lines and the incidence of a point to a line is a Pappian projective plane. (By [2], Chapter II, Section 11 and Theorems 2.16, 2.17, 2.18, this is therefore $\mathbb{P}^2(k)$ for some (commutative) field k).

(p2) The action of H by conjugation on $S(H)$ induces a faithful representation $m: H \to \text{Aut } \mathbb{P}^2(k)$.

(p3) $m(H) \subseteq PGL(3, k) \subseteq \text{Aut } \mathbb{P}^2(k)$. (Group-theoretic conditions distinguishing $PGL(3, k)$ in Aut $\mathbb{P}^2(k)$ are listed in [8], ch. IV, Section 1, Remarques.)

(p4) If L is a parabolic line, the group $Z_H([\bigcup_{M\in L} M, \bigcup_{M\in L} M])$ is a minimal centralizer in H.

(p5) If $h \in H$, $h^2 = 1$, defines some involutorial line then $Z_H([Z_H(h), Z_H(h)])$ is a minimal centralizer in H, let us denote it by $Z_H(h)^0$.

(p6) Let the mapping F from the set $\mathbb{P}^2(k)^*$ of lines in $\mathbb{P}^2(k)$ to the set $\mathbb{P}^2(k)$ of points be given by: F(parabolic line) $=$ (the minimal centralizer of (p4)) and F (involutorial line, defined by an involution $h \in H$) $= Z_H(h)^0$. Condition is:

there exists a symmetric non-degenerate bilinear form on the underlying space of $\mathbb{P}^2(k)$ such that $F(L) = r$ implies that the corresponding plane and line are orthogonal with respect to this form.

3.1.1. *Remarks.*

(i) The characteristic 2 case is rejected by (p5) since then the unipotent line is defined by $h = 1$ and $Z_H([Z_H(h), Z_H(h)]) = \{1\}$, which is not a minimal centralizer.

(ii) Possibly (p6) can be weakened to the assumption: F is a polarity. Then, of course, it can be either an orthogonal polarity or a unitary polarity and we shall need to prove that the unitary case contradicts other assumptions. (The symplectic case is impossible for dimension reasons.)

3.2. THEOREM.

(i) *Suppose that H satisfies* (p1)–(p6). *Then H is the group of rational points of a k-form of $PGL(2)$ for the field k. In this case* char $k \neq 2$.

(ii) *Conversely if $G = G^D$, D a quaternion algebra over k,* char $k \neq 2$, *then $G(k)$ satisfies* (p1)–(p6).

Proof. Let us first prove (ii). First, (p1) follows from 2.2.4. Next, (p2) holds since $PGL(2)$ is a simple algebraic group and its action on $\mathbb{P}^2$ is algebraic; so the kernel would be a normal algebraic subgroup. Further, (p3) follows again from algebraicity of action of G on $\mathbb{P}^2$. Then, (p4) follows from 1.6.2(i). Now, (p5) follow from 1.5.1(ii) and 1.3.5. Finally, (p6) follows from 2.3.1.

Now let us look at (i). The map F is H-equivariant, therefore H is contained (by (p6)) in the orthogonal group $SO(3, F)(k)$. Since $SO(3, F)$ is a form of $PGL(2)$ (cf. 1.1.2) our theorem will be proved once we show that H coincides with $SO(3, F)(k)$.

For every non-isotropic line L (i.e. regular plane in the corresponding inner product space) there exists a unique involution $h = h(L)$ which acts trivially on L. But these lines are exactly inolutorial lines (since for them and only for them $F(L) \notin L$). Thus $h \in H$. But $SO(3, F)(k)$ is generated by (such) involutions (there are no other involutions) (cf. [8], II, Section 6.1). This concludes the proof.

3.2.1. *Remarks.*

(i) Another characterization of groups $G^D(k)$ was given by R. Baer in [3], also in char $k \neq 2$.

(ii) To extend a characterization to char $k = 2$ we probably should be able to really describe our groups. Because in this case the group preserving F (cf. 3.2.4) is not semi-simple and we have to find some "abstract Levi section" (cf. [6], 8.18). But since this section need not be algebraic (even in our special case), we would not be able to identify H with an algebraic subgroup of $PGL(3)$.

4. Homomorphisms

Let $G = G^D$, where D is a quaternion algebra over an infinite field k. We consider also another field k' and an algebraic absolutely almost simple group G' defined over k'. Suppose we have a homomorphism α: $G(k) \to G'(k')$.

4.1. Theorem.

(i) *If the image of α is dense in G' then G' is of type A_1.*

(ii) *If α is a monomorphism and G' is a form of $PGL(2)$ then*

(a) *there exists a unique field homomorphism φ: $k \to k'$;*

(b) *G' is defined over $\varphi(k)$;*

(c) *there exists a unique $\varphi(k)$-isomorphism of algebraic groups β: ${}^{\varphi}G \to G$ such that $\alpha(g) = \beta(\varphi^0(g))$, $g \in G(k)$.*

Remarks.

(i) The case when G' is a k'-form of $SL(2)$ is not (and can not without too much stress) included into the statement (cf., however, Lemma 4.2.2 below).

(ii) The case (ii) in char $k \neq 2$ under assumption that α is an isomorphism was proved by R. Baer in [3].

4.2. *Proof of* 4.1(i),

4.2.1. Lemma. *Let M be an abstract group, $n \in \mathbb{N}$, α': $M \to G'(k')$ a homomorphism with a dense image. Then there exists a subset $M_{s,n}$ of M such that $\alpha'(M_{s,n})$ is dense in G' and consists of very strongly regular (in the sense that if $A(Z_{G'}(x)^0) = Z_{G'}(x)^0$ for $A \in \operatorname{Aut} G'$, then $A(x) = x$ implies that $A(t) = t$ for all $t \in Z_{G'}(x)^0$, compare* [12], 2.15) *semi-simple elements of order $> n$.*

Proof. It is clear since the set of very strongly regular elements of order $> n$ contains an open subset of G'.

4.2.2. Lemma. *Let G' be an almost-simple algebraic group, $h \in G'$, $h^2 = 1$. If h is regular in G', then G' is of type A_1. If, moreover,* char $k' \neq 2$, *then G' is a k-form of $PGL(2)$.*

Proof. If h is semi-simple, then regular means that for every root $a \in \Sigma$, $a(h) = -1$. But then if a_1, a_2, $a_1 + a_2$ are roots it is impossible for all values to be -1. So h is not semi-simple. Let then $h = h_1 \cdot h_2$ be the Jordan decomposition with h_1 semi-simple and h_2 unipotent. We must have $h_1^2 = h_2^2 = 1$. But if h_1 is semi-simple, $h_1 \neq 1$ and $h_1^2 = 1$, then char $k' \neq 2$, whence $h_2^2 \neq 1$.

Therefore, $h_1 = 1$, h is unipotent and char $k = 2$. The form of a regular unipotent element is given in [12]. It is

$$h = \prod_{a \in \Delta} x_a(1) \prod_{h(a)>1} x_a(t_a)$$

where Δ is a system of simple roots and $h(a)$ is the height of a with respect to Δ. Then

$$h^2 = \prod_{\substack{a+b \in \Sigma \\ a,b \in \Delta}} x_{a+b}(1) \prod_{h(a)>2} x_a(t_a).$$

In particular, if $a + b$ is a root for some $a, b \in \Delta$, then $h^2 \neq 1$. So we proved the first assertion. The second one follows from the fact that the only involution in $SL(2)$, char $k' \neq 2$, is central.

4.2.3. By [6] we can assume that G is anisotropic. Take $a \in G(k)$ such that $\alpha(a)$ is very strongly regular of order $> 2p$. Then $Z_G(a)$ is connected (cf. 1.5.1(i), 1.5.3(i), 1.5.4(i)). Since $a^2 \neq 1$ and G is anisotropic it follows that a is semisimple. Then we have

LEMMA. *If* $h \in N_G(Z_G(a))(k)$, $h \notin Z_G(a)$, $h^2 = 1$, *then every involution, inverting* $Z_G(a)$ *belongs to* $h \cdot Z_G(a)$.

Proof. If h_1 is another involution, inverting $Z_G(a)$, then hh_1 acts as 1 on $Z_G(a)$, whence $hh_1 \in Z_G(a)$, i.e., $h_1 \in hZ_G(a)$, as asserted.

4.2.4. Set $a' = \alpha(a)$, $T' = Z_{G'}(a')$. Since a' is very strongly regular, T' is a maximal torus in G'. Take h as in 4.2.1 and set $h' = \alpha(h)$. Then $h' \in N_{G'}(T')$. Set

$$M(h') = \{g' \in G' \mid h'g'h'^{-1} = g'^{-1}\}.$$

We have the mapping $m(h')$: $G' \to M(h')$ given by

$$m(h')g' = h'g'g'^{-1}g'^{-1}.$$

The fibers of $m(h')$ are principal homogeneous spaces under $Z_{G'}(h')$. In particular,

$$\dim M(h') = \dim G' - \dim Z_{G'}(h').$$

If we replace h' by $h' \cdot t'$ for $t' \in T' \cap M(h')$ then $M(h't') = d'M(h')\, d'^{-1}$, where $d' \in T'$, $d'^2 = t'^{-1}$. (The root exists since we are now in an algebraically closed field.)

Therefore, the union of $M(h't')$ over $t' \in T'$, $h't'h'^{-1} = t'^{-1}$ is contained in

$$N' = \bigcup_{t' \in T'} t'M(h')t'^{-1}.$$

Hence $\dim N' \leqslant \dim G' - \dim Z_{G'}(h') + \dim T'$. Since elements of order 2 are regular only in groups of type A_1, we must assume that

$$\dim N' < \dim G',$$

i.e., that N' is contained in a closed set.

Let $\tilde{N}'$ be the complement to N' in G' and $\bar{N}'$ be an open subset in $\tilde{N}'$ consisting of strongly regular elements of order $> 2p$. Then since $\alpha(G(k))$ is dense in G', we have, that $\alpha(G(k)) \cap \bar{N}'$ is dense in $\bar{N}'$. Take $b \in G(k)$ such that $\alpha(b) \in \bar{N}'$, and set $T_1' = Z_{G'}(b)$ (it is a maximal torus in G'). Then there exists an involution $h_1 \in G(k)$ such that $h_1 b h_1^{-1} = b^{-1}$, $h_1 a h_1^{-1} = a^{-1}$. We have $h \cdot h_1 \in T$, whence it follows that $\alpha(b) \in M(h'\alpha(T)) \subset N'$ which contradicts our choice of b. This proves 4.1(i).

4.3. *Proof of* 4.1(ii).

4.3.1. LEMMA. *Let P be a projective plane over a skew-field K and P' be a projective plane over a skew-field K'. Let π: $P \to P'$ be an imbedding such that three points on a line go into three points on a line, and three points not on a line go into three points not on a line. Then there exists an imbedding of skew-fields φ: $K \to K'$ and a $\varphi(K)$-linear monomorphism τ of underlying spaces of ${}^{\varphi}P$ and P': τ: ${}^{\varphi}V \to V'$ such that π is the composition of φ, π and of natural projections.*

Proof. This is of course a version of the Fundamental Theorem of Projective Geometry. The proof of this latter theorem given in Dieudonne ([8], Ch. II, Section 1.1) or O'Meara ([10], 4.2) goes through and gives the result.

We indicate also another way to prove this Lemma in the case when K is a field. By the main result of Borel-Tits [6] a homomorphism $PGL(3, k) \to PGL(3, K')$ can be obtained by composition of a field homomorphism and a group isomorphism. But under our assumptions the map of projective planes gives rise to a homomorphism $PGL(3, K) \to PGL(3, K')$ and we are through.

4.3.2. Let us begin with the following observation.

LEMMA. *α induces an imbedding $\bar{\alpha}$ of projective planes $S(G(k)) \to S(G'(k'))$.*

Proof. Since α is a monomorphism it maps a minimal centralizer of $G(k)$ into a minimal centralizer of $G'(k')$ and only one minimal centralizer of $G(K)$ is mapped into a minimal centralizer of $G'(k')$. So α induces a map $\bar{\alpha}$: $S(G(k)) \to S(G'(k'))$. Now α maps a Borel subgroup into a Borel subgroup and an involution into an involution. Thus $\bar{\alpha}$ preserves lines and our assertion is proved.

4.3.3. Now we state a variant of 4.1(ii) which we are going to use later.

PROPOSITION. *Suppose that H is a subgroup of $G(k)$ which intersects in an infinite set with every k-subtorus of G. Suppose that α: $H \to G'(k')$ is a monomor-*

phism which maps three semi-simple minimal centralizers in H which are on one line of $G(k)$ into three minimal centralizers in $G'(k')$ also belonging to one line. Then there exist φ and β satisfying (a), (b), (c), *of* 4.1(ii) *such that* $\alpha(h) = \beta(\varphi^0(h))$ *for* $h \in H$.

Remark. Our initial statement 4.1(ii) follows from 4.3.3 because of 4.3.2.

4.3.4. Conversely we have the following

LEMMA. *For α from* 4.3.3 *there exists a map of projective planes $\bar{\alpha}$: $S(G(k)) \to$ such that $\bar{\alpha}(T(k)) = \alpha(T(k) \cap H)$ for every k-torus T of G.*

Proof. Denote by C the unipotent curve of $S(G(k))$. Then by assumptions of 4.3.3 we have a map $\bar{\alpha}$: $S(G(k)) - C \to S(G'(k'))$ which maps points on a line into points on a line. Our task is to show that $\bar{\alpha}$ extends to the whole of $S(G(k))$.

First we note that parabolic lines L of $S(G)$ are distinguished by the property: there exist $M_1, M_2 \in L$ such that $M_1 \neq M_2$ and $D^2(\langle M_1, M_2\rangle) = 1$. This last property holds for M_1 and M_2 if and only if it holds for Zariski dense subsets of M_1 and M_2. This (and our assumptions) imply now that $\bar{\alpha}$ extends to the map of $X = [S(G(k)) - C \cup \{\text{the set of points lying on parabolic lines}\}]$.

If $\operatorname{char} k \neq 2$ then (by 1.4.2) this completes the proof. If $\operatorname{char} k = 2$ it remains to extend $\bar{\alpha}$ to points lying on C (which is now involutorial line) and such that they do not lie on any parabolic line (i.e., the corresponding unipotent subgroups do not lie in any Borel k-subgroup). But such points (if they are still missing) are described as follows: they are maximal sets of pairwise parallel lines of X. In this way $\bar{\alpha}$ extends to the whole of $S(G(k))$ and the lemma is proved.

4.3.5. By 4.3.4 we have a map of projective planes $\bar{\alpha}$: $S(G(k)) \to S(G'(k'))$. By 4.3.1 there exist a unique field homomorphism φ: $k \to k'$ and a (regular) isomorphism π: ${}^{\varphi}S(G) = \mathbb{P}_k{}^2 \to S(G') = \mathbb{P}^2_{k'}$ such that $\bar{\alpha} = \pi \circ \varphi^0$. The image $\pi \circ \varphi^0(S(G(k)))$ is an abstract projective subplane of $\mathbb{P}^2_{k'}$ isomorphic to $\mathbb{P}^2(\varphi(k))$. This endows $\mathbb{P}^2_{k'}$ with a structure of projective space over $\varphi(k)$ and with this structure the map π is defined over $\varphi(k)$. We replace k by $\varphi(k)$, so that we are able to assume that everything happens over k. We consider H and $G'(k')$ as acting on projective planes $S(G)$ and $S(G')$. For a minimal centralizer M this action is given by $g(M) = gMg^{-1}$.

LEMMA. $\alpha(g) \circ \pi = \pi \circ g$ *on* $S(G(k))$.

Proof. For a minimal centralizer M in H we have $(\alpha(g) \circ \pi)(M) = \alpha(g)(\bar{\alpha}(M)) = \alpha(g)(M)) = \alpha(g(M)) = \bar{\alpha}(g(M)) = \pi(g(M))$, which proves our assertion since we have shown in 4.3.4 that the action of α on minimal centralizers of H determines its action of $S(G(k))$.

4.3.6. *End of the proof of* 4.3.3. Denote by $\tilde{\beta}$ the isomorphism $\tilde{\beta}$: $PGL(3)_{\varphi(k)} \to PGL(3)_{k'}$ given by $\beta(x) = \pi \circ x \circ \pi^{-1}$. Then by the beginning paragraph of 4.3.5 we see that $PGL(3)_{k'}$ is endowed with a structure of a $\varphi(k)$-group and $\tilde{\beta}$ is defined over $\varphi(k)$ in this structure. Now Lemma 4.3.5 says that $\alpha = \tilde{\beta} \circ \varphi^0$ on H. Since the Zariski closures of H and $G'(k')$ are G and G' respectively, $\tilde{\beta}$ maps ${}^{\varphi}G$ into G' and we denote by β the restriction of $\tilde{\beta}$ to ${}^{\varphi}G$. So β is an isomorphism of ${}^{\varphi}G$ to G'. Now $(\beta \circ \varphi^0)(H)$ is contained in $G' \cap PGL(3, \varphi(k))$ and it is dense in G' (since for any proper algebraic subgroup R of a group of type A_1 we have $D^2R = 1$ and it is not so for H). Therefore G' is defined over $\varphi(k)$ and β is a $\varphi(k)$-isomorphism. This concludes the proof.

4.4. *Remarks on reconstructability.*

An obstacle in applying the ideas of this paper to subgroups of $G(k)$ is that we may not be able to determine in terms of our subgroup which minimal centralizers lie on one line. We can construct parabolic lines but they are few (if any). So the problem is to construct involutorial lines. Of these we can construct only pieces. Namely, we can use the fact that for two minimal centralizers M_1, M_2 lying on an involutorial line and for two $m_1 \in M_1$, $m_2 \in M_2$ we have that $m_1m_2m_1$ also belongs to a minimal centralizer on the same line. Using this operation we can try to increase the piece in our disposition, but we have no way to establish that this procedure stabilizes at the whole line. The only case I was able to handle in this way is the case when k is a locally compact field and the subgroup in question intersects every k-torus of G in an open set (in locally-compact topology). Thus 4.3.3 is applicable to such subgroups.

5. Appendix: On Forms of $SL(2)$

5.1. *Realizations.*

5.1.1. Let k be a field and let G be a k-form of $SL(2)$. It is known (cf. [13]) that G corresponds to unique algebra D of quaternions defined over k. The correspondence is such that the adjoint group of G is G^D.

5.1.2. In the above realization G represents the functor Ker(Nrd: $D(k')^* \to k'^*$) where k' varies over extensions of k (compare 1.1.1).

5.1.3. The group G can also be identified with the special unitary group of the norm form $x\bar{x} - ay\bar{y}$ (cf. 1.2.7) what can be easily seen from the representation of $D = D_a$ given in 1.2.6 (the notation: $\bar{x}$ and a are the same as in 1.2.6).

5.2. *Tori.*

5.2.1. As in the case of forms of $PGL(2)$ the k-subtori of G correspond to maximal commutative separable k-subalgebras of D. We write T^K for the sub-

torus corresponding to such a subalgebra. When K is fixed we write D as D_a (cf. 1.2.6).

5.2.2. PROPOSITION. *Let* $T = T^K$. *If* $-a \in N_{K/k}(K)$ *then* $[N_{G(k)}(T(k)) : T(k)] = 2$; *otherwise* $N_{G(k)}(T(k)) = T(k)$.

Proof. In representation of 1.2.6, $T(k)$ is represented by diagonal matrices (with $y = 0$). Then any $h \in N_{D(k)}(K) - K$ has a form $\left(\begin{smallmatrix} 0 & y \\ a\bar{y} & 0 \end{smallmatrix}\right)$ for some $y \in K^*$. The condition that $h \in G(k)$ reads: $\mathrm{Nrd}(h) = 1$, i.e., $-ay\bar{y} = 1$, i.e., $-a \in N_{K/k}(K)$. This proves our assertion.

5.2.3. PROPOSITION.

(i) *Let K and K' be k-isomorphic commutative separable two-dimensional k-subalgebras of D. Let T and T' be the corresponding k-tori. If* $\mathrm{Nrd}\, D(k) = N_{K/k}(K)$ *then T and T' are conjugate in $G(k)$.*

(ii) *Conversely, let K be a maximal commutative separable k-subalgebra of D. If any two k-subtori T_1, T_2 such that $K \simeq K_1 = Z_{D(k)}(T_1) \simeq K_2 = Z_{D(k)}(T_2)$ are conjugate by an element of $G(k)$, then $N_{K/k}(K) = \mathrm{Nrd}(D(k))$.*

Proof.

(i) By 1.2.3 there exists $d \in D(k)^*$ such that $dKd^{-1} = K'$. Take $c \in K^*$ such that $N_{K/k}(c) = \mathrm{Nrd}(d)$. Then $(dc^{-1})\, K(dc^{-1})^{-1} = K'$ and $\mathrm{Nrd}(dc^{-1}) = 1$ since $\mathrm{Nrd}\, c = N_{K/k}(c)$. So $g = dc^{-1} \in G(k)$.

(ii) By our assumption for every $d \in D(k)^*$ there exists $c \in G(k)$ (i.e. $c \in D(k)$ with $\mathrm{Nrd}\, c = 1$) such that $dKd^{-1} = cKc^{-1}$. Then $(c^{-1}d)\, K(c^{-1}d)^{-1} = K$ i.e. $c^{-1}d \in Z_{D(k)}(K) = K$. Then $\mathrm{Nrd}(d) = \mathrm{Nrd}(c^{-1}d) \in \mathrm{Nrd}\, K = N_{K/k}(K)$, as required.

5.2.4. COROLLARY. (Compare 1.3.6). *Let K be a maximal separable subfield of D and let B be a Borel subgroup of G. Set $q = 0$ if D is division and $q = 1$ if D. is split. If* $\mathrm{Nrd}\, D(k) = N_{K/k}(K)$ *then $G(k)$ has $q + 1$ or $q + 2$ orbits on $(G/B)(K)$ It has exactly $q + 1$ orbits only in the following case: $D = D_a$ with $-a \in N_{K/k}(K)$.*

Proof is the same as that of 1.3.6, but uses 5.2.2 and 5.2.3.

5.3. *Structure of $\mathbb{P}^2$ on the set of connected one-dimensional subgroups.*

5.3.1. The structure of $\mathbb{P}^2$ on the set of connected one-dimensional subgroups is defined as in the case of $PGL(2)$. There is no real difference. However we are unable to describe the abstract projective plane structure on the set of minimal centralizers, because some (or all) involutions in $G(k)$/(center) may be missing.

5.3.2. The statement 2.1.5 does not hold for forms of $SL(2)$ in characteristic 2 because in this case all tori are mapped by the map Lie into the center of Lie G.

Acknowledgments

I am glad to use this opportunity to express my sincere thanks to A. Borel and D. Kazhdan for many conversations and advice.

References

1. A. A. Albert, "Structure of algebras," Amer. Math. Soc. Colloquium Publ., New York, 1939.
2. E. Artin, "Algèbre géométrique," Gauthier–Villars, Paris, 1962.
3. R. Baer, The group of motions of a two-dimensional elliptic geometry, *Comp. Math.* **9** (1951), 241–288.
4. A. Borel and T. A. Springer, Rationality properties of algebraic groups, II, *Tohoku Math. J.* **20** (1968), 443–497.
5. A. Borel and J. Tits, Groupes réductifs, *Publ. Math. IHES* **27** (1965), 55–151.
6. A. Borel and J. Tits, Homomorphismes "abstraits" des groupes algébriques simples, *Ann. of Math.* **97** (1973), 499–571.
7. A. Borel and J. Tits, Éléments unipotents et sous-groupes paraboliques de groupes réductifs, I, *Invent. Math.* **12** (1971), 95–104.
8. J. Dieudonné, "La géometrie des groupes classiques," Springer-Verlag, Berlin, 1955.
9. N. Jacobson, "The Theory of Rings," Vol. 2, Amer. Math Soc. Math. Surveys, New York, 1943.
10. O. T. O'Meara, "Lectures on Linear Groups," Amer. Math. Society, Providence, R.I., 1974.
11. A. Schmidt, Über die Bewegungsgruppe der ebenen elliptischen Geometrie, *J. Reine Angew. Math.* **186** (1949), 230–240.
12. R. Steinberg, Regular elements of semi-simple algebraic groups, *Publ. Math. IHES* **25** (1965), 49–80.
13. J. Tits, Classification of algebraic semi-simple groups, "Proc. Symp. Pure Math.," Vol. 9, pp. 33–62, Amer. Math. Soc. Providence, R.I., 1966.