Regular characters of classical groups over complete discrete valuation rings

Shai Shechter

Department of Mathematics
Ben Gurion University of the Negev
Beer-Sheva 84105
Israel

Abstract

Let \( \mathfrak{o} \) be a complete discrete valuation ring with finite residue field \( k \) of odd characteristic, and let \( G \) be a symplectic or special orthogonal group scheme over \( \mathfrak{o} \). For any \( \ell \in \mathbb{N} \) let \( G^\ell \) denote the \( \ell \)-th principal congruence subgroup of \( G(\mathfrak{o}) \). An irreducible character of the group \( G(\mathfrak{o}) \) is said to be regular if it is trivial on a subgroup \( G^\ell + 1 \) for some \( \ell \), and if its restriction to \( G^\ell / G^\ell + 1 \cong \text{Lie}(G)(k) \) consists of characters of minimal \( G(k_{\text{alg}}) \)-stabilizer dimension. In the present paper we consider the regular characters of such classical groups over \( \mathfrak{o} \), and construct and enumerate all regular characters of \( G(\mathfrak{o}) \), when the characteristic of \( k \) is greater than two. As a result, we compute the regular part of their representation zeta function.

Keywords: Representations of compact p-adic groups, Representation zeta functions, Classical groups.

2010 MSC: 20C15, 20G05, 11M41.

1. Introduction

Let \( K \) be a non-archimedean local field, and let \( \mathfrak{o} \) be its valuation ring, with maximal ideal \( p \) and finite residue field \( k \) of odd characteristic. Let \( q \) and \( p \) denote the cardinality and characteristic of \( k \), respectively. Fix \( \pi \) to be a uniformizer of \( \mathfrak{o} \). Let \( G \subseteq \text{SL}_N \) be a symplectic or a special orthogonal group scheme over \( \mathfrak{o} \), i.e. the group of automorphisms of determinant 1, preserving a fixed non-degenerate anti-symmetric or symmetric \( \mathfrak{o} \)-defined bilinear form. In this article we study the set of irreducible regular characters of the group of \( \mathfrak{o} \)-points \( G = G(\mathfrak{o}) \), the definition of which we now present.

1.1. The basic definitions

Let \( \text{Irr}(G) \) denote the set of irreducible complex characters of \( G \) which afford a continuous representation with respect to the profinite topology. The level of a character \( \chi \in \text{Irr}(G) \) is the minimal number \( \ell \in \mathbb{N}_0 = \mathbb{N} \cup \{0\} \) such that the restriction of any representation associated to \( \chi \) to the principal congruence subgroup \( G^\ell + 1 = \ker (G \to G(\mathfrak{o}/p^\ell)) \) is trivial. For example, the set of characters of level 0 is naturally identified with the set of irreducible complex characters of \( G(k) \).

**Email address:** shais@post.bgu.ac.il (Shai Shechter)
1.1.1. The residual orbit of a character

Let $\mathfrak{g} = \text{Lie}(G) \subseteq \mathfrak{g}_N$ denote the Lie algebra scheme of $G$. The smoothness of $G$ implies the equality $G/G^{\ell+1} = G(\mathfrak{o}/p^{\ell+1})$, and consequently, the existence of a $G$-equivariant isomorphism of abelian groups between $\mathfrak{g}(k)$ and the quotient group $G^{\ell}/G^{\ell+1}$, for any $\ell \geq 1$ (see [9, II, §4, no. 3]). In the notation of [9], this isomorphism is denoted $x \mapsto e^{ix}$. The action of $G$ by conjugation on the quotient $G^{\ell}/G^{\ell+1}$ factors through its quotient $G(k)$, making the isomorphism above is $(G(k))$-equivariant. Additionally, by the assumption char($k$) $\neq 2$ and [25, I, Lemma 5.3], the underlying additive group of $\mathfrak{g}(k)$ can be naturally identified with its Pontryagin dual in a $G(k)$-equivariant manner. Consequently, there exists an isomorphism of $G(k)$-spaces

$$\mathfrak{g}(k) \xrightarrow{\sim} \text{Irr}(G^{\ell}/G^{\ell+1}).$$

(1.1)

Let $\chi \in \text{Irr}(G)$ have level $\ell > 0$. Consider the restriction $\chi_{G^{\ell}}$ of $\chi$ to $G^{\ell}$. By Clifford’s Theorem and the definition of level, the restricted character $\chi_{G^{\ell}}$ is equal to a multiple of the sum over a single $G(k)$-orbit of characters of $G^{\ell}/G^{\ell+1}$. Using (1.1), this orbit corresponds to a single $G(k)$-orbit in $\mathfrak{g}(k)$, which we call the residual orbit of $\chi$, and denote $\Omega_{1}(\chi) \in \text{Ad}(G(k)) \backslash \mathfrak{g}(k)$.

1.1.2. Regular characters

Let $k^{alg}$ be a fixed algebraic closure of $k$. An element of $\mathfrak{g}(k^{alg})$ is said to be regular if its centralizer in $G(k^{alg})$ has minimal dimension among such centralizers (cf. [29, §3.5]). By extension, an element of $\mathfrak{g}(k)$ is said to be regular if its image under the natural inclusion of $\mathfrak{g}(k)$ into $\mathfrak{g}(k^{alg})$ is regular.

**Definition 1.1.1** (Regular Characters). A character $\chi \in \text{Irr}(G)$ of positive level is said to be regular if its residual orbit $\Omega_{1}(\chi)$ consists of regular elements of $\mathfrak{g}(k)$.

For a general overview of regular elements in reductive algebraic groups over algebraically closed fields, we refer to [25, Ch. III]. The definition of regular characters goes back to Shintani [24] and Hill [14]. An overview of the history of regular characters of $\text{GL}_N(\mathfrak{o})$ can be found in [27]. Also see [17, 28] and [30] for the analysis of regular characters of isotropic groups of type $A_n$, as well as [23], for a partial treatment of anisotropic groups of type $A_n$.

1.2. Regular elements and regular characters

Following [14], we begin our investigation of regular characters with the study of regular elements in the finite Lie rings $\mathfrak{g}(\mathfrak{o}_m)$, where $\mathfrak{o}_m = \mathfrak{o}/p^m$ (see **Definition 3.1.1**).

A central feature of the analysis undertaken in [14] is the introduction and application of geometric methods to the study of regular characters. Given $x \in M_N(\mathfrak{o})$ and $m \in \mathbb{N}$, let $x_m$ denote the image of $x$ in $M_N(\mathfrak{o}_m)$ under the reduction map. The condition of commuting with $x_m$ defines a closed $\mathfrak{o}_m$-group subscheme of the fiber product\(^1\) $\text{GL}_N \times \mathfrak{o}_m$, which, upon application of the Greenberg functor, defines a $k$-group scheme [12, §4, Main Theorem.(5)]. The element $x_m$ is said to be regular if the group scheme thus obtained is of minimal dimension among such group schemes (see [14, Definition 3.2]). In [14, Theorem 3.6], Hill proved that $x_m \in M_n(\mathfrak{o}_m)$ is regular if and only if its image $x_1 \in M_n(k)$ is regular. Additionally, regularity of $x_m$ was shown to be equivalent to

\(^1\)The notation $G \times \mathfrak{o}_m$ is shorthand for the fiber product $G \times_{\text{Spec } k} \text{Spec } \mathfrak{o}_m$. Similar notation is used whenever the base change being performed is between spectra of rings, and the base ring of the given schemes is understood from context.
the cyclicity of the module $\mathfrak{o}_N^N$ over the ring $\mathfrak{o}_m[x_m] \subseteq M_N(\mathfrak{o}_m)$. We note that Hill’s definition of regularity is equivalent to Shintani’s definition of quasi-regularity [24, §2].

The equivalence of regularity over the ring $\mathfrak{o}_m$ and over $k$ was recently extended to general semisimple groups of type $A_n$ in [17]. In Section 3.2 we further extend this equivalence of to the generality of classical groups of type $B_n$, $C_n$ and $D_n$ in odd characteristic. However, the equivalence of regularity of an element $x_m \in g(\mathfrak{o}_m)$ with the cyclicity of the module $\mathfrak{o}_N^N$ over $\mathfrak{o}_m[x_m]$, while true in $GL_N$ and generically true in $G$ (see Lemma 4.2.1), is not a general phenomenon and in fact fails in certain cases (see Lemma 4.4.1). Nevertheless, in the present setting, it is possible to prove a supplementary result (Theorem 3.1.3), which specializes to the above equivalence in the case of $G = GL_N$, and provides us with the information needed in order to describe the inertia subgroup of such a character and enumerate the characters of $G$ lying above a given regular character. Consequently, we deduce the first main result of this article.

**Theorem I.** Let $\mathfrak{o}$ be a discrete valuation ring with finite residue field of odd characteristic, and let $\Omega \subseteq g(k)$ be an orbit consisting of regular elements and let $\ell \in \mathbb{N}$.

1. The number of regular characters $\chi \in \text{Irr}(G)$ of level $\ell$ whose residual orbit is equal to $\Omega$ is

$$\frac{|G(k)| \cdot q^{(\ell-1)n}}{|\Omega|}.$$

2. Any such character has degree $|\Omega| \cdot q^{(\ell-1)n}$, where $\alpha = \frac{\dim G - n}{2}$.

1.3. Regular representation zeta functions

Taking the perspective of representation growth, given a group $H$, one is often interested in understanding the asymptotic behaviour of the sequence $\{r_m(H)\}_{m=1}^{\infty}$, where $r_m(H) \in \mathbb{N} \cup \{0, \infty\}$ denotes the number of elements of $\text{Irr}(H)$ of degree $m$. In the case where the sequence $r_m(H)$ is bounded above by a polynomial in $m$, the representation zeta function of $H$ is defined to be the Dirichlet generating function

$$\zeta_H(s) = \sum_{m=1}^{\infty} r_m(H)m^{-s}, \quad (s \in \mathbb{C}). \quad (1.2)$$

In the specific case $H = G = G(\mathfrak{o})$, one may initially restrict to a description of the regular representation zeta function, i.e. the Dirichlet function counting only regular characters of $G$. In this respect, Theorem I implies that the rate of growth of regular characters of $G$ is polynomial of degree $\frac{2n}{\dim G - n}$. Furthermore, we obtain the following corollary.

**Corollary 1.3.1.** Let $X \subseteq \text{Ad}(G(k)) \setminus g(k)$ denote the set of orbits consisting of regular elements, and let

$$\mathcal{D}_{G(\mathfrak{o})}(s) = \sum_{\Omega \in X} |G(k)| \cdot |\Omega|^{-s+1}, \quad (s \in \mathbb{C}). \quad (1.3)$$

The regular zeta function of $G = G(\mathfrak{o})$ is of the form

$$\zeta_{G(\mathfrak{o})}^{\text{reg}}(s) = \frac{\mathcal{D}_{G(\mathfrak{o})}(s)}{1 - q^n - \alpha s}$$

where $n$ and $\alpha$ are as in Theorem I.
1.4. Classification of regular orbits in $\mathfrak{g}(k)$

The second goal of this article is to compute the regular representation zeta function of the symplectic and special orthogonal groups over $\mathfrak{o}$. In view of Corollary 1.3.1, to do so, one must classify and enumerate the regular orbits in $\mathfrak{g}(k)$, under the adjoint action of $G(k)$. This classification is undertaken in Section 4, and its consequences are summarized in Theorem 4.1.2 and Theorem 4.1.3. Our results in this section yield a uniform formula for each of the classical groups in question, which is independent of the cardinality of $k$.

Given $n \in \mathbb{N}$ let $X_n$ denote the set of triplets $\tau = (r, S, T)$, in which $r \in \mathbb{N}_0$ and $S = (S_{d,e})$ and $T = (T_{d,e})$ are $n \times n$ matrices with non-negative integer entries, satisfying the condition

$$r + \sum_{d,e=1}^{n} \text{deg}(S_{d,e} + T_{d,e}) = n. \quad (1.4)$$

Given $\tau = (r, S, T) \in X_n$, define the following polynomial in $\mathbb{Z}[t]$

$$c^\tau(t) = t^n \prod_{d,e} (1 + t^{-d})^{S_{d,e}} (1 - t^{-d})^{T_{d,e}} \quad (1.5)$$

and let $u_1(q) = |\text{Sp}_{2n}(k)| = |\text{SO}_{2n+1}(k)|$. Note that the value $u_1(q)$ is given by evaluation at $t = q$ of a polynomial $u_1(t) \in \mathbb{Z}[t]$, which is independent of $q$ (see, e.g., [35, § 3.5 and § 3.2.7]). Additionally, for any $\tau \in X_n$, let $M_\tau(q)$ denote the number of polynomials of type $\tau$ over a field of $q$ elements; see Definition 4.1.1. An explicit formula for $M_\tau(q)$ is computed in Section 4.1.1. We remark that the value of $M_\tau(q)$ is given by evaluation at $t = q$ of a uniform polynomial formula which is independent of $q$ as well; see (4.3).

**Theorem II.** Let $\mathfrak{o}$ be a complete discrete valuation ring of odd residual characteristic. Let $n \in \mathbb{N}$ and $G$ be one of the $\mathfrak{o}$-defined algebraic group schemes $\text{Sp}_{2n}$ or $\text{SO}_{2n+1}$, with $\mathfrak{g} = \text{Lie}(G)$.

Given $\tau = (r, S, T) \in X_n$ let

$$\nu(\tau) = \nu_G(\tau) = \begin{cases} 1 & \text{if } G = \text{Sp}_{2n} \text{ and } r > 0, \\ 0 & \text{otherwise}. \end{cases}$$

The Dirichlet polynomial $D_{\mathfrak{g}(\mathfrak{o})}(s)$ (see (1.3)) is given by

$$D_{\mathfrak{g}(\mathfrak{o})}(s) = \sum_{\tau \in X_n} \nu(\tau)^{-s} \cdot M_\tau(q) \cdot c^\tau(q) \cdot \left( \frac{u_1(q)}{2^{\nu(\tau)} c^\tau(q)} \right)^{-s}. \quad (1.6)$$

Recall that a symmetric bilinear form over a finite field of odd characteristic is determined by the Witt index of the form, i.e. the dimension of a maximal totally isotropic subspace with respect to the form. Following standard notation, we write $\text{SO}_{2n}^+$ and $\text{SO}_{2n}^-$ to the group schemes whose group of $k$-points are associated with a symmetric bilinear form of Witt index $n$ and $n - 1$ respectively. Also, for convenience, we often use the notation $\text{SO}_{2n}^\pm$ for $\text{SO}_{2n}^\pm$.

Given $\epsilon \in \{\pm 1\}$, let $u_2^\epsilon(q) = |\text{SO}_{2n}^\epsilon(k)|$. As in the previous case, note that the value $u_2^\epsilon(q)$ is given by evaluation at $t = q$ of a polynomial $u_2^\epsilon(t) \in \mathbb{Z}[t]$, which is independent of $q$ (see [35, § 3.2.7])

**Theorem III.** Let $\mathfrak{o}$ be a complete discrete valuation ring of odd residual characteristic, and whose residue field has more than 3 elements. Let $n \in \mathbb{N}$ and $\epsilon \in \{\pm 1\}$. Let $G^\epsilon = \text{SO}_{2n}^\epsilon$ be the $\mathfrak{o}$-defined special orthogonal group scheme, as described above, and let $\mathfrak{g}^\epsilon = \text{Lie}(G^\epsilon)$. 

4
Let $X^0_n$ denote the set of triplets $\tau = (r, S, T) \in X_n$ with $r = 0$, and let $X^0_{n,+1}$ denote the subset of $X^0_n$ consisting of elements $(0, S, T)$ such that $\sum_{d,e}eS_{d,e}$ is even and $X^0_{n,-1} = X^0_n \setminus X^0_{n,+1}$.

The Dirichlet polynomial $D_{g(\varnothing)}$ (see (1.3)) is given by

$$D_{g(\varnothing)}(s) = \sum_{\tau \in X^0_{n,\varnothing}} M_\tau(q) \cdot c^\tau(q) \cdot \left( \frac{u_2(q)}{c^\tau(q)} \right)^{-s} + \sum_{\tau \in X_n \setminus X^0_n} 4 \cdot M_\tau(q) \cdot c^\tau(q) \cdot \left( \frac{u_2(q)}{2 \cdot c^\tau(q)} \right)^{-s}. \quad (1.7)$$

1.5. Organization

Section 2 gathers necessary preliminary results and sets up notation. Section 3 contains basic structural results regarding the regular orbits of $g(\varnothing)$ and regular characters of $G(\varnothing)$, and the proof of Theorem I. Finally, in Section 4 we classify the regular adjoint orbits of $g(k)$ and compute the regular representation zeta function of $G(\varnothing)$.

2. Notation, preliminaries and basic definitions

2.1. The symplectic and orthogonal groups

Fix $N \in \mathbb{N}$ and a matrix $J \in \text{GL}_N(\varnothing)$ such that $J^t = \epsilon J$, with $\epsilon = -1$ in the symplectic case and $\epsilon = 1$ in the special orthogonal case. The group scheme $G$ is defined by

$$G(R) = \{ x \in M_N(R) \mid x^tJx = J \text{ and } \det(x) = 1 \}, \quad (2.1)$$

where $R$ is a commutative $\varnothing$-algebra and the notation $x^t$ stands for the transpose matrix of $x$. A standard computation (see, e.g. [33, §12.3]) shows that the Lie-algebra scheme $g = \text{Lie}(G)$ is given by

$$g(R) = \{ x \in M_N(R) \mid x^tJ + Jx = 0 \}. \quad (2.2)$$

Let $n$ and $d$ denote the dimension and the absolute rank of the generic fiber of $G$. Note that the absolute rank and dimension of the generic fiber of $G$ are equal to those of its special fiber, by flatness of $G$ and of its maximal tori (see [1, VI_B, Corollary 4.3]).

2.1.1. Adjoint operators

Let $R^N$ denote the $N$-th cartesian power of $R$, identified with the space $M_N \times 1(R)$ of column vectors, and define a non-degenerate bilinear form on $R^N$ by $B_R(u,v) = u^tJv$. One defines an $R$-anti-involution on $M_N(R) = \text{End}_R(R^N)$ by

$$A^* = J^{-1}A^tJ \quad (A \in M_N(R)), \quad (2.3)$$

or equivalently, by letting $A^*$ be the unique matrix satisfying $B_R(A^*u,v) = B_R(u,Av)$, for all $u, v \in R^N$. In this notation, we have that $A \in G(R)$ if and only if $\det(A) = 1$ and $A^*A = 1$, and that $A \in g(R)$ if and only if $A^* + A = 0$. 

5
2.1.2. Maximal tori and centralizers over algebraically closed fields

Let \( T \) be a maximal torus of \( G \) and let \( \mathfrak{t} \subset \mathfrak{g} \) be its Lie-algebra. Given an algebraically closed field \( L \), which is an \( \mathfrak{o} \)-algebra, we may assume that \( T(L) \) is the group of \( N \times N \) diagonal matrices. Moreover, up to possibly replacing \( J \) with a congruent matrix, which amounts to conjugation of the given embedding \( G \subset \text{GL}_N \) by a fixed matrix over \( \mathfrak{o} \), we may assume that \( T(L) \) is mapped onto the subgroup of diagonal matrices \( \text{diag}(\nu_1, \ldots, \nu_N) \), satisfying \( \nu_2 i = \nu_{2i-1}^{-1} \) for all \( i = 1, \ldots, \lfloor N/2 \rfloor \), and with \( \nu_N = 1 \) if \( N \) is odd. In particular, the absolute rank of the generic fiber of \( G \) is \( n = \dim(T \times \text{Spec} \, O) \), the algebraic closure of \( K \).

Under this embedding, the Lie-algebra \( t(L) \) consists of diagonal matrices of the form \( \text{diag}(\nu_1, \ldots, \nu_N) \), with \( \nu_2 i = -\nu_{2i-1} \) for all \( i = 1, \ldots, n \) and \( \nu_N = 0 \) if \( N \) is odd. We require the following well-known result.

**Proposition 2.1.1.** Let \( s \in \mathfrak{g}(L) \) be a semisimple element. Let \( \lambda_1, \ldots, \lambda_t \in L \) be such that \( \{ \pm \lambda_1, \ldots, \pm \lambda_t \} \) is the set of all non-zero eigenvalues of \( s \), with \( \lambda_i \neq \pm \lambda_j \) whenever \( i \neq j \), and let \( m_1, \ldots, m_t \) be their respective algebraic multiplicities. The centralizer of \( s \) under the adjoint action of \( G(L) \) is of the form

\[
\mathcal{C}_{G(L)}(s) \simeq \prod_{j=1}^t \text{GL}_{m_j}(L) \times \Delta(L),
\]

where \( \Delta \) is the \( L \)-algebraic group of isometries of the restriction of \( B \) to (a non-degenerate bilinear form on) \( \text{Ker}(s) \), the eigenspace associated with the eigenvalue 0.

**Proof.** Let \( V = L^N \) be the fixed \( L \)-vector space on which \( G(L) \subset \text{GL}_N(L) \) acts. The element \( s \) is thus considered as an endomorphism of \( V \). The decomposition of \( V \) into eigenspaces of \( s \) gives rise to a direct decomposition into isotypic \( \mathcal{C}_{\text{GL}_N(L)}(s) \)-modules, \( V = \bigoplus_{\lambda \in L} W_\lambda \), where \( W_\lambda = \text{Ker}(s - \lambda \text{Id}) \).

For any non-zero \( \lambda \in L \), put \( W_{\lambda} = W_\lambda \ominus W_{-\lambda} \). A simple computation reveals that the spaces \( W_0 \) and \( W_{|\lambda|} \) are non-degenerate with respect to the ambient symmetric or anti-symmetric bilinear form.

Since \( \mathcal{C}_{G(L)}(s) = \mathcal{C}_{\text{GL}_N(L)}(s) \cap G(L) \), it holds that \( x \in \mathcal{C}_{G(L)}(s) \) if and only if \( x \in \mathcal{C}_{\text{GL}_N(L)}(s) \) and \( x \) acts as an isometry with respect to the restriction of \( B \) to the spaces \( W_0 \) and \( W_{|\lambda|} \) (for \( \lambda \neq 0 \)).

Arguing as in [3, III, § 2.4], one verifies that for any \( \lambda \neq 0 \) the decomposition \( W_{|\lambda|} = W_\lambda \oplus W_{-\lambda} \) into maximal isotropic subspaces, and in particular \( \dim L W_\lambda = \dim L W_{-\lambda} \). Invoking Witt’s Theorem [32, § 1.2], and the \( \mathcal{C}_{\text{GL}_N(L)}(s) \)-isotypicity of the decomposition, we obtain that any automorphism of \( W_\lambda \) extends uniquely to an isometric automorphism of \( W_{|\lambda|} \) which commutes with the action of \( s \), and that the action of \( \mathcal{C}_{G(L)}(s) \) on \( W_{|\lambda|} \) is determined in this manner. Furthermore, it holds that any automorphism of \( W_0 = \text{Ker}(s) \) which preserves the restriction of \( B \) to \( W_0 \) necessarily commutes with \( s \), and that the action of \( \mathcal{C}_{G(L)}(s) \) on this subspace is by such automorphisms. The proposition follows. \( \square \)

2.2. Artinian discrete valuation rings

Let \( K^{\text{alg}} \) be a fixed algebraic closure of \( K \) and let \( K^{\text{unr}} \) be the maximal unramified extension of \( K \) in \( K^{\text{alg}} \). Let \( \mathcal{O} \) be the valuation ring of \( K^{\text{unr}} \), and \( \mathcal{P} = \pi \mathcal{O} \) its maximal ideal. The residue field of \( \mathcal{O} \) is identified with the algebraic closure \( k^{\text{alg}} \) of \( k \). Given \( m \in \mathbb{N} \) we put \( \mathfrak{o}_m := \mathfrak{o}/p^m \) and \( \mathcal{O}_m := \mathcal{O}/\mathcal{P}^m \) and write \( \eta_m : \mathcal{O} \rightarrow \mathcal{O}_m \) and \( \eta_{m,r} : \mathcal{O}_m \rightarrow \mathcal{O}_r \) for the reduction maps, for any \( 1 \leq r \leq m \). The notation \( \eta_m \) and \( \eta_{m,r} \) is also used to denote the coordinatewise reduction map on \( M_N(\mathcal{O}) \) and \( M_N(\mathcal{O}_m) \), respectively.

The map \( \eta_1 \) admits a canonical splitting map \( s : k^{\text{alg}} \rightarrow \mathcal{O} \), which restricts to a homomorphic embedding of \( (k^{\text{alg}})^{\times} \) into \( \mathcal{O}^{\times} \), and satisfies \( s(0) = 0 \); see [22, Ch. II, § 4, Proposition 8].
Let $\sigma : K^{\text{unr}} \to K^{\text{unr}}$ be the local Frobenius map whose fixed field is $K$. Then $\sigma$ restricts to a ring automorphism of $\mathcal{O}$, with fixed subring $\mathcal{O}^{\sigma} = \mathcal{o}$, and induces a map $\mathcal{O}_m \to \mathcal{O}_m$ for any $m \geq 1$ whose fixed subring is $\mathcal{o}_m$. In the special case $m = 1$, the map $\sigma : k^{\text{alg}} \to k^{\text{alg}}$ is given by the $q$-power map $x \mapsto x^q$, where $q = |k|.$

2.3. The Greenberg functor

The Greenberg functor was introduced in [12] and [13], as a generalization of Shimura’s reduction mod $p$ functor to higher powers of $p$. Given an artinian discrete valuation ring $R$ (or more generally, an artinian local ring) with a perfect residue field $\mathfrak{t}$, the Greenberg functor $\mathcal{F}_R$ associates to any $R$-scheme $Y$ locally of finite type a scheme $\mathcal{F}_R(Y)$ locally of finite type over the residue field $\mathfrak{t}$. Given another such ring $R'$ with residue field $\mathfrak{t}$ and a ring homomorphism $R \to R'$, the functors $\mathcal{F}_R$ and $\mathcal{F}_{R'}$ are related via connecting morphisms, on which we expand further below.

A defining characteristic of the functor is the existence of a canonical bijection

$$\mathcal{F}_R(Y)(\mathfrak{t}) = Y(R).$$

(2.4)

More generally, if $A$ is a perfect commutative unital $\mathfrak{t}$-algebra, then either $\mathcal{F}_R(Y)(A) = Y(R \otimes_{\mathfrak{t}} A)$, in the case where $R$ is a $\mathfrak{t}$-algebra, or otherwise

$$\mathcal{F}_R(Y)(A) = Y(R \otimes_{W(\mathfrak{t})} W(A))$$

(2.5)

where $W(\cdot)$ denotes the ring of $p$-typical Witt vectors [22, Ch. II, § 6]. For further introduction we refer to [5, p. 276].

Our application of the Greenberg functor is focused on the artinian discrete valuation rings $\mathcal{O}_m$. For any $m$, we let $G_{\mathcal{O}_m} = G \times \mathcal{O}_m$ and $g_{\mathcal{O}_m} = g \times \mathcal{O}_m$ denote the base change of the group and Lie-algebra schemes $G$ and $g$. Put $\Gamma_m = \mathcal{F}_{\mathcal{O}_m}(G_{\mathcal{O}_m})$ and $\gamma_m = \mathcal{F}_{\mathcal{O}_m}(g_{\mathcal{O}_m})$. Given $r \leq m$, we write $\eta_{m,r}^*$ to denote the connecting maps $\Gamma_m \to \Gamma_r$ and $\gamma_m \to \gamma_r$, and put $\Gamma_r = (\eta_{m,r}^*)^{-1}(1) = \text{Spec}(\kappa(1)) \times_{\mathfrak{t}} \Gamma_m$ (the scheme-theoretic group kernel) and $\gamma_r = (\eta_{m,r}^*)^{-1}(0) = \text{Spec}(\kappa(0)) \times_{\gamma_m} \gamma_r$ (the scheme-theoretic Lie-algebra kernel). Here, the notation $\kappa(\cdot)$ stands for the residue field at a rational point of a scheme.

Note that, a priori, the connecting morphism between a scheme and its base change is dependent on the scheme in question as well. The apparent abuse of notation in writing $\eta_{m,r}^*$ for the connecting morphisms of different schemes is made permissible by the following lemma, whose proof is essentially included in [12].

Lemma 2.3.1. Let $X$ be a locally closed sub-$\mathcal{O}_m$-scheme of $A^k_{\mathcal{O}_m}$, the affine $k$-space over $\mathcal{O}_m$, and let $\psi : \mathcal{F}_{\mathcal{O}_m}(X) \to \mathcal{F}_{\mathcal{O}_r}(X \times \mathcal{O}_r)$ be the associated connecting morphism. The map $\psi$ coincides pointwise with restriction of the coordinatewise reduction map from $\mathcal{F}_{\mathcal{O}_m}(A^k_{\mathcal{O}_m})$ to $\mathcal{F}_{\mathcal{O}_r}(X)$.

Proof. The case $X = A^k_{\mathcal{O}_m}$ is [12, Corollary 2, § 5]. In the general case, note that by properties of base change, the inclusion $X \times \mathcal{O}_r \subseteq A^k_{\mathcal{O}_m}$ is simply the base change over $\text{Spec}(\mathcal{O}_r)$ of the inclusion morphism $X \subseteq A^k_{\mathcal{O}_m}$. The lemma follows from Assertion 2 of the Main Theorem (preservation of arbitrary immersions) and Corollary 4, § 5, of [12].

The main properties which we require are summarized in the following lemma.

Lemma 2.3.2. For $m \in \mathbb{N}$ fixed, we have
1. The rings $\mathcal{O}_m$ are the $k^{alg}$-points of an $m$-dimensional algebraic ring scheme $O_m$ over $k^{alg}$.

The canonical map $s : k^{alg} \to \mathcal{O}_m$ defines a closed embedding $s^* : k^{alg}_{k^{alg}} \to O_m$ of the affine line over $k^{alg}$ into this ring variety. The restriction of $s^*$ to the multiplicative group $G_m \subseteq k^{alg}_{k^{alg}}$ is a monomorphism of $k^{alg}$-linear algebraic groups, satisfying $\eta_{m,1} m s^* = 1_{k^{alg}_{k^{alg}}}$. 

2. The group $\Gamma_m$ is a $d \cdot m$-dimensional linear algebraic group over $k^{alg}$. Moreover, if $\Delta \subseteq G_D$ is a closed sub-$G_m$-scheme with a smooth $d'$-dimensional fiber, then $F_{\Delta} m (\Delta)$ is a closed sub-$k^{alg}$-group of $\Gamma_m$ of dimension $d' \cdot m$.

3. The scheme $\gamma m$ is a $d \cdot m$-dimensional affine space over $k^{alg}$, which is naturally endowed with a Lie-bracket operation.

4. The connecting morphisms $\eta^* m, r$, for $r \leq m$, give rise to $k^{alg}$-group scheme epimorphisms $\Gamma_m \to \Gamma_r$. Similarly, for $\gamma_m \to \gamma_r$, these are Lie-ring epimorphisms.

5. The adjoint action of $G_D$ on the Lie-ring scheme $g_D$ with $r \leq m$, induces an action of the algebraic group $\Gamma_m$ on $\gamma_r$. The application of $F_{\Delta}$ preserves centralizers of $\mathcal{O}_m$-rational points of $g_D$.

**Proof.** 1. See [12, § 1, Proposition 4].

2. The Greenberg functor maps $D_m$-group schemes of finite type to $k^{alg}$-group schemes of finite type by Assertion (5) of the Main Theorem (§4) of [12]. By [13, Corollary 1, p. 263], the group $\Gamma_m$ is smooth over $k^{alg}$, and hence reduced [33, 11.6]. Thus $\Gamma_m$ is a linear algebraic $k^{alg}$-group.

Given $\Delta \subseteq G_D$ as above, $F_{\Delta} m (\Delta)$ is closed by [12, § 4, Proposition 8]. The assertion regarding the dimension of $F_{\Delta} (\Delta)$ may be proved by induction on $m$, the case $m = 1$ being trivially true. For $m > 1$, by [13, Corollary 2, p. 262], we have an exact sequence

$$1 \to \mathfrak{d} \to F_{\Delta} m (\Delta) \xrightarrow{\eta_{m, m-1}} F_{\Delta} m-1 (\Delta \times \mathcal{O}_m) \to 1$$

of $k^{alg}$-algebraic group schemes. By Greenberg’s Structure Theorem [13], the kernel $\mathfrak{d}$ is an affine $d'$-dimensional unipotent group over $k^{alg}$. Since $\Delta \times \mathcal{O}_m$ is a closed subgroup scheme of $\Gamma_m$ with the same fiber as $\Delta$, the assertion follows.

3. The assumption regarding dimensions in Assertion (3) follows from the Main Theorem and Proposition 4.4, § 1, of [12]. The Lie-bracket and addition on $g_D$ are transported by $F_{\Delta}$ to schematic morphisms $\gamma_m \times \gamma_m \to \gamma_m$ by [12, Corollary 3, p. 641]. The Lie-axioms on $F_{\Delta} (\gamma_m)$ may be verified using compatibility of the Greenberg functor with preimages [12, Corollary 3, p. 641]. For example, the Jacobi identity can be reformulated using the equality $g_\gamma = J^{-1}(0)$, where

$$J : g_\gamma \times g_\gamma \times g_\gamma \to g_\gamma$$

is the morphism satisfying $J(R)(x, y, z) = [[x, y], z] + [[y, z], x] + [z, x, y]$ for any $\mathcal{O}_m$-algebra $R$ and $x, y, z \in g_\gamma(R)$.

4. The connecting map is shown to be a group homomorphism in [12, § 5, Corollary 5], and the preservation of the Lie-bracket follows similarly from [12, § 5, Corollary 2]. Its surjectivity follows from the smoothness of $G_D$ (resp. $g_\gamma$), and [13, Corollary 2, p. 262].

5. The action of $\Gamma_m$ on $\gamma_r$ is given by $F_{\Delta} (\alpha_m) \circ (\eta_{m, r}^* \times 1_{\gamma_r}) : \Gamma_m \times \gamma_r \to \gamma_r$, where $\alpha_m : G_D \times g_D \to g_D$ is the adjunction map; see [26, § 3]. One notes easily that, since the group $\Gamma_m$ acts trivially on $\gamma_r$, this action commutes pointwise with the bijection (2.5). The preservation of centralizers follows from [26, Proposition 3.3], by taking $Y$ and $Z$ to be the sub-schemes defined by the spectrum of the reside field of $g_D$, at the given rational point.

**Remark.** In the case where $\mathcal{O}_m$ is a $k^{alg}$-algebra, Lemma 2.3.2.3 may be somewhat strengthened, as in this case $\gamma_m$ can be shown to coincide with the Lie-algebra of $\Gamma_m$. The equality $\gamma_m = \text{Lie}(\Gamma_m)$
is not as clear in the case of unequal characteristics, and is unknown to the author. In any event, it will not be necessary for our purposes.

We also require the following lemma.

**Lemma 2.3.3.** For any \( r, m \in \mathbb{N} \) with \( r \leq m \), there exists a monomorphism of the underlying additive group schemes \( \nu_{m,r}^* : \gamma_{m-r} \to \gamma_m \), such that

1. for any \( y \in \gamma_{m-r}(k^{alg}) = g(\mathcal{O}_{m-r}) \), it holds that \( \nu_{m,r}(k^{alg})(y) = \pi^r \tilde{y} \), where \( \tilde{y} \in g(\mathcal{O}_m) \) is such that \( \eta_{m,m-r}(\tilde{y}) = y \);
2. the sequence \( 0 \to \gamma_{m-r} \xrightarrow{\nu_{m,r}} \gamma_m \xrightarrow{\eta_{m,r}} \gamma_r \to 0 \) is exact;
3. for any \( y \in \gamma_{m-r}(k^{alg}) \) the square \((2.6)\) commutes

\[
\begin{array}{ccc}
\gamma_m & \xrightarrow{\text{ad}(\nu_{m,r}(y))} & \gamma_m \\
\downarrow{\eta_{m,m-r}} & & \uparrow{\nu_{m,r}^*} \\
\gamma_{m-r} & \xrightarrow{\text{ad}(y)} & \gamma_{m-r},
\end{array}
\]

(2.6)

where \( \text{ad}(z) : \gamma_k \times \gamma_k \to \gamma_k \) (for \( k \in \mathbb{N} \) and \( z \in \gamma_k(g^{alg}) \) is the map defined by \( \text{ad}(z)(A)(x) = [z,x] \) for any commutative unital \( k^{alg} \)-algebra \( A \) and \( x \in \gamma_k(A) \);
4. The equality \( \eta_{m,r+1} \circ \nu_{m,r}^* = \nu_{r+1,1}^* \circ \eta_{m-r,1}^* \) holds.

**Proof.** Given \( k \leq m \) and an \( \mathcal{O}_k \)-scheme \( X \), let \( X^{(m)} \) be the \( \mathcal{O}_m \)-scheme obtained by applying the forgetful functor, i.e. by composing the structure morphism \( X \to \text{Spec}(\mathcal{O}_k) \) with the natural injection \( \text{Spec}(\mathcal{O}_k) \to \text{Spec}(\mathcal{O}_m) \). Unfolding the definitions of the forgetful functor and of the functors in the bijection in the first assertion to the Main Theorem of [12], one verifies that there is a canonical isomorphism \( \mathcal{F}_{\mathcal{O}}(X) = \mathcal{F}_{\mathcal{O}_m}(X^{(m)}) \).

The map \( x \mapsto \pi_{m-r}^m x : g(\mathcal{O}_m) \to g(\mathcal{O}_m) \) gives rise to an injective \( \mathcal{O}_m \)-module map \( \nu_{m,r} : g(\mathcal{O}_r) \to g(\mathcal{O}_m) \), which in turn extends to a map of \( \mathcal{O}_m \)-modules, giving rise to the exact sequence

\[
0 \to g_{\mathcal{O}_{m-r}}(\mathcal{O}_m) \xrightarrow{\nu_{m,r}} g_{\mathcal{O}_m}(\mathcal{O}_m) \xrightarrow{\eta_{m,r}} g_{\mathcal{O}_r}(\mathcal{O}_m) \to 0.
\]

Applying [12, § 1, Proposition 3.(6)] to both maps of the above sequence, these define \( k \)-regular maps between associated module variety structures over \( k^{alg} \) of the modules above, which, in turn, define an exact sequence of \( k^{alg} \)-schemes

\[
0 \to \gamma_{m-r} \xrightarrow{\nu_{m,r}^*} \gamma_m \xrightarrow{\eta_{m,r}^*} \gamma_r \to 0,
\]

where the right-most map coincides with \( \eta_{m,r}^* \) by same proposition and by [12, Corollary 2, § 5]. The first and second assertions of the lemma follow.

As for the third assertion, in order to prove that the morphisms \( \nu_{m,r}^* \circ \text{ad}(y) \circ \eta_{m,m-r}^* \) and \( \text{ad}(\nu_{m,r}(y)) \) coincide, it is enough to show that, upon passing to their associated comorphisms, they induce the same endomorphism of the coordinate ring of \( \gamma_m \). Invoking the isomorphism \( \gamma_m \simeq A_{k^{alg}}^{dm} \) of **Lemma 2.3.2.(3)**, since an endomorphism of a polynomial algebra in \( dm \) variables is determined by specifying the images of \( t_1, \ldots, t_{dm} \) in \( k^{alg}[t_1, \ldots, t_{dm}] \), by Nullstellensatz, it is enough to show that the two endomorphisms above coincide pointwise on \( \gamma_m(k^{alg}) \). This is immediate by the first two assertions and the linearity of \( \text{ad}(\cdot) \) over \( \mathcal{O}_m \). The fourth assertion may be proved in a similar vein as Assertion (3).

\[\square\]
Lemma 2.4.1

Section 2.1.1

2.4. The Cayley map

Let $D$ be the affine $\mathfrak{g}$-scheme $\text{Spec}(\mathfrak{g}[t_{1,1},\ldots,t_{N,N},(\det(t + 1))^{-1}])$, where $t_{1,1},\ldots,t_{N,N}$ are indeterminates and $t + 1$ is the $N \times N$ matrix whose $(i,j)$-th entry is $t_{i,j} + \delta_{i,j}$, with $\delta_{i,j}$ the Kronecker delta function. Note that for any commutative unital $\mathfrak{g}$-algebra $R$, the set of $R$-points of $D$ is naturally identified with the set

$$\{ x \in M_N(R) \mid \det(1 + x) \in R^\times \}.$$  \hfill (2.7)

Remark. In the case where $\mathcal{D}$ is either a $k^{alg}$-algebra, or is absolutely unramified (i.e. $\mathcal{D} = \mathfrak{p} D$), and thus isomorphic to the ring $W(k^{alg})$, the map $v_{m,r}^*$ of the lemma may be described explicitly, by fixing a suitable coordinate system for $\gamma_m$ over $k^{alg}$ and taking $v_{m,r}^*$ to be either a coordinate shift in the former case, or given by successive applications of the verschiebung and Frobenius maps coordinatewise (see [22]) in the latter.

2.4.1. Properties of the Cayley map

Let $D$ be the affine $\mathfrak{g}$-scheme $\text{Spec}(\mathfrak{g}[t_{1,1},\ldots,t_{N,N},(\det(t + 1))^{-1}])$ by mapping $t_{i,j}$ to the $(i,j)$-th entry of the matrix $(1 - t)(1 + t)^{-1}$. Note that $\text{cay}^2(\det(t + 1))^{-1} = 2^{-N} \det(1 + t)$. A direct computation shows that, as 2 is invertible in $\mathfrak{g}$, the map $\text{cay}^2$ is its own inverse and thus $\text{cay}$ is an automorphism of $D$.

Under the identification (2.7) for $R$ an $\mathfrak{g}$-algebra as above, the action of $\text{cay}$ on the set of $R$-points of $D$ is given explicitly by

$$\text{cay}(R)(x) = (1 - x)(1 + x)^{-1}. \hfill (2.8)$$

In the specific case $R = k^{alg}$, the sets $(D \cap \mathfrak{g})(k^{alg})$ and $(D \cap F)(k^{alg})$ are principal open subsets of $\gamma(k^{alg})$ and $\Gamma(k^{alg})$ respectively. Using the description of $\mathfrak{g}$ and $F$ given in Section 2.1.1, one verifies that the restriction of $\text{cay}(k^{alg})$ to $(D \cap \mathfrak{g})(k^{alg})$ defines an algebraic isomorphism of affine varieties onto $(D \cap F)(k^{alg})$, and hence a birational map $\text{cay}(k^{alg}) : \mathfrak{g}(k^{alg}) \to F(k^{alg})$. Additionally, being given by a power series in $x$ on $(D \cap \mathfrak{g})(k^{alg})$, the map $\text{cay}(k^{alg})$ is equivariant with respect to the conjugation action of $F(k^{alg})$. The properties listed in this paragraph carry over to the associated $k^{alg}$-group schemes described in the previous section, as noted in Lemma 2.4.1 below.

The Cayley map was introduced in [8]. Its generalization to groups of arising as the set of unitary transformations with respect an anti-involution of an associative algebra is attributed to A. Weil [34, § 4]. See also [20] for a more generalized treatment of the Cayley map.

2.4.1. Properties of the Cayley map

Given $m \in \mathbb{N}$, put $D_m = D \times \mathcal{D}$ and let $\text{cay}_m = \text{cay} \times 1_{\mathcal{D}}$ be the base change of $\text{cay}$. Let $\Delta_m = \mathcal{F}_m(D_m)$ and $\text{cay}_m^\vee = \mathcal{F}_m(\text{cay}_m)$. Note that, by construction and by the Main Theorem of [12], $\Delta_m$ is an open affine subscheme of $k^{alg,N}_m$.

Lemma 2.4.1. Let $1 \leq r \leq m$. The map $\text{cay}_m^\vee$ has the following properties.

Cay1. The map $\text{cay}_m^\vee$ is a birational equivalence $\gamma_m \to \Gamma_m$. Furthermore, its restriction to the kernel $\gamma_m^r$ is a isomorphism of $k^{alg}$-varieties onto $\Gamma_m^r$, and is an isomorphism of abelian groups if $2r \geq m$.

\hfill 1Here $\cap$ denotes the scheme-theoretic intersection, $D \cap \mathfrak{g} = D \times \text{Spec}(\mathfrak{g}[t_{1,1},\ldots,t_{N,N}])$ $\gamma$ and likewise for $D \cap F$. 

10
Cay2. The map $\tilde{\text{cay}}_m$ is $\Gamma_m$-equivariant with respect to the adjoint action on $\gamma_m$ and with respect to group conjugation on $\Gamma_m$.

Cay3. The diagram in (2.9) commutes.

$$
\begin{array}{ccc}
\gamma_m & \xrightarrow{\text{cay}_m} & \Gamma_m \\
\eta_{m,r}^* & \downarrow & \eta_{m,r}^* \\
\gamma_r & \xrightarrow{\text{cay}_r} & \Gamma_r.
\end{array}
$$

(2.9)

Proof. 1. The inclusion map $D_m \cap g_\mathcal{O}_m \subseteq g_\mathcal{O}_m$ is an open immersion, and thus by Assertion (2) and (3) of the Main Theorem of [12], the $k^\text{alg}$-scheme $\Delta_m \cap \gamma_m$ is immersed as an open subscheme of $\gamma_m$. Similarly for $\Delta_m \cap \Gamma_m$. By functoriality, the morphism $\tilde{\text{cay}}_m$ is an isomorphism of $\Delta_m \cap \gamma_m$ onto $\Delta_m \cap \Gamma_m$, and hence $\gamma_m$ and $\Gamma_m$ are birationally equivalent.

To prove that $\tilde{\text{cay}}_m$ restricts to an isomorphism of $\gamma'_m$ onto $\Gamma'_m$, it would be enough that both are embedded as sub-schemes of $\Delta_m$ under the given inclusions into $k^\text{alg}_{\gamma_m}$. Note that by applying Greenberg’s Structure Theorem [13] inductively, both $\gamma'_m$ and $\Gamma'_m$ are reduced, and thus are $k^\text{alg}$-varieties. Thus, by Nullstellensatz, they are determined by their $k^\text{alg}$-points and it suffices to show they are included in the reduced subscheme $(\Delta_m)_{\text{red}} \subseteq \Delta_m$. This follows from the bijection (2.4), as $\gamma'_m(k^\text{alg}) = g_\mathcal{O}_m(\mathcal{O}_m) \cap \eta_{m,r}^{-1}(0)$ is included in the nilradical of the matrix algebra $M_N(\mathcal{O}_m)$, and hence included in $D_m(\mathcal{O}_m)$, and since $\Gamma'_m(k^\text{alg}) = G_\mathcal{O}_m(\mathcal{O}_m) \cap \eta_{m,r}^{-1}(1) \subseteq 1 + \pi M_N(\mathcal{O}_m) \subseteq \text{GL}_N(\mathcal{O}_m)$, and thus (since char($k^\text{alg}) \neq 2$) included in $D_m(\mathcal{O}_m)$.

Lastly, to prove that $\tilde{\text{cay}}_m$ is a group homomorphism whenever $2r \geq m$, it is equivalent to show that it preserves comultiplication in the Hopf-algebra structure of the coordinate ring of $\gamma'_m$ in this case. Arguing as in the proof Lemma 2.3.3, it sufficient to verify this on the $k^\text{alg}$-points of the variety. This follows from the definition of $\text{cay}$ (2.8), as in this case $\gamma'_m(k^\text{alg}) \subseteq g_\mathcal{O}_m(\mathcal{O}_m)$ is included in an ideal of vanishing square in $M_N(\mathcal{O}_m)$ and the map $\tilde{\text{cay}}_m$ coincides with the map $x \mapsto 1 - 2x$.

2. Property (Cay2) holds since $\mathcal{I}_\mathcal{O}_m$ preserves the cartesian square (2.10), which states the $\Gamma_m$-equivariance of $\text{cay}_m$:

$$
\begin{array}{ccc}
\Gamma_m \times \gamma_m & \xrightarrow{\alpha_{\Gamma_m,\gamma_m}} & \gamma_m \\
\downarrow & & \downarrow \\
\Gamma_m \times \text{cay}_m & \xrightarrow{\alpha_{\Gamma_m,\text{cay}_m}} & \text{cay}_m.
\end{array}
$$

(2.10)

Here $\alpha_{\Gamma_m, X}$ denotes the action map of $\Gamma_m$ on $X \in \{\Gamma_m, \gamma_m\}$.

3. Finally, property (Cay3) is simply an application of [12, Corollary 4, p.645], to the case $R = \mathcal{O}_m$, $R' = \mathcal{O}'_m$, $\varphi = \eta_{r,m}$, $X_1 = \gamma_m \cap D_m$, $X_2 = \Gamma_m \cap D_m$ and $g = \text{cay}_m$.

2.5. Groups, Lie algebras and characters

In general, given finite groups $\Delta \subseteq \Gamma$ and characters $\sigma \in \text{Irr}(\Delta)$ and $\chi \in \text{Irr}(\Gamma)$, we denote by $\chi_\Delta$ the restriction of $\chi$ to $\Delta$, and by $\sigma^\Gamma$ the character induced from $\sigma$ in $\Gamma$. Group commutators
are denoted by \((x, y) = xyx^{-1}y^{-1}\). Lie-algebra commutators are denoted by \([x, y] = xy - yx\). The center of a group \(\Gamma\) is denoted by \(Z(\Gamma)\).

The Pontryagin dual of a finite abelian group \(\Delta\) is denoted by \(\widehat{\Delta} = \text{Hom}(\Delta, \mathbb{C}^\times)\). If \(\Delta\) is given with additional structure (e.g. a ring or a Lie-algebra), then \(\widehat{\Delta}\) refers to the Pontryagin dual of the abelian group underlying \(\Delta\).

3. Regular elements and regular characters

3.1. Regular elements

We begin our analysis of regular characters by inspecting the group \(G(\mathcal{O})\). To do so, we first consider the regular orbits for the action of \(G(\mathcal{O})\) on \(g(\mathcal{O}_m)\), or, equivalently (see \([26, \S~3]\)), of \(\Gamma_m(k_{\text{alg}})\) on \(\gamma_m(k_{\text{alg}})\). The methods which we apply are influenced by \([14]\).

Recall that an element of a reductive algebraic group over an algebraically closed field is said to be regular if its centralizer is an algebraic group of minimal dimension among such centralizers \([29, \S3.5]\). Following \([14]\), this definition is extended to elements of \(\gamma_m\) with respect to the conjugation action of \(\Gamma_m\).

**Definition 3.1.1.** Let \(m \geq 1\). An element \(x \in g(\mathcal{O}_m)\) is said to be regular if the group scheme \(\mathcal{F}_m(\mathcal{C}_{G, m}(x)) = \mathcal{C}_{\Gamma_m}(x)\), obtained by applying the Greenberg functor to the centralizer group scheme of \(x\) in \(G_{\mathcal{O}_m}\), is of minimal dimension among such group schemes.

The following theorem lists the main properties of regular elements of \(\gamma_m\), which are proved in this section.

**Theorem 3.1.2.** Let \(G\) be a symplectic or a special orthogonal group scheme over \(\mathfrak{g}\) with Lie-algebra \(g = \text{Lie}(G)\). Fix \(m \in \mathbb{N}\) and let \(x \in g(\mathcal{O}_m)\).

1. If \(x_m\) is a regular element of \(g_{\mathcal{O}_m}(\mathcal{O}_m)\), then \(\mathcal{C}_{\Gamma_m}(x_m)\) is a \(k_{\text{alg}}\)-group scheme of dimension \(m \cdot n\), where \(n = \text{rk}(G \times K_{\text{alg}})\).

2. The element \(x_m\) is regular if and only if \(x_1 = \eta_{m, 1}(x_m)\) is a regular element of \(g(k_{\text{alg}})\).

3. Suppose \(x_m \in g(\mathcal{O}_m)\) is regular. The restriction of the reduction map \(\eta_{m, 1}\) to \(\mathcal{C}_{G(\mathcal{O}_m)}(x_m)\) is surjective onto \(\mathcal{C}_{G(k_{\text{alg}})}(x_1)\).

The proofs of Assertions (1), (2) and (3) of Theorem 3.1.2 are given, respectively, in sections 3.1.1, 3.1.2 and 3.1.3 below. Once the proof of Theorem 3.1.2 is complete, we return to analyse the case of regular elements of \(g_m = \gamma_m(\mathcal{O}_m)^\sigma\).

**Theorem 3.1.3.** Let \(G\) be a symplectic or a special orthogonal group scheme over \(\mathfrak{g}\) with \(g = \text{Lie}(G)\) and let \(x \in g = g(\mathfrak{o})\). Assume \(x_m = \eta_{m, 1}(x)\) is regular for some \(m \in \mathbb{N}\). Then

1. \(\mathcal{C}_G(x) = \lim_{\to m} \mathcal{C}_{G_m}(x_m)\), where \(G = G(\mathfrak{o})\) and \(G_m = G(\mathfrak{o}_m)\)

2. Furthermore, \(x\) is a regular element of \(g(K_{\text{alg}})\).

Theorem 3.1.3 has the following corollary.

**Corollary 3.1.4.** In the notation of Theorem 3.1.3, let \(x \in g\) such that \(x_m = \eta_{m, 1}(x)\) is a regular element of \(g_m\), for some \(m \in \mathbb{N}\). Then \(\mathcal{C}_{G_m}(x_m)\) is abelian.
3.1.1. General properties of the groups $\Gamma_m$

We begin by examining some basic properties of the group $\Gamma_m$ ($m \in \mathbb{N}$) and of centralizers of elements of $\gamma_m$, when considered as algebraic group schemes over $k^{\text{alg}}$. The following lemma summarizes the necessary components for the proof of Theorem 3.1.2.(1), and is mostly included in [26].

**Lemma 3.1.5.** 1. The group scheme $\Gamma_m$ is a connected algebraic group over $k^{\text{alg}}$.

2. The unipotent radical of $\Gamma_m$ is $\Gamma^u_m$.

3. Let $T$ be a maximal torus of $G$, defined over $\mathcal{O}$, and let $T_1 = T \times k^{\text{alg}} \subseteq \Gamma_1$. The restriction of the map $s^* : k^{\text{alg}} \to \mathcal{O}_m$ of Lemma 2.3.2.(1) to $\mathcal{G}_m$ extends to an embedding of $T_1$ as a maximal torus in $\Gamma_m$.

4. The centralizer of $s^*(T_1)$ in $\Gamma_m$ is the Cartan subgroup $T_{\mathcal{O}_m}(T \times \mathcal{O}_m)$. Moreover, $T_{\mathcal{O}_m}(T \times \mathcal{O}_m)$ is a linear algebraic $k^{\text{alg}}$-group of dimension $n \cdot m$.

**Proof.** 1. Connectedness is proved in [26, Lemma 4.2]. The remainder of the assertion appears above in Lemma 2.3.2.

2. See [26, Proposition 4.3].

3. May be proved by following the argument of [14, Proposition 2.2.(2)], practically verbatim, making use of the fact that $\Gamma_m$ and $\Gamma_1 = \eta^1_{\gamma_m}(\Gamma_m)$ are of the same rank by the previous assertion, and that $s^*(T_1)$ is a connected abelian subgroup of $\Gamma_m$ of dimension $n = \text{rk}(\Gamma_1)$.

4. The inclusion $T(\mathcal{O}_m) \subseteq C_{\Gamma_m}(k^{\text{alg}})(s^*(T_1)(k^{\text{alg}}))$ is clear, since $T(\mathcal{O}_m)$ is abelian and contains $s^*(T_1)(k^{\text{alg}})$, by Lemma 2.3.2.(1). The inclusion $T \times \mathcal{O}_m \subseteq C_{\Gamma_m}(s^*(T_1))$ follows (see [26, Proposition 3.2]). By [26, Theorem 4.5], $T_{\mathcal{O}_m}(T \times \mathcal{O}_m)$ is a Cartan subgroup of $\Gamma_m$ and hence is equal to the centralizer of $s^*(T_1)$. Finally, the statement regarding the dimension of $T_{\mathcal{O}_m}(T \times \mathcal{O}_m)$ follows from Lemma 2.3.2.(1) and [12, Proposition 4, § 1].

**Proof of Theorem 3.1.2.(1).** The alternative proof of [29, Ch. III, § 3.5, Proposition 1] shows that the minimal centralizer dimension of an element of $g(\mathcal{O}_m)$ is equal to that of a Cartan subgroup of $\Gamma_m$, provided that the Cartan subgroups of $\Gamma_m$ are abelian and that their union forms a dense subset of $\Gamma_m$. The former of these conditions holds by [26, Theorem 4.5], and the latter by [4, IV 12.1].

3.1.2. Regularity and the reduction maps

The first step towards the proof of the second assertion of Theorem 3.1.2 is an analogous result to [14, Lemma 3.5] in the Lie-algebra setting. Following this, we use the properties of the Cayley map in order to transfer the result to the group setting and to deduce the equivalence of regularity of an element of $\gamma_m$ and of its image in $\gamma_1$.

**Lemma 3.1.6.** Let $x \in g(\mathcal{O})$ be fixed, and for any $m \in \mathbb{N}$ put $x_m = \eta_m(x) \in g(\mathcal{O}_m)$. Let $C_{\gamma_m}(x_m)$ denote the Lie-algebra centralizer of $x_m$, i.e. $C_{\gamma_m}(x_m)(A) = \{ y \in \gamma_m(A) \mid \text{ad}(x_m)(A)(y) = 0 \}$, for any commutative unital $k^{\text{alg}}$-algebra $A$. The image of $C_{\gamma_m}(x_m)$ under the connecting morphism $\eta^*_{m,1}$ is a $k^{\text{alg}}$-group scheme of dimension greater or equal to $n$.

**Proof.** Assume towards a contradiction that the statement of the lemma is false, and let $m$ be minimal such that $\dim \eta^*_{m,1}(C_{\gamma_m}(x_m)) < n$. Note that, since $\eta^*_{m,1} \circ \eta^*_{r,m} = \eta^*_{r,1}$ for all $r > m$ (by [12, Proposition 3, § 5]) we also have that $\dim \eta^*_{r,1}(C_{\gamma_r}(x_r)) < n$ for all $r \geq m$.
Fix \( r \geq m \), and consider the sequence of immersions
\[
C_{\gamma_r(x_r)}(x_r) \supseteq C_{\gamma_{r+1}(x_r)}(x_r) \supseteq \ldots \supseteq C_{\gamma_0}(x_r) \supseteq 0,
\]
where \( C_{\gamma_i}(x_r) = C_{\gamma_r}(x_r) \cap \gamma_i \). Then
\[
\dim C_{\gamma_r}(x_r) = \sum_{i=0}^{r-1} \left( \dim C_{\gamma_i}(x_r) - \dim C_{\gamma_{i+1}}(x_r) \right),
\]
where \( \gamma^0 = \gamma_r \) and \( \gamma_r = \text{Spec} \langle \kappa(0) \rangle \).

For any \( 0 < i < r - 1 \), the map \( \psi_{x_r}^i : \gamma_{r-i} \to \gamma_r \) of Lemma 2.3.3 restricts, by Assertion (3) of the lemma, to an isomorphism of abelian \( k\text{alg} \)-group schemes \( C_{\gamma_{r-i}}(x_r) \approx C_{\gamma_r}(x_r) \), which restricts further, by Assertion (4) of the lemma, to an isomorphism \( C_{\gamma_{i+1}}(x_r) \approx C_{\gamma_{i-1}}(x_r) \). Using these isomorphisms and the exact sequence
\[
0 \to C_{\gamma_{r-i}}(x_r) \to C_{\gamma_{r-i}}(x_r) \xrightarrow{\eta_{r-i,1}} (C_{\gamma_{r-i}}(x_r-i)) \to 0,
\]
we deduce
\[
\dim C_{\gamma_r}(x_r) = \sum_{i=0}^{r-1} \left( \dim C_{\gamma_{r-i}}(x_r) - \dim C_{\gamma_{i+1}}(x_r) \right) = \sum_{i=0}^{r-1} \dim \eta_{r-i,1} \left( C_{\gamma_{r-i}}(x_r) \right)
\[
= \sum_{i=0}^{m-1} \dim \eta_{i,1} \left( C_{\gamma_r}(x_i) \right) + \sum_{i=m}^{r} \dim \eta_{i,1} \left( C_{\gamma_r}(x_i) \right)
\]
\[
\leq d \cdot (m - 1) + (n - \alpha) \cdot (r - m),
\]
for some integer \( \alpha \geq 1 \), where \( d = \dim \gamma_1 = \dim \Gamma_1 \).

For any \( r \in \mathbb{N} \), by Property (Cay2) of the Cayley map and the preservation of open immersions of the Greenberg functor, the Cayley map restricts to a birational equivalence of the Lie-centralizer \( C_{\gamma_r}(x_r) \) and the group-centralizer \( C_{\gamma_r}(x_r) \) of \( x_r \). In particular, by Theorem 3.1.2(1), we have that \( \dim C_{\gamma_r}(x_r) = \dim C_{\gamma_r}(x_r) \geq r \cdot n \). Manipulating the inequality (3.3), we get that
\[
\alpha \cdot r \leq d \cdot (m - 1) - m \cdot (n - \alpha)
\]
for all \( r > m \). A contradiction, since \( r \) can be chosen to be arbitrarily large while the right-hand side of (3.4) remains constant.

Using Lemma 2.4.1, we now pass to the group setting.

**Proposition 3.1.7.** Let \( x \in \gamma \) and \( x_m = \eta_{m,1}(x) \) for all \( m \in \mathbb{N} \). The group scheme \( \eta_{m,1} \left( C_{\gamma_m}(x_m) \right) \) is a \( k\text{alg} \)-algebraic group of dimension greater or equal to \( n \).

**Proof.** Properties (Cay2) and (Cay3) of the Cayley map imply the commutativity of the square (3.5)
\[
\begin{array}{ccc}
C_{\gamma_m}(x_m) & \xrightarrow{\text{Cay}_m} & C_{\gamma_m}(x_m) \\
\eta_{m,1} \downarrow & & \eta_{m,1} \downarrow \\
\eta_{m,1} \left( C_{\gamma_m}(x_m) \right) & \xrightarrow{\text{Cay}_{m\text{alg}}} & \eta_{m,1} \left( C_{\gamma_m}(x_m) \right).
\end{array}
\]

14
A short computation, using Property (Cay3), shows that this square is cartesian. Thus, by (Cay1), and the properties of the fiber product, it follows that the two terms of the bottom row are of the same dimension.

Proof of Theorem 3.1.2 (2). The assertion is proved by induction on \( m \), similarly to [14, Theorem 3.6], the case \( m = 1 \) being trivially true. Consider the following exact sequence

\[
1 \longrightarrow C_{1,m}(x_m) \longrightarrow C_m(x_m) \xrightarrow{\eta_{m,1}} C_{1,1}(x_1). \tag{3.6}
\]

Properties (Cay1) and (Cay2) imply that the map \( c\alpha \gamma_m \) is defined on \( C_{1,m}(x_m) \) and is mapped onto \( C_{1,m}(x_m) \). Combined with Lemma 2.3.3, we get that \( \dim C_{1,m}(x_m) = \dim C_{1,m-1}(x_{m-1}) \). Moreover, since \( \Delta_{m-1} \cap C_{1,m-1}(x_{m-1}) \) is a non-trivial open subscheme of \( C_{1,m-1}(x_{m-1}) \), and is mapped by \( c\alpha \gamma_m \) to an open subscheme of \( C_{1,m-1}(x_{m-1}) \), we deduce the equality

\[
\dim C_{1,m}(x_m) = \dim C_{1,m-1}(x_{m-1}). \tag{3.7}
\]

If \( x_1 \) is regular then by induction we have that \( \dim C_{1,m-1}(x_{m-1}) = n(m-1) \) and hence, by (3.6) and (3.7),

\[
\dim C_m(x_m) \leq \dim C_{1,m-1}(x_{m-1}) + \dim C_{1,1}(x_1) = m \cdot n.
\]

Conversely, if \( x_1 \) is not regular, then by induction \( x_{m-1} \) is not regular, and the dimension of \( C_{1,m-1}(x_{m-1}) \) is strictly greater than \( n(m-1) \). By Proposition 3.1.7 and (3.7), have

\[
\dim C_m(x_m) = \dim C_{1,m-1}(x_{m-1}) + \dim \eta_{1}(C_{1,m}(x_m)) > n(m-1) + n = n \cdot m,
\]

and \( x_m \) is not regular. \( \square \)

Before discussing the final assertion of Theorem 3.1.2, let us observe a simple corollary of Lemma 3.1.6, which is the Lie-algebra version of the assertion.

**Corollary 3.1.8.** Let \( m \in \mathbb{N} \) and \( x_m \in \gamma_m(k^{\text{alg}}) \). The restriction of \( \eta_{m,1} \) to \( C_{m}(x_m) \) is onto \( C_{g(k^{\text{alg}})}(x_m) \), where \( x_1 = \eta_{m,1}(x_m) \in g(k^{\text{alg}}) \).

**Proof.** Theorem 3.1.2 (2) implies that \( x_1 \) is regular and hence \( C_{1}(x_1)(k^{\text{alg}}) = C_{g(k^{\text{alg}})}(x_1) \) is a \( k^{\text{alg}} \)-vector space of dimension \( n = \dim C_{1,1}(x_1) \). By Lemma 3.1.6, the \( k^{\text{alg}} \)-points of the image of \( C_{1,m}(x_m) \) under \( \eta_{m,1} \) comprise a subspace of \( C_{g(k^{\text{alg}})}(x_1) \) of the same dimension. \( \square \)

### 3.1.3. The image of \( \eta_{m,1} \) on \( C_{m}(x_m) \)

To complete the proof of the third assertion of Theorem 3.1.2 we require the following proposition, which is stated here in a slightly more general setting than necessary at the moment, and will also be applied later on in the proof of Corollary 3.1.4.

**Proposition 3.1.9.** Let \( L \) be either \( k^{\text{alg}} \) or \( K^{\text{alg}} \), and let \( H = G \times \text{Spec}(L) \) and \( h = \text{Lie}(H) \) its Lie-algebra. Put \( H = H(L) \) and \( h = h(L) \). Let \( x \in h(L) \) be regular. Then

\[
C_{H}(x) = C_{H}(x)^{\circ}(L) \cdot Z(H),
\]

where \( C_{H}(x)^{\circ} \) is the connected component of \( 1 \). In particular, \( |C_{H}(x) : C_{H}(x)^{\circ}(L)| \leq 2 \) and \( C_{H}(x) \) is abelian.
Proposition 2.1.1 remains true when replacing the groups $25$, with respective multiplicities $29$, and Chevalley's Theorem \[ \text{Theorem 3.1.2} \]. An initial step towards this goal is to show that the third \[ \text{Proposition 3.1.7} \], it follows that \[ 10 \]. (3).

Evaluating the above inclusions at $k \subseteq Z$ by \[ \text{Theorem 3.1.3} \], we deduce the equality.

Additionally, the center $Z$ of $G$ is abelian by \[ \text{Lang's Theorem} \]. Furthermore, by \[ \text{Lemma 3.1.10} \].

Proof of \[ \text{Theorem 3.1.2} \](3). By \[ \text{Proposition 3.1.7} \] and Chevalley’s Theorem \[ \text{[10, IV, 1.8.4]} \], the image of $C_{G_m}(x_m)$ under $\eta_{m,1}^*$ contains the connected component $C_{G_m}(x_m)$ of the identity in $C_{G_m}(x_m)$. Additionally, the center $Z(\Gamma_m)$ of $\Gamma_m$ is clearly contained in $C_{G_m}(x_m)$ and is mapped by $\eta_{m,1}^*$ onto $Z(\Gamma_1)$. This implies the inclusion $C_{G_m}(x_m) \supseteq \eta_{m,1}^*(C_{G_m}(x_m)) \supseteq (C_{G_m}(x_m))^o \cdot Z(\Gamma_1)$.

Evaluating the above inclusions at $k^{\text{alg}}$-points, by \[ \text{Proposition 3.1.9} \], we deduce the equality.

3.1.4. Returning to the $\sigma$-rational setting

In this section we prove \[ \text{Theorem 3.1.3} \]. An initial step towards this goal is to show that the third assertion of \[ \text{Theorem 3.1.2} \] remains true when replacing the groups $G(\mathcal{O}_m)$ and Lie-rings $g(\mathcal{O}_m)$ with the group and Lie-rings of $\mathfrak{o}_m$-rational points, i.e. $G_m = G(\mathfrak{o}_m)$ and $g_m = g(\mathfrak{o}_m)$. Given $1 \leq r \leq m$, we write $G_m^r$ and $g_m^r$ to denote the congruence subgroup $\text{Ker}(G_m \xrightarrow{\eta_{m,r}} G_r) = G_m \cap \eta_{m,r}^{-1}(1)$ and congruence subring $\text{Ker}(g_m \xrightarrow{\eta_{m,r}} g_r) = g_m \cap \eta_{m,r}^{-1}(0)$, respectively.

Recall that $\sigma : \mathcal{O} \rightarrow \mathcal{O}$ was defined in \[ \text{Section 2.2} \] to be the local Frobenius automorphism of $\mathcal{O}$ over $\mathfrak{o}$, given on its quotient $k^{\text{alg}}$ by $\sigma(\xi) = \xi^{|k|}$. This automorphism gives rise to an automorphism of $G(\mathcal{O})$, and of its quotients $G(\mathcal{O}_m)$ and their Lie-rings. By definition, an element $x \in g_m$ is regular if and only if it is a regular $\sigma$-fixed element of $g(\mathcal{O}_m)$. We require the following variant of Lang's Theorem.

Lemma 3.1.10. Let $m \in \mathbb{N}$ and let $x_m \in g_m$ be a regular element and $x_1 = \eta_{m,1}(x_m)$. Given $g \in C_{G_1}(x_1) = C_{G(k^{[k]})}(x_1) \cap G_1$, let $F_g = \eta_{m,1}^{-1}(g) \cap C_{G(\mathcal{O}_m)}(x_m)$, and let $L_g$ be the map defined by $h \mapsto h \cdot \sigma(h)^{-1}$.

Then $L_g : F_g \rightarrow F_1$ is a well-defined surjective map.
Proof. The sets \( F_\gamma \) (\( g' \in C_{G_1}(x_1) \)) are simply cosets of the subgroup \( F_1 = C_{G_1}(k^{alg})(x_m) \). In particular, by (Cay1) and (Cay2), the \( F_\gamma \)'s are the \( k^{alg} \)-points of algebraic varieties, isomorphic to \( C_{\gamma,1}(k^{alg})(x_m) \) and hence affine \((m - 1)n\)-dimensional spaces over \( k^{alg} \).

Since the reduction map \( \eta_{m,1} \) commutes with the Frobenius maps, and since \( g \) is assumed fixed by \( \sigma \), we have that \( \mathcal{L}_g \) is well-defined. The surjectivity of \( \mathcal{L}_g \) now follows as in the proof of the classical Lang Theorem [19] (see also [25, I, 2.2] and [13, § 3]).

Corollary 3.1.11. Let \( x_m \in g_m \) be regular and \( x_1 = \eta_{m,1}(x_m) \). The restriction of \( \eta_{m,1} \) to \( C_{G_m}(x_m) \) is onto \( C_{G_1}(x_1) \).

Proof. Lemma 3.1.10 and Theorem 3.1.2.(3) imply that for any \( g \in C_{G_1}(x_1) \), there exists an element \( h \in C_{G_m}(x_m) \) such that \( \eta_{m,1}(h) = g \) and such that \( \mathcal{L}_g(h) = h\sigma(h)^{-1} = 1 \). In particular, \( h \) is fixed under \( \sigma \) and hence \( h \in C_{G_m}(x_m) \cap \eta_{m,1}(g) \).

Another necessary ingredient in the proof of Theorem 3.1.3 is the connection between the groups \( C_{G_m}(x_m) \) and \( C_G(x_r) \), where \( r \leq m \) and \( x \in g \) is such that \( x_m \) is regular.

Lemma 3.1.12. Let \( m \in \mathbb{N} \) and \( x_m \in g_m \) be regular. For any \( 1 \leq r \leq m \) write \( x_r = \eta_{m,r}(x_m) \).

1. The map \( \eta_{m,r} : C_{G_m}(x_m) \rightarrow C_{G_r}(x_r) \) is surjective.
2. The map \( \eta_{m,r} : C_{G_m}(x_m) \rightarrow C_{G_r}(x_r) \) is surjective.

Proof. We prove both assertions by induction on \( r \).

1. The case \( r = 1 \) follows in Corollary 3.1.8 and Lang’s Theorem, as \( C_{\gamma,1}(x_1) \) and \( \eta_{m,1}(C_{\gamma,1}(x_m)) \) are both affine \( \sigma \)-spaces over \( k^{alg} \). Consider the commutative diagram in (3.9), in which both rows are exact by induction hypothesis.

\[
\begin{array}{cccccc}
C_{g^{r-1}_m}(x_m) & \rightarrow & C_{g^r_m}(x_m) & \xrightarrow{\eta_{m,r}} & C_{g^{r-1}_r}(x_r) & \rightarrow & 0 \\
\downarrow & & \downarrow \eta_{m,r} & & \downarrow & & \\
C_{g^{r-1}_r}(x_r) & \rightarrow & C_{g^r_r}(x_r) & \xrightarrow{\eta_{r,r-1}} & C_{g^{r-1}_r}(x_r) & \rightarrow & 0
\end{array}
\tag{3.9}
\]

By the Four Lemma (on epimorphisms), in order to prove the surjectivity of the map \( \eta_{m,r} : C_{g^m_m}(x_m) \rightarrow C_{g^r_r}(x_r) \), it suffices to show that the restricted map \( \eta_{m,r} : C_{g^{r-1}_m}(x_m) \rightarrow C_{g^{r-1}_r}(x_r) \) is surjective. This follows from the commutativity of the square in (3.10), in which the maps on the top and bottom rows are given the \( \sigma \)-module isomorphism \( y \mapsto \pi^{r-1}y \) (cf. Lemma 2.3.3), and the map on the left column is surjective by the base of induction.

\[
\begin{array}{ccc}
C_{g^{r-1}_m}(x_m) & \xrightarrow{\sim} & C_{g^{r-1}_m}(x_m) \\
\eta_{m,r} \downarrow & & \eta_{m,r} \downarrow \\
C_{g^1_m}(x_1) & \xrightarrow{\sim} & C_{g^{r-1}_r}(x_r)
\end{array}
\tag{3.10}
\]

2. In the current setting, one invokes Lemma 3.1.10 in order to prove the induction base \( r = 1 \). The case \( r > 1 \) is handled in a manner completely analogous to the first case, applying the Four Lemma for a suitable diagram of groups. The main difference from the previous case is that in
proving the surjectivity of the map \( \eta_{m,r} : \mathbb{C}_{G_{r}^{-1}}(x_{m}) \to \mathbb{C}_{G_{r}^{-1}}(x_{r}) \), one considers the commutative square in (3.11) in which the leftmost vertical arrow is shown to be surjective in the previous case, and the horizontal arrows are given by the suitable Cayley maps. Note that the fact that the top horizontal arrow in (3.11) is not necessarily a group homomorphism does not affect the proof of the assertion.

\[
\begin{array}{ccc}
\mathbb{C}_{G_{r}^{-1}}(x_{m}) & \xrightarrow{cay_{m}} & \mathbb{C}_{G_{r}^{-1}}(x_{m}) \\
\eta_{m,r} \downarrow & & \downarrow \eta_{m,r} \\
\mathbb{C}_{g_{r}^{-1}}(x_{r}) & \xrightarrow{cay_{r}} & \mathbb{C}_{G_{r}^{-1}}(x_{r})
\end{array}
\] (3.11) □

**Proof of Theorem 3.1.3.**(1) Given \( g_{m} \in \mathbb{C}_{G_{m}}(x_{m}) \) one inductively invokes Lemma 3.1.12 to construct a converging sequence \((g_{r})_{r \geq m}\) such that \( g_{r} \in \mathbb{C}_{G_{r}}(\eta_{r}(x)) \) and such that \( \eta_{r}(g_{r}) = g_{r}' \) for all \( r \geq r' \geq m \). The limit \( y = \lim_{r} g_{r} \) is easily verified to be an element of \( \mathbb{C}_{G}(x) \), which is mapped by \( \eta_{m} \) to \( g_{m} \). □

To finish the proof of Theorem 3.1.3, we now prove that the lift \( x \in \mathfrak{g} \) of a regular element \( x_{m} \in \mathfrak{g}_{m} \) is a regular element of \( \mathfrak{g} \), i.e. that its centralizer in \( \mathcal{G} \times K^{\text{alg}} \) has minimal dimension. By *Theorem 3.1.2.*(1), it suffices to prove this claim for the case \( m = 1 \). Since the dimension of an algebraic group is invariant under base extension, it suffices to show that if the centralizer group scheme \( \mathbb{C}_{G \times \mathcal{D}}(x) \) of \( x \) has an \( n \)-dimensional special fiber, then it must have an \( n \)-dimensional generic fiber. The argument we invoke here due to A. Stasinski\(^{1}\)

**Lemma 3.1.13.** Let \( x \in \mathfrak{g} \) and let \( \mathbb{C}_{x} = \mathbb{C}_{G \times \mathcal{D}}(x) \) be the centralizer group scheme over \( \mathcal{D} \). The dimension of the generic fiber of \( \mathbb{C}_{x} \) is lesser or equal than that of the special fiber of \( \mathbb{C}_{x} \).

**Proof.** The proof of the lemma appears in [21, (2.5.2)]. We recall it here for completeness.

Let \( \omega : \mathbb{C}_{x} \to \text{Spec}(\mathcal{D}) \) be the structure morphism, and let \( t \) be the generic point and \( s \) the special (closed) point of \( \text{Spec}(\mathcal{D}) \). By Chevalley’s upper-semicontinuity theorem, for any \( e \in \mathbb{N} \), the set of elements \( y \in \mathbb{C}_{x} \) such that \( \dim \omega^{-1}(\omega(y)) \geq e \) is closed. Fix \( e = \dim \omega^{-1}(t) = \dim \mathbb{C}_{x} \times K^{\text{unr}} \). Arguing as in [10, IV, Corollary 13.1.6] we have that the set of elements \( y \in \mathbb{C}_{x}^{\mathbb{C}} \) for which \( \dim \omega^{-1}(\omega(y)) < e \) is empty. Since this statement remains true under the action of the group of connected components \( \pi_{0}(\mathbb{C}_{x}) = \mathbb{C}_{x}/C_{x}^{\mathbb{C}} \) on \( \mathbb{C}_{x} \), it follows that for any \( y \in \mathbb{C}_{x} \), \( \dim \omega^{-1}(\omega(y)) \geq e \). Taking \( y \) in the fiber of \( \omega \) over \( s \) we obtain

\[
\dim \mathbb{C}_{x} \times k^{\text{alg}} = \dim \omega^{-1}(\omega(y)) \geq e = \dim \mathbb{C}_{x} \times K^{\text{unr}}. 
\]

□

**Proof of Theorem 3.1.3.**(2) By Lemma 3.1.13, given that \( x_{1} = \eta_{1}(x) \) is regular, we have that

\[
\dim \mathbb{C}_{G \times K_{s}^{\text{alg}}}(x_{1}) = \dim (\mathbb{C}_{G \times \mathcal{D}}(x) \times K^{\text{unr}}) \leq \dim (\mathbb{C}_{G \times \mathcal{D}}(x) \times k^{\text{alg}}) = \dim \mathbb{C}_{G_{1}}(x_{1}) = n.
\]

On the other hand, by [29, 3.5, Proposition 1], the minimum value of centralizer dimension of an element of \( \mathfrak{g} \) is \( n = \text{rk}(\mathbb{G}) \). Hence, \( x \) is regular. □

---

\(^{1}\)personal communication
Finally, we deduce Corollary 3.1.4.

**Proof of Corollary 3.1.4.** The regularity of $x$ in $g$, and Proposition 3.1.9 (applied for $L = K^{\text{alg}}$), imply that the centralizer of $x$ in $G(K^{\text{alg}})$ is an abelian group. In particular, it follows from this that the group $C_G(x)$ is abelian as well, and consequently, by Theorem 3.1.3(1), so are its quotient groups $C_{G_m}(x_m)$ for all $m \in \mathbb{N}$. □

### 3.2. Regular characters

At this point, our description of the regular elements of the Lie-algebras $g_m$ is sufficient in order to initiate the description of regular characters of $G$ and to prove Theorem I and Corollary 1.3.1. To do so, we prove the following variant of [17, Theorem 3.1].

**Theorem 3.2.1.** Let $\Omega \in g_1$ be a regular orbit and let $m \in \mathbb{N}$ and $r = \lfloor \frac{m}{2} \rfloor$.

1. The set $\text{Irr}(G_r^m \mid \Omega)$ of characters of $G_r^m = \text{Ker}(G_m \to G_r)$ which lie above the regular orbit $\Omega$ consists of exactly $q^{n(m-r-1)}$ orbits for the coadjoint action of $G_m$.
2. Given a character $\sigma \in \text{Irr}(G_r^m \mid \Omega)$, the set of irreducible characters of $G_m$ whose restriction to $G_r^m$ has $\sigma$ as a constituent is in bijection with the Pontryagin dual of $C_{G_r}(x_r)$.
3. Any such character $\sigma \in \text{Irr}(G_r^m \mid \Omega)$ extends to its inertia group $I_{G_m}(\sigma)$. In particular, each such extension induces to a regular character of $G_m$.

Note that the first assertion of Theorem I follows from Assertions (1) and (2) of Theorem 3.2.1 and Corollary 3.1.11. The second assertion of Theorem I follows from the Assertion (3) of Theorem 3.2.1 and Proposition 3.2.6 below.

The proof of Theorem 3.2.1 follows the same path as [17, § 3]. For the sake of brevity, rather than rehashing the proof appearing in great detail in loc. cit., our focus for the remainder of this section would be on setting up the necessary preliminaries and state the necessary modification required in order to adapt the construction of [17] to the current setting.

Recall that the group $G = G(\mathfrak{o})$ and $g = g(\mathfrak{o})$ are naturally embedded in the matrix algebra $M_N(\mathfrak{o})$ (see Section 2.1). Similarly, the congruence quotients $G_m$ and $g_m$ are embedded in $M_n(\mathfrak{e}_m)$. From here on, all computations the are to be understood in the framework of the embedding of the given groups and Lie-rings in their respective matrix algebras.

#### 3.2.1. Duality for Lie-rings

The Lie-algebra $g = g(\mathfrak{o}) \subseteq M_N(\mathfrak{o})$ is endowed with a symmetric bilinear $G(\mathfrak{o})$-equivariant form

$$\kappa : g \times g \to \mathfrak{o}, \quad (x, y) \mapsto \text{Tr}(xy),$$

such that $\{ x \in g \mid \kappa(x, y) \in \mathfrak{p} \text{ for all } y \in g \} = \pi g$. Fixing a non-trivial character $\psi : K \to \mathbb{C}^\times$ with conductor $\mathfrak{o}$ (see e.g. [2, § 5.3]), for any $m \in \mathbb{N}$, we have a well-defined map

$$g_m \to \widehat{g}_m, \quad y \mapsto \varphi_y \text{ where } \varphi_y(x) = \psi(\pi^{-m}\kappa(x, y)). \quad (3.12)$$

Furthermore, by the assumption $\pi^{-1}\mathfrak{o} \not\subseteq \text{Ker}(\psi)$, the map above induces a $G_m$-equivariant bijection of $g_m$ with its Pontryagin dual $\widehat{g}_m$. 19
3.2.2. Exponential and logarithm

Lemma 3.2.2. Let \( r, m \in \mathbb{N} \) with \( \frac{m}{3} \leq r \leq m \). The truncated exponential map, defined by

\[
\exp(x) = 1 + x + \frac{1}{2}x^2 \quad (x \in \mathfrak{g}_m^r),
\]

is a well-defined bijection of \( \mathfrak{g}_m^r \) onto the group \( G_m^r \), and is equivariant with respect to the adjoint action of \( G_m \). The inverse of \( \exp \) is given by

\[
\log(1 + x) = x - \frac{1}{2}x^2 \quad (1 + x \in G_m^r).
\]

In the case where \( \frac{m}{2} \leq r \), the exponential map is simply given by \( \exp(x) = 1 + x \) and defines an isomorphism of abelian groups \( \mathfrak{g}_m^r \to G_m^r \). The following lemma lists some basic formulas regarding the truncated exponential and logarithm map in the more general setting.

Lemma 3.2.3. Let \( r, m \in \mathbb{N} \) be such that \( \frac{m}{3} \leq r \leq m \). For any \( x, y \in \mathfrak{g}_m^r \),

\[
\log((\exp(x), \exp(y))) = \{x, y\},
\]

where \( (\exp(x), \exp(y)) \) denotes the group commutator of \( \exp(x) \) and \( \exp(y) \) in \( G_m^r \). Furthermore, the following truncated version of the Baker-Campbell-Hausdorff formula holds

\[
\log(\exp(x) \cdot \exp(y)) = x + y + \frac{1}{2}\{x, y\}.
\]

3.2.3. Characters of \( G_m^{\lfloor m/2 \rfloor} \)

Fix \( m \in \mathbb{N} \) and put \( r = \lfloor \frac{m}{2} \rfloor \) and \( r' = \lceil \frac{m}{2} \rceil = m - r \). As mentioned above, the exponential map on \( \mathfrak{g}_m^{r'} \) is given by \( x \mapsto 1 + x : \mathfrak{g}_m^{r'} \to G_m^{r'} \) and defines a \( G_m \)-equivariant isomorphism of abelian groups. Taking into account the module isomorphism \( x \mapsto \pi r' x : \mathfrak{g}_r \to \mathfrak{g}_m^{r'} \) and (3.12) we obtain a \( G_m \)-equivariant bijection

\[
\Phi : \mathfrak{g}_r \to \hat{\mathfrak{g}_r} \to \hat{\mathfrak{g}_m} \to \text{Irr}(G_m^{r'}),
\]

given explicitly by \( \Phi(y)(1 + x) = \varphi_y(\pi^{-r'} x) \), for \( y \in \mathfrak{g}_r \) and \( x \in \mathfrak{g}_m^{r'} \). In the case where \( m = 2r \) deduce the following.

Lemma 3.2.4. Assume \( m = 2r \) is even. The map \( \Phi \) defined in (3.13) is a \( G_m \)-equivariant bijection of \( \text{Irr}(G_m^{r'}) \) and \( \mathfrak{g}_r \).

In the case where \( m = 2r + 1 \), the irreducible characters of \( G_m^{r'} \) are classified in terms of their restriction to \( G_m^{r'} \), using the method of Heisenberg lifts, which we briefly recall here. For a more elaborate survey we refer to [17, § 3.2] and [7, Ch. 8].

Let \( \vartheta \in \text{Irr}(G_m^{r'}) \) be given, and let \( y \in \mathfrak{g}_r \) be such that \( \vartheta = \Phi(y) \). Note that, as the group \( G_m^{r'} \) is central in \( G_m^r \) and \( (G_m^{r'}, G_m^r) \subseteq G_m^r \), the following map is a well defined alternating \( \mathbb{C}^\times \)-valued bilinear form

\[
B_\vartheta : G_m^r/G_m^{r'} \times G_m^r/G_m^{r'} \to \mathbb{C}^\times, \quad B_\vartheta(x_1 G_m^{r'}, x_2 G_m^{r'}) = \vartheta((x_1, x_2)).
\]
Using the definition of $\Phi(y) = \vartheta$ and the explicit isomorphism $x \mapsto \exp(\pi^*x) : g_1 \to G'_r, G''_r$, we obtain an alternating bilinear form $\beta_r : g_1 \times g_1 \to k$ given by $\beta_r(x_1, x_2) = \text{Tr}(\eta_{r,1}(y) \cdot [x_1, x_2])$, such that the diagram in (3.14) commutes.

$$
\begin{array}{ccc}
G'_r \times G''_r & \xrightarrow{\beta_r} & k \\
\uparrow & & \uparrow \\
g_1 \times g_1 & \xrightarrow{\beta_r} & k
\end{array}
$$

(3.14)

A short computation, using the non-degeneracy of the trace and the definition of $\beta_r$, shows that the radical of this form coincides with the centralizer sub-algebra $C_{g_1}(\eta_{r,1}(y))$ of $g_1$ (see [17, p. 125]). Let $R_y$ and $R_y$ denote the preimages of $r_y$ in $g'_m$ and in $G'_r$ under the associated quotient maps. Let $r_y \subseteq j \subseteq g_1$ be a maximal subspace such that $\beta_y(j, i) = \{0\}$ (i.e. such that $j/r_y$ is a maximal isotropic subspace of $g_1/r_y$), and let $\tilde{J} \subseteq g'_m$ and $J \subseteq G'_r$ be the corresponding preimages of $j$; see (3.15).

$$
\begin{array}{ccc}
G'_m & \xrightarrow{\log} & g'_m \\
\uparrow & & \uparrow \\
J & \xrightarrow{\log} & j \\
\uparrow & & \uparrow \\
R_y & \xrightarrow{\log} & R_y \\
\uparrow & & \uparrow \\
G''_r & \xrightarrow{\log} & g''_m & \xrightarrow{0}
\end{array}
$$

(3.15)

Let $\theta = \vartheta \circ \exp$ be the pull-back of $\vartheta$ to $g'_m$. By virtue of the commutativity of $R_y$, the character $\theta'$ extends to a character of $R_y$ in $|R_y : G''_m| = |r_y|$ many ways. By Lemma 3.2.3, given such an extension $\theta' \in \hat{R}_y$, the map $\vartheta' : R_y \to \mathbb{C}^\times$ is a character of $R_y$. Thus, the character $\vartheta$ admits $|r_y|$ many extensions to $R_y$.

The proof of the following lemma appears in [7, Ch. 8].

**Lemma 3.2.5.** 1. Any extension $\vartheta' \in \text{Irr}(R_y)$ of $\vartheta$ extends further to a character $\vartheta'' \in \text{Irr}(J)$. 2. The induced character $\sigma = (\vartheta'')^{G''_m}$ is irreducible and is independent of the choice of extension $\vartheta''$ and of $\vartheta$. 3. The character $\sigma$ is the unique character of $G''_m$, whose restriction to $R_y$ contains $\vartheta'$. Furthermore, all irreducible characters of $G''_m$ which lie above $\vartheta$ are obtained in this manner.

### 3.2.4. Inertia subgroups in $G(\varphi_m)$ of regular characters

The final ingredient required in order to implement the construction of [17] to the current setting is a structural description of the inertia subgroup of a character of $G''_m$ lying below a regular character of level $\ell = m + 1$. As in the previous section, put $r = [m]$ and $r' = m/2$, and let $\vartheta \in \text{Irr}(G''_m)$. Recall that the inertia subgroup of $\vartheta$ in $G_m$ is defined by

$$
I_{G_m}(\vartheta) = \left\{ g \in G_m \mid \vartheta(g^{-1}xg) = \vartheta(x) \text{ for all } x \in G''_m \right\}.
$$

(3.16)
By Section 3.2.3, there exists a unique \( y \in \mathfrak{g}_r \), such that \( \vartheta = \Phi(y) \).

**Proposition 3.2.6.** In the setting described above, assume \( y \in \mathfrak{g}_r \) is regular. Let \( \hat{y} \in \mathfrak{g} \) be an arbitrary lift of \( y \) and put \( \hat{y}_j = \eta_j(y) \), for any \( j \in \mathbb{N} \). The inertia subgroup of \( \vartheta \) is of the form

\[
I_{G_m}(\vartheta) = G_m^\prime \cdot C_{G_m}(\hat{y}_m).
\] (3.17)

**Proof.** The inclusion \( \supseteq \) in (3.17) holds, regardless of whether \( y \) is regular. The converse inclusion follows from the exactness of the sequence

\[
1 \to G_m^\prime \to I_{G_m}(\vartheta) \to C_{G_m}(\hat{y}_m) \to 1,
\]
which follows from Corollary 3.1.11.

**Proof of Theorem 3.2.1.** A short computation, based on Corollary 3.1.11, proves that the set \( \hat{\Omega} = \eta_{-1}(\Omega) \) consists of \( q^n(r-1) \) distinct adjoint orbits for the action of \( G_r \), and hence for the action of \( G_m \) as well. By the \( G_m \)-equivariance of the map \( \Phi \), defined in Section 3.2.3, it follows that the set \( \text{Irr}(G_m^r \mid \Omega) \) consists of \( q^n(r-1) \) coadjoint orbits of \( G_m \). In the case where \( m \) is even, the first assertion of Theorem 3.2.1 follows from Lemma 3.2.4, since \( r = m - r \). In the case of \( m \) odd, by Lemma 3.2.5, and by regularity of the elements of \( \Omega \), any character in \( \text{Irr}(G_m^r \mid \Omega) \) extends to \( G_m^r \) in exactly \( q^m \)-many ways. Thus, the number of coadjoint \( G_m \)-orbits in \( \text{Irr}(G_m^r) \) is \( q^n(r-1+n) = q^n(m-r-1) \), whence the first assertion.

The second assertion of Theorem 3.2.1 follows from the third assertion, Proposition 3.2.6 and [16, Corollary 6.17].

Lastly, for the proof of the third assertion of Theorem 3.2.1, we refer to [17, § 3.5] for the explicit construction, in the analogous case of \( \text{GL}_n(\mathfrak{o}) \) and \( U_n(\mathfrak{o}) \), of an extension of a character \( \sigma \in \text{Irr}(G_m^r) \) to its inertia subgroup \( I_{G_m}(\sigma) \). Note that the construction of loc. cit. can be applied verbatim to the present setting, invoking the fact the \( I_{G_m}(\sigma) \) is generated by two abelian subgroups (Proposition 3.2.6 and Corollary 3.1.4) in the generality of classical groups.

**4. The symplectic and orthogonal groups**

**4.1. Summary of section**

In this section we compute the regular representation zeta function of classical groups of types \( \mathcal{B}_n, \mathcal{C}_n \) and \( \mathcal{D}_n \). Following Corollary 1.3.1, to do so, we classify the regular orbits in the space of orbits \( \text{Ad}(G_1) \setminus \mathfrak{g}_1 \) and compute their cardinalities, in order to obtain a formula for the Dirichlet polynomial

\[
\mathcal{D}_g(s) = \sum_{\Omega \in \mathcal{X}} |G_1| \cdot |\Omega|^{-(s+1)}.
\]

As it turns out, the cases where \( G \) is of type \( \mathcal{B}_n \) or \( \mathcal{C}_n \), i.e. \( G = \text{SO}_{2n+1} \) or \( G = \text{Sp}_{2n} \), can be handled simultaneously, and are analyzed in Section 4.3. The case of the groups of the form \( \mathcal{D}_n \), i.e. even-dimensional orthogonal groups, is slightly more intricate. The analysis of this case is carried out in Section 4.4. The main difference between the two cases lies in the fact that regularity of an element of the Lie-algebras \( \mathfrak{sp}_{2n}(k) \) and \( \mathfrak{so}_{2n+1}(k) \) is equivalent to it being give by a regular matrix in \( M_N(k) \) (cf. [31, § 5]). This equivalence fails to hold for even-orthogonal groups; see Lemma 4.4.1 below. Nevertheless, in both cases, we obtain a classification of the regular orbits in the Lie-algebra \( \mathfrak{g}_1 \) in terms of the minimal polynomial of the elements within the orbit.

Recall that two matrices \( x, y \in M_N(k) \) are said to be similar if there exists a matrix \( g \in \text{GL}_N(k) \) such that \( y = gxg^{-1} \). Our description of regular orbits of \( \mathfrak{g}_1 \) follows the steps.
1. Classification of all similarity classes in \( \mathfrak{gl}_N(k) \) which intersect the set of regular elements in \( \mathfrak{g}_1 \) non-trivially;
2. Description of the intersection of such a similarity class with \( \mathfrak{g}_1 \) as a union of \( \text{Ad}(G_1) \)-orbits;
3. Computation of the cardinality of the \( \text{Ad}(G_1) \)-orbit of each regular element.

4.1.1. Enumerative set-up

**Definition 4.1.1** (Type of a polynomial). Let \( f(t) \in k[t] \) be a polynomial of degree \( N \) and \( n = \lfloor \frac{N}{2} \rfloor \). For any \( 1 \leq d, e \leq n \), let \( S_{d,e}(f) \) denote the number of distinct monic irreducible even polynomials of degree \( 2d \) which occur in \( f \) with multiplicity \( e \), and let \( T_{d,e}(f) \) denote the number of pairs \( \{\tau(t), \tau(-t)\} \), with \( \tau(t) \) monic, irreducible and coprime to \( \tau(-t) \), such that \( \tau \) is of degree \( d \) and occurs in \( f \) with multiplicity \( e \). Let \( r(f) \) be the maximal integer such that \( t^{2r(f)} \) divides \( f \). The **type** of \( f \) is defined to be the triplet \( (\tau(f), S(f), T(f)) \), where \( S(f) \) and \( T(f) \) are the matrices \( (S_{d,e}(f))_{d,e} \) and \( (T_{d,e}(f))_{d,e} \) respectively.

Recall that \( X_n \) denotes the set of triplets \( \tau = (r, S, T) \in \mathbb{N}_0 \times M_n(\mathbb{N}_0) \times M_n(\mathbb{N}_0) \), with \( S = (S_{d,e}) \) and \( T = (T_{d,e}) \) which satisfy
\[
r + \sum_{d,e=1}^{n} de \cdot (S_{d,e} + T_{d,e}) = n.
\]

Note that, for \( n = \lfloor \frac{N}{2} \rfloor \), it holds that \( \tau(f) \in X_n \) whenever \( f \) is monic and satisfies \( f(-t) = (-1)^N f(t) \).

The number of monic irreducible polynomials of degree \( d \) over \( k \) is given by evaluation at \( t = q \) of the function \( w_d(t) = \frac{1}{\varphi_m(t)} \mu \left( \frac{m}{t} \right) t^d \), where \( \mu(\cdot) \) is the Möbius function (see, e.g., [11, Ch. 14]). A polynomial \( f \in k[t] \) is said to be **even** (resp. **odd**) if it satisfies the condition \( f(-t) = f(t) \) (resp. \( f(-t) = -f(t) \)). Note that, by assumption the \( k \) is of odd characteristic, the only monic irreducible odd polynomial over \( k \) is \( f(t) = t \). The number of monic irreducible even polynomials of degree \( d \) over \( k \) is given by evaluation at \( t = q \) of the function\(^1\)
\[
E_d(t) = \begin{cases} \frac{1}{2} \sum_{r|m, 2|m} \mu \left( \frac{m}{t} \right) (t^r - 1) & \text{if } d = 2m \text{ is even} \\ 0 & \text{otherwise}. \end{cases} \tag{4.1}
\]

Put
\[
P_d(t) = \begin{cases} \frac{w_d(t) - E_d(t)}{t - 1} & \text{if } d > 1 \\ t - 1 & \text{if } d = 1. \end{cases} \tag{4.2}
\]

Note that, for \( q \) odd, \( P_d(q) \) is the number of irreducible polynomials of degree \( d \) which are neither odd nor even over a field of cardinality \( q \).

Given \( N \in \mathbb{N}, n = \lfloor \frac{N}{2} \rfloor \), and \( \tau \in X_n \), the number of polynomials \( f \in k[t] \) of type \( \tau(f) \) such that \( f(-t) = (-1)^N f(t) \) is given by evaluation at \( t = q \) of the polynomial
\[
M_{\tau}(t) = \left( \frac{1}{2} \right)^n \sum_{d,e} T_{d,e} \prod_{d=1}^{n} \left( S_{d,1}, S_{d,2}, \ldots, S_{d,n} \right) \cdot \left( E_{2d}(t) \right) \cdot \left( \sum_{e} T_{d,e} \right) \cdot \left( P_d(t) \right) \cdot \left( \sum_{e} T_{d,e} \right). \tag{4.3}
\]

\(^1\)The function \( E_d(t) \) is probably well-known. In the lack of a reference, a proof of (4.1) is given in Appendix A.

I wish to thank Jyrki Lahtonen [18] of the Mathematics Stack Exchange network taking part in computing this formula.
Theorem II

Theorem II

Theorem 4.1.3 and 4.3.2. Then Theorem 4.1.2 and 4.3.1, respectively. Theorem III may be completed by direct computation.

4.1.2. Statement of results- symplectic and odd-dimensional special orthogonal groups

Theorem 4.1.2. Assume \( \text{char}(k) \neq 2 \). Let \( V = k^n \) and let \( B \) be a non-degenerate bilinear form which is anti-symmetric if \( N = 2n \) is even, and symmetric if \( N = 2n + 1 \). Let \( G \in \{ \text{Sp}_{2n}, \text{SO}_{2n+1} \} \) be the algebraic group of isometries of \( V \) with respect to \( B \) and put \( G_1 = G(k) \) and \( g_1 = g(k) \) where \( g = \text{Lie}(G) \).

Let \( x \in M_N(k) \) have minimal polynomial \( m_x \in k[t] \).

1. The element \( x \) is similar to a regular element of \( g_1 \) if and only if \( m_x \) has degree \( N \) and satisfies \( m_x(-t) = (-1)^N m_x(t) \).

Furthermore, assume \( x \in g_1 \) is a regular element and let \( \Omega = \text{Ad}(G_1)x \) denote its orbit under \( G_1 \).

2. If \( N \) is even and \( m_x(0) = 0 \), then the intersection \( \text{Ad}(\text{GL}_N(k))x \cap g_1 \) is the union of two distinct \( \text{Ad}(G_1) \)-orbits. Otherwise, \( \text{Ad}(\text{GL}_N(k))x \cap g_1 = \Omega \).

3. Let \( \tau = \tau(m_x) = (r(m_x), S(m_x), T(m_x)) \) as in Definition 4.1.1. Then

\[
|\Omega| = q^{2n^2} \cdot \left( \frac{1}{2} \right)^\nu \frac{\prod_{i=1}^{n}(1 - q^{-2i})}{\prod_{i,d,e \leq n}(1 + q^{-d})^{S_d,e(m_x)} \cdot (1 - q^{-d})^{T_d,e(m_x)}},
\]

where \( \nu = 1 \) if \( N = 2n \) is even and \( m_x(0) = 0 \), and \( \nu = 0 \) otherwise.

The proofs of Assertions (1), (2) and (3) of the theorem are carried out in sections 4.3.1, 4.3.2 and 4.3.3 respectively.

4.1.3. Statement of results- even-dimensional special orthogonal groups

Theorem 4.1.3. Assume \( |k| > 3 \) and \( \text{char}(k) \neq 2 \). Let \( N = 2n \) with \( n \geq 2 \). Let \( V = k^n \) and let \( B^+ \) and \( B^- \) be non-degenerate symmetric forms on \( V \) of Witt index \( n \) and \( n-1 \), respectively. Given \( \epsilon \in \{ \pm 1 \} \), let \( G^\epsilon = \text{SO}_{2n}^\epsilon \) be the k-algebraic group of isometries of \( V \) with respect to \( B^\epsilon \) and put \( G_1^\epsilon = G_1^\epsilon(k) \) and let \( g_1^\epsilon = g_1^\epsilon(k) \), where \( g^\epsilon = \text{Lie}(G^\epsilon) \).

Let \( x \in M_N(k) \) have minimal polynomial \( m_x(t) \).

1. If \( m_x(0) = 0 \) (i.e. \( x \) is a singular matrix) then the following are equivalent.
   (a) The polynomial \( m_x \) has degree \( N - 1 \) and satisfies \( m_x(-t) = -m_x(t) \).
   (b) The element \( x \) is similar to a regular element of \( g_1^\epsilon \).
   (c) The element \( x \) is similar to a regular element of \( g_1^\epsilon \).

Otherwise, if \( m_x(0) \neq 0 \), let \( \epsilon = \epsilon(x) = (-1)^{\sum_{e \in S_d,e(m_x)}} \) where \( S = (S_d,e(m_x)) \) is as in Definition 4.1.1. Then \( x \) is similar to a regular element of \( g_1^\epsilon \) if and only if \( m_x \) has degree \( N \) and satisfies \( m_x(-t) = m_x(t) \). Moreover, in this case \( x \) is not similar to an element of \( g_1^{-\epsilon} \).

Furthermore, assume \( x \in g_1^\epsilon \) is a regular element and let \( \Omega^\epsilon = \text{Ad}(G_1^\epsilon)x \) denote its orbit under \( G_1^\epsilon \), for \( \epsilon \in \{ \pm 1 \} \) fixed.
2. In the case where \( m_x(0) = 0 \), the intersection \( \text{Ad}(\text{GL}_N(k))x \cap g_1^t \) is the disjoint union of two distinct \( \text{Ad}(G_1^t) \)-orbits. Otherwise, \( \text{Ad}(\text{GL}_N(k))x \cap g_1^t = \Omega^e \).

3. (a) Assume \( m_x(0) = 0 \) and let \( \tau = \tau(t \cdot m_x) \). Then

\[
\vert \Omega^e \vert = q^{2n^2} \cdot \frac{1}{2} \cdot \frac{(1 + eq^{-n}) \prod_{i=1}^{n-1} (1 - q^{2i})}{\prod_{1 \leq d, e \leq n} (1 + q^{-d})^{S_{d,e}(m_x)} \cdot (1 - q^{-d})^{T_{d,e}(m_x)}}.
\]

(b) Otherwise, let \( \tau = \tau(m_x) \). Then

\[
\vert \Omega^e \vert = q^{2n^2} \cdot \frac{(1 + eq^{-n}) \prod_{i=1}^{n-1} (1 - q^{2i})}{\prod_{1 \leq d, e \leq n} (1 + q^{-d})^{S_{d,e}(m_x)} \cdot (1 - q^{-d})^{T_{d,e}(m_x)}}.
\]

The proofs of Assertions (1), (2) and (3) of the theorem appear in sections 4.4.1, 4.4.2 and 4.4.3. The exclusion of the specific case of \( k = F_3 \) is done for technical reasons, and may possibly be undone by replacement of the argument in Lemma 4.4.8 below.

4.2. Preliminaries to the proofs Theorem 4.1.2 and Theorem 4.1.3

4.2.1. Regularity for non-singular elements

**Lemma 4.2.1.** Let \( x \in g(k^{alg}) \subseteq gl_N(k^{alg}) \) be non-singular. Then \( x \) is regular in \( g(k^{alg}) \) if and only if \( x \) is a regular element of \( gl_N(k^{alg}) \).

**Proof.** Let \( W = (k^{alg})^N \), so that \( g(k^{alg}) \) is given as the Lie-algebra of anti-symmetric operators with respect to a non-degenerate bilinear form \( B = B_{k^{alg}} \) on \( W \) (see Section 2.1.1). Note that the existence of non-singular elements in \( g(k^{alg}) \) implies that \( N = 2n \) is even. Indeed, \( x \in g(k^{alg}) \) if and only if \( x^* = -x \) (notation of Section 2.1.1), and \( \det(x) = \det(x^*) = (-1)^N \det(x) \) is possible if and only if \( N \) is even, since \( \text{char}(k^{alg}) \neq 2 \).

Let \( x = s + h \) be the Jordan decomposition of \( x \), with \( s, h \in g(k^{alg}) \), \( s \) semisimple, \( h \) nilpotent and \([s, h] = 0 \). Let \( \lambda_1, \ldots, \lambda_t \in k^{alg} \) be non-zero and such that \( \{\pm \lambda_1, \ldots, \pm \lambda_t\} \) is the set of all eigenvalues of \( s \) with \( \lambda_i \neq \pm \lambda_j \) whenever \( i \neq j \). As in Proposition 2.1.1, the space \( W \) decomposes as a direct sum \( W = \bigoplus_{i=1}^{t} (W_{\lambda_i} \oplus W_{-\lambda_i}) \), where, for any \( i = 1, \ldots, t \), the subspace \( W_{\lambda_i} = W_{\lambda_i} \oplus W_{-\lambda_i} \) is non-degenerate, and its subspaces \( W_{\lambda_i} \) and \( W_{-\lambda_i} \) are maximal isotropic. Comparing centralizer dimension, and invoking [29, § 3.5, Proposition 1], we have that \( x \) is regular if and only if the restriction of \( x \) to each of the subspaces \( W_{\lambda_i} \) (\( i = 1, \ldots, t \)) is regular in \( gl_N(W_{\lambda_i}) \). Likewise, \( x \) is regular in \( g(k^{alg}) \) if and only if the restriction of \( x \) to each subspace \( W_{\lambda_i} \) is regular within the Lie-algebra of anti-symmetric operators with respect to the restriction of \( B_{k^{alg}} \) to \( W_{\lambda_i} \). Thus, it is sufficient to prove the lemma in the case where \( s \) has precisely two eigenvalues \( \lambda, -\lambda \).

Representing \( s \) in a suitable eigen-basis, \( s \) may be identified with the block-diagonal matrix \( \text{diag}(\lambda 1_n, -\lambda 1_n) \). Under this identification, the centralizer of \( s \) in \( gl_N(k^{alg}) \) is identified with the subgroup of block diagonal matrices consisting of two \( n \times n \) blocks. Moreover, the involution \( * \) maps an element \( \text{diag}(y_1, y_2) \in C_{gl_N(k^{alg})}(s) \), with \( y_1, y_2 \in gl_n(k^{alg}) \) to the matrix \( \text{diag}(y_2, y_1^t) \). In particular, it follows that \( h \in C_{gl_n}(k^{alg}) \cap g(k^{alg}) \) is of the form \( h = \text{diag}(h_1, -h_1^t) \), where \( h_1 \in gl_n(k^{alg}) \) is nilpotent. Arguing as in [25, III, § 1], we have that

\[
C_{\text{GL}_N}(x) = C_{\text{GL}_N(s)}(h) \simeq C_{\text{GL}_n}(h_1) \times C_{\text{GL}_n}(-h_1^t) \simeq C_{\text{GL}_n}(h_1) \times C_{\text{GL}_n}(h_1)
\]

where the final isomorphism utilizes the isomorphism \( y \mapsto (y^t)^{-1} : C_{\text{GL}_n}(-h_1^t) \rightarrow C_{\text{GL}_n}(h_1) \).
Additionally, since the group $G$ is embedded in $GL_N$ as the group of unitary elements with respect to $\star$, we have $\text{diag}(y_1, y_2) \in C_{GL_N(k^{alg})}(s) \cap G(k^{alg})$ if and only if $y_2 = (y_1')^{-1}$, and hence the map $y \mapsto \text{diag}(y, (y')^{-1})$ is an isomorphism of $C_{GL_n}(h_2)$ onto $C_{C_G(s)}(h)$ and hence
\[ C_G(x) = C_{C_G(s)}(h) \simeq C_{GL_n}(h_1). \]
Thus
\[ \dim C_{GL_N}(x) = 2 \dim C_{GL_n}(h_1) = 2 \dim C_G(x), \]
and the lemma follows.

\[ \square \]

Remark. The assumption that $x$ is non-singular in Lemma 4.2.1 is crucial, as the proof relies heavily on the fact that the centralizer of a non-singular semisimple element of $\gamma_1$ is a direct product of groups of the form $GL_{n_i}(k^{alg})$. The same argumentation would not apply in the case where $x$ is singular, and in fact fails in certain cases; see Lemma 4.4.1 below.

4.2.2. From similarity classes to adjoint orbits

In this section develop some the tools required in order to analyze the decomposition of the set $\Pi_x = \text{Ad}(GL_N(k))x \cap \mathfrak{g}_1$, for $x \in \mathfrak{g}_1$ regular, in to $\text{Ad}(G_1)$-orbits. The results appearing below can also be derived from [32, § 2.6]. However, as the case of regular elements allows for a much more transparent argument, we present it here for completeness.

Let $\text{Sym}(\star; x)$ be the set of elements $Q \in C_{GL_N(k)}(x)$ such that $Q^* = Q$ and define an equivalence relation on $\text{Sym}(\star; x)$ by
\[ Q_1 \sim Q_2 \quad \text{if there exists } a \in C_{GL_N(k)}(x) \text{ such that } Q_1 = a^*Q_2a. \quad (4.4) \]

Let $\Theta_x$ be the set of equivalence classes of $\sim$ in $\text{Sym}(\star; x)$. In the case where $C_{GL_N(k)}(x)$ is abelian (e.g., when $x$ is a regular element of $\mathfrak{gl}_N(k)$), the set $\text{Sym}(\star; x)$ is a subgroup and the set $\Theta_x$ is simply its quotient by the image of restriction of $w \mapsto w^*w$ to $C_{GL_N(k)}(x)$.

Proposition 4.2.2. Let $x \in \mathfrak{g}_1$ and let $\Pi_x$ denote the intersection $\text{Ad}(GL_N(k))x \cap \mathfrak{g}_1$. There exists a map $\Lambda : \Pi_x \to \Theta_x$ such that $y_1, y_2 \in \Pi_x$ are $\text{Ad}(G_1)$-conjugate if and only if $\Lambda(y_1) = \Lambda(y_2)$.

Proof. 1. Construction of $\Lambda$. Let $y \in \Pi_x$ and let $w \in GL_N(k)$ be such that $y = wxw^{-1}$. Put $Q = w^*w$. Note that, as $x, y \in \mathfrak{g}_1$, by applying the anti-involution $\star$ to the equation $y = wxw^{-1}$, we deduce that $(w^*)^{-1}xw^* = y$ as well and consequently, that $Q = w^*w$ commutes with $x$. Since $Q^* = Q$, we get that $Q \in \text{Sym}(\star; x)$.

Define $\Lambda(y)$ to be the equivalence class of $Q$ in $\Theta_x$. To show that $\Lambda$ is well-defined, let $w' \in GL_N(k)$ be another element such that $y = w'xw'^{-1}$ and $Q' = w'^*w'$. Put $a = w^{-1}w'$. Then $a$ commutes with $x$, and
\[ a^*Qa = w'^*(w^*)^{-1}Qw^{-1}w' = w'^*w' = Q', \]
hence $Q \sim Q'$.

2. Proof that $y_1, y_2 \in \Pi_x$ are $\text{Ad}(G_1)$-conjugate if $\Lambda(y_1) = \Lambda(y_2)$. Let $w_1, w_2 \in GL_N(k)$ be such that $y_1 = w_1xw_1^{-1}$, and let $Q_i = w_i^*w_i$ ($i = 1, 2$). Then, by assumption, there exists $a \in C_{GL_N(k)}(x)$ such that $Q_2 = a^*Q_1a$. Put $z = w_1aw_2^{-1}$. Note that $z_{y_2}z^{-1} = y_1$. We claim that $z \in G_1$. This holds since for any $u, v \in V$
\[ B(zu, vz) = B(w_1aw_2^{-1}u, w_1aw_2^{-1}v) = B(a^*(w_1^*w_1)aw_2^{-1}u, w_2^{-1}v) \]
\[ = B(a^*Q_1aw_2^{-1}u, w_2^{-1}v) = B(Q_2w_1^{-1}u, w_2^{-1}v) \quad \text{(since } Q_2 = a^*Q_1a) \]
\[ = B(w_2^*u, w_2^{-1}v) = B(u, v). \]
3. Proof that \( y_1, y_2 \in \Pi_x \) are Ad(\( G_1 \))-conjugate only if \( \Lambda(y_1) = \Lambda(y_2) \). Assume now that \( z \in G_1 \) is such that \( y_1 = zy_2z^{-1} \), and let \( w_1, w_2 \in \text{GL}_N(k) \) be such that \( y_i = w_i x w_i^{-1} \) \((i = 1, 2)\). Then \( w_1 \) and \( zw_2 \) both conjugate \( x \) to \( y_1 \), and hence, by the unambiguity of the definition of \( \Lambda \) and fact that \( z \in G_1 \), we have that

\[
\Lambda(y_1) = [w_1^*w_1] = [w_2^*(z^*z)w_2] = [w_2^*w_2] = \Lambda(y_2).
\]

\( \square \)

A crucial property of the set \( \Theta_x \) in the case \( x \) is regular, which makes the analysis of adjoint orbits feasible, is that it may be realized within the quotient of an étale algebra over \( k \) by the image of the algebra under an involution. As a consequence, the set \( \Pi_x \) decomposes into \(|\text{Im}\Lambda|\) many \( \text{Ad}(G_1) \)-orbits, a quantity which does not exceed the value four in the regular case.

Let us state another general lemma, which will be required in the description of \( \Theta_x \).

**Lemma 4.2.3.** Let \( \mathcal{C} \subseteq M_N(k) \) be the ring of matrices commuting with a matrix \( x \), with \( x^* = -x \) \((\text{or } x^* = x)\), and let \( N \triangleleft \mathcal{C} \) be a nilpotent ideal, invariant under \( \star \). The following are equivalent, for any \( Q_1, Q_2 \in \text{Sym}(\mathcal{C}; x) \).

1. There exists \( a \in \mathcal{C} \) such that \( a^*Q_1a = Q_2 \);
2. There exists \( a \in \mathcal{C} \) such that \( a^*Q_1a \equiv Q_2 \mod N \).

**Proof.** The argument of \([32, \text{Theorem } 2.2.1]\) applies to the case where \( N \) is any nilpotent ideal which is invariant under \( \star \), provided that the required trace condition holds. In the present case the condition holds since \( \text{char}(k) \neq 2 \). \( \square \)

### 4.2.3. Similarity classes via bilinear forms

We recall a basic lemma which would allow us to determine when an element of \( \mathfrak{gl}_N(k) \) is similar to an element of \( \mathfrak{g}_1 \). Here and in the sequel, given a non-degenerate bilinear form \( C \) on a finite dimensional vector space \( V \) over \( k \), we call an operator \( x \in \text{End}(V) \) \textit{\( C \)-anti-symmetric}, if \( C(xu, v) + C(u, xv) = 0 \) holds for all \( u, v \in V \).

**Lemma 4.2.4.** Let \( C_1, C_2 \) be two non-degenerate bilinear forms on a vector space \( V = k^N \), and assume there exists \( g \in \text{End}(V) \) and \( \delta \in k \) such that \( C_1(gu, gv) = \delta C_2(u, v) \) for all \( u, v \in V \). Let \( x \in \mathfrak{gl}_N(k) \) be \( C_2 \)-anti-symmetric. Then \( gxg^{-1} \) is \( C_1 \)-anti-symmetric.

The proof of **Lemma 4.2.4** is by direct computation, and is omitted.

### 4.3. Symplectic and odd-dimensional special orthogonal groups

The following well-known fact will prove very useful in the classification of regular conjugacy classes in symplectic and odd-dimensional special orthogonal Lie-algebras.

**Lemma 4.3.1.** Let \( \epsilon = -1 \) and \( N = 2n \) in the symplectic case, or \( \epsilon = 1 \) and \( N = 2n + 1 \) in the special orthogonal case. Let \( C_1, C_2 \) be two non-degenerate forms on \( V = k^N \) such that \( C_i(u, v) = \epsilon C_i(v, u) \) for all \( u, v \in V \) and \( i = 1, 2 \). There exists \( \delta \in k \) and \( g \in \text{End}(V) \) such that \( C_1(gu, gv) = \delta C_2(u, v) \) for all \( u, v \in V \). Additionally, if \( \epsilon = -1 \) then \( \delta \) can be taken to be 1.

**Proof.** See, e.g., \([35, \S 3.4.4]\) in the symplectic case and \([35, \S 3.4.6 \text{ and } \S 3.7]\) in the special orthogonal case. \( \square \)
Lemma 4.3.2. Let \( x \in \mathfrak{gl}_N(k) \) with minimal polynomial \( m_x(t) \in k[t] \).

1. If \( x \) is similar to an element of \( \mathfrak{g}_1 \) then \( m_x(t) \) satisfies \( m_x(-t) = (-1)^{\deg m_x} m_x(t) \).
2. If \( x \) is a regular element of \( \mathfrak{gl}_N(k) \) (and hence \( \deg m_x = N \)) such that \( m_x(t) = (-1)^N m_x(t) \), then \( x \) is similar to an element of \( \mathfrak{g}_1 \).

Proof. For the first assertion, we may assume \( x \in \mathfrak{g}_1 \). Note that for any \( r \in \mathbb{N} \) we have that \( B(x^ru, v) = B(u, (-1)^rx^r v) \) for all \( u, v \in V \). Invoking the non-degeneracy of \( B \), we deduce that \( (-1)^{\deg m_x} m_x(-t) \) is a monic polynomial of degree \( \deg m_x \) which vanishes at \( x \), and hence equal to \( m_x(t) \).

By Lemma 4.2.4, to prove the second assertion it would suffice to construct a non-degenerate bilinear form \( C \) on \( V \) such that \( B \) and \( C \) satisfy the hypothesis of Lemma 4.2.4. In view of Lemma 4.3.1, in the present case it suffices to construct some non-degenerate bilinear form \( C \) on \( V \) such that \( C(u, v) = \epsilon C(v, u) \), where \( \epsilon = (-1)^N \), and such that \( x \) is \( C \)-anti-symmetric.

By [29, Ch. III, 3.5, Proposition 2], the assumption that \( x \) is a regular matrix is equivalent to \( V \) being a cyclic module over the ring \( k[x] \) (which, in turn, is equivalent to \( \deg m_x = N \)). In particular, there exists \( v_0 \in V \) such that \( (v_0, xv_0, \ldots, x^{N-1}v_0) \) is a \( k \)-basis for \( V \). Let \( \text{Prj}_{N-1} : V \to k \) denote the projection onto \( k \cdot x^{N-1}v_0 \). Given \( u_1, u_2 \in V \) let \( p_1, p_2 \in k[t] \) be polynomials such that \( u_i = p_i(x)v_0 \) and define
\[
C(u_1, u_2) = \text{Prj}_{N-1} (p_1(x)p_2(-x)v_0). \tag{4.5}
\]
The fact that \( C \) is well-defined, bilinear and satisfies \( C(u, v) = \epsilon C(c, u) \) follows by direct computation. Let us verify that \( C \) is non-degenerate.

Let \( u \in V \) be non-zero, and let \( p(t) \) be such that \( p(x)v_0 = u \). By unambiguity of the definition of \( C \), we may assume that \( \deg p(t) < N \). Let \( v = x^{N-\deg p}v_0 \in V \). Then
\[
C(u, v) = \text{Prj}_{N-1}((-1)^{N-\deg p}x^{N-\deg p}p(x)v_0)
\]
is non-zero, since \( t^{N-\deg p}p(t) \) is a polynomial of degree \( N-1 \).

Finally, for \( u_i = p_i(x)v_0 \) as above, we have that
\[
C(xu, v) + X(u, xv) = \text{Prj}_{N-1}(x p_1(x)p_2(x)v_0) + \text{Prj}_{N-1}(p_1(x) \cdot (-xp_2(-x)v_0)) = \text{Prj}_{N-1}(0) = 0,
\]
and hence \( x \) is \( C \)-anti-symmetric. \( \square \)

Note that Lemma 4.3.2 gives a criterion for a regular element of \( \mathfrak{gl}_N(k) \) to be similar to an element of \( \mathfrak{g}_1 \), but a-priori, not necessarily to a regular element of \( \mathfrak{g}_1 \). We will shortly see that it is indeed the case that the similarity class of such \( x \) meets \( \mathfrak{g}_1 \) at a regular orbit. Before proving this, let us consider an important example.

Example 4.3.3 (Regular nilpotent elements). Let \( x \in \mathfrak{gl}_N(k) \) be a regular nilpotent element, i.e. \( m_x(t) = t^N \). Picking a generator \( v_0 \) for \( V \) over \( k[x] \) and putting \( \mathcal{E} = (v_0, xv_0, \ldots, x^{N-1}v_0) \), the element \( x \) is represented in the basis \( \mathcal{E} \) by the matrix
\[
\Upsilon = \begin{pmatrix}
0 & 1 & \cdots & \cdots \\
\cdots & \ddots & \ddots & \ddots \\
0 & \cdots & 1 & 0
\end{pmatrix}. \tag{4.6}
\]
The bilinear form $C$ of Lemma 4.3.2 is represented in this basis by the matrix

$$c = \begin{pmatrix}
1 & & \\
& -1 & \\
& & \\
& & (-1)^{N-1}
\end{pmatrix}.$$  \hspace{1cm} (4.7)

To show that $\Upsilon$ is similar to a regular element of $\mathfrak{g}_1$ we now pass to the algebraic closure of $k$ and compute the dimension of the centralizer of $z\Upsilon z^{-1}$ in $\Gamma_1$, where $z\Gamma_1z^{-1} \in \mathfrak{g}_1$. Note that the centralizer of $\Upsilon$ in $\mathrm{GL}_N(k^{\text{alg}})$ consists of upper triangular Töplitz matrices,

$$C_{\mathrm{GL}_N(k^{\text{alg}})}(\Upsilon) = \left\{ \begin{pmatrix} a_0 & a_1 & \cdots & a_{N-1} \\
 & \ddots & \ddots & \\
 & & a_0 & a_1 \\
 & & & a_0 \\
 \end{pmatrix} \mid a_0, \ldots, a_{N-1} \in k^{\text{alg}}, a_0 \neq 0 \right\} \simeq (k^{\text{alg}}[t]/(t^N))^\times.$$

Additionally, the map $g \mapsto zg^{-1}$ induces an isomorphism of $C_{\Gamma_1}(z\Upsilon z^{-1})$ onto the subgroup of elements $y \in C_{\mathrm{GL}_N(k^{\text{alg}})}(\Upsilon)$ which preserve $C(\cdot, \cdot)$, i.e. such that $y^c c y = c$. Computing the dimension of this subgroup, e.g. by passing to its Lie-algebra, one easily verifies that it is of dimension (no greater than) $n$ over $k^{\text{alg}}$, and hence $\Upsilon$ is similar to a regular element of $\mathfrak{g}_1$.

**Proposition 4.3.4.** Let $x \in \mathfrak{g}_1$. Then $x$ is a regular element of $\mathfrak{g}_1$ if and only if $x$ is regular in $\mathfrak{gl}_N(k)$.

**Proof.** By [29, § 3.5, Proposition 1], we need to show dim $C_{\Gamma_1}(x) = n$ if and only if dim $C_{\mathrm{GL}_N \times k^{\text{alg}}}(x) = N$. Let $x = s + h$ be the Jordan decomposition of $x$ over $k^{\text{alg}}$, with $s, h \in \mathfrak{g}(k^{\text{alg}})$, $s$ semisimple, $h$ nilpotent, and $[s, h] = 0$. As seen in the proof of **Proposition 2.1.1**, the space $W = (k^{\text{alg}})^N$ decomposes as an orthogonal direct sum $W_1 \oplus W_0$ with respect to the ambient bilinear form $B_{k^{\text{alg}}}$, where $W_0 = \ker(s)$ and $s|_{W_1}$ is non-singular. Let $\Sigma \subseteq \mathfrak{g}(k^{\text{alg}})$ be the subgroup of elements acting trivially on $W_0$ and preserving $W_1$, and let $\Delta$ be as in **Proposition 2.1.1**. Then

$$C_{\Gamma_1}(x) = C_{\Sigma}(x) \times C_{\{1_{W_1}\} \times \Delta}(x)$$

and

$$C_{\mathrm{GL}_N(k^{\text{alg}})}(x) = C_{\mathrm{GL}(W_1) \times \{1_{W_0}\}}(x) \times C_{\{1_{W_1}\} \times \mathrm{GL}(W_0)}(x)$$

and therefore the proof reduces to the cases where $x$ is non-singular and where $x$ is a nilpotent element acting on $W_0$. The first case follows from **Lemma 4.2.1**, whereas the second case follows from **Example 4.3.3** and from the uniqueness of a regular nilpotent orbit over algebraically closed fields [29, III, Theorem 1.8].

**Proof of **Theorem 4.1.2.** (1).** **Proposition 4.3.4** implies that any element $x \in \mathfrak{M}_N(k)$ which is similar to a regular element of $\mathfrak{g}_1$ is regular as an element of $\mathfrak{gl}_N(k)$. It follows easily that deg $m_x = N$ and $m_x(-t) = (-1)^N m_x(t)$ (see **Lemma 4.3.2.** (1)). The converse implication is given by **Lemma 4.3.2.** (2).
4.3.2. From similarity classes to adjoint orbits

In this section is to we analyze decomposition of the set $\text{Ad}(\text{GL}_N(k))x \cap g_1$, for $x \in g_1$ regular, into $\text{Ad}(G_1)$-orbits, and prove Theorem 4.1.2.(2).

Notation 4.3.5. Given a polynomial $f(t) \in k[t]$ we write $k(f)$ for the quotient ring $k[t]/(f)$. For example, if $f$ is an irreducible polynomial over $k$ then $k(f)$ stands for the splitting field of $f$. We write $\text{GL}_1(k(f))$ for the group of units of $k(f)$.

Assuming further that $f(t) = \pm f(-t)$, let $\sigma_f$ denote the $k$-involution of $k(f)$, induced from the $k[t]$-involution $t \mapsto -t$, and let $U_1(k(f))$ be the group of elements $\xi \in k(f)$ such that $\sigma_f(\xi) \cdot \xi = 1$.

Proposition 4.3.6. Let $x \in g_1$ be a regular element, and put $\Pi_x = \text{Ad}(\text{GL}_N(k))x \cap g_1$. If $x$ is singular and $N$ is even, then the intersection $\Pi_x$ is the disjoint union of two distinct $\text{Ad}(G_1)$-orbits. Otherwise, $\Pi_x = \text{Ad}(G_1)x$.

Proof. The notation of Proposition 4.2.2 is used freely throughout the proof. We proceed in the following steps.

1. Computation of the cardinality of $\Theta_x$. Namely, we show that $|\Theta_x| = 2$ if $x$ is singular and equals 1 otherwise.
2. Description of the image of the map $\Lambda$ in $\Theta_x$.

By Lemma 4.3.2, the minimal polynomial $m_x$ of $x$ is of degree $N$ and satisfies $m_x(-t) = (-1)^N m_x(t)$. Thus, it can be expressed uniquely as the product of pairwise coprime factors

$$m_x(t) = t^{d_1} \prod_{i=1}^{d_2} \varphi_i(t)^{r_i} \prod_{i=1}^{d_3} \theta_i(t)^{r_i}, \quad (4.8)$$

where the polynomials $\varphi_1, \ldots, \varphi_{d_2}$ are irreducible, monic and even, and $\theta_1, \ldots, \theta_{d_3}$ are of the form $\theta_i(t) = \tau_i(t) \cdot \tau_i(-t)$ with $\tau_i(t)$ monic, irreducible and coprime to $\tau_i(-t)$. The centralizer $\mathcal{C} = \mathbb{C}_{G_M(k)}(x)$ is isomorphic to the ring $k(m_x)$ and the restriction of the involution $\ast$ to $\mathcal{C}$ is transferred via this isomorphism to the map $\sigma_{m_x}$, defined in Notation 4.3.5. By the Chinese remainder theorem, we get

$$\mathcal{C} \simeq k(t^{d_1}) \times \prod_{i=1}^{d_2} k(\varphi_i(t)^{m_i}) \times \prod_{i=1}^{d_3} k(\theta_i(t)^{r_i}). \quad (4.9)$$

Furthermore, the restriction of the involution $\sigma_{m_x}$ to each of the factors $k(f)$, for $f \in \{t^{d_1}, \varphi_i^{m_i}, \theta_j^{r_j}\}$ coincides with the respective involution $\sigma_f$, induced from $t \mapsto -t$. A short computation shows that the nilpotent radical of $\mathcal{C}$ is isomorphic to the direct product of the nilpotent radicals of all factors on the right hand side of (4.9), and that the quotient $\mathcal{C}/N$ is isomorphic to the étale algebra

$$\mathbb{K} = k^{r} \times \prod_{i=1}^{d_2} k(\varphi_i) \times \prod_{i=1}^{d_3} k(\theta_i), \quad (4.10)$$

where $r = 1$ if $d_1 > 0$ (i.e. if $x$ is singular) and equals 0 otherwise\footnote{Here it is understood that the ring $k^{0}$ is the trivial algebra $\{0\}$.}. Let $\dagger$ denote the involution induced on the $k$-algebra $\mathbb{K}$ in (4.10) from the restriction of $\ast$ to $\mathcal{C}$. From the observation regarding the action of $\ast$ on $\mathcal{C}$ above, we deduce the following properties of the involution $\dagger$ on $\mathbb{K}$.
D1. The involution \( \dagger \) preserves the factor \( k^r \) and acts trivially on it.

D2. The involution \( \dagger \) preserves the factors \( k \langle \varphi_i \rangle \) and coincides with the non-trivial field involution \( \sigma_{\varphi_i} \).

D3. The involution \( \dagger \) preserves the factors \( k \langle \theta_i \rangle \) and maps a pair \((\xi, \nu) \in k(\tau_i(t)) \times k(\tau_i(-t))\) to the pair \((\iota^{-1}(\nu), \iota(\xi))\), where \( \iota: k(\tau_i(t)) \to k(\tau_i(-t)) \) is the isomorphism induced from \( t \mapsto -t \).

Let \( \text{Sym}(\dagger) \) be subgroup of \( \mathcal{K}^\times \) of elements fixed by \( \dagger \). Note that, as \( \mathcal{K} \simeq \mathbb{C}/\mathbb{N} \) is a commutative ring, by Lemma 4.2.3, the set \( \Theta_x \) can be identified with the quotient of \( \text{Sym}(\dagger) \) by the image of the map \( z \mapsto z^1z : \mathcal{K} \to \text{Sym}(\dagger) \).

By (D2) and the theory of finite fields, the restriction of the map \( z \mapsto z^1z \) to the factors \( k \langle \varphi_i \rangle \) coincides with the field norm onto the subfield of element fixed by \( \dagger \), and is surjective onto this subfield. Furthermore, by (D3), it is evident that an element \((\xi, \nu) \in k(\tau_i(t)) \times k(\tau_i(-t))\) is fixed by \( \dagger \) if an only if \( \nu = \iota(\xi) \), in which case \((\xi, \nu) = (\xi, 1)^\dagger \cdot (1, 1)\). Lastly, by (D1) it holds that the image of the restriction of \( z \mapsto z^1z \) to the multiplicative group of \( k^r \) is either trivial, if \( r = 0 \), or the group of squares in \( k^r \), otherwise. It follows from this that the set \( \Theta_x \) is either in bijection with the quotient \((k^r/(k^r)^2)\), and hence of cardinality \( 2 \), if \( x \) singular, or otherwise trivial. This completes the first step of the proof.

For the second step, we divide the analysis according to the parity of \( N \), in order to describe the image of \( \Lambda \).

\( N \) even. In this case we show that \( \Lambda \) is surjective. To do so, let \( Q \in \text{Sym}(\ast; x) \). Note that, by assumption, \( Q^\ast = Q \) and \( Q \in \text{GL}_N(k) \), and hence the form \((u, v) \mapsto B(u, Qv)\) is alternating and non-degenerate. By Lemma 4.3.1, there exists \( w \in \text{GL}_N(k) \) such that \( Q = w^*w \). To show that \( Q \in \text{Im} \Lambda \) we only need to verify that \( y = wxw^{-1} \in \mathfrak{g}_1 \). This holds, as

\[
y^* = (w^*)^{-1}x^*w^* = -(w^*)^{-1}(QxQ^{-1})w^* = -wxw^{-1} = -y,
\]

since \( Q \) is assumed to commute with \( x \).

\( N \) odd. Note that in this case, all elements of \( \mathfrak{g}_1 \) are non-singular and hence \(|\Theta_x| = 2 \) for all \( x \in \mathfrak{g}_1 \). In this case we prove that the map \( \Lambda \) is not surjective. Note that by definition of the equivalence class \( \sim \), if \( Q_1, Q_2 \in \text{Sym}(\ast; x) \) are such that \( Q_1 \sim Q_2 \), then \( \det(Q_1)^{-1}\det(Q_2) \) is a square in \( k^\times \). This holds since \( \det(a^\ast) = \det(a) \) for all \( a \in M_N(k) \). By the same token, it follows that the \( \det(w^*w) \) is a square in \( k^\times \) for all \( w \in \text{GL}_N(k) \).

Therefore, to show that \( \Lambda \) is not surjective, it suffices to show that \( \text{Sym}(\ast; x) \) contains elements whose determinant is not a square in \( k \). One may take, for example, the element \( Q = \delta \cdot 1_N \), for \( \delta \in k^\times \) non-square.

\[ \square \]

4.3.3. Centralizers of regular elements

Finally, we compute the order of the centralizer of a regular element of \( \mathfrak{g}_1 \). The analysis we propose is analogous to \([17, \text{Proposition 4.4}]\).

**Lemma 4.3.7.** Let \( x \in \mathfrak{g}_1 \) be regular with minimal polynomial

\[
m_x(t) = t^{d_1} \prod_{i=1}^{d_2} \varphi_i(t)^{l_i} \prod_{i=1}^{d_3} \theta_i(t)^{r_i},
\]

31
where the product on the right hand side is as in (4.8), with $\theta_i(t) = \tau_i(t)\tau_i(-t)$. The determinant map induces a short exact sequence

$$1 \to C_{G_1}(x) \to U_1(k(t^{d_i})) \times \prod_{i=1}^{d_2} U_1(k(\varphi_i^{d_i})) \times \prod_{i=1}^{d_3} GL_1(k(\tau_i^{d_i})) \xrightarrow{\text{det}} Z \to 1 \quad (4.11)$$

where $Z \subseteq k^\times$ is the subgroup of order 2 if $N$ is odd and trivial otherwise.

**Proof.** As shown in the proof on Proposition 4.3.6, the centralizer of $x$ in $GL_N(k)$ is isomorphic to the group of units of the ring $C$, i.e. the direct product

$$C_{GL_N(k)}(x) \simeq GL_1(k(t^{d_1})) \times \prod_{i=1}^{d_2} GL_1(k(\varphi_i^{d_i})) \times \prod_{i=1}^{d_3} GL_1(k(\tau_i^{d_i})).$$

Furthermore, the involution $\ast$ of $GL_N(k)$ restricts to an involution of $C_{GL_N(k)}(x)$ which is transferred via this isomorphism to the involution $\sigma_{\theta_i^r}$, induced by $t \mapsto -t$, and restricts to the involution $\sigma_f$ on each of the factors $GL_1(k(f))$ for $f \in \{t^{d_1}, \varphi_i^{d_i}, \tau_i^{d_i}\}$.

The additional condition $z^\ast z = 1$, and the fact that $\ast$ preserves all factors in the decomposition (4.9), imply that the centralizer of $x$ in $G_1$ is embedded in the group

$$U_1(k(t^{d_1})) \times \prod_{i=1}^{d_2} U_1(k(\varphi_i(t)^{d_i})) \times \prod_{i=1}^{d_3} U_1(k(\theta_i(t)^{d_i})).$$

Similarly to Proposition 4.3.6, the map $\sigma_{\theta_i^r}$ acts on the factors $GL_1(k(\theta_i(t)^{d_i})) \simeq GL_1(k(\tau_i(t)^{d_i})) \times GL_1(k(\tau_i(-t)^{d_i}))$ as $(\xi, \nu) \mapsto (\nu^{-1}(\nu), \nu(\xi))$, where $\iota : k(\tau_i(t)^{d_i}) \to k(\tau_i(-t)^{d_i})$ is the isomorphism induced from $t \mapsto -t$. It follows from this that $(\xi, \nu) \in U_1(k(\theta_i^{d_i}))$ if and only if $\iota(\xi) = \nu^{-1}$, and hence that $U_1(k(\theta_i^{d_i})) \simeq GL_1(k(\tau_i^{d_i}))$.

Lastly, we compute order of the group $Z$. Since for any $w \in GL_N(k)$ we have that $\det(w^\ast) = \det(w)$, it follows that the condition $w^\ast w = 1$ implies that $\det(w) \in \{\pm 1\}$. Thus, to complete the lemma, we need to show that both values occur in the case of $N$ odd, and that only 1 is possible for $N$ even. Both statements are well-known. The former can be proved simply by considering the elements $\pm 1 \in GL_N(k)$, while the latter can be deduced by considering the Pfaffian of the matrix $w^T J w = J$. \[\square\]

**Lemma 4.3.8.** Let $f \in k[t]$ be a monic irreducible polynomial with $f(-t) = \pm f(t)$ and let $r \in \mathbb{N}$. Let $E_{f^r}$ denote the image of the map $z \mapsto \sigma_f^r(z) : GL_1(k(f^r)) \to GL_1(k(f^r))$. Given $y \in GL_1(k(f^r))$ it holds that $y \in E_{f^r}$ if and only if

1. $\sigma_f^r(y) = y$, and
2. there exists $z \in GL_1(k(f(t)^r))$ such that $y \equiv z \sigma_f^r(z) \pmod{f}$.

In particular, we have

$$|E_{f^r}| = \begin{cases} q^{\frac{1}{2}r \deg f (1 - q^{-\frac{1}{2} \deg f})} & \text{if } f(t) \neq t \\ q^{\frac{1}{2}r [q^r]^r} & \text{if } f(t) = t. \end{cases}$$
Proof. Let $W$ denote the vector space underlying the ring $k(f^r)$ and let $C$ be the bilinear form defined on $W$ as in Lemma 4.3.2. Let $x$ be the linear operator defined on $W$ by multiplication by $t$. The map $t \mapsto x$ sets up a ring isomorphism of $k(f^r)$ with the ring $\mathcal{C} \subseteq M_{n_{\deg f}}(k)$ of matrices commuting with $x$, and the involution $\ast$ on $\mathcal{C}$ is identified with the ring involution $\sigma_f$. Note that, in the current setting, if $y \in k(f^r)$ is the image modulo $(f^r)$ of a polynomial $\hat{y}(t)$, then the assumption $\sigma_f(y) = y$ is equivalent to $\hat{y}(x) \in \mathcal{C}$ satisfying $\hat{y}(x)^r = \hat{y}(x)$ or, in the notation of Section 4.2.2, to $\hat{y}(x) \in \text{Sym}(\ast; x)$. Also, the nilpotent radical of $\mathcal{C}$ is given as the image of the ideal $(f) \subseteq k(f^r)$. The equivalence stated in the lemma now follows from Lemma 4.2.3, by taking $Q_1 = 1$ and $Q_2 = \hat{y}(x) \in \text{Sym}(\ast; x)$.

We now compute the cardinality of $E_f$. In the case $f(t) = t$, the equivalence proved above implies that $E_f$ can be identified with the subgroup of the ring $k[t]/(t')$ of truncated polynomials of degree no greater than $r - 1$, which consists of even polynomials whose constant term is an invertible square of $k$. Hence $|E_f| = q^{\frac{r}{2} - \deg f}$. In the complementary case, by irreducibility, necessarily $f(t) = f(-t)$ and has even degree. In this case, by the Jordan-Chevalley Decomposition Theorem, there exist polynomials $S, H \in k[t]$ such that the endomorphism $S(x)$ (resp. $H(x)$) acts semisimply (resp. nilpotently) on the vector space $W = k(f^r)$, on which $x$ acts by multiplication by $t$, and such that $H(t) + S(t) \equiv t \pmod{f(t)^r}$ (see [15, § 4.2]; note that $S, H \in k[t]$ is possible since $k$ is perfect). It follows that $k(f^r) \simeq k[x] = k[S(x)][H(x)]$. A quick computation shows that the minimal polynomials of $S(x)$ and $H(x)$ are $f(t)$ and $t'$ respectively, and thus $k(f) \simeq k[S(x)][H(x)] \simeq k(f) \otimes_k (k[h]/(h^r))$. Moreover, by the properties of the Jordan-Chevalley decomposition, both $S(t)$ and $H(t)$ satisfy $S(-x) = -S(x)$ and $H(-x) = -H(x)$ [6, § 3, Proposition 3]. Thus, under this identification, the involution $\sigma_f$ is transferred to an involution of $k(f) \otimes_k (k[h]/(h^r))$, mapping $h$ to $-h$ and acting as $\sigma_f$ on the field $k(f)$.

By the equivalence in the lemma, and the theory of finite fields, the group $E_f$ is identified with the subgroup of $(k(f^r))^\times$ of elements fixed by $\sigma_f$. Using the identification above, this subgroup consists of elements of the form $\sum_{i=0}^{r-1} a_i \otimes h^i$, with $a_0, \ldots, a_{r-1} \in k(f)$, $a_0 \neq 0$, and

$$\sigma_f(a_i) = \begin{cases} a_i & \text{if } i \text{ is even} \\ -a_i & \text{if } i \text{ is even}. \end{cases}$$

The equality $|E_f| = q^{\frac{r}{2} \deg f} (1 - q^{-\frac{1}{2} \deg f})$ now follows by direct computation.

Proposition 4.3.9. Let $x \in \mathfrak{g}_1$ be a regular element with minimal polynomial $m_x \in k[t]$. Let $\tau(m_x) = (r(m_x), S(m_x), T(m_x)) \in \mathcal{X}_n$ be the type of $m_x$ (see Definition 4.1.1). Then

$$|C_G_t(x)| = 2^n q^n \prod_{d,e} (1 + q^{-d})^{S_{d,e}(m_x)} \cdot (1 - q^{-d})^{T_{d,e}(m_x)},$$

where $\nu = 1$ in the case where $N = 2n$ is even and $r(m_x) > 0$, and $\nu = 0$ otherwise.

Proof. Let $m_x = t^{d_1} \prod_{i=1}^{d_2} \varphi_i^{l_i} \prod_{i=1}^{d_3} \theta_i^{l_i}$ be a decomposition of $m_x$ as in (4.8), with $\varphi_i$ even and irreducible, and $\theta_i(t) = \tau_i(t)\tau_i(-t)$ with $\tau_i(t), \tau_i(-t)$ irreducible and coprime. Note that by definition of $\tau(m_x)$ we have that $r(m_x) = \left\lfloor \frac{d_1}{2} \right\rfloor$.

In view of Lemma 4.3.7 it suffices to show the following three assertions.

1. $|U_1(k(t^{d_1}))| = 2q^{r(m_x)}$;
Lemma 4.3.8: below we shall construct such an element

Theorem 4.1.2

Lemma 4.4.2

Proposition 4.3.9 follows directly from Theorem 4.1.2, the group \( \text{GL}_k \) in the even dimensional special orthogonal groups

...orthogonal case.

4.4. Even dimensional special orthogonal groups

The following lemma demonstrates the failure of the first assertion of Theorem 4.1.2 in the even orthogonal case.

Lemma 4.4.1: Let \( N = 2n \) be even and let \( x \in \text{gl}_N(k^{alb}) \) be a regular nilpotent element. Then \( x \) is not anti-symmetric with respect to any non-degenerate symmetric bilinear form on \( V = (k^{alb})^N \).

Proof. Note that, as \( x \) is conjugate to an \( N \times N \) nilpotent Jordan block, the kernel of \( x \) is one dimensional. Assume towards a contradiction that \( C \) is a symmetric non-degenerate bilinear form on \( V \) such that \( x \) is \( C \)-anti-symmetric. Consider the form \( F(u, v) = C(u, xv) \) on \( V \). By assumption \( C(xu, v) + C(u, xv) = 0 \), we have that \( F \) is anti-symmetric. Additionally, the radical of \( F \) coincides with the kernel of \( x \), by non-degeneracy of \( C \). By properties of antisymmetric forms, it follows that the kernel of \( x \) is even-dimensional. A contradiction.

Nonetheless, regular nilpotent elements in the case of even-dimensional special orthogonal groups are well-known to exist [25, III, 1.19]. In Lemma 4.4.2 below we shall construct such an element and compute its centralizer.

Recall that non-degenerate symmetric bilinear forms on \( V = k^N \) are classified by the dimension of a maximal totally isotropic subspace of \( V \) with respect to the given form (i.e. its Witt index), and that over a finite field of odd characteristic there are exactly two such forms, up to isometry. We fix \( B^+ \) and \( B^- \) to be bilinear forms on \( V \) of Witt index \( n \) and \( n - 1 \), respectively. In suitable bases, the forms \( B^+ \) and \( B^- \) are represented by the matrices

\[
J^+ = \begin{pmatrix}
0 & 1 \\
1 & 0 \\
. & . & & \\
0 & 1 \\
1 & 0
\end{pmatrix}
\quad \text{or} \quad
J^- = \begin{pmatrix}
0 & 1 \\
1 & 0 \\
. & . & & \\
0 & 1 \\
1 & 0
\end{pmatrix},
\]

34
where $\delta \in \mathfrak{o}^\times$ is a fixed non-square.

Given $\epsilon \in \{-1, 1\}$, let $G_1^\epsilon = \text{SO}_N^\epsilon(k)$ and $\mathfrak{g}_1^\epsilon = \mathfrak{so}_N^\epsilon(k)$ be the group of isometries of determinant 1 and the Lie-algebra of anti-symmetric operators with respect to the form $B^\epsilon$. We will also occasionally use the colloquial notation $G_1^\epsilon = G_1^+ \cup G_1^-$ and $\mathfrak{g}_1^\epsilon = \mathfrak{g}_1^+ \cup \mathfrak{g}_1^-$. For example, the phrase $x$ is a regular element of $\mathfrak{g}_1^\epsilon$ indicates that $x$ is either a regular element of $\mathfrak{g}_1^+$ or of $\mathfrak{g}_1^-$. 

### 4.4.1. Similarity classes of regular elements

In this section we prove the first assertion of Theorem 4.1.3, which classifies the similarity classes of $\mathfrak{gl}_N(k)$ whose intersection with $\mathfrak{g}_{1}^{\pm}$ consists of regular elements. Following this, we differentiate whether such a similarity class intersects $\mathfrak{g}_1^+$ or $\mathfrak{g}_1^-$. 

Note that if $x \in \mathfrak{g}_{1}^{\pm}(k)$ is a non-singular element whose minimal polynomial $m_x$ is even and has degree $N$ then, by applying the argument of Lemma 4.3.2.(2) verbatim, we have that $x$ is anti-symmetric with respect to a non-degenerate symmetric bilinear form and hence similar to an element of $\mathfrak{g}_1^\epsilon$. By Lemma 4.2.1, all non-singular regular elements of $\mathfrak{g}_1^\epsilon$ are obtained in this manner. Thus, for $x \in \mathfrak{g}_1^\epsilon(k)$ non-singular, it holds that $x$ is similar to a regular element of $\mathfrak{g}_1^\epsilon$ if and only if the minimal polynomial of $x$ is even and of degree $N$.

As explained below (see Proposition 4.4.9), the case of singular regular elements of $\mathfrak{g}_1^\epsilon$ is essentially reduced to the study of nilpotent regular elements. These elements are considered in the following lemma.

**Lemma 4.4.2.** Let $x \in \mathfrak{g}_1^\epsilon(k)$ have minimal polynomial $m_x(t) = t^{N-1}$. Then $x$ is similar to a regular nilpotent element of $\mathfrak{g}_1^+$, as well as to a regular nilpotent element of $\mathfrak{g}_1^-$. 

**Proof.** By considering the Jordan normal form of such an element $x$, there exist elements $v_0, u_0 \in V$ with $u_0 \in \text{Ker}(x)$ and such that $E = \{v_0, x_0, \ldots, x^{N-2}v_0, u_0\}$ is a $k$-basis for $V$.

Let $E' = \{v_0, \ldots, x^{N-2}v_0\}$ and $V' = \text{Span}_k E'$. Since the element $x |_{V'} \in \mathfrak{gl}(V')$ has minimal polynomial $t^{N-1} = t^{\dim V'}$, it is regular in $\mathfrak{gl}(V')$. By the proof of Lemma 4.3.2, there exists a non-degenerate symmetric bilinear form $C'$ on $V'$, with respect to which $x |_{V'}$ is anti-symmetric. We wish to extend $C'$ to a non-degenerate symmetric bilinear form on $V$, with respect to which $x$ is anti-symmetric. This is equivalent to finding an invertible matrix $d \in M_N(k)$, whose top-left $(N-1) \times (N-1)$ submatrix coincides with the matrix $c$ of Example 4.3.3 (see (4.7)), and such that

$$d' \Upsilon + \Upsilon d = 0 \quad \text{where} \quad \Upsilon = [x]_E = \begin{pmatrix} 0 & 1 & & \cdots & \cdots & 0 \\ & \ddots & \ddots & \ddots & \ddots & \end{pmatrix}. \quad (4.12)$$

A short computation shows that the matrix

$$d = d_\eta = \begin{pmatrix} \eta & & & \cdots & \cdots & 1 \\ & \ddots & \ddots & \ddots & \cdots & \end{pmatrix} \quad \text{and} \quad (4.13)$$

35
where \( \eta \in k^\times \) satisfies the required equality. Furthermore, by applying a signed permutation to \( \mathcal{E} \), one may verify easily that \( d_y \) is congruent to the matrix \( J^+ \) of (4.12) if \( \eta \) is a square, and to \( J^- \) otherwise. Thus, \( x \) is similar in this case to elements of both \( g^+_1 \) and \( g^-_1 \).

Lastly, we need to verify that \( x \) is similar to a regular element of \( g^+_1 \). To do so, we pass to the algebraic closure \( k^{\text{alg}} \) of \( k \) and compute the centralizer in \( G(k^{\text{alg}}) \) of an element \( zz^{-1} \in g_1 \).

Working in the basis \( \mathcal{E} \), by direct computation, one sees that the centralizer of \( x \) in \( M_N(k^{\text{alg}}) \) can be identified with the set of matrices \( y = \left( \begin{array}{cc} A & v \\ u & r \end{array} \right) \), where

1. \( A \in M_{N-1}(k^{\text{alg}}) \) and commutes with the restriction of \( \Upsilon \) to \( V' = \text{Span}_{k^{\text{alg}}} \mathcal{E}' \);
2. \( u, v \in (k^{\text{alg}})^{N-1} \) are elements of the kernel of \( \Upsilon \) and \( \mathcal{E}' \), respectively, and hence of the form \( v = (v_1, 0, \ldots, 0) \) and \( u = (0, \ldots, 0, u_{N-1}) \); and
3. \( r \in k^{\text{alg}} \) is arbitrary.

As in Example 4.3.3, the centralizer of \( zz^{-1} \in g_1 \) is conjugated in \( \text{GL}_N(k^{\text{alg}}) \) to the group

\[ \{ y \in C_{\text{GL}_N(k^{\text{alg}})}(\Upsilon) \mid y' \cdot d = d \} . \]

Computing its Lie-algebra, which consists of matrices \( y = \left( \begin{array}{cc} A & v \\ u & r \end{array} \right) \) satisfying \( y' \cdot d + dy = 0 \), we get the additional three conditions

1. \( A' \cdot c + c \cdot A = 0 \), where \( c \) is as in Example 4.3.3;
2. \( \eta \cdot u + cv = 0 \), i.e. \( v_1 = -\eta u_{N-1} \); and
3. \( 2pr = 0 \), and hence \( r = 0 \).

It follows that \( C_{T_1}(zz^{-1}) \) is at most \( n \)-dimensional, and hence \( x \) is regular.

To streamline the analysis of nilpotent regular orbits, let us fix some notation.

**Notation 4.4.3.** Given a matrix \( A \in M_{N-1}(k) \), column vectors \( v, u \in k^{N-1} \) and \( r \in k \), let \( \Xi(A, v, u, r) \) denote the \( N \times N \) matrix

\[ \Xi(A, v, u, r) = \left( \begin{array}{cc} A & v \\ u & r \end{array} \right) . \]

We also write \( A^\circ \) for the matrix \( cA' \cdot c \), where \( c \) is as in Example 4.3.3. Note that, in the case where \( d = d_y \) is the representing matrix for the symmetric bilinear form given on \( V' \), we have that

\[ \Xi(A, v, u, r)^* = \left( \begin{array}{cc} A^\circ & \eta cu \\ \eta^{-1}v' \cdot c & r \end{array} \right) = \Xi(A^\circ, \eta cu, \eta^{-1}cv, r). \quad (4.14) \]

The next step of the computation is to differentiate whether a given element \( x \in g_{N}(k) \), which is similar to a regular element of \( g^+_1 \), is similar to either \( g^+_1 \) or \( g^-_1 \). We first consider two specific cases, depending on the minimal polynomial of \( x \).

**Lemma 4.4.4.** Let \( x \in g_{N}(k) \) have minimal polynomial \( m_x \). Assume \( x \) is similar to a regular element of \( g^+_1 \).

1. If \( m_x(t) = f(t)f(-t) \) for some polynomial \( f \in k[t] \) with \( f(0) \neq 0 \), then \( x \) is similar to an element of \( g^+_1 \), and not to an element of \( g^-_1 \).
2. If \( m_x = \varphi^r \) for \( \varphi \in k[t] \) an even irreducible polynomial and \( r \in N \) odd, then \( x \) is similar to a regular element of \( g^+_1 \) and not to an element of \( g^-_1 \).
Proof. Let $C$ be a non-degenerate symmetric bilinear, with respect to which $x$ is $C$-anti-symmetric. We will show that $C$ necessarily has Witt index $n$ in the first case and $n-1$ in the second case.

1. By the assumption $m_+(0) \neq 0$ and Lemma 4.2.1, it follows that $x$ is also a regular element of $\mathfrak{gl}_N(k)$, and hence the space $V$ is cyclic as a $k[x]$ module. Put $W = f(x)V$. Then $W$ is isomorphic, as a $k[x]$-module, to $V/f(-x)V$, and hence is of dimension $n = \frac{n+1}{2}$ over $k$. Additionally, for any $u, v \in V$ we have $C(f(x)u, f(x)v) = C(f(x)f(-x)u, v) = 0$, and hence $W$ is totally isotropic.

2. Let us first consider the case where $r = 1$, and hence $V$ is isomorphic to the field extension $k\langle \varphi \rangle$ of $k$. Furthermore, the map $\sigma_\varphi \in \text{Aut}_k(k\langle \varphi \rangle)$, induced from $t \mapsto -t$ is a field involution of $k\langle \varphi \rangle$ over $k$, with fixed field $K$, such that $|k\langle \varphi \rangle : K| = 2$. Note that in this setting, without loss of generality, we may assume that $\langle u, v \rangle = \text{Tr}_{k\langle \varphi \rangle/k}(\sigma_\varphi(u)v)$ for all $u, v \in V$. Indeed, invoking the separability of the extension $k\langle \varphi \rangle/k$, there exists an element $c \in k\langle \varphi \rangle$ such that $\langle u, 1 \rangle = \text{Tr}_{k\langle \varphi \rangle/k}(c \cdot u)$ for all $u \in k\langle \varphi \rangle$. From the symmetry of $C$ and the invariance of $\text{Tr}_{k\langle \varphi \rangle/k}$ under $\sigma_\varphi$, it can be deduced that in fact $c \in K$. By the theory of finite fields, there exists an element $d \in k\langle \varphi \rangle$ such that $c = \sigma_\varphi(d)d$. It follows that multiplication by $d$ is an isometry of $C$ with the trace pairing $(u, v) \mapsto \text{Tr}_{k\langle \varphi \rangle/k}(\sigma_\varphi(u)v)$.

Note that an element $u \in k\langle \varphi \rangle$ is isotropic if and only if $\sigma_\varphi(u)u$ is a traceless element of $K$. Since the number of non-zero traceless elements in the extension $K/k$ is $q^n - 1$, and by the surjectivity of the norm map $N_{k\langle \varphi \rangle/K}$, it follows that the number of non-zero isotropic element of $k\langle \varphi \rangle$ is $(q^n - 1)(q^n - 1)$. The fact that $C$ is of Witt index $n - 1$ now follows as in [35, § 3.7.2].

For the case $r > 1$, put $l = \lfloor \frac{r}{2} \rfloor$ and $U = \varphi(x)^{l+1}V$. Then, similarly to (1), $U$ is an isotropic subspace of $V$, with perpendicular space $U^\perp = \varphi(x)^lV$. Moreover, the form $C$ reduces to a non-degenerate symmetric bilinear form on the quotient space $U^\perp/U$, on which $\varphi$ acts as an anti-symmetric operator with minimal polynomial $\varphi$. By the case $r = 1$, we find a two-dimensional anisotropic subspace $L \subseteq U^\perp/U$, whose pull-back to $U^\perp$ contains a two-dimensional anisotropic subspace of $V$. It follows that the Witt index of $C$ is necessarily $n - 1$.

\[ \square \]

Having Lemma 4.4.4 at hand, we need one more basic tool in order to complete the classification of similarity classes containing regular elements of $\mathfrak{gl}_1^\pm$.

**Notation 4.4.5.** Given a finite, even-dimensional vector space $U$ over $k$ with a non-degenerate symmetric bilinear form $C$, put $\delta_U = 1$ if $U$ is of Witt index $\frac{n}{2}$ and $\delta_U = -1$ otherwise.

**Lemma 4.4.6.** Let $U, W$ be finite, even dimensional vector spaces over $k$ with non-degenerate symmetric bilinear forms $C_U$ and $C_V$ respectively. Endow the space $U \oplus W$ with the non-degenerate symmetric bilinear form $C_{U \oplus W}(u + w, u' + w') = C_U(u, u') + C_W(w, w')$ where $u, u' \in U$ and $w, w' \in W$. Then

\[ \delta_{U \oplus W} = \delta_U \cdot \delta_W. \]

**Proof.** Since the direct sum of two isotropic subspaces is again isotropic, the only non-trivial case to be checked is when $\delta_U = \delta_W = -1$. To begin with, we consider the case where $\text{dim} U = \text{dim} W = 2$ and the forms $C_U$ and $C_W$ are anisotropic with orthogonal bases $(u_1, u_2)$ and $(w_1, w_2)$ of $U$ and $W$ respectively.

Let $f : U \oplus W \rightarrow k$ be the quadratic form associated to $C_{U \oplus W}$, i.e. $f(v) = C_{U \oplus W}(v, v)$ for all $v \in U \oplus W$. Note that, by the assumption that both forms are anisotropic, $f$ does not vanish on 37
the given bases and, necessarily \( f(u_1) \not\equiv f(u_2) \pmod{(k^*)^2} \) and \( f(w_1) \not\equiv f(w_2) \pmod{(k^*)^2} \). As the set \( \{f(u_1), f(u_2), f(w_1), f(w_2)\} \), must contain two elements from the same coset of \( k^*/(k^*)^2 \), without loss of generality we may assume \( f(u_1) \equiv f(w_1) \pmod{(k^*)^2} \). By general properties of finite fields, there exist \( \alpha_1, \alpha_2, \beta_1, \beta_2 \in k \) such that

\[
\alpha_1^2 f(u_1) + \beta_1^2 f(w_1) = -f(u_2) \quad \text{and} \quad \alpha_2^2 f(u_1) + \beta_2^2 f(w_1) = -f(w_2).
\]

It follows easily that the set \( \{\alpha_1 u_1 + \beta_1 w_1 + u_2, \alpha_2 u_1 + \beta_2 w_1 + w_2\} \) is linearly independent and consists of isotropic vectors. Therefore \( \delta_{U \oplus W} = 1 \).

For the general case, assume \( \delta_U = \delta_W = -1 \) and let \( U, W \) have dimensions \( 2m \) and \( 2r \) respectively. Let \( U' \) and \( W' \) be maximal isotropic subspaces of \( U \) and \( W \), respectively, and let \( \{u_1, u_2\} \subseteq U \smallsetminus U' \) and \( \{w_1, w_2\} \subseteq W \smallsetminus W' \) span 2-dimensional anisotropic subspaces of \( U \) and \( W \), respectively. Then, by the case \( \dim U = \dim W = 2 \), there exist \( \alpha_1, \alpha_2, \beta_1, \beta_2 \in k \) such that the space

\[
U' \oplus W' \oplus \text{Span}_k \{\alpha_1 u_2 m - 1 + \beta_1 w_1 m - 1 + u_2 m, \alpha_2 u_2 m - 1 + \beta_2 w_2 m - 1 + w_2 m\}
\]

is \((m - 1) + (r - 1) + 2 = \frac{1}{2} \dim(U \oplus W)\) dimensional and consists of isotropic vectors. Thus \( \delta_{U \oplus W} = 1 = \delta_U \cdot \delta_W \).

We are now ready to complete the proof of the first and second assertions of Theorem 4.1.3.

**Proposition 4.4.7.** Let \( x \in \mathfrak{gl}_N \) have minimal polynomial \( m_x \). Assume \( m_x(-t) = (-1)^{\deg m_x} m_x(t) \) and let

\[
m_x(t) = t^{d_1} \prod_{i=1}^{d_2} \varphi_i^{d_i} \prod_{i=1}^{d_3} \theta_i^{r_i}
\]

a decomposition as in (4.8), with \( \varphi_i(t) \) even and irreducible, and \( \theta_i(t) = \tau_i(t) \tau_i(-t) \) with \( \tau_i(t) \) monic, irreducible and coprime to \( \tau_i(t) \).

1. If \( d_1 > 0 \) then \( x \) is similar to a regular element of \( \mathfrak{g}_1^+ \) if and only if \( \deg m_x = N - 1 \). Moreover, in this case \( x \) is similar to an element of \( \mathfrak{g}_1^+ \) as well as to an element of \( \mathfrak{g}_1^- \).

2. Otherwise, if \( d_1 = 0 \) then \( x \) is similar to a regular element of \( \mathfrak{g}_1^± \) if and only if \( \deg m_x = N \).

   In this case, put \( \omega(m_x) = \sum_{i=1}^{d_3} l_i \).

   (a) If \( \omega(m_x) \) is even, then \( x \) is similar to an element of \( \mathfrak{g}_1^+ \) and not to an element of \( \mathfrak{g}_1^- \).

   (b) Otherwise, if \( \omega(m_x) \) is odd, then \( x \) is similar to an element of \( \mathfrak{g}_1^- \) and not to an element of \( \mathfrak{g}_1^+ \).

Proof. Considering the primary canonical form of \( x \), the space \( V \) decomposes as a \( k[x] \)-invariant direct sum \( V = W_{\varphi_i} \oplus \bigoplus_{i=1}^{d_2} W_{\varphi_i} \oplus \bigoplus_{i=1}^{d_3} W_{\theta_i^{r_i}} \), where the restriction of \( x \) to the spaces \( W_f \) has minimal polynomial \( f(t) \), with \( f \in \{t^{d_1}, \varphi_i^{d_i}, \theta_i^{r_i}\} \).

For any \( f(t) \not\equiv t^{d_1} \), the restriction of \( x \) to \( W_f \) is a regular element of \( \mathfrak{gl}(W_f) \). By Lemma 4.2.1, the space \( W_f \) is endowed with a non-degenerate symmetric bilinear form on which \( x |_{W_f} \) acts as an anti-symmetric operator. Furthermore, by Lemma 4.4.4, in the case where \( f = \theta_i^{r_i} \) for \( i = 1, \ldots, d_3 \) or \( f = \varphi_i^{d_i} \) with \( l_i \) even, then \( \delta_{W_f} = +1 \). Otherwise, if \( f = \varphi_i^{d_i} \) with \( l_i \) odd, \( \delta_{W_f} = -1 \). Assertion (2), in which \( d_1 = 0 \) is assumed, now follows from Lemma 4.4.6.

In the case where \( d_1 > 0 \), the assumption \( \deg m_x = N - 1 \) implies that \( t \cdot m_x(t) = c_x \), where \( c_x(t) \) is the characteristic polynomial of \( x \). It follows that the restriction of \( x \) to \( W_{\varphi_i} \) has minimal polynomial \( t^{d-1} \), and hence, by Lemma 4.4.2, is antisymmetric with respect to non-degenerate
symmetric forms of Witt index $\frac{d^2}{2}$ as well as $\frac{d^2}{2} - 1$. Thus $\delta W_{\pm}$ can be taken to be either $+1$ or $-1$. By the case where $x$ is non-singular, and by Lemma 4.4.6, $x$ is similar to an element of $g_1^+$ as well as to an element of $g_1$.

4.4.2. From Similarity classes to adjoint orbits

Our next goal, once the similarity classes containing regular elements of $g_1^+$ have been classified, is to describe the set $\Pi_x = \text{Ad}(\text{GL}_N(k)) x \cap g_1^+$ into $\text{Ad}(G_1^+)$-orbits, for $\epsilon \in \{\pm 1\}$ fixed. In order to complete the description, we require the following lemma, whose proof is appears after Proposition 4.4.9.

Lemma 4.4.8. Assume $|k| > 3$ and $\text{char}(k) \neq 2$. For any element $\gamma \in k^\times$ there exist $\nu, \delta \in k^\times$ such that $\nu \in (k^\times)^2$, $\delta \in k^\times \setminus (k^\times)^2$ and such that $\gamma = \nu - \delta$.

Proposition 4.4.9. Assume $|k| > 3$. Fix $\epsilon \in \{\pm 1\}$ and let $x \in g_1^+$ be regular. If $x$ is singular, then the intersection $\text{Ad}(\text{GL}_N(k)) x \cap g_1^+$ is the disjoint union of two distinct $\text{Ad}(G_1^+)$-orbits. Otherwise, $\text{Ad}(\text{GL}_N(k)) x \cap g_1^+ = \text{Ad}(G_1^+) x$.

Proof. In the notation of Proposition 4.2.2, let $\Pi_x = \text{Ad}(\text{GL}_N(k)) x \cap g_1$ and $\Theta_x$ the set of equivalence classes in $\text{Sym}(\mathbb{*}; x) = \{ Q \in C_{\text{GL}_N(k)}(x) \mid Q^* = Q \}$ under the equivalence relation $\sim$, defined in (4.4). Let $\Lambda : \Pi_x \rightarrow \Theta_x$ be the map $wxw^{-1} \mapsto [w^*w] \in \Theta_x$, for $y = wxw^{-1} \in \Pi_x$.

In the case where $x$ is non-singular, by applying the argument of Proposition 4.3.6 for non-singular elements verbatim, we have that $\Theta_x$ consists of a single element and therefore that $\Pi_x = \text{Ad}(G_1^+) x$.

Furthermore, in the case where $x$ is singular, by considering the decomposition of $x$ into primary rational canonical forms, one may restrict $x$ to a maximal subspace of $k^N$ on which $x$ acts as a regular nilpotent element. This subspace is even-dimensional and admits an orthogonal complement, on which $x$ acts as a non-singular regular element. Additionally, any operator commuting with $x$ must preserve this subspace as well as its orthogonal complement. It follows that to prove the proposition in the case where $x$ is singular it is sufficient to consider the case where $x$ is a nilpotent regular element of $g_1^+$.

In this case, by the uniqueness of a nilpotent regular element in $g(\text{alg})$ [25, III, Theorem 1.8], we may invoke Lemma 4.4.2 and fix a basis $\mathcal{C}$, with respect to which $x$ is represented by the matrix $\Upsilon$, defined in (4.12), and that the ambient non-degenerate symmetric bilinear form is represented in $\mathcal{C}$ by the matrix $d = d_\eta$ of (4.13), where $\eta \in k^\times$ is a square if $\epsilon = 1$ and non-square otherwise.

The centralizer $\mathcal{C}$ of $\Upsilon$ in $M_N(k)$ is isomorphic to the ring of $k[x]$-endomorphisms of $k[x] \times k$, and can be realized as the set of matrices $\Xi(A, v, u, r)$ (see Notation 4.4.3) with $v$ and $u$ elements of the kernel of $\Upsilon$ and $\Upsilon^t$ respectively, $A \in M_{N-1}(k)$ is an upper triangular Töplitz matrix, and $r \in k$. Note that the ideal generated by elements of the form $\Xi(0_{N-1}, v, u, 0) \in \mathcal{C}$ is nilpotent and in particular is contained in the nilpotent radical $N$ of $\mathcal{C}$. It follows that the quotient ring $\mathcal{C}/N$ is isomorphic to the étale algebra $k \times k$. Additionally, by Lemma 4.2.3, we have that $\Xi(A, v, u, r) \sim \Xi(A', v', u', r')$ if and only if there exists a block matrix $\Xi(q, 0, 0, s)$ such that

$$(q \quad v) (A \quad v) (q \quad s) \equiv (A' \quad v') (u'' \quad r') \pmod{N}.$$  

Applying a similar argument as in the nilpotent case of Proposition 4.3.6, we have that the involution $*$ restricts to the identity map on $\mathcal{C}/N$ and hence that the quotient $\Theta_x$ of $\text{Sym}(\mathbb{*}; x)$ by the
relation \(\sim\), defined in Section 4.2.2, is isomorphic to the quotient group \(k^\times/(k^\times)^2 \times k^\times/(k^\times)^2\) and is of order 4.

The final step of the proof is to compute the image of the map \(\Lambda\). Recall that \(\Lambda\) maps an element \(wxw^{-1} \in \Pi_x = \text{Ad}(GL_N(k))x \cap g_1^k\) to the equivalence class of \(w^*w\) in \(\Theta_x\). As in the odd orthogonal case, two elements which are equivalent with respect to \(\sim\) must have determinant in the same coset of \(k^\times/(k^\times)^2\). In particular, as \(w^*w\) has square determinant, the image of \(\Lambda\) in \(\Theta_x\) is contained in the subset of equivalence classes in \(\Theta_x\), containing block matrices \(\Xi(A, 0, 0, r)\) with \(\det A \equiv r \pmod{(k^\times)^2}\).

To complete the proof that \(|\text{Im}(\Lambda)| = 2\) it suffices to find an element \(w \in GL_N(k)\) such that \(wxw^{-1} \in g_1\) and such that \(w^*w\) is a block matrix of the form \(\Xi(A, 0, 0, r)\) with \(\det A, r \notin (k^\times)^2\).

Let \(\eta \in k^\times\) be as above put \(\alpha = (-1)^{(N-2)/2}\). Let \(\nu \in (k^\times)^2\) and \(\delta \in k^\times \setminus (k^\times)^2\) be such that \(\alpha \eta = \nu - \delta\); see Lemma 4.4.8. Let \(\nu_1 \in k^\times\) be such that \(\nu_1^2 = \nu\), and put \(z = \eta \cdot \nu_1^{-1}\). Let \(w \in GL_N(k)\) be represented in \(E\) by the matrix \(w\) of (4.15), in which the upper-left scalar block with \(\delta\) on the diagonal is \((N-2)/2 \times (N-2)/2\).

Recalling that \(w^*\) is represented by the matrix \(d^{-1}w^t d\), one verifies by direct computation that \(w^*w\) is given by the diagonal matrix \(\Xi(\delta 1_{N-1}, 0, 0, \nu^{-2} \delta)\), and consequently, that \(w^*w \in \text{Sym}(\nu ; x)\) and \(wxw^{-1} \in g_1^k\), and that \(w^*w\) is not equivalent to \(1_N\) under the relation \(\sim\).

\[
\begin{bmatrix}
\delta \\
\vdots \\
\delta \\
1 \\
\vdots \\
1
\end{bmatrix}
\]

(4.15)

**Proof of Lemma 4.4.8.** Let \(\xi \in k^\times\) be a non-square, and let \(K = k[t^2 - \xi]\) be the splitting field of \(t^2 - \xi\), with \(\xi_1 \in K^\times\) a square root of \(\xi\). The norm map \(\text{Nr}_{K/k} : K^\times \to k^\times\) is surjective and has fibers of order \(q + 1\). In particular, there exist \(\nu_1, \delta_1 \in k\) such that

\[\text{Nr}_{K/k}(\nu_1 + \xi_1 \delta_1) = \nu_1^2 - \xi \delta_1^2 = \gamma.\]

We claim that \(\nu_1\) and \(\delta_1\) can be taken to be both non-zero.

**Case 1.** \(\gamma \in k^\times \setminus (k^\times)^2\). Note that in this case we must have that \(\delta_1 \neq 0\), as otherwise \(\gamma = \nu_1^2 \in (k^\times)^2\). Furthermore, if \(\nu_1 = 0\) for any pair \((\nu_1, \delta_1)\) such that \(\nu_1^2 - \xi \delta_1^2 = \gamma\) then \(\text{Nr}_{K/k}^{-1}(\gamma) \subseteq \xi_1 k^\times\), and in particular has order smaller than \(q\). A contradiction.

**Case 2.** \(\gamma \in (k^\times)^2\). Consider the set \(\text{Nr}_{K/k}^{-1}(\gamma) \setminus k^\times\). Note that, as \(|\text{Nr}_{K/k}^{-1}(\gamma) \cap k^\times| = 2\) (namely, it consists of the two roots of \(\gamma\) in \(k\)), the order of \(\text{Nr}_{K/k}^{-1}(\gamma) \setminus k^\times\) is exactly \(q - 1\). Assume towards a contradiction that there is no solution \((\nu_1, \delta_1) \in k^\times \times k^\times\) for the equation

\[\nu_1^2 - \xi \delta_1^2 = \text{Nr}_{K/k}(\nu_1 - \xi_1 \delta_1) = \gamma.\]
This implies that any solution not in \( k^x \times \{0\} \) is an element of \( \{0\} \times k^x \), or in other words, that \( \text{Nr}_{\text{K}(k)}(\gamma) \setminus k^x \subseteq \xi_1 k^x \). By considering the cardinality of the two sets, we deduce that this inclusion is in fact an equality. In particular, this implies that for any \( \delta_1 \in k^x \),

\[
\text{Nr}_{\text{K}(k)}(\xi_1 \delta_1) = -\xi \delta_1^2 = \gamma.
\]

Thus, the set of squares in \( k^x \) equals the singleton set \( \{-\xi^{-1} \gamma\} \). This contradicts the assumption \( |k| > 3 \).

The lemma follows by taking \( \nu = \nu_1^2 \) and \( \delta = \xi \delta_1^2 \).

\[\square\]

### 4.4.3. Centralizers of regular elements

**Lemma 4.4.10.** Let \( \epsilon \in \{\pm 1\} \). Let \( x \in \mathfrak{g}_1 \) be regular, with minimal polynomial

\[
m_x(t) = t^{d_1} \prod_{i=1}^{d_2} \phi{i}^{d_i} \prod_{i=1}^{d_3} \theta_i^{r_i},
\]

a decomposition as in (4.8), with \( \theta_i = \tau_i(t)\tau_i(-t) \) and \( \tau_i(t) \) irreducible and coprime to \( \tau_i(-t) \).

1. If \( d_1 > 0 \), then there exists a short exact sequence

\[
1 \to \text{C}_G(x) \to A^\epsilon \times \prod_{i=1}^{d_2} U_1(k(\phi_i^{l_i})) \times \prod_{i=1}^{d_3} \text{GL}_1(k(\tau_i^{r_i})) \to \{\pm 1\} \to 1.
\]

where

\[
A^\epsilon = \left\{ w \in \text{C}_{\text{GL}_{d_1+1}(k)}(\mathfrak{g}) \mid w^d = d\right\},
\]

with \( \mathfrak{g} \) and \( d\) the \((d_1 + 1) \times (d_1 + 1)\) matrices defined as in (4.12) and (4.13).

2. Otherwise, the group \( \text{C}_G(x) \) is isomorphic to \( \prod_{i=1}^{d_2} U_1(k(\phi_i^{l_i})) \times \prod_{i=1}^{d_3} \text{GL}_1(k(\tau_i^{r_i})) \).

**Proof.** Similarly to Lemma 4.3.7, in order to prove the lemma, it is sufficient to compute the possible determinants of the middle term of (4.16). For the first assertion it is sufficient to verify that both \( +1 \) and \( -1 \) are obtained as determinant of elements from \( A^\epsilon \), for which it is enough to consider block diagonal matrices of the form \( \begin{pmatrix} 1 & 0 \\ 0 & \pm 1 \end{pmatrix} \) in \( A^\epsilon \).

For the second assertion, we need to verify that any element \( w \in \text{C}_{\text{GL}_N(k)}(x) \) such that \( w^* w = 1 \) has determinant 1. Since any element of \( \text{C}_{\text{GL}_N(k)}(x) \) preserves the invariant factors of the decomposition of \( V \) as a \( k[x] \)-module, it is sufficient to consider the following cases of the minimal polynomial of \( x \).

**Case 1.** Assume \( m_x(t) = \phi_i(t)^m \), with \( \phi_i \in k[t] \) irreducible and even and \( m \in \mathbb{N} \). Let \( x = s + h \) be the Jordan decomposition of \( x \), with \( s, h \in \mathfrak{g}_1 \), \( s \) semisimple, \( h \) nilpotent and \( [s, h] = 0 \). As \( m_x(0) \neq 0 \), by Proposition 4.4.9.(2), the space \( V \) is cyclic as a \( k[x] \)-module and hence \( \text{C}_{M_N(k)}(x) \simeq k[x] \simeq k[\phi_i]/(u^m) \) (see Lemma 4.3.8). Let \( \rho : k(\phi_i)[u]/(u^m) \to \text{C}_{M_N(k)}(x) \) be a \( k \)-linear isomorphism. The \( k \)-linearity of \( \rho \) and the nilpotency of \( u \) imply that

\[
\det(\rho(a_0 + a_1 u + \ldots + a_{m-1} u^{m-1})) = \text{Nr}_{k(\phi_i)/k}(a_0) = \text{Nr}_{k(\phi_i)/k}(a_0)^m.
\]

41
Furthermore, the restriction of the involution $\star$ to the image of $\rho$ induces a $k$-automorphism $\sigma_{\varphi^m}$ of $k\langle \varphi^m \rangle$ which acts on $k\langle \varphi_i \rangle$ as the involution $\sigma_{\varphi_i}$ and maps $u$ to $-u$. Consequently, if $z \in C_{GL_k(k)}(x)$ is given by $z = \rho(\alpha_0 + \alpha_1 u + \ldots + \alpha_{m-1} u^{m-1})$ and satisfies $z^* z = 1$ then necessarily $N_{r_k(k)}/k(\alpha_0) = \sigma_{\varphi_i}(\alpha_0) \alpha_0 = \rho^{-1}(z^* z) |_{u=0} = 1$ and
\[
\det(z) = \det(\rho(\alpha_0 + \alpha_1 u + \ldots + \alpha_{m-1} u^{m-1})) \\
= N_{r_k(k)}/k(\alpha_0)^m = (N_{r_k/k} \circ N_{r_k(k)}/k(\alpha_0))^m = 1.
\]

**Case 2.** Assume $m_x(t) = (\tau_t(t) \cdot \tau_t(-t))^r$, for $\tau_t(t)$ irreducible and coprime to $\tau(-t)$. In this case, by the cyclicity of the $k[x]$ module $V$, we have that $C_{ GL_k(k)}(x) \cong GL_1(k(\tau(t)^r)) \times GL_1(k(\tau(-t)^r))$. Moreover, the map $\star$ restricts to the map $(\xi, \nu) \mapsto (\nu^{-1}(\xi), \nu)$, where $\nu : k(\tau(t)^r) \rightarrow k(\tau(-t)^r)$ is the isomorphism induced from $t \mapsto -t$. Furthermore, since $\nu$ is a ring-isomorphism which preserves $k$, we have that $\det(\nu(\xi)) = \det(\xi)$ for all $\xi \in k(\tau(t)^r)$. In particular, if $(\xi, \nu)(\xi, \nu) = 1$ then $\nu = \nu^{-1}$ and hence, $\det((\xi, \nu)) = \det(\xi) \cdot \det(\nu) = 1.$

\[\square\]

**Proposition 4.4.11.** Let $x \in g_1^+$ be regular with minimal polynomial $m_x(t)$. Let $c_x$ denote the characteristic polynomial of $x$, i.e. $c_x = m_x$ if $x$ is non-singular, and $c_x(t) = t \cdot m_x(t)$ otherwise. Let $\tau(c_x) = (r(c_x), S(c_x), T(c_x)) \in X_n$ be the type of $c_x$ (see Definition 4.1.1). Then
\[
|C_{G_1}(x)| = 2q^n \prod_{d,e} (1 + q^{-d})^{S_{d,e}} \cdot (1 - q^{-d})^{T_{d,e}}.
\]
where $\epsilon \in \{\pm\}$ and $\nu = 1$ if $r(m_x) > 0$ and 0 otherwise.

**Proof.** In the case where $x$ is non-singular the assertion follows verbatim as in Proposition 4.3.9. Otherwise, if $x$ is singular, by decomposing $x$ into its primary rational canonical forms, it is sufficient to consider the case where $x$ is a regular nilpotent element, with minimal polynomial $m_x(t) = t^{2n-1}$, and show that $|C_{G_1}(x)| = 2q^n$.

Without loss of generality, we fix the basis $E$ of Lemma 4.4.2, with respect to which the ambient symmetric form $B^*$ is represented by the matrix $d = d_{\eta}$, for some $\eta \in k^\times$, and $x$ is represented by the matrix $Y$. Let $A^* = \{ z \in C_{GL_k(k)}(Y) \mid z^* dz = d \}$, as in Lemma 4.4.10. Let $N \subseteq A^*$ be the subgroup consisting of elements of the form
\[
\mathfrak{X}(\xi) = \begin{pmatrix}
1 & 2\eta \xi^2 & 2\xi \\
1 & \ddots & \\
1 & & 1
\end{pmatrix} \quad (\xi \in k).
\]

Note that $\mathfrak{X}$ defines a one-parameter subgroup of $A^*$ of order $|k| = q$. Additionally, $N = \text{Im}(\mathfrak{X})$ is the image under the Cayley map of the Lie-ideal generated by elements of the form $\Xi(0_{N-1}, u, v, 0) \in g_1$, and hence is normal in $A^*$.

Let $H^* \subseteq A^*$ be the subgroup of block diagonal matrices $\Xi(A, 0, 0, r)$. Note that, by (4.14) and the assumption $\Xi(A, 0, 0, r)^* \Xi(A, 0, 0, r) = 1_N$, we have that $A^* A = 1_{N-1}$ and $r^2 = 1$. Additionally, since $A$ commutes with the restriction of $Y$ to the subspace spanned by the first $N - 1$ elements
of $\mathcal{E}$, we have that $|\mathcal{E}| = \left| U_1(k(t^{2n-1})) \times \{\pm 1\} \right| = 4q^{n-1}$ (by the first assertion in the proof of Proposition 4.3.9).

Given an arbitrary element $\Xi(A, v, u, r) \in \mathcal{A}^\epsilon$, it holds that $A$ must be invertible, and that $v = \gamma du$ for some $\gamma \in k$. In particular, $v = 0$ if and only if $u = 0$. It follows from this, and by direct computation, that

$$\xi \left( -\frac{v_1}{a_{1,1} \eta} \right) \begin{pmatrix} A & v \\ u & r \end{pmatrix} \in \mathcal{H},$$

where $v_1$ is the first entry of $v$, and $a_{1,1}$ is the $(1,1)$-th entry of $A$. Therefore, we have that $\mathcal{A}^\epsilon = \mathcal{H} \cdot N$ and hence, as $\mathcal{H} \cap N = \{1\}$, that

$$|\mathcal{A}^\epsilon / N| = |\mathcal{H}| = 4q^{n-1}.$$

To conclude, we have that $|\mathcal{A}^\epsilon| = 4q^n$, and the result follows from Lemma 4.4.10.

The final assertion of Theorem 4.1.3 follows from Proposition 4.4.11.

**Acknowledgements**

This paper is part of the author’s doctoral thesis. I wish to thank Uri Onn for guiding and advising this research. I also wish to thank Alexander Stasinski for carefully reading through a preliminary version of this article and offering some essential remarks.

The present research was supported by the Israel Science Foundation (ISF) grant 1862.

**References**

[1] Artin, M., Bertin, J.-E., Demazure, M., Grothendieck, A., Gabriel, P., Raynaud, M., and Serre, J.-P. Schémas en groupes (SGA 3). Séminaire de Géométrie Algébrique de l’Institut des Hautes Études Scientifiques. Institut des Hautes Études Scientifiques, Paris, 1963/1966.

[2] Avni, N., Klopsch, B., Onn, U., and Voll, C. Similarity classes of integral $p$-adic matrices and representation zeta functions of groups of type $A_2$. *Proceedings of the London Mathematical Society* 112, 2 (2016), 267.

[3] Bialynicki Birula, A., Carrell, J. B., and McGovern, W. M. Algebraic quotients. Torus actions and cohomology. The adjoint representation and the adjoint action, vol. 131 of *Encyclopaedia of Mathematical Sciences*. Springer-Verlag, Berlin, 2002. Invariant Theory and Algebraic Transformation Groups, II.

[4] Borel, A. *Linear Algebraic Groups*. Graduate Texts in Mathematics. Springer New York, 1991.

[5] Bosch, S., Lütkebohmert, W., and Raynaud, M. Néron models, vol. 21 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1990.

[6] Bourbaki, N. *Éléments de mathématique. Fasc. XXVI. Groupes et algèbres de Lie. Chapitre I: Algèbres de Lie*. Seconde édition. Actualités Scientifiques et Industrielles, No. 1285. Hermann, Paris, 1971.
[7] Bushnell, C., and Fröhlich, A. *Gauss sums and p-adic division algebras*. Lecture notes in mathematics. Springer, 1983.

[8] Cayley, A. Sur quelques propriétés des déterminants gauches. *J. Reine Angew. Math.* 32 (1846), 119–123.

[9] Demazure, M., and Gabriel, P. *Introduction to algebraic geometry and algebraic groups*, vol. 39 of *North-Holland Mathematics Studies*. North-Holland Publishing Co., Amsterdam-New York, 1980. Translated from the French by J. Bell.

[10] Dieudonné, J., and Grothendieck, A. Éléments de géométrie algébrique. *Inst. Hautes Études Sci. Publ. Math.* 4, 8, 11, 17, 20, 24, 28, 32 (1961–1967).

[11] Dummit, D. S., and Foote, R. M. *Abstract Algebra - 3rd Edition*, 3 ed. John Wiley and Sons, Inc., 2004.

[12] Greenberg, M. J. Schemata over local rings. *Annals of Mathematics* 73, 3 (1961), 624–648.

[13] Greenberg, M. J. Schemata over local rings: II. *Annals of Mathematics* 78, 2 (1963), 256–266.

[14] Hill, G. Regular elements and regular characters of GL$_n$(O). *Journal of Algebra* 174 (1995), 610–635.

[15] Humphreys, J. E. *Introduction to Lie algebras and representation theory*, vol. 9 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1978. Second printing, revised.

[16] Isaacs, I. M. *Character theory of finite groups*. AMS Chelsea Publishing, Providence, RI, 2006. Corrected reprint of the 1976 original [Academic Press, New York; MR0460423].

[17] Krakovski, R., Onn, U., and Singla, P. Regular characters of groups of type An over discrete valuation rings. *J. Algebra* 496 (2018), 116–137.

[18] Lahtonen, J. Number of even irreducible monic polynomials of a given degree over a finite field. Mathematics Stack Exchange http://math.stackexchange.com/q/1833813.

[19] Lang, S. Algebraic groups over finite fields. *Amer. J. Math.* 78 (1956), 555–563.

[20] Lemire, N., Popov, V. L., and Reichstein, Z. Cayley groups. *J. Amer. Math. Soc.* 19, 4 (2006), 921–967.

[21] McNinch, G. J. The centralizer of a nilpotent section. *Nagoya Math. J.* 190 (2008), 129–181.

[22] Serre, J. *Local Fields*. Graduate Texts in Mathematics. Springer New York, 1995.

[23] Shechter, S. Characters of the norm-one units of local division algebras of prime degree. *J. Algebra* 474 (2017), 134–165.

[24] Shintani, T. On certain square integrable irreducible unitary representations of some p-adic linear groups. *Proceedings of the Japan Academy, Series A, Mathematical Sciences* 44, 1 (1968), 1–3.
[25] SPRINGER, T., AND STEINBERG, R. Conjugacy classes. In Seminar on Algebraic Groups and Related Finite Groups, vol. 131 of Lecture Notes in Mathematics. Springer Berlin Heidelberg, 1970, pp. 167–266.

[26] STASINSKI, A. Reductive group schemes, the Greenberg functor, and associated algebraic groups. Journal of Pure and Applied Algebra 216, 5 (2012), 1092 – 1101.

[27] STASINSKI, A. Representations of GL_N over finite local principal ideal rings - an overview. In Around Langlands Correspondences, vol. 691 of Contemp. math. American Mathematical Society, January 2017, pp. 336–358.

[28] STASINSKI, A., AND STEVENS, S. The regular representations of GL_N over finite local principal ideal rings, 2016.

[29] STEINBERG, R. Conjugacy classes in algebraic groups. Lecture notes in mathematics. Springer, 1974.

[30] TAKASE, K. Regular characters of GL_n(O) and Weil representations over finite fields. J. Algebra 449 (2016), 184–213.

[31] TAKASE, K. Regular irreducible characters of a hyperspecial compact group. ArXiv e-prints (Jan. 2017).

[32] WALL, G. E. On the conjugacy classes in the unitary, symplectic and orthogonal groups. Journal of the Australian Mathematical Society 3 (2 1963), 1–62.

[33] WATERHOUSE, W. C. Introduction to Affine Group Schemes. Graduate Texts in Mathematic. Springer, New York, Heidelberg, Berlin, 1979.

[34] WEIL, A. Algebras with involutions and the classical groups. J. Indian Math. Soc. 24 (1960), 589–623.

[35] WILSON, R. The Finite Simple Groups. Graduate Texts in Mathematics. Springer London, 2009.
A. Appendix: The number of monic irreducible even polynomials of a given degree over $\mathbb{F}_q$

Assume $p \neq 2$ is prime and $q = p^\alpha$, for $\alpha \in \mathbb{N}$. As above, we put $k = \mathbb{F}_q$. We wish to enumerate the number of monic irreducible polynomials $f \in k[t]$ of a given degree $2m$, which satisfy the condition $f(-t) = f(t)$.

We call an element $x \in k^{\text{alg}}$ even over $k$ if its minimal polynomial over $k$ is even. The set of even irreducible polynomials of degree $2m$ is naturally in bijection with the set of Galois orbits of non-zero even elements $x \in k^{\text{alg}}$ such that $(k(x) : k)$ is an extension of degree $2m$, and any such orbit has cardinality $2m$. In view of this, in the sequel we will enumerate the number of such elements $x \in k^{\text{alg}}$.

We begin with a criterion for an element of $x$ to be even.

**Lemma A.0.1.** Let $0 \neq x \in k^{\text{alg}}$ have minimal polynomial $f(t)$ over $k$. Then $f$ is even if and only if there exists $m \in \mathbb{N}$ such that $f(t)$ divides $t^{q^m} + t$.

**Proof.** Assume $f$ is even. Then $f(-x) = f(x) = 0$ and hence $x$ and $-x$ are Galois conjugates over $k$. In particular, by the theory of finite fields, this implies that $-x = x^{q^m}$ for some $m \in \mathbb{N}$. Thus $x$ is a root of $t^{q^m} + t$, and hence, since $f$ is its minimal polynomial, $f(t)$ divides $t^{q^m} + t$.

$\Leftarrow$ Let $\sigma \in \text{Gal}(k^{\text{alg}} \mid k)$ be the map $\sigma(y) = y^{q^m}$. Then, by the assumption $f(t) \mid t^{q^m} + t$, we have that $\sigma(x) = x^{q^m} = -x$.

Define a polynomial $g(t) = \frac{1}{2}(f(t) - f(-t))$. Then $g(t)$ is a monic odd polynomial (i.e. $g(-t) = -g(t)$) of degree smaller or equal to $\deg(f)$. Additionally

$$g(x) = \frac{1}{2}(f(x) - f(-x)) = \frac{1}{2}(f(x) - \sigma(x)) = 0,$$

as the coefficients of $f$ are fixed under $\sigma$. This implies that either $g = 0$ or $g = f$. But $g = f$ is impossible, since the condition $g(-t) = -g(t)$ implies that $g(0) = f(0) = 0$, and in particular $f$ is not irreducible. Thus $g = 0$ and $f(t) = f(-t)$. \hfill $\square$

We now wish to classify those even elements $x \in k^{\text{alg}}$ which generate a degree $2d$ extension of $k$. We first note the following.

**Lemma A.0.2.** Let $m \in \mathbb{N}$, and let $0 \neq x \in k^{\text{alg}}$ be a root of $t^{q^m} + t$. Then $|k(x) : k| = 2d$ for some $d \in \mathbb{N}$ such that $d \mid m$ and $\frac{m}{d}$ is an odd integer. Furthermore, in this case we have that $x^{q^d} + x = 0$.

**Proof.** By Lemma A.0.1, the assumption that $x^{q^m} + x = 0$ implies that $x$ is even and hence has an even minimal polynomial $f$, say of degree $2d$. Hence $|k(x) : k| = 2d$. Also, note that

$$x^{q^m} = \left(x^{q^d}\right)^{q^m} = x$$

and so $k(x)$ is fixed under the map $y \mapsto y^{q^m}$, whence a subfield of $\mathbb{F}_{q^{2m}}$. This gives us that $d \mid m$. Additionally, since $f(x) = f(-x) = 0$, there exists an element $\sigma \in \text{Gal}(k(x) \mid k)$ such that $\sigma(x) = -x$. In particular, $\sigma^2(x) = x$ and hence $\sigma$ is an involution of $k(x)$. As the Galois group
Gal(k(x) | k) is cyclic of order 2d and generated by the Frobenius map \( F(y) = y^q \) (\( y \in k(x) \)), it follows that \( \sigma(y) = F^d(y) = y^{q^d} \) for all \( y \in k(x) \) and hence
\[
x^{q^d} = \sigma(x) = -x.
\]
Lastly, we show that \( r = \frac{m}{d} \) is odd. This follows since
\[
-x = x^{q^m} = F^m(x) = (F^d)^r(x) = (-1)^r x,
\]
and hence \( r \) is odd.

Note that the converse of Lemma A.0.2 is true as well. Namely, if \( d \mid m \) and \( r = \frac{m}{d} \) is an odd integer then any non-zero \( x \in k_{\text{alg}} \) which satisfies \( x^{q^d} + x = F^d(x) + x = 0 \) also satisfies
\[
x^{q^m} + x = (F^d)^r(x) + x = (-1)^r x + x = 0.
\]
Thus, we obtain the following.

**Corollary A.0.3.** For any \( m \in \mathbb{N} \) let \( S_m \) denote the set of non-zero roots of the polynomial \( t^{q^m} + t \). Then

1. \( S_d \subseteq S_m \) if and only if \( d \mid m \) and \( \frac{m}{d} \) is an odd integer.
2. The set non-zero even elements \( x \in k_{\text{alg}} \) which generate an extension of \( k \) of degree \( 2m \) is
\[
S_m \setminus \bigcup_{d \mid m, \frac{m}{d} \text{ is odd}} S_d.
\]

As the set \( S_m \) has cardinality \( q^m - 1 \) (since the field \( k \) is perfect and the roots of \( t^{q^m} + t \) are all simple), by exclusion-inclusion we deduce that the non-zero even elements of \( k_{\text{alg}} \) which generate a degree \( 2m \) extension of \( k \) is
\[
\sum_{d \mid m, \frac{m}{d} \text{ is odd}} \mu\left(\frac{m}{d}\right) (q^d - 1),
\]
where \( \mu \) is the Möbius function.