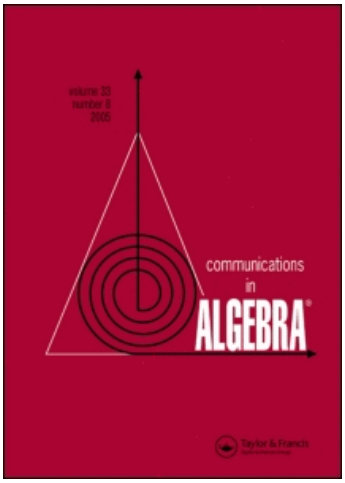

Communications in Algebra
Publication details, including instructions for authors and subscription information:
http://www.informaworld.com/smpp/title~content=t713597239

Sets of Transvections Generating Subgroups Isomorphic to Special Linear Groups

L. Di Martino [a]; A. Previtali [b]; R. Radina [c]
[a] Dipartimento di Matematica e Applicazioni, Università Degli Studi di Milano-Bicocca, Milano, Italy [b] Dipartimento di Fisica e Matematica, Università dell'Insubria, Como, Italy [c] Dipartimento di Matematica, Università degli Studi di Milano, Milano, Italy

To cite this Article Martino, L. Di, Previtali, A. and Radina, R.'Sets of Transvections Generating Subgroups Isomorphic to Special Linear Groups', Communications in Algebra, 33: 6, 1663 — 1691
To link to this Article: DOI: 10.1081/AGB-200058379
URL: http://dx.doi.org/10.1081/AGB-200058379

Communications in Algebra®, 33: 1663–1691, 2005

ISSN: 0092-7872 print/1532-4125 online
DOI: 10.1081/AGB-200058379

Taylor & Francis
Taylor & Francis Group

SETS OF TRANSVECTIONS GENERATING SUBGROUPS ISOMORPHIC TO SPECIAL LINEAR GROUPS[#]

L. Di Martino
Dipartimento di Matematica e Applicazioni, Università Degli Studi di Milano-Bicocca, Milano, Italy

A. Previtali
Dipartimento di Fisica e Matematica, Università dell'Insubria, Como, Italy

R. Radina
Dipartimento di Matematica, Università degli Studi di Milano, Milano, Italy

The main result of this paper is a graph-theoretic necessary and sufficient condition, for a given set of transvections in $SL(n, K)$ ($n > 2$ and K a finite field of characteristic not 2 or 3), to generate a group isomorphic to $SL(m, L)$, for some m and some subfield L of K.

Key Words: Digraphs; Special linear groups; Transvections.

1991 Mathematics Subject Classification: 20G40; 05C25; 05C50.

1. INTRODUCTION

There is a rich literature on groups generated by transvections (elations) in linear (projective) spaces. In particular, the irreducible linear groups generated by transvections over a finite field of odd characteristic were completely classified in the 70s by Wagner (1974) and (independently) by Zalesskii and Serežkin (1976). The even characteristic case was dealt with in McLaughlin (1967); Piper (1966); Wagner (1974) and Pollatsek (1976) (with the exception of the case where each axis arises from a unique transvection). Finally, in 1979 these results found their place as special cases of the classification of subgroups of classical groups generated by long root elements (Kantor, 1979).

In the early 80s Brown and Humphries wrote several papers (Brown and Humphries, 1986a,b; Humphries, 1985, 1986, 1987), in which they introduced a graph-theoretic approach to the study of groups generated by transvections. However, it should be emphasized that whenever Brown and Humphries speak of

Received January 2004; Accepted March 2004
[#]Communicated by A. Facchini.
Address correspondence to L. Di Martino, Dipartimento di Matematica e Applicazioni, Università Degli Studi di Milano-Bicocca, via Bicocca degli Arcimboldi 8, 20126 Milano, Italy; E-mail: lino.dimartino@unimib.it

"transvections," they actually mean "root subgroups"; that is, their results concern generation by parameter subgroups R_t, where t ranges over a finite set U of transvections in $SL(n, K)$ (cfr. 2. below). Secondly, Brown and Humphries generally assume from the start that the subgroup $\langle R_t \mid t \in U \rangle$ acts irreducibly on the column space K^n. In Brown and Humphries (1986a,b), the sets of "transvections" (over an arbitrary field) generating the symplectic group are classified in graph-theoretic terms, while in Humphries (1986) the sets of n "transvections" generating $SL(n, K)$, where K is a finite field, are classified. Finally, the main result in Humphries (1987) describes the key options for the graph associated to an irreducible group generated by root subgroups, thus allowing recognition procedures for such a group. In this paper, we consider instead transvections in strict sense, and look for conditions to be imposed on a set of transvections in $SL(n, K)$, K a finite field of characteristic p, in order to generate a subgroup isomorphic to a special linear group (possibly modulo a normal p-subgroup) without any preventive assumption on the generated subgroup. Furthermore, while working with full root subgroups allows one to obtain characteristic-free results, dealing with single transvections means that Dickson's Lemma comes into play (see Sec. 6). This is why our main result (Main Theorem, Sec. 9) applies to fields of odd characteristic. Nevertheless, many intermediate results, also of independent interest, work for any characteristic.

As the proof of our Main Theorem is obtained via a finite procedure, the present paper offers in principle an algorithm recognizing whether or not a given set of transvections generates a group isomorphic to a special linear group.

2. GENERALITIES ON TRANSVECTIONS

Let K be a finite field of characteristic p. We denote by K^n the space of column vectors of size n over K, and by ${}^nK$ the space of row vectors of size n over K. Then the group $GL(n, K)$ of invertible $n \times n$ matrices over K acts in the obvious way on the left on K^n and on the right on ${}^nK$. Suppose $n \geq 1$. A non-identity linear transformation $t : K^n \to K^n$ is a *transvection* if it has the form $t = \mathrm{Id} + c(t)a(t)$, where $a(t) \in {}^nK$, $c(t) \in K^n$ and $a(t)c(t) = 0$. It is clear that t has order p and $t^{-1} = \mathrm{Id} - c(t)a(t)$ is again a transvection. The 1-dimensional subspace of K^n generated by $c(t)$ is called the *centre* of t, while the hyperplane of K^n defined by $a(t)$, that is the set of all $x \in K^n$ such that $a(t)x = 0$, is called the *axis* of t (so, the centre of t lies on the axis of t). Obviously, t determines $a(t)$ and $c(t)$ only up to a scalar multiple: more precisely, for any $\zeta \in K^*$, we can replace $a(t)$ and $c(t)$ by $a_1(t) = \zeta a(t)$ and $c_1(t) = \zeta^{-1}c(t)$. Observe that the conjugate of a transvection is again a transvection. Namely, if $g \in GL(n, K)$ and $t = \mathrm{Id} + c(t)a(t)$, then $t^g = g^{-1}tg = \mathrm{Id} + (g^{-1}c(t))(a(t)g)$, a transvection with centre defined by $g^{-1}c(t)$ and axis defined by $a(t)g$. Let (e_i) and (e'_i) be the standard bases of K^n and ${}^nK$, respectively. For $i \neq j \in [n]$, $\xi \in K^*$, set $T_{ij}(\xi) = \mathrm{Id} + \xi E_{ij}$, where $E_{ij} = e_i e'_j$ is the so-called elementary $n \times n$-matrix, having 1 in position (i, j) and zeros elsewhere. Thus $T_{ij}(\xi)$ is a transvection with centre $\langle e_i \rangle$ and axis defined by e'_j. We call any such $T_{ij}(\xi)$ an *elementary transvection*. By the above, it is clear that any given transvection t is conjugated under $GL(n, K)$ to an elementary transvection. In particular, all transvections have determinant 1, i.e., belong to the *special linear group* $SL(n, K)$. Furthermore, it is well known that the transvections form a single conjugacy class within $SL(n, K)$, unless $n = 2$ and $K^2 \neq K$. For a transvection $t = \mathrm{Id} + c(t)a(t)$, we

set $R_t = \{\mathrm{Id} + \delta c(t)a(t) \mid \delta \in K\}$. Clearly R_t is a subgroup of $SL(n, K)$ isomorphic to the additive group $(K, +)$ of the field K. We say that R_t is the *root subgroup* relative to t. In particular, if $t = T_{ij}(\xi)$, we set $R_{T_{ij}(\xi)} = R_{ij}$ and say that R_{ij} is an *elementary root subgroup*. [It is well known that $SL(n, K)$ is generated by its elementary root subgroups. Indeed, viewing $SL(n, K)$ as the simply connected group of Lie type $\mathbb{A}_{n-1}(K)$, the transvections $T_{ij}(\xi)$ are precisely the standard generators of $\mathbb{A}_{n-1}(K)$ associated to the elements of the canonical root system of type $\mathbb{A}_{n-1}$.]

3. SETS OF TRANSVECTIONS AND ASSOCIATED MATRICES AND DIGRAPHS

Let $U = \{t_1, \ldots, t_h\}$ denote a finite set of transvections of $GL(n, K)$, where (for later convenience) $t_1, \ldots, t_h$ are not necessarily supposed to be pairwise distinct (that is, strictly speaking, U is a finite multiset). For each $i \in [h]$, set $t_i = \mathrm{Id} + c(t_i)a(t_i)$. We associate to U the following three matrices:

$$A(U) = \begin{bmatrix} a(t_1) \\ a(t_2) \\ \cdots \\ a(t_h) \end{bmatrix}, \qquad C(U) = [c(t_1)\ c(t_2) \cdots c(t_h)], \qquad H(U) = A(U) \cdot C(U).$$

Thus, $H(U)$ is the $h \times h$ matrix whose (i, j) entry is $a(t_i)c(t_j)$. It was introduced by Humphries (1986). Obviously, $H(U)$ is not uniquely determined by U. Indeed, it depends on the chosen ordering of the elements of U, as well as on the chosen representatives $a(t_i)$, $c(t_i)$ for the axis and the centre of each t_i. However, it is easily seen that $\det H(U)$ is invariant with respect to a reordering of the elements of U and to any other choice of representatives for their axes and centres. We also observe that, by conjugating via $g \in GL(n, K)$, that is transforming the set $U = \{t_1, \ldots, t_h\}$ into the set $U^g = \{t_1^g, \ldots, t_h^g\}$, the matrices $A(U)$ and $C(U)$ are trasformed into the matrices $A(U)g$ and $g^{-1}C(U)$, respectively, and therefore $H(U) = H(U^g)$.

Following the graph-theoretic approach of Brown and Humphries, via the matrix $H(U)$ we can associate to the set U a simple arc-labelled digraph $\Gamma(U)$, defined as follows: the vertex set of $\Gamma(U)$ is U, and a vertex t_i is connected to a vertex t_j by an arc with label α iff $\alpha = a(t_i)c(t_j) \neq 0$. The nomenclature we are going to use from graph theory is fairly standard. In particular, a *path* $\mathbf{p}$ in $\Gamma(U)$ is understood to be an oriented path, that is a sequence of consecutive oriented arcs:

$$\mathbf{p} := t_{i_1} \xrightarrow{\alpha_1} t_{i_2} \xrightarrow{\alpha_2} \cdots \longrightarrow t_{i_{s-1}} \xrightarrow{\alpha_{s-1}} t_{i_s}.$$

$\mathbf{p}$ is said to be closed if $t_{i_1} = t_{i_s}$. As customary, we will say that $\Gamma(U)$ is (path)-*connected* if, for every ordered pair (t_i, t_j) of distinct elements of U, there is a path in $\Gamma(U)$ starting from t_i and ending in t_j. A path $\mathbf{p} := t_{i_1} \xrightarrow{\alpha_1} t_{i_2} \xrightarrow{\alpha_2} \cdots \longrightarrow t_{i_{s-1}} \xrightarrow{\alpha_{s-1}} t_{i_s}$ in $\Gamma(U)$ is said to be *simple* if its nodes are pairwise distinct, except possibly for being $t_{i_s} = t_{i_1}$. If $t_{i_s} \neq t_{i_1}$ the simple path $\mathbf{p}$ is also called an (open) *chain* (of length $s - 1$). If $s > 2$ and $t_{i_s} = t_{i_1}$, the closed path $\mathbf{p}$ is said to be a *cycle* (of length $s - 1$). By abuse of language, we will say that the digraph $\Gamma(U)$ is itself a chain (a cycle) when $U = \{t_1, \ldots, t_h\}$, the path $t_1 \xrightarrow{\alpha_1} t_2 \xrightarrow{\alpha_2} \cdots \longrightarrow t_{h-1} \xrightarrow{\alpha_{h-1}} t_h$ is a chain (a cycle), and there are no other arcs in $\Gamma(U)$.

Obviously, the labelling of the arcs of $\Gamma(U)$ depends on the choice of representatives for the axes and centres of the transvections t_i. However, it is important to observe that the product of the labels along any simple closed path in $\Gamma(U)$ is left invariant by a change of representatives. To see this, suppose that the path passes through the node t_i :

$$\cdots \longrightarrow t_j \xrightarrow{\alpha} t_i \xrightarrow{\beta} t_k \longrightarrow \cdots .$$

Upon replacing $a(t_i)$ and $c(t_i)$ with $\zeta a(t_i)$ and $\zeta^{-1}c(t_i)$, the labelling changes to:

$$\cdots \longrightarrow t_j \xrightarrow{\zeta^{-1}\alpha} t_i \xrightarrow{\zeta\beta} t_k \longrightarrow \cdots .$$

Clearly, as no other labels are involved, the label product on the closed path does not change. In particular it follows that, when considering a cycle in $\Gamma(U)$ with label product δ, we may always assume that one of the labels (arbitrarily chosen) equals δ, while all the other labels equal 1.

Remark. Suppose that, for $t_i, t_j \in U$, $a(t_i)c(t_j) = 0$, that is, there is no arc in $\Gamma(U)$ joining t_i to t_j. In this case, it will be sometimes convenient to say, alternatively, that t_i is connected to t_j by an arc with label 0. Likewise, we may wish to consider, instead of $\Gamma(U)$, the complete labelled digraph $\widehat{\Gamma}(U)$ obtained from $\Gamma(U)$ by adding all arcs $t_i \xrightarrow{0} t_j$ with label 0.

In proving our main theorem, a key role is played by the following concept, introduced in Humphries (1986):

Definition 1. $\Gamma(U)$ is said to be a one-way digraph if there are $t_i, t_j \in U$, such that the arc $t_i \longrightarrow t_j$ is present in $\Gamma(U)$, but the arc $t_j \longrightarrow t_i$ is not.

4. THE GEOMETRY OF PAIRS OF TRANSVECTIONS

We summarize in this section (and translate in terms of digraphs) some known facts concerning the geometric relationships that can occur between pairs of transvections. For the relevant proofs and further details, the reader can refer to Di Martino and Vavilov (1994, 1996) and the references quoted there.

4.1. Mutual Positions

Let s, t be two transvections in $SL(n, K)$ and denote by $a(s)$, $a(t)$ and $c(s)$, $c(t)$ their respective axes and centres. Furthermore, suppose that s and t do not have the same axis and centre (i.e., do not belong to the same root subgroup).

It is well known that there are only a few possibilities for the mutual positions of the axes and centres of s and t, corresponding to the angle θ between the corresponding roots in the root system $\mathbb{A}_{n-1}$. Namely, one of the following holds:

(a) $\theta = \pi$. In this case, s and t have distinct axes and centres and the centre of s (resp. t) does not lie on the axis of t (resp. s). This amounts to saying that $a(s)c(t)$ and $a(t)c(s)$ are both different from zero.
(b) $\theta = \pi/2$. Here again s and t have distinct axes and centres, but $a(s)c(t) = a(t)c(s) = 0$.

(c) $\theta = \pi/3$. Here two mutually dual cases arise: either s and t have the same centre and distinct axes, or s and t have the same axis and distinct centres. Here again $a(s)c(t) = a(t)c(s) = 0$.
(d) $\theta = 2\pi/3$. In this case, s and t have distinct axes and centres, and exactly one of the following holds: either the centre of t lies on the axis of s, or the centre of s lies on the axis of t.

The transvections s and t are called *opposite* in case (a) and *orthogonal* in case (b). s and t commute in cases (b) and (c), while the commutator $[s, t]$ is again a transvection in case (d). Namely, suppose that centre of s lies on the axis of t: then $[s, t] = sts^{-1}t^{-1} = \mathrm{Id} + \beta c(s)a(t)$, where $\beta = a(s)c(t)$. In case (d), we will say that s and t are *non-commuting*.

4.2. Orbits Under *GL*

Lemma 1 (e.g., see Di Martino and Vavilov, 1994, Lemma 9). *Any pair (s, t) of transvections is simultaneously conjugated to a pair of elementary transvections. In other words, there exists $g \in GL(n, K)$ such that $g^{-1}sg = T_{ij}(\xi)$, $g^{-1}tg = T_{hk}(\eta)$, for some $1 \le i, j, h, k \le n$; $i \ne j$; $h \ne k$; $\xi, \eta \in K$.*

In each of the cases listed in 4.1, the pair (s, t) is conjugate under the action of $GL(n, K)$ to a suitable pair of elementary transvections. More precisely, set $a(s)c(t) = \xi$ and $a(t)c(s) = \eta$. Then the following holds:

Case (a): (s, t) is conjugate to the pair $(T_{12}(\xi), T_{21}(\eta))$.
Case (b): (s, t) is conjugate to the pair $(T_{12}(\xi), T_{34}(\eta))$.
Case (c): Two subcases arise. The pair (s, t) is conjugate either to the pair $(T_{12}(\xi), T_{13}(\eta))$, or to the pair $(T_{21}(\xi), T_{31}(\eta))$. These two orbits are fused under $\mathrm{Aut}(GL(n, K))$.
Case (d): As in the previous case, two subcases arise. The pair (s, t) is conjugate either to the pair $(T_{12}(\xi), T_{23}(\eta))$, or to the pair $(T_{23}(\xi), T_{12}(\eta))$. The two orbits are fused under $\mathrm{Aut}(GL(n, K))$.

4.3. Associated Digraphs

The digraphs associated to the above configurations are as follows (omitting the labels):

Case (a): $\underset{s}{\bullet} \rightleftarrows \underset{t}{\bullet}$
Case (b): $\underset{s}{\bullet} \quad \underset{t}{\bullet}$
Case (c): $\underset{s}{\bullet} \quad \underset{t}{\bullet}$
Case (d): $\underset{s}{\bullet} \longrightarrow \underset{t}{\bullet}$ or $\underset{s}{\bullet} \longleftarrow \underset{t}{\bullet}$

5. CONJUGATING AND PARAMETER CHANGING: THE EQUIVALENCE RELATION $\approx$ AND THE DIGRAPH $\Gamma(\widetilde{U})$

Here and in the sequel of the paper, we will denote by $\mathcal{T}$ the set of all transvections in $SL(n, K)$. With a slight abuse of notation we will write $U \subseteq \mathcal{T}$

if U is a (multi) set consisting of elements of $\mathcal{T}$. As we are essentially concerned in recognizing the subgroup $\langle U\rangle$ generated by a set of transvections U, we are allowed to perform transformations on U, as long as $\langle U\rangle$ is left invariant. We are particularly interested in certain basic transformations, that we are going to describe in the next subsections.

Notation. In order to memorize computation rules and perform computations involving the aforementioned tranformations, it is convenient from now on to adopt the following notation: for a pair of transvections s, t in $SL(n, K)$, we write $s * t$ for $a(s)c(t)$. Thus $s * t$ is the label (possibly 0) of the arc $s \to t$ in $\widehat{\Gamma}(s, t)$.

5.1. Conjugating

For $s, t \in U$, we may either (i): add to U the conjugate $t^{-1}st = s^t$; (ii) replace s with s^t. Indeed, setting $U' = U \cup \{s^t\}$ in case (i), $U' = (U - \{s\}) \cup \{s^t\}$ in case (ii), it is clear that $\langle U'\rangle = \langle U\rangle$. It is important to observe that the labels of the arcs starting from and ending into s^t are obtained from those starting from and ending into s, t, according to the following rules:

Lemma 2. *Let* $r, s, t \in U$. *Then* $s^t * r = s * r + (s * t)(t * r)$ *and* $r * s^t = r * s - (r * t)(t * s)$.

Proof. Direct computations, using the fact that $a(s^t) = a(s) + (s * t)a(t)$ and $c(s^t) = c(s) - (t * s)c(t)$. □

Remark. A few extra words are helpful in illustrating the basic transformations of type (ii). We observe explicitly that in the statement of the above Lemma any of the labels involved may equal zero. Thus the lemma shows that replacing U with U' may result in adding arcs to, or removing arcs from the digraph we started with. In particular: if $s * r = -(s * t)(t * r)$ (resp. $r * s = (r * t)(t * s)$), replacing s with s^t results in deleting the arc joining s to r (resp. r to s).

Definition 2. We denote by $\widetilde{U}$ the closure of U under conjugation within $\langle U\rangle$, that is: $\widetilde{U} = \{t^h \mid t \in U,\ h \in \langle U\rangle\}$.

Obviously, $\langle U\rangle = \langle \widetilde{U}\rangle$ and $\widetilde{\widetilde{U}} = \widetilde{U}$.

5.2. Parameter Changing: The Subfields $\underline{L}$ and $\overline{L}$

For a transvection $t = \mathrm{Id} + c(t)a(t)$ and for $\lambda \in K$, we set $t^\lambda = \mathrm{Id} + \lambda c(t)a(t) = \mathrm{Id} + \lambda(t - \mathrm{Id})$. Clearly, $(t^\lambda)^s = (t^s)^\lambda$ and $(t^\lambda)^\mu = t^{\lambda\mu}$ for every $s \in GL(n, K)$ and every $\lambda, \mu \in K$. For a subset J of K, we set $t^J = \{t^\lambda \mid \lambda \in J\}$. In particular: $t^K = R_t$, the root subgroup relative to t. More generally, for any $U = \{t_1, \ldots, t_h\} \subseteq \mathcal{T}$, we denote by $\langle U\rangle^J$ the subgroup $\langle t_1^J, \ldots, t_h^J\rangle$.

It is also convenient, for computational purposes, to introduce a "normalization rule": that is, we will always assume that $a(t^\lambda) = \lambda a(t)$ (and hence, $c(t^\lambda) = c(t)$). Thus, if (say) $t * s = \alpha$, then $(t^\lambda) * s = \lambda\alpha$.

Given $U \subseteq \mathcal{T}$ and chosen $t \in U$, $\lambda \in K$, one cannot guarantee, in general, that $t^\lambda \in \langle U\rangle$. However, for our purposes it will be enough to make sure that the latter

property holds for certain choices of λ. This, as well as the very statement of our Main Theorem, leads us to define two subfields of K associated to $\widetilde{U}$.

Definition 3. We will denote by $\overline{L}(U)$ (resp. $\overline{L}(\widetilde{U})$) the subfield of K generated by the label products taken along all closed paths in $\Gamma(U)$ (resp. $\Gamma(\widetilde{U})$). The subfield of $\overline{L}(U)$ (resp. $\overline{L}(\widetilde{U})$) generated by the label products taken along all cycles of length 2 will be denoted by $\underline{L}(U)$ (resp. $\underline{L}(\widetilde{U})$). (Here it is understood that $\underline{L}(U)$ coincides with the prime subfield of K if there are no cycles of length 2 in $\Gamma(U)$. Similarly for the other relevant subfields of K.)

As we shall see, the following holds:

Proposition 1. *Let* $char(K) = p \neq 2, 3$. *Suppose that* $\Gamma(U)$ *is connected,* $t \in \widetilde{U}$ *and* $\lambda \in \underline{L}(\widetilde{U})$. *Then* $t^{\lambda} \in \langle U \rangle$.

The proof of the above proposition, however, is far from direct. It relies on several auxiliary results and will only be at hand in Sec. 7.

We close this section observing that $\overline{L}(U)$ is the "right" field to consider when dealing with the group $\langle U \rangle$, in the sense that it is the smallest subfield of K on which $\langle U \rangle$ can be written. More precisely: $\langle U \rangle$ can be realized over $\overline{L}(U)$, and if F is a subfield of K such that $\langle U \rangle$ can be conjugated into a subgroup of $SL(n, F)$, then $F \supseteq \overline{L}(U)$. This is shown by proving that the label products in $\Gamma(U)$ are integer linear combinations of traces of elements of $\langle U \rangle$ (and conversely).

First of all, for a pair of transvections s, t we define

$$\ell(s, t) = (s * t)(t * s),$$

and generalize to any finite list of transvections $(t_1, \ldots, t_r)$ setting

$$\ell(t_1, t_2, \ldots, t_r) = (t_1 * t_2) \cdots (t_{r-1} * t_r)(t_r * t_1).$$

Let $U = \{t_1, \ldots, t_h\}$. For $k \in \mathbb{N}$ set $I \in [h]^k$. A sublist J of I is a list obtained upon deleting some elements from I. Writing $J \preceq I$, we consider the poset $(I, \preceq)$. For a sublist J of I, set $t_J = \prod_{j \in J} t_j$ and $\ell_J = \ell((t_j)_{j \in J})$, where the product is taken in ascending order. Then the following holds:

Proposition 2. $\mathrm{Tr}(t_I) = \sum_{J \preceq I} \ell_J$ *and* $\ell_I = (-)^k \sum_{J \preceq I} (-)^{|J|} \mathrm{Tr}(t_J)$, *where* $k = |I|$.

Proof. We proceed by induction on k. Set $t_i = 1 + c_i a_i$, $i \in I$. Then $t_I = \sum_{J \preceq I} \prod_{j \in J} c_j a_j$, where the product of length 0 is taken to be the identity. Furthermore, as $ac = \mathrm{Tr}(ac) = \mathrm{Tr}(ca)$ for any $a \in^n K$ and $c \in K^n$, $\ell_J = \mathrm{Tr}(\prod_{j \in J} c_j a_j)$. Thus $\mathrm{Tr}(t_I) = \sum_{J \preceq I} \ell_J$. Applying the Moebius inversion formula to $(I, \preceq)$, we get $\ell_I = \sum_{J \preceq I} \mu(J) \mathrm{Tr}(t_J)$. Since $(I, \preceq)$ is isomorphic to $([k], \subseteq)$, $(-)^k \mu(J) = (-)^{|J|}$. □

Corollary 1. *Let* $U = \{t_1, \ldots, t_h\}$. *Then, up to conjugation,* $\langle U \rangle$ *can be embedded in* $SL(n, \overline{L}(U))$.

Proof. By the previous proposition, $\overline{L}(U) = \mathbb{F}_p\big[\{\mathrm{Tr}(g) \mid g \in \langle U \rangle\}\big]$. Since the Schur index of a representation over a finite field is 1, the result follows. □

6. THE CYCLIC CASE: A GENERALIZATION OF DICKSON'S LEMMA

Let $char(K) = p$, and denote by $\mathbb{F}_p$ the prime subfield of K. For $\delta \in K$ denote by $\mathbb{F}_p[\delta]$ the subfield of K generated by δ. The following classical result was first proved about one hundred years ago by Dickson:

Lemma 3 (Dickson's Lemma). *Assume* $char(K) = p \neq 2$, $|K| \neq 9$ *and* $K = \mathbb{F}_p[\delta]$. *Then* $\langle \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 1 & 0 \\ \delta & 1 \end{smallmatrix}\right] \rangle = SL(2, K)$.

Corollary 2. *Assume* $char(K) = p \neq 2$ *and* $|K| \neq 9$. *Let* s, t *be opposite trans vections of* $SL(n, K)$ *such that* $s * t = \xi$ *and* $t * s = \eta$. *Set* $\delta = \xi\eta$. *Then* $\langle s, t \rangle \simeq SL(2, \mathbb{F}_p[\delta])$.

Proof. By the above, the pair (s, t) is conjugated to the pair $(T_{12}(\xi), T_{21}(\eta))$. The latter is conjugated by the matrix $\mathrm{diag}(\xi^{-1}, \mathrm{Id}_{n-1})$ into $(T_{12}(1), T_{21}(\delta))$. The statement follows by Dickson's Lemma. □

The above Corollary gives us the structure of the group $\langle U \rangle$ when $\Gamma(U)$ is a cycle of length 2 and either $char(K) \neq 2$ or $|K| \neq 9$. [If $char(K) = 2$, then two opposite transvections s, t generate a dihedral group of order $2k$, where k is odd (see Suzuki, 1982, Theorem 6.17). If $|K| = 9$, then $\langle s, t \rangle \simeq SL(2, \mathbb{F}_p[\delta])$, unless $\delta^2 = -1$, in which case $\langle s, t \rangle \simeq SL(2, 5)$.] In this section, we will focus on the general case when $\Gamma(U)$ is a cycle of length $h \geq 2$ and label product δ, and K is of arbitrary characteristic. First of all, we note that, under these assumptions, $\det H(U) = \pm\delta$. In particular, $\mathrm{rank}(H(U)) = \mathrm{rank}(A(U)) = \mathrm{rank}(C(U))$.

Next, we prove a technical result of general independent interest:

Proposition 3 (Simultaneous Conjugation). *Let* $U = \{t_1, \ldots, t_h\}$ *be a set of transvections in* $SL(n, K)$. *Set* $H = H(U)$, $A = A(U)$ *and* $C = C(U)$. *For* $X \in GL(n, K)$, *set*

$$U' = U^X := \{X^{-1}t_1X, \ldots, X^{-1}t_hX\}, \quad A' = A(U') \quad \textit{and} \quad C' = C(U').$$

If $\det H \neq 0$, *then* X *can be chosen in such a way that*

$$A' = [\mathrm{Id}_h \,|\, 0] \quad \textit{and} \quad C' = \left[\frac{H}{0}\right].$$

Proof. Recall that, for any $X \in GL(n, K)$, $A' = AX$, $C' = X^{-1}C$. Since $\det H \neq 0$, the rows of A are h independent elements of ${}^nK$. Thus, there exists $X_1 \in GL(n, K)$ such that $AX_1 = [\mathrm{Id}_h \,|\, 0]$. Whence it also follows that $X_1^{-1}C = \left[\begin{smallmatrix} H \\ D \end{smallmatrix}\right]$ for a suitable matrix D. Now, let X_2 be any element of $GL(n, K)$ of shape $\left[\begin{smallmatrix} \mathrm{Id}_h & 0 \\ E & \mathrm{Id}_{n-h} \end{smallmatrix}\right]$. Then $AX_1X_2 = [\mathrm{Id}_h \,|\, 0]$ and $(X_1X_2)^{-1}C = \left[\begin{smallmatrix} H \\ -(EH)+D \end{smallmatrix}\right]$. Setting $E := DH^{-1}$ and $X = X_1X_2$, we see that A' and C' have the required shape. □

As customary, if $x_1, \ldots, x_h$ ($h > 2$) are elements of a group G, we recursively define the "higher commutator" $[x_1, \ldots, x_h]$ to be $[[x_1, \ldots, x_{h-1}], x_h]$.

The following easy Lemma is sometimes useful:

Lemma 4. *Let* $t_1, \ldots, t_h$ *be transvections in* $SL(n, K)$, *and set* $t_i = \mathrm{Id} + c(t_i)a(t_i)$, $(i = 1, \ldots, h)$. *Suppose that in* $\widehat{\Gamma}(t_1, \ldots, t_h)$ *all the arcs ending in* t_1 *have label* 0

(that is, $t_i * t_1 = 0$ for every i) and let β be the label product along the path $t_1 \longrightarrow \cdots \longrightarrow t_h$. Then $[t_1, \ldots, t_h] = \mathrm{Id} + \beta c(t_1)a(t_h)$. In other words, if $\beta \neq 0$ $[t_1, \ldots, t_h]$ is a transvection with the same axis as t_h and the same centre as t_1. □

Proof. This was noticed above for $h = 2$. The statement follows by induction on h. □

Theorem 1. *Suppose that $U = \{t_1, \ldots, t_h\}$ is a set of $h > 2$ transvections of $SL(n, K)$ such that $\Gamma(U)$ is a cycle of length h with label product δ. Then $\langle U \rangle$ is isomorphic to $SL(h, \mathbb{F}_p[\delta])$.*

Proof. We observe that, by the previous proposition, conjugation via a suitable element of $GL(n, K)$ transforms the set U into the set $\{T_{h1}(\delta), T_{12}(1), \ldots, T_{(h-1)h}(1)\}$ and maps the root subgroups $t_1^{\mathbb{F}_p[\delta]}, t_2^{\mathbb{F}_p[\delta]}, \ldots, t_h^{\mathbb{F}_p[\delta]}$ into the elementary root subgroups $R_{h1}, R_{12}, \ldots, R_{h-1,h}$ of $SL(h, \mathbb{F}_p[\delta])$ (not necessarily in this order). We also recall (see Humphries, 1986, Theorem 2.1) that $SL(h, \mathbb{F}_p[\delta])$ is generated by the root subgroups $R_{12}, R_{23}, \ldots, R_{h1}$. So, it will be enough to show that $\langle U \rangle$ contains every root subgroup $t_i^{\mathbb{F}_p[\delta]}$, $1 \leq i \leq h$.

Fix $i \in \{1, \ldots, h\}$ (taken $\mod h$). Since the label δ is allowed to freely float along a cycle *without altering* the original generating transvections, w.l.o.g. we may assume that $\Gamma(U) = t_i \overset{\delta}{\longrightarrow} t_{i+1} \overset{1}{\longrightarrow} \cdots \overset{1}{\longrightarrow} t_{i-1} \overset{1}{\longrightarrow} t_i$. Fix a non-negative integer j. Then $t_i^{\delta^j} * t_{i+1} = \delta^{j+1}$. The previous lemma yields:

$$[t_i^{\delta^j}, t_{i+1}, \ldots, t_{i-2}, [t_{i-1}, t_i]] = [t_i^{\delta^j}, t_{i+1}, \ldots, \mathrm{Id} + 1 \cdot c(t_{i-1})a(t_i)]$$
$$= \mathrm{Id} + \delta^{j+1} c(t_i^{\delta^j}) a(\mathrm{Id} + 1 \cdot c(t_{i-1})a(t_i)) = t_i^{\delta^{j+1}}.$$

Thus, by induction, $t_i^{\delta^j} \in \langle U \rangle$ for all $j \geq 0$. It readily follows that the full root subgroup $t_i^{\mathbb{F}_p[\delta]}$ is contained in $\langle U \rangle$. Done. □

Remark. Clearly, the previous theorem can be viewed as a generalization of Dickson's Lemma. It should be noted that its statement is characteristic-free. On the contrary, Dickson's Lemma breaks down if $char(K) = 2$ or $|K| = 9$. Thus, the case $h = 2$ provides a real exception.

7. THE EQUIVALENCE RELATION ≈ AND THE DIGRAPH $\Gamma(\widetilde{U})$

We start by defining two basic binary relations on the set $\mathcal{T}$ of all (multi)sets of transvections in $SL(n, K)$. Namely, if $U, V \subseteq \mathcal{T}$, we set:

(1) $U \sim_1 V$ iff there exists $s, t \in U$, such that $V = U \cup \{t^s\}$.
(2) $U \sim_2 V$ iff there exists $t \in U$ and $\lambda \in \underline{L}(\widetilde{U})$ such that $V = U \cup \{t^\lambda\}$.

Next, we denote by $\approx_1$, $\approx_2$ the symmetrizations of $\sim_1$, $\sim_2$, respectively, and define the following equivalence relation $\approx$ on $\mathcal{T}$:

Definition 4. Let $U, V \subseteq \mathcal{T}$. Then $U \approx V$ iff there exists a sequence $U = V_0, V_1, \ldots, V_r = V$, such that $V_i \subseteq \mathcal{T}$ and either $V_i \approx_1 V_{i+1}$ or $V_i \approx_2 V_{i+1}$ for all $i \geq 0$.

Lemma 5.

(a) $U \approx \widetilde{U}$.
(b) *Let* $U \subseteq V \subseteq \widetilde{U}$. *Then* $U \approx V$.
(c) *For every* $U, V, W \subseteq \mathcal{T}$, $U \approx V$ *implies* $(U \cup W) \approx (V \cup W)$.

Proof. $\widetilde{U}$ is obtained from U by repeated application of $\sim_1$, whence (a). As for (b), note that obviously $\widetilde{U} = \widetilde{V}$. Thus (b) follows from (a). (c) is straightforward. □

Lemma 6. *Let* $U \subseteq \mathcal{T}$.

(1) *If* $s, t \in U$, *then* $U \approx (U - \{t\}) \cup \{t^s\}$.
(2) *If* $t \in U$, $s \in \langle U - \{t\}\rangle$, *then* $U \approx (U - \{t\}) \cup \{t^s\}$.
(3) *Suppose that* $t \in U$, $\lambda \in \underline{L}(\widetilde{U})$ *and set* $V = (U - \{t\}) \cup \{t^\lambda\}$. *If* $\lambda \in \underline{L}(\widetilde{V})$, *then* $U \approx V$.

Proof. (1) Set $V = (U - \{t\}) \cup \{t^s\}$. Observe that $s \in V$. It follows $V \approx V \cup \{(t^s)^{s^{p-1}}\} = V \cup \{t\} = U \cup \{t^s\} \approx U$.

(2) By assumption, we may write $s = s_1 s_2 \cdots s_a$, where $s_i \in U - \{t\}$ $(i = 1, \ldots, a)$. As above, set $V = (U - \{t\}) \cup \{t^s\}$. Then $V \approx V \cup \{(t^s)^{s_a^{p-1} \cdots s_2^{p-1} s_1^{p-1}}\} = V \cup \{t\} = U \cup \{t^s\} \approx U$.

(3) $V \approx V \cup \{(t^\lambda)^{\lambda^{-1}}\} = U \cup \{t^\lambda\} \approx U$. □

Remark. We observe that, under the assumptions on $\langle U\rangle$ imposed in Humphries (1986), our relation $\approx$ is an analogue of the notion of "t-equivalence", as defined by Brown and Humphries in their papers.

Proposition 4. *Let* $U, V \subseteq \mathcal{T}$ *where* $|U| \geq 1$, $|V| \geq 1$, *and assume that* $U \approx V$. *Then* $\Gamma(U)$ *is connected iff* $\Gamma(V)$ *is connected.*

Proof. First, observe that it is enough to prove the statement in the following two instances: (i) $U \sim_1 V$; (ii) $U \sim_2 V$.

Suppose that (i) holds and $V = U \cup \{t^s\}$ for $s, t \in U$. If $\Gamma(U)$ is connected, there is a path $s \longrightarrow \cdots \longrightarrow u \longrightarrow t$. Thus, in order to prove that $\Gamma(V)$ is connected, we only need to show that there exists in $\Gamma(V)$ both an arc ending in t^s and an arc starting from t^s. If $u * t^s \neq 0$, then in $\Gamma(V)$ there is an arc ending in t^s. If $u * t^s = 0$, then $0 \neq u * t = (u * s)(s * t)$ by Lemma 2, and hence $s * t = s * t^s \neq 0$. Thus in $\Gamma(V)$ there is an arc $s \to t^s$. Reversing the arrows, one similarly shows that there exists in $\Gamma(V)$ an arc starting from t^s.

Next, suppose that (i) holds and $\Gamma(V)$ is connected. If $p, q \in U$, then by assumption there is in $\Gamma(V)$ a path $\mathbf{p}$ from p to q. If $\mathbf{p}$ lies in $\Gamma(U)$, we are done. Otherwise $\mathbf{p}$ involves t^s, say $\mathbf{p}{:=}p \longrightarrow \cdots \longrightarrow r \longrightarrow t^s \longrightarrow v \longrightarrow \cdots \longrightarrow q$. However, in this case $r * t^s = a(r)(c(t) - \alpha c(s)) \neq 0$. Hence either $r * t \neq 0$, or $\alpha(r * s) \neq 0$, which means that in $\mathbf{p}$ we can replace the arc $r \longrightarrow t^s$ either with the arc $r \longrightarrow t$ or with the path $r \longrightarrow s \longrightarrow t$. A similar argument shows that an arc $t^s \longrightarrow v$ can be replaced either by an arc $t \longrightarrow v$ or by a path $t \longrightarrow s \longrightarrow v$. This proves that $\Gamma(U)$ is connected.

Now suppose that (ii) holds, that is $V = U \cup \{t^{\lambda}\}$, where $\lambda \in \underline{L}(\widetilde{U})$. Observe that, for any $p \in U$, there exists the arc $p \longrightarrow t$ ($t \longrightarrow p$) in $\Gamma(U)$ iff there exists the arc $p \longrightarrow t^{\lambda}$ ($t^{\lambda} \longrightarrow p$) in $\Gamma(V)$. This clearly shows that $\Gamma(U)$ is connected iff $\Gamma(V)$ is connected. □

Lemma 7. *Let $r, t, v \in \mathcal{T}$. Suppose that in $\Gamma(r, t, v)$ the arcs $r \longrightarrow t$, $t \longrightarrow v$, $v \longrightarrow r$ are present, but no other arc occurs except possibly $r \longrightarrow v$. Then, up to conjugation in $GL(n, K)$ one may assume that $t = T_{12}(1)$, $v = T_{23}(1)$ and $r = T_{31}(\xi)T_{32}(\eta)$ for suitable $\xi, \eta \in K$ and the following holds*:

(1) *If $char(K) \neq 2$, $H = \langle r, t, v\rangle \simeq SL(3, K_0)$, where $K_0 = \mathbb{F}_p[\xi, \eta]$.*
(2) *If $char(K) = 2$, (1) holds unless $\xi = 1$ and $\langle \eta\rangle = \mathbb{F}_4^*$. In the latter case $H \simeq 3 \cdot \mathbb{A}_6$, the unique perfect 3-fold cover of the alternating group $\mathbb{A}_6$.*
(3) *The matrices $x - \mathrm{Id}$, where x ranges over all the transvections in $H = \langle r, t, v\rangle$ that are opposite to t, span over K a Lie algebra isomorphic to $\mathfrak{sl}(3, K)$.*

Proof. By 4.2, adjusting the labels we may assume $t = T_{12}(1)$, $v = T_{23}(1)$. Furthermore, direct computation shows that we can pick an element g in $GL(n, K)$, such that g centralizes both t and v, and $grg^{-1} = T_{31}(\xi)T_{32}(\eta)$ for suitable $\xi, \eta \in K$ (where $\eta = r * v$ and $\xi = r * t$). This proves the first part of the statement. In particular, it is clear that we may assume $n = 3$.

The case when $\eta = 0$ is easy. Indeed, by Theorem 1 the group $H = \langle r, t, v\rangle$ is isomorphic to $SL(3, \mathbb{F}_p[\xi])$. It follows that a transvection in H, say $x = \mathrm{Id} + (c_1, c_2, c_3)^t(a_1, a_2, a_3)$, is opposite to t if and only if $a_1c_2 \neq 0$. It is then readily seen that $\mathrm{Span}_K(x - \mathrm{Id})$, where x ranges over all such transvections, contains the standard basis of $\mathfrak{sl}(3, K)$.

From now on, we suppose that $\eta \neq 0$, that is, $\Gamma(r, v)$ is a cycle.

Notice first that $[t, r] = [T_{12}(1), T_{31}(\xi)T_{32}(\eta)] = T_{32}(-\xi) \in H$. If $\xi = \pm\eta$, then $r^{\pm 1}[t, r] = T_{31}(\xi)$. Since the graph $\Gamma\{t, v, r[t, r]\}$ is a 3-cycle, by Theorem 1 $H \simeq SL(3, \mathbb{F}_p[\xi])$ and we are done. So, assume $\xi \neq \pm\eta$ and set $K_0 = \mathbb{F}_p[\xi, \eta]$. Let $H_1 = Stab_H(e_1')$ and $\pi : H_1 \to SL(2, K)$ be the projection of H_1 to ${}^3K/\langle e_1'\rangle$. For $\alpha \in K$, denote by $D(\alpha)$ the subgroup of $SL(2, \mathbb{F}_p[\alpha])$ generated by $T_{12}(1)$ and $T_{21}(\alpha)$. We claim that

$$\pi(H_1) = SL(2, K_0).$$

Indeed, $\pi(H_1) \geq \langle D(\xi), D(\eta)\rangle$. By Dickson's Lemma, $D(\alpha) = SL(2, \mathbb{F}_p[\alpha])$ unless $p = 2$ or $p = 3$ and $\alpha^2 = -1$. Thus, if $p = 3$ the result follows unless $\xi^2 = \eta^2 = -1$, and hence $\xi = \pm\eta$, a case that has been dealt with above. Next, suppose that $p = 2$. According to the list of subgroups of $SL(2, K)$ (see Suzuki, 1982, Theorem 6.17), $\langle D(\xi), D(\eta)\rangle$ can only be either dihedral of order $2k$, where k is odd, or $SL(2, K_0)$, or $SL(2, K_0) : 2$. It readily follows that $\pi(H_1) = \langle D(\xi), D(\eta)\rangle = SL(2, K_0)$.

Now, set $N = \ker \pi$. We claim that if $N \neq 1$, then $N \simeq K_0^2$. Indeed, the action of H_1 on N by conjugation is permutationally isomorphic to the natural action of $SL(2, K_0)$ on K_0^2. As $SL(2, K_0)$ acts transitively on $K_0^2 \backslash 0$, the claim follows. In particular, if $N \neq 1$, then $T_{31}(\alpha) \in H$ for any $\alpha \in K_0$ and again by Theorem 1 we get $H \simeq SL(3, K_0)$.

We are left with the case when $N = 1$. Then $H_1 \simeq SL(2, K_0)$ and for any $a \in SL(2, K_0)$ there exists a unique $u = u(a) \in K_0^2$ such that $\left[\begin{smallmatrix} 1 & 0 \\ u & a \end{smallmatrix}\right] \in H$. To be more precise: the map $u : a \mapsto u(a)$ defines a 1-cocycle from $SL(2, K_0)$ to K_0^2. Set $u(T_{21}(x)) = (\alpha(x), \beta(x))^t$ for $x \in K_0$ and $u(\mathrm{diag}(\lambda, \lambda^{-1})) = (\gamma(\lambda), \delta(\lambda))^t$, for $\lambda \in K_0^*$. First, we observe that α is an additive map on K_0 and $\alpha(\eta) = 0$. Setting $t_x = \pi^{-1}(T_{21}(x))$, $g_\lambda = \pi^{-1}(\mathrm{diag}(\lambda, \lambda^{-1}))$ and computing $t_x^{g_\lambda}$ we get the following constraint on α: $\alpha(\lambda^2 x) = \lambda^{-1}\alpha(x)$. Let $z \in K_0$: it is well known that there exists y, $t \in K_0$ such that $z = t^2 + y^2$. Thus $\alpha(z\eta) = \alpha(t^2\eta) + \alpha(y^2\eta)$, whence $\alpha(z\eta) = 0$, $\alpha(z\eta) = \alpha(t^2\eta) + \alpha(y^2\eta)$, since $\alpha(\eta) = \alpha(0) = 0$. We conclude that α is the zero map, whence it also follows that β is an additive map on K_0 and satisfies the constraint: $(*)$ $\beta(\lambda^2 x) = \lambda(\beta(x) + x\gamma(\lambda))$ for all $x \in K_0$ and $\lambda \in K_0^*$. Note that $\gamma \in Z^1(K_0^*, K_0^+)$. As $\gamma(\lambda\mu) = \gamma(\lambda) + \lambda\gamma(\mu)$ for all $\lambda, \mu \in K_0^*$, it follows immediately that $\gamma(\lambda) = g(\lambda - 1)$, for some constant $g \in K_0$ (in other words, $H^1(K_0^*, K_0^+) = 0$). Furthermore, $g \neq 0$. Otherwise $\beta(\lambda^2 x) = \lambda\beta(x)$ by $(*)$, and hence, as $T_{32}(-\xi) \in H$ forces $\beta(\xi) = 0$, also $\beta(\lambda^2\xi) = 0$. As above, this would imply that β is the zero map. A contradiction, since $\beta(\eta) = \xi \neq 0$.

We claim that $p = 2$. First of all, note that, as $\beta(\xi) = 0$, it follows from $(*)$ that $\beta(\lambda^2\xi) = g\xi\lambda(\lambda - 1)$. Next, observe that, provided $|K_0| > 5$ and p is odd, there exists $\rho \in K_0$ and $\lambda, \mu \in K_0^*$ such that $\rho^2 = \lambda^2 + \mu^2$. (Indeed, the conic $\mathscr{C} : x^2 + y^2 = \rho^2$ has exactly $q + (-1)^{\frac{q+1}{2}}$ points, of which at most four have a zero coordinate.) For a triple (ρ, λ, μ) satisfying the above condition, we then have

$$g\xi\rho(\rho - 1) = \beta(\rho^2\xi) = \beta(\lambda^2\xi) + \beta(\mu^2\xi) = g\xi\lambda(\lambda - 1) + g\xi\mu(\mu - 1).$$

Whence $\rho = \lambda + \mu$, $2\lambda\mu = 0$ and hence $p = 2$. On the other hand, if $|K_0| = 3, 5$ direct computation shows that the conditions $\beta(\xi) = 0$ and $\beta(\eta) = \xi$ are not compatible. Thus, from now on, we may assume $p = 2$. In this case, elementary calculations show that $\beta(x) = (\eta + \sqrt{\eta\xi})^{-1}\xi(x + \sqrt{\xi x})$. In particular, $\ker\beta = \langle\xi\rangle$. Now, $[t, T_{31}(\beta(x))T_{32}(x)] = T_{32}(\beta(x)) \in H$. Thus $\beta^2(x) = x$ for every $x \in K$. Since $\dim\ker\beta = 1$, it follows that $K_0 = \ker\beta^2$ has dimension at most 2. Thus $|K_0| \leq 4$. The case $|K_0| = 2$ obviously implies $\xi = \eta$, against our current assumptions. Thus $|K_0| = 4$. Making use of the MAGMA package (see Bosma and Cannon, 1995), one sees that the unique proper subgroup of $SL(3, 4)$ generated by r, t, v is isomorphic to $3.\mathbb{A}_6$ and only occurs if $\xi = 1$ and $\mathbb{F}_4^* = \langle\eta\rangle$. Furthermore, the K-linear span of the transvections in this group which are opposite to t still equals $\mathfrak{sl}(3, K)$. □

Proposition 5. *Let $U \subseteq \mathscr{T}$, $s \neq t \in \widetilde{U}$ and assume that $\Gamma(U)$ is connected. Then either s and t are opposite (that is, $\Gamma(s, t) := \overset{s}{\bullet} \leftrightarrows \overset{t}{\bullet}$), or there exists a transvection $u \in \widetilde{U}$ that is opposite to both s and t (that is, $\Gamma(s, U) := \overset{s}{\bullet} \leftrightarrows \overset{u}{\bullet}$ and $\Gamma(u, t) := \overset{u}{\bullet} \leftrightarrows \overset{t}{\bullet}$).*

Proof. Suppose that $\Gamma(s, t)$ is not connected, say $s * t = 0$. We claim that in $\Gamma(\widetilde{U})$ there is a path of length 2 from s to t. For, let us consider a path from s to t in $\Gamma(\widetilde{U})$ and suppose that it has length $a \geq 2$. Say, $\mathbf{p} := s \longrightarrow r_1 \longrightarrow r_2 \longrightarrow \cdots \longrightarrow r_a = t$. If $s * r_2 \neq 0$, we can shorten $\mathbf{p}$ to $\mathbf{p}' := s \longrightarrow r_2 \longrightarrow \cdots \longrightarrow t$. Otherwise, there is an arc $s \longrightarrow r_2^{r_1}$, since $s * r_2^{r_1} = -(s * r_1)(r_1 * r_2) \neq 0$. Now, if $r_1 * r_3 \neq 0$ we can shorten $\mathbf{p}$ to $\mathbf{p}'' := s \longrightarrow r_1 \longrightarrow r_3 \longrightarrow \cdots \longrightarrow t$. Otherwise, by Lemma 2 $r_2^{r_1} * r_3 = r_2 * r_3 \neq 0$, and therefore $\mathbf{p}$ can be shortened to $\mathbf{p}''' := s \longrightarrow r_2^{r_1} \longrightarrow r_3 \longrightarrow \cdots \longrightarrow t$.

Thus, in all cases we can switch from **p** to a path from s to t of length $a-1$. This shows that in $\Gamma(\widetilde{U})$ there is a path of length 2 from s to t, say: $s \longrightarrow r \longrightarrow t$.

Next, we split the proof into separate cases:

Case 1. $t * s \neq 0$ (but $s * t = 0$). Case 1 splits into three subcases.

Subcase 1a. $r * s = t * r = 0$, that is, $\Gamma(s, r, t)$ is a 3-cycle. In this case, by Theorem 1, the subgroup $\langle s, r, t\rangle$ is isomorphic to $SL(3, \mathbb{F}_p[\delta])$, where δ is the label product along $\Gamma(s, r, t)$. It follows immediately that we can find in $\langle s, r, t\rangle$ a transvection u opposite to both s and t. Moreover, u clearly belongs to $\widetilde{U}$, since in $SL(3, \mathbb{F}_p[\delta])$ the transvections form a single conjugacy class.

Subcase 1b. r is opposite to s and $t * r = 0$. Then clearly s and r^s are also opposite. Moreover, $t * r^s = -(t * s)(s * r) \neq 0$ and $r^s * t = r * t \neq 0$. Thus r^s is opposite to both s and t, and we are done.

Subcase 1c. r is opposite to t and $r * s = 0$. Arguing as in 1b, we see that the transvection r^t meets our requirements.

Case 2. s and t commute, that is $s * t = t * s = 0$. By the first part of the proof, we can find in $\Gamma(\widetilde{U})$ a path $s \longrightarrow r \longrightarrow t$ as well as a path $t \longrightarrow q \longrightarrow s$. We claim that r can be chosen in such a way that either s or t are opposite to either r or q. For, suppose the contrary. Assume first that either $r * q \neq 0$, or $q * r \neq 0$. Then $s * r^q = s * r$, $r^q * s = (r * q)(q * s)$, $r^q * t = r * t$, $t * r^q = -(t * q)(q * r)$. This means that r^q is opposite to either s or t, and we are done. Next, suppose that $r * q = q * r = 0$. Then $s * r^t = s * r$, $r^t * s = 0$, $t * r^t = 0$, $r^t * t = r * t$. Replacing r with r^t, we observe that $r^t * q = (r * t)(t * q) \neq 0$. Thus, as before, we conclude that $(r^t)^q$ is opposite to either s or t.

In view of the above argument, we may assume at this stage that there exists a path $s \longrightarrow r \longrightarrow t$ in $\Gamma(\widetilde{U})$, such that r is opposite to either s or t.

Assume that r is opposite to s. Since $s * t^r = -(s * r)(r * t)$ and $t^r * s = (t * r)(r * s)$, then either r is opposite to t, in which case we are done, or $\Gamma(s, t^r) := \underset{s}{\bullet} \longrightarrow \underset{t^r}{\bullet}$. In the latter instance, we are back to Case 1 (applied to s and t^r). Therefore, we know that there exists in $\widetilde{U}$ a transvection v which is opposite to both s and t^r. Since $t^r * v = (t * v) + (t * r)(r * v) \neq 0$, either r is opposite to t and we are done, or $t * v \neq 0$. If $v * t \neq 0$, then v is opposite to both s and t, so again we are done. Otherwise, $0 \neq v * t^r = -(v * r)(r * t)$ forces $v * r \neq 0$. Thus $\Gamma(r, t, v)$ satisfies the assumptions of the previous lemma. In particular, $H = \langle r, t, v\rangle$ can be viewed as acting on the natural 3-dimensional module K^3. Since s is opposite to v, it is clear that $a(s)$ and $c(s)$ have nonzero projections onto ${}^3K$ and K^3, respectively. Since $\mathfrak{sl}(3, K)$ acts irreducibly on K^3, it then follows from the same lemma that there exists in H a transvection x opposite to t, such that $a(s)(x - \mathrm{Id})c(s) \neq 0$. This obviously implies that x is also opposite to s.

Finally, assume that r is opposite to t. Evaluating $s^r * t$ and $t * s^r$ and arguing along the same lines as above one falls back into Case 1 (applied to s^r and t) and hence is led to a graph $\Gamma(r, s, v)$ satisfying the assumptions of the previous lemma. Whence the desired conclusion. □

Remark. Note that, by the above proposition, if $\Gamma(U)$ is connected, then any two distinct nodes in $\Gamma(\widetilde{U})$ are joined by a path of length at most 2.

Corollary 3. *Let $U \subseteq \mathcal{T}$, $t \in \widetilde{U}$. Suppose that $|U| \geq 1$ and $\Gamma(U)$ is connected. Then there exists $u \in \widetilde{U}$ such that $u \neq t$ and $> \Gamma(u, t) := \underset{u}{\bullet} \rightleftarrows \underset{t}{\bullet}$.*

Proof. Let $s \neq t \in \widetilde{U}$. If $\Gamma(s, t) := \underset{s}{\bullet} \rightleftarrows \underset{t}{\bullet}$, we are done. Otherwise, pick u as in the proposition. □

Proposition 6. *Assume $char(K) \neq 2, 3$. Let $U = \{a, b, c\} \subseteq \mathcal{T}$ and suppose that $\Gamma(a, b)$ and $\Gamma(b, c)$ are cycles with label product α and β, respectively. Let $\mathbb{F}_p[\alpha, \beta]$ denote the subfield of K generated by $\{\alpha, \beta\}$. Then $\langle U \rangle = \langle U \rangle^{\mathbb{F}_p[\alpha,\beta]}$.*

Proof. W.l.o.g., we may assume that $\Gamma(a, b) := a \underset{1}{\overset{\alpha}{\rightleftarrows}} b$ and $\Gamma(b, c) := b \underset{\beta}{\overset{1}{\rightleftarrows}} c$. Let C be the subgroup of the multiplicative group of K generated by $\{\alpha, \beta\}$, and let $\alpha^d\beta^e$ be a generator of C. Then it is readily seen that $\mathbb{F}_p[\alpha, \beta] = \mathbb{F}_p[\alpha^d\beta^e]$. Next, observe that, by Dickson's Lemma applied to the cycles $\Gamma(a, b)$ and $\Gamma(b, c)$, b^{α^d} and $c^{\beta^{e-1}}$ certainly belong to $\langle U \rangle$. Replacing b with b^{α^d} and c with $c^{\beta^{e-1}}$ (but keeping the same representatives for their centres) we obtain the following digraphs: $\Gamma(a, b^{\alpha^d}) := a \underset{\alpha^d}{\overset{\alpha}{\rightleftarrows}} b^{\alpha^d}$; $\Gamma(b^{\alpha^d}, c^{\beta^{e-1}}) := b^{\alpha^d} \underset{\beta^e}{\overset{\alpha^d}{\rightleftarrows}} c^{\beta^{e-1}}$. Now, Dickson's Lemma applied to $\Gamma(b^{\alpha^d}, c^{\beta^{e-1}})$ tells us that both the subgroups

$$(b^{\alpha^d})^{\mathbb{F}_p[\alpha^d\beta^e]} = (b^{\alpha^d})^{\mathbb{F}_p[\alpha,\beta]} = b^{\mathbb{F}_p}[\alpha, \beta] \quad \text{and}$$
$$(c^{\beta^{e-1}})^{\mathbb{F}_p[\alpha^d\beta^e]} = (c^{\beta^{e-1}})^{\mathbb{F}_p[\alpha,\beta]} = c^{\mathbb{F}_p[\alpha,\beta]} \quad \text{lie in } \langle U \rangle.$$

Likewise, by symmetry reasons, if we had considered a and b, instead of b and c, we would have gotten that $a^{\mathbb{F}_p[\alpha,\beta]}$ and $b^{\mathbb{F}_p[\alpha,\beta]}$ lie in $\langle U \rangle$. The statement follows. □

We are now ready to prove Proposition 1.

Proof of Proposition 1. By definition, $\underline{L}(\widetilde{U})$ is generated by the label products taken along all cycles of length 2. So, we first show that, if $a, b \in \widetilde{U}$ are such that $\Gamma(a, b) := \underset{1}{\overset{\lambda}{\rightleftarrows}} b$, then $t^\lambda \in \langle U \rangle$. This is clear, by Dickson's Lemma, if either $t = a$ or $t = b$. If $t \neq a, b$ and, say, $\Gamma(b, t)$ is a cycle, the statement follows from Proposition 6. If $t \neq a, b$ and $\Gamma(b, t)$ is not a cycle, then by Proposition 5 there exists $r \in \widetilde{U}$ such that both $\Gamma(b, r)$ and $\Gamma(r, t)$ are cycles. Suppose that $\Gamma(b, r) := b \underset{1}{\overset{\mu}{\rightleftarrows}} r$. Then Proposition 6 applied to the set $\{r, b, a\}$ tells us that $b^{\mathbb{F}_p[\lambda,\mu]} \subseteq \langle U \rangle$. In particular, $b^{\lambda\mu^{-1}} \in \langle U \rangle$. Observe that $\Gamma(b^{\lambda\mu^{-1}}, r) := b^{\lambda\mu^{-1}} \underset{1}{\overset{\lambda}{\rightleftarrows}} r$. Therefore, by Proposition 6 applied to the set $\{b^{\lambda\mu^{-1}}, r, t\}$, we get that $t^\lambda \in \langle U \rangle$, as desired.

Next, assume that $t^\lambda, t^\mu \in \langle U \rangle$. By Corollary 3, there exists $r \in \widetilde{U}$ such that $\Gamma(r, t)$ is a cycle. Moreover, by Dickson's Lemma, we may assume that $\Gamma(r, t) := r \underset{1}{\overset{1}{\rightleftarrows}} t$. Proposition 6 applied to $\{r, t^\lambda, t^\mu\}$ tells us that $(t^\lambda)^{\mathbb{F}_p[\lambda,\mu]} = t^{\mathbb{F}_p[\lambda,\mu]} \subseteq \langle U \rangle$.

Thus, we have shown that the set $\{\lambda \in K \mid t^\lambda \in \langle U\rangle\}$ is a subfield of K. The statement of the proposition now follows. □

Proposition 1 has an immediate but important consequence, namely:

Corollary 4. *Assume* $char(K) \neq 2, 3$. *Suppose that* $\Gamma(U)$ *is connected and* $U \approx V$. *Then* $\langle U\rangle = \langle V\rangle$.

Proof. By the very definitions of $\sim_1$ and $\sim_2$, Propositions 4 and 6. □

Remark. Observe that the above statement breaks down in characteristic 2. In other words two equivalent sets can generate different groups, an example being provided by the subgroup $3 \cdot \mathbb{A}_6$ of $SL(3, \mathbb{F}_4)$ arisen in Lemma 7.

Next, we would like to control the behaviour of the subfields $\overline{L}(U)$ and $\underline{L}(\widetilde{U})$ under the equivalence relation $\approx$. The following holds:

Proposition 7. *Let* $U, V \subseteq \mathcal{T}$, *and suppose that* $U \approx V$. *Then*:

(i) $\overline{L}(U) = \overline{L}(V)$.
(ii) $\underline{L}(\widetilde{U}) = \underline{L}(\widetilde{V})$.

Proof. It will be enough to prove statements (i) and (ii) in the following "basic" cases: (1) $U \sim_1 V$, that is, $V = U \cup \{t^s\}$ for some $s, t \in U$; (2) $U \sim_2 V$, that is, $V = U \cup \{t^\lambda\}$ for some $t \in U$, $\lambda \in \underline{L}(\widetilde{U})$. Also, we may as well work with the complete digraphs $\widehat{\Gamma}(U)$, $\widehat{\Gamma}(V)$, since switching from Γ to $\widehat{\Gamma}$ clearly does not affect the subfields $\underline{L}, \overline{L}$.

(i) case (1). Since obviously $\overline{L}(U) \subseteq \overline{L}(V)$, we need to show that $\overline{L}(V) \subseteq \overline{L}(U)$. For this purpose, we only need to consider the (simple) closed paths through t^s, say: $\mathbf{p} := \cdots \longrightarrow q \xrightarrow{\varphi} t^s \xrightarrow{\psi} r \longrightarrow \cdots$. Suppose that $\widehat{\Gamma}(t, s) := t \overset{\tau}{\underset{\sigma}{\rightleftarrows}} s$ and set $q * s = \alpha$, $q * t = \beta$, $s * r = \gamma$, $t * r = \delta$. Then by Lemma 2 $\varphi = \beta - \sigma\alpha$ and $\psi = \delta + \tau\gamma$. Thus the label product of $\mathbf{p}$ equals $(\beta - \sigma\alpha)(\delta + \tau\gamma)\pi$, where π is the product of the labels along the arcs of $\mathbf{p}$ other than $q \xrightarrow{\varphi} t^s$ and $t^s \xrightarrow{\psi} r$. Now consider the following variants of $\mathbf{p}$ in $\widehat{\Gamma}(U)$:

$$\begin{aligned}
\mathbf{p}_1 &:= \cdots \longrightarrow q \longrightarrow t \longrightarrow r \longrightarrow \cdots \\
\mathbf{p}_2 &:= \cdots \longrightarrow q \longrightarrow s \longrightarrow t \longrightarrow r \longrightarrow \cdots \\
\mathbf{p}_3 &:= \cdots \longrightarrow q \longrightarrow t \longrightarrow s \longrightarrow r \longrightarrow \cdots \\
\mathbf{p}_4 &:= \cdots \longrightarrow q \longrightarrow s \longrightarrow t \longrightarrow s \longrightarrow r \longrightarrow \cdots
\end{aligned}$$

(the portions of each path not explicitely drawn being the same as in $\mathbf{p}$). The above closed paths have label products $\beta\delta\pi$, $\alpha\sigma\delta\pi$, $\beta\tau\gamma\pi$ and $\alpha\sigma\tau\gamma\pi$, respectively. Since these values all belong to $\overline{L}(U)$, the label product of $\mathbf{p}$ also belongs to $\overline{L}(U)$, whence $\overline{L}(V) \subseteq \overline{L}(U)$.

(i) case (2). For every closed path $\mathbf{p}$ passing through t^λ in $\Gamma(V)$, there is a corresponding path in $\Gamma(U)$ obtained by replacing t^λ with t. If the latter path has

label product μ, then $\mathbf{p}$ has label product $\lambda\mu$. Hence, in order to show that $\overline{L}(U) = \overline{L}(V)$, it is enough to show that $\lambda \in \overline{L}(U)$. To this end, observe that by assumption $\lambda \in \underline{L}(\widetilde{U}) \subseteq \overline{L}(\widetilde{U})$. Since one obtains $\widetilde{U}$ from U by repeated application of $\sim_1$, it follows from case (1) that $\overline{L}(U) = \overline{L}(\widetilde{U})$, whence $\lambda \in \overline{L}(U)$.

(ii) case (1). In this instance, (ii) is trivially true, since $\widetilde{U} = \widetilde{V}$.

(ii) case (2). For every cycle of length 2 through t^λ having label product μ in $\Gamma(\widetilde{V})$, there is a corresponding cycle in $\Gamma(\widetilde{U})$ obtained by replacing t^λ with t and thus having label product $\lambda^{-1}\mu$. However, by assumption $\lambda \in \underline{L}(\widetilde{U})$. It follows that $\mu \in \underline{L}(\widetilde{U})$, whence $\underline{L}(\widetilde{U}) = \underline{L}(\widetilde{V})$, as desired. □

Corollary 5. *Let $U \subseteq \mathcal{T}$. Then $\underline{L}(\widetilde{U}) \subseteq \overline{L}(U)$.*

Proof. Since $U \approx \widetilde{U}$, by point (i) of the previous proposition we have $\overline{L}(U) = \overline{L}(\widetilde{U})$. But $\underline{L}(\widetilde{U}) \subseteq \overline{L}(\widetilde{U})$, done. □

Remark. We observe explicitly that in the previous proposition (ii) cannot be replaced by the stronger statement $\underline{L}(U) = \underline{L}(V)$. The latter is clearly false. For example, let $\Gamma(U)$ be a cycle of length ≥ 3 with label product $\delta \notin \mathbb{F}_p$. Then $\underline{L}(U) = \mathbb{F}_p$, but it is easily seen (using Lemma 2), that $\underline{L}(\widetilde{U}) \ni \delta$.

As for the behaviour of the matrices $A(U)$, $C(U)$ and $H(U)$ under $\approx$, the following holds:

Proposition 8. *Let $U, V \subseteq \mathcal{T}$, and suppose that $U \approx V$. Then*:

(a) $\operatorname{rank}(A(U)) = \operatorname{rank}(A(V))$.
(b) $\operatorname{rank}(C(U)) = \operatorname{rank}(C(V))$.
(c) $\operatorname{rank}(H(U)) = \operatorname{rank}(H(V))$.

Proof. It is enough to prove the statements in the "basic" cases: (1) $U \sim_1 V$; (2) $U \sim_2 V$. In case (1) $A(V)$ and $C(V)$ are obtained by adding to $A(U)$ and $C(U)$ the row $a(t^s)$ and the column $c(t^s)$, respectively. Since $a(t^s)$ is a linear combination of $a(s)$ and $a(t)$, and $c(t^s)$ is a linear combination of $c(s)$ and $c(t)$, (a) and (b) follow. In case (2), $A(V)$ and $C(V)$ are obtained by adding to $A(U)$ and $C(U)$ the row $a(t^\lambda)$ and the column $c(t^\lambda)$, respectively, which are multiples of $a(t)$ and $c(t)$. Thus again (a) and (b) trivially follow.

As for (c), observe that

$$\operatorname{rank}(A(U)C(U)) = \operatorname{rank}(A(U)C(V)) = \operatorname{rank}(A(V)C(V)).$$

in both cases (1) and (2). □

8. REDUCTION TO "NORMAL FORM"

The main aim of this section is to prove that, provided $char(K) \neq 2, 3$, we can transform a given set $U \subseteq \mathcal{T}$ (where $|U| \geq 3$) such that $\Gamma(U)$ is connected and $\Gamma(\widetilde{U})$ is a one-way digraph, into an equivalent set $V = \{s_1, s_2, \ldots, s_h, t_1, t_2, \ldots, t_k\}$ (where

$|V| = h + k$, $h \geq 3$) such that $\Gamma(s_1, s_2, \ldots, s_h)$ is a cycle, $\text{rank}(H(V)) = h$, and the following extra-conditions hold: for each $l = 1, \ldots, k$, $t_l * s_j \neq 0$ in $\Gamma(V)$ for some j; $s_i * t_l \neq 0$ in $\Gamma(V)$ iff $i = h$; $t_l * s_1 = 0$; $t_l * t_m = 0$ for all $m = 1, \ldots, k$. A set $V \subseteq \mathcal{T}$ with the above properties will be loosely said to be in "normal form". Reduction to "normal form" is vitally instrumental to the proof of our Main Theorem. It should be pointed out that a somewhat similar but simpler reduction process is outlined in Humphries (1986, 1987). On the other hand, the assumptions of Humphries (1986, 1987) make sure *a priori* that $t^\lambda \in U$ for all $t \in U$, $\lambda \in K$, and hence, trivially, $\underline{L}(\widetilde{U}) = \overline{L}(U) = K$. The equality $(*)$ $\underline{L}(\widetilde{U}) = \overline{L}(U)$ is useful in our context, as it often allows to "delete" arcs up to equivalence. In general, the inequality $\underline{L}(\widetilde{U}) \subseteq \overline{L}(U)$ holds, as seen in Corollary 5. On the other hand, unitary groups are generated by suitable transvection sets U, and these provide examples where $\underline{L}(\widetilde{U}) \neq \overline{L}(U)$. This is why, under our substantially weaker assumptions, we have to set up a more complicated machinery. The crucial point is that $(*)$ allows us to reduce a transvection set to "normal form", and furthermore that a transvection set in "normal form" does satisfy $(*)$ (cfr. Proposition 9 and Corollary 6).

Our first result lists several conditions under which equality $\underline{L}(\widetilde{U}) = \overline{L}(U)$ holds.

Lemma 8. *Let $U \subseteq \mathcal{T}$, and suppose that any of the following holds*:

(a) $\Gamma(U\backslash\{t\})$ *is a chain, for some* $t \in U$.
(b) $\Gamma(U)$ *is a cycle.*
(c) *For some* $t \in U$, $\Gamma(U\backslash\{t\})$ *is a cycle of length* ≥ 3.
(d) *There exists* $V \subseteq U$ *such that*: (i) *any cycle in* $\Gamma(U)$ *has at most one node belonging to* V; (ii) $\Gamma(U\backslash V)$ *is a cycle of length* ≥ 3.

Then $\underline{L}(\widetilde{U}) = \overline{L}(U)$.

Proof. Since $\underline{L}(\widetilde{U}) \subseteq \overline{L}(U)$, we need to show that $\overline{L}(U) \subseteq \underline{L}(\widetilde{U})$.

(a) Setting $U = \{s_1, s_2, \ldots, s_a, t\}$, we assume that $\Gamma(U\backslash\{t\}) := s_1 \longrightarrow s_2 \longrightarrow \cdots \longrightarrow s_a$ and U is a counterexample of minimal size. It follows that there must be in $\Gamma(U)$ a closed path $\mathbf{p} := t \longrightarrow s_1 \longrightarrow s_2 \longrightarrow \cdots \longrightarrow s_a \longrightarrow t$ with label product π such that $\pi \in \overline{L}(U)\backslash\underline{L}(\widetilde{U})$. Set $s_1 * s_2 = \alpha$. Suppose that $a \geq 3$ and set $V = (U\backslash\{s_1, s_2\}) \cup \{s_1^{s_2}\}$. Then, since $a(s_1^{s_2}) = a(s_1) + \alpha a(s_2)$ and $c(s_1^{s_2}) = c(s_1)$, there exists in $\Gamma(V)$ a closed path $\overline{\mathbf{p}} := t \longrightarrow s_1^{s_2} \longrightarrow s_3 \longrightarrow \cdots \longrightarrow s_a \longrightarrow t$ with label product π. Since $|V| = |U| - 1$, this contradicts the minimal choice of U. Hence we conclude that $a = 2$, that is $\mathbf{p} := t \longrightarrow s_1 \longrightarrow s_2 \longrightarrow t$. We claim that $\Gamma(s_1, t)$ is a cycle. For, assume that $s_1 * t = 0$. Then $s_1^{s_2} * t = \alpha(s_2 * t)$ implies that $\Gamma(s_1^{s_2}, t)$ is a cycle with label product π, which in turn implies that $\pi \in \underline{L}(\widetilde{U})$, a contradiction. Now, suppose that $\Gamma(s_1, t)$ has label product β. Then, computation shows that $\Gamma(s_1^{s_2}, t)$ is a cycle with label product $\beta + \pi$. Thus $\beta + \pi \in \underline{L}(\widetilde{U})$. Since obviously β also belongs to $\underline{L}(\widetilde{U})$, it follows that $\pi \in \underline{L}(\widetilde{U})$, against our assumption.

(b) This is a subcase of (a), unless $|U| = 2$, in which case the lemma is trivially true.

(c) First, we prove a preliminary result:

Suppose that $|U| = 4$, say $U = \{a, b, c, t\}$, and $\Gamma(a, b, c)$ is a cycle. Suppose furthermore that there exists in $\Gamma(U)$ a simple closed path $\mathbf{c}$ of length 4 (that is

a cycle visiting all nodes) with label product ξ. Then $\xi \in \underline{L}(\widetilde{U})$. Let $\Gamma(a, b, c) := a \xrightarrow{\varphi} b \xrightarrow{\chi} c \xrightarrow{\psi} a$ and denote by φ', χ', ψ' the label products of the paths $a \longrightarrow t \longrightarrow b$, $b \longrightarrow t \longrightarrow c$, $c \longrightarrow t \longrightarrow a$, respectively, in $\widehat{\Gamma}(U)$. Then ξ can only take one of the values $\varphi'\chi\psi$, $\varphi\chi'\psi$, $\varphi\chi\psi'$. We proceed to show that $\varphi'\chi\psi \in \underline{L}(\widetilde{U})$ (the proof in the case of $\varphi\chi'\psi$, $\varphi\chi\psi'$ is entirely similar). Suppose first that $t * a = 0$. Set $V = \{a^t, b, c\}$. Then, in $\widehat{\Gamma}(V)$ there is a path $a^t \xrightarrow{\varphi+\varphi'} b \xrightarrow{\chi} c \xrightarrow{\psi} a^t$. Now $\Gamma(V\backslash\{a^t\})$ is a chain, hence V satisfies (a). It follows that the label product $(\varphi + \varphi')\chi\psi$ belongs to $\underline{L}(\widetilde{U})$. Observing that $\varphi\chi\psi \in \underline{L}(\widetilde{U})$, since $\Gamma(a, b, c)$ satisfies (b), it follows that $\varphi'\chi\psi \in \underline{L}(\widetilde{U})$. Next, suppose that $b * t = 0$. Set $V = \{a, b^t, c\}$. Then, in $\widehat{\Gamma}(V)$ there is a path $b^t \xrightarrow{\chi} c \xrightarrow{\psi} a \xrightarrow{\varphi-\varphi'} b^t$. Now $\Gamma(V\backslash\{b^t\})$ is a chain, hence V satisfies (a) and therefore $\chi\psi(\varphi - \varphi') \in \underline{L}(\widetilde{U})$. As before, it follows that $\varphi'\chi\psi \in \underline{L}(\widetilde{U})$. Finally, suppose that $t * a$ and $b * t$ are both nonzero, so that the graph $\Gamma(a, b, t)$ is connected. Let φ'' be the label product of the path $b \longrightarrow t \longrightarrow a$. In $\Gamma(a, b, t)$ there exist a path $a \longrightarrow b \longrightarrow t \longrightarrow a$ with label product $\varphi\varphi''$ and a path $t \longrightarrow b \longrightarrow t \longrightarrow a \longrightarrow t$ with label product $\varphi''\varphi'$. Since $\Gamma(a, b)$ is a chain, by (a) both $\varphi\varphi''$ and $\varphi''\varphi'$ belong to $\underline{L}(\widetilde{U})$. Hence $\varphi^{-1}\varphi' \in \underline{L}(\widetilde{U})$. Now $\varphi\chi\psi \in \underline{L}(\widetilde{U})$ forces $\varphi'\chi\psi \in \underline{L}(\widetilde{U})$, done.

We now prove (c). We may assume that $U = \{s_1, s_2, \ldots, s_a, t\}$ and $\Gamma(s_1, s_2, \ldots, s_a)$ is a cycle of length $a \geq 3$. Suppose that U is a counterexample of minimal size. Then, there must be in $\Gamma(U)$ a cycle of length greater than 2, with label product $\pi \in \overline{L}(U)\backslash\underline{L}(\widetilde{U})$. Let V denote the set of nodes of $\mathbf{p}$. If $t \notin V$, then $V \subseteq \{s_1, s_2, \ldots, s_a\}$ and hence $V \equiv \{s_1, s_2, \ldots, s_a\}$. Thus V satisfies (b), and therefore $\pi \in \underline{L}(\widetilde{U})$, a contradiction. So, suppose that $t \in V$. If $V \neq U$, then $\Gamma(V\backslash\{t\})$ is a chain; hence V satisfies (a), and therefore again $\pi \in \underline{L}(\widetilde{U})$, a contradiction. If $V = U$, we may set $\mathbf{p} := t \longrightarrow s_1 \longrightarrow s_2 \longrightarrow \cdots \longrightarrow s_a \longrightarrow t$. Assuming $a \geq 4$, let us consider the path $\bar{\mathbf{p}} := t \longrightarrow s_1^{s_2} \longrightarrow s_3 \longrightarrow \cdots \longrightarrow s_a \longrightarrow t$. Set $W = \{s_1^{s_2}, s_3, \ldots, s_a, t\}$, so that $|W| = |U| - 1$. Since $\bar{\mathbf{p}}$ has label product π, W would also provide a counterexample, contradicting the minimality of U. So, $a = 3$. But this is impossible, by the result proven above.

(d) Let $\mathbf{p}$ be a cycle in $\Gamma(U)$ with set of nodes W. By assumption, either $|W \cap V| = 0$ or $|W \cap V| = 1$. In the former case $\mathbf{p} = \Gamma(U\backslash V)$, hence W satisfies (b). If $|W \cap V| = 1$ and $v \in W \cap V$, then $\Gamma(W\backslash\{v\})$ is either a chain or a cycle of length ≥ 3. Thus W satisfies either (a) or (c), and we are done. □

As already mentioned, the relevance of the condition $\underline{L}(\widetilde{U}) = \overline{L}(U)$ stems from the fact that it allows to delete arcs from a given digraph, as shown in the lemmas which follow.

Lemma 9. *Let $U = V \cup \{r, s, t\} \subseteq \mathcal{T}$, $V \cap \{r, s, t\} = \emptyset$. Suppose that* (a) *$\Gamma(U)$ is connected*; (b) *$\Gamma(V \cup \{r, s\})$ is either a chain or a cycle of length ≥ 3*; (c) *$r * s$, $t * r$ and $t * s$ are all nonzero. Set $W = V \cup \{r, s, \hat{t}\}$, where $\hat{t} = \left(t^{r^\lambda}\right)^\mu$, $\lambda, \mu \in \underline{L}(\widetilde{U})$. Then, for suitable choices of λ and μ, the following holds*: (d) *$U \approx W$*; (e) *in $\Gamma(W)$ $\hat{t} * s = 0$.*

Proof. W.l.o.g. we may assume that $r * s = t * r = 1$. Set $t * s = \alpha$ and let $\mathbf{p}$ be a path from s to t in $\Gamma(U)$, with label product β. Adding to $\mathbf{p}$ the paths $t \longrightarrow r \longrightarrow s$ and $t \longrightarrow s$, one obtains closed paths with label product $\beta \cdot 1 \cdot 1 = \beta$ and $\alpha\beta$, respectively. Hence $\alpha, \beta \in \overline{L}(U)$. As U satisfies either assumption (a) or

assumption (c) of Lemma 8, it follows that $\alpha, \beta \in \underline{L}(\widetilde{U})$. Set $U' = V \cup \{r, r^{-\alpha}, s, t\}$, $U'' = V \cup \{r, r^{-\alpha}, s, t^{r^{-\alpha}}\}$. Clearly $U \approx U' \approx U''$ (by Lemma 6(1)). Thus, by Lemma 8 and Proposition 7, $\underline{L}(\widetilde{U''}) = \overline{L}(U'')$. Now, observe that in $\Gamma(U'')$ $t^{r^{-\alpha}} * s = 0$ (use Lemma 2). Since, by Proposition 4, $\Gamma(U'')$ is connected, there exists in $\Gamma(U'')$ a closed path $\mathbf{p}'$ through $t^{r^{-\alpha}}$. Moreover, if $r^{-\alpha} \neq r$, by replacing $r^{-\alpha}$ by r, we may assume that $\mathbf{p}'$ does not contain $r^{-\alpha}$. Let γ be the label product of $\mathbf{p}'$: $\gamma \in \overline{L}(U'') = \underline{L}(\widetilde{U''})$. Let $0 \neq \varepsilon$ be such that $\mathbb{F}_p[\gamma\varepsilon] = \underline{L}(\widetilde{U''})$. Clearly, both α and ε belong to $\underline{L}(\widetilde{U''})$ (the former because $\alpha \in \underline{L}(\widetilde{U}) = \underline{L}(\widetilde{U''})$. Now set $\hat{t} = (t^{r^{-\alpha}})^{\varepsilon}$, $U'' = V \cup \{r, r^{-\alpha}, s, \hat{t}\}$, $W = V \cup \{r, s, \hat{t}\}$. Then $\Gamma(W)$ contains the closed path obtained from $\mathbf{p}'$ by replacing $t^{r^{-\alpha}}$ with $\hat{t}$. This path has label product $\gamma\varepsilon$; hence, applying Lemma 8 to W, we get that $\gamma\varepsilon \in \underline{L}(\widetilde{W})$. As $\alpha \in \mathbb{F}_p[\gamma\varepsilon]$, it follows that $\alpha \in \underline{L}(\widetilde{W})$. Hence $W \approx U'''$, and by Proposition 7, (ii) $\gamma\varepsilon \in \underline{L}(\widetilde{W})$ implies $\gamma\varepsilon \in \underline{L}(\widetilde{U'''})$. As $\varepsilon \in \mathbb{F}_p[\gamma\varepsilon]$, it follows that $\varepsilon \in \underline{L}(\widetilde{U'''})$. On the other hand $\varepsilon \in \underline{L}(\widetilde{U''})$ and hence, by Lemma 6, (3), $U''' \approx U''$. We conclude that W satisfies both (d) and (e) (as in $\Gamma(U'')$ $t^{r^{-\alpha}} * s = 0$). □

Reversing the arrows and replacing $r^{-\alpha}$ by r^{α} in the proof of the previous Lemma, one obtains the following "dual" version:

Lemma 10. *Let $U = V \cup \{r, s, t\} \subseteq \mathcal{T}$, $V \cap \{r, s, t\} = \emptyset$. Suppose that* (a) $\Gamma(U)$ *is connected*; (b) $\Gamma(V \cup \{r, s\})$ *is either a chain or a cycle of length* ≥ 3; (c) $s * r$, $r * t$ *and $s * t$ are all nonzero. Set $W = V \cup \{r, s, \hat{t}\}$, where $\hat{t} = \left(t^{r^{\lambda}}\right)^{\mu}$, $\lambda, \mu \in \underline{L}(\widetilde{U})$. Then, for suitable choices of λ and μ the following holds*: (d) $U \approx W$; (e) $s * \hat{t} = 0$.

Lemma 11. *Let $U \subseteq \mathcal{T}$, and suppose that*:

(a) $\Gamma(U)$ *is connected.*
(b) $\Gamma(\widetilde{U})$ *is one-way.*

Then there exists $W \subseteq \mathcal{T}$ such that: (i) $U \approx W$; (ii) *for suitable $s_1, s_2, s_3 \in W$, $\Gamma(s_1, s_2, s_3)$ is a cycle.*

Proof. By Proposition 4 $\Gamma(\widetilde{U})$ is connected, and by (b) there are suitable $s_1, s_2 \in \widetilde{U}$ such that $s_1 * s_2 \neq 0$, but $s_2 * s_1 = 0$. It follows from Proposition 5 that there exists $t \in \widetilde{U}$ such that t is opposite to both s_1 and s_2. In particular, we may apply Lemma 9 (with $V = \emptyset$, $r = s_1$, $s = s_2$) and deduce that, for suitable $\lambda, \mu \in \underline{L}(\widetilde{U})$, $\left(t^{s_1^{\lambda}}\right)^{\mu} * s_2 = 0$ and hence also $t^{s_1^{\lambda}} * s_2 = 0$. Set $t' = t^{s_1^{\lambda}}$. Clearly $\{s_1, s_2, t\} \approx \{s_1, s_2, t'\}$, and $\Gamma(s_1, s_2, t')$ has exactly four arcs: $s_1 \longrightarrow s_2$, $s_2 \longrightarrow t'$, $t' \longrightarrow s_1$ and $s_1 \longrightarrow t'$. Next, we may apply Lemma 10 to $\{s_1, s_2, t'\}$ (with $V = \emptyset$, $r = s_2$, $s = s_1$, $t = t'$) and deduce that, for suitable $\lambda, \mu \in \underline{L}(\widetilde{U})$, $s_1 * \left(t'^{s_2^{\lambda}}\right)^{\mu} = 0$ and hence also $s_1 * t'^{s_2^{\lambda}} = 0$. Set $s_3 = t'^{s_2^{\lambda}}$. Then $\{s_1, s_2, t'\} \approx \{s_1, s_2, s_3\}$, and $\Gamma(s_1, s_2, s_3)$ has exactly three arcs: $s_1 \longrightarrow s_2$, $s_2 \longrightarrow s_3$, $s_3 \longrightarrow s_1$. Thus $\Gamma(s_1, s_2, s_3)$ is a cycle, and we are done by Lemma 5(c). □

Lemma 12. *Assume $char(K) \neq 2$. Let $V \subseteq \mathcal{T}$, and suppose that*:

(a) $\Gamma(V)$ *is connected.*
(b) *There exist $s_1, s_2, \ldots, s_h \in \overline{V}$ such that $\Gamma(s_1, s_2, \ldots, s_h)$ is a cycle.*

Then there exists $\overline{V} \approx V$ such that $s_1, s_2, \ldots, s_h \in \overline{V}$ and $\Gamma(s_1, s_2, \ldots, s_h, \bar{t})$ is connected for every $\bar{t} \in \overline{V}$.

Proof. Set $n(V) = |\{t \in V \mid \Gamma(s_1, s_2, \ldots, s_h, t) \text{ is not connected}\}|$ and suppose that $n(V) \geq 0$. Under this assumption, we show that we can find $V' \approx V$ such that $s_1, s_2, \ldots, s_h \in V'$ and $n(V') \leq n(V)$. For, let $t \in V$ be such that $\Gamma(s_1, s_2, \ldots, s_h, t)$ is not connected. Since $\Gamma(V)$ is connected, there exists a path $\mathbf{p} := r_0 \longrightarrow r_1 \longrightarrow \cdots \longrightarrow r_k = t$, where $r_0 \in \{s_1, s_2, \ldots, s_h\}$. Choose $\mathbf{p}$ so as to have minimal length (thus $r_i \neq t$ for $i \neq k$, and for $i \leq j$ $r_i * r_j = 0$ unless $i + 1 = j$). By Lemma 2, $r_{k-2} * t^{r_{k-1}} \neq 0$ in $\Gamma(\widetilde{V})$, whereas, for all $i \leq k-2$, $r_i * t^{r_{k-1}} = 0$. Thus, applying repeatedly Lemma 2, one also checks that in $\Gamma(\widetilde{V})$ $r_{k-3} * t^{r_{k-1}r_{k-2}}, \ldots, r_0 * t^{r_{k-1}r_{k-2}\cdots r_1}$ are all nonzero. Set $t' = t^{r_{k-1}r_{k-2}\cdots r_1}$. As $t' \in t^{\langle V-\{t\}\rangle}$, by Lemma 6(2) $V' = (V - \{t\}) \cup \{t'\} \approx V$. Thus $\Gamma(V')$ is connected, and therefore there exists in $\Gamma(V')$ a path $\mathbf{p}' := t' = q_0 \longrightarrow q_1 \longrightarrow \cdots \longrightarrow q_k$, where $q_k \in \{s_1, s_2, \ldots, s_h\}$. Again, choose $\mathbf{p}'$ so as to have minimal length. Replacing t' with $(t')^{q_1}$, we obtain a path $\mathbf{p}'' := (t')^{q_1} \longrightarrow q_2 \longrightarrow \cdots \longrightarrow q_k$ of length one less. In doing so, the arc $r_0 \longrightarrow t^{q_1}$ might get lost. If so, and provided $char(K) \neq 2$, we can replace q_1 by q_1^{-1} (still keeping us "equivalent" to V, by Lemma 6(3)), so that $r_0 * (t')^{q_1^{-1}} \neq 0$. Iterating the above procedure, we eventually obtain a transvection $t'' = (t')^{q_1^{\varepsilon_1} q_2^{\varepsilon_2} \cdots q_{k-1}^{\varepsilon_{k-1}}}$ ($\varepsilon_i = \pm 1$ for $1 \leq i \leq k$) such that, provided the ε_i's are suitably chosen, both $r_0 * t''$ and $t'' * q_k$ are nonzero. Therefore, as $r_0, q_k \in \{s_1, s_2, \ldots, s_h\}$, $\Gamma(s_1, s_2, \ldots, s_h, t'')$ is connected. Setting $V'' = (V' - \{t'\}) \cup \{t''\}$ (where the "original" V' may have been altered by suitable choices of ε_i's), we conclude that $V'' \approx V$ and $n(V'') = n(V) - 1$.

Now, repeated application of the above argument leads us to a sequence of pair-wise equivalent transvection sets with strictly decreasing $n(V)$'s. Thus, eventually we must obtain a set $\overline{V} \approx V$ satisfying the statement of the Lemma. □

Lemma 13. *Let $V = \{s_1, s_2, \ldots, s_h, t\} \subseteq \mathcal{T}$, where $|V| = h + 1$ and $h \geq 3$. Suppose that $\Gamma(V)$ is connected and $\Gamma(s_1, s_2, \ldots, s_h)$ is a cycle. For $r \in \mathcal{T}$, $U = \{s_1, s_2, \ldots, s_h, r\}$, denote by $I(r)$ the set of all indices i for which $s_i * r \neq 0$, by $J(r)$ the set of all indices j for which $r * s_j \neq 0$. Then*:

(1) *There exists $\tilde{t} \in \mathcal{T}$, such that $\widetilde{V} = \{s_1, s_2, \ldots, s_h, \tilde{t}\} \approx V$ and $I(\tilde{t}) = \{1, 2, \ldots, h\}$.*
(2) *There exists $\hat{t} \in \mathcal{T}$, such that $\widehat{V} = \{s_1, s_2, \ldots, s_h, \hat{t}\} \approx V$ and $J(\hat{t}) = \{1, 2, \ldots, h\}$.*

Proof. (1) As $\Gamma(V)$ is connected, $I(t) \neq \emptyset$. Assuming $|I(t)| \leq h$, there must exist an index k such that $k - 1 \notin I(t)$, but $k \in I(t)$ (here it is understood that $k - 1 = h$ if $k = 1$). Setting $t' = t^{s_k}$, it then follows that $I(t') = I(t) \cup \{k - 1\}$. Thus $|I(t')| = |I(t)| + 1$, and obviously $\{s_1, s_2, \ldots, s_h, t'\}$ is equivalent to V (by Lemma 6(1)). It is clear that, iterating this procedure, we end up with a transvection $\tilde{t}$ such that $\widetilde{V} = \{s_1, s_2, \ldots, s_h, \tilde{t}\}$ is equivalent to V and $|I(\tilde{t})| = h$.

(2) As $\Gamma(V)$ is connected, $J(t) \neq \emptyset$. Observe that if $|J(t)| \leq h$, there must exist an index k such that $k \in J(t)$, but $k + 1 \notin J(t)$ (here it is understood that $k + 1 = 1$ if $k = h$). Then argue as in (1). □

Lemma 14. *Let $V = \{s_1, s_2, \ldots, s_h, t\} \subseteq \mathcal{T}$, where $|V| = h + 1$ and $h \geq 3$. Suppose that $\Gamma(V)$ is connected and $\Gamma(s_1, s_2, \ldots, s_h)$ is a cycle. Then there exists $\bar{t} \in \mathcal{T}$ such that $\overline{V} = \{s_1, s_2, \ldots, s_h, \bar{t}\}$ is equivalent to V and $s_i * \bar{t} \neq 0$ iff $i = h$.*

Proof. Observe that, if a set $U = \{s_1, s_2, \ldots, s_h, r\}$ satisfies the assumptions of the Lemma and $k, k + 1 \in I(r)$, then the set $\{s_{k+1}, s_k, r\}$ satisfies the assumptions

of Lemma 10. Thus, there exist $\lambda, \mu \in \underline{L}(\widetilde{U})$ such that, setting $r' = \left(r^{s_{k+1}^{\lambda}}\right)^{\mu}$, $s_k * r' = 0$. Hence $I(r') = I(r) - \{k\}$ (and clearly $U' = \{s_1, s_2, \ldots, s_h, r'\} \approx U$). In view of Lemma 13, we may apply this argument starting from $r = \tilde{t}$, $k = 1$, then considering r', $k = 2$ and so forth up to $k = h - 1$, eventually obtaining a transvection $\bar{t}$ such that $I(\bar{t}) = \{h\}$ and $\overline{V} = \{s_1, s_2, \ldots, s_h, \bar{t}\} \approx V$. □

Lemma 15. *Let* $V = \{s_1, s_2, \ldots, s_h, t_1, t_2\} \subseteq \mathcal{T}$, *where* $|V| = h + 2$ *and* $h \geq 3$. *Suppose that*:

(a) $\Gamma(s_1, s_2, \ldots, s_h)$ *is a cycle.*
(b) $\Gamma(s_1, s_2, \ldots, s_h, t_1)$ *and* $\Gamma(s_1, s_2, \ldots, s_h, t_2)$ *are connected.*
(c) $s_i * t_1 \neq 0$ *iff* $i = h$, $s_i * t_2 \neq 0$ *iff* $i = h$.
(d) $t_1 * s_1 = t_2 * s_1 = 0$.
(e) $t_1 * t_2 \neq 0$. *Then there exists a set* $\widehat{V} = \{s_1, s_2, \ldots, s_h, \hat{t}_1, \hat{t}_2\}$ *equivalent to* V, *such that*:
(f) $s_i * \hat{t}_1 \neq 0$ *iff* $i = h$.
(g) $\hat{t}_1 * s_1 \neq 0$.

Proof. (i) First, we show that we may assume that $t_2 * s_h \neq 0$. For, otherwise, (b) implies that there is $k < h$ such that $t_2 * s_k \neq 0$, whereas $t_2 * s_i = 0$ for $i \geq k$. It follows that $\Gamma(\{s_1, s_2, \ldots, s_h, t_1, t_2^{s_k}\})$ contains the arc $t_2^{s_k} \longrightarrow s_{k+1}$ while satisfying the assumptions of the lemma. If $k + 1 = h$ we are done. Otherwise, we repeat the process.

(ii) Next, suppose that $t_1 * s_h = 0$. In this case, we may apply Lemma 10 to the set $\{t_1, s_h, t_2\}$. Setting $t_2' = \left(t_2^{t_1^{\lambda}}\right)^{\mu}$ for suitable $\lambda, \mu \in K$, we obtain $\{s_h, t_1, t_2'\} \approx \{s_h, t_1, t_2\}$ and $s_h * t_2' = 0$. Obviously, by Lemma 5(c) $\{s_1, s_2, \ldots, s_h, t_1, t_2'\} \approx V$. Setting $\hat{t}_2 = t_2'^{s_h}$, one checks that $\hat{t}_2 * s_1 \neq 0$. Finally, setting $\hat{t}_1 = t_1^{\hat{t}_2}$, a little computation shows that $\hat{t}_1 * s_1$ is also nonzero, and moreover (f) holds.

(iii) Now, suppose that both $t_1 * s_h$ and $t_1 * s_i$, for some $i \neq h$, are nonzero. Arguing as in (i), we can find a suitable conjugate t_1' of t_1 such that $t_1' * s_{h-1} \neq 0$ (and obviously $t_1' * s_h \neq 0$). Hence, setting $U = V - \{t_2\}$, $r = s_{h-1}$, $s = s_h$, $t = t_1'$ and applying Lemma 9, we can pick a transvection $t_1'' = \left((t_1')^{s_{h-1}^{\lambda}}\right)^{\mu}$ such that, for suitable $\lambda, \mu \in K$, $V'' = \{s_1, s_2, \ldots, s_h, t_1''\}$ is equivalent to $\{s_1, s_2, \ldots, s_h, t_1\}$ and $t_1'' * s_h = 0$. By Lemma 5(c), it follows that $\{s_1, s_2, \ldots, s_h, t_1'', t_2\}$ is equivalent to V and hence we are brought back to (ii).

(iv) We are left with the case when $t_1 * s_i \neq 0$ iff $i = h$. Replacing t_1 by $t_1' = t_1^{s_1^{s_h}}$, we see that $t_1' * s_2$ and $t_1' * s_h$ are both nonzero. Hence, we are back to case (iii). □

Lemma 16. *Let* $V = \{s_1, s_2, \ldots, s_h, t\} \subseteq \mathcal{T}$, *where* $|V| = h + 1$ *and* $h \geq 3$. *Suppose that*:

(a) $\Gamma(s_1, s_2, \ldots, s_h)$ *is a cycle.*
(b) $s_i * t \neq 0$ *iff* $i = h$.
(c) $t * s_1 \neq 0$.

Then there exists a set $\widehat{V} = \{s_1, s_2, \ldots, s_{h-1}, \hat{s}_h, \hat{s}_{h+1}\}$ *equivalent to* V, *such that* $\Gamma(\widehat{V})$ *is a cycle.*

Proof. By Lemma 13 we can find $t' \in \mathcal{T}$, such that $V' = \{s_1, s_2, \ldots, s_h, t'\} \approx V$ and $J(t') = \{1, 2, \ldots, h\}$. Moreover, as $t * s_1 \neq 0$ already in $\Gamma(V)$, no conjugate of type r^{s_h} $(r \in \mathcal{T})$ is involved in the process. Hence V' still satisfies (b). Arguing as in Lemma 14 (using Lemma 9 this time, and taking decreasing values of k from $h-1$ to 1), we obtain a set $V'' = \{s_1, s_2, \ldots, s_h, t''\}$ equivalent to V, such that $J(t'') = \{1\}$ and V'' satisfies (b). Finally, we apply Lemma 9 to the set $\{t, s_1, s_h\}$ (note that $\Gamma(t, s_1)$ is a line): setting $\hat{s}_h = \left(s_h^{t''^{\lambda}}\right)^{\mu}$ for suitable $\lambda, \mu \in K$, and $\hat{s}_{h+1} = t$, we obtain the required set $\widehat{V}$. □

Lemma 17. *Assume* $char(K) \neq 2$. *Let* $V \subseteq \mathcal{T}$, *and suppose that*:

(a) $\Gamma(V)$ *is connected.*
(b) $V \supseteq \{s_1, s_2, \ldots, s_h\}$, $h \geq 3$, *such that* $\Gamma(s_1, s_2, \ldots, s_h)$ *is a cycle.*
(c) $\mathrm{rank}(H(V)) > h$.

Then there exists $\widehat{V} \approx V$ *such that* $\hat{s}_1, \hat{s}_2, \ldots, \hat{s}_{h+1} \in \widehat{V}$ *and* $\Gamma(\hat{s}_1, \hat{s}_2, \ldots, \hat{s}_{h+1})$ *is a cycle.*

Proof. Set $V = \{s_1, s_2, \ldots, s_h, t_1, t_2, \ldots, t_k\}$, where $|V| = h + k$. By Lemma 12 and via repeated application of Lemma 14, we may assume that, for each $j = 1, \ldots, k$, $\Gamma(s_1, s_2, \ldots, s_h, t_j)$ is connected and $s_i * t_j \neq 0$ iff $i = h$. It follows that $H(V)$ has the following shape:

$$H(V) = \begin{bmatrix} A & \overset{0}{\overbrace{\quad}} \\ C & \underset{****}{B} \end{bmatrix},$$

where: $A = (a_{rs})$ is a square matrix of size h such that $a_{i,i+1} \neq 0$ for $1 \leq i \leq h-1$; $a_{h1} \neq 0$ and $a_{rs} = 0$ elsewhere; $B = (b_{lm})$ is a square matrix of size k; $C = (c_{uv})$ is a $(k \times h)$-matrix with no zero rows; 0 denotes the null matrix of type $(h-1) \times k$, and $****$ stands for a row with k nonzero entries.

If $c_{u1} \neq 0$ for some u, we may apply Lemma 16 to the set $\{s_1, s_2, \ldots, s_h, t_u\}$ obtaining the set $\{s_1, s_2, \ldots, s_{h-1}, \hat{s}_h, \hat{s}_{h+1}\}$. Then the set $\widehat{V} = \{s_1, s_2, \ldots, s_{h-1}, \hat{s}_h, \hat{s}_{h+1}\} \cup \{t_i \mid i \neq k\}$ will do. So, let us suppose that $c_{u1} = 0$ for every u. If $B = 0$, then the last k rows of $H(V)$ would be linear combinations of the first $h-1$ rows, and therefore $H(V)$ would have rank h, against assumption (c). Thus $b_{lm} \neq 0$ for some $l \neq m$, which means that $t_l * t_m \neq 0$ in $\Gamma(V)$. But now we are in a position to apply Lemma 15 to the set $\{s_1, s_2, \ldots, s_h, t_l, t_m\}$, which takes us back, up to equivalence, to the case where $c_{u1} \neq 0$ for some u. □

Proposition 9. *Assume* $char(K) \neq 2$. *Let* $U = \{s_1, s_2, \ldots, s_h, t_1, t_2, \ldots, t_k\} \subseteq \mathcal{T}$, *where* $|U| = h + k$ *and* $h \geq 3$, *and suppose that*:

(a) $\Gamma(U)$ *is connected.*
(b) $\Gamma(s_1, s_2, \ldots, s_h)$ *is a cycle.*
(c) $\mathrm{rank}(H(U)) = h$.

Then, up to equivalence, we may assume that the following holds for each $l = 1, \ldots, k$:

(d) $t_l * s_j \neq 0$ *for some* j.
(e) $s_i * t_l \neq 0$ *iff* $i = h$.

(f) $t_l * s_1 = 0$.
(g) $t_l * t_m = 0$ *for all* $m = 1, \ldots, k$.

Proof. As in Lemma 17, we may assume that (d) and (e) hold in $\Gamma(U)$. It follows that $H(U)$ has the shape described in Lemma 17. As $\operatorname{rank}(H(U)) = h$, and clearly B has zero diagonal, the last k rows of $H(U)$ must be linear combinations of the first $h-1$ rows. It follows that $B = 0$ and the first column of C is also null, that is, (f) and (g) hold. □

Definition 5. A set $U \subseteq \mathcal{T}$ fulfilling all conditions from (a) to (g) of Proposition 9 is said to be in "normal form".

Corollary 6. *If* $U \subseteq \mathcal{T}$ *is in "normal form", then the equality* $\underline{L}(\widetilde{U}) = \overline{L}(U)$ *holds.*

Proof. Suppose that U is in "normal form". Then it is clear that, setting $V = \{t_1, t_2, \ldots, t_k\}$, condition (d) of Lemma 8 is fulfilled. □

9. MAIN THEOREM

We focus first on some elementary observations, which yield in particular necessary conditions for a given set U of transvections in $SL(n, K)$ to generate a subgroup isomorphic to a special linear group $SL(m, L)$ for some $m \leq n$ and some subfield L of the field K.

Let $U = \{t_1, \ldots, t_h\}$. Suppose that $\operatorname{rank}(C(U)) = r$ and $\operatorname{rank}(A(U)) = s$. Without loss we may assume that $(c(t_1), \ldots, c(t_r))$ is a basis for the subspace of K^n generated by the centres of the elements of U. Extending $(c(t_1), \ldots, c(t_r))$, we obtain a basis of K^n, with respect to which $C(U)$ has shape $\begin{bmatrix} \mathrm{Id}_r & * \\ 0 & 0_{n-r} \end{bmatrix}$ and the elements of U (and hence of $\langle U \rangle$) have shape $\begin{bmatrix} X & * \\ 0 & \mathrm{Id}_{n-r} \end{bmatrix}$ [In particular this shows that, if t is any transvection in $\langle U \rangle$, then $c(t)$ is a linear combination of $c(t_1), \ldots, c(t_r)$.]

Dually, we may choose a basis of the row space ${}^nK$ such that, with respect to this basis, $A(U)$ has shape $\begin{bmatrix} \mathrm{Id}_s & 0 \\ * & 0_{n-s} \end{bmatrix}$ and the elements of $\langle U \rangle$ have shape $\begin{bmatrix} Y & 0 \\ * & \mathrm{Id}_{n-s} \end{bmatrix}$ [In particular this shows that, if t is any transvection in $\langle U \rangle$, then $a(t)$ is a linear combination of $a(t_1), \ldots, a(t_s)$.]

Let π_r (${}_r\pi$) be the map sending each vector of K^n (${}^nK$) to the vector of K^r (${}^rK$) obtained by deletion of the last $n-r$ components. Let us consider the map $\Pi_r : \langle U \rangle \longrightarrow SL(r, K)$ sending $t = \begin{bmatrix} X_t & * \\ 0 & \mathrm{Id}_{n-r} \end{bmatrix}$ to the $r \times r$ matrix X_t. Clearly, Π_r is a homomorphism; furthermore, if $t \in U$ then X_t is either the identity or a transvection in $SL(r, K)$. Indeed, if $t = \mathrm{Id} + c(t)a(t)$, then $\Pi_r(t) = \mathrm{Id} + \pi_r(c(t))_r\pi(a(t))$. As ${}_r\pi(a(t))\pi_r(c(t)) = a(t)c(t)$, the claim follows.

With a slight abuse, we write

$$A(\Pi_r(U)) = \begin{bmatrix} {}_r\pi(a(t_1)) \\ {}_r\pi(a(t_2)) \\ \cdots \\ {}_r\pi(a(t_h)) \end{bmatrix},$$

$C(\Pi_r(U)) = [\pi_r(c(t_1))\pi_r(c(t_2)) \cdots \pi_r(c(t_h))]$, $H(\Pi_r(U)) = A(\Pi_r(U)) \cdot C(\Pi_r(U))$. It then follows from the remark above that $H(\Pi_r(U)) = H(U)$. Furthermore, by our choice of basis $C(\Pi_r(U)) = [\mathrm{Id}_r *]$.

The above arguments can be dualized to the map ${}_s\Pi : \langle U \rangle \longrightarrow SL(s, K)$ sending $t = \begin{bmatrix} Y_t & 0 \\ * & \mathrm{Id}_{n-s} \end{bmatrix}$ to the $s \times s$ matrix Y_t. Clearly ${}_s\Pi$ is a group homomorphism with same behaviour as Π_r. In particular, they can be specialized to yield to following:

Lemma 18. *If $\langle U \rangle$ is isomorphic to $SL(m, L)$ for some $m \leq n$ and some subfield L of the field K, then the maps Π_r, ${}_s\Pi$ defined above are monomorphisms. In particular, $\Pi_r(U)$ and ${}_s\Pi(U)$ are sets of transvections of the same cardinality as U. Furthermore,* $\mathrm{rank}(C(\Pi_r(U))) = r$ *and* $\mathrm{rank}(A({}_s\Pi(U))) = s$.

Proof. $\ker(\pi_r)$ $[\ker({}_s\pi)]$ is an elementary abelian normal p-subgroup of $\langle U \rangle$. Since $O_p(SL(m, L)) = 1$ for all m and L, the first part of the statement follows. The rest is obvious. □

Main Theorem. *Let $char(K) = p \neq 2, 3$. Suppose that $\Gamma(U)$ is connected and $\Gamma(\widetilde{U})$ is a one-way digraph* (*equivalently*: *there exists a set V equivalent to U such that $\Gamma(V)$ is one-way*). *Then the following holds*:

(a) $\underline{L}(\widetilde{U}) = \overline{L}(U)$.
(b) *Set* $r = \mathrm{rank}(H(U))$, $\mathbb{F}_p[\delta] = \overline{L}(U)$. *Then* $r > 2$, $\langle U \rangle$ *contains a subset V consisting of r transvections such that $\Gamma(V)$ is a cycle with label product δ, and $\langle V \rangle$ is isomorphic to $SL(r, \overline{L}(U))$.*
(c) *$\langle U \rangle$ is the semi-direct product of a normal p-subgroup N and a subgroup S isomorphic to $SL(r, \overline{L}(U))$. Furthermore, N contains a normal elementary abelian subgroup M such that the quotient group N/M is also elementary abelian.*
(d) $N = 1$ *if and only if $A(U)$, $C(U)$ and $H(U)$ have the same rank.*

Proof. We will prove the statement in several steps. At each step it will be shown that U can transformed into an equivalent set V satisfying the same assumptions as U, plus certain suitable extra properties.

Step 1. Up to equivalence, we may assume that $\Gamma(U)$ contains as a subgraph a cycle $\Gamma(s_1, \ldots, s_h)$ of length $h \geq 3$.

By Lemma 11, there exists $V \approx U$ and $s_1, s_2, s_3 \in V$ such that the subgraph $\Gamma(s_1, s_2, s_3)$ of $\Gamma(V)$ is a cycle of length 3. Obviously, as V is equivalent to U, $\Gamma(V)$ is connected. Moreover, $\Gamma(\widetilde{V})$ is a one-way digraph, as, say, $s_1 * s_2 \neq 0$ but $s_2 * s_1 = 0$. Thus (cf. Corollary 4) U fulfills the statement of the theorem if and only if so does V.

Step 2. Set $r = \mathrm{rank}(H(U))$. Then $r \geq 3$, and up to equivalence we may assume that $\Gamma(U)$ contains a cycle $\Gamma(s_1, \ldots, s_r)$ of length r.

By Step 1, we may assume that $\Gamma(U)$ contains a cycle $\Gamma(s_1, \ldots, s_h)$ of length $h \geq 3$. Since $\det H(\{s_1, \ldots, s_h\}) \neq 0$, it follows that $r \geq h \geq 3$. If $r > h$, repeated application of Lemma 17 shows that there exists $\widehat{U} \approx U$ and $\{\hat{s}_1, \ldots, \hat{s}_r\} \subseteq \widehat{U}$ such that $\Gamma(\hat{s}_1, \ldots, \hat{s}_r)$ is a cycle. As $\mathrm{rank}(H(U)) = \mathrm{rank}(H(\widehat{U}))$, we are done.

Step 3. Up to equivalence, we may assume that U is reduced to "normal form". Hence $\underline{L}(\widetilde{U}) = \overline{L}(U)$, that is: (a) holds.

By steps 1 and 2, U satisfies the assumptions of Proposition 9. Whence the claim.

Step 4. Up to equivalence, we may assume that $\underline{L}(\widetilde{U}) = \langle\alpha\rangle$, where α is the label product along the cycle $\Gamma(s_1, \ldots, s_r)$. In particular, (b) holds with $V = \{s_1, s_2, \ldots, s_r\}$. Furthermore, we may assume that all labels in $\Gamma(U)$ belong to $\underline{L}(\widetilde{U})$.

Assume that $U = \{s_1, s_2, \ldots, s_r, t_1, t_2, \ldots, t_k\}$ is in "normal form" (Proposition 9, with $h = r$). Let α be the label product along the cycle $\Gamma(s_1, \ldots, s_r)$ and set $\underline{L}(\widetilde{U}) = \mathbb{F}_p[\delta]$. If $\langle\alpha\rangle \neq \underline{L}(\widetilde{U})$, then we replace U with the equivalent set $(U\backslash\{s_1\}) \cup \{s_1^{\delta\alpha^{-1}}\}$. Clearly this will do. It is also clear that we may assume that the arc $s_r \longrightarrow s_1$ is labelled α, while all the remaining arcs of the cycle $\Gamma(s_1, \ldots, s_r)$ are labelled 1. Furthermore, we may impose that each arc $s_r \longrightarrow t_l$ is also labelled 1, so that eventually all the labels of $\Gamma(U)$ belong to $\overline{L}(U)$. Whence the statement.

Step 5. (c) holds.

Suppose that $\mathrm{rank}(C(U)) = r_1$ and consider the homomorphism $\Pi_{r_1} : \langle U\rangle \longrightarrow SL(r_1, K)$ defined above. Next, suppose that $\mathrm{rank}(A(\Pi_{r_1}(U))) = r_2$. Consider the homomorphism ${}_{r_2}\Pi : \Pi_{r_1}(\langle U\rangle) \longrightarrow SL(r_2, K)$ and the composition $\Pi = {}_{r_2}\Pi \circ \Pi_{r_1}$. Set $A(\Pi(U)) = A_2$, $C(\Pi(U)) = C_2$, $H(\Pi(U)) = H_2$. As $C(\Pi_{r_1}(U)) = [\mathrm{Id}_{r_1} *]$, and C_2 is obtained multiplying the latter matrix on the left by a non-singular matrix and deleting the last $r_1 - r_2$ rows, it follows that $\mathrm{rank}(C_2) = r_2$. Now, as we may assume $A_2 = \left[\begin{smallmatrix} \mathrm{Id}_{r_2} \\ * \end{smallmatrix}\right]$, $H_2 = A_2 \cdot C_2 = \left[\begin{smallmatrix} C_2 \\ * \end{smallmatrix}\right]$. Hence $\mathrm{rank}(H_2) = r_2$. On the other hand $H(\Pi(U)) = H(U)$, whence $r = r_2$.

Recall that, by Step 2, $\Gamma(s_1, \ldots, s_r)$ is a cycle of length r. As $H(U)$ is Π-stable, it follows that $\Gamma(\Pi(s_1), \ldots, \Pi(s_r))$ is also a cycle. In fact, Theorem 1 shows that, up to conjugation within $GL(r, K)$, we may assume that $\{\Pi(s_1), \ldots, \Pi(s_r)\} = \{T_{r1}(\alpha), T_{12}(1), \ldots, T_{(r-1)r}(1)\}$ and hence the group $\langle\Pi(s_1), \ldots, \Pi(s_r)\rangle = SL(r, \langle\alpha\rangle) = SL(r, \overline{L}(U))$ (by Step 4).

Now we turn to the subgroup $\langle\Pi(t_1), \ldots, \Pi(t_k)\rangle$. W.l.o.g., we assume that U is as in Step 4 and $\{\Pi(s_1), \ldots, \Pi(s_r)\} = \{T_{r1}(\alpha), T_{12}(1), \ldots, T_{(r-1)r}(1)\}$. Then $a(\Pi(s_j))c(\Pi(t_l)) = e_j c(\Pi(t_l)) = 0$ for $j \leq r$ and $a(\Pi(s_r))c(\Pi(t_l)) = e_r c(\Pi(t_l)) = 1$. Hence $c(\Pi(t_l)) = e'_r$ for each $l = 1, \ldots, k$. On the other hand, $a(\Pi(t_l))c(\Pi(s_j)) = a(\Pi(t_l))e'_{j-1}$ for $j \geq 1$ and $a(\Pi(t_l))c(\Pi(s_1)) = a(\Pi(t_l))\alpha e'_r$. Since $H(\Pi(U)) = H(U)$ and all the labels of $\Gamma(U)$ belong to $\overline{L}(U)$, it follows that the components of $a(\Pi(t_l))$ and $c(\Pi(t_l)$ belong to $\overline{L}(U)$ for all $l = 1, \ldots, k$. This in turn implies that $\langle\Pi(t_1), \ldots, \Pi(t_k)\rangle$ is contained in $SL(r, \overline{L}(U))$.

Set $N = \ker\Pi$, $S = \langle s_1, \ldots, s_r\rangle$. By Theorem 1, $S \simeq SL(r, \overline{L}(U))$. By the above, $\Pi(\langle U\rangle) = \Pi(S) = SL(r, \overline{L}(U))$. Hence $\Pi_{|S}$ is an isomorphism. It follows that $S \cap N = 1$ and $\langle U\rangle = [N]S$, a semidirect product. This proves (c).

Step 6. (d) holds.

If $N = 1$, then $\langle U\rangle = S$ and hence $t_1, t_2, \ldots, t_k \in \langle s_1, \ldots, s_r\rangle$. By the remarks introducing the current section, the axes and centres of $t_1, t_2, \ldots, t_k$ are combinations of the axes and centres of $s_1, \ldots, s_r$. We conclude that $\mathrm{rank}(A(U)) = \mathrm{rank}(C(U)) = r$.

Conversely, suppose that $\operatorname{rank}(A(U)) = \operatorname{rank}(C(U)) = r$. By Proposition 8, we may assume that $U = \{s_1, s_2, \ldots, s_r, t_1, t_2, \ldots, t_k\}$ is in "normal form", and furthermore that the axes and centres of $t_1, t_2, \ldots, t_k$ are combinations of the axes and centres of $s_1, \ldots, s_r$. Let $R \in N$. Then $R = \mathrm{Id} + \sum_{i,j\in[r]} \xi_{ij} c(s_i) a(s_j)$ for suitable coefficients $\xi_{ij} \in K$, $\mathrm{Id} = \Pi(R) = \mathrm{Id} + \sum_{i,j\in[r]} \xi_{ij} c(\Pi(s_i)) a(\Pi(s_j))$, and hence $\sum_{i,j\in[r]} \xi_{ij} c(\Pi(s_i)) a(\Pi(s_j)) = 0$. As $a(\Pi(s_j)) = e_j$ and $c(\Pi(s_i)) = e'_{i-1}$, we get $\sum_{i,j\in[r]} \xi_{ij} E_{i-1,j} = 0$, whence $\xi_{ij} = 0$ for all i, j, that is $R = \mathrm{Id}$. □

Remark. The proof above shows that, up to equivalence, U contains a subset V such that $\Gamma(V)$ is a cycle of length r. In particular, if $N = 1$, that is $\langle U \rangle = SL(r, \overline{L}(U))$, then $\langle U \rangle = \langle V \rangle$. It then follows, by the "Simultaneous Conjugation" theorem, that $\langle U \rangle$ is conjugated to the *standard* embedding

$$\begin{bmatrix} SL(r, \overline{L}(U)) & 0 \\ 0 & \mathrm{Id}_{n-r} \end{bmatrix}.$$

Finally, we wish to show that the conditions imposed on $\Gamma(U)$ in the Main Theorem are necessarily satisfied whenever a set of transvections U is given, such that $\langle U \rangle$ is isomorphic to $SL(m, L)$ for some $m \leq n$ and some subfield L of the field K. To this purpose, the following well-known cohomological result is needed:

Lemma 19. *Let K be a field, $V = K^n$, T a subspace of V of dimension $m < n$, and assume that $\sigma : SL(T) \to GL(V)$ is a monomorphism such that, for every $f \in SL(T)$:* (i) $f^\sigma_{|T} = f$, (ii) $f^\sigma_{|V/T} = \mathrm{Id}_{V/T}$ *(i.e., in matrix terms, with respect to a basis of V extending a basis of T, $M(f^\sigma) = \left[\begin{smallmatrix} M(f) & * \\ 0 & \mathrm{Id} \end{smallmatrix}\right]$). Then there exists a subspace U of V such that*: (i) $V = T \oplus U$, ii) *for every $f \in SL(T)$ $f^\sigma(U) = U$, and $f^\sigma_{|U} = \mathrm{Id}_U$ (i.e., there exists a basis of V with respect to which $M(f^\sigma) = \left[\begin{smallmatrix} M(f) & 0 \\ 0 & \mathrm{Id} \end{smallmatrix}\right]$), unless one of the following holds*:

(a) $m = 2$ *and* $char(K) = 2$.
(b) $m = 3$ *and* $K = \mathbb{F}_2$.

The above statement is in fact equivalent to asserting the triviality of the first cohomology group $H^1(SL(T), T)$ unless cases (a) or (b) occur, and its proof goes back to Higman (1962, Lemma 4).

We also record the following:

Lemma 20. *Suppose that $\langle U \rangle$ acts irreducibly on K^n. Then $\Gamma(U)$ is connected.*

Proof. Let $U = \{t_1, \ldots, t_h\}$ and assume that $\Gamma(U)$ is not connected. Then there exist two nodes t_i, t_j such that there is no path from t_i to t_j. Let V be the set of all nodes in U from which there is a path to t_j. Let C_V be the set of the centres of the transvections belonging to V. Set $S = \langle C_V \rangle$. Note that $a(t_i)c = 0$ $\forall c \in C_V$. For, otherwise, there would be a path $t_i \to t_c \to \cdots \to t_j$ for some $c \in C_V$. This implies $S \subseteq a(t_i)$. Now we observe that, if $s \in S$, written as $s = \sum \lambda_m c_m$ ($c \in C_V$), and $s \notin a(t_l)$ for some l, then $t_l * c_m \neq 0$ for some m. But then there is a path $t_l \to \cdots \to t_j$, which means that $c(t_l) \in C_V$. Thus $S \subseteq a(t_l)$ $\forall t_l$ such that $c(t_l) \notin C_V$. It follows that S is $\langle U \rangle$-stable, and hence $\langle U \rangle$ is reducible. □

Remark. The converse of the above statement is obviously false, e.g., take the reducible embedding

$$SL(r,K) \hookrightarrow \langle U\rangle = \begin{bmatrix} SL(r,K) & 0 \\ 0 & \mathrm{Id}_{n-r} \end{bmatrix} \subset SL(n,K),\ \ 2 < r < n, \quad \text{where}$$
$$U = \{T_{12}(1), T_{23}(1), \ldots, T_{r1}(\delta)\},\ \ K = \mathbb{F}_p[\delta].$$

However, the following can be proved:

$\langle U\rangle$ acts irreducibly on K^n if and only if: the centres of the elements of U span K^n; the axes of the elements of U span the row space ${}^nK$; $\Gamma(U)$ is connected.

We can now prove a converse of the Main Theorem, provided the unipotent radical N is trivial.

Proposition 10. *Let U be a finite set of transvections in $SL(n,K)$, where $n > 2$ and $char(K) \neq 2$. Suppose that the group $\langle U\rangle$ is isomorphic to $SL(m,L)$ for some $2 < m \leq n$ and some subfield L of the field K. Then $\Gamma(U)$ is connected and $\Gamma(\widetilde{U})$ is a one-way digraph. Furthermore, $m = \mathrm{rank}(H(U))$ and $L = \overline{L}(U)$.*

Proof. Let us consider the irreducible constituents of $\langle U\rangle$ on the natural $SL(n,K)$-module K^n. As U is a set of transvections in $SL(n,K)$, by rank reasons these constituents are all trivial but one. Let θ denote such non-trivial constituent, and suppose that $\dim\theta = r$. Using Lemma 19, one sees that, up to conjugation, $\langle U\rangle$ can be reduced to the standard shape:

$$\begin{bmatrix} X & 0 \\ 0 & \mathrm{Id}_{n-r} \end{bmatrix},$$

where $X = \theta(\langle U\rangle)$ is an irreducible subgroup of $SL(r,K)$ isomorphic to $\langle U\rangle$. As the projection of U onto X is a transvection set, it follows from the classification of the irreducible subgroups generated by transvections (Wagner, 1974; Zalesskii and Serežkin, 1976) that $m = r$. It then also follows by Lemma 20 that $\Gamma(\theta(U))$, and hence $\Gamma(U)$, is connected. Finally, $\Gamma(\widetilde{U})$ is a one-way digraph. Indeed, as $m \geq 3$, $\theta(\widetilde{U})$ contains all the transvections in $SL(r,L)$. Note that the above also shows that $r = \dim\theta = \mathrm{rank}(H(U))$. That is, the rank of the Humphries matrix of U coincides with the degree of a non-trivial irreducible constituent of $\langle U\rangle$. □

Remark. We observe explicitly that if $\langle U\rangle$ is isomorphic to $N \cdot SL(m,L)$, where N a non-trivial normal p-subgroup, then $\Gamma(U)$ need not be connected, as easy examples show already when $n = 3$ and $|U| = 3$.

FINAL REMARKS

What happens if $\Gamma(\widetilde{U})$ is NOT a one-way digraph? If $char(K)$ is odd, the classification of irreducible groups generated by transvections shows that symplectic and unitary groups over subfields of K are bound to arise. In both cases, since the elements of $\widetilde{U}$ preserve a reflexive form, $\Gamma(\widetilde{U})$ cannot be one-way. $char(K) = 2$ is a richer world. Certain orthogonal and symmetric groups, as well as monomial

subgroups of $SL(n, K)$, also arise (and here again $\Gamma(\widetilde{U})$ is not one-way), plus the subgroup $3 \cdot \mathbb{A}_6$ of $SL(3, 4)$ considered in Lemma 7, plus a cross embedding 3. $P\Omega^{-,\pi}(6, 3) \subset SL(6, 4)$.

The statement of the Main Theorem is false in general when $char(K) = 2$, an exception being provided by the subgroup $3 \cdot \mathbb{A}_6$ of $SL(3, 4)$. Indeed, this group is generated by a set U of three transvections such that $\Gamma(U)$ is connected and $\Gamma(\widetilde{U})$ is one-way. On the other hand, the exclusion of characteristic 3 seems only to depend on technical reasons (the exception $|K| = 9$ arising from the use of Dickson's Lemma), and might be dealt with *ad hoc* arguments.

Drawing from the results of Humphries (1985, 1987) it is shown that if U is a set of transvections in $SL(n, K)$, K a finite field, and the subgroup $H = \langle R_t \mid t \in U \rangle$ is irreducible, then $\Gamma(U)$ is connected and there is a transvection set V equivalent to U such that either $\Gamma(V)$ is one-way or $\Gamma(V)$ is a "tree" (that is, in $\Gamma(V)$ there are no cycles of length greater than 2). In the former case $H = SL(n, K)$, whereas in the latter case either H is the symplectic group $Sp(n, K)$ or $p = 2$ and $H \subset Sp(n, K)$ is an orthogonal or a symmetric group. (As for the symplectic case, it was shown in Brown and Humphries, 1986a,b (but see also McLaughlin, 1967) that if U is a set of symplectic transvections in $SL(n, K)$, K an arbitrary field, whose centres span $K^n$and such that $\Gamma(U)$ is connected, then the subgroup $H = \langle R_t \mid t \in U \rangle$ is the full symplectic group $Sp(n, K)$.) Obviously, the unitary groups (as well as the rest of the aforementioned groups in characteristic 2, if $|K| > 2$) fail to show up in the Brown–Humphries context, since only full root subgroups are considered.

In our setting, while a full treatment of the $char(K) = 2$ case requires a more delicate analysis, we have evidence that the following can be conjectured:

Let $char(K) = p \neq 2$. Let U, $\Gamma(U)$, $\underline{L}(U)$ and $\overline{L}(U)$ be defined as above. Suppose that $\Gamma(U)$ is connected. Then the following holds:

(1) If $\overline{L}(U) = \underline{L}(\widetilde{U})$ and $\Gamma(\widetilde{U})$ is not one-way, then $\langle U \rangle \simeq N \cdot Sp(r, \overline{L}(U))$.
(2) If $\overline{L}(U) \neq \underline{L}(\widetilde{U})$, then $\Gamma(\widetilde{U})$ is not one-way, $|\overline{L}(U) : \underline{L}(\widetilde{U})| = 2$ and $\langle U \rangle \simeq N \cdot SU(r, \underline{L}(\widetilde{U}))$.

REFERENCES

Bosma, W., Cannon, J. J. (1995). *Handbook of Magma Functions*. Sydney: School of Mathematics and Statistics, University of Sydney.

Brown, R., Humphries, S. P. (1986a). Orbits under symplectic transvections I. *Proc. London Math. Soc.* 52(3):517–531.

Brown, R., Humphries, S. P. (1986b). Orbits under symplectic transvections II: The case $K = \mathbb{F}_2$. *Proc. London Math. Soc.* 52(3):532–556.

Di Martino, L., Vavilov, N. (1994). (2, 3)-generation of $SL(n, q)$. I. Cases $n = 5, 6, 7$. *Comm. Algebra* 22:1321–1347.

Di Martino, L., Vavilov, N. (1996). (2, 3)-generation of $SL(n, q)$. II. Cases $n \geq 8$. *Comm. Algebra* 24:487–515.

Higman, D. G. (1962). Flag-transitive collineation groups of finite projective spaces. *llinois J. Math.* 6:434–446.

Humphries, S. P. (1985). Graphs and Nielsen transformations of symmetric, orthogonal and symplectic groups. *Quart. J. Math. Oxford* 36(2):297–313.

Humphries, S. P. (1986). Generation of special linear groups by transvections *J. Algebra* 99:480–495.

Humphries, S. P. (1987). Identification of root subgroups of $SL_n(F)$. Unpublished.
Kantor, W. (1979). Subgroups of classical groups generated by long root elements. *Trans. Am. Math. Soc.* 248:347–379.
McLaughlin, J. (1967). Some groups generated by transvections. *Arch. Math.* 18:364–368; Some subgroups of $SL_n(\mathbb{F}_2)$. *Illinois J. Math.* 13 (1969), 108–115.
Piper, F. C. (1966). On elations of finite projective spaces of odd order. *J. London Math. Soc.* 41:641–648; On elations of finite projective spaces of even order. *J. London Math. Soc.* 43 (1968), 456–464.
Pollatsek, H. (1976). Irreducible groups generated by transvections over fields of characteristic two. *J. Algebra* 39:328–333.
Suzuki, M. (1982). *Group Theory. I.* Berlin: Springer Verlag.
Wagner, A. (1974). Groups generated by elations. *Abh. Math. Sem. Univ. Hamburg* 41:190–205.
Zalesskii, A. E., Serežkin, V. N. (1976). Linear groups generated by transvections. *Math. USSR Izvestija* 10(1):25–46.