Journal of Pure and Applied Algebra 223 (2019) 4384–4425

Contents lists available at ScienceDirect

Journal of Pure and Applied Algebra

www.elsevier.com/locate/jpaa

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

ARTICLE INFO

Article history:
Received 13 September 2017
Received in revised form 21 November 2018
Available online 22 January 2019
Communicated by D. Nakano

MSC:
20C15; 20G05; 11M41

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

ABSTRACT

Let $\mathfrak{o}$ be a complete discrete valuation ring with finite residue field k of odd characteristic, and let $\mathbf{G}$ be a symplectic or special orthogonal group scheme over $\mathfrak{o}$. For any $\ell \in \mathbb{N}$ let G^ℓ denote the ℓ-th principal congruence subgroup of $\mathbf{G}(\mathfrak{o})$. An irreducible character of the group $\mathbf{G}(\mathfrak{o})$ is said to be **regular** if it is trivial on a subgroup $G^{\ell+1}$ for some ℓ, and if its restriction to $G^\ell/G^{\ell+1} \simeq \mathrm{Lie}(\mathbf{G})(\mathsf{k})$ consists of characters of minimal $\mathbf{G}(\mathsf{k}^{\mathrm{alg}})$-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 $\mathbf{G}(\mathfrak{o})$, when the characteristic of k is greater than two. As a result, we compute the regular part of their representation zeta function.

1. Introduction

Let K be a non-archimedean local field, and let $\mathfrak{o}$ be its valuation ring, with maximal ideal $\mathfrak{p}$ and finite residue field k of odd characteristic. Let q and p denote the cardinality and characteristic of k, respectively. Fix π to be a uniformizer of $\mathfrak{o}$. Let $\mathbf{G} \subseteq \mathrm{SL}_N$ 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 $G = \mathbf{G}(\mathfrak{o})$, the definition of which we now present.

1.1. The basic definitions

Let $\mathrm{Irr}(G)$ 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 $\chi \in \mathrm{Irr}(G)$ is the minimal number $\ell \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$ such that the restriction of any representation associated to χ to the principal congruence subgroup

E-mail address: shais@post.bgu.ac.il.

https://doi.org/10.1016/j.jpaa.2019.01.013
0022-4049/

$G^{\ell+1} = \mathrm{Ker}\left(G \to \mathbf{G}(\mathfrak{o}/\mathfrak{p}^{\ell+1})\right)$ is trivial. For example, the set of characters of level 0 is naturally identified with the set of irreducible complex characters of $\mathbf{G}(\mathsf{k})$.

1.1.1. The residual orbit of a character

Let $\mathbf{g} = \mathrm{Lie}(\mathbf{G}) \subseteq \mathfrak{gl}_N$ denote the Lie algebra scheme of $\mathbf{G}$. The smoothness of $\mathbf{G}$ implies the equality $G/G^{\ell+1} = \mathbf{G}(\mathfrak{o}/\mathfrak{p}^{\ell+1})$, and moreover, the existence of an isomorphism of abelian groups between $\mathbf{g}(\mathsf{k})$ and the quotient group $G^{\ell}/G^{\ell+1}$, for any $\ell \geq 1$ (see [11, II, § 4, no. 3]). In the notation of [11], this isomorphism is denoted $x \mapsto e^{\pi^{\ell} x}$. The action of G by conjugation on the quotient $G^{\ell}/G^{\ell+1}$ factors through its quotient $\mathbf{G}(\mathsf{k})$, making the isomorphism above $\mathbf{G}(\mathsf{k})$-equivariant, with respect to the action given by $\mathrm{Ad} \circ \alpha_{\ell}$, where Ad denotes the adjoint action of $\mathbf{G}(\mathsf{k})$ on $\mathbf{g}(\mathsf{k})$, and $\alpha_{\ell} : \mathbf{G}(\mathsf{k}) \to \mathbf{G}(\mathsf{k})$ is a bijective endomorphism of $\mathbf{G}(\mathsf{k})$, determined by a field automorphism of k (see, e.g. [25, Lemma 3] and the reference therein). Additionally, by the assumption $\mathrm{char}(\mathsf{k}) \neq 2$ and [32, I, Lemma 5.3], the underlying additive group of $\mathbf{g}(\mathsf{k})$ can be naturally identified with its Pontryagin dual in a $\mathbf{G}(\mathsf{k})$-equivariant manner. Consequently, there exists an isomorphism of $\mathbf{G}(\mathsf{k})$-spaces

$$\mathbf{g}(\mathsf{k}) \xrightarrow{\sim} \mathrm{Irr}\left(G^{\ell}/G^{\ell+1}\right). \tag{1.1}$$

Let $\chi \in \mathrm{Irr}(G)$ have level $\ell > 0$. Consider the restriction $\chi_{G^{\ell}}$ of χ to G^{ℓ}. 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 $\mathbf{G}(\mathsf{k})$-orbit of characters of $G^{\ell}/G^{\ell+1}$. Using (1.1), this orbit corresponds to a single $\mathbf{G}(\mathsf{k})$-orbit in $\mathbf{g}(\mathsf{k})$, which we call the **residual orbit of** χ, and denote $\Omega_1(\chi) \in \mathrm{Ad} \circ \alpha_{\ell}(\mathbf{G}(\mathsf{k}))\backslash\mathbf{g}(\mathsf{k}) = \mathrm{Ad}\left(\mathbf{G}(\mathsf{k})\right)\backslash\mathbf{g}(\mathsf{k})$.

1.1.2. Regular characters

Let $\mathsf{k}^{\mathrm{alg}}$ be a fixed algebraic closure of k. An element of $\mathbf{g}(\mathsf{k}^{\mathrm{alg}})$ is said to be **regular** if its centralizer in $\mathbf{G}(\mathsf{k}^{\mathrm{alg}})$ has minimal dimension among such centralizers (cf. [36, § 3.5]). By extension, an element of $\mathbf{g}(\mathsf{k})$ is said to be regular if its image under the natural inclusion of $\mathbf{g}(\mathsf{k})$ into $\mathbf{g}(\mathsf{k}^{\mathrm{alg}})$ is regular.

Definition 1.1.1 *(Regular Characters).* A character $\chi \in \mathrm{Irr}(G)$ of positive level is said to be **regular** if its residual orbit $\Omega_1(\chi)$ consists of regular elements of $\mathbf{g}(\mathsf{k})$.

For a general overview of regular elements in reductive algebraic groups over algebraically closed fields, we refer to [32, Ch. III]. The definition of regular characters goes back to Shintani [31] and Hill [18]. An overview of the history of regular characters of $\mathrm{GL}_N(\mathfrak{o})$ can be found in [34]. Also- see [22,35] and [37] for the analysis of regular characters of isotropic groups of type A_n, as well as [30], for a partial treatment of anisotropic groups of type A_n.

1.2. Regular elements and regular characters

Following [18], we begin our investigation of regular characters with the study of regular elements in the finite Lie rings $\mathbf{g}(\mathfrak{o}_r)$, where $\mathfrak{o}_r = \mathfrak{o}/\mathfrak{p}^r$ (see Definition 3.1.1).

A central feature of the analysis undertaken in [18] is the introduction and application of geometric methods to the study of regular characters. Given $x \in \mathrm{M}_N(\mathfrak{o})$ and $r \in \mathbb{N}$, let x_r denote the image of x in $\mathrm{M}_N(\mathfrak{o}_r)$ under the reduction map. The condition of commuting with x_r defines a closed $\mathfrak{o}_r$-group subscheme of the fiber product[1] $\mathrm{GL}_N \times \mathfrak{o}_r$, which, upon application of the Greenberg functor, defines a k-group scheme [16, § 4, Main Theorem.(5)]. The element x_r is said to be **regular** if the group scheme thus obtained is of

[1] The notation $\mathbf{G} \times \mathfrak{o}_r$ is shorthand for the fiber product $\mathbf{G} \times_{\mathrm{Spec}\,\mathfrak{o}} \mathrm{Spec}\,\mathfrak{o}_r$. 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.

minimal dimension among such group schemes (see [18, Definition 3.2]). In [18, Theorem 3.6], Hill proved that $x_r \in \mathrm{M}_n(\mathfrak{o}_r)$ is regular if and only if its image $x_1 \in \mathrm{M}_n(\mathsf{k})$ is regular. Additionally, regularity of x_r was shown to be equivalent to the cyclicity of the module $\mathfrak{o}_r^N$ over the ring $\mathfrak{o}_r[x_r] \subseteq \mathrm{M}_N(\mathfrak{o}_r)$. We note that Hill's definition of regularity is equivalent to Shintani's definition of *quasi-regularity* [31, § 2].

The equivalence of regularity over the ring $\mathfrak{o}_r$ and over k was recently extended to general semisimple groups of type A_n in [22]. 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 $x_r \in \mathbf{g}(\mathfrak{o}_r)$ with the cyclicity of the module $\mathfrak{o}_r^N$ over $\mathfrak{o}_r[x_r]$, while true in GL_N and generically true in $\mathbf{G}$ (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 (Proposition 3.1.4), which specializes to the above equivalence in the case of $\mathbf{G} = \mathrm{GL}_N$, 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 orbit. 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 $\mathbf{G}$ be a symplectic or a special orthogonal group over $\mathfrak{o}$ with generic fiber of absolute rank n. Let $\Omega \subseteq \mathbf{g}(\mathsf{k})$ be an $\mathrm{Ad}(\mathbf{G}(\mathsf{k}))$-orbit consisting of regular elements and let $\ell \in \mathbb{N}$.*

1. *The number of regular characters $\chi \in \mathrm{Irr}(G)$ of level ℓ whose residual orbit is equal to Ω is $\frac{|\mathbf{G}(\mathsf{k})|}{|\Omega|} \cdot q^{(\ell-1)n}$.*
2. *Any such character has degree $|\Omega| \cdot q^{(\ell-1)\alpha}$, where $\alpha = \frac{\dim \mathbf{G} - n}{2}$.*

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 $\mathrm{Irr}(H)$ 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

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

In the specific case $H = G = \mathbf{G}(\mathfrak{o})$, 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 $\frac{2n}{\dim \mathbf{G} - n}$. Furthermore, we obtain the following.

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

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

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

$$\zeta_G^{\mathrm{reg}}(s) = \frac{\mathfrak{D}_{\mathbf{g}(\mathfrak{o})}(s)}{1 - q^{n - \alpha s}}$$

where n and α are as in Theorem I.

1.4. Classification of regular orbits in $\mathbf{g}(\mathsf{k})$

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 $\mathbf{g}(\mathsf{k})$, under the adjoint action of $\mathbf{G}(\mathsf{k})$. This classification is undertaken in Section 4, and its consequences are summarized in Theorem 4.1.2 and Theorem 4.1.3. The classification of regular adjoint classes in the $\mathbf{g}(\mathsf{k})$ is closely related to the question of classifying conjugacy classes in classical groups over a finite field, a question which was solved in complete generality by Wall in [39, § 2.6]. Taking a enumerative perspective, the regular semisimple conjugacy classes in finite classical groups were enumerated in [14], using generating functions. Another closely related question is that of enumerating *cyclic* conjugacy classes in finite classical groups. This question is addressed in [15,28]; see Section 4.1 for further discussion. The enumeration carried out in this paper yields uniform formulae for the function $\mathfrak{D}_{\mathbf{g}(\mathfrak{o})}$ (and, consequently, for the regular representation zeta function) of each of the classical groups in question, which are independent of the cardinality of k.

Given $n \in \mathbb{N}$ let $\mathcal{X}_n$ denote the set of triplets $\boldsymbol{\tau} = (r, S, T)$, 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 entires, satisfying the condition

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

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

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

and let $u_1(q) = |\mathrm{Sp}_{2n}(\mathsf{k})| = |\mathrm{SO}_{2n+1}(\mathsf{k})|$. 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., [42, § 3.5 and § 3.2.7]). Additionally, for any $\boldsymbol{\tau} \in \mathcal{X}_n$, let $M_{\boldsymbol{\tau}}(q)$ denote the number of polynomials of type $\boldsymbol{\tau}$ over a field of q elements; see Definition 4.1.1. An explicit formula for $M_{\boldsymbol{\tau}}(q)$ is computed in Section 4.1.1. We remark that the value of $M_{\boldsymbol{\tau}}(q)$ 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 $\mathbf{G}$ be one of the $\mathfrak{o}$-defined algebraic group schemes Sp_{2n} or SO_{2n+1}, with $\mathbf{g} = \mathrm{Lie}(\mathbf{G})$.*

Given $\boldsymbol{\tau} = (r, S, T) \in \mathcal{X}_n$ let

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

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

$$\mathfrak{D}_{\mathbf{g}(\mathfrak{o})}(s) = \sum_{\boldsymbol{\tau} \in \mathcal{X}_n} 4^{\nu(\boldsymbol{\tau})} M_{\boldsymbol{\tau}}(q) \cdot c^{\boldsymbol{\tau}}(q) \cdot \left(\frac{u_1(q)}{2^{\nu(\boldsymbol{\tau})} c^{\boldsymbol{\tau}}(q)} \right)^{-s}. \tag{1.6}$$

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 SO_{2n}^{+} and 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 $\mathrm{SO}_{2n}^{\pm 1}$ for $\mathrm{SO}_{2n}^{\pm}$.

Given $\epsilon \in \{\pm 1\}$, let $u_2^\epsilon(q) = |\mathrm{SO}_{2n}^\epsilon(\mathsf{k})|$. 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 [42, § 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 $\mathbf{G}^\epsilon = \mathrm{SO}_{2n}^\epsilon$ be the $\mathfrak{o}$-defined special orthogonal group scheme, as described above, and let $\mathbf{g}^\epsilon = \mathrm{Lie}(\mathbf{G}^\epsilon)$.*

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

The Dirichlet polynomial $\mathfrak{D}_{\mathbf{g}(\mathfrak{o})}$ (see (1.3)) is given by

$$\mathfrak{D}_{\mathbf{g}^\epsilon(\mathfrak{o})}(s) = \sum_{\boldsymbol{\tau} \in \mathcal{X}_n^{0,\epsilon}} M_{\boldsymbol{\tau}}(q) \cdot c^{\boldsymbol{\tau}}(q) \cdot \left(\frac{u_2^\epsilon(q)}{c^\tau(q)}\right)^{-s} + \sum_{\boldsymbol{\tau} \in \mathcal{X}_n \smallsetminus \mathcal{X}_n^0} 4 \cdot M_{\boldsymbol{\tau}}(q) \cdot c^{\boldsymbol{\tau}}(q) \cdot \left(\frac{u_2^\epsilon(q)}{2 \cdot c^\tau(q)}\right)^{-s}. \tag{1.7}$$

1.5. Organization

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

2. Notation, preliminaries and basic definitions

2.1. The symplectic and orthogonal groups

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

$$\mathbf{G}(R) = \left\{\mathbf{x} \in \mathrm{M}_N(R) \mid \mathbf{x}^t \mathbf{J} \mathbf{x} = \mathbf{J} \text{ and } \det(\mathbf{x}) = 1\right\}, \tag{2.1}$$

where R is a commutative $\mathfrak{o}$-algebra and the notation $\mathbf{x}^t$ stands for the transpose matrix of $\mathbf{x}$. A standard computation (see, e.g. [40, § 12.3]) shows that the Lie-algebra scheme $\mathbf{g} = \mathrm{Lie}(\mathbf{G})$ is given by

$$\mathbf{g}(R) = \left\{\mathbf{x} \in \mathrm{M}_N(R) \mid \mathbf{x}^t \mathbf{J} + \mathbf{J} \mathbf{x} = 0\right\}. \tag{2.2}$$

Let n and d denote the dimension and the absolute rank of the generic fiber of $\mathbf{G}$. Note that the absolute rank and dimension of the generic fiber of $\mathbf{G}$ are equal to those of its special fiber, by flatness of $\mathbf{G}$ 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 $\mathrm{M}_{N\times 1}(R)$ of column vectors, and define a non-degenerate bilinear form on R^N by $B_R(u, v) = u^t \mathbf{J} v$. One defines an R-anti-involution on $\mathrm{M}_N(R) = \mathrm{End}_R(R^N)$ by

$$A^\star = \mathbf{J}^{-1} A^t \mathbf{J} \quad (A \in \mathrm{M}_N(R)), \tag{2.3}$$

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

2.1.2. Maximal tori and centralizers over algebraically closed fields

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

Under this embedding, the Lie-algebra $\mathbf{t}(L)$ consists of diagonal matrices of the form $\mathrm{diag}(\nu_1, \ldots, \nu_N)$, with $\nu_{2i} = -\nu_{2i-1}$ 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 $s \in \mathbf{g}(L)$ be a semisimple element. The centralizer of s under the adjoint action of $\mathbf{G}(L)$ is of the form*

$$\mathbf{C}_{\mathbf{G}(L)}(s) \simeq \prod_{j=1}^{t} \mathrm{GL}_{m_j}(L) \times \Delta(L),$$

where Δ is the L-algebraic group of isometries of the restriction of B_L to (a non-degenerate bilinear form on) $\mathrm{Ker}(s)$, the eigenspace associated with the eigenvalue 0, and the values $m_1, \ldots, m_t$ are the algebraic multiplicities of all non-zero eigenvalues of s such that for any such eigenvalue λ, there exists a unique $j = 1, \ldots, t$ such that m_j is the algebraic multiplicity of λ and $-\lambda$.

Proof. Let $V = L^N$ be the fixed L-vector space on which $\mathbf{G}(L) \subseteq \mathrm{GL}_N(L)$ 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 $\mathbf{C}_{\mathrm{GL}_N(L)}(s)$-modules, $V = \oplus_{\lambda \in L} W_\lambda$, where $W_\lambda = \mathrm{Ker}(s - \lambda \mathbf{1})$. For any non-zero $\lambda \in L$, put $W_{[\lambda]} = W_\lambda \oplus W_{-\lambda}$. 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 $\mathbf{C}_{\mathbf{G}(L)}(s) = \mathbf{C}_{\mathrm{GL}_N(L)}(s) \cap \mathbf{G}(L)$, it holds that $x \in \mathbf{C}_{\mathbf{G}(L)}(s)$ if and only if $x \in \mathbf{C}_{\mathrm{GL}_N(L)}(s)$ 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 [4, III, § 2.4], one verifies that for any $\lambda \neq 0$ the decomposition $W_{[\lambda]} = W_\lambda \oplus W_{-\lambda}$ is into maximal isotropic subspaces, and in particular $\dim_L W_\lambda = \dim_L W_{-\lambda} = m_j$, for some $j = 1, \ldots, t$. Invoking Witt's Theorem [39, § 1.2], and the $\mathbf{C}_{\mathrm{GL}_N(L)}(s)$-isotipicity of the decomposition, we obtain that any automorphism of W_λ extends uniquely to an isometric automorphism of $W_{[\lambda]}$ which commutes with the action of s, and that the action of $\mathbf{C}_{\mathbf{G}(L)}(s)$ on $W_{[\lambda]}$ is determined in this manner. Furthermore, it holds that any automorphism of $W_0 = \mathrm{Ker}(s)$ which preserves the restriction of B to W_0 necessarily commutes with s, and that the action of $\mathbf{C}_{\mathbf{G}(L)}(s)$ on this subspace is by such automorphisms. The proposition follows. □

2.2. Artinian local principal ideal rings

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

The map η_1 admits a canonical splitting map $s : \mathsf{k}^{\mathrm{alg}} \to \mathfrak{O}$, which restricts to a homomorphic embedding of $(\mathsf{k}^{\mathrm{alg}})^\times$ into $\mathfrak{O}^\times$, and satisfies $s(0) = 0$; see [29, Ch. II, § 4, Proposition 8].

Let $\sigma : K^{\mathrm{unr}} \to K^{\mathrm{unr}}$ be the local Frobenius map whose fixed field is K. Then σ restricts to a ring automorphism of $\mathfrak{O}$, with fixed subring $\mathfrak{O}^\sigma = \mathfrak{o}$, and induces a map $\mathfrak{O}_r \to \mathfrak{O}_r$ for any $r \geq 1$ whose fixed subring is $\mathfrak{o}_r$. In the special case $r = 1$, the map $\sigma : \mathsf{k}^{\mathrm{alg}} \to \mathsf{k}^{\mathrm{alg}}$ is given by the q-power map $x \mapsto x^q$, where $q = |\mathsf{k}|$.

2.3. The Greenberg functor

The Greenberg functor was introduced in [16] and [17], as a generalization of Shimura's reduction mod $\mathfrak{p}$ functor to higher powers of $\mathfrak{p}$. Given an artinian local principal ideal ring R (or more generally, an artinian local ring) with a perfect residue field $\mathfrak{k}$, the Greenberg functor $\mathcal{F}_R$ associates to any R-scheme $\mathbf{Y}$ locally of finite type a scheme $\mathcal{F}_R(\mathbf{Y})$ locally of finite type over the residue field $\mathfrak{k}$. Given another such ring R' with residue field $\mathfrak{k}$ 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 property of the functor is the existence of a canonical bijection

$$\mathcal{F}_R(\mathbf{Y})(\mathfrak{k}) = \mathbf{Y}(R). \tag{2.4}$$

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

$$\mathcal{F}_R(\mathbf{Y})(A) = \mathbf{Y}(R \otimes_{W(\mathfrak{k})} W(A)) \tag{2.5}$$

where $W(\cdot)$ denotes the ring of p-typical Witt vectors [29, Ch. II, § 6]. For further introduction we refer to [6, p. 276].

Our application of the Greenberg functor is focused on the artininan principal ideal rings $\mathfrak{O}_r$. For any r, we let $\mathbf{G}_{\mathfrak{O}_r} = \mathbf{G} \times \mathfrak{O}_r$ and $\mathbf{g}_{\mathfrak{O}_r} = \mathbf{g} \times \mathfrak{O}_r$ denote the base change of the group and Lie-algebra schemes $\mathbf{G}$ and $\mathbf{g}$. Put $\mathbf{\Gamma}_r = \mathcal{F}_{\mathfrak{O}_r}(\mathbf{G}_{\mathfrak{O}_r})$ and $\gamma_r = \mathcal{F}_{\mathfrak{O}_r}(\mathbf{g}_{\mathfrak{O}_r})$. Given $m \leq r$, we write $\eta^*_{r,m}$ to denote the connecting maps $\mathbf{\Gamma}_r \to \mathbf{\Gamma}_m$ and $\gamma_r \to \gamma_m$, and put $\mathbf{\Gamma}_r^m = (\eta^*_{r,m})^{-1}(1) = \mathrm{Spec}\,(\kappa(1)) \times_{\mathbf{\Gamma}_m} \mathbf{\Gamma}_r$ (the scheme-theoretic group kernel) and $\gamma_r^m = (\eta^*_{r,m})^{-1}(0) = \mathrm{Spec}\,(\kappa(0)) \times_{\gamma_m} \gamma_r$ (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 $\eta^*_{r,m}$ for the connecting morphisms of different schemes is permissible by [16, § 5, Corollary 4], applied for g the inclusion morphism (see also Assertion 2 of the Main Theorem of [16]).

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

Lemma 2.3.1. *For $r \in \mathbb{N}$ fixed, we have*

1. *The rings $\mathfrak{O}_r$ are the $\mathsf{k}^{\mathrm{alg}}$-points of an r-dimensional algebraic ring scheme $\mathbf{O}_r$ over $\mathsf{k}^{\mathrm{alg}}$.*
   The canonical map $s : \mathsf{k}^{\mathrm{alg}} \to \mathfrak{O}_r$ defines a closed embedding $s^* : \mathbb{A}^1_{\mathsf{k}^{\mathrm{alg}}} \to \mathbf{O}_r$ of the affine line over $\mathsf{k}^{\mathrm{alg}}$ into this ring variety. The restriction of s^* to the multiplicative group $\mathbb{G}_m \subseteq \mathbb{A}^1_{\mathsf{k}^{\mathrm{alg}}}$ is a monomorphism of $\mathsf{k}^{\mathrm{alg}}$-linear algebraic groups, satisfying $\eta^*_{r,1} \circ s^* = \mathbf{1}_{\mathbb{A}^1_{\mathsf{k}^{\mathrm{alg}}}}$.
2. *The group $\mathbf{\Gamma}_r$ is a $d \cdot r$-dimensional linear algebraic group over $\mathsf{k}^{\mathrm{alg}}$.*
3. *The Greenberg functor maps smooth closed sub-$\mathfrak{O}_r$-group schemes of $\mathbf{G}_{\mathfrak{O}_r}$ to closed algebraic $\mathsf{k}^{\mathrm{alg}}$-subgroups of $\mathbf{\Gamma}_r$.*
4. *The scheme γ_r is a $d \cdot r$-dimensional affine space over $\mathsf{k}^{\mathrm{alg}}$, which is naturally endowed with the structure of a Lie-algebra scheme over the ring scheme $\mathbf{O}_r$.*

5. *The connecting morphisms $\eta^*_{r,m}$, for $m \leq r$, give rise to surjective $\mathsf{k}^{\mathrm{alg}}$-group scheme $\mathbf{\Gamma}_r \to \mathbf{\Gamma}_m$ morphisms. Similarly, for $\gamma_r \to \gamma_m$, these are surjective Lie-ring morphisms.*
6. *The adjoint action of $\mathbf{G}_{\mathfrak{O}_r}$ on the Lie-ring scheme $\mathbf{g}_{\mathfrak{O}_m}$ with $m \leq r$, induces an action of the algebraic group $\mathbf{\Gamma}_r$ on γ_m. The application of $\mathcal{F}_{\mathfrak{O}_r}$ preserves centralizers of $\mathfrak{O}_m$-rational points of $\mathbf{g}_{\mathfrak{O}_m}$.*

Proof. 1. See [16, § 1, Proposition 4].

2. The group $\mathbf{\Gamma}_r$ is a smooth affine group scheme of finite type over $\mathsf{k}^{\mathrm{alg}}$ (see [16, § 4, Theorem.(5)] and [17, Corollary 1, p. 263]). Thus, by [40, 11.6], $\mathbf{\Gamma}_r$ is a linear algebraic $\mathsf{k}^{\mathrm{alg}}$-group (see also [33, § 4]). The dimension of $\mathbf{\Gamma}_r$ may be computed by induction on r, using Greenberg's Structure Theorem [17] (see remark on p. 266 of [17]; also, see [3, Lemma 4.1.1] for an explicit argument in the case where r is divisible by the absolute ramification index of $\mathfrak{o}$).

3. Let $\Delta \subseteq \mathbf{G}_{\mathfrak{O}_r}$ be a closed smooth sub-$\mathfrak{O}_r$-scheme. The argument of the previous assertion shows that $\mathcal{F}_{\mathfrak{O}_r}(\Delta)$ is a linear algebraic group over $\mathsf{k}^{\mathrm{alg}}$. That $\mathcal{F}_{\mathfrak{O}_r}(\Delta)$ is a closed subgroup of $\mathbf{\Gamma}_r$ follows from Assertions (2) and (5) of the Main Theorem of [16, p. 643].

4. The Lie-algebra scheme $\mathbf{g}_{\mathfrak{O}_r}$ is isomorphic to the affine d-dimensional space $\mathbb{A}^d_{\mathfrak{O}_r}$ over $\mathfrak{O}_r$, and is endowed with $\mathfrak{O}_r$-regular maps, defining an $\mathfrak{O}_r$-module structure and an $\mathfrak{O}_r$-bilinear Lie-bracket on $\mathbf{g}_{\mathfrak{O}_r}$. It follows from the Main Theorem of [16, p. 643], that $\gamma_r = \mathcal{F}_{\mathfrak{O}_r}(\mathbf{g}_{\mathfrak{O}_r})$ is isomorphic to $\mathbb{A}^{dr}_{\mathsf{k}^{\mathrm{alg}}}$, the affine space of dimension $d \cdot r$ over $\mathsf{k}^{\mathrm{alg}}$. Multiplication by scalars from $\mathbf{O}_r$, the Lie-bracket and addition on $\mathbf{g}_{\mathfrak{O}_r}$ are transported by $\mathcal{F}_{\mathfrak{O}_r}$ to schematic morphisms $\mathbf{O}_r \times \gamma_r \to \gamma_r$ and $\gamma_r \times \gamma_r \to \gamma_r$ by [16, Corollary 3, p. 641]. The Lie-axioms on $\mathcal{F}_{\mathfrak{O}_r}(\gamma_r)$ may be verified using compatibility of the Greenberg functor with preimages [16, Corollary 3, p. 641]. For example, the Jacobi identity can be reformulated using the equality $\mathbf{g}_{\mathfrak{O}_r} \times \mathbf{g}_{\mathfrak{O}_r} \times \mathbf{g}_{\mathfrak{O}_r} = J^{-1}(0)$, where $J : \mathbf{g}_{\mathfrak{O}_r} \times \mathbf{g}_{\mathfrak{O}_r} \times \mathbf{g}_{\mathfrak{O}_r} \to \mathbf{g}_{\mathfrak{O}_r}$ is the morphism satisfying $J(R)(x,y,z) = [[x,y],z] + [[y,z],x] + [[z,x],y]$ for any $\mathfrak{O}_r$-algebra R and $x,y,z \in \mathbf{g}_{\mathfrak{O}_r}(R)$.

5. The connecting map is shown to be a group homomorphism in [16, § 5, Corollary 5], and the preservation of the Lie-bracket follows similarly from [16, § 5, Corollary 2]. Its surjectivity follows from the smoothness of $\mathbf{G}_{\mathfrak{O}_r}$ (resp. $\gamma_{\mathfrak{O}_r}$), and [17, Corollary 2, p. 262].

6. The action of $\mathbf{\Gamma}_r$ on γ_m is given by $\mathcal{F}_{\mathfrak{O}_m}(\alpha_m) \circ (\eta^*_{r,m} \times \mathbf{1}_{\gamma_m}) : \mathbf{\Gamma}_r \times \gamma_m \to \gamma_m$, where $\alpha_m : \mathbf{G}_{\mathfrak{O}_m} \times \mathbf{g}_{\mathfrak{O}_m} \to \mathbf{g}_{\mathfrak{O}_m}$ is the adjunction map; see [33, § 3]. One notes easily that, since the group $\mathbf{\Gamma}^m_r$ acts trivially on γ_m, this action commutes pointwise with the bijection (2.5). The preservation of centralizers follows from [33, Proposition 3.6], by taking $\mathbf{Y}$ and $\mathbf{Z}$ to be the sub-schemes defined by the spectrum of the reside field of $\mathbf{g}_{\mathfrak{O}_m}$ at the given rational point. □

Remark 2.3.2. In the case where $\mathfrak{O}_r$ is a $\mathsf{k}^{\mathrm{alg}}$-algebra, Lemma 2.3.1.(3) may be somewhat strengthened, as in this case γ_r can be shown to coincide with the Lie-algebra of $\mathbf{\Gamma}_r$. In the case of unequal characteristic, the equality $\gamma_r = \mathrm{Lie}(\mathbf{\Gamma}_r)$ is generally false. For example, in the case of $\mathbf{G} = \mathbb{G}_a$, the additive group scheme, we have that $\gamma_2(\mathsf{k}^{\mathrm{alg}}) = \mathrm{Lie}(\mathbb{G}_a)(W_2(\mathsf{k}^{\mathrm{alg}})) = W_2(\mathsf{k}^{\mathrm{alg}})$ is a ring of characteristic p^2, while $\mathrm{Lie}(\mathbf{\Gamma}_2)(\mathsf{k}^{\mathrm{alg}})$ is a two-dimensional $\mathsf{k}^{\mathrm{alg}}$-Lie-algebra and, in particular, has p-torsion.

We also require the following lemma.

Lemma 2.3.3. *For any $m, r \in \mathbb{N}$ with $m \leq r$, there exists an injective homomorphism of the underlying additive group schemes $v^*_{r,m} : \gamma_{r-m} \to \gamma_r$, such that*

1. *for any $y \in \gamma_{r-m}(\mathsf{k}^{\mathrm{alg}}) = \mathbf{g}(\mathfrak{O}_{r-m})$, it holds that $v^*_{r,m}(\mathsf{k}^{\mathrm{alg}})(y) = \pi^m \tilde{y}$, where $\tilde{y} \in \mathbf{g}(\mathfrak{O}_r)$ is such that $\eta_{r,r-m}(\tilde{y}) = y$;*
2. *the sequence $0 \to \gamma_{r-m} \xrightarrow{v^*_{r,m}} \gamma_r \xrightarrow{\eta^*_{r,m}} \gamma_m \to 0$ is exact;*

3. *for any* $y \in \boldsymbol{\gamma}_{r-m}(\mathsf{k}^{\mathrm{alg}})$ *the square* (2.6) *commutes*

$$\begin{array}{ccc} \boldsymbol{\gamma}_r & \xrightarrow{\mathrm{ad}(v^*_{r,m}(y))} & \boldsymbol{\gamma}_r \\ {\scriptstyle \eta^*_{r,r-m}}\downarrow & & \uparrow{\scriptstyle v^*_{r,m}} \\ \boldsymbol{\gamma}_{r-m} & \xrightarrow{\mathrm{ad}(y)} & \boldsymbol{\gamma}_{r-m}, \end{array} \tag{2.6}$$

where $\mathrm{ad}(z) : \boldsymbol{\gamma}_j \times \boldsymbol{\gamma}_j \to \boldsymbol{\gamma}_j$ *(for* $j \in \mathbb{N}$ *and* $z \in \boldsymbol{\gamma}_j(\mathsf{k}^{\mathrm{alg}})$*) is the map defined by* $\mathrm{ad}(z)(A)(x) = [z, x]$ *for any commutative unital* $\mathsf{k}^{\mathrm{alg}}$*-algebra* A *and* $x \in \boldsymbol{\gamma}_j(A)$*;*

4. *The equality* $\eta^*_{r,m+1} \circ v^*_{r,m} = v^*_{m+1,1} \circ \eta^*_{r-m,1}$ *holds.*

Proof. The map $x \mapsto \pi^m x \colon \mathbf{g}(\mathfrak{o}_r) \to \mathbf{g}(\mathfrak{o}_r)$ gives rise to an injective $\mathfrak{o}_r$-module map $v_{r,m} : \mathbf{g}(\mathfrak{o}_{r-m}) \to \mathbf{g}(\mathfrak{o}_r)$, which in turn extends to a map of $\mathfrak{O}_r$-modules, giving rise to the exact sequence

$$0 \to \mathbf{g}_{\mathfrak{O}_{r-m}}(\mathfrak{O}_r) \xrightarrow{v_{r,m}} \mathbf{g}_{\mathfrak{O}_r}(\mathfrak{O}_r) \xrightarrow{\eta_{r,m}} \mathbf{g}_{\mathfrak{O}_m}(\mathfrak{O}_r) \to 0.$$

Applying [16, § 1, Proposition 3.(6)] to both maps of the above sequence, these define k-regular maps between associated module variety structures over $\mathsf{k}^{\mathrm{alg}}$ of the modules above, which, in turn, define an exact sequence of $\mathsf{k}^{\mathrm{alg}}$-schemes

$$0 \to \boldsymbol{\gamma}_{r-m} \xrightarrow{v^*_{r,m}} \boldsymbol{\gamma}_r \xrightarrow{\eta^*_{r,m}} \boldsymbol{\gamma}_m \to 0,$$

where the right-most map coincides with $\eta^*_{r,m}$ by same proposition and by [16, § 5, Corollary 2]. The first and second assertions of the lemma follow.

As for the third assertion, in order to prove that the morphisms $v^*_{r,m} \circ \mathrm{ad}(y) \circ \eta^*_{r,r-m}$ and $\mathrm{ad}(v_{r,m}(y))$ coincide, it is enough to show that, upon passing to their associated comorphisms, they induce the same endomorphism of the coordinate ring of $\boldsymbol{\gamma}_r$. Invoking the isomorphism $\boldsymbol{\gamma}_r \simeq \mathbb{A}^{dm}_{\mathsf{k}^{\mathrm{alg}}}$ of Lemma 2.3.1.(3), since an endomorphism of a polynomial algebra in dm variables is determined by specifying the images of $t_1, \ldots, t_{dm}$ in $\mathsf{k}^{\mathrm{alg}}[t_1, \ldots, t_{dm}]$, by Nullstellensatz, it is enough to show that the two endomorphisms above coincide pointwise on $\boldsymbol{\gamma}_r(\mathsf{k}^{\mathrm{alg}})$. This is immediate by the first two assertions and the linearity of $\mathrm{ad}(\cdot)$ over $\mathfrak{O}_r$. The fourth assertion may be proved in a similar vein as Assertion (3). □

Remark 2.3.4. In the case where $\mathfrak{O}$ is either a $\mathsf{k}^{\mathrm{alg}}$-algebra, or is absolutely unramified (i.e. $\mathfrak{P} = p\mathfrak{O}$), and thus isomorphic to the ring $W(\mathsf{k}^{\mathrm{alg}})$, the map $v^*_{r,m}$ of the lemma may be described explicitly, by fixing a suitable coordinate system for $\boldsymbol{\gamma}_r$ over $\mathsf{k}^{\mathrm{alg}}$ and taking $v^*_{r,m}$ to be either a coordinate shift in the former case, or given by successive applications of the verschiebung and Frobenius maps coordinatewise (see [29]) in the latter.

2.4. The Cayley map

Let D be the affine $\mathfrak{o}$-scheme $\mathrm{Spec}\,(\mathfrak{o}[t_{1,1}, \ldots, t_{N,N}, (\det(\mathbf{t}+1))^{-1}])$, where $t_{1,1}, \ldots, t_{N,N}$ are indeterminates and $\mathbf{t}+1$ 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 $\mathfrak{o}$-algebra R, the set of R-points of D is naturally identified with the set

$$\left\{\mathbf{x} \in \mathrm{M}_N(R) \mid \det(1+\mathbf{x}) \in R^\times\right\}. \tag{2.7}$$

Let $\mathrm{cay} : D \to D$ be the $\mathfrak{o}$-scheme morphism with associated comorphism $\mathrm{cay}^\sharp$ given on generators of $\mathfrak{o}[t_{1,1}, \dots, t_{N,N}, (\det(1+\mathbf{t}))^{-1}]$ by mapping $t_{i,j}$ to the (i,j)-th entry of the matrix $(1-\mathbf{t})(1+\mathbf{t})^{-1}$. Note that $\mathrm{cay}^\sharp(\det(1+\mathbf{t})^{-1}) = 2^{-N}\det(1+\mathbf{t})$. A direct computation shows that, as 2 is invertible in $\mathfrak{o}$, the map $\mathrm{cay}^\sharp$ is its own inverse and thus cay is an isomorphism of D onto itself.

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

$$\mathrm{cay}(R)(\mathbf{x}) = (1-\mathbf{x})(1+\mathbf{x})^{-1}. \tag{2.8}$$

In the specific case $R = \mathsf{k}^{\mathrm{alg}}$, the sets $(D \cap \mathbf{g})(\mathsf{k}^{\mathrm{alg}})$ and $(D \cap \mathbf{G})(\mathsf{k}^{\mathrm{alg}})$ are principal open subsets of $\mathbf{g}(\mathsf{k}^{\mathrm{alg}})$ and $\mathbf{G}(\mathsf{k}^{\mathrm{alg}})$ respectively.[2] Using the description of $\mathbf{g}$ and $\mathbf{G}$ given in Section 2.1.1, one verifies that the restriction of $\mathrm{cay}(\mathsf{k}^{\mathrm{alg}})$ to $(D \cap \mathbf{g})(\mathsf{k}^{\mathrm{alg}})$ defines an algebraic isomorphism of affine varieties onto $(D \cap \mathbf{G})(\mathsf{k}^{\mathrm{alg}})$, and hence a birational map $\mathrm{cay}(\mathsf{k}^{\mathrm{alg}}) : \mathbf{g}(\mathsf{k}^{\mathrm{alg}}) \dashrightarrow \mathbf{G}(\mathsf{k}^{\mathrm{alg}})$. Additionally, being given by a rational function in $\mathbf{x}$ on $(D \cap \mathbf{g})(\mathsf{k}^{\mathrm{alg}})$, the map $\mathrm{cay}(\mathsf{k}^{\mathrm{alg}})$ is equivariant with respect to the conjugation action of $\mathbf{G}(\mathsf{k}^{\mathrm{alg}})$. The properties listed in this paragraph carry over to the associated $\mathsf{k}^{\mathrm{alg}}$-group schemes described in the previous section, as noted in Lemma 2.4.1 below.

The Cayley map was introduced in [10]. Its generalization to groups arising as the set of unitary transformations with respect an anti-involution of an associative algebra is attributed to A. Weil [41, § 4]. See also [24] for a more generalized treatment of the Cayley map.

2.4.1. Properties of the Cayley map

Given $r \in \mathbb{N}$, put $D_r = D \times \mathfrak{O}_r$ and let $\mathrm{cay}_r = \mathrm{cay} \times \mathbf{1}_{\mathfrak{O}_r}$ be the base change of cay. Let $\mathbf{\Delta}_r = \mathcal{F}_{\mathfrak{O}_r}(D_r)$ and $\widehat{\mathrm{cay}}_r = \mathcal{F}_{\mathfrak{O}_r}(\mathrm{cay}_r)$. Note that, by construction and by the Main Theorem of [16], $\mathbf{\Delta}_r$ is an open affine subscheme of $\mathbb{A}^{N^2m}_{\mathsf{k}^{\mathrm{alg}}}$.

Lemma 2.4.1. *Let $1 \le m \le r$. The map $\widehat{\mathrm{cay}}_r$ has the following properties.*

Cay1. *The map $\widehat{\mathrm{cay}}_r$ is a birational equivalence $\boldsymbol{\gamma}_r \dashrightarrow \mathbf{\Gamma}_r$. Furthermore, its restriction to the kernel $\boldsymbol{\gamma}_r^m$ is an isomorphism of $\mathsf{k}^{\mathrm{alg}}$-varieties onto $\mathbf{\Gamma}_r^m$, and is an isomorphism of abelian groups if $2m \ge r$.*

Cay2. *The map $\widehat{\mathrm{cay}}_r$ is $\mathbf{\Gamma}_r$-equivariant with respect to the action given in Lemma 2.3.1.(6) on $\boldsymbol{\gamma}_r$ and with respect to group conjugation on $\mathbf{\Gamma}_r$.*

Cay3. *The diagram in (2.9) commutes.*

$$\begin{array}{ccc} \boldsymbol{\gamma}_r & \xrightarrow{\widehat{\mathrm{cay}}_r} & \mathbf{\Gamma}_r \\ {\scriptstyle \eta^*_{r,m}}\downarrow & & \downarrow{\scriptstyle \eta^*_{r,m}} \\ \boldsymbol{\gamma}_m & \xrightarrow{\widehat{\mathrm{cay}}_m} & \mathbf{\Gamma}_m. \end{array} \tag{2.9}$$

Proof. 1. The inclusion map $D_r \cap \mathbf{g}_{\mathfrak{O}_r} \subseteq \mathbf{g}_{\mathfrak{O}_r}$ is an open immersion, and thus by Assertion (2) and (3) of the Main Theorem of [16], the $\mathsf{k}^{\mathrm{alg}}$-scheme $\mathbf{\Delta}_r \cap \boldsymbol{\gamma}_r$ is immersed as an open subscheme of $\boldsymbol{\gamma}_r$. Similarly for $\mathbf{\Delta}_r \cap \mathbf{\Gamma}_r$. By functoriality, the morphism $\widehat{\mathrm{cay}}_r$ is an isomorphism of $\mathbf{\Delta}_r \cap \boldsymbol{\gamma}_r$ onto $\mathbf{\Delta}_r \cap \mathbf{\Gamma}_r$, and hence $\boldsymbol{\gamma}_r$ and $\mathbf{\Gamma}_r$ are birationally equivalent.

[2] Here $\cap$ denotes the scheme-theoretic intersection, $D \cap \mathbf{g} = D \times_{\mathrm{Spec}\,(\mathfrak{o}[t_{1,1},\dots,t_{N,N}])} \boldsymbol{\gamma}$. Note that, in the present setting, as $\mathbf{g} \subseteq \mathrm{M}_N \times \mathfrak{o} = \mathrm{Spec}\,(\mathfrak{o}[t_{1,1}, \dots, t_{N,N}])$, for any $\mathfrak{o}$-algebra R, $(D \cap \mathbf{g})(R)$ is simply the set of matrices $\mathbf{x} \in \mathbf{g}(R)$ such that the matrix $\mathbf{1} + \mathbf{x}$ is invertible. Likewise for $D \cap \mathbf{G}$, using the inclusions $\mathbf{G} \subseteq \mathrm{SL}_N \times \mathfrak{o} \subseteq \mathrm{M}_N \times \mathfrak{o}$.

To prove that $\widehat{\mathrm{cay}}_r$ restricts to an isomorphism of $\boldsymbol{\gamma}_r^m$ onto $\boldsymbol{\Gamma}_r^m$, it would be enough that both are embedded as sub-schemes of $\boldsymbol{\Delta}_r$ under the given inclusions into $\mathbb{A}_{\mathsf{k}^{\mathrm{alg}}}^{N^2m}$. Note that by applying Greenberg's Structure Theorem [17] inductively, both $\boldsymbol{\gamma}_r^m$ and $\boldsymbol{\Gamma}_r^m$ are reduced, and thus are $\mathsf{k}^{\mathrm{alg}}$-varieties. Thus, by Nullstellensatz, they are determined by their $\mathsf{k}^{\mathrm{alg}}$-points and it suffices to show they are included in the reduced subscheme $(\boldsymbol{\Delta}_r)_{\mathrm{red}} \subseteq \boldsymbol{\Delta}_r$. This follows from the bijection (2.4), as $\boldsymbol{\gamma}_r^m(\mathsf{k}^{\mathrm{alg}}) = \mathbf{g}_{\mathfrak{O}_r}(\mathfrak{O}_r) \cap \eta_{r,m}^{-1}(0)$ is included in the nilradical of the matrix algebra $\mathrm{M}_N(\mathfrak{O}_r)$, and hence included in $D_r(\mathfrak{O}_r)$, and since $\boldsymbol{\Gamma}_r^m(\mathsf{k}^{\mathrm{alg}}) = \mathbf{G}_{\mathfrak{O}_r}(\mathfrak{O}_r) \cap \eta_{r,m}^{-1}(1) \subseteq 1 + \pi \mathrm{M}_N(\mathfrak{O}_r) \subseteq \mathrm{GL}_N(\mathfrak{O}_r)$, and thus (since $\mathrm{char}(\mathsf{k}^{\mathrm{alg}}) \neq 2$) included in $D_r(\mathfrak{O}_r)$.

Lastly, to prove that $\widehat{\mathrm{cay}}_r$ is a group homomorphism whenever $2m \geq r$, it is equivalent to show that it preserves comultiplication in the Hopf-algebra structure of the coordinate ring of $\boldsymbol{\gamma}_r^m$ in this case. Arguing as in the proof Lemma 2.3.3, it sufficient to verify this on the $\mathsf{k}^{\mathrm{alg}}$-points of the variety. This follows from the definition of cay (2.8), as in this case $\boldsymbol{\gamma}_r^m(\mathsf{k}^{\mathrm{alg}}) \subseteq \mathbf{g}_{\mathfrak{O}_r}(\mathfrak{O}_r)$ is included in an ideal of vanishing square in $\mathrm{M}_N(\mathfrak{O}_r)$ and the map $\widehat{\mathrm{cay}}_r$ coincides with the map $\mathbf{x} \mapsto 1 - 2\mathbf{x}$.

2. Property (Cay2) holds since $\mathcal{F}_{\mathfrak{O}_r}$ maps the cartesian square (2.10), which states the $\mathbf{G}_{\mathfrak{O}_r}$-equivariance of cay_r, to a corresponding cartesian square, stating the $\boldsymbol{\Gamma}_r$-equivariance of $\widehat{\mathrm{cay}}_r$.

$$\begin{array}{ccc} \mathbf{G}_{\mathfrak{O}_r} \times \mathbf{g}_{\mathfrak{O}_r} & \xrightarrow{\alpha_{\mathbf{G}_{\mathfrak{O}_r},\mathbf{g}_{\mathfrak{O}_r}}} & \mathbf{g}_{\mathfrak{O}_r} \\ \downarrow{\scriptstyle \mathbf{1}_{\mathbf{G}_{\mathfrak{O}_r}} \times \mathrm{cay}_r} & \square & \downarrow{\scriptstyle \mathrm{cay}_r} \\ \mathbf{G}_{\mathfrak{O}_r} \times \mathbf{G}_{\mathfrak{O}_r} & \xrightarrow{\alpha_{\mathbf{G}_{\mathfrak{O}_r},\mathbf{G}_{\mathfrak{O}_r}}} & \mathbf{G}_{\mathfrak{O}_r} \end{array} \tag{2.10}$$

Here $\alpha_{\mathbf{G}_{\mathfrak{O}_r},\mathbf{X}}$ denotes the action map of $\mathbf{G}_{\mathfrak{O}_r}$ on $\mathbf{X} \in \{\mathbf{G}_{\mathfrak{O}_r}, \mathbf{g}_{\mathfrak{O}_r}\}$ by either conjugation or by the adjoint action.

3. Finally, property (Cay3) is simply an application of [16, Corollary 4, p. 645], to the case $R = \mathfrak{o}_r$, $R' = \mathfrak{o}_m$, $\varphi = \eta_{r,m}$, $X_1 = \boldsymbol{\gamma}_r \cap D_r$, $X_2 = \boldsymbol{\Gamma}_r \cap D_r$ and $g = \mathrm{cay}_r$. □

2.5. Groups, Lie algebras and characters

In general, given finite groups $\Delta \subseteq \Gamma$ and characters $\sigma \in \mathrm{Irr}(\Delta)$ and $\chi \in \mathrm{Irr}(\Gamma)$, we denote by χ_Δ the restriction of χ to Δ, and by σ^Γ the character induced from σ in Γ. 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 Γ is denoted by $\mathbf{Z}(\Gamma)$.

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

3. Regular elements and regular characters

3.1. Regular elements

We begin our analysis of regular characters by inspecting the group $\mathbf{G}(\mathfrak{O})$. To do so, we first consider the regular orbits for the action of $\mathbf{G}(\mathfrak{O}_r)$ on $\mathbf{g}(\mathfrak{O}_r)$, or, equivalently (see [33, § 3]), of $\boldsymbol{\Gamma}_r(\mathsf{k}^{\mathrm{alg}})$ on $\boldsymbol{\gamma}_r(\mathsf{k}^{\mathrm{alg}})$, via the action described in Lemma 2.3.1.(6). The methods which we apply are influenced by [18].

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 [36, § 3.5]. Following [18], this definition is extended to elements of $\boldsymbol{\gamma}_r$.

Definition 3.1.1. Let $r \geq 1$. An element $x \in \mathbf{g}(\mathfrak{O}_r)$ is said to be **regular** if the group scheme $\mathcal{F}_{\mathfrak{O}_r}\left(\mathbf{C}_{\mathbf{G}_{\mathfrak{O}_r}}(x)\right) = \mathbf{C}_{\mathbf{\Gamma}_r}(x)$, obtained by applying the Greenberg functor to the centralizer group scheme of x in $\mathbf{G}_{\mathfrak{O}_r}$, is of minimal dimension among such group schemes.

The following theorem lists the main properties of regular elements of γ_r, which are proved in this section.

Theorem 3.1.2. *Let $\mathbf{G}$ be a symplectic or a special orthogonal group scheme over a complete discrete valuation ring $\mathfrak{o}$ of odd residue field characteristic, with Lie-algebra $\mathbf{g} = \mathrm{Lie}(\mathbf{G})$. Fix $r \in \mathbb{N}$ and let $x \in \mathbf{g}(\mathfrak{O}_r)$.*

1. *If x_r is a regular element of $\mathbf{g}_{\mathfrak{O}_r}(\mathfrak{O}_r)$, then $\mathbf{C}_{\mathbf{\Gamma}_r}(x_r)$ is a $\mathsf{k}^{\mathrm{alg}}$-group scheme of dimension $r \cdot n$, where $n = \mathrm{rk}(\mathbf{G} \times K^{\mathrm{alg}})$.*
2. *The element x_r is regular if and only if $x_1 = \eta_{r,1}(x_r)$ is a regular element of $\mathbf{g}(\mathsf{k}^{\mathrm{alg}})$.*
3. *Suppose $x_r \in \mathbf{g}(\mathfrak{O}_r)$ is regular. The restriction of the reduction map $\eta_{r,1}$ to $\mathbf{C}_{\mathbf{G}(\mathfrak{O}_r)}(x_r)$ is surjective onto $\mathbf{C}_{\mathbf{G}(\mathsf{k}^{\mathrm{alg}})}(x_1)$.*

Remark 3.1.3. Assertions (1) and (3) of Theorem 3.1.2, as well as Assertion (1) of Proposition 3.1.4 below, are formal consequences of the stronger statement that the centralizer group scheme $\mathbf{C}_{\mathbf{G}_{\mathfrak{O}_r}}(x)$ is smooth over $\mathfrak{O}_r$, whenever $x \in \mathbf{g}(\mathfrak{O}_r)$ is regular. This statement, while plausible, is not proved in this article.

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 analyze the case of regular elements of $\mathfrak{g}_r = \gamma_r(\mathfrak{O}_r)^{\sigma}$.

Proposition 3.1.4. *Let $\mathbf{G}$ be a symplectic or a special orthogonal group over $\mathfrak{o}$ with $\mathbf{g} = \mathrm{Lie}(\mathbf{G})$ and let $x \in \mathfrak{g} = \mathbf{g}(\mathfrak{o})$. Assume $x_r = \eta_r(x)$ is regular for some $r \in \mathbb{N}$. Then*

1. *$\mathbf{C}_G(x) = \varprojlim_r \mathbf{C}_{G_r}(x_r)$, where $G = \mathbf{G}(\mathfrak{o})$ and $G_r = \mathbf{G}(\mathfrak{o}_r)$*
2. *Furthermore, x is a regular element of $\mathbf{g}(K^{\mathrm{alg}})$.*

Proposition 3.1.4 has the following corollary.

Corollary 3.1.5. *In the notation of Proposition 3.1.4, let $x \in \mathfrak{g}$ such that $x_r = \eta_r(x)$ is a regular element of $\mathfrak{g}_r$, for some $r \in \mathbb{N}$. Then $\mathbf{C}_{G_r}(x_r)$ is abelian.*

3.1.1. General properties of the groups $\mathbf{\Gamma}_r$

We begin by examining some basic properties of the group $\mathbf{\Gamma}_r$ ($r \in \mathbb{N}$) and of centralizers of elements of γ_r, when considered as algebraic group schemes over $\mathsf{k}^{\mathrm{alg}}$. The following lemma summarizes the necessary components for the proof of Theorem 3.1.2.(1), and is mostly included in [33].

Lemma 3.1.6.

1. *The group scheme $\mathbf{\Gamma}_r$ is a connected linear algebraic group over $\mathsf{k}^{\mathrm{alg}}$.*
2. *The unipotent radical of $\mathbf{\Gamma}_r$ is $\mathbf{\Gamma}_r^1$.*
3. *Let $\mathbf{T}$ be a maximal torus of $\mathbf{G}$, defined over $\mathfrak{O}$, and let $\mathbf{T}_1 = \mathbf{T} \times \mathsf{k}^{\mathrm{alg}} \subseteq \mathbf{\Gamma}_1$. The restriction of the map $s^* : \mathbb{A}^1_{\mathsf{k}^{\mathrm{alg}}} \to \mathbf{O}_r$ of Lemma 2.3.1.(1) to $\mathbb{G}_m$ extends to an embedding of $\mathbf{T}_1$ as a maximal torus in $\mathbf{\Gamma}_r$.*
4. *The centralizer of $s^*(\mathbf{T}_1)$ in $\mathbf{\Gamma}_r$ is the Cartan subgroup $\mathcal{F}_{\mathfrak{O}_r}(\mathbf{T} \times \mathfrak{O}_r)$. Moreover, $\mathcal{F}_r(\mathbf{T} \times \mathfrak{O}_r)$ is a linear algebraic $\mathsf{k}^{\mathrm{alg}}$-group of dimension $n \cdot r$.*

Proof. 1. Connectedness is proved in [33, Lemma 4.2]. The fact that $\mathbf{\Gamma}_r$ is linear algebraic over $\mathsf{k}^{\mathrm{alg}}$ is shown in Lemma 2.3.1.(1).

2. See [33, Proposition 4.3].

3. May be proved by following the argument of [18, Proposition 2.2.(2)], practically verbatim, making use of the fact that $\mathbf{\Gamma}_r$ and $\mathbf{\Gamma}_1 = \eta_{r,1}^*(\mathbf{\Gamma}_r)$ are of the same rank by the previous assertion, and that $s^*(\mathbf{T}_1)$ is a connected abelian subgroup of $\mathbf{\Gamma}_r$ of dimension $n = \mathrm{rk}(\mathbf{\Gamma}_1)$.

4. The inclusion $\mathbf{T}(\mathfrak{O}_r) \subseteq \mathbf{C}_{\mathbf{\Gamma}_r(\mathsf{k}^{\mathrm{alg}})}(s^*(\mathbf{T}_1)(\mathsf{k}^{\mathrm{alg}}))$ is clear, since $\mathbf{T}(\mathfrak{O}_r)$ is abelian and contains $s^*(\mathbf{T}_1)(\mathsf{k}^{\mathrm{alg}})$, by Lemma 2.3.1.(1). The inclusion $\mathbf{T} \times \mathfrak{O}_r \subseteq \mathbf{C}_{\mathbf{\Gamma}_r}(s^*(\mathbf{T}_1))$ follows (see [33, Proposition 3.2]). By [33, Theorem 4.5], $\mathcal{F}_{\mathfrak{O}_r}(\mathbf{T} \times \mathfrak{O}_r)$ is a Cartan subgroup of $\mathbf{\Gamma}_r$ and hence is equal to the centralizer of $s^*(\mathbf{T}_1)$. Finally, the statement regarding the dimension of $\mathcal{F}_r(\mathbf{T} \times \mathfrak{O}_r)$ follows from Lemma 2.3.1.(1). □

Proof of Theorem 3.1.2.(1). The alternative proof of [36, Ch. III, § 3.5, Proposition 1] shows that the minimal centralizer dimension of an element of $\mathbf{g}(\mathfrak{O}_r)$ is equal to that of a Cartan subgroup of $\mathbf{\Gamma}_r$, provided that the Cartan subgroups of $\mathbf{\Gamma}_r$ are abelian and that their union forms a dense subset of $\mathbf{\Gamma}_r$. The former of these conditions holds by [33, Theorem 4.5], and the latter by [5, 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 [18, 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 $\boldsymbol{\gamma}_r$ and of its image in $\boldsymbol{\gamma}_1$.

Lemma 3.1.7. *Let $x \in \mathbf{g}(\mathfrak{O})$ be fixed, and for any $r \in \mathbb{N}$ put $x_r = \eta_r(x) \in \mathbf{g}(\mathfrak{O}_r)$. Let $\mathbf{C}_{\boldsymbol{\gamma}_r}(x_r)$ denote the Lie-algebra centralizer of x_r, i.e. $\mathbf{C}_{\boldsymbol{\gamma}_r}(x_r)(A) = \{y \in \boldsymbol{\gamma}_r(A) \mid \mathrm{ad}(x_r)(A)(y) = 0\}$, for any commutative unital $\mathsf{k}^{\mathrm{alg}}$-algebra A. The image of $\mathbf{C}_{\boldsymbol{\gamma}_r}(x_r)$ under the connecting morphism $\eta_{r,1}^*$ is a $\mathsf{k}^{\mathrm{alg}}$-group scheme of dimension greater or equal to n.*

Proof. Assume towards a contradiction that the statement of the lemma is false, and let r be minimal such that $\dim \eta_{r,1}^*\left(\mathbf{C}_{\boldsymbol{\gamma}_r}(x_r)\right) < n$. Note that, since $\eta_{r,1}^* \circ \eta_{m,r}^* = \eta_{m,1}^*$ for all $m > r$ (by [16, Proposition 3, § 5]) we also have that $\dim \eta_{m,1}^*\left(\mathbf{C}_{\boldsymbol{\gamma}_m}(x_m)\right) < n$ for all $m \geq r$.

Fix $m \geq r$, and consider the sequence of immersions

$$\mathbf{C}_{\boldsymbol{\gamma}_m}(x_m) \supseteq \mathbf{C}_{\boldsymbol{\gamma}_m^1}(x_m) \supseteq \ldots \supseteq \mathbf{C}_{\boldsymbol{\gamma}_m^{m-1}}(x_m) \supseteq 0, \tag{3.1}$$

where $\mathbf{C}_{\boldsymbol{\gamma}_m^i}(x_m) = \mathbf{C}_{\boldsymbol{\gamma}_m}(x_m) \cap \boldsymbol{\gamma}_m^i$. Then

$$\dim \mathbf{C}_{\boldsymbol{\gamma}_m}(x_m) = \sum_{i=0}^{m-1} \left(\dim \mathbf{C}_{\boldsymbol{\gamma}_m^i}(x_m) - \dim \mathbf{C}_{\boldsymbol{\gamma}_m^{i+1}}(x_m)\right), \tag{3.2}$$

where $\boldsymbol{\gamma}_m^0 = \boldsymbol{\gamma}_m$ and $\boldsymbol{\gamma}_m^m = \mathrm{Spec}\,(\kappa(0))$.

For any $0 \leq i \leq m-1$, the map $v_{i,m}^* : \boldsymbol{\gamma}_{m-i} \to \boldsymbol{\gamma}_m$ of Lemma 2.3.3 restricts, by Assertion (3) of the lemma, to an isomorphism of abelian $\mathsf{k}^{\mathrm{alg}}$-group schemes $\mathbf{C}_{\boldsymbol{\gamma}_{m-i}}(x_{m-i}) \simeq \mathbf{C}_{\boldsymbol{\gamma}_m^i}(x_m)$, which restricts further, by Assertion (4) of the lemma, to an isomorphism $\mathbf{C}_{\boldsymbol{\gamma}_m^{i+1}}(x_m) \simeq \mathbf{C}_{\boldsymbol{\gamma}_{m-i}^1}(x_{m-i})$. Using these isomorphisms and the exact sequence

$$0 \to \mathbf{C}_{\boldsymbol{\gamma}_{m-i}^1}(x_{m-i}) \to \mathbf{C}_{\boldsymbol{\gamma}_{m-i}}(x_{m-i}) \xrightarrow{\eta_{m-i,1}^*} \eta_{m-i,1}^*\left(\mathbf{C}_{\boldsymbol{\gamma}_{m-i}}(x_{m-i})\right) \to 0,$$

we deduce

$$\begin{aligned}\dim \mathbf{C}_{\gamma_m}(x_m) &= \sum_{i=0}^{m-1}\left(\dim \mathbf{C}_{\gamma_{m-i}}(x_{m-i}) - \dim \mathbf{C}_{\gamma^1_{m-i}}(x_{m-i})\right) = \sum_{i=0}^{m-1}\dim \eta^*_{m-i,1}\left(\mathbf{C}_{\gamma_{m-i}}(x_{m-i})\right)\\ &= \sum_{i=1}^{r-1}\dim \eta^*_{i,1}\left(\mathbf{C}_{\gamma_i}(x_i)\right) + \sum_{i=r}^{m}\dim \eta^*_{i,1}\left(\mathbf{C}_{\gamma_i}(x_i)\right)\\ &\leq d\cdot(r-1) + (n-\alpha)\cdot(m-r), \end{aligned} \tag{3.3}$$

for some integer $\alpha \geq 1$, where $d = \dim \boldsymbol{\gamma}_1 = \dim \boldsymbol{\Gamma}_1$.

For any $m \in \mathbb{N}$, 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 $\mathbf{C}_{\gamma_m}(x_m)$ and the group-centralizer $\mathbf{C}_{\boldsymbol{\Gamma}_m}(x_m)$ of x_m. In particular, by Theorem 3.1.2.(1), we have that $\dim \mathbf{C}_{\gamma_m}(x_m) = \dim \mathbf{C}_{\boldsymbol{\Gamma}_m}(x_m) \geq m\cdot n$. Manipulating the inequality (3.3), we get that

$$\alpha\cdot m \leq d\cdot(r-1) - r\cdot(n-\alpha) \tag{3.4}$$

for all $m > r$. A contradiction, since m 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 3.1.8. *Let $x \in \boldsymbol{\gamma}$ and $x_r = \eta_r(x)$ for all $r \in \mathbb{N}$. The group scheme $\eta^*_{r,1}\left(\mathbf{C}_{\boldsymbol{\Gamma}_r}(x_r)\right)$ is a linear algebraic $\mathsf{k}^{\mathrm{alg}}$-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)

$$\begin{array}{ccc} \mathbf{C}_{\gamma_r}(x_r) & \xrightarrow{\widehat{\mathrm{cay}}_r} & \mathbf{C}_{\boldsymbol{\Gamma}_r}(x_r) \\ \Big\downarrow{\scriptstyle \eta^*_{r,1}} & & \Big\downarrow{\scriptstyle \eta^*_{r,1}} \\ \eta^*_{r,1}\left(\mathbf{C}_{\gamma_r}(x_r)\right) & \xrightarrow{\mathrm{cay}_{\mathsf{k}^{\mathrm{alg}}}} & \eta^*_{r,1}\left(\mathbf{C}_{\boldsymbol{\Gamma}_r}(x_r)\right). \end{array} \tag{3.5}$$

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 r, similarly to [18, Theorem 3.6], the case $r = 1$ being trivially true. Consider the following exact sequence

$$1 \longrightarrow \mathbf{C}_{\boldsymbol{\Gamma}^1_r}(x_r) \longrightarrow \mathbf{C}_{\boldsymbol{\Gamma}_r}(x_r) \xrightarrow{\eta^*_{r,1}} \mathbf{C}_{\boldsymbol{\Gamma}_1}(x_1). \tag{3.6}$$

Properties (Cay1) and (Cay2) imply that the map $\widehat{\mathrm{cay}}_r$ is defined on $\mathbf{C}_{\boldsymbol{\Gamma}^1_r}(x_r)$ and is mapped onto $\mathbf{C}_{\gamma^1_r}(x_r)$. Combined with Lemma 2.3.3, we get that $\dim \mathbf{C}_{\boldsymbol{\Gamma}^1_r}(x_r) = \dim \mathbf{C}_{\gamma_{r-1}}(x_{r-1})$. Moreover, since $\boldsymbol{\Delta}_{r-1} \cap \mathbf{C}_{\gamma_{r-1}}(x_{r-1})$ is a non-trivial open subscheme of $\mathbf{C}_{\gamma_{r-1}}(x_{r-1})$, and is mapped by $\widehat{\mathrm{cay}}_r$ to an open subscheme of $\mathbf{C}_{\boldsymbol{\Gamma}_{r-1}}(x_{r-1})$, we deduce the equality

$$\dim \mathbf{C}_{\boldsymbol{\Gamma}^1_r}(x_r) = \dim \mathbf{C}_{\boldsymbol{\Gamma}_{r-1}}(x_{r-1}). \tag{3.7}$$

If x_1 is regular then by induction we have that $\dim \mathbf{C}_{\boldsymbol{\Gamma}_{r-1}}(x_{r-1}) = n(r-1)$ and hence, by (3.6) and (3.7),

$$\dim \mathbf{C}_{\boldsymbol{\Gamma}_r}(x_r) \leq \dim \mathbf{C}_{\boldsymbol{\Gamma}_{r-1}}(x_{r-1}) + \dim \mathbf{C}_{\boldsymbol{\Gamma}_1}(x_1) = r\cdot n.$$

Conversely, if x_1 is not regular, then by induction x_{r-1} is not regular, and the dimension of $\mathbf{C}_{\mathbf{\Gamma}_{r-1}}(x_{r-1})$ is strictly greater than $n(r-1)$. By Proposition 3.1.8 and (3.7), have

$$\dim \mathbf{C}_{\mathbf{\Gamma}_r}(x_r) = \dim \mathbf{C}_{\mathbf{\Gamma}_{r-1}}(x_{r-1}) + \dim \eta_1 \left(\mathbf{C}_{\mathbf{\Gamma}_r}(x_r)\right) > n(r-1) + n = n \cdot r,$$

and x_r is not regular. □

Before discussing the final assertion of Theorem 3.1.2, let us observe a simple corollary of Lemma 3.1.7, which is the Lie-algebra version of the assertion.

Corollary 3.1.9. *Let $r \in \mathbb{N}$ and $x_r \in \gamma_r(\mathsf{k}^{\mathrm{alg}})$ be regular. The restriction of $\eta_{r,1}$ to $\mathbf{C}_{\mathbf{g}(\mathfrak{O}_r)}(x_r)$ is onto $\mathbf{C}_{\mathbf{g}(\mathsf{k}^{\mathrm{alg}})}(x_1)$, where $x_1 = \eta_{r,1}(x_r) \in \mathbf{g}(\mathsf{k}^{\mathrm{alg}})$.*

Proof. Theorem 3.1.2.(2) implies that x_1 is regular and hence $\mathbf{C}_{\gamma_1}(x_1)(\mathsf{k}^{\mathrm{alg}}) = \mathbf{C}_{\mathbf{g}(\mathsf{k}^{\mathrm{alg}})}(x_1)$ is a $\mathsf{k}^{\mathrm{alg}}$-vector space of dimension $n = \dim \mathbf{C}_{\mathbf{\Gamma}_1}(x_1)$. By Lemma 3.1.7, the $\mathsf{k}^{\mathrm{alg}}$-points of the image of $\mathbf{C}_{\gamma_r}(x_r)$ under $\eta^*_{r,1}$ comprise a subspace of $\mathbf{C}_{\mathbf{g}(\mathsf{k}^{\mathrm{alg}})}(x_1)$ of the same dimension. □

3.1.3. The image of $\eta_{r,1}$ on $\mathbf{C}_{\mathbf{\Gamma}_r}(x_r)$

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 3.1.5.

Proposition 3.1.10. *Let L be either $\mathsf{k}^{\mathrm{alg}}$ or K^{alg}, and let $\mathbf{H} = \mathbf{G} \times \mathrm{Spec}\,(L)$ and $\mathbf{h} = \mathrm{Lie}(\mathbf{H})$ its Lie-algebra. Put $H = \mathbf{H}(L)$ and $\mathfrak{h} = \mathbf{h}(L)$. Let $x \in \mathbf{h}(L)$ be regular. Then*

$$\mathbf{C}_H(x) = \mathbf{C}_{\mathbf{H}}(x)^\circ(L) \cdot \mathbf{Z}(H),$$

where $\mathbf{C}_{\mathbf{H}}(x)^\circ$ is the connected component of 1. In particular, $|\mathbf{C}_H(x) : \mathbf{C}_{\mathbf{H}}(x)^\circ(L)| \leq 2$ and $\mathbf{C}_H(x)$ is abelian.

Proof. Let $x = s + h$ be the Jordan decomposition of x, with $s, h \in \mathfrak{h}$, s semisimple, h nilpotent and $[s,h] = 0$. Note that, as an element of H commutes with x if and only if it commutes with both s and h, we have that $\mathbf{C}_H(x) = \mathbf{C}_{\mathbf{C}_H(s)}(h)$. From Proposition 2.1.1, it follows that

$$\mathbf{C}_H(x) = \mathbf{C}_{\mathbf{C}_H(s)}(h) = \prod_{j=1}^{t} \mathbf{C}_{\mathrm{GL}_{m_j}(L)}\left(h\,|_{W_{\lambda_j}}\right) \times \mathbf{C}_{\Delta(L)}\left(h\,|_{\mathrm{Ker}(s)}\right), \tag{3.8}$$

where Δ is a classical linear algebraic group over L of automorphisms preserving a non-degenerate bilinear form on a subspace of L^N, and $\pm\lambda_1, \ldots, \pm\lambda_t$ are the non-zero eigenvalues of s, as described in Proposition 2.1.1, with respective multiplicities $m_1, \ldots, m_t$, and $W_{\lambda_j} = \mathrm{Ker}(s - \lambda_j \mathbf{1})$. Additionally, by [36, 3.5, Proposition 5], the restricted operators $h\,|_{W(\lambda_j)}$ and $h\,|_{\mathrm{Ker}(s)}$ are regular as elements of the Lie-algebras of GL_{m_j} and of Δ over L, respectively.

By [32, III, 3.2.2] it is known that all factors in (3.8), apart from $\mathbf{C}_\Delta(h\,|_{\mathrm{Ker}(s)})$, are connected. Furthermore, by [32, III, 1.14] and the assumption $\mathrm{char}(L) \neq 2$, we have

$$\mathbf{C}_\Delta\left(h\,|_{\mathrm{Ker}(s)}\right) = \mathbf{C}_\Delta\left(h\,|_{\mathrm{Ker}(s)}\right)^\circ \cdot \mathbf{Z}(\Delta),$$

(see [32, I, 4.3]). Taking into account the fact that, as $\mathrm{char}(L) \neq 2$, $\mathbf{Z}(\Delta(L))$ is the finite group $\{\pm 1\}$, one easily deduces from this the equality

$$\mathbf{C}_H(x) = \mathbf{C}_{\mathbf{H}}(x)^\circ(L) \cdot \mathbf{Z}(H).$$

Lastly, $\mathbf{C}_H(x)^\circ$ is abelian by [32, Corollary 1.4], and $|\mathbf{C}_H(x) : \mathbf{C}_H(x)^\circ| \leq |\mathbf{Z}(H)| = 2$. □

Proof of Theorem 3.1.2.(3). By Proposition 3.1.8 and Chevalley's Theorem [12, IV, 1.8.4], the image of $\mathbf{C}_{\mathbf{\Gamma}_r}(x_r)$ under $\eta^*_{r,1}$ contains the connected component $\mathbf{C}_{\mathbf{\Gamma}_1}(x_1)^\circ$ of the identity in $\mathbf{C}_{\mathbf{\Gamma}_1}(x)$. Additionally, the center $\mathbf{Z}(\mathbf{\Gamma}_r)$ of $\mathbf{\Gamma}_r$ is clearly contained in $\mathbf{C}_{\mathbf{\Gamma}_r}(x_r)$ and is mapped by $\eta^*_{r,1}$ onto $\mathbf{Z}(\mathbf{\Gamma}_1)$. This implies the inclusion

$$\mathbf{C}_{\mathbf{\Gamma}_1}(x_1) \supseteq \eta^*_{r,1}\left(\mathbf{C}_{\Gamma_r}(x_r)\right) \supseteq \left(\mathbf{C}_{\Gamma_1}(x_1)\right)^\circ \cdot \mathbf{Z}(\mathbf{\Gamma}_1).$$

Evaluating the above inclusions at $\mathsf{k}^{\mathrm{alg}}$-points, by Proposition 3.1.10, we deduce the equality. □

3.1.4. Returning to the $\mathfrak{o}$-rational setting

In this section we prove Proposition 3.1.4. An initial step towards this goal is to show that the third assertion of Theorem 3.1.2 remains true when replacing the groups $\mathbf{G}(\mathfrak{O}_r)$ and Lie-rings $\mathbf{g}(\mathfrak{O}_r)$ with the group and Lie-rings of $\mathfrak{o}_r$-rational points, i.e. $G_r = \mathbf{G}(\mathfrak{o}_r)$ and $\mathfrak{g}_r = \mathbf{g}(\mathfrak{o}_r)$. Given $1 \leq m \leq r$, we write G^m_r and $\mathfrak{g}^m_r$ to denote the congruence subgroup $\mathrm{Ker}(G_r \xrightarrow{\eta_{r,m}} G_m) = G_r \cap \eta^{-1}_{r,m}(1)$ and congruence subring $\mathrm{Ker}(\mathfrak{g}_r \xrightarrow{\eta_{r,m}} \mathfrak{g}_m) = \mathfrak{g}_r \cap \eta^{-1}_{r,m}(0)$, respectively.

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

Lemma 3.1.11. *Let $r \in \mathbb{N}$ and let $x_r \in \mathfrak{g}_r$ be a regular element and $x_1 = \eta_{r,1}(x_r)$. Given $g \in \mathbf{C}_{G_1}(x_1) = \mathbf{C}_{\mathbf{G}(\mathsf{k}^{\mathrm{alg}})}(x_1) \cap G_1$, let $F_g = \eta^{-1}_{r,1}(g) \cap \mathbf{C}_{\mathbf{G}(\mathfrak{O}_r)}(x_r)$, and let $\mathcal{L}_g$ be the map defined by*

$$h \mapsto h \cdot \sigma(h)^{-1}.$$

Then $\mathcal{L}_g : F_g \to F_1$ is a well-defined surjective map.

Proof. The sets $F_{g'}$ ($g' \in \mathbf{C}_{G_1}(x_1)$) are simply cosets of the subgroup $F_1 = \mathbf{C}_{\mathbf{\Gamma}^1_r(\mathsf{k}^{\mathrm{alg}})}(x_r)$. In particular, by (Cay1) and (Cay2), the $F_{g'}$'s are the $\mathsf{k}^{\mathrm{alg}}$-points of algebraic varieties, isomorphic to $\mathbf{C}_{\gamma^1_r(\mathsf{k}^{\mathrm{alg}})}(x_r)$ and hence affine $(r-1)n$-dimensional spaces over $\mathsf{k}^{\mathrm{alg}}$.

Since the reduction map $\eta_{r,1}$ commutes with the Frobenius maps, and since g is assumed fixed by σ, 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 [23], using the fact that F_1 is a connected linear algebraic group over $\mathsf{k}^{\mathrm{alg}}$ (see also [32, I, 2.2] and [17, § 3]). □

Corollary 3.1.12. *Let $x_r \in \mathfrak{g}_r$ be regular and $x_1 = \eta_{r,1}(x_r)$. The restriction of $\eta_{r,1}$ to $\mathbf{C}_{G_r}(x_r)$ is onto $\mathbf{C}_{G_1}(x_1)$.*

Proof. Lemma 3.1.11 and Theorem 3.1.2.(3) imply that for any $g \in \mathbf{C}_{G_1}(x_1)$, there exists an element $h \in \mathbf{C}_{\mathbf{\Gamma}_r}(x_r)$ such that $\eta_{r,1}(h) = g$ and such that $\mathcal{L}_g(h) = h\sigma(h)^{-1} = 1$. In particular, h is fixed under σ and hence $h \in \mathbf{C}_{G_r}(x_r) \cap \eta^{-1}_{r,1}(g)$. □

Another necessary ingredient in the proof of Proposition 3.1.4 is the connection between the groups $\mathbf{C}_{G_r}(x_r)$ and $\mathbf{C}_{G_m}(x_m)$, where $m \leq r$ and $x \in \mathfrak{g}$ is such that x_r is regular.

Lemma 3.1.13. *Let $r \in \mathbb{N}$ and $x_r \in \mathfrak{g}_r$ be regular. For any $1 \leq m \leq r$ write $x_m = \eta_{r,m}(x_r)$.*

1. *The map $\eta_{r,m} : \mathbf{C}_{\mathfrak{g}_r}(x_r) \to \mathbf{C}_{\mathfrak{g}_m}(x_m)$ is surjective.*
2. *The map $\eta_{r,m} : \mathbf{C}_{G_r}(x_r) \to \mathbf{C}_{G_m}(x_m)$ is surjective.*

Proof. We prove both assertions by induction on m.

1. The case $m = 1$ follows in Corollary 3.1.9 and Lang's Theorem, as $\mathbf{C}_{\gamma_1}(x_1)$ and $\eta_{r,1}^*(\mathbf{C}_{\gamma_r}(x_r))$ are both affine n-spaces over $\mathsf{k}^{\mathrm{alg}}$. Consider the commutative diagram in (3.9), in which both rows are exact by induction hypothesis.

$$\begin{array}{ccccccc} \mathbf{C}_{\mathfrak{g}_r^{m-1}}(x_r) & \longrightarrow & \mathbf{C}_{\mathfrak{g}_r}(x_r) & \xrightarrow{\eta_{r,m-1}} & \mathbf{C}_{\mathfrak{g}_{m-1}}(x_{m-1}) & \longrightarrow & 0 \\ \downarrow & & \downarrow{\scriptstyle \eta_{r,m}} & & \| & & \| \\ \mathbf{C}_{\mathfrak{g}_m^{m-1}}(x_m) & \longrightarrow & \mathbf{C}_{\mathfrak{g}_m}(x_m) & \xrightarrow[\eta_{m,m-1}]{} & \mathbf{C}_{\mathfrak{g}_{m-1}}(x_{m-1}) & \longrightarrow & 0 \end{array} \tag{3.9}$$

By the Four Lemma (on epimorphisms), in order to prove the surjectivity of the map $\eta_{r,m} : \mathbf{C}_{\mathfrak{g}_r}(x_r) \to \mathbf{C}_{\mathfrak{g}_m}(x_m)$, it suffices to show that the restricted map $\eta_{r,m} : \mathbf{C}_{\mathfrak{g}_r^{m-1}}(x_r) \to \mathbf{C}_{\mathfrak{g}_m^{m-1}}(x_m)$ 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 $\mathfrak{o}$-module isomorphism $y \mapsto \pi^{m-1}y$ (cf. Lemma 2.3.3), and the map on the left column is surjective by the base of induction.

$$\begin{array}{ccc} \mathbf{C}_{\mathfrak{g}_{r-m+1}}(x_{r-m+1}) & \xrightarrow{\sim} & \mathbf{C}_{\mathfrak{g}_r^{m-1}}(x_r) \\ {\scriptstyle \eta_{r-m+1,1}}\downarrow\!\!\downarrow & & \downarrow{\scriptstyle \eta_{r,m}} \\ \mathbf{C}_{\mathfrak{g}_1}(x_1) & \xrightarrow{\sim} & \mathbf{C}_{\mathfrak{g}_m^{m-1}}(x_m) \end{array} \tag{3.10}$$

2. In the current setting, one invokes Lemma 3.1.11 in order to prove the induction base $m = 1$. The case $m > 1$ 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 $\eta_{r,m} : \mathbf{C}_{G_r^{m-1}}(x_r) \to \mathbf{C}_{G_m^{m-1}}(x_m)$, 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.

$$\begin{array}{ccc} \mathbf{C}_{\mathfrak{g}_r^{m-1}}(x_r) & \xrightarrow{\mathrm{cay}_r} & \mathbf{C}_{G_r^{m-1}}(x_r) \\ {\scriptstyle \eta_{r,m}}\downarrow\!\!\downarrow & & \downarrow{\scriptstyle \eta_{r,m}} \\ \mathbf{C}_{\mathfrak{g}_m^{m-1}}(x_m) & \xrightarrow{\mathrm{cay}_m} & \mathbf{C}_{G_m^{m-1}}(x_m) \end{array} \tag{3.11}$$

□

Proof of Proposition 3.1.4. 1. Given $g_r \in \mathbf{C}_{G_r}(x_r)$ one inductively invokes Lemma 3.1.13 to construct a converging sequence $(g_m)_{m \geq r}$ such that $g_m \in \mathbf{C}_{G_m}(\eta_m(x))$ and such that $\eta_{m',m}(g_{m'}) = g_m$ for all $m' \geq m \geq r$. The limit $g = \lim_m g_m$ is easily verified to be an element of $\mathbf{C}_G(x)$, which is mapped by η_r to g_r.
2. By Theorem 3.1.2, it suffices to consider the case where $x_1 = \eta_1(x) \in \mathbf{g}(\mathsf{k})$ is regular. By [26, (2.5.2)], under this assumption, we have that

$$\dim \mathbf{C}_{\mathbf{G} \times K^{\mathrm{alg}}}(x) = \dim \left(\mathbf{C}_{\mathbf{G} \times \mathfrak{O}}(x) \times K^{\mathrm{unr}}\right) \leq \dim \left(\mathbf{C}_{\mathbf{G} \times \mathfrak{O}}(x) \times \mathsf{k}^{\mathrm{alg}}\right) = \dim \mathbf{C}_{\mathbf{\Gamma}_1}(x_1) = n,$$

as $\mathbf{C}_{\mathbf{G}\times\mathfrak{D}}(x)\times K^{\mathrm{unr}}$ and $\mathbf{C}_{\mathbf{G}\times\mathfrak{D}}(x)\times \mathsf{k}^{\mathrm{alg}}$ are, respectively, the generic and special fiber of $\mathbf{C}_{\mathbf{G}\times\mathfrak{D}}(x)$. On the other hand, by [36, 3.5, Proposition 1], the minimum value of centralizer dimension of an element of $\mathfrak{g}$ is $n=\mathrm{rk}(\mathbf{G})$. Hence, x is regular. □

Finally, we deduce Corollary 3.1.5.

Proof of Corollary 3.1.5. The regularity of x in $\mathfrak{g}$, and Proposition 3.1.10 (applied for $L=K^{\mathrm{alg}}$), imply that the centralizer of x in $\mathbf{G}(K^{\mathrm{alg}})$ is an abelian group. In particular, it follows from this that the group $\mathbf{C}_G(x)$ is abelian as well, and consequently, by Proposition 3.1.4.(1), so are its quotient groups $\mathbf{C}_{G_r}(x_r)$ for all $r\in\mathbb{N}$. □

3.2. Regular characters

At this point, our description of the regular elements of the Lie-algebras $\mathfrak{g}_r$ 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 [22, Theorem 3.1].

Theorem 3.2.1. *Let $\Omega\subseteq\mathfrak{g}_1$ be a regular orbit and let $r\in\mathbb{N}$ and $m=\lfloor\frac{r}{2}\rfloor$.*

1. *The set $\mathrm{Irr}(G_r^m\mid\Omega)$ of characters of $G_r^m=\mathrm{Ker}(G_r\to G_m)$ which lie above the regular orbit Ω consists of exactly $q^{n(r-m-1)}$ orbits for the coadjoint action of G_r.*
2. *Given a character $\sigma\in\mathrm{Irr}(G_r^m\mid\Omega)$, the set of irreducible characters of G_r whose restriction to G_r^m has σ as a constituent is in bijection with the Pontryagin dual of $\mathbf{C}_{G_m}(x_m)$, for $x_m\in\mathfrak{g}_m$ any element such that $\eta_{m,1}(x_m)\in\Omega$.*
3. *Any such character $\sigma\in\mathrm{Irr}(G_r^m\mid\Omega)$ extends to its inertia group $I_{G_r}(\sigma)$. In particular, each such extension induces to a regular character of G_r.*

Note that the first assertion of Theorem I follows from Assertions (1) and (2) of Theorem 3.2.1 and Corollary 3.1.12. The second assertion of Theorem I follows from the Assertion (3) of Theorem 3.2.1 and (3.17) below.

The proof of Theorem 3.2.1 follows the same path as [22, § 3]. For the sake of brevity, rather then rehashing the proof appearing in great detail in [22], 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 [22] to the current setting.

Recall that the group $G=\mathbf{G}(\mathfrak{o})$ and $\mathfrak{g}=\mathbf{g}(\mathfrak{o})$ are naturally embedded in the matrix algebra $\mathrm{M}_N(\mathfrak{o})$ (see Section 2.1). Similarly, the congruence quotients G_r and $\mathfrak{g}_r$ are embedded in $\mathrm{M}_N(\mathfrak{o}_r)$. From here on, all computation 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 $\mathfrak{g}=\mathbf{g}(\mathfrak{o})\subseteq\mathrm{M}_N(\mathfrak{o})$ is endowed with a symmetric bilinear $G(\mathfrak{o})$-invariant form

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

Note that, by the assumption $p=\mathrm{char}(\mathsf{k})$ is odd, the form κ reduces to a non-degenerate form on $\mathfrak{g}_1$ (see [32, Lemma 5.3]), and hence $\{x\in\mathfrak{g}\mid\kappa(x,y)\in\mathfrak{p}\text{ for all }y\in\mathfrak{g}\}=\pi\mathfrak{g}$. Fixing a non-trivial character $\psi:K\to\mathbb{C}^\times$ with conductor $\mathfrak{o}$ (see e.g. [2, § 5.3]), for any $r\in\mathbb{N}$, we have a well-defined map

$$\mathfrak{g}_r\to\widehat{\mathfrak{g}_r},\quad y\mapsto\varphi_y\text{ where }\varphi_y(x)=\psi(\pi^{-r}\kappa(x,y)).\tag{3.12}$$

Furthermore, by the assumption $\pi^{-1}\mathfrak{o} \nsubseteq \mathrm{Ker}(\psi)$, the map above induces a G_r-equivariant bijection of $\mathfrak{g}_r$ with its Pontryagin dual $\widehat{\mathfrak{g}_r}$.

3.2.2. Exponential and logarithm

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

$$\exp(x) = 1 + x + \frac{1}{2}x^2 \quad (x \in \mathfrak{g}_r^m),$$

is a well-defined bijection of $\mathfrak{g}_r^m$ onto the group G_r^m, and is equivariant with respect to the adjoint action of G_r, with an inverse map given by

$$\log(1 + x) = x - \frac{1}{2}x^2 \quad (1 + x \in G_r^m).$$

In the case where $\frac{r}{2} \leq m$, the exponential map is simply given by $\exp(x) = 1 + x$ and defines an isomorphism of abelian groups $\mathfrak{g}_r^m \xrightarrow{\sim} G_r^m$. In the more general setting we have the following.

Lemma 3.2.2. *Let $m, r \in \mathbb{N}$ be such that $\frac{r}{3} \leq m \leq r$. For any $x, y \in \mathfrak{g}_r^m$,*

$$\log\left((\exp(x), \exp(y))\right) = [x, y]\,,$$

where $(\exp(x), \exp(y))$ denotes the group commutator of $\exp(x)$ and $\exp(y)$ in G_r^m. Furthermore, the following truncated version of the Baker–Campbell–Hausdorff formula holds

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

The formulae in Lemma 3.2.2 may be verified by direct computation; their proof is omitted.

3.2.3. Characters of $G_r^{\lfloor r/2 \rfloor}$

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

$$\Phi \quad : \quad \mathfrak{g}_{m'} \to \widehat{\mathfrak{g}_{m'}} \to \widehat{\mathfrak{g}_r^m} \to \mathrm{Irr}(G_r^m), \tag{3.13}$$

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

Lemma 3.2.3. *Assume $r = 2m$ is even. The map Φ defined in (3.13) is a G_r-equivariant bijection of $\mathrm{Irr}(G_r^{m'})$ and $\mathfrak{g}_{m'}$.*

In the case where $r = 2m' + 1$, the irreducible characters of $G_r^{m'}$ are classified in terms of their restriction to G_r^m, using the method of Heisenberg lifts, which we briefly recall here. For a more elaborate survey we refer to [22, § 3.2] and [9, Ch. 8].

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

$$B_\vartheta : G_r^{m'}/G_r^m \times G_r^{m'}/G_r^m \to \mathbb{C}^\times, \quad B_\vartheta(x_1 G_r^m, x_2 G_r^m) = \vartheta\left((x_1, x_2)\right).$$

Using the definition of $\Phi(y) = \vartheta$ and the explicit isomorphism $x \mapsto \exp(\pi^r x) : \mathfrak{g}_1 \to G_m^{m'} = G_r^{m'}/G_r^m$, we obtain an alternating bilinear form $\beta_y : \mathfrak{g}_1 \times \mathfrak{g}_1 \to \mathsf{k}$ given by $\beta_y(x_1, x_2) = \mathrm{Tr}(\eta_{m',1}(y) \cdot [x_1, x_2])$, such that the diagram in (3.14) commutes.

$$\begin{array}{ccccc} G_m^{m'} & \times & G_m^{m'} & \xrightarrow{B_\vartheta} & \mathbb{C}^\times \\ \uparrow\wr & & \uparrow\wr & & \uparrow{\scriptstyle \psi(\pi^{-1}(\cdot))} \\ \mathfrak{g}_1 & \times & \mathfrak{g}_1 & \xrightarrow{\beta_y} & \mathsf{k} \end{array} \tag{3.14}$$

A short computation, using the non-degeneracy of the trace and the definition of β_y, shows that the radical of this form coincides with the centralizer sub-algebra $\mathbf{C}_{\mathfrak{g}_1}(\eta_{m',1}(y))$ of $\mathfrak{g}_1$ (see [22, p. 125]). Let $\mathfrak{R}_y$ and R_y denote the preimages of $\mathfrak{m}_y$ in $\mathfrak{g}_r^{m'}$ and in $G_r^{m'}$ under the associated quotient maps. Let $\mathfrak{m}_y \subseteq \mathfrak{j} \subseteq \mathfrak{g}_1$ be a maximal subspace such that $\beta_y(\mathfrak{j}, \mathfrak{j}) = \{0\}$ (i.e. such that $\mathfrak{j}/\mathfrak{m}_y$ is a maximal isotropic subspace of $\mathfrak{g}_1/\mathfrak{m}_y$), and let $\mathfrak{J} \subseteq \mathfrak{g}_r^{m'}$ and $J \subseteq G_r^{m'}$ be the corresponding preimages of $\mathfrak{j}$; see (3.15).

$$\begin{array}{ccccc} G_r^{m'} & \overset{\log}{\dashrightarrow} & \mathfrak{g}_r^{m'} & \longrightarrow & \mathfrak{g}_1 \\ | & & | & & | \\ J & \overset{\log}{\dashrightarrow} & \mathfrak{J} & \longrightarrow & \mathfrak{j} \\ | & & | & & | \\ R_y & \overset{\log}{\dashrightarrow} & \mathfrak{R}_y & \longrightarrow & \mathfrak{m}_y \\ | & & | & & | \\ G_r^m & \underset{\log}{\xrightarrow{\sim}} & \mathfrak{g}_r^m & \longrightarrow & 0 \end{array} \tag{3.15}$$

Let $\theta = \vartheta \circ \exp$ be the pull-back of ϑ to $\mathfrak{g}_r^m$. By virtue of the commutativity of $\mathfrak{R}_y$, the character θ' extends to a character of $\mathfrak{R}_y$ in $|\mathfrak{R}_y : G_r^m| = |\mathfrak{m}_y|$ many ways. By Lemma 3.2.2, given such an extension $\theta' \in \widehat{\mathfrak{R}_y}$, the map $\vartheta' : R_y \to \mathbb{C}^\times$ is a character of R_y. Thus, the character ϑ admits $|\mathfrak{m}_y|$ many extensions to R_y.

Lemma 3.2.4.

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

Proof. The triple $(G_r^{m'}, R_y, \vartheta')$ satisfies the hypothesis of [9, § 8.3], and the alternating bilinear form β_y (which corresponds to h_χ in the notation of [9]) reduces to a non-degenerate form on the elementary abelian group $G_r^{m'}/R_y \simeq \mathfrak{g}_1/\mathfrak{r}_y$. The subgroup $J \subseteq G_r^{m'}$ may be identified with the group denoted in [9, Proposition 8.3.3] by G_1, and the extension of ϑ' to an irreducible character of J exists by virtue of $J/\mathrm{Ker}(\vartheta')$ being finite and abelian. The irreducibility and independence of the choice of J are shown within the proof of [9, Proposition 8.3.3], as well as uniqueness of σ as the only irreducible character of $G_r^{m'}$ whose restriction to R_y contains ϑ'. The final assertion, that all characters of $G_r^{m'}$ lying above ϑ are obtained in this manner is obvious, as the restriction of any such character of $G_r^{m'}$ to R_y necessarily contains an extension ϑ' of ϑ. □

3.2.4. Inertia subgroups in $\mathbf{G}(\mathfrak{o}_r)$ of regular characters

The final ingredient required in order to implement the construction of [22] to the current setting is a structural description of the inertia subgroup of a character of $G_r^{\lceil r/2 \rceil}$ lying below a regular character of level $\ell = r+1$. As in the previous section, put $m' = \lfloor \frac{r}{2} \rfloor$ and $m = \lceil \frac{r}{2} \rceil$, and let $\vartheta \in \mathrm{Irr}(G_r^m)$. Recall that the inertia subgroup of ϑ in G_r is defined by

$$I_{G_r}(\vartheta) = \left\{ g \in G_r \mid \vartheta(g^{-1}xg) = \vartheta(x) \text{ for all } x \in G_r^m \right\}. \tag{3.16}$$

By Section 3.2.3, there exists a unique $y \in \mathfrak{g}_{m'}$ such that $\vartheta = \Phi(y)$. Moreover, letting $\hat{y}_r \in \mathfrak{g}_r$ be an arbitrary lift of $y_{m'}$ to $\mathfrak{g}_r$, we have that

$$I_{G_r}(\vartheta) = G_r^m \cdot \mathbf{C}_{G_r}(\hat{y}_r). \tag{3.17}$$

Indeed, the only non-trivial step to proving (3.17) is the inclusion $\subseteq$, which from follows Lemma 3.1.13, as both hands of the equation are mapped by $\eta_{r,m}$ onto the group $\mathbf{C}_{G_m}(\eta_{r,m}(\hat{y}_r))$.

Proof of Theorem 3.2.1. A short computation, proves that the set $\tilde{\Omega} = \eta_{m',1}^{-1}(\Omega)$ consists of $q^{n(m'-1)}$ distinct adjoint orbits for the action of $G_{m'}$, and hence for the action of G_r as well. Indeed, $\tilde{\Omega}$ is a $G_{m'}$-stable set of order $|\Omega| \cdot \left|G_{m'}^1\right| = |\Omega|\, q^{d(m'-1)}$, invoking the bijection $\mathfrak{g}_{m'}^1 \to G_{m'}^1$ induced by the Cayley map, and each of the orbits $G_{m'}$-orbits in $\tilde{\Omega}$ has cardinality

$$\left|G_{m'} : \mathbf{C}_{G_{m'}}(x)\right| = |G_1 : \mathbf{C}_{G_1}(\eta_{m',1}(x))| \cdot \left|G_{m'}^1 : \mathbf{C}_{G_{m'}^1}(x)\right| = |\Omega| \cdot q^{(d-n)(m'-1)},$$

by Corollary 3.1.12, for any $x \in \tilde{\Omega}$. By the G_r-equivariance of the map Φ, defined in Section 3.2.3, it follows that the set $\mathrm{Irr}(G_r^m \mid \Omega)$ consists of $q^{n(m'-1)}$ coadjoint orbits of G_r. In the case where r is even, the first assertion of Theorem 3.2.1 follows from Lemma 3.2.3, since $m = r-m$. In the case of r odd, by Lemma 3.2.4, and by regularity of the elements of Ω, any character in $\mathrm{Irr}(G_r^m \mid \Omega)$ extends to $G_r^{m'}$ in exactly q^n-many ways. Thus, the number of coadjoint G_r-orbits in $\mathrm{Irr}(G_r^{m'})$ is $q^{n(m'-1)+n} = q^{n(r-m'-1)}$, whence the first assertion.

The second assertion of Theorem 3.2.1 follows from the third assertion, (3.17) and [21, Corollary 6.17].

Lastly, for the proof of the third assertion of Theorem 3.2.1, we refer to [22, § 3.5] for the explicit construction, in the analogous case of $\mathrm{GL}_n(\mathfrak{o})$ and $\mathrm{U}_n(\mathfrak{o})$, of an extension of a character $\sigma \in \mathrm{Irr}(G_r^{m'})$ to its inertia subgroup $I_{G_r}(\sigma)$. Note that the construction of [22] can be applied verbatim to the present setting, invoking the fact the $I_{G_r}(\sigma)$ is generated by two abelian subgroups, one of which is normal in G_r ((3.17) and Corollary 3.1.5) 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 $\mathsf{B}_n, \mathsf{C}_n$ and D_n. Following Corollary 1.3.1, to do so, we classify the regular orbits in the space of orbits $\mathrm{Ad}(G_1)\backslash\mathfrak{g}_1$ and compute their cardinalities, in order to obtain a formula for the Dirichlet polynomial

$$\mathfrak{D}_{\mathfrak{g}}(s) = \sum_{\Omega \in X} |G_1| \cdot |\Omega|^{-(s+1)}.$$

As it turns out, the cases where $\mathbf{G}$ is of type B_n or C_n, i.e. $\mathbf{G} = \mathrm{SO}_{2n+1}$ or $\mathbf{G} = \mathrm{Sp}_{2n}$, can be handled simultaneously, and are analyzed in Section 4.3. The case of the groups of the form 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 $\mathfrak{sp}_{2n}(\mathsf{k})$ and $\mathfrak{so}_{2n+1}(\mathsf{k})$ is equivalent to it being give by a regular matrix in $\mathrm{M}_N(\mathsf{k})$; see Proposition 4.3.4 (also, cf. [38, § 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 $x, y \in \mathrm{M}_N(\mathsf{k})$ are said to be **similar** if there exists a matrix $g \in \mathrm{GL}_N(\mathsf{k})$ such that $y = gxg^{-1}$. Our description of regular orbits of $\mathfrak{g}_1$ follows the following steps.

1. Classification of all similarity classes in $\mathfrak{gl}_N(\mathsf{k})$ 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 $\mathrm{Ad}(G_1)$-orbits;
3. Computation of the cardinality of the $\mathrm{Ad}(G_1)$-orbit of each regular element.

A rich theory of centralizers and conjugacy classes in classical groups over finite fields already exists, most notably Wall's extensive analysis in [39, § 2.6]. The enumeration of elements of a finite classical group G_1 whose representing matrix is cyclic (i.e. regular when considered as an element of $\mathrm{GL}_N(\mathsf{k}^{\mathrm{alg}})$) was addressed in [28] and [15] where the proportion of such elements in G_1, for all classical groups, was estimated and its limit as $\mathrm{rk}(\mathbf{G})$ tends to infinit was computed using generating functions. The precise number of regular semisimple conjugacy classes was computed, again using generating functions, in [14], where the discrepancy between regularity of semisimple elements of the even dimensional orthogonal groups and of regularity of their representing matrices in $\mathrm{GL}_N(\mathsf{k}^{\mathrm{alg}})$ is determined (see [14, Lemma 5.1]). In the case of the symplectic group, the equivalence of regularity of an element of $\mathrm{Sp}_{2n}(\mathsf{k})$ and of its representing matrix in $\mathrm{GL}_{2n}(\mathsf{k}^{\mathrm{alg}})$ was noted in [15, § 1.1]. Examples of regular elements of $\mathrm{SO}_{2n}(\mathsf{k})$ which do not satisfy this equivalence appear in [27, Note 8.1].

The setting considered in the present manuscript, while akin to, is rather simpler than the one dealt with in [39]. Namely, the relatively simpler theory of centralizers for the adjoint action of $\mathbf{G}(\mathsf{k}^{\mathrm{alg}})$ on $\mathbf{g}(\mathsf{k}^{\mathrm{alg}})$, in comparison with that of $\mathbf{G}(\mathsf{k}^{\mathrm{alg}})$ on itself by conjugation (compare, for example, Proposition 2.1.1 and [20, § 2.14]), allows one to retrace much of Wall's analysis in the Lie-algebra setting, without having to invoke the notion of *multipliers* (see [39, p. 11]). Furthermore, the focus on *regular* adjoint classes results in a fairly "well-behaved" elementary divisor decomposition of the elements in the orbits under inspection. We also remark that steps (1), (2) and (3) above are in direct parallel with items (i), (ii) and (iv), respectively, of [39, § 2.6.(B) and (C)], and may be derived from [39] by the following procedure. Given $x \in \mathrm{M}_N(\mathsf{k})$ let $\lambda \in \mathsf{k}$ be such that $x - \lambda\mathbf{1}$ is a non-singular matrix, and consider the dilated Cayley transform $g_x = (x-\lambda\mathbf{1})^{-1}(x+\lambda\mathbf{1})$. Then x is similar to an element of $\mathfrak{g}_1$ if and only if g_x is similar to an element of G_1, and the map $x' \mapsto (x'-\lambda\mathbf{1})(x'+\lambda\mathbf{1})$ is a bijection between the adjoint orbit of x under $\mathrm{GL}_N(\mathsf{k})$ (resp. under G_1), and the similarity (resp. adjoint) class of g_x. However, applying such an argument necessitates imposing additional restrictions on the characteristic of k, and is somewhat less suitable for the purpose of enumeration of regular classes. Given these complications, and the relative simplicity of the adjoint classes in question, we have opted to present a self-contained and independent analysis of the regular adjoint classes in $\mathfrak{g}_1$, which is presented in Sections 4.2-4.4 below.

4.1.1. Enumerative set-up

Definition 4.1.1 *(Type of a polynomial).* Let $f(t) \in \mathsf{k}[t]$ 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 τ 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 $\boldsymbol{\tau}(f) = (r(f), S(f), T(f))$, 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 $\mathcal{X}_n$ denotes the set of triplets $\boldsymbol{\tau} = (r, S, T) \in \mathbb{N}_0 \times \mathrm{M}_n(\mathbb{N}_0) \times \mathrm{M}_n(\mathbb{N}_0)$, 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 $\boldsymbol{\tau}(f) \in \mathcal{X}_n$ 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 $w_d(t) = \frac{1}{d} \sum_{r|d} \mu\left(\frac{d}{r}\right) t^d$, where $\mu(\cdot)$ is the Möbius function (see, e.g., [13, Ch. 14]). A polynomial $f \in \mathsf{k}[t]$ 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

$$E_d(t) = \begin{cases} \frac{1}{d} \displaystyle\sum_{m|d\,,\ m \text{ odd}} \mu(m)\left(t^{d/2m} - 1\right) & \text{if } d \text{ is even} \\ 0 & \text{otherwise;} \end{cases} \tag{4.1}$$

cf. [8, Lemma 3.2], noting that the set of monic irreducible even polynomials of degree d is in bijection with the set $N^{*1}(d, q) \subseteq \mathsf{k}[t]$, defined in [8], via the map $f(t) \mapsto \frac{(1+t)^{\deg f}}{f(-1)} f(\frac{1-t}{1+t})$.

Put

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

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 $\boldsymbol{\tau} \in \mathcal{X}_n$, the number of polynomials $f \in \mathsf{k}[t]$ of type $\boldsymbol{\tau}(f)$ such that $f(-t) = (-1)^N f(t)$ is given by evaluation at $t = q$ of the polynomial

$$M_{\boldsymbol{\tau}}(t) = \left(\frac{1}{2}\right)^{\sum_{d,e} T_{d,e}} \prod_{d=1}^{n} \binom{\sum_e S_{d,e}}{S_{d,1}, S_{d,2}, \ldots, S_{d,n}} \cdot \binom{E_{2d}(t)}{\sum_e S_{d,e}} \cdot \binom{\sum_e T_{d,e}}{T_{d,1}, T_{d,2}, \ldots, T_{d,n}} \cdot \binom{P_d(t)}{\sum_e T_{d,e}}. \tag{4.3}$$

The combinatorial data described above is utilized in Theorem II and Theorem III, where it allows to enumerate the similarity classes in $\mathrm{M}_N(\mathsf{k})$ which meet the Lie-algebra $\mathfrak{g}_1$ non-trivially in terms of the minimal polynomial of the class elements. The classification of such similarity classes and their decomposition into $\mathrm{Ad}(G_1)$ is described Theorem 4.1.2 and Theorem 4.1.3 below.

Once Theorems 4.1.2 and 4.1.3 are proved, the proof of Theorem II and of 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* $\mathrm{char}(\mathsf{k}) \neq 2$. *Let* $V = \mathsf{k}^N$ *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* $\mathbf{G} \in \{\mathrm{Sp}_{2n}, \mathrm{SO}_{2n+1}\}$ *be the algebraic group of isometries of* V *with respect to* B *and put* $G_1 = \mathbf{G}(\mathsf{k})$ *and* $\mathfrak{g}_1 = \mathbf{g}(\mathsf{k})$ *where* $\mathbf{g} = \mathrm{Lie}(\mathbf{G})$.

Let $x \in \mathrm{M}_N(\mathsf{k})$ *have minimal polynomial* $m_x \in \mathsf{k}[t]$.

1. *The element x is similar to a regular element of $\mathfrak{g}_1$ if and only if m_x has degree N and satisfies $m_x(-t) = (-1)^N m_x(t)$.*

Furthermore, assume $x \in \mathfrak{g}_1$ is a regular element and let $\Omega = \mathrm{Ad}(G_1)x$ denote its orbit under G_1.

2. *If N is even and $m_x(0) = 0$, then the intersection $\mathrm{Ad}(\mathrm{GL}_N(\mathsf{k}))x \cap \mathfrak{g}_1$ is the union of two distinct $\mathrm{Ad}(G_1)$-orbits. Otherwise, $\mathrm{Ad}(\mathrm{GL}_N(\mathsf{k}))x \cap \mathfrak{g}_1 = \Omega$.*
3. *Let $\boldsymbol{\tau} = \boldsymbol{\tau}(m_x) = (r(m_x), S(m_x), T(m_x))$ as in Definition 4.1.1. Then*

$$|\Omega| = q^{2n^2} \cdot \left(\frac{1}{2}\right)^{\nu} \frac{\prod_{i=1}^{n}(1-q^{-2i})}{\prod_{1\le d,e\le n}(1+q^{-d})^{S_{d,e}(m_x)} \cdot (1-q^{-d})^{T_{d,e}(m_x)}},$$

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 $|\mathsf{k}| > 3$ and $\mathrm{char}(\mathsf{k}) \neq 2$. Let $N = 2n$ with $n \geq 2$. Let $V = \mathsf{k}^N$ 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 $\mathbf{G}^\epsilon = \mathrm{SO}^\epsilon_{2n}$ be the k-algebraic group of isometries of V with respect to B^ϵ and put $G_1^\epsilon = \mathbf{G}_1^\epsilon(\mathsf{k})$ and let $\mathfrak{g}_1^\epsilon = \mathbf{g}^\epsilon(\mathsf{k})$, where $\mathbf{g}^\epsilon = \mathrm{Lie}(\mathbf{G})$.*

Let $x \in \mathrm{M}_N(\mathsf{k})$ 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 $\mathfrak{g}_1^+$.*
   (c) *The element x is similar to a regular element of $\mathfrak{g}_1^-$.*
   Otherwise, if $m_x(0) \neq 0$, let $\epsilon = \epsilon(x) = (-1)^{\sum_e e S_{d,e}(m_x)}$ where $S = (S_{d,e}(m_x))$ is as in Definition 4.1.1. Then x is similar to a regular element of $\mathfrak{g}_1^\epsilon$ 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 $\mathfrak{g}_1^{-\epsilon}$.

Furthermore, assume $x \in \mathfrak{g}_1^\epsilon$ is a regular element and let $\Omega^\epsilon = \mathrm{Ad}(G_1^\epsilon)x$ denote its orbit under G_1^ϵ, for $\epsilon \in \{\pm 1\}$ fixed.

2. *In the case where $m_x(0) = 0$, the intersection $\mathrm{Ad}(\mathrm{GL}_N(\mathsf{k}))x \cap \mathfrak{g}_1^\epsilon$ is the disjoint union of two distinct $\mathrm{Ad}(G_1^\epsilon)$-orbits. Otherwise, $\mathrm{Ad}(\mathrm{GL}_N(\mathsf{k}))x \cap \mathfrak{g}_1^\epsilon = \Omega^\epsilon$.*
3. (a) *Assume $m_x(0) = 0$ and let $\boldsymbol{\tau} = \boldsymbol{\tau}(t \cdot m_x)$. Then*

$$|\Omega^\epsilon| = q^{2n^2} \cdot \frac{1}{2} \cdot \frac{(1+\epsilon q^{-n})\prod_{i=1}^{n-1}(1-q^{-2i})}{\prod_{1\le d,e\le n}(1+q^{-d})^{S_{d,e}(m_x)} \cdot (1-q^{-d})^{T_{d,e}(m_x)}}.$$

   (b) *Otherwise, let $\boldsymbol{\tau} = \boldsymbol{\tau}(m_x)$. Then*

$$|\Omega^\epsilon| = q^{2n^2} \cdot \frac{(1+\epsilon q^{-n})\prod_{i=1}^{n-1}(1-q^{-2i})}{\prod_{1\le d,e\le n}(1+q^{-d})^{S_{d,e}(m_x)} \cdot (1-q^{-d})^{T_{d,e}(m_x)}}.$$

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 $\mathsf{k} = \mathbb{F}_3$ 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 $x \in \mathbf{g}(\mathsf{k}^{\mathrm{alg}}) \subseteq \mathfrak{gl}_N(\mathsf{k}^{\mathrm{alg}})$ be non-singular. Then x is regular in $\mathbf{g}(\mathsf{k}^{\mathrm{alg}})$ if and only if x is a regular element of $\mathfrak{gl}_N(\mathsf{k}^{\mathrm{alg}})$.*

Proof. Let $W = (\mathsf{k}^{\mathrm{alg}})^N$, so that $\mathbf{g}(\mathsf{k}^{\mathrm{alg}})$ is given as the Lie-algebra of anti-symmetric operators with respect to a non-degenerate bilinear form $B = B_{\mathsf{k}^{\mathrm{alg}}}$ on W (see Section 2.1). Note that the existence of non-singular elements in $\mathbf{g}(\mathsf{k}^{\mathrm{alg}})$ implies that $N = 2n$ is even. Indeed, $x \in \mathbf{g}(\mathsf{k}^{\mathrm{alg}})$ if and only if $x^\star = -x$ (notation of Section 2.1.1), and $\det(x) = \det(x^\star) = (-1)^N \det(x)$ is possible if and only if N is even, since $\mathrm{char}(\mathsf{k}^{\mathrm{alg}}) \neq 2$.

Let $x = s + h$ be the Jordan decomposition of x, with $s, h \in \mathbf{g}(\mathsf{k}^{\mathrm{alg}})$, s semisimple, h nilpotent and $[s, h] = 0$. Let $\lambda_1, \ldots, \lambda_t \in \mathsf{k}^{\mathrm{alg}}$ 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_{λ_i} and $W_{-\lambda_i}$ are maximal isotropic. Comparing centralizer dimension, and invoking [36, § 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 $\mathfrak{gl}_N(W_{[\lambda_i]})$. Likewise, x is regular in $\mathbf{g}(\mathsf{k}^{\mathrm{alg}})$ 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 $B_{\mathsf{k}^{\mathrm{alg}}}$ 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 eigenbasis, it be identified with the block-diagonal matrix $\mathrm{diag}(\lambda\mathbf{1}_n, -\lambda\mathbf{1}_n)$. Under this identification, the centralizer of s in $\mathfrak{gl}_N(\mathsf{k}^{\mathrm{alg}})$ is identified with the subgroup of block diagonal matrices consisting of two $n \times n$ blocks. Moreover, the involution $\star$ maps an element $\mathrm{diag}(y_1, y_2) \in \mathbf{C}_{\mathfrak{gl}_N(\mathsf{k}^{\mathrm{alg}})}(s)$, with $y_1, y_2 \in \mathfrak{gl}_n(\mathsf{k}^{\mathrm{alg}})$ to the matrix $\mathrm{diag}(y_2^t, y_1^t)$. In particular, it follows that $h \in \mathbf{C}_{\mathfrak{gl}_N}(\mathsf{k}^{\mathrm{alg}}) \cap \mathbf{g}(\mathsf{k}^{\mathrm{alg}})$ is of the form $h = \mathrm{diag}(h_1, -h_1^t)$, where $h_1 \in \mathfrak{gl}_n(\mathsf{k}^{\mathrm{alg}})$ is nilpotent. Arguing as in [32, III, § 1], we have that

$$\mathbf{C}_{\mathrm{GL}_N}(x) = \mathbf{C}_{\mathbf{C}_{\mathrm{GL}_N}(s)}(h) \simeq \mathbf{C}_{\mathrm{GL}_n}(h_1) \times \mathbf{C}_{\mathrm{GL}_n}(-h_1^t) \simeq \mathbf{C}_{\mathrm{GL}_n}(h_1) \times \mathbf{C}_{\mathrm{GL}_n}(h_1)$$

where the final isomorphism utilizes the isomorphism $y \mapsto (y^t)^{-1} : \mathbf{C}_{\mathrm{GL}_n}(-h_1^t) \to \mathbf{C}_{\mathrm{GL}_n}(h_1)$.

Finally, since the group $\mathbf{G}$ is embedded in GL_N as the group of unitary elements with respect to $\star$, we have $\mathrm{diag}(y_1, y_2) \in \mathbf{C}_{\mathrm{GL}_N(\mathsf{k}^{\mathrm{alg}})}(s) \cap \mathbf{G}(\mathsf{k}^{\mathrm{alg}})$ if and only if $y_2 = (y_1^t)^{-1}$, and hence the map $y \mapsto \mathrm{diag}(y, (y^t)^{-1})$ is an isomorphism of $\mathbf{C}_{\mathrm{GL}_n}(h_1)$ onto $\mathbf{C}_{\mathbf{C}_{\mathbf{G}}(s)}(h)$ and hence

$$\mathbf{C}_{\mathbf{G}}(x) = \mathbf{C}_{\mathbf{C}_{\mathbf{G}}(s)}(h) \simeq \mathbf{C}_{\mathrm{GL}_n}(h_1).$$

Thus

$$\dim \mathbf{C}_{\mathrm{GL}_N}(x) = 2 \dim \mathbf{C}_{\mathrm{GL}_n}(h_1) = 2 \dim \mathbf{C}_{\mathbf{G}}(x),$$

and the lemma follows. □

Remark 4.2.2. 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 $\boldsymbol{\gamma}_1(\mathsf{k}^{\mathrm{alg}})$ in $\boldsymbol{\Gamma}_1(\mathsf{k}^{\mathrm{alg}})$ is a direct product of groups of the form $\mathrm{GL}_{m_j}(\mathsf{k}^{\mathrm{alg}})$ (see Proposition 2.1.1). 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 $\Pi_x = \mathrm{Ad}(\mathrm{GL}_N(\mathsf{k}))x \cap \mathfrak{g}_1$, for $x \in \mathfrak{g}_1$ regular, in to $\mathrm{Ad}(G_1)$-orbits. The results appearing below can also be derived from [39, § 2.6]. However, as the case of regular elements of the Lie-algebra $\mathfrak{g}_1$ allows for a much more transparent argument, we present it here for completeness.

Let $\mathrm{Sym}(\star; x)$ be the set of elements $Q \in \mathbf{C}_{\mathrm{GL}_N(\mathsf{k})}(x)$ such that $Q^\star = Q$ and define an equivalence relation on $\mathrm{Sym}(\star; x)$ by

$$Q_1 \sim Q_2 \quad \text{if there exists } a \in \mathbf{C}_{\mathrm{GL}_N(\mathsf{k})}(x) \text{ such that } Q_1 = a^\star Q_2 a. \tag{4.4}$$

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

Proposition 4.2.3. *Let $x \in \mathfrak{g}_1$ and let Π_x denote the intersection $\mathrm{Ad}(\mathrm{GL}_N(\mathsf{k}))x \cap \mathfrak{g}_1$. There exists a map $\Lambda : \Pi_x \to \Theta_x$ such that $y_1, y_2 \in \Pi_x$ are $\mathrm{Ad}(G_1)$-conjugate if and only if $\Lambda(y_1) = \Lambda(y_2)$.*

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

Define $\Lambda(y)$ to be the equivalence class of Q in Θ_x. To show that Λ is well-defined, let $w' \in \mathrm{GL}_N(\mathsf{k})$ be another element such that $y = w'xw'^{-1}$ and $Q' = w'^\star w'$. Put $a = w^{-1}w'$. Then a commutes with x, and

$$a^\star Q a = w'^\star (w^\star)^{-1} Q w^{-1} w' = w'^\star w' = Q',$$

hence $Q \sim Q'$.

2. *Proof that $y_1, y_2 \in \Pi_x$ are $\mathrm{Ad}(G_1)$-conjugate if $\Lambda(y_1) = \Lambda(y_2)$.* Let $w_1, w_2 \in \mathrm{GL}_N(\mathsf{k})$ be such that $y_i = w_i x w_i^{-1}$, and let $Q_i = w_i^\star w_i$ $(i = 1, 2)$. Then, by assumption, there exists $a \in \mathbf{C}_{\mathrm{GL}_N(\mathsf{k})}(x)$ such that $Q_2 = a^\star Q_1 a$. Put $z = w_1 a w_2^{-1}$. Note that $z y_2 z^{-1} = y_1$. We claim that $z \in G_1$. This holds since for any $u, v \in V$

$$\begin{aligned} B(zu, zv) &= B(w_1 a w_2^{-1} u, w_1 a w_2^{-1} v) = B(a^\star (w_1^\star w_1) a w_2^{-1} u, w_2^{-1} v) \\ &= B(a^\star Q_1 a w_2^{-1} u, w_2^{-1} v) = B(Q_2 w_2^{-1} u, w_2^{-1} v) \qquad \text{(since } Q_2 = a^\star Q_1 a\text{)} \\ &= B(w_2^\star u, w_2^{-1} v) = B(u, v). \end{aligned}$$

3. *Proof that $y_1, y_2 \in \Pi_x$ are $\mathrm{Ad}(G_1)$-conjugate only if $\Lambda(y_1) = \Lambda(y_2)$.* Assume now that $z \in G_1$ is such that $y_1 = z y_2 z^{-1}$, and let $w_1, w_2 \in \mathrm{GL}_N(\mathsf{k})$ be such that $y_i = w_i x w_i^{-1}$ $(i = 1, 2)$. Then w_1 and $z w_2$ both conjugate x to y_1, and hence, by the unambiguity of the definition of Λ and fact that $z \in G_1$, we have that

$$\Lambda(y_1) = [w_1^\star w_1] = [w_2^\star (z^\star z) w_2] = [w_2^\star w_2] = \Lambda(y_2). \quad \square$$

A crucial property of the set Θ_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 Π_x decomposes into $|\mathrm{Im}\Lambda|$ many $\mathrm{Ad}(G_1)$-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 Θ_x.

Lemma 4.2.4. *Let $\mathcal{C} \subseteq \mathrm{M}_N(\mathsf{k})$ be the ring of matrices commuting with a matrix x, with $x^\star = -x$ (or $x^\star = x$), and let $\mathcal{N} \lhd \mathcal{C}$ be a nilpotent ideal, invariant under $\star$. The following are equivalent, for any $Q_1, Q_2 \in \mathrm{Sym}(\star; x)$.*

1. *There exists $a \in \mathcal{C}$ such that $a^\star Q_1 a = Q_2$;*
2. *There exists $a \in \mathcal{C}$ such that $a^\star Q_1 a \equiv Q_2 \pmod{\mathcal{N}}$.*

Proof. The argument of [39, Theorem 2.2.1] applies to the case where $\mathcal{N}$ is any nilpotent ideal which is invariant under $\star$, provided that the required trace condition holds. In the present case the condition holds since $\mathrm{char}(\mathsf{k}) \neq 2$. □

4.2.3. Similarity classes via bilinear forms

We recall a basic lemma which would allow us to determine when an element of $\mathfrak{gl}_N(\mathsf{k})$ 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 $x \in \mathrm{End}(V)$ C-**anti-symmetric**, if $C(xu, v) + C(u, xv) = 0$ holds for all $u, v \in V$.

Lemma 4.2.5. *Let C_1, C_2 be two non-degenerate bilinear forms on a vector space $V = \mathsf{k}^N$, and assume there exists $g \in \mathrm{End}(V)$ and $\delta \in \mathsf{k}$ such that $C_1(gu, gv) = \delta C_2(u, v)$ for all $u, v \in V$. Let $x \in \mathfrak{gl}_N(\mathsf{k})$ be C_2-anti-symmetric. Then gxg^{-1} is C_1-anti-symmetric.*

The proof of Lemma 4.2.5 is by direct computation, and is omitted.

4.3. Symplectic and odd-dimensional special orthogonal groups

Throughout Section 4.3, we assume $\mathbf{G} = \mathrm{Sp}_{2n}$ or $\mathbf{G} = \mathrm{SO}_{2n+1}$. The following well-known fact is very useful in the classification of regular adjoint classes in the Lie-algebra $\mathfrak{g}_1$.

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 $V = \mathsf{k}^N$ such that $C_i(u, v) = \epsilon C_i(v, u)$ for all $u, v \in V$ and $i = 1, 2$. There exists $\delta \in \mathsf{k}$ and $g \in \mathrm{End}(V)$ such that $C_1(gu, gv) = \delta C_2(u, v)$ for all $u, v \in V$. Additionally, if $\epsilon = -1$ then δ can be taken to be 1.*

Proof. See, e.g., [42, § 3.4.4] in the symplectic case and [42, § 3.4.6 and § 3.7] in the special orthogonal case. □

4.3.1. Similarity classes of regular elements

The following lemma gives a criterion for a regular matrix to be similar to an element of $\mathfrak{g}_1$.

Lemma 4.3.2. *Let $x \in \mathfrak{gl}_N(\mathsf{k})$ with minimal polynomial $m_x(t) \in \mathsf{k}[t]$.*

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 $\mathfrak{gl}_N(\mathsf{k})$ (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 $B(x^r u, v) = B(u, (-1)^r x^r v)$ for all $u, v \in V = \mathsf{k}^N$. 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 4.2.5, 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 4.2.5. 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 [36, 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 $\mathsf{k}[x]$ (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 $\mathrm{Prj}_{N-1} : V \to \mathsf{k}$ denote the projection onto $\mathsf{k} \cdot x^{N-1}v_0$. Given $u_1, u_2 \in V$ let $p_1, p_2 \in \mathsf{k}[t]$ be polynomials such that $u_i = p_i(x)v_0$ and define

$$C(u_1,u_2) = \mathrm{Prj}_{N-1}\left(p_1(x)p_2(-x)v_0\right). \tag{4.5}$$

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 $v = x^{N-1-\deg p}v_0 \in V$. Then

$$C(u,v) = \mathrm{Prj}_{N-1}((-1)^{N-1-\deg p}x^{N-1-\deg p}p(x)v_0)$$

is non-zero, since $t^{N-1-\deg p}p(t)$ is a polynomial of degree $N-1$.

Finally, for $u_i = p_i(x)v_0$ as above, we have that

$$C(xu,v) + X(u,xv) = \mathrm{Prj}_{N-1}(xp_1(x)p_2(x)v_0) + \mathrm{Prj}_{N-1}(p_1(x)\cdot(-xp_2(-x))v_0) = \mathrm{Prj}_{N-1}(0) = 0,$$

and hence x is C-anti-symmetric. □

Note that Lemma 4.3.2 gives a criterion for a regular element of $\mathfrak{gl}_N(\mathsf{k})$ 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 $x \in \mathfrak{gl}_N(\mathsf{k})$ be a regular nilpotent element, i.e. $m_x(t) = t^N$. Picking a generator v_0 for V over $\mathsf{k}[x]$ 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 Υ, given by an $N \times N$ nilpotent Jordan block. The bilinear form C of Lemma 4.3.2 is represented in this basis by the matrix

$$\mathbf{c} = \begin{pmatrix} & & & 1 \\ & & -1 & \\ & \iddots & & \\ (-1)^{N-1} & & & \end{pmatrix}. \tag{4.6}$$

To show that Υ is similar to a *regular* element of $\mathfrak{g}_1$, by [36, 3.5, Proposition 1] and [20, § 1.10, Proposition], it suffices to show that the centralizer of Υ within the Lie-algebra $\mathfrak{h} \subseteq \mathrm{M}_N(\mathsf{k}^{\mathrm{alg}})$, of matrices y satisfying the condition $y^t\mathbf{c} + \mathbf{c}y$ (i.e. the Lie-algebra of the linear algebraic $\mathsf{k}^{\mathrm{alg}}$-group of isometries of $C(\cdot,\cdot)$), is of dimension n over $\mathsf{k}^{\mathrm{alg}}$. By direct computation, one shows that

$$\mathbf{C}_{\mathfrak{h}}(\Upsilon) = \left\{ \begin{pmatrix} a_1 & a_2 & \ldots & a_N \\ & \ddots & \ddots & \vdots \\ & & a_1 & a_2 \\ & & & a_1 \end{pmatrix} \in \mathrm{M}_N(\mathsf{k}^{\mathrm{alg}}) \mid 2a_{2i-1} = 0 \text{ for all } i = 1, \ldots, \lceil N/2 \rceil \right\}.$$

Recalling that $\mathrm{char}(\mathsf{k}^{\mathrm{alg}}) \neq 2$, it follows that $a_{2i+1} = 0$ for all $i = 0, \ldots, \lceil N/2 \rceil$ and hence $\dim_{\mathsf{k}^{\mathrm{alg}}} \mathbf{C}_{\mathfrak{h}}(\Upsilon) = \lfloor N/2 \rfloor = n$.

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 $\mathfrak{gl}_N(\mathsf{k})$.*

Proof. By [36, § 3.5, Proposition 1], we need to show $\dim \mathbf{C}_{\mathbf{\Gamma}_1}(x) = n$ if and only if $\dim \mathbf{C}_{\mathrm{GL}_N \times \mathsf{k}^{\mathrm{alg}}}(x) = N$. Let $x = s + h$ be the Jordan decomposition of x over $\mathsf{k}^{\mathrm{alg}}$, with $s, h \in \mathbf{g}(\mathsf{k}^{\mathrm{alg}})$, s semisimple, h nilpotent, and $[s, h] = 0$. As seen in the proof of Proposition 2.1.1, the space $W = (\mathsf{k}^{\mathrm{alg}})^N$ decomposes as an orthogonal direct sum $W_1 \oplus W_0$ with respect to the ambient bilinear form $B_{\mathsf{k}^{\mathrm{alg}}}$, where $W_0 = \mathrm{Ker}(s)$ and $s\mid_{W_1}$ is non-singular. Let $\Sigma \subseteq \mathbf{G}(\mathsf{k}^{\mathrm{alg}})$ be the subgroup of elements acting trivially on W_0 and preserving W_1, and let Δ be as in Proposition 2.1.1. Then

$$\mathbf{C}_{\mathbf{\Gamma}_1}(x) = \mathbf{C}_{\Sigma}(x) \times \mathbf{C}_{\{1_{W_1}\} \times \Delta}(x)$$

and

$$\mathbf{C}_{\mathrm{GL}_N(\mathsf{k}^{\mathrm{alg}})}(x) = \mathbf{C}_{\mathrm{GL}(W_1) \times \{1_{W_0}\}}(x) \times \mathbf{C}_{\{1_{W_1}\} \times \mathrm{GL}(W_0)}(x)$$

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 [36, III, Theorem 1.8]. □

Proof of Theorem 4.1.2.(1). Proposition 4.3.4 implies that any element $x \in \mathrm{M}_N(\mathsf{k})$ which is similar to a regular element of $\mathfrak{g}_1$ is regular as an element of $\mathfrak{gl}_N(\mathsf{k})$. 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 $\mathrm{Ad}(\mathrm{GL}_N(\mathsf{k}))x \cap \mathfrak{g}_1$, for $x \in \mathfrak{g}_1$ regular, into $\mathrm{Ad}(G_1)$-orbits, and prove Theorem 4.1.2.(2).

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

Assuming further that $f(t) = \pm f(-t)$, let σ_f denote the k-involution of $\mathsf{k}\langle f \rangle$, induced from the $\mathsf{k}[t]$-involution $t \mapsto -t$, and let $\mathrm{U}_1(\mathsf{k}\langle f \rangle)$ be the group of elements $\xi \in \mathsf{k}\langle f \rangle$ such that $\sigma_f(\xi) \cdot \xi = 1$.

Proposition 4.3.6. *Let $x \in \mathfrak{g}_1$ be a regular element, and put $\Pi_x = \mathrm{Ad}(\mathrm{GL}_N(\mathsf{k}))x \cap \mathfrak{g}_1$. If x is singular and N is even, then the intersection Π_x is the disjoint union of two distinct $\mathrm{Ad}(G_1)$-orbits. Otherwise, $\Pi_x = \mathrm{Ad}(G_1)x$.*

Proof. The notation of Proposition 4.2.3 is used freely throughout the proof. We proceed in the following steps.

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

$$m_x(t) = t^{d_1} \cdot \prod_{i=1}^{d_2} \varphi_i(t)^{l_i} \cdot \prod_{i=1}^{d_3} \theta_i(t)^{r_i}, \tag{4.7}$$

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 $\tau(-t)$. The centralizer $\mathcal{C} = \mathbf{C}_{\mathrm{M}_N(\mathsf{k})}(x)$ is isomorphic to the ring $\mathsf{k}\langle m_x\rangle$ and the restriction of the involution $\star$ to $\mathcal{C}$ is transferred via this isomorphism to the map σ_{m_x}, defined in Notation 4.3.5. By the Chinese remainder theorem, we get

$$\mathcal{C} \simeq \mathsf{k}\langle t^{d_1}\rangle \times \prod_{i=1}^{d_2} \mathsf{k}\langle \varphi_i(t)^{m_1}\rangle \times \prod_{i=1}^{d_3} \mathsf{k}\langle \theta_i(t)^{r_i}\rangle. \tag{4.8}$$

Furthermore, the restriction of the involution σ_{m_x} to each of the factors $\mathsf{k}\langle f\rangle$, for $f \in \left\{t^{d_1}, \varphi_i^{l_i}, \theta_j^{r_j}\right\}$ coincides with the respective involution σ_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 (4.8), and that the quotient $\mathcal{C}/\mathcal{N}$ is isomorphic to the étale algebra

$$\mathcal{K} = \mathsf{k}^r \times \prod_{i=1}^{d_2} \mathsf{k}\langle \varphi_i\rangle \times \prod_{i=1}^{d_3} \mathsf{k}\langle \theta_i\rangle, \tag{4.9}$$

where $r = 1$ if $d_1 > 0$ (i.e. if x is singular) and equals 0 otherwise.[3] Let $\dagger$ denote the involution induced on the k-algebra $\mathcal{K}$ in (4.9) from the restriction of $\star$ to $\mathcal{C}$. From the observation regarding the action of $\star$ on $\mathcal{C}$ above, we deduce the following properties of the involution $\dagger$ on $\mathcal{K}$.

D1. The involution $\dagger$ preserves the factor k^r and acts trivially on it.
D2. The involution $\dagger$ preserves the factors $\mathsf{k}\langle\varphi_i\rangle$ and coincides with the non-trivial field involution σ_{φ_i}.
D3. The involution $\dagger$ preserves the factors $\mathsf{k}\langle\theta_i\rangle \simeq \mathsf{k}\langle\tau_i(t)\rangle \times \mathsf{k}\langle\tau_i(-t)\rangle$ and maps a pair $(\xi,\nu) \in \mathsf{k}\langle\tau_i(t)\rangle \times \mathsf{k}\langle\tau_i(-t)\rangle$ to the pair $(\iota^{-1}(\nu), \iota(\xi))$, where $\iota : \mathsf{k}\langle\tau_i(t)\rangle \to \mathsf{k}\langle\tau_i(-t)\rangle$ is the isomorphism induced from $t \mapsto -t$.

Let $\mathrm{Sym}(\dagger)$ be subgroup of $\mathcal{K}^\times$ of elements fixed by $\dagger$. Note that, as $\mathcal{K} \simeq \mathcal{C}/\mathcal{N}$ is a commutative ring, by Lemma 4.2.4, the set Θ_x can be identified with the quotient of $\mathrm{Sym}(\dagger)$ by the image of the map $z \mapsto z^\dagger z : \mathcal{K} \to \mathrm{Sym}(\dagger)$.

By (D2) and the theory of finite fields, the restriction of the map $z \mapsto z^\dagger z$ to the factors $\mathsf{k}\langle\varphi_i\rangle$ 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 $(\xi,\nu) \in \mathsf{k}\langle\tau_i(t)\rangle \times \mathsf{k}\langle\tau_i(-t)\rangle$ is fixed by $\dagger$ if an only if $\nu = \iota(\xi)$, in which case $(\xi,\nu) = (\xi,1)^\dagger \cdot (\xi,1)$. Lastly, by (D1) it holds that the image of the restriction of $z \mapsto z^\dagger z$ to the multiplicative group of k^r is either trivial, if $r = 0$, or the group of squares in $\mathsf{k}^\times$, otherwise. It follows from this that the set Θ_x is either in bijection with the quotient $\left(\mathsf{k}^\times/(\mathsf{k}^\times)^2\right)$, 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 Λ.

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

$$y^\star = (w^\star)^{-1}x^\star w^\star = -(w^\star)^{-1}(QxQ^{-1})w^\star = -wxw^{-1} = -y,$$

since Q is assumed to commute with x.

[3] Here it is understood that the ring k^0 is the trivial algebra $\{0\}$.

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 Λ is not surjective. Note that by definition of the equivalence class $\sim$, if $Q_1, Q_2 \in \mathrm{Sym}(\star; x)$ are such that $Q_1 \sim Q_2$, then $\det(Q_1)^{-1}\det(Q_2)$ is a square in $\mathsf{k}^\times$. This holds since $\det(a^\star) = \det(a)$ for all $a \in \mathrm{M}_N(\mathsf{k})$. By the same token, it follows that the $\det(w^\star w)$ is a square in $\mathsf{k}^\times$ for all $w \in \mathrm{GL}_N(\mathsf{k})$.

Therefore, to show that Λ is not surjective, it suffices to show that $\mathrm{Sym}(\star; x)$ contains elements whose determinant is not a square in k. One may take, for example, the element $Q = \delta \cdot 1_N$, for $\delta \in \mathsf{k}^\times$ non-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 [22, Proposition 4.4].

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

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

where the product on the right hand side is as in (4.7), with $\theta_i(t) = \tau_i(t)\tau_i(-t)$. The determinant map induces a short exact sequence

$$1 \to \mathbf{C}_{G_1}(x) \to \mathrm{U}_1(\mathsf{k}\langle t^{d_1}\rangle) \times \prod_{i=1}^{d_2} \mathrm{U}_1(\mathsf{k}\langle \varphi_i^{l_i}\rangle) \times \prod_{i=1}^{d_3} \mathrm{GL}_1(\mathsf{k}\langle \tau_i^{r_i}\rangle) \xrightarrow{\det} Z \to 1 \tag{4.10}$$

where $Z \subseteq \mathsf{k}^\times$ 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 $\mathrm{GL}_N(\mathsf{k})$ is isomorphic to the group of units of the ring $\mathcal{C}$, i.e. the direct product

$$\mathbf{C}_{\mathrm{GL}_N(\mathsf{k})}(x) \simeq \mathrm{GL}_1(\mathsf{k}\langle t^{d_1}\rangle) \times \prod_{i=1}^{d_2} \mathrm{GL}_1(\mathsf{k}\langle \varphi_i^{l_i}\rangle) \times \prod_{i=1}^{d_3} \mathrm{GL}_1(\mathsf{k}\langle \theta_i^{r_i}\rangle).$$

Furthermore, the involution $\star$ of $\mathrm{GL}_N(\mathsf{k})$ restricts to an involution of $\mathbf{C}_{\mathrm{GL}_N(\mathsf{k})}(x)$ which is transferred via this isomorphism to the involution σ_{m_x}, induced by $t \mapsto -t$, and restricts to the involution σ_f on each of the factors $\mathrm{GL}_1(\mathsf{k}\langle f\rangle)$ for $f \in \left\{t^{d_1}, \varphi_i^{l_i}, \theta_i^{r_i}\right\}$.

The additional condition $z^\star z = 1$, and the fact that $\star$ preserves all factors in the decomposition (4.8), imply that the centralizer of x in G_1 is embedded in the group

$$\mathrm{U}_1(\mathsf{k}\langle t^{d_1}\rangle) \times \prod_{i=1}^{d_2} \mathrm{U}_1(\mathsf{k}\langle \varphi_i(t)^{l_i}\rangle \times \prod_{i=1}^{d_3} \mathrm{U}_1(\mathsf{k}\langle \theta_i(t)^{r_i}\rangle).$$

Similarly to Proposition 4.3.6, the map $\sigma_{\theta_i^{r_i}}$ acts on the factors $\mathrm{GL}_1(\mathsf{k}\langle \theta_i(t)^{r_i}\rangle) \simeq \mathrm{GL}_1(\mathsf{k}\langle \tau_i(t)^{r_i}\rangle) \times \mathrm{GL}_1(\mathsf{k}\langle \tau_i(-t)^{r_i}\rangle)$ as $(\xi, \nu) \mapsto (\iota^{-1}(\nu), \iota(\xi))$, where $\iota : \mathsf{k}\langle \tau_i(t)^{r_i}\rangle \to \mathsf{k}\langle \tau_i(-t)^{r_i}\rangle$ is the isomorphism induced from $t \mapsto -t$. It follows from this that $(\xi, \nu) \in \mathrm{U}_1(\mathsf{k}\langle \theta_i^{r_i}\rangle)$ if and only if $\iota(\xi) = \nu^{-1}$, and hence that $\mathrm{U}_1(\mathsf{k}\langle \theta_i^{r_i}\rangle) \simeq \mathrm{GL}_1(\mathsf{k}\langle \tau_i^{r_i}\rangle)$.

Lastly, we compute order of the group Z. Since for any $w \in \mathrm{GL}_N(\mathsf{k})$ we have that $\det(w^\star) = \det(w)$, it follows that the condition $w^\star w = 1$ 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 $\pm 1 \in \mathrm{GL}_N(\mathsf{k})$, while the latter can be deduced by considering the Pfaffian of the matrix $w^t \mathbf{J} w = \mathbf{J}$. □

Lemma 4.3.8. *Let $f \in \mathsf{k}[t]$ 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 $z \mapsto \sigma_{f^r}(z) \cdot z : \mathrm{GL}_1(\mathsf{k}\langle f^r \rangle) \to \mathrm{GL}_1(\mathsf{k}\langle f^r \rangle)$. Given $y \in \mathrm{GL}_1(\mathsf{k}\langle f^r \rangle)$ it holds that $y \in E_{f^r}$ if and only if*

1. *$\sigma_{f^r}(y) = y$, and*
2. *there exists $z \in \mathrm{GL}_1(\mathsf{k}\langle f(t)^r \rangle)$ such that $y \equiv z\sigma_{f^r}(z) \pmod f$.*

In particular, we have

$$|E_{f^r}| = \begin{cases} q^{\frac{1}{2} r \deg f}(1 - q^{-\frac{1}{2}\deg f}) & \text{if } f(t) \neq t \\ \frac{q-1}{2} q^{\lceil \frac{r}{2} \rceil - 1} & \text{if } f(t) = t. \end{cases}$$

Proof. Let W denote the vector space underlying the ring $\mathsf{k}\langle f^r \rangle$ 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 $\mathsf{k}\langle f^r \rangle$ with the ring $\mathcal{C} \subseteq \mathrm{M}_{r \cdot \deg f}(\mathsf{k})$ of matrices commuting with x, and the involution $\star$ on $\mathcal{C}$ is identified with the ring involution σ_{f^r}. Note that, in the current setting, if $y \in \mathsf{k}\langle f^r \rangle$ is the image modulo (f^r) of a polynomial $\tilde{y}(t)$, then the assumption $\sigma_{f^r}(y) = y$ is equivalent to $\tilde{y}(x) \in \mathcal{C}$ satisfying $\tilde{y}(x)^\star = \tilde{y}(x)$ or, in the notation of Section 4.2.2, to $\tilde{y}(x) \in \mathrm{Sym}(\star; x)$. Also, the nilpotent radical of $\mathcal{C}$ is given as the image of the ideal $(f) \subseteq \mathsf{k}\langle f^r \rangle$. The equivalence stated in the lemma now follows from Lemma 4.2.4, by taking $Q_1 = 1$ and $Q_2 = \tilde{y}(x) \in \mathrm{Sym}(\star; x)$.

We now compute the cardinality of E_{f^r}. In the case $f(t) = t$, the equivalence proved above implies that E_{f^r} can be identified with the subgroup of the ring $\mathsf{k}[t]/(t^r)$ 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 $|E_{f^r}| = \frac{q-1}{2} q^{\lceil \frac{r}{2} \rceil - 1}$.

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 $S, H \in \mathsf{k}[t]$ such that the endomorphism $S(x)$ (resp. $H(x)$) acts semisimply (resp. nilpotently) on the vector space $W = \mathsf{k}\langle f^r \rangle$, on which x acts by multiplication by t, and such that $H(t) + S(t) \equiv t \pmod{f(t)^r}$ (see [19, § 4.2]; note that $S, H \in \mathsf{k}[t]$ is possible since k is perfect). It follows that $\mathsf{k}\langle f^r \rangle \simeq \mathsf{k}[x] = \mathsf{k}[S(x)][H(x)]$. A quick computation shows that the minimal polynomials of $S(x)$ and $H(x)$ are $f(t)$ and t^r respectively, and thus $\mathsf{k}\langle f \rangle \simeq \mathsf{k}[S(x)][H(x)] \simeq \mathsf{k}\langle f \rangle \otimes_{\mathsf{k}} (\mathsf{k}[h]/(h^r))$. Moreover, by the properties of the Jordan–Chevalley decomposition, both $S(t)$ and $H(t)$ satisfy $S(-x) = -S(x)$ and $H(-x) = -H(x)$ [7, § 3, Proposition 3]. Thus, under this identification, the involution σ_{f^r} is transferred to an involution of $\mathsf{k}\langle f \rangle \otimes_{\mathsf{k}} (\mathsf{k}[h]/(h^r))$, mapping h to $-h$ and acting as σ_f on the field $\mathsf{k}\langle f \rangle$.

By the equivalence in the lemma, and the theory of finite fields, the group E_{f^r} is identified with the subgroup of $(\mathsf{k}\langle f^r \rangle)^\times$ of elements fixed by σ_{f^r}. Using the identification above, this subgroup consists of elements of the form $\sum_{i=0}^{r-1} a_i \otimes h^i$, with $a_0, \ldots, a_{r-1} \in \mathsf{k}\langle f \rangle$, $a_0 \neq 0$, 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 $|E_{f^r}| = q^{\frac{1}{2} r \deg f}(1 - q^{-\frac{1}{2}\deg f})$ now follows by direct computation. □

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

$$|\mathbf{C}_{G_1}(x)| = 2^{\nu} q^n \prod_{d,e} \left(1+q^{-d}\right)^{S_{d,e}(m_x)} \cdot \left(1-q^{-d}\right)^{T_{d,e}(m_x)},$$

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

Proof. Let $m_x = t^{d_1} \prod_{i=1}^{d_2} \varphi_i^{l_i} \prod_{i=1}^{d_3} \theta_i^{r_i}$ be a decomposition of m_x as in (4.7), with φ_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 $\boldsymbol{\tau}(m_x)$ we have that $r(m_x) = \lfloor \frac{d_1}{2} \rfloor$.

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

1. $\left|\mathrm{U}_1(\mathsf{k}\langle t^{d_1}\rangle)\right| = 2q^{r(m_x)}$;
2. $\left|\mathrm{U}_1(\mathsf{k}\langle \varphi_i^{l_i}\rangle)\right| = q^{\frac{1}{2} l_i \cdot \deg \varphi_i}(1+q^{-\frac{1}{2}\deg \varphi_i})$;
3. $|\mathrm{GL}_1(\mathsf{k}\langle \tau_i^{r_i}\rangle)| = q^{r_i \cdot \deg \tau_i}(1-q^{-\deg \tau_i})$.

Note that for any irreducible polynomial $f(t) \in \mathsf{k}[t]$ and $r \in \mathbb{N}$, invoking the Jordan–Chevalley Decomposition as in Lemma 4.3.8, the group $\mathrm{GL}_1(\mathsf{k}\langle f^r\rangle)$ is isomorphic to the group of units of the ring $\mathsf{k}\langle f\rangle[u]/(u^r)$, and hence $|\mathrm{GL}_1(\mathsf{k}\langle f^r\rangle)| = q^{r\cdot \deg f}\left(1-q^{-\deg f}\right)$. Assertion (3) follows by taking $f(t) = \tau_i(t)$ and $r = r_i$.

Assertions (1) and (2) follow from the exactness of the sequence

$$1 \to \mathrm{U}_1(\mathsf{k}\langle f^r\rangle) \to \mathrm{GL}_1(\mathsf{k}\langle f^r\rangle) \xrightarrow{x \mapsto \sigma_{f^r}(x)\cdot x} E_{f^r} \to 1,$$

which holds for any irreducible $f \in \mathsf{k}[t]$ with $f(-t) = \pm f(t)$ and $r \in \mathbb{N}$, and from the computation of $|E_{f^r}|$ in Lemma 4.3.8 and $|\mathrm{GL}_1(\mathsf{k}\langle f^r\rangle)|$ for the case where $f(t) = t$ and $r = d_1$, and the cases $f(t) = \varphi_i(t)$ and $r = l_i$. □

The final assertion of Theorem 4.1.2 follows directly from Proposition 4.3.9.

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 $x \in \mathfrak{gl}_N(\mathsf{k}^{\mathrm{alg}})$ be a regular nilpotent element. Then x is not anti-symmetric with respect to any non-degenerate symmetric bilinear form on $V = (\mathsf{k}^{\mathrm{alg}})^N$.*

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 the $C(xu, v) + C(u, xv) = 0$, 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 [32, 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 $V = \mathsf{k}^N$ 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, upto 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

$$\mathbf{J}^+ = \begin{pmatrix} 0 & 1 & & & & & \\ 1 & 0 & & & & & \\ & & \ddots & & & & \\ & & & 0 & 1 & & \\ & & & 1 & 0 & & \\ & & & & & 0 & 1 \\ & & & & & 1 & 0 \end{pmatrix} \quad \text{or} \quad \mathbf{J}^- = \begin{pmatrix} 0 & 1 & & & & & \\ 1 & 0 & & & & & \\ & & \ddots & & & & \\ & & & 0 & 1 & & \\ & & & 1 & 0 & & \\ & & & & & 1 & 0 \\ & & & & & 0 & \delta \end{pmatrix}, \tag{4.11}$$

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

Given $\epsilon \in \{\pm 1\}$, let $G_1^\epsilon = \mathrm{SO}_N^\epsilon(\mathsf{k})$ and $\mathfrak{g}_1^\epsilon = \mathfrak{so}_N^\epsilon(\mathsf{k})$ be the group of isometries of determinant 1 and the Lie-algebra of anti-symmetric operators with respect to the form B^ϵ. We will also occasionally use the colloquial notation $G_1^\pm = G_1^+ \cup G_1^-$ and $\mathfrak{g}_1^\pm = \mathfrak{g}_1^+ \cup \mathfrak{g}_1^-$. For example, the phrase *x is a regular element of* $\mathfrak{g}_1^\pm$ 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 $\mathfrak{gl}_N(\mathfrak{o})$ 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 $x \in \mathfrak{gl}_N(\mathsf{k})$ 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 $\mathfrak{g}_1^\pm$. By Lemma 4.2.1, all non-singular regular elements of $\mathfrak{g}_1$ are obtained in this manner. Thus, for $x \in \mathfrak{gl}_N(\mathsf{k})$ non-singular, it holds that x is similar to a regular element of $\mathfrak{g}^\pm$ 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 $\mathfrak{g}_1^\pm$ is essentially reduced to the study of nilpotent regular elements. These elements are considered in the following lemma.

Lemma 4.4.2. *Let $x \in \mathfrak{gl}_N(\mathsf{k})$ 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 $u_0 \in \mathrm{Ker}(x)$ and such that $\mathcal{E} = \{v_0, xv_0, \ldots, x^{N-2}v_0, u_0\}$ is a k-basis for V.

Let $\mathcal{E}' = \{v_0, \ldots x^{N-2}v_0\}$ and $V' = Span_{\mathsf{k}}\, \mathcal{E}'$. 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 $\mathbf{d} \in \mathrm{M}_N(\mathsf{k})$, whose top-left $(N-1)\times(N-1)$ submatrix coincides with the matrix $\mathbf{c}$ of Example 4.3.3 (see (4.6)), and such that

$$\mathbf{d}^t\Upsilon + \Upsilon\mathbf{d} = 0 \quad \text{where} \quad \Upsilon = [x]_{\mathcal{E}} = \begin{pmatrix} 0 & 1 & & & \\ & \ddots & \ddots & & \\ & & 0 & 1 & \\ & & & 0 & 0 \\ & & & & 0 \end{pmatrix}. \tag{4.12}$$

A short computation shows that the matrix

$$\mathbf{d} = \mathbf{d}_\eta = \begin{pmatrix} & & & 1 \\ & & -1 & \\ & \iddots & & \\ 1 & & & \\ & & & \eta \end{pmatrix}, \tag{4.13}$$

where $\eta \in \mathsf{k}^\times$ satisfies the required equality. Furthermore, by applying a signed permutation to $\mathcal{E}$, one may verify easily that $\mathbf{d}_\eta$ is congruent to the matrix $\mathbf{J}^+$ of (4.11) if η is a square, and to $\mathbf{J}^-$ otherwise. Thus, x is similar in this case to elements of both $\mathfrak{g}_1^+$ and of $\mathfrak{g}_1^-$.

Lastly, we need to verify that x is similar to a *regular* element of $\mathfrak{g}_1^\pm$. To do so, we pass to the algebraic closure $\mathsf{k}^{\mathrm{alg}}$ of k and compute the centralizer in $\mathbf{G}(\mathsf{k}^{\mathrm{alg}})$ of an element $zxz^{-1} \in \mathfrak{g}_1$. Working in the basis $\mathcal{E}$, by direct computation, one sees that the centralizer of x in $\mathrm{M}_N(\mathsf{k}^{\mathrm{alg}})$ can be identified with the set of matrices $\mathbf{y} = \left(\begin{smallmatrix} \mathbf{A} & \mathbf{v} \\ \mathbf{u}^t & r \end{smallmatrix}\right)$, where

1. $\mathbf{A} \in \mathrm{M}_{N-1}(\mathsf{k}^{\mathrm{alg}})$ and commutes with the restriction of Υ to $V' = Span_{\mathsf{k}^{\mathrm{alg}}} \mathcal{E}'$;
2. $\mathbf{u}, \mathbf{v} \in (\mathsf{k}^{\mathrm{alg}})^{N-1}$ are elements of the kernel of Υ and Υ^t, respectively, and hence of the form $\mathbf{v} = (v_1 \quad 0 \quad \dots \quad 0)^t$ and $\mathbf{u} = (0 \quad \dots \quad 0 \quad u_{N-1})^t$; and
3. $r \in \mathsf{k}^{\mathrm{alg}}$ is arbitrary.

As in Example 4.3.3, the centralizer of $zxz^{-1} \in \mathfrak{g}_1$ is conjugated in $\mathrm{GL}_N(\mathsf{k}^{\mathrm{alg}})$ to the group

$$\left\{ \mathbf{y} \in \mathbf{C}_{\mathrm{GL}_N(\mathsf{k}^{\mathrm{alg}})}(\Upsilon) \mid \mathbf{y}^t \mathbf{d} \mathbf{y} = \mathbf{d} \right\}.$$

Computing its Lie-algebra, which consists of matrices $\mathbf{y} \in \mathbf{C}_{\mathrm{M}_N(\mathsf{k}^{\mathrm{alg}})}(\Upsilon)$ satisfying $\mathbf{y}^t \mathbf{d} + \mathbf{d}\mathbf{y} = 0$, we get the additional three conditions

1. $\mathbf{A}^t \mathbf{c} + \mathbf{c}\mathbf{A} = 0$, where $\mathbf{c}$ is as in Example 4.3.3;
2. $\eta \mathbf{u} + \mathbf{c}\mathbf{v} = 0$, i.e. $v_1 = -\eta u_{N-1}$; and
3. $2\eta r = 0$, and hence $r = 0$.

It follows that $\mathbf{C}_{\mathbf{\Gamma}_1}(zxz^{-1})$ 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 $\mathbf{A} \in \mathrm{M}_{N-1}(\mathsf{k})$, column vectors $\mathbf{v}, \mathbf{u} \in \mathsf{k}^{N-1}$ and $r \in \mathsf{k}$, let $\Xi(\mathbf{A}, \mathbf{v}, \mathbf{u}, r)$ denote the $N \times N$ matrix

$$\Xi(\mathbf{A}, \mathbf{v}, \mathbf{u}, r) = \begin{pmatrix} \mathbf{A} & \mathbf{v} \\ \mathbf{u}^t & r \end{pmatrix}.$$

We also write $\mathbf{A}^\flat$ for the matrix $\mathbf{c}\mathbf{A}^t\mathbf{c}$, where $\mathbf{c}$ is as in Example 4.3.3. Note that, in the case where $\mathbf{d} = \mathbf{d}_\eta$ is the representing matrix for the symmetric bilinear form given on V, we have that

$$\Xi(\mathbf{A}, \mathbf{v}, \mathbf{u}, r)^\star = \begin{pmatrix} \mathbf{A}^\flat & \eta \mathbf{c}\mathbf{u} \\ \eta^{-1} \mathbf{v}^t \mathbf{c} & r \end{pmatrix} = \Xi(\mathbf{A}^\flat, \eta \mathbf{c}\mathbf{u}, \eta^{-1}\mathbf{c}\mathbf{v}, r). \tag{4.14}$$

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

Lemma 4.4.4 *(cf. [39, § 2.6.(B).(i) and (i')]). Let $x \in \mathfrak{gl}_N(\mathsf{k})$ have minimal polynomial m_x. Assume x is similar to a regular element of $\mathfrak{g}_1^{\pm}$.*

1. *If $m_x(t) = f(t)f(-t)$ for some polynomial $f \in \mathsf{k}[t]$ with $f(0) \neq 0$, then x is similar to an element of $\mathfrak{g}_1^{+}$, and not to an element of $\mathfrak{g}_1^{-}$.*
2. *If $m_x = \varphi^r$ for $\varphi \in \mathsf{k}[t]$ an even irreducible polynomial and $r \in \mathbb{N}$ odd, then x is similar to a regular element of $\mathfrak{g}_1^{-}$ and not to an element of $\mathfrak{g}_1^{+}$.*

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 $m_x(0) \neq 0$ and Lemma 4.2.1, it follows that x is also a regular element of $\mathfrak{gl}_N(\mathsf{k})$, and hence the space V is cyclic as a $\mathsf{k}[x]$ module. Put $W = f(x)V$. Then W is isomorphic, as a $\mathsf{k}[x]$-module, to $V/f(-x)V$, and hence is of dimension $n = \frac{N}{2}$ 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 $\mathsf{k}\langle\varphi\rangle$ of k. Furthermore, the map $\sigma_\varphi \in \mathrm{Aut}_{\mathsf{k}}(\mathsf{k}\langle\varphi\rangle)$, induced from $t \mapsto -t$ is a field involution of $\mathsf{k}\langle\varphi\rangle$ over k, with fixed field K, such that $|\mathsf{k}\langle\varphi\rangle : \mathsf{K}| = 2$. Note that in this setting, without loss of generality, we may assume that $C(u, v) = \mathrm{Tr}_{\mathsf{k}\langle\varphi\rangle/\mathsf{k}}(\sigma_\varphi(u)v)$ for all $u, v \in V$. Indeed, invoking the separability of the extension $\mathsf{k}\langle\varphi\rangle/\mathsf{k}$, there exists an element $c \in \mathsf{k}\langle\varphi\rangle$ such that $C(u, 1) = \mathrm{Tr}_{\mathsf{k}\langle\varphi\rangle/\mathsf{k}}(c \cdot u)$ for all $u \in \mathsf{k}\langle\varphi\rangle$. From the symmetry of C and the invariance of $\mathrm{Tr}_{\mathsf{k}\langle\varphi\rangle/\mathsf{k}}$ under σ_φ, it can be deduced that in fact $c \in \mathsf{K}$. By the theory of finite fields, there exists an element $d \in \mathsf{k}\langle\varphi\rangle$ such that $c = \sigma_\varphi(d)d$. It follows that multiplication by d is an isometry of C with the trace pairing $(u, v) \mapsto \mathrm{Tr}_{\mathsf{k}\langle\varphi\rangle/\mathsf{k}}(\sigma_\varphi(u)v)$.

   Note that an element $u \in \mathsf{k}\langle\varphi\rangle$ 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 $q^{n-1} - 1$, and by the surjectivity of the norm map $\mathrm{Nr}_{\mathsf{k}\langle\varphi\rangle/\mathsf{K}}$, it follows that the number of non-zero isotropic element of $\mathsf{k}\langle\varphi\rangle$ is $(q^n + 1)(q^{n-1} - 1)$. The fact that C is of Witt index $n-1$ now follows as in [42, § 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 $U^\perp = \varphi(x)^l V$. Moreover, the form C reduces to a non-degenerate symmetric bilinear form on the quotient space $U^\perp/U$, on which x acts as an anti-symmetric operator with minimal polynomial φ. By the case $r = 1$, we find a two-dimensional anisotropic subspace $\bar{L} \subseteq U^\perp/U$, whose pull-back to $U^\perp$ is contains a two-dimensional anisotropic subspace of V. It follows that the Witt index of C is necessarily $n-1$. □

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 $\mathfrak{g}_1^{\pm}$.

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 $\frac{1}{2}\dim_{\mathsf{k}} U$ 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. The lemma follows, e.g., from [42, § 3.7.4, p. 68], noting that the direct product of the groups of isometries of C_U and C_W is embedded in the group of isometries of $C_{U\oplus W}$. □

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*

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

a decomposition as in (4.7), 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 $\mathfrak{g}_1^{\pm}$ 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 $\mathfrak{g}_1^{\pm}$ if and only if $\deg m_x = N$. In this case, put $\omega(m_x) = \sum_{i=1}^{d} l_i$.*
   (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 $\mathsf{k}[x]$-invariant direct sum $V = W_{t^{d_1}} \oplus \bigoplus_{i=1}^{d_2} W_{\varphi_i^{l_i}} \oplus \bigoplus_{i=1}^{d_3} W_{\theta_i^{r_i}}$, where the restriction of x to the spaces W_f has minimal polynomial $f(t)$, with $f \in \left\{t^{d_1}, \varphi_i^{l_i}, \theta_i^{r_i}\right\}$.

For any $f(t) \neq t^{d_1}$, 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 $f = \varphi_i^{l_i}$ with l_i even, then $\delta_{W_f} = +1$. Otherwise, if $f = \varphi_i^{l_i}$ 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 $W_{t^{d_1}}$ 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 $\frac{d_1}{2}$ as well as $\frac{d_1}{2} - 1$. Thus $\delta_{W_{t^{d_1}}}$ 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 $\mathfrak{g}_1^{+}$ as well as to an element of $\mathfrak{g}_1^{-}$. □

4.4.2. From similarity classes to adjoint orbits

Our next goal, once the similarity classes containing regular elements of $\mathfrak{g}_1^{\pm}$ have been classified, is to describe the set $\Pi_x = \mathrm{Ad}(\mathrm{GL}_N(\mathsf{k}))x \cap \mathfrak{g}_1^{\epsilon}$ into $\mathrm{Ad}(G_1^{\epsilon})$-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 $|\mathsf{k}| > 3$ and $\mathrm{char}(\mathsf{k}) \neq 2$. For any element $\gamma \in \mathsf{k}^{\times}$ there exist $\nu, \delta \in \mathsf{k}^{\times}$ such that $\nu \in (\mathsf{k}^{\times})^2$, $\delta \in \mathsf{k}^{\times} \smallsetminus (\mathsf{k}^{\times})^2$ and such that $\gamma = \nu - \delta$.*

Proposition 4.4.9. *Assume $|\mathsf{k}| > 3$. Fix $\epsilon \in \{\pm 1\}$ and let $x \in \mathfrak{g}_1^{\epsilon}$ be regular. If x is singular, then the intersection $\mathrm{Ad}(\mathrm{GL}_N(\mathsf{k}))x \cap \mathfrak{g}_1^{\epsilon}$ is the disjoint union of two distinct $\mathrm{Ad}(G_1^{\epsilon})$-orbits. Otherwise, $\mathrm{Ad}(\mathrm{GL}_N(\mathsf{k}))x \cap \mathfrak{g}_1^{\epsilon} = \mathrm{Ad}(G_1^{\epsilon})x$.*

Proof. In the notation of Proposition 4.2.3, let $\Pi_x = \mathrm{Ad}(\mathrm{GL}_N(\mathsf{k}))x \cap \mathfrak{g}_1$ and Θ_x the set of equivalence classes in $\mathrm{Sym}(\star; x) = \left\{Q \in \mathbf{C}_{\mathrm{GL}_N(\mathsf{k})}(x) \mid Q^{\star} = Q\right\}$ under the equivalence relation $\sim$, defined in (4.4). Let $\Lambda : \Pi_x \to \Theta_x$ be the map $wxw^{-1} \mapsto [w^{\star}w] \in \Theta_x$, 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 Θ_x consists of a single element and therefore that $\Pi_x = \mathrm{Ad}(G_1^{\epsilon})x$.

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 $\mathfrak{g}_1^\epsilon$.

In this case, by the uniqueness of a nilpotent regular element in $\mathbf{g}(\mathsf{k}^{\mathrm{alg}})$ [32, III, Theorem 1.8], we may invoke Lemma 4.4.2 and fix a basis $\mathcal{E}$, with respect to which x is represented by the matrix Υ, defined in (4.12), and that the ambient non-degenerate symmetric bilinear form is represented in $\mathcal{E}$ by the matrix $\mathbf{d} = \mathbf{d}_\eta$ of (4.13), where $\eta \in \mathsf{k}^\times$ is a square if $\epsilon = 1$ and non-square otherwise.

The centralizer $\mathcal{C}$ of Υ in $\mathrm{M}_N(\mathsf{k})$ is isomorphic to the ring of $\mathsf{k}[x]$-endomorphisms of $\mathsf{k}[x] \times \mathsf{k}$, and can be realized as the set of matrices $\Xi(\mathbf{A}, \mathbf{v}, \mathbf{u}, r)$ (see Notation 4.4.3) with $\mathbf{v}$ and $\mathbf{u}$ elements of the kernel of Υ and Υ^t respectively, $\mathbf{A} \in \mathrm{M}_{N-1}(\mathsf{k})$ is an upper triangular Töplitz matrix, and $r \in \mathsf{k}$. Note that the ideal generated by elements of the form $\Xi(0_{N-1}, \mathbf{v}, \mathbf{u}, 0) \in \mathcal{C}$ is nilpotent and in particular is contained in the nilpotent radical $\mathcal{N}$ of $\mathcal{C}$. It follows that the quotient ring $\mathcal{C}/\mathcal{N}$ is isomorphic to the étale algebra $\mathsf{k} \times \mathsf{k}$. Additionally, by Lemma 4.2.4, we have that $\Xi(\mathbf{A}, \mathbf{v}, \mathbf{u}, r) \sim \Xi(\mathbf{A}', \mathbf{v}', \mathbf{u}', r')$ if and only if there exists a block matrix $\Xi(\mathbf{q}, 0, 0, s)$ such that

$$\begin{pmatrix} \mathbf{q} & \\ & s \end{pmatrix}^\star \begin{pmatrix} \mathbf{A} & \mathbf{v} \\ \mathbf{u}^t & r \end{pmatrix} \begin{pmatrix} \mathbf{q} & \\ & s \end{pmatrix} \equiv \begin{pmatrix} \mathbf{A}' & \mathbf{v}' \\ \mathbf{u}'^t & r' \end{pmatrix} \pmod{\mathcal{N}}.$$

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

The final step of the proof is to compute the image of the map Λ. Recall that Λ maps an element $wxw^{-1} \in \Pi_x = \mathrm{Ad}(\mathrm{GL}_N(\mathsf{k}))x \cap \mathfrak{g}_1^\epsilon$ to the equivalence class of $w^\star w$ in Θ_x. As in the odd orthogonal case, two elements which are equivalent with respect to $\sim$ must have determinant in the same coset of $\mathsf{k}^\times/(\mathsf{k}^\times)^2$. In particular, as $w^\star w$ has square determinant, the image of Λ in Θ_x is contained in the subset of equivalence classes in Θ_x, containing block matrices $\Xi(\mathbf{A}, 0, 0, r)$ with $\det \mathbf{A} \equiv r \pmod{(\mathsf{k}^\times)^2}$.

To complete the proof that $|\mathrm{Im}(\Lambda)| = 2$ it suffices to find an element $w \in \mathrm{GL}_N(\mathsf{k})$ such that $wxw^{-1} \in \mathfrak{g}_1$ and such that $w^\star w$ is a block matrix of the form $\Xi(\mathbf{A}, 0, 0, r)$ with $\det \mathbf{A}, r \notin (\mathsf{k}^\times)^2$.

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

Recalling that $w^\star$ is represented by the matrix $\mathbf{d}^{-1}\mathbf{w}^t\mathbf{d}$, one verifies by direct computation that $w^\star w$ is given by the diagonal matrix $\Xi(\delta 1_{N-1}, 0, 0, \nu^{-1}\delta)$, and consequently, that $w^\star w \in \mathrm{Sym}(\star; x)$ and $wxw^{-1} \in \mathfrak{g}_1^\epsilon$, and that $w^\star w$ is not equivalent to 1_N under the relation $\sim$.

$$\mathbf{w} = \begin{pmatrix} \delta & & & & & & & & \\ & \ddots & & & & & & & \\ & & \delta & & & & & & \\ & & & \nu_1 & & & & \alpha z & \\ & & & & 1 & & & & \\ & & & & & \ddots & & & \\ & & & & & & 1 & & \\ & & & -\eta^{-1}\nu_1 z & & & & 1 & \end{pmatrix}. \quad \square \tag{4.15}$$

Proof of Lemma 4.4.8. Let $\xi \in \mathsf{k}^\times$ be a non-square, and let $\mathsf{K} = \mathsf{k}\langle t^2 - \xi \rangle$ be the splitting field of $t^2 - \xi$, with $\xi_1 \in \mathsf{K}^\times$ a square root of ξ. The norm map $\mathrm{Nr}_{\mathsf{K}|\mathsf{k}} : \mathsf{K}^\times \to \mathsf{k}^\times$ is surjective and has fibers of order $q+1$. In particular, there exist $\nu_1, \delta_1 \in \mathsf{k}$ such that

$$\mathrm{Nr}_{\mathsf{K}|\mathsf{k}}(\nu_1 + \xi_1\delta_1) = \nu_1^2 - \xi\delta_1^2 = \gamma.$$

We claim that ν_1 and δ_1 can be taken to be both non-zero.

Case 1, $\gamma \in \mathsf{k}^\times \smallsetminus (\mathsf{k}^\times)^2$. Note that in this case we must have that $\delta_1 \neq 0$, as otherwise $\gamma = \nu_1^2 \in (\mathsf{k}^\times)^2$. Furthermore, if $\nu_1 = 0$ for any pair (ν_1, δ_1) such that $\nu_1^2 - \xi\delta_1^2 = \gamma$ then $\mathrm{Nr}^{-1}_{\mathsf{K}|\mathsf{k}}(\gamma) \subseteq \xi_1\mathsf{k}^\times$, and in particular has order smaller than q. A contradiction.
Case 2, $\gamma \in (\mathsf{k}^\times)^2$. Consider the set $\mathrm{Nr}^{-1}_{\mathsf{K}|\mathsf{k}}(\gamma) \smallsetminus \mathsf{k}^\times$. Note that, as $\left|\mathrm{Nr}^{-1}_{\mathsf{K}|\mathsf{k}}(\gamma) \cap \mathsf{k}^\times\right| = 2$ (namely, it consists of the two roots of γ in k), the order of $\mathrm{Nr}^{-1}_{\mathsf{K}|\mathsf{k}}(\gamma) \smallsetminus \mathsf{k}^\times$ is exactly $q-1$. Assume towards a contradiction that there is no solution $(\nu_1, \delta_1) \in \mathsf{k}^\times \times \mathsf{k}^\times$ for the equation

$$\nu_1^2 - \xi\delta_1^2 = \mathrm{Nr}_{\mathsf{K}|\mathsf{k}}(\nu_1 - \xi_1\delta_1) = \gamma.$$

This implies that any solution not in $\mathsf{k}^\times \times \{0\}$ is an element of $\{0\} \times \mathsf{k}^\times$, or in other words, that $\mathrm{Nr}^{-1}_{\mathsf{K}|\mathsf{k}}(\gamma) \smallsetminus \mathsf{k}^\times \subseteq \xi_1\mathsf{k}^\times$. 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 $\delta_1 \in \mathsf{k}^\times$,

$$\mathrm{Nr}_{\mathsf{K}|\mathsf{k}}(\xi_1\delta_1) = -\xi\delta_1^2 = \gamma.$$

Thus, the set of squares in $\mathsf{k}^\times$ equals the singleton set $\left\{-\xi^{-1}\gamma\right\}$. This contradicts the assumption $|\mathsf{k}| > 3$.

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

4.4.3. Centralizers of regular elements

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

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

a decomposition as in (4.7), 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*

$$1 \to \mathbf{C}_{G_1^\epsilon}(x) \to \mathcal{A}^\epsilon \times \prod_{i=1}^{d_2} \mathrm{U}_1(\mathsf{k}\langle\varphi_i^{l_i}\rangle) \times \prod_{i=1}^{d_3} \mathrm{GL}_1(\mathsf{k}\langle\tau_i^{r_i}\rangle) \xrightarrow{\det} \{\pm 1\} \to 1. \tag{4.16}$$

   where

$$\mathcal{A}^\epsilon = \left\{ \mathbf{w} \in \mathbf{C}_{\mathrm{GL}_{d_1+1}(\mathsf{k})}(\Upsilon) \mid \mathbf{w}^t \mathbf{d}_\eta \mathbf{w} = \mathbf{d}_\eta \right\},$$

   with Υ and $\mathbf{d}_\eta$ the $(d_1+1) \times (d_1+1)$ matrices defined as in (4.12) and (4.13).
2. *Otherwise, the group $\mathbf{C}_{G_1^\epsilon}(x)$ is isomorphic to $\prod_{i=1}^{d_2} \mathrm{U}_1(\mathsf{k}\langle\varphi_i^{l_i}\rangle) \times \prod_{i=1}^{d_3} \mathrm{GL}_1(\mathsf{k}\langle\tau_i^{r_i}\rangle)$.*

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 $\mathcal{A}^\epsilon$, for which it is enough to consider block diagonal matrices of the form $\left(\begin{smallmatrix} 1_{d_1} & 0 \\ 0 & \pm 1 \end{smallmatrix}\right) \in \mathcal{A}^\epsilon$.

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

Case 1. Assume $m_x(t) = \varphi_i(t)^m$, with $\varphi_i \in \mathsf{k}[t]$ irreducible and even and $m \in \mathbb{N}$. Let $x = s + h$ be the Jordan decomposition of x, with $s, h \in \mathfrak{g}_1^\epsilon$, 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 $\mathsf{k}[x]$-module and hence $\mathbf{C}_{\mathrm{M}_N(\mathsf{k})}(x) \simeq \mathsf{k}[x] = \mathsf{k}[s][h] \simeq \mathsf{k}\langle\varphi_i\rangle[u]/(u^m)$ (see Lemma 4.3.8). Let $\rho : \mathsf{k}\langle\varphi_i\rangle[u]/(u^m) \to \mathbf{C}_{\mathrm{M}_N(\mathsf{k})}(x)$ be a k-linear isomorphism. The k-linearity of ρ and the nilpotency of u imply that

$$\det(\rho(\alpha_0 + \alpha_1 u + \ldots + \alpha_{m-1}u^{m-1})) = \mathrm{Nr}_{\mathsf{k}\langle\varphi_i\rangle/\mathsf{k}}(\alpha_0)^m.$$

Furthermore, the restriction of the involution $\star$ to the image of ρ induces a k-automorphism $\sigma_{\varphi_i^m}$ of $\mathsf{k}\langle\varphi_i^m\rangle$ which acts on $\mathsf{k}\langle\varphi_i\rangle$ as the involution σ_{φ_i}, and maps u to $-u$. Consequently, if $z \in \mathbf{C}_{\mathrm{GL}_N(\mathsf{k})}(x)$ is given by $z = \rho(\alpha_0 + \alpha_1 u + \ldots + \alpha_{m-1}u^{m-1})$ and satisfies $z^\star z = 1$ then necessarily $\mathrm{Nr}_{\mathsf{k}\langle\varphi_i\rangle/\mathsf{K}}(\alpha_0) = \sigma_{\varphi_i}(\alpha_0)\alpha_0 = \rho^{-1}(z^\star z)\mid_{u=0} = 1$ and

$$\begin{aligned}\det(z) &= \det(\rho(\alpha_0 + \alpha_1 u + \ldots + \alpha_{m-1}u^{m-1})) \\ &= \mathrm{Nr}_{\mathsf{k}\langle\varphi_i\rangle/\mathsf{k}}(\alpha_0)^m = \left(\mathrm{Nr}_{\mathsf{K}/\mathsf{k}} \circ \mathrm{Nr}_{\mathsf{k}\langle\varphi_i\rangle/\mathsf{K}}(\alpha_0)\right)^m = 1.\end{aligned}$$

Case 2. Assume $m_x(t) = (\tau_i(t)\cdot\tau_i(-t))^r$, for $\tau_i(t)$ irreducible and coprime to $\tau(-t)$. In this case, by the cyclicity of the $\mathsf{k}[x]$ module V, we have that $\mathbf{C}_{\mathrm{GL}_N(\mathsf{k})}(x) \simeq \mathrm{GL}_1(\mathsf{k}\langle\tau(t)^r\rangle) \times \mathrm{GL}_1(\mathsf{k}\langle\tau(-t)^r\rangle)$. Moreover, the map $\star$ restricts to the map $(\xi,\nu) \mapsto (\iota^{-1}(\xi), \iota(\nu))$, where $\iota : \mathsf{k}\langle\tau(t)^r\rangle \to \mathsf{k}\langle\tau(-t)^r\rangle$ is the isomorphism induced from $t \mapsto -t$. Furthermore, since ι is a ring-isomorphism which preserves k, we have that $\det(\iota(\xi)) = \det(\xi)$ for all $\xi \in \mathsf{k}\langle\tau(t)^r\rangle$. In particular, if $(\xi,\nu)^\star(\xi,\nu) = 1$ then $\nu = \iota(\xi)^{-1}$ and hence, $\det((\xi,\nu)) = \det(\xi)\cdot\det(\xi)^{-1} = 1$. □

Proposition 4.4.11. *Let $x \in \mathfrak{g}_1^\pm$ 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 $\boldsymbol{\tau}(c_x) = (r(c_x), S(c_x), T(c_x)) \in \mathcal{X}_n$ be the type of c_x (see Definition 4.1.1). Then*

$$\left|\mathbf{C}_{G_1^\epsilon}(x)\right| = 2^\nu q^n \prod_{d,e}\left(1+q^{-d}\right)^{S_{d,e}(m_x)}\cdot\left(1-q^{-d}\right)^{T_{d,e}(m_x)},$$

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 $|\mathbf{C}_{G_1}(x)| = 2q^n$.

Without loss of generality, we fix the basis $\mathcal{E}$ of Lemma 4.4.2, with respect to which the ambient symmetric form B^ϵ is represented by the matrix $\mathbf{d} = \mathbf{d}_\eta$, for some $\eta \in \mathsf{k}^\times$, and x is represented by the matrix Υ. Let $\mathcal{A}^\epsilon = \left\{z \in \mathbf{C}_{\mathrm{GL}_N(\mathsf{k})}(\Upsilon) \mid z^t\mathbf{d}z = \mathbf{d}\right\}$, as in Lemma 4.4.10. Let $\mathcal{N} \subseteq \mathcal{A}^\epsilon$ be the subgroup consisting of elements of the form

$$\mathfrak{X}(\xi) = \begin{pmatrix} 1 & & & 2\eta\xi^2 & 2\xi \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \\ & & & 2\eta\xi & 1 \end{pmatrix} \quad (\xi \in \mathsf{k}).$$

Note that $\mathfrak{X}$ defines a one-parameter subgroup of $\mathcal{A}^\epsilon$ of order $|\mathsf{k}| = q$. Additionally, $\mathcal{N} = \mathrm{Im}(\mathfrak{X})$ is the image under the Cayley map of the Lie-ideal generated by elements of the form $\Xi(0_{N-1}, \mathbf{u}, \mathbf{v}, 0) \in \mathfrak{g}_1$, and hence is normal in $\mathcal{A}^\epsilon$.

Let $\mathcal{H} \subseteq \mathcal{A}^\epsilon$ be the subgroup of block diagonal matrices $\Xi(\mathbf{A}, 0, 0, r)$. Note that, by (4.14) and the assumption $\Xi(\mathbf{A}, 0, 0, r)^\star \Xi(\mathbf{A}, 0, 0, r) = 1_N$, we have that $\mathbf{A}^\flat \mathbf{A} = 1_{N-1}$ and $r^2 = 1$. Additionally, since $\mathbf{A}$ commutes with the restriction of Υ to the subspace spanned by the first $N-1$ elements of $\mathcal{E}$, we have that $|\mathcal{H}| = \left|\mathrm{U}_1(\mathsf{k}\langle t^{2n-1}\rangle) \times \{\pm 1\}\right| = 4q^{n-1}$ (by the first assertion in the proof of Proposition 4.3.9).

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

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

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

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

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. Finally, I wish to acknowledge the valuable input offered by the anonymous referee.

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

References

[1] M. Artin, J.-E. Bertin, M. Demazure, A. Grothendieck, P. Gabriel, M. Raynaud, J.-P. Serre, Schémas en groupes (SGA 3), in: Séminaire de Géométrie Algébrique de l'Institut des Hautes Études Scientifiques, Institut des Hautes Études Scientifiques, Paris, 1963/1966.
[2] N. Avni, B. Klopsch, U. Onn, C. Voll, Similarity classes of integral p-adic matrices and representation zeta functions of groups of type A_2, Proc. Lond. Math. Soc. 112 (2) (2016) 267.
[3] L. Bégueri, Dualité sur un corps local à corps résiduel algébriquement clos, Mém. Soc. Math. Fr. (N.S.) 4 (1980/81) 121.
[4] A. Białynicki Birula, J.B. Carrell, W.M. McGovern, Algebraic quotients. Torus actions and cohomology. The adjoint representation and the adjoint action, in: Invariant Theory and Algebraic Transformation Groups, II, in: Encyclopaedia of Mathematical Sciences, vol. 131, Springer-Verlag, Berlin, 2002, II.
[5] A. Borel, Linear Algebraic Groups, Graduate Texts in Mathematics, Springer, New York, 1991.
[6] S. Bosch, W. Lütkebohmert, M. Raynaud, Néron Models, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas, vol. 21, Springer-Verlag, Berlin, 1990.
[7] N. Bourbaki, Algèbres de Lie, in: Groupes et Algèbres de Lie, seconde édition, in: Éléments de mathématique, vol. XXVI, Actualités Scientifiques et Industrielles, No. 1285. Hermann, Paris, 1971.
[8] J.R. Britnell, Cyclic, separable and semisimple transformations in the finite conformal groups, J. Group Theory 9 (5) (2006) 571–601.

[9] C. Bushnell, A. Fröhlich, Gauss Sums and p-adic Division Algebras, Lecture Notes in Mathematics, Springer, 1983.
[10] A. Cayley, Sur quelques propriétés des déterminants gauches, J. Reine Angew. Math. 32 (1846) 119–123.
[11] M. Demazure, P. Gabriel, Introduction to Algebraic Geometry and Algebraic Groups, North-Holland Mathematics Studies, vol. 39, North-Holland Publishing Co., Amsterdam–New York, 1980. Translated from the French by J. Bell.
[12] J. Dieudonné, A. Grothendieck, Éléments de géométrie algébrique, Inst. Hautes Études Sci. Publ. Math. 4 (8, 11, 17, 20, 24), 28, 32 (1961–1967).
[13] D.S. Dummit, R.M. Foote, Abstract Algebra, 3rd edition, John Wiley and Sons, Inc., 2004.
[14] J. Fulman, R. Guralnick, The number of regular semisimple conjugacy classes in the finite classical groups, Linear Algebra Appl. 439 (2) (2013) 488–503.
[15] J. Fulman, P.M. Neumann, C.E. Praeger, A generating function approach to the enumeration of matrices in classical groups over finite fields, Mem. Am. Math. Soc. 176 (830) (2005), vi+90.
[16] M.J. Greenberg, Schemata over local rings, Ann. Math. 73 (3) (1961) 624–648.
[17] M.J. Greenberg, Schemata over local rings: II, Ann. Math. 78 (2) (1963) 256–266.
[18] G. Hill, Regular elements and regular characters of $\mathrm{GL}_n(\mathfrak{O})$, J. Algebra 174 (1995) 610–635.
[19] J.E. Humphreys, Introduction to Lie Algebras and Representation Theory, Graduate Texts in Mathematics, vol. 9, Springer-Verlag, New York–Berlin, 1978. Second printing, revised.
[20] J.E. Humphreys, Conjugacy Classes in Semisimple Algebraic Groups, reprint ed., Mathematical Surveys and Monographs, vol. 043, American Mathematical Society, 1995.
[21] I.M. Isaacs, Character Theory of Finite Groups, AMS Chelsea Publishing, Providence, RI, 2006. Corrected reprint of the 1976 original [Academic Press, New York; MR0460423].
[22] R. Krakovski, U. Onn, P. Singla, Regular characters of groups of type A_n over discrete valuation rings, J. Algebra 496 (2018) 116–137.
[23] S. Lang, Algebraic groups over finite fields, Am. J. Math. 78 (1956) 555–563.
[24] N. Lemire, V.L. Popov, Z. Reichstein, Cayley groups, J. Am. Math. Soc. 19 (4) (2006) 921–967.
[25] G.J. McNinch, Faithful representations of SL_2 over truncated Witt vectors, J. Algebra 265 (2) (2003) 606–618.
[26] G.J. McNinch, The centralizer of a nilpotent section, Nagoya Math. J. 190 (2008) 129–181.
[27] P.M. Neumann, C.E. Praeger, Cyclic matrices over finite fields, J. Lond. Math. Soc. (2) 52 (2) (1995) 263–284.
[28] P.M. Neumann, C.E. Praeger, Cyclic matrices in classical groups over finite fields, J. Algebra 234 (2) (2000) 367–418. Special issue in honor of Helmut Wielandt.
[29] J. Serre, Local Fields, Graduate Texts in Mathematics, Springer, New York, 1995.
[30] S. Shechter, Characters of the norm-one units of local division algebras of prime degree, J. Algebra 474 (2017) 134–165.
[31] T. Shintani, On certain square integrable irreducible unitary representations of some $\mathfrak{p}$-adic linear groups, Proc. Jpn. Acad., Ser. A, Math. Sci. 44 (1) (1968) 1–3.
[32] T. Springer, R. Steinberg, Conjugacy classes, in: Seminar on Algebraic Groups and Related Finite Groups, in: Lecture Notes in Mathematics, vol. 131, Springer Berlin Heidelberg, 1970, pp. 167–266.
[33] A. Stasinski, Reductive group schemes, the Greenberg functor, and associated algebraic groups, J. Pure Appl. Algebra 216 (5) (2012) 1092–1101.
[34] A. Stasinski, Representations of GL_N over finite local principal ideal rings – an overview, in: Around Langlands Correspondences, in: Contemp. Math., vol. 691, American Mathematical Society, January 2017, pp. 336–358.
[35] A. Stasinski, S. Stevens, The regular representations of GL_N over finite local principal ideal rings, 2016.
[36] R. Steinberg, Conjugacy Classes in Algebraic Groups, Lecture Notes in Mathematics, Springer, 1974.
[37] K. Takase, Regular characters of $GL_n(O)$ and Weil representations over finite fields, J. Algebra 449 (2016) 184–213.
[38] K. Takase, Regular irreducible characters of a hyperspecial compact group, ArXiv e-prints (Jan. 2017).
[39] G.E. Wall, On the conjugacy classes in the unitary, symplectic and orthogonal groups, J. Aust. Math. Soc. 3 (2) (1963) 1–62.
[40] W.C. Waterhouse, Introduction to Affine Group Schemes, Graduate Texts in Mathematic, Springer, New York, Heidelberg, Berlin, 1979.
[41] A. Weil, Algebras with involutions and the classical groups, J. Indian Math. Soc. 24 (1960) 589–623.
[42] R. Wilson, The Finite Simple Groups, Graduate Texts in Mathematics, Springer, London, 2009.