Pacific Journal of Mathematics

ANISOTROPIC GROUPS OF TYPE A_n AND THE COMMUTING GRAPH OF FINITE SIMPLE GROUPS

Yoav Segev and Gary M. Seitz

Volume 202 No. 1 January 2002

PACIFIC JOURNAL OF MATHEMATICS
Vol. 202, No. 1, 2002

ANISOTROPIC GROUPS OF TYPE A_n AND THE COMMUTING GRAPH OF FINITE SIMPLE GROUPS

Yoav Segev and Gary M. Seitz

In this paper we make a contribution to the Margulis-Platonov conjecture, which describes the normal subgroup structure of algebraic groups over number fields. We establish the conjecture for inner forms of anisotropic groups of type A_n. We obtain information on the commuting graph of nonabelian finite simple groups, and consequently, using the paper by Segev, 1999, we obtain results on the normal structure and quotient groups of the multiplicative group of a division algebra.

0. Introduction.

Let $\mathfrak{G}$ be a simple, simply connected algebraic group defined over an algebraic number field K. Let T be the (finite) set of all nonarchimedean places v of K such that $\mathfrak{G}$ is K_v-anisotropic, and define $\mathfrak{G}(K,T)$ to be $\prod_{v\in T}\mathfrak{G}(K_v)$ with the topology of the direct product if $T \neq \emptyset$, and let $\mathfrak{G}(K,T) = \{e\}$ if $T = \emptyset$ (which is always the case if $\mathfrak{G}$ is not of type A_n). Let $\delta : \mathfrak{G}(K) \to \mathfrak{G}(K,T)$ be the diagonal embedding in the first case, and the trivial homomorphism in the second case.

Conjecture (Margulis and Platonov)**.** *For any noncentral normal subgroup $N \le \mathfrak{G}(K)$ there exists an open normal subgroup $W \le \mathfrak{G}(K,T)$ such that $N = \delta^{-1}(W)$; in particular, if $T = \emptyset$, the group $\mathfrak{G}(K)$ has no proper noncentral normal subgroups* (*i.e., it is projectively simple*)*.*

The conjecture has been established for almost all isotropic groups and for most anisotropic groups except for those of type A_n. The anisotropic groups of type A_n are thus the main unresolved case of the conjecture.

Inner forms of anisotropic groups of type A_n have the form $SL_{1,D}$, the reduced norm 1 group of a finite dimensional division algebra D over K (see 2.17 and 2.12 of [**10**]). In this case Potapchik and Rapinchuk showed (Theorem 2.1 of [**11**]) that if $SL_{1,D}$ fails to satisfy the Conjecture, then there exists a proper normal subgroup N of $D^* = D - \{0\}$ such that D^*/N is a nonabelian finite simple group.

In recent work the first named author ([14]) established a result, relating finite simple images of the multiplicative group of a finite dimensional division algebra over an arbitrary field to information about the commuting graph of finite simple groups. To state this result we need the following definitions.

Let H be a finite group. The *commuting graph of H* denoted $\Delta(H)$ is the graph whose vertex set is $H - Z(H)$ and whose edges are pairs $\{h, g\} \subseteq H - Z(H)$, such that $h \neq g$ and $[h, g] \in Z(H)$. We denote the diameter of $\Delta(H)$ by $\operatorname{diam}(\Delta(H))$.

Let $d : \Delta(H) \times \Delta(H) \to \mathbb{Z}^{\geq 0}$ be the distance function on $\Delta(H)$. We say that $\Delta(H)$ is *balanced* if there exists $x, y \in \Delta(H)$ such that the distances $d(x, y)$, $d(x, xy)$, $d(y, xy)$, $d(x, x^{-1}y)$, $d(y, x^{-1}y)$ are all larger than 3.

Theorem (Segev [14]). *Let D be a finite dimensional division algebra over an arbitrary field and L a nonabelian finite simple group. If* $\operatorname{diam}(\Delta(L)) > 4$, *or $\Delta(L)$ is balanced, then L cannot be isomorphic to a quotient of D^*.*

Consequently, the Margulis-Platonov Conjecture for inner forms of anisotropic groups of type A_n is resolved by the following theorem, which is the main result of this paper.

Theorem 1. *Let L be a nonabelian finite simple group. Then either* $\operatorname{diam}(\Delta(L)) > 4$ *or $\Delta(L)$ is balanced.*

The following results are then immediate corollaries:

Theorem 2. *The Margulis-Platonov Conjecture holds for $\mathfrak{G} = \mathbf{SL}_{1,D}$.*

Theorem 3. *If D is a finite dimensional division algebra over an arbitrary field, then no quotient of D^* is a nonabelian finite simple group.*

In Section 12 we show that the following theorem is a consequence of Theorem 2.

Theorem 4. *Let D be a finite dimensional division algebra over a number field. Let N be a noncentral normal subgroup of D^*. Then D^*/N is a solvable group.*

To prove Theorem 1 we need to establish results on the commuting graph of a finite simple group. These results may have independent interest, so we state them as separate theorems corresponding to the various types of finite simple groups.

The main obstacle in establishing Theorem 1 occurs for classical groups. Here we prove the following theorem.

Theorem 5. *Let L be a finite simple group of classical type. Then $\Delta(L)$ is balanced. The required elements can be taken as opposite regular unipotent elements.*

Corollary. *If L is a finite simple classical group, then* $\operatorname{diam}(\Delta(L)) \geq 4$.

We mention that except for some small cases the elements x, y used to establish balance in Theorem 5 satisfy $d(x, y) = 4$ (see Section 12).

The following result covers exceptional groups of Lie type and Sporadic groups.

Theorem 6. *Let $L \not\simeq E_7(q)$ be either an exceptional group of Lie type or a Sporadic group. Then $\Delta(L)$ is disconnected. If $L = E_7(q)$, then $\Delta(L)$ is balanced, where the elements x, y can be chosen to be semisimple elements.*

For the alternating groups we have:

Theorem 7. *If L is a simple alternating group, then* $\operatorname{diam}(\Delta(L)) > 4$.

Finally, in Section 12 we prove the following theorem:

Theorem 8. *Let $G(q)$ be a simple classical group with $q > 5$. Then $\Delta(G(q))$ is disconnected if and only if one of the following holds*

(i) *$G(q) \simeq L_n^{\epsilon}(q)$ and n is a prime.*
(ii) *$G(q) \simeq L_n^{\epsilon}(q)$, $n - 1$ is a prime and $q - \epsilon \mid n$.*
(iii) *$G(q) \simeq S_{2n}(q), O_{2n}^{-}(q)$, or $O_{2n+1}(q)$ and $n = 2^c$, for some c.*

Moreover, if $\Delta(G(q))$ is connected then $\operatorname{diam}(\Delta(G(q))) \leq 10$.

We draw the attention of the reader to the remark at the end of Section 12, for additional information about the connectivity of the commuting graph of finite simple groups.

In Chapter 1, which consists of Sections 1-7 we prove Theorem 5. In Chapter 2, which consists of Sections 8-9 we prove Theorem 6, when L is an exceptional group of Lie-type. Section 10 is devoted to the Alternating groups and the short Section 11 is devoted to the Sporadic groups. Finally in Section 12 we derive Theorem 4 from Theorem 2 and we include some results and remarks about the commuting graph of the classical groups.

We would like to thank Michael Aschbacher for various discussions, in particular, for contributions in Sections 8 and 9.

Chapter 1. The Classical Groups.

1. Notation and preliminaries.

The notation and definitions that will be introduced in this section will prevail *throughout Chapter* 1. $\mathbb{F}$ denotes a finite field and V denotes a vector space of dimension n over $\mathbb{F}$. We fix an ordered basis

$$\mathcal{B} = \{v_1, \ldots, v_n\}$$

of V. For a subset $S \subseteq V$, $\langle S\rangle$ denotes the subspace generated by S. We set:

$$\text{For } \ 1 \le i \le n, \quad \mathcal{V}_i = \langle v_1, v_2, \dots, v_i\rangle.$$

We write $M(V)$ for both $\mathrm{Hom}_{\mathbb{F}}(V,V)$, the set of all linear operators on V, and for the set of $n \times n$ matrices over $\mathbb{F}$. When we wish to emphasize that we are dealing with matrices we'll write $M_n(\mathbb{F})$ for the set of $n \times n$ matrices over $\mathbb{F}$. Also $GL(V) \subseteq M(V)$, denotes both the set of invertible linear operators on V and the set of invertible $n \times n$ matrices over $\mathbb{F}$. To emphasize matrices we write $GL_n(\mathbb{F})$, for the set of $n\times n$ invertible matrices over $\mathbb{F}$. Finally, $SL(V) \subseteq M(V)$ are the elements of determinant 1; again, we write $SL_n(\mathbb{F})$ for the set of $n \times n$ matrices of determinant 1. We use the same notation for the linear operator and its matrix, *with respect to the basis* $\mathcal{B}$. All our matrices are also linear operators whose matrix is the given matrix always with respect to our fixed basis $\mathcal{B}$, unless explicitly mentioned otherwise. Thus if $a \in M(V)$, then a is an $n \times n$ matrix over $\mathbb{F}$ whose (i,j)-th entry we always denote by a_{ij}. Also $a : V \to V$ is a linear operator such that $v_i a = \sum_{j=1}^{n} a_{ij} v_j$.

Given a bilinear form f (resp. a quadratic form Q) on V, we denote by $O(V,f)$ (resp. $O(V,Q)$) the elements in $GL(V)$ preserving f (resp. Q). $SO(V,f)$ (resp. $SO(V,Q)$) denotes the elements in $O(V,f)$ (resp. $O(V,Q)$) of determinant 1.

We fix *the letter* $\mathcal{R}$ to denote either $\mathbb{F}$, or the ring of polynomials over $\mathbb{F}, \mathbb{F}[\lambda]$. We'll denote by $M_n(\mathcal{R})$, the set of $n \times n$ matrices over $\mathcal{R}$.

Let H be a finite group. The *commuting graph of* H denoted $\Delta(H)$ is the graph whose vertex set is $H - Z(H)$ and whose edges are pairs $\{h, g\} \subseteq H - Z(H)$, such that $h \neq g$ and $[h, g] \in Z(H)$. (*Note* that our definition of the commuting graph differs a bit from what the reader may be used to, i.e., the vertex set of $\Delta(H)$ is $H - Z(H)$ and not $H - \{1\}$ and two elements form an edge when they commute *modulo the center of* H and not only when they commute.) We denote by $d_{\Delta(H)}$ the distance function of $\Delta(H)$. We fix the letter Δ to denote $\Delta(GL(V))$ and the letter d to denote the distance function of Δ (see 1.3 for further notation and definitions for the commuting graph).

Our goal in Chapter 1 is to prove Theorem 5 of the Introduction, which shows that $\Delta(L)$ is balanced, for all simple classical groups L. In principle we present a uniform approach to this, by showing that in all cases we can take the elements x, y to be opposite regular unipotent elements. However, the details are fairly complicated. In this section and the next we lay the ground work for the proof.

1.1. Notation and definitions for matrices over $\mathcal{R}$. Let $m \ge 1$ be an integer.

(1) First we mention that given $\alpha \in \mathbb{F}$, whenever we write $\bar{\alpha}$ inside a matrix, this means $\bar{\alpha} = -\alpha$.
(2) I_m denotes the identity $m \times m$ matrix.
(3) For integers $i, j \geq 1$, $0_{i,j}$ denotes the zero $i \times j$ matrix. We denote by 0_i the zero $i \times i$ matrix.
(4) Given $g \in M_m(\mathbb{F})$, we denote the transpose of g by g^t.
(5) Given $A \in M_m(\mathcal{R})$, $M_{i,j}(A) \in M_{m-1}(\mathcal{R})$, denotes the (i,j)-minor of A, i.e., the matrix A without the i-th row and j-th column. Also $M_{(i_1,i_2),(j_1,j_2)}(A) \in M_{m-2}(\mathcal{R})$ is the matrix without the i_1, i_2 rows and without the j_1, j_2 columns.
(6) Suppose $m = k_1 + k_2 + \cdots + k_t$ and that $g_i \in M_{k_i}(\mathcal{R})$, $1 \leq i \leq t$. We write $g = \operatorname{diag}(g_1, g_2, \dots, g_t)$ for the $m \times m$ matrix with $g_1, g_2, \dots, g_t$ on the main diagonal (in that order) and zero elsewhere. Of course if $g_i \in \mathcal{R}$, for all i ($k_i = 1$, for all i), then g is a diagonal matrix in the usual sense.
(7) Suppose $m \geq 2$ and let $1 \leq i \leq m-1$ and $\alpha \in \mathbb{F}$. We denote by $u_i^m(\alpha) \in M_m(\mathbb{F})$, the matrix which has 1 on the main diagonal, α in the $(i+1, i)$ entry and zero elsewhere.
(8) Suppose $m \geq 2$ and let $\beta_1, \beta_2, \dots, \beta_{m-1} \in \mathbb{F}^*$. We denote

$$a_m(\beta_1, \beta_2, \dots, \beta_{m-1}) = u_1^m(\beta_{m-1}) u_2^m(\beta_{m-2}) \cdots u_{m-2}^m(\beta_2) u_{m-1}^m(\beta_1)$$
$$b_m(\beta_1, \beta_2, \dots, \beta_{m-1}) = u_1^m(-\beta_1) u_2^m(-\beta_2) \cdots u_{m-2}^m(-\beta_{m-2}) u_{m-1}^m(-\beta_{m-1}).$$

Of course

$$a_m(\beta_1, \dots, \beta_{m-1}) = \begin{bmatrix} 1 & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ \beta_{m-1} & 1 & 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & \beta_{m-2} & 1 & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & \beta_{m-3} & 1 & 0 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & 0 & \beta_2 & 1 & 0 \\ 0 & \cdot & \cdot & \cdot & \cdot & 0 & \beta_1 & 1 \end{bmatrix},$$

$$b_m(\beta_1, \dots, \beta_{m-1}) = \begin{bmatrix} 1 & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ \bar{\beta}_1 & 1 & 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & \bar{\beta}_2 & 1 & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & \bar{\beta}_3 & 1 & 0 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & 0 & \bar{\beta}_{m-2} & 1 & 0 \\ 0 & \cdot & \cdot & \cdot & \cdot & 0 & \bar{\beta}_{m-1} & 1 \end{bmatrix}.$$

(9) We denote $a_1 = b_1 = [1]$ and for $m \geq 2$,

$$a_m = a_m(1, 1, \dots, 1) \quad \text{and} \quad b_m = b_m(1, 1, \dots, 1).$$

Hence

$$a_m = \begin{bmatrix} 1 & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ 1 & 1 & 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 1 & 1 & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & 1 & 1 & 0 & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & 0 & 1 & 1 & 0 \\ 0 & \cdot & \cdot & \cdot & & 0 & 1 & 1 \end{bmatrix} \qquad b_m = \begin{bmatrix} 1 & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ \bar{1} & 1 & 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & \bar{1} & 1 & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & \bar{1} & 1 & 0 & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & 0 & \bar{1} & 1 & 0 \\ 0 & \cdot & \cdot & \cdot & & 0 & \bar{1} & 1 \end{bmatrix}.$$

(10) Suppose $m \geq 2$ and $1 \leq r \leq m-1$. We denote by $\mathcal{T}_m(r)$ the set of $m \times m$ matrices $t \in M_m(\mathbb{F})$ such that:
(i) $t_{i,j} = 0$, for all $1 \leq i \leq r$ and $1 \leq j \leq m$.
(ii) $t_{r+i,i} \neq 0$ and $t_{r+i,\ell} = 0$, for all $1 \leq i \leq m-r$ and all $i < \ell \leq m$.
Thus t has the form

$$t = \begin{bmatrix} 0 & 0 & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ t_{r+1,1} & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ * & t_{r+2,2} & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ * & * & t_{r+3,3} & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ * & * & * & * & * & t_{m,m-r} & 0 & \cdot & \cdot & 0 \end{bmatrix}$$

where $*$ represents any element of $\mathbb{F}$.

(11) Throughout Chapter 1, J_m denotes the following $m \times m$ matrix. If we set, $J = J_m$, then $J_{i,m+1-i} = (-1)^{i+1}$, for all $1 \leq i \leq m$, and $J_{i,j} = 0$, otherwise. Thus

$$J_m = \begin{bmatrix} 0 & 0 & \cdot & \cdot & \cdot & \cdot & 0 & 1 \\ 0 & 0 & \cdot & \cdot & \cdot & 0 & \bar{1} & 0 \\ 0 & 0 & \cdot & \cdot & 0 & 1 & 0 & 0 \\ 0 & 0 & \cdot & 0 & \bar{1} & 0 & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \bar{1}^m & 0 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \bar{1}^{m+1} & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \end{bmatrix}.$$

Note that $J_m^{-1} = J_m^t$, $J_m^2 = (-1)^{m+1} I_m$ and if $m = 2\ell$ is even, then

$$J_{2\ell} = \begin{bmatrix} 0_\ell & J_\ell \\ (-1)^\ell J_\ell & 0_\ell \end{bmatrix}.$$

1.2. Notation for polynomials, characteristic polynomials and characteristic vectors. Let $m \geq 1$ be an integer.

(1) Let $g \in M_m(\mathbb{F})$. We denote by $F_g[\lambda]$, the characteristic polynomial of g. We often write F_g for $F_g[\lambda]$.
(2) If F is the characteristic polynomial of $g \in GL_m(\mathbb{F})$, we denote by $\overline{F}$ the characteristic polynomial of g^{-1}.
(3) Given a polynomial $F[\lambda]$, we denote by $\alpha(F, \ell)$, the coefficient of λ^ℓ in F.
(4) Throughout Chapter 1 we denote by $F_m[\lambda]$ the characteristic polynomial of $a_m^t a_m$ (a_m as in 1.1.9). We mention that several properties of $F_m[\lambda]$ are given in 2.6.
(5) Throughout Chapter 1, $G_m[\lambda]$ denotes the characteristic polynomial of the following $m \times m$ matrix

$$\begin{bmatrix} 2 & 1 & 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ 1 & 2 & 1 & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & 1 & 2 & 1 & 0 & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & 0 & 1 & 2 & 1 & 0 \\ 0 & \cdot & \cdot & \cdot & 0 & 1 & 2 & 1 \\ 0 & \cdot & \cdot & \cdot & \cdot & 0 & 1 & 2 \end{bmatrix}.$$

(6) We denote $Q_m[\lambda] = \lambda^m - \lambda^{m-1} + \lambda^{m-2} + \cdots + (-1)^{m-1}\lambda + (-1)^m$.
(7) Let $g \in GL(V)$ and suppose that $v \in V$ is a characteristic vector for g. We denote by $\lambda_g(v) \in \mathbb{F}$ the scalar such that $vg = \lambda_g(v)v$.

1.3. Notation for the commuting graph. Let H be a group and let $\Lambda = \Delta(H)$.

(1) Given elements $X, Y \in \Lambda$, we write $B_\Lambda(X, Y)$ if the distances $d_\Lambda(X, Y)$, $d_\Lambda(X, XY)$ and $d_\Lambda(X, X^{-1}Y)$ are all > 3. We write $B(X, Y) = B_\Delta(X, Y)$ (recall that $\Delta = \Delta(GL(V))$).
(2) We say that Λ is *balanced* if there are elements $X, Y \in \Lambda$ such that $B_\Lambda(X, Y)$ and $B_\Lambda(Y, X)$.
(3) We use the usual notation for graphs, thus, for example, $\Delta^{\leq i}(X)$ means the set of all elements at distance at most i from X, in Δ.

1.4. Further notation and definitions. Let $g \in GL(V)$, $0 \neq v \in V$ and $H \leq GL(V)$, a subgroup.

(1) We denote by $\mathcal{O}(v, g)$ the orbit of v under $\langle g \rangle$.
(2) Given an ordered basis $\mathcal{A} = \{w_1, \dots, w_n\}$ of V we denote by $[g]_\mathcal{A}$ the matrix of g with respect to the basis $\mathcal{A}$. Thus, the i-th *row* of $[g]_\mathcal{A}$ are the coordinates of $w_i g$ with respect to $\mathcal{A}$.
(3) We say that H is *closed under transpose* if $h \in H$ implies $h^t \in H$.

(4) We fix the letter τ to denote the graph automorphism of $SL_n(\mathbb{F})$ such that $\tau : u_i^n(\alpha) \to u_{n-i}^n(\alpha)$ and $\tau : (u_i^n(\alpha))^t \to (u_{n-i}^n(\alpha))^t$, for all $\alpha \in \mathbb{F}$ and all $1 \le i \le n-1$. Note that τ commutes with the transpose map.
(5) If $|\mathbb{F}| = q^2$, we let $\sigma_q : GL_n(\mathbb{F}) \to GL_n(\mathbb{F})$, be the Frobenius automorphism taking each entry of $g \in GL_n(\mathbb{F})$ to its q power.

By a *Classical Group* we mean $L \le GL(V)$, where L is one of the groups $SL_n(q)$, $Sp_n(q)$, $\Omega_n^\epsilon(q)$, or $SU_n(q)$, where for orthogonal groups we use $\epsilon \in \{+,-\}$ only in even dimension and for unitary groups we work over the field of order q^2. In all cases we take L to be quasisimple, avoiding the few cases when this does not hold. By a *Simple Classical Group* we mean $L/Z(L)$, with L a classical group. In the respective cases we denote the simple classical groups by $L_n(q), S_n(q), O_n(q), O_n^\epsilon(q)$ and $U_n(q)$.

1.5. (1) *For even q and odd n, $O_n(q) \simeq S_{n-1}(q)$.*
(2) *For all q, $O_3(q) \simeq L_2(q)$, $O_4^+(q) \simeq L_2(q) \times L_2(q)$, $O_4^-(q) \simeq L_2(q^2)$, $O_5(q) \simeq S_4(q)$, $O_6^+(q) \simeq L_4(q)$ and $O_6^-(q) \simeq U_4(q)$.*

The purpose of Chapter 1 is to prove:

Theorem 1.6. *Let L be a finite simple classical group. Then $\Delta(L)$ is balanced.*

We mention that in Remark 1.18 ahead we indicate our strategy for proving Theorem 1.6.

1.7. *Let H be a group. Suppose that $Z(H/Z(H)) = 1$ and that $\Delta(H)$ is balanced. Then $\Delta(H/Z(H))$ is balanced.*

Proof. This is obvious since if $X, Y \in \Delta(H)$ satisfy $B(X,Y)$ and $B(Y,X)$, then $XZ(H)$, $YZ(H)$ satisfy the same condition in $\Delta(H/Z(H))$.

1.8. *Let $L \le SL(V)$ be a classical group. Set $\Lambda = \Delta(L)$ and suppose that L is closed under transpose. Then:*
(1) *The maps $g \to g^{-1}$, $g \to g^t$ and conjugation are isomorphisms of Λ.*
(2) *Let $g, h \in \Lambda$ and let $\epsilon \in \{1,-1\}$, then any one of the following imply $d_\Lambda(g, g^\epsilon h) > 3$:*
(i) $d_\Lambda(g, hg^\epsilon) > 3$*;*
(ii) $d_\Lambda(g, h^{-1}g^{-\epsilon}) > 3$*;*
(iii) $d_\Lambda(g, g^{-\epsilon}h^{-1}) > 3$.

Proof. (1) is easy. (2) follows from (1) noting that $(g^\epsilon h)^{g^\epsilon} = hg^\epsilon$, $(g^{-\epsilon}h^{-1})^{g^{-\epsilon}} = h^{-1}g^{-\epsilon}$ and that the distance between g and t is the same as that from g to t^{-1}.

1.9. *Let $L \le SL(V)$ be a classical group. Set $\Lambda = \Delta(L)$ and suppose that L is closed under transpose. Let $X, Y \in L$. Then:*

(1) *If $B(X,Y)$, then $B(X^t,Y^t)$.*
In particular:
(2) *If $B(X,X^t)$, then $B(X^t,X)$.*

Proof. Suppose that $B(X,Y)$ holds. By 1.8.1, $d_\Lambda(X^t,Y^t)>3$. Also since $d_\Lambda(X,XY)>3$, $d_\Lambda(X^t,(XY)^t)>3$. Hence $d_\Lambda(X^t,Y^tX^t)>3$. By 1.8.2, $d_\Lambda(X^t,X^tY^t)>3$. Finally since $d_\Lambda(X,X^{-1}Y)>3$, $d_\Lambda(X^t,(X^{-1}Y)^t)>3$. Thus $d_\Lambda(X^t,Y^t(X^t)^{-1})>3$ and then, $d_\Lambda(X^t,(X^t)^{-1}Y^t)>3$.

Corollary 1.10. *Let $L\le SL(V)$ be a classical group. Set $\Lambda=\Delta(L)$ and suppose that L is closed under transpose. Suppose one of the following holds:*
(i) *There exists $X\in L$ such that $B_\Lambda(X,X^t)$.*
(ii) *There exists $X,Y\in L$ such that $B_\Lambda(X,Y^t)$ and $B_\Lambda(Y,X^t)$.*

Then $\Delta(L)$ is balanced.

Proof. If (i) holds, then it is immediate from 1.9.2, and definition, that $\Delta(L)$ is balanced. If (ii) holds, then by 1.9.1, also $B_\Lambda(Y^t,X)$, so by definition $\Delta(L)$ is balanced.

1.11. *Suppose $n=2k+\epsilon\ge 2$, with $\epsilon\in\{0,1\}$. Let $\beta_1,\beta_2,\dots,\beta_{k-1}\in\mathbb{F}^*$. Set $a=a_k(\beta_1,\beta_2,\dots,\beta_{k-1})$ and $b=b_k(\beta_1,\beta_2,\dots,\beta_{k-1})$. Let $\tau: SL_n(\mathbb{F})\to SL_n(\mathbb{F})$ be the automorphism defined in 1.4.4. If $\epsilon=0$, then* $\mathrm{diag}\,(a,b^{-1})\in\mathrm{Fix}\,(\tau)$ *and if $\epsilon=1$, then* $\mathrm{diag}\,(a,1,b^{-1})\in\mathrm{Fix}\,(\tau)$.

Proof. Just observe that if $\epsilon=0$, then

$$\begin{aligned}&\mathrm{diag}\,(a,b^{-1})\\ &=u_1^n(\beta_{k-1})u_{n-1}^n(\beta_{k-1})u_2^n(\beta_{k-2})u_{n-2}^n(\beta_{k-2})\cdots u_{k-1}^n(\beta_1)u_{k+1}^n(\beta_1)\end{aligned}$$

and if $\epsilon=1$, then

$$\begin{aligned}&\mathrm{diag}\,(a,1,b^{-1})\\ &=u_1^n(\beta_{k-1})u_{n-1}^n(\beta_{k-1})u_2^n(\beta_{k-2})u_{n-2}^n(\beta_{k-2})\cdots u_{k-1}^n(\beta_1)u_{k+2}^n(\beta_1).\end{aligned}$$

1.12. *Let $\tau,\sigma_q: SL(V)\to SL(V)$ be the automorphisms defined in 1.4.4 and 1.4.5. Set $J=J_n$ (see 1.1.11). Then:*
(1) *$g\tau=J(g^t)^{-1}J^{-1}=J(g^t)^{-1}J^t$, for all $g\in SL(V)$.*
(2) *τ and σ_q commute with the transpose map.*
(3) *For an automorphism $\phi: SL(V)\to SL(V)$, let $\mathrm{Fix}\,(\phi)=\{h\in SL(V): h\phi=h\}$. Then if $|\mathbb{F}|=q^2$, $\mathrm{Fix}\,(\tau\sigma_q)\simeq SU_n(q)$; if n is even, then $\mathrm{Fix}\,(\tau)\simeq Sp_n(q)$ and if n is odd and q is odd, $\mathrm{Fix}\,(\tau)\simeq SO_n(q)$.*
(4) *In the notation of (3), $\mathrm{Fix}\,(\tau)$ and $\mathrm{Fix}\,(\tau\sigma_q)$ are closed under transpose.*
(5) *Suppose $n=2k$ is even, $x,y\in SL_k(\mathbb{F})$ are such that $\mathrm{diag}\,(x,y^{-1})\in\mathrm{Fix}\,(\tau)$. Then $y=J_kx^tJ_k^{-1}=J_kx^tJ_k^t$.*

Proof. First recall that $J^{-1}=J^t$. Let $\tau': SL(V)\to SL(V)$, be the automorphism $g\to J(g^t)^{-1}J^{-1}$. It is easy to check that $u_i^n(\alpha)\tau'=u_i^n(\alpha)\tau$, and $(u_i^n(\alpha))^t\tau'=(u_i^n(\alpha))^t\tau$, for all $1\le i\le n-1$, and all $\alpha\in\mathbb{F}$. Thus $\tau'=\tau$.

Evidently τ and σ_q commute with the transpose map. Next note that $g \in \mathrm{Fix}\,(\tau)$ iff $gJg^t = J$; thus $g \in SO(V,f)$, where f is the bilinear form given by $f(v_i,v_j) = J_{i,j}$. Hence $\mathrm{Fix}\,(\tau)$ is as claimed in (3). Now if $|\mathbb{F}| = q^2$, then $g \in \mathrm{Fix}\,(\tau\sigma_q)$ iff $gJ(g\sigma_q)^t = J$, so as above, $g \in SO(V,f)$, for a suitable unitary form f.

To prove (5), set $g = \mathrm{diag}\,(x, y^{-1})$. Then by (1), $g\tau = J(g^t)^{-1}J^t = J\mathrm{diag}\,((x^t)^{-1}, y^t)J^t$. Now using Definition 1.1.11, we get

$$\begin{aligned} g\tau &= \begin{bmatrix} 0_k & J_k \\ (-1)^k J_k & 0_k \end{bmatrix} \cdot \begin{bmatrix} (x^t)^{-1} & 0_k \\ 0_k & y^t \end{bmatrix} \cdot \begin{bmatrix} 0_k & (-1)^k J_k^t \\ J_k^t & 0_k \end{bmatrix} \\ &= \begin{bmatrix} 0_k & J_k y^t \\ (-1)^k J_k (x^t)^{-1} & 0_k \end{bmatrix} \cdot \begin{bmatrix} 0_k & -J_k \\ (-1)^{k+1} J_k & 0_k \end{bmatrix} \\ &= \begin{bmatrix} (-1)^{k+1} J_k y^t J_k & 0_k \\ 0_k & (-1)^{k+1} J_k (x^t)^{-1} J_k \end{bmatrix}. \end{aligned}$$

Since we are assuming that $g\tau = g$, we see that $(-1)^{k+1}J_k y^t J_k = x$, so since $J_k^{-1} = (-1)^{k+1}J_k = J_k^t$, we see that $x = J_k^t y^t J_k$, so $y = J_k x^t J_k^{-1} = J_k x^t J_k^t$, as asserted.

1.13. *Let $X \in GL_n(V)$ be a lower triangular matrix such that $X - I_n \in \mathcal{T}_n(1)$ (see 1.1.10 for $\mathcal{T}_n(1)$). Let $h \in M_n(\mathbb{F})$ be a matrix commuting with X. Then:*

1. *h is a lower triangular matrix.*
2. *There exists $1 \le r < n$, and $\beta \in \mathbb{F}$ such that $h - \beta I_n \in \mathcal{T}_n(r)$.*
3. *If $X_{i,i-1} = X_{j,j-1}$, for all $2 \le i,\ j \le n$, then $h_{r+i,i} = h_{r+j,j}$, for all $1 \le i,j \le n-r$.*

Proof. For $2 \le i \le n$, set $\alpha_i := X_{i,i-1}$. Note that by definition (see 1.1.10), $\alpha_i \ne 0$, for all $2 \le i \le n$. Note further that h commutes with the matrix $X - I_n$, and clearly for $1 \le i \le n-1$, $\ker(X - I_n)^i = \mathcal{V}_i$. Since h commutes with $(X - I_n)^i$, h fixes $\ker(X - I_n)^i$, so (1) holds.

Next set $Xh = g$ and $hX = q$. It is easy to check that for $2 \le i \le n$, $g_{i,i-1} = \alpha_i h_{i-1,i-1} + h_{i,i-1}$ and that $q_{i,i-1} = h_{i,i-1} + \alpha_i h_{i,i}$. Since $g = q$, and $\alpha_i \ne 0$, for all i, we see that $h_{1,1} = h_{2,2} = \cdots = h_{n,n}$. Set $\beta = h_{1,1}$ and $t = h - \beta I_n$. Then t has the form

$$t = \begin{bmatrix} 0 & 0 & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ t_{r+1,1} & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ * & t_{r+2,2} & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ * & * & t_{r+3,3} & 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ * & * & * & * & * & t_{n,n-r} & 0 & \cdot & 0 \end{bmatrix}$$

where $1 \le r \le n-1$ and for some $1 \le j \le n-r$, $t_{r+j,j} \ne 0$. Note that $X - I_n$ commutes with t.

Set $(X-I_n)t = g$ and $t(X-I_n) = q$. Then it is easy to check that $g_{r+2,1} = \alpha_{r+2}t_{r+1,1}$, $g_{r+3,2} = \alpha_{r+3}t_{r+2,2}, \dots, g_{n,n-r-1} = \alpha_n t_{n-1,n-r-1}$. Similarly, $q_{r+2,1} = \alpha_2 t_{r+2,2}$, $q_{r+3,2} = \alpha_3 t_{r+3,3}, \dots, q_{n,n-r-1} = \alpha_{n-r}t_{n,n-r}$. Since $g = q$, $\alpha_i \ne 0$, for all i, and $t_{r+j,j} \ne 0$, for some $1 \le j \le n-r$, $t_{r+i,i} \ne 0$, for all $1 \le i \le n-r$ and $t \in \mathcal{T}_n(r)$ as asserted. Further, it is easy to check that (3) holds.

1.14. *Let $R, S \in GL(V)$. Set $\mathfrak{Z} = Z(GL(V))$ and $\mathcal{W} = \langle \mathcal{O}(w_1, S)\rangle$. Suppose that:*

(a) *$R^{-1}SR = \mu S$, for some $\mu \in \mathbb{F}^*$.*
(b) *v_1 is a characteristic vector of R.*

Then:

(1) *If $\mu = 1$, then $\mathcal{W}$ is a set of characteristic vectors of R and for $w \in \mathcal{W}$, $\lambda_R(w) = \lambda_R(v_1)$. In particular, if $\mathcal{W} = V$, then $R \in \mathfrak{Z}$.*

Suppose $\mathcal{W} = V$, and let $F_S[\lambda] = \lambda^n - \sum_{i=0}^{n-1} \alpha_i\lambda^i$. Then:

(2) *R is conjugate in $GL(V)$ to some member of* $\operatorname{diag}(1, \mu, \mu^2, \dots, \mu^{n-1})\mathfrak{Z}$.
(3) *$\mu^i = 1$, for each $1 \le i \le n$ such that $\alpha_{n-i} \ne 0$.*
(4) *$\mu^n = 1$.*
(5) *If $gcd\Big\{\{i : \alpha_{n-i} \ne 0\} \cup \{|\mathbb{F}^*|\}\Big\} = 1$, then $R \in \mathfrak{Z}$.*

Proof. Notice that by hypotheses (a) and (b), $\mathcal{O}(v_1, S)$ is a set of characteristic vectors of R. Further if $\mu = 1$, clearly (1) holds. For the remaining parts assume $\mathcal{W} = V$. Then $\mathcal{A} = \{v_1, v_1S, v_1S^2, \dots, v_1S^{n-1}\}$ is a basis of V. The matrix of S with respect to the basis $\mathcal{A}$ is

$$S' := [S]_{\mathcal{A}} = \begin{bmatrix} 0 & 1 & 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & 1 & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & 0 & 1 & 0 & \cdot & \cdot & 0 \\ 0 & \cdot & \cdot & 0 & 1 & 0 & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 & 1 \\ \alpha_0 & \alpha_1 & \alpha_2 & \cdot & \cdot & \cdot & \cdot & \alpha_{n-1} \end{bmatrix}$$

and the matrix of R with respect to the basis $\mathcal{A}$ is $R' = \operatorname{diag}(R_1, R_2, \dots, R_n)$. Replacing R with a scalar multiple of R we may assume that $R_1 = 1$. Note that for $1 \le i \le n-1$, the $(i, i+1)$-entry of the matrix $(R')^{-1}S'R'$ is $R_i^{-1}R_{i+1}$. Since $(R')^{-1}S'R' = \mu S'$, we conclude that $R_i = \mu^{i-1}$, $1 \le i \le n$ and (2) holds.

Next note that for $1 \le i \le n$, the $(n, n-i+1)$-entry of $(R')^{-1}S'R'$ is $R_n^{-1}R_{n-i+1}\alpha_{n-i} = \mu^{1-n}\mu^{n-i}\alpha_{n-i} = \mu^{1-i}\alpha_{n-i}$. Thus, since $(R')^{-1}S'R' = \mu S'$, $\mu^{1-i}\alpha_{n-i} = \mu\alpha_{n-i}$, so if $\alpha_{n-i} \ne 0$, $\mu^i = 1$. This shows (3). Of course

(4) follows from (3), since $\alpha_0 = (-1)^{n+1}\det(R) \neq 0$. Finally (5) is an immediate consequence of (2), (3) and (4).

1.15. *Suppose $S, T \in M(V)$, $R \in GL(V)$ and $j, m, \ell \geq 0$ are integers such that:*

(a) $1 \leq j \leq n-1$ *and for all* $1 \leq i \leq j$ *and* $i+1 < k \leq n$, $S_{i,i+1} \neq 0$ *and* $S_{i,k} = 0$.
(b) $\mathcal{V}_j \subseteq \ker(T)$.
(c) $v_{j+1} \notin \ker(S^\ell T)$.
(d) $1 \leq m \leq j+1$, *and* $\mathcal{V}_m$ *is R-invariant.*
(e) *If we set* $\mathfrak{Z} = Z(GL(V))$ *then* $R^{-1}SR \in \mathfrak{Z}S$ *and* $R^{-1}TR \in \mathfrak{Z}T$.

Then v_1 is a characteristic vector of R.

Proof. For $i \geq 0$, set $z_i = S^i T$. Note that $R^{-1}z_i R \in \mathfrak{Z}z_i$, for all $i \geq 0$ and hence

(i) $$\ker(z_i) \text{ is } R\text{-invariant}, \text{ for all } i \geq 0.$$

Notice that by (a):

(ii) $$\text{For all } i \geq 0, \text{ if } \mathcal{V}_{j+1} \subseteq \ker(z_i), \text{ then } \mathcal{V}_j \subseteq \ker(z_{i+1}).$$

Now without loss we may assume that ℓ is the least nonnegative integer i such that $v_{j+1} \notin \ker(z_i)$. Since by (b), $\mathcal{V}_j \subseteq \ker(z_0)$, minimality of ℓ and (ii) imply that $\mathcal{V}_j \subseteq \ker(z_\ell)$. Thus

(iii) $$v_{j+1} \notin \ker(z_\ell) \quad \text{and} \quad \mathcal{V}_j \subseteq \ker(z_\ell).$$

Now, by (a) and (iii), we get that

(iv) $$\ker(z_{\ell+i}) \cap \mathcal{V}_{j-i+1} = \mathcal{V}_{j-i}, \qquad \text{for all } 0 \leq i \leq j-1.$$

By (i), (iv), (d) and since $1 \leq m \leq j+1$, we see that $\mathcal{V}_m, \mathcal{V}_{m-1}, \dots, \mathcal{V}_1$ are all R-invariant, so since $\mathcal{V}_1$ is R-invariant, v_1 is a characteristic vector of R.

1.16. *Suppose $n \geq 2$ and let $Z \in GL(n, \mathbb{F})$. Let $v \in V$ such that $\langle \mathcal{O}(v, Z) \rangle = V$ and let $\alpha \in \mathbb{F}$. Then $\langle \mathcal{O}(\alpha v + vZ, Z) \rangle \neq V$ iff $-\alpha$ is a characteristic value of Z.*

Proof. Since $\langle \mathcal{O}(v, Z) \rangle = V$, $\mathcal{C} := \{v, vZ, \dots, vZ^{n-1}\}$ is a basis of V. Now $\langle \mathcal{O}(\alpha v + vZ, Z) \rangle = V$, iff $\mathcal{D} := \{\alpha v + vZ, (\alpha v + vZ)Z, \dots, (\alpha v + vZ)Z^{n-1}\}$ is a basis of V. Now $\mathcal{D}$ is obtained from $\mathcal{C}$ by applying the transformation $\alpha I_n + Z$ to the basis $\mathcal{C}$. Thus $\mathcal{D}$ is a basis of V iff $\alpha I_n + Z$ is invertible and the lemma follows.

Corollary 1.17. *Suppose $n = 2k+1$ (with $k \geq 1$), let $S \in GL(n, \mathbb{F})$ and write*

$$S = \begin{bmatrix} R_{1,1} & R_{1,2} \\ R_{2,1} & Z \end{bmatrix}$$

with $R_{1,1}, R_{1,2}, R_{2,1}$ and Z a $k \times k$, $k \times (k+1)$, $(k+1) \times k$ and $(k+1) \times (k+1)$ matrices, respectively. Set $\mathcal{W} = \langle \mathcal{O}(v_1, S) \rangle$ and assume:

(a) $\mathcal{V}_k \subseteq \mathcal{W}$.
(b) $Z \in GL_{k+1}(\mathbb{F})$ *and* $\langle \mathcal{O}(v_{k+1}, \mathrm{diag}\,(I_k, Z))\rangle = \langle v_{k+1}, \dots, v_n\rangle$.
(c) $\alpha v_{k+1} + v_{k+1}\mathrm{diag}\,(I_k, Z) \in \mathcal{W}$, *for some* $\alpha \in \mathbb{F}$.

If $-\alpha$ *is not a characteristic value of the matrix* Z, *then* $V = \langle \mathcal{O}(v_1, S)\rangle$.

Proof. Set $\mathcal{U} = \langle v_{k+1}, \dots, v_n\rangle$ and let Z denote also the linear operator $Z : \mathcal{U} \to \mathcal{U}$, given by the matrix Z, with respect to the basis $\{v_{k+1}, \dots, v_n\}$. Then, by (b), $\mathcal{U} = \langle \mathcal{O}(v_{k+1}, Z)\rangle$. Also it is easy to check that hypothesis (a) implies that if $u \in \mathcal{U} \cap \mathcal{W}$, then $uZ \in \mathcal{U} \cap \mathcal{W}$. Hence by hypothesis (c), $\mathcal{O}(\alpha v_{k+1} + v_{k+1}Z, Z) \subseteq \mathcal{W}$. Now 1.16 and hypotheses (b) and (c) imply that if $-\alpha$ is not a characteristic value of Z, then $\mathcal{U} \subseteq \mathcal{W}$, so by (a), $\mathcal{W} = V$ as asserted.

1.18. Important remark. Throughout Chapter 1, the following strategy will be used to prove Theorem 1.6. Let $L \leq SL(V)$ be a classical group. Let $\Lambda = \Delta(L)$. We carefully choose $X, Y \in \Lambda$. To show $B_\Lambda(X, Y)$, let $S \in \{Y, XY, X^{-1}Y\}$. In order to show that $d_\Lambda(X, S) > 3$, suppose $R \in \Lambda^{\leq 2}(X) \cap \Lambda^{\leq 1}(S)$. We do the following steps.

Step 1. We obtain information about $C_L(X)$. Part of the work was already done in 1.13.

Step 2. Using Step 1, we show that if $h \in \Lambda^{\leq 1}(X) \cap \Lambda^{\leq 1}(R)$, then there exists $\beta \in \mathbb{F}^*$ and an integer $k \geq 1$ such that if we set $T := (h - \beta I_n)^k$, then there are integers $j, \ell, m \geq 0$ such that T, S, R, j, ℓ, m satisfy all the hypotheses of 1.15. Thus we conclude from 1.15 that v_1 is a characteristic vector of R.

Step 3. We compute $\langle \mathcal{O}(v_1, S)\rangle$. In all cases X, Y are chosen so that either $\langle \mathcal{O}(v_1, S)\rangle = V$, or $[S, R] = 1$, (so that we can use 1.14.1) and $\langle \mathcal{O}(v_1, S)\rangle$ has codimension 1 or 2 in V.

Step 4. We obtain information on the characteristic polynomial of S. This information is aimed to fit the hypotheses of 1.14.5.

Step 5. We use Step 2, Step 3 and Step 4, together with 1.14, to get that $R \in Z(L)$ and obtain a contradiction.

2. Some information about characteristic polynomials.

Throughout this section $n = 2k+\epsilon \geq 2$ is a positive integer, where $\epsilon \in \{0, 1\}$. a_m and b_m are as in 1.1.9. We draw the attention of the reader to 1.1 and 1.2, where we fixed our notation for matrices and polynomials. In particular, recall that the polynomials $F_m[\lambda], G_m[\lambda]$ and $Q_m[\lambda]$ are defined in 1.2.4, 1.2.5 and 1.2.6 respectively.

2.1. Notation. For an integer $\ell \geq 1$ and a prime r, $|\ell|_r$ is the largest power of r dividing ℓ. Hence, if $\gcd(\ell, r) = 1$, then $|\ell|_r = 0$.

2.2. *Let $\ell \geq 1$ be a positive integer. Suppose $\ell = \sum_{i=0}^{s} \epsilon_i 2^i$, with $\epsilon_i \in \{0, 1\}$, for all i. Then $|\ell!|_2 = \ell - \sum_{i=0}^{s} \epsilon_i$.*

Proof. It is easy to see that

$$\begin{aligned}
|\ell!|_2 &= \left[\frac{\ell}{2}\right] + \left[\frac{\ell}{4}\right] + \left[\frac{\ell}{8}\right] + \cdots + 1 \\
&= \sum_{i=1}^{s} \epsilon_i 2^{i-1} + \sum_{i=2}^{s} \epsilon_i 2^{i-2} + \cdots + \sum_{i=s-1}^{s} \epsilon_i 2^{i-s+1} + \epsilon_s \\
&= \epsilon_1 + \epsilon_2 \sum_{i=0}^{1} 2^i + \epsilon_3 \sum_{i=0}^{2} 2^i + \cdots + \epsilon_s \sum_{i=0}^{s-1} 2^i \\
&= \epsilon_0(2^0 - 1) + \epsilon_1(2^1 - 1) + \epsilon_2(2^2 - 1) + \cdots + \epsilon_s(2^s - 1) \\
&= \ell - \sum_{i=0}^{s} \epsilon_i.
\end{aligned}$$

2.3. *Suppose $k = m2^{s+1} - 1$, with $s \geq 1$ and m odd. Then:*

(1) *If $1 \leq \ell < 2^s$, then $\binom{k+\ell}{2\ell} \equiv 0 \pmod 2$.*
(2) *If $1 \leq \ell < 2^s$, then $\binom{k+\ell}{2\ell+1} \equiv 0 \pmod 2$.*
(3) $\binom{k+2^s}{2^{s+1}} \equiv 1 \pmod 2$.
(4) $\binom{2k-2^s}{2^s} \equiv 0 \pmod 2$.
(5) $\binom{2k-2^s}{2^s-2} \equiv 1 \pmod 2$.
(6) $\binom{2k-2^s+1}{2^s-1} \equiv 1 \pmod 2$.

Proof. For (1) note that by comparing 2−parts of factors we have

$$\binom{k+\ell}{2\ell} \equiv \frac{\left\{\prod_{i=\ell-1}^{1}((k+1)+i)\right\} \cdot (k+1) \cdot \left\{\prod_{i=1}^{\ell}((k+1)-i)\right\}}{2^\ell \cdot \ell!} \pmod 2.$$

Since $k + 1 = m2^{s+1}$ for $\ell \leq 2^s$, we get

$$\binom{k+\ell}{2\ell} \equiv \frac{(\ell-1)! \cdot 2^{s+1} \cdot \ell!}{2^\ell \cdot \ell!} \pmod 2$$

hence

$$\begin{aligned}
\left|\binom{k+\ell}{2\ell}\right|_2 &= \{|(\ell-1)!|_2 + s + 1 + |\ell!|_2\} - (\ell + |\ell!|_2) \\
&= |(\ell-1)!|_2 + s + 1 - \ell.
\end{aligned}$$

If $\ell < 2^s$, then $\ell - 1 < 2^s - 1$, so if we write $\ell - 1 = \sum_{i=0}^{s-1} \epsilon_i 2^i$, we see that $\sum_{i=0}^{s-1} \epsilon_i < s$. Thus, by 2.2, $|(\ell-1)!|_2 > \ell - 1 - s$, so $|\binom{k+\ell}{2\ell}|_2 > \ell - 1 - s + s + 1 - \ell = 0$. This shows (1). In (3), $\ell = 2^s$, so, by 2.2, $|(\ell-1)!|_2 = \ell - 1 - s$, thus $= |\binom{k+2^s}{2^{s+1}}|_2 = 0$.

For (2), note that

$$\binom{k+\ell}{2\ell+1} \equiv (k-\ell)\binom{k+\ell}{2\ell} \pmod 2.$$

Hence (2) following from (1).

We proceed with the proof of (4) and (5).

$$\begin{aligned}\binom{2k-2^s}{2^s} &\equiv \frac{\prod_{i=0}^{2^s-1}((m2^{s+2}-2^s-2)-i)}{2^s!} \equiv \frac{\prod_{i=0}^{2^s-1}(2^s+i+2)}{2^s!} \\ &\equiv \frac{2\cdot 2^s!}{2^s!} \equiv 0 \pmod 2,\end{aligned}$$

and as above,

$$\begin{aligned}\binom{2k-2^s}{2^s-2} &\equiv \frac{\prod_{i=0}^{2^s-3}((m2^{s+2}-2^s-2)-i)}{(2^s-2)!} \\ &\equiv \frac{\prod_{i=0}^{2^s-3}(2^s+i+2)}{(2^s-2)!} \equiv 1 \pmod 2.\end{aligned}$$

Finally, for (6), note that

$$\begin{aligned}\binom{2k-2^s+1}{2^s-1} &\equiv \frac{\prod_{i=0}^{2^s-2}((m2^{s+2}-2^s-1)-i)}{(2^s-1)!} \\ &\equiv \frac{\prod_{i=0}^{2^s-2}(2^s+i+1)}{(2^s-1)!} \equiv 1 \pmod 2.\end{aligned}$$

2.4. *Suppose $n = 2k$ and let $\tau : SL_n(\mathbb{F}) \to SL_n(\mathbb{F})$ be the automorphism defined in 1.4.4. Let $a_i, b_i \in SL_k(\mathbb{F})$ and suppose* $\operatorname{diag}(a_i, b_i^{-1}) \in \operatorname{Fix}(\tau)$, *$i = 1, 2$. Then for $\epsilon \in \{1, -1\}$, $F_{a_1^t a_2^\epsilon}[\lambda] = F_{b_1^t b_2^\epsilon}[\lambda]$.*

Proof. By 1.12.5, $b_i = J_k(a_i)^t J_k^t$. Hence, $b_1^t b_2 = J_k a_1 J_k^t J_k (a_2)^t J_k^t$. Recall now that $J_k^t = J_k^{-1}$. Hence $b_1^t b_2$ is conjugate to $a_1 a_2^t$, so $F_{a_1^t a_2} = F_{b_1^t b_2}$. Also $b_1^t b_2^{-1} = J_k a_1 J_k^t J_k (a_2^{-1})^t J_k^t$. Again we see that $b_1^t b_2^{-1}$ is conjugate to $a_1 (a_2^{-1})^t$. Hence $F_{a_1^t a_2^{-1}} = F_{b_1^t b_2^{-1}}$.

2.5. *Let $m \geq 1$ and let $x = a_m$ or b_m. Then the characteristic polynomial of $x^t x^{-1}, x^{-1} x^t$, and $x(x^t)^{-1}$ is*

$$Q_m[\lambda] = \lambda^m - \lambda^{m-1} + \lambda^{m-2} - \cdots + (-1)^m.$$

Proof. First note that, by 1.11, $\operatorname{diag}(a_m, b_m^{-1}) \in \operatorname{Fix}(\tau)$, where $\tau : SL_{2m}(\mathbb{F}) \to SL_{2m}(\mathbb{F})$ is as defined in 1.4.4. Hence by 2.4,

(i) $$F_{a_m^t a_m^{-1}} = F_{b_m^t b_m^{-1}}.$$

Next, note that $x^t x^{-1}$ and $x^{-1}x^t$ are conjugate in $GL(m,\mathbb{F})$ and $x(x^t)^{-1}$, and $(x^t)^{-1}x$ are conjugate in $GL(m,\mathbb{F})$, so it suffices to show the lemma for $x^t x^{-1}$ and $x(x^t)^{-1}$. Now, by 2.7.1 (ahead), since $x(x^t)^{-1} = (x^t x^{-1})^{-1}$, $F_{x(x^t)^{-1}}[\lambda] = (-1)^m \lambda^m F_{x^t x^{-1}}[\lambda^{-1}]$, so if $F_{x^t x^{-1}}[\lambda] = Q_m[\lambda]$, then also $F_{x(x^t)^{-1}}[\lambda] = Q_m[\lambda]$. By (i), it remains to show that $Q_m[\lambda] = F_{a_m^t a_m^{-1}}[\lambda]$. Note now that,

$$a_m^t a_m^{-1} = \begin{bmatrix} 0 & 1 & 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & 1 & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & 0 & 1 & 0 & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & 0 & 1 & 0 \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 & 1 \\ \cdot & \cdot & \cdot & \cdot & \bar{1} & 1 & \bar{1} & 1 \end{bmatrix}$$

and hence $F_{a_m^t a_m^{-1}}[\lambda] = Q_m[\lambda]$.

2.6. *Let $m \geq 1$. Then:*

(1) *For $x = a_m$ or b_m, $F_{x^t x}[\lambda] = F_{x x^t}[\lambda] = F_m[\lambda]$.*
(2) *For $m \geq 3$, $F_m = (\lambda - 2)F_{m-1} - F_{m-2}$, $F_m = (\lambda - 1)G_{m-1} - G_{m-2}$ and $G_m = (\lambda - 2)G_{m-1} - G_{m-2}$.*
(3) *$G_m[\lambda]$ is the characteristic polynomial of the $m \times m$ matrices*

$$y_m = \begin{bmatrix} 2 & 1 & 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ 1 & 2 & 1 & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & 1 & 2 & 1 & 0 & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & 0 & 1 & 2 & 1 & 0 \\ 0 & \cdot & \cdot & \cdot & 0 & 1 & 2 & 1 \\ 0 & \cdot & \cdot & \cdot & \cdot & 0 & 1 & 2 \end{bmatrix} \qquad \text{and}$$

$$z_m = \begin{bmatrix} 2 & \bar{1} & 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ \bar{1} & 2 & \bar{1} & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & \bar{1} & 2 & \bar{1} & 0 & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & 0 & \bar{1} & 2 & \bar{1} & 0 \\ 0 & \cdot & \cdot & \cdot & 0 & \bar{1} & 2 & \bar{1} \\ 0 & \cdot & \cdot & \cdot & \cdot & 0 & \bar{1} & 2 \end{bmatrix}.$$

(4) $F_m[\lambda] = \sum_{\ell=0}^{m}(-1)^{m+\ell}\binom{m+\ell}{2\ell}\lambda^\ell$.
(5) $G_m[\lambda] = \sum_{\ell=0}^{m}(-1)^{m+\ell}\binom{m+\ell+1}{2\ell+1}\lambda^\ell$.
(6) *Let $\gamma \in \mathbb{F}$ and suppose that for some $\ell \geq 2$, $F_\ell[\gamma] = 0$. Then $G_{\ell-1}[\gamma] \neq 0$.*

Proof. For (1), we already observed (using 1.11) that $\operatorname{diag}(a_m, b_m^{-1}) \in \operatorname{Fix}(\tau)$ and (1) follows from 2.4, and since, by definition, $F_m = F_{a_m^t a_m}$. Next, by definition $G_m = F_{y_m}$ (y_m as in (3)). Observe now that

$$a_m^t a_m = \begin{bmatrix} 2 & 1 & 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ 1 & 2 & 1 & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & 1 & 2 & 1 & 0 & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & 0 & 1 & 2 & 1 & 0 \\ 0 & \cdot & \cdot & \cdot & 0 & 1 & 2 & 1 \\ 0 & \cdot & \cdot & \cdot & \cdot & 0 & 1 & 1 \end{bmatrix}.$$

Now $F_m = \det(\lambda I_m - a_m^t a_m)$. Developing $\det(\lambda I_m - a_m^t a_m)$ using the first row, we easily get that for $m \geq 3$, $F_m = (\lambda - 2)F_{m-1} - F_{m-2}$. Developing $\det(\lambda I_m - a_m^t a_m)$ using the last row, we easily get $F_m = (\lambda-1)G_{m-1} - G_{m-2}$. Also developing $\det(\lambda I_m - y_m)$ using the first row gives $G_m = (\lambda-2)G_{m-1} - G_{m-2}$ and (2) is proved.

For (3), note that z_m is obtained from y_m by conjugating by $\operatorname{diag}(1, -1, 1, -1, \dots, (-1)^{m+1})$, so $F_{z_m}[\lambda] = F_{y_m}[\lambda] = G_m[\lambda]$.

To prove (4) and (5), note that $F_1 = \lambda - 1$, $F_2 = \lambda^2 - 3\lambda + 1$ and $G_1 = \lambda - 2$, $G_2 = \lambda^2 - 4\lambda + 3$. So (4) and (5) are the characteristic polynomials when $m = 1, 2$. Then, using (2), for $m \geq 3$, $\alpha(F_m, 0) = -2\alpha(F_{m-1}, 0) - \alpha(F_{m-2}, 0)$ and for $1 \leq \ell \leq m$, $\alpha(F_m, \ell) = \alpha(F_{m-1}, \ell - 1) - 2\alpha(F_{m-1}, \ell) - \alpha(F_{m-2}, \ell)$. The same equalities hold if we replace F by G. We must show that for $m \geq 3$.

(i) $$(-1)^m = -2(-1)^{m-1} - (-1)^{m-2}$$

(ii) $$(-1)^m \binom{m+1}{1} = -2(-1)^{m-1}\binom{m}{1} - (-1)^{m-2}\binom{m-1}{1}$$

(iii) $$\begin{aligned}(-1)^{m+\ell}\binom{m+\ell}{2\ell} &= (-1)^{m-1+\ell-1} \cdot \binom{m+\ell-2}{2\ell-2} \\ &\quad - 2(-1)^{m-1+\ell} \cdot \binom{m+\ell-1}{2\ell} \\ &\quad - (-1)^{m-2+\ell} \cdot \binom{m+\ell-2}{2\ell}\end{aligned}$$

(iv) $$(-1)^{m+\ell}\cdot\binom{m+\ell+1}{2\ell+1} = (-1)^{m-1+\ell-1}\cdot\binom{m+\ell-1}{2\ell-1} - 2(-1)^{m-1+\ell}\cdot\binom{m+\ell}{2\ell+1} - (-1)^{m-2+\ell}\cdot\binom{m+\ell-1}{2\ell+1}.$$

For (i), note that $-2(-1)^{m-1}-(-1)^{m-2} = 2(-1)^m-(-1)^m$. For (ii), note that $-2(-1)^{m-1}\binom{m}{1}-(-1)^{m-2}\binom{m-1}{1} = 2(-1)^m m-(-1)^m(m-1) = (-1)^m(m+1)$.

For (iii) we have

$$\begin{aligned}&(-1)^{m-1+\ell-1}\cdot\binom{m+\ell-2}{2\ell-2} - 2(-1)^{m-1+\ell}\cdot\binom{m+\ell-1}{2\ell}\\ &\quad - (-1)^{m-2+\ell}\cdot\binom{m+\ell-2}{2\ell}\\ &= (-1)^{m+\ell}\left\{\binom{m+\ell-2}{2\ell-2}+2\binom{m+\ell-1}{2\ell}-\binom{m+\ell-2}{2\ell}\right\}.\end{aligned}$$

Note now that

$$\begin{aligned}&\binom{m+\ell-2}{2\ell-2}-\binom{m+\ell-2}{2\ell}\\ &= \binom{m+\ell-2}{2\ell-2}+\binom{m+\ell-2}{2\ell-1}-\binom{m+\ell-2}{2\ell-1}-\binom{m+\ell-2}{2\ell}\\ &= \binom{m+\ell-1}{2\ell-1}-\binom{m+\ell-1}{2\ell}.\end{aligned}$$

Thus

$$\begin{aligned}&(-1)^{m+\ell}\left\{\binom{m+\ell-2}{2\ell-2}+\binom{m+\ell-1}{2\ell}-\binom{m+\ell-2}{2\ell}\right\}\\ &= (-1)^{m+\ell}\left\{\binom{m+\ell-1}{2\ell-1}+\binom{m+\ell-1}{2\ell}\right\}\\ &= (-1)^{m+\ell}\cdot\binom{m+\ell}{2\ell}\end{aligned}$$

and (iii) is proved.

For (iv) we have

$$\begin{aligned}
&(-1)^{m-1+\ell-1}\cdot\binom{m+\ell-1}{2\ell-1}-2(-1)^{m-1+\ell}\cdot\binom{m+\ell}{2\ell+1}\\
&\quad-(-1)^{m-2+\ell}\cdot\binom{m+\ell-1}{2\ell+1}\\
&=(-1)^{m+\ell}\left\{\binom{m+\ell-1}{2\ell-1}+2\binom{m+\ell}{2\ell+1}-\binom{m+\ell-1}{2\ell+1}\right\}
\end{aligned}$$

and as in the previous paragraph of the proof we get (iv). This shows (4) and (5).

Suppose that $F_\ell[\gamma]=0=G_{\ell-1}[\gamma]$, for some $\ell\geq 2$, then, by (2), also $G_{\ell-2}[\gamma]=0$. Then, using (2), we see that $G_m[\gamma]=0$, for all $1\leq m\leq\ell$. In particular, $G_1[\gamma]=0=G_2[\gamma]$, so $\gamma=2$ and $0=2^2-4\cdot 2+3=-1$, a contradiction.

2.7. *Let $h,g\in SL_n(\mathbb{F})$ and let $Q[\lambda]=F_g$. Then:*

(1) $\overline{Q}=(-1)^n\lambda^nQ[\lambda^{-1}]$. *In particular, for all $0\leq\ell\leq n$, $\alpha(\overline{Q},\ell)=(-1)^n\alpha(Q,n-\ell)$.*
(2) $F_{hg}[\lambda]=F_{gh}[\lambda]=\det(\lambda h^{-1}-g)$.
(3) *Suppose $\ell,m\geq 1$ are integers and $\epsilon\in\{1,-1\}$. Suppose $h^{-1}=\operatorname{diag}(I_{\ell-1},s^{-1},I_{m-1})$, where s is a $(2+\epsilon)\times(2+\epsilon)$ matrix. Then $F_{hg}=\det(r+(\lambda I-g))$, where $r=\operatorname{diag}(0_{\ell-1},\lambda s^{-1}-\lambda I_{2+\epsilon},0_{m-1})$.*

Proof. Set $I=I_n$. Then $F_{g^{-1}}=\det(\lambda I-g^{-1})=\det\{-\lambda I(\lambda^{-1}I-g)g^{-1}\}=(-\lambda)^n\det(\lambda^{-1}I-g)=(-1)^n\lambda^nQ[\lambda^{-1}]$.

For (2), we have $\det(\lambda I-gh)=\det\{(\lambda h^{-1}-g)h\}=\det(\lambda h^{-1}-g)$. Finally, for (3), $\det(\lambda h^{-1}-g)=\det(\lambda h^{-1}-\lambda I+\lambda I-g)=\det(r+\lambda I-g)$, because $r=\lambda h^{-1}-\lambda I$.

2.8. *Let $\ell,m\geq 1$ be two integers such that $\ell+m=2k$. Let $\mathfrak{A}\in M_\ell(\mathfrak{R})$ and $\mathfrak{B}\in M_m(\mathfrak{R})$. If $\epsilon=0$, let $g=\operatorname{diag}(\mathfrak{A},\mathfrak{B})$, while if $\epsilon=1$, let $g=\operatorname{diag}(\mathfrak{A},\mu,\mathfrak{B})$, with $0\neq\mu\in\mathfrak{R}$. Let f be the following $(2+\epsilon)\times(2+\epsilon)$ matrix over $\mathfrak{R}$*

$$f=\begin{bmatrix}\alpha&\beta\\\gamma&\delta\end{bmatrix}\qquad\textit{when}\;\;\epsilon=0,$$

$$f=\begin{bmatrix}\alpha_{11}&\alpha_{12}&\alpha_{13}\\\alpha_{21}&\alpha_{22}&\alpha_{23}\\\alpha_{31}&\alpha_{32}&\alpha_{33}\end{bmatrix}\qquad\textit{when}\;\;\epsilon=1.$$

Let $r=\operatorname{diag}(0_{\ell-1},f,0_{m-1})$. Then:

(1) *If* $\epsilon = 0$, *then*

$$\begin{aligned}\det(r+g) = {} & \det(\mathfrak{A})\det(\mathfrak{B}) + \delta\det(\mathfrak{A})\det(M_{1,1}(\mathfrak{B})) \\ & + \alpha\det(M_{\ell,\ell}(\mathfrak{A}))\det(\mathfrak{B}) \\ & + \det\begin{bmatrix}\alpha & \beta \\ \gamma & \delta\end{bmatrix}\det(M_{\ell,\ell}(\mathfrak{A}))\det(M_{1,1}(\mathfrak{B})).\end{aligned}$$

(2) *If* $\epsilon = 1$, *then*

$$\begin{aligned}\det(r+g) = {} & (\alpha_{22}+\mu)\det(\mathfrak{A})\det(\mathfrak{B}) \\ & + \det\begin{bmatrix}\alpha_{22}+\mu & \alpha_{23} \\ \alpha_{32} & \alpha_{33}\end{bmatrix}\det(\mathfrak{A})\det(M_{1,1}(\mathfrak{B})) \\ & + \det\begin{bmatrix}\alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22}+\mu\end{bmatrix}\det(M_{\ell,\ell}(\mathfrak{A}))\det(\mathfrak{B}) \\ & + \det\begin{bmatrix}\alpha_{11} & \alpha_{12} & \alpha_{13} \\ \alpha_{21} & \alpha_{22}+\mu & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33}\end{bmatrix}\det(M_{\ell,\ell}(\mathfrak{A}))\det(M_{1,1}(\mathfrak{B})).\end{aligned}$$

Proof. (1) is proved by expanding $\det(r+g)$ along row $\ell+1$. For (2), expanding $\det(r+g)$ along the $(\ell+1)$-row, we get

$$\text{(i)}\quad \begin{aligned}\det(r+g) = {} & -\alpha_{21}\det(r_1+g_1) \\ & + (\alpha_{22}+\mu)\det(r_2+g_2) - \alpha_{23}\det(r_3+g_3)\end{aligned}$$

where $r_1 = \operatorname{diag}\left(0_{\ell-1}, \begin{bmatrix}\alpha_{12} & \alpha_{13} \\ \alpha_{32} & \alpha_{33}\end{bmatrix}, 0_{m-1}\right)$, $g_1 = \operatorname{diag}(\mathfrak{A}_1, \mathfrak{B})$, and $\mathfrak{A}_1$ is obtained from $\mathfrak{A}$ by replacing the last column by a column of zeros. $r_2 = \operatorname{diag}\left(0_{\ell-1}, \begin{bmatrix}\alpha_{11} & \alpha_{13} \\ \alpha_{31} & \alpha_{33}\end{bmatrix}, 0_{m-1}\right)$, and $g_2 = \operatorname{diag}(\mathfrak{A}, \mathfrak{B})$. $r_3 = \operatorname{diag}\left(0_{\ell-1}, \begin{bmatrix}\alpha_{11} & \alpha_{12} \\ \alpha_{31} & \alpha_{32}\end{bmatrix}, 0_{m-1}\right)$, $g_3 = \operatorname{diag}(\mathfrak{A}, \mathfrak{B}_1)$, and $\mathfrak{B}_1$ is obtained from $\mathfrak{B}$ by replacing the first column by a column of zeros. Notice now that $\det(\mathfrak{A}_1) = 0 = \det(\mathfrak{B}_1)$ and $\det(M_{\ell,\ell}(\mathfrak{A}_1)) = \det(M_{\ell,\ell}(\mathfrak{A}))$, while $\det(M_{1,1}(\mathfrak{B}_1)) = \det(M_{1,1}(\mathfrak{B}))$. Now, by (1), we get

$$\text{(ii)}\quad \begin{aligned}\det(r_1+g_1) = {} & \alpha_{12}\det(M_{\ell,\ell}(\mathfrak{A}))\det(\mathfrak{B}) \\ & + \det\begin{bmatrix}\alpha_{12} & \alpha_{13} \\ \alpha_{32} & \alpha_{33}\end{bmatrix}\det(M_{\ell,\ell}(\mathfrak{A}))\det(M_{1,1}(\mathfrak{B})).\end{aligned}$$

(iii) $$\det(r_2+g_2) = \det(\mathfrak{A})\det(\mathfrak{B}) + \alpha_{33}\det(\mathfrak{A})\det(M_{1,1}(\mathfrak{B})) + \alpha_{11}\det(M_{\ell,\ell}(\mathfrak{A}))\det(\mathfrak{B}) + \det\begin{bmatrix}\alpha_{11} & \alpha_{13}\\ \alpha_{31} & \alpha_{33}\end{bmatrix}\det(M_{\ell,\ell}(\mathfrak{A}))\det(M_{1,1}(\mathfrak{B})).$$

(iv) $$\det(r_3+g_3) = \alpha_{32}\det(\mathfrak{A})\det(M_{1,1}(\mathfrak{B})) + \det\begin{bmatrix}\alpha_{11} & \alpha_{12}\\ \alpha_{31} & \alpha_{32}\end{bmatrix}\det(M_{\ell,\ell}(\mathfrak{A}))\det(M_{1,1}(\mathfrak{B})).$$

Note now that (2) follows from (i)-(iv).

2.9. *Let $\ell, m \geq 1$ be two integers such that $\ell + m = 2k$. Let $A \in M_\ell(\mathbb{F})$ and $B \in M_m(\mathbb{F})$. Let $g = \operatorname{diag}(A, B)$. Let $s \in GL_2(\mathbb{F})$ such that $s^{-1} = \begin{bmatrix}\beta_{11} & \beta_{12}\\ \beta_{21} & \beta_{22}\end{bmatrix}$. Let $h = \operatorname{diag}(I_{\ell-1}, s, I_{m-1})$. Then*

$$F_{hg} = F_AF_B + (\beta_{22}-1)\lambda F_AF_{M_{1,1}(B)} + (\beta_{11}-1)\lambda F_{M_{\ell,\ell}(A)}F_B + \det\begin{bmatrix}(\beta_{11}-1)\lambda & \beta_{12}\lambda\\ \beta_{21}\lambda & (\beta_{22}-1)\lambda\end{bmatrix}F_{M_{\ell,\ell}(A)}F_{M_{1,1}(A)}.$$

Proof. First we mention, that, by definition, if R is a 1×1 matrix over $\mathbb{F}$, we always take $F_{M_{1,1}(R)} = 1$. Next note that $h^{-1} = \operatorname{diag}(I_{\ell-1}, s^{-1}, I_{m-1})$. By 2.7.3, $F_{gh} = \det(r + (\lambda I_n - g))$, where $r = \operatorname{diag}(0_{\ell-1}, \lambda s^{-1} - \lambda I_2, 0_{m-1})$. Note now that

$$\lambda s^{-1} - \lambda I_2 = \begin{bmatrix}(\beta_{11}-1)\lambda & \beta_{12}\lambda\\ \beta_{21}\lambda & (\beta_{22}-1)\lambda\end{bmatrix}$$

also,

$$\lambda I_n - g = \operatorname{diag}(\lambda I_\ell - A, \lambda I_m - B).$$

So if we set $\mathfrak{A} = \lambda I_\ell - A$ and $\mathfrak{B} = \lambda I_m - B$, then by 2.8.1,

$$\begin{aligned}&\det(r + (\lambda I - g))\\ &= \det(\mathfrak{A})\det(\mathfrak{B}) + (\beta_{22}-1)\lambda\det(\mathfrak{A})\det(M_{1,1}(\mathfrak{B}))\\ &\quad + (\beta_{11}-1)\lambda\det(M_{\ell,\ell}(\mathfrak{A}))\det(\mathfrak{B})\\ &\quad + \det\begin{bmatrix}(\beta_{11}-1)\lambda & \beta_{12}\lambda\\ \beta_{21}\lambda & (\beta_{22}-1)\lambda\end{bmatrix}\det(M_{\ell,\ell}(\mathfrak{A}))\det(M_{1,1}(\mathfrak{B})).\end{aligned}$$

The lemma follows.

2.10. *Let $g = \operatorname{diag}(A, 1, B)$, with $A, B \in M_k(\mathbb{F})$. Let $s \in SL_3(\mathbb{F})$ such that*

$$s^{-1} = \begin{bmatrix}\beta_{11} & \beta_{12} & \beta_{13}\\ \beta_{21} & \beta_{22} & \beta_{23}\\ \beta_{31} & \beta_{32} & \beta_{33}\end{bmatrix}.$$

Let $h = \operatorname{diag}(I_{k-1}, s, I_{k-1})$. *Then* $\alpha(F_{hg}, 1) = \alpha(R[\lambda], 1)$, *where*

$$R[\lambda] = (\beta_{22}\lambda - 1)F_A F_B - (\beta_{33} - 1)\lambda F_A F_{M_{1,1}(B)} - (\beta_{11} - 1)\lambda F_{M_{k,k}(A)} F_B.$$

Proof. We use 2.8.2, with $\ell = m = k$. First note that $h^{-1} = \operatorname{diag}(I_{k-1}, s^{-1}, I_{k-1})$. By 2.7.3, $F_{gh} = \det(r + (\lambda I - g))$, where

$$r = \operatorname{diag}(0_{k-1}, \lambda s^{-1} - \lambda I_3, 0_{k-1}).$$

Note now that

$$\lambda s^{-1} - \lambda I_3 = \begin{bmatrix} (\beta_{11} - 1)\lambda & \beta_{12}\lambda & \beta_{13}\lambda \\ \beta_{21}\lambda & (\beta_{22} - 1)\lambda & \beta_{23}\lambda \\ \beta_{31}\lambda & \beta_{32}\lambda & (\beta_{33} - 1)\lambda \end{bmatrix}$$

also, if we set $I = I_n$, then

$$\lambda I - g = \operatorname{diag}(\lambda I_k - A, \lambda - 1, \lambda I_k - B).$$

We use 2.8.2 with $\mathfrak{A} = \lambda I_k - A$, $\mathfrak{B} = \lambda I_k - B$ and $\mu = \lambda - 1$. The α_{ij} are given by the matrix $\lambda s^{-1} - \lambda I_3$ above. By 2.8.2

$$\begin{aligned}
&\det(r + (\lambda I - g)) \\
&= (\beta_{22}\lambda - 1)\det(\mathfrak{A})\det(\mathfrak{B}) \\
&\quad + \det \begin{bmatrix} \beta_{22}\lambda - 1 & \beta_{23}\lambda \\ \beta_{32}\lambda & (\beta_{33} - 1)\lambda \end{bmatrix} \det(\mathfrak{A})\det(M_{1,1}(\mathfrak{B})) \\
&\quad + \det \begin{bmatrix} (\beta_{11} - 1)\lambda & \beta_{12}\lambda \\ \beta_{21}\lambda & \beta_{22}\lambda - 1 \end{bmatrix} \det(M_{k,k}(\mathfrak{A}))\det(\mathfrak{B}) \\
&\quad + \det \begin{bmatrix} (\beta_{11} - 1)\lambda & \beta_{12}\lambda & \beta_{13}\lambda \\ \beta_{21}\lambda & \beta_{22}\lambda - 1 & \beta_{23}\lambda \\ \beta_{31}\lambda & \beta_{32}\lambda & (\beta_{33} - 1)\lambda \end{bmatrix} \det(M_{k,k}(\mathfrak{A}))\det(M_{1,1}(\mathfrak{B}))
\end{aligned}$$

so we see that the only expressions in $\det(r + (\lambda I - g))$ which contribute to the coefficient of λ in $\det(r + (\lambda I - g))$ are

$$\begin{aligned}
(\beta_{22}\lambda - 1)\det(\mathfrak{A})\det(\mathfrak{B}) - (\beta_{33} - 1)\lambda\det(\mathfrak{A})\det(M_{1,1}(\mathfrak{B})) \\
- (\beta_{11} - 1)\lambda\det(M_{k,k}(\mathfrak{A}))\det(\mathfrak{B})
\end{aligned}$$

because the other expressions are in $\lambda^2\mathbb{F}[\lambda]$. This shows the lemma.

2.11. *Let* $m \geq 2$ *be an integer and let* $c, d \in SL_m(\mathbb{F})$ *be two unipotent elements such that* c *is lower triangular and* d *is upper triangular. Let* $x \in SL_m(\mathbb{F})$. *Then:*

(1) $M_{\ell,\ell}(dx) = M_{\ell,\ell}(d)M_{\ell,\ell}(x)$, *for* $\ell \in \{1, (1,2)\}$.
(2) $M_{\ell,\ell}(xc) = M_{\ell,\ell}(x)M_{\ell,\ell}(c)$, *for* $\ell \in \{1, (1,2)\}$.
(3) $M_{m,m}(cx) = M_{m,m}(c)M_{m,m}(x)$ *and* $M_{m,m}(xd) = M_{m,m}(x)M_{m,m}(d)$.
(4) $M_{\ell,\ell}(y^{-1}) = \{M_{\ell,\ell}(y)\}^{-1}$, *for* $y \in \{c, d\}$ *and* $\ell \in \{1, m, (1,2)\}$.

Proof. (1), (2) and (3) are obvious and (4) follows from them.

2.12. *Let $m \geq 3$, $\beta_1, \beta_2, \dots, \beta_m$, $\gamma_1, \gamma_2, \dots, \gamma_m \in \mathbb{F}^*$. For $1 \leq i \leq 3$, let*

$$B_i := b_{m+2-i}(\beta_i, \dots, \beta_m) \quad \textit{and} \quad C_i := b_{m+2-i}(\gamma_i, \dots, \gamma_m).$$

Then:

(1) $F_{C_1^tB_1} = (\lambda - 1)F_{C_2^tB_2} - \beta_1\gamma_1\lambda F_{M_{1,1}(B_2C_2^t)}$.
(2) $F_{(C_1^tB_1)^{-1}} = \{(1+\beta_1\gamma_1)\lambda - 1\}F_{(C_2^tB_2)^{-1}} - \beta_1\gamma_1\lambda^2 F_{(C_3^tB_3)^{-1}}$.
(3) $F_{C_1^tB_1^{-1}} = (\lambda - 1)F_{C_2^tB_2^{-1}} + \beta_1\gamma_1\lambda F_{C_3^tB_3^{-1}}$.
(4) *If* $B_2 = C_2 = b_m$, $F_{C_1^tB_1} = (\lambda - 1)F_m - \beta_1\gamma_1\lambda G_{m-1}$.
(5) *If* $B_2 = C_2 = b_m$, *then* $F_{C_1^tB_1^{-1}} = (\lambda - 1)Q_m + \beta_1\gamma_1\lambda Q_{m-1}$.

Proof. First note that (4) and (5) follow from (1) and (3) respectively, since, if $B_2 = C_2 = b_m$, then, by 2.6, $F_{C_2^tB_2} = F_m$ and, by 2.5, $F_{C_2^tB_2^{-1}} = Q_m$, $F_{C_3^tB_3^{-1}} = Q_{m-1}$ and we leave it for the reader to verify that $F_{M_{1,1}(B_2C_2^t)} = G_{m-1}$.

To prove (1), (2) and (3), let $u = u_1^{m+1}(-\beta_1)$ and $w = u_1^{m+1}(-\gamma_1)$. Note first that $B_1 = u\,\mathrm{diag}\,(1, B_2)$ and $C_1 = w\,\mathrm{diag}\,(1, C_2)$. Hence

(i) $$C_1^tB_1 = \mathrm{diag}\,(1, C_2^t)w^tu\,\mathrm{diag}\,(1, B_2)$$

(ii) $$(C_1^tB_1)^{-1} = \mathrm{diag}\,(1, B_2^{-1})u^{-1}(w^t)^{-1}\mathrm{diag}\,(1, (C_2^t)^{-1})$$

(iii) $$C_1^tB_1^{-1} = \mathrm{diag}\,(1, C_2^t)\mathrm{diag}\,(1, B_2^{-1})w^tu^{-1}$$

where (iii) follows from the fact that $\mathrm{diag}\,(1, B_2^{-1})$ and w^t commute.

For (1), (2) and (3), given $S \in \{C_1^tB_1, C_1^tB_1^{-1}, (C_1^tB_1)^{-1}\}$, we find $g, h \in SL_{m+1}(\mathbb{F})$ and $B \in SL_m(\mathbb{F})$ (g, h and B depend on S) such that S is conjugate to hg, with $g = \mathrm{diag}\,(1, B)$ and $h^{-1} = \mathrm{diag}\,(s, I_{m-1})$. Then we use 2.9 (with $\ell = 1$ and $m = m$) to compute F_{hg}. Note that by 2.9 if $A \in M_1(\mathbb{F})$, $B \in M_m(\mathbb{F})$, then for $g = \mathrm{diag}\,(A, B)$ and $h^{-1} = \mathrm{diag}\left(\begin{bmatrix}\alpha & \beta\\ \gamma & \delta\end{bmatrix}, I_{m-1}\right)$,

(iv) $$F_{hg} = F_AF_B + (\delta - 1)\lambda F_AF_{M_{1,1}(B)} + (\alpha - 1)\lambda F_B + \det\begin{bmatrix}(\alpha-1)\lambda & \beta\gamma\\ \gamma\lambda & (\delta-1)\lambda\end{bmatrix}F_{M_{1,1}(B)}.$$

In all cases we take $A = 1$.

(v) In (1), take $B = B_2C_2^t$; in (2) take $B = (B_2C_2^t)^{-1}$; in (3) take $B = C_2^tB_2^{-1}$.

Also

(vi) in (1), take $h^{-1} = (w^tu)^{-1} = \mathrm{diag}\left(\begin{bmatrix}1 & \gamma_1\\ \beta_1 & \beta_1\gamma_1 + 1\end{bmatrix}, I_{m-1}\right)$;

in (2) take $h^{-1} = w^tu = \mathrm{diag}\left(\begin{bmatrix}1+\beta_1\gamma_1 & -\gamma_1\\ -\beta_1 & 1\end{bmatrix}, I_{m-1}\right)$;

in (3) take $h^{-1} = (w^tu^{-1})^{-1} = \mathrm{diag}\left(\begin{bmatrix}1 & \gamma_1\\ -\beta_1 & -\beta_1\gamma_1 + 1\end{bmatrix}, I_{m-1}\right)$.

We now use (iv), (v) and (vi) to prove (1) (2) and (3).

In (1), taking $B = B_2C_2^t$, we get

$$\begin{aligned} F_{C_1^tB_1} &= (\lambda-1)F_B + \beta_1\gamma_1\lambda(\lambda-1)F_{M_{1,1}(B)} \\ &\quad + \det\begin{bmatrix} 0 & \gamma_1\lambda \\ \beta_1\lambda & \beta_1\gamma_1\lambda \end{bmatrix} F_{M_{1,1}(B)} \\ &= (\lambda-1)F_{B_2C_2^t} - \beta_1\gamma_1\lambda F_{M_{1,1}(B_2C_2^t)} \end{aligned}$$

also, in (3), taking $B = C_2^tB_2^{-1}$, we get

$$\begin{aligned} F_{C_1^tB_1^{-1}} &= (\lambda-1)F_B - \beta_1\gamma_1\lambda(\lambda-1)F_{M_{1,1}(B)} \\ &\quad + \det\begin{bmatrix} 0 & \gamma_1\lambda \\ -\beta_1\lambda & -\beta_1\gamma_1\lambda \end{bmatrix} F_{M_{1,1}(B)} \\ &= (\lambda-1)F_{C_2^tB_2^{-1}} + \beta_1\gamma_1\lambda F_{M_{1,1}(C_2^tB_2^{-1})}. \end{aligned}$$

Since $M_{1,1}(C_2^tB_2^{-1}) = C_3^tB_3^{-1}$, we get (3). Finally in (2), taking $B = (B_2C_2^t)^{-1}$, we get

$$\begin{aligned} F_{(C_1^tB_1)^{-1}} &= (\lambda-1)F_B + \beta_1\gamma_1\lambda F_B \\ &\quad + \det\begin{bmatrix} \beta_1\gamma_1\lambda & -\gamma_1\lambda \\ -\beta_1\lambda & 0 \end{bmatrix} F_{M_{1,1}(B)} \\ &= \{\lambda - 1 + \beta_1\gamma_1\lambda\}F_{(B_2C_2^t)^{-1}} - \beta_1\gamma_1\lambda^2 F_{M_{1,1}((B_2C_2^t)^{-1})}. \end{aligned}$$

Note however that $F_{(B_2C_2^t)^{-1}} = F_{(C_2^tB_2)^{-1}}$ and that, by 2.11.1, $M_{1,1}\{(B_2C_2^t)^{-1}\} = (B_3C_3^t)^{-1}$ and again $F_{(B_3C_3^t)^{-1}} = F_{(C_3^tB_3)^{-1}}$.

2.13. *Suppose $n=2k$. Let $\alpha\in\mathbb{F}^*$ and set $u=u_k^n(\alpha)$. Let $X=\operatorname{diag}(a_k, b_k^{-1})u$ and let H_n be the characteristic polynomial of X^tX. Then:*

(1) $$H_n = \overline{F}_k(F_k + \alpha^2\lambda G_{k-1}) - \alpha^2\lambda^2 G_{k-1}\overline{F}_{k-1}.$$

(2) $$\alpha(H_n, 1) = -\binom{k+1}{2} - (\alpha^2+2)k + 1.$$

Suppose $\alpha = 1$. Then:

(3) *If* $\operatorname{char}(\mathbb{F}) = 3$ *and* $k \equiv 0$ *or* $2 \pmod 3$, *then* $\alpha(H_n, 1) \neq 0$.
(4) *If* $\operatorname{char}(\mathbb{F}) = 2$ *and* $k \equiv 0$ *or* $1 \pmod 4$, *then* $\alpha(H_n, 1) \neq 0$.
(5) *If* $\operatorname{char}(F) = 2$ *and* $k \equiv -2$ *or* $3 \pmod 8$, *then* $\alpha(H_n, 2) \neq 0$.
(6) *If* $\operatorname{char}(F) = 2$ *and* $k \equiv 2 \pmod 8$, *then either* $\alpha(H_n, 4) \neq 0$ *or* $\alpha(H_n, 7) \neq 0$.
(7) *If* $\operatorname{char}(F) = 2$ *and* $k \equiv -1 \pmod 8$, *then* $\alpha(H_n, 2^s) = 1$, *where s is defined by $k = m2^{s+1} - 1$, with m odd.*

Proof. For (1), we'll use 2.9. But first we observe that

(i) $$X^tX = u^t\operatorname{diag}(a_k^ta_k, (b_k^t)^{-1}b_k^{-1})u.$$

Further, by definition and by 2.6.1,

(ii) $$F_{a_k^t a_k} = F_k \qquad F_{(b_k^t)^{-1} b_k^{-1}} = \overline{F}_k.$$

Also, by 2.11.1 and 2.11.4,

(iii) $$M_{1,1}((b_k^t)^{-1} b_k^{-1}) = (b_{k-1}^t)^{-1} b_{k-1}^{-1} \quad \text{so} \quad F_{M_{1,1}((b_k^t)^{-1} b_k^{-1})} = \overline{F}_{k-1}.$$

Finally observe that by definition and by the shape of $a_k^t a_k$

(iv) $$F_{M_{k,k}(a_k^t a_k)} = G_{k-1}.$$

Set $h = uu^t$. Of course $h = \operatorname{diag}(I_{k-1}, s, I_{k-1})$, with $s^{-1} = \begin{bmatrix} \alpha^2+1 & \bar{\alpha} \\ \bar{\alpha} & 1 \end{bmatrix}$. Note that, by (i), H_n is the characteristic polynomial of hg, with $g = \operatorname{diag}(A, B)$, $A = a_k^t a_k$ and $B = (b_k^t)^{-1} b_k^{-1}$. Thus by 2.9

$$\begin{aligned} H_n = F_{hg} &= F_A F_B + \alpha^2 \lambda F_{M_{k,k}(A)} F_B \\ &\qquad + \det \begin{bmatrix} \alpha^2\lambda & \bar{\alpha}\lambda \\ \bar{\alpha}\lambda & 0 \end{bmatrix} F_{M_{k,k}(A)} F_{M_{1,1}(B)} \\ &= F_A F_B + \alpha^2 \lambda F_{M_{k,k}(A)} F_B - \alpha^2 \lambda^2 F_{M_{k,k}(A)} F_{M_{1,1}(B)}. \end{aligned}$$

Using (ii), (iii) and (iv) we see that (1) holds. Next, using 2.6 and 2.7,

$$\begin{aligned} &\alpha(H_n, 1) = \alpha(\overline{F}_k, 0)\{\alpha(F_k, 1) + \alpha^2 \alpha(G_{k-1}, 0)\} + \alpha(F_k, 0)\alpha(\overline{F}_k, 1) \\ &\alpha(\overline{F}_k, 0) = (-1)^k = \alpha(F_k, 0), \quad \alpha(G_{k-1}, 0) = (-1)^{k-1}\binom{k}{1} \\ &\alpha(F_k, 1) = (-1)^{k+1}\binom{k+1}{2}, \quad \alpha(\overline{F}_k, 1) = (-1)^k(1-2k). \end{aligned}$$

Thus

$$\begin{aligned} \alpha(H_n, 1) &= (-1)^k \left\{ (-1)^{k+1}\binom{k+1}{2} + \alpha^2 (-1)^{k-1}\binom{k}{1} \right\} \\ &\qquad + (-1)^k(-1)^k(1-2k) \\ &= -\binom{k+1}{2} - \binom{k}{1}\alpha^2 - 2k + 1 \\ &= -\binom{k+1}{2} - (\alpha^2+2)k + 1. \end{aligned}$$

This shows (2). For the remainder of the proof we assume that $\alpha = 1$. Suppose first that $\operatorname{char}(\mathbb{F}) = 3$. By (2), $\alpha(H_n, 1) = -\binom{k+1}{2} + 1$. Thus if $k \equiv 0$ or $2 \pmod 3$, $\alpha(H_n, 1) \neq 0$ and (3) is proved.

So suppose that $\operatorname{char}(\mathbb{F}) = 2$. By (2), $\alpha(H_n, 1) = \binom{k+1}{2} + k + 1$. Hence if $k \equiv 0$ or $1 \pmod 4$, $\alpha(H_n, 1) = 1$ and (4) is proved. Recall from 2.6 and 2.7

that

(∗)

$$F_k[\lambda] = 1 + \binom{k+1}{2}\lambda + \binom{k+2}{4}\lambda^2 + \binom{k+3}{6}\lambda^3 + \binom{k+4}{8}\lambda^4 + \cdots$$
$$\overline{F}_k[\lambda] = 1 + \binom{2k-1}{1}\lambda + \binom{2k-2}{2}\lambda^2 + \binom{2k-3}{3}\lambda^3 + \binom{2k-4}{4}\lambda^4 + \cdots$$
$$\overline{F}_{k-1}[\lambda] = 1 + \binom{2k-3}{1}\lambda + \binom{2k-4}{2}\lambda^2 + \binom{2k-5}{3}\lambda^3 + \binom{2k-6}{4}\lambda^4 + \cdots$$
$$G_{k-1} = k + \binom{k+1}{3}\lambda + \binom{k+2}{5}\lambda^2 + \binom{k+3}{7}\lambda^3 + \binom{k+4}{9}\lambda^4 + \cdots.$$

Suppose first that $k \equiv -2 \pmod 8$. Using (∗), note that $\overline{F}_k \equiv 1 + \lambda + \lambda^2 \pmod{(\lambda^3)}$, $F_k \equiv 1 + \lambda \pmod{(\lambda^3)}$ and $G_{k-1} \equiv \lambda \pmod{(\lambda^2)}$. Hence modulo the ideal (λ^3), $\overline{F}_k(F_k + \lambda G_{k-1}) - \lambda^2 G_{k-1}\overline{F}_{k-1} \equiv (1+\lambda+\lambda^2)(1+\lambda+\lambda^2) \equiv 1 + \lambda^2$. Thus $\alpha(H_n, 2) \neq 0$.

Suppose $k \equiv 3 \pmod 8$. Then by (∗), $\overline{F}_k \equiv 1+\lambda \pmod{(\lambda^3)}$, $F_k \equiv 1+\lambda^2 \pmod{(\lambda^3)}$, $G_{k-1} \equiv 1 \pmod{(\lambda^2)}$ and $\overline{F}_{k-1} \equiv 1 \pmod{(\lambda)}$. Hence, modulo the ideal (λ^3), $\overline{F}_k(F_k + \lambda G_{k-1}) - \lambda^2 G_{k-1}\overline{F}_{k-1} \equiv (1+\lambda)(1+\lambda^2+\lambda) + \lambda^2 \equiv 1 + \lambda^2$. This completes the proof of (5).

Suppose $k = 8m + 2$. Note that $\binom{k+1}{2} \equiv 1 \pmod 2$, $\binom{k+2}{4} \equiv \frac{4\cdot 2}{4\cdot 2} \equiv 1 \pmod 2$, $\binom{k+3}{6} \equiv \frac{4\cdot 2\cdot(k-2)}{2\cdot 4\cdot 2} \equiv 0 \pmod 2$, $\binom{k+4}{8} \equiv \frac{2\cdot 4\cdot 2\cdot(k-2)}{8\cdot 2\cdot 4\cdot 2} \equiv m \pmod 2$, $\binom{k+5}{10} \equiv \frac{2\cdot 4\cdot 2\cdot(k-2)\cdot 2}{2\cdot 8\cdot 2\cdot 4\cdot 2} \equiv m \pmod 2$. $\binom{k+6}{12} \equiv \frac{(k+6)2\cdot 4\cdot 2\cdot(k-2)\cdot 2}{4\cdot 2\cdot 8\cdot 2\cdot 4\cdot 2} \equiv \frac{(k+6)\cdot(k-2)}{4\cdot 8} \equiv 0 \pmod 2$, and similarly, $\binom{k+7}{14} \equiv 0 \pmod 2$. Hence, by (∗),

$$F_k \equiv 1 + \lambda + \lambda^2 + m\lambda^4 + m\lambda^5 \pmod{(\lambda^8)}.$$

Next, $\binom{2k-1}{1} \equiv 1 \pmod 2$, $\binom{2k-2}{2} \equiv 1 \pmod 2$, $\binom{2k-3}{3} \equiv 0 \pmod 2$, $\binom{2k-4}{4} \equiv 0 \pmod 2$ and $\binom{2k-5}{5} \equiv \frac{2\cdot 4}{4\cdot 2} \equiv 1 \pmod 2$, $\binom{2k-6}{6} \equiv \frac{2\cdot 4\cdot 2}{2\cdot 4\cdot 2} \equiv 1 \pmod 2$, $\binom{2k-7}{7} \equiv 0 \pmod 2$. Hence, by (∗),

$$\overline{F}_k = 1 + \lambda + \lambda^2 + \lambda^5 + \lambda^6 \pmod{(\lambda^8)}.$$

Next, $\binom{2k-3}{1} \equiv 1 \pmod 2$, $\binom{2k-4}{2} \equiv 0 \pmod 2$, $\binom{2k-5}{3} \equiv 1 \pmod 2$, $\binom{2k-6}{4} \equiv 1 \pmod 2$, $\binom{2k-7}{5} \equiv 1 \pmod 2$. Hence, by (∗),

$$\overline{F}_{k-1} = 1 + \lambda + \lambda^3 + \lambda^4 + \lambda^5 \pmod{(\lambda^6)}.$$

Finally, $\binom{k}{1} \equiv 0 \pmod 0 \pmod 2$, $\binom{k+1}{3} \equiv 1 \pmod 2$, $\binom{k+2}{5} \equiv \frac{4\cdot 2\cdot(k-2)}{2\cdot 4\cdot 2} \equiv 0 \pmod 2$, $\binom{k+3}{7} \equiv \frac{4\cdot 2\cdot(k-2)}{2\cdot 4\cdot 2} \equiv 0 \pmod 2$, $\binom{k+4}{9} \equiv \frac{2\cdot 4\cdot 2\cdot(k-2)\cdot 2}{8\cdot 2\cdot 4\cdot 2} \equiv 0 \pmod 2$, $\binom{k+5}{11} \equiv \frac{2\cdot 4\cdot 2\cdot(k-2)\cdot 2}{2\cdot 8\cdot 2\cdot 4\cdot 2} \equiv m \pmod 2$, $\binom{k+6}{13} \equiv \frac{(k+6)2\cdot 4\cdot 2\cdot(k-2)\cdot 2\cdot 4}{4\cdot 2\cdot 8\cdot 2\cdot 4\cdot 2} \equiv 0 \pmod 2$. Hence, by (∗),

$$G_{k-1} \equiv \lambda + m\lambda^5 \pmod{(\lambda^7)}.$$

Hence, modulo the ideal (λ^8),

$$\begin{aligned}
&\overline{F}_k(F_k+\lambda G_{k-1})-\lambda^2 G_{k-1}\overline{F}_{k-1}\\
&=(1+\lambda+\lambda^2+\lambda^5+\lambda^6)(1+\lambda+\lambda^2+m\lambda^4+m\lambda^5+\lambda^2+m\lambda^6)\\
&\quad+\lambda^2(\lambda+m\lambda^5)(1+\lambda+\lambda^3+\lambda^4+\lambda^5)\\
&=(1+\lambda+\lambda^2+\lambda^5+\lambda^6)(1+\lambda+m\lambda^4+m\lambda^5+m\lambda^6)\\
&\quad+(\lambda^3+m\lambda^7)(1+\lambda+\lambda^3+\lambda^4+\lambda^5).
\end{aligned}$$

Thus $\alpha(H_n,4)=m+1$ and $\alpha(H_n,7)=(m+m+1)+(1+m)=m$. Hence either $\alpha(H_n,4)\neq 0$, or $\alpha(H_n,7)\neq 0$ and (6) is proved.

Finally, suppose $k\equiv -1 \pmod 8$. Write $k=m2^{s+1}-1$, with $s\geq 2$ and m odd. Recall that we are assuming $\operatorname{char}(F)=2$. We claim that $\alpha(H_n,2^s)=1$. Set

$$t=2^s.$$

Note that by 2.6 and 2.7, for $1\leq \ell\leq t$, $\alpha(F_k,\ell)=\binom{k+\ell}{2\ell}$,

$$\begin{aligned}
\alpha(G_{k-1},\ell)&=\binom{k+\ell}{2\ell+1},\\
\alpha(\overline{F}_k,t)&=\alpha(F_k,k-t)=\binom{2k-t}{t}=\binom{2k-2^s}{2^s},\\
\alpha(\overline{F}_k,t-1)&=\alpha(F_k,k-(t-1))=\binom{2k-(t-1)}{t-1}=\binom{2k-2^s+1}{2^s-1}\ \text{and}\\
\alpha(\overline{F}_{k-1},t-2)&=\alpha(F_{k-1},(k-1)-(t-2))=\binom{2(k-1)-(t-2)}{t-2}\\
&=\binom{2k-2^s}{2^s-2}.
\end{aligned}$$

Using 2.3, we see that

$$\begin{aligned}
&F_k\equiv 1+\lambda^t \pmod{(\lambda^{t+1})} \qquad G_{k-1}\equiv 1 \pmod{(\lambda^t)}\\
&\alpha(\overline{F}_k,t)=0,\quad \alpha(\overline{F}_k,t-1)=1,\quad \alpha(\overline{F}_{k-1},t-2)=1.
\end{aligned}$$

Hence $\alpha(H_n,t)$ is the coefficient of λ^t in the polynomial

$$(1+\lambda^{t-1})(1+\lambda+\lambda^t)+\lambda^2\lambda^{t-2}$$

which is 1.

2.14. *Suppose* $\operatorname{char}(\mathbb{F})=3$ *and* $n=2k$. *Let* $\beta\in\{1,-1\}$. *Set* $u=u_k^n(1)$, $h=uu^t$ *and*

$$\begin{aligned}
a(\beta)&=u_1^k(1)u_2^k(1)\cdots u_{k-2}^k(1)u_{k-1}^k(\beta)\\
b(\beta)&=u_1^k(-\beta)u_2^k(-1)u_3^k(-1)\cdots u_{k-1}^k(-1)\\
X(\beta)&=\operatorname{diag}(a(\beta),\{b(\beta)\}^{-1})u.
\end{aligned}$$

Then:

(1) $h = \operatorname{diag}(I_{k-1}, s, I_{k-1})$, *with* $s^{-1} = \begin{bmatrix} 2 & \bar{1} \\ \bar{1} & 1 \end{bmatrix}$.

(2) *If* $x = (a(\beta))^t a(-\beta)$ *and* $y = b(-\beta)(b(\beta))^t$, *then*

$$F_x = F_y = F_k - \lambda G_{k-2}.$$

(3) *Suppose* $k \equiv 1 \pmod 3$. *Set* $X = X(\beta)$, $Y = X(-\beta)$ *and* $L_n[\lambda] = F_{X^tY}$. *Then* $\alpha(L_n, 1) = -1$.

Proof. (1) is obvious. For (2), note that

$$a(\beta) = \begin{bmatrix} 1 & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ 1 & 1 & 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 1 & 1 & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & 1 & 1 & 0 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & 1 & 1 & 0 \\ 0 & \cdot & \cdot & \cdot & \cdot & 0 & \beta & 1 \end{bmatrix} \text{ and } b(\beta) = \begin{bmatrix} 1 & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ \bar{\beta} & 1 & 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & \bar{1} & 1 & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & \bar{1} & 1 & 0 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & \bar{1} & 1 & 0 \\ 0 & \cdot & \cdot & \cdot & \cdot & 0 & \bar{1} & 1 \end{bmatrix}.$$

Hence

$$x = \begin{bmatrix} 1 & 1 & 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 1 & 1 & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & 1 & 1 & 0 & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & 0 & 1 & 1 & 0 \\ 0 & \cdot & \cdot & \cdot & \cdot & 0 & 1 & \beta \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ 1 & 1 & 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 1 & 1 & 0 & \cdot & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & 0 & 1 & 1 & 0 & 0 \\ 0 & \cdot & \cdot & \cdot & \cdot & 1 & 1 & 0 \\ 0 & \cdot & \cdot & \cdot & \cdot & 0 & \bar{\beta} & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 2 & 1 & 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ 1 & 2 & 1 & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & 1 & 2 & 1 & 0 & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & 0 & 1 & 2 & 1 & 0 \\ 0 & \cdot & \cdot & \cdot & 0 & 1 & 0 & \beta \\ 0 & \cdot & \cdot & \cdot & \cdot & 0 & \bar{\beta} & 1 \end{bmatrix},$$

$$y=\begin{bmatrix}1&0&\cdot&\cdot&\cdot&\cdot&\cdot&0\\ \beta&1&0&\cdot&\cdot&\cdot&\cdot&0\\ 0&\bar{1}&1&0&\cdot&\cdot&\cdot&0\\ \cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot\\ \cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot\\ 0&\cdot&\cdot&0&\bar{1}&1&0&0\\ 0&\cdot&\cdot&\cdot&0&\bar{1}&1&0\\ 0&\cdot&\cdot&\cdot&\cdot&0&\bar{1}&1\end{bmatrix}\cdot\begin{bmatrix}1&\bar{\beta}&0&\cdot&\cdot&\cdot&\cdot&0\\ 0&1&\bar{1}&0&\cdot&\cdot&\cdot&0\\ 0&0&1&\bar{1}&0&\cdot&\cdot&0\\ \cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot\\ \cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot\\ 0&\cdot&\cdot&\cdot&0&1&\bar{1}&0\\ 0&\cdot&\cdot&\cdot&\cdot&0&1&\bar{1}\\ 0&\cdot&\cdot&\cdot&\cdot&\cdot&0&1\end{bmatrix}$$

$$=\begin{bmatrix}1&\bar{\beta}&0&\cdot&\cdot&\cdot&\cdot&0\\ \beta&0&\bar{1}&0&\cdot&\cdot&\cdot&0\\ 0&\bar{1}&2&\bar{1}&0&\cdot&\cdot&0\\ \cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot\\ \cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot\\ 0&\cdot&\cdot&0&\bar{1}&2&\bar{1}&0\\ 0&\cdot&\cdot&\cdot&0&\bar{1}&2&\bar{1}\\ 0&\cdot&\cdot&\cdot&\cdot&0&\bar{1}&2\end{bmatrix}.$$

To compute F_x expand $\det(\lambda I_k - x)$ along the last row. Thus

$$F_x = (\lambda-1)F_{M_{k,k}(x)} + G_{k-2}$$

(since $\beta^2 = 1$). Also it is easy to see that

(i) $$F_{M_{k,k}(x)} = \lambda G_{k-2} - G_{k-3}.$$

Thus

(ii) $$F_x = (\lambda-1)\{\lambda G_{k-2} - G_{k-3}\} + G_{k-2}.$$

Expanding F_y along the first row we see that $F_y = F_x$. Recall now from 2.6, that $F_k = (\lambda-1)G_{k-1} - G_{k-2}$ and that $G_{k-1} = (\lambda-2)G_{k-2} - G_{k-3} = (\lambda+1)G_{k-2} - G_{k-3}$. Hence

(iii) $$F_k = (\lambda-1)\{(\lambda+1)G_{k-2} - G_{k-3}\} - G_{k-2}.$$

Thus, from (ii) and (iii) we see that $F_k - F_x = (\lambda-1)G_{k-2} - 2G_{k-2} = (\lambda-1)G_{k-2} + G_{k-2} = \lambda G_{k-2}$. This shows (2).

We proceed with the proof of (3). Note that $X^tY = u^t\mathrm{diag}\,((a(\beta))^t, (\{b(\beta)\}^{-1})^t)\mathrm{diag}\,(a(-\beta), \{b(-\beta)\}^{-1})u = u^t\mathrm{diag}\,(x, y^{-1})u$, with x and y as in (1). Now X^tY is conjugate to $h\mathrm{diag}\,(x, y^{-1})$, so we can use 2.9 to compute L_n. By 2.9 and (1),

(iv) $$L_n = \{F_x + \lambda F_{M_{k,k}(x)}\}F_{y^{-1}} - \lambda^2 F_{M_{k,k}(x)}F_{M_{1,1}(y^{-1})}.$$

Thus, by (iv),

(v) $$\alpha(L_n, 1) = \alpha(\{F_x + \lambda F_{M_{k,k}(x)}\}F_{y^{-1}}, 1).$$

Now, by (i) and (ii), $F_x + \lambda F_{M_{k,k}(x)} = F_k - \lambda G_{k-2} + \lambda\{\lambda G_{k-2} - G_{k-3}\}$. So

(vi) $$F_x + \lambda F_{M_{k,k}(x)} = F_k - \lambda G_{k-2} - \lambda G_{k-3} + \lambda^2 G_{k-2}.$$

Hence, by (v) and (vi),

(vii) $$\alpha(L_n, 1) = \alpha(\{F_k - \lambda G_{k-2} - \lambda G_{k-3}\}F_{y^{-1}}, 1).$$

Now modulo the ideal (λ^2), $F_k \equiv (-1)^k(1-\lambda)$, $\lambda G_{k-2} \equiv (-1)^{k-2}\binom{k-1}{1}\lambda \equiv 0$, $\lambda G_{k-3} \equiv (-1)^{k-3}\binom{k-2}{1}\lambda \equiv (-1)^{k-2}\lambda \equiv (-1)^k\lambda$. Thus

(viii) $$F_k - \lambda G_{k-2} - \lambda G_{k-3} \equiv (-1)^k(1+\lambda) \pmod{(\lambda^2)}.$$

Now, by (2), $F_y = F_k - \lambda G_{k-2} = (\lambda^k - \lambda^{k-1} + \cdots) - (\lambda^{k-1} + \cdots) = \lambda^k + \lambda^{k-1} + \cdots$. It follows from 2.7.1, that

(ix) $$F_{y^{-1}} \equiv (-1)^k(1+\lambda) \pmod{(\lambda^2)}.$$

Hence by (vii), (viii) and (ix), $\alpha(L_n, 1) = \alpha((1+\lambda)^2, 1) = -1$, and (3) is proved.

2.15. *Suppose $n=2k$. Let $\alpha \in \mathbb{F}^*$ and set $u = u_k^n(\alpha)$. Let $X = \mathrm{diag}\,(a_k, b_k^{-1})u$ and set $x = a_k^t a_k^{-1}$ and $y = b_k^{-1}b_k^t$. Then*

$$\alpha\,(F_{X^tX^{-1}}, 1) = \alpha^2 - 2.$$

Proof. Note that $X^tX^{-1} = u^t\mathrm{diag}\,(a_k^t, (b_k^t)^{-1})u^{-1}\mathrm{diag}\,(a_k^{-1}, b_k)$. A moment of thought will convince the reader that u commutes with $\mathrm{diag}\,(a_k^t, (b_k^t)^{-1})$, hence

(i) $$X^tX^{-1} = u^tu^{-1}\mathrm{diag}\,(x, y^{-1}).$$

Set $h = u^tu^{-1}$ and $g = \mathrm{diag}\,(x, y^{-1})$. Then

(ii) $$h^{-1} = \mathrm{diag}\left(I_{k-1}, \begin{bmatrix} 1 & \bar{\alpha} \\ \alpha & 1-\alpha^2 \end{bmatrix}, I_{k-1}\right).$$

We use 2.9, with $A = x$, $B = y^{-1}$, $h = u^tu^{-1}$. By (i), $X^tX^{-1} = hg$. By 2.9,

(iii) $$F_{X^tX^{-1}} = F_xF_{y^{-1}} + (\beta_{22}-1)\lambda F_xF_{M_{1,1}(y^{-1})} + (\beta_{11}-1)\lambda F_{M_{k,k}(x)}F_{y^{-1}} + \det\begin{bmatrix} (\beta_{11}-1)\lambda & \beta_{12}\lambda \\ \beta_{21}\lambda & (\beta_{22}-1)\lambda \end{bmatrix} F_{M_{k,k}(x)}F_{M_{1,1}(y^{-1})}.$$

Of course, by (ii), here $\beta_{11} = 1$, $\beta_{12} = -\alpha$, $\beta_{21} = \alpha$ and $\beta_{22} = 1 - \alpha^2$. Note that by 2.5,

(iv) $$F_x = F_{y^{-1}} = Q_k.$$

Further, by 2.11.1 and 2.11.4, $F_{M_{1,1}(y^{-1})} = F_{(b_{k-1}^{-1})b_{k-1}}$, so by 2.5,

(v) $$F_{M_{1,1}(y^{-1})} = Q_{k-1}.$$

Now by (iii), (iv) and (v), we get

$$F_{X^tX^{-1}} = Q_k\{Q_k - \alpha^2\lambda Q_{k-1}\} + \alpha^2\lambda^2 \cdot F_{M_{k,k}(x)} \cdot F_{M_{1,1}(y^{-1})}.$$

Whence,

$$\begin{aligned}\alpha\left(F_{X^tX^{-1}}, 1\right) &= \alpha(Q_k\{Q_k - \alpha^2\lambda Q_{k-1}\}, 1)\\ &= (-1)^k\{(-1)^{k+1} - \alpha^2(-1)^{k-1}\} + (-1)^k(-1)^{k+1}\\ &= -1 + \alpha^2 - 1\\ &= \alpha^2 - 2.\end{aligned}$$

2.16. *Suppose* $\mathrm{char}\,(\mathbb{F}) = 3$*,* $n = 2k \geq 8$ *and that* $k \equiv 1 \pmod 3$*. Let* $\beta \in \{1, -1\}$ *and let* $a(\beta), b(\beta), X, Y$ *and* u *be as in* 2.14*. Set* $x = (a(\beta))^t(a(-\beta))^{-1}$ *and* $y = (b(-\beta))^{-1}(b(\beta))^t$*. Then*

$$F_x = F_y = \lambda^k + (-1)^k = F_{y^{-1}}, \tag{1}$$

$$\alpha\left(F_{X^tY^{-1}}, 1\right) = 1. \tag{2}$$

Proof. Note that $X^tY^{-1} = u^t\mathrm{diag}\,((a(\beta))^t, ((b(\beta))^t)^{-1})u^{-1}\mathrm{diag}\,((a(-\beta))^{-1}, b(-\beta))$. Now a moment of thought will convince the reader that u commutes with $\mathrm{diag}\,((a(\beta))^t, ((b(\beta))^t)^{-1})$, hence

$$X^tY^{-1} = u^tu^{-1}\mathrm{diag}\,(x, y^{-1}). \tag{i}$$

Set $h = u^tu^{-1}$ and $g = \mathrm{diag}\,(x, y^{-1})$. Then

$$h^{-1} = \mathrm{diag}\left(I_{k-1}, \begin{bmatrix}1 & \bar{1}\\ 1 & 0\end{bmatrix}, I_{k-1}\right). \tag{ii}$$

Next note that, by 1.11, $\mathrm{diag}\,(a(\beta), \{b(\beta)\}^{-1}), \mathrm{diag}\,(a(-\beta), \{b(-\beta)\}^{-1}) \in \mathrm{Fix}\,(\tau)$, so, by 2.4, $F_x = F_y$. Also if $F_y = \lambda^k + (-1)^k$, then, by 2.7.1, $F_{y^{-1}} = \lambda^k + (-1)^k$. We now use 2.12.3 to compute F_y. Take in 2.12.3, $B_1 = b_k(-\beta, 1, \ldots, 1)$ and $C_1 = b_k(\beta, 1, \ldots, 1)$ (notice that $\beta_1 = -\beta$ and $\gamma_1 = \beta$). By 2.12.3, $F_y = (\lambda - 1)Q_{k-1} - \beta^2\lambda Q_{k-2}$ and since $\beta^2 = 1$, $F_y = (\lambda - 1)Q_{k-1} - \lambda Q_{k-2}$. Notice now that $\lambda Q_{k-1} = \lambda^k - Q_{k-1} + (-1)^{k-1}$, and $\lambda Q_{k-2} = Q_{k-1} - (-1)^{k-1}$. Hence $F_y = (\lambda^k - Q_{k-1} + (-1)^{k-1}) - Q_{k-1} - (Q_{k-1} - (-1)^{k-1}) = \lambda^k - 3Q_{k-1} + 2(-1)^{k-1}$. Since $\mathrm{char}\,(\mathbb{F}) = 3$, (1) follows.

Next, $y^{-1} = (\{b(\beta)\}^{-1})^t(b(-\beta))$. By 2.11.4 and 2.11.1, $M_{1,1}(y^{-1}) = (b_{k-1}^{-1})^t b_{k-1}$ and so $F_{M_{1,1}(y^{-1})} = F_{(b_{k-1}^{-1})^t b_{k-1}}$, hence by 2.5

$$F_{M_{1,1}(y^{-1})} = Q_{k-1}. \tag{iii}$$

For (2), we use 2.9, with $A = x$, $B = y^{-1}$, $g = \mathrm{diag}\,(A, B)$ and $h = u^tu^{-1}$. By 2.9,

$$\begin{aligned}F_{hg} = F_AF_B &+ (\beta_{22} - 1)\lambda F_AF_{M_{1,1}(B)} + (\beta_{11} - 1)\lambda F_{M_{k,k}(A)}F_B\\ &+ \det\begin{bmatrix}(\beta_{11} - 1)\lambda & \beta_{12}\lambda\\ \beta_{21}\lambda & (\beta_{22} - 1)\lambda\end{bmatrix} F_{M_{k,k}(A)}F_{M_{1,1}(B)}.\end{aligned}$$

By (i), $X^tY^{-1} = hg$ and by (ii), here $\beta_{11} = 1$, $\beta_{12} = -1$, $\beta_{21} = 1$ and $\beta_{22} = 0$. Using 2.9, (1) and (iii), we get

$$F_{X^tY^{-1}} = (\lambda^k + (-1)^k)\{\lambda^k + (-1)^k - \lambda Q_{k-1}\} + \lambda^2 F_{M_{k,k}(A)} \cdot F_{M_{1,1}(B)}.$$

Hence, $\alpha(F_{X^tY^{-1}}, 1) = \alpha((\lambda^k + (-1)^k)\{\lambda^k + (-1)^k - \lambda Q_{k-1}\}, 1) = 1$, as is easily checked.

3. The Special Linear Groups.

In this section we prove Theorem 1.6 for the groups $L_n(q)$. We let $L = SL_n(\mathbb{F})$. Of course all notation and definitions introduced in Section 1 are maintained here. By 1.7 and 1.9.2, all we have to do is to find an element $X \in L$, such that $B(X, X^t)$. We take

$$X = a_n.$$

3.1. *Let $S \in \{X^tX, X^tX^{-1}, X^t\}$ and let $R \in \Delta^{\leq 2}(X) \cap \Delta^{\leq 1}(S)$. Then v_1 is a characteristic vector of R.*

Proof. Let $h \in \Delta^{\leq 1}(X) \cap \Delta^{\leq 1}(R)$. Note that since X is unipotent and $[X, h] \in Z(L)$, $[X, h] = 1$. By 1.13, there exists $\beta \in \mathbb{F}$ and $1 \leq r < n$, such that $h - \beta I_n \in \mathcal{T}_n(r)$ (see notation in 1.1.10). Put $T = h - \beta I_n$, $j = m = r$ and $\ell = 0$. We'll show that S, T, R, j, m and ℓ satisfy the hypotheses of 1.15. Hence, by 1.15, v_1 is a characteristic vector of R.

Since $(X^t)_{i,i+1} = 1$, while, $(X^t)_{i,k} = 0$, for all $1 \leq i \leq n-1$ and all $i + 1 < k \leq n$, and since X^ϵ is unipotent lower triangular, for $\epsilon \in \{1, -1\}$, it is easy to see that hypothesis (a) of 1.15 is satisfied. Of course $\mathcal{V}_j = \mathcal{V}_r \subseteq \ker(T)$. By definition, $v_{j+1} \notin \ker(T)$. Since $\mathcal{V}_m = \mathcal{V}_r = \ker(T)$ and since R centralizes $T, \mathcal{V}_m$ is R-invariant. By now we verified all hypotheses of 1.15 and the proof of 3.1 is complete.

3.2. *Let $S = XX^t$. Then:*

(1) *If* $\operatorname{char}(\mathbb{F}) \neq 3$, *or* $n - 2 \not\equiv 0 \pmod 3$, *then either* $\alpha(F_S, n-1) \neq 0$ *or* $\alpha(F_S, 1) \neq 0$.
(2) *If* $\operatorname{char}(\mathbb{F}) = 3$ *and* $n - 2 \equiv 3, 6 \pmod 9$, *then* $\alpha(F_S, n-2) \neq 0 \neq \alpha(F_S, n-3)$.
(3) *If* $\operatorname{char}(\mathbb{F}) = 3$ *and* $n - 2 \equiv 0 \pmod 9$, *then* $\alpha(F_S, n-2) \neq 0 \neq \alpha(F_S, n-5)$.

Proof. By definition 1.2.4, $F_S = F_n$. So by 2.6.4,

$$F_S = \sum_{\ell=0}^{n} (-1)^{n+\ell} \binom{n+\ell}{2\ell} \lambda^\ell.$$

In particular, $\alpha(F_S, n-1) = 1 - 2n$ and $\alpha(F_S, 1) = (-1)^{n+1}\binom{n+1}{2}$. Let $p = \operatorname{char}(\mathbb{F})$ and suppose $\alpha(F_S, n-1) = \alpha(F_S, 1) = 0$. It is easy to check that we must have $p = 3$ and $n \equiv -1 \pmod 3$. So suppose $\operatorname{char}(\mathbb{F}) = 3$ and

$n \equiv -1 \pmod 3$. Note that $\alpha(F_S, n-2) = (n-1)(2n-3)$, so $\alpha(F_S, n-2) \neq 0$. If $n-2 \equiv 3, 6 \pmod 9$, then $\alpha(F_S, n-3) = -\binom{2n-3}{3} \not\equiv 0 \pmod 3$. Finally, if $n-2 \equiv 0 \pmod 9$, then $\alpha(F_S, n-5) = -\binom{2n-5}{5} \not\equiv 0 \pmod 3$. We remark that when $n = 2$, Δ is disconnected and there exists no path from X to S in Δ, so evidently $B(X, X^t)$ holds.

3.3. (1) *Let* $S \in \{X^tX, X^tX^{-1}, X^t\}$, *then* $d(X, S) > 3$.
(2) $\Delta(L)$ *is balanced.*

Proof. Let $R \in \Delta^{\leq 2}(X) \cap \Delta^{\leq 1}(S)$. By 3.1,

(i) $$v_1 \text{ is a characteristic vector of } R.$$

Note that for all $1 \leq i \leq n-1$, $v_iS = u + v_{i+1}$, with $u \in \mathcal{V}_i$. Thus

(ii) $$\langle \mathcal{O}(v_1, S)\rangle = V.$$

Now if $S = X^t$, then, by (i), (ii) and 1.14.1, $R \in Z(GL(V))$, a contradiction.

Suppose $S = X^tX$. Note that by 3.2, $\gcd\Big\{\{i : \alpha_{n-i} \neq 0\} \cup \{n\}\Big\} = 1$, thus, by (i), (ii) and 1.14.5, $R \in Z(GL(V))$, a contradiction. Finally suppose $S = X^tX^{-1}$. Then, by 2.5, $\alpha(F_S, n-1) \neq 0$, and again, by 1.14.5, $R \in Z(GL(V))$, a contradiction. This shows (1). (2) follows immediately from (1), since, by definition, $B(X, X^t)$ and then, by 1.9.2, $B(X^t, X)$, so by definition, $\Delta(L)$ is balanced.

4. The Symplectic Groups and Unitary Groups in even dimension.

In this section $n = 2k \geq 4$. Further, $\mathbb{F}$ is a field of order q^2 and $\mathbb{K} \leq \mathbb{F}$ is a field of order q. L is one of the following groups. Either $L = \mathrm{Fix}\,(\tau)$, where $\tau : SL_n(\mathbb{K}) \to SL_n(\mathbb{K})$ is the automorphism defined in 1.4.4, or $L = \mathrm{Fix}\,(\tau\sigma_q)$, where $\tau\sigma_q : SL_n(\mathbb{F}) \to SL_n(\mathbb{F})$ is the automorphism defined in 1.4.4 and 1.4.5. Thus, by 1.12.3, in the first case $L \simeq Sp_n(q)$, and in the second case $L \simeq SU_n(q)$. The purpose of this section is to prove that Theorem 1.6 holds for (the simple version of) L. We'll pick two elements $X, Y \in L$ and show that $B(X, Y^t)$ and $B(Y, X^t)$. By 1.9.1, also $B(Y^t, X)$ and thus the elements X, Y show that $\Delta(L)$ is balanced. In most cases, we'll take $X = Y$, but when $\mathrm{char}\,(\mathbb{F}) = 3$, it turns out that we must pick $Y \neq X$. For the moment we fix elements $\beta_1, \ldots, \beta_{k-1}, \gamma_1, \ldots, \gamma_{k-1}, \alpha \in \mathbb{K}^*$. Using the notation in 1.1.8 we let

$$\begin{aligned} a &= a_k(\beta_1, \ldots, \beta_{k-1}) & a_1 &= a_k(\gamma_1, \ldots, \gamma_{k-1}) \\ b &= b_k(\beta_1, \ldots, \beta_{k-1}) & b_1 &= b_k(\gamma_1, \ldots, \gamma_{k-1}) \\ g &= \mathrm{diag}\,(a, b^{-1}) & g_1 &= \mathrm{diag}\,(a_1, b_1^{-1}) \end{aligned}$$
$$u = u_k^n(\alpha)$$
$$X = gu \qquad\qquad Y = g_1u.$$

Towards the end of Section 4 we'll specialize and give concrete values to β_i, γ_i and α. Note that by 1.11, $X, Y \in L$.

4.1. *Let $u = u_k^n(\alpha)$. Then:*

(1)
$$uu^t = \operatorname{diag}\left(I_{k-1}, \begin{bmatrix} 1 & \alpha \\ \alpha & \alpha^2+1 \end{bmatrix}, I_{k-1}\right)$$
$$(uu^t)^{-1} = \operatorname{diag}\left(I_{k-1}, \begin{bmatrix} \alpha^2+1 & \overline{\alpha} \\ \overline{\alpha} & 1 \end{bmatrix}, I_{k-1}\right).$$

(2)
$$u^{-1}u^t = \operatorname{diag}\left(I_{k-1}, \begin{bmatrix} 1 & \alpha \\ \overline{\alpha} & 1-\alpha^2 \end{bmatrix}, I_{k-1}\right)$$
$$(u^{-1}u^t)^{-1} = \operatorname{diag}\left(I_{k-1}, \begin{bmatrix} 1-\alpha^2 & \overline{\alpha} \\ \alpha & 1 \end{bmatrix}, I_{k-1}\right).$$

(3) $[u, g^t] = 1$.

Proof. This is obvious.

4.2. *Let $\epsilon \in \{1, -1\}$. Then:*

(1) $XY^t = guu^t g_1^t$, $(X, Y^t)^{-1} = (g_1^t)^{-1}(uu^t)^{-1}g^{-1}$.
(2) $X^{-1}Y^t = u^{-1}u^t g^{-1} g_1^t$ *and* $(X^{-1}Y^t)^{-1} = (g_1^t)^{-1} g (u^{-1}u^t)^{-1}$.
(3) $X = \begin{bmatrix} a & 0_{k,k} \\ E & b^{-1} \end{bmatrix}$ *with E some $k \times k$ matrix, such that $E_{1,k} = \alpha$.*
(4) $X^\epsilon Y^t = \begin{bmatrix} a^\epsilon a_1^t & R_{1,2} \\ R_{2,1} & R_{2,2} \end{bmatrix}$ $(X^\epsilon Y^t)^{-1} = \begin{bmatrix} R'_{1,1} & R'_{1,2} \\ R'_{2,1} & b_1^t b^\epsilon \end{bmatrix}$ *with $R_{i,j}$ and $R'_{i,j}$ some $k \times k$ matrices. Further, the first $k-1$ rows of $R_{1,2}$ are zero.*
(5) *Let $S \in \{Y^t, X^\epsilon Y^t\}$. Then for $1 \le i \le k-1$, $v_i S = v + \delta_{i+1} v_{i+1}$, with $v \in \mathcal{V}_i$ and $\delta_{i+1} \in \mathbb{K}^*$.*
(6) *Let $S \in \{Y^t, X^\epsilon Y^t\}$. Then for $k \le i \le n-1$, $v_i S^{-1} = v + \delta_{i+1} v_{i+1}$, with $v \in \mathcal{V}_i$ and $\delta_{i+1} \in \mathbb{K}^*$.*
(7) *Let $S \in \{Y^t, X^\epsilon Y^t\}$, then $V = \langle \mathcal{O}(v_1, S) \rangle$.*
(8) *Let $S \in \{Y^t, X^\epsilon Y^t\}$, then $S_{k,n} \neq 0$.*

Proof. (1) is obvious. For (2), we have $X^{-1}Y^t = u^{-1}g^{-1}u^t g_1^t$. By 4.1.3, $[g^{-1}, u^t] = 1$, and (2) follows. (3) is clear, the $(1, k)$-entry of E is $\alpha \cdot (b^{-1})_{1,1} = \alpha$.

To show(4) and (5), let $1 \le i \le k-1$, then $v_i u^{-1} u^t = v_i$, so $v_i X^{-1} Y^t = v_i g^{-1} g_1^t$. Also $v_i g \in \mathcal{V}_i$, so $v_i g(uu^t) = v_i g$ and $v_i XY^t = v_i g g_1^t$. We conclude that:

(i)
$$\text{For } 1 \le i \le k-1,\ v_i X^\epsilon Y^t = v_i g^\epsilon g_1^t.$$

Now the shape of $X^\epsilon Y^t$ follows from (3) and (i), since, by (i), the first $k-1$ rows of $R_{1,2}$ are zero. Also the shape of $(X^\epsilon Y^t)^{-1}$, follows from (3). For (5), we use (i). Note that a^ϵ is unipotent, lower triangular and a_1^t is upper triangular unipotent with $(a_1^t)_{i,j} = 0$, for $j > i+1$, and $(a_1^t)_{i,i+1} \neq 0$. This easily implies (5), for $S = X^\epsilon Y^t$. For $S = Y^t$, $v_i Y^t = v_i + \beta_{k-i} v_{i+1}$, for all $1 \le i \le k-1$, thus (5) holds for Y^t as well.

For (6), note that for $h \in \{b_1^t, b_1^t b^\epsilon\}, h_{i,j} = 0$, for $j > i+1$, and $h_{i,i+1} \neq 0$, for all $1 \le i \le k-1$. This clearly holds for b_1^t and since this holds for b_1^t and b^ϵ is unipotent lower triangular, it also hold for $b_1^t b^\epsilon$. Thus, by (4), (6) holds for $S \in \{Y^t, X^\epsilon Y^t\}$ and $k+1 \le i \le n-1$. We compute that $v_k(Y^t)^{-1} = v_k(g_1^t)^{-1}(u^t)^{-1} = v_k(u^t)^{-1} = v_k - \alpha v_{k+1}$. Also $v_k(X^\epsilon Y^t)^{-1} = v_k(Y^t)^{-1}X^{-\epsilon} = (v_k - \alpha v_{k+1})X^{-\epsilon} = v_k X^{-\epsilon} - \alpha v_{k+1} X^{-\epsilon}$. Now $v_k X^{-\epsilon} \in \mathcal{V}_k$, and $v_{k+1}X^{-\epsilon} \equiv v_{k+1} \pmod{\mathcal{V}_k}$, so (6) follows. (7) follows from (5) and (6), since by (5), $\mathcal{V}_k \subseteq \langle \mathcal{O}(v_1, S)\rangle$, and then by (6), $\langle \mathcal{O}(v_1, S)\rangle = V$.

Finally, to show (8), note that $v_k X^\epsilon = v + v_k$, with $v \in \mathcal{V}_{k-1}$, and by (5), $vY^t \in \mathcal{V}_k$. Thus for $S \in \{Y^t, X^\epsilon Y^t\}$, $S_{k,n} = (Y^t)_{k,n}$. Now $v_k Y^t = v_k u^t g_1^t = (v_k + \alpha v_{k+1})g_1^t = v_k + \alpha v_{k+1} g_1^t$. Now it is easy to check that $(b_1^{-1})_{k,1} = \prod_{i=1}^k \gamma_i \neq 0$, thus $(g_1^t)_{k+1,n} = (b_1^{-1})_{k,1} \neq 0$, hence $(Y^t)_{k,n} = (g_1^t)_{k+1,n} \neq 0$ and (8) is proved.

4.3. *Let $\epsilon \in \{1, -1\}$ and let $S \in \{Y^t, X^\epsilon Y^t\}$. Let $R \in \Delta^{\le 2}(X) \cap \Delta^{\le 1}(S)$. Then v_1 is a characteristic vector of R.*

Proof. Let $h \in \Delta^{\le 1}(X) \cap \Delta^{\le 1}(R)$. Then, $[h, X] = 1$, so by 4.2.3 and 1.13, there exists $0 \neq \beta \in \mathbb{K}$, and $1 \le r \le n-1$, such that $h - \beta I_n \in \mathcal{T}_n(r)$. We use 1.15. We take in 1.15, $T = h - \beta I_n$. Note that R commutes with h and hence with T.

Suppose first that $r \le k-1$, we take in 1.15 $j = r = m$ and $\ell = 0$. Notice that by 4.2.5, hypothesis (a) of 1.15 is satisfied, hypothesis (b) and (c) of 1.15 are satisfied by definition, and we observed that hypothesis (e) of 1.15 is satisfied. Finally, since R centralizes T, $\mathcal{V}_r$ is R-invariant. Hence 1.15 completes the proof in this case.

Suppose next that $r \ge k$, we take in 1.15, $j = k-1$, $\ell = 1$ and $m = \dim(\mathrm{im}(T))$. Notice that $\mathrm{im}\,(T) = \mathcal{V}_m$ and $\mathrm{im}\,(T)$ is R-invariant. Also, by 4.2.8, $S_{k,n} \neq 0$, so clearly $v_k \notin \ker(ST)$ and hypothesis (c) of 1.15 holds. Thus 1.15 completes the proof in this case too.

From this point to the end of Section 4 we specialize and set:

$$\text{If } |\mathbb{K}| = 2, \text{ or } |\mathbb{K}| > 3, \text{ or } k \not\equiv 1 \pmod 3,$$
$$\beta_i = \gamma_i = 1, \text{ for all } 1 \le i \le k-1, \text{ in particular, } X = Y.$$
$$\text{If } |\mathbb{K}| = 3 \text{ and } k \equiv 1 \pmod 3,$$
$$\beta_i = \gamma_i = 1, \text{ for all } 2 \le i \le k-1 \text{ and } \beta_1 = -\gamma_1 = \beta.$$

4.4. (1) *If $|\mathbb{K}| > 3$, or $k \not\equiv 1 \pmod 3$, we can find $\alpha \in \mathbb{K}^*$ such that $\alpha(F_S, 1) \neq 0$ for all $S \in \{XY^t, X^{-1}Y^t\}$.*

(2) *If $|\mathbb{K}| = 3$, or $k \equiv 1 \pmod 3$, then for $\alpha = 1$ we have $\alpha(F_S, 1) \neq 0$, for all $S \in \{XY^t, X^{-1}Y^t\}$.*

(3) *If* $|\mathbb{K}| = 2$, *then for* $\alpha = 1$, $\gcd\Big\{\{i : \alpha(F_S, n-i) \neq 0\} \cup \{n\}\Big\}$ *is relatively prime to* 3, *for all* $S \in \{XY^t, X^{-1}Y^t\}$.

Proof. For (1), note that by our choice of X and Y, $X = Y$. Further, F_{XX^t} is the polynomial H_n of 2.13. Thus, $\alpha(F_{XX^t}, 1) = -\binom{k+1}{2} - (\alpha^2+2)k + 1$ by 2.13.2. Also, by 2.15, $\alpha(F_{X^{-1}X^t}, 1) = \alpha^2 - 2$. The reader may now easily verify (using also 2.13.3) that we can choose $\alpha \in \mathbb{K}^*$ as asserted in (1).

So suppose $|\mathbb{K}| = 3$ and $k \equiv 1 \pmod 3$. Then by 2.14.3, and 2.16, (2) holds. Finally assume $|\mathbb{K}| = 2$. Then (3) holds by 2.13.4-2.13.7 and by 2.15.

We now specialize further and choose α as in 4.4, in the respective cases.

4.5. *Set* $\Lambda = \Delta(L)$ *and let* $\epsilon \in \{1, -1\}$ *and let* $S \in \{Y^t, X^\epsilon Y^t\}$. *Then:*
(1) $d_\Lambda(X, S) > 3$.
(2) $B_\Lambda(X, Y^t)$ *and* $B_\Lambda(Y, X^t)$.
(3) $\Delta(L)$ *is balanced.*

Proof. Suppose $d_\Lambda(X, S) \leq 3$ and let $R \in \Lambda^{\leq 2}(X) \cap \Lambda^{\leq 1}(S)$. Of course $R \in \Delta^{\leq 2}(X) \cap \Delta^{\leq 1}(S)$, so by 4.3,

(i) v_1 is a characteristic vector of R.

If $S = Y^t$, then $[R, S] = 1$, so by (i), 4.2.7 and 1.14.1, $R \in Z(L)$, a contradiction. So (1) holds in case $S = Y^t$. So assume $S = X^\epsilon Y^t$.

Suppose first that $|\mathbb{K}| > 3$, or $|\mathbb{K}| = 3$ and $k \not\equiv 1 \pmod 3$, then using 4.4.1, (i), 4.2.7 and 1.14.5, we see that $R \in Z(L)$, a contradiction. This shows (1) in this case. By (1), $B_\Lambda(X, Y^t)$ holds here, and since here $X = Y$, 1.9.2 implies (2) in this case.

Suppose $|\mathbb{K}| = 3$ and $k \equiv 1 \pmod 3$. Then using 4.4.2, (i), 4.2.7 and 1.14.5, we see that $R \in Z(L)$, a contradiction. Hence (1) holds here and by (1) and definition, $B_\Lambda(X, Y^t)$ holds in this case. By Symmetry $d(Y, X^t) > 3$ and $d(Y, Y^\epsilon X^t) > 3$. Thus $B_\Lambda(Y, X^t)$ also holds and (2) holds in this case as well.

Finally, suppose $|\mathbb{K}| = 2$. If $L \simeq Sp_n(q)$, then $Z(L) = 1$, so $[R, S] = 1$, and hence, by (i), 4.2.7 and 1.14.1, $R = 1$, a contradiction. So assume $L \simeq SU_n(q)$. Then $|\mathbb{F}^*| = 3$. Now 4.4.3, (i), 4.2.7 and 1.14.5 show that $R \in Z(L)$, a contradiction. Again we see that (1) holds, and since $X = Y$ here, (2) holds here (as above). Note that (2) implies (3) by 1.9 and by definition.

5. The Unitary and Orthogonal Groups in odd dimension.

In this section $\mathbb{F}$ is a field of order q^2 and $\mathbb{K} \leq \mathbb{F}$ is the subfield of order q. We let $n = 2k+1 \geq 3$ be an odd integer and $U \simeq SU(n, \mathbb{F}) \leq SL(n, \mathbb{F})$ is the special unitary group. We view U as the fixed points of the automorphism

$\tau\sigma_q : SL(n,\mathbb{F}) \to SL(n,\mathbb{F})$, described in 1.12.3. We denote by $U \geq O \simeq SO(n,\mathbb{K})$, the subgroup $O = U \cap SL(n,\mathbb{K})$. L denotes one of the groups U or O. When $L = O$, we assume that $n \geq 7$ and that q is odd (this is because if q is even or $n < 7$, O' is either not simple, or isomorphic to simple groups that we handled earlier). We continue the notation of Section 1. In particular, V is a vector space of dimension n over $\mathbb{F}$.

Throughout this section $\Lambda = \Delta(L)$. The purpose of this section is to prove that when $L'/Z(L')$ is simple, $\Delta(L')$ is balanced (and hence, by 1.7, $\Delta(L'/Z(L'))$ is balanced). For that we'll indicate elements $X, Y \in L'$ such that $B_\Lambda(X, Y^t)$ and $B_\Lambda(Y, X^t)$ (see 1.10).

Notation 5.1. (1) given an element $r = \operatorname{diag}(I_{k-1}, s, I_{k-1}) \in GL(n,\mathbb{F})$, we denote $s(r) := s$ (note that $s \in GL_3(\mathbb{F})$).

(2) Let $\theta \in \mathbb{F}^*$. We denote by $u_0(\theta) = \operatorname{diag}(I_{k-1}, s, I_{k-1})$, with

$$s = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \theta & 0 & 1 \end{bmatrix}.$$

(3) Whenever we write $u_i(\alpha)$, we mean $u_i^n(\alpha)$ (see 1.1.7).

5.2. *Let $\alpha \in \mathbb{F}^*$ and $\beta_1, \dots, \beta_{k-1} \in \mathbb{K}^*$. Set $a = a_k(\beta_1, \dots, \beta_{k-1})$, $b = b_k(\beta_1, \dots, \beta_{k-1})$, $B = b_{k+1}(\alpha, \beta_1, \dots, \beta_{k-1})$ and $g = \operatorname{diag}(a, 1, b^{-1})$. Let $u = u_k(\alpha)u_{k+1}(\alpha^q)u_0(\theta)$. Then:*

(1) $g \in O$.
(2) $gu_{k+1}^n(\alpha) = \operatorname{diag}(a, B^{-1})$.
(3) $[g, u^t] = 1$.

Proof. (1) is 1.11. For (2), note that $g = \operatorname{diag}(a, z)$, with

$$z = u_k^{k+1}(\beta_{k-1})u_{k-1}^{k+1}(\beta_{k-2}) \cdots u_2^{k+1}(\beta_1).$$

Also $u_{k+1}(\alpha) = \operatorname{diag}(I_k, u_1^{k+1}(\alpha))$. Thus $gu_{k+1}(\alpha) = \operatorname{diag}(a, h)$, with $h = zu_1^{k+1}(\alpha) = u_k^{k+1}(\beta_{k-1})u_{k-1}^{k+1}(\beta_{k-2}) \cdots u_2^{k+1}(\beta_1)u_1^{k+1}(\alpha) = B^{-1}$.

(3) follows from the fact that $(u_k(\alpha))^t, (u_{k+1}(\alpha^q))^t$, and $(u_0(\theta))^t$ commute with g.

5.3. *Let $\alpha, \beta, \theta \in \mathbb{F}$ and set $u = u_k(\alpha)u_{k+1}(\beta)u_0(\theta)$. Then:*

(1) $s(u_k(\alpha)u_{k+1}(\beta)) = \begin{bmatrix} 1 & 0 & 0 \\ \alpha & 1 & 0 \\ 0 & \beta & 1 \end{bmatrix}$.

(2) $s(u_{k+1}(\beta)u_k(\alpha)) = \begin{bmatrix} 1 & 0 & 0 \\ \alpha & 1 & 0 \\ \alpha\beta & \beta & 1 \end{bmatrix}$.

(3)

$$\begin{aligned} u_0(\theta) &= u_k(1)u_{k+1}(-\theta)u_k(-1)u_{k+1}(\theta) \\ &= u_{k+1}(1)u_k(\theta)u_{k+1}(-1)u_k(-\theta). \end{aligned}$$

(4) $u_0(\theta)\tau = u_0(-\theta)$.
(5) $u \in \mathrm{Fix}\,(\tau\sigma_q)$ *iff* $\beta = \alpha^q$ *and* $\theta + \theta^q = \alpha^{q+1}$.

Proof. (1) and (2) are easy to check. For (3) we have

$$\begin{aligned} & s\Big\{u_k(1)u_{k+1}(-\theta)u_k(-1)u_{k+1}(\theta)\Big\} \\ &= \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & \bar{\theta} & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ \bar{1} & 1 & 0 \\ 0 & \theta & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \theta & 0 & 1 \end{bmatrix} = s(u_0(\theta)) \end{aligned}$$

and

$$\begin{aligned} & s\Big\{u_{k+1}(1)u_k(\theta)u_{k+1}(-1)u_k(-\theta)\Big\} \\ &= \begin{bmatrix} 1 & 0 & 0 \\ \theta & 1 & 0 \\ \theta & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ \bar{\theta} & 1 & 0 \\ \theta & \bar{1} & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \theta & 0 & 1 \end{bmatrix} = s(u_0(\theta)). \end{aligned}$$

For (4), note that by (3), $u_0(\theta)\tau = \{u_k(1)u_{k+1}(-\theta)u_k(-1)u_{k+1}(\theta)\}\tau = u_{k+1}(1)u_k(-\theta)u_{k+1}(-1)u_k(\theta) = u_0(-\theta)$.

For (5), we have

$$s(u) = \begin{bmatrix} 1 & 0 & 0 \\ \alpha & 1 & 0 \\ \theta & \beta & 1 \end{bmatrix}.$$

Now, by (4), $u\tau\sigma_q = u_{k+1}(\alpha^q)u_k(\beta^q)u_0(-\theta^q)$, so

$$s(u\tau\sigma_q) = \begin{bmatrix} 1 & 0 & 0 \\ \beta^q & 1 & 0 \\ (\alpha\beta - \theta)^q & \alpha^q & 1 \end{bmatrix}.$$

So the lemma follows.

Notation 5.4. Let $\alpha, \theta \in \mathbb{F}$ such that $\theta + \theta^q = \alpha^{q+1}$.

(1) We denote
$$\begin{aligned}u^n(\alpha,\theta)=u(\alpha,\theta)&=u_k(\alpha)u_{k+1}(\alpha^q)u_0(\theta)\\&=u_{k+1}(\alpha^q)u_k(\alpha)u_0(-\theta^q).\end{aligned}$$
(2) We denote $X(\alpha,\theta)=\mathrm{diag}\,(a_k,1,b_k^{-1})u(\alpha,\theta)$.

Note that we denote $u(\alpha,\theta)$ and $X(\alpha,\theta)$ only when $\theta+\theta^q=\alpha^{q+1}$, so that $u(\alpha,\theta),\ X(\alpha,\theta)\in U$.

5.5. *Let $\alpha,\beta\in\mathbb{F}^*$ and let $u=u_1^{k+1}(-\alpha)$, $w=u_1^{k+1}(-\beta)$ and $\epsilon\in\{1,-1\}$. Then:*

(1) $(w^tu^\epsilon)^{-1}=\mathrm{diag}\left(\begin{bmatrix}1&\beta\\ \epsilon\alpha&\epsilon\alpha\beta+1\end{bmatrix},I_{k-1}\right)$.

(2) $w^tu^\epsilon=\mathrm{diag}\left(\begin{bmatrix}1+\epsilon\alpha\beta&\overline{\beta}\\ -\epsilon\alpha&1\end{bmatrix},I_{k-1}\right)$.

Proof. This is obvious.

5.6. *Suppose* $\mathrm{char}\,(\mathbb{F})=3$*. Then:*

(1) *For $B=b_{k+1}$, $F_{B^tB}=F_{k+1}$ and $F_{B^tB^{-1}}=Q_{k+1}$, in particular $F_{B^tB}[-1]\neq 0$ and $F_{B^tB^{-1}}[-1]=Q_{k+1}[-1]=(-1)^{k+1}(k+2)$.*

(2) *Suppose $k\geq 4$ and let $B=b_{k+1}(1,1,1,\beta_4,1,\dots,1)$ and $C=b_{k+1}(1,1,1,\gamma_4,1,\dots,1)$, with $\beta_4\gamma_4=-1$. Then for $\{T,Z\}=\{B,C\}$, and $\epsilon\in\{1,-1\}$, $F_{T^tZ^\epsilon}[-1]\neq 0$.*

Proof. By definition 1.2.4 and by 2.6, if $B=b_{k+1}$, then $F_{B^tB}=F_{k+1}$ and by 2.5, $F_{B^tB^{-1}}=Q_{k+1}$. Next note that $F_1[\lambda]=\lambda-1$, $F_2[\lambda]=\lambda^2-3\lambda+1$ and for $m\geq 3$, $F_m[\lambda]=(\lambda-2)F_{m-1}[\lambda]-F_{m-2}[\lambda]$ (see 2.6). Since $\mathrm{char}\,(\mathbb{F})=3$, $F_m[-1]=-F_{m-2}[-1]$. Hence

(i) $$F_m[-1]\neq 0\quad\text{for all } m\geq 1.$$

Further, for $m\geq 1$, $Q_m[-1]=(-1)^m\{1-(-1)+(-1)^2-(-1)^3+\cdots\}=(-1)^m(m+1)$. Hence

(ii) $$Q_m[-1]=(-1)^m(m+1),\quad\text{for all } m\geq 1.$$

Now (i) and (ii) imply (1).

For (2), let $\beta_1,\beta_2,\dots,\beta_k,\gamma_1,\gamma_2,\dots,\gamma_k\in\mathbb{F}^*$. Let $B=b_{k+1}(\beta_1,\beta_2,\dots,\beta_k)$, $b=b_k(\beta_2,\beta_3,\dots,\beta_k)$, $C=b_{k+1}(\gamma_1,\gamma_2,\dots,\gamma_k)$, $c=b_k(\gamma_2,\gamma_3,\dots,\gamma_k)$ and for $1\leq i\leq 4$, $b_i=b_{k-1}(\beta_{i+2},\dots,\beta_k)$ and $c_i=b_{k-i}(\gamma_{i+2},\dots,\gamma_k)$. We claim that

(iii) $$F_{(C^tB)^{-1}}[-1]=(1-\beta_1\gamma_1)F_{(c^tb)^{-1}}[-1]-\beta_1\gamma_1F_{(c_1^tb_1)^{-1}}[-1].$$

(iv) $$F_{C^tB^{-1}}[-1]=F_{c^tb^{-1}}[-1]-\beta_1\gamma_1F_{c_1^tb_1^{-1}}[-1].$$

(v) $$\text{If } \beta_1\gamma_1=1, \text{ then } F_{(C^tB)^{-1}}[-1]=-F_{(c_1^tb_1)^{-1}}[-1].$$

(vi) $$\text{If } \beta_1\gamma_1=1, \text{ then } F_{C^tB^{-1}}[-1]=-\beta_2\gamma_2F_{c_2^tb_2^{-1}}[-1].$$

Indeed, (iii) follows from 2.12.2, and (iv) follows from 2.12.3. (v) follows from (iii). For (vi), note that by (iv), $F_{c^t b^{-1}}[-1] = F_{c_1^t b_1^{-1}}[-1] - \beta_2\gamma_2 F_{c_2^t b_2^{-1}}[-1]$. Thus, by (iv) again,

$$\begin{aligned} F_{C^t B^{-1}}[-1] &= F_{c^t b^{-1}}[-1] - F_{c_1^t b_1^{-1}}[-1] \\ &= F_{c_1^t b_1^{-1}}[-1] - \beta_2\gamma_2 F_{c_2^t b_2^{-1}}[-1] - F_{c_1^t b_1^{-1}}[-1] \\ &= -\beta_2\gamma_2 F_{c_2^t b_2^{-1}}[-1]. \end{aligned}$$

Let now B and C be as in (2). Then $\beta_1\gamma_1 = \beta_3\gamma_3 = 1$, so applying (v) twice, we see that $F_{(C^t B)^{-1}}[-1] = -F_{(c_1^t b_1)^{-1}}[-1] = F_{(c_3^t b_3)^{-1}}[-1] = \overline{F}_{k-3}[-1]$, where the last equality follows from the fact that $c_3 = b_3 = b_{k-3}$. Note now that (by 2.7.1), $\overline{F}_{k-3}[-1] = F_{k-3}[-1]$, so by (i), $\overline{F}_{k-3}[-1] \neq 0$, and hence $F_{(C^t B)^{-1}}[-1] \neq 0$. Next, by (vi), $F_{C^t B^{-1}}[-1] = -F_{c_2^t b_2^{-1}}[-1] = -\{F_{c_3^t b_3^{-1}}[-1] - \beta_4\gamma_4 F_{c_4^t b_4^{-1}}[-1]\} = -\{Q_{k-3}[-1] + Q_{k-4}[-1]\} = -\{(-1)^{k-3}(k-2) + (-1)^{k-4}(k-3)\} \in \{1, -1\}$. (Note that this also works when $k = 4$ and 5, where $-F_{c_2^t b_2^{-1}}[-1]$ can be easily computed.) This completes the proof of (2).

5.7. (1) *There are at least $q - 2 - [\frac{q-2}{2}]$ elements $\delta \in \mathbb{K}$ such that the polynomial $x^2 - \delta x + \delta$ is irreducible over $\mathbb{K}$.*

(2) *If $\delta \in \mathbb{K}$ is as in (1) and $\alpha \in \mathbb{F}$ is a root of the polynomial $x^2 - \delta x + \delta$, then $\delta = \alpha^{q+1} = \alpha + \alpha^q$.*

Proof. Consider the set of polynomials $P := \{x^2 - \delta x + \delta : \delta \in \mathbb{K}\}$. There are q polynomials in P. For $\delta \in \mathbb{K}$, denote $p_\delta = x^2 - \delta x + \delta$. For $p \in P$, let $r(p)$ be the set of roots of p. Note that for $0, 4 \neq \delta \in \mathbb{K}$, $|r(p_\delta)| = 2$ and if $\gamma, \delta \in \mathbb{K}$ are distinct, then $r(p_\gamma) \cap r(p_\delta) = \emptyset$. Hence if t is the number of polynomials $p_\delta \in P$ such $\delta \neq 0, 4$ and p_δ has a root in $\mathbb{K}$, then $2t + 2 \leq q$, so $t \leq [\frac{q-2}{2}]$. Thus $|\{\delta \in \mathbb{K} : p_\delta \text{ has a root in } \mathbb{K}\}| \leq [\frac{q-2}{2}] + 2$, and (1) follows.

Let $\delta \in \mathbb{K}$ as in (1). Let α be a root of p_δ in $\mathbb{F}$. Then the other root of p_δ is α^q so $p_\delta = (x - \alpha)(x - \alpha^q)$ and hence $\delta = \alpha^{q+1} = \alpha^q + \alpha$.

Notation 5.8. (1) We denote $\Xi = \{\alpha \in \mathbb{F} - \mathbb{K} : \alpha + \alpha^q = \alpha^{q+1}\}$.

(2) We denote by $\mathcal{D} = \{\delta \in \mathbb{K} : p_\delta[\lambda] = \lambda^2 - \delta\lambda + \delta \text{ is irreducible over } \mathbb{K}\}$.

5.9. *Set $u = u(\alpha, \theta)$ and $w = u(\beta, \rho)$. Then:*

$$s(u) = \begin{bmatrix} 1 & 0 & 0 \\ \alpha & 1 & 0 \\ \theta & \alpha^q & 1 \end{bmatrix} \qquad (s(u))^t = \begin{bmatrix} 1 & \alpha & \theta \\ 0 & 1 & \alpha^q \\ 0 & 0 & 1 \end{bmatrix}, \tag{1}$$

$$(s(u))^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ -\alpha & 1 & 0 \\ \theta^q & -\alpha^q & 1 \end{bmatrix} \qquad ((s(u))^{-1}) = \begin{bmatrix} 1 & -\alpha & \theta^q \\ 0 & 1 & -\alpha^q \\ 0 & 0 & 1 \end{bmatrix}, \tag{2}$$

$$s(uw^t) = \begin{bmatrix} 1 & \beta & \rho \\ \alpha & \alpha\beta + 1 & \alpha\rho + \beta^q \\ \theta & \beta\theta + \alpha^q & \theta\rho + \alpha^q\beta^q + 1 \end{bmatrix}, \tag{3}$$

$$s((uw^t)^{-1}) = \begin{bmatrix} 1 + \alpha\beta + \theta^q\rho^q & \bar{\beta} - \alpha^q\rho^q & \rho^q \\ -\alpha - \beta^q\theta^q & \alpha^q\beta^q + 1 & -\beta^q \\ \theta^q & -\alpha^q & 1 \end{bmatrix}, \tag{4}$$

$$s(u^{-1}w^t) = \begin{bmatrix} 1 & \beta & \rho \\ -\alpha & 1 - \alpha\beta & -\alpha\rho + \beta^q \\ \theta^q & \beta\theta^q - \alpha^q & \rho\theta^q - \alpha^q\beta^q + 1 \end{bmatrix}, \tag{5}$$

$$s((u^{-1}w^t)^{-1}) = \begin{bmatrix} 1 - \alpha\beta + \theta\rho^q & -\beta + \alpha^q\rho^q & \rho^q \\ \alpha - \theta\beta^q & 1 - \alpha^q\beta^q & -\beta^q \\ \theta & \alpha^q & 1 \end{bmatrix}. \tag{6}$$

Proof. (1) is obvious. For (2), observe that $u^{-1} = u_0(-\theta)u_{k+1}(-\alpha^q)u_k(-\alpha)$, so

$$\begin{aligned} s(u^{-1}) &= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -\theta & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ -\alpha & 1 & 0 \\ \alpha^{q+1} & -\alpha^q & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 & 0 \\ -\alpha & 1 & 0 \\ \theta^q & -\alpha^q & 1 \end{bmatrix}. \end{aligned}$$

For (3) and (4), we compute:

$$\begin{aligned} s(uw^t) &= \begin{bmatrix} 1 & 0 & 0 \\ \alpha & 1 & 0 \\ \theta & \alpha^q & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & \beta & \rho \\ 0 & 1 & \beta^q \\ 0 & 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & \beta & \rho \\ \alpha & \alpha\beta + 1 & \alpha\rho + \beta^q \\ \theta & \beta\theta + \alpha^q & \theta\rho + \alpha^q\beta^q + 1 \end{bmatrix}. \\ s((uw^t)^{-1} &= \begin{bmatrix} 1 & -\beta & \rho^q \\ 0 & 1 & -\beta^q \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ -\alpha & 1 & 0 \\ \theta^q & -\alpha^q & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 + \alpha\beta + \theta^q\rho^q & \bar{\beta} - \alpha^q\rho^q & \rho^q \\ -\alpha - \beta^q\theta^q & \alpha^q\beta^q + 1 & -\beta^q \\ \theta^q & -\alpha^q & 1 \end{bmatrix}. \end{aligned}$$

For (5) and (6) we compute:

$$s(u^{-1}w^t) = \begin{bmatrix} 1 & 0 & 0 \\ -\alpha & 1 & 0 \\ \theta^q & -\alpha^q & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & \beta & \rho \\ 0 & 1 & \beta^q \\ 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & \beta & \rho \\ -\alpha & 1-\alpha\beta & -\alpha\rho+\beta^q \\ \theta^q & \beta\theta^q-\alpha^q & \rho\theta^q-\alpha^q\beta^q+1 \end{bmatrix}$$

$$s((u^{-1}w^t)^{-1}) = \begin{bmatrix} 1 & -\beta & \rho^q \\ 0 & 1 & -\beta^q \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ \alpha & 1 & 0 \\ \theta & \alpha^q & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1-\alpha\beta+\theta\rho^q & -\beta+\alpha^q\rho^q & \rho^q \\ \alpha-\theta\beta^q & 1-\alpha^q\beta^q & -\beta^q \\ \theta & \alpha^q & 1 \end{bmatrix}.$$

5.10. *Let $X = X(\alpha,\theta)$ and $Y = X(\beta,\rho)$. Then:*

(1) $\alpha\,(F_{XY^t}, 1) = \binom{k+1}{2} + (\alpha\beta + \theta^q\rho^q + 2)k + \alpha^q\beta^q$.

(2) $\alpha\,(F_{X^{-1}Y^t}, 1) = 3 - \alpha\beta - \alpha^q\beta^q + \theta\rho^q$.

(3) *If* $\alpha\,(F_{XY^t}, 1) = 0$, *then* $(\alpha^q\beta^q - \alpha\beta)(k-1) = (\theta^q\rho^q - \theta\rho)k$.

(4) *If* $\alpha\,(F_{XX^t}, 1) = 0$, *then* $(\alpha^{2q} - \alpha^2)(k-1) = (\theta^{2q} - \theta^2)k$. *Further, if* $\alpha \in \Xi$, *then* $(\alpha^q - \alpha)(k-1) = (\theta^q - \theta)k$.

Suppose further that $\alpha \in \Xi$, *and set* $\delta = \alpha + \alpha^q = \alpha^{q+1}$. *Then:*

(5) *If* $\alpha(F_{X^{-1}X^t}, 1) = 0$, *then* $\delta^2 - 2\delta = 3 + \theta^{q+1}$.

(6) *If* $\theta = \alpha$, *then* $\alpha(F_{XX^t}, 1) \neq 0$, *while if* $\theta = \alpha^q$, *then either* $\alpha(F_{XX^t}, 1) \neq 0$, *or* $2k - 1 \equiv 0 \pmod{\mathrm{char}(\mathbb{K})}$ *and* $8\delta^2 - 16\delta + 11 = 0$.

(7) *If* $\theta = \alpha$ *or* α^2, *then either* $\alpha(F_{X^{-1}X^t}, 1) \neq 0$, *or* $\delta^2 - 3\delta - 3 = 0$.

(8) *Suppose* $\mathrm{char}\,(\mathbb{K}) \neq 2$. *Suppose further that* $\beta = \alpha^q$, $\rho = \theta$ *and* $\theta \neq \mathbb{K}$, *then for* $\{T, Z\} = \{X, Y\}$, $\alpha(F_{TZ^t}, 1) \neq 0$.

(9) *If* $\beta = \alpha^q$, $\rho = \theta$ *and* $2\delta \neq 3 + \theta^{q+1}$, *then for* $\{T, Z\} = \{X, Y\}$, $\alpha(F_{T^{-1}Z^t}, 1) \neq 0$.

(10) *We can choose* $\alpha \in \Xi$ *and* $\theta \in \mathbb{F} - \mathbb{K}$, *with* $\theta + \theta^q = \alpha^{q+1} = \delta$, *such that if we set* $X = X(\alpha,\theta)$ *and* $Y = X(\alpha^q,\theta)$, *then either*

(10i) $q = 2, \theta = \alpha$, *and for* $\epsilon \in \{1,-1\}$, *and* $Z \in \{X, Y\}, \alpha(F_{Z^\epsilon Z^t}, 1) \neq 0$. *Or*

(10ii) $q = 4, \theta = \alpha + 1$ *and there exists* $\beta \in \mathbb{F} - \{\alpha, \alpha^q\}$, *with* $\beta^{q+1} = \delta$, *such that if we set* $W = X(\beta,\theta)$, *then for* $\epsilon \in \{1,-1\}$, *and* $Z \in \{X, Y, W\}, \alpha(F_{Z^\epsilon Z^t}, 1) \neq 0$. *Or*

(10iii) $q \neq 2, 4$ *and* $\alpha(F_{T^\epsilon Z^t}, 1) \neq 0$, *for* $T, Z \in \{X, Y\}$ *and* $\epsilon \in \{1,-1\}$.

Proof. Set $u = u(\alpha,\theta)$ and $w = u(\beta,\rho)$. For (1), let $x_k = a_k^t a_k$, $y_k = b_k b_k^t$, and $g = \mathrm{diag}\,(x_k, 1, y_k^{-1})$. Note that $F_{XY^t} = F_{Y^tX}$. Further $Y^tX = w^t\mathrm{diag}\,(a_k^t, 1, (b_k^{-1})^t)\mathrm{diag}\,(a_k, 1, b_k^{-1})u$. Thus, clearly, $F_{XY^t} = F_{hg}$, where

$h = uw^t$. By 5.9.4, $h^{-1} = \operatorname{diag}(I_{k-1}, s, I_{k-1})$, with

$$s = s((uw^t)^{-1}) = \begin{bmatrix} 1+\alpha\beta+\theta^q\rho^q & \bar{\beta}-\alpha^q\rho^q & \rho^q \\ -\alpha-\beta^q\theta^q & \alpha^q\beta^q+1 & -\beta^q \\ \theta^q & -\alpha^q & 1 \end{bmatrix}.$$

Thus, by 2.10 (with $A = x_k$ and $B = y_k^{-1}$), $\alpha(F_{hg}, 1) = \alpha(R[\lambda], 1)$, where

(i) $$R[\lambda] = (\beta_{22}\lambda - 1)F_A F_B - (\beta_{33} - 1)\lambda F_A F_{M_{1,1}(B)} \\ -(\beta_{11} - 1)\lambda F_{M_{k,k}(A)} F_B,$$

and the β_{ij} are given by matrix s above. Using 2.6, we see that

$$F_A = F_k, \quad F_{M_{k,k}(A)} = G_{k-1} \quad \text{and} \quad F_B = \overline{F}_k.$$

Hence (i) implies

$$R[\lambda] = \{(\alpha^q\beta^q + 1)\lambda - 1\}F_k\overline{F}_k - (\alpha\beta + \theta^q\rho^q)\lambda G_{k-1} \cdot \overline{F}_k.$$

Now 2.6 gives

$$F_k \equiv (-1)^k \left\{1 - \binom{k+1}{2}\lambda\right\} \pmod{(\lambda^2)}$$
$$G_{k-1} \equiv (-1)^{k-1} \left\{k - \binom{k+1}{3}\lambda\right\} \pmod{(\lambda^2)}$$
$$\overline{F}_k \equiv (-1)^k\{1 - (2k-1)\lambda\} \pmod{(\lambda^2)}$$

Hence modulo the ideal (λ^2),

$$R[\lambda] \equiv \{(\alpha^q\beta^q + 1)\lambda - 1\} \cdot \left\{1 - \binom{k+1}{2}\lambda\right\} \cdot \{1 - (2k-1)\lambda\} \\ + (\alpha\beta + \theta^q\rho^q)\lambda k \\ \equiv -1 + \left\{\binom{k+1}{2} + (\alpha\beta + \theta^q\rho^q + 2)k + \alpha^q\beta^q\right\}\lambda.$$

This shows (1).

For (2), let $x_k = a_k^{-1}a_k^t$, $y_k = b_k(b_k^{-1})^t$ and $g = \operatorname{diag}(x_k, 1, y_k)$. Using 5.2.3, we see that $X^{-1}Y^t = u^{-1}\operatorname{diag}(a_k^{-1}, 1, b_k)w^t\operatorname{diag}(a_k^t, 1, (b_k^{-1})^t) = u^{-1}w^t\operatorname{diag}(a_k^{-1}, 1, b_k)\operatorname{diag}(a_k^t, 1, (b_k^{-1})^t) = hg$, where $h = u^{-1}w^t$. Thus, $F_{X^{-1}Y^t} = F_{hg}$. By 5.9.6, $h^{-1} = \operatorname{diag}(I_{k-1}, s, I_{k-1})$, with

$$s = s((u^{-1}w^t)^{-1}) = \begin{bmatrix} 1-\alpha\beta+\theta\rho^q & -\beta+\alpha^q\rho^q & \rho^q \\ \alpha-\theta\beta^q & 1-\alpha^q\beta^q & -\beta^q \\ \theta & \alpha^q & 1 \end{bmatrix}.$$

Using 2.10 again (with $A = x_k$ and $B = y_k$), $\alpha(F_{hg}, 1) = \alpha(R[\lambda], 1)$, with $R[\lambda]$ as in (i) and the β_{ij} are given by the matrix s above. Using 2.5 and 2.11, we see that

$$F_A = Q_k, \quad F_{M_{k,k}(A)} = Q_{k-1}, \quad F_B = Q_k.$$

Hence

$$R[\lambda] = \{(1-\alpha^q\beta^q)\lambda - 1\}Q_k^2 - (-\alpha\beta + \theta\rho^q)\lambda Q_{k-1}\cdot Q_k.$$

Now

$$\begin{aligned} Q_k &\equiv (-1)^k(1-\lambda) \pmod{(\lambda^2)} \\ Q_{k-1} &\equiv (-1)^{k-1} \pmod{(\lambda)}. \end{aligned}$$

Hence modulo the ideal (λ^2),

$$\begin{aligned} R[\lambda] &\equiv \{(1-\alpha^q\beta^q)\lambda - 1\}(1-\lambda)^2 + (-\alpha\beta + \theta\rho^q)\lambda \\ &\equiv -1 + \{3 - \alpha\beta - \alpha^q\beta^q + \theta\rho^q\}\lambda. \end{aligned}$$

This shows (2).

Suppose $\alpha(F_{XY^t}, 1) = 0$. Applying σ_q, we get

$$\alpha(F_{XY^t}, 1) = 0 = \alpha(F_{XY^t}, 1)\sigma_q,$$

hence

$$(\alpha\beta + \theta^q\rho^q)k + \alpha^q\beta^q = (\alpha^q\beta^q + \theta\rho)k + \alpha\beta$$

so

$$(\alpha^q\beta^q - \alpha\beta)(k-1) = (\theta^q\rho^q - \theta\rho)k$$

and (3) is proved. For (4), take $Y = X$ in (3), to get $(\alpha^{2q}-\alpha^2)(k-1) = (\theta^{2q}-\theta^2)k$. Further, $(\alpha^{2q}-\alpha^2) = (\alpha^q+\alpha)(\alpha^q-\alpha)$, and $(\theta^{2q}-\theta^2) = (\theta^q+\theta)(\theta^q-\theta)$. So if $\alpha \in \Xi$, $(\alpha^q + \alpha) = \alpha^{q+1} = \theta^q + \theta$. This shows (4).

From now on assume $\alpha \in \Xi$ and set $\delta = \alpha^{q+1}$. For (5), take $X = Y$ in (2) and note that $\alpha^2 + \alpha^{2q} = (\alpha + \alpha^q)^2 - 2\alpha^{q+1} = \delta^2 - 2\delta$.

Suppose $\theta = \alpha$ and $\alpha(F_{XX^t}, 1) = 0$. Then, by (4), $(\alpha^q - \alpha)(k-1) = (\alpha^q - \alpha)k$. Hence $\alpha^q = \alpha$, which is false, since $\alpha \notin \mathbb{K}$. Suppose $\theta = \alpha^q$ and $\alpha(F_{XX^t}, 1) = 0$. Then, by (4), $(\alpha^q - \alpha)(k-1) = (\alpha - \alpha^q)k$ hence $(2k-1)(\alpha^q - \alpha) = 0$. As above, we get $2k - 1 = 0$ in $\mathbb{K}$, so $\binom{k+1}{2} = \frac{3}{8}$ in $\mathbb{K}$. Also, by (1), $0 = \alpha(F_{XX^t}, 1) = \binom{k+1}{2} + (\alpha^2 + \theta^{2q} + 2)k + \alpha^{2q} = \frac{3}{8} + (\alpha^2 + \alpha^2 + 2)\frac{1}{2} + \alpha^{2q} = \frac{11}{8} + \alpha^2 + \alpha^{2q}$. Since $\alpha^2 + \alpha^{2q} = \delta^2 - 2\delta$, we get that $\frac{11}{8} + \delta^2 - 2\delta = 0$. This shows (6).

For (7) suppose that $\theta = \alpha$ or α^q. Then, $\theta^{q+1} = \delta$, so, by (5), if $\alpha(F_{X^{-1}X^t}, 1) = 0$, then $\delta^2 - 2\delta = 3 + \delta$, and $\delta^2 - 3\delta - 3 = 0$, this shows (7).

Assume the hypothesis of (8). Note that $\alpha^q\beta^q - \alpha\beta = 0$. Thus, by (3), if $\alpha(F_{XY^t}, 1) = 0$, then $0 = (\theta^{2q} - \theta^2)k = \delta(\theta^q - \theta)k$. Thus since $\delta \neq 0$ and since we are assuming that $\theta \notin \mathbb{K}$, $k = 0$, in $\mathbb{K}$. Then, (1) implies that $\delta = 0$, a contradiction. By symmetry, (8) holds.

Assume the hypothesis of (9). Note again that $\alpha\beta = \delta$, so (9) follows immediately from (2).

For (10), assume $Y = X(\alpha^q, \theta)$. Suppose first that char $(\mathbb{K}) = 2$. Note that by (4):

(ii) If $\alpha,\, \theta \in \mathbb{F} - \mathbb{K}$ such that $\theta + \theta^q = \alpha^{q+1}$, then for $X = X(\alpha, \theta)$, $\alpha(F_{XX^t}, 1) \neq 0$.

This is because (4) implies that if k is odd and $\alpha(F_{XX^t}, 1) = 0$, then $\theta^q + \theta = 0$, while if k is even and $\alpha(F_{XX^t}, 1) = 0$, then $\alpha^q + \alpha = 0$.

For $q = 2$, take $\delta = 1$, for $q > 2$, pick $1 \neq \delta \in \mathcal{D}$ (note that this is possible by 5.7). Further, if $q > 4$, take δ such that $\delta^2 + \delta + 1 \neq 0$ (note that this is possible). Let $\alpha \in \Xi$, with $\alpha^{q+1} = \delta$. If $q = 2$, take $\theta = \alpha$, if $q = 4$, take $\theta = \alpha + 1$ and if $q > 4$, take $\theta = \alpha + \delta$. Note that $\theta \notin \mathbb{K}$. When $q = 4$, we take $W = X(\beta, \theta)$, with $\beta \in \mathbb{F} - (\mathbb{K} \cup \{\alpha, \alpha^q\})$, such that $\beta^{q+1} = \alpha^{q+1} = \delta$. Note that such a choice of β is possible. Now, by (ii), for all $q \geq 2$, $\alpha(F_{ZZ^t}, 1) \neq 0$, for $Z \in \{X, Y, W\}$.

Next, for $q = 4$, $\theta^{q+1} = (\alpha+1)^{q+1} = (\alpha^q+1)(\alpha+1) = \alpha^{q+1} + (\alpha^q+\alpha)+1 = 1$. Of course, when $q = 2$, $\theta^{q+1} = 1$. Also, by (2), for $Z \in \{X, Y, W\}$, if $Z = X(\gamma, \theta)$, then $\alpha(F_{Z^{-1}Z^t}, 1) = 3 + \gamma^2 + \gamma^{2q} + 1 = \gamma^2 + \gamma^{2q} = (\gamma + \gamma^q)^2$. Since $\gamma \notin \mathbb{K}$, for all possibilities of γ and for $q = 2, 4$, $\alpha(F_{Z^{-1}Z^t}, 1) \neq 0$. Thus (10i) and (10ii) are proved.

We now assume that char $(\mathbb{F}) = 2$ and $q > 4$. Now $\theta^{q+1} = (\alpha + \delta)^{q+1} = (\alpha^q+\delta)(\alpha+\delta) = \alpha^{q+1}+\delta(\alpha^q+\alpha)+\delta^2 = \delta+\delta^2+\delta^2 = \delta$. Hence, $3+\theta^{q+1} = \delta+1$. So if $\delta^2 - 2\delta = 3 + \theta^{q+1}$, then $\delta^2 = \delta + 1$, this contradicts the choice of δ (recall $\delta^2 + \delta + 1 \neq 0$). Hence, by (5), $\alpha(F_{Z^{-1}Z^t}, 1) \neq 0$, for $Z \in \{X, Y\}$.

Suppose $\alpha(F_{XY^t}, 1) = 0$. Then, by (3), (with $\beta = \alpha^q$), we get $0 = (\theta^q + \theta)^2 k = \delta^2 k$, so $k \equiv 0 \pmod 2$. Then by (1), $\binom{k+1}{2} + \delta = 0$. Thus $k \equiv 2 \pmod 4$ (since $\delta \neq 0$) and $\delta = 1$, contradicting the choice of δ. Thus $\alpha(F_{XY^t}, 1) \neq 0$; by symmetry, $\alpha(F_{YX^t}, 1) \neq 0$.

Next note that we showed that $\theta^{q+1} = \delta$. Thus $\theta^{q+1} + 3 = \delta + 1$. Since $\delta \neq 1$, $\delta + 1 \neq 0$, so by (9), $\alpha(F_{T^{-1}Z^t}, 1) = 0$, for $\{T, Z\} = \{X, Y\}$. Thus (10iii) holds in case char $(\mathbb{K}) = 2$.

So suppose char $(\mathbb{K}) \neq 2$. Suppose further that $q \neq 5$. We take $3 \neq \delta \in \mathcal{D}$, $\alpha \in \Xi$, with $\alpha^{q+1} = \delta$ and $\theta = \alpha$. Since $\theta \notin \mathbb{K}$, (8) implies that for $\{T, Z\} = \{X, Y\}$, $\alpha(F_{TZ^t}, 1) \neq 0$. Since $\delta \neq 3$, (and $\theta^{q+1} = \alpha^{q+1} = \delta$), (9) implies that for $\{T, Z\} = \{X, Y\}$, $\alpha(F_{T^{-1}Z^t}, 1) \neq 0$. Next we show that we can pick $\delta \in \mathcal{D}$, such that

(iii) $\delta \neq 3 \quad \text{and} \quad 8\delta^2 - 16\delta + 11 \neq 0 \neq \delta^2 - 3\delta - 3.$

By (6) and (7), this shows (10), for $q \neq 5$. If $q \geq 13$, then, by 5.7.1, $|\mathcal{D}| \geq 6$, so clearly, we can pick $\delta \neq 3$ such that (iii) holds. So suppose $q \leq 11$. Suppose char $(\mathbb{K}) = 3$. Then $\delta^2 - 3\delta - 3 \neq 0$, so if $q = 9$, then, by 5.7.1, we can pick δ ($\neq 3$) so that $8\delta^2 - 16\delta + 11 \neq 0$, while if $q = 3$, take $\delta = -1$, so (iii) holds in this case. For $q = 11$, take $\delta = 1$. For $q = 7$, take $\delta = 2$.

Finally, suppose $q = 5$. We take $\delta = 1$, $\alpha \in \Xi$, with $\alpha^{q+1} = \delta$ and we let θ be as follows. If $k \not\equiv 2 \pmod 5$, $\theta = \theta_1 = \alpha + 3(\alpha - \alpha^q) = 2\alpha^q - \alpha$, while if $k \equiv 2 \pmod 5$, $\theta = \theta_1^q$ (note that $\theta + \theta^q = \alpha + \alpha^q = \alpha^{q+1}$). Note that if $\theta \in \mathbb{K}$, then $\alpha \in \mathbb{K}$, which is false. Thus $\theta \notin \mathbb{K}$. Hence, by (8), for $\{T, Z\} = \{X, Y\}$, $\alpha(F_{TZ^t}, 1) \neq 0$. Next, $\theta^{q+1} = (2\alpha - \alpha^q)(2\alpha^q - \alpha) = 4\delta - 2(\alpha^2 + \alpha^{2q}) + \delta = -2(\delta^2 - 2\delta)$. Thus

$$\theta^{q+1} = 2. \tag{iv}$$

By (iv) $\theta^{q+1} + 3 = 0 \neq 2\delta$. Hence, by (9), for $\{T, Z\} = \{X, Y\}$, $\alpha(F_{T^{-1}Z^t}, 1) \neq 0$. Also, $\delta^2 - 2\delta = -1 \neq 0 = 3 + \theta^{q+1}$, so, by (5), $\alpha(F_{Z^{-1}Z^t}, 1) \neq 0$, for $Z \in \{X, Y\}$.

Next, $\theta_1^q - \theta_1 = 2(\alpha - \alpha^q) - (\alpha^q - \alpha) = 3(\alpha - \alpha^q) = 2(\alpha^q - \alpha)$. So:

$$\begin{aligned} &\text{If } k \not\equiv 2 \pmod 5,\ \theta^q - \theta = 2(\alpha^q - \alpha) \\ &\text{and if } k \equiv 2 \pmod 5,\ \theta^q - \theta = 3(\alpha^q - \alpha). \end{aligned} \tag{v}$$

Suppose first that $k \not\equiv 2 \pmod 5$. Suppose $\alpha(F_{XX^t}, 1) = 0$, then by (4) and (v), $(k - 1) = 2k$ so $k \equiv -1 \pmod 5$. Then, by (1), $\alpha(F_{XX^t}, 1) = \binom{k+1}{2} + (\alpha^2 + \theta^{2q} + 2)k + \alpha^{2q} = -(\alpha^2 + \theta^{2q} + 2) + \alpha^{2q} = \alpha^{2q} - \alpha^2 - \theta^{2q} - 2 = \alpha^{2q} - \alpha^2 - (2\alpha - \alpha^q)^2 - 2 = \alpha^{2q} - \alpha^2 - 4\alpha^2 + 4 - \alpha^{2q} - 2 = 2 \neq 0$, a contradiction.

Suppose $\alpha(F_{YY^t}, 1) = 0$. Then, by (4), and (v) (replacing α by α^q in (4)), $-(k - 1) \equiv 2k \pmod 5$, so $k \equiv 2 \pmod 5$, a contradiction.

Finally, suppose $k \equiv 2 \pmod 5$. Then, by (1), $\alpha(F_{XX^t}, 1) = \binom{k+1}{2} + (\alpha^{2q} + \theta^{2q} + 2)k + \alpha^2 = 3 + 2(\alpha^{2q} + \theta^{2q} + 2) + \alpha^2 = 2 + 2\alpha^{2q} + \alpha^2 + 2\theta^{2q} = 2 + 2\alpha^{2q} + \alpha^2 + 2(2\alpha^q - \alpha)^2 = 2 + 2\alpha^{2q} + \alpha^2 + 2(4\alpha^{2q} - 4 + \alpha^2) = -1 + 3\alpha^2 \neq 0$.

Suppose $\alpha(F_{YY^t}, 1) = 0$. Then, by (4), and (v) (replacing α by α^q in (4)), $-(k - 1) \equiv 3k \pmod 5$, so $k \equiv -1 \pmod 5$, a contradiction. This completes the proof of (10) and of 5.10.

5.11. *Let $\beta_1, \dots, \beta_{k-1}$, $\gamma_1, \dots, \gamma_{k-1} \in \mathbb{K}^*$. Let also $\alpha, \theta, \beta, \rho \in \mathbb{F}^*$ such that $\alpha^{q+1} = \theta + \theta^q$, $\beta^{q+1} = \rho + \rho^q$. Set $a = a_k(\beta_1, \dots, \beta_{k-1})$, $a_1 = a_k(\gamma_1, \dots, \gamma_{k-1})$, $b = b_k(\beta_1, \dots, \beta_{k-1})$, $b_1 = b_k(\gamma_1, \dots, \gamma_{k-1})$, $g = \operatorname{diag}(a, 1, b^{-1})$, $g_1 = \operatorname{diag}(a_1, 1, b_1^{-1})$, $B = u_1^{k+1}(-\alpha^q)\operatorname{diag}(1, b)$, $B_1 = u_1^{k+1}(-\beta^q)\operatorname{diag}(1, b_1)$, $u = u(\alpha, \theta)$, $w = u(\beta, \rho)$, $X = gu$ and $Y = g_1 w$. Finally let $\epsilon \in \{-1, 1\}$. Then:*

(1) $XY^t = guw^t g_1^t$, $(XY^t)^{-1} = (g_1^t)^{-1}(uw^t)^{-1}g^{-1}$.

(2) $X^{-1}Y^t = u^{-1}w^t g^{-1} g_1^t$ *and* $(X^{-1}Y^t)^{-1} = (g_1^t)^{-1} g (u^{-1}w^t)^{-1}$.

(3) $X = \begin{bmatrix} a & 0_{k,k+1} \\ E & B^{-1} \end{bmatrix}$ *with E some $(k + 1) \times k$ matrix, such that $E_{1,k} = \alpha \neq 0$.*

(4)

$$X^\epsilon Y^t = \begin{bmatrix} a^\epsilon a_1^t & R \\ S & T \end{bmatrix} \qquad (X^\epsilon Y^t)^{-1} = \begin{bmatrix} T' & R' \\ S' & B_1^t B^\epsilon \end{bmatrix}$$

with T', T, R, R', S, S' some $k\times k$, $(k+1)\times(k+1)$, $k\times(k+1)$, $k\times(k+1)$, $(k+1)\times k$, $(k+1)\times k$, matrices respectively. Further, the first $k-1$ rows of R are zero.

(5) *Let $S \in \{Y^t, X^\epsilon Y^t\}$. Then for $1 \le i \le k-1$, $v_i S = v + \delta_{i+1} v_{i+1}$, with $v \in \mathcal{V}_i$ and $\delta_{i+1} \in \mathbb{K}^*$.*

(6) *$S_{k,n} \neq 0$, for all $S \in \{Y^t, X^\epsilon Y^t\}$.*

(7) *For $S \in \{Y^t, X^\epsilon Y^t\}$, there exists $v \in \mathcal{V}_k$, $\eta \in \mathbb{F}$ and $\mu \in \mathbb{F}^*$ such that:*

(7i) $$v_{k+1} S^{-1} \equiv \eta v_{k+1} + \mu v_{k+2} \pmod{\mathcal{V}_k}.$$

(7ii) $$v S^{-1} \equiv (\eta + \rho^{1-q}) v_{k+1} + \mu v_{k+2} \pmod{\mathcal{V}_k}.$$

(7iii) *In all cases $\mu = -\beta^q$. If $S = Y^t$, $\eta = 1$, while if $S = X^\epsilon Y^t$, $\eta = 1 + \epsilon\alpha^q\beta^q$.*

(8) *For $S \in \{Y^t, X^\epsilon Y^t\}$, $V = \langle \mathcal{O}(v_1, S)\rangle$ iff $-\rho^{1-q}$ is not a root of F_Z, where $Z = B_1^t$, if $S = Y^t$ and $Z = B_1^t B^\epsilon$, if $S = X^\epsilon Y^t$.*

(9) *If $\beta \neq 0$, then $V = \langle \mathcal{O}(v_1, Y^t)\rangle$.*

Proof. (1) is obvious. For (2), we have $X^{-1}Y^t = u^{-1}g^{-1}w^t g_1^t$. By 5.2.3, $[g^{-1}, w^t] = 1$, and (2) follows. For (3) recall from 5.4.1 that

$$u = u_{k+1}(\alpha^q) u_k(\alpha) u_0(-\theta^q).$$

Further by 5.2.2, $g u_{k+1}(\alpha^q) = \operatorname{diag}(a, B^{-1})$. Thus

$$X = \operatorname{diag}(a, B^{-1}) u_k(\alpha) u_0(-\theta^q).$$

Note now that

$$s(u_k(\alpha)u_0(-\theta^q)) = \begin{bmatrix} 1 & 0 & 0 \\ \alpha & 1 & 0 \\ -\theta^q & 0 & 1 \end{bmatrix}.$$

Hence (3) follows, the $(1,k)$-entry of E is $\alpha(B^{-1})_{1,1} - \theta^q (B^{-1})_{1,2} = \alpha\cdot 1 - \theta^q \cdot 0 = \alpha$.

To show (4) and (5), let $1 \le i \le k-1$, then $v_i u^{-1} w^t = v_i$, so $v_i X^{-1} Y^t = v_i g^{-1} g_1^t$. Also $v_i g \in \mathcal{V}_i$, so $v_i g(uw^t) = v_i g$ and $v_i X Y^t = v_i g g_1^t$. We conclude that:

(i) $$\text{For } 1 \le i \le k-1,\ v_i X^\epsilon Y^t = v_i g^\epsilon g_1^t.$$

Now the shape of $X^\epsilon Y^t$ follows from (3) and (i), since, by (i), the first $k-1$ rows of R are zero. Also the shape of $(X^\epsilon Y^t)^{-1}$, follows from (3). For (5), we use (i). Note that a^ϵ is unipotent, lower triangular and a_1^t is upper triangular unipotent with $(a_1^t)_{i,j} = 0$, for $j > i+1$, and $(a_1^t)_{i,i+1} \neq 0$. This easily implies (5), for $S = X^\epsilon Y^t$. For $S = Y^t$, $v_i Y^t = v_i + \gamma_{k-i} v_{i+1}$, for all $1 \le i \le k-1$, thus (5) holds for Y^t as well.

Recall now that

$$s(uw^t) = \begin{bmatrix} 1 & \beta & \rho \\ \alpha & \alpha\beta + 1 & \alpha\rho + \beta^q \\ \theta & \beta\theta + \alpha^q & \theta\rho + \alpha^q\beta^q + 1 \end{bmatrix}$$

$$s((uw^t)^{-1}) = \begin{bmatrix} 1 + \alpha\beta + \theta^q\rho^q & \bar{\beta} - \alpha^q\rho^q & \rho^q \\ -\alpha - \beta^q\theta^q & \alpha^q\beta^q + 1 & -\beta^q \\ \theta^q & -\alpha^q & 1 \end{bmatrix}$$

$$s(u^{-1}w^t) = \begin{bmatrix} 1 & \beta & \rho \\ -\alpha & 1 - \alpha\beta & -\alpha\rho + \beta^q \\ \theta^q & \beta\theta^q - \alpha^q & \rho\theta^q - \alpha^q\beta^q + 1 \end{bmatrix}$$

$$s((u^{-1}w^t)^{-1}) = \begin{bmatrix} 1 - \alpha\beta + \theta\rho^q & -\beta + \alpha^q\rho^q & \rho^q \\ \alpha - \theta\beta^q & 1 - \alpha^q\beta^q & -\beta^q \\ \theta & \alpha^q & 1 \end{bmatrix}.$$

Note now that $v_k g^{-1} \equiv v_k \equiv v_k g \pmod{\mathcal{V}_{k-1}}$, $v_{k+1}g^{-1} = v_{k+1}$ and $v_{k+2}g^{-1} = v_{k+2}$. Since $u^\epsilon w^t$ fixes $\mathcal{V}_{k-1}$, we see that,

$$v_k(X^\epsilon Y^t) \equiv v_k(u^\epsilon w^t)g_1^t \pmod{\mathcal{V}_{k-1}}.$$

Thus modulo $\mathcal{V}_k$, $v_k(X^\epsilon Y^t) \equiv (\beta v_{k+1} + \rho v_{k+2})g_1^t \equiv \beta v_{k+1} + \rho(v' + \eta v_n)$, with $v' \in \langle v_{k+2}, \dots, v_{n-1}\rangle$, $\eta \in \mathbb{F}^*$. This is because the $(k,1)$ entry of b_1^{-1} is $\eta = \gamma_1\gamma_2\cdots\gamma_{k-1}$, and $g_1^t = \operatorname{diag}(a_1^t, 1, (b_1^{-1})^t)$. This shows (6), for $S = X^\epsilon Y^t$ and it is easy to see that (6) holds for $S = Y^t$ as well.

Next, modulo $\mathcal{V}_k$, we have $-\rho^{-q}\beta^q v_k(XY^t)^{-1} = -\rho^{-q}\beta^q v_k(uw^t)^{-1}g^{-1} \equiv ((\alpha^q\beta^q + \beta^{q+1}\rho^{-q})v_{k+1} - \beta^q v_{k+2})g^{-1} = (\alpha^q\beta^q + \beta^{q+1}\rho^{-q})v_{k+1} - \beta^q v_{k+2}$. Since $\beta^{q+1} = \rho + \rho^q$, we see that $-\rho^{-q}\beta^q v_k(XY^t)^{-1} \equiv (\alpha^q\beta^q + 1 + \rho^{1-q})v_{k+1} - \beta^q v_{k+2}$. Note that $v_{k+1}(XY^t)^{-1} \equiv (\alpha^q\beta^q + 1)v_{k+1} - \beta^q v_{k+2} \pmod{\mathcal{V}_k}$. This shows (7), for $S = XY^t$.

Let $v \in \mathcal{V}_k$, such that $v(g_1^t)^{-1}g = v_k$. Then, modulo $\mathcal{V}_k$,

$$\begin{aligned} -\rho^{-q}\beta^q v(X^{-1}Y^t)^{-1} &= -\rho^{-q}\beta^q v_k(u^{-1}w^t)^{-1} \\ &\equiv ((\beta^{q+1}\rho^{-q} - \alpha^q\beta^q)v_{k+1} - \beta^q v_{k+2}) \\ &= (1 - \alpha^q\beta^q + \rho^{1-q})v_{k+1} - \beta^q v_{k+2}. \end{aligned}$$

Note that $v_{k+1}(X^{-1}Y^t)^{-1} \equiv (1 - \alpha^q\beta^q)v_{k+1} - \beta^q v_{k+2} \pmod{\mathcal{V}_k}$. This shows (7), for $S = X^{-1}Y^t$.

Next

$$\begin{aligned} -\rho^{-q}\beta^q v_k(Y^t)^{-1} &= -\rho^{-q}\beta^q v_k(g_1^t)^{-1}(w^t)^{-1} = -\rho^{-q}\beta^q v_k(w^t)^{-1} \\ &= -\rho^{-q}\beta^q v_k + \rho^{-q}\beta^{q+1}v_{k+1} - \beta^q v_{k+2} \\ &= -\rho^{-q}\beta^q v_k + (1 + \rho^{1-q})v_{k+1} - \beta^q v_{k+2}. \end{aligned}$$

Also $v_{k+1}(Y^t)^{-1} = v_{k+1} - \beta^q v_{k+2}$, thus (7) holds for $S = Y^t$ and (7) is proved.

For (8), set $\mathcal{W} = \langle \mathcal{O}(v_1, S)\rangle$. Set also $Z = B_1^t$, if $S = Y^t$ and $Z = B_1^t B^\epsilon$, if $S = X^\epsilon Y^t$. By (5), $\mathcal{V}_k \subseteq \mathcal{W}$. Let $\eta, \mu \in \mathbb{F}$ be as in (7iii). Since $\mathcal{V}_k \subseteq \mathcal{W}$,

$$\text{(ii)} \qquad \rho^{1-q} v_{k+1} + \eta v_{k+1} + \mu v_{k+2} \in \mathcal{W}.$$

Also, by (3), (4) and (7i), $v_{k+1}\mathrm{diag}\,(I_k, Z) = \eta v_{k+1} + \mu v_{k+2}$. Thus, by (ii), $\rho^{1-q} v_{k+1} + v_{k+1}\mathrm{diag}\,(I_k, Z) \in \mathcal{W}$, now (8) follows from (4), (5) and 1.17 (taking S^{-1} in place of S in 1.17); note that $\langle \mathcal{O}(v_{k+1}, \mathrm{diag}\,(I_k, Z))\rangle = \langle v_{k+1}, \dots, v_n\rangle$.

Finally, for (9), note that if $\beta \neq 0$, then $\rho^{1-q} \neq -1$, since $0 \neq \beta^{q+1} = \rho + \rho^q$. Since 1 is the only root of $F_{B_1^t}$, $-\rho^{1-q}$ is not a root of $F_{B_1^t}$, so (9) follows from (8).

5.12. *Let $\beta_1, \dots, \beta_{k-1}, \gamma_1, \dots, \gamma_{k-1} \in \mathbb{K}^*$. Let also $\alpha, \theta, \beta, \rho \in \mathbb{F}^*$ such that $\alpha^{q+1} = \theta + \theta^q$, $\beta^{q+1} = \rho + \rho^q$. Set $a = a_k(\beta_1, \dots, \beta_{k-1})$, $a_1 = a_k(\gamma_1, \dots, \gamma_{k-1})$, $b = b_k(\beta_1 \dots, \beta_{k-1})$, $b_1 = b_k(\gamma_1, \dots, \gamma_{k-1})$, $g = \mathrm{diag}\,(a, 1, b^{-1})$, $g_1 = \mathrm{diag}\,(a_1, 1, b_1^{-1})$, $u = u(\alpha, \theta)$, $w = u(\beta, \rho)$, $X = gu$ and $Y = g_1 w$. Finally let $\epsilon \in \{-1, 1\}$.*

Let $S \in \{Y^t, X^\epsilon Y^t\}$ and $R \in \Delta^{\leq 2}(X) \cap \Delta^{\leq 1}(S)$. Then v_1 is a characteristic vector of R.

Proof. The proof is almost identical to the proof of 4.3. Note first that, by 5.11.3, X satisfies the hypotheses of 1.13. Let $h \in \Delta^{\leq 1}(X) \cap \Delta^{\leq 1}(R)$. Then, $[h, X] = 1$, so by 1.13, there exists $0 \neq \beta \in \mathbb{K}$, and $1 \leq r \leq n-1$, such that $h - \beta I_n \in \mathcal{T}_n(r)$. We use 1.15. We take in 1.15, $T = h - \beta I_n$. Note that R commutes with h and hence with T.

Suppose first that $r \leq k-1$, we take in 1.15, $j = r = m$ and $\ell = 0$. Notice that by 5.11.5, hypothesis (a) of 1.15 is satisfied, hypothesis (b) and (c) of 1.15 are satisfied, by definition and we observed that hypothesis (e) of 1.15 is satisfied. Finally, since R centralizes T, $\mathcal{V}_r$ is R-invariant. Hence 1.15 completes the proof in this case.

Suppose next that $r \geq k$, we take in 1.15, $j = k-1$, $\ell = 1$ and $m = k$, if $r = k$ and $m = \dim(\mathrm{im}\,(T))$, if $r > k$. Notice that $\mathcal{V}_m$ is R-invariant. Also, by 5.11.6, $S_{k,n} \neq 0$, so clearly $v_k \notin \ker(ST)$ and hypothesis (c) of 1.15 holds. Thus 1.15 completes the proof in this case too.

5.13. *For $i \in \{1, 2, 3, 4\}$, let $\alpha_i \in \mathbb{F}^*$ and set $B_i = u_1^{k+1}(-\alpha_i)\mathrm{diag}\,(1, b_k)$. Let also $\epsilon \in \{1, -1\}$ and $1 \neq \gamma \in \mathbb{F}^*$. Then:*

(1) *If $F_{B_1^t B_2^\epsilon}[\gamma] = 0 = F_{B_3^t B_4^\epsilon}[\gamma]$, then $\alpha_1\alpha_2 = \alpha_3\alpha_4$.*
(2) *Suppose $\alpha_1^2 \notin \mathbb{K}$ and $\alpha_2 = \alpha_1^q$. Then γ is a root of at most one of the polynomials $F_{B_1^t B_1^\epsilon}, F_{B_2^t B_2^\epsilon}$ and $F_{B_1^t B_2^\epsilon}$.*
(3) *Suppose $\alpha_1^2 \notin \mathbb{K}$ and $\alpha_2 = \alpha_1^q$. Then either we can find $j \in \{1, 2\}$, such that $F_{B_j^t B_j}[\gamma] \neq 0 \neq F_{B_j^t B_j^{-1}}[\gamma]$, or for $\{B, C\} = \{B_1, B_2\}$, $F_{B^t C}[\gamma] \neq 0 \neq F_{B^t C^{-1}}[\gamma]$.*

(4) *If* $\operatorname{char}(\mathbb{K}) \neq 2$ *and* $q > 3$*, then we can find* $\alpha_1, \alpha_2 \in \mathbb{K}^*$*, such that* $F_{B_1^tB_2}[-1], F_{B_1^tB_2^{-1}}[-1], F_{B_2^tB_1}[-1], F_{B_2^tB_1^{-1}}[-1]$ *are all distinct from* 0.

(5) *Suppose that* $q = 2$*, and that* $\alpha_1 \notin \mathbb{K}$*. Then,* $F_{B_1^tB_1^{-1}}[\gamma] \neq 0$*. In particular, we can pick* $\alpha_1 \in \mathbb{F}-\mathbb{K}$ *such that* $F_{B_1^tB_1}[\gamma] \neq 0 \neq F_{B_1^tB_1^{-1}}[\gamma]$.

Proof. First observe that, for $1 \leq i \leq 4$, $B_i = b_{k+1}(\alpha_i, 1, \dots, 1)$. We mention that for small values of k ($k = 1, 2$ or 3), direct calculations show (1). For the general case in (1), suppose $F_{B_1^tB_2}[\gamma] = 0 = F_{B_3^tB_4}[\gamma]$. Then, by 2.12.4, $(\gamma-1)F_k[\gamma] - \alpha_1\alpha_2\gamma G_{k-1}[\gamma] = 0 = (\gamma-1)F_k[\gamma] - \alpha_3\alpha_4\gamma G_{k-1}[\gamma]$. Suppose $\alpha_1\alpha_2 \neq \alpha_3\alpha_4$. Then $G_{k-1}[\gamma] = 0$, and as $\gamma \neq 1$, $F_k[\gamma] = 0$. This contradicts 2.6.6. Using 2.12.5, it is easy to see that if $F_{B_1^tB_2^{-1}}[\gamma] = 0 = F_{B_3^tB_4^{-1}}[\gamma]$, then $\alpha_1\alpha_2 = \alpha_3\alpha_4$. (2) follows immediately from (1), noticing that $\alpha_1^2, \alpha_1^{2q}$ and α_1^{q+1} are distinct. (3) follows from (2) noticing that, by 2.12.4 and 2.12.5, $F_{B_1^tB_2^\epsilon}[\gamma] = F_{B_2^tB_1^\epsilon}[\gamma]$.

For (4), just choose $\alpha_1, \alpha_2 \in \mathbb{K}^*$ such that -1 is not a root of the polynomial $F_{B_1^tB_2} = F_{B_2^tB_1} = (\lambda-1)F_k - \alpha_1\alpha_2\lambda G_{k-1}$ nor of the polynomial $F_{B_1^tB_2^{-1}} = F_{B_2^tB_1^{-1}} = (\lambda-1)Q_k + \alpha_1\alpha_2\lambda Q_{k-1}$, using (1).

For (5), note that as $q = 2$, 2.12.5 shows that, $F_{B_1^tB_1^{-1}}[\lambda] = (\lambda+1)Q_k + \alpha_1^2\lambda Q_{k-1} = \lambda^{k+1} + 1 + \alpha_1^2\lambda Q_{k-1}$. Suppose $\gamma = \alpha_1$. Then (since $\alpha_1^3 = 1$), $F_{B_1^tB_1^{-1}}[\alpha_1] = \alpha_1^{k+1} + 1 + Q_{k-1}[\alpha_1] = \alpha_1^{k+1} + \alpha_1^{k-1} + \alpha_1^{k-2} + \dots + \alpha_1$. Recall that $\alpha_1^2+\alpha_1+1 = 0$. Thus, if $k-1 \equiv 0 \pmod 3$, $F_{B_1^tB_1^{-1}}[\alpha_1] = \alpha_1^2+0 = \alpha_1^2$, if $k-1 \equiv 1 \pmod 3$, then $F_{B_1^tB_1^{-1}}[\alpha_1] = 1+\alpha_1 = \alpha_1^2$, and if $k-1 \equiv 2 \pmod 3$, $F_{B_1^tB_1^{-1}}[\alpha_1] = \alpha_1 + \alpha_1^2 + \alpha_1 = \alpha_1^2$. Suppose $\gamma = \alpha_1^2$. Then, $F_{B_1^tB_1^{-1}}[\alpha_1^2] = \alpha_1^{2k+2} + 1 + \alpha_1 Q_{k-1}[\alpha_1^2]$. Note that if $k \equiv 0 \pmod 3$, $Q_{k-1}[\alpha_1^2] = 0$, if $k \equiv 1 \pmod 3$, $Q_{k-1}[\alpha_1^2] = 1$ and if $k \equiv 2 \pmod 3$, $Q_{k-1}[\alpha_1^2] = \alpha_1$. Thus, if $k \equiv 0 \pmod 3$, then $F_{B_1^tB_1^{-1}}[\alpha_1^2] = \alpha_1^2 + 1 + \alpha_1 \cdot 0 = \alpha_1$, if $k \equiv 1 \pmod 3$, $F_{B_1^tB_1^{-1}}[\alpha_1^2] = \alpha_1 + 1 + \alpha \cdot 1 = 1$ and if $k \equiv 2 \pmod 3$, $F_{B_1^tB_1^{-1}}[\alpha_1^2] = 1 + 1 + \alpha_1 \cdot \alpha_1 = \alpha_1^2$. This shows first part of (5). The second part of (5) follows from (1), just choose $\alpha_1 \in \mathbb{F}-\mathbb{K}$ so that $F_{B_1^tB_1}[\gamma] \neq 0$.

Corollary 5.14. (1) *Let* $\alpha_1 \in \Xi$ *and let* $\theta \in \mathbb{F}$ *such that* $\theta + \theta^q = \alpha_1^{q+1}$*. Then we can pick* $\alpha, \beta \in \{\alpha_1, \alpha_1^q\}$ *such that if we set* $X = X(\alpha, \theta)$ *and* $Y = X(\beta, \theta)$*, then for* $\{T, Z\} = \{X, Y\}$ *and* $S \in \{TZ^t, T^{-1}Z^t, T^t, Z^t\}$*,* $\langle \mathcal{O}(v_1, S)\rangle = V$*. Further, if* $q = 2$*,* $\alpha = \beta$.

(2) *Suppose* $q = 4$ *and let* $\theta \in \mathbb{F}^*$*. Suppose* $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}^*$ *are distinct elements such that* $\theta + \theta^q = \alpha_i^{q+1}$*,* $1 \leq i \leq 3$*. Then there exist* $\beta \in \{\alpha_1, \alpha_2, \alpha_3\}$ *such that for* $X = X(\beta, \theta)$*, and* $S \in \{XX^t, X^{-1}X^t, X^t\}$*,* $\langle \mathcal{O}(v_1, S)\rangle = V$*.*

(3) *If* $q \neq 3$ *is odd, or* $q = 3$ *and* $k \not\equiv 1 \pmod 3$*, then there are* $\alpha, \beta \in \mathbb{K}^*$*, such that if we set* $X = X(\alpha, \theta)$ *and* $Y = X(\beta, \rho)$*, with* $\theta = \frac{1}{2}\alpha^2$ *and*

$\rho = \frac{1}{2}\beta^2$, *then for* $\{T, Z\} = \{X, Y\}$ *and* $S \in \{TZ^t, T^{-1}Z^t, T^t, Z^t\}$, $\langle \mathcal{O}(v_1, S)\rangle = V$.

(4) *If* $q = 3$ *and* $k \geq 4$, *let* $a = a_k(1, 1, -1, 1, 1, \dots, 1)$ *and* $b = b_k(1, 1, -1, 1, 1, \dots, 1)$. *Let* $X = \operatorname{diag}(a_k, 1, b_k^{-1})u(1, \frac{1}{2})$ *and* $Y = \operatorname{diag}(a, 1, b^{-1})u(1, \frac{1}{2})$. *Then for* $\{T, Z\} = \{X, Y\}$ *and* $S \in \{TZ^t, T^{-1}Z^t, T^t, Z^t\}$, $\langle \mathcal{O}(v_1, S)\rangle = V$.

Proof. For (1), pick $\alpha, \beta \in \{\alpha_1, \alpha_1^q\}$. Let $B = u_1^{k+1}(-\alpha^q)\operatorname{diag}(1, b_k)$ and $B_1 = u_1^{k+1}(-\beta^q)\operatorname{diag}(1, b_k)$. By 5.11.8, for $\epsilon \in \{1, -1\}$, $\langle \mathcal{O}(v_1, X^\epsilon Y^t)\rangle = V$, iff $-\theta^{1-q}$ is not a root of $F_{B_1^t B^\epsilon}$. Note that since $\theta + \theta^q = \alpha_1^{q+1} \neq 0$, $\theta^{1-q} \neq -1$. Hence, using 5.13.3 (when $q > 2$, notice that $\alpha_1^2 \notin \mathbb{K}$ follows from the equation $\alpha_1^q + \alpha_1 = \alpha_1^{q+1}$), or 5.13.5 (when $q = 2$), we can pick $\alpha, \beta \in \{\alpha_1, \alpha_1^q\}$ such that $-\theta^{1-q}$ is not a root of $F_{B^t B_1^\epsilon}$ and not a root of $F_{B_1^t B^\epsilon}$ (with $\alpha = \beta$ when $q = 2$, by 5.13.5). Of course, by 5.11.9, $\langle \mathcal{O}(v_1, Y^t)\rangle = V = \langle \mathcal{O}(v_1, X^t)\rangle$, this shows (1).

The proof of (2) is similar. Setting $X_i = X(\alpha_i, \theta)$ and

$$B_i = u_1^{k+1}(-\alpha_i^q)\operatorname{diag}(1, b_k), \qquad 1 \leq i \leq 3,$$

we see, using 5.11.8, that for $\epsilon \in \{1, -1\}$, $\langle \mathcal{O}(v_1, X_i^\epsilon X_i^t)\rangle = V$, iff $-\theta^{1-q}$ is not a root of $F_{B_i^t B_i^\epsilon}$. Again we observe that $\theta^{1-q} \neq -1$. Further, since α_1, α_2 and α_3 are distinct, also, $\alpha_1^{2q}, \alpha_2^{2q}$ and α_3^{2q} are distinct, so by 5.13.1, there exists $1 \leq i \leq 3$, such that $\gamma = -\theta^{1-q}$ is not a root of the polynomial $F_{B_i^t B_i}$ and $F_{B_i^t B_i^{-1}}$.

For (3), notice first that, by 5.3.5, given $\alpha \in \mathbb{K}^*$, if we set $\theta = \theta(\alpha) = \frac{1}{2}\alpha^2$, then $X(\alpha, \theta) \in L$ and $\theta^{q-1} = 1$. Hence if $q > 3$, (3) follows from 5.11.8 and 5.13.4 (in the same way as we proved (1) and (2), noticing that since $\theta \in \mathbb{K}^*$, $\theta^{1-q} = 1$), and if $q = 3$, take $\alpha = \beta = 1$ and use 5.6.1. Finally (4) follows similarly using 5.11.8 and 5.6.2.

Theorem 5.15. (1) *We can pick* $\theta, \alpha, \beta \in \mathbb{F}$, *with* $\theta + \theta^q = \alpha^{q+1} = \beta^{q+1}$, *such that if we set* $X = X(\alpha, \theta)$ *and* $Y = X(\beta, \theta)$, *then:*

(i) *For* $\{T, Z\} = \{X, Y\}$ *and* $S \in \{TZ^t, T^{-1}Z^t, T^t, Z^t\}$, $\langle \mathcal{O}(v_1, S)\rangle = V$ *and:*

(ii) *For* $S \in \{TZ^t, T^{-1}Z^t\}$, $\alpha(F_S, 1) \neq 0$.

(2) *The commuting graph* $\Delta(L')$ *is balanced.*

Proof. For (1), suppose first that $q \neq 2, 4$. Then, by 5.10.10iii, we can find $\alpha_1 \in \Xi$, and $\theta \in \mathbb{F} - \mathbb{K}$, with $\theta + \theta^q = \alpha_1^{q+1}$, such that *for all* $\alpha, \beta \in \{\alpha_1, \alpha_1^q\}$, if we set $X = X(\alpha, \theta)$ and $Y = X(\beta, \theta)$, $\alpha(F_{T^\epsilon Z^t}, 1) \neq 0$, for $T, Z \in \{X, Y\}$ and $\epsilon \in \{1, -1\}$. Now, use 5.14.1, to pick $\alpha, \beta \in \{\alpha_1, \alpha_1^q\}$, such that for $\{T, Z\} = \{X, Y\}$ and $S \in \{TZ^t, T^{-1}Z^t, T^t, Z^t\}$, $\langle \mathcal{O}(v_1, S)\rangle = V$. This shows (1), in case $q \neq 2, 4$.

Suppose next that $q=2$. Let $\alpha \in \mathbb{F}-\mathbb{K}$. Then, by 5.10.10i, for $X_1 \in \{X(\alpha,\alpha), X(\alpha^q,\alpha)\}$, and $\epsilon \in \{1,-1\}$, $\alpha(F_{X_1^\epsilon X_1^t},1) \neq 0$. By 5.14.1, there exists $X \in \{X(\alpha,\alpha), X(\alpha^q,\alpha)\}$, such that $V = \langle \mathcal{O}(v_1,S)\rangle$, for $S \in \{XX^t, X^{-1}X^t, X^t\}$, so (1) holds in case $q=2$, choosing $Y=X$. The proof of (1) in case $q=4$, is similar,using 5.10.10ii and 5.14.2.

We proceed with the proof of (2). Set $\Lambda = \Delta(L)$. Suppose $L \simeq SU(n,q)$ and let $X, Y \in L$ be as in (1). We show that $B_\Lambda(X,Y^t)$ holds. The proof that $B_\Lambda(Y,X^t)$ holds is symmetric and by 1.9, Λ is balanced. Let $S \in \{XY^t, X^{-1}Y^t, Y^t\}$. Suppose $R \in \Lambda^{\leq 2}(X) \cap \Lambda^{\leq 1}(S)$. By 5.12,

$$(*) \qquad v_1 \text{ is a characteristic vector of } R.$$

Now if $S = Y^t$, then S commutes with R, so since $V = \langle \mathcal{O}(v_1, Y^t)\rangle$, $(*)$ implies that $R \in Z(L)$, a contradiction. Suppose $S \in \{XY^t, X^{-1}Y^t\}$. Then, by (ii) of (1), $\gcd\{\{i : \alpha(F_S,i) \neq 0\} \cup \{n\}\} = 1$, so, by $(*)$ and 1.14.5, $R \in Z(L)$, a contradiction.

Suppose $L \simeq SO_n(q)$. Pick X, Y as in 5.14.3 and 5.14.4. Since $Z(L)=1$, to show $B_\Lambda(X,Y^t)$ holds, it suffices, by 1.14.1, to show that $V = \langle \mathcal{O}(v_1,S)\rangle$, for $S \in \{XY^t, X^{-1}Y^t, Y^t\}$, but this holds by the choice of X, Y. By symmetry also $B_\Lambda(Y,X^t)$ holds and the proof of the theorem is complete.

6. The Orthogonal Groups in odd characteristic and even dimension.

In this section $\mathbb{F}$ is a field of odd order and $n = 2k \geq 8$ is even. Let J be the following $n \times n$ matrix:

$$J = \begin{bmatrix} 0 & 0 & \cdot & \cdot & \cdot & \cdot & 0 & 1 & 0 \\ 0 & 0 & \cdot & \cdot & \cdot & 0 & \bar{1} & 0 & 0 \\ 0 & 0 & \cdot & \cdot & 0 & 1 & 0 & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 1 & 0 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \bar{1} & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 & 0 \\ 0 & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 & \nu \end{bmatrix}.$$

Let $L \simeq SO^\epsilon(\mathbb{F})$ be the subgroup of $SL_n(\mathbb{F})$ defined by $L = \{x \in SL_n(\mathbb{F}) : xJx^t = J\}$. Of course, for a suitable choice of ν ($\nu = (-1)^k$) $\epsilon = +$ and for a suitable choice of ν ($(-1)^k\nu$ a nonsquare in $\mathbb{F}$) $\epsilon = -$.

We continue with the notation of Section 1. In addition we let $f : V \times V \to \mathbb{F}$ be a bilinear form whose matrix with respect to the basis $\mathcal{B} = \{v_1, \dots, v_n\}$ is J.

6.1. *Let $u \in GL_n(q)$ be a matrix of the form*

$$u = \begin{bmatrix} 1 & 0 & 0 & \cdot & \cdot & \cdot & \cdot & 0 & 0 \\ \alpha_2 & 1 & 0 & 0 & \cdot & \cdot & \cdot & 0 & 0 \\ * & \alpha_3 & 1 & 0 & 0 & \cdot & \cdot & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ * & \cdot & \cdot & \cdot & * & \alpha_{n-2} & 1 & 0 & 0 \\ * & \cdot & \cdot & \cdot & \cdot & * & \alpha_{n-1} & 1 & 0 \\ 0 & 0 & 0 & \cdot & \cdot & \cdot & \cdot & 0 & 1 \end{bmatrix} \qquad \alpha_i \in \mathbb{F}^*, \quad \textit{for all } \ i.$$

Let $h \in GL(n,\mathbb{F}) - Z(GL(n,\mathbb{F}))$ be a matrix commuting with u. Then:

(1) *h has the form*

$$h = \begin{bmatrix} M & E \\ F & c \end{bmatrix}$$

where M is an $(n-1)\times(n-1)$ matrix commuting with $M_{n,n}(u)$, $c \in \mathbb{F}^*$, E is a column $(n-1)\times 1$ matrix of the form $(0,0,\dots,\rho)^t$, F is a row $1\times(n-1)$ matrix of the form $(\theta,0,\dots,0)$.

(2) *Suppose $u,h \in L$, and let $\rho,\theta \in \mathbb{F}$ as in (1). Then there exists $\epsilon \in \{1,-1\}$ such that $h_{i,i} = \epsilon$, for all $1 \le i \le n$. Further, $\theta = -\rho f(v_n,v_n)$.*

(3) *If $u,h \in L$, then there exists $\epsilon \in \{1,-1\}$, and $1 \le r' < n-1$, such that*

$$h - \epsilon I_n = \begin{bmatrix} t' & E \\ F & 0 \end{bmatrix}$$

with $t' \in \mathcal{T}_{n-1}(r')$ (see notation in 1.1.10).

(4) *Suppose $u,h \in L$ and let t' and r' be as in (3) and ρ as in (2). Suppose that either $\rho = 0$, or $r' \neq k-1$. There exists $\epsilon \in \{1,-1\}$, $i \in \{1,2\}$ and $1 \le r < n-1$, such that*

$$(h - \epsilon I_n)^i = \begin{bmatrix} t & 0_{n-1,1} \\ 0_{1,n-1} & 0 \end{bmatrix}$$

where $t \in \mathcal{T}_{n-1}(r)$.

(5) *Suppose $u,h \in L$ and let t' and r' be as in (3) and ρ,θ as in (2). Suppose $r' = k-1$ and $\rho \neq 0$. Then:*

(5i) *k is even.*

(5ii) *If, in addition, $(h-\epsilon I_n)^2 = 0$, then we may assume that $f(v_n,v_n) = 1$ (so $\nu = 1$) and if we set $d = t'_{k,1}$, then $d^2 = \theta^2$.*

Proof. Note that h commutes with the matrix $u - I_n$, and clearly for $1 \le i \le n-1$, $\operatorname{im}(u-I_n)^i = \mathcal{V}_{n-i-1}$. Since h commutes with $(u-I_n)^i$, h fixes $\operatorname{im}(u-I_n)^i$. Thus h fixes $\mathcal{V}_i$, for $1 \le i \le n-2$. Also $\ker(u - I_n) = \langle v_1, v_n\rangle$, so h fixes $\langle v_1, v_n\rangle$, thus h has the form

$$h = \begin{bmatrix} M & E \\ F & c \end{bmatrix}$$

with M some $(n-1)\times(n-1)$ matrix and E, F and c as in (1). Let $u_1 = M_{n,n}(u)$. Then

$$hu = \begin{bmatrix} Mu_1 & E \\ F & c \end{bmatrix} \quad \text{and} \quad uh = \begin{bmatrix} u_1 M & E \\ F & c \end{bmatrix}$$

this shows (1).

For (2), note that $v_n h = \theta v_1 + c v_n$, thus $0 \neq f(v_n, v_n) = f(v_n h, v_n h) = c^2 f(v_n, v_n)$. Thus $c = \epsilon$, for some $\epsilon \in \{1, -1\}$. Also, since u_1 commutes with M, 1.13.2 implies that there exists $\beta \in \mathbb{F}$, such that $h_{i,i} = \beta$, for all $1 \le i \le n-1$. Since v_k is a nonsingular vector, it is easy to check that we must have $\beta = 1$ or -1. Since $\det(h) = 1$, $\beta = \epsilon$ and the first part of (2) is proved. For the second part we have $0 = f(v_{n-1}, v_n) = f(v_{n-1}h, \theta v_1 + \epsilon v_n) = f(v' + \epsilon v_{n-1} + \rho v_n, \theta v_1 + \epsilon v_n)$, with $v' \in \mathcal{V}_{n-2}$. But $f(v_1, v') = f(v_n, v') = 0$. Thus $0 = f(v_{n-1}, v_n) = f(\epsilon v_{n-1} + \rho v_n, \theta v_1 + \epsilon v_n) = \epsilon\theta + \epsilon\rho f(v_n, v_n)$ and the second part of (2) is proved.

Next note that by (1), $u_1 := M_{n,n}(u)$, commutes with M so, by 1.13 and (2), $(M - \epsilon I_{n-1}) \in \mathcal{T}_{n-1}(r')$, for some $1 \le r' < n-1$. Thus (3) follows from (1) and (2).

For (4), we use (3). If $\rho = 0$, then, by (2) also $\theta = 0$, and so by (3), (4) holds with $i = 1$, $r = r'$ and $t = t'$. Suppose $\rho \neq 0$. Note that EF is an $(n-1)\times(n-1)$ matrix whose $(n-1, 1)$-entry is $\rho\theta$ and for $(i, j) \neq (n-1, 1)$, $(EF)_{ij} = 0$. Further $t'E = 0_{n-1,1}$ (the last column of t' is zero), $Ft' = 0_{1,n-1}$ (the first row of t' is zero) and $FE = 0$. Thus

$$(h - \epsilon I_n)^2 = \begin{bmatrix} t' & E \\ F & 0 \end{bmatrix} \cdot \begin{bmatrix} t' & E \\ F & 0 \end{bmatrix} = \begin{bmatrix} (t')^2 + EF & 0_{n-1,1} \\ 0_{1,n-1} & 0 \end{bmatrix}.$$

Since we are assuming that $\rho \neq 0$ and $r' \neq k-1$, either $r' > k-1$, in which case $(t')^2 = 0$, and $t = EF \in \mathcal{T}_{n-1}(n-2)$. Or $r' < k-1$, in which case, $(t')^2 \in \mathcal{T}_{n-1}(r)$, for some $1 < r < n-2$, and then $t := (t')^2 + EF \in \mathcal{T}_{n-1}(r)$. This shows (4).

Finally assume the hypotheses of (5). Suppose first that k is odd. Let $j = \frac{k+1}{2}$, then $r' + j = (k-1) + \frac{k+1}{2} = \frac{3k-1}{2}$ and $t'_{r'+j,j} \neq 0$. But $v_{r'+j}h = v' + t'_{r'+j,j} v_j + \epsilon v_{r'+j}$, with $v' \in \mathcal{V}_{j-1}$. But $0 = f(v_{r'+j}, v_{r'+j}) = f(v_{r'+j}h, v_{r'+j}h) = 2\epsilon t'_{r'+j} f(v_j, v_{r'+j}) \neq 0$, a contradiction. Hence k is even. To prove (5ii), set $d = t'_{k,1}$. We claim that $t'_{n-1,k} = d$. Indeed, $0 = f(v_k, v_{n-1}) = f(v_k h, v_{n-1}h) = f(dv_1 + \epsilon v_k, t'_{n-1,1}v_1 + \cdots + t'_{n-1,k}v_k + \epsilon v_{n-1} + \rho v_n) = \epsilon d + (-1)^{k+1}\epsilon t'_{n-1,k}$, thus $t'_{n-1,k} = (-1)^k d = d$. Also the $(n-1, 1)$-entry of $(t')^2$ is d^2 and the remaining entries of $(t')^2$ are zero. Since $(h - \epsilon I_n)^2 = 0$, we must have (see the proof of (4)), $(t')^2 + EF = 0$, so

$d^2+\theta\rho=0$. But $\theta\rho=-\rho^2 f(v_n,v_n)$ (see (2)), so $d^2=\rho^2 f(v_n,v_n)$. Hence, $f(v_n,v_n)$ is a square in $\mathbb{F}$, so we may take $f(v_n,v_n)=1$. Then $d^2=\rho^2$, and since, by (2), $\theta=-\rho$, $d^2=\theta^2$.

Notation. For the remainder of this section, we fix the following notation. Let $\beta_1,\dots,\beta_{k-2},\gamma_1,\dots,\gamma_{k-2}\in\mathbb{F}^*$. Let also $\alpha,\beta\in\mathbb{F}^*$. We set $a=a_{k-1}(\beta_1,\dots,\beta_{k-2})$, $a_1=a_{k-1}(\gamma_1,\dots,\gamma_{k-2})$, $b=b_{k-1}(\beta_1,\dots,\beta_{k-2})$, $b_1=b_{k-1}(\gamma_1,\dots,\gamma_{k-2})$, $g=\operatorname{diag}(a,1,b^{-1})$, $g_1=\operatorname{diag}(a_1,1,b_1^{-1})$, $B=b_k(\alpha,\beta_1,\dots,\beta_{k-2})$, $B_1=b_k(\beta,\gamma_1,\dots,\gamma_{k-2})$, $u=u^{n-1}(\alpha,\frac{1}{2}\alpha^2)$, $w=u^{n-1}(\beta,\frac{1}{2}\beta^2)$ (notation as in 5.4.1), $\mathcal{X}=gu$ and $\mathcal{Y}=g_1w$. Finally, we let $X=\operatorname{diag}(\mathcal{X},1)$ and $Y=\operatorname{diag}(\mathcal{Y},1)$.

6.2. *Let $\epsilon'\in\{1,-1\}$, and $\mathcal{S}\in\{\mathcal{Y}^t,\mathcal{X}^{\epsilon'}\mathcal{Y}^t\}$. Set $S=\operatorname{diag}(\mathcal{S},1)$ and let $R\in\Delta^{\le 2}(X)\cap\Delta^{\le 1}(S)$. Then v_1 is characteristic vector of R.*

Proof. Let $h\in\Delta^{\le 1}(X)\cap\Delta^{\le 1}(R)$. Note that by 5.11.3, X satisfies the hypothesis for u in 6.1, there exists $\epsilon\in\{-1,1\}$ and $1\le r'<n-1$, such that

$$h-\epsilon I_n=\begin{bmatrix} t' & E\\ F & 0\end{bmatrix}$$

with $t'\in\mathcal{T}_{n-1}(r')$.

We'll show that there exists $i\in\{1,2\}$ such that if we set $T:=(h-\epsilon I_n)^i$, then T,S and R satisfy all the hypotheses of 1.15, for a suitable choice of j,m and ℓ. Then the lemma follows from 1.15. First, $R^{-1}TR=T$ and $[R,S]\in Z(L)$, so hypothesis (e) of 1.15 is satisfied. Note next that by 5.11.5:

(i) S satisfies hypothesis (a) of 1.15 for any $j\le k-2$.

We now distinguish two cases as follows.

Case 1. There exists $i\in\{1,2\}$ and $1\le r<n-1$, such that

$$(h-\epsilon I_n)^i=\begin{bmatrix} t & 0_{n-1,1}\\ 0_{1,n-1} & 0\end{bmatrix}\quad\text{where } t\in\mathcal{T}_{n-1}(r).$$

Let $T:=(h-\epsilon I_n)^i$, with i as above. Observe that $M_{n,n}(ST)=\mathcal{S}t$, hence we get from 5.11.6 (replacing k by $k-1$) that:

(ii) If $r\ge k-1$, then $v_{k-1}\notin\ker(ST)$ and $\mathcal{V}_{k-2}\subseteq\ker(ST)$.

Next observe that if $r>k-1$ (and (ii) necessarily holds), $n-r-1\le k-1$ and $\operatorname{im}(T)=\mathcal{V}_{n-r-1}$ is R-invariant. Thus:

(iii) If $r>k-1$, then $n-r-1\le k-1$ and $\mathcal{V}_{n-r-1}$ is R-invariant.

Hence if $r>k-1$, take $j=k-2$, $m=n-r-1$ and $\ell=1$ and, by (i), (ii) and (iii), all hypotheses of 1.15 are met, so we are done.

Next observe that if $r \leq k-1$, then $\ker(T) = \langle v_1, \dots, v_r, v_n\rangle$ and the radical of the form f, reduced to $\ker(T)$ is $\mathcal{V}_r$. Thus:

(iv) If $r \leq k-1$, then $\mathcal{V}_r$ is an R-invariant subspace and $v_{r+1} \notin \ker(T)$.

Thus if $r = k-1$, take $m = r$, $j = k-2$ and $\ell = 1$, and, by (i), (ii) and (iv) we are done, while if $r < k-1$, take $j = m = r$ and $\ell = 0$ and observe that by (i) and (iv) we are done.

Case 2. $r' = k-1$, $\rho \neq 0 \neq \theta$, $\nu = f(v_n, v_n) = 1$ and for $d = t'_{k,1}$, $d^2 = \theta^2$.

Note that by 6.1.4 and 6.1.5, either Case 1 holds or Case 2 holds. Let $T = X - \epsilon I_n$. Write $d = -\epsilon''\theta$, with $\epsilon'' \in \{1, -1\}$. Observe that $\ker(T) = \{v_1, \dots, v_{k-1}, v_n + \epsilon'' v_k\}$. First we claim that:

(v) There exists $v \in \mathcal{V}_{k-1}$ such that modulo $\mathcal{V}_{k-1}$, we have

$$v_k S^{-1} \equiv \eta v_k + \mu v_{k+1}, \quad \text{with } \eta \in \mathbb{F} \text{ and } \mu \in \mathbb{F}^*$$
$$\{(v_n + \epsilon'' v_k) - \epsilon'' v\} S^{-1} \equiv v_n - \epsilon'' v_k.$$

Indeed, we use 5.11.7. We take in 5.11, $n = 2k-1 = 2(k-1)+1$, α, β, and ρ (of 5.11) in the fixed field of σ_q (so $\rho^{1-q} = 1$). Thus, for all possibilities of $\mathcal{S}$ the following holds:

(vi) There exists $v \in \mathcal{V}_{k-1}$, $\eta \in \mathbb{F}$ and $\mu \in \mathbb{F}^*$ such that

$$v_k \mathcal{S}^{-1} \equiv \eta v_k + \mu v_{k+1} \pmod{\mathcal{V}_{k-1}}$$
$$v \mathcal{S}^{-1} \equiv (\eta+1) v_k + \mu v_{k+1} \pmod{\mathcal{V}_{k-1}}.$$

Where in all cases $\mu = -\beta$. If $\mathcal{S} = \mathcal{Y}^t$, $\eta = 1$, while

$$\text{if } \mathcal{S} = \mathcal{X}^{\epsilon'} \mathcal{Y}^t, \ \ \eta = 1 + \epsilon' \alpha\beta.$$

Thus, by (vi), modulo $\mathcal{V}_{k-1}$ we get that

$$\begin{aligned}
&\{(v_n + \epsilon'' v_k) - \epsilon'' v\} S^{-1} \\
&\equiv v_n + \epsilon''\{\eta v_k + \mu v_{k+1}\} - \epsilon''\{(\eta+1) v_k + \mu v_{k+1}\} \\
&\equiv v_n + \{\eta\epsilon'' - (\eta+1)\epsilon''\} v_k + (\mu\epsilon'' - \mu\epsilon'') v_{k+1} \\
&\equiv v_n - \epsilon'' v_k.
\end{aligned}$$

This shows (v).

Let v and ϵ'' be as in (v). Since $v, v_n + \epsilon'' v_k \in \ker(T)$, $\mathcal{U} := \langle v S^{-1}, (v_n + \epsilon'' v_k) S^{-1}\rangle \subseteq \ker(ST)$. Notice that (v) implies that $v_n - \epsilon'' v_k \in \mathcal{U} + \mathcal{V}_{k-1}$ and also that $v S^{-1} \equiv \mu v_{k+1} \pmod{\mathcal{V}_k}$ (μ as in (v)). Hence we conclude that $\mathcal{U} \cap \ker(T) = (0)$. Since $\dim(\mathcal{U}) = 2$, and since $\dim(\ker(T)) = k$, we get that $\dim(\ker(T) \cap \ker(ST)) \leq k-2$. But $\mathcal{V}_{k-2} \subseteq \ker(ST)$ and hence $\ker(T) \cap \ker(ST) = \mathcal{V}_{k-2}$. Clearly $\ker(T) \cap \ker(ST)$ is R-invariant, so we conclude that:

(vii) $\mathcal{V}_{k-2}$ is R-invariant.

Observe that (ii) holds here as well, since $M_{n,n}(ST) = \mathcal{S}t$, holds here as well. Hence if we take $m = k-2 = j$ and $\ell = 1$, we see that all hypotheses of 1.15 hold here as well and the proof of 6.2 is complete.

6.3. *Let $\epsilon \in \{1,-1\}$ and let $S \in \{Y^t, X^\epsilon Y^t\}$. Set $\mathcal{S} = M_{n,n}(S)$ and suppose $\langle \mathcal{O}(v_1, \mathcal{S})\rangle = \mathcal{V}_{n-1}$. Then $d_\Lambda(X,S) > 3$, where $\Lambda = \Delta(L)$.*

Proof. Let $R \in \Delta^{\le 2}(X) \cap \Delta^{\le 1}(S)$. By 6.2, v_1 is a characteristic vector of R and since $\langle \mathcal{O}(v_1, \mathcal{S})\rangle = \mathcal{V}_{n-1}$, $\mathcal{V}_{n-1}$ is an R-invariant subspace. Thus $\mathcal{V}_{n-1}^\perp = \langle v_n\rangle$ is R-invariant as well. Set $R_1 = M_{n,n}(R)$. Since $[R,S] \in Z(L)$, $[R_1, \mathcal{S}] = \pm I_{n-1}$ and since $\det([R_1,\mathcal{S}]) = 1$, $[R_1,\mathcal{S}] = I_{n-1}$. Thus $[R,S] = 1$, and since v_1 is a characteristic vector of R and $\langle \mathcal{O}(v_1, \mathcal{S})\rangle = \mathcal{V}_{n-1}$, $R_1 = \pm I_{n-1}$. Of course $R_{n,n} \in \{1,-1\}$ and since $\det(R) = 1$, $R \in Z(L)$, a contradiction.

Theorem 6.4. *$\Delta(L)$ is balanced.*

Proof. In 5.14.3 and 5.14.4, we showed that we can pick $\mathcal{X}, \mathcal{Y}$ such that for $\{\mathcal{T}, \mathcal{Z}\} = \{\mathcal{X}, \mathcal{Y}\}$, $\epsilon \in \{1,-1\}$ and $\mathcal{S} \in \{\mathcal{T}^t, \mathcal{T}^\epsilon \mathcal{Z}^t\}$, $\langle \mathcal{O}(v_1, \mathcal{S})\rangle = \mathcal{V}_{n-1}$. Hence the theorem follows from 6.3 and by definition.

7. The Orthogonal Groups in even dimension and even characteristic.

In this section $n = 2k \ge 8$ is even and $\mathbb{F}$ is a field of even order. We keep the notation of Section 1. In particular V is a vector space of dimension n over $\mathbb{F}$ and $\mathcal{B} = \{v_1, \dots, v_n\}$ is our fixed basis of V. Let f be the symplectic form on V whose matrix with respect to $\mathcal{B}$ is

$$J = \begin{bmatrix} 0 & 0 & \cdot & \cdot & \cdot & \cdot & 0 & 1 \\ 0 & 0 & \cdot & \cdot & \cdot & 0 & 1 & 0 \\ 0 & 0 & \cdot & \cdot & 0 & 1 & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 1 & 0 & \cdot & \cdot & \cdot & \cdot \\ 0 & 1 & 0 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \end{bmatrix}.$$

For $\epsilon \in \{+,-\}$ let Q^ϵ be the quadratic form on V defined as follows. First $Q^\epsilon(v+w) = Q^\epsilon(v) + Q^\epsilon(w) + f(v,w)$, for all $v, w \in V$. Second, $Q^\epsilon(v_i) = 0$, for all $1 \le i \le k-1$ and all $k+2 \le i \le n$. We define $Q^\epsilon(v_k) = Q^\epsilon(v_{k+1}) = \nu_\epsilon$, where $\nu_\epsilon = 0$, when $\epsilon = +$ and when $\epsilon = -$, $\nu_\epsilon \neq 0$, is such that $\nu_\epsilon\lambda^2 + \lambda + \nu_\epsilon$ is an irreducible polynomial in $\mathbb{F}[\lambda]$. Of course V is an orthogonal space of type ϵ in the respective cases. We let $Q = Q^\epsilon$. We denote by $Q^\epsilon(V,Q)$ the full orthogonal group of type $\epsilon \in \{+,-\}$ in the respective cases. We let L be the commutator subgroup of $O^\epsilon(V,Q)$. Thus L is a simple group and L has index 2 in $O^\epsilon(V,Q)$. The purpose of this section is to prove

Theorem 1.6 for L. For that we'll show that L is closed under transpose (see 1.4.3) and indicate an element $X \in L$ such that $B_\Lambda(X, X^t)$ holds, where $\Lambda = \Delta(L)$. Then, by 1.9.2, Λ is balanced. We'll define X shortly. The following Theorem is useful.

7.1. *Let $g \in O^\epsilon(V, Q)$. Then $g \in L$ if and only if $\dim C_V(g)$ is even.*

Proof. See [**3**], Theorem 3.

7.2. *L is closed under transpose.*

Proof. Regard J above as an element of $GL(V)$. Then J is an involution and $J^t = J$ (J is symmetric). We claim that $J \in Q^\epsilon(V, Q)$. Indeed $JJJ^t = J \in O(V, f)$ and since $v_iJ = v_{n+1-i}$, for all $1 \leq i \leq n$, J preserves the quadratic form Q, since in both types $Q(v_i) = Q(v_{n+1-i})$. But for $g \in L$, $g^t = Jg^{-1}J$, so $g^t \in L$.

Notation 7.3. (1) Let $g \in GL(V)$ such that $g = \operatorname{diag}(I_{k-2}, s, I_{k-2})$, where s is some 4×4 matrix. We denote s by $s(g)$.

(2) Throughtout this section $u := \operatorname{diag}(I_{k-2}, s, I_{k-2})$, where

$$s = s(u) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}.$$

(3) Throughout this section we let

$$g = \operatorname{diag}(a_k, b_k^{-1})$$
$$X = gu$$

where for $m \geq 1$, a_m and b_m are as in 1.1.9. Note that since $\operatorname{char}(\mathbb{F}) = 2$, $a_m = b_m$.

(4) We denote by $\mathcal{C}$, the ordered basis $(w_1 \dots, w_n)$, where $w_i = v_i$, for $1 \leq i \leq k-2$, $w_{k-1} = v_{k-1} + v_k + v_{k+1}$, $w_i = v_{i+2}$, for $k \leq i \leq n-2$, $w_{n-1} = v_k + v_{k+1}$ and $w_n = v_k + v_{k+2}$. Thus

$$\mathcal{C} = (v_1, v_2, \dots, v_{k-2}, v_{k-1} + v_k + v_{k+1}, v_{k+2}, \dots, v_n, v_k + v_{k+1}, v_k + v_{k+2}).$$

7.4. (1)

$$s(u) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \qquad (s(u))^t = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

(2) $u^{-1} = u$.

(3)

$$s(uu^t) = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

(4)

$$s((uu^t)^{-1}) = s(u^t u) = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}.$$

(5) $s(u^{-1}u^t) = s(uu^t)$ *and* $s((u^{-1}u^t)^{-1}) = s(u^t u)$.
(6) $[g^t, u] = 1$.

Proof. (1) is by definition. Clearly $u^{-1} = u$. For (3) and (4), we compute

$$s(uu^t) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

$$s((uu^t)^{-1}) = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}.$$

(5) follows from (2). For (6) we have, $v_i g^t u = v_i g^t = v_i u g^t$, for $i \notin \{k+1, k+2\}$. $v_{k+1} g^t u = (v_{k+1} + \cdots + v_n)u = v_{k-1} + v_k + \cdots + v_n$ and $v_{k+1} u g^t = (v_{k-1} + v_{k+1}) g^t = v_{k-1} + v_k + \cdots + v_n$. $v_{k+2} g^t u = (v_{k+2} + \cdots + v_n) u = v_k + v_{k+2} + \cdots + v_n$ and $v_{k+2} u g^t = (v_k + v_{k+2}) g^t = v_k + v_{k+2} + \cdots + v_n$.

7.5. (1)

$$X = \left[\begin{array}{cccccccccccccccc}
1 & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 & & & & & & & & \\
1 & 1 & 0 & \cdot & \cdot & \cdot & \cdot & 0 & & & & & & & & \\
0 & 1 & 1 & 0 & \cdot & \cdot & \cdot & 0 & & & & & & & & \\
0 & 0 & 1 & 1 & 0 & \cdot & \cdot & 0 & & & & & & & & \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & & & & & & & & \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & & & & & & & & \\
0 & \cdot & \cdot & \cdot & 0 & 1 & 1 & 0 & & & & & & & & \\
0 & \cdot & \cdot & \cdot & \cdot & 0 & 1 & 1 & & & & & & & & \\
 & & & & & & 1 & 0 & 1 & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\
 & & & & & & 1 & 1 & 1 & 1 & 0 & \cdot & \cdot & \cdot & \cdot & 0 \\
 & & & & & & 1 & 1 & 1 & 1 & 1 & 0 & \cdot & \cdot & \cdot & 0 \\
 & & & & & & 1 & 1 & 1 & 1 & 1 & 1 & 0 & \cdot & \cdot & 0 \\
 & & & & & & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
 & & & & & & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
 & & & & & & 1 & 1 & 1 & \cdot & \cdot & \cdot & \cdot & 1 & 1 & 0 \\
 & & & & & & 1 & 1 & 1 & \cdot & \cdot & \cdot & \cdot & 1 & 1 & 1
\end{array}\right]$$

where the blank spots are zeros. Also the upper submatrix of X is a $k \times k$ matrix and the lower submatrix of X is a $k \times (k+2)$ matrix.

(2) *The matrix of X with respect to the basis $\mathcal{C}$ is*

$$[X]_{\mathcal{C}} = \left[\begin{array}{cccccccccccccccc}
1 & 0 & \cdot & \cdot & \cdot & \cdot & 0 & & & & & & & & & \\
1 & 1 & 0 & \cdot & \cdot & \cdot & 0 & & & & & & & & & \\
0 & 1 & 1 & 0 & \cdot & \cdot & 0 & & & & & & & & & \\
0 & 0 & 1 & 1 & 0 & \cdot & 0 & & & & & & & & & \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & & & & & & & & & \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & & & & & & & & & \\
0 & \cdot & \cdot & 0 & 1 & 1 & 0 & & & & & & & & & \\
0 & \cdot & \cdot & \cdot & 0 & 1 & 1 & & & & & & & & & \\
 & & & & & & 1 & 1 & 0 & \cdot & \cdot & \cdot & \cdot & 0 & & \\
 & & & & & & 1 & 1 & 1 & 0 & \cdot & \cdot & \cdot & 0 & & \\
 & & & & & & 1 & 1 & 1 & 1 & 0 & \cdot & \cdot & 0 & & \\
 & & & & & & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & & \\
 & & & & & & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & & \\
 & & & & & & 1 & 1 & \cdot & \cdot & \cdot & \cdot & 1 & 0 & & \\
 & & & & & & 1 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & & \\
 & & & & & & & & & & & & & & 1 & 0 \\
 & & & & & & & & & & & & & & 1 & 1
\end{array}\right]$$

where the blank spots are zeros. Also the upper submatrix of $[X]_{\mathcal{C}}$ is a $(k-1) \times (k-1)$ matrix, the middle submatrix of $[X]_{\mathcal{C}}$ is a $(k-1) \times k$ matrix and of course the lower submatrix of $[X]_{\mathcal{C}}$ is a 2×2 matrix.

(3) $X \in L$.

Proof. (1) and (2) are easy calculations and we omit the details. Next, since $\mathcal{V}_{k-1}$ and $\langle v_{k+2}, \dots, v_n\rangle$ are totally singular subspaces (in both types), $Q(v_iX) = 0$, for $1 \le i \le k-1$. Also, for $k+2 \le i \le n$, $Q(v_iX) = Q(v_{k-1} + v_k + v_{k+1} + v_{k+2} + \cdots + v_i) = Q(v_{k-1} + v_k + v_{k+1} + v_{k+2}) = Q(v_{k-1} + v_{k+2}) + Q(v_k + v_{k+1}) = 1 + 1 = 0$. Further, for $s \in \{k, k+1\}$, $Q(v_sX) = Q(v_{k-1} + v_s) = Q(v_s)$.

We leave it for the reader to verify that $XJX^t = J$, so $X \in O(V, f)$. Since $C_V(X) = \langle v_1, v_k + v_{k+1}\rangle$, $X \in L$, by 7.1.

7.6. *Let B be the following $(k+1)\times(k+1)$ matrix*

$$B = \begin{bmatrix} 1 & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 1 & 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ 1 & 1 & 1 & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & 1 & 1 & 0 & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & 0 & 1 & 1 & 0 \\ 0 & \cdot & \cdot & \cdot & \cdot & 0 & 1 & 1 \end{bmatrix}.$$

Then:

(1)
$$B^{-1} = \begin{bmatrix} 1 & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 1 & 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ 1 & 1 & 1 & 0 & \cdot & \cdot & \cdot & 0 \\ 1 & 1 & 1 & 1 & 0 & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & 1 & \cdot & \cdot & \cdot & \cdot & 1 & 0 \\ 1 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & 1 \end{bmatrix}.$$

(2)
$$B^tB = \begin{bmatrix} 0 & 1 & 1 & 0 & \cdot & \cdot & \cdot & 0 \\ 1 & 0 & 1 & 0 & \cdot & \cdot & \cdot & 0 \\ 1 & 1 & 0 & 1 & 0 & \cdot & \cdot & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & 0 & 1 & 0 & 1 \\ 0 & \cdot & \cdot & \cdot & \cdot & 0 & 1 & 1 \end{bmatrix} \qquad B^tB^{-1} = \begin{bmatrix} 0 & 1 & 1 & 0 & \cdot & \cdot & \cdot & 0 \\ 1 & 0 & 1 & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & 0 & 1 & 0 & \cdot & \cdot & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdot & \cdot & \cdot & \cdot & 0 & 1 \\ 1 & 1 & \cdot & \cdot & \cdot & \cdot & 1 & 1 \end{bmatrix}.$$

Proof. (1) is easy to check. For (2), we compute

$$B^tB = \begin{bmatrix} 1 & 0 & 1 & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 1 & 1 & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & 1 & 1 & 0 & \cdot & \cdot & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdot & \cdot & \cdot & 0 & 1 & 1 \\ 0 & 0 & \cdot & \cdot & \cdot & \cdot & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 1 & 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ 1 & 1 & 1 & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & 1 & 1 & 0 & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & 0 & 1 & 1 & 0 \\ 0 & \cdot & \cdot & \cdot & \cdot & 0 & 1 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 1 & 1 & 0 & \cdot & \cdot & \cdot & 0 \\ 1 & 0 & 1 & 0 & \cdot & \cdot & \cdot & 0 \\ 1 & 1 & 0 & 1 & 0 & \cdot & \cdot & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & 0 & 1 & 0 & 1 \\ 0 & \cdot & \cdot & \cdot & \cdot & 0 & 1 & 1 \end{bmatrix},$$

$$B^tB^{-1} = \begin{bmatrix} 1 & 0 & 1 & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 1 & 1 & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & 1 & 1 & 0 & \cdot & \cdot & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdot & \cdot & \cdot & 0 & 1 & 1 \\ 0 & 0 & \cdot & \cdot & \cdot & \cdot & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 1 & 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ 1 & 1 & 1 & 0 & \cdot & \cdot & \cdot & 0 \\ 1 & 1 & 1 & 1 & 0 & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & 1 & \cdot & \cdot & \cdot & \cdot & 1 & 0 \\ 1 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 1 & 1 & 0 & \cdot & \cdot & \cdot & 0 \\ 1 & 0 & 1 & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & 0 & 1 & 0 & \cdot & \cdot & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdot & \cdot & \cdot & \cdot & 0 & 1 \\ 1 & 1 & \cdot & \cdot & \cdot & \cdot & 1 & 1 \end{bmatrix}.$$

7.7. *Set $a = a_{k-1}$ and $v = v_k + v_{k+1}$. Let B be as in 7.6 and let $\epsilon \in \{-1, 1\}$. Then:*

(1) $XX^t = guu^tg^t$, $(XX^t)^{-1} = (g^t)^{-1}(u^tu)g^{-1}$.
(2) $X^{-1}X^t = uu^tg^{-1}g^t$ *and* $(X^{-1}X^t)^{-1} = (g^t)^{-1}gu^tu$.
(3) $X = \begin{bmatrix} a & 0_{k-1,k+1} \\ E & B^{-1} \end{bmatrix}$ *with E some $(k+1) \times (k-1)$ matrix.*

(4) $X^\epsilon X^t = \begin{bmatrix} a^\epsilon a^t & R_{1,2} \\ R_{2,1} & R_{2,2} \end{bmatrix}$ $(X^\epsilon X^t)^{-1} = \begin{bmatrix} R'_{1,1} & R'_{1,2} \\ R'_{2,1} & B^t B^\epsilon \end{bmatrix}$ *with* $R'_{1,1}, R_{2,2}, R_{1,2}, R'_{1,2}, R_{2,1}, R'_{2,1}$ *some* $(k-1)\times(k-1)$, $(k+1)\times(k+1)$, $(k-1)\times(k+1)$, $(k-1)\times(k+1)$, $(k+1)\times(k-1)$, $(k+1)\times(k-1)$ *matrices respectively. Further, the first* $k-2$ *rows of* $R_{1,2}$ *are zero.*

(5) *Let* $S \in \{X^t, X^\epsilon X^t\}$. *Then for* $1 \le i \le k-2$, $v_i S = w + v_{i+1}$, *with* $w \in \mathcal{V}_i$. *In particular,* $\mathcal{V}_{k-1} \subseteq \langle \mathcal{O}(v_1, S)\rangle$.

(6) *Let* $S \in \{X^t, X^\epsilon X^t\}$. *Then* $v_{k-1}S = w + v_n$, *with* $w \in \mathcal{V}_{n-1}$.

(7)(7i) *Let* $S = X^t$, *then* $v_{k-1}S^{-1} = v_{k-1} + v_k + v_{k+1} + v_{k+2}$, $v_k S^{-1} = v_k + v_{k+2}$, *and* $v_{k+1}S^{-1} = v_{k+1} + v_{k+2}$.

(7ii) *Let* $S = XX^t$, *then* $v_{k-1}S^{-1} = v_{k+2}$, $v_k S^{-1} = v_{k+1} + v_{k+2}$, *and* $v_{k+1}S^{-1} = v_k + v_{k+2}$.

(7iii) *Let* $S = X^{-1}X^t$, *then* $v_{k-1}S^{-1} = v_{k-2} + v_{k+2}$, $v_k S^{-1} = v_{k+1} + v_{k+2}$, *and* $v_{k+1}S^{-1} = v_k + v_{k+2}$.

(8) $\langle \mathcal{O}(v_1, X^t)\rangle = \langle \mathcal{V}_{k-1}, v + v_{k+2}, v_{k+3}, \dots, v_n\rangle$. *Further if we set* $\mathcal{W} = \langle \mathcal{O}(v_1, X^t)\rangle$, *then* $\mathcal{W}^\perp = \langle v, v_{k-1} + v_k\rangle$, $vX^t = v$ *and* $(v_{k-1}+v_k)X^t = v + (v_{k-1} + v_k)$.

(9) *Let* $S = XX^t$. *Then:*

(9i) *If* $k \equiv 1$ *or* $2 \pmod 3$, *then*

$$\langle \mathcal{O}(v_1, S)\rangle = \langle \mathcal{V}_{k-1}, v, v_{k+2}, v_{k+3}, \dots, v_n\rangle.$$

(9ii) *If* $k \equiv 0 \pmod 3$, *then*

$$\langle \mathcal{O}(v_1, S)\rangle = \Big\langle \mathcal{V}_{k-1}, v_{k+2}, v + v_{k+3j}, v + v_{k+3j+1}, v_{k+3j+2}, v + v_n : 1 \le j \le \frac{1}{3}k - 1\Big\rangle.$$

Further, in (9ii), if we set $\mathcal{W} = \langle \mathcal{O}(v_1, S)\rangle$, *then* $\mathcal{W}^\perp = \langle v, v'\rangle$, *where*

$$v' = (v_1 + v_3) + (v_4 + v_6) + (v_7 + v_9) + \cdots + (v_{k-2} + v_k),$$

$vS = v$ *and* $v'S = v + v'$.

(10) *Let* $S = X^{-1}X^t$. *Then*

$$\langle \mathcal{O}(v_1, S)\rangle = \langle \mathcal{V}_{k-1}, v, v_{k+2}, v_{k+3}, \dots, v_n\rangle.$$

Proof. (1) is obvious, recalling (see 7.4.2) that $u^{-1} = u$. For (2), we have $X^{-1}X^t = u^{-1}g^{-1}u^t g^t$. By 7.4.6, $[g^{-1}, u^t] = 1$, and (2) follows. For (3), just observe that X is given in 7.5.

(4) follows from (3), except that we must show that the first $k-2$ rows of $R_{1,2}$ are zero. This will of course follow from (5). To show (5), let $1 \le i \le k-2$. Suppose first that $S = X^t$. Then $v_i S = v_i u^t g^t = v_i g^t = v_i + v_{i+1}$. Next $v_i u u^t = v_i$, so $v_i X^{-1}X^t = v_i g^{-1} g^t$. Also $v_i g \in \mathcal{V}_i$, so $v_i g(uu^t) = v_i g$ and $v_i XX^t = v_i g g^t$. We conclude that:

$$(*) \qquad \text{For } 1 \le i \le k-2,\ v_i X^\epsilon Y^t = v_i g^\epsilon g^t.$$

Note that a_k^ϵ is unipotent, lower triangular and a_k^t is upper triangular unipotent with $(a_k^t)_{i,j} = 0$, for $j > i+1$, and $(a_k^t)_{i,i+1} = 1$. This easily implies (5), for $S = X^\epsilon Y^t$.

To show (6), note that X is given in 7.5.1, so we have $v_{k-1}X^t = v_{k-1}+v_k+\cdots+v_n$. Next, $v_{k-1}XX^t = v_{k-1}guu^tg^t = (v_{k-2}+v_{k-1})uu^tg^t = (v_{k-2}+v_{k-1}+v_{k+1})g^t = v_{k-2}+v_k+v_{k+1}+\cdots+v_n$. Also $v_{k-1}X^{-1}X^t = v_{k-1}uu^tg^{-1}g^t = (v_{k-1}+v_{k+1})g^{-1}g^t = (v_1+\cdots+v_{k-1}+v_{k+1})g^t = v_1+v_k+v_{k+1}+\cdots+v_n$.

For (7) we compute $v_{k-1}(X^t)^{-1} = v_{k-1}(g^t)^{-1}(u^t)^{-1} = (v_{k-1}+v_k)u^t = v_{k-1}+v_k+v_{k+1}+v_{k+2}$. $v_k(X^t)^{-1} = v_k(g^t)^{-1}(u^t)^{-1} = v_ku^t = v_k+v_{k+2}$ and $v_{k+1}(X^t)^{-1} = v_{k+1}(g^t)^{-1}(u^t)^{-1} = (v_{k+1}+v_{k+2})u^t = v_{k+1}+v_{k+2}$. This shows (7i). For (7ii) and (7iii), we use (7i). We compute (using (7i)) that, for $\epsilon \in \{1,-1\}$, $v_{k-1}(X^\epsilon X^t)^{-1} = (v_{k-1}+v_k+v_{k+1}+v_{k+2})X^{-\epsilon}$. If $\epsilon = 1$, we get $(v_{k-1}+v_k+v_{k+1}+v_{k+2})u^{-1}g^{-1} = (v_{k+1}+v_{k+2})g^{-1} = v_{k+2}$. If $\epsilon = -1$, we get, $(v_{k-1}+v_k+v_{k+1}+v_{k+2})gu = (v_{k-2}+v_k+v_{k+2})u = v_{k-2}+v_{k+2}$.

Next, $v_k(X^\epsilon X^t)^{-1} = (v_k+v_{k+2})X^{-\epsilon}$. If $\epsilon = 1$, we get, $(v_k+v_{k+2})u^{-1}g^{-1} = v_{k+2}g^{-1} = v_{k+1}+v_{k+2}$. If $\epsilon = -1$, we get $(v_k+v_{k+2})gu = (v_{k-1}+v_k+v_{k+1}+v_{k+2})u = v_{k+1}+v_{k+2}$.

Finally, $v_{k+1}(X^\epsilon X^t)^{-1} = (v_{k+1}+v_{k+2})X^{-\epsilon}$. If $\epsilon = 1$, we get $(v_{k+1}+v_{k+2})u^{-1}g^{-1} = (v_{k-1}+v_k+v_{k+1}+v_{k+2})g^{-1} = v_k+v_{k+2}$. If $\epsilon = -1$, we get $(v_{k+1}+v_{k+2})gu = v_{k+2}u = v_k+v_{k+2}$. This completes the proof of (7).

For (8), let $\mathcal{W} = \langle \mathcal{O}(v_1, X^t)\rangle$. By (5), $\mathcal{V}_{k-1} \subseteq \mathcal{W}$. Next, by (7i), $v_{k-1}(X^t)^{-1} = v_{k-1}+v_k+v_{k+1}+v_{k+2}$. Hence

(i) $$v + v_{k+2} \in \mathcal{W}.$$

Using (3) and 7.6 and computing modulo $\mathcal{V}_{k-1}$, $(v+v_{k+2})(X^t)^{-1} \equiv v+v_{k+2}+v_{k+3}$. Hence

(ii) $$v_{k+3} \in \mathcal{W}.$$

Now, for $k+3 \le i \le n-1$, $v_i(X^t)^{-1} = v_i + v_{i+1}$. Hence, by (ii)

(iii) $$\langle v_{k+3}, \dots, v_n\rangle \subseteq \mathcal{W}.$$

Let $\mathcal{W}' = \langle \mathcal{V}_{k-1}, v+v_{k+2}, v_{k+3}, \dots, v_n\rangle$. The reader may easily verify that $\langle v, v_{k-1}+v_k\rangle^\perp = \mathcal{W}'$ and that $vX^t = v$. We compute that $(v_{k-1}+v_k)X^t = (v_{k-1}+v_k)u^tg^t = (v_{k-1}+v_k+v_{k+1}+v_{k+2})g^t = (v_{k-1}+v_k)g^t + (v_{k+1}+v_{k+2})g^t = v_{k-1}+v_{k+1} = v+v_{k-1}+v_k$. Hence $\langle v, v_{k-1}+v_k\rangle$ is S-invariant, and it follows that $\mathcal{W}'$ is S-invariant. It follows that $\mathcal{W} = \mathcal{W}'$ and (8) is proved.

For (9), let $S = XX^t$ and set $\mathcal{W} = \langle \mathcal{O}(v_1, S)\rangle$. By (5), $\mathcal{V}_{k-1} \subseteq \mathcal{W}$. Next, by (7ii), $v_{k-1}S^{-1} = v_{k+2}$. Hence

(i′) $$v_{k+2} \in \mathcal{W}.$$

Next, we mention that all our calculations are done modulo $\mathcal{V}_{k-1}$ and we use (4) and 7.6.2. We have $v_{k+2}S^{-1} \equiv v + v_{k+3}$. Thus

(ii′) $$v + v_{k+3} \in \mathcal{W}.$$

Now $vS^{-1} = v_kS^{-1} + v_{k+1}S^{-1} = v$, by (7ii). Thus

(iii′) $$vS^{-1} = v.$$

Next $(v + v_{k+3})S^{-1} \equiv v + v_{k+2} + v_{k+4}$, hence, by (i′) and (ii′)

(iv′) $$v + v_{k+4} \in \mathcal{W}.$$

By (ii′) and (iv′)

(v′) $$v_{k+3} + v_{k+4} \in \mathcal{W}.$$

Now if $k = 4$, then $(v+v_{k+2}+v_{k+4})S^{-1} \equiv v+v+v_{k+3}+v_{k+3}+v_{k+4} = v_{k+4}$, so $v_8 \in \mathcal{W}$. It is easy to check now that by (v′), (iv′) and (ii′), (9i) holds. So from now until the end of the proof of (9) we assume that $k \geq 5$.

Next $(v + v_{k+2} + v_{k+4})S^{-1} \equiv v + v + v_{k+3} + v_{k+3} + v_{k+5} = v_{k+5}$. Thus

(vi′) $$v_{k+5} \in \mathcal{W}.$$

Suppose $k = 5$. By the above we get that $\mathcal{V}_4 \cup \{v_7, v+v_9, v_8+v_9, v_{10}\} \subseteq \mathcal{W}$. Also, $v_{10}S^{-1} = v_9 + v_{10} \in \mathcal{W}$ and (9i) holds. So from now until the end of the proof of (9) we assume that $k \geq 6$.

Now $v_{k+5}S^{-1} \equiv v_{k+4}+v_{k+6} \in \mathcal{W}$, thus $v+v_{k+4}+v_{k+4}+v_{k+6} = v+v_{k+6} \in \mathcal{W}$, so by (ii′)

(vii′) $$v_{k+3} + v_{k+6} \in \mathcal{W}.$$

Now for $i \geq k + 3$, $(v_i + v_{i+3})S^{-1} \equiv (v_{i-1} + v_{i+2}) + (v_{i+1} + v_{i+4})$, since $v_{k+2} + v_{k+5} \in \mathcal{W}$, we conclude from (vii′) that:

(viii′) $$\text{For } k+2 \leq i \leq n-3,\ v_i + v_{i+3} \in \mathcal{W}.$$

Now $(v_{n-3} + v_n)S^{-1} \equiv (v_{n-4} + v_{n-1}) + (v_{n-2} + v_n)$, so from (viii′) we get

(ix′) $$v_{n-2} + v_n \in \mathcal{W}.$$

Note also that by (i′) and (viii′),

(x′) $$v_{k+j} \in \mathcal{W}, \text{ for all } 2 \leq j \leq k, \text{ such that } j \equiv 2 \pmod 3.$$

Thus, by (x′), if $k \equiv 2 \pmod 3$, $v_n \in \mathcal{W}$ and if $k \equiv 1 \pmod 3$, $v_{n-2} \in \mathcal{W}$. Thus, by (ix′), if $k \equiv 1$ or $2 \pmod 3$, $v_{n-2}, v_n \in \mathcal{W}$. It follows from (viii′) that:

(xi′) If $k \equiv 1$ or $2 \pmod 3$ then there exists $\nu \in \{0, 1\}$ such that
$$v_{k+j} \in \mathcal{W}, \text{ for all } 2 \leq j \leq k, \text{ such that } j \equiv \nu \pmod 3.$$

Since $v_{k+3} + v_{k+4} \in \mathcal{W}$, we get from (iv′), (x′), (xi′) and (viii′) that:

(xii′) If $k \equiv 1$ or $2 \pmod 3$, $\mathcal{W} \supseteq \langle \mathcal{V}_{k-1}, v_k + v_{k+1}, v_{k+2}, v_{k+3}, \dots, v_n \rangle$.

Notice that $v^\perp = \langle \mathcal{V}_{k-1}, v_k + v_{k+1}, v_{k+2}, v_{k+3}, \dots, v_n\rangle$ is S-invariant, as $vS = v$, so (9i) holds.

Suppose $k \equiv 0 \pmod 3$. We get from (ii′), (iv′) and (viii′), that

(xiii′) $\quad v + v_{k+j} \in \mathcal{W}$, for all $3 \le j \le k$ such that $j \equiv 0$ or $1 \pmod 3$.

This, together with (x′), shows that

$$\mathcal{W}' := \Big\langle \mathcal{V}_{k-1}, v_{k+2}, v + v_{k+3j}, \\ v + v_{k+3j+1}, v_{k+3j+2}, v + v_n : 1 \le j \le \frac{1}{3}k - 1\Big\rangle \subseteq \mathcal{W}.$$

It easy to check that $\langle v, v'\rangle^\perp = \mathcal{W}'$. We show that $v'S = v + v'$; this implies that $\langle v, v'\rangle$ is S-invariant, and hence $\mathcal{W}'$ is S-invariant, so (9ii) holds. We compute that

$$\begin{aligned} v'S &= \{(v_1 + v_3) + (v_4 + v_6) + (v_7 + v_9) + \dots + (v_{k-2} + v_k)\}guu^tg^t \\ &= \{(v_1 + v_2) + (v_4 + v_5) + (v_7 + v_8) + \dots + (v_{k-2} + v_{k-1}) + v_k\}uu^tg^t \\ &= \{(v_1 + v_2) + (v_4 + v_5) + \dots + (v_{k-2} + v_{k-1}) + v_k + v_{k+1} + v_{k+2}\}g^t \\ &= \{(v_1 + v_2) + (v_4 + v_5) + \dots + (v_{k-2} + v_{k-1}) + v_k\}g^t \\ &\quad + (v_{k+1} + v_{k+2})g^t \\ &= \{(v_1 + v_3) + (v_4 + v_6) + (v_7 + v_9) + \dots + (v_{k-5} + v_{k-3}) + v_{k-2}\} \\ &\quad + v_{k+1} \\ &= v + v'. \end{aligned}$$

We now turn to the proof of (10). Set $S = X^{-1}X^t$ and $\mathcal{W} = \langle \mathcal{O}(v_1, S)\rangle$. By (5), $\mathcal{V}_{k-1} \subseteq \mathcal{W}$. Next, by (7iii), $v_{k-1}S^{-1} = v_{k-2} + v_{k+2}$. Thus

(i″) $$v_{k+2} \in \mathcal{W}.$$

Next, for $k + 2 \le i \le n - 1$, $v_iS^{-1} \equiv v_{i+1}$. Hence, by (i″)

(ii″) $$v_i \in \mathcal{W}, \quad \text{for all} \quad k + 2 \le i \le n.$$

Also $v_nS^{-1} \equiv v + v_{k+2} + \dots + v_n$, so by (ii″)

(iii″) $$v \in \mathcal{W}.$$

Again, since $v^\perp = \langle \mathcal{V}_{k-1}, v, v_{k+2}, v_{k+3}, \dots, v_n\rangle$ and $vS = v$, (10) holds.

7.8. *Let $1 \ne h \in C_L(X)$. Write $H = [h]_{\mathcal{C}}$ and set $Z := [X]_{\mathcal{C}}$. Write $Z = \operatorname{diag}(Z_1, Z_2)$, with $Z_1 = M_{(n-1,n,)(n-1,n)}([X]_{\mathcal{C}})$, and $Z_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$. Then:*

(1) *h fixes $\langle w_1\rangle, \langle w_1, w_2\rangle, \dots, \langle w_1, \dots, w_{n-4}\rangle$.*
(2) *h fixes $\langle w_1, w_{n-1}\rangle$ and $\langle w_1, w_2, w_{n-1}, w_n\rangle$.*

(3) *H has the form*

$$H = \begin{bmatrix} R & E \\ F & P \end{bmatrix}$$

such that:

(3i) *$I_{n-2} \neq R$ is an $(n-2)\times(n-2)$ matrix commuting with $Z, P = \begin{bmatrix} 1 & 0 \\ \delta & 1 \end{bmatrix}$, with $\delta \in \{0,1\}$, E is an $(n-2)\times 2$ matrix whose first $n-4$ rows are zero, and $E_{n-3,2} = 0$. F is a $2\times(n-2)$ matrix whose last $n-4$ columns are zero and $F_{1,2} = 0$.*

(3ii) *$H_{i,i} = 1$, for all $1 \leq i \leq n$.*

(3iii) *We fix the notation $\alpha := E_{n-3,1}$, $\beta := E_{n-2,1}$, $\gamma := F_{2,1}$. We have $\alpha = E_{n-2,2} = F_{1,1} = F_{2,2}$.*

(4) *There exists $1 \leq r \leq n-3$, such that $R - I_{n-2} \in \mathcal{T}_{n-2}(r)$. We fix the letter r to denote this integer.*

(5)

$$(H - I_n)^2 = \begin{bmatrix} (R - I_{n-2})^2 + EF & E' \\ F' & 0_{2,2} \end{bmatrix}$$

such that $E'$is a $(n-2)\times 2$ matrix with $E'_{n-2,1} = \alpha(R_{n-2,n-3} + \delta)$ (δ as in (3i) and α as in (3iii)) and $E'_{ij} = 0$ otherwise, F' is a $2\times(n-2)$ matrix such that $F'_{2,1} = \alpha(R_{2,1} + \delta)$ and $F'_{ij} = 0$ otherwise. EF is an $(n-2)\times(n-2)$ matrix such that $(EF)_{n-3,1} = \alpha^2 = (EF)_{n-2,2}$, $(EF)_{n-2,1} = \alpha(\beta+\gamma)$ and $(EF)_{i,j} = 0$, otherwise.

Proof. First we mention that we think of h and H as the same linear operator, but they are distinct as matrices. The same remark holds for X and $[X]_{\mathcal{C}}$. It is easy to check that $\ker([X]_{\mathcal{C}} - I_n) = \langle w_1, w_{n-1}\rangle$, $\ker([X]_{\mathcal{C}} - I_n)^2 = \langle w_1, w_2, w_{n-1}, w_n\rangle$. Further, for $j \geq 2$, $\operatorname{im}([X]_{\mathcal{C}} - I_n)^j = \langle w_1, \dots, w_{n-j-2}\rangle$. Thus (1) and (2) clearly hold.

Next, by (1), the first $n-4$ rows of E are zero and by (2), the last $n-4$ columns of F are zero. Also, since $\langle w_1, w_{n-1}\rangle$ is h-invariant, $F_{1,2} = 0$. Next

$$ZH = \begin{bmatrix} Z_1 & 0 \\ 0 & Z_2 \end{bmatrix} \cdot \begin{bmatrix} R & E \\ F & P \end{bmatrix} = \begin{bmatrix} Z_1R & Z_1E \\ Z_2F & Z_2P \end{bmatrix}$$

$$HZ = \begin{bmatrix} R & E \\ F & P \end{bmatrix} \cdot \begin{bmatrix} Z_1 & 0 \\ 0 & Z_2 \end{bmatrix} = \begin{bmatrix} RZ_1 & EZ_2 \\ FZ_1 & PZ_2 \end{bmatrix}$$

so since $ZH = HZ$, R commutes with Z_1 and P commutes with Z_2. Thus $P = \begin{bmatrix} \rho & 0 \\ \mu & \rho \end{bmatrix}$. Now $(v_k + v_{k+1})h = F_{1,1}v_1 + \rho(v_k + v_{k+1})$. But $1 = Q(v_k + v_{k+1}) = Q((v_k + v_{k+1})h) = \rho^2$, so $\rho = 1$. Further, $(v_k + v_{k+1})h = F_{2,1}v_1 + F_{2,2}v_2 + \mu(v_k + v_{k+1}) + (v_k + v_{k+2})$. Hence $Q((v_k + v_{k+2})h) = \mu^2 + \nu_\epsilon + \mu$. It follows that $\nu_\epsilon = Q(v_k + v_{k+2}) = Q((v_k + v_{k+2})h) = \mu^2 + \nu_\epsilon + \mu$. Thus $\mu = 0$ or 1 and $P = \begin{bmatrix} 1 & 0 \\ \delta & 1 \end{bmatrix}$, with $\delta \in \{0,1\}$.

Next since R commutes with Z_1, 1.13 implies that, $H_{i,i} = R_{i,i} = R_{j,j} = H_{j,j}$, for all $1 \leq i, j \leq n-2$. Now

$$\begin{aligned} 1 = f(v_1, v_n) &= f(v_1 H, v_n H) \\ &= f(H_{1,1} v_1, H_{n-2,n-2} v_n) = H_{1,1} H_{n-2,n-2}. \end{aligned}$$

Since $H_{1,1} = H_{n-2,n-2}$, we see that $H_{1,1} = 1$. Since $H_{n-1,n-1} = P_{1,1} = 1$ and $H_{n,n} = P_{2,2} = 1$, we see that $H_{i,i} = 1$, for all $1 \leq i \leq n$. Now since R commutes with Z_1, 1.13 implies that $R - I_{n-2} \in \mathcal{T}_{n-2}(r)$, for some $1 \leq r \leq n-3$.

Let $\begin{bmatrix} \alpha & \rho \\ \beta & \mu \end{bmatrix}$ be the last two rows of E. Then the last two rows of $Z_1 E$ are $\begin{bmatrix} \alpha & \rho \\ \alpha+\beta & \rho+\mu \end{bmatrix}$ and the last two rows of EZ_2 are $\begin{bmatrix} \alpha+\rho & \rho \\ \beta+\mu & \mu \end{bmatrix}$. Since $Z_1 E = EZ_2$, $\rho = 0$ and $\alpha = \mu$. Thus:

$$\text{The last two rows of } E \text{ are } \begin{bmatrix} \alpha & 0 \\ \beta & \alpha \end{bmatrix}.$$

Next let $\begin{bmatrix} \rho & 0 \\ \gamma & \mu \end{bmatrix}$ be the first two columns of F. Then the first two columns of $Z_2 F$ are $\begin{bmatrix} \rho & 0 \\ \rho+\gamma & \mu \end{bmatrix}$ and the first two columns of FZ_1 are $\begin{bmatrix} \rho & 0 \\ \gamma+\mu & \mu \end{bmatrix}$. Thus $\rho = \mu$. Hence:

$$\text{The first two columns of } F \text{ are } \begin{bmatrix} \rho & 0 \\ \gamma & \rho \end{bmatrix}.$$

Next $(v_k + v_{k+1})H = \rho v_1 + v_k + v_{k+1}$ and observe that $v_n H = w + v_n + \alpha(v_k + v_{k+2})$, with $w \in \langle v_1, \dots, v_{k-1}, v_k + v_{k+1}, v_{k+2}, \dots, v_{n-1} \rangle \subseteq \langle v_1, v_k + v_{k+1} \rangle^{\perp}$. Thus $0 = f(v_k + v_{k+1}, v_n) = f((v_k + v_{k+1})h, v_n h) = f(\rho v_1 + (v_k + v_{k+1}), w + v_n + \alpha(v_k + v_{k+2})) = f(\rho v_1 + (v_k + v_{k+1}), v_n + \alpha(v_k + v_{k+2})) = \rho + \alpha$. Hence $\rho = \alpha$. This completes the proof of (3) and (4), except that we must show that $R \neq I_{n-2}$. Now if $R = I_{n-2}$, then, it follows that $0 = Q(v_{n-1}) = Q(v_{n-1} H) = Q(v_{n-1} + \alpha(v_k + v_{k+1})) = \alpha$. Also, since $0 = Q(v_n) = Q(v_n H)$, $\beta = 0$. Now δ (of (3i)) must be 0; so since $h \in L$, 7.1 implies that $h = I_n$, contradicting $h \neq I_n$.

To prove (5) note that

$$\begin{aligned} (H - I_n)^2 &= \begin{bmatrix} R - I_{n-2} & E \\ F & P - I_2 \end{bmatrix} \cdot \begin{bmatrix} R - I_{n-2} & E \\ F & P - I_2 \end{bmatrix} \\ &= \begin{bmatrix} (R - I_{n-2})^2 + EF & (R - I_{n-2})E + E(P - I_2) \\ F(R - I_{n-2}) + (P - I_2)F & FE + (P - I_2)^2 \end{bmatrix}. \end{aligned}$$

Now, since the last column of $(R - I_{n-2})$ is zero, $(R - I_{n-2})E$ is an $(n-2) \times 2$ matrix, whose $(n-2, 1)$-entry is $\alpha R_{n-2,n-3}$, and whose other entries are zero. Hence it is easy to check that $E' = (R - I_{n-2})E + E(P - I_2)$, is as claimed.

Next, since the first row of $(R - I_{n-2})$ is zero, $F(R - I_{n-2})$ is a $2 \times (n-2)$ matrix whose $(2,1)$-entry is $\alpha R_{2,1}$ and whose other entries are zero. Hence, it is easy to check that $F' = F(R - I_{n-2}) + (P - I_2)F$ is as claimed. Finally, $FE = 0_{2,2}$ and clearly $(P - I_2)^2 = 0_{2,2}$. It is easy to check that EF has the claimed shape and (5) is proved.

Before formulating the next lemma it is important that the reader will recall that for a linear operator a on our vector space V, $a_{i,j}$ is the (i,j)-entry of the matrix of a, *with respect to the basis* $\mathcal{B}$, unless otherwise specified (see the beginning of Chapter 1).

7.9. *Let* $1 \neq h \in C_L(X)$. *Set* $\mathbb{T} = h - I_n$. *Write* $H = [h]_{\mathcal{C}}$. *Let* $R, P, E, F, \delta, \alpha, \beta, \gamma$ *be as in 7.8.3 and* r *as in 7.8.4. Then:*

(1) *Suppose* $k - 1 \leq r \leq n - 3$. *Then, there exists* $i \in \{1, 2\}$ *such that for* $T := \mathbb{T}^i$, *we have:*
  (1a) $\mathcal{V}_{k-1} \subseteq \ker(T)$.
  (1b) *There exists* $1 \leq f \leq n$, *such that* $T_{s,f} = 0$, *for all* $1 \leq s \leq n-1$, *and* $T_{n,f} \neq 0$.
  Further, one of the following holds.
  (1c) $\alpha \neq \delta \neq 0$, $i = 2$, $f = k+1$ *and* $\operatorname{im} T = \langle v_1, \alpha v_2 + v_k + v_{k+1} \rangle$.
  (1d) $\alpha \neq 0 = \delta$, $i = 2$, $f = 2$ *and* $\operatorname{im} T = \langle v_1, v_2 \rangle$.
  (1e) $\alpha = 0 = \delta$, $i = 1$, $f = n - r - 2$ *and*

$$\operatorname{im} T = \langle v_1, v_2, \dots, v_{n-r-2}, v_k + v_{k+1} \rangle.$$

  (1f) $\alpha = 0 = \delta$, $i = 1$, $f = n - r - 2$ *and*

$$\operatorname{im}(T) = \langle v_1, v_2, \dots, v_{n-r-3}, v_{n-r-2} + \mu(v_k + v_{k+1}) \rangle, \quad \mu \in \mathbb{F}^*.$$

  (1g) $\alpha = 0 = \delta$, $i = 1$, $f = n - r - 2$ *and* $\operatorname{im} T = \mathcal{V}_{n-r-2}$.
  (1h) $\alpha = 0 = \delta$, $r = n - 3$, $i = 1$, $f = k + 1$ *and* $\operatorname{im} T = \langle v_1, v_k + v_{k+1} \rangle$.

(2) *Suppose* $r = k - 2$ $\alpha \neq 0 = \delta$. *Then either* $\mathbb{T}^2 \in \mathcal{T}_n(n - s)$, *for some* $s \in \{1, 2\}$, *or the following holds:*
  (2a) $\mathbb{T}^2 = 0$, $H_{k-1,1} = \alpha = H_{n-2,k-1}$, $\mathcal{V}_{k-1} \subseteq \ker \mathbb{T}$, *and*
  (2b) *For all* $S \in \{X^t, XX^t, X^{-1}X^t\}$, $\ker(S\mathbb{T}) \cap \ker \mathbb{T} = \mathcal{V}_{k-2}$.

(3) *Suppose* $1 \leq r < k - 1$, *but exclude the case of (2). Then one of the following holds:*
  (3a) $r = 1$, *and* $\mathbb{T}^{n-3} \in \mathcal{T}_n(n-1)$.
  (3b) $r > 1$, $\alpha \neq 0 \neq \delta$, *and* $\ker \mathbb{T} = \{v_1, \dots, v_r, \rho v_{r+1} + \mu(v_k + v_{k+1})\}$, *with* $\rho, \mu \in \mathbb{F}^*$.
  (3c) $r = k - 2$, $\alpha \neq 0 \neq \delta$, $H_{k-1,1} = \alpha$, *and* $\ker \mathbb{T} = \mathcal{V}_{k-1}$. *Further,* $\mathbb{T}_{s,k-1} = 0$, *for all* $1 \leq s \leq n - 1$, *and* $\mathbb{T}_{n,k-1} \neq 0$.
  (3d) $r = k - 2$, $\alpha \neq 0 \neq \delta$, $H_{k-1,1} = \alpha$, *and* $\operatorname{im} \mathbb{T}^2 = \langle v_1, v_k + v_{k+1} \rangle$.
  (3e) *There exists* $i \geq 1$ *and* $1 \leq m \leq k - 2$, *such that* $\operatorname{im} \mathbb{T}^i = \langle v_1, \dots, v_m \rangle$, $\mathcal{V}_{k-1} \subseteq \ker \mathbb{T}^i$ *and* $\mathbb{T}^i \in \mathcal{T}_n(n - m)$.

(3f) *There exists* $i \geq 1$*, such that* $\operatorname{im} \mathbb{T}^i = \langle v_1, \dots, v_{k-2}, v_{k-1}+v_k+v_{k+1}\rangle$ *and* $\mathcal{V}_{k-1} \subseteq \ker \mathbb{T}^i$*. Further,* $(\mathbb{T}^i)_{s,k-1} = 0$*, for all* $1 \leq s \leq n-1$*, and* $(\mathbb{T}^i)_{n,k-1} \neq 0$.

Proof. Assume the hypothesis of (1). Note that since $r \geq k-1$, $R_{2,1} = R_{n-2,n-3} = 0$. Notice also that $(R - I_{n-2})^2 = 0_{n-2,n-2}$. Suppose $\alpha \neq 0 \neq \delta$, then it is easy to verify, using 7.8.5, that (1c) holds. Similarly if $\alpha \neq 0 = \delta$, then by 7.8.5, $E' = 0_{n-2,2}$ (E' as in 7.8.5) and it is easy to verify using 7.8.5 that (1d) holds (both in the case when $\gamma = 0$ and in the case $\gamma \neq 0$). Hence we may assume that $\alpha = 0$.

We claim that:

(i) $$\text{If } r = n-3 \text{ then } \delta = 0.$$

For suppose $r = n-3$. Then $v_n H = R_{n-2,1}v_1 + v_n + \beta(v_k + v_{k+1})$. Hence $0 = Q(v_n) = Q(v_n H) = R_{n-2,1} + \beta^2$. Since by 7.8.3i, $R \neq I_{n-2}$, we get that $0 \neq R_{n-2,1} = \beta^2$. Also, $0 = f(v_n, v_k + v_{k+2}) = f(v_n H, (v_k + v_{k+2})H) = f(R_{n-2,1}v_1 + v_n + \beta(v_k + v_{k+1}), \gamma v_1 + \delta(v_k + v_{k+1}) + (v_k + v_{k+2})) = \gamma + \beta$. Hence $\gamma = \beta$. Now if $\delta = 1$, then we get that $\operatorname{im}(H - I_n) = \beta v_1 + (v_k + v_{k+1})$. But then $\dim C_V(h) = n-1$ is odd, this contradicts 7.1, since $h \in L$. So (i) holds. Further, if $r = n-3$, then, $v_n\mathbb{T} = \beta^2 v_1 + \beta(v_k + v_{k+1})$, $v_k\mathbb{T} = v_{k+1}\mathbb{T} = \beta v_1$ and $\ker \mathbb{T} = \langle \mathcal{V}_{k-1}, v_k + v_{k+1}, v_{k+2}, \dots, v_{n-1}\rangle$. Hence (1h) holds. So from now on we also assume that $k - 1 \leq r < n-3$.

Note that since $\alpha = 0$, $v_k + v_{k+1} \in \ker(H - I_n)$. Hence

(ii) $$v_k\mathbb{T} = v_{k+1}\mathbb{T}$$

also, $v_k = v_{k+2} + (v_k + v_{k+2})$, so $v_k(H - I_n) = v_{k+2}(H - I_n) + (v_k + v_{k+2})(H - I_n) = H_{k,1}v_1 + \gamma v_1 + \delta(v_k + v_{k+1})$. It follows from (ii) that since $k - 1 \leq r < n-3$,

(iii) $$\mathbb{T}_{k,n-r-2} = \mathbb{T}_{k+1,n-r-2} = 0.$$

Since $v_{k-1} + v_k + v_{k+1}$, $v_k + v_{k+1} \in \operatorname{Ker}(H - I_n)$, $v_{k-1} \in \operatorname{Ker}\mathbb{T}$, so since $\mathcal{V}_{k-2} \subseteq \operatorname{Ker}\mathbb{T}$, we get that $\mathcal{V}_{k-1} \subseteq \ker\mathbb{T}$, so (1a) holds. Also, since $R - I_{n-2} \in \mathcal{T}_{n-2}(r)$, and $\alpha = 0$, $v_i(H - I_n) = v_i(h - I_n) \in \mathcal{V}_{n-r-3}$, for $k+2 \leq i \leq n-1$. Thus $(h - I_n)_{i,n-r-2} = 0$, for $k+2 \leq i \leq n-1$. Finally, since $R - I_{n-2} \in \mathcal{T}_{n-2}(r)$, $H_{n-2,n-r-2} \neq 0$, so $(h - I_n)_{n,n-r-2} \neq 0$. We showed that:

(iv) If $\alpha = 0$, then $\mathbb{T}_{s,n-r-2} = 0$, for all $1 \leq s \leq n-1$, and $\mathbb{T}_{n,n-r-2} \neq 0$.

So (1b) holds for $f = n - r - 2$.

Suppose $\delta \neq 0$. We leave it for the reader to verify that $\operatorname{im}\mathbb{T} = \langle v_1, v_2, \dots, v_{n-r-2}, v_k + v_{k+1}\rangle$. Hence (1e) holds.

Suppose next that $\delta = 0 = \beta$, then either $r > k-1$, in which case $\operatorname{im}\mathbb{T} = \mathcal{V}_{n-r-2}$ and (1g) holds, or $r = k-1$, in which case (1f) holds, with $\mu = 1$.

Finally suppose $\delta = 0 \neq \beta$. If $r > k-1$, then (1f) holds, with $\mu = \beta/H_{n-2,n-r-2}$, and if $r = k-1$, then either (1g) holds (in case $H_{n-2,k-1} = \beta$), or (1f) holds (otherwise). This completes the proof of (1).

Assume the hypothesis of (2). Suppose first that $(H-I_n)^2 \neq 0$. Notice that since $\delta = 0$, 7.8.5 implies that

$$(H-I_n)^2 = \begin{bmatrix} (R-I_n)^2 + EF & 0_{n-2,2} \\ 0_{2,n-2} & 0_{2,2} \end{bmatrix}.$$

Also, since $r = k-2$, $(R-I_n)^2 \in \mathcal{T}_{n-2}(n-4)$. Notice further, that by 1.13.3, $R_{r+i,i} = R_{r+s,s}$, for all $1 \leq i, s \leq n-r-2$. Thus the $(n-3,1)$-entry and the $(n-2,2)$-entry of $(R-I_n)^2$ are both equal to $R^2_{r+1,1}$. Since $(EF)_{n-3,1} = (EF)_{n-2,2} = \alpha^2$, it is clear that $(h-I_n)^2 \in \mathcal{T}_n(n-s)$, for some $s \in \{1,2\}$.

Suppose next that $(H-I_n)^2 = 0$. Then, the above considerations imply that $R_{r+i,i} = \alpha$, for all $1 \leq i \leq n-r-2$. Note that $\mathcal{V}_{k-2} \subseteq \ker \mathbb{T}$. Also $v_{k-1}(H-I_n) = (v_{k-1}+v_k+v_{k+1})(H-I_n)+(v_k+v_{k+1})(H-I_n) = \alpha v_1+\alpha v_1 = 0$. So $v_{k-1} \in \ker \mathbb{T}$. Thus (2a) is proved.

Next note that $\dim(\operatorname{im}(H-I_n)) = \dim(\ker(H-I_n))$, so since $(H-I_n)^2 = 0$, $\operatorname{im}(H-I_n) = \ker(H-I_n)$. Also $v_n(H-I_n) = v' + R_{n-2,k-1}(v_{k-1}+v_k+v_{k+1})+\alpha v_{k+2}+\beta(v_k+v_{k+1})+\alpha(v_k+v_{k+2}) = v''+\alpha v_k+(R_{n-2,k-1}+\beta)(v_k+v_{k+1})$, with $v' \in \mathcal{V}_{k-2}$ and $v'' \in \mathcal{V}_{k-1}$. Hence

(v) $\quad v_n(H-I_n) \equiv \alpha v_k + (R_{n-2,k-1}+\beta)(v_k+v_{k+1}) (\operatorname{mod} \mathcal{V}_{k-1}).$

Since $\mathcal{V}_{k-1} \subseteq \ker(H-I_n)$, we get from (v) that

(vi) $\quad \rho v_k + \mu v_{k+1} \in \ker(H-I_n),\;$ for some $\mu, \rho \in \mathbb{F}$, with $\mu \neq \rho$.

Thus

(vii) $\quad \ker \mathbb{T} = \langle \mathcal{V}_{k-1}, \rho v_k + \mu v_{k+1} \rangle \quad \rho, \mu\;$ as in (vi).

For (2b), we'll show that if ρ, μ are as in (vi) and $S \in \{X^t, XX^t, X^{-1}X^t\}$, $\langle v_{k-1}S^{-1}, (\rho v_k+\mu v_{k+1})S^{-1}\rangle \cap \ker \mathbb{T} = (0)$. This easily implies $\ker \mathbb{T} \cap \ker S\mathbb{T}$ has dimension $\leq k-2$. Since, by (vii) and 7.7.5, $\mathcal{V}_{k-2} \subseteq \ker \mathbb{T} \cap \ker S\mathbb{T}$, (2b) follows. Let $v \in \langle v_{k-1}S^{-1}, (\rho v_k + \mu v_{k+1})S^{-1}\rangle$.

Suppose $S = X^t$. By 7.7.7i, $v = \theta_1 v_{k-1}S^{-1} + \theta_2(\rho v_k + \mu v_{k+1})S^{-1} = \theta_1(v_{k-1}+v_k+v_{k+1}+v_{k+2}) + \theta_2(\rho(v_k+v_{k+2})+\mu(v_{k+1}+v_{k+2})) = \theta_1 v_{k-1} + (\theta_1+\theta_2\rho)v_k + (\theta_1+\theta_2\mu)v_{k+1} + (\theta_1+\theta_2(\rho+\mu))v_{k+2}$. So if $v \in \ker \mathbb{T}$, then, by (vii), $\theta_1+\theta_2(\rho+\mu) = 0$. Thus, $\theta_1+\theta_2\rho = \theta_2\mu$ and $\theta_1+\theta_2\mu = \theta_2\rho$. It follows that $\theta_2\mu v_k+\theta_2\rho v_{k+1} \in \ker \mathbb{T}$. Hence, we may assume that $\theta_2\mu v_k+\theta_2\rho v_{k+1} = \rho v_k + \mu v_{k+1}$. Hence $\theta_2\mu+\rho = \theta_2\rho+\mu = 0$. This is possible only if $\rho = \mu$, a contradiction.

Suppose $S = XX^t$. Then, by 7.7.7ii, $v = \theta_1 v_{k-1}S^{-1} + \theta_2(\rho v_k+\mu v_{k+1})S^{-1} = \theta_1 v_{k+2} + \theta_2\{\rho(v_{k+1}+v_{k+2})+\mu(v_k+v_{k+2})\} = \theta_2\mu v_k + \theta_2\rho v_{k+1} + (\theta_1 + \theta_2(\rho+\mu))v_{k+2}$. So if $v \in \ker(h-I_n)$, then, by (vii), $\theta_1+\theta_2(\rho+\mu) = 0$ and $\theta_2\mu v_k + \theta_2\rho v_{k+1} \in \ker \mathbb{T}$, which we have seen to be impossible.

Suppose $S = X^{-1}X^t$. Then, by 7.7.7iii, $v = \theta_1 v_{k-1}S^{-1} + \theta_2(\rho v_k + \mu v_{k+1})S^{-1} = \theta_1(v_{k-2} + v_{k+2}) + \theta_2(\rho(v_{k+1} + v_{k+2}) + \mu(v_k + v_{k+2}))$ and as in the case $S = XX^t$, we get a contradiction. This completes the proof of (2).

Assume the hypothesis of (3).

Case 1. $r = 1$.

By 7.8.5, $(H - I_n)^2 = \begin{bmatrix} t & E' \\ F' & 0_{2,2} \end{bmatrix}$, with $t \in \mathcal{T}_{n-2}(2)$. Then, it is easy to verify that $(H - I_n)^3 = \begin{bmatrix} t' & 0 \\ 0 & 0_{2,2} \end{bmatrix}$, with $t' \in \mathcal{T}_{n-2}(3)$ and from that (3a) follows easily.

So from now on we assume that $r > 1$.

Case 2. $\alpha \neq 0 \neq \delta$.

If $r \neq k-2$, or $r = k-2$ and $H_{k-1,1} \neq \alpha$, then it is easily checked that (3b) holds. So suppose that $r = k - 2$, and $H_{k-1,1} = \alpha$. Then $v_{k-1}\mathbb{T} = (v_{k-1} + v_k + v_{k+1})\mathbb{T} + (v_k + v_{k+1})\mathbb{T} = \alpha v_1 + \alpha v_1 = 0$. So clearly $\ker \mathbb{T} = \mathcal{V}_{k-1}$. Also, for $k+2 \leq s \leq n-2$, $v_s\mathbb{T} \in \mathcal{V}_{k-2}$. Further, $(v_k + v_{k+2})\mathbb{T} = \gamma v_1 + \alpha v_2 + (v_k + v_{k+1})$ and $v_{k+2}\mathbb{T} = R_{k,1}v_1 + R_{k,2}v_2$. Since $v_k\mathbb{T} = v_{k+2}\mathbb{T} + (v_k + v_{k+2})\mathbb{T}$, we conclude that $\mathbb{T}_{k,k-1} = 0$. Also since $(v_k + v_{k+1})\mathbb{T} = \alpha v_1$, we see that $\mathbb{T}_{k+1,k-1} = 0$. Hence, we see that $\mathbb{T}_{s,k-1} = 0$, for all $1 \leq s \leq n-1$. Now $v_n\mathbb{T} = v' + R_{n-2,k-1}(v_{k-1} + v_k + v_{k+1}) + R_{n-2,k}v_{k+2} + \beta(v_k + v_{k+1}) + \alpha(v_k + v_{k+1})$, with $v' \in \mathcal{V}_{k-2}$. Hence, if $R_{n-2,k-1} \neq 0$, then $\mathbb{T}_{n,k-1} \neq 0$, and case (3c) holds. Finally, suppose $R_{n-2,k-1} = 0$. Then $v_n h = v_n H = v'' + v_n + \beta w_{n-1} + \alpha w_n$, with $v'' \in \langle \mathcal{V}_{k-2}, v_{k+2} \rangle$ and $w_n h = \gamma v_1 + \alpha v_2 + w_{n-1} + w_n$. Hence $0 = f(v_n, w_n) = f(v_n h, w_n h) = \gamma + \beta + \alpha$. Hence $\beta + \gamma = \alpha$. Also, $v_{k+2}h = R_{k,1}v_1 + R_{k,2}v_2 + v_{k+2}$. Hence, $0 = f(v_{k+2}, v_n) = f(v_{k+2}h, v_n h) = R_{k,1}$. So $R_{k,1} = 0$. Since $\beta + \gamma = \alpha$, 7.8.5 yields $(EF)_{n-2,1} = \alpha^2$. Then, since $R_{k,1} = R_{n-2,k-1} = 0$ and $R_{k-1,1} = R_{n-2,k} = \alpha$ (see 1.13.3), we get, using 7.8.5, that $(R - I_{n-2})^2 + EF \in \mathcal{T}_{n-2}(n-3)$. Now using 7.8.5, it is easy to check that (3d) holds.

Case 3. $\alpha \neq 0 = \delta$ and $r \neq k-2$; or $\alpha = 0$.

Using 7.8.5 we get that

$$(H - I_n)^2 = \begin{bmatrix} (R - I_n)^2 + EF & 0_{n-2,2} \\ 0_{2,n-2} & 0_{2,2} \end{bmatrix}.$$

Now if $\alpha = 0$, $EF = 0$, while if $\alpha \neq 0 = \delta$, and $r \neq k-2$, then $(R - I_n)^2 + EF \in \mathcal{T}_{n-2}(r')$, for some $1 \leq r' < n-2$. Thus in either case

$$(H - I_n)^2 = \begin{bmatrix} t & 0_{n-2,2} \\ 0_{2,n-2} & 0_{2,2} \end{bmatrix}$$

with $t \in \mathcal{T}_{n-2}(r')$, for some $1 \leq r' < n-2$. It follows that for some i,

$$(H - I_n)^i = \begin{bmatrix} t' & 0_{n-2,2} \\ 0_{2,n-2} & 0_{2,2} \end{bmatrix}$$

with $t' \in \mathcal{T}_{n-2}(r'')$, for some $k-1 \le r'' < n-2$. If $r'' > k-1$, we get case (3e). So suppose $r'' = k-1$. Clearly, $\operatorname{im} \mathbb{T}^i = \langle v_1, \dots, v_{k-2}, v_{k-1}+v_k+v_{k+1}\rangle$ and $\mathcal{V}_{k-1} \subseteq \ker \mathbb{T}^i$. So, to establish (3f), it remains to show that $(\mathbb{T}^i)_{s,k-1} = 0$, for all $1 \le s \le n-1$, and $(\mathbb{T}^i)_{n,k-1} \neq 0$. Now for $k+2 \le s \le n-1$, $v_s(H-I_n)^i \in \mathcal{V}_{k-2}$, so $(\mathbb{T}^i)_{s,k-1} = 0$. Further since $(v_k + v_{k+1})\mathbb{T}^i = (v_k + v_{k+2})\mathbb{T}^i = 0$, $v_k\mathbb{T}^i = v_{k+1}\mathbb{T}^i = v_{k+2}\mathbb{T}^i \in \langle v_1\rangle$. Hence $(\mathbb{T}^i)_{k,k-1} = (\mathbb{T}^i)_{k+1,k-1} = 0$. Finally, since $t' \in \mathcal{T}_{n-2}(k-1)$, $(\mathbb{T}^i)_{n,k-1} \neq 0$. Thus, (3f) holds.

7.10. *Let $\epsilon \in \{-1, 1\}$ and let $S \in \{X^t, X^\epsilon X^t\}$. Let $R \in C_L(S)$ and suppose v_1 is a characteristic vector of R. Then $R = 1$.*

Proof. Set $\mathcal{W} = \langle \mathcal{O}(v_1, S)\rangle$. Using, 7.7.8, 7.7.9 and 7.7.10, it is clear that $\mathcal{W}$ is nonsingular (in all cases) and hence R centralizes $\mathcal{W}$. Set $v = v_k + v_{k+1}$.

Suppose first that $S = X^t$. Then, by 7.7.8, $\mathcal{W}^\perp = \langle v, v'\rangle$, with $v' = v_{k-1} + v_k$, $vS = v$ and $v'S = v + v'$. Clearly $\mathcal{W}^\perp$ is R-invariant and since $R \in C_L(S)$, $vR = \alpha v$ and $v'R = \beta v + \alpha v'$. Since $Q(v) = 1$, $\alpha = 1$. Hence R centralizes $\langle \mathcal{W}, v\rangle$ of dimension $n-1$. Thus, by 7.1 (and since $\det(R) = 1$), $R = 1$.

Suppose next that $S = XX^t$ and that $k \equiv 0 \pmod 3$. Then using 7.7.9 and arguing exactly as in previous paragraph we get $R = 1$.

Finally suppose $S = XX^t$ and $k \not\equiv 0 \pmod 3$, or $S = X^{-1}X^t$. By 7.7.9 and 7.7.10, $\dim(\mathcal{W}) = n-1$, so by 7.1, $R = 1$.

7.11. *Let $\epsilon \in \{1, -1\}$ and let $S \in \{X^t, X^\epsilon X^t\}$. Suppose $R \in \Delta^{\le 2}(X) \cap \Delta^{\le 1}(S)$. Then v_1 is a characteristic vector of R.*

Proof. Let $h \in \Delta^{\le 1}(X) \cap \Delta^{\le 1}(R)$. We'll show that there exists $i \ge 1$, such that if we set $T = (h - I_n)^i$, then there are integers $j, m, \ell \ge 0$ such that all the hypotheses of 1.15 are satisfied for S, T and R. The lemma will follow from 1.15. We'll use 7.9, so we adopt the notation of 7.9. For a subspace $\mathcal{W} \subseteq V$, let $\mathfrak{S}(\mathcal{W}) = \langle w \in \mathcal{W} : Q(w) = 0\rangle$ (the singular vectors of $\mathcal{W}$).

Case 1. $k-1 \le r \le n-3$.

In each case (1c)-(1h) of 7.9.1 we pick i as defined in these cases. We take $j = k-2$, in all cases. Notice that by 7.7.5, hypothesis (a) of 1.15 is satisfied. We let $m = \dim\{\mathfrak{S}(\operatorname{im} T)\}$ and $\ell = 1$. Using 7.7.6 and (1b) of 7.9.1, we get hypothesis (c) of 1.15. The remaining hypotheses of 1.15 are readily verified using 7.9.1.

Case 2. $r = k-2$ and $\alpha \neq 0 = \delta$.

In this case, if $(h - I_n)^2 \in \mathcal{T}_n(n-s)$, for some $s \in \{1, 2\}$, we take $i = 2$, $m = s$, $j = k-2$ and $\ell = 1$. Otherwise we take $i = 1$, $j = k-2 = m$ and $\ell = 1$. Using 7.9.2, we see that the hypotheses of 1.15 are satisfied.

Case 3. $1 \le r < k-1$, but Case 2 does not occur.

If case 7.9.3a holds, take $i = n-3$ and $m = 1$, to get the lemma trivially. If case 7.9.3b holds, take $i = 1$, $j = m = \dim(\mathfrak{S}(\ker T))$ and $\ell = 0$. If case 7.9.3c holds, take $i = 1$, $j = k-2$, $m = k-1$ and $\ell = 1$. Notice again that by 7.7.6, hypothesis (c) of 1.15 holds. If case 7.9.3d holds, then $\mathfrak{S}(\operatorname{im}(h-I_n)^2) = \langle v_1\rangle$ and trivially, $\langle v_1\rangle$ is R-invariant. If case 7.9.3e holds, take i as in 7.9.3e, $j = k-2$, m as in 7.9.3e and $\ell = 1$. If case 7.9.3f holds, take i as in 7.9.3f, $j = k-2$, $m = \dim\{\mathfrak{S}(\operatorname{im}(T)\} = k-2$, and $\ell = 1$. Using 7.7.6, the hypotheses of 1.15 are readily verified in cases 7.9.3e and 7.9.3f and the proof of 7.11 is complete.

7.12. *Let $\Lambda = \Delta(L)$, $\epsilon \in \{1, -1\}$ and let $S \in \{X^t, X^\epsilon X^t\}$. Then $d_\Lambda(X, S) \geq 4$.*

Proof. Suppose $d_\Lambda(X, S) \leq 3$ and let $R \in \Delta^{\leq 2}(X) \cap \Delta^{\leq 1}(S)$. By 7.11, v_1 is a characteristic vector of R and by 7.10, $R = 1$, a contradiction.

Theorem 7.13. *$\Delta(L)$ is balanced.*

Proof. Let $\Lambda = \Delta(L)$. Note that 7.12 implies that $B_\Lambda(X, X^t)$ and by 1.9, $B_\Lambda(X^t, X)$, so Λ is balanced.

Chapter 2. The Exceptional Groups of Lie type.

In Section 8 we prove that for all exceptional groups of Lie type L excluding $E_7(q)$, the commuting graph $\Delta(L)$ is disconnected (Theorem 8.8). In Section 9 we prove that if $L \cong E_7(q)$, then $\Delta(L)$ is balanced (see 1.3.2).

8. The Exceptional Groups excluding $E_7(q)$.

In this section L is a finite exceptional group of Lie type, excluding $E_7(q)$. We take $L = G_\sigma$, where G is a simply connected simple algebraic group and σ is a Frobenius morphism. Hence L is one of the following groups: ${}^2B_2(2^{2m+1})$, $G_2(q)$, ${}^2G_2(3^{2m+1})$, ${}^3D_4(q)$, $F_4(q)$, ${}^2F_4(2^{2m+1})$, $E_6(q)$, ${}^2E_6(q)$, $E_8(q)$. We exclude certain small cases where L is either solvable or L' is of classical type. So we exclude ${}^2B_2(2)$, $G_2(2)$,${}^2G_2(3)$. The remaining groups are all quasisimple, with the exception of ${}^2F_4(2)$, which has derived group of index 2. We let $L^* = L/Z(L)$. Of course $Z(L) = 1$, except when $L \cong E_6(q)$, in which case $|Z(L)| = (3, q-1)$, and when $L \cong {}^2E_6(q)$, in which case $|Z(L)| = (3, q+1)$.

8.1. *Assume G is a simply connected simple algebraic group and σ is a Frobenius morphism with quasisimple fixed point group G_σ. Let T be a σ invariant maximal torus. Suppose $s \in T_\sigma$ is an element such that $s \notin S_\sigma$, for any σ-invariant maximal torus S, such that $|S_\sigma| \neq |T_\sigma|$. Then $C_{G_\sigma}(s) = T_\sigma$.*

Proof. It will suffice to show that $C_G(s) = T$. As G is simply connected, $C_G(s) = C_G(s)^0$ ([**1**, II, 3.9]) and this is a reductive group. Write $C_G(s) = DZ$, where $Z = Z(C_G(s))^0$ and $D = C_G(s)'$. Thus D is a semisimple group. Note that $T \leq C_G(s)$ and that s is contained in all maximal tori of $C_G(s)$ (as maximal tori are self centralizing).

If $D = 1$, then $C_G(s) = T$, as required. Suppose this is not the case and let $\{D_1, \ldots, D_r\}$ be an orbit of $\langle\sigma\rangle$ on simple components of D. Then σ^r induces a Frobenius morphism on each D_i. By [**1**, I, 2.9], this Frobenius morphism normalizes a maximal torus contained in an invariant Borel of D_1. Taking images under powers of σ we get a maximal torus of each D_i with the same properties.

For the moment exclude the case where $p = 2$ and $D_i = B_2, C_2$. Then σ^r acts on the various root systems, stabilizing the positive roots, and fixing the root of highest height and its negative. Hence for each i, σ^r normalizes J_i, the fundamental SL_2 generated by the corresponding root subgroups. Also σ normalizes $J_1 \cdots J_r$. The centralizer in $C_G(s)$ of this group is also σ-stable and so contains a σ-stable maximal torus, say E.

There are two classes of σ-invariant maximal tori in $J_1 \cdots J_r$. These correspond to maximal tori in the fixed point group (of type $A_1(q^r)$ of order $q^r + 1$ and $q^r - 1$). Hence there are two classes of σ-invariant maximal tori of $(J_1 \cdots J_r)E$ whose fixed points in $J_1 \cdots J_r$ have order $q^r + 1$ and $q^r - 1$. A representative of one of these tori, say $\bar{T}$ has fixed points of order different than that of T_σ, however, by earlier remarks, $s \in \bar{T}_\sigma$, contradicting the hypothesis.

Finally consider the case $p = 2$, and $D_i = B_2, C_2$. This is only possible when $G = F_4$. There cannot be more than one such simple component in D, since the product of two has trivial centralizer, so cannot lie in $C_G(s)$. Thus D_1 is σ-invariant and we can use the same argument unless $(D_1)_\sigma = Sz(q)$. Here too there are at least two classes of maximal tori, so we can proceed as above.

Corollary 8.2. *Let G be a simple connected simple algebraic group and let σ be a Frobenius morphism of G such that $G_\sigma = L$. Let T be a σ-invariant torus and assume:*

(a) *If $S \leq G$ is a σ-invariant maximal torus such that $|S_\sigma| \neq |T_\sigma|$, then $(|T_\sigma|, |S_\sigma|) = |Z(L)|$.*
(b) *$(|T_\sigma : Z(L)|, |Z(L)|) = 1$.*

Let T^*_σ be the image of T_σ in L^*. Then $T^*_\sigma - \{1\}$ is a component of $\Delta(L^*)$.

Proof. We'll show that $C_{L^*}(s) = T^*_\sigma$, for every $1 \neq s^* \in T^*_\sigma$. Let $s \in T_\sigma - Z(L)$. We claim that $s \notin S_\sigma$, for every σ-invariant maximal torus S of G, such that $|S_\sigma| \neq |T_\sigma|$. Indeed, since $s \in T_\sigma - Z(L)$, (b) implies that

$|s| \nmid |Z(L)|$, where $|s|$ is the order of s. However, if $s \in S_\sigma$, for some σ-invariant maximal torus S of G, then $|s|$ divides $(|T_\sigma|, |S_\sigma|)$. Hence, by (a), $|S_\sigma| = |T_\sigma|$.

By 8.1, $C_L(s) = T_\sigma$. Hence, from (b) we get that $C_{L^*}(s^*) = T^*_\sigma$.

Notation and definitions. We denote by $\Phi_n(x)$, the n-th cyclotomic polynomial (of degree $\phi(n)$). Given a prime p and an integer b, the *p-share* of b is the largest power of p dividing b.

8.3. *Let $n, a \geq 2$ and let p be a prime. When $(a, p) = 1$, denote by $d_p(a)$ the order of a mod p. Then:*

(1) *$p \mid \Phi_n(a)$ iff $(a, p) = 1$, and $n = p^e d_p(a)$, for some $e \geq 0$.*
(2) *If $n \geq 3$, and $p \mid \Phi_n(a)$, then either $n = d_p(a)$, or the p-share of $\Phi_n(a)$ is p.*

Proof. This is well-known, see, e.g., [**9**, p. 27].

Corollary 8.4. *Let r be a prime, q a positive power of r and $2 \leq m < n$. Then:*

(1) *If $m \nmid n$ or if $\frac{n}{m}$ is not a prime power, then $(\Phi_n(q), \Phi_m(q)) = 1$.*
(2) *If $\frac{n}{m} = p^f$, with $r \neq p$ a prime and $f \geq 1$, then $(\Phi_n(q), \Phi_m(q)) = p^t$, with $t \geq 0$.*

Proof. Let p be a prime such that $p \mid (\Phi_n(q), \Phi_m(q))$. By 8.3.1, $p \neq r$, $m = p^{e_1} d_p(q)$ and $n = p^{e_2} d_p(q)$. Thus $m \mid n$ and $\frac{n}{m} = p^{e_2 - e_1}$. This shows (1). It also shows (2), since, we just saw that there can be at most one prime dividing $(\Phi_n(q), \Phi_m(q))$.

In the following lemma we list the cyclotomic polynomials of degree ≤ 8. These are the relevant cyclotomic polynomials in calculating the order of maximal tori in exceptional groups of Lie type.

8.5. *The cyclotomic polynomials of degree ≤ 8 are given in the following table.*

The degree	*The cyclotomic polynomials*
1	$\Phi_1(x) = x - 1, \quad \Phi_2(x) = x + 1.$
2	$\Phi_3(x), \quad \Phi_4(x) = x^2 + 1, \quad \Phi_6(x) = x^2 - x + 1.$
4	$\Phi_5(x), \quad \Phi_8(x) = x^4 + 1, \quad \Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1,$ $\Phi_{12}(x) = x^4 - x^2 + 1.$
6	$\Phi_7(x), \quad \Phi_9(x) = x^6 + x^3 + 1,$ $\Phi_{14}(x) = x^6 - x^5 + x^4 - x^3 + x^2 - x + 1,$ $\Phi_{18}(x) = x^6 - x^3 + 1.$
8	$\Phi_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1, \quad \Phi_{16}(x) = x^8 + 1,$ $\Phi_{20}(x) = x^8 - x^6 + x^4 - x^2 + 1, \quad \Phi_{24}(x) = x^8 - x^4 + 1,$ $\Phi_{30} = x^8 + x^7 - x^5 - x^4 - x^3 + x + 1.$

Proof. The degree of $\Phi_n(x)$ is $\phi(n) = \prod_{i=1}^k p_i^{m_i-1}(p_i - 1)$, where $n = \prod_{i=1}^k p_i^{m_i}$ and it is easy to calculate the table.

Corollary 8.6. *Let q be a positive power of a prime r. Then:*

(1) $(\Phi_{12}(q), f(q)) = 1$, *for any cyclotomic polynomial $f(x)$ of degree ≤ 4 distinct from $\Phi_{12}(x)$.*

(2) *Let $f(x)$ be a cyclotomic polynomial of degree ≤ 6, distinct from $\Phi_9(x)$. Then:*
   (i) *If $f(x) \notin \{\Phi_1(x), \Phi_3(x)\}$, then $(\Phi_9(q), f(q)) = 1$.*
   (ii) *The 3-share of $\Phi_9(q)$ is $(3, q-1)$.*
   (iii) *If $f(x) \in \{\Phi_1(x), \Phi_3(x)\}$, then $(\Phi_9(q), f(q)) = (3, q-1)$.*

(3) *Let $f(x)$ be a cyclotomic polynomial of degree ≤ 6, distinct from $\Phi_{18}(x)$. Then:*
   (i) *If $f(x) \notin \{\Phi_2(x), \Phi_6(x)\}$, then $(\Phi_{18}(q), f(q)) = 1$.*
   (ii) *The 3-share of $\Phi_{18}(q)$ is $(3, q+1)$.*
   (iii) *If $f(x) \in \{\Phi_2(x), \Phi_6(x)\}$, then $(\Phi_{18}(q), f(q)) = (3, q+1)$.*

(4) $(\Phi_{30}(q), f(q)) = 1$, *for any cyclotomic polynomial $f(x)$, of degree ≤ 8, distinct from $\Phi_{30}(x)$.*

(5) *Let $f(x)$ be a cyclotomic polynomial of degree ≤ 6, distinct from $\Phi_{14}(x)$. Then:*
   (i) *If $f(x) \neq \Phi_2(x)$, then $(\Phi_{14}(q), f(q)) = 1$.*
   (ii) $(\Phi_{14}(q), \Phi_2(q)) = (q+1, 7)$.

(6) *Let $f(x)$ be a cyclotomic polynomial of degree ≤ 6, distinct from $\Phi_7(x)$. Then:*
   (i) *If $f(x) \neq x - 1$, then $(\Phi_7(q), f(q)) = 1$.*
   (ii) $(\Phi_7(q), q-1) = (q-1, 7)$.

Proof. (1): We have $\Phi_{12}(x) = x^4 - x^2 + 1$, hence clearly $(\Phi_{12}(q), \Phi_1(q)) = 1$. Let $\Phi_{12}(x) \neq f(x)$ be a cyclotomic polynomial of degree ≤ 4. Note that $\Phi_{12}(q)$ is odd and $\Phi_{12}(q) \equiv 1 \pmod 3$. Now, by 8.5, $f(x) = \Phi_m(x)$, with $m < 12$, so (1) follows from 8.4.

(2): Next $\Phi_9(x) = q^6 + q^3 + 1$. Let $\Phi_9(x) \neq f(x)$ be a cyclotomic polynomial of degree ≤ 6. Since $\Phi_9(q)$ is odd, 8.4 implies that $(\Phi_9(q), \Phi_{18}(q)) = 1$. Now, by 8.5 and 8.4, $(\Phi_9(q), f(q)) = 1$, except when $q \equiv 1 \pmod 3$ and $f(x) = \Phi_1(x)$ or $\Phi_3(x)$, in which case $(\Phi_9(q), f(q)) = 3^t$, for some $t \geq 1$. Suppose $q \equiv 1 \pmod 3$, then $d_3(q) = 1$, so by 8.3.2, the 3-share of $\Phi_9(q)$ is 3 and (2) follows.

(3): Next, $\Phi_{18}(x) = x^6 - x^3 + 1$. We already observed that $(\Phi_{18}(q), \Phi_9(q)) = 1$. Let $\Phi_{18}(x) \neq f(x)$ be a cyclotomic polynomial of degree ≤ 6. Notice that $(\Phi_{18}(q), \Phi_1(q)) = 1$. Since $\Phi_{18}(q)$ is odd, 8.5 and 8.4 imply that, $(\Phi_{18}(q), f(q)) = 1$, except when $f(x) = \Phi_2(x)$ or $\Phi_6(x)$ and $q \equiv -1 \pmod 3$, in which case $(\Phi_{18}(q), f(q)) = 3^t$, for some $t \geq 1$. But by 8.3.2, if $q \equiv -1 \pmod 3$, the 3-share of $\Phi_{18}(q)$ is 3 and (3) holds.

(4): Let $\Phi_{30}(x) \neq f(x)$ be a cyclotomic polynomial of degree ≤ 8 and suppose $(\Phi_{30}(q), f(q)) \neq 1$. Now $\Phi_{30}(x) = x^8 + x^7 - x^5 - x^4 - x^3 + x + 1$, so $\Phi_{30}(q)$ is odd. Notice that $(\Phi_{30}(q), \Phi_1(q)) = 1$. By 8.5 and 8.4, $f(x) = \Phi_m(x)$ for some $1 < m < 30$. By 8.4, if p is a prime dividing $(\Phi_{30}(q), f(q))$, then $p = 3$ or 5. Now by 8.3.1, $\Phi_{30}(q) \not\equiv 0 \pmod 3$ and $\Phi_{30}(q) \not\equiv 0 \pmod 5$ so (4) follows.

(5): Let $\Phi_{14}(x) \neq f(x)$ be a cyclotomic polynomial of degree ≤ 6 and suppose $(\Phi_{14}(q), f(q)) \neq 1$. Now $\Phi_{14}(x) = x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$, so $\Phi_{14}(q)$ is odd. Using 8.5 and 8.4, we see that $f(x) = \Phi_2(x)$ and $(\Phi_{14}(q), \Phi_2(q)) = 7^t$, for some $t \geq 1$. Hence $q \equiv -1 \pmod 7$ and by 8.3.2, $t = 1$.

(6): Let $\Phi_7(x) \neq f(x)$ be a cyclotomic polynomial of degree ≤ 6 and suppose $(\Phi_7(q), f(q)) \neq 1$. Now $\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, so $\Phi_7(q)$ is odd. Using 8.5 and 8.4, we see that $f(x) = x - 1$. Now $\Phi_7(x) = (x^5 + 2x^4 + 3x^3 + 4x^2 + 5x + 6)(x - 1) + 7$. Hence $(\Phi_7(q), q - 1) = (q - 1, 7)$.

8.7. *There exists a maximal torus $T_\sigma \leq L$ satisfying the hypotheses of 8.2.*

Proof. We begin with the Suzuki and Ree groups ${}^2B_2(q)$, ${}^2G_2(q)$, ${}^2F_4(q)$, where $p = 2, 3, 2$ respectively. Here $q = p^{2m+1}$ and we set $q_0 = \sqrt{q}$. Suppose first that $L \simeq {}^2B_2(q)$. As is well-known, (see, e.g., [**1**, p. 191]) there are 3 classes of maximal tori in L of orders $(q - 1)$, $(q - \sqrt{2q} + 1)$ and $(q + \sqrt{2q} + 1)$. So taking, e.g., $|T_\sigma| = q - 1$, we are done.

Suppose next that $L \cong {}^2G_2(q)$. Then, there are 4 classes of maximal tori in L (see, e.g., [**1**, p. 213]) of orders $(q - 1)$, $(q + 1)$, $q - \sqrt{3q} + 1$ and $q + \sqrt{3q} + 1$ and taking, e.g., $|T_\sigma| = q + \sqrt{3q} + 1$, we are done.

Suppose that $L \cong {}^2F_4(q)$. By [**17**], the order of a maximal torus of L either divides $[\Phi_1(q)]^2[\Phi_2(q)]^2\Phi_4(q)\Phi_6(q)$, or is of order $q_0^4 + \epsilon\sqrt{2}q_0^3 + q_0^2 + \epsilon\sqrt{2}q_0 + 1$,

$\epsilon \in \{1,-1\}$ and hence divides $\Phi_{12}(q)$. Let $|T_\sigma| = q_0^4 + \sqrt{2}q_0^3 + q_0^2 + \sqrt{2}q_0 + 1$ and let $S_\sigma \leq L$ be a maximal torus with $|S_\sigma| \neq |T_\sigma|$. Since $|T_\sigma|$ divides $\Phi_{12}(q)$, we deduce from 8.6.1, that $(|T_\sigma|, |S_\sigma|) = 1$, except perhaps when $|S_\sigma| = q_0^4 - \sqrt{2}q_0^3 + q_0^2 - \sqrt{2}q_0 + 1$. But it is easy to check that $(q_0^4 + \sqrt{2}q_0^3 + q_0^2 + \sqrt{2}q_0 + 1, q_0^4 - \sqrt{2}q_0^3 + q_0^2 - \sqrt{2}q_0 + 1) = 1$.

Suppose L is one of the remaining types. Let $S_\sigma \leq L$ be a maximal torus. As is well-known, if n is the rank of L, then

$$(*) \qquad |S_\sigma| = g(q)$$

where $g(x)$ is a polynomial of degree n, a product of cyclotomic polynomials.

If $L \cong G_2(q)$, with $q \not\equiv -1 \pmod 3$ we let $|T_\sigma| = \Phi_6(q)$, while if $q \equiv -1 \pmod 3$, we let $|T_\sigma| = \Phi_3(q)$. If $L \cong {}^3D_4(q)$, we let $|T_\sigma| = \Phi_{12}(q)$. If $L \cong F_4(q)$, we let $|T_\sigma| = \Phi_{12}(q)$. If $L \cong E_6(q)$ we let $|T_\sigma| = \Phi_9(q)$. If $L \cong {}^2E_6(q)$, we let $|T_\sigma| = \Phi_{18}(q)$. Finally, if $L \cong E_8(q)$, we let $|T_\sigma| = \Phi_{30}(q)$.

In all cases T_σ exists (see, e.g., [**1**, pp. 304-305] and [**5**]). By 8.6 and $(*)$, T_σ satisfies the hypotheses of 8.2.

Theorem 8.8. *Let L^* be an exceptional finite simple group of Lie type. Suppose L^* is not of type E_7. Then $\Delta(L^*)$ is disconnected.*

Proof. This is immediate from 8.2 and 8.7.

9. The group $E_7(q)$.

In this section q is a prime power and L is a simple group with $L \cong E_7(q)$. We let $\delta = \gcd(q-1, 2)$. Recall that

$$|L| = \frac{1}{\delta}q^{63}(q^{18}-1)(q^{14}-1)(q^{12}-1)(q^{10}-1)(q^8-1)(q^6-1)(q^2-1).$$

Thus if $\tilde{L}$ is the universal group of type E_7 defined over the field of q elements, then $|Z(\tilde{L})| = \delta$ and $\tilde{L}/Z(\tilde{L}) = L$. We let $\Delta = \Delta(L)$ be the commuting graph of L. Our notation for graphs and the commuting graph are as introduced in Section 1 (see 1.3), in particular, for $a \in \Delta$, $\Delta^i(a) = \{x \in \Delta : d(a,x) = i\}$ (d is the distance function) and $\Delta(a) = \Delta^1(a)$.

The purpose of this section is to prove that Δ is balanced (Theorem 9.14), we do this by showing that, in the notation of 9.2 (below), there exists $a \in \Delta$ such that $\Xi(a) \neq \emptyset$. Then, by definition, for each $b \in \Xi(a)$, $B_\Delta(a,b)$ and $B_\Delta(b,a)$, so Δ is balanced.

Notation. We denote $SL_n^\epsilon(q) = SL_n(q)$, $SU_n(q)$, according to whether $\epsilon = 1, -1$. Similarly for GL_n^ϵ and PSL_n^ϵ.

In what follows we take $\epsilon = 1$, unless $4 \mid q-1$, in which case we take $\epsilon = -1$. Of course $4 \nmid q - \epsilon$.

9.1. (1) *L contains a subgroup $K \cong PSL_8^\epsilon(q)$.*

(2) *K contains a subgroup $H \cong GL_7^\epsilon(q)/\mathbb{Z}_{(2,q-\epsilon)}$, which contains a cyclic maximal torus of order $(q^7-\epsilon)/(2,q-\epsilon)$.*
(3) *$Z(H) \cong \mathbb{Z}_{(q-\epsilon)/(2,q-\epsilon)}$, a group of odd order.*
(4) *Let $1 \neq a \in Z(H)$. Then $C_L(a) = H$.*

Proof. View $L = (\bar{L}_\sigma)'$, where $\bar{L}$ is an adjoint group of type E_7 and σ is a Frobenius morphism. Then L has index δ in $\bar{L}_\sigma$. There is a σ-invariant maximal rank subgroup $A_7 < \bar{L}$ with center of order δ. Then $N_{E_7}(A_7) = A_7.2$, the extra involution being the long word in a suitable Weyl group and inducing a graph automorphism on A_7. It follows from [**1**, I, 2.8], that there are two classes of σ-invariant conjugates of A_7. For elements in one class σ induces a field morphism and on the other a graph-field morphism. Let $\overline{E}$ be an element of one of these classes, determined by ϵ. Then $\overline{E}_\sigma < \bar{L}_\sigma$.

Let $\hat{E} = SL_8$, the simply connected group of type A_7. There is a surjective homomorphism $\theta : \hat{E} \to \overline{E}$, with kernel of order 4 or 1, according to whether q is odd or even. Moreover, there is a Frobenius morphism of $\hat{E}$, which we also call σ, which commutes with θ.

Now $\hat{K} = (\hat{E})_\sigma = SL_8^\epsilon(q)$ and this group contains $\hat{H} \cong GL_7^\epsilon(q)$, which arises by taking fixed points of a σ-invariant subgroup of $\hat{E}$ of type A_6T_1.

Set $K = \theta(\hat{K})$, so that $K \cong SL_8^\epsilon(q)/\mathbb{Z}_{(4,q-\epsilon)}$. Our choice of ϵ forces $K \cong PSL_8^\epsilon(q)$ giving (1).

Let $\overline{D} = \theta(A_6T_1) < \overline{E}$. Then $\overline{D}_\sigma$ and $(A_6T_1)_\sigma$ have the same order (see the proof of (2.12) in [**15**]), so $\overline{D}_\sigma \geq \theta(GL_7^\epsilon(q))$ as a subgroup of index $(4, q-\epsilon)$. Also $\overline{D}_\sigma$ covers $\bar{L}_\sigma/L$.

Our choice of ϵ implies that $GL_7^\epsilon(q) = J \times S$, where $J = O^{2'}(GL_7^\epsilon(q))$ and $S \cong \mathbb{Z}_{(2,q-\epsilon)}$. Then θ restricts to an isomorphism on J and setting $H = \theta(J)$ we obtain (2). We note that H has index $(2, q-\epsilon)$ in $\overline{D}_\sigma$, and if the index is 2, then there is an involution in $\overline{D}_\sigma$ which is in $\bar{L}_\sigma - L$ ((2.12) in [**15**]). Also H contains a cyclic maximal torus of order $(q^7-\epsilon)/(2,q-\epsilon)$. Thus (2) holds. (3) follows from (2) and our choice of ϵ.

Fix $1 \neq a \in Z(H)$. Then $C_{\overline{L}}(a)^0 \geq \overline{D}$, a maximal rank group of type A_6T_1. If the containment is strict, then $C_{\overline{L}}(a)^0$ would have to be a semisimple group of rank 7. But a consideration of root systems shows that the only such subgroups of E_7 containing A_6 are of type A_7 and such a group has centralizer of order at most 2. Thus equality holds and taking fixed points we have $C_{\overline{L}_\sigma}(a) = \overline{D}_\sigma$. Intersecting with L yields (4).

9.2. Notation and definitions.

(1) $\mathcal{T}$ denotes the set of maximal tori in L of order $(q^7-\epsilon)/(2,q-\epsilon)$ as in 9.1.2. Of course $\mathcal{T}$ is a conjugacy class of tori in L.
(2) Given $T \in \mathcal{T}$, we denote by $R_T \leq T$, the unique subtorus of order $(q-\epsilon)/(2,q-\epsilon)$. We let $\Lambda_T = T - R_T$. We set $\Lambda = \cup_{T\in\mathcal{T}}\Lambda_T$ and we let $\lambda = |\Lambda|$.

(3) Given $T \in \mathcal{T}$, we let $H_T = C_L(R_T)$.

Let $a \in \Lambda$.

(4) We let $\Theta(a) = \Delta^{\leq 3}(a)$. We denote $\theta = |\Theta(a)|$. We'll see in 9.3 below that θ is independent of a.

(5) We let $\Gamma(a) = \{b \in \Lambda : d(a, ab) > 3 < d(a, a^{-1}b)\}$.

(6) We denote $\Gamma^*(a) = \{b \in \Lambda : a \in \Gamma(b)\}$.

(7) We denote $\Xi(a) = \Gamma(a) \cap \Gamma^*(a) \cap \Lambda^{>3}(a)$.

9.3. *Let $a \in \Lambda$. Then:*

(1) *There exists a unique $T \in \mathcal{T}$ such that $a \in T$. Further, $C_L(a) = T$.*

Let $T \in \mathcal{T}$ be the unique torus containing $\{a\}$. Then:

(2) $\Delta(a) = T - \{1, a\}$.

(3) $\Delta^2(a) = H_T - T$.

(4) $|\Delta^k(a)| = |\Delta^k(b)|$, *for all $b \in \Lambda$ and all k.*

Proof. Let $a \in \Lambda$. To show (1), suppose first that the order of a, $|a|$ is not a power of 7. We claim that a satisfies the hypotheses for s in 8.1. Recall that if $S_\sigma \leq \tilde{L}$ is a maximal torus, then $|S_\sigma| = g(q)$, where $g(x)$ is a polynomial of degree 7, a product of cyclotomic polynomials, hence the hypotheses of 8.1 follow from 8.6.5 if $\epsilon = -1$ and from 8.6.6, if $\epsilon = 1$. So suppose $|a|$ is a power of 7. Let $T \in \mathcal{T}$ such that $a \in T$. Since T is cyclic, $1 \neq a^k \in R_T$, for some $k \geq 2$. Then $C_L(a) \leq C_L(a^k) = C_L(R_T)$, by 9.1.4. Hence, (1) follows from inspecting $C_H(a)$, where $H = H_T$. This shows (1). Now, (2) is immediate from (1), and (3) is immediate from (2) and 9.1.4. Also (3) says that $\Delta^2(x) = \Delta^2(y)$, for $x, y \in \Lambda_T$, so since $\mathcal{T}$ is a conjugacy class of subgroups, (4) follows.

9.4. *Let $a \in \Lambda$ and set $\Theta = \Theta(a)$. Then:*

(1) $\Gamma(a) = \Lambda - ((a^{-1}(a\Lambda \cap \Theta)) \cup (a(a^{-1}\Lambda \cap \Theta)))$.

(2) $|\Gamma(a)| \geq \lambda - 2\theta$.

Proof. Note that $\{b \in \Lambda : d(a, ab) \leq 3\} = a^{-1}(a\Lambda \cap \Theta(a))$ and $\{b \in \Lambda : d(a, a^{-1}b) \leq 3\} = a(a^{-1}\Lambda \cap \Theta(a))$. Hence (1) holds. (2) is immediate from (1).

9.5. *There exists $a \in \Lambda$ such that $|\Gamma^*(a)| \geq \lambda - 2\theta$.*

Proof. Let $M = \mathrm{Max}_{b \in \Lambda} |\Gamma^*(b)|$. Count the number of pairs $X = \{(a, b) : a, b \in \Lambda \text{ and } b \in \Gamma(a)\}$. Using 9.4, we have $\lambda(\lambda - 2\theta) \leq \sum_{a \in \Lambda} |\Gamma(a)| = |X| = \sum_{b \in \Lambda} |\Gamma^*(b)| \leq \lambda M$. Thus $M \geq (\lambda - 2\theta)$ as asserted.

9.6. Notation. From now on we fix $a \in \Lambda$ such that $|\Gamma^*(a)| \geq \lambda - 2\theta$, and we set $\Theta = \Theta(a)$, $\Xi = \Xi(a)$ and $\xi = |\Xi|$. Let T denote the unique member of $\mathcal{T}$ containing $\{a\}$ and set $H = H_T$.

9.7. (1) $|\Gamma(a) \cap \Gamma^*(a)| \geq \lambda - 4\theta$.

(2) $\xi \geq \lambda - 5\theta$.

Proof. $|\Gamma(a)\cap\Gamma^*(a)| \geq |\Gamma(a)|-|\Lambda-\Gamma^*(a)| \geq (\lambda-2\theta)-(\lambda-(\lambda-2\theta)) = \lambda-4\theta$. The proof of (2) is similar.

The remainder of this section is devoted to showing that $\Xi \neq \emptyset$, or that $\xi > 0$. It will be done by producing an upper bound to θ. To estimate sizes of subgroups we'll use the following lemma.

9.8. *Let $2 \leq a_1 < a_2 < \dots < a_k$ be integers and let $\epsilon_1, \epsilon_2, \dots, \epsilon_k \in \{1, -1\}$. Then*

$$\frac{1}{2} \leq \frac{(q^{a_1}+\epsilon_1)(q^{a_2}+\epsilon_2)\cdots(q^{a_k}+\epsilon_k)}{q^{a_1+a_2+\cdots+a_k}} \leq 2.$$

Proof. This is taken from [**18**, p. 2100]. We include the proof in [**18**]. For $i \geq 2$, we have

$$1-\frac{1}{2^i} \geq \frac{\frac{1}{2}+\frac{1}{2^i}}{\frac{1}{2}+\frac{1}{2^{i-1}}}, \quad 1+\frac{1}{2^i} \leq \frac{1-\frac{1}{2^i}}{1-\frac{1}{2^{i-1}}}.$$

Therefore the fraction

$$\frac{(q^{a_1}+\epsilon_1)(q^{a_2}+\epsilon_2)\cdots(q^{a_k}+\epsilon_k)}{q^{a_1+a_2+\cdots+a_k}}$$

is at least

$$\begin{aligned}\prod_{i=1}^{k}\left(1-\frac{1}{q^{a_i}}\right) &\geq \prod_{i=2}^{K}\left(1-\frac{1}{q^{i}}\right) \geq \prod_{i=2}^{K}\left(1-\frac{1}{2^{i}}\right)\\ &\geq \prod_{i=2}^{K}\frac{\frac{1}{2}+\frac{1}{2^i}}{\frac{1}{2}+\frac{1}{2^{i-1}}} = \frac{1}{2}+\frac{1}{2^K} > \frac{1}{2},\end{aligned}$$

(where $K = a_k$) and at most

$$\begin{aligned}\prod_{i=1}^{k}\left(1+\frac{1}{q^{a_i}}\right) &\leq \prod_{i=2}^{K}\left(1+\frac{1}{q^{i}}\right) \leq \prod_{i=2}^{K}\left(1+\frac{1}{2^{i}}\right)\\ &\leq \prod_{i=2}^{K}\frac{1-\frac{1}{2^i}}{1-\frac{1}{2^{i-1}}} = 2-\frac{1}{2^{K-1}} < 2.\end{aligned}$$

9.9. (1) $|H| \leq 3q^{49} \leq q^{51}$.
(2) $|L| \geq \frac{1}{2\delta}q^{133}$.
(3) $\lambda \geq \frac{1}{14\delta}q^{133}$.

Proof. By 9.1.2, $|H| = \frac{1}{(2,q-\epsilon)}\,|GL_7^\epsilon(q)|$. By 9.8, $|SL_7^\epsilon(q)| \leq 2q^{48}$. Hence, $\frac{1}{(2,q-\epsilon)}|GL_7^\epsilon(q)| = \frac{1}{(2,q-\epsilon)}(q-\epsilon)|SL_7^\epsilon(q)| \leq \frac{2}{(2,q-\epsilon)}(q-\epsilon)q^{48} \leq 3q^{49}$. (2) follows immediately from 9.8. Now $|\Lambda_T| = |T-R_T| = \frac{1}{(2,q-\epsilon)}\{q^7-\epsilon-(q-\epsilon)\} =$

$\frac{1}{(2,q-\epsilon)}(q^7-q)$. Since every element of Λ lies in a unique member of $\mathcal{T}$, we get that

$$
\begin{aligned}
|\Lambda| = |\Lambda_T|\,|\mathcal{T}| &\geq \frac{1}{(2,q-\epsilon)}(q^7-q)\cdot\frac{|L|}{7|T|} = \frac{1}{7\delta}|L|\,\frac{q^7-q}{q^7-\epsilon} \\
&= \frac{1}{7\delta}q^{63}(q^7-q)(q^7+\epsilon)(q^{18}-1)(q^{12}-1)(q^{10}-1)(q^8-1)(q^6-1)(q^2-1) \\
&\geq \frac{1}{14\delta}q^{133}
\end{aligned}
$$

by 9.8; notice that the argument in the proof of 9.8 applies even though we have q^6-1 appearing twice in the last product.

Corollary 9.10. (1) *Suppose $\theta < \frac{1}{70\delta}q^{133}$. Then $\xi > 0$.*
(2) *Suppose $\theta < q^{126}$. Then $\xi > 0$.*

Proof. By 9.7.2, $\xi \geq \lambda - 5\theta$. Now $\lambda - 5\theta > 0$, iff $\lambda > 5\theta$ iff $\theta < \frac{1}{5}\lambda$. By 9.9.3, $\lambda \geq \frac{1}{14\delta}q^{133}$, so $\frac{1}{5}\lambda \geq \frac{1}{70\delta}q^{133}$. (2) follows immediately from (1).

9.11. *Let $\mathfrak{M} = \{h \in H - \{1\} : |C_L(h)| \geq q^{74}\}$. Set $\mathbb{M} = \cup_{h\in\mathfrak{M}} C_L(h)$ and $\mu = |\mathbb{M}|$. If $\mu \leq q^{125}$, then $\xi > 0$.*

Proof. By 9.10.2, it suffices to show that $\theta \leq q^{126}$. Of course, by 9.3.3, any element in Θ centralizes a nontrivial element of H. Hence

$$
\theta \leq \left|\bigcup_{h\in H-\{1\}} C_L(h)\right|. \tag{i}
$$

Let $\mathbb{M}_1 = \bigcup\{C_L(h) : 1 \neq h \in H - \mathfrak{M}\}$. Of course, $|\mathbb{M}_1| \leq \sum_{1\neq h\in H-\mathfrak{M}} |C_L(h)| < |H|q^{74} \leq q^{125}$. Also, $\bigcup\{C_L(h) : 1 \neq h \in H\} = \mathbb{M}_1 \cup \mathbb{M}$, so by (i), $\theta \leq |\mathbb{M}_1| + |\mathbb{M}| \leq q^{125} + q^{125} \leq q^{126}$.

Hence, it remains to show that $\mu \leq q^{125}$.

9.12. *Let $x \in H$ satisfy $|C_L(x)| \geq q^{74}$. Then one of the following holds:*

(1) *x is unipotent of class A_1, $|C_L(x)| \leq 2q^{99}$, $x^L \cap H$ is a conjugacy class of H and $|H : C_H(x)| \leq 4q^{12}$.*
(2) *x is unipotent of class $2A_1$, $|C_L(x)| \leq 2q^{81}$, $x^L \cap H$ is a conjugacy class of H, and $|H : C_H(x)| \leq 4q^{20}$.*
(3) *x is semisimple, $C_L(x)' \cong E_6(q)$ or ${}^2E_6(q)$ according to whether $\epsilon = 1$ or -1. $C_L(x) = C_L(x)'S$, where S is cyclic of order $(q-\epsilon)/(2,q-\epsilon)$. Hence $|C_L(x)| \leq 3q^{79}$. Either $|H : C_H(x)| = |GL_7^\epsilon(q) : GL_5^\epsilon(q)GL_2^\epsilon(q)| \leq 4q^{20}$ or $|H : C_H(x)| = |GL_7^\epsilon(q) : GL_6^\epsilon(q)GL_1^\epsilon(q)| \leq 2q^{12}$.*

Proof. Write $x = su$ as a commuting product of a semisimple and a unipotent element. Then $C_L(x) \leq C_L(s)$. The latter group is obtained by taking the set of fixed points under σ from the centralizer in the algebraic group, then intersecting with L. In the algebraic group the centralizer is a reductive subgroup of maximal rank and a trivial check of subsystems shows that the only subsystems giving a large enough centralizer are of type E_7 or E_6T_1. In the first case, $s = 1$ and in the latter case $u = 1$ in order to have large enough centralizer (see [**7**]).

Suppose $s = 1$, so that x is unipotent. Then a check of [**8**] shows that x has types A_1, $(2A_1)$, or $(3A_1)''$. Now x is contained in a subsystem subgroup of $\tilde{L}$ of type A_6. The Jordan form of a unipotent element of A_6 determines a subsystem group containing the unipotent element as a regular element. Each of the relevant subsystems is a Levi factor, so by the classification of unipotent elements, x must also be of type $A_1, 2A_1$, or $3A_1$ within A_6.

Now E_7 has just one class of subsystem groups of type A_1 and $2A_1$, but it has two classes of subsystem groups of type $3A_1$ and we claim that the class $(3A_1)''$ is not represented in A_6. To see this start from a subsystem group of type A_1, with centralizer D_6. Working in A_1D_6 we see that there are two classes of groups of type $3A_1$, with centralizers $D_4, 4A_1$, respectively. Only unipotent elements of type $(3A_1)''$ have centralizer involving D_4, so the former class is of type $(3A_1)''$. On the other hand, the group $3A_1$ in A_6 is contained in A_1A_4, so from the centralizer of the first factor we get $A_4 < D_6$ and from here we see that the full centralizer of $3A_1$ cannot contain D_4, so this must be the class $(3A_1)'$, establishing the claim.

One checks that the centralizers of unipotent elements of type A_1 and $2A_1$ in $A_6T_1 \cong GL_7$ are connected, so each type is represented by a single class in $GL_7^\epsilon(q)$ ([**1**, I, 2.8]) and hence in H. Centralizers are given in [**8**], so the numerical information in (1) and (2) follows by taking fixed points and using 9.8.

Now suppose $s \neq 1$. We again consider the group $A_7 = \overline{E} < \bar{L}$. It is shown in (2.3) of [**6**] the the 56-dimensional restricted module for a simple connected group of type E_7 restricts to a subgroup of type A_7 as the wedge square of the natural module and its dual. In each of these three irreducible modules the Weyl group of E_7 or A_7 with respect to a maximal torus is transitive on weight spaces within the module. The stabilizer in $W(E_7)$ of a weight space is $W(E_6)$ and this is also the centralizer in $W(E_7)$ of the central torus in $C_L(s)$.

Choose a σ-invariant maximal torus $R < \overline{E}$. Taking Weyl groups with respect to R, it follows from the above paragraph that $W(A_7)$ has two orbits on 1-dimensional tori in R, with centralizer of type $W(E_6)$. Each has stabilizer in $W(A_7)$ of type $W(A_5)W(A_1)$. So for such a 1-dimensional torus, the centralizer in A_7 is a reductive group with Weyl group of type $W(A_5)W(A_1)$. The only possibility is that the centralizer has the form $A_5A_1T_1$.

Elements of the above 1-dimensional torus are represented in $\overline{E}$ as images of elements of SL_8 having one eigenvalue of multiplicity 6 and another of multiplicity 2. Taking fixed points and working in $GL_7^\epsilon(q)$ we see that there are two types of semisimple elements in H of the correct type. In the action on the natural 7-dimensional module one type has one eigenvalue of multiplicity 6 and one eigenvalue of multiplicity 1, while for the other class there is one eigenvalue of multiplicity 5 and another of multiplicity 2. The conclusion follows.

Corollary 9.13. $\mu \leq q^{125}$.

Proof. For $i = 1, 2$ let u_i denote a unipotent element as in 9.12.1, and set $M_i = u_i^L \cap H$. Let S_1, S_2 be subgroups of order $(q - \epsilon)/(2, q - \epsilon)$ in H corresponding to subgroups of $GL_7^\epsilon(q)$ with centralizer $GL_5^\epsilon(q)GL_2^\epsilon(q)$ or $GL_6^\epsilon(q)GL_1^\epsilon(q)$, respectively. We claim that $C_L(S) = C_L(y)$, for $S \in \{S_1, S_2\}$ and $1 \neq y \in S$. This follows from the fact that the preimage of S in $\tilde{L}$ has centralizer of type E_6T_1, which is maximal among reductive subgroups of E_7. Recall that we defined $\mathfrak{M} = \{h \in H - \{1\} : |C_L(h)| \geq q^{74}\}$ and $\mathbb{M} = \bigcup_{h \in \mathfrak{M}} C_L(h)$. By 9.12 we have

$$\mu = |\mathbb{M}| \leq \sum_{x \in M_1} |C_L(x)| + \sum_{x \in M_2} |C_L(x)| + \sum_{x \in S_1^H} |C_L(x)| + \sum_{x \in S_2^H} |C_L(x)|.$$

Hence $\mu \leq (2q^{99})(4q^{12}) + (2q^{81})(4q^{20}) + (3q^{79})(4q^{20}) + (3q^{79})(4q^{12}) \leq q^{125}$.

Theorem 9.14. *Δ is balanced.*

Proof. By 9.13, $\mu \leq q^{125}$, so by 9.11 $\xi > 0$. Hence $\Xi(a) \neq \emptyset$ and as we remarked at the beginning of Section 9, this shows (by definition) that Δ is balanced.

10. The Alternating Groups.

In this section A_m denote the Alternating Group on $\{1, 2, \ldots, m\}$. The purpose of this section is to prove the following theorem:

Theorem 10.1. *Let $m > 3$ and let $L \cong A_m$. Then* $\operatorname{diam}(\Delta(L)) > 4$.

Throughout this section $n > 2$ is a fixed even integer, such that $n - 1$ is not a prime. We let G be the Symmetric Group on $\{1, 2, \ldots, n\}$. We use cyclic notation for permutations in G. We apply permutations on the right, so for $\sigma \in G$, and $i \in \{1, 2, \ldots, n\}$, $i\sigma$ is the image of i under σ. In addition, when we write a permutation as a product of cycles, the even numbers that occur are bolded and enlarged. For example, if $1 \leq k \leq n$ is an odd number congruent to 1 (mod 4), then

$$\rho = (1, 5, 9, \cdots, k)(\mathbf{k+1}, \mathbf{k+3}, \cdots, \mathbf{2k})$$

is the permutation with $i\rho = i+4$, if $1 \leq i \leq k-4$ is congruent to 1 (mod 4), $k\rho = 1$, $i\rho = i + 2$, if $k + 1 \leq i \leq 2k - 2$ is even, and $(2k)\rho = k + 1$.

Another convention that we'll use is that $\cdots$ means continue with the same pattern. Thus for example, in ρ, the $\cdots$ after 9 means that $9\rho = 13$, $13\rho = 17$, and so on until we get to $k-4$. Another example is

$$\eta = (1, \mathbf{2}, 3, \cdots, \mathbf{k-1}, \mathbf{k+3}, \cdots, \mathbf{4k})$$

is a cycle such that $i\eta = i+1$, $1 \le i \le k-2$, $i\eta = i+4$, if $k-1 \le i \le 4k-4$, is congruent to $0 \pmod 4$ and $(4k)\eta = 1$.

Notation. (1) For a permutation $\sigma \in G$, we denote by $\operatorname{supp}(\sigma)$ the set of elements moved by σ.

(2) We fix once and for all the letter g to denote the permutation

$$g = g_n = (1, \mathbf{2}, 3, \cdots, \mathbf{n-2}, n-1).$$

(3) We fix once and for all the letter s to denote the permutation

$$s = s_n = (3, \mathbf{4})(5, \mathbf{6}) \cdots (n-1, \mathbf{n}).$$

(4) Let p be a prime divisor of $n-1$. We write $n_p = \frac{n-1}{p}$. Thus $n-1 = pn_p$.

(5) Let p be a prime divisor of $n-1$. We denote

$$\theta_p = g^{n_p}.$$

The main result of this section, from which Theorem 10.1 follows, is the following theorem.

Theorem 10.2. *Let $n > 2$ be an even number. Suppose $n-1$ is not a prime and let p, q be prime divisors of $n-1$, with $p \le q$. Let $\Gamma = \langle \theta_p, s\theta_q^{-1}s \rangle$. Then:*

(1) *Γ is a transitive subgroup of G.*

(2) *$C_G(\Gamma) = \{1\}$.*

We'll now prove Theorem 10.1, under the assumption that Theorem 10.2 holds.

Proof of Theorem 10.1. Let $L = A_m$. We assume that Theorem 10.2 holds and we prove Theorem 10.1. Let d be the distance function on $\Delta(L)$. Suppose first that m is even. If $m-1$ is a prime, then it is easy to check that $\langle g_m \rangle - \{1\}$ is a connected component of $\Delta(L)$. So assume $m-1$ is a composite odd number. Let $g = g_m$ and $s = s_m$. We'll show that $d(g, sg^{-1}s) > 4$. So suppose $d(g, sg^{-1}s) \le 4$. Since $C_L(g) = \langle g \rangle$, and $C_L(sg^{-1}s) = \langle sg^{-1}s \rangle$, there are prime divisors p, q of $m-1$ such that $\pi := g, g^{\frac{(m-1)}{p}}, x, sg^{\frac{(1-m)}{q}}s, sg^{-1}s$ is a path in $\Delta(L)$. But then $x \in C_L\left(\left\langle g^{\frac{(m-1)}{p}}, sg^{\frac{(1-m)}{q}}s \right\rangle\right)$, so if $p \le q$, this contradicts Theorem 10.2, while if $p > q$, then inverting the path π and conjugating by s, we get that $g, g^{\frac{(m-1)}{q}}, sx^{-1}s, sg^{\frac{(1-m)}{p}}s, sg^{-1}s$ is also a path in $\Delta(L)$, and this contradicts Theorem 10.2.

Suppose next that m is odd. If $m-2$ is a prime, then $\langle g_{m-1} \rangle - \{1\}$ is a connected component of $\Delta(L)$. So assume $m-2$ is a composite odd number. Let $g = g_{m-1}$ and $s = s_{m-1}$. Let p, q be prime divisors of $m-2$. Let $\Gamma = \left\langle g^{\frac{(m-2)}{p}}, sg^{\frac{(2-m)}{q}}s \right\rangle$. By Theorem 10.2, $\{1, 2, \cdots, m-1\}$ is an orbit of Γ, so the centralizer of Γ in L fixes m, and hence by Theorem 10.2, it is trivial. Then, the same proof as in the case when m is even shows that $d(g, sg^{-1}s) > 4$.

10.3. *Let p be a prime divisor of $n-1$. Then:*

1. $\theta_p = (1, \mathbf{n}_p + \mathbf{1}, \cdots, (p-1)n_p + 1)(\mathbf{2}, n_p + 2, \cdots, (\mathbf{p} - \mathbf{1})\mathbf{n}_p + \mathbf{2}) \cdots (n_p, \mathbf{2n}_p, \cdots, n-1)$ *and θ_p fixes n.*
2. *Two indices $i, j \in \{1, 2, \cdots, n-1\}$ are in the same orbit of θ_p, iff they are congruent modulo n_p.*
3. *For all $1 \leq i \leq n-1$, and all integers $k, ig^k = k + i$, in particular, $i\theta_p = n_p + i$, and $i\theta_p^{-1} = i - n_p$, where indices are taken modulo $(n-1)$.*
4. *For $\sigma \in G$, and $i, k \in \{1, \ldots, n-1\}$, if $i\sigma = j \neq n$, then $(k+i)g^{-k}\sigma g^k = k + j$ and $(i-k)g^k\sigma g^{-k} = j - k$, in particular, $(n_p + i)\theta_p^{-1}\sigma\theta_p = n_p + j$, $(i - n_p)\theta_p\sigma\theta_p^{-1} = j - n_p$ and $(n_p - n_q + i)g^{(n_q - n_p)}\sigma g^{(n_p - n_q)} = n_p - n_q + j$, where indices are taken modulo $(n-1)$.*

Proof. The proof is straightforward.

Important Remark. In order to verify the calculations in this section, we emphasize that n_p denotes $\mathbf{\frac{n-1}{p}}$ and not $\frac{n}{p}$. In addition $ig^k = i + k$, **modulo $(\mathbf{n} - \mathbf{1})$** and not modulo n.

Notation. From now on we fix two primes p and q dividing $n-1$, such that $p \leq q$.

10.4.

1. $\theta_q^{-1}s\theta_q = (\mathbf{n}_q + \mathbf{3}, n_q + 4)(\mathbf{n}_q + \mathbf{5}, n_q + 6) \cdots (\mathbf{n} - \mathbf{2}, n-1)(1, \mathbf{2})(3, \mathbf{4}) \cdots (n_q - 2, \mathbf{n}_q - \mathbf{1})(n_q, \mathbf{n})$.
2. $\theta_q s\theta_q^{-1} = (n - n_q + 2, \mathbf{n} - \mathbf{n}_q + \mathbf{3}) \cdots (n-3, \mathbf{n} - \mathbf{2})(n-1, 1)(\mathbf{2}, 3)(\mathbf{4}, 5) \cdots (\mathbf{n} - \mathbf{n}_q - \mathbf{3}, n - n_q - 2)(\mathbf{n} - \mathbf{n}_q - \mathbf{1}, \mathbf{n})$.
3. $\theta_q^{-1}s\theta_q s = (n_q, n-1, n-3, \cdots, n_q + 4, n_q + 2, \mathbf{n}_q + \mathbf{3}, \mathbf{n}_q + \mathbf{5}, \cdots, \mathbf{n} - \mathbf{2}, \mathbf{n}, \mathbf{n}_q + \mathbf{1})(1, \mathbf{2})$.
4. $\theta_q s\theta_q^{-1}s = (\mathbf{2}, \mathbf{4}, \cdots, \mathbf{n} - \mathbf{n}_q - \mathbf{1}, n-1, 1, \mathbf{n}, n - n_q - 2, n - n_q - 4, \cdots, 3)(n - n_q, \mathbf{n} - \mathbf{n}_q + \mathbf{1})$.
5. $[\theta_p, s\theta_q^{-1}s] = g^{(n_q - n_p)}\theta_q^{-1}s\theta_q sg^{(n_p - n_q)}\theta_q s\theta_q^{-1}s$.
6. *If $p \neq q$, then*

$$g^{(n_q - n_p)}\theta_q^{-1}s\theta_q sg^{(n_p - n_q)} =$$

$$(n_p, \mathbf{n}_p - \mathbf{n}_q, \mathbf{n}_p - \mathbf{n}_q - \mathbf{2}, \cdots, \mathbf{2}, n-1, n-3, \cdots, n_p + 2, \mathbf{n}_p + \mathbf{3}, \mathbf{n}_p + \mathbf{5}, \cdots, \mathbf{n} - \mathbf{2}, 1, 3, \cdots, n_p - n_q - 1, \mathbf{n}, \mathbf{n}_p + \mathbf{1})(n_p - n_q + 1, \mathbf{n}_p - \mathbf{n}_q + \mathbf{2}).$$

Proof. For (1), we have,
$\theta_q^{-1}s\theta_q = (3\theta_q, 4\theta_q)(5\theta_q, 6\theta_q)\cdots((n-1)\theta_q, n\theta_q) =$

$$(\mathbf{n}_q+\mathbf{3}, n_q+4)(\mathbf{n}_q+\mathbf{5}, n_q+6)\cdots(\mathbf{n}-\mathbf{2}, n-1)(1,\mathbf{2})(3,\mathbf{4})$$
$$\cdots(n_q-2, \mathbf{n}_q-1)(n_q,\mathbf{n})$$

where we use 10.3 to verify this equality, noting that θ_q fixes n. (2) is proved similarly.

We now prove (3). We first write $\theta_q^{-1}s\theta_q$ and s one below the other.

$$(\mathbf{n}_q+\mathbf{3}, n_q+4)(\mathbf{n}_q+\mathbf{5}, n_q+6)\cdots(\mathbf{n}-\mathbf{2}, n-1)(1,\mathbf{2})(3,\mathbf{4})$$
$$\cdots(n_q-2, \mathbf{n}_q-\mathbf{1})(n_q,\mathbf{n})\cdot$$
$$(3,\mathbf{4})(5,\mathbf{6})\cdots(n-3,\mathbf{n}-\mathbf{2})(n-1,\mathbf{n}) = .$$

Note that $(3,\mathbf{4})(5,\mathbf{6})\cdots(n_q-2,\mathbf{n}_q-\mathbf{1})$ is canceled. Hence

$$= (\mathbf{n}_q+\mathbf{3}, n_q+4)(\mathbf{n}_q+\mathbf{5}, n_q+6)\cdots(\mathbf{n}-\mathbf{2}, n-1)(1,\mathbf{2})(n_q,\mathbf{n})\cdot$$
$$(n_q,\mathbf{n}_q+\mathbf{1})(n_q+2,\mathbf{n}_q+\mathbf{3})\cdots(n-3)(\mathbf{n}-\mathbf{2})(n-1,\mathbf{n}) = .$$

Now start with n_q and carefully work though the product.

$$= (n_q, n-1, n-3, \cdots, n_q+4, n_q+2, \mathbf{n}_q+\mathbf{3}, \mathbf{n}_q+\mathbf{5}, \cdots,$$
$$\mathbf{n}-\mathbf{2}, \mathbf{n}, \mathbf{n}_q+1)(1,\mathbf{2}).$$

Next we prove (4). We first write $\theta_q s\theta_q^{-1}$ and s one below the other.

$$(n-n_q+2, \mathbf{n}-\mathbf{n}_q+\mathbf{3})\cdots(n-3,\mathbf{n}-\mathbf{2})(n-1,1)(\mathbf{2},3)(\mathbf{4},5)\cdots$$
$$(\mathbf{n}-\mathbf{n}_q-\mathbf{3}, n-n_q-2)(\mathbf{n}-\mathbf{n}_q-\mathbf{1},\mathbf{n})\cdot$$
$$(3,\mathbf{4})(5,\mathbf{6})\cdots(n-3,\mathbf{n}-\mathbf{2})(n-1,\mathbf{n}) = .$$

Note that $(n-n_q+2, \mathbf{n}-\mathbf{n}_q+\mathbf{3})\cdots(n-3,\mathbf{n}-\mathbf{2})$ is canceled. Hence

$$= (n-1,1)(\mathbf{2},3)(\mathbf{4},5)\cdots(\mathbf{n}-\mathbf{n}_q-\mathbf{3}, n-n_q-2)(\mathbf{n}-\mathbf{n}_q-\mathbf{1},\mathbf{n})$$
$$(3,\mathbf{4})(5,\mathbf{6})\cdots(n-n_q-2,\mathbf{n}-\mathbf{n}_q-\mathbf{1})(n-n_q,\mathbf{n}-\mathbf{n}_q+\mathbf{1})(n-1,\mathbf{n})$$
$$= (\mathbf{2},\mathbf{4},\cdots,\mathbf{n}-\mathbf{n}_q-\mathbf{1}, n-1, 1, \mathbf{n}, n-n_q-2, n-n_q-4,$$
$$\cdots,3)(n-n_q,\mathbf{n}-\mathbf{n}_q+\mathbf{1}).$$

We now compute $[\theta_p, s\theta_q^{-1}s] = \theta_p^{-1}s\theta_q s\theta_p s\theta_q^{-1}s$. Recall that by definition, $\theta_p = g^{n_p}$ and $\theta_q = g^{n_q}$. Hence $[\theta_p, s\theta_q^{-1}s] = g^{(n_q-n_p)}\theta_q^{-1}s\theta_q s g^{(n_p-n_q)}\theta_q s\theta_q^{-1}s$.

Finally,

$$\begin{aligned} & g^{(n_q-n_p)}\theta_q^{-1}s\theta_q s g^{(n_p-n_q)} \\ = & g^{(n_q-n_p)}(n_q, n-1, n-3, \cdots, n_q+4, n_q+2, \mathbf{n}_q+\mathbf{3}, \mathbf{n}_q+\mathbf{5}, \\ & \cdots, \mathbf{n}-\mathbf{2}, \mathbf{n}, \mathbf{n}_q+\mathbf{1})(1, \mathbf{2})g^{(n_p-n_q)}. \end{aligned}$$

Now using 10.3.4 we get

$$\begin{aligned} = & (n_p, \mathbf{n}_p-\mathbf{n}_q, \mathbf{n}_p-\mathbf{n}_q-\mathbf{2}, \cdots \mathbf{2}, n-1, n-3, \\ & \cdots, n_p+2, \mathbf{n}_p+\mathbf{3}, \mathbf{n}_p+\mathbf{5}, \cdots, \mathbf{n}-\mathbf{2}, \\ & 1, 3, \cdots, n_p-n_q-1, \mathbf{n}, \mathbf{n}_p+\mathbf{1})(n_p-n_q+1, \mathbf{n}_p-\mathbf{n}_q+\mathbf{2}). \end{aligned}$$

10.5. *Suppose $n_p - n_q > 2$, then:*

(1) *The fixed points of $[\theta_p, s\theta_q^{-1}s]$ are*

$$\{3, \mathbf{4}, \ldots, n_p-n_q-3, \mathbf{n}_p-\mathbf{n}_q-\mathbf{2}, \mathbf{n}_p-\mathbf{n}_q\}$$

where if $n_p - n_q = 4$, then $\{4\}$ is the unique fixed point.

(2) *If $n - n_p - n_q \equiv 2 \pmod 4$, then $[\theta_p, s\theta_q^{-1}s] =$*

$$\begin{gathered} (1, \mathbf{2})\cdot \\ (n_p-n_q-1, n-n_q-2, n-n_q-6, \cdots, n_p, \mathbf{n}_p-\mathbf{n}_q+\mathbf{2})\cdot \\ (n_p-2, n_p-4, \cdots, n_p-n_q+1, \mathbf{n}_p-\mathbf{n}_q+\mathbf{4}, \\ \mathbf{n}_p-\mathbf{n}_q+\mathbf{6}, \cdots, \mathbf{n}_p-\mathbf{1}, \mathbf{n}_p+\mathbf{1})\cdot \\ (n-n_q, n-n_q-4, \cdots, n_p+4, n_p+2, \mathbf{n}_p+\mathbf{5}, \mathbf{n}_p+\mathbf{9}, \cdots, \mathbf{n}-\mathbf{n}_q-\mathbf{1})\cdot \\ (n-1, n-3, \cdots, n-n_q+2, \mathbf{n}-\mathbf{n}_q+\mathbf{1}, \mathbf{n}-\mathbf{n}_q+\mathbf{3}, \cdots, \mathbf{n}-\mathbf{2}, \mathbf{n}, \\ \mathbf{n}_p+\mathbf{3}, \mathbf{n}_p+\mathbf{7}, \cdots, \mathbf{n}-\mathbf{n}_q-\mathbf{3}). \end{gathered}$$

(3) *If* $n - n_p - n_q \equiv 0 \pmod 4$, *then* $[\theta_p, s\theta_q^{-1}s] =$

$$(1, \mathbf{2}) \cdot$$
$$(n_p - n_q - 1, n - n_q - 2, n - n_q - 6, \cdots, n_p + 2,$$
$$\mathbf{n}_p + \mathbf{5}, \mathbf{n}_p + \mathbf{9}, \cdots, \mathbf{n} - \mathbf{n}_q - \mathbf{3},$$
$$n - 1, n - 3, \cdots, n - n_q + 2, \mathbf{n} - \mathbf{n}_q + \mathbf{1}, \mathbf{n} - \mathbf{n}_q + \mathbf{3}, \cdots, \mathbf{n} - \mathbf{2}, \mathbf{n},$$
$$\mathbf{n}_p + \mathbf{3}, \mathbf{n}_p + \mathbf{7}, \cdots, \mathbf{n} - \mathbf{n}_q - \mathbf{5}, \mathbf{n} - \mathbf{n}_q - \mathbf{1},$$
$$n - n_q, n - n_q - 4, \cdots, n_p + 4, n_p, \mathbf{n}_p - \mathbf{n}_q + \mathbf{2}) \cdot$$
$$(n_p - 2, n_p - 4, \cdots, n_p - n_q + 1, \mathbf{n}_p - \mathbf{n}_q + \mathbf{4},$$
$$\mathbf{n}_p - \mathbf{n}_q + \mathbf{6}, \cdots, \mathbf{n}_p - \mathbf{1}, \mathbf{n}_p + \mathbf{1}).$$

Proof. Note, $n_p - n_q > 2$ implies $n_p > 5$. By 10.4.5,

$$[\theta_p, s\theta_q^{-1}s] = g^{(n_q - n_p)}\theta_q^{-1}s\theta_q s g^{(n_p - n_q)} \cdot \theta_q s\theta_q^{-1}s$$

so by 10.4, $[\theta_p, s\theta_q^{-1}s] =$

$$(n_p, \mathbf{n}_p - \mathbf{n}_q, \mathbf{n}_p - \mathbf{n}_q - \mathbf{2}, \cdots, \mathbf{2}, n - 1, n - 3, \cdots, n - n_q, \cdots, n_p + 2,$$
$$\mathbf{n}_p + \mathbf{3}, \mathbf{n}_p + \mathbf{5}, \cdots, \mathbf{n} - \mathbf{2}, 1, 3, \cdots, n_p - n_q - 1, \mathbf{n}, \mathbf{n}_p + \mathbf{1}) \cdot$$
$$(n_p - n_q + 1, \mathbf{n}_p - \mathbf{n}_q + \mathbf{2}) \cdot$$
$$(\mathbf{2}, \mathbf{4}, \cdots, \mathbf{n} - \mathbf{n}_q - \mathbf{1}, n - 1, 1, \mathbf{n}, n - n_q - 2, n - n_q - 4, \cdots, 3) \cdot$$
$$(n - n_q, \mathbf{n} - \mathbf{n}_q + \mathbf{1}).$$

Now we leave it for the reader to verify that the fixed points are as claimed.

Case 1. $\mathbf{n} - \mathbf{n}_q - \mathbf{n}_p - \mathbf{2} \equiv 0 \pmod 4$.

We write the cycles of $[\theta_p, s\theta_q^{-1}s]$ and let the reader verify the product. $[\theta_p, s\theta_q^{-1}s] =$

$$(1, \mathbf{2}) \cdot$$
$$(n_p - n_q - 1, n - n_q - 2, n - n_q - 6, \cdots, n_p, \mathbf{n}_p - \mathbf{n}_q + \mathbf{2}) \cdot$$
$$(n_p - 2, n_p - 4, \cdots, n_p - n_q + 1, \mathbf{n}_p - \mathbf{n}_q + \mathbf{4},$$
$$\mathbf{n}_p - \mathbf{n}_q + \mathbf{6}, \cdots, \mathbf{n}_p - \mathbf{1}, \mathbf{n}_p + \mathbf{1}) \cdot$$
$$(n - n_q, n - n_q - 4, \cdots, n_p + 6, n_p + 2, \mathbf{n}_p + \mathbf{5}, \mathbf{n}_p + \mathbf{9}, \cdots, \mathbf{n} - \mathbf{n}_q - \mathbf{1}) \cdot$$
$$(n - 1, n - 3, \cdots, n - n_q + 2, \mathbf{n} - \mathbf{n}_q + \mathbf{1}, \mathbf{n} - \mathbf{n}_q + \mathbf{3}, \cdots, \mathbf{n} - \mathbf{2}, \mathbf{n},$$
$$\mathbf{n}_p + \mathbf{3}, \mathbf{n}_p + \mathbf{7}, \cdots, \mathbf{n} - \mathbf{n}_q - \mathbf{3}).$$

Case 2. $\mathbf{n}-\mathbf{n}_p-\mathbf{n}_q \equiv 0 \pmod 4$.
$[\theta_p, s\theta_q^{-1}s] =$

$$(1, \mathbf{2})\cdot$$
$$(n_p-n_q-1, n-n_q-2, n-n_q-6, \cdots, n_p+2,$$
$$\mathbf{n}_p+\mathbf{5}, \mathbf{n}_p+\mathbf{9}, \cdots, \mathbf{n}-\mathbf{n}_q-\mathbf{3},$$
$$n-1, n-3, \cdots, n-n_q+2, \mathbf{n}-\mathbf{n}_q+\mathbf{1}, \mathbf{n}-\mathbf{n}_q+\mathbf{3}, \cdots, \mathbf{n}-\mathbf{2}, \mathbf{n},$$
$$\mathbf{n}_p+\mathbf{3}, \mathbf{n}_p+\mathbf{7}, \cdots, \mathbf{n}-\mathbf{n}_q-\mathbf{5}, \mathbf{n}-\mathbf{n}_q-\mathbf{1}, n-n_q,$$
$$n-n_q-4, \cdots, n_p+4, n_p, \mathbf{n}_p-\mathbf{n}_q+\mathbf{2})\cdot$$
$$(n_p-2, n_p-4, \cdots, n_p-n_q+1, \mathbf{n}_p-\mathbf{n}_q+\mathbf{4},$$
$$\mathbf{n}_p-\mathbf{n}_q+\mathbf{6}, \cdots, \mathbf{n}_p-\mathbf{1}, \mathbf{n}_p+\mathbf{1}).$$

10.6. *Suppose* $n_p-n_q=2$. *Then:*

(1) *If* $n-2n_p \equiv 2 \pmod 4$, *then* $[\theta_p, s\theta_q^{-1}s] =$

$$(1, n-n_p, n-n_p-4, \cdots, n_p+2, \mathbf{n}_p+\mathbf{5}, \mathbf{n}_p+\mathbf{9}, \cdots, \mathbf{n}-\mathbf{n}_p-\mathbf{1},$$
$$n-1, n-3, \cdots, n-n_p+4, \mathbf{n}-\mathbf{n}_p+\mathbf{3}, \mathbf{n}-\mathbf{n}_p+\mathbf{5}, \cdots, \mathbf{n}-\mathbf{2}, \mathbf{n},$$
$$\mathbf{n}_p+\mathbf{3}, \mathbf{n}_p+\mathbf{7}, \cdots, \mathbf{n}-\mathbf{n}_p+\mathbf{1}, n-n_p+2, n-n_p-2, \cdots, n_p, \mathbf{4}, \mathbf{2})\cdot$$
$$(\mathbf{6}, \mathbf{8}, \cdots, \mathbf{n}_p+\mathbf{1}, n_p-2, , n_p-4, \cdots, 5, 3).$$

(2) *If* $n-2n_p \equiv 0 \pmod 4$, *then* $[\theta_p, s\theta_q^{-1}s] =$

$$(1, n-n_p, n-n_p-4, \cdots, n_p, \mathbf{4}, \mathbf{2})\cdot$$
$$(\mathbf{6}, \mathbf{8}, \cdots, \mathbf{n}_p+\mathbf{1}, n_p-2, n_p-4, \cdots, 5, 3)\cdot$$
$$(n-1, n-3, \cdots, n-n_p+4, \mathbf{n}-\mathbf{n}_p+\mathbf{3}, \mathbf{n}-\mathbf{n}_p+\mathbf{5},$$
$$\cdots, \mathbf{n}-\mathbf{2}, \mathbf{n}, \mathbf{n}_p+\mathbf{3}, \mathbf{n}_p+\mathbf{7}, \cdots, \mathbf{n}-\mathbf{n}_p-\mathbf{1})\cdot$$
$$(n-n_p+2, n-n_p-2, \cdots, n_p+2, \mathbf{n}_p+\mathbf{5}, \mathbf{n}_p+\mathbf{9}, \cdots, \mathbf{n}-\mathbf{n}_p+\mathbf{1}).$$

Proof. By 10.4.5, $[\theta_p, s\theta_q^{-1}s] =$

$$g^{(n_q-n_p)}\theta_q^{-1}s\theta_q s g^{(n_p-n_q)}\cdot$$
$$\theta_q s\theta_q^{-1}s$$

so by 10.4, (replacing n_q by $n_p - 2$), $[\theta_p, s\theta_q^{-1}s] =$

$$(\mathbf{n}_p, \mathbf{2}, n-1, n-3, \cdots, n-n_p+2, \cdots, n_p+2,$$
$$\mathbf{n}_p+\mathbf{3}, \mathbf{n}_p+\mathbf{5}, \cdots, \mathbf{n}-\mathbf{2}, 1, \mathbf{n}, \mathbf{n}_p+\mathbf{1})(3, \mathbf{4}) \cdot$$
$$(\mathbf{2}, \mathbf{4}, \cdots, \mathbf{n}-\mathbf{n}_p+\mathbf{1}, n-1, 1, \mathbf{n}, n-n_p, n-n_p-2, \cdots, 3) \cdot$$
$$(n-n_p+2, \mathbf{n}-\mathbf{n}_p+\mathbf{3}).$$

Case 1. $\mathbf{n}-\mathbf{2n}_p-\mathbf{2} \equiv 0 \pmod 4$.

We write the cycles of $[\theta_p, s\theta_q^{-1}s]$ and let the reader verify the product.

$$[\theta_p, s\theta_q^{-1}s] =$$
$$(1, n-n_p, n-n_p-4, \cdots, n_p+2, \mathbf{n}_p+\mathbf{5}, \mathbf{n}_p+\mathbf{9}, \cdots, \mathbf{n}-\mathbf{n}_p-\mathbf{1},$$
$$n-1, n-3, \cdots, n-n_p+4, \mathbf{n}-\mathbf{n}_p+\mathbf{3}, \mathbf{n}-\mathbf{n}_p+\mathbf{5}, \cdots, \mathbf{n}-\mathbf{2}, \mathbf{n},$$
$$\mathbf{n}_p+\mathbf{3}, \mathbf{n}_p+\mathbf{7}, \cdots, \mathbf{n}-\mathbf{n}_p+\mathbf{1}, n-n_p+2, n-n_p-2, \cdots, n_p, \mathbf{4}, \mathbf{2}) \cdot$$
$$(\mathbf{6}, \mathbf{8}, \cdots, \mathbf{n}_p+\mathbf{1}, n_p-2, n_p-4, \cdots, 5, 3).$$

Case 2. $\mathbf{n}-\mathbf{2n}_p \equiv 0 \pmod 4$

$$[\theta_p, s\theta_q^{-1}s] =$$
$$(1, n-n_p, n-n_p-4, \cdots, n_p, \mathbf{4}, \mathbf{2}) \cdot$$
$$(\mathbf{6}, \mathbf{8}, \cdots, \mathbf{n}_p+\mathbf{1}, n_p-2, n_p-4, \cdots, 5, 3) \cdot$$
$$(n-1, n-3, \cdots, n-n_p+4, \mathbf{n}-\mathbf{n}_p+\mathbf{3}, \mathbf{n}-\mathbf{n}_p+\mathbf{5},$$
$$\cdots, \mathbf{n}-\mathbf{2}, \mathbf{n}, \mathbf{n}_p+\mathbf{3}, \mathbf{n}_p+\mathbf{7}, \cdots, \mathbf{n}-\mathbf{n}_p-\mathbf{1}) \cdot$$
$$(n-n_p+2, n-n_p-2, \cdots, n_p+2, \mathbf{n}_p+\mathbf{5}, \mathbf{n}_p+\mathbf{9}, \cdots, \mathbf{n}-\mathbf{n}_p+\mathbf{1}).$$

We can now complete the proof of Theorem 10.2.

Proof of Theorem 10.2. First we show that (1) implies (2). Since Γ is transitive, $C_G(\Gamma)$ is a semi-regular subgroup of G. But $[\theta_p, C_G(\Gamma)] = 1$, and θ_p has a single fixed point, hence $C_G(\Gamma) = 1$.

We proceed with the proof of (1). Assume first that $p = q$. Then $\theta_q s\theta_q^{-1}s \in \Gamma$. Recall from 10.4 that

$$\theta_q s\theta_q^{-1}s =$$
$$(\mathbf{2}, \mathbf{4}, \cdots, \mathbf{n}-\mathbf{n}_q-\mathbf{1}, n-1, 1, \mathbf{n}, n-n_q-2, n-n_q-4,$$
$$\cdots, 3)(n-n_q, \mathbf{n}-\mathbf{n}_q+\mathbf{1}).$$

Hence $\{1, \mathbf{2}, 3, \mathbf{4}, \cdots, \mathbf{n}-\mathbf{n}_q-\mathbf{1}\}$ are in the same orbit of Γ. However, since $q \geq 3$, $n-n_q-1 > n_q$, and the above set contains a representative from each orbit of θ_q. Hence $\{1, 2, \cdots, n-1\}$ are in the same orbit of Γ, and looking at $\theta_q s \theta_q^{-1} s$, we see that n is also there.

Suppose next that $n_p - n_q > 2$. Note that $[\theta_p, s\theta_q^{-1}s] \in \Gamma$. Assume first that $n - n_q - n_p \equiv 2 \pmod 4$. We use 10.5.2. We write the cycles in $[\theta_p, s\theta_q^{-1}s]$

$$\sigma_1 = (1, \mathbf{2})$$

$$\sigma_2 = (n_p - n_q - 1, n - n_q - 2, n - n_q - 6, \cdots, n_p, \mathbf{n}_p - \mathbf{n}_q + \mathbf{2})$$

$$\begin{aligned}\sigma_3 = (&n_p - 2, n_p - 4, \cdots, n_p - n_q + 1,\\ &\mathbf{n}_p - \mathbf{n}_q + \mathbf{4}, \mathbf{n}_p - \mathbf{n}_q + \mathbf{6}, \cdots, \mathbf{n}_p - \mathbf{1}, \mathbf{n}_p + \mathbf{1})\end{aligned}$$

$$\begin{aligned}\sigma_4 = (&n - n_q, n - n_q - 4, \cdots, n_p + 4, n_p + 2,\\ &\mathbf{n}_p + \mathbf{5}, \mathbf{n}_p + \mathbf{9}, \cdots, \mathbf{n} - \mathbf{n}_q + \mathbf{1})\end{aligned}$$

$$\begin{aligned}\sigma_5 = (&n - 1, n - 3, \cdots, n - n_q + 2, \mathbf{n} - \mathbf{n}_q + \mathbf{1}, \mathbf{n} - \mathbf{n}_q + \mathbf{3},\\ &\cdots, \mathbf{n} - \mathbf{2}, \mathbf{n}, \mathbf{n}_p + \mathbf{3}, \mathbf{n}_p + \mathbf{7}, \cdots, \mathbf{n} - \mathbf{n}_q - \mathbf{3}).\end{aligned}$$

Recall that the orbits of θ_p are

$$X_i = \{i, n_p + i, 2n_p + i, \cdots, (p-1)n_p + i\}, \quad 1 \le i \le n_p.$$

Let $\mathcal{O}$ be the orbit of 1 (under Γ), then $\operatorname{supp}(\sigma_1) \subseteq \mathcal{O}$. Note that $1, n_p + 1 \in X_1$ hence $\operatorname{supp}(\sigma_3) \subseteq \mathcal{O}$. Note that $n_p - 1, n - 2 \in X_{n_p - 1}$, hence $\operatorname{supp}(\sigma_5) \subseteq \mathcal{O}$. Note that $2, n_p + 2 \in X_2$, hence $\operatorname{supp}(\sigma_4) \subseteq \mathcal{O}$. Also $n_p, n-1 \in X_{n_p}$, hence $\operatorname{supp}(\sigma_2) \subseteq \mathcal{O}$. Since no two elements in $\operatorname{Fix}([\theta_p, s\theta_q^{-1}s])$, are in the same orbit of θ_p, $\mathcal{O} = \{1, 2, \cdots, n\}$ and Γ is transitive.

Assume next that $n - n_q - n_p \equiv 0 \pmod 4$. We use 10.5.3. We write the cycles in $[\theta_p, s\theta_q^{-1}s]$

$$\gamma_1 = (1, \mathbf{2}).$$

$$\begin{aligned}\gamma_2 = (&n_p - n_q - 1, n - n_q - 2, n - n_q - 6, \cdots, n_p + 2,\\ &\mathbf{n}_p + \mathbf{5}, \mathbf{n}_p + \mathbf{9}, \cdots, \mathbf{n} - \mathbf{n}_q - \mathbf{3},\\ &n - 1, n - 3, \cdots, n - n_q + 2, \mathbf{n} - \mathbf{n}_q + \mathbf{1}, \mathbf{n} - \mathbf{n}_q + \mathbf{3}, \cdots, \mathbf{n} - \mathbf{2}, \mathbf{n},\\ &\mathbf{n}_p + \mathbf{3}, \mathbf{n}_p + \mathbf{7}, \cdots, \mathbf{n} - \mathbf{n}_q - \mathbf{5}, \mathbf{n} - \mathbf{n}_q - \mathbf{1},\\ &n - n_q, n - n_q - 4, \cdots, n_p + 4, n_p, \mathbf{n}_p - \mathbf{n}_q + \mathbf{2}).\end{aligned}$$

$$\begin{aligned}\gamma_3 = (&n_p - 2, n_p - 4, \cdots, n_p - n_q + 1,\\ &\mathbf{n}_p - \mathbf{n}_q + \mathbf{4}, \mathbf{n}_p - \mathbf{n}_q + \mathbf{6}, \cdots, \mathbf{n}_p - \mathbf{1}, \mathbf{n}_p + \mathbf{1}).\end{aligned}$$

Let $\mathcal{O}$ be the orbit of 1. Then $\operatorname{supp}(\gamma_1) \subseteq \mathcal{O}$. Then, as $1,\ n_p+1 \in X_1$, $\operatorname{supp}(\gamma_3) \subseteq \mathcal{O}$, and as $2,\ n_p+2 \in X_2$, $\operatorname{supp}(\gamma_2) \subseteq \mathcal{O}$, so as above, $\mathcal{O} = \{1, 2, \cdots, n\}$.

Finally, suppose that $n_p - n_q = 2$. Assume first that $n - 2n_p \equiv 2 \pmod 4$. We use 10.6.1. We write the cycles in $[\theta_p, s\theta_q^{-1}s]$

$$\alpha_1 = (1, n-n_p, n-n_p-4, \cdots, n_p+2, \mathbf{n}_p+\mathbf{5}, \mathbf{n}_p+\mathbf{9}, \cdots, \mathbf{n}-\mathbf{n}_p-\mathbf{1},$$
$$n-1, n-3, \cdots, n-n_p+4, \mathbf{n}-\mathbf{n}_p+\mathbf{3}, \mathbf{n}-\mathbf{n}_p+\mathbf{5}, \cdots, \mathbf{n}-\mathbf{2}, \mathbf{n},$$
$$\mathbf{n}_p+\mathbf{3}, \mathbf{n}_p+\mathbf{7}, \cdots, \mathbf{n}-\mathbf{n}_p+\mathbf{1}, n-n_p+2, n-n_p-2, \cdots, n_p, \mathbf{4}, \mathbf{2}).$$
$$\alpha_2 = (\mathbf{6}, \mathbf{8}, \cdots, \mathbf{n}_p+\mathbf{1}, n_p-2, n_p-4, \cdots, 5, 3).$$

Let $\mathcal{O}$ be the orbit of 1. Then $\operatorname{supp}(\alpha_1) \subseteq \mathcal{O}$. Then as $1,\ n_p+1 \in X_1$, $\operatorname{supp}(\alpha_2) \subseteq \mathcal{O}$ so $\mathcal{O} = \{1, 2, \cdots, n\}$.

Finally, assume that $n - 2n_p \equiv 0 \pmod 4$. We use 10.6.2. We write the cycles in $[\theta_p, s\theta_q^{-1}s]$

$$\beta_1 = (1, n-n_p, n-n_p-4, \cdots, n_p, \mathbf{4}, \mathbf{2})$$
$$\beta_2 = (\mathbf{6}, \mathbf{8}, \cdots, \mathbf{n}_p+\mathbf{1}, n_p-2, n_p-4, \cdots, 5, 3)$$
$$\beta_3 = (n-1, n-3, \cdots, n-n_p+4,$$
$$\mathbf{n}-\mathbf{n}_p+\mathbf{3}, \mathbf{n}-\mathbf{n}_p+\mathbf{5}, \cdots, \mathbf{n}-\mathbf{2}, \mathbf{n}, \mathbf{n}_p+\mathbf{3}, \mathbf{n}_p+\mathbf{7}, \cdots, \mathbf{n}-\mathbf{n}_p-\mathbf{1})$$
$$\beta_4 = (n-n_p+2, n-n_p-2, \cdots, n_p+2, \mathbf{n}_p+\mathbf{5}, \mathbf{n}_p+\mathbf{9}, \cdots, \mathbf{n}-\mathbf{n}_p+\mathbf{1}).$$

Let $\mathcal{O}$ be the orbit of 1. Then $\operatorname{supp}(\beta_1) \subseteq \mathcal{O}$. Then as $1,\ n_p+1 \in X_1$, $\operatorname{supp}(\beta_2) \subseteq \mathcal{O}$, and as $3,\ n_p+3 \in X_3$, $\operatorname{supp}(\beta_3) \subseteq \mathcal{O}$. Now, since 2, $n_p+2 \in X_2$, $\operatorname{supp}(\beta_4) \subseteq \mathcal{O}$, so $\mathcal{O} = \{1, 2, \cdots, n\}$. This completes the proof of Theorem 10.2.

11. The Sporadic Groups.

In this short section we point out the following theorem.

Theorem 11.1. *Let L be a Sporadic finite simple group. Then $\Delta(L)$ is disconnected.*

Proof. Let L be a sporadic group. We show that there exists a prime $p = p(L)$, such that if $x \in L$ is an element of order p, then $C_L(x) = \langle x \rangle$. Of course $\langle x \rangle - \{1\}$ is a connected component of $\Delta(L)$. We use the Atlas [**2**]. The following table gives the value of $p(L)$.

L	$p(L)$	L	$p(L)$	L	$p(L)$
M_{11}	11	M_{12}	11	M_{22}	11
M_{23}	23	M_{24}	23	Co_1	23
Co_2	23	Co_3	23	J_1	19
J_2	7	J_3	19	J_4	43
Fi_{22}	13	Fi_{23}	23	Fi'_{24}	29
F_1	71	F_2	47	F_3	31
F_5	19	He	17	McL	11
HS	11	Suz	13	O'N	31
Ly	67	Ru	29		

12. Concluding results.

In this section we prove Theorem 4 of the introduction and present related results on division algebras. In addition, we include a number of results and remarks related to the commuting graph of the classical groups. Throughout $\mathfrak{G}$ will denote a connected reductive algebraic group over an algebraically closed field defined over an infinite field K. Let $\mathfrak{G}(K)$ denote the K rational points.

12.1. ([**10**, Thm. 2.2].) Let $\mathfrak{G}$ be a connected nonabelian reductive group defined over an infinite field K. Then $\mathfrak{G}(K)$ is Zariski dense in $\mathfrak{G}$.

12.2. *Let K be an abelian field and $\mathfrak{G}$ a nonabelian reductive algebraic group defined over K. Then:*

1. $\mathfrak{G}(K)/Z(\mathfrak{G}(K))$ *does not have finite exponent.*
2. *Let $Z \leq Z(\mathfrak{G}(K))$. If A/Z is an abelian normal subgroup of $\mathfrak{G}(K)/Z$, then $A \leq Z(\mathfrak{G}(K))$.*
3. $\mathfrak{G}(K)$ *is not solvable.*

Proof. By 12.1, $\mathfrak{G}(K)$ is Zariski dense in $\mathfrak{G}$. As centralizers of elements in $\mathfrak{G}$ are Zariski closed, it follows that $Z(\mathfrak{G}(K)) \leq Z(\mathfrak{G})$. Then $\mathfrak{G}(K)/Z(\mathfrak{G}(K))$ is Zariski dense in $\mathfrak{G}/Z(\mathfrak{G}(K))$.

(1): If $\mathfrak{G}/Z(\mathfrak{G}(K))$ has exponent n, then, as the set of elements of order n in $\mathfrak{G}/Z(\mathfrak{G}(K))$ is Zariski closed, this forces $\mathfrak{G}/Z(\mathfrak{G}(K))$ to be of finite exponent. But this is clearly false as seen by considering a torus.

Let $Z \leq Z(\mathfrak{G}(K))$ and suppose $1 < A/Z \lhd \mathfrak{G}(K)/Z$ with A/Z abelian. The Zariski closure, say B/Z, of A/Z in $\mathfrak{G}/Z$ is abelian (indeed the center of $\bigcap_{a\in A} C_{\mathfrak{G}/Z}(Za)$ is a closed abelian subgroup of $\mathfrak{G}/Z$ containing A/Z). Also B/Z is normalized by $\mathfrak{G}(K)/Z$. Now normalizers are closed, so B/Z is an abelian normal closed subgroup in $\mathfrak{G}/Z$. But as $\mathfrak{G}$ is a connected reductive group, $B \leq Z(\mathfrak{G})$, a contradiction. This proves (2) and (3) follows.

Corollary 12.3. *Let D be a division algebra over K. Then D^* is not solvable.*

Proof. This follows from 12.2.3 by noting that D^* can be realized as the K rational points of GL_d, where $d = \deg(D)$.

We can now derive Theorem 4 of the introduction.

Theorem 12.4. *Let D be a finite dimensional division algebra over a number field K. Let N be a noncentral normal subgroup of D^*. Then D^*/N solvable.*

Proof. Let $S := SL_1(D)$ be the elements of D^* whose reduced norm is 1. Then $N/(N \cap S) \cong NS/S$ is abelian, so by 12.2.2, $N \cap S$ is noncentral in D^* (alternatively, use [**13**]).

Hence it suffices to show that if M is a noncentral normal subgroup of $SL_1(D)$, then $SL_1(D)/M$ is solvable. Here we take $\mathfrak{G}$ a simple, simply connected algebraic group of type A_n such that $\mathfrak{G}(K) = SL_1(D)$.

Suppose $M \lhd \mathfrak{G}(K)$ and M is not central. We apply Theorem 2 (of the introduction). If $T = \emptyset$, then $M = \mathfrak{G}(K)$ and there is nothing to prove. Thus we suppose $T \neq \emptyset$. Hence we can consider $\mathfrak{G}(K) < \prod_{v \in T} \mathfrak{G}(K_v)$, via the diagonal embedding. By Theorem 2, $M = \mathfrak{G}(K) \cap L$, where $L \lhd \prod_{v \in T} \mathfrak{G}(K_v)$, with L open. Then $\mathfrak{G}(K)/M = \mathfrak{G}(K)/(\mathfrak{G}(K) \cap L) \cong \mathfrak{G}(K)L/L$ and so it suffices to show that $\prod_{v \in T} \mathfrak{G}(K_v)/L$ is solvable.

Notice that for each $v \in T$, $[\mathfrak{G}(K_v), L] \leq \mathfrak{G}(K_v) \cap L$ is a normal subgroup of $\mathfrak{G}(K_v)$ and of course $\prod_{v \in T} \mathfrak{G}(K_v)/L$ is an image of $\prod_{v \in T}(\mathfrak{G}(K_v)/[\mathfrak{G}(K_v), L])$. So it suffices to show that $\mathfrak{G}(K_v)/[\mathfrak{G}(K_v), L]$ is solvable. Let M_v (resp. L_v) be the projection of M (resp. L) on $\mathfrak{G}(K_v)$. Since M is noncentral in $\mathfrak{G}(K)$, M_v and hence L_v is noncentral in $\mathfrak{G}(K_v)$. Then, by 12.2.2, $[\mathfrak{G}(K_v), L] = [\mathfrak{G}(K_v), L_v]$ is noncentral in $\mathfrak{G}(K_v)$. Then, by [**12**] (see also [**10**, Prop. 1.8, p. 32]), $[\mathfrak{G}(K_v), L]$ contains C_s, for some s, where C_s are the congruence subgroups of $\mathfrak{G}(K_v) = SL_1(D_v)$ (where $D_v = D \otimes_K K_v$). These congruence subgroups are defined in [**10**, p. 31 (1.4.4)]. Since $\mathfrak{G}(K_v)/C_s$ is solvable ([**10**, Corollary, p. 32]), we are done.

Next we focus our attention on the commuting graph of the classical groups. We mention that as noted in Theorem 5 of the Introduction, the elements x, y required for showing that $\Delta(L)$ is balanced can be taken as opposite unipotent elements. We remark that except for some small cases this usually implies $d(x, y) = 4$. To see this note that $C_L(x), C_L(y)$ contain root elements r, s lying in root groups corresponding to opposite long roots of the root system. The normalizer of these root groups are opposite parabolic subgroups, hence contain a common Levi factor. Choosing $1 \neq t$ in this Levi factor (which is possible in all but a few cases) we have a path x, r, t, s, y of length 4.

In the following theorem we use the same ϵ notation as given in the beginning of Section 9.

Theorem 12.5. *Let $G(q)$ be a simple classical group with $q > 5$. Then $\Delta(G(q))$ is disconnected if and only if one of the following holds:*

(i) *$G(q) \simeq L_n^\epsilon(q)$ and n is a prime.*
(ii) *$G(q) \simeq L_n^\epsilon(q)$, $n-1$ is a prime and $q-\epsilon \mid n$.*
(iii) *$G(q) \simeq S_{2n}(q)$, $O_{2n}^-(q)$, or $O_{2n+1}(q)$ and $n = 2^c$, for some c.*

Moreover, if $\Delta(G(q))$ is connected then $\operatorname{diam}(\Delta(G(q))) \leq 10$.

Proof. Let $\hat{G}(q)$ denote the corresponding quasisimple classical group and let V be the natural module for $\hat{G}(q)$. For a nondegenerate subspace $W \leq V$, we write $I(W)$ for $GL(W), GU(W), Sp(W)$ or $SO(W)$, in the respective cases. We let $\hat{G}(W) \leq \hat{G}(q)$ be the subgroup acting trivially on $W^\perp$ (and acting trivially on a specified complement U, in the case when $\hat{G}(q) \simeq SL_n(q)$, the complement U in this case will be clear from the context).

For the orthogonal groups we assume that $\dim(V) \geq 7$. First suppose that $G(q)$ does not satisfy any of the conditions (i)-(iii). Here we will show that $\operatorname{diam}(\Delta(G(q))) \leq 10$. The following is the key step.

($*$) Each $g \in G(q)$ is at distance at most 3 from some unipotent element in $\Delta(G(q))$.

We proceed by contradiction assuming that ($*$) does not hold. If g is the commuting product of a nontrivial unipotent element and a semisimple element, then ($*$) is obvious. Therefore g is a semisimple element.

Let h be a preimage of g in $\hat{G}(q)$. Then h is contained in a maximal torus T of $I(V)$. When $I(V) \simeq SO_{2n+1}(q)$, all maximal tori are contained in $SO_{2n}^\epsilon(q)$, for $\epsilon = 1$ or -1, so here all considerations can be reduced to even dimensional orthogonal groups and we therefore ignore odd dimensional orthogonal groups in the following.

The action of T on V is completely reducible and given by Lemma 2 of [**16**] (the $q > 5$ hypothesis is sufficient to establish that lemma). Alternatively, one can obtain a suitable torus working directly from a decomposition of V under the action of h. In any case, T preserves a decomposition $V = V_1 \perp \ldots \perp V_k \perp (V_{k+1} \oplus V'_{k+1}) \perp \ldots \perp (V_\ell \oplus V'_\ell)$, where if we set $\dim(V_i) = r_i$, $1 \leq i \leq \ell$, then $r_1 \geq \ldots \geq r_k$, and for $k < i \leq \ell$, $\dim(V_i) = \dim(V'_i)$, with both subspaces being totally singular.

Corresponding to this decomposition we have $T = T_1 \times \cdots \times T_\ell$, such that for $1 \leq i \leq \ell$, T_i induces a Singer cycle on V_i and for $k < i \leq \ell$, T_i also induces a Singer cycle on V'_i. We note that $k = \ell$ in the general linear case. Also for $1 \leq i \leq k$, one of the following holds: $|T_i| = q^{r_i} - 1$, $q^{r_i} + 1$ (with r_i odd), $q^{r_i/2} + 1$, $q^{r_i/2} + 1$, with $I(V_i) = GL_{r_i}(q), GU_{r_i}(q), Sp_{r_i}(q)$, or $SO_{r_i}^-(q)$, respectively. We make a series of reductions under the assumption that $(*)$ fails to hold for g.

Step 1. $\dim(V_i) = 1$, for each $i > k$.

For suppose $k < i \le \ell$ and $\dim(V_i) > 1$, $T_i \le GL_{r_i}(q)$ ($GL_{r_i}(q^2)$ in the unitary case) with dual action on V_i and V_i'. Then T_i contains a subgroup Z_i of order $q-1$ (q^2-1 in the unitary case) which induces (inverse) scalars on V_i, and V_i'. Elements of Z_i have determinant 1 and since we are assuming $q > 5$, we can find a noncentral element of Z_i in $\hat{G}(q)$. Since all elements of this group centralize unipotent elements of $GL_{r_i}(q)$, we obtain $(*)$ in this case, a contradiction.

Step 2. $\ell \le k+1$, if $G(q) \ne O^{\epsilon}_{2n}(q)$. Otherwise $\ell \le k+2$.

For suppose $\ell > k$. Then Z_{k+1} centralizes $\hat{G}(V_{k+2} \oplus \cdots \oplus V_\ell')$, so this group contains no unipotent elements. Hence either $\ell = k+1$, or $G(q)$ is an orthogonal group and $\ell = k+2$.

Step 3. $k = \ell$.

First assume $k = 0$. Then Step 1 and Step 2 show that either $\dim(V) = 2$, or $\dim(V) = 4$, with $G(q) \simeq O_4^-(q)$ (as $G(q)$ is simple). In either case (i) or (iii) holds, a contradiction. Now suppose $0 < k < \ell$. Then Z_ℓ commutes with $\hat{G}(V_1 \oplus \cdots \oplus V_k)$ and the latter group contains unipotent elements unless either $V_1 \oplus \cdots \oplus V_k$ is a 2-dimensional orthogonal space or a 1-dimensional unitary space (we already mentioned that $k = \ell$ if $G(q) \simeq L_n(q)$). In the former case Step 2 implies $\dim(V) \le 6$, against our supposition. And in the unitary case, $\dim(V) = 3$ and hence satisfies (i). This is again a contradiction.

Step 4. $r_1 > 1$.

Suppose $r_1 = 1$. This can only occur for $G(q) = L_n^\epsilon(q)$. We are assuming that (i) does not hold, so here $k = n \ge 4$. Then $(T_1 \times T_2) \cap \hat{G}(q)$ contains a noncentral subgroup of order $q - \epsilon$ centralizing unipotent elements in $\hat{G}(V_3 \oplus \cdots \oplus V_k)$, a contradiction.

Step 5. Either $V = V_1$ or $G(q) = L_n^\epsilon(q)$, $V = V_1 \oplus V_2$, and $\dim(V_2) = 1$.

It follows from Step 4 that T_1 contains noncentral elements of $\hat{G}(q)$. Since we are assuming that $(*)$ does not hold, $\hat{G}(V_2 \oplus \cdots \oplus V_k)$ contains no non-identity unipotent elements.

If $G = L_n^\epsilon(q)$, this forces $\dim(V_2 \oplus \cdots \oplus V_k) \le 1$. In the symplectic case, necessarily $V = V_1$. We argue that this holds for the orthogonal case as well. For otherwise, $k = 2$ and $\dim(V_2) = 2$. Hence $\dim(V_1) \ge 5$. But then there are noncentral elements of T_2 which centralize unipotent elements of $\hat{G}(V_1)$, a contradiction.

We now treat the remaining configurations. First assume $V = V_1$, so that $r_1 = n$. If $G(q) = L_n^\epsilon(q)$, then $|T| = q^n - \epsilon$. Also n is odd in the unitary case.

We are assuming that n is not a prime, so we may write $n = rs$, with $r, s > 1$ and such that s is odd in the unitary case. Then there is a (cyclic) subgroup $E < T$ of order $q^r - \epsilon$ intersecting $\hat{G}(q)$ in a noncentral subgroup. As T acts irreducibly on V, E acts homogeneously, so that $V = W_1 \oplus \cdots \oplus W_s$, with each W_i of dimension r and irreducible under the action of E. In the unitary case where s is odd, it is easily checked that we may take W_1 nondegenerate and perpendicular to the remaining summands. Now h centralizes E which in turn centralizes a Singer cycle in $\hat{G}(W_1)$. This Singer cycle centralizes a unipotent element in $\hat{G}(W_2 \oplus \cdots \oplus W_s)$ so we have ($*$), a contradiction.

In the symplectic and orthogonal cases, we have $|T| = q^n + 1$. Here we are assuming that n is not a power of 2, so the same argument works.

The final case is where $V = V_1 \oplus V_2$, with $\dim(V_2) = 1$ and $G = L_n^\epsilon(q)$. Then $r_1 = n - 1$. If $n - 1$ is not a prime, we argue as above, working in $SL_{n-1}^\epsilon(q)$. Suppose $n - 1$ is a prime. Then T contains a subgroup of order $(q-\epsilon)^2$ which induces scalars on V_i. Intersecting with $\hat{G}(q)$ we get a group of order $q - \epsilon$ so this gives a noncentral element centralizing a unipotent element of $\hat{G}(V_1)$, unless $q - \epsilon \mid n$. This concludes the proof of ($*$).

It is now an easy matter to show that $\Delta(G(q))$ is connected of diameter at most 10. By ($*$) g is at distance at most 3 from a nontrivial unipotent element of $G(q)$. The center of a maximal unipotent subgroup of $G(q)$ contains long root elements. Hence g is at distance at most 4 from a long root element.

Now let $g, g' \in \Delta(G(q))$. Let u, u' be long root elements at distance at most 4 from g, g' respectively. It is well-known that either u, u' commute, lie in an extraspecial p-subgroup (hence commute with the center), or lie in a group $J = SL_2(q)$ generated by the long root subgroups corresponding to u, u'. In the latter case, we can choose a root element w lying in a conjugate of J and commuting with J. This completes the argument.

To complete the proof of the theorem we now assume that $G(q)$ satisfies either (i), (ii) or (iii). Here we argue that $\Delta(G(q))$ is disconnected. If (i) holds with $n = p$ a prime, then $GL_p^\epsilon(q)$ contains a cyclic maximal torus T of order $q^p - \epsilon$. If $p = 2$, then we immediately see that opposite unipotent elements cannot be joined. So assume p is odd. Let $h \in E = T \cap SL_p^\epsilon(q)$ with $h \notin Z(SL_p^\epsilon(q))$. So h acts irreducibly on V. Suppose $y \in SL_p^\epsilon(q)$ centralizes h projectively. Hence $h^y = hz$, where $z \in Z(SL_p^\epsilon(q))$. The centralizer of h and of h^y in $SL_p^\epsilon(q)$ is E, so y normalizes E, hence induces an automorphism on E of order dividing p. Hence z has order dividing $(p, q - \epsilon)$. So either $z = 1$, or is of order p. In the latter case, by 8.3, $|E/(E \cap Z(SL_p^\epsilon(q)))|$ has order prime to p, so we may assume h has order prime to p, and this also forces $z = 1$. But the centralizer of h in $SL_p^\epsilon(q)$ is E, so the image of $E - \{1\}$ in $G(q)$ is a connected component of $\Delta(G(q))$.

The same argument applies if (iii) holds, taking T to be a Singer cycle of order q^n+1 and noting that the resulting torus of the simple group has odd order.

The last case is where (ii) holds with $n-1=p$ a prime and $q-\epsilon$ dividing $n=p+1$. In this case take a decomposition $V=V_1\perp V_2$, with $\dim(V_1)=p$. Then $GL_n^\epsilon(q)$ contains a maximal torus $T_1\times T_2$ of order $(q^p-\epsilon)(q-\epsilon)$. The resulting torus $E<SL_n^\epsilon(q)$ has order $(q^p-\epsilon)$ and in the simple group the torus has order $(q^p-\epsilon)/(q-\epsilon)$. The argument is thus the same as in the case where (i) holds. This completes the proof of Theorem 12.5.

Remarks. (1) In the papers [**19**] and [**4**] the connected components of the prime graph of all nonabelian finite simple groups are determined. It is easy to see that the prime graph is connected if and only if the commuting graph is connected. Thus the nonabelian finite simple groups L for which $\Delta(L)$ is disconnected are known. We note that in the connected case of Theorem 12.2 we prove that the diameter of $\Delta(G(q))$ is bounded.

(2) We assume $q>5$, in the above result, in order to simplify the statement and the proof. With extra work one should be able to obtain information for smaller values of q. However, there will be additional examples where the graph is disconnected.

References

[1] A. Borel, R. Carter, N. Iwahori, T.A. Springer and R. Steinberg, *Seminar on Algebraic Groups and Related Finite Groups*, Lecture Notes in Math., **131**, Springer-Verlag, 1970, MR 48 #11106, Zbl 192.36201.

[2] J.H. Conway et al, *Atlas of Finite Groups*, Clarendon Press, Oxford, 1985, MR 88g:20025, Zbl 568.20001.

[3] R.H. Dye, *A geometric characterization of the special orthogonal groups and the Dickson invariant*, J. London Math. Soc., **15**(**2**) (1977), 472-476, MR 56 #11899, Zbl 358.20054.

[4] N. Iiyori and H. Yamaki, *Prime graph components of the simple groups of Lie type over the fields of even characteristic*, J. Algebra, **115** (1993), 335-343, MR 94e:05268, Zbl 799.20016; *Corrections*, J. Algebra, **181** (1996), 659, CMP 1 383 487.

[5] P. Kleidman, *The maximal subgroups of the Steinberg triality groups* $^3D_4(q)$ *and their automorphism groups*, J. Algebra, **115**(**1**) (1988), 182-199, MR 89f:20024, Zbl 642.20013.

[6] M. Liebeck and G. Seitz, *Reductive subgroups of exceptional algebraic groups*, Memoirs of the AMS, **121** (1996), MR 96i:20059, Zbl 851.20045.

[7] K. Mizuno, *The conjugate classes of Chevalley groups of type* E_6, J. Fac. Sci. Tokyo Univ. IA-Math., **24** (1977), 525-563, MR 58 #5951, Zbl 399.20044.

[8] ———, *The conjugate classes of unipotent elements of Chevalley groups* E_7 *and* E_8, Tokyo J. Math., **3**(**2**) (1980), 391-459, MR 82m:20046, Zbl 454.20046.

[9] K. Motose, *On values of cyclotomic polynomials* II, Math. J. of Okayama Univ., **37** (Dec. 1995), 27-36, MR 97h:11151.

[10] V. Platonov and A. Rapinchuk, *Algebraic Groups and Number Theory*, 'Nauka' Publishers, Moscow, 1991; English translation: Pure and Applied Mathematics series, **139**, Academic Press, 1994, MR 95b:11039, Zbl 732.20027.

[11] A. Potapchik and A. Rapinchuk, *Normal subgroups of $SL_{1,D}$ and the classification of finite simple groups*, Proc. Indian Acad. Sci. (Math. Sci.), **106**(**4**) (1996), 329-368, MR 98i:20049, Zbl 879.20027.

[12] C. Riehm, *The norm* 1 *group of p-adic division algebras*, Amer. J. Math., **92**(**2**) (1970), 499-523, MR 1 #6860, Zbl 199.37601.

[13] W.R. Scott, *On the multiplicative group of a division ring*, Proc. Amer. Math. Soc., **8** (1957), 303-305, MR 18,788g, Zbl 079.05402.

[14] Y. Segev, *On finite homomorphic images of the multiplicative group of a division algebra*, Ann. of Math., **149** (1999), 219-251, MR 2000e:16022, Zbl 935.20009.

[15] G.M. Seitz, *Generation of finite groups of Lie type*, Trans. AMS, **271**(**2**) (1982), 351-407, MR 83h:20021, Zbl 514.20013.

[16] ———, *On the subgroup structure of classical groups*, Communications in Algebra, **10** (1982), 875-885, MR 83k:20052, Zbl 483.20026.

[17] K. Shinoda, *The conjugacy classes of the finite Ree groups of type* (F_4), J. Fac. Sci. Tokyo Univ. IA-Math., **22** (1975), 1-15, MR 51 #8281, Zbl 306.20014.

[18] P.H. Tiep and A.E. Zalesskii, *Minimal characters of the finite classical groups*, Comm. in Alg., **24**(**6**) (1996), 2093-2167, MR 97f:20018, Zbl 901.20031.

[19] J.S. Williams, *Prime graph components of finite groups*, J. Algebra, **69** (1981), 485-513, MR 82j:20054, Zbl 471.20013.

Received April 28, 1999 and revised August 23, 1999. The first author was partially supported by BSF 92-003200 and by grant no. 6782-1-95 from the Israeli Ministry of Science and Art. The second author was partially supported by an NSF grant.

Ben-Gurion University
Beer-Sheva 84105, Israel
E-mail address: yoavs@math.bgu.ac.il

University of Oregon
Eugene, OR 97403-122
E-mail address: seitz@math.uoregon.edu