TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 352, Number 8, Pages 3881–3912
S 0002-9947(00)02438-7
Article electronically published on April 18, 2000

GALOIS EMBEDDINGS FOR LINEAR GROUPS

SHREERAM S. ABHYANKAR

Abstract. A criterion is given for the solvability of a central Galois embedding problem to go from a projective linear group covering to a vectorial linear group covering.

1. Introduction

By a GEP (Galois Embedding Problem) we mean a (finite) Galois extension M/K together with an epimorphism $d_M : G \to \mathrm{Gal}(M,K)$ where G is a finite group. By a solution of this GEP we mean a Galois extension L/K together with an isomorphism $d_L : G \to \mathrm{Gal}(L,K)$ such that L is an overfield of M and $d_M(g) = d_{L,M}(d_L(g))$ for all $g \in G$ where $d_{L,M} : \mathrm{Gal}(L,K) \to \mathrm{Gal}(M,K)$ is the Galois theoretic epimorphism. The GEP is solvable means it has a solution. The GEP is a CGEP (Central GEP) if $\ker d_M =$ the center $Z(G)$ of G. Note that for any group G we have $Z(G) \lhd G$ (where $\lhd$ denotes normal subgroup); actually $Z(G)$ is a characteristic subgroup of G, i.e., $Z(G)$ is mapped onto itself by every automorphism of G, and hence we get a natural homomorphism $\mathrm{Aut}(G) \to \mathrm{Aut}(G/Z(G))$ (where Aut denotes the group of all automorphisms).

Let $m > 0$ be an integer, and let $q > 1$ be a power of a prime p. Recall that $\mathrm{GL}(m,q)$ is the group of all nonsingular m by m matrices over the field $\mathrm{GF}(q)$ of q elements, and $\mathrm{SL}(m,q)$ is the subgroup of $\mathrm{GL}(m,q)$ consisting of those matrices whose determinant equals one. Note that $\mathrm{GF}(q)^* \approx Z(\mathrm{GL}(m,q)) =$ the set of all nonzero m by m scalar matrices over $\mathrm{GF}(q)$ (where $\mathrm{GF}(q)^*$ denotes the multiplicative group of all nonzero elements of $\mathrm{GF}(q)$ and $\approx$ denotes isomorphism), and $Z(\mathrm{SL}(m,q)) = \mathrm{SL}(m,q) \cap Z(\mathrm{GL}(m,q))$ (see Corollaries 1 and 2 on page 78 of [Suz]); also note that $\mathrm{PGL}(m,q) = \mathrm{GL}(m,q)/Z(\mathrm{GL}(m,q))$, and $\mathrm{PSL}(m,q)$ is the image of $\mathrm{SL}(m,q)$ under the canonical epimorphism $\mathrm{GL}(m,q) \to \mathrm{PGL}(m,q)$. Consider the CGEP given by a Galois extension M/K together with an epimorphism $G \to \mathrm{Gal}(M,K)$ whose kernel is $Z(G)$; the aim of this paper is to give a criterion for this to have a solution when $\mathrm{GF}(q) \subset K$ and $\mathrm{SL}(m,q) < G < \mathrm{GL}(m,q)$ with m divisible by $q-1$, where $<$ denotes subgroup. To abbreviate frequently occurring expressions, for every integer $i \geq -1$ we put

$$\langle i \rangle = 1 + q + q^2 + \cdots + q^i \quad (\text{convention: } \langle 0 \rangle = 1 \text{ and } \langle -1 \rangle = 0).$$

To formulate our criterion, we recall that, according to the definitions introduced in [Ab2] and [Ab3], if K is a field of characteristic p, then $f(Y) \in K[Y]$ (resp.

Received by the editors May 5, 1998 and, in revised form, September 15, 1998.
2000 *Mathematics Subject Classification.* Primary 12F10, 14H30, 20D06, 20E22.
This work was partially supported by NSF Grant DMS 91-01424 and NSA grant MDA 904-97-1-0010.

$F(Y) \in K[Y]$) is said to be a monic projective (resp. monic vectorial) q-polynomial of q-prodegree (resp. q-degree) m (in Y) over K if it is of the form $f(Y) = Y^{\langle m-1 \rangle} + \sum_{i=1}^{m} a_i Y^{\langle m-1-i \rangle}$ (resp. $F(Y) = Y^{q^m} + \sum_{i=1}^{m} a_i Y^{q^{m-i}}$) with $a_i \in K$. Note that $f(Y)$ (resp. $F(Y)$) is separable (i.e., its Y-discriminant is nonzero) $\Leftrightarrow$ $a_m \neq 0$, and note that $F_Y(Y) = F_Y(0) = a_m$ where $F_Y(Y)$ is the Y-derivative of $F(Y)$. Also note that $f(Y) \mapsto F(Y) = Y f(Y^{q-1})$ gives a bijection of monic projectives to monic vectorials (= their vectorial associates).

Now we may state the following:

Embedding Criterion (1.1). *Let $SL(m,q) < G < GL(m,q)$ with m divisible by $q-1$, and let K be a field with $GF(q) \subset K$. Then the CGEP given by a Galois extension M/K together with an epimorphism $d_M : G \to Gal(M,K)$, whose kernel is $Z(G)$, is solvable $\Leftrightarrow$ M/K is the splitting field of a separable monic projective q-polynomial of q-prodegree m over K.*

In Section 2 we shall give a review on vectorial polynomials. Then in Section 3 we shall prove the following Polynomial Theorem, where $|K|$ denotes the cardinality of K.

Polynomial Theorem (1.2). *If L/K is a Galois extension where K is a field with $GF(q) \subset K$ and $|K| \geq q^m$, then $Gal(L,K)$ is abstractly isomorphic to a subgroup of $GL(m,q)$ $\Leftrightarrow$ L/K is the splitting field of a separable monic vectorial q-polynomial of q-degree m over K.*

For a more detailed version of the Polynomial Theorem see Proposition (2.1) of Section 2 and Proposition (3.7) of Section 3. In Section 4, the above Embedding Criterion will be deduced as a consequence of the Polynomial Theorem. For a more detailed version of the Embedding Criterion see Propositions (4.3) and (4.4) of Section 4. In the proof of the Embedding Criterion we shall also use the following Automorphism Lemma which we shall prove in Section 6 as part of Lemma (6.6).

Automorphism Lemma (1.3). *For any group G with $SL(m,q) < G < GL(m,q)$, the natural map $Aut(G) \to Aut(G/Z(G))$ is surjective.*

The proof of the Automorphism Lemma will be based on the following Invariance Lemma about transvections which we shall prove in Section 5 as part of Lemma (5.17). Recall that a transvection is a nonidentity member of $\mathrm{SL}(m,q)$ which leaves some hyperplane in $\mathrm{GF}(q)^m$ elementwise fixed, and a projective transvection is the image of a transvection under the natural epimorphism $\mathrm{GL}(m,q) \to \mathrm{PGL}(m,q)$. [1]

Invariance Lemma (1.4). *Every automorphism of $SL(m,q)$ permutes the set of all transvections. Likewise, every automorphism of $PSL(m,q)$ permutes the set of all projective transvections.*

As a by-product, in Section 6, from the Invariance Lemma we shall also deduce the Automorphism Theorem (6.7) which gives a complete description of the automorphism group of any group between $\mathrm{PSL}(m,q)$ and $\mathrm{PGL}(m,q)$. The various proofs of the Automorphism Theorem available in the literature (cf. Schreier-van der Waerden [ScW], Hua [Hu1], [Hu2], Dieudonné [Di1], [Di2], Steinberg [Ste], and Carter [Car]) not being terribly accessible, for the benefit of the reader (which really

[1] In the language of matrices, transvections correspond to elementary row and column operations. In projective geometry, they correspond to elations (cf. [Dem]). As we shall see in Sections 5 and 6, the ubiquity of transvections in the geometry of projective spaces is all pervasive.

means for the benefit of the author), we have included a self-contained elementary version.[2] Moreover, we have arranged the matter so that most of it remains valid when $\mathrm{GF}(q)$ is replaced by any infinite field.

It is a great pleasure to thank (in alphabetical order) Michael Aschbacher, Walter Feit, Nick Inglis, Bill Kantor, Gregor Kemper, Arne Ledet, B. H. Matzat, J-P. Serre, Ernie Shult, and Gernot Stroth, for many stimulating (electronic, oral or telephonic) conversations concerning the material of this paper.

2. Vectorial polynomials

To review some relevant material on vectorial polynomials given in Lemma (2.5) of [Ab1] and items (3.1) to (3.9) of [Ab3], let $\mathrm{GF}(q) = k \subset K \subset \Omega$ be fields where Ω is an algebraic closure of K, let

$$e(Y) = Y^{\langle m-1\rangle} + \sum_{i=1}^{m} A_i Y^{\langle m-1-i\rangle} \text{ with } A_i \in K \text{ and } A_m \neq 0$$

be a separable monic projective q-polynomial of q-prodegree m in Y over K, and let

$$E(Y) = Y^{q^m} + \sum_{i=1}^{m} A_i Y^{q^{m-i}}$$

be the vectorial associate of $e(Y)$. Let R be the set of all roots of $E(Y)$ in Ω, and note that then R is an m-dimensional k-vector-subspace of Ω; to see this it suffices to observe that $|R| = q^m$ and for all ξ, η, in Ω and $\mu \in k$ we have $E(\xi + \eta) = E(\xi) + E(\eta)$ and $E(\mu\eta) = \mu E(\eta)$. For any $g \in \mathrm{Gal}(K_E, K)$, where $K_E = K(R) =$ the splitting field of $E(Y)$ over K in Ω, we get $\delta(g) \in \mathrm{GL}(R)$ by taking $\delta(g)(\zeta) = g(\zeta)$ for all $\zeta \in R$. This gives a monomorphism $\delta : \mathrm{Gal}(K_E, K) \to \mathrm{GL}(R)$. Let $\overline{R}$ be the set of all roots of $e(Y)$ in Ω. Then $\zeta \mapsto \zeta^{q-1}$ gives a surjective map $R \setminus \{0\} \to \overline{R}$ whose fibers are punctured 1-spaces, i.e., 1-spaces minus the zero vector. Therefore we may identify $\overline{R}$ with the projective space associated with R, and this gives us a monomorphism $\overline{\delta} : \mathrm{Gal}(K_e, K) \to \mathrm{PGL}(R)$, induced by δ, where $K_e = K(\overline{R}) =$ the splitting field of $e(Y)$ over K in Ω. By taking a k-basis of R, we get isomorphisms $\mathrm{GL}(R) \to \mathrm{GL}(m, q)$ and $\mathrm{PGL}(R) \to \mathrm{PGL}(m, q)$, and by composing these with δ and $\overline{\delta}$ respectively, we get natural monomorphisms $D_E : \mathrm{Gal}(K_E, K) \to \mathrm{GL}(m, q)$ and $D_e : \mathrm{Gal}(K_e, K) \to \mathrm{PGL}(m, q)$. Since $\zeta \mapsto \zeta^{q-1}$ gives a surjective map $R \setminus \{0\} \to \overline{R}$, we see that K_e is a subfield of K_E, and hence we get a Galois theoretic epimorphism $D_{E,e} : \mathrm{Gal}(K_E, K) \to \mathrm{Gal}(K_e, K)$. Let $\Theta : \mathrm{GL}(m, q) \to \mathrm{PGL}(m, q)$ be the residue class epimorphism. Then for all $g \in \mathrm{Gal}(E, K)$ we clearly have $\Theta(D_E(g)) = D_e(D_{E,e}(g))$. Thus we have proved the following:

Proposition (2.1). *Let $GF(q) = k \subset K \subset \Omega$ be fields such that Ω is an algebraic closure of K, let $e(Y)$ be a separable monic projective q-polynomial of q-prodegree m in Y over K, and let $E(Y)$ be the vectorial associate of $e(Y)$. Then the roots of $E(Y)$ in Ω form an m-dimensional k-vector-subspace of Ω whose associated projective space consists of the roots of $e(Y)$ in Ω, the splitting field K_e of $e(Y)$ over K in Ω is a subfield of the splitting field K_E of $E(Y)$ over K in Ω, and we have natural monomorphisms $D_E : Gal(K_E, K) \to GL(m, q)$ and $D_e : Gal(K_e, K) \to$*

[2] Without Lie Theory, but based on projective geometry.

$PGL(m,q)$ such that for all $g \in Gal(K_E,K)$ we have $\Theta(D_E(g)) = D_e(D_{E,e}(g))$ where $D_{E,e} : Gal(K_E,K) \to Gal(K_e,K)$ is the Galois theoretic epimorphism and $\Theta : GL(m,q) \to PGL(m,q)$ is the residue class epimorphism.

By taking a k-vector-space basis $B_1,\dots,B_m$ of R, by the above expression of $E(Y)$ we get

$$Y^{q^m} + \sum_{i=1}^{m} A_i Y^{q^{m-i}} = \prod_{(\lambda_1,\dots,\lambda_m)\in k^m} (Y - \lambda_1 B_1 - \cdots - \lambda_m B_m)$$

and from this equation we conclude that: if $A_1,\dots,A_m$ are algebraically independent over K, then $B_1,\dots,B_m$ are algebraically independent over K and we have $A_i = \Gamma_i(B_1,\dots,B_m)$ for $1 \le i \le m$ where $\Gamma_i(B_1,\dots,B_m)$ is a polynomial in $B_1,\dots,B_m$ over K. If $E^*(Y)$ is any monic polynomial of degree q^m in Y over K such that the roots of $E^*(Y)$ in Ω form an m-dimensional k-vector-subspace R^* of Ω, then by substituting a k-vector-space basis $B_1^*,\dots,B_m^*$ of R^* for $B_1,\dots,B_m$ in the above identity we conclude that

$$E^*(Y) = Y^{q^m} + \sum_{i=1}^{m} A_i^* Y^{q^{m-i}} \text{ with } A_i^* = \Gamma_i(B_1^*,\dots,B_m^*) \in K \text{ for } 1 \le i \le m.$$

Thus we have proved the following:

Proposition (2.2). *Let $GF(q) = k \subset K \subset \Omega$ be fields such that Ω is an algebraic closure of K, let $E^*(Y)$ be a monic polynomial of degree q^m in Y over K such that the roots of $E^*(Y)$ in Ω form an m-dimensional k-vector-subspace of Ω. Then $E^*(Y)$ is a separable monic vectorial q-polynomial of q-degree m in Y over K.*

3. Polynomial theorem

Let $\mathrm{GF}(q) = k \subset L$ be fields, and let $V = k^m$ and $W = L^m$. Note that then $V \subset W$. Also note that, given any finite set I together with set-theoretic maps $c : I \to L$ and $d : I \to V$ we have

$$\sum_{i\in I} c(i)\cdot d(i) \in W$$

where the dot stands for scalar multiplication of L on V, i.e., for $l \in L$ and $v \in V$ we have $l \cdot v \in W$, and moreover by equating components we get the following obvious:

Lemma (3.1). *If $\sum_{i\in I} c(i)\cdot d(i) = 0$ and the family $c(i)_{i\in I}$ is linearly independent over k, then $d(i) = 0$ for all $i \in I$.*

Let V' and W' be the respective duals of V and W, i.e., V' is the k-vector-space of all k-linear maps $V \to k$, and W' is the L-vector-space of all L-linear maps $W \to L$. For any $z \in V'$ let $z^\dagger$ be the unique member of W' such that $z^\dagger(v) = z(v)$ for all $v \in V$. Note that then $^\dagger : V' \to W'$ is a k-linear injection. To simplify notation, we define the action of any $z \in V'$ on W by putting $z(t) = z^\dagger(t)$ for all $t \in W$. Then we have the following obvious:

Lemma (3.2). *For any $t \in W$, the map $V' \to L$ given by $z \mapsto z(t)$ is k-linear.*

Also we note the following obvious:

Lemma (3.3). *Let $s : C \to D$ be a set-theoretic injective map, and let a group H act faithfully on C as well as D. Assume that for all $h \in H$ and $z \in C$ we have $h(s(z)) = s(h(z))$. Then $s(C)$ is an H-invariant subset of D, and H acts faithfully on $s(C)$.*

Recall that the action of $\mathrm{GL}(m,q) = \mathrm{GL}(V)$ on V' is defined by setting $g(z)(v) = z(g^{-1}(v))$ for all $g \in \mathrm{GL}(m,q)$ and $z \in V'$ and $v \in V$; note that this action is faithful on V'. Let G be a subgroup of $\mathrm{GL}(m,q) = \mathrm{GL}(V)$. By a *$G$-generating-subset* of V we mean a subset U of V such that every element of V can be expressed as a k-linear combination of the family $g(u)_{(g,u)\in G\times U}$.

Now let K be a field between k and L such that L/K is a Galois extension for which we have an abstract group isomorphism $^{\ddagger} : G \to \mathrm{Gal}(L,K)$. Again, to simplify notation, we define the action of any $g \in G$ on L by putting $g(l) = g^{\ddagger}(l)$ for all $l \in L$.

Given $y \in L$ and a set-theoretic map $x : U \to K$ with $U \subset V$, let

$$w = \sum_{(g,u)\in G\times U} (g(y)x(u)) \cdot g(u) \in W$$

and let the map

$$r : V' \to L \quad \text{be defined by putting} \quad r(z) = z(w) \text{ for all } z \in V'.$$

Now for any $z \in V'$ we have

$$r(z) = \sum_{(g,u)\in G\times U} (g(y)x(u)) \cdot z(g(u)) \in L$$

and if the families $g(y)_{g\in G}$ and $x(u)_{u\in U}$ are linearly independent over K and k respectively, then the family $(g(y)x(u))_{(g,u)\in G\times U}$ is linearly independent over k. Therefore, if $r(z) = 0$ and the families $g(y)_{g\in G}$ and $x(u)_{u\in U}$ are linearly independent over K and k respectively, then by (3.1) $z(g(u)) = 0$ for all $(g,u) \in G \times U$, and if U is also a G-generating-subset of V, then by the k-linearity of z we get $z(v) = 0$ for all $v \in V$ and hence $z = 0$. Thus, in view of (3.2), we have the following:

Lemma (3.4). *If U is a G-generating-subset of V and the families $g(y)_{g\in G}$ and $x(u)_{u\in U}$ are linearly independent over K and k respectively, then $r : V' \to L$ is an injective k-linear map.*

For any $h \in G$ and $z \in V'$ we have

$$\begin{aligned}
h(r(z)) &= h\left(\sum_{(g,u)\in G\times U} (g(y)x(u)) \cdot z(g(u))\right) \\
&= \sum_{(g,u)\in G\times U} (h(g(y))x(u)) \cdot z(g(u)) \\
&= \sum_{(j,u)\in G\times U} ((hj)(y)x(u)) \cdot z(j(u)) \\
&= \sum_{(g,u)\in G\times U} (g(y)x(u)) \cdot z(h^{-1}g(u)) \\
&= \sum_{(g,u)\in G\times U} (g(y)x(u)) \cdot h(z)(g(u)) \\
&= r(h(z))
\end{aligned}$$

where the fourth equality follows by putting $hj = g$. Thus we have proved the following:

Lemma (3.5). *For all $h \in G$ and $z \in V'$ we have $h(r(z)) = r(h(z))$.*

By (3.3) to (3.5) we see that: if U is a G-generating-subset of V and the families $g(y)_{g\in G}$ and $x(u)_{u\in U}$ are linearly independent over K and k respectively, then $r : V' \to L$ is an injective k-linear map, $r(V')$ is a G-invariant subset of L, and the action of G on $r(V')$ is faithful, and hence $L = K(r(V'))$; and upon letting

$$F(Y) = \prod_{z\in V'} (Y - r(z))$$

by Proposition (2.2) we get

$$F(Y) = Y^{q^m} + \sum_{i=1}^{m} a_i Y^{q^{m-i}} \text{ with } a_i \in K \text{ and } a_m \neq 0$$

i.e., $F(Y)$ is a separable monic vectorial q-polynomial of q-degree m in Y over K. Thus we have proved the following:

Lemma (3.6). *If U is a G-generating-subset of V and the families $g(y)_{g\in G}$ and $x(u)_{u\in U}$ are linearly independent over K and k respectively, then $r : V' \to L$ is an injective k-linear map, $r(V')$ is a G-invariant subset of L, the action of G on $r(V')$ is faithful, and upon letting $F(Y) = \prod_{z\in V'}(Y - r(z))$ we have that $F(Y)$ is a separable monic vectorial q-polynomial of q-degree m in Y over K, and $L = K(r(V'))$ = the splitting field of $F(Y)$ over K.*

[Note that by the normal basis theorem we can always find $y \in L$ such that the family $g(y)_{g\in G}$ is linearly independent over K. Also note that if $|U| \leq [K : k]$, then we can find a map $x : U \to K$ such that the family $x(u)_{u\in U}$ is linearly independent over k. Moreover, note that any k-vector-space basis U of V is always a G-generating-subset of V with $|U| = m$. Finally, note that $m \leq [K : k] \Leftrightarrow |K| \geq q^m$.]

By paraphrasing Lemma (3.6) we get the following:

Proposition (3.7). *Let $GF(q) = k \subset K \subset L$ be fields where L/K is Galois with $Gal(L, K)$ abstractly isomorphic to a subgroup G of $GL(m, q)$ for which, upon letting $V = k^m$ we have that (•) V has a G-generating-subset U with $|U| \leq [K : k]$. Then L/K is the splitting field of a separable monic vectorial q-polynomial of q-degree m over K.*

[Note that condition (•) on G is automatically satisfied if $|K| \geq q^m$. Also note that G is transitive on $V \setminus \{0\} \Rightarrow G$ is irreducible on $V \Rightarrow G$ is cyclic on $V \Rightarrow G$ satisfies condition (•), where irreducible means $\{0\}$ and V are the only G-invariant subspaces of V, and cyclic means V has a G-generating-subset U with $|U| = 1$. Finally, note that if $SL(m, q) < G < GL(m, q)$, then G satisfies condition (•); namely, for $m = 1$ this is trivial, whereas for $m > 1$ it follows from what we have just said because in that case G is clearly transitive on $V \setminus \{0\}$.]

By combining Propositions (2.1) and (3.7) we get the **Polynomial Theorem (1.2)** stated in the Introduction.

4. Embedding criterion

As a consequence of standard group theory material (see (9.2) on page 74 and (4.19) on page 141 of [Suz]), the following Transvection Lemma was proved in (2.3) of [Ab1] (where it was assumed that $m > 1$, but the case of $m = 1$ is trivial):

Transvection Lemma (4.1). *Upon letting $\Theta : GL(m,q) \to PGL(m,q)$ be the residue class epimorphism, for any $G < GL(m,q)$ we have $SL(m,q) < G \Leftrightarrow PSL(m,q) < \Theta(G)$.*

Recall that the quasi-p part of a finite group H is denoted by $p(H)$ and is defined to be the subgroup of H generated by all of its p-Sylow subgroups. It can also be characterized as the subgroup of H generated by all of its elements of p-power order. Yet another characterization of it would be as the smallest normal subgroup of H which is the kernel of an epimorphism of H onto a group whose order is prime to p. It follows that $p(H)$ is the only subgroup of H which is isomorphic to $p(H)$. Since $\mathrm{SL}(m,q) \lhd \mathrm{GL}(m,q)$ with $[\mathrm{GL}(m,q) : \mathrm{SL}(m,q)] = q-1$ where $q-1$ is prime to p, and since $\mathrm{SL}(m,q)$ is generated by elements of order p (namely transvections, cf. page 74 of [Suz]), we see that $p(\mathrm{GL}(m,q)) = \mathrm{SL}(m,q)$ (which is the crucial fact used in the proof of Lemma (4.1) above, i.e., in the proof of Lemma (2.3) of [Ab1]). Consequently, by taking homomorphic images, we get $p(\mathrm{PGL}(m,q)) = \mathrm{PSL}(m,q)$. This proves the following:

Subgroup Lemma (4.2). *$SL(m,q)$ is the only subgroup of $GL(m,q)$ which is isomorphic to $SL(m,q)$. Likewise, $PSL(m,q)$ is the only subgroup of $PGL(m,q)$ which is isomorphic to $PSL(m,q)$.*

Now let $\mathrm{SL}(m,q) < G < \mathrm{GL}(m,q)$, let $\Theta : \mathrm{GL}(m,q) \to \mathrm{PGL}(m,q)$ be the residue class epimorphism, let $\mathrm{GF}(q) \subset K \subset M$ be fields such that M/K is a Galois extension for which there is an epimorphism $d_M : G \to \mathrm{Gal}(M,K)$ with $\ker d_M = Z(G)$, and let us take splitting fields in a fixed algebraic closure Ω of M.

First assume that: (*) there exists a Galois extension L/K with $M \subset L \subset \Omega$ for which there is an isomorphism $d_L : G \to \mathrm{Gal}(L,K)$ with $d_M(g) = d_{L,M}(d_L(g))$ for all $g \in G$ where $d_{L,M} : \mathrm{Gal}(L,K) \to \mathrm{Gal}(M,K)$ is the Galois theoretic epimorphism. Then by (3.7), L/K is the splitting field of a separable monic vectorial q-polynomial $E(Y)$ of q-degree m in Y over K. Let $e(Y)$ be the separable monic projective q-polynomial of q-prodegree m in Y over K such that $E(Y)$ is the vectorial associate of $e(Y)$, and let K_e be the splitting field of $e(Y)$ over K. Then by taking $L = K_E$ in (2.1) we see that K_e is a subfield of L, and there exist monomorphisms $D_E : \mathrm{Gal}(L,K) \to \mathrm{GL}(m,q)$ and $D_e : \mathrm{Gal}(K_e,K) \to \mathrm{PGL}(m,q)$ such that for all $g \in \mathrm{Gal}(L,K)$ we have $\Theta(D_E(g)) = D_e(D_{E,e}(g))$ where $D_{E,e} : \mathrm{Gal}(L,K) \to \mathrm{Gal}(K_e,K)$ is the Galois theoretic epimorphism. Since $\mathrm{SL}(m,q) \approx D_E(d_L(\mathrm{SL}(m,q))) < D_E(\mathrm{Gal}(L,K)) < \mathrm{GL}(m,q)$, by (4.2) we see that $\mathrm{SL}(m,q) < D_E(\mathrm{Gal}(L,K))$, and hence $D_E(\mathrm{Gal}(L,K)) \cap \ker\Theta = Z(D_E(\mathrm{Gal}(L,K)))$, and therefore via the monomorphism D_E we conclude that $\ker D_{E,e} = Z(\mathrm{Gal}(L,K))$. Since $\ker d_M = Z(G)$, via the isomorphism d_L we also see that $\ker d_{L,M} = Z(\mathrm{Gal}(L,K))$. Thus $\ker d_{L,M} = \ker D_{E,e}$, and hence by Galois correspondence we get $M =$ the fixed field of $\ker d_{L,M} =$ the fixed field of $\ker D_{E,e} = K_e$, i.e., $M =$ the splitting field of $e(Y)$ over K.

Next, instead of assuming (*), assume that: (**) m is divisible by $q-1$ and M/K is the splitting field of a separable monic projective q-polynomial $e(Y)$ of

q-prodegree m in Y over K. Let L be the splitting field of the vectorial associate $E(Y)$ of $e(Y)$ over K. Then by taking $(M, L) = (K_e, K_E)$ in (2.1) we see that M is a subfield of L, and there exist monomorphisms $D_E : \mathrm{Gal}(L, K) \to \mathrm{GL}(m, q)$ and $D_e : \mathrm{Gal}(M, K) \to \mathrm{PGL}(m, q)$ such that for all $g \in \mathrm{Gal}(L, K)$ we have $\Theta(D_E(g)) = D_e(d_{L,M}(g))$ where $d_{L,M} : \mathrm{Gal}(L, K) \to \mathrm{Gal}(M, K)$ is the Galois theoretic epimorphism. Since $\mathrm{PSL}(m, q) \approx d_M(\mathrm{SL}(m, q)) < \mathrm{Gal}(M, K) \approx D_e(\mathrm{Gal}(M, K)) < \mathrm{PGL}(m, q)$, by (4.2) we get $\mathrm{PSL}(m, q) < D_e(\mathrm{Gal}(M, K))$. Therefore, since $D_E(\mathrm{Gal}(L, K)) < \mathrm{GL}(m, q)$ with $\Theta(D_E(\mathrm{Gal}(L, K))) = D_e(\mathrm{Gal}(M, K))$, by (4.1) we get $\mathrm{SL}(m, q) < D_E(\mathrm{Gal}(L, K))$. Thus $D_E(\mathrm{Gal}(L, K))$ and G are both groups between $\mathrm{SL}(m, q)$ and $\mathrm{GL}(m, q)$ and their images under Θ are isomorphic to each other because, respectively via d_M and D_e, these images are isomorphic to $\mathrm{Gal}(M, K)$. Therefore, since m is divisible by $q - 1$, we must have $D_E(\mathrm{Gal}(L, K)) = G$. This gives rise to an isomorphism $d_L^* : G \to \mathrm{Gal}(L, K)$ such that $D_E(d_L^*(g)) = g$ for all $g \in G$. We get an epimorphism $d_M^* : G \to \mathrm{Gal}(M, K)$ by taking $d_M^*(g) = d_{L,M}(d_L^*(g))$ for all $g \in G$. Now d_M and d_M^* are both epimorphisms $G \to \mathrm{Gal}(M, K)$ with kernel $Z(G)$. Therefore, there exists an automorphism h of $\mathrm{Gal}(M, K)$ such that $h(d_M(g)) = d_M^*(g)$ for all $g \in G$. Consequently, in view of the **Automorphism Lemma (1.3)** which was stated in the Introduction and which will be proved in Section 6, by composing d_L^* with an automorphism of G we get an isomorphism $d_L : G \to \mathrm{Gal}(L, K)$ such that $d_M(g) = d_{L,M}(d_L(g))$ for all $g \in G$.

Thus we have proved Propositions (4.5) and (4.6) below.

Proposition (4.5). *Let $SL(m, q) < G < GL(m, q)$, let $GF(q) \subset K \subset M$ be fields such that M/K is a Galois extension for which there is an epimorphism $d_M : G \to Gal(M, K)$ with ker $d_M = Z(G)$, and let us take splitting fields in a fixed algebraic closure Ω of M. Assume that there exists a Galois extension L/K with $M \subset L \subset \Omega$ for which there is an isomorphism $d_L : G \to Gal(L, K)$ with $d_M(g) = d_{L,M}(d_L(g))$ for all $g \in G$ where $d_{L,M} : Gal(L, K) \to Gal(M, K)$ is the Galois theoretic epimorphism. Then M/K is the splitting field of a separable monic projective q-polynomial $e(Y)$ of q-prodegree m in Y over K, and L/K is the splitting field of the vectorial associate $E(Y)$ of $e(Y)$.*

Proposition (4.6). *Let $SL(m, q) < G < GL(m, q)$ with m divisible by $q - 1$, let $GF(q) \subset K \subset M$ be fields such that M/K is a Galois extension for which there is an epimorphism $d_M : G \to Gal(M, K)$ with ker $d_M = Z(G)$, and let us take splitting fields in a fixed algebraic closure Ω of M. Assume that M/K is the splitting field of a separable monic projective q-polynomial $e(Y)$ of q-prodegree m in Y over K, and let L be the splitting field of the vectorial associate $E(Y)$ of $e(Y)$ over K. Then there exists an isomorphism $d_L : G \to Gal(L, K)$ such that $d_M(g) = d_{L,M}(d_L(g))$ for all $g \in G$.*

From Propositions (4.5) and (4.6) we immediately conclude with the **Embedding Criterion (1.1)** stated in the Introduction.

5. Invariance lemma

To prove the Invariance Lemma (1.4) stated in the Introduction, let $k = \mathrm{GF}(q)$ and $V = k^m$. Recall that a transvection (on V) is a nonidentity member of $\mathrm{SL}(m, q)$ which leaves some hyperplane in V (i.e., an $(m-1)$-dimensional k-vector-subspace of V) elementwise fixed. Also recall that a projective transvection (on V) is the image of a transvection under the natural epimorphism $\Theta : \mathrm{GL}(m, q) \to \mathrm{PGL}(m, q)$. *Let*

T be the set of all transvections, and let $\widehat{T}$ be the set of all projective transvections. If $m = 1$, then T and $\widehat{T}$ are empty and we have nothing to show. *So henceforth assume that $m > 1$.*[3]

Let $\mathcal{P}(V)$ (resp. $\mathcal{P}'(V)$) be the projective space (resp. dual projective space) associated with V, i.e., $\mathcal{P}(V)$ (resp. $\mathcal{P}'(V)$) is the set of all 1-dimensional (resp. $(m-1)$-dimensional) k-vector-subspaces of V. Also let $\mathcal{P}^*(V)$ be the set of all pairs $P^* = (P, P') \in \mathcal{P}(V) \times \mathcal{P}'(V)$ with $P \subset P'$.

Now if a k-linear map $V \to V$ leaves two distinct hyperplanes in V elementwise fixed, then clearly it must be the identity map $1 : V \to V$. Therefore a transvection t determines the hyperplane $X'(t)$ in V which it leaves elementwise fixed, and this gives us a map $X' : T \to \mathcal{P}'(V)$. For a transvection t, $\ker(t-1) = \{v \in V : t(v) = v\}$ is a proper subspace of V containing $X'(t)$ and hence $\ker(t-1) = X'(t)$ and therefore upon letting $X(t) = \mathrm{im}(t-1) = \{t(v) - v : v \in V\}$ we get $X(t) \in \mathcal{P}(V)$, and this gives us a map $X : T \to \mathcal{P}(V)$. For a transvection t, we clearly have $t(X(t)) = X(t)$ and hence if the induced map $X(t) \to X(t)$ was not the identity, then we can take a basis $(v_1, \ldots, v_m)$ of V with $X'(t) = kv_1 + \cdots + kv_{m-1}$ and $X(t) = kv_m$ and then $t(v_1) = v_1, \ldots, t(v_{m-1}) = v_{m-1}$ and $t(v_m) = \lambda v_m$ with $0 \neq \lambda \neq 1$ in k, and obviously the determinant of t with respect to this basis equals λ which contradicts the assumption of t being in $\mathrm{SL}(m, q)$. Therefore for a transvection t we necessarily have $X(t) \subset X'(t)$ and hence upon letting $X^*(t) = (X(t), X'(t))$ we get a map $X^* : T \to \mathcal{P}^*(V)$.

For any $P \in \mathcal{P}(V)$ we put $T(P) = X^{-1}(P)$, for any $P' \in \mathcal{P}'(V)$ we put $T'(P') = X'^{-1}(P')$, and for any $P^* \in \mathcal{P}^*(V)$ we put $T^*(P^*) = X^{*-1}(P^*)$. Since $T(P)$, $T'(P')$ and $T^*(P^*)$ are defined in terms of inverse images of maps, we obviously get the following:

Lemma (5.1). *For any $P \neq Q$ in $\mathcal{P}(V)$ we have $T(P) \cap T(Q) = \emptyset$. For any $P' \neq Q'$ in $\mathcal{P}'(V)$ we have $T'(P') \cap T'(Q') = \emptyset$. For any $P^* \neq Q^*$ in $\mathcal{P}^*(V)$ we have $T^*(P^*) \cap T^*(Q^*) = \emptyset$.*

Let, if possible, $P_i^* = (P_i, P_i') \in \mathcal{P}^*(V)$ and $t_i \in T^*(P_i^*)$ for $1 \leq i \leq 2$ be such that $t_1 \neq t_2$ but $\Theta(t_1) = \Theta(t_2)$. Then for some $\lambda \in k$ with $0 \neq \lambda \neq 1$ we must have $(t_1^{-1}t_2)(v) = \lambda v$ for all $v \in V$.[4] Clearly $(t_1^{-1}t_2)(v) = v$ for all $v \in P_1' \cap P_2'$, and hence $P_1' \cap P_2' = \{0\}$. Consequently, we must have $m = 2$ and $P_1 = P_1' \neq P_2' = P_2$. Therefore we can take a basis (v_1, v_2) of V such that $P_i' = kv_i$ for $1 \leq i \leq 2$, and for any such basis we have $t_i(v_i) = v_i$ for $1 \leq i \leq 2$, and $t_1(v_2) = v_2 + \lambda_1 v_1$ and $t_2(v_1) = v_1 + \lambda_2 v_2$ with $\lambda_i \in k$ for $1 \leq i \leq 2$. It follows that $(t_1^{-1}t_2)(v_2) = v_2 - \lambda_1 v_1$ which is a contradiction because for all $v \in V$ we have $(t_1^{-1}t_2)(v) = \lambda v$ with $1 \neq \lambda \in k$. Thus we have proved the following:

Lemma (5.2). *For any $t_1 \neq t_2$ in T we have $\Theta(t_1) \neq \Theta(t_2)$. In other words, Θ induces a bijection $T \to \widehat{T}$.*

By Lemma (5.2) we see that, for any $\tau \in \widehat{T}$ there is a unique $\widehat{X}(\tau) \in \mathcal{P}(V)$ and a unique $\widehat{X}'(\tau) \in \mathcal{P}'(V)$ such that upon letting t be a unique member of T

[3] In this section, in addition to proving the Invariance Lemma, we shall also prove various other basic facts about transvections. We have arranged the matter so that most of it is valid for any field k, and we have preferred to give an intrinsic geometric treatment. At the end of the section, in Remark (5.18), we shall give an alternative matrix treatment of some things.

[4] We are using the functional notation, i.e., for maps s and t, the map st is given by $(st)(v) = s(t(v))$.

with $\Theta(t) = \tau$ we have $\widehat{X}(\tau) = X(t)$ and $\widehat{X}'(\tau) = X'(t)$. This gives us maps $\widehat{X} : \widehat{T} \to \mathcal{P}(V)$ and $\widehat{X}' : \widehat{T} \to \mathcal{P}'(V)$. By putting $\widehat{X}^*(\tau) = (\widehat{X}(\tau), \widehat{X}'(\tau))$ we also get a map $\widehat{X}^* : \widehat{T} \to \mathcal{P}^*(V)$.

For any $P \in \mathcal{P}(V)$ we put $\widehat{T}(P) = \widehat{X}^{-1}(P)$, for any $P' \in \mathcal{P}'(V)$ we put $\widehat{T}'(P') = \widehat{X}'^{-1}(P')$, and for any $P^* \in \mathcal{P}^*(V)$ we put $\widehat{T}^*(P^*) = \widehat{X}^{*-1}(P^*)$.[5] Since $\widehat{T}(P)$, $\widehat{T}'(P')$ and $\widehat{T}^*(P^*)$ are defined in terms of inverse images of maps, we obviously get the following:

Lemma (5.3). *For any $P \neq Q$ in $\mathcal{P}(V)$ we have $\widehat{T}(P) \cap \widehat{T}(Q) = \emptyset$. For any $P' \neq Q'$ in $\mathcal{P}'(V)$ we have $\widehat{T}'(P') \cap \widehat{T}'(Q') = \emptyset$. For any $P^* \neq Q^*$ in $\mathcal{P}^*(V)$ we have $\widehat{T}^*(P^*) \cap \widehat{T}^*(Q^*) = \emptyset$.*

Given any $P' \in \mathcal{P}'(V)$ and any s and t in $T'(P')$ with $st \neq 1$, for all $v \in P'$ we have $(st)(v) = s(t(v)) = s(v) = v$ and hence $st \in T'(P')$. Given any $P^* = (P, P') \in \mathcal{P}^*(V)$ and any s and t in $T^*(P^*)$ with $st \neq 1$, by what we just proved we have $st \in T'(P')$, and by taking some $u \in V \setminus P'$ we get $s(u) = u + w$ and $t(u) = u + w'$ with w and w' in P and hence $(st)(u) = u + w + w'$ with $w + w' \in P$ and therefore $st \in T(P)$ and hence $st \in T^*(P^*)$. Given any $P \in \mathcal{P}(V)$ and any s and t in $T(P)$ with $st \neq 1$ and $X'(s) = X'(t)$, by what we have just proved we get $st \in T(P)$. Finally, given any $P \in \mathcal{P}(V)$ and any s and t in $T(P)$ with $X'(s) \neq X'(t)$, upon letting $P^\flat = X'(s) \cap X'(t)$ we see that $P^\flat$ is an $(m-2)$-dimensional k-vector-subspace of V and we can take u and u^* in $V \setminus P^\flat$ such that $X'(s) = P^\flat + ku^*$ and $X'(t) = P^\flat + ku$ and $V = P^\flat + ku + ku^*$, and now we have $s(u) = u + w$ and $t(u^*) = u^* + \lambda w$ with $0 \neq w \in P$ and $0 \neq \lambda \in k$, and upon letting $u' = \lambda u - u^*$ and $P' = P^\flat + u'k$ we get $P' \in \mathcal{P}'(V)$ with $V = P' + u^*k$ and we have $(st)(u^*) = u^* + \lambda w$ and $(st)(u') = u'$, and therefore $st \in T$ with $X(st) = P$ and $X'(st) = P'$ and hence, in particular, $st \in T(P)$. Thus we have proved the following:

Lemma (5.4). *For any $P \in \mathcal{P}(V)$ we have $T(P) \cup \{1\} < SL(m, q)$. For any $P' \in \mathcal{P}'(V)$ we have $T'(P') \cup \{1\} < SL(m, q)$. For any $P^* \in \mathcal{P}^*(V)$ we have $T^*(P^*) \cup \{1\} < SL(m, q)$.*

Let, if possible, $P_i^* = (P_i, P_i') \in \mathcal{P}^*(V)$ and $t_i \in T^*(P_i^*)$ for $1 \leq i \leq 3$ be such that $t_1 t_2 = t_3$ and $P_1 \neq P_2$ and $P_1' \neq P_2'$. Now by (5.4) we see that $t_i^{-1} \in T^*(P_i^*)$ for $1 \leq i \leq 3$. Since $t_1^{-1} t_3 = t_2$ and $t_3 t_2^{-1} = t_1$, by (5.4) we also see that $P_1 \neq P_3 \neq P_2$ and $P_1' \neq P_3' \neq P_2'$. By the equation $t_1 t_2 = t_3$ we get $t_3(v) = v$ for all $v \in P_1' \cap P_2'$, and hence $P_1' \cap P_2' \subset P_3'$, and therefore upon letting $P^\flat = P_1' \cap P_2'$ we see that $P^\flat$ is an $(m-2)$-dimensional k-vector-subspace of V and there exist vectors u_1, u_2, u_3 in $V \setminus P^\flat$ such that $P_i' = P^\flat + u_i k$ for $1 \leq i \leq 3$ and $V = P^\flat + u_1 k + u_2 k$ and $u_1 + u_2 = u_3$. Note that then the vectors u_1 and u_2 are linearly independent (over k) modulo $P^\flat$, and for $1 \leq i \leq 3$ we have $t_i(u_i) = u_i$ and $t_i(v) = v$ for all $v \in P^\flat$. Moreover, we can find $0 \neq w_i \in P_i$ for $1 \leq i \leq 2$ such that $t_1(u_2) = u_2 + w_1$ and $t_2(u_1) = u_1 + w_2$. Note that then the vectors w_1 and w_2 are linearly independent (over k), and we have $t_1^{-1}(u_2) = u_2 - w_1$ and $t_2^{-1}(u_1) = u_1 - w_2$. If $P_2 \subset P^\flat$, then $w_2 \in P_1'$ and hence $(t_1 t_2)(u_1 + u_2) = t_1(u_1 + u_2 + w_2) = u_1 + u_2 + w_1 + w_2$ and therefore by the equations $t_1 t_2 = t_3$ and $u_1 + u_2 = u_3$ we get $t_3(u_3) - u_3 = w_1 + w_2$

[5] In geometric terms, $\widehat{T}(P)$ are the elations with center P, and $\widehat{T}'(P')$ are the elations with axis P'. Similarly, if $P^* = (P, P')$, then $\widehat{T}^*(P^*)$ are the elations with center P and axis P'; see [Dem].

which is a contradiction because $t_3(u_3) - u_3 = 0$ but the vectors w_1 and w_2 are linearly independent. If $P_1 \subset P^\flat$, then $w_1 \in P_2'$ and hence $(t_2^{-1}t_1^{-1})(u_1+u_2) = t_2^{-1}(u_1+u_2-w_1) = u_1+u_2-w_1-w_2$ and therefore by the equations $t_2^{-1}t_1^{-1} = t_3^{-1}$ and $u_1+u_2 = u_3$ we get $t_3^{-1}(u_3)-u_3 = -w_1-w_2$ which is a contradiction because $t_3^{-1}(u_3)-u_3 = 0$ but the vectors w_1 and w_2 are linearly independent. Finally, if $P_1 \not\subset P^\flat$ and $P_2 \not\subset P^\flat$, then we must have $w_i = \lambda_i u_i + w_i'$ with $0 \neq \lambda_i \in k$ and $w_i' \in P^\flat$ for $1 \leq i \leq 2$, and now

$$\begin{aligned}(t_1t_2)(u_1+u_2) &= t_1(u_1+u_2+w_2) = t_1(u_1+(1+\lambda_2)u_2+w_2')\\ &= u_1+(1+\lambda_2)(u_2+w_1)+w_2' = (1+\lambda_1+\lambda_1\lambda_2)u_1+(1+\lambda_2)u_2+w_3'\end{aligned}$$

with $w_3' = (1+\lambda_2)w_1'+w_2' \in P^\flat$, and therefore by the equations $t_1t_2 = t_3$ and $u_1+u_2 = u_3$ we get $t_3(u_3)-u_3 = (\lambda_1+\lambda_1\lambda_2)u_1+\lambda_2u_2+w_3'$ which is a contradiction because $t_3(u_3)-u_3 = 0$ but the vectors u_1 and u_2 are linearly independent modulo $P^\flat$. Thus we have proved the following:

Lemma (5.5). *If $P_i^* = (P_i, P_i') \in \mathcal{P}^*(V)$ and $t_i \in T^*(P_i^*)$ for $1 \leq i \leq 2$ are such that $t_1t_2 \in T \cup \{1\}$, then either $P_1 = P_2$ or $P_1' = P_2'$.*

We shall now prove the following characterization of the sets $T(P)$, $T'(P')$, and $T^*(P^*)$ in terms of k-linear maps.

Lemma (5.6). *Let $t : V \to V$ be a k-linear map. Then:*

(5.6.1) For any $P \in \mathcal{P}(V)$ we have $t \in T(P)\cup\{1\} \Leftrightarrow im(t-1) \subset P \subset ker(t-1)$, and we have $t \in T(P) \Leftrightarrow im(t-1) = P \subset ker(t-1)$.

(5.6.2) For any $P' \in \mathcal{P}'(V)$ we have $t \in T'(P')\cup\{1\} \Leftrightarrow im(t-1) \subset P' \subset ker(t-1)$, and we have $t \in T'(P') \Leftrightarrow im(t-1) \subset P' = ker(t-1)$.

(5.6.3) For any $P^* = (P, P') \in \mathcal{P}^*(V)$ we have $t \in T^*(P^*)\cup\{1\} \Leftrightarrow im(t-1) \subset P \subset P' \subset ker(t-1)$, and we have $t \in T^*(P^*) \Leftrightarrow im(t-1) = P \subset P' = ker(t-1)$.

Namely, for the k-linear map $t-1 : V \to V$ we obviously have $\mathrm{im}(t-1) = \{0\} \Leftrightarrow t = 1 \Leftrightarrow \ker(t-1) = V$, and hence all six implications "$\Rightarrow$" in (5.6.1) to (5.6.3) follow from the discussion at the beginning (in the third paragraph) of this section. Now for a moment suppose that $\mathrm{im}(t-1) \subset P \subset \ker(t-1)$ for some $P \in \mathcal{P}(V)$; then we can take a basis $(v_1, \ldots, v_m)$ of V with $P = kv_1$, and for any such basis we have $t(v_1) = v_1, t(v_2) = v_2+\lambda_2v_1, \ldots, t(v_m) = v_m+\lambda_mv_1$ with $\lambda_2, \ldots, \lambda_m$ in k, and hence $t \in \mathrm{SL}(m,q)$, and therefore $t \neq 1 \Leftrightarrow \mathrm{im}(t-1) = P \Leftrightarrow \ker(t-1) \in \mathcal{P}'(V) \Leftrightarrow t \in T(P)$, which proves (5.6.1). Next for a moment suppose that $\mathrm{im}(t-1) \subset P' \subset \ker(t-1)$ for some $P' \in \mathcal{P}'(V)$; then we can take a basis $(v_1, \ldots, v_m)$ of V with $P' = kv_1+\cdots+kv_{m-1}$, and for any such basis we have $t(v_1) = v_1, \ldots, t(v_{m-1}) = v_{m-1}, t(v_m) = \lambda_1v_1+\cdots+\lambda_{m-1}v_{m-1}+v_m$ with $\lambda_1, \ldots, \lambda_{m-1}$ in k, and hence $t \in \mathrm{SL}(m,q)$, and therefore $t \neq 1 \Leftrightarrow \ker(t-1) = P' \Leftrightarrow t \in T'(P')$, which proves (5.6.2). Finally, for a moment suppose that $\mathrm{im}(t-1) \subset P \subset P' \subset \ker(t-1)$ for some $P^* = (P, P') \in \mathcal{P}^*(V)$; then we can take a basis $(v_1, \ldots, v_m)$ of V with $P = kv_1$ and $P' = kv_1+\cdots+kv_{m-1}$, and for any such basis we have $t(v_1) = v_1, \ldots, t(v_{m-1}) = v_{m-1}, t(v_m) = \lambda_1v_1+v_m$ with λ_1 in k, and hence $t \in \mathrm{SL}(m,q)$, and therefore $t \neq 1 \Leftrightarrow \mathrm{im}(t-1) = P \Leftrightarrow \ker(t-1) = P' \Leftrightarrow t \in T^*(P^*)$, which proves (5.6.3).

By using the above characterization, we shall now reprove Lemma (5.4) and also obtain a description of the isomorphism types of the groups $T(P)\cup\{1\}$, $T'(P')\cup\{1\}$, and $T^*(P^*)\cup\{1\}$ by establishing the following Lemma (5.7), where k^+ denotes the

underlying additive group of k, and $(k^+)^n$ denotes the direct sum of n copies of k^+. For a matrix treatment of Lemma (5.7) and its proof see Remark (5.18).

Lemma (5.7). *For any $P \in \mathcal{P}(V)$ we have $(k^+)^{m-1} \approx T(P) \cup \{1\} < SL(m,q)$. For any $P' \in \mathcal{P}'(V)$ we have $(k^+)^{m-1} \approx T'(P') \cup \{1\} < SL(m,q)$. For any $P^* \in \mathcal{P}^*(V)$ we have $k^+ \approx T^*(P^*) \cup \{1\} < SL(m,q)$.*

[Thus, in particular, $T(P)$, $T'(P')$, and $T^*(P^*)$ are transvectal punctured subgroups of $SL(m,q)$, where by a "punctured subgroup" we mean a nonempty subset of a group which does not contain the identity but forms a subgroup when augmented by the identity, and by "transvectal" we mean consisting only of transvections.]

Namely, given any $P \in \mathcal{P}(V)$, we can take a basis $(v_1, \dots, v_m)$ of V with $P = kv_1$, and then for any $\lambda = (\lambda_2, \dots, \lambda_m) \in (k^+)^{m-1}$ we have a unique k-linear map $t_\lambda : V \to V$ such that $t_\lambda(v_1) = v_1, t_\lambda(v_2) = \lambda_2 v_1 + v_2, \dots, t_\lambda(v_m) = \lambda_m v_1 + v_m$; by (5.6.1) we see that $\lambda \mapsto t_\lambda$ gives a bijection $(k^+)^{m-1} \to T(P) \cup \{1\}$; for any λ and λ' in $(k^+)^{m-1}$ we clearly have $(t_\lambda(t_{\lambda'}(v)) = t_{\lambda+\lambda'}(v)$ for all $v \in V$; therefore $(k^+)^{m-1} \approx T(P) \cup \{1\} < \mathrm{SL}(m,q)$. Likewise, given any $P' \in \mathcal{P}'(V)$, we can take a basis $(v_1, \dots, v_m)$ of V with $P' = kv_1 + \cdots + kv_{m-1}$, and then for any $\lambda = (\lambda_1, \dots, \lambda_{m-1}) \in (k^+)^{m-1}$ we have a unique k-linear map $t_\lambda : V \to V$ such that $t_\lambda(v_1) = v_1, \dots, t_\lambda(v_{m-1}) = v_{m-1}, t_\lambda(v_m) = \lambda_1 v_1 + \cdots + \lambda_{m-1} v_{m-1} + v_m$; by (5.6.2) we see that $\lambda \mapsto t_\lambda$ gives a bijection $(k^+)^{m-1} \to T'(P') \cup \{1\}$; for any λ and λ' in $(k^+)^{m-1}$ we clearly have $(t_\lambda(t_{\lambda'}(v)) = t_{\lambda+\lambda'}(v)$ for all $v \in V$; therefore $(k^+)^{m-1} \approx T'(P') \cup \{1\} < \mathrm{SL}(m,q)$. Finally, given any $P^* = (P, P') \in \mathcal{P}^*(V)$, we can take a basis $(v_1, \dots, v_m)$ of V with $P = kv_1$ and $P' = kv_1 + \cdots + kv_{m-1}$, and then for any $\lambda \in k = k^+$ we have a unique k-linear map $t_\lambda : V \to V$ such that $t_\lambda(v_1) = v_1, \dots, t_\lambda(v_{m-1}) = v_{m-1}, t_\lambda(v_m) = \lambda v_1 + v_m$; by (5.6.3) we see that $\lambda \mapsto t_\lambda$ gives a bijection $k^+ \to T^*(P^*) \cup \{1\}$; for any λ and λ' in k^+ we clearly have $(t_\lambda(t_{\lambda'}(v)) = t_{\lambda+\lambda'}(v)$ for all $v \in V$; therefore $k^+ \approx T^*(P^*) \cup \{1\} < \mathrm{SL}(m,q)$. This completes the proof of (5.7).

By Lemmas (5.1) and (5.7) we get the following:

Lemma (5.8). *The map $X : T \to \mathcal{P}(V)$ is surjective and the set T can be expressed as the union $T = \coprod_{P \in \mathcal{P}(V)} T(P)$ of pairwise disjoint nonempty subsets. The map $X' : T \to \mathcal{P}'(V)$ is surjective and the set T can be expressed as the union $T = \coprod_{P' \in \mathcal{P}'(V)} T'(P')$ of pairwise disjoint nonempty subsets. The map $X^* : T \to \mathcal{P}^*(V)$ is surjective and the set T can be expressed as the union $T = \coprod_{P^* \in \mathcal{P}^*(V)} T^*(P^*)$ of pairwise disjoint nonempty subsets.*

Let us note that a *maximal transvectal punctured subgroup* of $\mathrm{SL}(m,q)$ is a nonempty subset S of T such that $S \cup \{1\} < \mathrm{SL}(m,q)$ and such that there is no subset S' of T other than S for which $S \subset S'$ and $S' \cup \{1\} < \mathrm{SL}(m,q)$. Now by (5.5) we see that $S \subset T$ with $S \cup \{1\} < \mathrm{SL}(m,q) \Rightarrow$ either $S \subset T(P)$ for some $P \in \mathcal{P}(V)$ or $S \subset T'(P')$ for some $P' \in \mathcal{P}'(V)$. Moreover, if $m > 2$, then for all $P \in \mathcal{P}(V)$ and $P' \in \mathcal{P}'(V)$ we clearly have $T(P) \not\subset T'(P') \not\subset T(P)$ [say because every $P' \in \mathcal{P}'(V)$ contains some $P_1 \neq P_2$ in $\mathcal{P}(V)$, every $P \in \mathcal{P}(V)$ passes through some $P'_1 \neq P'_2$ in $\mathcal{P}'(V)$, and for every $P^* = (P, P') \in \mathcal{P}^*(V)$ we have $T^*(P^*) = T(P) \cap T'(P')$]. Likewise, if $m = 2$, then for every $P^* = (P, P') \in \mathcal{P}^*(V)$ we clearly have $P = P'$ and $T(P) = T'(P') = T^*(P^*)$. Therefore by (5.1) and (5.7) we get the following:

Lemma (5.9). *If $m > 2$, then the two families $T(P)_{P \in \mathcal{P}(V)}$ and $T'(P')_{P' \in \mathcal{P}'(V)}$ give us exactly all the distinct maximal transvectal punctured subgroups of $SL(m,q)$.*

If $m = 2$, then the family $T^*(P^*)_{P^* \in \mathcal{P}^*(V)}$ gives us exactly all the distinct maximal transvectal punctured subgroups of $SL(m, q)$.

[In other words, if $m > 2$, then for every $P \in \mathcal{P}(V)$, the set $T(P)$ is a maximal transvectal punctured subgroup of $SL(m, q)$ such that $T(P) \neq T(Q)$ for all $Q \neq P$ in $\mathcal{P}(V)$, and $T(P) \neq T'(P')$ for all P' in $\mathcal{P}'(V)$; for every $P' \in \mathcal{P}'(V)$, the set $T'(P')$ is a maximal transvectal punctured subgroup of $SL(m, q)$ such that $T'(P') \neq T'(Q')$ for all $Q' \neq P'$ in $\mathcal{P}'(V)$, and $T'(P') \neq T(P)$ for all P in $\mathcal{P}(V)$; and for every maximal transvectal punctured subgroup S of $SL(m, q)$ we have either $S = T(P)$ for some $P \in \mathcal{P}(V)$ or $S = T'(P')$ for some $P' \in \mathcal{P}'(V)$. Likewise, if $m = 2$, then for every $P^* \in \mathcal{P}^*(V)$, the set $T^*(P^*)$ is a maximal transvectal punctured subgroup of $SL(m, q)$ such that $T^*(P^*) \neq T^*(Q^*)$ for all $Q^* \neq P^*$ in $\mathcal{P}^*(V)$; and for every maximal transvectal punctured subgroup S of $SL(m, q)$ we have $S = T^*(P^*)$ for some $P^* \in \mathcal{P}^*(V)$.]

In Lemma (5.10) we shall characterize the groups $T^*(P^*) \cup \{1\}$ as centers of *quotient stabilizers of complete flags*. Recall that a complete flag in V is a sequence $\Phi = (\Phi_1, \ldots, \Phi_{m-1})$ where Φ_i is an i-dimensional subspace of V for $1 \leq i \leq m-1$ such that $\Phi_i \subset \Phi_{i+1}$ for $1 \leq i \leq m-2$. *Let $\mathcal{P}^{**}(V)$ denote the set of all complete flags in V.* Recall that the stabilizer of Φ in $\mathrm{GL}(V) = \mathrm{GL}(m, q)$ is the subgroup $\mathrm{stab}(\Phi)$ of $\mathrm{GL}(V)$ defined by $\mathrm{stab}(\Phi) = \bigcap_{1 \leq i \leq m-1} \{g \in \mathrm{GL}(V) : g(v) \in \Phi_i \text{ for all } v \in \Phi_i\}$; *as notation we put $\Lambda(\Phi) = \mathrm{stab}(\Phi)$.* Let $\Phi_0 = \{0\}$ and $\Phi_m = V$. Then, for $1 \leq i \leq m$, there is an obvious homomorphism $\Lambda(\Phi) \to \mathrm{GL}(\Phi_i/\Phi_{i-1})$ and hence $\Lambda(\Phi)$ acts on Φ_i/Φ_{i-1}. Now by definition, the elementwise stabilizer of $(\Phi_1/\Phi_0, \ldots, \Phi_m/\Phi_{m-1})$ in $\Lambda(\Phi)$ is the subgroup $\mathrm{estab}(\Phi_1/\Phi_0, \ldots, \Phi_m/\Phi_{m-1})$ of $\Lambda(\Phi)$ defined by $\mathrm{estab}(\Phi_1/\Phi_0, \ldots, \Phi_m/\Phi_{m-1}) = \bigcap_{1 \leq i \leq m} \{g \in \Lambda(\Phi) : g(v) = v \text{ for all } v \in \Phi_i/\Phi_{i-1}\}$; *as notation we put $\Delta(\Phi) = \mathrm{estab}(\Phi_1/\Phi_0, \ldots, \Phi_m/\Phi_{m-1})$ and we call this the "quotient stabilizer" of Φ.* For any $H < \mathrm{GL}(m, q)$, *we let $\Psi(H)$ denote the set of all subspaces U of V with $\{0\} \neq U \neq V$ such that for all $h \in H$ we have $h(U) = U$.* Finally, by k^* we denote the multiplicative group of all the nonzero elements of k. For a matrix treatment of Lemma (5.10) and its proof see Remark (5.18).

Lemma (5.10). *For any $\Phi = (\Phi_1, \ldots, \Phi_{m-1}) \in \mathcal{P}^{**}(V)$, we have the following:*

(5.10.1) $\Delta(\Phi) < SL(m, q)$ and $\Delta(\Phi) < \Theta^{-1}(\Theta(\Delta(\Phi))) < \Lambda(\Phi) < GL(m, q)$.

(5.10.2) For any H with $\Delta(\Phi) < H < \Lambda(\Phi)$, we have $\Psi(H) = \{\Phi_1, \ldots, \Phi_{m-1}\}$.

(5.10.3) Upon letting $P^* = (P, P') \in \mathcal{P}^*(V)$ with $P = \Phi_1$ and $P' = \Phi_{m-1}$, we have $Z(\Delta(\Phi)) = T^*(P^*) \cup \{1\}$.

(5.10.4) There exists a basis $(v_1, \ldots, v_m)$ of V such that $\Phi_i = kv_1 + \cdots + kv_i$ for $1 \leq i \leq m-1$, and any such basis gives rise to bijections $(k^+)^{m(m-1)/2} \to \Delta(\Phi)$ and $(k^*)^m \times (k^+)^{m(m-1)/2} \to \Lambda(\Phi)$ (which are not claimed to be homomorphisms) in the following manner. For any $\beta = (\beta_{ij}) \in (k^+)^{m(m-1)/2}$, with $\beta_{ij} \in k$ for $1 \leq i < j \leq m$, we have a unique k-linear map $\rho(\beta) : V \to V$ such that $\rho(\beta)(v_j) = v_j + \sum_{1 \leq i \leq j-1} \beta_{ij} v_i$ for $1 \leq j \leq m$. Moreover, $\beta \mapsto \rho(\beta)$ gives the said bijection $(k^+)^{m(m-1)/2} \to \Delta(\Phi)$. Likewise, for any $\alpha = (\alpha_{ij}) \in (k^*)^m \times (k^+)^{m(m-1)/2}$, with $\alpha_{ii} \in k^*$ for $1 \leq i \leq m$ and $\alpha_{ij} \in k$ for $1 \leq i < j \leq m$, we have a unique k-linear map $\rho'(\alpha) : V \to V$ such that $\rho'(\alpha)(v_j) = \sum_{1 \leq i \leq j} \alpha_{ij} v_i$ for $1 \leq j \leq m$. Moreover, $\alpha \mapsto \rho'(\beta)$ gives the said bijection $(k^*)^m \times (k^+)^{m(m-1)/2} \to \Lambda(\Phi) < GL(m, q)$.

Namely, given any $\Phi = (\Phi_1, \ldots, \Phi_{m-1}) \in \mathcal{P}^{**}(V)$, we can take a basis $(v_1, \ldots, v_m)$ of V such that $\Phi_i = kv_1 + \cdots + kv_i$ for $1 \leq i \leq m-1$. For any $\beta = (\beta_{ij}) \in$

$(k^+)^{m(m-1)/2}$, with $\beta_{ij} \in k$ for $1 \leq i < j \leq m$, we have a unique k-linear map $\rho(\beta) : V \to V$ such that $\rho(\beta)(v_j) = v_j + \sum_{1 \leq i \leq j-1} \beta_{ij} v_i$ for $1 \leq j \leq m$. Clearly $\beta \mapsto \rho(\beta)$ gives a bijection $(k^+)^{m(m-1)/2} \to \Delta(\Phi)$, and for every $\beta \in (k^+)^{m(m-1)/2}$ we have $\rho(\beta) \in \mathrm{SL}(m,q)$, and hence $\Delta(\Phi) < \mathrm{SL}(m,q)$. For $1 \leq i < j \leq m$ and $\mu \in k^+$, we have a unique k-linear map $\gamma(i,j,\mu) : V \to V$ such that $\gamma(i,j,\mu)(v_j) = \mu v_i + v_j$ and $\gamma(i,j,\mu)(v_{j'}) = v_{j'}$ for all j' in $\{1, \ldots, j-1, j+1, \ldots, m\}$. Now, for $1 \leq i < j \leq m$ and $\mu \in k^+$, we clearly have $\gamma(i,j,\mu) \in \Delta(\Phi)$. Moreover, upon letting $P^* = (P, P') \in \mathcal{P}^*(V)$ with $P = \Phi_1$ and $P' = \Phi_{m-1}$, by (5.6.3) we see that $\mu \mapsto \gamma(1,m,\mu)$ gives a bijection $k^+ \to T^*(P^*)$. Given any $\mu \in k^+$, by direct calculation we see that for every $\beta \in (k^+)^{m(m-1)/2}$ we have $\gamma(1,m,\mu)(\rho(\beta)(v)) = \rho(\beta)(\gamma(1,m,\mu)(v))$ for all $v \in V$ and hence $\gamma(1,m,\mu) \in Z(\Delta(\Phi))$. Moreover, if $\beta \in (k^+)^{m(m-1)/2}$ is such that $\rho(\beta) \neq \gamma(1,m,\mu)$ for every $\mu \in k^+$, then either $\beta_{1j} \neq 0$ for some j with $1 < j < m$, or $\beta_{ij} \neq 0$ for some (i,j) with $1 < i < j \leq m$; in the first case we get $\gamma(j,m,1)(\rho(\beta)(v_m)) = \beta_{1m} v_1 + v_j + v_m + \sum_{2 \leq i \leq m-1} \beta_{im} v_i \neq (\beta_{1j} + \beta_{1m}) v_1 + v_j + v_m + \sum_{2 \leq i \leq j-1} \beta_{ij} v_i + \sum_{2 \leq i \leq m-1} \beta_{im} v_i = \rho(\beta)(\gamma(j,m,1)(v_m))$, and in the second case we get $\gamma(1,i,1)(\rho(\beta)(v_j)) = \beta_{ij} v_1 + v_j + \sum_{2 \leq i' \leq j-1} \beta_{i'j} v_{i'} \neq v_j + \sum_{2 \leq i' \leq j-1} \beta_{i'j} v_{i'} = \rho(\beta)(\gamma(1,i,1)(v_j))$. Therefore $Z(\Delta(\Phi)) = T^*(P^*) \cup \{1\}$. Enlarging the above definition of ρ, for any $\alpha = (\alpha_{ij}) \in (k^*)^m \times (k^+)^{m(m-1)/2}$, with $\alpha_{ii} \in k^*$ for $1 \leq i \leq m$ and $\alpha_{ij} \in k$ for $1 \leq i < j \leq m$, we have a unique k-linear map $\rho'(\alpha) : V \to V$ such that $\rho'(\alpha)(v_j) = \sum_{1 \leq i \leq j} \alpha_{ij} v_i$ for $1 \leq j \leq m$. Clearly $\alpha \mapsto \rho'(\beta)$ gives a bijection $(k^*)^m \times (k^+)^{m(m-1)/2} \to \Lambda(\Phi) < \mathrm{GL}(m,q)$. Also clearly we have $\Psi(\Delta(\Phi)) = \{\Phi_1, \ldots, \Phi_{m-1}\}$ and $\Psi(\Lambda(\Phi)) = \{\Phi_1, \ldots, \Phi_{m-1}\}$, and hence for any H with $\Delta(\Phi) < H < \Lambda(\Phi)$ we have $\Psi(H) = \{\Phi_1, \ldots, \Phi_{m-1}\}$. This completes the proof of (5.10).

We shall now prove the following projective version of Lemma (5.5).

Lemma (5.11). *We have the following:*

(5.11.1) For any $1 \neq \mu \in k$ and $t \in T \cup \{1\}$ we have $\ker(\mu t - 1) = 0$.

(5.11.2) If $m > 2$ and $P_i^* = (P_i, P_i') \in \mathcal{P}^*(V)$ and $\tau_i \in \widehat{T}^*(P_i^*)$ for $1 \leq i \leq 2$ are such that $\tau_1 \tau_2 \in \widehat{T} \cup \{1\}$, then either $P_1 = P_2$ or $P_1' = P_2'$.

(5.11.3) If $m = 2 = p$ and $P_i^* = (P_i, P_i') \in \mathcal{P}^*(V)$ and $\tau_i \in \widehat{T}^*(P_i^*)$ for $1 \leq i \leq 2$ are such that $\tau_1 \tau_2 \in \widehat{T} \cup \{1\}$, then $P_1 = P_2$ and $P_1' = P_2'$.

(5.11.4) If $P_i^* = (P_i, P_i') \in \mathcal{P}^*(V)$ and $\tau_i \in \widehat{T}^*(P_i^*)$ for $1 \leq i \leq 2$ are such that $\tau_1 \tau_2 \in \widehat{T} \cup \{1\}$ and $\tau_1 \tau_2^2 \in \widehat{T} \cup \{1\}$, then either $P_1 = P_2$ or $P_1' = P_2'$.

To prove (5.11.1), let there be given any $1 \neq \mu \in k$ and $t \in T \cup \{1\}$. Then $\mathrm{Im}(t-1) \subset \ker(t-1)$, and hence: (i) for all $v \in V$ we have $(t-1)((t-1)(v)) = 0$, and therefore: (ii) for all $v \in V$ we have $(t-1)(t(v)) = (t-1)(v)$. And obviously: (iii) for all $v \in V$ we have $(\mu t - 1)(v) - (t-1)(v) = (\mu - 1)(t(v))$. Now $v \in \ker(\mu t - 1) \cap \ker(t-1) \Rightarrow$ (obviously) $(\mu t - 1)(v) - (t-1)(v) = 0 \Rightarrow$ (by (iii)) $(\mu - 1)(t(v)) = 0 \Rightarrow$ (0bviously) $t(v) = 0 \Rightarrow$ (0bviously) $v = 0$, and hence: (iv) $v \in \ker(\mu t - 1) \cap \ker(t-1) \Rightarrow v = 0$. Moreover, $v \in \ker(\mu t - 1) \Rightarrow$ (by (i)) $(t-1)((\mu t - 1)(v) - (t-1)(v)) = 0 \Rightarrow$ (by (iii)) $(t-1)((\mu - 1)t(v)) = 0 \Rightarrow$ (obviously) $(t-1)(t(v)) = 0 \Rightarrow$ (by (ii)) $(t-1)(v) = 0$, and hence by (iv) we see that $v \in \ker(\mu t - 1) \Rightarrow v = 0$ which completes the proof of (5.11.1).

To prove (5.11.2)–(5.11.4), let there be given any $P_i^* = (P_i, P_i') \in \mathcal{P}^*(V)$ and $t_i \in T^*(P_i^*)$ for $1 \leq i \leq 2$ such that $t_1 t_2 = \nu t$ for some $0 \neq \nu \in k$ and $t \in T \cup \{1\}$. Let $P^\flat = P_1' \cap P_2'$. Then $P^\flat$ is a subspace of V with $\dim P^\flat \geq m - 2$, and clearly

$\ker(\nu t-1)=\ker(t_1t_2-1)\subset P^\flat$. $P^\flat\subset\ker(t_1t_2-1)=\ker(\nu t-1)$. Therefore by (5.11.1) we see that if $m>2$, then $\nu=1$, and hence (5.11.2) follows from (5.5). Also clearly $\nu^m=1$, and hence if $m=2=p$, then $\nu=1$, whereas if $m=2\neq p$, then $\nu=\pm1$. Therefore (5.11.3) also follows from (5.5).

Henceforth assume that $m=2\neq p$ and $t_1t_2^2=\nu^*t^*$ for some $0\neq\nu^*\in k$ and $t^*\in T\cup\{1\}$. We shall show that then $P_1'=P_2'$ and, in view of (5.11.2) and (5.11.3), this will complete the proof of (5.11.4). Suppose, if possible, that $P_1'\neq P_2'$. Then, in view of what we have said above, by (5.5) and (5.7) we must have $\nu=-1=\nu^*$. We can take a basis (u_1,u_2) of V such that $t_1(u_1)=u_1$, $t_1(u_2)=u_2+u_1$, $t_2(u_2)=u_2$, and $t_2(u_1)=u_1+\lambda u_2$ for some $0\neq\lambda\in k$. Since $t\in T\cup\{1\}$, we have $t(v)=v$ for all v in some 1-dimensional subspace of V. Since $t=-t_1t_2$, we get $t(u_2)=-u_1-u_2$. Therefore $t(u_1+\kappa u_2)=u_1+\kappa u_2$ for some $\kappa\in k$. Since $t=-t_1t_2$, we get $t(u_1+\kappa u_2)=-(1+\lambda+\kappa)u_1-(\lambda+\kappa)u_2$. Therefore $-(1+\lambda+\kappa)=1$ and $-(\lambda+\kappa)=\kappa$. Hence $\kappa=2$ and $\lambda=-4$. Now clearly $t_2^2(u_2)=u_2$ and $t_2^2(u_1)=u_1+\lambda^*$ with $\lambda^*=2\lambda$; also $t^*=-t_1t_2^2\in T\cup\{1\}$, therefore by taking (t_2^2,t^*,λ^*) for (t_2,t,λ) in the above argument we get $\lambda^*=-4$. This is a contradiction because $\lambda^*=2\lambda=-8$ and $p\neq2$. This completes the proof of (5.11.4).[6]

By Lemmas (5.2) and (5.7) we get the following:

Lemma (5.12). *For any $P\in\mathcal{P}(V)$ we have $(k^+)^{m-1}\approx\widehat{T}(P)\cup\{1\}<PSL(m,q)$ and Θ induces an isomorphism $T(P)\cup\{1\}\to\widehat{T}(P)\cup\{1\}$. For any $P'\in\mathcal{P}'(V)$ we have $(k^+)^{m-1}\approx\widehat{T}'(P')\cup\{1\}<PSL(m,q)$ and Θ induces an isomorphism $T'(P')\cup\{1\}\to\widehat{T}'(P')\cup\{1\}$. For any $P^*\in\mathcal{P}^*(V)$ we have $k^+\approx\widehat{T}^*(P^*)\cup\{1\}<PSL(m,q)$ and Θ induces an isomorphism $T^*(P^*)\cup\{1\}\to\widehat{T}^*(P^*)\cup\{1\}$.*

[Thus, in particular, $\widehat{T}(P)$, $\widehat{T}'(P')$, and $\widehat{T}^*(P^*)$ are projective transvectal punctured subgroups of $PSL(m,q)$, where by "projective transvectal" we mean consisting only of projective transvections.]

By Lemmas (5.3) and (5.12) we get the following:

Lemma (5.13). *The map $\widehat{X}:\widehat{T}\to\mathcal{P}(V)$ is surjective and the set $\widehat{T}$ can be expressed as the union $\widehat{T}=\coprod_{P\in\mathcal{P}(V)}\widehat{T}(P)$ of pairwise disjoint nonempty subsets. The map $\widehat{X}':\widehat{T}\to\mathcal{P}'(V)$ is surjective and the set $\widehat{T}$ can be expressed as the union $\widehat{T}=\coprod_{P'\in\mathcal{P}'(V)}\widehat{T}'(P')$ of pairwise disjoint nonempty subsets. The map $\widehat{X}^*:\widehat{T}\to\mathcal{P}^*(V)$ is surjective and the set $\widehat{T}$ can be expressed as the union $\widehat{T}=\coprod_{P^*\in\mathcal{P}^*(V)}\widehat{T}^*(P^*)$ of pairwise disjoint nonempty subsets.*

Let us note that a *maximal projective transvectal punctured subgroup* of $\mathrm{PSL}(m,q)$ is a nonempty subset $\widehat{S}$ of $\widehat{T}$ such that $\widehat{S}\cup\{1\}<\mathrm{PSL}(m,q)$ and such that there is no subset $\widehat{S}'$ of $\widehat{T}$ other than $\widehat{S}$ for which $\widehat{S}\subset\widehat{S}'$ and $\widehat{S}'\cup\{1\}<\mathrm{PSL}(m,q)$. Now by (5.11.4) we see that $\widehat{S}\subset\widehat{T}$ with $\widehat{S}\cup\{1\}<\mathrm{PSL}(m,q)\Rightarrow$ either $\widehat{S}\subset\widehat{T}(P)$ for

[6]The above proof also shows that, in case of $m=2\neq p$, the conclusion of (5.11.4) does not hold if we drop the assumption that $\tau_1\tau_2^2\in\widehat{T}\cup\{1\}$. More explicitly, let (u_1,u_2) be a basis of V, and let $P_1^*=(P_1,P_1')$, $P_2^*=(P_2,P_2')$, and $P^*=(P,P')$ in $\mathcal{P}^*(V)$ be given by $P_1'=P_1=u_1k$, $P_2'=P_2=u_2k$, and $P'=P=(u_1-2u_2)k$. Then $P_1\neq P_2$ and $P_1'\neq P_2'$. Let t_1, t_2, and t in $\mathrm{GL}(2,q)$ be given by $t_1(u_1)=u_1$, $t_1(u_2)=u_2+u_1$, $t_2(u_2)=u_2$, $t_2(u_1)=u_1-4u_2$, $t(u_1+2u_2)=u_1+2u_2$, and $t(u_2)=-u_1-u_2$. Then $t_1\in T^*(P*_1)$, $t_2\in T^*(P*_2)$, $t\in T^*(P^*)$, but $t_1t_2=-t$.

some $P \in \mathcal{P}(V)$ or $\widehat{S} \subset \widehat{T}'(P')$ for some $P' \in \mathcal{P}'(V)$. Moreover, if $m > 2$, then for all $P \in \mathcal{P}(V)$ and $P' \in \mathcal{P}'(V)$ we clearly have $\widehat{T}(P) \not\subset \widehat{T}'(P') \not\subset \widehat{T}(P)$ [say because every $P' \in \mathcal{P}'(V)$ contains some $P_1 \neq P_2$ in $\mathcal{P}(V)$, every $P \in \mathcal{P}(V)$ passes through some $P'_1 \neq P'_2$ in $\mathcal{P}'(V)$, and for every $P^* = (P, P') \in \mathcal{P}^*(V)$ we have $\widehat{T}^*(P^*) = \widehat{T}(P) \cap \widehat{T}'(P')$]. Likewise, if $m = 2$, then for every $P^* = (P, P') \in \mathcal{P}^*(V)$ we clearly have $P = P'$ and $\widehat{T}(P) = \widehat{T}'(P') = \widehat{T}^*(P^*)$. Therefore by (5.3) and (5.12) we get the following:

Lemma (5.14). *If $m > 2$, then the two families $\widehat{T}(P)_{P \in \mathcal{P}(V)}$ and $\widehat{T}'(P')_{P' \in \mathcal{P}'(V)}$ give us exactly all the distinct maximal projective transvectal punctured subgroups of $PSL(m, q)$. If $m = 2$, then the family $\widehat{T}^*(P^*)_{P^* \in \mathcal{P}^*(V)}$ gives us exactly all the distinct maximal projective transvectal punctured subgroups of $PSL(m, q)$.*

[In other words, if $m > 2$, then for every $P \in \mathcal{P}(V)$, the set $\widehat{T}(P)$ is a maximal projective transvectal punctured subgroup of $PSL(m, q)$ such that $\widehat{T}(P) \neq \widehat{T}(Q)$ for all $Q \neq P$ in $\mathcal{P}(V)$, and $\widehat{T}(P) \neq \widehat{T}'(P')$ for all P' in $\mathcal{P}'(V)$; for every $P' \in \mathcal{P}'(V)$, the set $\widehat{T}'(P')$ is a maximal projective transvectal punctured subgroup of $PSL(m, q)$ such that $\widehat{T}'(P') \neq \widehat{T}'(Q')$ for all $Q' \neq P'$ in $\mathcal{P}'(V)$, and $\widehat{T}'(P') \neq \widehat{T}(P)$ for all P in $\mathcal{P}(V)$; and for every maximal projective transvectal punctured subgroup $\widehat{S}$ of $PSL(m, q)$ we have either $\widehat{S} = \widehat{T}(P)$ for some $P \in \mathcal{P}(V)$ or $\widehat{S} = \widehat{T}'(P')$ for some $P' \in \mathcal{P}'(V)$. Likewise, if $m = 2$, then for every $P^* \in \mathcal{P}^*(V)$, the set $\widehat{T}^*(P^*)$ is a maximal projective transvectal punctured subgroup of $PSL(m, q)$ such that $\widehat{T}^*(P^*) \neq \widehat{T}^*(Q^*)$ for all $Q^* \neq P^*$ in $\mathcal{P}^*(V)$; and for every maximal projective transvectal punctured subgroup $\widehat{S}$ of $PSL(m, q)$ we have $\widehat{S} = \widehat{T}^*(P^*)$ for some $P^* \in \mathcal{P}^*(V)$.]

For any complete flag $\Phi = (\Phi_1, \ldots, \Phi_{m-1})$ in V, *let* $\widehat{\Delta}(\Phi) = \Theta(\Delta(\Phi))$ *and let us call* $\widehat{\Delta}(\Phi)$ *the projective quotient stabilizer of* Φ. Now as noted in (5.10), $\beta \mapsto \rho(\beta)$ gives a bijection $(k^+)^{m(m-1)/2} \to \Delta(\Phi)$. Moreover, with the notation of (5.10), for any $\beta \in (k^+)^{m(m-1)/2}$ we clearly have $\Theta(\rho(\beta)) = 1 \Leftrightarrow \rho(\beta)(v_i) = \lambda v_i$ for $1 \leq i \leq m$ and some $0 \neq \lambda \in k \Leftrightarrow \rho(\beta)(v_i) = v_i$ for $1 \leq i \leq m \Leftrightarrow \rho(\beta) = 1$. Therefore by (5.10) and (5.12) we get the following:

Lemma (5.15). *For any $\Phi = (\Phi_1, \ldots, \Phi_{m-1}) \in \mathcal{P}^{**}(V)$, we have the following:*

(5.15.1) $\widehat{\Delta}(\Phi) < PSL(m, q)$ and $\Delta(\Phi) < \Theta^{-1}(\widehat{\Delta}(\Phi)) < \Lambda(\Phi) < GL(m, q)$.

(5.15.2) For any H with $\Delta(\Phi) < H < \Lambda(\Phi)$, we have $\Psi(H) = \{\Phi_1, \ldots, \Phi_{m-1}\}$.

(5.15.3) Upon letting $P^* = (P, P') \in \mathcal{P}^*(V)$ with $P = \Phi_1$ and $P' = \Phi_{m-1}$, we have $Z(\widehat{\Delta}(\Phi)) = \widehat{T}^*(P^*) \cup \{1\}$, and Θ induces isomorphisms $\Delta(\Phi) \to \widehat{\Delta}(\Phi)$ and $Z(\Delta(\Phi)) \to Z(\widehat{\Delta}(\Phi))$.

(5.15.4) In the notation of (5.10), $\beta \mapsto \rho(\beta)$ gives a bijection $(k^+)^{m(m-1)/2} \to \widehat{\Delta}(\Phi)$ (which is not claimed to be a homomorphism).

[Note that $\Phi \mapsto P^*$ gives a surjection $\mathcal{P}^{**}(V) \to \mathcal{P}^*(V)$ of the set of all complete flags in V onto the set of all short flags in V, where by a "short flag" in V we mean a member of $\mathcal{P}^*(V)$; the said surjection sends a complete flag to the short flag "dominated by it" in the obvious sense. This surjection is equally relevant in connection with Lemma (5.10).]

Remark (5.16). Observe that whatever we have said in this section up to this point is valid for an arbitrary field k. Now for the first time we are going to use the fact that k is the finite field $\mathrm{GF}(q)$ and hence $\mathrm{GL}(V) = \mathrm{GL}(m, q)$ is a finite group. Note

that then, for every positive integer n, the group $(k^+)^n$ is an elementary abelian p-group of order q^n (cf. page 159 of [Suz]). In particular, for all $P \in \mathcal{P}(V)$ and $P' \in \mathcal{P}'(V)$, by Lemmas (5.7) and (5.12) we see that $T(P)\cup\{1\}$, $\widehat{T}(P)\cup\{1\}$, $T'(P')\cup\{1\}$, and $\widehat{T}'(P')\cup\{1\}$ are elementary abelian p-groups of order q^{m-1}, and likewise, for all $P^* \in \mathcal{P}^*(V)$, by Lemmas (5.7) and (5.12) we see that $T^*(P^*)\cup\{1\}$ and $\widehat{T}^*(P^*)\cup\{1\}$ are elementary abelian p-groups of order q. Since $\ker\Theta = Z(\mathrm{GL}(m,q))$ and the order of $\ker\Theta$ is prime to p, it follows that Θ induces an order preserving bijection of the set of all p-power-order elements in any subgroup G of $\mathrm{GL}(m,q)$ onto the set of all p-power-order elements in $\Theta(G)$, and likewise Θ induces a bijection of the set of all p-power-order subgroups of G onto the set of all p-power-order subgroups of $\Theta(G)$, and moreover, for any p-power-order subgroup H of G, the map $H \to \Theta(H)$ induced by Θ is an isomorphism. This reproves Lemma (5.2) as well as the claim about Θ made in Lemma (5.15).

Recall that the set of all p-Sylow subgroups of a finite group H is denoted by $\mathrm{Syl}_p(H)$. As a consequence of Lemmas (5.7) to (5.15) we shall now prove Lemma (5.17) below, whose parts (5.17.7) and (5.17.8) subsume the **Invariance Lemma (1.4)** stated in the Introduction.

Lemma (5.17). *For any group G with $SL(m,q) < G < GL(m,q)$ we have the following:*

(5.17.1) $\Phi \mapsto \Delta(\Phi)$ gives a bijection $\mathcal{P}^{**}(V) \to Syl_p(G)$.

(5.17.2) $\Phi \mapsto \widehat{\Delta}(\Phi)$ gives a bijection $\mathcal{P}^{**}(V) \to Syl_p(\Theta(G))$.

(5.17.3) $T = \bigcup_{A\in Syl_p(G)}(Z(A)\setminus\{1\}) =$ a set of elements of order p.

(5.17.4) $\widehat{T} = \bigcup_{A\in Syl_p(\Theta(G))}(Z(A)\setminus\{1\}) =$ a set of elements of order p.

(5.17.5) If $m = 2$, then $\mathcal{P}'(V) = \mathcal{P}(V)$, and for every $P \in \mathcal{P}(V)$ we have $T'(P) = T(P)$ and $k^+ \approx T(P)\cup\{1\} \in Syl_p(G)$, and moreover $P \mapsto T(P)\cup\{1\}$ gives a bijection $\mathcal{P}(V) \to Syl_p(G)$, and the set T can be expressed as the union $T = \coprod_{P\in\mathcal{P}(V)} T(P)$ of pairwise disjoint nonempty subsets.

(5.17.6) If $m = 2$, then $\mathcal{P}'(V) = \mathcal{P}(V)$, and for every $P \in \mathcal{P}(V)$ we have $\widehat{T}'(P) = \widehat{T}(P)$ and $k^+ \approx \widehat{T}(P)\cup\{1\} \in Syl_p(\Theta(G))$, and moreover $P \mapsto \widehat{T}(P)\cup\{1\}$ gives a bijection $\mathcal{P}(V) \to Syl_p(\Theta(G))$, and the set $\widehat{T}$ can be expressed as the union $\widehat{T} = \coprod_{P\in\mathcal{P}(V)} T(P)$ of pairwise disjoint nonempty subsets.

(5.17.7) Every automorphism of G maps T onto itself.

(5.17.8) Every automorphism of $\Theta(G)$ maps $\widehat{T}$ onto itself.

Namely, since $q^{m(m-1)/2}$ is the highest power of p which divides $|\mathrm{SL}(m,q)|$ (cf. page 81 of [Suz]), and since $|G|/|\mathrm{SL}(m,q)|$ as well as $|G|/|\Theta(G)|$ are prime to p, by (5.10) and (5.15) we respectively see that $\Phi \mapsto \Delta(\Phi)$ and $\Phi \mapsto \widehat{\Delta}(\Phi)$ give injective maps $\mathcal{P}^{**}(V) \to \mathrm{Syl}_p(G)$ and $\mathcal{P}^{**}(V) \to \mathrm{Syl}_p(\Theta(G))$. By Sylow's Theorem, $\mathrm{Syl}_p(G)$ is a complete set of G-conjugates, and $\mathrm{Syl}_p(\Theta(G))$ is a complete set of $\Theta(G)$-conjugates. Moreover, for any $g \in G$ and any $\Phi \in \mathcal{P}^{**}(V)$, we clearly have $g(\Phi) \in \mathcal{P}^{**}(V)$ and $\Delta(g(\Phi)) = g\Delta(\Phi)g^{-1}$ and $\widehat{\Delta}(g(\Phi)) = \Theta(g)\widehat{\Delta}(\Phi)\Theta(g)^{-1}$. Therefore the above maps $\mathcal{P}^{**}(V) \to \mathrm{Syl}_p(G)$ and $\mathcal{P}^{**}(V) \to \mathrm{Syl}_p(\Theta(G))$ are surjective. This proves (5.17.1) and (5.17.2). By (5.7), (5.8), (5.9), (5.10) and (5.17.1) we get (5.17.3) and (5.17.5), and by (5.12), (5.13), (5.14), (5.15) and (5.17.2) we get (5.17.4) and (5.17.6). Finally, assertions (5.17.7) and (5.17.8) follow from (5.17.3) and (5.17.4) respectively; in the case of $m = 2$ these assertions also follow from (5.17.5) and (5.17.6) respectively.

Remark (5.18). To see how some of the material of this section, say Lemmas (5.7), (5.10), and (5.17), would look in the language of matrices, in this remark, let us think of V as consisting of column vectors and $\mathrm{GL}(m,q)$ as a subset of the set of all $m \times m$ matrices $a = (a_{ij})$ over k which act on the column vectors by left multiplication.

For $1 \le i \le m$ let $C_i \subset \mathrm{SL}(m,q)$ be defined as the set of all $m \times m$ matrices a over k such that $a_{i'j'} = 0$ for all $i' \ne j'$ in $\{1,2,\dots,m\}$ with $i' \ne i$, and $a_{i'i'} = 1$ for $1 \le i' \le m$. By multiplying matrices we see that for any a and a' in C_i we have $aa' \in C_i$ with $(aa')_{ij} = a_{ij} + a'_{ij}$ for all j in $\{1,\dots,i-1,i+1,\dots,m\}$. Since the elements in the i-th row of a member of C_i can be chosen arbitrarily except for the i-th column, it follows that $(k^+)^{m-1} \approx C_i < \mathrm{SL}(m,q)$.

For $1 \le j \le m$ let $C'_j \subset \mathrm{SL}(m,q)$ be defined as the set of all $m \times m$ matrices a over k such that $a_{i'j'} = 0$ for all $i' \ne j'$ in $\{1,2,\dots,m\}$ with $j' \ne j$, and $a_{j'j'} = 1$ for $1 \le j' \le m$. By multiplying matrices we see that for any a and a' in C'_j we have $aa' \in C'_j$ with $(aa')_{ij} = a_{ij} + a'_{ij}$ for all i in $\{1,\dots,j-1,j+1,\dots,m\}$. Since the elements in the j-th column of a member of C'_j can be chosen arbitrarily except for the j-th row, it follows that $(k^+)^{m-1} \approx C'_j < \mathrm{SL}(m,q)$.

For $i \ne j$ in $\{1,2,\dots,m\}$ and $\mu \in k$, let $c(i,j,\mu) \in \mathrm{SL}(m,q)$ be given by $c(i,j,\mu)_{ij} = \mu$ and $c(i,j,\mu)_{i'i'} = 1$ for $1 \le i' \le m$ and $c(i,j,\mu)_{i'j'} = 0$ for all $i' \ne j'$ in $\{1,2,\dots,m\}$ with $(i',j') \ne (i,j)$. For $i \ne j$ in $\{1,2,\dots,m\}$, let $C^*_{ij} = \{c(i,j,\mu) : \mu \in k\}$. By multiplying matrices we see that for $i \ne j$ in $\{1,2,\dots,m\}$ we have $c(i,j,\mu)c(i,j,\nu) = c(i,j,\mu+\nu)$ for all $\mu \in k$ and $\nu \in k$. Therefore $k^+ \approx C^*_{ij} < \mathrm{SL}(m,q)$.

For $1 \le j \le m$, let $e_j \in V$ be the column vector with 1 in the j-th place and zeroes elsewhere, and let $Q'_j \in \mathcal{P}'(V)$ consist of those column vectors whose j-th component is zero, i.e., Q'_j is generated by $e_1,\dots,e_{j-1},e_{j+1},\dots,e_m$. For $1 \le i \le m$, let $Q_i \in \mathcal{P}(V)$ consist of those column vectors whose j-th component is zero for all $j \ne i$, i.e., Q_i consists of all the multiples of e_i. For $i \ne j$ in $\{1,2,\dots,m\}$, let $Q^*_{ij} = (Q_i, Q'_j) \in \mathcal{P}^*(V)$.

Let a be an $m \times m$ matrix over k. Then for $1 \le j \le m$ we have $ae_j =$ the j-th column of a. Consequently, for any fixed j in $\{1,2,\dots,m\}$ we have $av - v = 0$ for all $v \in Q'_j \Leftrightarrow ae_{j'} - e_{j'} = 0$ for all j' in $\{1,\dots,j-1,j+1,\dots,m\} \Leftrightarrow a_{i'j'} = 0$ for all $i' \ne j'$ in $\{1,2,\dots,m\}$ with $j' \ne j$ and $a_{j'j'} = 1$ for all j' in $\{1,\dots,j-1,j+1,\dots,m\}$, and hence $C'_j = T'(Q'_j) \cup \{1\}$. Likewise, for any fixed i in $\{1,2,\dots,m\}$ we have $av - v \in Q_i$ for all $v \in V \Leftrightarrow ae_j - e_j \in ke_i$ for all j in $\{1,2,\dots,m\} \Leftrightarrow a_{i'j'} = 0$ for all $i' \ne j'$ in $\{1,2,\dots,m\}$ with $i' \ne i$ and $a_{i'i'} = 1$ for all i' in $\{1,\dots,i-1,i+1,\dots,m\}$, and hence in view of (5.6.1) we get $C_i = T(Q_i) \cup \{1\}$. Finally, for any fixed $i \ne j$ in $\{1,2,\dots,m\}$ we have $C^*_{ij} = C_i \cap C'_j$ and $T^*(Q^*_{ij}) = T(Q_i) \cap T'(Q'_j)$, and hence $C^*_{ij} = T^*(Q^*_{ij}) \cup \{1\}$.

Let B be the set of all uni-upper-triangulars in $\mathrm{SL}(m,q)$, i.e., the set of all $m \times m$ matrices $b = (b_{ij})$ over k such that $b_{ii} = 1$ for $1 \le i \le m$, and $b_{ij} = 0$ for $1 \le j < i \le m$. Then B is a subgroup of $\mathrm{SL}(m,q)$ and $|B| = q^{m(m-1)/2}$ which is the highest power of p which divides $|\mathrm{SL}(m,q)|$ (cf. page 81 of [Suz]). Therefore $B \in \mathrm{Syl}_p(\mathrm{SL}(m,q))$. Let $\overline{B}$ be the set of all upper-triangulars in $\mathrm{GL}(m,q)$, i.e., the set of all $m \times m$ matrices $\overline{b} = (\overline{b}_{ij})$ over k such that $\overline{b}_{ii} \ne 0$ for $1 \le i \le m$, and $\overline{b}_{ij} = 0$ for $1 \le j < i \le m$. Also let $\Phi = (\Phi_1,\dots,\Phi_{m-1}) \in \mathcal{P}^{**}(V)$ be the complete flag given by $\Phi_i = ke_1 + \cdots + ke_i$. Then clearly $\overline{B}$ is the stabilizer $\Lambda(\Phi)$ of Φ, and B is the quotient stabilizer $\Delta(\Phi)$ of Φ.

Now the matrices $c(i,j,\mu)$ represent elementary row and column operations in the sense that multiplying any $m \times m$ matrix over k from the left (resp. right) amounts to adding the μ-th multiple of the j-th row (resp. i-th column) to the i-th row (resp. j-th column). From this it follows that $c(1,m,\mu)b = bc(1,m,\mu)$ for all $\mu \in k$ and $b \in B$. Moreover, if $b \in B$ is such that $b \neq c(1,m,\mu)$ for all $\mu \in k$, then either $b_{1j} \neq 0$ for some j with $1 < j < m$, or $b_{1j} = 0$ for all j with $1 < j < m$ but $b_{ij} \neq 0$ for some (i,j) with $1 < i < j \leq m$; in the first case we get $(c(j,m,1)b)_{11} = b_{1m} \neq b_{1j} + b_{1m} = (bc(j,m,1))_{11}$, and in the second case we get $(c(1,i,1)b)_{11} = b_{ij} \neq 0 = (bc(1,i,1))_{11}$. Therefore $Z(B) = C^*_{1m}$.

Thus we have partially reproved Lemmas (5.7), (5.10), and (5.17.1).

6. Automorphism lemma

To prove the Automorphism Lemma (1.3) stated in the Introduction, let $k = \mathrm{GF}(q)$ and $V = k^m$. The Automorphism Lemma being trivial for $m = 1$, *again henceforth assume that* $m > 1$. Let the rest of the notation be also as in section 5.[7]

Definition (6.1). Recall that an ϵ-linear isomorphism of V onto an m-dimensional vector space $\overline{V}$ over a field $\overline{k}$, where $\epsilon : k \to \overline{k}$ is an isomorphism, is a bijective additive map $g : V \to \overline{V}$ such that for all $v \in V$ and $\mu \in k$ we have $g(\mu v) = \epsilon(\mu)g(v)$, and we note that then g *induces* bijections $\mathcal{P}(V) \to \mathcal{P}(\overline{V})$ and $\mathcal{P}'(V) \to \mathcal{P}'(\overline{V})$ and hence also a bijection $\mathcal{P}(V) \cup \mathcal{P}'(V) \to \mathcal{P}(\overline{V}) \cup \mathcal{P}'(\overline{V})$; by $\mathrm{Lin}_\epsilon(V,\overline{V})$ we denote the *set of all ϵ-linear isomorphisms* of V onto $\overline{V}$; if $\overline{k} = k$, then by $\mathrm{Sem}(V,\overline{V})$ we denote the set $\bigcup_{\epsilon \in \mathrm{Aut}(k)} \mathrm{Lin}_\epsilon(V,\overline{V})$, and, for any $g \in \mathrm{Sem}(V,\overline{V})$, by $\iota(g)$ we denote the unique $\epsilon \in \mathrm{Aut}(k)$ such that $g \in \mathrm{Lin}_\epsilon(V,\overline{V})$, i.e., $\iota(g)$ is the unique member of $\mathrm{Aut}(k)$ such that $g \in \mathrm{Lin}_{\iota(g)}(V,\overline{V})$; we call members of $\mathrm{Sem}(V,\overline{V})$ *k-semilinear isomorphisms* of V onto $\overline{V}$, and we call $\iota(g)$ the *autoassociate* of g. Recall that the group $\mathrm{Sem}(V,V)$, i.e., the *group of all semilinear maps* of V, is denoted by $\Gamma\mathrm{L}(V) = \Gamma\mathrm{L}(m,q)$. Since $\mathrm{GL}(V)$ is the kernel of the natural epimorphism $\Gamma\mathrm{L}(V) \to \mathrm{Aut}(k)$ which sends every $g \in \Gamma\mathrm{L}(V)$ to $\iota(g)$, we see that $\mathrm{GL}(V) \lhd \Gamma\mathrm{L}(V)$. Let $\mathrm{HL}(V) = \mathrm{HL}(m,q)$ be the *group of all homotheties,* i.e., maps $V \to V$ of the form $v \mapsto \mu v$ with $0 \neq \mu \in k$. Then $\mathrm{HL}(V) = Z(\mathrm{GL}(V))$, and hence $\mathrm{HL}(V)$ is a characteristic subgroup of $\mathrm{GL}(V)$, and therefore $\mathrm{HL}(V) \lhd \Gamma\mathrm{L}(V)$. Let $\mathrm{P}\Gamma\mathrm{L}(V) = \mathrm{P}\Gamma\mathrm{L}(m,q) = \Gamma\mathrm{L}(V)/\mathrm{HL}(V)$, and let $\Theta : \Gamma\mathrm{L}(V) \to \mathrm{P}\Gamma\mathrm{L}(V)$ be the canonical epimorphism; this should cause no confusion with the fact that until now Θ denoted the canonical epimorphism $\mathrm{GL}(V) \to \mathrm{PGL}(V)$; in other words, we identify $\mathrm{PGL}(V)$ with a subgroup of $\mathrm{P}\Gamma\mathrm{L}(V)$.

Let V' be the dual of V. Then $g \mapsto g^\natural$ gives an isomorphism $\mathrm{Sem}(V,V) \to \mathrm{Sem}(V',V')$ where for all $g \in \mathrm{Sem}(V,V)$ and $v \in V$ and $v' \in V'$ we have $g^\natural(v')(v) = \iota(g)(v'(g^{-1}(v)))$, and likewise $g \mapsto g^\natural$ gives a bijection $\mathrm{Sem}(V,V') \to \mathrm{Sem}(V',V)$ where for all $g \in \mathrm{Sem}(V,V')$ and $v' \in V'$ we have $g(v)(g^\natural(v')) = \iota(g)(v'(v))$.[8] Regarding V and V' as subspaces of $V \oplus V'$, we put $\mathrm{QL}(V) = \mathrm{QL}(m,q) =$ the set of all $g \in \Gamma\mathrm{L}(V \oplus V')$ such that either $(g(V), g(V')) = (V, V')$ and upon letting $g_1 \in \mathrm{Sem}(V,V)$ and $g_2 \in \mathrm{Sem}(V',V')$ be induced by g we have $(g_1)^\natural = g_2$, or $(g(V), g(V')) = (V', V)$ and upon letting $g_1 \in \mathrm{Sem}(V,V')$ and $g_2 \in \mathrm{Sem}(V',V)$

[7] In this section, in addition to proving the Automorphism Lemma, we shall also prove the Automorphism Theorem. We have arranged the matter so that most of it is valid for any field k, and we have preferred to give an intrinsic geometric treatment. At the end of the section, in Remark (6.10), we shall give an alternative matrix treatment of some things.

[8] In both cases, $g^\natural$ may be called the inverse-adjoint of g. Note that in both cases we have $\iota(g^\natural) = \iota(g)$.

be induced by g we have $(g_1)^\natural = g_2$; we note that then $\mathrm{QL}(V) < \Gamma\mathrm{L}(V \oplus V')$ and we call $\mathrm{QL}(V)$ the *group of all quasilinear maps* of V. We get a natural monomorphism $\pi : \Gamma\mathrm{L}(V) \to \mathrm{QL}(V)$ which sends every $g \in \Gamma\mathrm{L}(V)$ to $\pi(g) = g^\pi \in \mathrm{QL}(V)$ with $(g^\pi(V), g^\pi(V')) = (V, V')$ such that g is induced by g^π. Let $\mathrm{HL}^\pi(V) = \mathrm{HL}^\pi(m,q)$, $\mathrm{SL}^\pi(V) = \mathrm{SL}^\pi(m,q)$, $\mathrm{GL}^\pi(V) = \mathrm{GL}^\pi(m,q)$, and $\Gamma\mathrm{L}^\pi(V) = \Gamma\mathrm{L}^\pi(m,q)$ be the images of $\mathrm{HL}(V)$, $\mathrm{SL}(V)$, $\mathrm{GL}(V)$, and $\Gamma\mathrm{L}(V)$ under π respectively.[9] Let $\pi^* : \Gamma\mathrm{L}^\pi(V) \to \Gamma\mathrm{L}(V)$ be the isomorphism such that for all $g \in \Gamma\mathrm{L}(V)$ we have $\pi^*(g^\pi) = g$. Now clearly $\mathrm{QL}(V) \setminus \Gamma\mathrm{L}^\pi(V) \neq \emptyset$, and by the last footnote we see that the product of any two elements in $\mathrm{QL}(V) \setminus \Gamma\mathrm{L}^\pi(V)$ belongs to $\Gamma\mathrm{L}^\pi(V)$; therefore $\Gamma\mathrm{L}(V)^\pi \lhd \mathrm{QL}(V)$ with $|\mathrm{QL}(V)/\Gamma\mathrm{L}^\pi(V)| = 2$. Also clearly $\mathrm{GL}(V \oplus V') \cap \mathrm{QL}(V) \lhd \mathrm{QL}(V)$ and $\mathrm{GL}^\pi(V) = \mathrm{GL}(V \oplus V') \cap \Gamma\mathrm{L}^\pi(V)$, and hence $\mathrm{GL}^\pi(V) \lhd \mathrm{QL}(V)$ which we can also directly see by the last footnote. Moreover, $\mathrm{HL}^\pi(V) = Z(\mathrm{GL}^\pi(V))$ and hence $\mathrm{HL}^\pi(V)$ is a characteristic subgroup of $\mathrm{GL}^\pi(V)$. Therefore $\mathrm{HL}^\pi(V) \lhd \mathrm{QL}(V)$. Let $\mathrm{PQL}(V) = \mathrm{PQL}(m,q) = \mathrm{QL}(V)/\mathrm{HL}^\pi(V)$ and let $\Theta_Q : \mathrm{QL}(V) \to \mathrm{PQL}(V)$ be the canonical epimorphism. Let $\widehat{\pi} : \mathrm{P}\Gamma\mathrm{L}(V) \to \mathrm{PQL}(V)$ be the unique monomorphism such that for all $g \in \Gamma\mathrm{L}(V)$ we have $\widehat{\pi}(\Theta(g)) = \Theta_Q(g^\pi)$. Let $\mathrm{PSL}^\pi(V) = \mathrm{PSL}^\pi(m,q)$, $\mathrm{PGL}^\pi(V) = \mathrm{PGL}^\pi(m,q)$, and $\mathrm{P}\Gamma\mathrm{L}^\pi(V) = \mathrm{P}\Gamma\mathrm{L}^\pi(m,q)$ be the images of $\mathrm{PSL}(V)$, $\mathrm{PGL}(V)$, and $\mathrm{P}\Gamma\mathrm{L}(V)$ under $\widehat{\pi}$ respectively. For any $\phi \in \mathrm{P}\Gamma\mathrm{L}(V)$ let $\phi^\pi = \widehat{\pi}(\phi)$. Let $\widehat{\pi}^* : \mathrm{P}\Gamma\mathrm{L}^\pi(V) \to \mathrm{P}\Gamma\mathrm{L}(V)$ be the isomorphism such that for all $\phi \in \mathrm{P}\Gamma\mathrm{L}(V)$ we have $\widehat{\pi}^*(\phi^\pi) = \phi$. Since $\Gamma\mathrm{L}(V)^\pi \lhd \mathrm{QL}(V)$ with $|\mathrm{QL}(V)/\Gamma\mathrm{L}^\pi(V)| = 2$, we see that $\mathrm{P}\Gamma\mathrm{L}(V)^\pi \lhd \mathrm{PQL}(V)$ with $|\mathrm{PQL}(V)/\mathrm{P}\Gamma\mathrm{L}^\pi(V)| = 2$.

As usual, by $\mathrm{Sym}(D)$ we denote the *group of all bijections* of a set D. For instance, given any $g \in \Gamma\mathrm{L}(m,q)$, $P \mapsto g(P)$ gives a member of $\mathrm{Sym}(\mathcal{P}(V))$. Moreover, $\mathrm{P}\Gamma\mathrm{L}(m,q)$ acts faithfully on $\mathcal{P}(V)$ where the action is defined by setting $\Theta(g)(P) = g(P)$ for all $g \in \Gamma\mathrm{L}(m,q)$ and $P \in \mathcal{P}(V)$; in other words, for any $\phi \in \mathrm{P}\Gamma\mathrm{L}(m,q)$, $P \mapsto \phi(P)$ gives a member of $\mathrm{Sym}(\mathcal{P}(V))$ and the resulting map $\mathrm{P}\Gamma\mathrm{L}(m,q) \to \mathrm{Sym}(\mathcal{P}(V))$ is an injective homomorphism, i.e., $\mathrm{P}\Gamma\mathrm{L}(m,q)$ is naturally isomorphic to a subgroup of $\mathrm{Sym}(\mathcal{P}(V))$. Similarly $\mathrm{P}\Gamma\mathrm{L}(m,q)$ is naturally isomorphic to a subgroup of $\mathrm{Sym}(\mathcal{P}'(V))$. Given any disjoint sets D and D', by $\mathrm{Int}(D, D')$ we denote the *set of all interchangers* of D and D', i.e., the set of all $z \in \mathrm{Sym}(D \cup D')$ with $z(D) = D'$. For example, $P \mapsto P^\sharp$ together with $Q' \mapsto Q'^\sharp$ gives a member of $\mathrm{Int}(\mathcal{P}(V), \mathcal{P}'(V'))$, where for every $P \in \mathcal{P}(V)$ we define $P^\sharp \in \mathcal{P}'(V')$ by putting $P^\sharp = \{w \in V' : w(v) = 0 \text{ for all } v \in P\}$, and for every $Q' \in \mathcal{P}'(V')$ we define $Q'^\sharp \in \mathcal{P}(V)$ by putting $Q'^\sharp = \{v \in V : w(v) = 0 \text{ for all } w \in Q'\}$; we call $P^\sharp$ and $Q'^\sharp$ the *sharpenings of* P and Q' respec-

[9] To see that $\mathrm{QL}(V) < \Gamma\mathrm{L}(V \oplus V')$ and $\pi : \Gamma\mathrm{L}(V) \to \mathrm{QL}(V)$ is a monomorphism, first note that $\Gamma\mathrm{L}^\pi(V)$ essentially consists of all pairs $g = (g_1, g_2)$ with $g_1 \in \Gamma\mathrm{L}(V)$ and $g_2 = (g_1)^\natural \in \Gamma\mathrm{L}(V')$, and for any such pair we have $\iota(g) = \iota(g_1) = \iota(g_2)$. Moreover, for any other $\bar{g} = (\bar{g}_1, \bar{g}_2)$ in $\Gamma\mathrm{L}^\pi(V)$ we have $g\bar{g} = (g_1, g_2)(\bar{g}_1, \bar{g}_2) = (g_1\bar{g}_1, g_2\bar{g}_2) \in \Gamma\mathrm{L}^\pi(V)$ with $g_2\bar{g}_2 = (g_1\bar{g}_1)^\natural$. Next note that $\mathrm{QL}(V) \setminus \Gamma\mathrm{L}^\pi(V)$ essentially consists of all pairs $h = (h_1, h_2)$ with $h_1 \in \mathrm{Sem}(V, V')$ and $h_2 = (h_1)^\natural \in \mathrm{Sem}(V', V)$, and for any such pair we have $\iota(h) = \iota(h_1) = \iota(h_2)$. Moreover, for any other $\bar{h} = (\bar{h}_1, \bar{h}_2)$ in $\mathrm{QL}(V) \setminus \Gamma\mathrm{L}^\pi(V)$ we have $h\bar{h} = (h_1, h_2)(\bar{h}_1, \bar{h}_2) = (h_2\bar{h}_1, h_1\bar{h}_2) \in \Gamma\mathrm{L}^\pi(V)$ with $h_1\bar{h}_2 = (h_2\bar{h}_1)^\natural$, and hence, in particular, $h^{-1} = (h_1, h_2)^{-1} = (h_2^{-1}, h_1^{-1}) \in \mathrm{QL}(V) \setminus \Gamma\mathrm{L}^\pi(V)$ with $h_1^{-1} = (h_2^{-1})^\natural$. We also have $hg = (h_1, h_2)(g_1, g_2) = (h_1g_1, h_2g_2) \in \mathrm{QL}(V) \setminus \Gamma\mathrm{L}^\pi(V)$ with $h_2g_2 = (h_1g_1)^\natural$, and $gh = (g_1, g_2)(h_1, h_2) = (g_2h_1, g_1h_2) \in \mathrm{QL}(V) \setminus \Gamma\mathrm{L}^\pi(V)$ with $g_1h_2 = (g_2h_1)^\natural$. One way to see all this is by showing the existence of an element j in $\mathrm{QL}(V) \setminus \Gamma\mathrm{L}^\pi(V)$ with $j^2 = 1$ such that $\mathrm{QL}(V) \setminus \Gamma\mathrm{L}^\pi(V) = j\Gamma\mathrm{L}^\pi(V) = \Gamma\mathrm{L}^\pi(V)j$; for an explicit method of finding such an element j, see the last paragraph of Remark (6.10) where, in terms of a suitable basis of $V \oplus V'$, such an element j is expressed as a $2m \times 2m$ matrix J.

tively. As another example, $Q \mapsto Q^\sharp$ together with $P' \mapsto P'^\sharp$ gives a member of $\mathrm{Int}(\mathcal{P}(V'), \mathcal{P}'(V))$, where for every $Q \in \mathcal{P}(V')$ we define $Q^\sharp \in \mathcal{P}'(V)$ by putting $Q^\sharp = \{v \in V : w(v) = 0 \text{ for all } w \in Q\}$, and for every $P' \in \mathcal{P}'(V)$ we define $P'^\sharp \in \mathcal{P}(V')$ by putting $P'^\sharp = \{w \in V' : w(v) = 0 \text{ for all } v \in P'\}$; again we call $Q^\sharp$ and $P'^\sharp$ the *sharpenings of* Q and P' respectively. As a family of examples, if $m > 2$, then given any $g \in \mathrm{QL}(m,q) \setminus \Gamma\mathrm{L}^\pi(m,q)$, $P \mapsto g(P)^\sharp$ together with $P' \mapsto g(P')^\sharp$ gives a member of $\mathrm{Int}(\mathcal{P}(V), \mathcal{P}'(V))$. Moreover, if $m > 2$, then for any $g \in \mathrm{QL}(m,q) \setminus \Gamma\mathrm{L}^\pi(m,q)$, we put $\Theta_Q(g)(P) = g(P)$ for all $P \in \mathcal{P}(V)$, and we put $\Theta_Q(g)(Q) = g(Q)$ for all $Q \in \mathcal{P}(V')$. Now note that if $m > 2$, then given any $\phi \in \mathrm{PQL}(m,q) \setminus \mathrm{P}\Gamma\mathrm{L}^\pi(m,q)$, $P \mapsto \phi(P)^\sharp$ together with $P' \mapsto \phi(P')^\sharp$ gives a member of $\mathrm{Int}(\mathcal{P}(V), \mathcal{P}'(V))$.[10]

Given any groups $G < H$ and any group homomorphism $\theta : H \to \widehat{H}$, we say that $\eta \in \mathrm{Aut}(\theta(G))$ is *induced* by $y \in \mathrm{Aut}(G)$ to mean that for all $g \in G$ we have $\theta(y(g)) = \eta(\theta(g))$; note that then $y \in \mathrm{Aut}(G)$ induces some (and hence a unique) $\eta \in \mathrm{Aut}(\theta(G)) \Leftrightarrow y((\ker\theta) \cap G) = (\ker\theta) \cap G$; also note that if $G \lhd H$, then for any $h \in H$, upon letting $\psi = \theta(h)$, we have that $\eta \in \mathrm{Aut}(\theta(G))$ given by putting $\eta(\phi) = \psi\phi\psi^{-1}$ for all $\phi \in \theta(G)$ is induced by $y \in \mathrm{Aut}(G)$ given by putting $y(g) = hgh^{-1}$ for all $g \in G$.

The following observations will be deduced as consequences of Lemmas (5.2), (5.6) and (5.7):

Observations. *(6.1.1) For all $g \in \Gamma L(m,q)$ and $P \in \mathcal{P}(V)$ we have $gT(P)g^{-1} = T(g(P))$.*

(6.1.2) For all $\phi \in P\Gamma L(m,q)$ and $P \in \mathcal{P}(V)$ we have $\phi\widehat{T}(P)\phi^{-1} = \widehat{T}(\phi(P))$.

(6.1.3) For all $g \in \Gamma L(m,q)$ and $P' \in \mathcal{P}'(V)$ we have $gT'(P')g^{-1} = T'(g(P'))$.

(6.1.4) For all $\phi \in P\Gamma L(m,q)$ and $P' \in \mathcal{P}'(V)$ we have $\phi\widehat{T}'(P')\phi^{-1} = \widehat{T}'(\phi(P'))$.

(6.1.5) If $m > 2$, then for all $h \in QL(m,q) \setminus \Gamma L^\pi(m,q)$ and $P \in \mathcal{P}(V)$ and $P' \in \mathcal{P}'(V)$ we have $h\pi(T(P))h^{-1} = \pi(T'(h(P)^\sharp)))$ and $h\pi(T'(P'))h^{-1} = \pi(T(h(P')^\sharp)))$.

(6.1.6) If $m > 2$, then for all $\psi \in PQL(m,q) \setminus P\Gamma L^\pi(m,q)$ and $P \in \mathcal{P}(V)$ and $P' \in \mathcal{P}'(V)$ we have $\psi\widehat{\pi}(\widehat{T}(P))\psi^{-1} = \widehat{\pi}(\widehat{T}'(\psi(P)^\sharp)))$ and $\psi\widehat{\pi}(\widehat{T}'(P'))\psi^{-1} = \widehat{\pi}(\widehat{T}(\psi(P')^\sharp)))$.

(6.1.7) If $m > 2$, then for any $P \in \mathcal{P}(V)$ and $P' \in \mathcal{P}'(V)$ we have $P \subset P' \Leftrightarrow T(P) \cap T'(P') \neq \emptyset$.

(6.1.8) If $m > 2$, then for any $P \in \mathcal{P}(V)$ and $P' \in \mathcal{P}'(V)$ we have $P \subset P' \Leftrightarrow \widehat{T}(P) \cap \widehat{T}'(P') \neq \emptyset$.

Namely, (6.1.1) follows from (5.6.1), and then (6.1.2) follows from (6.1.1). Likewise, (6.1.3) follows from (5.6.2), and then (6.1.4) follows from (6.1.3). Similarly, (6.1.5) follows from (5.6.1) and (5.6.2), and then (6.1.6) follows from (6.1.5). Next,

[10]The actions of members of $\mathrm{P\Gamma L}(V)$ on $\mathcal{P}(V)$ and $\mathcal{P}'(V)$ are called collineations (cf. [Dem]). Since, via sharpening, $\mathcal{P}'(V)$ and $\mathcal{P}(V)$ can be identified with $\mathcal{P}(V')$ and $\mathcal{P}'(V')$, we get two ways of looking at things. Our definition of inverse-adjoints of members g of $\Gamma\mathrm{L}(V)$ was meant to make sure that g and $g^\sharp$ give rise to the same collineation. Likewise, in the case of $m > 2$, the actions of members of $\mathrm{PQL}(V) \setminus \Gamma\mathrm{L}^\pi(V)$ on $\mathcal{P}(V) \cup \mathcal{P}'(V)$ are called correlations (cf. [Dem]). Since, via sharpening, $\mathcal{P}(V) \cup \mathcal{P}'(V)$ can be identified with $\mathcal{P}'(V') \cup \mathcal{P}(V')$, once more we get two ways of looking at things. Our definition of inverse-adjoints of members g of $\mathrm{Sem}(V, V')$ was again meant to make sure that g and $g^\sharp$ give rise to the same correlation. In greater detail, for all $P \in \mathcal{P}(V)$, $Q \in \mathcal{P}(V')$, $P' \in \mathcal{P}'(V)$, and $Q' \in \mathcal{P}'(V')$ we have $(P^\sharp)^\sharp = P$, $(Q^\sharp)^\sharp = Q$, $(P'^\sharp)^\sharp = P'$, and $(Q'^\sharp)^\sharp = Q'$, and moreover for all $h \in \mathrm{QL}(V)$ we have $h(P^\sharp) = h(P)^\sharp$, $h(Q^\sharp) = h(Q)^\sharp$, $h(P'^\sharp) = h(P')^\sharp$, and $h(Q'^\sharp) = h(Q')^\sharp$.

(6.1.7) follows from (5.7) by noting that if $m > 2$, then for any $P \in \mathcal{P}(V)$ and $P' \in \mathcal{P}'(V)$ with $P \subset P'$, upon letting $P^* = (P, P')$ we clearly have $T^*(P^*) = T(P) \cap T'(P')$, and for any $P \in \mathcal{P}(V)$ and $P' \in \mathcal{P}'(V)$ with $P \not\subset P'$ we clearly have $T(P) \cap T'(P') = \emptyset$. Finally, (6.1.8) follows from (5.2) and (6.1.7).

Using these observations, we shall now prove the following lemma which relates various automorphisms with some of the actions described above.

Lemma (6.2). *For any group G with $SL(m,q) < G < \Gamma L(m,q)$ we have the following:*

(6.2.1) If $\eta \in Aut(\Theta(G))$ and $z \in Sym(\mathcal{P}(V))$ are such that $\eta(\widehat{T}(P)) = \widehat{T}(z(P))$ for all $P \in \mathcal{P}(V)$, then $\eta(\phi)(z(P)) = z(\phi(P))$ for all $\phi \in \Theta(G)$ and $P \in \mathcal{P}(V)$.

(6.2.2) If $\eta, \overline{\eta}$ in $Aut(\Theta(G))$ and $z, \overline{z}$ in $Sym(\mathcal{P}(V))$ are such that for all $P \in \mathcal{P}(V)$ we have $\eta(\widehat{T}(P)) = \widehat{T}(z(P))$ and $\overline{\eta}(\widehat{T}(P)) = \widehat{T}(\overline{z}(P))$, and if $z(P) = \overline{z}(P)$ for all $P \in \mathcal{P}(V)$, then $\eta(\phi) = \overline{\eta}(\phi)$ for all $\phi \in \Theta(G)$.

(6.2.3) If $\eta, \overline{\eta}$ in $Aut(\Theta(G))$ and $z, \overline{z}$ in $Sym(\mathcal{P}(V))$ are such that for all $P \in \mathcal{P}(V)$ we have $\eta(\widehat{T}(P)) = \widehat{T}(z(P))$ and $\overline{\eta}(\widehat{T}(P)) = \widehat{T}(\overline{z}(P))$, then $\eta\overline{\eta}$ in $Aut(\Theta(G))$ and $z\overline{z}$ in $Sym(\mathcal{P}(V))$ are such that for all $P \in \mathcal{P}(V)$ we have $(\eta\overline{\eta})(\widehat{T}(P)) = \widehat{T}((z\overline{z})(P))$.

(6.2.4) If $\eta \in Aut(\Theta(G))$ with $G \lhd \Gamma L(m,q)$ and $\psi \in P\Gamma L(m,q)$ are such that $\eta(\widehat{T}(P)) = \widehat{T}(\psi(P))$ for all $P \in \mathcal{P}(V)$, then $\eta(\phi) = \psi\phi\psi^{-1}$ for all $\phi \in \Theta(G)$.

(6.2.5) If $m > 2$ and $\eta \in Aut(\Theta(G))$ and $z \in Sym(\mathcal{P}(V) \cup \mathcal{P}'(V))$ with $z(\mathcal{P}(V)) = \mathcal{P}(V)$ are such that $\eta(\widehat{T}(P)) = \widehat{T}(z(P))$ for all $P \in \mathcal{P}(V)$ and $\eta(\widehat{T}'(P')) = \widehat{T}'(z(P'))$ for all $P' \in \mathcal{P}'(V)$, then for any $P \in \mathcal{P}(V)$ and $P' \in \mathcal{P}'(V)$ we have $P \subset P' \Leftrightarrow z(P) \subset z(P')$.

(6.2.6) If $m > 2$ and $\eta \in Aut(\Theta(G))$ and $z \in Int(\mathcal{P}(V), \mathcal{P}'(V))$ are such that $\eta(\widehat{T}(P)) = \widehat{T}'(z(P))$ for all $P \in \mathcal{P}(V)$ and $\eta(\widehat{T}'(P')) = \widehat{T}(z(P'))$ for all $P' \in \mathcal{P}'(V)$, then $\eta(\phi)(z(P)) = z(\phi(P))$ for all $\phi \in \Theta(G)$ and $P \in \mathcal{P}(V)$.

(6.2.7) If $m > 2$ and $\eta, \overline{\eta}$ in $Aut(\Theta(G))$ and $z, \overline{z}$ in $Int(\mathcal{P}(V), \mathcal{P}'(V))$ are such that for all $P \in \mathcal{P}(V)$ we have $\eta(\widehat{T}(P)) = \widehat{T}'(z(P))$ and $\overline{\eta}(\widehat{T}(P)) = \widehat{T}'(\overline{z}(P))$ and for all $P' \in \mathcal{P}'(V)$ we have $\eta(\widehat{T}'(P')) = \widehat{T}(z(P'))$ and $\overline{\eta}(\widehat{T}'(P')) = \widehat{T}(\overline{z}(P'))$, and if $z(P) = \overline{z}(P)$ for all $P \in \mathcal{P}(V)$, then $\eta(\phi) = \overline{\eta}(\phi)$ for all $\phi \in \Theta(G)$.

(6.2.8) If $m > 2$ and $\eta \in Aut(\Theta(G))$ with $\pi(G) \lhd QL(m,q)$ and $\psi \in PQL(m,q) \setminus P\Gamma L^{\pi}(m,q)$ are such that $\eta(\widehat{T}(P)) = \widehat{T}'(\psi(P)^{\sharp})$ for all $P \in \mathcal{P}(V)$ and $\eta(\widehat{T}'(P')) = \widehat{T}(\psi(P')^{\sharp})$ for all $P' \in \mathcal{P}'(V)$, then $\eta(\phi) = \widehat{\pi}^*(\psi\phi^{\pi}\psi^{-1})$ for all $\phi \in \Theta(G)$.

(6.2.9) If $m > 2$ and $\eta \in Aut(\Theta(G))$ and $z \in Int(\mathcal{P}(V), \mathcal{P}'(V))$ with $z(\mathcal{P}(V)) = \mathcal{P}'(V)$ are such that $\eta(\widehat{T}(P)) = \widehat{T}'(z(P))$ for all $P \in \mathcal{P}(V)$ and $\eta(\widehat{T}'(P')) = \widehat{T}(z(P'))$ for all $P' \in \mathcal{P}'(V)$, then for any $P \in \mathcal{P}(V)$ and $P' \in \mathcal{P}'(V)$ we have $P \subset P' \Leftrightarrow z(P') \subset z(P)$.

(6.2.10) If $m > 2$ and $\eta \in Aut(\Theta(G))$ and $z \in Sym(\mathcal{P}(V) \cup \mathcal{P}'(V))$ with $z(\mathcal{P}(V)) \neq \mathcal{P}(V)$ are such that for all $P \in \mathcal{P}(V)$ we have $\eta(\widehat{T}(P)) = \widehat{T}(z(P))$ or $\eta(\widehat{T}(P)) = \widehat{T}'(z(P))$ accordingly as $z(P) \in \mathcal{P}(V)$ or $z(P) \in \mathcal{P}'(V)$, and for all $P' \in \mathcal{P}'(V)$ we have $\eta(\widehat{T}'(P')) = \widehat{T}(z(P'))$ or $\eta(\widehat{T}'(P')) = \widehat{T}'(z(P'))$ accordingly as $z(P') \in \mathcal{P}(V)$ or $z(P') \in \mathcal{P}'(V)$, then $z(\mathcal{P}(V)) = \mathcal{P}'(V)$.

To prove (6.2.1), we want to show that if $\eta \in \mathrm{Aut}(\Theta(G))$ and $z \in \mathrm{Sym}(\mathcal{P}(V))$ are such that $\eta(\widehat{T}(P)) = \widehat{T}(z(P))$ for all $P \in \mathcal{P}(V)$, then (1*) $\eta(\phi)(z(P)) = z(\phi(P))$ for all $\phi \in \Theta(G)$ and $P \in \mathcal{P}(V)$. To see this, given any $\phi \in \Theta(G)$ and $P \in \mathcal{P}(V)$,

by taking $\phi(P)$ for P in the equation $\eta(\widehat{T}(P)) = \widehat{T}(z(P))$ we get the equation $\eta(\widehat{T}(\phi(P))) = \widehat{T}(z(\phi(P)))$ and, in view of these two equations, by applying η to both sides of (6.1.2) we conclude that: (2*) $\eta(\phi)\widehat{T}(z(P))\eta(\phi)^{-1} = \widehat{T}(z(\phi(P)))$. Taking $(\eta(\phi), z(P))$ for (ϕ, P) in the LHS of (6.1.2) we see that the LHS of (2*) equals $\widehat{T}(\eta(\phi)(z(P)))$ and by equating this to the RHS of (2*) we conclude that: (3*) $\widehat{T}(\eta(\phi)(z(P))) = \widehat{T}(z(\phi(P)))$. Now (1*) follows from (3*) because by (5.13) we know that for all $P_1 \neq P_2$ in $\mathcal{P}(V)$ we have $\widehat{T}(P_1) \neq \widehat{T}(P_2)$. This completes the proof of (6.2.1).

To prove (6.2.2), we note that if $\eta, \overline{\eta}$ in $\mathrm{Aut}(\Theta(G))$ and $z, \overline{z}$ in $\mathrm{Sym}(\mathcal{P}(V))$ are such that for all $P \in \mathcal{P}(V)$ we have $\eta(\widehat{T}(P)) = \widehat{T}(z(P))$ and $\overline{\eta}(\widehat{T}(P)) = \widehat{T}(\overline{z}(P))$ then, given any $\phi \in \Theta(G)$, by (6.2.1) we see that $\eta(\phi)(z(P)) = z(\phi(P))$ and $\overline{\eta}(\phi)(\overline{z}(P)) = \overline{z}(\phi(P))$ for all $P \in \mathcal{P}(V)$, and hence if $z(P) = \overline{z}(P)$ for all $P \in \mathcal{P}(V)$, then $\eta(\phi)((z(P)) = \overline{\eta}(\phi)(z(P))$ for all $P \in \mathcal{P}(V)$ and therefore $\eta(\phi)(P) = \overline{\eta}(\phi)(P)$ for all $P \in \mathcal{P}(V)$ and hence $\eta(\phi) = \overline{\eta}(\phi)$. This proves (6.2.2). The proof of (6.2.3) is straightforward.

To prove (6.2.4), we note that if $\eta \in \mathrm{Aut}(\Theta(G))$ with $G \lhd \Gamma\mathrm{L}(m, q)$ and $\psi \in \mathrm{P}\Gamma\mathrm{L}(m, q)$ are such that $\eta(\widehat{T}(P)) = \widehat{T}(\psi(P))$ for all $P \in \mathcal{P}(V)$, then, upon letting $\overline{\eta}(\phi) = \psi\phi\psi^{-1}$ for all $\phi \in \Theta(G)$ and $z(P) = \overline{z}(P) = \psi(P)$ for all $P \in \mathcal{P}(V)$, in view of (6.1.2) we see that $\overline{\eta} \in \mathrm{Aut}(\Theta(G))$ and $z = \overline{z} \in \mathrm{Sym}(\mathcal{P}(V))$ are such that for all $P \in \mathcal{P}(V)$ we have $\eta(\widehat{T}(P)) = \widehat{T}(z(P))$ and $\overline{\eta}(\widehat{T}(P)) = \widehat{T}(\overline{z}(P))$, and hence by (6.2.2) we conclude that $\eta(\phi) = \psi\phi\psi^{-1}$ for all $\phi \in \Theta(G)$. This proves (6.2.4).

To prove (6.2.5), we note that if $m > 2$ and $\eta \in \mathrm{Aut}(\Theta(G))$ and $z \in \mathrm{Sym}(\mathcal{P}(V) \cup \mathcal{P}'(V))$ with $z(\mathcal{P}(V)) = \mathcal{P}(V)$ are such that $\eta(\widehat{T}(P)) = \widehat{T}(z(P))$ for all $P \in \mathcal{P}(V)$ and $\eta(\widehat{T}'(P')) = \widehat{T}'(z(P'))$ for all $P' \in \mathcal{P}'(V)$, then, since η is an automorphism, for any subsets H and H' of $\Theta(G)$ we have $H \cap H' \neq \emptyset \Leftrightarrow \eta(H) \cap \eta(H') \neq \emptyset$, and hence for any $P \in \mathcal{P}(V)$ and $P' \in \mathcal{P}'(V)$ we have $\widehat{T}(P) \cap \widehat{T}'(P') \neq \emptyset \Leftrightarrow \eta(\widehat{T}(P)) \cap \eta(\widehat{T}'(P')) \neq \emptyset$, and therefore in view of (6.1.8) we see that for any $P \in \mathcal{P}(V)$ and $P' \in \mathcal{P}'(V)$ we have $P \subset P' \Leftrightarrow z(P) \subset z(P')$. This proves (6.2.5).

To prove (6.2.6), we want to show that if $m > 2$ and $\eta \in \mathrm{Aut}(\Theta(G))$ and $z \in \mathrm{Int}(\mathcal{P}(V), \mathcal{P}'(V))$ are such that $\eta(\widehat{T}(P)) = \widehat{T}'(z(P))$ for all $P \in \mathcal{P}(V)$ and $\eta(\widehat{T}'(P')) = \widehat{T}(z(P'))$ for all $P' \in \mathcal{P}'(V)$, then (1′) $\eta(\phi)(z(P)) = z(\phi(P))$ for all $\phi \in \Theta(G)$ and $P \in \mathcal{P}(V)$. To see this, given any $\phi \in \Theta(G)$ and $P \in \mathcal{P}(V)$, by taking $\phi(P)$ for P in the equation $\eta(\widehat{T}(P)) = \widehat{T}'(z(P))$ we get the equation $\eta(\widehat{T}(\phi(P))) = \widehat{T}'(z(\phi(P)))$ and, in view of these two equations, by applying η to both sides of (6.1.2) we conclude that: (2′) $\eta(\phi)\widehat{T}'(z(P))\eta(\phi)^{-1} = \widehat{T}'(z(\phi(P)))$. Taking $(\eta(\phi), z(P))$ for (ϕ, P') in the LHS of (6.1.4) we see that the LHS of (2′) equals $\widehat{T}'(\eta(\phi)(z(P)))$ and by equating this to the RHS of (2′) we conclude that: (3′) $\widehat{T}'(\eta(\phi)(z(P))) = \widehat{T}'(z(\phi(P)))$. Now (1′) follows from (3′) because by (5.13) we know that for all $P_1' \neq P_2'$ in $\mathcal{P}'(V)$ we have $\widehat{T}'(P_1') \neq \widehat{T}'(P_2')$. This completes the proof of (6.2.6).

To prove (6.2.7), we note that if $m > 2$ and $\eta, \overline{\eta}$ in $\mathrm{Aut}(\Theta(G))$ and $z, \overline{z}$ in $\mathrm{Int}(\mathcal{P}(V), \mathcal{P}'(V))$ are such that for all $P \in \mathcal{P}(V)$ we have $\eta(\widehat{T}(P)) = \widehat{T}'(z(P))$ and $\overline{\eta}(\widehat{T}(P)) = \widehat{T}'(\overline{z}(P))$ and for all $P' \in \mathcal{P}'(V)$ we have $\eta(\widehat{T}'(P')) = \widehat{T}(z(P'))$ and $\overline{\eta}(\widehat{T}'(P')) = \widehat{T}(\overline{z}(P'))$, then, given any $\phi \in \Theta(G)$, by (6.2.6) we see that $\eta(\phi)(z(P)) = z(\phi(P))$ and $\overline{\eta}(\phi)(\overline{z}(P)) = \overline{z}(\phi(P))$ for all $P \in \mathcal{P}(V)$, and hence if $z(P) = \overline{z}(P)$ for all $P \in \mathcal{P}(V)$, then $\eta(\phi)((z(P)) = \overline{\eta}(\phi)(z(P))$ for all $P \in \mathcal{P}(V)$

and therefore $\eta(\phi)(P') = \overline{\eta}(\phi)(P')$ for all $P' \in \mathcal{P}'(V)$ and hence $\eta(\phi) = \overline{\eta}(\phi)$. This proves (6.2.7).

To prove (6.2.8), we note that if $m > 2$ and $\eta \in \mathrm{Aut}(\Theta(G))$ with $\pi(G) \lhd \mathrm{QL}(m,q)$ and $\psi \in \mathrm{PQL}(m,q) \setminus \mathrm{P\Gamma L}^\pi(m,q)$ are such that $\eta(\widehat{T}(P)) = \widehat{T}'(\psi(P)^\sharp)$ for all $P \in \mathcal{P}(V)$ and $\eta(\widehat{T}'(P')) = \widehat{T}(\psi(P')^\sharp)$ for all $P' \in \mathcal{P}'(V)$, then, upon letting $\overline{\eta}(\phi) = \widehat{\pi}^*(\psi\phi^\pi\psi^{-1})$ for all $\phi \in \Theta(G)$ and $z(P) = \overline{z}(P) = \psi(P)^\sharp$ for all $P \in \mathcal{P}(V)$ and $z(P') = \overline{z}(P') = \psi(P')^\sharp$ for all $P' \in \mathcal{P}'(V)$, in view of (6.1.6) we see that $\overline{\eta} \in \mathrm{Aut}(\Theta(G))$ and $z = \overline{z} \in \mathrm{Int}(\mathcal{P}(V), \mathcal{P}'(V))$ are such that for all $P \in \mathcal{P}(V)$ we have $\eta(\widehat{T}(P)) = \widehat{T}'(z(P))$ and $\overline{\eta}(\widehat{T}(P)) = \widehat{T}'(\overline{z}(P))$ and for all $P' \in \mathcal{P}'(V)$ we have $\eta(\widehat{T}'(P')) = \widehat{T}(z(P'))$ and $\overline{\eta}(\widehat{T}'(P')) = \widehat{T}(\overline{z}(P'))$, and hence by (6.2.7) we conclude that $\eta(\phi) = \widehat{\pi}^*(\psi\phi^\pi\psi^{-1})$ for all $\phi \in \Theta(G)$. This proves (6.2.8).

To prove (6.2.9), we note that if $m > 2$ and $\eta \in \mathrm{Aut}(\Theta(G))$ and $z \in \mathrm{Int}(\mathcal{P}(V), \mathcal{P}'(V))$ with $z(\mathcal{P}(V)) = \mathcal{P}'(V)$ are such that $\eta(\widehat{T}(P)) = \widehat{T}'(z(P))$ for all $P \in \mathcal{P}(V)$ and $\eta(\widehat{T}'(P')) = \widehat{T}(z(P'))$ for all $P' \in \mathcal{P}'(V)$, then, since η is an automorphism, for any subsets H and H' of $\Theta(G)$ we have $H \cap H' \neq \emptyset \Leftrightarrow \eta(H) \cap \eta(H') \neq \emptyset$, and hence for any $P \in \mathcal{P}(V)$ and $P' \in \mathcal{P}'(V)$ we have $\widehat{T}(P) \cap \widehat{T}'(P') \neq \emptyset \Leftrightarrow \eta(\widehat{T}(P)) \cap (\widehat{T}'(P')) \neq \emptyset$, and therefore in view of (6.1.8) we see that for any $P \in \mathcal{P}(V)$ and $P' \in \mathcal{P}'(V)$ we have $P \subset P' \Leftrightarrow z(P') \subset z(P)$. This proves (6.2.9).

Finally, since $\mathrm{PSL}(m,q)$ acts transitively on $\mathcal{P}(V)$ as well as on $\mathcal{P}'(V)$, by (5.14), (6.1.2) and (6.1.4) we see that if $m > 2$, then $\widehat{T}(P)_{P \in \mathcal{P}(V)}$ and $\widehat{T}'(P')_{P' \in \mathcal{P}'(V)}$ are two disjoint conjugacy classes of subsets of $\Theta(G)$, where by a conjugacy class of subsets of a group H we mean the set of all H-conjugates of a subset D of H, i.e., the set of all subsets of H of the form hDh^{-1} with h varying in H. Therefore (6.2.10) follows from the obvious fact which says that if y is an automorphism of a group H and D is a subset of H, then the y images of the H-conjugates of D are the H-conjugates of $y(D)$.

We are now ready to prove the following:

Proposition (6.3). *Given any group G with $SL(m,q) < G < \Gamma L(m,q)$, and given any $\eta \in Aut(\Theta(G))$, we have the following:*

(6.3.1) If $m = 2$ with $G \lhd \Gamma L(m,q)$ and there exists $z \in Sym(\mathcal{P}(V))$ such that for all $P \in \mathcal{P}(V)$ we have $\eta(\widehat{T}(P)) = \widehat{T}(z(P))$, then there exists $h \in \Gamma L(m,q)$ such that upon letting $\psi = \Theta(h)$ we have $\eta(\phi) = \psi\phi\psi^{-1}$ for all $\phi \in \Theta(G)$, and hence η is induced by $y \in Aut(G)$ defined by putting $y(g) = hgh^{-1}$ for all $g \in G$.

(6.3.2) If $m > 2$ with $G \lhd \Gamma L(m,q)$ and there exists $z \in Sym(\mathcal{P}(V) \cup \mathcal{P}'(V))$ with $z(\mathcal{P}(V)) = \mathcal{P}(V)$ such that for all $P \in \mathcal{P}(V)$ we have $\eta(\widehat{T}(P)) = \widehat{T}(z(P))$, and for all $P' \in \mathcal{P}'(V)$ we have $\eta(\widehat{T}'(P')) = \widehat{T}'(z(P'))$, then there exists $h \in \Gamma L(m,q)$ such that upon letting $\psi = \Theta(h)$ we have $\eta(\phi) = \psi\phi\psi^{-1}$ for all $\phi \in \Theta(G)$, and hence η is induced by $y \in Aut(G)$ defined by putting $y(g) = hgh^{-1}$ for all $g \in G$.

(6.3.3) If $m > 2$ with $\pi(G) \lhd QL(m,q)$ and there exists $z \in Sym(\mathcal{P}(V) \cup \mathcal{P}'(V))$ with $z(\mathcal{P}(V)) \neq \mathcal{P}(V)$ such that for all $P \in \mathcal{P}(V)$ we have $\eta(\widehat{T}(P)) = \widehat{T}(z(P))$ or $\eta(\widehat{T}(P)) = \widehat{T}'(z(P))$ accordingly as $z(P) \in \mathcal{P}(V)$ or $z(P) \in \mathcal{P}'(V)$, and for all $P' \in \mathcal{P}'(V)$ we have $\eta(\widehat{T}'(P')) = \widehat{T}(z(P'))$ or $\eta(\widehat{T}'(P')) = \widehat{T}'(z(P'))$ accordingly as $z(P') \in \mathcal{P}(V)$ or $z(P') \in \mathcal{P}'(V)$, then $z(\mathcal{P}(V)) = \mathcal{P}'(V)$ and there exists $h \in QL(m,q) \setminus \Gamma L^\pi(m,q)$ such that upon letting $\psi = \Theta_Q(h)$ we have $\eta(\phi) = \widehat{\pi}^*(\psi\phi^\pi\psi^{-1})$ for all $\phi \in \Theta(G)$, and hence η is induced by $y \in Aut(G)$ defined by putting $y(g) = \pi^*(hg^\pi h^{-1})$ for all $g \in G$.

To prove (6.3.1), first assume that $m = 2$ with $G \triangleleft \Gamma\mathrm{L}(m,q)$ and there exists $z \in \mathrm{Sym}(\mathcal{P}(V))$ such that for all $P \in \mathcal{P}(V)$ we have $\eta(\widehat{T}(P)) = \widehat{T}(z(P))$. Let (u,v) be a basis of V. Then $x \mapsto P(x) = kw(x)$ gives a bijection $k \cup \{\infty\} \to \mathcal{P}(V)$ where $w(x) = u + xv$ or $w(x) = v$ accordingly as $x \in k$ or $x = \infty$. For any $e \in \mathrm{GL}(2,q)$, let $\eta_e \in \mathrm{Aut}(\Theta(G))$ be given by setting $\eta_e(\Theta(g)) = \eta(\Theta(ege^{-1}))$ for all $g \in G$, and let $z_e \in \mathrm{Sym}(\mathcal{P}(V))$ be given by setting $z_e(P) = z(e(P))$ for all $P \in \mathcal{P}(V)$. Then by (6.1.2) and (6.2.3) we see that $\eta_e(\widehat{T}(P)) = \widehat{T}(z_e(P))$ for all $P \in \mathcal{P}(V)$. Since $\mathrm{GL}(2,q)$ acts 3-transitively on $\mathcal{P}(V)$, by choosing e suitably, we may assume that $z_e(P(\kappa)) = P(\kappa)$ for $\kappa = 0, 1, \infty$. Then we get a

(1) $$\text{bijection } \sigma : k \to k \text{ with } \sigma(0) = 0 \text{ and } \sigma(1) = 1$$

such that for all $x \in k$ we have $z_e(P(x)) = P(\sigma(x))$. We shall show that actually $\sigma \in \mathrm{Aut}(k)$.

First we note that by (6.2.1) we have

(2) $$\eta_e(\phi)(z_e(P)) = z_e(\phi(P)) \quad \text{for all } \phi \in \mathrm{PSL}(2,q) \text{ and } P \in \mathcal{P}(V).$$

Next,[11] referring to the proof of (5.7), $\lambda \mapsto g_\lambda$ gives a bijection $k \to T(P(\infty)) \cup \{1\}$ where $g_\lambda(u) = u + \lambda v$ and $g_\lambda(v) = v$. Therefore, upon letting $\phi_\lambda = \Theta(g_\lambda)$, in view of (5.2), $\lambda \mapsto \phi_\lambda$ gives a bijection $k \to \widehat{T}(P(\infty)) \cup \{1\}$, and hence, because of the equations $\eta_e(\widehat{T}(P)) = \widehat{T}(z_e(P))$ and $z_e(P(\infty)) = P(\infty)$, we see that

(3) $$\text{for every } \lambda \in k \text{ we have } \eta_e(\phi_\lambda) = \phi_{\lambda'} \text{ for some } \lambda' \in k.$$

Clearly members of $\widehat{T}(P(\infty))$ correspond to addition, i.e., for all x, λ, λ' in k we have $\phi_\lambda(P(x)) = P(x + \lambda)$ and $\phi_{\lambda'}(P(x)) = P(x + \lambda')$. Therefore, with λ and λ' related as in (3), by taking $(\phi_\lambda, P(x))$ for (ϕ, P) in (2) we get $P(\sigma(x) + \lambda') = P(\sigma(x + \lambda))$; by taking $x = 0$ in this equation and remembering that $\sigma(0) = 0$, we get $P(\lambda') = P(\sigma(\lambda))$ and hence $\lambda' = \sigma(\lambda)$; consequently, for all x and λ in k we have $P(\sigma(x) + \sigma(\lambda)) = P(\sigma(x + \lambda))$ and hence

(4) $$\sigma(x + \lambda) = \sigma(x) + \sigma(\lambda) \quad \text{for all } x \text{ and } \lambda \text{ in } k.$$

Let $N^\dagger$ be the set of all ϕ in $\mathrm{PSL}(2,q)$ which normalize $\widehat{T}(P(0))$ and $\widehat{T}(P(\infty))$, and let $N^\ddagger$ be the set of all ϕ in $\mathrm{PSL}(2,q)$ which interchange $\widehat{T}(P(0))$ and $\widehat{T}(P(\infty))$, i.e.,

$$N^\dagger = \{\phi \in \mathrm{PSL}(2,q) : \phi\widehat{T}(P(0))\phi^{-1} = \widehat{T}(P(0)) \text{ and } \phi\widehat{T}(P(\infty))\phi^{-1} = \widehat{T}(P(\infty))\}$$

and

$$N^\ddagger = \{\phi \in \mathrm{PSL}(2,q) : \phi\widehat{T}(P(0))\phi^{-1} = \widehat{T}(P(\infty)) \text{ and } \phi\widehat{T}(P(\infty))\phi^{-1} = \widehat{T}(P(0))\}.$$

In a moment we shall see that members of $N^\dagger$ correspond to multiplication, and members of $N^\ddagger$ correspond to reciprocation.

By the above definitions of $N^\dagger$ and $N^\ddagger$ it follows that

(5) $$\eta_e(N^\dagger) = N^\dagger \quad \text{and} \quad \eta_e(N^\ddagger) = N^\ddagger.$$

[11] As the most exciting part of the theory of transvections, following Schreier-van der Waerden [ScW], we now proceed to characterize the three basic operations of field theory, addition, multiplication, and reciprocation, in terms of transvections which themselves are the vector-space incarnations of elementary row and column operations of matrix theory.

Moreover, by (6.1.2) we get the alternative characterizations of $N^\dagger$ and $N^\ddagger$ saying that

$$N^\dagger = \{\Theta(g) : g \in \mathrm{SL}(2,q) \text{ with } g(P(0)) = P(0) \text{ and } g(P(\infty)) = P(\infty)\}$$

and

$$N^\ddagger = \{\Theta(g) : g \in \mathrm{SL}(2,q) \text{ with } g(P(0)) = P(\infty) \text{ and } g(P(\infty)) = P(0)\}.$$

For any μ and ν in k^* let $\phi^\dagger_\mu = \Theta(g^\dagger_\mu)$ and $\phi^\ddagger_\nu = \Theta(g^\ddagger_\nu)$, where $g^\dagger_\mu$ is the member of $\mathrm{SL}(2,q)$ such that $g^\dagger_\mu(u) = \mu^{-1}u$ and $g^\dagger_\mu(v) = \mu v$, and $g^\ddagger_\nu$ is the member of $\mathrm{SL}(2,q)$ such that $g^\ddagger_\nu(u) = -\nu^{-1}v$ and $g^\ddagger_\nu(v) = \nu u$. By the above alternative characterizations of $N^\dagger$ and $N^\ddagger$ we see that $\mu \mapsto \phi^\dagger_\mu$ gives a surjection $k^* \to N^\dagger$, and $\nu \mapsto \phi^\ddagger_\nu$ gives a surjection $k^* \to N^\ddagger$. Therefore by (5) we conclude that

(6) for every $\mu \in k^*$ we have $\eta_e(\phi^\dagger_\mu) = \phi^\dagger_{\mu'}$ for some $\mu' \in k^*$

and

(7) for every $\nu \in k^*$ we have $\eta_e(\phi^\ddagger_\nu) = \phi^\ddagger_{\nu'}$ for some $\nu' \in k^*$.

Now clearly members of $N^\dagger$ correspond to multiplication, i.e., for all x, μ, μ' in k^* we have $\phi^\dagger_\mu(P(x)) = \mu^2 x$ and $\phi^\dagger_{\mu'}(P(x)) = \mu'^2 x$. Therefore, with μ and μ' related as in (6), by taking $(\phi^\dagger_\mu, P(x))$ for (ϕ, P) in (2) we get $P(\mu'^2\sigma(x)) = P(\sigma(\mu^2 x))$; by taking $x = 1$ in this equation and remembering that $\sigma(1) = 1$, we get $P(\mu'^2) = P(\sigma(\mu^2))$ and hence $\mu'^2 = \sigma(\mu^2)$; consequently, for all x and μ in k^* we have $P(\sigma(\mu^2)\sigma(x)) = P(\sigma(\mu^2 x))$ and hence

(8) $$\sigma(\mu^2 x) = \sigma(\mu^2)\sigma(x) \quad \text{for all } \mu \text{ and } x \text{ in } k^*.$$

Again, clearly members of $N^\ddagger$ correspond to reciprocation, i.e., for all x, ν, ν' in k^* we have $\phi^\ddagger_\nu(P(x)) = -\nu^2/x$ and $\phi^\ddagger_{\nu'}(P(x)) = -\nu'^2/x$. Therefore, with ν and ν' related as in (7), by taking $(\phi^\ddagger_\nu, P(x))$ for (ϕ, P) in (2) we get $P(-\mu'^2/\sigma(x)) = P(\sigma(-\mu^2/x))$; by taking $x = 1 = \mu$ in this equation and remembering that $\sigma(1) = 1$, we get $P(-\mu'^2) = P(\sigma(-1))$ and hence $-\mu'^2 = \sigma(-1)$; consequently, for all x in k^* we have $P(\sigma(-1)/\sigma(x)) = P(\sigma(-1/x))$ and hence $\sigma(-1/x) = \sigma(-1)/\sigma(x)$; by (1) and (4) we see that $\sigma(-1/x) = -\sigma(1/x)$ and $\sigma(-1)/\sigma(x) = -(1/\sigma(x))$ and hence

(9) $$\sigma(1/x) = 1/\sigma(x) \quad \text{for all } x \in k^*.$$

By (1), (4), (8) and (9) we see that for any $\mu \in k^*$ with $\mu \neq 1$ we have

$$\frac{\sigma(\mu^2)}{\sigma(\mu)-1} = \sigma\left(\frac{\mu^2}{\mu-1}\right) = \sigma\left(\mu+1+\frac{1}{\mu-1}\right) = \sigma(\mu)+1+\frac{1}{\sigma(\mu)-1} = \frac{\sigma(\mu)^2}{\sigma(\mu)-1}$$

and hence $\sigma(\mu^2) = \sigma(\mu)^2$; since this is obviously true for $\mu = 1$, we conclude that

(10) $$\sigma(\mu^2) = \sigma(\mu)^2 \quad \text{for all } \mu \in k^*,$$

Given any μ and x in k, if $p \neq 2$, then by (1), (4), (8), (9), (10) we see that

$$\sigma(\mu x) = \sigma\left(\frac{(\mu+x)^2}{4} - \frac{(\mu-x)^2}{4}\right) = \frac{(\sigma(\mu)+\sigma(x))^2}{4} - \frac{(\sigma(\mu)-\sigma(x))^2}{4} = \sigma(\mu)\sigma(x)$$

and hence $\sigma(\mu x) = \sigma(\mu)\sigma(x)$, and if $p = 2$, then by (8), (9), (10) we see that

$$\sigma(\mu x)^2 = \sigma((\mu x)^2) = \sigma(\mu^2 x^2) = \sigma(\mu)^2\sigma(x)^2 = (\sigma(\mu)\sigma(x))^2$$

and hence again $\sigma(\mu x) = \sigma(\mu)\sigma(x)$. Thus we always have

$$\sigma(\mu x) = \sigma(\mu)\sigma(x) \quad \text{for all } \mu \text{ and } x \text{ in } k. \tag{11}$$

By (1), (4) and (11) we conclude that $\sigma \in \mathrm{Aut}(k)$. Therefore we get $\psi_e = \Theta(h_e) \in \mathrm{P\Gamma L}(2,q)$ where $h_e \in \Gamma\mathrm{L}(2,q)$ is defined by putting $h_e(\mu u + \nu v) = \sigma(\mu)u + \sigma(\nu)v$ for all μ, ν in k. Since $z_e(P(\infty)) = P(\infty)$ and $z_e(P(x)) = P(\sigma(x))$ for all $x \in k$, it follows that $z_e(P) = \psi_e(P)$ for all $P \in \mathcal{P}(V)$. Since $\eta_e(\widehat{T}(P)) = \widehat{T}(z_e(P))$ for all $P \in \mathcal{P}(V)$, we conclude that $\eta_e(\widehat{T}(P)) = \widehat{T}(\psi_e(P))$ for all $P \in \mathcal{P}(V)$. Therefore by (6.2.4) we see that $\eta_e(\phi) = \psi_e \phi \psi_e^{-1}$ for all $\phi \in \Theta(G)$. Since $\eta_e(\Theta(g)) = \eta(\Theta(ege^{-1}))$ for all $g \in G$, upon letting $\psi = \Theta(h) \in \mathrm{P\Gamma L}(2,q)$ with $h = h_e e^{-1} \in \Gamma\mathrm{L}(2,q)$, we get $\eta(\phi) = \psi\phi\psi^{-1}$ for all $\phi \in \Theta(G)$. It follows that η is induced by $y \in \mathrm{Aut}(G)$ defined by putting $y(g) = hgh^{-1}$ for all $g \in G$. This completes the proof of (6.3.1).

To prove (6.3.2), next assume that $m > 2$ with $G \triangleleft \Gamma\mathrm{L}(m,q)$ and there exists $z \in \mathrm{Sym}(\mathcal{P}(V) \cup \mathcal{P}'(V))$ with $z(\mathcal{P}(V)) = \mathcal{P}(V)$ such that for all $P \in \mathcal{P}(V)$ we have $\eta(\widehat{T}(P)) = \widehat{T}(z(P))$, and for all $P' \in \mathcal{P}'(V)$ we have $\eta(\widehat{T}'(P')) = \widehat{T}'(z(P'))$. Then by (6.2.5) we see that for any $P \in \mathcal{P}(V)$ and $P' \in \mathcal{P}'(V)$ we have $P \subset P' \Leftrightarrow z(P) \subset z(P')$. Therefore by the Fundamental Theorem of Projective Geometry,[12] there exists $h \in \Gamma\mathrm{L}(m,q)$ such that, upon letting $\psi = \Theta(h)$, for every $P \in \mathcal{P}(V)$ we have $z(P) = \psi(P)$ and for every $P' \in \mathcal{P}'(V)$ we have $z(P') = \psi(P')$. Now by (6.2.4) we conclude that $\eta(\phi) = \psi\phi\psi^{-1}$ for all $\phi \in \Theta(G)$. It follows that η is induced by $y \in \mathrm{Aut}(G)$ defined by putting $y(g) = hgh^{-1}$ for all $g \in G$. This completes the proof of (6.3.2).

To prove (6.3.3), finally assume that $m > 2$ with $\pi(G) \triangleleft \mathrm{QL}(m,q)$ and there exists $z \in \mathrm{Sym}(\mathcal{P}(V) \cup \mathcal{P}'(V))$ with $z(\mathcal{P}(V)) \neq \mathcal{P}(V)$ such that for all $P \in \mathcal{P}(V)$ we have $\eta(\widehat{T}(P)) = \widehat{T}(z(P))$ or $\eta(\widehat{T}(P)) = \widehat{T}'(z(P))$ accordingly as $z(P) \in \mathcal{P}(V)$ or $z(P) \in \mathcal{P}'(V)$, and for all $P' \in \mathcal{P}'(V)$ we have $\eta(\widehat{T}'(P')) = \widehat{T}(z(P'))$ or $\eta(\widehat{T}'(P')) = \widehat{T}'(z(P'))$ accordingly as $z(P') \in \mathcal{P}(V)$ or $z(P') \in \mathcal{P}'(V)$. Then by (6.2.9) and (6.2.10) we see that $z(\mathcal{P}(V)) = \mathcal{P}'(V)$ and for any $P \in \mathcal{P}(V)$ and $P' \in \mathcal{P}'(V)$ we have $P \subset P' \Leftrightarrow z(P') \subset z(P)$. Therefore by the Fundamental Theorem of Projective Geometry,[13] there exists $h \in \mathrm{QL}(m,q) \backslash \Gamma\mathrm{L}^{\pi}(m,q)$ such that, upon letting $\psi = \Theta_Q(h)$, for every $P \in \mathcal{P}(V)$ we have $z(P) = \psi(P)^{\sharp}$ and for every $P' \in \mathcal{P}'(V)$ we have $z(P') = \psi(P')^{\sharp}$. Now by (6.2.8) we conclude that $\eta(\phi) = \widehat{\pi}^*(\psi\phi^{\pi}\psi^{-1})$ for all $\phi \in \Theta(G)$. It follows that η is induced by $y \in \mathrm{Aut}(G)$ defined by putting $y(g) = \pi^*(hg^{\pi}h^{-1})$ for all $g \in G$. This completes the proof of (6.3.3).

In Lemma (6.4) we shall relate automorphisms with homomorphisms of groups and centralizers of subgroups, where we recall that for any groups $G < H$, the *centralizer* of G in H is the subgroup of H defined by putting $Z_H(G) = \{h \in H : hg = gh \text{ for all } g \in G\}$.

Lemma (6.4). *For any groups $G < H$ we have the following:*

[12] The Fundamental Theorem of Projective Geometry (cf. [VeY] or [Di2] or [Art]) says that if $m > 2$ and $z : \mathcal{P}(V) \cup \mathcal{P}'(V) \to \mathcal{P}(\overline{V}) \cup \mathcal{P}'(\overline{V})$ is a bijection with $z(\mathcal{P}(V)) = \mathcal{P}(\overline{V})$ such that for any $P \in \mathcal{P}(V)$ and $P' \in \mathcal{P}'(V)$ we have $P \subset P' \Leftrightarrow z(P) \subset z(P')$, where $\overline{V}$ is an m-dimensional vector space over a field $\overline{k}$, then there exists an ϵ-linear isomorphism h of V onto $\overline{V}$, where $\epsilon : k \to \overline{k}$ is an isomorphism which is uniquely determined by z, such that z is induced by h. In the proof of (6.3.2) we are using this case when $\overline{k} = k$ and $\overline{V} = V$, whereas in the proof of (6.3.3) we shall be using this case when $\overline{k} = k$ and $\overline{V} = V'$.

[13] See the previous footnote.

(6.4.1) If H acts faithfully on a set D with $|D| \geq 3$, and G is 2-transitive on D, then $Z_H(G) = 1$.

(6.4.2) If $G \lhd H$, and $y \in Aut(H)$ is such that $y(g) = g$ for all $g \in G$, then for any $h \in H$, upon letting $\chi(h) = h^{-1}y(h)$, we have $y(h) = h\chi(h)$ with $\chi(h) \in Z_H(G)$, and $h \mapsto h\chi(h)$ gives a bijection $Z_H(G) \to Z_H(G)$.

(6.4.3) If $G \lhd H$ is such that $Z_H(G) = Z(H)$, and $y \in Aut(H)$ is such that $y(g) = g$ for all $g \in G$, then upon letting $\chi(h) = h^{-1}y(h)$ for all $h \in H$ we get a homomorphism $\chi : H \to Z(H)$ such that $h \mapsto h\chi(h)$ gives a bijection $Z(H) \to Z(H)$. Conversely, without any reference to the subgroup G, if $\chi : H \to Z(H)$ is any homomorphism such that $h \mapsto h\chi(h)$ gives a bijection $Z(H) \to Z(H)$ then, upon letting $y(h) = h\chi(h)$ for all $h \in H$, we get $y \in Aut(H)$.

(6.4.4) If $G \lhd H$ is such that $Z_H(G) = 1$, and $y \in Aut(H)$ is such that $y(g) = g$ for all $g \in G$, then $y(h) = h$ for all $h \in H$.

(6.4.5) If $SL(m,q) < G < H < \Gamma L(m,q)$, then $\Theta(H)$ acts faithfully on $\mathcal{P}(V)$, and $\Theta(G)$ is 2-transitive on $\mathcal{P}(V)$.

(6.4.6) If $SL(m,q) < G < H < \Gamma L(m,q)$, then $Z_{\Theta(H)}(\Theta(G)) = 1$.

(6.4.7) If $SL(m,q) < G \lhd H < \Gamma L(m,q)$ and $\eta \in Aut(\Theta(H))$ is such that $\eta(\phi) = \phi$ for all $\phi \in \Theta(G)$, then $\eta(\psi) = \psi$ for all $\psi \in \Theta(H)$.

(6.4.8) If $SL(m,q) < G < H < \Gamma L(m,q)$ and $y \in Aut(H)$ with $y(HL(m,q) \cap H) = HL(m,q) \cap H$ is such that $y(T) = T$, and $\eta(\phi) = \phi$ for all $\phi \in \Theta(G)$ where $\eta \in Aut(\Theta(H))$ is induced by y, then $y(g) = g$ for all $g \in SL(m,q)$.

To prove (6.4.1), we note that if H acts faithfully on a set D with $|D| \geq 3$, then given any $1 \neq h \in H$ we can find three distinct elements x_1, x_2, x_3 in D such that $h(x_1) = x_2$, and if G is 2-transitive on D, then for some $g \in G$ we have $g(x_1) = x_1$ and $g(x_2) = x_3$, and we get $(hg)(x_1) = x_2 \neq x_3 = (gh)(x_1)$ and hence $hg \neq gh$ and therefore $h \notin Z_H(G)$. This proves (6.4.1).

To prove (6.4.2) to (6.4.4), for a moment assume that $G \lhd H$, and let $y \in \mathrm{Aut}(H)$ be such that $y(g) = g$ for all $g \in G$. Now for any $h \in H$, upon letting $\chi(h) = h^{-1}y(h)$, we clearly have $y(h) = h\chi(h)$, and for any $g \in G$ we have $hgh^{-1} \in G$ and hence $hgh^{-1} = y(hgh^{-1}) = y(h)y(g)y(h)^{-1} = y(h)gy(h)^{-1}$ and therefore $hgh^{-1} = y(h)gy(h)^{-1}$ and hence $gh^{-1}y(h) = h^{-1}y(h)g$, i.e., $g\chi(h) = \chi(h)g$ and therefore $\chi(h) \in Z_H(G)$; it follows that $h \mapsto h\chi(h)$ gives a bijection $Z_H(G) \to Z_H(G)$. This proves (6.4.2). Moreover, if $Z_H(G) = Z(H)$, then for any h and h' in H we have $\chi(hh') = (hh')^{-1}y(hh') = h'^{-1}h^{-1}y(h)y(h') = h'^{-1}\chi(h)y(h') = \chi(h)h'^{-1}y(h') = \chi(h)\chi(h')$, and hence $\chi : H \to Z(H)$ is a homomorphism such that $h \mapsto h\chi(h)$ gives a bijection $Z(H) \to Z(H)$. Conversely, without any reference to the subgroup G, if $\chi : H \to Z(H)$ is any homomorphism, then, upon letting $y(h) = h\chi(h)$ for all $h \in H$, we see that for all h and h' in H we have $y(hh') = (hh')\chi(hh') = hh'\chi(h)\chi(h') = h\chi(h)h'\chi(h') = y(h)y(h')$, and hence $y : H \to H$ is a homomorphism; moreover if $h \mapsto h\chi(h)$ gives a bijection $Z(H) \to Z(H)$, then clearly $y \in \mathrm{Aut}(H)$. This proves (6.4.3). Finally, if $Z_H(G) = 1$, then for all $h \in H$, upon letting $\chi(h) = h^{-1}y(h)$, by (6.4.2) we get $y(h) = h\chi(h)$ with $\chi(h) \in Z_H(G)$ and hence $\chi(h) = 1$ and therefore $y(h) = h$. This proves (6.4.4).

Obviously $\mathrm{P\Gamma L}(m,q)$ acts faithfully on $\mathcal{P}(V)$, and by (3.6) on page 312 of [Suz] we know that $\mathrm{PSL}(m,q)$ is 2-transitive on $\mathcal{P}(V)$. This proves (6.4.5). By (6.4.1) and (6.4.5) we get (6.4.6). Obviously $|\mathcal{P}(V)| \geq 3$ and hence by (6.4.4) and (6.4.6) we get (6.4.7).

To prove (6.4.8), we note that if $\mathrm{SL}(m,q) < G < H < \Gamma L(m,q)$ and $y \in \mathrm{Aut}(H)$ with $y(\mathrm{HL}(m,q) \cap H) = \mathrm{HL}(m,q) \cap H$ is such that $y(T) = T$, and $\eta(\phi) = \phi$ for all $\phi \in \Theta(G)$ where $\eta \in \mathrm{Aut}(\Theta(H))$ is induced by y, then by Lemma (5.2) we see that $y(t) = t$ for all $t \in T$ and hence, because $\mathrm{SL}(m,q)$ is generated by T (cf. page 76 of [Suz]), we get $y(g) = g$ for all $g \in \mathrm{SL}(m,q)$. This proves (6.4.6).

We shall now prove the following sharpening of (6.4), where the action of a group G on a set D is said to be *pseudotransitive* if for every $x_1 \neq x_2$ in D there exists $g \in G$ with $g(x_1) = x_1$ and $g(x_2) \neq x_2$. Note that if $D \geq 3$, then 2-transitive $\Rightarrow$ pseudotransitive.

Lemma (6.5). *For any groups $G' < H'$ we have the following:*

(6.5.1) If H' acts faithfully on a set D, and G' is pseudotransitive on D, then $Z_{H'}(G') = 1$.

(6.5.2) If $m > 2$ and $SL(m,q) < G < \Gamma L(m,q)$ with $\widehat{\pi}(\Theta(G)) = G' < H' < PQL(m,q)$, then H' acts faithfully on $\mathcal{P}(V) \cup \mathcal{P}'(V)$, and G' is pseudotransitive on $\mathcal{P}(V) \cup \mathcal{P}'(V)$.

(6.5.3) If $m > 2$ and $SL(m,q) < G < \Gamma L(m,q)$ with $\widehat{\pi}(\Theta(G)) = G' < H' < PQL(m,q)$, then $Z_{H'}(G') = 1$.

(6.5.4) If $m > 2$ and $SL(m,q) < G < \Gamma L(m,q)$ with $\widehat{\pi}(\Theta(G)) = G' \triangleleft H' < PQL(m,q)$, and $\eta \in Aut(H')$ is such that $\eta(\phi) = \phi$ for all $\phi \in G'$, then $\eta(\psi) = \psi$ for all $\psi \in H'$.

To prove (6.5.1), we note that if H' acts faithfully on a set D, then given any $1 \neq h \in H'$ we can find $x_1 \neq x_2$ in D such that $h(x_1) = x_2$, and if G' is pseudotransitive on D, then for some $g \in G$ we have $g(x_1) = x_1$ and $g(x_2) \neq x_2$, and we get $(hg)(x_1) = x_2 \neq g(x_2) = (gh)(x_1)$ and hence $hg \neq gh$ and therefore $h \neq Z_{H'}(G')$. This proves (6.5.1).

To prove (6.5.2) assume that $m > 2$. Now there is a natural bijection between $\mathcal{P}'(V)$ and $\mathcal{P}(V')$, and hence there is a natural faithful action of $\mathrm{PQL}(m,q)$ on $\mathcal{P}(V) \cup \mathcal{P}'(V)$, which (by restriction) induces a natural faithful action of H' on $\mathcal{P}(V) \cup \mathcal{P}'(V)$. By (3.6) on page 312 of [Suz] we know that $\mathrm{PSL}(m,q)$ is 2-transitive on $\mathcal{P}(V)$, and hence given any $P_1 \neq P_2$ in $\mathcal{P}(V)$ there exists $\phi \in \mathrm{PSL}^{\pi}(m,q)$ with $\phi(P_1) = P_1$ and $P_2 \neq \phi(P_2) \in \mathcal{P}(V)$. By (3.6) on page 312 of [Suz] it follows that $\mathrm{PSL}(m,q)$ is 2-transitive on $\mathcal{P}'(V)$, and hence given any $P_1' \neq P_2'$ in $\mathcal{P}'(V)$ there exists $\phi \in \mathrm{PSL}^{\pi}(m,q)$ with $\phi(P_1') = P_1'$ and $P_2' \neq \phi(P_2') \in \mathcal{P}'(V)$. Finally, given any $P_1 \in \mathcal{P}(V)$ and $P_2' \in \mathcal{P}'(V)$, first we can find P_2 and P_3 in $\mathcal{P}(V)$ such that $P_1 \neq P_2 \subset P_2'$ and $P_1 \neq P_3 \not\subset P_2'$, and then, since $\mathrm{PSL}(m,q)$ is 2-transitive on $\mathcal{P}(V)$, we can find $\phi \in \mathrm{PSL}^{\pi}(m,q)$ such that $\phi(P_1) = P_1$ and $\phi(P_2) = P_3$, and hence $P_2' \neq \phi(P_2') \in \mathcal{P}'(V)$. Thus $\mathrm{PSL}^{\pi}(m,q)$ is pseudotransitive on $\mathcal{P}(V) \cup \mathcal{P}'(V)$, and hence so is G'. This proves (6.5.2). By (6.5.1) and (6.5.2) we get (6.5.3). Likewise by (6.5.5) and (6.5.3) we get (6.5.4).

Note that for any group G with $\mathrm{SL}(m,q) < G < \mathrm{GL}(m,q)$ we have $G \triangleleft \Gamma\mathrm{L}(m,q)$ and $\pi(G) \triangleleft \mathrm{QL}(m,q)$.[14] As a consequence of Lemma (5.14), Lemma (5.17), and Proposition (6.3), we shall now prove Lemma (6.6) below, which subsumes the **Automorphism Lemma (1.3)** stated in the Introduction.

[14] As noted in Definition (6.1), $\mathrm{GL}(m,q) \triangleleft \Gamma\mathrm{L}(m,q)$ and $\mathrm{GL}^{\pi}(m,q) \triangleleft \mathrm{QL}(m,q)$. Likewise, as noted in the proof of Lemma (4.2), $p(\mathrm{GL}(m,q)) = \mathrm{SL}(m,q)$ and hence $\mathrm{SL}(m,q)$ is a characteristic subgroup of $\mathrm{GL}(m,q)$. Since $\mathrm{GL}(m,q)/\mathrm{SL}(m,q)$ is a finite cyclic group, it follows that every G with $\mathrm{SL}(m,q) < G < \mathrm{GL}(m,q)$ is a characteristic subgroup of $\mathrm{GL}(m,q)$, and hence for it we have $G \triangleleft \Gamma\mathrm{L}(m,q)$ and $\pi(G) \triangleleft \mathrm{QL}(m,q)$.

Lemma (6.6). *For any group G with $SL(m,q) < G < GL(m,q)$, and any $\eta \in Aut(\Theta(G))$, we have the following:*

(6.6.1) If $m = 2$, then there exists $h \in \Gamma L(m,q)$ such that upon letting $\psi = \Theta(h)$ we have $\eta(\phi) = \psi\phi\psi^{-1}$ for all $\phi \in \Theta(G)$, and hence η is induced by $y \in Aut(G)$ defined by putting $y(g) = hgh^{-1}$ for all $g \in G$.

(6.6.2) If $m > 2$, then there exists $h \in QL(m,q)$ such that upon letting $\psi = \Theta_Q(h)$ we have $\eta(\phi) = \widehat{\pi}^*(\psi\phi^\pi\psi^{-1})$ for all $\phi \in \Theta(G)$, and hence η is induced by $y \in Aut(G)$ defined by putting $y(g) = \pi^*(hg^\pi h^{-1})$ for all $g \in G$.

Namely, if $m = 2$, then by (5.14) and (5.17.8) we see that there exists $z \in \mathrm{Sym}(\mathcal{P}(V))$ such that for all $P \in \mathcal{P}(V)$ we have $\eta(\widehat{T}(P)) = \widehat{T}(z(P))$, and therefore by (6.3.1) there exists $h \in \Gamma\mathrm{L}(m,q)$ such that upon letting $\psi = \Theta(h)$ we have $\eta(\phi) = \psi\phi\psi^{-1}$ for all $\phi \in \Theta(G)$, and hence η is induced by $y \in \mathrm{Aut}(G)$ defined by putting $y(g) = hgh^{-1}$ for all $g \in G$. This proves (6.6.1).

Likewise, if $m > 2$, then by (5.14) and (5.17.8) we see that there exists $z \in \mathrm{Sym}(\mathcal{P}(V) \cup \mathcal{P}'(V))$ such that for all $P \in \mathcal{P}(V)$ we have $\eta(\widehat{T}(P)) = \widehat{T}(z(P))$ or $\eta(\widehat{T}(P)) = \widehat{T}'(z(P))$ accordingly as $z(P) \in \mathcal{P}(V)$ or $z(P) \in \mathcal{P}'(V)$, and for all $P' \in \mathcal{P}'(V)$ we have $\eta(\widehat{T}'(P')) = \widehat{T}(z(P'))$ or $\eta(\widehat{T}'(P')) = \widehat{T}'(z(P'))$ accordingly as $z(P') \in \mathcal{P}(V)$ or $z(P') \in \mathcal{P}'(V)$, and therefore by (6.3.2) and (6.3.3) there exists $h \in \mathrm{QL}(m,q)$ such that upon letting $\psi = \Theta_Q(h)$ we have $\eta(\phi) = \widehat{\pi}^*(\psi\phi^\pi\psi^{-1})$ for all $\phi \in \Theta(G)$, and hence η is induced by $y \in \mathrm{Aut}(G)$ defined by putting $y(g) = \pi^*(hg^\pi h^{-1})$ for all $g \in G$. This proves (6.6.2).

Note that if $G \lhd H$ are groups, then any $h \in H$ gives the automorphism of G which sends every $g \in G$ to its h-conjugate hgh^{-1}; this gives a *natural homomorphism* $H \to \mathrm{Aut}(G)$; for instance in the situation of (6.6) we have a natural homomorphism $\mathrm{P\Gamma L}(m,q) \to \mathrm{Aut}(\Theta(G))$. More generally, if $G \lhd H$ are groups and $\omega : H \to \widetilde{H}$ is a group monomorphism with $\omega(G) \lhd \widetilde{H}$, then any $\widetilde{h} \in \widetilde{H}$ gives the automorphism of G which sends every $g \in G$ to $\omega^*(\widetilde{h}g^\omega\widetilde{h}^{-1})$, where for every $h \in H$ we are putting $h^\omega = \omega(h)$ and where $\omega^* : \omega(H) \to H$ is the isomorphism defined by putting $\omega^*(h^\omega) = h$ for all $h \in H$;[15] for instance, if $m > 2$, then in the situation of (6.6) we get a natural homomorphism $\mathrm{PQL}(m,q) \to \mathrm{Aut}(\Theta(G))$. As a consequence of Lemmas (6.4) to (6.6) we shall now prove the following:

Automorphism Theorem (6.7). *For any group G with $SL(m,q) < G < GL(m,q)$ we have the following:*

(6.7.1) If $m = 2$, then the natural homomorphism $P\Gamma L(m,q) \to Aut(\Theta(G))$ is an isomorphism.

(6.7.2) If $m > 2$, then the natural homomorphism $PQL(m,q) \to Aut(\Theta(G))$ is an isomorphism.

Namely, the surjectivity of the said natural homomorphism follows from Lemma (6.6), and its injectivity follows from Lemmas (6.4.6) and (6.5.3).

Remark (6.8). Thus we have deduced the Automorphism Theorem from the Automorphism Lemma by using Lemmas (6.4.6) and (6.5.3). Moreover, the general case of the Automorphism Theorem can be deduced from the special case of $\mathrm{Aut}(\mathrm{PSL}(m,q))$ by using Lemmas (6.4.7) and (6.5.4). Most of the proofs of the Automorphism Theorem available in the literature (cf. [Car] or [ScW] or [Ste]) only deal with the said special case. As we shall make explicit elsewhere, in the context

[15]Note that in h^ω the action is from the left in spite of appearances.

of (6.7), the rest of Lemmas (6.4) and (6.5) can be used for describing $\mathrm{Aut}(G)$ in terms of $\mathrm{Aut}(\Theta(G))$.

Remark (6.9). As observed in Remark (5.16), the assumption of k being a finite field was not used in Section 5 until Lemma (5.17). Also observe that the assumption of k being a finite field was not used in Section 6 until Lemma (6.6). Elsewhere we shall show that appropriate versions of the relevant parts of Lemma (5.17), and hence appropriate versions of the Automorphism Lemma and the Automorphism Theorem remain valid over any field.

Remark (6.10). To see how some of the material of Section 6, say items (6.1), (6.6) and (6.7), would look in the language of matrices, in this Remark, let us think of V as consisting of column vectors and $\mathrm{GL}(m,q)$ as a subset of the set of all $m \times m$ matrices $a = (a_{ij})$ over k which act on the column vectors by left multiplication.

Now let us explicitly describe the groups $\mathrm{HL}(m,q)$, $\Gamma\mathrm{L}(m,q)$ and $\mathrm{QL}(m,q)$ introduced in Definition (6.1), and in terms of them describe the automorphisms discussed in Lemma (6.6) and Theorem (6.7). First note that, in the explicit description, $\mathrm{HL}(m,q)$ consists of all $m \times m$ nonsingular scalar matrices over k.

Turning to $\Gamma\mathrm{L}(m,q)$, given any $\sigma \in \mathrm{Aut}(k)$, for every $\lambda \in k$ let λ^σ denote the image of λ under σ, and for every matrix $d = (d_{ij})$ over k let $d^\sigma = (d_{ij}^\sigma)$, and note that then for every $v = \lambda_1 e_1 + \cdots + \lambda_m e_m \in V$ with $\lambda_1, \ldots, \lambda_m$ in k we have $v^\sigma = \lambda_1^\sigma e_1 + \cdots + \lambda_m^\sigma e_m \in V$, and for every $g = (g_{ij}) \in \mathrm{GL}(m,q)$ we have $g^\sigma = (g_{ij}^\sigma) \in \mathrm{GL}(m,q)$. Now we may regard $\Gamma\mathrm{L}(m,q)$ as consisting of all pairs (g,σ) where $g = (g_{ij}) \in \mathrm{GL}(m,q)$ and $\sigma \in \mathrm{Aut}(k)$, with its action on V given by $(g,\sigma)v = gv^\sigma$. For any other (h,τ) in $\Gamma\mathrm{L}(m,q)$ we have $(h,\tau)((g,\sigma)v) = (h,\tau)(gv^\sigma) = hg^\tau v^{\tau\sigma}$ and hence $(h,\tau)(g,\sigma) = (hg^\tau, \tau\sigma)$. It follows that $(h,\tau)^{-1} = ((h^{-1})^{\tau^{-1}}, \tau^{-1})$ and hence $(h,\tau)(g,\sigma)(h,\tau)^{-1} = (hg^\tau(h^{-1})^{\tau\sigma\tau^{-1}}, \tau\sigma\tau^{-1})$. In particular, taking $\sigma = 1 \in \mathrm{Aut}(k)$, we get $(h,\tau)(g,1)(h,\tau)^{-1} = (hg^\tau h^{-1}, 1)$.

Finally, turning to $\mathrm{QL}(m,q)$, for any matrix $d = (d_{ij})$ let $d^\dagger = (d_{ij}^\dagger)$ be the transpose of d given by $d_{ij}^\dagger = d_{ji}$, and for every $g \in \mathrm{GL}(m,q)$ then let $g^\natural$ be the inverse-transpose of g, i.e., $g^\natural = (g^{-1})^\dagger = (g^\dagger)^{-1} \in \mathrm{GL}(m,q)$. Let us think of V' as consisting of row vectors, and let $(e_1', \ldots, e_m')$ be the basis of V' dual to $(e_1, \ldots, e_m)$, i.e., for $1 \le i \le m$, let e_i' be the row vector with 1 in the i-th place and zeroes elsewhere, and note that then in terms of the Kronecker delta we have $e_i' e_j = \delta_{ij}$, and hence for all $v = \lambda_1 e_1 + \cdots + \lambda_m e_m \in V$ and $v' = \lambda_1' e_1' + \cdots + \lambda_m' e_m' \in V'$ with $\lambda_1, \ldots, \lambda_m, \lambda_1', \ldots, \lambda_m'$ in k we have $v'v = \lambda_1'\lambda_1 + \cdots + \lambda_m'\lambda_m \in k$ giving the action of V on V'. We may regard $\Gamma\mathrm{L}(V \oplus V') = \Gamma\mathrm{L}(2m,q)$ as consisting of all pairs (R,σ) where $R \in \mathrm{GL}(2m,q)$ and $\sigma \in \mathrm{Aut}(k)$, with its action on $V \oplus V'$ given by $(R,\sigma)w = Aw^\sigma$ where $w = (v^\dagger, v')^\dagger \in V \oplus V'$ with $v \in V$ and $v' \in V'$, and then for any other $(S,\tau) \in \Gamma\mathrm{L}(2m,q)$, by the above calculation, we get $(S,\tau)(R,\sigma) = (SR^\tau, \tau\sigma)$ and $(S,\tau)(R,1)(S,\tau)^{-1} = (SR^\tau S^{-1}, 1)$. For every $R \in \mathrm{GL}(2m,q)$, let us write $R = (R_{ij})$ where R_{ij} is an $m \times m$ matrix over k for $1 \le i \le 2$ and $1 \le j \le 2$. For every $g \in \mathrm{GL}(m,q)$, let $R(g) \in \mathrm{GL}(2m,q)$ be such that $R(g)_{11} = g$ and $R(g)_{22} = g^\natural$ and $R(g)_{12} = R(g)_{21} = 0$, let $S(g) \in \mathrm{GL}(2m,q)$ be such that $S(g)_{12} = g$ and $S(g)_{21} = g^\natural$ and $S(g)_{11} = S(g)_{22} = 0$, and note that then $S(g) = R(g)J$ with $J^2 = 1$ where $J \in \mathrm{GL}(2m,q)$ is given by $J_{12} = J_{21} = 1$ and $J_{11} = J_{22} = 0$. Now we identify $\Gamma\mathrm{L}^\pi(m,q)$ with the set of all $(R(g),\sigma) \in \Gamma\mathrm{L}(2m,q)$ with g varying in $\mathrm{GL}(m,q)$, and we identify $\mathrm{QL}(m,q) \setminus \Gamma\mathrm{L}^\pi(m,q)$ with the set of all $(S(g),\sigma) \in \Gamma\mathrm{L}(2m,q)$ with g varying in $\mathrm{GL}(m,q)$. Note

that then $\mathrm{GL}^\pi(m,q) = \{(R(g),1) : g \in \mathrm{GL}(m,q)\}$. Moreover, given any $(R(g),1)$ in $\mathrm{GL}^\pi(m,q)$, for every $(R(h),\tau) \in \Gamma\mathrm{L}^\pi(m,q)$ we have $(R(h),\tau)(R(g),1)(R(h),\tau)^{-1} = (R(hg^\tau h^{-1}),1) \in \mathrm{GL}^\pi(m,q)$, and for every $(S(h),\tau) \in \mathrm{QL}(m,q) \setminus \Gamma\mathrm{L}^\pi(m,q)$ we have $(S(h),\tau)(R(g),1)(S(h),\tau)^{-1} = (R(h(g^\natural)^\tau h^{-1}),1) \in \mathrm{GL}^\pi(m,q)$.

References

[Ab1] S. S. Abhyankar, *Nice equations for nice groups*, Israel Journal of Mathematics **88** (1994), 1-24. MR **96f:**12003

[Ab2] S. S. Abhyankar, *Projective polynomials*, Proceedings of the American Mathematical Society **125** (1997), 1643-1650. MR **98a:**12001

[Ab3] S. S. Abhyankar, *Galois theory of semilinear transformations*, London Math. Soc. Lecture Note Ser., 256, Cambridge Univ. Press, Cambridge, 1999. CMP 2000:01

[Art] E. Artin, *Geometric Algebra*, Interscience, 1957. MR **18:**553e

[Car] R. W. Carter, *Simple Groups of Lie Type*, Wiley, 1977.

[Dem] P. Dembowski, *Finite Geometries*, Springer-Verlag, 1968. MR **97i:**51005

[Di1] J. Dieudonné, *On the Automorphisms of the Classical Groups*, Memoirs of the American Mathematical Society No. 2, 1951. MR **13:**531a

[Di2] J. Dieudonné, *La Géométrie des Groupes Classiques*, Springer-Verlag, 1955. MR **17:**236a

[Hu1] L. K. Hua, *On the automorphisms of the symplectic group over any field*, Annals of Mathematics **49** (1948), 739-759. MR **10:**352e

[Hu2] L. K. Hua, *Supplement to Dieudonné's book On the Automorphisms of the Classical Groups*, Memoirs of the American Mathematical Society No. 2, 1951, pp. 96-122. MR **82c:**20079

[ScW] O. Schreier and B. L. van der Waerden, *Die Automorphismen der projectiven Gruppen*, Abhand. Math. Seminar Univ. Hamburg **6** (1928), 303-322.

[Ste] R. Steinberg, *Automorphisms of finite linear groups*, Canadian Journal of Mathematics **12** (1960), 606-615. MR **22:**12165

[Suz] M. Suzuki, *Group Theory I*, Springer-Verlag, 1982. MR **82k:**20001c

[VeY] O. Veblen and J. W. Young, *Projective Geometry, Vols. I and II*, Ginn and Company, 1910-1918.

Department of Mathematics, Purdue University, West Lafayette, Indiana 47907
E-mail address: ram@cs.purdue.edu