On Regularity and Approximative Results Regarding the Representation Zeta Functions of Groups

Thesis submitted in partial fulfillment
of the requirements for the degree of
“DOCTOR OF PHILOSOPHY”

By

Shai Shechter

Submitted to the Senate of Ben-Gurion University
of the Negev

October 2, 2018

Beer-Sheva

On Regularity and Approximative Results Regarding the Representation Zeta Functions of Groups

Thesis submitted in partial fulfillment
of the requirements for the degree of
"DOCTOR OF PHILOSOPHY"

By

Shai Shechter

Submitted to the Senate of Ben-Gurion University
of the Negev

Approved by the advisor ___________________

Approve by the Dean of the Kreitman School of Advanced Graduate Studies ___________________

October 2, 2018

Beer-Sheva

This work was carried out under the supervision of

Prof. Uri Onn

In the Department of Mathematics

Faculty of Natural Sciences

Research-Student's Affidavit when Submitting the Doctoral Thesis for Judgment

I _______________, whose signature appears below, hereby declare that
(Please mark the appropriate statements):

___ I have written this Thesis by myself, except or the help and guidance offered by my Thesis Advisors.

___ The scientific materials included in this Thesis are products of my own research, culled from the period during which I was a research student.

___ This Thesis incorporates research materials produced in cooperation with others, excluding the technical help commonly received during experimental work. Therefore, I am attaching another affidavit stating the contributions made by myself and the other participants in this research, which has been approved by them and submitted with their approval.

Date: _______________ Student's name: _______________ Signature: _______________

Acknowledgements

I am indebted to my supervisor, Uri Onn, for having introduced me to the subject of representation growth, for guiding me through my first years as a researcher and for always being available to listen and advise me throughout the past seven years.

I have learned a lot from the many researchers who have offered their time for discussing the research questions I encountered throughout my PhD, and for that I am grateful to all of them. In particular, I wish to thank Benjamin Klopsch, Nadya Gurevich, Eitan Sayag, Michael Schein, Alex Stasinski and Christopher Voll. I also wish to thank the anonymous referees of my submitted papers, from whose comments I have learned a great deal.

I am thankful to the administrative staff of the Mathematics Department at Ben Gurion university for doing their very best to allow for a suitable research environment and to keep all bureaucratic handling to its bare minimum. I also wish to thank the administrative staffs at the Heinrich Heine Institute, at Bielefeld University and at the Australian National University for making my travels to their respective institutes effortless.

Finally, and most importantly, I wish to thank my love and life partner, Mor Harpaz, for supporting me and giving me perspective whenever I lost my way throughout the process of researching and writing this dissertation. Words can not express my gratitude. I could not have done this without you.

In memory of

Ido Meir Spira z"l

and in honour of the scientist he might have been

לזכרו של

עידו מאיר שפירא ז"ל

ולמדען שיכול היה להיות

Contents

Abstract

The following thesis reports on two independent research projects undertaken as part of my PhD. Both projects originate from the study of representation growth of compact p-adic groups given as $\mathfrak{p}$-adic completions of semisimple arithmetic groups.

Let $\mathfrak{o}$ be a discrete valuation ring with residue field $\mathbb{F}_q$ of odd characteristic, and let $\mathbf{G}$ be a symplectic or special orthogonal group scheme defined over $\mathfrak{o}$. For any $\ell \in \mathbb{N}$ let G^ℓ denote the ℓ-th principal congruence subgroup of $\mathbf{G}(\mathfrak{o})$. In the first part of the thesis, we consider the *regular characters* of $\mathbf{G}(\mathfrak{o})$. A character $\chi \in \mathrm{Irr}(\mathbf{G}(\mathfrak{o}))$ is said to be regular if it is trivial on $G^{\ell+1}$, for some $\ell \geq 1$, and if its restriction to the quotient $G^\ell/G^{\ell+1} \simeq \mathrm{Lie}(\mathbf{G})(\mathbb{F}_q)$ consists of characters of minimal $\mathbf{G}(\overline{\mathbb{F}_q})$-stabilizer dimension. Our first main result in this part is the construction and enumeration of all regular characters of $\mathbf{G}(\mathfrak{o})$, for classical group schemes of the aforementioned types. Following this, we classify the regular adjoint orbits for the action of $\mathbf{G}(\mathbb{F}_q)$ on the Lie-algebra $\mathrm{Lie}(\mathbf{G})(\mathbb{F}_q)$. As a result, we obtain explicit formulae for the regular parts of the representation zeta functions of the symplectic and special orthogonal groups over $\mathfrak{o}$.

In the second part of the thesis, we consider the representation zeta function of a finite group of Lie-type $\mathbf{G}(\mathbb{F}_q)$, where $\mathbf{G}$ is a connected reductive algebraic group defined over $\mathbb{F}_q$, in comparison with the Dirichlet series

$$\epsilon_{\mathbf{g}(\mathbb{F}_q)}(s) = \sum_{[x] \in \mathrm{Ad}(\mathbf{G}(\mathbb{F}_q)) \backslash \mathbf{g}(\mathbb{F}_q)} \left| \mathbf{g}(\mathbb{F}_q) : \mathbf{C}_{\mathbf{g}(\mathbb{F}_q)}(x) \right|^{-s/2},$$

enumerating adjoint classes for the action of $\mathbf{G}(\mathbb{F}_q)$ on the $\mathbb{F}_q$-point of its Lie-algebra $\mathbf{g} = \mathrm{Lie}(\mathbf{G})$. We postulate that $\epsilon_{\mathbf{g}(\mathbb{F}_q)}$ may be considered as an approximant for the representation zeta function of $\mathbf{G}(\mathbb{F}_q)$, in a manner which we formalize in Conjecture 5.2.1. We devise a strategy for proving the approximation conjecture, using a Jordan-type decomposition of both functions, and complete the comparative analysis of the semisimple parts of both functions, for $\mathbf{G}$ semisimple of adjoint type. We state a conjectural formula for the unipotent parts, and prove it for the special linear and unitary groups, of arbitrary rank, and for the symplectic group of rank no greater than 41.

Introduction

The following thesis focuses on two main topics which arise from the study of representation growth of $\mathfrak{p}$-adic completions of arithmetic groups, the first of which is regular representations, and the second is representations of level zero, or, more generally, representations of finite reductive groups of Lie-type.

Let G be a group and, for any $n \in \mathbb{N}$, let $r_n(G) \in \mathbb{N}_0 \cup \{\infty\}$ denote the number of equivalence classes of irreducible complex valued[1] representations of G. Let $\mathrm{Irr}(G)$ denote the set of equivalence classes of irreducible representations of G. The sequence $(r_n(G))$ is the *representation growth sequence* of G. Assuming $r_n(G)$ grows at most polynomially in n, one may define the *representation zeta function of* G, to be the Dirichlet series

$$\zeta_G(s) = \sum_{n=1}^{\infty} r_n(G) n^{-s} \quad (s \in \mathbb{C}). \tag{1}$$

The abscissa of convergence α_G of G is the infimum over the set of real numbers α such that the series (1) converges on the right half plane $\{s \in \mathbb{C} : \Re(s) > \alpha\}$. This value gives the best upper approximation for the rate of polynomial growth of $(r_n(G))$, that is, it is the infimum value α such that $\sum_{j=1}^{n} r_j(G) = O(n^{\alpha+\epsilon})$ for all $\epsilon > 0$.

This thesis is concerned with the representation growth of compact p-adic groups arising as $\mathfrak{p}$-adic completions of arithmetic groups defined over a global ring. To be more precise, let F be a global field, i.e. a finite extension of either $\mathbb{Q}$ or of the field $\mathbb{F}_p(t)$ of rational functions over the finite field of p elements, and let $\mathfrak{O}$ be its ring of integers. Let $\mathbf{G}$ be a connected, simply-connected and semisimple algebraic group defined over $\mathfrak{O}$, with a fixed embedding $\mathbf{G} \hookrightarrow \mathrm{GL}_N$. The groups considered in this thesis are completions of arithmetic groups, such as the group

$$\Gamma = \mathbf{G}(\mathfrak{O}) = \mathbf{G}(F) \cap \mathrm{GL}_N(\mathfrak{O}).$$

Writing $\mathfrak{O}_\mathfrak{p}$ for the completion of $\mathfrak{O}$ at a prime $\mathfrak{p}$, the completion of Γ at the prime $\mathfrak{p}$ is $\Gamma_\mathfrak{p} = \mathbf{G}(\mathfrak{O}_\mathfrak{p})$. Over a field of characteristic 0, the representation zeta functions enumerating *continuous* irreducible representations of the groups $\Gamma_\mathfrak{p}$ play an important role in the study of the representation growth of Γ. Namely, assuming Γ has the congruence subgroup property (see [38]), the representation zeta

[1] Throughout, all representations are assumed to be complex valued. Vector spaces over fields other than $\mathbb{C}$ with an action of G by linear transformations will be called G-modules

functions of the $\Gamma_\mathfrak{p}$, as $\mathfrak{p}$ ranges over all non-zero primes of $\mathfrak{O}$, are the local factors in the Euler product decomposition

$$\zeta_\Gamma(s) = \zeta_{\mathbf{G}(\mathbb{C})}(s)^{|F:\mathbb{Q}|} \cdot \prod_{\mathfrak{p} \text{ non-zero prime}} \zeta_{\Gamma_\mathfrak{p}}(s);$$

see [36, Proposition 1.3]. For the general case, the representation zeta functions of the $\Gamma_\mathfrak{p}$'s are of independent interest.

Let us now inspect to groups $\Gamma_\mathfrak{p}$ more closely. We fix a non-zero prime $\mathfrak{p}$ of $\mathfrak{O}$ and put $\mathfrak{o} = \mathfrak{O}_\mathfrak{p}$ and $K = F_\mathfrak{p}$ for the completions of $\mathfrak{O}$ and F with respect to the $\mathfrak{p}$-adic topology. Slightly abusing notation, we write $\mathfrak{p}$ for the maximal ideal generated by $\mathfrak{p}$ in $\mathfrak{o}$ (i.e., the $\mathfrak{p}$-adic completion of $\mathfrak{p}$). Let $\mathbb{F}_q$ be the residue field of $\mathfrak{o}$, of cardinality q and characteristic p.

Put $G = \mathbf{G}(\mathfrak{o})$ and, for any $\ell \geq 1$, let G^ℓ denote the ℓ-th congruence kernel $G^\ell = G \cap \mathrm{Ker}\left(\mathrm{GL}_N(\mathfrak{o}) \to \mathrm{GL}_N(\mathfrak{o}/\mathfrak{p}^\ell)\right)$. The groups G^ℓ ($\ell \in \mathbb{N}$) form a neighbourhood base at 1 for the $\mathfrak{p}$-adic topology on G, and hence any continuous finite-dimensional representations of G factors through a finite quotient of the form G/G^j, for some $j \in \mathbb{N}$. The *level* of an irreducible representation $\rho \in \mathrm{Irr}(G)$ is the minimal integer ℓ such that ρ factors through the quotient $G/G^{\ell+1}$. For example, the set of representations of level zero, denoted by $\mathrm{Irr}^{[0]}(G)$ is identified with the set $\mathrm{Irr}(\mathbf{G}(\mathbb{F}_q))$, of representations of the finite group $\mathbf{G}(\mathbb{F}_q) \simeq G/G^1$. This set is the object of study in the second part of this thesis. In order to present the subject of the first part, we require some definitions.

0.1 Regular characters of classical groups over complete discrete valuation rings

Let $\mathbf{g}$ denote the Lie-algebra scheme of $\mathbf{G}$. As explained in Section 1.1 below, for any $\ell \geq 1$, the underlying additive group of the Lie-algebra $\mathbf{g}(\mathbb{F}_q)$ is (non-canonically) isomorphic to the quotient $G^\ell/G^{\ell+1}$, via a $\mathbf{G}(\mathbb{F}_q)$-equivariant isomorphism. For example, if one identifies G with a concrete subgroup of $\mathrm{GL}_N(\mathfrak{o})$, and $\mathbf{g}(\mathbb{F}_q)$ with a Lie-subalgebra of $\mathfrak{gl}_N(\mathbb{F}_q)$, this isomorphism may be given explicitly by $x \mapsto 1 + \pi^\ell \widetilde{x}$, where π is a uniformizer of $\mathfrak{p}$ and $\widetilde{x} \in \mathfrak{gl}_N(\mathfrak{o})$ is a lift of x. Furthermore, omitting finitely many cases of p, the existence of non-degenerate $\mathbf{G}(\mathbb{F}_q)$-invariant bilinear form on $\mathbf{g}(\mathbb{F}_q)$ gives rise to an isomorphism of $\mathbf{G}(\mathbb{F}_q)$-sets

$$\mathbf{g}(\mathbb{F}_q) \to \mathrm{Irr}(G^\ell/G^{\ell+1}), \tag{2}$$

with respect to the adjoint action of $\mathbf{G}(\mathbb{F}_q)$ on $\mathbf{g}(\mathbb{F}_q)$, twisted by a power of the Frobenius map on $\mathbf{G}(\mathbb{F}_q)$, and the coadjoint action of $\mathbf{G}(\mathbb{F}_q)$ on $\mathrm{Irr}(G^\ell/G^{\ell+1})$.

Let $\rho \in \mathrm{Irr}(G)$ be of level $\ell > 0$. By Clifford's Theorem, the restriction of ρ to G^ℓ is equal to the multiple of the sum over a single coadjoint $\mathbf{G}(\mathbb{F}_q)$-orbit of elements of $\mathrm{Irr}(G^\ell/G^{\ell+1})$, which corresponds uniquely, via (2), to an adjoint orbit in $\mathbf{g}(\mathbb{F}_q)$. We call this the *residual orbit* of ρ. The representation ρ is said to be *regular* if its residual orbit consists of regular elements of $\mathbf{g}(\mathbb{F}_q)$; that is, elements $x \in \mathbf{g}(\mathbb{F}_q)$ for which the centralizer group scheme $\mathbf{C}_{\mathbf{G}_{\mathbb{F}_q}}(x)$ is of minimal dimension among such centralizers. Here $\mathbf{G}_{\mathbb{F}_q}$ denotes the base change of $\mathbf{G}$ over $\mathbb{F}_q$.

The first part of this thesis concerns the set of regular characters in the case where $\mathbf{G}$ is a classical $\mathfrak{o}$-defined semieimple group scheme, i.e. the subgroup of $\mathrm{GL}_N \times \mathfrak{o}$ of elements preserving a fixed symmetric or antisymmetric $\mathfrak{o}$-defined bilinear form (see Section 2.1). Our first main result of this part is Theorem I, which classifies the regular characters of G in terms of their residual orbits, giving the precise number of regular representations of G of given level ℓ giving rise to a residual orbit, as well as the dimension of such a representation. This result parallels [33, Theorems B and C], for the case of $\mathbf{G}$ an $\mathfrak{o}$-group scheme of type A_n (see also [54, § 4]).

The study of regular characters was initiated by Shintani in [48], and later extended using geometric method by Hill [26]. Our results in Part I extend the analysis undertaken by Hill to general classical groups, making use of the Cayley map (see § 2.4.1) which allows us to supplement the inclusion $\mathrm{GL}_N \times \mathfrak{o} \hookrightarrow \mathfrak{gl}_N \times \mathfrak{o}$, which is central in Hill's analysis, by a birational equivalence. Once Theorem I is proved, we proceed to apply it in order to compute the regular part of the representation zeta function of the symplectic and special orthogonal groups over $\mathfrak{o}$, under the restriction that the residual characteristic of $\mathfrak{o}$ is odd; see Theorem II and Theorem III.

0.2 Approximating the representation zeta functions of finite groups of Lie-type

The second part of this thesis reports on an ongoing project attempting to relate the representation zeta function of a finite group of Lie-type $\mathbf{G}(\mathbb{F}_q)$ with the somewhat simpler Dirichlet series, enumerating adjoint classes in its Lie algebra $\mathrm{Lie}(\mathbf{G})(\mathbb{F}_q)$. Namely, letting, for this section $G = \mathbf{G}(\mathbb{F}_q)$ and $\mathfrak{g} = \mathbf{g}(\mathbb{F}_q)$, for $\mathbf{G}$ a connected reducive $\mathbb{F}_q$-defined linear algebraic group, we compare the functions

$$\zeta_G(s) = \sum_{\rho \in \mathrm{Irr}(G)} (\dim \rho)^{-s} \quad \text{and} \quad \epsilon_{\mathfrak{g}}(s) = \sum_{[x] \in \mathrm{Ad}(G)\backslash \mathfrak{g}} |\mathfrak{g} : \mathbf{C}_{\mathfrak{g}}(x)|^{-s},$$

where $\mathrm{Ad}(G)\backslash\mathfrak{g}$ is the set of orbits for the adjoint action of G on $\mathfrak{g}$, and $\mathbf{C}_{\mathfrak{g}}(x)$ is the Lie-algebra centralizer of some $x \in [x] \in \mathrm{Ad}(G)\backslash\mathfrak{g}$. Assuming $\mathrm{char}(\mathbb{F}_q) > 2$, the function $\epsilon_{\mathfrak{g}}$ is an integral linear combination of powers of q^{-s}. In contrast, the representation zeta function G is quite distant from being such a linear combination, as character dimensions of $\mathbf{G}(\mathbb{F}_q)$ are rarely powers of q. However, inspecting several cases of $\mathbf{G}(\mathbb{F}_q)$, for $\mathbf{G}$ of small dimension, one may observe that the function $\epsilon_{\mathfrak{g}}$ is, in a sense, a "good approximation" of ζ_G by a linear combination of powers of q^{-s}, in the sense that the function ζ_G admits a presentation of the form $\zeta_G(s) = \sum_{i \in I} u_i(q) v_i(q)^{-s}$, with respect to which the adjoint class function may be written as $\sum_{i=1} u_i'(q) q^{-\deg v_i \cdot s}$, with $\deg u_i = \deg u_i'$ for all $i \in I$.

Our main conjecture in Part II states that this observation is in fact an instance of a general phenomenon; see Conjecture 5.2.1. In an attempt to prove this conjecture, we make use of a Jordan type decomposition of the representation zeta function of G and the adjoint class function of $\mathfrak{g}$, which allows us to separate the analysis to semisimple classes in G and $\mathfrak{g}$, and to the comparison of unipotent representations of G and nilpotent classes of $\mathfrak{g}$.

Our main result in Chapter 7 is the comparative analysis of the semisimple classes in G and $\mathfrak{g}$, which is summarized in Theorem 7.0.1. It is undertaken in the generality of semisimple groups of adjoint type. This analysis leads us to a conjectural formula for the comparison of Dirichlet series enumerating nilpotent classes in $\mathfrak{g}$ with a finite sum of Dirichlet series, enumerating the unipotent representations of G and of a certain family of subgroups of G (viz. centralizers of isolated elements); see (8.2). This conjectural formula is verified in certain specific cases in Chapter 8; see Theorem 8.0.1.

0.3 Supplementary remarks

The results reported upon in this dissertation comprise a substantial portion of the research performed during my PhD studies. In addition to those, during this time I have also extended the results of my M.Sc. thesis, computing the representation zeta function of the norm-one subgroup of a division algebra of prime degree over a compact discrete valuation ring of odd residual characteristic, different than the degree of the algebra, in a paper published in the Journal of Algebra; see [46]. I also took part in writing a joint paper with C. Voll and A. Carnevale, computing the so-called *image zeta function* of the Lie-algebra of traceless matrices over a complete discrete valuation ring of arbitrary characteristic. This paper was published in the Israel Journal of Mathematics [12].

Part I

Regular characters of classical groups over complete discrete valuation rings

Chapter 1

Outline and main results of Part I

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 $\mathbb{F}_q$ of odd characteristic. Let q and p denote the cardinality and characteristic of $\mathbb{F}_q$, 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 part of the dissertation 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 present below.

The results described in this part of the dissertation were submitted for publication, and are now in advanced stages of review with the Journal of Pure and Applied Algebra. They have been thoroughly revised, following an initial referee report, and a final referee report, requesting additional minor changes, was sent to me in September 2018. The submitted manuscript is available online; see [47].

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

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 a G-equivariant isomorphism of abelian groups between $\mathbf{g}(\mathbb{F}_q)$ and the quotient group $G^\ell/G^{\ell+1}$, for any $\ell \geq 1$ (see [16, II, §4, no. 3]). In the notation of [16], 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 $\mathbf{G}(\mathbb{F}_q)$, making the isomorphism above $\mathbf{G}(\mathbb{F}_q)$-equivariant, with respect to the ℓ-th Frobenius twist of the adjoint action of $\mathbf{G}(\mathbb{F}_q)$ on $\mathbf{g}(\mathbb{F}_q)$ (see [15, § A.6]). Additionally, by the assumption $\mathrm{char}(\mathbb{F}_q) \neq 2$ and [51, I, Lemma 5.3], the underlying additive group of $\mathbf{g}(\mathbb{F}_q)$ can be naturally identified with its Pontryagin dual in a $\mathbf{G}(\mathbb{F}_q)$-equivariant manner. Consequently, there exists an isomorphism of $\mathbf{G}(\mathbb{F}_q)$-spaces

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

Let $\chi \in \mathrm{Irr}(G)$ have level $\ell > 0$. Consider the restriction χ_{G^ℓ} of χ to G^ℓ. By Clifford's Theorem and the definition of level, the restricted character χ_{G^ℓ} is equal to a multiple of the sum over a single $\mathbf{G}(\mathbb{F}_q)$-orbit of characters of $G^\ell/G^{\ell+1}$. Using (1.1), this orbit corresponds to a single $\mathbf{G}(\mathbb{F}_q)$-orbit in $\mathbf{g}(\mathbb{F}_q)$, which we call the **residual orbit of** χ, and denote $\Omega_1(\chi) \in \mathrm{Ad}\left(\mathbf{G}(\mathbb{F}_q)\right)\backslash\mathbf{g}(\mathbb{F}_q)$.

1.1.2 Regular characters

Let $\boldsymbol{k}$ be a fixed algebraic closure of $\mathbb{F}_q$. An element of $\mathbf{g}(\boldsymbol{k})$ is said to be **regular** if its centralizer in $\mathbf{G}(\boldsymbol{k})$ has minimal dimension among such centralizers (cf. [56, § 3.5]). By extension, an element of $\mathbf{g}(\mathbb{F}_q)$ is said to be regular if its image under the natural inclusion of $\mathbf{g}(\mathbb{F}_q)$ into $\mathbf{g}(\boldsymbol{k})$ 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 $\mathbf{g}(\mathbb{F}_q)$.

For a general overview of regular elements in reductive algebraic groups over algebraically closed fields, we refer to [51, Ch. III]. The definition of regular characters goes back to Shintani [48], who, motivated by the study of unitary square integrable representations of $\mathrm{GL}_N(K)$, defined the notion of *quasi-regular* elements of $\mathrm{M}_N(\mathfrak{o}_m)$ in terms of minimal polynomial degree of their images in $\mathrm{M}_N(\mathbb{F}_q) \simeq \mathrm{M}_N(\mathfrak{o}_m)/\mathfrak{p}\,\mathrm{M}_N(\mathfrak{o}_m)$, and constructed irreducible representations of $\mathrm{GL}_N(\mathfrak{o})$ associated to the adjoint orbit in $\mathrm{M}_N(\mathfrak{o}_m)$ containing such elements, under the assumption of m even. Subsequently, and independently, Hill gave a more geometrically oriented definition of regularity, by minimality of centralizer dimension, which he showed to be equivalent to Shintani's definition in [26]. In *loc. cit.* Hill also extended Shintani's construction of characters to a larger family, including certain regular characters of odd level, i.e. associated to regular orbits in $\mathrm{M}_N(\mathfrak{o}_m)$ for m odd. This construction was further generalized by Takase in [59] to regular characters associated to regular adjoint orbits with separable minimal polynomial modulo $\mathfrak{p}$, under the assumption of odd residue field characteristic. Finally, two independent constructions of the regular characters of $\mathrm{GL}_N(\mathfrak{o})$ have recently been found. In [33], Krakowski, Onn and Singla completed the classification and enumeration of all irreducible characters of $\mathrm{GL}_N(\mathfrak{o})$ and $\mathrm{GU}_N(\mathfrak{o})$ in odd residual characteristic, further generalizing the construction of [26]. Simultaneously, in [54], Stasinski and Stevens gave an independent construction of regular characters of $\mathrm{GL}_N(\mathfrak{o})$, which is free of restrictions on the characteristic of $\mathbb{F}_q$, completing the classification of all regular character of $\mathrm{GL}_N(\mathfrak{o})$. The construction described in [33] has also been implemented to the study of representations of the group of norm-one elements of division algebras of prime Schur index over K in [46]. For a more comprehensive overview of the study regular characters of $\mathrm{GL}_N(\mathfrak{o})$, we refer the reader to [53].

1.2 Regular elements and regular characters

Following [26], we begin our investigation of regular characters with the study of regular elements in the finite Lie rings $\mathbf{g}(\mathfrak{o}_m)$, where $\mathfrak{o}_m = \mathfrak{o}/\mathfrak{p}^m$ (see Definition 3.1.1).

A central feature of the analysis undertaken in [26] is the introduction and application of geometric methods to the study of regular characters. Given $x \in \mathrm{M}_N(\mathfrak{o})$ and $m \in \mathbb{N}$, let x_m denote the image of x in $\mathrm{M}_N(\mathfrak{o}_m)$ under the reduction map. The condition of commuting with x_m defines a closed $\mathfrak{o}_m$-group subscheme of the fiber product[1] $\mathrm{GL}_N \times \mathfrak{o}_m$, which, upon application of the Greenberg functor, defines a $\mathbb{F}_q$-group scheme [24, § 4, Main Theorem.(5)]. The element x_m is said to be **regular** if the group scheme thus obtained is of minimal dimension among such group schemes (see [26, Definition 3.2]). In [26, Theorem 3.6], Hill proved that $x_m \in \mathrm{M}_n(\mathfrak{o}_m)$ is regular if and only if its image $x_1 \in \mathrm{M}_n(\mathbb{F}_q)$ is regular. Additionally, regularity of x_m was shown to be equivalent to the cyclicity of the module $\mathfrak{o}_m^N$ over the ring $\mathfrak{o}_m[x_m] \subseteq \mathrm{M}_N(\mathfrak{o}_m)$. We note that Hill's definition of regularity is equivalent to Shintani's definition of *quasi-regularity* [48, § 2].

The equivalence of regularity over the ring $\mathfrak{o}_m$ and over $\mathbb{F}_q$ was recently extended to general semisimple groups of type A_n in [33]. In Section 3.2 we further extend this equivalence of to the generality of classical groups of type B_n, C_n and D_n in odd characteristic. However, the equivalence of regularity of an element $x_m \in \mathbf{g}(\mathfrak{o}_m)$ with the cyclicity of the module $\mathfrak{o}_m^N$ over $\mathfrak{o}_m[x_m]$, 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 (Theorem 3.1.3), 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 a character lying over a given regular orbit and enumerate the characters of G lying above such an orbit. Consequently, we deduce our first main result.

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 $\Omega \subseteq \mathbf{g}(\mathbb{F}_q)$ be an 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 $\frac{|\mathbf{G}(\mathbb{F}_q)|}{|\Omega|} \cdot q^{(\ell-1)n}$.*

[1]The notation $\mathbf{G} \times \mathfrak{o}_m$ is shorthand for the fiber product $\mathbf{G} \times_{\mathrm{Spec}\,\mathfrak{o}} \mathrm{Spec}\,\mathfrak{o}_m$. Similar notation is used whenever the base change being performed is between spectra of rings, and the base ring of the given schemes is understood from context.

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

1.2.1 Regular representation zeta functions

Theorem I has an application to the study of representation growth of the group G. Namely, when attempting to compute the representation zeta function $\zeta_G(s) = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^{-s}$, one may initially restrict to the collection of the regular representation zeta function of G, 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.

Corollary 1.2.1. *Let* $X \subseteq \mathrm{Ad}(\mathbf{G}(\mathbb{F}_q)) \backslash \mathbf{g}(\mathbb{F}_q)$ *denote the set of orbits consisting of regular elements, and let*

$$\mathfrak{D}_{\mathbf{g}(\mathfrak{o})}(s) = \sum_{\Omega \in X} |\mathbf{G}(\mathbb{F}_q)| \cdot |\Omega|^{-(s+1)}, \quad (s \in \mathbb{C}). \tag{1.2}$$

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.*

1.3 Classification of regular orbits in $\mathbf{g}(\mathbb{F}_q)$

The second goal of this part of the thesis is to compute the regular representation zeta function of the symplectic and special orthogonal groups over $\mathfrak{o}$. In view of Corollary 1.2.1, to do so, one must classify and enumerate the regular orbits in $\mathbf{g}(\mathbb{F}_q)$, under the adjoint action of $\mathbf{G}(\mathbb{F}_q)$. The study of regular orbits for the action of a classical group over a finite field on its Lie-algebra already has a rather extensive tradition, most prominently in [60] (see also [10, 22, 23, 43]). In Chapter 4 we carry out a self-contained analysis of the regular adjoint orbits in $\mathbf{g}(\mathbb{F}_q)$, the consequences of which are summarized in Theorems 4.1.2 and 4.1.3. Our analysis in this section yields a uniform formula for the regular representation zeta function of each of the classical groups in question, whose terms are given by polynomials in the cardinality of $\mathbb{F}_q$.

Given $n \in \mathbb{N}$ let $\mathfrak{X}_n$ 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

$$r + \sum_{d,e=1}^{n} de\,(S_{d,e} + T_{d,e}) = n. \tag{1.3}$$

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

$$c^{\boldsymbol{\tau}}(t) = t^n \prod_{d,e} (1 + t^{-d})^{S_{d,e}} (1 - t^{-d})^{T_{d,e}} \tag{1.4}$$

and let $u_1(q) = |\mathrm{Sp}_{2n}(\mathbb{F}_q)| = |\mathrm{SO}_{2n+1}(\mathbb{F}_q)|$. 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., [63, § 3.5 and § 3.2.7]). Additionally, for any $\boldsymbol{\tau} \in \mathfrak{X}_n$, 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 § 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 $\boldsymbol{\tau} = (r, S, T) \in \mathfrak{X}_n$ 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 finite Dirichlet series $\mathfrak{D}_{\mathbf{g}(\mathfrak{o})}(s)$ (see (1.2)) is given by

$$\mathfrak{D}_{\mathbf{g}(\mathfrak{o})}(s) = \sum_{\boldsymbol{\tau} \in \mathfrak{X}_n} 4^{\nu(\boldsymbol{\tau})} M_{\boldsymbol{\tau}}(q) \cdot c^{\boldsymbol{\tau}}(q) \cdot \left(\frac{u_1(q)}{2^{\nu(\boldsymbol{\tau})} c^{\boldsymbol{\tau}}(q)} \right)^{-s}. \tag{1.5}$$

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 denote the group schemes whose groups of $\mathbb{F}_q$-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 $u_2^{\epsilon}(q) = |\mathrm{SO}_{2n}^{\epsilon}(\mathbb{F}_q)|$. 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 [63, § 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 $\mathfrak{X}_n^0$ denote the set of triplets $\boldsymbol{\tau} = (r, S, T) \in \mathfrak{X}_n$ with $r = 0$, and let $\mathfrak{X}_n^{0,+1}$ denote the subset of $\mathfrak{X}_n^0$ consisting of elements $(0, S, T)$ such that $\sum_{d,e} e S_{d,e}$ is even and $\mathfrak{X}_n^{0,-1} = \mathfrak{X}_n^0 \smallsetminus \mathfrak{X}_n^{0,+1}$.

The finite Dirichlet series $\mathfrak{D}_{\mathbf{g}(\mathfrak{o})}$ (see (1.2)) is given by

$$\mathfrak{D}_{\mathbf{g}^{\epsilon}(\mathfrak{o})}(s) = \sum_{\boldsymbol{\tau} \in \mathfrak{X}_n^{0,\epsilon}} M_{\boldsymbol{\tau}}(q) \cdot c^{\boldsymbol{\tau}}(q) \cdot \left(\frac{u_2^{\epsilon}(q)}{c^{\tau}(q)} \right)^{-s} + \sum_{\boldsymbol{\tau} \in \mathfrak{X}_n \smallsetminus \mathfrak{X}_n^0} 4 \cdot M_{\boldsymbol{\tau}}(q) \cdot c^{\boldsymbol{\tau}}(q) \cdot \left(\frac{u_2^{\epsilon}(q)}{2 \cdot c^{\tau}(q)} \right)^{-s}. \tag{1.6}$$

1.4 Organization of Part I

In Chapter 2 we recall the necessary preliminaries for the proof of Theorem I, specifically regarding the Greenberg functor and the Cayley map. We also set up the basic definitions and recall some basic properties of classical group schemes. Chapter 3 contains basic structural results regarding the regular orbits of $\mathbf{g}(\mathfrak{o})$ and regular characters of $\mathbf{G}(\mathfrak{o})$, which lead to the proof of Theorem I. Finally, as already mentioned, in Chapter 4 we undertake the classification of the regular adjoint orbits of $\mathbf{g}(\mathbb{F}_q)$ and compute the regular representation zeta function of $\mathbf{G}(\mathfrak{o})$, and complete the proof of Theorems II and III.

Chapter 2

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. [61, § 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 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 $\operatorname{diag}(\nu_1, \dots, \nu_N)$, satisfying $\nu_{2i} = \nu_{2i-1}^{-1}$ for all $i = 1, \dots, \lfloor N/2 \rfloor$, and with $\nu_N = 1$ if N is odd. In particular, the absolute rank of the generic fiber of $\mathbf{G}$ is $n = \dim(\mathbf{T} \times_{\operatorname{Spec} \mathfrak{o}} \operatorname{Spec} L) = \lfloor N/2 \rfloor$, for $L = \overline{K}$ the algebraic closure of K.

Under this embedding, the Lie-algebra $\mathbf{t}(L)$ consists of diagonal matrices $\operatorname{diag}(\nu_1, \dots, \nu_N)$, with $\nu_{2i} = -\nu_{2i-1}$ for all $i = 1, \dots, n$ 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. Let $\lambda_1, \dots, \lambda_t \in L$ be such that $\{\pm\lambda_1, \dots, \pm\lambda_t\}$ is the set of all non-zero eigenvalues of s, with $\lambda_i \neq \pm\lambda_j$ whenever $i \neq j$, and let $m_1, \dots, m_t$ be their respective algebraic multiplicities. 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 $B = B_L$ to (a non-degenerate bilinear form on) $\operatorname{Ker}(s)$, the eigenspace associated with the eigenvalue 0.

Proof. Let $V = L^N$ the 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 $W_\lambda = \operatorname{Ker}(s - \lambda \mathbf{1})$. 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 [5, 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 $\dim_L W_\lambda = \dim_L W_{-\lambda}$. Invoking Witt's Theorem [60, § 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 $W_0 = \operatorname{Ker}(s)$ 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. $\square$

2.2 Artinian principal ideal rings

Let $\overline{K}$ be a fixed algebraic closure of K and let K^{unr} be the maximal unramified extension of K in $\overline{K}$. 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 $\boldsymbol{k}$ of $\mathbb{F}_q$. Given $m \in \mathbb{N}$ we put $\mathfrak{o}_m := \mathfrak{o}/\mathfrak{p}^m$ and $\mathfrak{O}_m := \mathfrak{O}/\mathfrak{P}^m$ and write $\eta_m : \mathfrak{O} \to \mathfrak{O}_m$ and $\eta_{m,r} : \mathfrak{O}_m \to \mathfrak{O}_r$ for the reduction maps, for any $1 \leq r \leq m$. The notation η_m and $\eta_{m,r}$ is also used to denote the coordinatewise reduction map on $\mathrm{M}_N(\mathfrak{O})$ and $\mathrm{M}_N(\mathfrak{O}_m)$, respectively.

The map η_1 admits a canonical splitting map $s : \boldsymbol{k} \to \mathfrak{O}$, which restricts to a homomorphic embedding of $\boldsymbol{k}^\times$ into $\mathfrak{O}^\times$, and satisfies $s(0) = 0$; see [45, 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 $\mathfrak{O}_m \to \mathfrak{O}_m$ for any $m \geq 1$ whose fixed subring is $\mathfrak{o}_m$. In the special case $m = 1$, the map $\sigma : \boldsymbol{k} \to \boldsymbol{k}$ is given by the ordinary Frobenius map $F_q = (x \mapsto x^q)$, where $q = |\mathbb{F}_q|$.

2.3 The Greenberg functor

The Greenberg functor was introduced in [24] and [25], as a generalization of Shimura's reduction mod $\mathfrak{p}$ functor to higher powers of $\mathfrak{p}$. Given an artinian 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 characteristic 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 [45, Ch. II,§ 6]. For further introduction we refer to [8, p. 276].

Our application of the Greenberg functor is focused on the artinian principal ideal rings $\mathfrak{O}_m$. For any m, we let $\mathbf{G}_{\mathfrak{O}_m} = \mathbf{G} \times \mathfrak{O}_m$ and $\mathbf{g}_{\mathfrak{O}_m} = \mathbf{g} \times \mathfrak{O}_m$ denote the base change of the group and Lie-algebra schemes $\mathbf{G}$ and $\mathbf{g}$. Put $\boldsymbol{\Gamma}_m = \mathcal{F}_{\mathfrak{O}_m}(\mathbf{G}_{\mathfrak{O}_m})$ and $\boldsymbol{\gamma}_m = \mathcal{F}_{\mathfrak{O}_m}(\mathbf{g}_{\mathfrak{O}_m})$. Given $r \leq m$, we write $\eta^*_{m,r}$ to denote the connecting maps $\boldsymbol{\Gamma}_m \to \boldsymbol{\Gamma}_r$ and $\boldsymbol{\gamma}_m \to \boldsymbol{\gamma}_r$, and put $\boldsymbol{\Gamma}^r_m = (\eta^*_{m,r})^{-1}(1) = \mathrm{Spec}(\kappa(1)) \times_{\boldsymbol{\Gamma}_r} \boldsymbol{\Gamma}_m$ (the scheme-theoretic group kernel) and $\boldsymbol{\gamma}^r_m = (\eta^*_{m,r})^{-1}(0) = \mathrm{Spec}(\kappa(0)) \times_{\boldsymbol{\gamma}_r} \boldsymbol{\gamma}_m$

(the scheme-theoretic Lie-algebra kernel). Here, the notation $\kappa(\cdot)$ stands for the residue field at a rational point of a scheme.

Note that, a priori, the connecting morphism between a scheme and its base change is dependent on the scheme in question as well. The apparent abuse of notation in writing $\eta^*_{m,r}$ for the connecting morphisms of different schemes is made permissible by the following lemma, whose proof is essentially included in [24].

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

Proof. The case $\mathbf{X} = \mathbb{A}^k_{\mathfrak{O}_m}$ is [24, Corollary 2, § 5]. In the general case, by properties of base change, the inclusion $\mathbf{X} \times \mathfrak{O}_r \subseteq \mathbb{A}^k_{\mathfrak{O}_r}$ is simply the base change over $\mathrm{Spec}(\mathfrak{O}_r)$ of the inclusion morphism $\mathbf{X} \subseteq \mathbb{A}^k_{\mathfrak{O}_m}$. The lemma follows from Assertion 2 of the Main Theorem (preservation of arbitrary immersions) and Corollary 4, § 5, of [24]. $\square$

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

Lemma 2.3.2. *For $m \in \mathbb{N}$ fixed, we have*

1. *The rings $\mathfrak{O}_m$ are the $\boldsymbol{k}$-points of an m-dimensional algebraic ring scheme $\mathbf{O}_m$ over $\boldsymbol{k}$.*

   The canonical map $s : \boldsymbol{k} \to \mathfrak{O}_m$ defines a closed embedding $s^* : \mathbb{A}^1_{\boldsymbol{k}} \to \mathbf{O}_m$ of the affine line over $\boldsymbol{k}$ into this ring variety. The restriction of s^* to the multiplicative group $\mathbb{G}_m \subseteq \mathbb{A}^1_{\boldsymbol{k}}$ is a monomorphism of $\boldsymbol{k}$-linear algebraic groups, satisfying $\eta^*_{m,1} \circ s^* = \mathbf{1}_{\mathbb{A}^1_{\boldsymbol{k}}}$.

2. *The group $\mathbf{\Gamma}_m$ is a $d \cdot m$-dimensional linear algebraic group over $\boldsymbol{k}$. Moreover, if $\Delta \subseteq \mathbf{G}_{\mathfrak{O}_m}$ is a smooth closed sub-$\mathfrak{O}_m$-group scheme, then $\mathcal{F}_{\mathfrak{O}_m}(\Delta)$ is a smooth closed sub-$\boldsymbol{k}$-group of $\mathbf{\Gamma}_m$ of dimension $d' \cdot m$.*

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

4. *The connecting morphisms $\eta^*_{m,r}$, for $r \leq m$, give rise to surjective $\boldsymbol{k}$-group scheme morphism $\mathbf{\Gamma}_m \to \mathbf{\Gamma}_r$. Similarly, for $\boldsymbol{\gamma}_m \to \boldsymbol{\gamma}_r$, these are surjective Lie-ring morphisms.*

5. *The adjoint action of $\mathbf{G}_{\mathfrak{O}_m}$ on the Lie-ring scheme $\mathbf{g}_{\mathfrak{O}_r}$ with $r \leq m$, induces an action of the algebraic group $\mathbf{\Gamma}_m$ on $\boldsymbol{\gamma}_r$. The application of $\mathcal{F}_{\mathfrak{O}_m}$ preserves centralizers of $\mathfrak{O}_r$-rational points of $\mathbf{g}_{\mathfrak{O}_r}$.*

Proof. 1. See [24, § 1, Proposition 4].

2. The Greenberg functor maps $\mathfrak{O}_m$-group schemes of finite type to $\boldsymbol{k}$-group schemes of finite type by Assertion (5) of the Main Theorem (§ 4) of [24]. By [25, Corollary 1, p. 263], the group $\mathbf{\Gamma}_m$ is smooth over $\boldsymbol{k}$, and hence reduced [61, 11.6]. Thus $\mathbf{\Gamma}_m$ is a linear algebraic $\boldsymbol{k}$-group. Given $\Delta \subseteq \mathbf{G}_{\mathfrak{O}_m}$ as above, $\mathcal{F}_{\mathfrak{O}_m}(\Delta)$ is closed by [24, § 4, Proposition 8]. The assertion regarding the dimension of $\mathcal{F}_m(\Delta)$ may be proved by induction on m, the case $m = 1$ being trivially true. For $m > 1$, by [25, Corollary 2, p. 262], we have an exact sequence

$$1 \to \mathfrak{d} \to \mathcal{F}_{\mathfrak{O}_m}(\Delta) \xrightarrow{\eta^*_{m,m-1}} \mathcal{F}_{\mathfrak{O}_{m-1}}(\Delta \times \mathfrak{O}_{m-1}) \to 1$$

of $\boldsymbol{k}$-algebraic group schemes. By Greenberg's Structure Theorem [25], the kernel $\mathfrak{d}$ is an affine d'-dimensional unipotent group over $\boldsymbol{k}$. Since $\Delta \times \mathfrak{O}_{m-1}$ is a smooth closed subgroup scheme of $\mathbf{\Gamma}_{m-1}$, the assertion follows.

3. The assumption regarding dimensions in Assertion (3) follows from the Main Theorem and Proposition 4.(4), § 1, of [24]. The Lie-bracket and addition on $\mathbf{g}_{\mathfrak{O}_m}$ are transported by $\mathcal{F}_{\mathfrak{O}_m}$ to schematic morphisms $\boldsymbol{\gamma}_m \times \boldsymbol{\gamma}_m \to \boldsymbol{\gamma}_m$ by [24, Corollary 3, p.641]. The Lie-axioms on $\mathcal{F}_{\mathfrak{O}_m}(\boldsymbol{\gamma}_m)$ may be verified using compatibility of the Greenberg functor with preimages [24, Corollary 3, p. 641]. For example, the Jacobi identity can be reformulated using the equality $\mathbf{g}_{\mathfrak{O}_m} = J^{-1}(0)$, where $J : \mathbf{g}_{\mathfrak{O}_m} \times \mathbf{g}_{\mathfrak{O}_m} \times \mathbf{g}_{\mathfrak{O}_m} \to \mathbf{g}_{\mathfrak{O}_m}$ is the morphism satisfying $J(R)(x, y, z) = [[x, y], z] + [[y, z], x] + [[z, x], y]$ for any $\mathfrak{O}_m$-algebra R and $x, y, z \in \mathbf{g}_{\mathfrak{O}_m}(R)$.

4. The connecting map is shown to be a group homomorphism in [24, § 5, Corollary 5], and the preservation of the Lie-bracket follows similarly from [24, § 5, Corollary 2]. Its surjectivity follows from the smoothness of $\mathbf{G}_{\mathfrak{O}_m}$ (resp. $\boldsymbol{\gamma}_{\mathfrak{O}_m}$), and [25, Corollary 2, p. 262].

5. The action of $\mathbf{\Gamma}_m$ on $\boldsymbol{\gamma}_r$ is given by $\mathcal{F}_{\mathfrak{O}_r}(\alpha_r) \circ (\eta^*_{m,r} \times \mathbf{1}_{\boldsymbol{\gamma}_r}) : \mathbf{\Gamma}_m \times \boldsymbol{\gamma}_r \to \boldsymbol{\gamma}_r$, where $\alpha_r : \mathbf{G}_{\mathfrak{O}_r} \times \mathbf{g}_{\mathfrak{O}_r} \to \mathbf{g}_{\mathfrak{O}_r}$ is the adjunction map; see [52, § 3]. One notes easily that, since the group $\mathbf{\Gamma}^r_m$ acts trivially on $\boldsymbol{\gamma}_r$, this action commutes pointwise with the bijection (2.5). The preservation of centralizers follows from [52, Proposition 3.6], by taking $\mathbf{Y}$ and $\mathbf{Z}$ to be the sub-schemes defined by the spectrum of the reside field of $\mathbf{g}_{\mathfrak{O}_r}$ at the given rational point.

□

Remark 2.3.3. In the case where $\mathfrak{O}_m$ is a $\boldsymbol{k}$-algebra, Lemma 2.3.2.(3) may be somewhat strengthened, as in this case $\boldsymbol{\gamma}_m$ can be shown to coincide with the Lie-algebra of $\mathbf{\Gamma}_m$. In unequal characteristic, the equality $\boldsymbol{\gamma}_m = \mathrm{Lie}(\mathbf{\Gamma}_m)$ is usually false, e.g. for $\mathbf{G} = \mathbb{G}_a \times \mathfrak{O}$, the additive group scheme over $\mathfrak{O}$, it holds that $\boldsymbol{\gamma}_2(\boldsymbol{k})$ is the ring of Witt vectors of length 2 over $\boldsymbol{k}$, while $\mathrm{Lie}(\mathbf{\Gamma}_2)(\boldsymbol{k})$ is a $\boldsymbol{k}$-vector space of dimension 2. In any event, this equality will not be necessary for our purposes.

We also require the following lemma.

Lemma 2.3.4. *For any $r, m \in \mathbb{N}$ with $r \leq m$, there exists a monomorphism of the underlying additive group schemes $v^*_{m,r} : \boldsymbol{\gamma}_{m-r} \to \boldsymbol{\gamma}_m$, such that*

1. *for any* $y \in \boldsymbol{\gamma}_{m-r}(\boldsymbol{k}) = \mathbf{g}(\mathfrak{O}_{m-r})$*, it holds that* $v^*_{m,r}(\boldsymbol{k})(y) = \pi^r \widetilde{y}$*, where* $\widetilde{y} \in \mathbf{g}(\mathfrak{O}_m)$ *is such that* $\eta_{m,m-r}(\widetilde{y}) = y$*;*

2. *the sequence* $0 \to \boldsymbol{\gamma}_{m-r} \xrightarrow{v^*_{m,r}} \boldsymbol{\gamma}_m \xrightarrow{\eta^*_{m,r}} \boldsymbol{\gamma}_r \to 0$ *is exact;*

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

$$\begin{tikzcd} \boldsymbol{\gamma}_m \arrow[r, "\mathrm{ad}(v^*_{m,r}(y))"] \arrow[d, "\eta^*_{m,m-r}"'] & \boldsymbol{\gamma}_m \\ \boldsymbol{\gamma}_{m-r} \arrow[r, "\mathrm{ad}(y)"] & \boldsymbol{\gamma}_{m-r}, \arrow[u, "v^*_{m,r}"'] \end{tikzcd} \tag{2.6}$$

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

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

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

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

Applying [24, § 1, Proposition 3.(6)] to both maps of the above sequence, these define $\mathbb{F}_q$-regular maps between associated module variety structures over $\boldsymbol{k}$ of the modules above, which, in turn, define an exact sequence of $\boldsymbol{k}$-schemes

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

where the right-most map coincides with $\eta^*_{m,r}$ by the same proposition and by [24, Corollary 2, § 5]. The first and second assertions of the lemma follow.

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

Remark 2.3.5. In the case where $\mathfrak{O}$ is either a $\boldsymbol{k}$-algebra, or is absolutely unramified (i.e. $\mathfrak{P} = p\mathfrak{O}$), and thus isomorphic to the ring $W(\boldsymbol{k})$, the map $v^*_{m,r}$ of the lemma may be described explicitly, by fixing a suitable coordinate system for $\boldsymbol{\gamma}_m$ over $\boldsymbol{k}$ and taking $v^*_{m,r}$ to be either a coordinate shift in the former case, or given by successive applications of the verschiebung and Frobenius maps coordinatewise (see [45]) 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

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

Let $\mathrm{cay} : D \to D$ be the $\mathfrak{o}$-scheme morphism with associated comorphism $\mathrm{cay}^{\sharp}$ given on generators of $\mathfrak{o}[t_{1,1},\ldots,t_{N,N},(\det(1+\mathbf{t}))^{-1}]$ 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 automorphism of D.

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 $R=\boldsymbol{k}$, the sets $(D\cap \mathbf{g})(\boldsymbol{k})$ and $(D\cap \mathbf{G})(\boldsymbol{k})$ are principal open subsets of $\boldsymbol{\gamma}(\boldsymbol{k})$ and $\boldsymbol{\Gamma}(\boldsymbol{k})$ respectively[1]. Using the description of $\mathbf{g}$ and $\mathbf{G}$ given in § 2.1.1, one verifies that the restriction of $\mathrm{cay}(\boldsymbol{k})$ to $(D\cap\mathbf{g})(\boldsymbol{k})$ defines an algebraic isomorphism of affine varieties onto $(D\cap\mathbf{G})(\boldsymbol{k})$, and hence a birational map $\mathrm{cay}(\boldsymbol{k}) : \mathbf{g}(\boldsymbol{k}) \dashrightarrow \mathbf{G}(\boldsymbol{k})$. Additionally, being given by a power series in $\mathbf{x}$ on $(D\cap\mathbf{g})(\boldsymbol{k})$, the map $\mathrm{cay}(\boldsymbol{k})$ is equivariant with respect to the conjugation action of $\mathbf{G}(\boldsymbol{k})$. The properties listed in this paragraph carry over to the associated $\boldsymbol{k}$-group schemes described in the previous section, as noted in Lemma 2.4.1 below.

The Cayley map was introduced in [14]. 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 [62, § 4]. See also [37] for a more generalized treatment of the Cayley map.

2.4.1 Properties of the Cayley map

Given $m\in\mathbb{N}$, put $D_m = D\times\mathfrak{O}_m$ and let $\mathrm{cay}_m = \mathrm{cay}\times \mathbf{1}_{\mathfrak{O}_m}$ be the base change of cay. Let $\boldsymbol{\Delta}_m = \mathfrak{F}_{\mathfrak{O}_m}(D_m)$ and $\widehat{\mathrm{cay}}_m = \mathfrak{F}_{\mathfrak{O}_m}(\mathrm{cay}_m)$. Note that, by construction and by the Main Theorem of [24], $\boldsymbol{\Delta}_m$ is an open affine subscheme of $\mathbb{A}_{\boldsymbol{k}}^{N^2 m}$.

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

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

Cay2. The map $\widehat{\mathrm{cay}}_m$ is $\boldsymbol{\Gamma}_m$-equivariant with respect to the adjoint action on $\boldsymbol{\gamma}_m$ and with respect to group conjugation on $\boldsymbol{\Gamma}_m$.

[1] Here $\cap$ denotes the scheme-theoretic intersection, $D\cap\mathbf{g} = D\times_{\mathrm{Spec}(\mathfrak{o}[t_{1,1},\ldots,t_{N,N}])}\boldsymbol{\gamma}$ and likewise for $D\cap\mathbf{G}$.

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

$$\begin{tikzcd}
\boldsymbol{\gamma}_m \arrow[r, dashed, "\widehat{\mathrm{cay}}_m"] \arrow[d, "\eta^*_{m,r}"'] & \boldsymbol{\Gamma}_m \arrow[d, "\eta^*_{m,r}"] \\
\boldsymbol{\gamma}_r \arrow[r, dashed, "\widehat{\mathrm{cay}}_r"] & \boldsymbol{\Gamma}_r.
\end{tikzcd} \tag{2.9}$$

Proof. 1. The inclusion map $D_m \cap \mathbf{g}_{\mathfrak{O}_m} \subseteq \mathbf{g}_{\mathfrak{O}_m}$ is an open immersion, and thus by Assertion (2) and (3) of the Main Theorem of [24], the $\boldsymbol{k}$-scheme $\boldsymbol{\Delta}_m \cap \boldsymbol{\gamma}_m$ is immersed as an open subscheme of $\boldsymbol{\gamma}_m$. Similarly for $\boldsymbol{\Delta}_m \cap \boldsymbol{\Gamma}_m$. By functoriality, the morphism $\widehat{\mathrm{cay}}_m$ is an isomorphism of $\boldsymbol{\Delta}_m \cap \boldsymbol{\gamma}_m$ onto $\boldsymbol{\Delta}_m \cap \boldsymbol{\Gamma}_m$, and hence $\boldsymbol{\gamma}_m$ and $\boldsymbol{\Gamma}_m$ are birationally equivalent.
To prove that $\widehat{\mathrm{cay}}_m$ 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 $\boldsymbol{\Delta}_m$ under the given inclusions into $\mathbb{A}^{N^2 m}_{\boldsymbol{k}}$. Note that by applying Greenberg's Structure Theorem [25] inductively, both $\boldsymbol{\gamma}^r_m$ and $\boldsymbol{\Gamma}^r_m$ are reduced, and thus are $\boldsymbol{k}$-varieties. Thus, by Nullstellensatz, they are determined by their $\boldsymbol{k}$-points and it suffices to show they are included in the reduced subscheme $(\boldsymbol{\Delta}_m)_{\mathrm{red}} \subseteq \boldsymbol{\Delta}_m$. This follows from the bijection (2.4), as $\boldsymbol{\gamma}^r_m(\boldsymbol{k}) = \mathbf{g}_{\mathfrak{O}_m}(\mathfrak{O}_m) \cap \eta^{-1}_{m,r}(0)$ is included in the nilradical of the matrix algebra $\mathrm{M}_N(\mathfrak{O}_m)$, and hence included in $D_m(\mathfrak{O}_m)$, and since $\boldsymbol{\Gamma}^r_m(\boldsymbol{k}) = \mathbf{G}_{\mathfrak{O}_m}(\mathfrak{O}_m) \cap \eta^{-1}_{m,r}(1) \subseteq 1 + \pi\, \mathrm{M}_N(\mathfrak{O}_m) \subseteq \mathrm{GL}_N(\mathfrak{O}_m)$, and thus (since $\mathrm{char}(\boldsymbol{k}) \neq 2$) included in $D_m(\mathfrak{O}_m)$.
Lastly, to prove that $\widehat{\mathrm{cay}}_m$ is a group homomorphism whenever $2r \geq m$, it is equivalent to show that it preserves comultiplication in the Hopf-algebra structure of the coordinate ring of $\boldsymbol{\gamma}^r_m$. Arguing as in the proof Lemma 2.3.4, it sufficient to verify this on the $\boldsymbol{k}$-points of the variety. This follows from the definition of cay (2.8), as in this case $\boldsymbol{\gamma}^r_m(\boldsymbol{k}) \subseteq \mathbf{g}_{\mathfrak{O}_m}(\mathfrak{O}_m)$ is included in an ideal of vanishing square in $\mathrm{M}_N(\mathfrak{O}_m)$ and the map $\widehat{\mathrm{cay}}_m$ coincides with the map $\mathbf{x} \mapsto 1 - 2\mathbf{x}$.

2. Property (Cay2) holds since $\mathcal{F}_{\mathfrak{O}_m}$ preserves the cartesian square (2.10), which states the $\boldsymbol{\Gamma}_m$-equivariance of cay_m. Here $\alpha_{\boldsymbol{\Gamma}_m, \mathbf{X}}$ denotes the action map of $\boldsymbol{\Gamma}_m$ on $\mathbf{X} \in \{\boldsymbol{\Gamma}_m, \boldsymbol{\gamma}_m\}$.

$$\begin{tikzcd}
\boldsymbol{\Gamma}_m \times \boldsymbol{\gamma}_m \arrow[r, "\alpha_{\boldsymbol{\Gamma}_m,\boldsymbol{\gamma}_m}"] \arrow[d, dashed, "\mathbf{1}_{\boldsymbol{\Gamma}_m} \times \mathrm{cay}_m"'] \arrow[dr, phantom, "\square"] & \boldsymbol{\gamma}_m \arrow[d, dashed, "\mathrm{cay}_m"] \\
\boldsymbol{\Gamma}_m \times \boldsymbol{\Gamma}_m \arrow[r, "\alpha_{\boldsymbol{\Gamma}_m,\boldsymbol{\Gamma}_m}"] & \boldsymbol{\Gamma}_m.
\end{tikzcd} \tag{2.10}$$

3. Finally, property (Cay3) is simply an application of [24, Corollary 4, p.645], to the case $R = \mathfrak{o}_m$, $R' = \mathfrak{o}'_m$, $\varphi = \eta_{r,m}$, $X_1 = \boldsymbol{\gamma}_m \cap D_m$, $X_2 = \boldsymbol{\Gamma}_m \cap D_m$ and $g = \mathrm{cay}_m$.

$\square$

Chapter 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 $\mathbf{G}(\mathfrak{O})$ on $\mathbf{g}(\mathfrak{O}_m)$, or, equivalently (see [52, § 3]), of $\boldsymbol{\Gamma}_m(\boldsymbol{k})$ on $\boldsymbol{\gamma}_m(\boldsymbol{k})$. The methods which we apply are influenced by [26].

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 [56, §3.5]. Following [26], this definition is extended to elements of $\boldsymbol{\gamma}_m$ with respect to the conjugation action of $\boldsymbol{\Gamma}_m$.

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

The following theorem lists the main properties of regular elements of $\boldsymbol{\gamma}_m$, which are proved in this section.

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

1. *If x_m is a regular element of $\mathbf{g}_{\mathfrak{O}_m}(\mathfrak{O}_m)$, then $\mathbf{C}_{\boldsymbol{\Gamma}_m}(x_m)$ is a $\boldsymbol{k}$-group scheme of dimension $m \cdot n$, where $n = \mathrm{rk}(\mathbf{G} \times \overline{K})$.*

2. *The element x_m is regular if and only if $x_1 = \eta_{m,1}(x_m)$ is a regular element of $\mathbf{g}(\boldsymbol{k})$.*

3. *Suppose $x_m \in \mathbf{g}(\mathfrak{O}_m)$ is regular. The restriction of the reduction map $\eta_{m,1}$ to $\mathbf{C}_{\mathbf{G}(\mathfrak{O}_m)}(x_m)$ is surjective onto $\mathbf{C}_{\mathbf{G}(\boldsymbol{k})}(x_1)$.*

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

Theorem 3.1.3. *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 $x_m = \eta_m(x)$ is regular for some $m \in \mathbb{N}$. Then*

1. $\mathbf{C}_G(x) = \varprojlim_m \mathbf{C}_{G_m}(x_m)$, *where $G = \mathbf{G}(\mathfrak{o})$ and $G_m = \mathbf{G}(\mathfrak{o}_m)$*

2. *Furthermore, x is a regular element of $\mathbf{g}(\overline{K})$.*

Theorem 3.1.3 has the following corollary.

Corollary 3.1.4. *In the notation of Theorem 3.1.3, let $x \in \mathfrak{g}$ such that $x_m = \eta_m(x)$ is a regular element of $\mathfrak{g}_m$, for some $m \in \mathbb{N}$. Then $\mathbf{C}_{G_m}(x_m)$ is abelian.*

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

We begin by examining some basic properties of the group $\mathbf{\Gamma}_m$ ($m \in \mathbb{N}$) and of centralizers of elements of $\boldsymbol{\gamma}_m$, when considered as algebraic group schemes over $\boldsymbol{k}$. The following lemma summarizes the necessary components for the proof of Theorem 3.1.2.(1), and is mostly included in [52].

Lemma 3.1.5.

1. *The group scheme $\mathbf{\Gamma}_m$ is a connected algebraic group over $\boldsymbol{k}$.*

2. *The unipotent radical of $\mathbf{\Gamma}_m$ is $\mathbf{\Gamma}_m^1$.*

3. *Let $\mathbf{T}$ be a maximal torus of $\mathbf{G}$, defined over $\mathfrak{O}$, and let $\mathbf{T}_1 = \mathbf{T} \times \boldsymbol{k} \subseteq \mathbf{\Gamma}_1$. The restriction of the map $s^* : \mathbb{A}^1_{\boldsymbol{k}} \to \mathbf{O}_m$ of Lemma 2.3.2.(1) to $\mathbb{G}_m$ extends to an embedding of $\mathbf{T}_1$ as a maximal torus in $\mathbf{\Gamma}_m$.*

4. *The centralizer of $s^*(\mathbf{T}_1)$ in $\mathbf{\Gamma}_m$ is the Cartan subgroup $\mathcal{F}_{\mathfrak{O}_m}(\mathbf{T} \times \mathfrak{O}_m)$. Moreover, $\mathcal{F}_m(\mathbf{T} \times \mathfrak{O}_m)$ is a linear algebraic $\boldsymbol{k}$-group of dimension $n \cdot m$.*

Proof. 1. Connectedness is proved in [52, Lemma 4.2]. The remainder of the assertion appears above in Lemma 2.3.2.

2. See [52, Proposition 4.3].

3. May be proved by following the argument of [26, Proposition 2.2.(2)], practically verbatim, making use of the fact that $\mathbf{\Gamma}_m$ and $\mathbf{\Gamma}_1 = \eta^*_{m,1}(\mathbf{\Gamma}_m)$ are of the same rank by the previous assertion, and that $s^*(\mathbf{T}_1)$ is a connected abelian subgroup of $\mathbf{\Gamma}_m$ of dimension $n = \mathrm{rk}(\mathbf{\Gamma}_1)$.

4. The inclusion $\mathbf{T}(\mathfrak{O}_m) \subseteq \mathbf{C}_{\mathbf{\Gamma}_m(\boldsymbol{k})}(s^*(\mathbf{T}_1)(\boldsymbol{k}))$ is clear, since $\mathbf{T}(\mathfrak{O}_m)$ is abelian and contains $s^*(\mathbf{T}_1)(\boldsymbol{k})$, by Lemma 2.3.2.(1). The inclusion $\mathbf{T} \times \mathfrak{O}_m \subseteq \mathbf{C}_{\mathbf{\Gamma}_m}(s^*(\mathbf{T}_1))$ follows (see [52, Proposition 3.2]). By [52, Theorem 4.5], $\mathcal{F}_{\mathfrak{O}_m}(\mathbf{T} \times \mathfrak{O}_m)$ is a Cartan subgroup of $\mathbf{\Gamma}_m$ and hence is equal to the centralizer of $s^*(\mathbf{T}_1)$. Finally, the statement regarding the dimension of $\mathcal{F}_m(\mathbf{T} \times \mathfrak{O}_m)$ follows from Lemma 2.3.2.(1) and [24, Proposition 4, § 1].

□

Proof of Theorem 3.1.2.(1). The alternative proof of [56, Ch. III, § 3.5, Proposition 1] shows that the minimal centralizer dimension of an element of $\mathbf{g}(\mathfrak{O}_m)$ is equal to that of a Cartan subgroup of $\mathbf{\Gamma}_m$, provided that the Cartan subgroups of $\mathbf{\Gamma}_m$ are abelian and that their union forms a dense subset of $\mathbf{\Gamma}_m$. The former of these conditions holds by [52, Theorem 4.5], and the latter by [7, IV 12.1]. $\square$

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 [26, 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 $\boldsymbol{\gamma}_m$ and of its image in $\boldsymbol{\gamma}_1$.

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

Proof. Assume towards a contradiction that the statement of the lemma is false, and let m be minimal such that $\dim \eta^*_{m,1}\left(\mathbf{C}_{\boldsymbol{\gamma}_m}(x_m)\right) < n$. Note that, since $\eta^*_{m,1} \circ \eta^*_{r,m} = \eta^*_{r,1}$ for all $r > m$ (by [24, Proposition 3, § 5]) we also have that $\dim \eta^*_{r,1}\left(\mathbf{C}_{\boldsymbol{\gamma}_r}(x_r)\right) < n$ for all $r \geq m$.

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

$$\mathbf{C}_{\boldsymbol{\gamma}_r}(x_r) \supseteq \mathbf{C}_{\boldsymbol{\gamma}_r^1}(x_r) \supseteq \ldots \supseteq \mathbf{C}_{\boldsymbol{\gamma}_r^{r-1}}(x_r) \supseteq 0, \tag{3.1}$$

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

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

where $\boldsymbol{\gamma}_r^0 = \boldsymbol{\gamma}_r$ and $\boldsymbol{\gamma}_r^r = \mathrm{Spec}(\kappa(0))$.

For any $0 \leq i \leq r-1$, the map $v^*_{i,r} : \boldsymbol{\gamma}_{r-i} \to \boldsymbol{\gamma}_r$ of Lemma 2.3.4 restricts, by Assertion (3) of the lemma, to an isomorphism of abelian $\boldsymbol{k}$-group schemes $\mathbf{C}_{\boldsymbol{\gamma}_{r-i}}(x_{r-i}) \simeq \mathbf{C}_{\boldsymbol{\gamma}_r^i}(x_r)$, which restricts further, by Assertion (4) of the lemma, to an isomorphism $\mathbf{C}_{\boldsymbol{\gamma}_r^{i+1}}(x_r) \simeq \mathbf{C}_{\boldsymbol{\gamma}_{r-i}^1}(x_{r-i})$. Using these isomorphisms and the exact sequence

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

we deduce

$$\begin{aligned}\dim \mathbf{C}_{\boldsymbol{\gamma}_r}(x_r) &= \sum_{i=0}^{r-1}\Big(\dim \mathbf{C}_{\boldsymbol{\gamma}_{r-i}}(x_{r-i}) - \dim \mathbf{C}_{\boldsymbol{\gamma}_{r-i}^1}(x_{r-i})\Big) = \sum_{i=0}^{r-1} \dim \eta^*_{r-i,1}\left(\mathbf{C}_{\boldsymbol{\gamma}_{r-i}}(x_{r-i})\right) \\ &= \sum_{i=1}^{m-1} \dim \eta^*_{i,1}\left(\mathbf{C}_{\boldsymbol{\gamma}_i}(x_i)\right) + \sum_{i=m}^{r} \dim \eta^*_{i,1}\left(\mathbf{C}_{\boldsymbol{\gamma}_i}(x_i)\right)\end{aligned}$$

$$\leq d \cdot (m-1) + (n-\alpha) \cdot (r-m), \tag{3.3}$$

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

For any $r \in \mathbb{N}$, by Property (Cay2) of the Cayley map and the preservation of open immersions of the Greenberg functor, the Cayley map restricts to a birational equivalence of the Lie-centralizer $\mathbf{C}_{\boldsymbol{\gamma}_r}(x_r)$ and the group-centralizer $\mathbf{C}_{\boldsymbol{\Gamma}_r}(x_r)$ of x_r. In particular, by Theorem 3.1.2.(1), we have that $\dim \mathbf{C}_{\boldsymbol{\gamma}_r}(x_r) = \dim \mathbf{C}_{\boldsymbol{\Gamma}_r}(x_r) \geq r \cdot n$. Manipulating the inequality (3.3), we get that

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

for all $r > m$. A contradiction, since r can be chosen to be arbitrarily large while the right-hand side of (3.4) remains constant. □

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

Proposition 3.1.7. *Let $x \in \boldsymbol{\gamma}$ and $x_m = \eta_{m,1}(x)$ for all $m \in \mathbb{N}$. The group scheme $\eta^*_{m,1}\left(\mathbf{C}_{\boldsymbol{\Gamma}_m}(x_m)\right)$ is a $\boldsymbol{k}$-algebraic group of dimension greater or equal to n.*

Proof. Properties (Cay2) and (Cay3) of the Cayley map imply the commutativity of the square (3.5)

$$\begin{tikzcd}
\mathbf{C}_{\boldsymbol{\gamma}_m}(x_m) \arrow[r, dashed, "\widehat{\mathrm{cay}}_m"] \arrow[d, "\eta^*_{m,1}"'] & \mathbf{C}_{\boldsymbol{\Gamma}_m}(x_m) \arrow[d, "\eta^*_{m,1}"] \\
\eta^*_{m,1}\left(\mathbf{C}_{\boldsymbol{\gamma}_m}(x_m)\right) \arrow[r, dashed, "\mathrm{cay}_{\boldsymbol{k}}"] & \eta^*_{m,1}\left(\mathbf{C}_{\boldsymbol{\Gamma}_m}(x_m)\right).
\end{tikzcd} \tag{3.5}$$

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 m, similarly to [26, Theorem 3.6], the case $m = 1$ being trivially true. Consider the following exact sequence

$$1 \longrightarrow \mathbf{C}_{\boldsymbol{\Gamma}^1_m}(x_m) \longrightarrow \mathbf{C}_{\boldsymbol{\Gamma}_m}(x_m) \xrightarrow{\eta^*_{m,1}} \mathbf{C}_{\boldsymbol{\Gamma}_1}(x_1). \tag{3.6}$$

Properties (Cay1) and (Cay2) imply that the map $\widehat{\mathrm{cay}}_m$ is defined on $\mathbf{C}_{\boldsymbol{\Gamma}^1_m}(x_m)$ and is mapped onto $\mathbf{C}_{\boldsymbol{\gamma}^1_m}(x_m)$. Combined with Lemma 2.3.4, we get that $\dim \mathbf{C}_{\boldsymbol{\Gamma}^1_m}(x_m) = \dim \mathbf{C}_{\boldsymbol{\gamma}_{m-1}}(x_{m-1})$. Moreover, since $\boldsymbol{\Delta}_{m-1} \cap \mathbf{C}_{\boldsymbol{\gamma}_{m-1}}(x_{m-1})$ is a non-trivial open subscheme of $\mathbf{C}_{\boldsymbol{\gamma}_{m-1}}(x_{m-1})$, and is mapped by $\widehat{\mathrm{cay}}_m$ to an open subscheme of $\mathbf{C}_{\boldsymbol{\Gamma}_{m-1}}(x_{m-1})$, we deduce the equality

$$\dim \mathbf{C}_{\boldsymbol{\Gamma}^1_m}(x_m) = \dim \mathbf{C}_{\boldsymbol{\Gamma}_{m-1}}(x_{m-1}). \tag{3.7}$$

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

$$\dim \mathbf{C}_{\boldsymbol{\Gamma}_m}(x_m) \leq \dim \mathbf{C}_{\boldsymbol{\Gamma}_{m-1}}(x_{m-1}) + \dim \mathbf{C}_{\boldsymbol{\Gamma}_1}(x_1) = m \cdot n.$$

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

$$\dim \mathbf{C}_{\mathbf{\Gamma}_m}(x_m) = \dim \mathbf{C}_{\mathbf{\Gamma}_{m-1}}(x_{m-1}) + \dim \eta_1\left(\mathbf{C}_{\mathbf{\Gamma}_m}(x_m)\right) > n(m-1) + n = n \cdot m,$$

and x_m is not regular. □

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

Corollary 3.1.8. *Let $m \in \mathbb{N}$ and $x_m \in \boldsymbol{\gamma}_m(\boldsymbol{k})$. The restriction of $\eta_{m,1}$ to $\mathbf{C}_{\mathbf{g}(\mathfrak{O}_m)}(x_m)$ is onto $\mathbf{C}_{\mathbf{g}(\boldsymbol{k})}(x_1)$, where $x_1 = \eta_{m,1}(x_m) \in \mathbf{g}(\boldsymbol{k})$.*

Proof. Theorem 3.1.2.(2) implies that x_1 is regular and hence $\mathbf{C}_{\boldsymbol{\gamma}_1}(x_1)(\boldsymbol{k}) = \mathbf{C}_{\mathbf{g}(\boldsymbol{k})}(x_1)$ is a $\boldsymbol{k}$-vector space of dimension $n = \dim \mathbf{C}_{\mathbf{\Gamma}_1}(x_1)$. By Lemma 3.1.6, the $\boldsymbol{k}$-points of the image of $\mathbf{C}_{\boldsymbol{\gamma}_m}(x_m)$ under $\eta_{m,1}^*$ comprise a subspace of $\mathbf{C}_{\mathbf{g}(\boldsymbol{k})}(x_1)$ of the same dimension. □

3.1.3 The image of $\eta_{m,1}$ on $\mathbf{C}_{\mathbf{\Gamma}_m}(x_m)$

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

Proposition 3.1.9. *Let L be either $\boldsymbol{k}$ or $\overline{K}$, 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

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

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 $\pm\lambda_1, \dots, \pm\lambda_t$ are the non-zero eigenvalues of s, as described in Proposition 2.1.1, with respective multiplicities $m_1, \dots, m_t$, and $W_{\lambda_j} = \mathrm{Ker}(s - \lambda_j \mathbf{1})$. Additionally, by [56, 3.5, Proposition 5], the restricted operators $h\mid_{W(\lambda_j)}$ and $h\mid_{\mathrm{Ker}(s)}$ are regular as elements of the Lie-algebras of GL_{m_j} and of Δ over L, respectively.

By [51, III, 3.2.2] it is known that all factors in (3.8), apart from $\mathbf{C}_\Delta(h\mid_{\mathrm{Ker}(s)})$, are connected. Furthermore, by [51, III, 1.14] and the assumption $\mathrm{char}(L)\neq 2$, we have

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

(see [51, 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 [51, 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 3.1.7 and Chevalley's Theorem [18, IV, 1.8.4], the image of $\mathbf{C}_{\mathbf{\Gamma}_m}(x_m)$ under $\eta^*_{m,1}$ 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 $\mathbf{Z}(\mathbf{\Gamma}_m)$ of $\mathbf{\Gamma}_m$ is clearly contained in $\mathbf{C}_{\mathbf{\Gamma}_m}(x_m)$ and is mapped by $\eta^*_{m,1}$ onto $\mathbf{Z}(\mathbf{\Gamma}_1)$. This implies the inclusion

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

Evaluating the above inclusions at $\boldsymbol{k}$-points, by Proposition 3.1.9, we deduce the equality. □

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

In this section we prove Theorem 3.1.3. An initial step towards this goal is to show that the third assertion of Theorem 3.1.2 remains true when replacing the groups $\mathbf{G}(\mathfrak{O}_m)$ and Lie-rings $\mathbf{g}(\mathfrak{O}_m)$ with the group and Lie-rings of $\mathfrak{o}_m$-rational points, i.e. $G_m=\mathbf{G}(\mathfrak{o}_m)$ and $\mathfrak{g}_m=\mathbf{g}(\mathfrak{o}_m)$. Given $1\leq r\leq m$, we write G_m^r and $\mathfrak{g}_m^r$ to denote the congruence subgroup $\mathrm{Ker}(G_m\xrightarrow{\eta_{m,r}}G_r)=G_m\cap\eta_{m,r}^{-1}(1)$ and congruence subring $\mathrm{Ker}(\mathfrak{g}_m\xrightarrow{\eta_{m,r}}\mathfrak{g}_r)=\mathfrak{g}_m\cap\eta_{m,r}^{-1}(0)$, 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 $\boldsymbol{k}$ by $\sigma(\xi)=\xi^q$. This automorphism gives rise to an automorphism of $\mathbf{G}(\mathfrak{O})$, and of its quotients $\mathbf{G}(\mathfrak{O}_m)$ and their Lie-algebras. By definition, an element $x\in\mathfrak{g}_m$ is regular if and only if it is a regular σ-fixed element of $\mathbf{g}(\mathfrak{O}_m)$. We require the following variant of Lang's Theorem.

Lemma 3.1.10. *Let $m\in\mathbb{N}$ and let $x_m\in\mathfrak{g}_m$ be a regular element and $x_1=\eta_{m,1}(x_m)$. Given $g\in\mathbf{C}_{G_1}(x_1)=\mathbf{C}_{\mathbf{G}(\boldsymbol{k})}(x_1)\cap G_1$, let $F_g=\eta_{m,1}^{-1}(g)\cap\mathbf{C}_{\mathbf{G}(\mathfrak{O}_m)}(x_m)$, and let L_g be the map defined by*

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

Then $\mathsf{L}_g:F_g\to F_1$ 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 $F_1 = \mathbf{C}_{\mathbf{\Gamma}^1_m(\boldsymbol{k})}(x_m)$. In particular, by (Cay1) and (Cay2), the $F_{g'}$'s are the $\boldsymbol{k}$-points of algebraic varieties, isomorphic to $\mathbf{C}_{\boldsymbol{\gamma}^1_m(\boldsymbol{k})}(x_m)$ and hence affine $(m-1)n$-dimensional spaces over $\boldsymbol{k}$.

Since the reduction map $\eta_{m,1}$ commutes with the Frobenius maps, and since g is assumed fixed by σ, we have that L_g is well-defined. The surjectivity of L_g now follows as in the proof of the classical Lang Theorem [35] (see also [51, I, 2.2] and [25, § 3]). □

Corollary 3.1.11. *Let $x_m \in \mathfrak{g}_m$ be regular and $x_1 = \eta_{m,1}(x_m)$. The restriction of $\eta_{m,1}$ to $\mathbf{C}_{G_m}(x_m)$ is onto $\mathbf{C}_{G_1}(x_1)$.*

Proof. Lemma 3.1.10 and Theorem 3.1.2.(3) imply that for any $g \in \mathbf{C}_{G_1}(x_1)$, there exists an element $h \in \mathbf{C}_{\mathbf{\Gamma}_m}(x_m)$ such that $\eta_{m,1}(h) = g$ and such that $\mathsf{L}_g(h) = h\sigma(h)^{-1} = 1$. In particular, h is fixed under σ and hence $h \in \mathbf{C}_{G_m}(x_m) \cap \eta^{-1}_{m,1}(g)$. □

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

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

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

Proof. We prove both assertions by induction on r.

1. The case $r = 1$ follows in Corollary 3.1.8 and Lang's Theorem, as $\mathbf{C}_{\boldsymbol{\gamma}_1}(x_1)$ and $\eta^*_{m,1}(\mathbf{C}_{\boldsymbol{\gamma}_m}(x_m))$ are both affine n-spaces over $\boldsymbol{k}$. Consider the commutative diagram in (3.9), in which both rows are exact by induction hypothesis.

$$\begin{tikzcd}
\mathbf{C}_{\mathfrak{g}_m^{r-1}}(x_m) \arrow[r] \arrow[d] & \mathbf{C}_{\mathfrak{g}_m}(x_m) \arrow[r, "\eta_{m,r-1}"] \arrow[d, "\eta_{m,r}"] & \mathbf{C}_{\mathfrak{g}_{r-1}}(x_{r-1}) \arrow[r] \arrow[d, equal] & 0 \arrow[d, equal] \\
\mathbf{C}_{\mathfrak{g}_r^{r-1}}(x_r) \arrow[r] & \mathbf{C}_{\mathfrak{g}_r}(x_r) \arrow[r, "\eta_{r,r-1}"'] & \mathbf{C}_{\mathfrak{g}_{r-1}}(x_{r-1}) \arrow[r] & 0
\end{tikzcd} \tag{3.9}$$

By the Four Lemma (on epimorphisms), in order to prove the surjectivity of the map $\eta_{m,r} : \mathbf{C}_{\mathfrak{g}_m}(x_m) \to \mathbf{C}_{\mathfrak{g}_r}(x_r)$, it suffices to show that the restricted map $\eta_{m,r} : \mathbf{C}_{\mathfrak{g}_m^{r-1}}(x_m) \to \mathbf{C}_{\mathfrak{g}_r^{r-1}}(x_r)$ is surjective. This follows from the commutativity of the square in (3.10), in which the maps on the top and bottom rows are given the $\mathfrak{o}$-module isomorphism $y \mapsto \pi^{r-1}y$ (cf. Lemma 2.3.4), and the map on the left column is surjective by the base of induction.

$$\begin{tikzcd}
\mathbf{C}_{\mathfrak{g}_{m-r+1}}(x_{m-r+1}) \arrow[r, "\sim"] \arrow[d, two heads, "\eta_{m-r+1,1}"'] & \mathbf{C}_{\mathfrak{g}_m^{r-1}}(x_m) \arrow[d, "\eta_{m,r}"] \\
\mathbf{C}_{\mathfrak{g}_1}(x_1) \arrow[r, "\sim"] & \mathbf{C}_{\mathfrak{g}_r^{r-1}}(x_r)
\end{tikzcd} \tag{3.10}$$

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

$$\begin{tikzcd} \mathbf{C}_{\mathfrak{g}_m^{r-1}}(x_m) \arrow[r, "\mathrm{cay}_m"] \arrow[d, two heads, "\eta_{m,r}"'] & \mathbf{C}_{G_m^{r-1}}(x_m) \arrow[d, "\eta_{m,r}"] \\ \mathbf{C}_{\mathfrak{g}_r^{r-1}}(x_r) \arrow[r, "\mathrm{cay}_r"] & \mathbf{C}_{G_r^{r-1}}(x_r) \end{tikzcd} \tag{3.11}$$

□

Proof of Theorem 3.1.3.(1). Given $g_m \in \mathbf{C}_{G_m}(x_m)$ one inductively invokes Lemma 3.1.12 to construct a converging sequence $(g_r)_{r\geq m}$ such that $g_r \in \mathbf{C}_{G_r}(\eta_r(x))$ and such that $\eta_{r,r'}(g_r) = g'_r$ for all $r \geq r' \geq m$. The limit $g = \lim_r g_r$ is easily verified to be an element of $\mathbf{C}_G(x)$, which is mapped by η_m to g_m. □

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

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

Proof. The proof of the lemma appears in [42, (2.5.2)]. We recall it here for completeness.

Let $\omega : \mathbf{C}_x \to \mathrm{Spec}(\mathfrak{O})$ be the structure morphism, and let t be the generic point and s the special (closed) point of $\mathrm{Spec}(\mathfrak{O})$. By Chevalley's upper-semicontinuity theorem, for any $e \in \mathbb{N}$, the set of elements $y \in \mathbf{C}_x$ such that $\dim \omega^{-1}(\omega(y)) \geq e$ is closed. Fix $e = \dim \omega^{-1}(t) = \dim \mathbf{C}_x \times K^{\mathrm{unr}}$. Arguing as in [18, IV, Corollary 13.1.6] we have that the set of elements $y \in \mathbf{C}_x^\circ$ for which $\dim \omega^{-1}(\omega(y)) < e$ is empty. Since this statement remains true under the action of the group of connected components $\pi_0(\mathbf{C}_x) = \mathbf{C}_x/\mathbf{C}_x^\circ$ on $\mathbf{C}_x$, it follows that for any $y \in \mathbf{C}_x$, $\dim \omega^{-1}(\omega(y)) \geq e$. Taking y in the fiber of ω over s we obtain

$$\dim \mathbf{C}_x \times \boldsymbol{k} = \dim \omega^{-1}(\omega(y)) \geq e = \dim \mathbf{C}_x \times K^{\mathrm{unr}}.$$

[1] personal communication

□

Proof of Theorem 3.1.3.(2). By Lemma 3.1.13, given that $x_1 = \eta_1(x)$ is regular, we have that

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

On the other hand, by [56, 3.5, Proposition 1], the minimum value of centralizer dimension of an element of $\mathfrak{g}$ (and, more generally, of $\mathfrak{g}\otimes\overline{K}$) is $n = \mathrm{rk}(\mathbf{G})$. Hence, x is a regular element of $\mathfrak{g}\otimes\overline{K}$. □

Finally, we deduce Corollary 3.1.4.

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

3.2 Regular characters

At this point, our description of the regular elements of the Lie-algebras $\mathfrak{g}_m$ is sufficient in order to initiate the description of regular characters of G and to prove Theorem I and Corollary 1.2.1. To do so, we prove the following variant of [33, Theorem 3.1].

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

1. *The set $\mathrm{Irr}(G_m^r \mid \Omega)$ of characters of $G_m^r = \mathrm{Ker}(G_m \to G_r)$ which lie above the regular orbit Ω consists of exactly $q^{n(m-r-1)}$ orbits for the coadjoint action of G_m.*

2. *Given a character $\tau \in \mathrm{Irr}(G_m^r \mid \Omega)$, the set of irreducible characters of G_m whose restriction to G_m^r has τ as a constituent is in bijection with the Pontryagin dual of $\mathbf{C}_{G_r}(x_r)$.*

3. *Any such character $\tau \in \mathrm{Irr}(G_m^r \mid \Omega)$ extends to its inertia group $I_{G_m}(\tau)$. In particular, each such extension induces to a regular character of G_m.*

Note that the first assertion of Theorem I follows from Assertions (1) and (2) of Theorem 3.2.1 and Corollary 3.1.11. The second assertion of Theorem I follows from the Assertion (3) of Theorem 3.2.1 and the description of the inertia subgroup $I_{G_m}(\tau)$, noted below.

The proof of Theorem 3.2.1 follows the same path as [33, § 3]. For the sake of brevity, rather then rehashing the proof appearing in great detail in *loc. cit.*, our focus for the remainder of this section would be on setting up the necessary preliminaries and state the necessary modification required in order to adapt the construction of [33] 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_m and $\mathfrak{g}_m$ are embedded in $\mathrm{M}_n(\mathfrak{o}_m)$. From here on, all computations 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 $\mathfrak{g} = \mathfrak{g}(\mathfrak{o}) \subseteq \mathrm{M}_N(\mathfrak{o})$ is endowed with a symmetric bilinear $G(\mathfrak{o})$-equivariant form

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

such that $\{x \in \mathfrak{g} \mid \kappa(x, y) \in \mathfrak{p} \text{ for all } y \in \mathfrak{g}\} = \pi\mathfrak{g}$. Fixing a non-trivial character $\psi : K \to \mathbb{C}^\times$ with conductor $\mathfrak{o}$ (see e.g. [3, § 5.3]), for any $m \in \mathbb{N}$, we have a well-defined map

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

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

3.2.2 Exponential and logarithm

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

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

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

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

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

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

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

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

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

3.2.3 Characters of $G_m^{\lfloor m/2 \rfloor}$

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

$$\Phi \quad : \quad \mathfrak{g}_r \to \widehat{\mathfrak{g}_r} \to \widehat{\mathfrak{g}_m^{r'}} \to \mathrm{Irr}(G_m^{r'}), \tag{3.13}$$

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

Lemma 3.2.4. *Assume $m = 2r$ is even. The map Φ defined in* (3.13) *is a G_m-equivariant bijection of $\mathfrak{g}_r$ onto $\mathrm{Irr}(G_m^r)$.*

In the case where $m = 2r+1$, the irreducible characters of G_m^r are classified in terms of their restriction to $G_m^{r'}$, using the method of Heisenberg lifts, which we briefly recall here. For a more elaborate survey we refer to [33, § 3.2] and [11, Ch. 8].

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

$$B_\vartheta : G_m^r/G_m^{r'} \times G_m^r/G_m^{r'} \to \mathbb{C}^\times, \quad B_\vartheta(x_1G_m^{r'}, x_2G_m^{r'}) = \vartheta\left((x_1,x_2)\right).$$

Using the definition of $\Phi(y) = \vartheta$ and the explicit isomorphism $x \mapsto \exp(\pi^r x) : \mathfrak{g}_1 \to G_{r'}^r = G_m^r/G_m^{r'}$, the map $\beta_y(x_1,x_2) = \mathrm{Tr}(\eta_{r,1}(y)\cdot[x_1,x_2])$ is an alternating bilinear form $\beta_y : \mathfrak{g}_1 \times \mathfrak{g}_1 \to \mathbb{F}_q$, such that the diagram in (3.14) commutes.

$$\begin{tikzcd} G_{r'}^r \times G_{r'}^r \arrow[r, "B_\vartheta"] & \mathbb{C}^\times \\ \mathfrak{g}_1 \times \mathfrak{g}_1 \arrow[u, "\wr"] \arrow[r, "\beta_y"] & \mathbb{F}_q \arrow[u, "\psi(\pi^{-1}(\cdot))"'] \end{tikzcd} \tag{3.14}$$

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 $\mathbf{C}_{\mathfrak{g}_1}(\eta_{r,1}(y))$ of $\eta_{r,1}(y)$ in $\mathfrak{g}_1$ (see [33, p. 125]). Let $\mathfrak{R}_y$ and R_y denote the preimages of $\mathfrak{r}_y$ in $\mathfrak{g}_m^r$ and in G_m^r under the associated quotient maps. Let $\mathfrak{r}_y \subseteq \mathfrak{j} \subseteq \mathfrak{g}_1$ be a maximal subspace such that $\beta_y(\mathfrak{j},\mathfrak{j}) = \{0\}$ (i.e. such that $\mathfrak{j}/\mathfrak{r}_y$ is a maximal isotropic subspace of $\mathfrak{g}_1/\mathfrak{r}_y$), and let $\mathfrak{J} \subseteq \mathfrak{g}_m^r$ and $J \subseteq G_m^r$ be the corresponding preimages of $\mathfrak{j}$; see (3.15).

$$\begin{tikzcd} G_m^r \arrow[r, dashed, "\log"'] \arrow[d, dash] & \mathfrak{g}_m^r \arrow[r] \arrow[d, dash] & \mathfrak{g}_1 \arrow[d, dash] \\ J \arrow[r, dashed, "\log"'] \arrow[d, dash] & \mathfrak{J} \arrow[r] \arrow[d, dash] & \mathfrak{j} \arrow[d, dash] \\ R_y \arrow[r, dashed, "\log"'] \arrow[d, dash] & \mathfrak{R}_y \arrow[r] \arrow[d, dash] & \mathfrak{r}_y \arrow[d, dash] \\ G_m^{r'} \arrow[r, "\sim", "\log"'] & \mathfrak{g}_m^{r'} \arrow[r] & 0 \end{tikzcd} \tag{3.15}$$

Let $\theta = \vartheta \circ \exp$ be the pull-back of ϑ to $\mathfrak{g}_m^{r'}$. By virtue of the commutativity of $\mathfrak{R}_y$, the character θ' extends to a character of $\mathfrak{R}_y$ in $\left|\mathfrak{R}_y : G_m^{r'}\right| = |\mathfrak{r}_y|$ many ways. By Lemma 3.2.3, 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 $|\mathfrak{r}_y|$ many extensions to R_y.

The proof of the following lemma appears in [11, Ch. 8].

Lemma 3.2.5. *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 $\tau = (\vartheta'')^{G_m^r}$ is irreducible and is independent of the choice of extension ϑ'' and of $\mathfrak{j}$.

3. The character τ is the unique character of G_m^r whose restriction to R_y contains ϑ'. Furthermore, all irreducible characters of G_m^r which lie above ϑ are obtained in this manner.

3.2.4 Inertia subgroups in $\mathrm{G}(\mathfrak{o}_m)$ of regular characters

The final ingredient required in order to implement the construction of [33] to the current setting is a structural description of the inertia subgroup of a character of $G_m^{\lceil m/2\rceil}$ lying below a regular character of level $\ell = m+1$. As in the previous section, put $r = \lfloor \frac{m}{2} \rfloor$ and $r' = \lceil \frac{m}{2} \rceil$, and let $\vartheta \in \mathrm{Irr}(G_m^{r'})$. Recall that the inertia subgroup of ϑ in G_m is defined by

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

By § 3.2.3, there exists a unique $y \in \mathfrak{g}_r$ such that $\vartheta = \Phi(y)$. Also note that, by the surjectivity of the map $\eta_{m,r'} : I_{G_m}(\vartheta) \to \mathbf{C}_{G_{r'}}(\widehat{y}_{r'})$, it holds that

$$I_{G_m}(\vartheta) = G_m^{r'} \cdot \mathbf{C}_{G_m}(\widehat{y}_m). \tag{3.17}$$

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

The second assertion of Theorem 3.2.1 follows from the third assertion, (3.17) and [31, Corollary 6.17].

Lastly, for the proof of the third assertion of Theorem 3.2.1, we refer to [33, § 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 $\tau \in \mathrm{Irr}(G_m^r)$ to its inertia subgroup $I_{G_m}(\tau)$. Note that the construction of *loc. cit.* can be applied verbatim to the present setting, invoking the fact the $I_{G_m}(\tau)$ is generated by two abelian subgroups, with $G_m^{r'} \lhd I_{G_m}(\vartheta)$ ((3.17) and Corollary 3.1.4) in the generality of classical groups. $\square$

Chapter 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 1.2.1, 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 finite Dirichlet series

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

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 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 $\mathfrak{sp}_{2n}(\mathbb{F}_q)$ and $\mathfrak{so}_{2n+1}(\mathbb{F}_q)$ is equivalent to it being given by a regular matrix in $\mathrm{M}_N(\mathbb{F}_q)$ (cf. [58, § 5]). This equivalence fails to hold for even-orthogonal groups; see Lemma 4.4.1 below.

Recall that two matrices $x, y \in \mathrm{M}_N(\mathbb{F}_q)$ are said to be **similar** if they are conjugate by an element of $\mathrm{GL}_N(\mathbb{F}_q)$. Our description of regular orbits of $\mathfrak{g}_1$ follows the following steps.

1. Classification of all similarity classes in $\mathfrak{gl}_N(\mathbb{F}_q)$ 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.

4.1.1 Enumerative set-up

Definition 4.1.1 (Type of a polynomial)**.** Let $f(t) \in \mathbb{F}_q[t]$ 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 $\mathfrak{X}_n$ 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 $\boldsymbol{\tau}(f) \in \mathfrak{X}_n$ whenever f is monic and satisfies $f(-t) = (-1)^N f(t)$.

The number of monic irreducible polynomials of degree d over $\mathbb{F}_q$ is given by evaluation at $t = q$ of the function $w_d(t) = \frac{1}{d} \sum_{m|d} \mu\left(\frac{d}{m}\right) t^d$, where $\mu(\cdot)$ is the Möbius function (see, e.g., [20, Ch. 14]). A polynomial $f \in \mathbb{F}_q[t]$ 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 that $\mathbb{F}_q$ is of odd characteristic, the only monic irreducible odd polynomial over $\mathbb{F}_q$ is $f(t) = t$. The number of monic irreducible even polynomials of degree d over $\mathbb{F}_q$ is given by evaluation at $t = q$ of the function[1]

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

Put

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

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 $\boldsymbol{\tau} \in \mathfrak{X}_n$, the number of polynomials $f \in \mathbb{F}_q[t]$ 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 $\mathrm{M}_N(\mathbb{F}_q)$ 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.

[1] The function $E_d(t)$ is probably well-known. In the lack of a reference, a proof of (4.1) is given in Appendix A. I wish to thank Jyrki Lahtonen [34] of the Mathematics Stack Exchange network taking part in computing this formula.

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

Theorem 4.1.2. *Assume* $\mathrm{char}(\mathbb{F}_q) \neq 2$. *Let* $V = \mathbb{F}_q{}^N$ *and let* $B = B_{\mathbb{F}_q}$ *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* $G_1 = \mathbf{G}(\mathbb{F}_q)$ *and* $\mathfrak{g}_1 = \mathbf{g}(\mathbb{F}_q)$ *where* $\mathbf{g} = \mathrm{Lie}(\mathbf{G})$.

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

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* $\mathrm{Ad}(\mathrm{GL}_N(\mathbb{F}_q))x \cap \mathfrak{g}_1$ *is the union of two distinct* $\mathrm{Ad}(G_1)$*-orbits. Otherwise,* $\mathrm{Ad}(\mathrm{GL}_N(\mathbb{F}_q))x \cap \mathfrak{g}_1 = \Omega$.

3. *Let* $\boldsymbol{\tau} = \boldsymbol{\tau}(m_x) = (r(m_x), S(m_x), T(m_x))$ *as in Definition 4.1.1. Then*
$$|\Omega| = q^{2n^2} \cdot \left(\frac{1}{2}\right)^{\nu} \frac{\prod_{i=1}^{n}(1-q^{-2i})}{\prod_{1\leq d,e\leq n}(1+q^{-d})^{S_{d,e}(m_x)} \cdot (1-q^{-d})^{T_{d,e}(m_x)}},$$
where $\nu = 1$ *if* $N = 2n$ *is even and* $m_x(0) = 0$, *and* $\nu = 0$ *otherwise.*

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

4.1.3 Statement of results- even-dimensional special orthogonal groups

Theorem 4.1.3. *Assume* $|\mathbb{F}_q| > 3$ *and* $\mathrm{char}(\mathbb{F}_q) \neq 2$. *Let* $N = 2n$ *with* $n \geq 2$. *Let* $V = \mathbb{F}_q{}^N$ *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* $\mathbf{G}^\epsilon = \mathrm{SO}_{2n}^\epsilon$ *be the* $\mathbb{F}_q$*-algebraic group of isometries of* V *with respect to* B^ϵ *and put* $G_1^\epsilon = \mathbf{G}_1^\epsilon(\mathbb{F}_q)$ *and let* $\mathfrak{g}_1^\epsilon = \mathbf{g}^\epsilon(\mathbb{F}_q)$, *where* $\mathbf{g}^\epsilon = \mathrm{Lie}(\mathbf{G})$.

Let $x \in \mathrm{M}_N(\mathbb{F}_q)$ *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* $\epsilon = \epsilon(x) = (-1)^{\sum_e eS_{d,e}(m_x)}$ *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 $\mathrm{Ad}(\mathrm{GL}_N(\mathbb{F}_q))x \cap \mathfrak{g}_1^\epsilon$ is the disjoint union of two distinct $\mathrm{Ad}(G_1^\epsilon)$-orbits. Otherwise, $\mathrm{Ad}(\mathrm{GL}_N(\mathbb{F}_q))x \cap \mathfrak{g}_1^\epsilon = \Omega^\epsilon$.*

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 $\mathbb{F}_q = \mathbb{F}_3$ 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 of Theorems 4.1.2 and 4.1.3

4.2.1 Regularity for non-singular elements

Lemma 4.2.1. *Let $x \in \mathrm{g}(\boldsymbol{k}) \subseteq \mathfrak{gl}_N(\boldsymbol{k})$ be non-singular. Then x is regular in $\mathrm{g}(\boldsymbol{k})$ if and only if x is a regular element of $\mathfrak{gl}_N(\boldsymbol{k})$.*

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

Let $x = s + h$ be the Jordan decomposition of x, with $s, h \in \mathrm{g}(\boldsymbol{k})$, s semisimple, h nilpotent and $[s,h] = 0$. Let $\lambda_1, \ldots, \lambda_t \in \boldsymbol{k}$ 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 [56, § 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 $\mathrm{g}(\boldsymbol{k})$ 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 $B_{\boldsymbol{k}}$ 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 may 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 $\mathfrak{gl}_N(\boldsymbol{k})$ is identified with the subgroup of block diagonal matrices consisting of two $n \times n$ blocks. Moreover, the involution $\star$ maps an element $\mathrm{diag}(y_1, y_2) \in \mathbf{C}_{\mathfrak{gl}_N(\boldsymbol{k})}(s)$, with $y_1, y_2 \in \mathfrak{gl}_n(\boldsymbol{k})$ to the matrix $\mathrm{diag}(y_2^t, y_1^t)$. In particular, it follows that $h \in \mathbf{C}_{\mathfrak{gl}_N}(\boldsymbol{k}) \cap \mathbf{g}(\boldsymbol{k})$ is of the form $h = \mathrm{diag}(h_1, -h_1^t)$, where $h_1 \in \mathfrak{gl}_n(\boldsymbol{k})$ is nilpotent. Arguing as in [51, 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 $y \mapsto (y^t)^{-1} : \mathbf{C}_{\mathrm{GL}_n}(-h_1^t) \to \mathbf{C}_{\mathrm{GL}_n}(h_1)$.

Additionally, since the group $\mathbf{G}$ is embedded in GL_N as the group of unitary elements with respect to $\star$, we have $\mathrm{diag}(y_1, y_2) \in \mathbf{C}_{\mathrm{GL}_N(\boldsymbol{k})}(s) \cap \mathbf{G}(\boldsymbol{k})$ 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 $\boldsymbol{\gamma}_1$ is a direct product of groups of the form $\mathrm{GL}_{m_j}(\boldsymbol{k})$. 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 $\Pi_x = \mathrm{Ad}(\mathrm{GL}_N(\mathbb{F}_q))x \cap \mathfrak{g}_1$, for $x \in \mathfrak{g}_1$ regular, in to $\mathrm{Ad}(G_1)$-orbits. The results appearing below can also be derived from [60, § 2.6]. However, as the case of regular elements allows for a much more transparent argument, we present it here for completeness.

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

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

Let Θ_x to be the set of equivalence classes of $\sim$ in $\mathrm{Sym}(\star; x)$. In the case where $\mathbf{C}_{\mathrm{GL}_N(\mathbb{F}_q)}(x)$ is abelian (e.g., when x is a regular element of $\mathfrak{gl}_N(\mathbb{F}_q)$), 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 $\mathbf{C}_{\mathrm{GL}_N(\mathbb{F}_q)}(x)$.

Proposition 4.2.3. *Let $x \in \mathfrak{g}_1$ and let Π_x denote the intersection $\mathrm{Ad}(\mathrm{GL}_N(\mathbb{F}_q))x \cap \mathfrak{g}_1$. 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 $w \in \mathrm{GL}_N(\mathbb{F}_q)$ 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 $w' \in \mathrm{GL}_N(\mathbb{F}_q)$ 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 $w_1, w_2 \in \mathrm{GL}_N(\mathbb{F}_q)$ 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 $a \in \mathbf{C}_{\mathrm{GL}_N(\mathbb{F}_q)}(x)$ such that $Q_2 = a^\star Q_1 a$. Put $z = w_1 a w_2^{-1}$. Note that $zy_2z^{-1} = y_1$. We claim that $z \in G_1$. This holds since for any $u, v \in V$

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

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 $y_1 = zy_2z^{-1}$, and let $w_1, w_2 \in \mathrm{GL}_N(\mathbb{F}_q)$ be such that $y_i = w_i x w_i^{-1}$ $(i = 1, 2)$. Then w_1 and zw_2 both conjugate x to y_1, and hence, by the unambiguity of the definition of Λ and fact that $z \in G_1$, we have that

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

□

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 cokernel of an involution of an étale algebra over $\mathbb{F}_q$. 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* $\mathcal{C} \subseteq \mathrm{M}_N(\mathbb{F}_q)$ *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 [60, 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 $\mathrm{char}(\mathbb{F}_q) \neq 2$. □

4.2.3 Similarity classes via bilinear forms

We recall a basic lemma which would allow us to determine when an element of $\mathfrak{gl}_N(\mathbb{F}_q)$ 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 $\mathbb{F}_q$, 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 $V = {\mathbb{F}_q}^N$, and assume there exists $g \in \mathrm{End}(V)$ and $\delta \in \mathbb{F}_q$ such that $C_1(gu, gv) = \delta C_2(u, v)$ for all $u, v \in V$. Let $x \in \mathfrak{gl}_N(\mathbb{F}_q)$ 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

Recall the following well-known fact.

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 $V = {\mathbb{F}_q}^N$ such that $C_i(u, v) = \epsilon C_i(v, u)$ for all $u, v \in V$ and $i = 1, 2$. There exists $\delta \in \mathbb{F}_q$ 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., [63, §3.4.4] in the symplectic case and [63, § 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 $x \in \mathfrak{gl}_N(\mathbb{F}_q)$ with minimal polynomial $m_x(t) \in \mathbb{F}_q[t]$.*

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 $\mathfrak{gl}_N(\mathbb{F}_q)$ (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 $u, v \in V = {\mathbb{F}_q}^N$. 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 [56, 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 $\mathbb{F}_q[x]$ (which, in turn, is equivalent to $\deg m_x = N$). In particular, there exists $v_0 \in V$ such that $(v_0, xv_0, \dots, x^{N-1}v_0)$ is a $\mathbb{F}_q$-basis for V. Let $\mathrm{Prj}_{N-1} : V \to \mathbb{F}_q$ denote the projection onto $\mathbb{F}_q \cdot x^{N-1}v_0$. Given $u_1, u_2 \in V$ let $p_1, p_2 \in \mathbb{F}_q[t]$ 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. Also, the fact that x is C-antisymmetric is immediate from the definition of C. 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 $N-1$.

□

Note that Lemma 4.3.2 gives a criterion for a regular element of $\mathfrak{gl}_N(\mathbb{F}_q)$ 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 $x \in \mathfrak{gl}_N(\mathbb{F}_q)$ be a regular nilpotent element, i.e. $m_x(t) = t^N$. Picking a generator v_0 for V over $\mathbb{F}_q[x]$ and putting $\mathcal{E} = (v_0, xv_0, \dots, x^{N-1}v_0)$, the element x is represented in the basis $\mathcal{E}$ by an $N \times N$ nilpotent Jordan block, say $\Upsilon = J_n(0)$. 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 $\mathfrak{g}_1$ we now pass to the algebraic closure of $\mathbb{F}_q$ and compute the dimension of the centralizer of $z\Upsilon z^{-1}$ in $\mathbf{\Gamma}_1$, where $z\mathbf{\Gamma}_1 z^{-1} \in \mathfrak{g}_1$. Note that the centralizer of Υ in $\mathrm{GL}_N(\boldsymbol{k})$ consists of upper triangular Töplitz matrices,

$$\mathbf{C}_{\mathrm{GL}_N(\boldsymbol{k})}(\Upsilon) = \left\{ \begin{pmatrix} a_0 & a_1 & \dots & a_{N-1} \\ & \ddots & \ddots & \vdots \\ & & a_0 & a_1 \\ & & & a_0 \end{pmatrix} \mid a_0, \dots, a_{N-1} \in \boldsymbol{k},\ a_0 \neq 0 \right\} \simeq \left(\boldsymbol{k}[t]/(t^N)\right)^{\times}.$$

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

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

Proof. By [56, § 3.5, Proposition 1], we need to show $\dim \mathbf{C}_{\boldsymbol{\Gamma}_1}(x) = n$ if and only if $\dim \mathbf{C}_{\mathrm{GL}_N \times \boldsymbol{k}}(x) = N$. Let $x = s + h$ be the Jordan decomposition of x over $\boldsymbol{k}$, with $s, h \in \mathbf{g}(\boldsymbol{k})$, s semisimple, h nilpotent, and $[s, h] = 0$. As seen in the proof of Proposition 2.1.1, the space $W = \boldsymbol{k}^N$ decomposes as an orthogonal direct sum $W_1 \oplus W_0$ with respect to the ambient bilinear form $B_{\boldsymbol{k}}$, where $W_0 = \mathrm{Ker}(s)$ and $s\mid_{W_1}$ is non-singular. Let $\Sigma \subseteq \mathbf{G}(\boldsymbol{k})$ 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

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

and

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

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 [56, III, Theorem 1.8]. $\square$

Proof of Theorem 4.1.2.(1). Proposition 4.3.4 implies that any element $x \in \mathrm{M}_N(\mathbb{F}_q)$ which is similar to a regular element of $\mathfrak{g}_1$ is regular as an element of $\mathfrak{gl}_N(\mathbb{F}_q)$. 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). $\square$

4.3.2 From similarity classes to adjoint orbits

In this section is to we analyze decomposition of the set $\mathrm{Ad}(\mathrm{GL}_N(\mathbb{F}_q))x \cap \mathfrak{g}_1$, 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 $f(t) \in \mathbb{F}_q[t]$ we write $\mathbb{F}_q\langle f\rangle$ for the quotient ring $\mathbb{F}_q[t]/(f)$. For example, if f is an irreducible polynomial over $\mathbb{F}_q$ then $\mathbb{F}_q\langle f\rangle$ stands for the splitting field of f. We write $\mathrm{GL}_1(\mathbb{F}_q\langle f\rangle)$ for the group of units of $\mathbb{F}_q\langle f\rangle$.

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

Proposition 4.3.6. *Let $x \in \mathfrak{g}_1$ be a regular element, and put $\Pi_x = \mathrm{Ad}(\mathrm{GL}_N(\mathbb{F}_q))x \cap \mathfrak{g}_1$. 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 $\varphi_1,\dots,\varphi_{d_2}$ are irreducible, monic and even, and $\theta_1,\dots,\theta_{d_3}$ 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 $\mathcal{C} = \mathbf{C}_{\mathrm{M}_N(\mathbb{F}_q)}(x)$ is isomorphic to the ring $\mathbb{F}_q\langle m_x\rangle$ 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

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

Furthermore, the restriction of the involution σ_{m_x} to each of the factors $\mathbb{F}_q\langle f\rangle$, 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

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

where $r = 1$ if $d_1 > 0$ (i.e. if x is singular) and equals 0 otherwise[2]. Let $\dagger$ denote the involution induced on the $\mathbb{F}_q$-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 $\mathcal{K}$.

[2]Here it is understood that the ring ${\mathbb{F}_q}^0$ is the trivial algebra $\{0\}$.

D1. The involution $\dagger$ preserves the factor ${\mathbb{F}_q}^r$ and acts trivially on it.

D2. The involution $\dagger$ preserves the factors $\mathbb{F}_q\langle\varphi_i\rangle$ and coincides with the non-trivial field involution σ_{φ_i}.

D3. The involution $\dagger$ preserves the factors $\mathbb{F}_q\langle\theta_i\rangle \simeq \mathbb{F}_q\langle\tau_i(t)\rangle \times \mathbb{F}_q\langle\tau_i(-t)\rangle$ and maps a pair $(\xi,\nu) \in \mathbb{F}_q\langle\tau_i(t)\rangle \times \mathbb{F}_q\langle\tau_i(-t)\rangle$ to the pair $(\iota^{-1}(\nu), \iota(\xi))$, where $\iota : \mathbb{F}_q\langle\tau_i(t)\rangle \to \mathbb{F}_q\langle\tau_i(-t)\rangle$ 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 $\mathbb{F}_q\langle\varphi_i\rangle$ 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 $(\xi,\nu) \in \mathbb{F}_q\langle\tau_i(t)\rangle \times \mathbb{F}_q\langle\tau_i(-t)\rangle$ 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 ${\mathbb{F}_q}^r$ is either trivial, if $r = 0$, or the group of squares in ${\mathbb{F}_q}^\times$, otherwise. It follows from this that the set Θ_x is either in bijection with the quotient $\left({\mathbb{F}_q}^\times/({\mathbb{F}_q}^\times)^2\right)$, 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 $Q \in \mathrm{GL}_N(\mathbb{F}_q)$, and hence the form $(u,v) \mapsto B(u,Qv)$ is alternating and non-degenerate. By Lemma 4.3.1, there exists $w \in \mathrm{GL}_N(\mathbb{F}_q)$ 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.

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 ${\mathbb{F}_q}^\times$. This holds since $\det(a^\star) = \det(a)$ for all $a \in \mathrm{M}_N(\mathbb{F}_q)$. By the same token, it follows that the $\det(w^\star w)$ is a square in ${\mathbb{F}_q}^\times$ for all $w \in \mathrm{GL}_N(\mathbb{F}_q)$.

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 $\mathbb{F}_q$. One may take, for example, the element $Q = \delta \cdot 1_N$, for $\delta \in {\mathbb{F}_q}^\times$ 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 [33, 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*

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

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

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

Furthermore, the involution $\star$ of $\mathrm{GL}_N(\mathbb{F}_q)$ restricts to an involution of $\mathbf{C}_{\mathrm{GL}_N(\mathbb{F}_q)}(x)$ 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 $\mathrm{GL}_1(\mathbb{F}_q\langle f\rangle)$ for $f \in \{t^{d_1}, \varphi_i^{l_i}, \theta_i^{r_i}\}$.

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

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

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

Lastly, we compute order of the group Z. Since for any $w \in \mathrm{GL}_N(\mathbb{F}_q)$ 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 $\pm 1 \in \mathrm{GL}_N(\mathbb{F}_q)$, while the latter can be deduced by considering the Pfaffian of the matrix $w^t \mathbf{J} w = \mathbf{J}$. $\square$

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

1. *$\sigma_{f^r}(y) = y$, and*
2. *there exists $z \in \mathrm{GL}_1(\mathbb{F}_q\langle f(t)^r\rangle)$ 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 $\mathbb{F}_q\langle f^r\rangle$ 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 $\mathbb{F}_q\langle f^r\rangle$ with the ring $\mathcal{C} \subseteq \mathrm{M}_{r\cdot\deg f}(\mathbb{F}_q)$ 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 $y \in \mathbb{F}_q\langle f^r\rangle$ is the image modulo (f^r) of a polynomial $\widetilde{y}(t)$, then the assumption $\sigma_{f^r}(y) = y$ is equivalent to $\widetilde{y}(x) \in \mathcal{C}$ satisfying $\widetilde{y}(x)^\star = \widetilde{y}(x)$ or, in the notation of § 4.2.2, to $\widetilde{y}(x) \in \mathrm{Sym}(\star; x)$. Also, the nilpotent radical of $\mathcal{C}$ is given as the image of the ideal $(f) \subseteq \mathbb{F}_q\langle f^r\rangle$. The equivalence stated in the lemma now follows from Lemma 4.2.4, by taking $Q_1 = 1$ and $Q_2 = \widetilde{y}(x) \in \mathrm{Sym}(\star; x)$.

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 $\mathbb{F}_q[t]/(t^r)$ of truncated polynomials of degree no greater than $r - 1$, which consists of even polynomials whose constant term is an invertible square of $\mathbb{F}_q$. 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 $S, H \in \mathbb{F}_q[t]$ such that the endomorphism $S(x)$ (resp. $H(x)$) acts semisimply (resp. nilpotently) on the vector space $W = \mathbb{F}_q\langle f^r\rangle$, on which x acts by multiplication by t, and such that $H(t) + S(t) \equiv t \pmod{f(t)^r}$ (see [28, § 4.2]; note that $S, H \in \mathbb{F}_q[t]$ is possible since $\mathbb{F}_q$ is perfect). It follows that $\mathbb{F}_q\langle f^r\rangle \simeq \mathbb{F}_q[x] = \mathbb{F}_q[S(x)][H(x)]$. A quick computation shows that the minimal polynomials of $S(x)$ and $H(x)$ are $f(t)$ and t^r respectively, and thus $\mathbb{F}_q\langle f\rangle \simeq \mathbb{F}_q[S(x)][H(x)] \simeq \mathbb{F}_q\langle f\rangle \otimes_{\mathbb{F}_q} (\mathbb{F}_q[h]/(h^r))$. Moreover, by the properties of the Jordan-Chevalley decomposition, both $S(t)$ and $H(t)$ satisfy $S(-x) = -S(x)$ and $H(-x) = -H(x)$ [9, § 3, Proposition 3]. Thus, under this identification, the involution σ_{f^r} is transferred to an involution of $\mathbb{F}_q\langle f\rangle \otimes_{\mathbb{F}_q} (\mathbb{F}_q[h]/(h^r))$, mapping h to $-h$ and acting as σ_f on the field $\mathbb{F}_q\langle f\rangle$.

By the equivalence in the lemma, and the theory of finite fields, the group E_{f^r} is identified with the subgroup of $(\mathbb{F}_q\langle f^r\rangle)^\times$ 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 $a_0, \ldots, a_{r-1} \in \mathbb{F}_q\langle f\rangle$, $a_0 \neq 0$, 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 $m_x \in \mathbb{F}_q[t]$. Let $\boldsymbol{\tau}(m_x) = (r(m_x), S(m_x), T(m_x)) \in \mathfrak{X}_n$ 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. $\left|\mathrm{U}_1(\mathbb{F}_q\langle t^{d_1}\rangle)\right| = 2q^{r(m_x)}$;

2. $\left|\mathrm{U}_1(\mathbb{F}_q\langle \varphi_i^{l_i}\rangle)\right| = q^{\frac{1}{2}l_i \cdot \deg \varphi_i}(1 + q^{-\frac{1}{2}\deg \varphi_i})$;

3. $|\mathrm{GL}_1(\mathbb{F}_q\langle \tau_i^{r_i}\rangle)| = q^{r_i \cdot \deg \tau_i}(1 - q^{-\deg \tau_i})$.

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

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

which holds for any irreducible $f \in \mathbb{F}_q[t]$ 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 $|\mathrm{GL}_1(\mathbb{F}_q\langle f^r\rangle)|$ 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 $x \in \mathfrak{gl}_N(\boldsymbol{k})$ be a regular nilpotent element. Then x is not anti-symmetric with respect to any non-degenerate symmetric bilinear form on $V = \boldsymbol{k}^N$.*

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 [51, 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 $V = {\mathbb{F}_q}^N$ 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

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

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

Given $\epsilon \in \{\pm 1\}$, let $G_1^\epsilon = \mathrm{SO}_N^\epsilon(\mathbb{F}_q)$ and $\mathfrak{g}_1^\epsilon = \mathfrak{so}_N^\epsilon(\mathbb{F}_q)$ 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 $x \in \mathfrak{gl}_N(\mathbb{F}_q)$ 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 $x \in \mathfrak{gl}_N(\mathbb{F}_q)$ 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 $x \in \mathfrak{gl}_N(\mathbb{F}_q)$ 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 $u_0 \in \operatorname{Ker}(x)$ and such that $\mathcal{E} = \{v_0, xv_0, \ldots, x^{N-2}v_0, u_0\}$ is a $\mathbb{F}_q$-basis for V.

Let $\mathcal{E}' = \{v_0, \ldots x^{N-2}v_0\}$ and $V' = \operatorname{Span}_{\mathbb{F}_q} \mathcal{E}'$. Since the element $x \mid_{V'} \in \mathfrak{gl}(V')$ 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 $x \mid_{V'}$ 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 $\mathbf{d} \in \mathrm{M}_N(\mathbb{F}_q)$, 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 $\mathbf{d}^t\Upsilon + \Upsilon\mathbf{d} = 0$ where $\Upsilon = [x]_{\mathcal{E}} = J_{N-1}(0) \oplus J_1(0)$ is a nilpotent $N \times N$ matrix with an $(N-1) \times (N-1)$ upper-left nilpotent Jordan block. A short computation shows that the matrix

$$\mathbf{d} = \mathbf{d}_\eta = \begin{pmatrix} & & & 1 & \\ & & -1 & & \\ & \iddots & & & \\ 1 & & & & \\ & & & & \eta \end{pmatrix}, \tag{4.11}$$

where $\eta \in \mathbb{F}_q^\times$ 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 $\boldsymbol{k}$ of $\mathbb{F}_q$ and compute the centralizer in $\mathbf{G}(\boldsymbol{k})$ 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 $\mathrm{M}_N(\boldsymbol{k})$ 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. $\mathbf{A} \in \mathrm{M}_{N-1}(\boldsymbol{k})$ and commutes with the restriction of Υ to $V' = \operatorname{Span}_{\boldsymbol{k}} \mathcal{E}'$;

2. $\mathbf{u}, \mathbf{v} \in \boldsymbol{k}^{N-1}$ are elements of the kernel of Υ and Υ^t, respectively, and hence of the form $\mathbf{v} = \begin{pmatrix} v_1 & 0 & \dots & 0 \end{pmatrix}^t$ and $\mathbf{u} = \begin{pmatrix} 0 & \dots & 0 & u_{N-1} \end{pmatrix}^t$; and

3. $r \in \boldsymbol{k}$ is arbitrary.

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

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

Computing its Lie-algebra, which consists of matrices $\mathbf{y} \in \mathbf{C}_{\mathrm{M}_N(\boldsymbol{k})}(\Upsilon)$ 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 $\mathbf{A} \in \mathrm{M}_{N-1}(\mathbb{F}_q)$, column vectors $\mathbf{v}, \mathbf{u} \in {\mathbb{F}_q}^{N-1}$ and $r \in \mathbb{F}_q$, 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

$$\Xi(\mathbf{A}, \mathbf{v}, \mathbf{u}, r)^\star = \begin{pmatrix} \mathbf{A}^\flat & \eta\mathbf{c}\mathbf{u} \\ \eta^{-1}\mathbf{v}^t\mathbf{c} & r \end{pmatrix} = \Xi(\mathbf{A}^\flat, \eta\mathbf{c}\mathbf{u}, \eta^{-1}\mathbf{c}\mathbf{v}, r). \tag{4.12}$$

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

   Note that an element $u \in \mathbb{F}_q\langle\varphi\rangle$ 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 $\mathsf{K}/\mathbb{F}_q$ is $q^{n-1}-1$, and by the surjectivity of the norm map $\mathrm{Nr}_{\mathbb{F}_q\langle\varphi\rangle/\mathsf{K}}$, it follows that the number of non-zero isotropic element of $\mathbb{F}_q\langle\varphi\rangle$ is $(q^n+1)(q^{n-1}-1)$. The fact that C is of Witt index $n-1$ now follows as in [63, § 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 $\overline{L} \subseteq U^\perp/U$, 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 $\mathbb{F}_q$ with a non-degenerate symmetric bilinear form C, put $\delta_U = 1$ if U is of Witt index $\frac{1}{2}\dim_{\mathbb{F}_q} U$ and $\delta_U = -1$ otherwise.

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

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

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

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

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

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

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

$$U' \oplus W' \oplus \operatorname{Span}_{\mathbb{F}_q} \{\alpha_1 u_{2m-1} + \beta_1 w_{m-1} + u_{2m}, \alpha_2 u_{2m-1} + \beta_2 w_{2m-1} + w_{2m}\}$$

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

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 $\mathbb{F}_q[x]$-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 $x\mid_{W_f}$ 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 $\Pi_x = \mathrm{Ad}(\mathrm{GL}_N(\mathbb{F}_q))x \cap \mathfrak{g}_1^\epsilon$ 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 $|\mathbb{F}_q| > 3$ and $\mathrm{char}(\mathbb{F}_q) \neq 2$. For any element $\gamma \in \mathbb{F}_q{}^\times$ there exist $\nu, \delta \in \mathbb{F}_q{}^\times$ such that $\nu \in (\mathbb{F}_q{}^\times)^2$, $\delta \in \mathbb{F}_q{}^\times \smallsetminus (\mathbb{F}_q{}^\times)^2$ and such that $\gamma = \nu - \delta$.*

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

Proof. In the notation of Proposition 4.2.3, let $\Pi_x = \mathrm{Ad}(\mathrm{GL}_N(\mathbb{F}_q))x \cap \mathfrak{g}_1$ and Θ_x the set of equivalence classes in $\mathrm{Sym}(\star; x) = \left\{Q \in \mathbf{C}_{\mathrm{GL}_N(\mathbb{F}_q)}(x) \mid Q^\star = Q\right\}$ 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 $\mathbb{F}_q{}^N$ 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 $\mathbf{g}(\boldsymbol{k})$ [51, 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 the lemma, and that the ambient non-degenerate symmetric bilinear form is represented in $\mathcal{E}$ by the matrix $\mathbf{d} = \mathbf{d}_\eta$ of (4.11), where $\eta \in \mathbb{F}_q{}^\times$ is a square if $\epsilon = 1$ and non-square otherwise.

The centralizer $\mathcal{C}$ of Υ in $\mathrm{M}_N(\mathbb{F}_q)$ is isomorphic to the ring of $\mathbb{F}_q[x]$-endomorphisms of $\mathbb{F}_q[x] \times \mathbb{F}_q$, 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, $\mathbf{A} \in \mathrm{M}_{N-1}(\mathbb{F}_q)$ is an upper triangular Töplitz matrix, and $r \in \mathbb{F}_q$. 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 $\mathbb{F}_q \times \mathbb{F}_q$. 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 § 4.2.2, is isomorphic to the quotient group $\mathbb{F}_q{}^\times/(\mathbb{F}_q{}^\times)^2 \times \mathbb{F}_q{}^\times/(\mathbb{F}_q{}^\times)^2$ 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 $wxw^{-1} \in \Pi_x = \mathrm{Ad}(\mathrm{GL}_N(\mathbb{F}_q))x \cap \mathfrak{g}_1^\epsilon$ 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 $\mathbb{F}_q{}^\times/(\mathbb{F}_q{}^\times)^2$. 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 $\det \mathbf{A} \equiv r \pmod{(\mathbb{F}_q{}^\times)^2}$.

To complete the proof that $|\mathrm{Im}(\Lambda)| = 2$ it suffices to find an element $w \in \mathrm{GL}_N(\mathbb{F}_q)$ 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 $\det \mathbf{A}, r \notin (\mathbb{F}_q{}^\times)^2$.

Let $\eta \in \mathbb{F}_q{}^\times$ be as above put $\alpha = (-1)^{(N-2)/2}$. Let $\nu \in (\mathbb{F}_q{}^\times)^2$ and $\delta \in \mathbb{F}_q{}^\times \setminus (\mathbb{F}_q{}^\times)^2$ be such that $\alpha\eta = \nu - \delta$; see Lemma 4.4.8. Let $\nu_1 \in \mathbb{F}_q{}^\times$ be such that $\nu_1^2 = \nu$, and put $z = \eta \cdot \nu_1^{-1}$. Let $w \in \mathrm{GL}_N(\mathbb{F}_q)$ be represented in $\mathcal{E}$ by the matrix $\mathbf{w}$ of (4.13), 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 $\sim$.

$$\mathbf{w} = \begin{pmatrix} \delta & & & & & & \\ & \ddots & & & & & \\ & & \delta & & & & \\ & & & \nu_1 & & & \alpha z \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & -\eta^{-1}\nu_1 z & & & 1 \end{pmatrix}. \tag{4.13}$$

□

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

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

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

Case 1, $\gamma \in \mathbb{F}_q^\times \setminus (\mathbb{F}_q^\times)^2$. Note that in this case we must have that $\delta_1 \neq 0$, as otherwise $\gamma = \nu_1^2 \in (\mathbb{F}_q^\times)^2$. Furthermore, if $\nu_1 = 0$ for any pair (ν_1, δ_1) such that $\nu_1^2 - \xi\delta_1^2 = \gamma$ then $\mathrm{Nr}^{-1}_{\mathsf{K}|\mathbb{F}_q}(\gamma) \subseteq \xi_1\mathbb{F}_q^\times$, and in particular has order smaller than q. A contradiction.

Case 2, $\gamma \in (\mathbb{F}_q^\times)^2$. Consider the set $\mathrm{Nr}^{-1}_{\mathsf{K}|\mathbb{F}_q}(\gamma) \setminus \mathbb{F}_q^\times$. Note that, as $\left|\mathrm{Nr}^{-1}_{\mathsf{K}|\mathbb{F}_q}(\gamma) \cap \mathbb{F}_q^\times\right| = 2$, the order of $\mathrm{Nr}^{-1}_{\mathsf{K}|\mathbb{F}_q}(\gamma) \setminus \mathbb{F}_q^\times$ is exactly $q-1$. Assume towards a contradiction that there is no solution $(\nu_1, \delta_1) \in \mathbb{F}_q^\times \times \mathbb{F}_q^\times$ for the equation $\nu_1^2 - \xi\delta_1^2 = \mathrm{Nr}_{\mathsf{K}|\mathbb{F}_q}(\nu_1 - \xi_1\delta_1) = \gamma$. This implies that any solution not in $\mathbb{F}_q^\times \times \{0\}$ is an element of $\{0\} \times \mathbb{F}_q^\times$, or in other words, that $\mathrm{Nr}^{-1}_{\mathsf{K}|\mathbb{F}_q}(\gamma) \setminus \mathbb{F}_q^\times \subseteq \xi_1\mathbb{F}_q^\times$. 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 $\delta_1 \in \mathbb{F}_q^\times$, $\mathrm{Nr}_{\mathsf{K}|\mathbb{F}_q}(\xi_1\delta_1) = -\xi\delta_1^2 = \gamma$. Thus, the set of squares in $\mathbb{F}_q^\times$ equals the singleton set $\{-\xi^{-1}\gamma\}$. This contradicts the assumption $|\mathbb{F}_q| > 3$.

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 $\epsilon \in \{\pm 1\}$ and $x \in \mathfrak{g}_1^\epsilon$ regular with minimal polynomial $m_x(t) = t^{d_1}\prod_{i=1}^{d_2}\varphi_i^{l_i}\prod_{i=1}^{d_3}\theta_i^{r_i}$, decomposed 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*

$$1 \to \mathbf{C}_{G_1^\epsilon}(x) \to \mathcal{A}^\epsilon \times \prod_{i=1}^{d_2}\mathrm{U}_1(\mathbb{F}_q\langle\varphi_i^{l_i}\rangle) \times \prod_{i=1}^{d_3}\mathrm{GL}_1(\mathbb{F}_q\langle\tau_i^{r_i}\rangle) \xrightarrow{\det} \{\pm 1\} \to 1. \tag{4.14}$$

where $\mathcal{A}^\epsilon = \left\{\mathbf{w} \in \mathbf{C}_{\mathrm{GL}_{d_1+1}(\mathbb{F}_q)}(\Upsilon) \mid \mathbf{w}^t\mathbf{d}_\eta\mathbf{w} = \mathbf{d}_\eta\right\}$, *with* Υ *and* $\mathbf{d}_\eta$ *the* $(d_1+1)\times(d_1+1)$ *matrices defined in Lemma 4.4.2.*

2. *Otherwise, the group* $\mathbf{C}_{G_1^\epsilon}(x)$ *is isomorphic to* $\prod_{i=1}^{d_2} \mathrm{U}_1(\mathbb{F}_q\langle\varphi_i^{l_i}\rangle) \times \prod_{i=1}^{d_3} \mathrm{GL}_1(\mathbb{F}_q\langle\tau_i^{r_i}\rangle)$.

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 (4.14). 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 $\begin{pmatrix} 1_{d_1} & 0 \\ 0 & \pm1 \end{pmatrix} \in \mathcal{A}^\epsilon$.

For the second assertion, we need to verify that any element $w \in \mathbf{C}_{\mathrm{GL}_N(\mathbb{F}_q)}(x)$ such that $w^\star w = 1$ has determinant 1. Since any element of $\mathbf{C}_{\mathrm{GL}_N(\mathbb{F}_q)}(x)$ preserves the invariant factors of the decomposition of V as a $\mathbb{F}_q[x]$-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 $\varphi_i \in \mathbb{F}_q[t]$ 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 $\mathbb{F}_q[x]$-module and hence $\mathbf{C}_{\mathrm{M}_N(\mathbb{F}_q)}(x) \simeq \mathbb{F}_q[x] = \mathbb{F}_q[s][h] \simeq \mathbb{F}_q\langle\varphi_i\rangle[u]/(u^m)$ (see Lemma 4.3.8). Let $\rho : \mathbb{F}_q\langle\varphi_i\rangle[u]/(u^m) \to \mathbf{C}_{\mathrm{M}_N(\mathbb{F}_q)}(x)$ be a $\mathbb{F}_q$-linear isomorphism. The $\mathbb{F}_q$-linearity of ρ and the nilpotency of u imply that

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

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

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

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 $\mathbb{F}_q[x]$ module V, we have that $\mathbf{C}_{\mathrm{GL}_N(\mathbb{F}_q)}(x) \simeq \mathrm{GL}_1(\mathbb{F}_q\langle\tau(t)^r\rangle) \times \mathrm{GL}_1(\mathbb{F}_q\langle\tau(-t)^r\rangle)$. Moreover, the map $\star$ restricts to the map $(\xi,\nu) \mapsto (\iota^{-1}(\xi), \iota(\nu))$, where $\iota : \mathbb{F}_q\langle\tau(t)^r\rangle \to \mathbb{F}_q\langle\tau(-t)^r\rangle$ is the isomorphism induced from $t \mapsto -t$. Furthermore, since ι is a ring-isomorphism which preserves $\mathbb{F}_q$, we have that $\det(\iota(\xi)) = \det(\xi)$ for all $\xi \in \mathbb{F}_q\langle\tau(t)^r\rangle$. 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 $\boldsymbol{\tau}(c_x) = (r(c_x), S(c_x), T(c_x)) \in \mathfrak{X}_n$ 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 $\eta \in \mathbb{F}_q{}^{\times}$, and x is represented by the matrix Υ. Let $\mathcal{A}^{\epsilon} = \left\{z \in \mathbf{C}_{\mathrm{GL}_N(\mathbb{F}_q)}(\Upsilon) \mid z^t \mathbf{d} z = \mathbf{d}\right\}$, as in Lemma 4.4.10. Let $\mathcal{N} \subseteq \mathcal{A}^{\epsilon}$ be the subgroup consisting of elements of the form

$$\mathfrak{X}(\xi) = \begin{pmatrix} 1 & & 2\eta\xi^2 & 2\xi \\ & \ddots & & \\ & & 1 & \\ & & 2\eta\xi & 1 \end{pmatrix} \qquad (\xi \in \mathbb{F}_q).$$

Note that $\mathfrak{X}$ defines a one-parameter subgroup of $\mathcal{A}^{\epsilon}$ of order $|\mathbb{F}_q| = q$. 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 (4.12) 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 $|\mathcal{H}| = |\mathrm{U}_1(\mathbb{F}_q\langle t^{2n-1}\rangle) \times \{\pm 1\}| = 4q^{n-1}$ (by the first assertion in the proof of Proposition 4.3.9).

The condition $\Xi(\mathbf{A}, \mathbf{v}, \mathbf{u}, r) \in \mathcal{A}^{\epsilon}$, implies that $\mathbf{A}$ is invertible, and that $\mathbf{v} = \gamma \mathbf{d}\mathbf{u}$ for some $\gamma \in \mathbb{F}_q$. In particular, $\mathbf{v} = 0$ if and only if $\mathbf{u} = 0$. It follows 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.

Part II

Approximating the representation zeta function of finite groups of Lie type

Chapter 5

Outline and main results of Part II

Let $\boldsymbol{k} = \overline{\mathbb{F}_q}$ be a fixed algebraic closure of a finite field of characteristic $p > 3$, and let $\mathbf{G} \subseteq \mathrm{GL}_N(\boldsymbol{k})$ be a connected reductive algebraic group over $\boldsymbol{k}$, defined over $\mathbb{F}_q$. Let σ be an endomorphism such that the group $G = \mathbf{G}^\sigma$, of fixed points of σ, is finite. Following [41], we call such an endomorphism a *Steinberg endomorphism.* Let $\mathfrak{G} = \mathrm{Lie}(\mathbf{G})$ and $\mathfrak{g} = \mathfrak{G}^\sigma$, the $\mathbb{F}_q$-Lie-algebra of σ-fixed points. We note that the action of σ on $\mathfrak{G}$ is as defined in [32], which mandates the assumption $p > 3$.

In this setting, the representation zeta function of G is the complex valued function

$$\zeta_G(s) = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^{-s} \quad (s \in \mathbb{C}), \tag{5.1}$$

where $\mathrm{Irr}(G)$ denotes the set of irreducible characters of G. The *adjoint class function* of $\mathfrak{g}$ is defined to be the finite Dirichlet series

$$\epsilon_{\mathfrak{g}}(s) = \sum_{[x] \in \mathrm{Ad}(G)\backslash \mathfrak{g}} |\mathfrak{g} : \mathbf{C}_{\mathfrak{g}}(x)|^{-s/2} \quad (s \in \mathbb{C}), \tag{5.2}$$

where $\mathrm{Ad}(G)\backslash\mathfrak{g}$ is the space of orbits for the adjoint action of G on $\mathfrak{g}$, and $\mathbf{C}_{\mathfrak{g}}(x) = \mathrm{Ker}(\mathrm{ad}(x))$ is the Lie-algebra centralizer of x. Note that, under the additional assumption that p is *good* for $\mathbf{G}$ (see [56, I,§ 4.3]), it holds that $|\mathfrak{g} : \mathbf{C}_{\mathfrak{g}}(x)|$ is an integer square, and hence $\epsilon_{\mathfrak{g}}(s)$ is in fact a Dirichlet series in s (cf. [30, Proposition 1.11] and the succeeding discussion).

In this part of the dissertation we report on an ongoing project, relating the two functions defined above, in a manner which allows us to view the adjoint class function of $\mathfrak{g}$ as an approximant for the representation zeta function of G (see Conjecture 5.2.1 below). Let us briefly review our motivation for considering such an approximation, which arises from the study of representation of semisimple algebraic groups defined over finite extensions of $\mathbb{Z}_p$.

For simplicity, consider an affine $\mathbb{Z}_p$-group scheme $\mathscr{G}$ whose generic fibre is connected, simply-connected and semisimple (e.g. $\mathscr{G} = \mathrm{SL}_d$), and put $\Gamma = \mathscr{G}(\mathbb{Z}_p)$. For any $i \in \mathbb{N}$, let Γ^i be the congruence subgroup of Γ, i.e. $\Gamma^i = \mathrm{Ker}(\Gamma \to \mathscr{G}(\mathbb{Z}/p^i\mathbb{Z}))$. The factor group $G = \Gamma/\Gamma^1$ is finite semisimple of Lie-type over $\mathbb{F}_p$, and its representation zeta is given by the Dirichlet series enumerating irreducible characters of Γ whose restriction to Γ^1 contains the trivial character. The associated adjoint class function, while not equal to, is very closely related to the Dirichlet series enumerating characters of Γ^1 whose restriction to Γ^3 contains the trivial character, which is given by

$$\zeta_{\Gamma^1/\Gamma^3}(s) = q^{\dim \mathscr{G}} \cdot \sum_{x \in \mathrm{Lie}(\mathscr{G})(\mathbb{F}_p)} \left| \mathrm{Lie}(\mathscr{G})(\mathbb{F}_p) : \mathbf{C}_{\mathrm{Lie}(\mathscr{G})(\mathbb{F}_p)}(x) \right|^{-1-s/2}.$$

A recent ongoing project, joint with Uri Onn, has shown that the connection between ζ_{Γ/Γ^1} and $\zeta_{\Gamma^1/\Gamma^3}$ might be key in formulating a general connection between the representation zeta function of Γ and that of Γ^1, allowing one to possibly consider (a normalized version of) ζ_{Γ^1} as a viable approximant for ζ_Γ.

The precise approximation conjecture is stated in Section 5.2 below. Prior to presenting the precise statement, let us define a relation on the space of finite Dirichlet series, which formalizes our notion of approximation.

5.1 A relation on finite Dirichlet series

Given positive integers c and q, let $\mathbb{Q}_c[t]$ denote the set of polynomials with coefficients in the set $\frac{1}{c}\mathbb{Z} \cap [-c, c]$, and let $\mathscr{D}_{c,q}$ denote the set of finite Dirichlet series with non-negative integer coefficients which admit a presentation of the form $F(s) = \sum_{i=1}^{r} u_i(q)v_i(q)^{-s}$, with $u_i(t), v_i(t) \in \mathbb{Q}_c[t]$.

Definition 5.1.1. The series F_1 and F_2 are said to be (c, q)*-related*, denoted $F_1 \sim_{(c,q)} F_2$, if F_1 and F_2 can be written in the form $F_j(s) = \sum_{i=1}^{r_j} u_{i,j}(q)v_{i,j}(q)^{-s}$ ($j = 1, 2$) with $r_1 = r_2$ and such that $\deg u_{i,1} = \deg u_{i,2}$ and $\deg v_{i,1} = \deg v_{i,2}$ for all $i = 1, \ldots, r_1$.

5.2 The main conjecture

Consider the following example. Let $G = \mathrm{GL}_2(\mathbb{F}_q)$. The representation zeta function of G is well-known to be

$$\begin{aligned}\zeta_{\mathrm{GL}_2(\mathbb{F}_q)}(s) = (q-1) + (q-1)q^{-s} + \\ + \frac{1}{2}(q-1)(q-2)(q+1)^{-s} + \frac{1}{2}q(q-1)(q-1)^{-s}.\end{aligned}$$

Using the fact that non-central adjoint classes in $\mathfrak{gl}_2(\mathbb{F}_q)$ are parametrized by the characteristic polynomial of their elements, the adjoint class function of its Lie-algebra $\mathfrak{gl}_2(\mathbb{F}_q)$ can be easily computed, to obtain

$$\epsilon_{\mathfrak{gl}_2(\mathbb{F}_q)}(s) = q + q^{2-s}.$$

From the above two equations, rewriting $\epsilon_{\mathfrak{gl}_2(\mathbb{F}_q)}(s)$ as $q + \frac{1}{2}q^{1-s} + \frac{1}{2}(q^2 - q)q^{-s} + \frac{1}{2}q^{2-s}$, we see that $\zeta_{\mathrm{GL}_2(\mathbb{F}_q)}, \epsilon_{\mathfrak{gl}_2(\mathbb{F}_q)} \in \mathscr{D}_{2,q}$ and that

$$\zeta_{\mathrm{GL}_2(\mathbb{F}_q)} \sim_{(2,q)} \epsilon_{\mathfrak{gl}_2(\mathbb{F}_q)}.$$

Note that this remains true regardless of the value of q.

The results we report upon below arise from a general project, whose goal is to show that the phenomenon described above for $\mathrm{GL}_2(\mathbb{F}_q)$ is an instance of a much more general fact. Namely, we aim to prove the following.

Conjecture 5.2.1. *Let* $\mathsf{R} = (\Phi, X, \Phi^\vee, Y)$ *a root datum. There exists a natural number* $c = c(\mathsf{R})$ *and a prime number* $p_0 = p_0(\mathsf{R})$ *such that the following hold. For any finite field* $\mathbb{F}_q$ *of characteristic* $p > p_0$ *and cardinality* q*, and any* $\mathbb{F}_q$*-defined connected reductive algebraic group* $\mathbf{G}$ *over* $\boldsymbol{k} = \overline{\mathbb{F}_q}$ *with root datum* R *and Steinberg endomorphism* σ*, it holds that* $\zeta_G(s), \epsilon_{\mathfrak{g}}(s) \in \mathscr{D}_{c,q}$ *and*

$$\zeta_G(s) \sim_{(c,q)} \epsilon_{\mathfrak{g}}(s),$$

where $G = \mathbf{G}^\sigma$ *and* $\mathfrak{g} = \mathrm{Lie}(\mathbf{G})^\sigma$*.*

5.3 Proof strategy and statement of main results

5.3.1 Jordan-type decomposition

In order to approach the question of comparing the representation zeta function and the adjoint class function we make use of a Jordan-type decomposition related to each of these functions, which allows us to separate our analysis into that of "semisimple objects" and of "unipotent objects".

To begin with, we consider the adjoint class function. Using the additive Jordan decomposition on $\mathfrak{g}$, we have that

$$\begin{aligned} \epsilon_{\mathfrak{g}}(s) &= \sum_{[x] \in \mathrm{Ad}(G)\backslash \mathfrak{g}} |\mathfrak{g} : \mathbf{C}_{\mathfrak{g}}(x)|^{-s/2} \\ &= \sum_{[x_s] \in \mathrm{Ad}(G)\backslash \mathfrak{g}_{\mathrm{ss}}} |\mathfrak{g} : \mathbf{C}_{\mathfrak{g}}(x_s)|^{-s/2} \cdot \epsilon^{\mathrm{nil}}_{\mathbf{C}_{\mathfrak{g}}(x_s)}(s), \end{aligned} \tag{5.3}$$

where $\mathfrak{g}_{\mathrm{ss}}$ denotes the locus of semisimple elements in $\mathfrak{g}$, $\epsilon^{\mathrm{nil}}_{\mathfrak{h}}(s) = \sum_{[x_n] \in \mathrm{Ad}(H)\backslash \mathfrak{h}_{\mathrm{nil}}} |\mathfrak{h} : \mathbf{C}_{\mathfrak{h}}(x_n)|^{-s/2}$, and $\mathfrak{h}_{\mathrm{nil}}$ denotes the locus of nilpotent elements, whenever $\mathfrak{h} = \mathrm{Lie}(\mathbf{H})^\sigma$ is the Lie-algebra of σ-fixed points of a closed and σ-stable subgroup $\mathbf{H} \subseteq \mathbf{G}$, and $H = \mathbf{H}^\sigma$.

A similar type of decomposition for the representation zeta function is due to Lusztig (see [39, p. ix-x]). To define this decomposition, let $\mathbf{G}^*$ be the dual algebraic group of $\mathbf{G}$, with σ^* a dual endomorphism to σ (see Section 6.5 below), and put $G^* = (\mathbf{G}^*)^{\sigma^*}$. By [19, Proposition 13.17], the set $\mathrm{Irr}(G)$ may be partitioned into *Lusztig series*, indexed by semisimple conjugacy classes in G^* (see Section 6.6 for additional details). Using Theorem 13.23 and Remark 13.24 of [19], it follows that

$$\zeta_G(s) = \sum_{[g_s] \in \mathrm{Ad}(G^*)\backslash G^*_{\mathrm{ss}}} \left(\frac{|G|_{p'}}{|\mathbf{C}_{G^*}(g_s)|_{p'}} \right)^{-s} \zeta^{\mathrm{unip}}_{\mathbf{C}^*_G(g_s)}(s), \tag{5.4}$$

where $x_{p'}$ denotes the prime-to-p part of an integer x, $\zeta_H^{\mathrm{unip}}(s) = \sum_{\chi \in \mathcal{E}(H,(1))} \chi(1)^{-s}$, and $\mathcal{E}(H,(1))$ is the set of *unipotent characters* of H, for any finite reductive group of Lie-type $H = \mathbf{H}^\sigma$ (see Section 6.6).

5.3.2 Semisimple classes

Our first step towards achieving the comparison of the representation zeta function of G and of the adjoint class function $\epsilon_{\mathfrak{g}}$, as in Conjecture 5.2.1, is a parallel analysis of the semisimple conjugacy classes in G^* and of the semisimple adjoint classes in $\mathfrak{g}$. This analysis is performed in Chapter 7, in the generality of $\mathbf{G}$ a semismiple group of adjoint type, and its results are summarized in Theorem 7.0.1 below.

The results of the analysis of Chapter 7 allow us to rearrange the terms in (5.3) and (5.4) as sums indexed by a "globally" defined index set. That is to say, we find a finite index set I and a prime p_0, dependent only on the root datum of $\mathbf{G}$. For any $i \in I$, there exist finite Dirichlet series $\mathscr{X}_i^G$, $\mathscr{E}_i^{\mathfrak{g}}$ of the form

$$\mathscr{X}_i^G(s) = \sum_{j=1}^{n_i} u_{i,j}^G(q) v_{i,j}^G(q)^{-s} \zeta_{H_{i,j}^*}^{\mathrm{unip}}(s) \quad \text{and} \quad \mathscr{E}_i^{\mathfrak{g}}(s) = u_i^{\mathfrak{g}}(q) v_i^{\mathfrak{g}}(q)^{-s} \epsilon_{\mathfrak{h}_{i,1}}^{\mathrm{nil}}(s), \tag{5.5}$$

with $H_{i,j}^*$ subgroups of G^* and $\mathfrak{h}_{i,1}$ a sub-Lie-algebra of $\mathfrak{g}$, such that, assuming $p > p_0$,

$$\zeta_G(s) = \sum_{i \in I} \mathscr{X}_i^G(s) \quad \text{and} \quad \epsilon_{\mathfrak{g}}(s) = \sum_{i \in I} \mathscr{E}_i^{\mathfrak{g}}(s).$$

While the series $\mathscr{X}_i^G$, $\mathscr{E}_i^{\mathfrak{g}}$ themselves are dependent on the field of definition, their variation upon replacing this field is shown to be rather tame. The precise meaning of this "tameness of variation" is explicated in Theorem 7.0.1 below. Informally, it means that the degree to which these series vary becomes increasingly negligible as the cardinality of the field of definition increases. Slightly more precisely, the numbers n_i and the degrees of the $u_{i,j}^G$, $v_{i,j}^G$, $u_i^{\mathfrak{g}}$ and $v_i^{\mathfrak{g}}$ are determined by the set I, and hence by the root datum of $\mathbf{G}$, and furthermore, the coefficients of these polynomials are taken from a finite and predetermined set of rational numbers, also dependent on the root datum of $\mathbf{G}$.

One notable difference between the semisimple loci of G^* and $\mathfrak{g}$, which is apparent already in (5.5), is the distinctly richer array of centralizers of semisimple elements, up to isomorphism, in the group case, as opposed to the Lie-algebra case. Specifically, excluding finitely many cases of p, it follows from [57, Corollary 3.8] and [41, Proposition 12.10] that centralizers of semisimple elements of $\mathfrak{g}$ are given by Levi subgroups of $\mathbf{G}$ (also see Proposition 2.1.1 above for a direct proof in the classical case). In contrast, the centralizer of a semisimple group element may in fact not be included in any Levi subgroup. Such elements are called *isolated*. This difference is apparent in the fact that, while the series $\mathscr{E}_i^{\mathfrak{g}}$ involve a single reductive subalgebra $\mathfrak{h}_{i,1}$ of $\mathfrak{g}$, the series $\mathscr{X}_i^G$ often involve a multitude of groups $H_{i,j}^*$. The groups $H_{i,j}^*$ are in fact of the form $(\mathbf{H}_{i,j}^*)^{\sigma^*}$, for $\mathbf{H}_{i,j}^*$ a σ^*-stable reductive subgroup of $\mathbf{G}^*$. The first of these $\mathbf{H}_{i,1}^*$ is always taken to be a Levi-subgroup of

$\mathbf{G}^*$, and the groups $\mathbf{H}^*_{i,j}$, for $j \geq 2$, are the centralizers of isolated element of $H^*_{i,1}$. The Lie-algebra $\mathfrak{h}_{i,1}$ is the σ-fixed subalgebra of $\mathrm{Lie}(\mathbf{H}_{i,1})$, for $\mathbf{H}_{i,1}$ the dual algebraic group of $\mathbf{H}^*_{i,1}$.

5.3.3 Unipotent representations and nilpotent classes

The analysis of Chapter 7 leads us to consider the following question.

Question 5.3.1. *Let $\mathbf{H}$ be a $\mathbb{F}_q$-defined connected reductive group over $\boldsymbol{k}$ with root system Φ and Steinberg endomorphism σ, and let $\mathbf{H}_1, \ldots, \mathbf{H}_r$ be distinct representatives for all conjugacy classes of centralizers of σ-fixed isolated elements of $\mathbf{H}$, and put $\mathbf{H}_0 = \mathbf{H}$. Write $H_i = \mathbf{H}_i^\sigma$, and put $\mathfrak{h}^* = \mathrm{Lie}(\mathbf{H}^*)^{\sigma^*}$, where $(\mathbf{H}^*, \sigma^*)$ is the dual algebraic group of $\mathbf{H}$, with dual Steinberg endomorphism σ^*. Does there exist a constant $c = c(\Phi)$ and a prime $p_0 = p_0(\Phi)$, determined by Φ, such that*

$$\epsilon^{\mathrm{nil}}_{\mathfrak{h}^*}(s) \sim_{(c,q)} \sum_{j=0}^{r} |H_0 : H_j|_{p'}^{-s} \, \zeta^{\mathrm{unip}}_{H_j}(s), \tag{5.6}$$

whenever $p = \mathrm{char}(\boldsymbol{k}) > p_0$?

One case for which giving a positive answer to Question 5.3.1 is immediately approachable is the case of $\mathbf{H}$ a group of type A_ℓ, as in this case it is known that no isolated elements exist in $\mathbf{H}$. Therefore, in this case the question reduces to whether

$$\epsilon^{\mathrm{nil}}_{\mathfrak{h}^*}(s) \sim_{(c,q)} \zeta^{\mathrm{unip}}_{H}(s),$$

for some c and $p_0 < \mathrm{char}(\boldsymbol{k})$. In Section 8.1 below, we give an affirmative answer to this question for the case of $\mathbf{H} = \mathrm{SL}_n(\boldsymbol{k})$, with the Steinberg endomorphisms giving rise to $H = \mathrm{SL}_n(\mathbb{F}_q)$ and $H = \mathrm{SU}_n(\mathbb{F}_{q^2}, \mathbb{F}_q)$.

A more intricate case which we also consider in Chapter 8 is that of the symplectic group $\mathrm{Sp}_{2n}(\boldsymbol{k})$. In this case, centralizers of isolated elements do exists, and are all of the form $\mathbf{H}_i = \mathrm{Sp}_{2i}(\boldsymbol{k}) \times \mathrm{Sp}_{2(n-i)}(\boldsymbol{k})$, for $i = 1, \ldots, \lfloor n/2 \rfloor$. In Section 8.2 we give an affirmative answer to Question 5.3.1 in the case of $\mathbf{H} = \mathrm{Sp}_{2n}(\boldsymbol{k})$ with the Frobenius endomorphism, such that $H = \mathrm{Sp}_{2n}(\mathbb{F}_q)$, for $n = 1, \ldots, 41$. The somewhat awkward restriction of n is a consequence of a combinatorial identity which, to date, I was unable to prove rigorously (see Lemma B.2.2). The identity has verified using MathLab for $n \leq 41$. Our results are summarized in Theorem 8.0.1.

In both cases, our proofs are combinatorially oriented, and rely heavily on the existing knowledge of dimensions of unipotent characters [13, § 13.8] and the dimensions of centralizers of nilpotent elements in classical Lie-algebras [51, Ch. IV]. Lamentably, deep theoretical insight regarding the origin of our results in Chapter 8 is still lacking.

5.4 Discussion and Future research

One obvious goal for future research is the extension of our results to the generality of connected reductive groups. As far as the analysis of semisimple classes goes, the central step towards this extension would be to pass from groups of adjoint type to general semisimple groups. This extension seems highly likely, from inspection of the representation zeta function and adjoint class zeta function associated to several cases of non-adjoint groups of small rank. Regarding the analysis of unipotent representations and nilpotent characters, as in Question 5.3.1, several cases of classical groups of type B_n and D_n of small rank have been inspected as well, showing the question to be answered in the positive in these cases as well. Analysis of the remaining simple group types is, to date, only partial. However, it is highly likely to be achievable as well.

5.5 Organization of Part II

In Chapter 6 we present the necessary preliminaries which we require in our analysis; namely, regarding linear algebraic groups and the root data. We set up the technical tools which we require in proving Theorem 7.0.1, including the passage from the analysis of an algebraic group and its Lie-algebra to its dual algebraic group, and recall the basic definitions of Deligne-Lustig theory. Finally, we gather some basic properties regarding the set $\mathbb{Q}_c[t]$ and the relation $\sim_{(c,q)}$.

Chapter 7 deals with the comparative analysis of semisimple conjugacy classes in $\mathbf{G}^*$ and of semisimple adjoint classes in $\mathfrak{g}$. Following this, we conclude in Chapter 8 by proving specific instances of Question 5.3.1.

5.5.1 Remarks regarding terminology

This part of the dissertation deals simultaneously with characters, polynomials and graph vertices, all of which have an independent notion of degree. In order to avoid confusion between these terms, we will use the alternative terminology of "character dimensions", rather than "character degrees" and "valency of a vertex" rather than "degree of a vertex". Thus, the term degree is used solely for "the degree of a polynomial".

The mathematical language of this part is slightly different, and rather more antiquated, than that of the previous part. Namely, we follow the conventions of [13, 19, 41, 51], and consider our groups as the subgroups of fixed points under an endomorphism of a linear algebraic subgroup of $\mathrm{GL}_N(\boldsymbol{k})$, rather than as the $\mathbb{F}_q$-point of a, say e.g. $\mathbb{Z}$-defined, group scheme. This terminology, while at times slightly cumbersome, has proved more convenient for the current study. It is most likely that everything may be rephrased completely analogously in the more modern language of group schemes.

Chapter 6

Preliminaries and basic definitions on finite reductive groups

6.1 Linear algebraic groups over $\boldsymbol{k}$

As in the introduction, we fix a prime $p > 3$ and $q = p^a$, for some $a \in \mathbb{N}$, and let $\boldsymbol{k}$ denote the algebraic closure of the finite field $\mathbb{F}_q$. Recall that a linear algebraic group $\mathbf{G} \subseteq \mathrm{GL}_N(\boldsymbol{k})$ is said to be *defined over* $\mathbb{F}_q$ (or $\mathbb{F}_q$-defined, for short) if its underlying algebraic variety can be defined by a set of polynomials $I \subseteq \mathbb{F}_q[t_1, \dots, t_{N^2}]$ with coefficients in $\mathbb{F}_q$. Note that, the Frobenius map $F_q : \mathrm{GL}_N(\boldsymbol{k}) \to \mathrm{GL}_N(\boldsymbol{k})$, $(a_{i,j}) \mapsto (a_{i,j}^q)$ restricts to an automorphism of $\mathbf{G}$, whenever $\mathbf{G}$ is $\mathbb{F}_q$-defined. A *Steinberg endomorphism* on such a group is a homomorphism $\sigma : \mathbf{G} \to \mathbf{G}$ such that, for some $m \geq 1$, the power $\sigma^m : \mathbf{G} \to \mathbf{G}$ coincides with a power F_q^b of the Frobenius map on $\mathbf{G}$. This definition is equivalent to the one given in Chapter 5; see [41, Theorem 21.5]. The following theorem is central in the study of groups equipped with such endomorphisms.

Theorem 6.1.1 (Lang-Steinberg,[55, Theorem 10.1])**.** *Let $\mathbf{G}$ be a connected linear algebraic group over $\boldsymbol{k}$ with a Steinberg endomorphism $\sigma : \mathbf{G} \to \mathbf{G}$, and let*

$$\mathsf{L} : \mathbf{G} \to \mathbf{G}, \quad x \mapsto x\sigma(x)^{-1}$$

be the associated Lang map. Then L is surjective.

We also recall an important definition (see [51, p. 173]).

Definition 6.1.2. Let A be an abstract group and $\psi : A \to A$ an endomorphism. Two elements $a, b \in A$ are said to be ψ-conjugate, denoted $a \sim_\psi b$, if there exists $c \in A$ such that $a = cb\psi(c)^{-1}$. The set of ψ-conjugacy classes of A is denoted by $H^1(\psi, A)$.

Remark 6.1.3. In the case where $A = \mathbf{G}$ is an $\mathbb{F}_q$-defined linear algebraic group over $\boldsymbol{k}$ and $\sigma = F_q$ is the Frobenius map, the set $H^1(\sigma, \mathbf{G})$ is precisely the first Galois cohomology $H^1(\mathrm{Gal}(\boldsymbol{k}/\mathbb{F}_q), \mathbf{G})$ (see, e.g. [61, Ch. 17]).

Lemma 6.1.4. *Let* $\mathbf{G}$ *and* σ *be as above.*

1. *Let* $\mathbf{H}$ *be a closed* σ*-stable subgroup of* $\mathbf{G}$*. Then the identity component* $\mathbf{H}^\circ$ *of* $\mathbf{H}$ *is also* σ*-stable and the natural map* $[x] \mapsto [x\mathbf{H}^\circ] : H^1(\sigma, \mathbf{H}) \to H^1(\sigma, \mathbf{H}/\mathbf{H}^\circ)$ *is a bijection.*

2. *Let* $\mathbf{X}$ *be a non-empty left homogeneous space for* $\mathbf{G}$ *on which* σ *acts in a compatible manner, i.e.* $\sigma(gx) = \sigma(g)\sigma(x)$ *for all* $g \in \mathbf{G}$ *and* $x \in \mathbf{X}$*. Then* $\mathbf{X}$ *contains a* σ*-fixed point. Moreover, given* $x_0 \in \mathbf{X}^\sigma$*, a* σ*-fixed point with* $\mathbf{H} = \mathrm{Stab}^{\mathbf{G}}(x_0)$*, the stabilizer subgroup, a closed subgroup of* $\mathbf{G}$*, we have a bijection*

$$\left\{\text{Orbits in } \mathbf{X}^\sigma \text{ for the action of } \mathbf{G}^\sigma\right\} \quad \longleftrightarrow \quad H^1(\sigma, \mathbf{H}/\mathbf{H}^\circ).$$

Proof. See [51, I, 2.6 and 2.7]. □

In particular, applying Lemma 6.1.4 to the action of $\mathbf{G}$ on the set $\mathbf{X}$ of pairs $(\mathbf{T}, \mathbf{B})$, where $\mathbf{T}$ is a maximal torus in $\mathbf{G}$ and $\mathbf{B}$ is a Borel subgroup containing $\mathbf{T}$, given by $g.(\mathbf{T}, \mathbf{B}) = (g\mathbf{T}g^{-1}, g\mathbf{B}g^{-1})$, one deduces the following (see [51, I, 2.9])

Lemma 6.1.5. *Let* $\mathbf{G}$ *be a connected reductive algebraic group over* $\boldsymbol{k}$ *with Steinberg endomorphism* σ*. Then* σ *fixes a Borel subgroup* $\mathbf{B} \subseteq \mathbf{G}$ *and a maximal torus* $\mathbf{T} \subseteq \mathbf{B}$*. Furthermore, any two such couples are conjugate by an element* $\mathbf{G}^\sigma$*.*

A σ-stable maximal torus $\mathbf{T} \subseteq \mathbf{G}$ is said to be *maximally split* if it is included in a σ-stable Borel subgroup $\mathbf{B} \subseteq \mathbf{G}$. From here on, we fix a maximally split maximal torus and σ-stable Borel subgroup $\mathbf{T} \subseteq \mathbf{B} \subseteq \mathbf{G}$ and write T, B and G for the respective σ-fixed subgroups $\mathbf{T}^\sigma, \mathbf{B}^\sigma$ and $\mathbf{G}^\sigma$.

6.1.1 The Lie-algebra of $\mathbf{G}$

The Lie-algebra of a linear algebraic group $\mathbf{G}$ is defined to be the tangent space of $\mathbf{G}$ at 1, that is

$$\begin{aligned}\mathrm{Lie}(\mathbf{G}) &= T_1(\mathbf{G}) \\ &= \{\delta \in \mathrm{Hom}_{\boldsymbol{k}}(\boldsymbol{k}[\mathbf{G}], \boldsymbol{k}) : \delta(fg) = f(1)\delta(g) + \delta(f)g(1) \text{ for all } f, g \in \boldsymbol{k}[\mathbf{G}]\}\,. \end{aligned} \tag{6.1}$$

Here $\boldsymbol{k}[\mathbf{G}]$ denotes the algebra of regular functions on $\mathbf{G}$. The Lie-bracket on $\mathrm{Lie}(\mathbf{G})$ is pulled back from the bracket operation on the space $\mathscr{L}(\mathbf{G}) \subseteq \mathrm{Der}_{\boldsymbol{k}}(\boldsymbol{k}[\mathbf{G}])$ of left-invariant $\boldsymbol{k}$-derivations on $\boldsymbol{k}[\mathbf{G}]$, via the isomorphism

$$\eta : \mathrm{Lie}(\mathbf{G}) \to \mathscr{L}(\mathbf{G}) \quad \eta(\delta)(f)(x) = \delta(\lambda_{x^{-1}} f) \quad (x \in \mathbf{G},\ f \in \boldsymbol{k}[\mathbf{G}]),$$

where $\lambda_{x^{-1}} f(g) = f(x^{-1}g)$ is the left regular action on $\boldsymbol{k}[\mathbf{G}]$ (see [27, 9.2]).

Given a morphism of algebraic groups $\varphi : \mathbf{G}_1 \to \mathbf{G}_2$ the *differential* of φ at 1 is defined by $d\varphi = (\delta \mapsto \delta \circ \varphi^*) : T_1(\mathbf{G}_1) \to T_1(\mathbf{G}_2)$, where $\varphi^* = (f \mapsto f \circ \varphi) : \boldsymbol{k}[\mathbf{G}_2] \to \boldsymbol{k}[\mathbf{G}_1]$ is the comorphism associated to φ. In this situation, the map $\mathrm{Lie}(\varphi) = d\varphi : \mathrm{Lie}(\mathbf{G}_1) \to \mathrm{Lie}(\mathbf{G}_2)$ is a Lie-algebra homomorphism, and the association $\varphi \mapsto \mathrm{Lie}(\varphi)$ is functorial.

Let $\mathbf{G}$ be a linear algebraic group over $\boldsymbol{k}$ with Steinberg endomorphism σ, and let $\mathfrak{G} = \mathrm{Lie}(\mathbf{G})$. The differential of σ is a nilpotent operator on $\mathfrak{G}$ (see [55, 10.5]), and in particular has no fixed points. It is, however, possible the extend the notion of a σ-fixed subalgebra of $\mathfrak{G}$, as is done in [32], under certain mild assumptions on the characteristic of $\boldsymbol{k}$. The precise definition of the action of σ on $\mathfrak{G}$ and the subalgebra $\mathfrak{g}$ of σ-fixed elements is recalled in § 6.2.4 below. For the meanwhile, it is sufficient for us to know that $\mathfrak{g}$ is a $\mathbb{F}_q$-form of $\mathfrak{G}$ (i.e. $\mathfrak{G} = \mathfrak{g} \otimes \boldsymbol{k}$, see [32, 1.4]), and that the functor Lie induces a bijection between the set of maximal tori in $\mathbf{G}$, and the set of maximal toric subalgebras of $\mathfrak{G}$, mapping σ-stable tori to σ-stable subalgebras; see [32, § 3].

6.2 Root data

From here on we assume $\mathbf{G}$ is connected reductive. The group $\mathbf{G}$ acts on its Lie-algebra via the adjoint map $\mathrm{Ad} : \mathbf{G} \to \mathrm{Aut}(\mathfrak{G})$; its subgroup $\mathbf{T}$ acts a subgroup of simultaneously diagonalizable operators on $\mathfrak{G}$. The set of *roots* of $\mathbf{G}$ with respect to $\mathbf{T}$ is

$$\begin{aligned}\Phi &= \Phi(\mathbf{G}, \mathbf{T}) \\ &= \{\alpha \in \mathrm{Hom}(\mathbf{T}, \mathbb{G}_m) : \exists x \in \mathfrak{G} \text{ non-zero, such that } \mathrm{Ad}(t)x = \alpha(t)x \text{ for all } t \in \mathbf{T}\} .\end{aligned}$$

Put $X = X(\mathbf{T}) = \mathrm{Hom}(\mathbf{T}, \mathbb{G}_m)$ and $Y = Y(\mathbf{T}) = \mathrm{Hom}(\mathbb{G}_m, \mathbf{T})$ the groups of characters and cocharacters of $\mathbf{T}$, respectively. A subset $S \subseteq \Phi$ is called a *base* of Φ, if the set $\{\alpha \otimes 1 : \alpha \in S\} \subseteq E = X \otimes_{\mathbb{Z}} \mathbb{R}$ is a vector space basis over $\mathbb{R}$, and if any element $\beta \in \Phi$ may be written as $\beta = \sum_{\alpha \in S} c_\alpha \alpha$ with either all $c_\alpha \geq 0$ or all $c_\alpha \leq 0$. In this situation, it holds that $\Phi \subseteq \mathbb{Z}S$, i.e. any element of ϕ is an *integral* linear combination of elements of S (see [41, Corollary A.12]). The set $\Phi^+ = \left\{\beta = \sum_{\alpha \in S} c_\alpha \alpha : \sum_\alpha c_\alpha \geq 0\right\}$ is the set of *positive roots* of Φ with respect to S. Furthermore, any subset of Φ of the form $\{\alpha : \lambda \geq 0\}$ for a linear function λ on E contains a unique base of Φ, and is then the set of positive roots with respect to this base.

Recall that there exists a prefect pairing $\langle\, , \rangle : X \times Y \to \mathbb{Z}$ given by the condition $\chi \circ \gamma(\xi) = \xi^{\langle \chi, \gamma \rangle}$ for all $\chi \in X, \gamma \in Y$ and $\xi \in \mathbb{G}_m$. For any $\alpha \in \Phi$ there exists a unique $\alpha^\vee \in Y$ such that $\langle \alpha, \alpha^\vee \rangle = 2$ and such that the map

$$s_\alpha = (\chi \mapsto \chi - \langle \chi, \alpha^\vee \rangle \alpha) \tag{6.2}$$

is an automorphism of X, which preserves Φ and extends to a reflection on the Euclidean space E along the vector $\alpha \otimes 1$. Put $\Phi^\vee = \{\alpha^\vee : \alpha \in \Phi\}$, the set of *coroots* of $\mathbf{G}$ with respect to $\mathbf{T}$. The sets Φ and $\Phi^\vee$ are abstract root systems in E and $E^\vee = Y \otimes_{\mathbb{Z}} \mathbb{R}$ (see [41, Definition 9.1]). Furthermore, given a base S of Φ, the set $S^\vee = \{\alpha^\vee : \alpha \in S\}$ is a base of $\Phi^\vee$. The quadruple $(X, \Phi, Y, \Phi^\vee)$ is the *root datum* of $\mathbf{G}$ with respect to $\mathbf{T}$ [41, Proposition 9.11].

6.2.1 The Weyl group

The Weyl group of $\mathbf{G}$ with respect to $\mathbf{T}$ is the finite group $W = W_{\mathbf{G}}(\mathbf{T}) = \mathbf{N}_{\mathbf{G}}(\mathbf{T})/\mathbf{T}$. The conjugation action of W on $\mathbf{T}$ naturally gives rise to faithful actions of W on X and on Y via

$$(w\chi)(t) = \chi({}^{w^{-1}}t) \qquad \text{for all } w \in W,\ \chi \in X,\ t \in \mathbf{T};\ \text{and} \tag{6.3}$$

$$(w\gamma)(\xi) = {}^{w}(\gamma(\xi)) \qquad \text{for all } w \in W,\ \gamma \in Y \text{ and } \xi \in \mathbb{G}_m. \tag{6.4}$$

Here and in the sequel the notation ${}^{w}t$ stands for $n_w t n_w^{-1}$, where $n_w \in \mathbf{N}_{\mathbf{G}}(\mathbf{T})$ is some coset representative of w.

The image of W in $\mathrm{Aut}(X)$, under the action (6.3), is identified with W, and is generated by the set of reflections $\{s_\alpha : \alpha \in \Phi\}$ [41, Proposition 8.20]. In particular $W(\Phi) = \Phi$. Note that, by definition, the pairing $\langle\ ,\ \rangle$ on $X \times Y$ is W invariant, i.e.

$$\langle w\chi, w\gamma\rangle = \langle \chi, \gamma\rangle \text{ for all } \chi \in X \text{ and } \gamma \in Y. \tag{6.5}$$

Furthermore, the uniqueness of $\alpha^\vee$ and (6.5) imply that

$$s_{\alpha^\vee}\gamma = \gamma - \langle \alpha, \gamma\rangle \alpha^\vee \quad \text{for all } \alpha^\vee \in \Phi^\vee \text{ and } \gamma \in Y,$$

where $s_{\alpha^\vee}$ is the reflection of $E^\vee = Y \otimes_{\mathbb{Z}} \mathbb{R}$ along the root $\alpha^\vee$; see [41, Proposition 9.11]. Using this equation and the equality $s_{s_\alpha\beta} = s_\alpha s_\beta s_\alpha$, one easily verifies that $(s_\alpha\beta)^\vee = s_{\alpha^\vee}\beta^\vee$ for all $\alpha, \beta \in \Phi$.

6.2.2 Closed subsystems of Φ

Definition 6.2.1 (Parabolic subsystem). A closed subsystem $\Psi \subseteq \Phi$ is said to be *parabolic* if there exists a base S of Φ such that $I = S \cap \Psi$ is a base of Ψ.

Note that a subsystem $\Psi \subseteq \Phi$ is parabolic if and only if the group W_Ψ, generated by reflections of $E = X \otimes_{\mathbb{Z}} \mathbb{R}$ along the roots in Ψ is a parabolic subgroup of W (see, e.g. [21, § 2]).

Definition 6.2.2 (Locally isolated subsystem). Let $\Sigma \subseteq \Psi \subseteq \Phi$ be two closed subsystems. We say that Σ is *isolated in* Ψ if $\mathrm{Span}_{\mathbb{R}}\, \Sigma = \mathrm{Span}_{\mathbb{R}}\, \Psi \subseteq E$ and $\Sigma \neq \Psi$. We call Σ *locally isolated* if there exists a closed subsystem $\Psi \subseteq \Phi$ such that Σ is isolated in Ψ.

In particular, if Σ is isolated in Ψ, then any two bases of Σ and Ψ are of the same cardinality.

Lemma 6.2.3. 1. *Let $\Psi \subseteq \Phi$ be a parabolic subsystem and assume $\Sigma \subseteq \Phi$ is another closed subsystem such that* $\mathrm{Span}_{\mathbb{R}}\, \Sigma = \mathrm{Span}_{\mathbb{R}}\, \Psi$. *Then $\Sigma \subseteq \Psi$.*

2. *If Σ is locally isolated then there exists a unique parabolic subsystem $\Psi \subseteq \Phi$ such that Σ is isolated in Ψ.*

Proof. 1. Let S be a base for Φ and $I \subseteq S$, a base for Ψ. Let $\beta \in \Sigma$ be arbitrary. Then, since $\mathrm{Span}_{\mathbb{R}} \Sigma = \mathrm{Span}_{\mathbb{R}} \Psi$ there exist $c_\alpha \in \mathbb{R}$ ($\alpha \in I$) such that $\beta = \sum_{\alpha \in I} c_\alpha \alpha$. Also, since $\beta \in \Phi$, it holds that $\beta = \sum_{\alpha \in S} d_\alpha \alpha$, with either all d_α non-negative or all d_α non-positive. By linear independence of S, $d_\alpha = 0$ for any $\alpha \notin I$ and $d_\alpha = c_\alpha \in \mathbb{Z}$ for all $\alpha \in I$, and in particular, either $c_\alpha \geq 0$ for all $\alpha \in I$ or $c_\alpha \leq 0$ for all $\alpha \in I$. Thus, I is a base for a subsystem of Φ which contains Σ. Invoking a standard argument (see [41, Corollaries B.1 and B.2]) one may now verify that necessarily $\Sigma \subseteq \Psi$.

2. Consider the closed subsystem $\Psi = \Phi \cap \mathrm{Span}_{\mathbb{R}} \Sigma$. Clearly, $\Psi \supseteq \Sigma$ and $\mathrm{Span}_{\mathbb{R}} \Sigma = \mathrm{Span}_{\mathbb{R}} \Psi$. Furthermore, the uniqueness of Ψ follows from the previous assertion. To show that Ψ is parabolic, let U denote the orthogonal complement of $\mathrm{Span}_{\mathbb{R}} \Psi$ in E with respect to $(\cdot, \cdot)$, and note that the Weyl group W_Ψ of Ψ coincides with the subgroup of elements of W which fix U pointwise. Then W_Ψ is a parabolic subgroup of W by [29, 1.12 Theorem], and hence there exists a basis S of Φ, and a subset $I \subseteq \Phi$ such that $W_\Psi = \langle s_\alpha : \alpha \in I \rangle$ and I is a base for Ψ.

□

Corollary 6.2.4. *Any closed subsystem $\Sigma \subseteq \Phi$ is either parabolic, or is isolated in a unique closed parabolic subsystem $\Psi \subseteq \Phi$.*

Remark 6.2.5 (Regarding terminology). The term parabolic subsystem is fairly common in the literature. It is closely related to the notion of a parabolic subgroup of $\mathbf{G}$, as any such subsystem gives rise to a parabolic subgroup $\mathbf{P}_\Psi$ of $\mathbf{G}$ of the form $\mathbf{P}_\Psi = \bigsqcup_{w \in W_\Psi} \mathbf{B}' w \mathbf{B}'$, where W_Ψ is the Weyl group of Ψ, as above, and $\mathbf{B}'$ is a Borel subgroup of $\mathbf{G}$, which determines an order on Φ such that all elements of the fixed base S are positive. In this case, the group $\mathbf{H}_\Psi$, generated by $\mathbf{T}$ and the root subgroups $\mathbf{U}_\alpha$, for $\alpha \in \Psi$, is a Levi factor of $\mathbf{P}_\Psi$.

Locally isolated subsystems are so named for their connection with the notion of isolated elements of $\mathbf{G}$ and of its Levi factors. Recall that an element of a connected reductive group is said to be isolated if its centralizer is not contained in any Levi subgroup of $\mathbf{G}$. It follows, for example, that the subsystem of roots vanishing on an isolated element of $\mathbf{G}$ is isolated in Φ (see [6]). The question of whether a given isolated subsystem $\Sigma \subseteq \Phi$ arises in this manner is addressed in § 8.0.1.

Finally, we note the following fact regarding parabolic subsystems.

Lemma 6.2.6. *Let $\Psi \subseteq \Phi$ be a closed parabolic subsystem, and let $\Psi^\vee = \{\alpha^\vee : \alpha \in \Phi\}$. Then $\Psi^\vee$ is a closed parabolic subsystem of the coroot system $\Phi^\vee$.*

Proof. Let S be a base of Φ and $I \subseteq \Phi$ a base of Ψ. Then, as noted at the beginning of Section 6.2, by definition of base, the set $S^\vee$ is a base for the root system $\Phi^\vee$ and $I^\vee = \{\alpha^\vee : \alpha \in I\} \subseteq \Psi^\vee$ is a base of $\Psi^\vee$, included in $S^\vee$. □

Note that Lemma 6.2.6 fails if Ψ is not assumed to be parabolic. For example, the root system of type C_2 (e.g., the root system of the symplectic group $\mathrm{Sp}_4(\boldsymbol{k})$) contains a closed isolated subsystem Σ of type $\mathsf{A}_1 \times \mathsf{A}_1$ (the subsystem consisting of long roots), such that $\Sigma^\vee$ is not closed.

6.2.3 The action of σ on X and Y

The assumption $\sigma(\mathbf{T}) = \mathbf{T}$ implies that σ permutes the character group of $\mathbf{T}$, as well as its cocharacter group. The normalizer of $\mathbf{T}$ is also σ-stable and hence $\sigma(W) = W$. The action of σ on X and Y is given by

$$(\sigma\chi)(t) = \chi(\sigma(t)) \qquad \text{for all } \chi \in X,\ t \in \mathbf{T};\ \text{and} \tag{6.6}$$

$$(\sigma\gamma)(\xi) = \sigma(\gamma(\xi)) \qquad \text{for all } \gamma \in Y \text{ and } \xi \in \mathbb{G}_m, \tag{6.7}$$

and satisfies

$$\langle \sigma\chi, \gamma \rangle = \langle \chi, \sigma\gamma \rangle \quad \text{for all } \chi \in X,\ \text{and } \gamma \in Y. \tag{6.8}$$

Example 6.2.7. 1. Let $\mathbf{G} = \mathrm{GL}_N(\boldsymbol{k})$, with $\sigma = F_q$, the Frobenius map over $\mathbb{F}_q$ and $\mathbf{T}$ the diagonal torus. For any $\chi \in X$ and $t \in \mathbf{T}$ we have that $(\sigma\chi)(t) = \chi(t^q) = (q \cdot \chi)(t)$, and hence σ acts on X as the $\mathbb{Z}$-module endomorphism $q\mathbf{1}_X$.

2. Again, take $\mathbf{G} = \mathrm{GL}_N(\boldsymbol{k})$ and $\mathbf{T}$ the diagonal torus, but now with $\sigma(a) = F_q(a^{-t})^{w_0}$, where $w_0 = \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix} \in \mathrm{GL}_N(\boldsymbol{k})$ and a^{-t} denotes the inverse of the transpose matrix of a. In this example we have that $\mathbf{G}^\sigma = \mathrm{U}_N(\mathbb{F}_q)$ is the unitary group in $\mathrm{GL}_N(\mathbb{F}_{q^2})$. Explicating the action of σ on X we have that, for $t = \mathrm{diag}(t_1, \ldots, t_N) \in \mathbf{T}$,

$$(\sigma\chi)(t) = \chi(\mathrm{diag}(t_N^{-q}, \ldots, t_1^{-q})) = q \cdot \phi_\sigma(\chi)(t),$$

where ϕ_σ is the automorphism of X defined by $\phi_\sigma(\chi)(t) = -\chi(\mathrm{diag}(t_N, \ldots, t_1))$. Note that, for $\chi = \alpha_{i,j} = (t \mapsto t_i/t_j) \in \Phi$ with $i < j$, it holds that $\phi_\sigma(\alpha_{i,j}) = (t \mapsto t_{N-j+1}/t_{N-i+1}) \in \Phi$.

The phenomena outlined in Example 6.2.7 are special cases of a general fact regarding the action of σ on X. Recall that, for any $\alpha \in \Phi$, there exists an embedding of algebraic groups $u_\alpha : \mathbb{G}_a \to \mathbf{G}$ with the property that $tu_\alpha(\xi)t^{-1} = u_\alpha(\alpha(t)\xi)$ for all $t \in \mathbf{T}$ and $\xi \in \mathbb{G}_a$ [41, Theorem 8.17]. Also recall that the choice of a Borel subgroup $\mathbf{B} \supseteq \mathbf{T}$ determines a set of positive roots in Φ, and hence a base S of Φ, by the condition $\alpha \in \Phi^+$ if and only if $\mathrm{Im}(u_\alpha) \subseteq \mathbf{B}$ [49, § 7.4]. The σ-stability of $\mathbf{B}$ implies that $\sigma(\Phi^+) = \Phi^+$. Also note that, writing $\mathbf{U}_\alpha = \mathrm{Im}(u_\alpha)$ for the root subgroup associated to $\alpha \in \Phi$, the action of $\mathbf{N_G}(\mathbf{T})$ on the set $\{\mathbf{U}_\alpha : \alpha \in \Phi\}$ reduces to a simply transitive action of W on these subgroups, such that ${}^w\mathbf{U}_\alpha = \mathrm{Ad}(n_w)\mathbf{U}_\alpha = \mathbf{U}_{w\alpha}$, where n_w is a coset representative of $w \in W$.

Proposition 6.2.8 ([41, Proposition 22.2])**.** *Let $\mathbf{G}$ be an $\mathbb{F}_q$-defined connected reductive algebraic group over $\boldsymbol{k}$ with Steinberg endomorphism σ, and let $\mathbf{T} \subseteq \mathbf{B}$ be a σ-stable torus inside a σ-stable Borel subgroup. The following hold.*

1. *There exists a permutation ρ_σ of the set $\Phi^+ = \{\alpha \in \Phi : \mathrm{Im}(u_\alpha) \subseteq \mathbf{B}\}$ and, for each $\alpha \in \Phi$, a positive integral power q_α of $p = \mathrm{char}(\boldsymbol{k})$ and $a_\alpha \in \mathbb{G}_m$, such that $\sigma(\rho_\sigma(\alpha)) = q_\alpha \cdot \alpha$ and $\sigma(u_\alpha(\xi)) = u_{\rho_\sigma(\alpha)}(a_\alpha \xi^{q_\alpha})$ for all $\xi \in \mathbb{G}_a$.*

2. *There exists $\delta \in \mathbb{N}$ and $r \in \frac{1}{\delta}\mathbb{Z}$ such that σ^δ acts as $p^{r\delta}\mathbf{1}_X$ on X and such that $\sigma = p^r \phi_\sigma$ on the real vector space $X \otimes_\mathbb{Z} \mathbb{R}$, for $\phi_\sigma \in \mathrm{Aut}(X \otimes_\mathbb{Z} \mathbb{R})$, an operator of order δ, satisfying $\phi_\sigma \mid_{\Phi^+} = \rho_\sigma^{-1}$.*

The fact that σ permutes the set of positive roots implies in particular that it is determined by a permutation of the unique base $S \subseteq \Phi$, and hence a *diagram automorphism* of its Coxeter diagram (see [44, Ch. 4, § 1.9]). Conversely, any pair of the form (p^r, ϕ), in which $r \in \mathbb{N}$ and ϕ is a Dynkin diagram automorphism gives rise to a uniquely determined, up to inner automorphism of $\mathbf{G}$, Steinberg endomorphism of $\mathbf{G}$ (see [55, § 11.6], also [41, Theorem 22.5])

We note that, under some mild assumptions on p and $\mathbf{G}$, the constants q_α and p^r of the proposition admit a much simpler description. That is, the following holds.

Lemma 6.2.9. *In the setting of Proposition 6.2.8, assume further that $p = \mathrm{char}(\boldsymbol{k}) > 3$ and that $\mathbf{G}$ is semisimple of simply connected type (see [41, Definition 9.14]).*

1. *For any $\alpha \in \Phi$ we have that $q_\alpha = q$, the cardinality of the field of definition of $\mathbf{G}$, and $a_\alpha = 1$.*

2. *The action of σ on $X \otimes_\mathbb{Z} \mathbb{R}$ is given by $q\phi_\sigma$, where $\phi_\sigma \in \mathrm{Aut}(X \otimes_\mathbb{Z} \mathbb{R})$ is as above.*

Proof. Let $\Phi = \Phi_1 \sqcup \cdots \sqcup \Phi_r$ be the decomposition of its root system with respect to $\mathbf{T}$ into simple subsystems. In the case where $\rho_\sigma(\Phi_i^+) \subseteq \Phi_i^+$ for all i the lemma reduces to the cases where $\mathbf{G}$ is simple with root system Φ_i, which is well-known; see [51, 1.5.(a)]. Otherwise, it holds that the permutation ρ_σ stabilizes the positive system determined by $\mathbf{B}$, hence also the base included in this system, and defines a graph automorphism of the respective Dynkin diagram. Therefore, by Chevalley's Existence Theorem [41, Theorem 11.12] there exists an algebraic automorphism $\tau : \mathbf{G} \to \mathbf{G}$, stabilizing $\mathbf{T}$ and $\mathbf{B}$, such that

$$\tau(u_\alpha(\xi)) = u_{\rho_\sigma(\alpha)}(\xi) \quad \text{for all } \alpha \in \Phi^+ \text{ and } \xi \in \mathbb{G}_a.$$

One easily verifies that the permutation associated to $\tau^{-1} \circ \sigma$ acts trivially on Φ^+, and hence, by the previous case, that $\tau^{-1} \circ \sigma$ acts as $q\mathbf{1}_X$ on X. Thus $\tau^{-1} \circ \sigma = F_q$, the Frobenius map on $\mathbf{G}$. It therefore holds that

$$u_\alpha(\xi^q) = \tau^{-1} \circ \sigma(u_\alpha(\xi)) = \tau^{-1}(u_{\rho_\sigma}(a_\alpha \xi^{q_\alpha})) = u_\alpha(a_\alpha \xi^{q_\alpha}),$$

whence the first assertion. The second assertion also follows, since $\sigma(\chi) = \tau(q\chi) = q\phi_\sigma(\chi)$, for $\chi \in \mathrm{Aut}(X)$. Here the final equality holds since $\phi_\tau \mid_{\Phi^+} = \rho_\sigma^{-1} = \phi_\sigma \mid_{\Phi^+}$, by the same proof as [41, Proposition 22.2], and since Φ^+ spans $X \otimes_\mathbb{Z} \mathbb{R}$. $\square$

Note that the map τ, described above, necessarily commutes with the Frobenius map. We have thus recovered a well-known fact, assuming $\mathrm{char}(\boldsymbol{k}) > 3$, any Steinberg endomorphism σ of $\mathbf{G}$ admits a decomposition of the form $\sigma = \tau \circ F_q = F_q \circ \tau$, with τ an algebraic automorphism stabilizing $\mathbf{T}$ and $\mathbf{B}$ (see also [32, § 1]).

6.2.4 The action of σ on $\mathfrak{G}$

It is now possible to present the definition of the action of σ on $\mathfrak{G}$, as given in [32], under the assumption $p > 3$. Applying the decomposition of the previous section, let $\tau : \mathbf{G} \to \mathbf{G}$ be the algebraic automorphism, stabilizing $\mathbf{T}$ and $\mathbf{B}$, such that $\sigma = F_q \circ \tau = \tau \circ F_q$. Recalling that $\mathbf{G}$ is $\mathbb{F}_q$-defined, the algebra $\mathbb{F}_q[\mathbf{G}] = \mathbb{F}_q[t_1, \ldots, t_{N^2}]/I$, where I is the ideal of definition of $\mathbf{G}$, is an $\mathbb{F}_q$-form of the coordinate algebra $\boldsymbol{k}[\mathbf{G}]$, on which the comorphism of F_q acts as the q-power map. One may therefore define an action of F_q on $\mathfrak{G} = T_1(\mathbf{G})$ by $(F_q\gamma)(\sum a_i f_i) = \sum a_i \gamma(f_i)^q$, for any $\gamma \in T_1(\mathbf{G})$, $f_1, \ldots, f_r \in \mathbb{F}_q[\mathbf{G}]$ and $a_1, \ldots, a_r \in \boldsymbol{k}$. In the case where $\mathbf{G} = \mathrm{GL}_N(\mathbb{F}_q)$, by identifying $\mathfrak{G} = \mathfrak{gl}_N(\mathbb{F}_q)$ with the algebra of $N \times N$ matrices over $\mathbb{F}_q$, this definition coincides with the ordinary Frobenius map $(a_{i,j}) \mapsto (a_{i,j}^q)$.

Being an algebraic automorphism, the map τ has a non-zero differential. One may therefore defined the action of σ on $\mathfrak{G}$ via the composition $d\tau \circ F$. The following holds.

Proposition 6.2.10. *Let* $\mathrm{Ad} : \mathbf{G} \to \mathrm{Aut}(\mathfrak{G})$ *be the adjoint map. For any* $g \in \mathbf{G}$ *and* $x \in \mathfrak{G}$*, it holds that* $\sigma(\mathrm{Ad}(g)x) = \mathrm{Ad}(\sigma(g))\sigma(x)$*. In particular, the map* Ad *restricts to an* $\mathbb{F}_q$*-defined action of* G *on* $\mathfrak{g}$.

Proof. See [32, 1.1]. □

Remark 6.2.11. We chose not to make any notational distinction between the action of σ on $\mathbf{G}$ and on $\mathfrak{G}$, attempting to avoid over-cluttering. However, one should be cautious and recall that these might be given by different maps when visualizing $\mathbf{G}$ and $\mathfrak{G}$ as subsets of the matrix algebra $\mathrm{M}_N(\boldsymbol{k})$, as occurs, for example, in the case where $\mathbf{G} = \mathrm{GL}_N(\boldsymbol{k})$ with the twisted Steinberg endomorphism defined in Example 6.2.7.

6.3 Classification of σ-stable tori in G

Recall the notation $G = \mathbf{G}^\sigma$ and $\mathfrak{g} = \mathfrak{G}^\sigma$, where the Lie-algebra of σ-fixed point is as defined in § 6.2.4. Let W be the Weyl group of $\mathbf{G}$ with respect to the fixed maximally split torus $\mathbf{T} \subseteq \mathbf{B}$. We recall an important consequence of Lemma 6.1.4.

Lemma 6.3.1. *There exist bijective maps*

$$\left\{ \begin{matrix} \mathrm{Ad}(G)\text{-classes of } \sigma\text{-stable} \\ \text{maximal tori in } \mathbf{G} \end{matrix} \right\} \xleftrightarrow{1-1} H^1(\sigma, W)$$

and

$$\left\{ \begin{matrix} \mathrm{Ad}(G)\text{-classes of } \sigma\text{-stable} \\ \text{maximal tori in } \mathfrak{G} \end{matrix} \right\} \overset{1-1}{\longleftrightarrow} H^1(\sigma, W).$$

Proof. The existence of the first bijection is proved, e.g., in [41, Proposition 25.1]. The second bijection can be shown to exist in a similar vein, by considering the action of $\mathbf{G}$ on the set of maximal tori in $\mathfrak{G}$, noting that the Lie-algebra of $\mathbf{T}$ is a σ-stable point under this action with stabilizer $\mathbf{N_G}(\mathbf{t}) = \mathbf{N_G}(\mathbf{T})$ (see also [32, Theorem 3.1]). □

Remark 6.3.2. The assumption that $\mathbf{T}$ is maximally split is actually superfluous for the proof of Lemma 6.3.1. It is, however, convenient for our purposes to consider the $\mathrm{Ad}(G)$-class of the maximally split torus as a "point of reference", and describe all other classes of maximal tori in $\mathbf{G}$ with respect to it.

Let us write down the bijections of Lemma 6.3.1 explicitly. The notation set up in this paragraph are in force throughout the remainder of the essay, and are summarized in Table 6.1 below. Given a class $\kappa \in H^1(\sigma, W)$, let $w_\kappa \in \kappa$ be a representative, and $n_{w_\kappa} \in \mathbf{N_G}(\mathbf{T})$ a coset representative of w_κ. Invoking the connectedness of $\mathbf{G}$ and the Lang-Steinberg Theorem (Theorem 6.1.1), let g_κ be such that $\mathsf{L}(g_\kappa) = g_\kappa \sigma(g_\kappa)^{-1} = n_{w_\kappa}$. The $\mathrm{Ad}(G)$-class of maximal tori in $\mathbf{G}$ (resp. in $\mathfrak{G}$) associated to κ is that of $\mathbf{T}_\kappa = \mathrm{Ad}(g_\kappa)\mathbf{T}$ (resp. $\mathbf{t}_\kappa = \mathrm{Ad}(g_\kappa)\mathbf{t}$). One verifies by direct computation that these tori are σ-stable, and that their $\mathrm{Ad}(G)$-classes are independent of the choices made above.

Symbol	Meaning
w_κ	Representative of $\kappa \in H^1(\sigma, W)$
n_w	Coset representative of $w \in W$
g_κ	Fixed preimage of n_{w_κ} in $\mathbf{G}$ under L
$\mathbf{T}_\kappa$	The maximal torus $\mathrm{Ad}(g_\kappa)\mathbf{T} \subseteq \mathbf{G}$
$\mathbf{t}_\kappa$	The maximal torus $\mathrm{Ad}(g_\kappa)\mathbf{t} \subseteq \mathfrak{G}$

Table 6.1: σ-stable tori in $\mathbf{G}$ and $\mathfrak{G}$

The map $\mathrm{Ad}(g_\kappa)$ establishes an isomorphism $\mathbf{T} \to \mathbf{T}_\kappa$, such that the diagram

$$\begin{tikzcd} \mathbf{T} \arrow[r, "\mathrm{Ad}(g_\kappa)"] \arrow[d, "{}^{w_\kappa}\sigma"'] & \mathbf{T}_\kappa \arrow[d, "\sigma"] \\ \mathbf{T} \arrow[r, "\mathrm{Ad}(g_\kappa)"'] & \mathbf{T}_\kappa \end{tikzcd} \tag{6.9}$$

commutes. It follows that the group $\mathbf{T}_\kappa^\sigma$ of σ-fixed points of $\mathbf{T}_\kappa$ is isomorphic, as an abstract group, to the group of elements of $\mathbf{T}$ which are fixed by ${}^{w_\kappa}\sigma$.

Lemma 6.3.3. *1. Let $g \in \mathbf{T}$ and $\kappa \in H^1(\sigma, W)$. The maximal torus $\mathbf{T}_\kappa$ contains a σ-fixed $\mathrm{Ad}(\mathbf{G})$-conjugate of g if and only if there exists $w \in \kappa$ such that ${}^w\sigma(g) = g$.*

2. *Let $x \in \mathfrak{t}$ and $\kappa \in H^1(\sigma, W)$. The maximal torus $\mathfrak{t}_\kappa$ contains a σ-fixed $\mathrm{Ad}(\mathbf{G})$-conjugate of x if and only if there exists $w \in \kappa$ such that ${}^w\sigma(x) = x$.*

Proof. We prove only the first assertion; the proof of the second assertion is completely analogous. For the *if* implication, let $w \in \kappa$ be such that ${}^w(\sigma(g)) = g$, and let $h \in \mathbf{G}$ be such that $\mathsf{L}(h) = n_w$. Then $\sigma(h^{-1}gh) = h^w\sigma(g)h^{-1} = hgh^{-1}$. Additionally, since w and w_κ are both element of κ, it follows that $\mathrm{Ad}(h)\mathbf{T}$ is $\mathrm{Ad}(G)$-conjugate to $\mathbf{T}_\kappa$, and hence $\mathbf{T}_\kappa$ contains an $\mathrm{Ad}(G)$-conjugate of hgh^{-1}, which is a σ-stable $\mathrm{Ad}(\mathbf{G})$-conjugate of g.

To prove the implication *only if*, assume $h \in \mathbf{G}$ is such that $hgh^{-1} \in \mathbf{T}_\kappa$ is σ-fixed. Then $\mathrm{Ad}(h^{-1})\mathbf{T}_\kappa$ and $\mathbf{T}$ are two maximal tori containing g, whence maximal tori in $\mathbf{C}_{\mathbf{G}}(g)^\circ$. Consequently, there exists $c \in \mathbf{C}_{\mathbf{G}}(g)^\circ$ such that $\mathrm{Ad}(c)\mathbf{T} = \mathrm{Ad}(h^{-1})\mathbf{T}_\kappa$. Since both $\mathbf{T}$ and $\mathbf{T}_\kappa$ are σ-stable, it follows that $\mathsf{L}((hc)^{-1}) =\in \mathbf{N}_{\mathbf{G}}(\mathbf{T})$. Put $w = \mathsf{L}((hc)^{-1})\mathbf{T} \in W$. Then

$$
{}^w(\sigma(g)) = (hc)^{-1}\sigma(hcgc^{-1}h^{-1})hc = c^{-1}h\sigma(hgh^{-1})hc = g.
$$

Moreover, since $\mathrm{Ad}(hc)\mathbf{T} = \mathbf{T}_\kappa = \mathrm{Ad}(g_\kappa)\mathbf{T}$, by Lemma 6.3.1, it follows that $w \in \kappa$. □

6.4 The set $\mathcal{I}_{\Phi,\phi_\sigma}$

The following definition is central in our analysis of semisimple classes in $\mathbf{G}$ and $\mathfrak{G}$.

Definition 6.4.1. Let $\mathcal{I}_{\Phi,\phi_\sigma}$ denote the set of pairs $\boldsymbol{i} = (\kappa, \Sigma)$, where $\kappa \in H^1(\sigma, W)$ and $\Sigma \subseteq \Phi$ is either empty or a closed root subsystem which is stable under the action $w_\kappa \circ \phi_\sigma^{-1}$, where $\phi_\sigma \in \mathrm{Aut}(X \otimes_{\mathbb{Z}} \mathbb{R})$ is the operator defined in Proposition 6.2.8.(2), and w_κ is as in Table 6.1.

Remark 6.4.2. Note that, since ϕ_σ preserves a set of generators of W (viz. the reflections along roots of $\mathbf{G}$ with respect to $\mathbf{T}$), it follows that the group $W \cdot \langle \phi_\sigma \rangle \subseteq \mathrm{Aut}(X)$, generated by W and ϕ_σ is the semidirect product of two finite groups, and hence finite. In particular, the assumption that Σ is fixed by $\phi_\sigma \circ w_\kappa$ in Definition 6.4.1 implies that Σ is fixed by $(w_\kappa \circ \phi_\sigma)^j$, for all $j \in \mathbb{Z}$.

Note that the set $\mathcal{I}_{\Phi,\phi_\sigma}$ is *completely determined* by the root datum of $\mathbf{G}$ and the action of σ on X, and is independent of the field of definition.

Example 6.4.3. The tables in Figure 6.1 list the elements of $\mathcal{I}_{\Phi,\phi_\sigma}$ for Φ the root system of the group $\mathbf{G} = \mathrm{GL}_3(\boldsymbol{k})$ with respect to the automorphism ϕ_σ defined by the Frobenius map $\sigma = F_q$ (i.e. $\phi_\sigma = \mathbf{1}_X$) and by the Steinberg endomorphism $\sigma(a) = F_q(a^{-t})^{w_0}$ (see Example 6.2.7). The maximally split maximal torus $\mathbf{T}$ in these examples is the diagonal torus, and the root system of $\mathbf{G}$ with respect to $\mathbf{T}$ is

$$
\Phi = \{\alpha_{i,j} = (\mathrm{diag}(t_1, t_2, t_3) \mapsto t_i/t_j) : 1 \leq i \neq j \leq 3\}.
$$

The Weyl group W is identified with the symmetric group $\mathfrak{S}_3$ on 3 elements, and its action on Φ is given by $\tau(\alpha_{i,j}) = \alpha_{\tau(i),\tau(j)}$. The leftmost column of each of the tables lists the equivalence classes in $H^1(\sigma, W)$. The middle column contains a fixed representative in W for each equivalence class κ, and the rightmost the possible closed subsystems.

κ	w_κ	Σ
$\{\mathbf{1}\}$	$\mathbf{1}$	All Σ's
$\left\{\begin{matrix}(12),(13),\\(23)\end{matrix}\right\}$	(12)	$\varnothing, \Phi, \{\pm\alpha_{1,2}\}$
$\{(123),(132)\}$	(123)	$\varnothing, \Phi$

κ	w_κ	Σ
$\left\{\begin{matrix}\mathbf{1},(123),\\(132)\end{matrix}\right\}$	$\mathbf{1}$	$\varnothing, \Phi, \{\pm\alpha_{1,3}\}$
$\{(12),(23)\}$	(12)	$\varnothing, \Phi, \{\pm\alpha_{1,2}\}$
$\{(13)\}$	(13)	All Σ's

Figure 6.1: The set $\mathcal{I}_{\mathrm{GL}_3(\boldsymbol{k}),\sigma}$ for $\sigma = F_q$ (left) and for $\sigma(a) = F_q(a^{-t})^{w_0}$ (right)

6.4.1 The groups $\mathbf{H}(\boldsymbol{i})$

Fix a pair $\boldsymbol{i} = (\kappa, \Sigma) \in \mathcal{I}_{\Phi,\phi_\sigma}$, and, for any $\alpha \in \Sigma$, let $\mathbf{U}_\alpha = \mathrm{Im}(u_\alpha)$ be the corresponding root subgroup with $\mathbf{u}_\alpha = \mathrm{Lie}(\mathbf{U}_\alpha)$. Also, put $\mathbf{U}_{\kappa,\alpha} = \mathrm{Ad}(g_\kappa)\mathbf{U}_\alpha$ and $\mathbf{u}_{\kappa,\alpha} = \mathrm{Ad}(g_\kappa)\mathbf{u}_\alpha = \mathrm{Lie}(\mathbf{U}_{\kappa,\alpha})$. Note that, by construction, the maps $\alpha \circ \mathrm{Ad}(g_\kappa^{-1}) \in X(\mathbf{T}_\kappa)$ are the roots of $\mathbf{T}_\kappa$, and the subgroup $\mathbf{U}_{\kappa,\alpha} = \mathrm{Im}(u_{\alpha\circ\mathrm{Ad}(g_\kappa^{-1})})$ are the corresponding root subgroups. Also note that, by the defining condition of $\boldsymbol{i}$ and Proposition 6.2.8, it holds that

$$\sigma(\mathbf{U}_{\kappa,\alpha}) = \mathrm{Ad}(g_\kappa)\mathrm{Ad}(n_{w_\kappa})\sigma\left(\mathbf{U}_\alpha\right) = \mathrm{Ad}(g_\kappa)\mathbf{U}_{w_\kappa\circ\phi_\sigma^{-1}(\alpha)} = \mathbf{U}_{\kappa,\alpha'}, \tag{6.10}$$

for $\alpha' = w_\kappa \circ \phi_\sigma^{-1}(\alpha) \in \Sigma$.

Definition 6.4.4. Given $\boldsymbol{i} = (\kappa, \Sigma) \in \mathcal{I}_{\Phi,\phi_\sigma}$, let $\mathbf{H}(\boldsymbol{i}) \subseteq \mathbf{G}$ be the algebraic subgroup generated by $\mathbf{T}_\kappa$ and the subgroups $\mathbf{U}_{\kappa,\alpha}$, for all $\alpha \in \Sigma$, and put $\mathbf{h}(\boldsymbol{i}) = \mathbf{t}_\kappa \oplus \bigoplus_{\alpha\in\Sigma} \mathbf{u}_{\kappa,\alpha}$.

The following holds.

Proposition 6.4.5. *Let $\boldsymbol{i} \in \mathcal{I}_{\Phi,\phi_\sigma}$. The group $\mathbf{H}(\boldsymbol{i})$ is connected reductive and σ-stable of maximal rank, with root system $\Sigma_\kappa = \{\alpha \circ \mathrm{Ad}(g_\kappa^{-1}) : \alpha \in \Sigma\}$ with respect to the maximal torus $\mathbf{T}_\kappa$ and Weyl group generated by the reflections $s_{\alpha\circ\mathrm{Ad}(g_\kappa^{-1})}$ for $\alpha \in \Sigma$. Furthermore, $\mathbf{h}(\boldsymbol{i}) = \mathrm{Lie}(\mathbf{H}(\boldsymbol{i}))$, and the decomposition $\mathbf{h}(\boldsymbol{i}) = \mathbf{t}_\kappa \oplus \bigoplus_{\alpha\in\Sigma} \mathbf{u}_{\kappa,\alpha}$ is the root spaces decomposition of $\mathbf{h}(\boldsymbol{i})$ with respect to $\mathbf{t}_\kappa$.*

Proof. The fact that $\mathbf{H}(\boldsymbol{i})$ is σ-stable follows from the σ-stability of $\mathbf{T}_\kappa$ and from (6.10). All other properties of $\mathbf{H}(\boldsymbol{i})$ follow from [41, Theorem 13.6], noting that the assumption that Σ is closed implies its p-closedness (cf. [41, Definition 13.2])

The fact that $\mathbf{u}_{\kappa,\alpha}$ are the root-subalgebras of $\mathbf{H}(\boldsymbol{i})$ is immediate from their definition, and

$$\mathrm{Lie}(\mathbf{H}(\boldsymbol{i})) = \mathrm{Lie}(\mathbf{T}_\kappa) \oplus \bigoplus_{\alpha\in\Sigma} \mathbf{u}_{\kappa,\alpha} = \mathbf{h}(\boldsymbol{i})$$

is proved in [41, Theorem 8.17]. $\square$

6.5 Dual algebraic groups

Retaining the notation introduced thus far, let $\mathbf{G}^*$ be another connected reductive algebraic group with maximal torus $\mathbf{T}^*$ and root datum $(X^*, \Phi^*, Y^*, (\Phi^*)^\vee)$. The group $\mathbf{G}^*$ is said to be *dual* to $\mathbf{G}$ if there exist isomorphisms of abelian groups $X \xrightarrow{\sim} Y^*$ and $Y \xrightarrow{\sim} X^*$, mapping roots to coroots and vice versa, and preserving the natural pairing and the operation $\alpha \mapsto \alpha^\vee$ (see [13, § 4.2]). Equivalently, $\mathbf{G}$ and $\mathbf{G}^*$ are in duality if there exists an isomorphism $f : X \xrightarrow{\sim} Y^*$, such that $f(\Phi) = (\Phi^*)^\vee$ and such that

$$\langle \chi, \alpha^\vee \rangle = \langle \alpha^*, f(\chi) \rangle \quad \text{for all } \chi \in X \text{ and } \alpha \in \Phi, \tag{6.11}$$

where $\alpha^* \in \Phi^*$ is the unique root of $\mathbf{G}^*$ such that $(\alpha^*)^\vee = f(\alpha)$ [13, Proposition 4.2.2]. Keeping this notation, given a subset $\Sigma \subseteq \Phi$ we write

$$\Sigma^* = \{\alpha^* \in \Phi^* : \alpha \in \Sigma\}.$$

The following lemma follows directly from Lemma 6.2.6 and from definition; its proof is omitted.

Lemma 6.5.1. *Let Σ be a parabolic subsystem of Φ. Then Σ^* is a parabolic subsystem of Φ^*.*

Also note that the existence of $f : X \to Y^*$, and the duality of X^* and Y^* imply that any endomorphism $\vartheta \in \mathrm{End}(X)$ gives rise to a *unique* endomorphism $\vartheta^* \in \mathrm{End}(X^*)$, such that the equation

$$\langle \eta, f(\vartheta\chi) \rangle = \langle \vartheta^*\eta, f(\chi) \rangle \tag{6.12}$$

holds for any $\chi \in X$ and $\eta \in X^*$.

6.5.1 Dual Steinberg endomorphisms

Let σ^* be a Steinberg endomorphism of $\mathbf{G}^*$, and assume that the maximal torus $\mathbf{T}^*$ is σ^*-stable. For the purposes of this section we assume that $\mathbf{T} \subseteq \mathbf{G}$ is σ-stable, but not necessarily maximally split. In this situation, we say that the pairs $(\mathbf{G}, \sigma)$ and $(\mathbf{G}, \sigma^*)$ are dual if the isomorphism $f : X \to Y^*$ intertwines the respective actions of σ and σ^*, i.e. $f(\sigma\chi) = \sigma^*(f(\chi))$, for any $\chi \in X$.

6.5.2 The dual Weyl group

Considering the Weyl group $W = W_{\mathbf{G}}(\mathbf{T})$ as a subgroup of $\mathrm{Aut}(X)$, the duality map of (6.12) restricts to an anti-isomorphism of W onto the Weyl group $W^* = W_{\mathbf{G}^*}(\mathbf{T}^*)$ of $\mathbf{G}^*$ with respect to $\mathbf{T}^*$, such that $(s_\alpha)^* = s_{\alpha^*}$. Combined with (6.8) and the fact that f intertwines the actions of σ and σ^*, one readily deduces the equality

$$(\sigma(w))^* = (\sigma^*)^{-1}(w^*) \quad \text{for all } w \in W. \tag{6.13}$$

Also, we have the following.

Lemma 6.5.2 (cf. [13, Proposition 4.3.4])**.** *The anti-isomorphism $w \mapsto w^* : W \to W^*$ gives rise to a bijection*

$$(\kappa \mapsto \kappa^*) : H^1(\sigma, W) \xrightarrow{1-1} H^1(\sigma^*, W^*).$$

Proof. Let $w_1, w_2 \in W$. Then w_1, w_2 lie in the same equivalence class $\kappa \in H^1(\sigma, W)$ if and only there exists $z \in W$ such that $w_1 = zw_2\sigma(z)^{-1}$. Applying the map $*$ to this equality, and letting $y = (\sigma(z)^{-1})^* = (\sigma^*)^{-1}(z^*))^{-1}$, it follows that $w_1^* = yw_2^*\sigma^*(y)^{-1}$, and hence w_1^*, w_2^* lie in the same class in $H^1(\sigma^*, W^*)$. The converse implication follows symmetrically. □

In particular, Lemmas 6.3.1 and 6.5.2 imply that the set of $\mathrm{Ad}(G)$-classes of σ-stable tori in $\mathbf{G}$ is in bijection with the set of $\mathrm{Ad}((\mathbf{G}^*)^{\sigma^*})$-conjugacy classes of σ^*-stable tori in $\mathbf{G}^*$.

6.5.3 Duality for a subset of $\mathcal{I}_{\Phi,\phi_\sigma}$

Let $\mathcal{I} = \mathcal{I}_{\Phi,\phi_\sigma}$ and let $\mathcal{I}^P$ denote the subset of pairs $\boldsymbol{i} = (\kappa, \Psi)$ in which Ψ is a *parabolic* subsystem of Φ. Let $\mathcal{I}^* = \mathcal{I}_{\Phi^*,\phi_{\sigma^*}}$, and define $(\mathcal{I}^*)^P$ analogously. The definition of the map $\alpha \mapsto \alpha^*$ (6.11), the defining equation (6.12) and the assumption that f intertwines the actions of σ and σ^* on X and Y^* imply that

$$\left(w \circ \phi_\sigma^{-1}(\alpha)\right)^* = \left(w^* \circ \phi_{\sigma^*}^{-1}\right)^{-1}(\alpha^*) \quad \text{for all } w \in W \text{ and } \alpha \in \Phi.$$

It follows from this that a closed subsystem $\Sigma \subseteq \Phi$ is stable under the automorphism $w_\kappa \circ \phi_\sigma^{-1}$, for $\kappa \in H^1(\sigma, W)$ if and only if the subset $\Sigma^* = \{\alpha^* : \alpha \in \Sigma\}$ is stable under the map $w_{\kappa^*} \circ \phi_{\sigma^*}^{-1}$, where $w_{\kappa^*} \in W$ is any representative of the equivalence class $\kappa^* \in H^1(\sigma^*, W^*)$, defined in Lemma 6.5.2.

Under the additional assumption that Σ is parabolic, we have that Σ^* is a parabolic subsystem of Φ^*. Thus, Lemmas 6.5.1 and 6.5.2 imply the existence of a bijection

$$* : \mathcal{I}^P \to (\mathcal{I}^*)^P,$$

mapping the pair $\boldsymbol{i} = (\kappa, \Sigma)$ to $\boldsymbol{i}^* = (\kappa^*, \Sigma^*)$.

Given $\kappa^* \in H^1(\sigma^*, W^*)$, let $w_{\kappa^*} \in W^*$, $n_{w_{\kappa^*}} \in \mathbf{N}_{\mathbf{G}^*}(\mathbf{T}^*)$, $g_{\kappa^*} \in \mathbf{G}^*$ and $\mathbf{T}^*_{\kappa^*} = \mathrm{Ad}(g_{\kappa^*})\mathbf{T}^*$ be defined in analogy to the notation of Table 6.1. Given $\alpha^* \in \Phi^*$, we write $\mathbf{U}^*_{\alpha^*} \subseteq \mathbf{G}^*$ for the root subgroup corresponding to α^* and $\mathbf{U}_{\kappa^*,\alpha^*} = \mathrm{Ad}(g_{\kappa^*})\mathbf{U}_{\alpha^*}$.

Lemma 6.5.3. *Let $\boldsymbol{i} \in \mathcal{I}^P$ and let $\mathbf{H}(\boldsymbol{i}) \subseteq \mathbf{G}$ be the group defined in § 6.4.1, and let $\mathbf{H}^*(\boldsymbol{i}^*)$ be the subgroup of $\mathbf{G}^*$ generated by $\mathbf{T}^*_{\kappa^*}$ and the root subgroups $\mathbf{U}^*_{\kappa^*,\alpha^*}$. The pairs $(\mathbf{H}(\boldsymbol{i}), \sigma)$ and $(\mathbf{H}^*(\boldsymbol{i}^*), \sigma^*)$ are dual.*

Proof. Recall that $f : X = X(\mathbf{T}) \to Y^* = Y(\mathbf{T}^*)$ denotes the duality map for the pairs $(\mathbf{G}, \sigma)$ and $(\mathbf{G}^*, \Sigma^*)$, and define a map

$$f_\kappa = (\chi \mapsto \mathrm{Ad}(g_{\kappa^*}) \circ f(\chi \circ \mathrm{Ad}(g_\kappa))) : X(\mathbf{T}_\kappa) \to Y(\mathbf{T}^*_{\kappa^*}).$$

Clearly, f_κ is an isomorphism of abelian group. Also, recall from Proposition 6.4.5 that the root system Σ_κ of $\mathbf{H}(\boldsymbol{i})$ (resp. $\Sigma^*_{\kappa^*}$ of $\mathbf{H}^*(\boldsymbol{i}^*)$) consists of the characters $\alpha \circ \mathrm{Ad}(g_\kappa^{-1})$ for $\alpha \in \Sigma$ (resp. $\alpha^* \circ \mathrm{Ad}(g_{\kappa^*}^{-1})$ for $\alpha^* \in \Sigma^*$). Note that, by definition of f_κ and f, we have that

$$f_\kappa(\alpha \circ \mathrm{Ad}(g_\kappa^{-1})) = \mathrm{Ad}(g_{\kappa^*}) \circ f(\alpha) = \mathrm{Ad}(g_{\kappa^*}) \circ (\alpha^*)^\vee, \quad \text{for all } \alpha \in \Sigma.$$

Furthermore, by definition of the natural pairing $\langle \cdot, \cdot \rangle$ (both for $\mathbf{T}$ and for $\mathbf{T}_\kappa$), we have that

$$\langle \alpha^* \circ \mathrm{Ad}(g_{\kappa^*}^{-1}), \mathrm{Ad}(g_{\kappa^*}) \circ (\alpha^*)^\vee \rangle = \langle \alpha^*, (\alpha^*)^\vee \rangle = 2,$$

and hence, by uniqueness, we have that $f_\kappa\left(\alpha \circ \mathrm{Ad}(g_\kappa^*)\right) = \left(\alpha^* \circ \mathrm{Ad}(g_{\kappa^*}^{-1})\right)^\vee$ for any $\alpha \in \Sigma$, and thus $f_\kappa(\Sigma_\kappa) = (\Sigma^*_{\kappa^*})^\vee$. Finally, by direct computation, noting that any $\chi \in X(\mathbf{T}_\kappa)$ may be written uniquely as $\chi' \circ \mathrm{Ad}(g_\kappa^{-1})$ for $\chi' = \chi \circ \mathrm{Ad}(g_\kappa) \in X(\mathbf{T})$, one verifies that equation (6.11) is held by f_κ for all $\chi \in X(\mathbf{T}_\kappa)$ and $\alpha' = \alpha \circ \mathrm{Ad}(g_\kappa^{-1}) \in \Sigma_\kappa$. The duality of $\mathbf{H}(\boldsymbol{i})$ and $\mathbf{H}^*(\boldsymbol{i}^*)$ follows, by [13, Proposition 4.2.2]. Finally, we note that $\mathbf{T}_\kappa$ and $\mathbf{T}^*_{\kappa^*}$ are σ- and σ^*-stable, and that the map f_κ intertwines the action of σ and σ^* on their respective character and cocharacter groups. This is proved directly from the definition of f_κ, using the commutative diagram (6.9). □

6.6 Deligne-Lusztig theory

In this section we recall, without proofs, the basic definitions of Delinge and Lusztig's construction of irreducible characters of G. For more information, we refer to [13, 19, 39].

Let $\mathbf{T} \subseteq \mathbf{G}$ be a σ-stable, but not necessarily maximally split, maximal torus of $\mathbf{G}$. Let $\mathbf{B}$ a Borel subgroup containing $\mathbf{T}$, and let $\mathbf{U} = R_u(\mathbf{B})$ be the unipotent radical of $\mathbf{B}$. Thus $\mathbf{B} = \mathbf{TU}$. One defines an algebraic subset of $\mathbf{G}$ by $\boldsymbol{X} = \mathsf{L}^{-1}(\mathbf{U})$, where $\mathsf{L}(g) = g\sigma(g)^{-1}$ is the Lang map, defined in Theorem 6.1.1. The set $\boldsymbol{X}$ is in fact an affine algebraic variety over $\mathbb{F}_q$, and there is an action of the direct product $G \times T$ on $\boldsymbol{X}$ where $G = \mathbf{G}^\sigma$ acts by left multiplication, and $T = \mathbf{T}^\sigma$ acts by right multiplication. Note that the action of T on $\boldsymbol{X}$ is well-defined, since T normalizes $\mathbf{U}$.

The action of $G \times T$ on $\boldsymbol{X}$ gives rise to a structure of (G, T)-bimodule on the l-adic cohomology groups with compact support $H^i_c(\boldsymbol{X}, \overline{\mathbb{Q}_l})$ of $\boldsymbol{X}$, for $i \in \mathbb{N}_0$. Here $\overline{\mathbb{Q}_l}$ is the algebraic closure of the field of l-adic numbers, where $l \neq p$ is a prime number. For the definition of $H^i_c(\boldsymbol{X}, \overline{\mathbb{Q}_l})$, we refer to [13, Appendix]. We note that $H^i_c(\boldsymbol{X}, \overline{\mathbb{Q}_l})$ are vector spaces over $\overline{\mathbb{Q}_l}$, and are zero for all $i > 2\dim \boldsymbol{X}$. The actions of G and T on $H^i_c(\boldsymbol{X}, \overline{\mathbb{Q}_l})$ commute, i.e.

$$(gv)t = g(vt) \quad \text{for all } g \in G, t \in T, \text{ and } v \in H^i_c(\boldsymbol{X}, \overline{\mathbb{Q}_l}).$$

The Deligne-Lusztig *generalized characters* of G may now be defined as follows. Let $\theta \in \mathrm{Irr}(T)$ be an irreducible complex character. Being the character of a finite group, the image of θ is included in the field of algebraic numbers, and hence θ may be considered as a homomorphism $\theta : T \to \overline{\mathbb{Q}_l}$.

For any i, let $H^i_c(\boldsymbol{X}, \overline{\mathbb{Q}_l})_\theta$ be the maximal subspace on which T acts by the character θ. This space is a left G-module. The generalized character $R_{T,\theta} : G \to \overline{\mathbb{Q}_l}$ is defined by

$$R_{T,\theta}(g) = \sum_{i\geq 0})(-1)^i \mathrm{Tr}(g, H^i_c(\boldsymbol{X}, \overline{\mathbb{Q}_l})_\theta). \tag{6.14}$$

The map $R_{T,\theta}$ is an integral combinations of characters of G with values in the field of algebraic numbers. Thus we may consider $R_{T,\theta}$ as a complex valued class function on G.

The definition of $R_{T,\theta}$ is independent of the choice of Borel subgroup containing $\mathbf{T}$ [13, Proposition 7.3.6]. In the case where $\mathbf{T}$ is maximally split, the generalized character $R_{T,\theta}$ coincides with the Harish-Chandra induction of θ to G, with respect to a σ-stable Borel subgroup containing $\mathbf{T}$ [13, Proposition 7.2.4]. Given T, θ as above, write $\mathcal{E}(G, (T, \theta))$ for the set of irreducible constituents of $R_{T,\theta}$. Given another pair (T', θ'), where $T' = (\mathbf{T}')^\sigma$ for another σ-stable maximal torus $\mathbf{T}'$ of $\mathbf{G}$, and $\theta \in \mathrm{Irr}(T')$, it holds that $\mathcal{E}(G, (T, \theta)) \cap \mathcal{E}(G, (T', \theta')) = \varnothing$ unless (T, θ) and (T', θ') are *geometrically conjugate,* i.e. they satisfy the conditions of [13, Proposition 4.1.3]. See [13, Theorem 7.3.8] as well as [19, Corollary 11.15] and the ensuing discussion. The set of geometric conjugacy classes of G is in bijection with the set of $(\mathbf{G}^*)^{\sigma^*}$-conjugacy classes of semisimple elements in the σ^*-fixed subgroup of the dual algebraic group $\mathbf{G}^*$ of $\mathbf{G}$ [19, Proposition 13.13].

The set $\mathcal{E}(G, (s)) = \bigcup \mathcal{E}(G, (\mathbf{T}, \theta))$, where the union rangess over all elements in the geometric conjugacy class corresponding to $(s) \subseteq \mathrm{Ad}(G^*)\backslash G^*_{\mathrm{ss}}$, is the *Lusztig series* associated to (s). Then

$$\mathrm{Irr}(G) = \bigsqcup_{(s)\in \mathrm{Ad}(G^*)\backslash G^*_{\mathrm{ss}}} \mathcal{E}(G, (s));$$

see [19, Proposition 13.17].

The elements of the series $\mathcal{E}(G, (1))$ are the *unipotent characters* of G, i.e. characters which arise as constituents of $R_{T,\mathbf{1}}$, where $T = \mathbf{T}^\sigma$ for *some* σ-stable maximal torus of $\mathbf{G}$. By [19, Theorem 13.23], for any $\mathrm{Ad}(G^*)$-conjugacy class (s), there exists a bijection between the Lusztig series $\mathcal{E}(G, (s))$ and $\mathcal{E}(\mathbf{C}_{G^*}(s), (1))$, the Lusztig series of unipotent characters of the centralizer of any representative $s \in (s)$ in G^*. Furthermore, the ratio between the dimension of a character in $\mathcal{E}(G, (s))$ and that of its target unipotent character is given by an explicit formula in s; see [19, Remark 13.24]. Unipotent characters are further discussed in § 8.0.2.

6.7 Properties of the sets $\mathbb{Q}_c[t]$

In this section we collect some necessary lemmas regarding the sets $\mathbb{Q}_c[t]$ ($c \in \mathbb{N}$), which will be used in order to find uniform bounds on the coefficients of polynomials arising in our analysis. Recall that $\mathbb{Q}_c[t]$ consists of polynomials with coefficients in $\frac{1}{c}\mathbb{Z} \cap [-c, c]$.

Lemma 6.7.1. *Let $c \in \mathbb{N}$ and $\varphi, \psi \in \mathbb{Q}_c[t]$.*

1. *The coefficient of t^j ($j \in \mathbb{N}_0$) in $\varphi \cdot \psi$ lies in the set $\frac{1}{(j+1)c^2}\mathbb{Z} \cap [-(j+1)c^2, (j+1)c^2]$.*
2. *Assume $|\varphi(0)| = 1$ and that $\tau = \psi/\varphi \in \mathbb{Q}[t]$. For any $j \in \mathbb{N}_0$ put $a_j = 2^{j+1} + 2^j - 1$. The coefficient of t^j in τ lies in the set $\frac{1}{a_j c}\mathbb{Z} \cap [-a_j c, a_j c]$.*

Proof. Put $\varphi(t) = x_0 + x_1 t + \cdots + x_r t^r$ and $\psi(t) = y_0 + y_1 t + \cdots y_k t^k$.

1. The coefficient of t^j in $\varphi \cdot \psi$ is $\sum_{i=0}^{j} x_i y_{j-i}$, which is the sum of $j+1$ elements of $\frac{1}{c^2}\mathbb{Z} \cap [-c^2, c^2]$.
2. Write $\tau(t) = z_0 + z_1 t + \cdots + z_m t^m$, for $m = k - r$. Comparing coefficients in the equality $\tau \cdot \varphi = \psi$ one easily verifies the equality

$$z_j = x_0^{-1}\left(y_j - \sum_{i=0}^{j-1} z_i x_{j-i}\right).$$

Noting that $x_0^{-1} = x_0$ by assumption, and that the sequence a_j is the unique solution to the non-linear recurrence relation $a_{j+1} = 2a_j + 1$ with $a_0 = 2$, one easily deduces the second assertion.

□

In particular, Lemma 6.7.1 implies that the product of $\varphi, \psi \in \mathbb{Q}_c[t]$, as well as their quotient in the case where φ divides ψ, is an element of $\mathbb{Q}_{c'}[t]$, for some c' which is dependent on c and on the degrees of φ and ψ.

It should also be noted that, for $c \in \mathbb{N}$ fixed, the evaluation at q map $u \mapsto u(q) : \mathbb{Q}_c[t] \to \mathbb{N}$ is injective for all but finitely many $q \in \mathbb{N}$. Specifically, we have the following.

Lemma 6.7.2. *Fix $c \in \mathbb{N}$ and let $\varphi, \psi \in \mathbb{Q}_c[t]$. Assume $\varphi(q) = \psi(q)$ for $q > 2c^2 + 1$. Then $\varphi = \psi$.*

Proof. Arguing by contraposition, let $\varphi, \psi \in \mathbb{Q}_c[t]$ be distinct, and write $\varphi - \psi = x_0 + x_1 t + \cdots + x_m t^m$, with $x_m \neq 0$. Note that $x_i \in \frac{1}{c}\mathbb{Z} \cap [-2c, 2c]$ for all $i = 1, \ldots, m$. Then

$$\begin{aligned}|(\varphi - \psi)(q)| &= \left|\sum_{i=0}^{m} x_i q^i\right| \geq |x_m|\, q^m - \sum_{i=0}^{m-1} |x_i|\, q^i \\ &\geq \frac{1}{c} q^m - \sum_{i=0}^{m-1} 2cq^i = \frac{1}{c}\left(q^m - 2c^2 \frac{q^m - 1}{q - 1}\right) > \frac{1}{c} > 0.\end{aligned}$$

In particular $\varphi(q) \neq \psi(q)$. □

Chapter 7

Enumeration of semisimple classes

The following chapter sets up the comparative analysis of the terms relating to centralizers of semisimple elements in $G^* = (\mathbf{G}^*)^{\sigma^*}$ and $\mathfrak{g}$ in (5.4) and (5.3). Specifically, we prove the following.

Theorem 7.0.1. *Let* $\mathsf{R} = (\Phi, X, \Phi^\vee, Y)$ *be the root datum of a semisimple group of adjoint type and* $\phi \in \mathrm{Aut}(X)$*, which restricts to a permutation on a base of* Φ*. There exist*

1. *a finite set* $I = I(\mathsf{R}, \phi)$ *and, for any* $i \in I$*, a number* $n_i \in \mathbb{N}$*;*

2. *a natural number* $d = d(\mathsf{R}, \phi)$*; and*

3. *a prime number* $p_0 = p_0(\mathsf{R}, \phi)$*,*

all dependent only on R *and* ϕ*, such that the following holds.*

Let $p > p_0$ *be a prime and* $\boldsymbol{k} = \overline{\mathbb{F}_q}$*, where* $q = p^b$*, for* $b \in \mathbb{N}$*. Let* $\mathbf{G}$ *be an* $\mathbb{F}_q$*-defined semisimple group over* $\boldsymbol{k}$ *with root datum* R *and Lie-algebra* $\mathfrak{G}$*, and let* σ *be a Steinberg endomorphism of* $\mathbf{G}$ *determined by the pair* (q, ϕ) *(see § 6.2.3). Put* $G = \mathbf{G}^\sigma$ *and* $\mathfrak{g} = \mathfrak{G}^\sigma$

For any $i \in I$ *and* $j = 1, \ldots, n_i$*, there exist a connected reductive and* σ*-stable subgroup* $\mathbf{H}_{i,j} \subseteq \mathbf{G}$ *and polynomials* $u_i^{\mathfrak{g}}, v_i^{\mathfrak{g}}, u_{i,j}^G, v_{i,j}^G \in \mathbb{Q}_d[t]$ *such that, for any* $i \in I$*,*

1. $\deg u_i^{\mathfrak{g}} = \deg u_{i,1}^G$ *and* $v_i^{\mathfrak{g}}(t) = t^{\deg v_{i,1}^G}$*;*

2. *for any* $j = 2, \ldots, n_i$*, either* $\deg u_{i,j}^G = \deg u_{i,1}^G$ *or* $u_{i,j}^G = 0$*; and*

3. *for any* $j = 2, \ldots, n_i$*,* $\deg v_{i,j}^G > \deg v_{1,j}^G$ *and* $v_{i,j}(q)/v_{i,1}(q) = \left|(\mathbf{H}_{1,j}^*)^{\sigma^*} : (\mathbf{H}_{i,j}^*)^{\sigma^*}\right|_{p'}$*,*

and such that, writing

$$\mathscr{Z}_i^G(s) = \sum_{j=1}^{n_i} u_{i,j}^G(q) v_{i,j}^G(q)^{-s} \zeta^{\mathrm{unip}}_{(\mathbf{H}_{i,j}^*)^{\sigma^*}}(s) \quad \textit{and} \quad \mathscr{E}_i^{\mathfrak{g}}(s) = u_i^{\mathfrak{g}}(q) v_i^{\mathfrak{g}}(q)^{-s} \epsilon^{\mathrm{nil}}_{\mathrm{Lie}(\mathbf{H}_{i,1})^\sigma}(s),$$

we have that

$$\zeta_G(s) = \sum_{i \in I} \mathscr{Z}_i^G(s) \quad \textit{and} \quad \epsilon_{\mathfrak{g}}(s) = \sum_{i \in I} \mathscr{E}_i^{\mathfrak{g}}(s).$$

Here $(\mathbf{H}^*_{i,j}, \sigma^*)$ *is the pair of algebraic group and Steinberg endomorphism dual to* $(\mathbf{H}_{i,j}, \sigma)$.

As mentioned above, the comparison of the functions ζ_G and $\epsilon_{\mathfrak{g}}$ mandates a parallel analysis of the semisimple classes conjugacy classes in G^* and the semisimple adjoint classes in $\mathfrak{g}$. Our initial step towards this is to simultaneously analyse the set of semisimple classes in $\mathbf{G}^*$ and in *its own* Lie-algebra, which is undertaken in Section 7.1. To accomplish this analysis, we introduce bipartite graphs, with which we parametrize the semisimple classes of $\mathbf{G}^*$ and $\mathrm{Lie}(\mathbf{G}^*)$ in terms of the sets $\mathcal{I}_{\Phi^*,\phi_{\sigma^*}}$ (see Section 6.4). In order to shed a level notational complexity, the roles of $\mathbf{G}$ and $\mathbf{G}^*$ are interchanged in Section 7.1, and the group $\mathbf{G}$ considered therein is assumed to be simply-connected. The main result of this section are Proposition 7.1.3 and Corollary 7.1.5, which is our "first approximation" of Theorem 7.0.1.

Following this, we apply the results of Section 7.1 in order to pass from the enumeration and analysis of semisimple classes in $\mathrm{Lie}(\mathbf{G}^*)^{\sigma^*}$ to that of $\mathfrak{g}$. This is performed in Proposition 7.3.3, which is our final approximation towards the proof of Theorem 7.0.1.

7.1 Class enumerating graphs of G and $\mathfrak{g}$

In this section we compare the σ-stable semisimple classes of a simply-connected group $\mathbf{G}$ and those of its Lie-algebra. In order to perform this analysis, we define bipartite graphs Γ_G and $\Gamma_{\mathfrak{g}}$ with vertex sets

$$(\mathrm{Ad}(G)\backslash G_{\mathrm{ss}}) \sqcup \mathcal{I}_{\Phi,\phi_\sigma} \quad \text{and} \quad (\mathrm{Ad}(G)\backslash \mathfrak{g}_{\mathrm{ss}}) \sqcup \mathcal{I}_{\Phi,\phi_\sigma},$$

respectively. The adjacency relation on Γ_G and $\Gamma_{\mathfrak{g}}$ is defined so that the adjacency of a semisimple class with a vertex $\boldsymbol{i} \in \mathcal{I}_{\Phi,\phi_\sigma}$ implies that the centralizer of an element in the class is isomorphic to $\mathbf{H}(\boldsymbol{i})$, in the former case, or $\mathbf{h}(\boldsymbol{i})$ in the latter. To define the adjacency relation on Γ_G and $\Gamma_{\mathfrak{g}}$, we require the following.

Definition 7.1.1. Given a maximal torus $\mathbf{S} \subseteq \mathbf{G}$, not necessarily σ-stable, and $g \in \mathbf{S}$ let $\Delta(g, \mathbf{S})$ denote the set $\{\alpha \in \Phi(\mathbf{G}, \mathbf{S}) : \alpha(g) = 1\}$ of roots of $\mathbf{G}$ with respect to $\mathbf{S}$ which vanish on g. Similarly, given a maximal toric subalgebra $\mathbf{s}$ of $\mathfrak{G}$ and $x \in \mathbf{s}$, let $\Delta(x, \mathbf{s}) = \{\alpha \in \Phi : d\alpha(x) = 0\}$, where $d\alpha : \mathbf{s} \to \mathbb{G}_a$ is the differential of α at 1.

By definition, the sets $\Delta(g, \mathbf{S})$ and $\Delta(x, \mathbf{s})$ are closed subsystems of the root system $\Phi(\mathbf{G}, \mathbf{S})$, for any maximal torus $\mathbf{S} \subseteq \mathbf{G}$. Specifying to the case where $\mathbf{S} = \mathbf{T}$ is a maximally split maximal torus, it further holds that $\Delta(g, \mathbf{T})$ (resp. $\Delta(x, \mathbf{t})$) is stable under the automorphism $w \circ \phi_\sigma^{-1} \in \mathrm{Aut}(X(\mathbf{T}))$, for $w \in W = W_{\mathbf{G}}(\mathbf{T})$, whenever g (resp. x) satisfies the equality $g = {}^w\sigma(g)$ (resp. $x = {}^w\sigma(x)$); see Lemma 7.1.7.

Definition 7.1.2 (Adjacency relations)**.** Given a semisimple class $[g] \in \mathrm{Ad}(G)\backslash G_{\mathrm{ss}}$ and $\boldsymbol{i} = (\kappa, \Sigma) \in \mathcal{I}$, we declare $[g]$ and $\boldsymbol{i}$ to be adjacent in Γ_G if there exists an element $h \in \mathrm{Ad}(\mathbf{G})g \cap \mathbf{T}$ such that ${}^{w_\kappa}\sigma(h) = h$ and such that $\Delta(h, \mathbf{T}) = \Sigma$.

A semisimple adjoint class $[x] \in \mathrm{Ad}(G)\backslash \mathfrak{g}_{\mathrm{ss}}$ and $\boldsymbol{i} = (\kappa, \Sigma)$ are declared to be adjacent in $\Gamma_{\mathfrak{g}}$ if there exists $y \in \mathrm{Ad}(\mathbf{G})x \cap \mathbf{t}$ such that ${}^{w_\kappa}\sigma(y) = y$ and such that $\Delta(y, \mathbf{t}) = \Sigma$.

No other edges exist in Γ_G or $\Gamma_{\mathfrak{g}}$.

The necessary properties of the graphs Γ_G and $\Gamma_{\mathfrak{g}}$ are summarized in the following proposition.

Proposition 7.1.3. *Let Φ be the root system of a semisimple group. There exist a prime number $p_0 = p_0(\Phi)$ and a positive integer $c = c(\Phi)$ such that the following holds whenever $\mathrm{char}(\boldsymbol{k}) \geq p_0$. Let $\mathbf{G}$ be simply-connected semisimple algebraic group over $\boldsymbol{k}$ with root system Φ and Steinberg endomorphism σ with respect to an $\mathbb{F}_q$-structure on $\mathbf{G}$, and put $\mathcal{I} = \mathcal{I}_{\Phi,\phi_\sigma}$. The graphs Γ_G and $\Gamma_{\mathfrak{g}}$ satisfy the following properties.*

1. *Let $\boldsymbol{i} \in \mathcal{I}$ and $[g] \in \mathrm{Ad}(G)\backslash G_{\mathrm{ss}}$ be adjacent in Γ_G. The group $\mathbf{H}(\boldsymbol{i})$, defined in Definition 6.4.4 is isomorphic to the centralizer of g in $\mathbf{G}$, for any representative $g \in [g]$. Furthermore, $\mathbf{C}_G(g) \simeq (\mathbf{H}(\boldsymbol{i}))^\sigma$.*

2. *Let $\boldsymbol{i} \in \mathcal{I}$ and $[x] \in \mathrm{Ad}(G)\backslash \mathfrak{g}_{\mathrm{ss}}$ be adjacent in $\Gamma_{\mathfrak{g}}$. The Lie-algebra $\mathbf{h}(\boldsymbol{i})$ is isomorphic to the centralizer of x in $\mathfrak{G}$, for any representative $x \in [x]$. Furthermore, $\mathbf{C}_{\mathfrak{g}}(x) \simeq (\mathbf{h}(\boldsymbol{i}))^\sigma$.*

3. *There exists a map $\omega = \omega_G : \mathcal{I} \to \mathbb{Q}_c[t]$ such that, for any $\boldsymbol{i} = (\kappa, \Sigma) \in \mathcal{I}$*
$$\frac{|G|_{p'}}{|(\mathbf{H}(\boldsymbol{i}))^\sigma|_{p'}} = \omega(\boldsymbol{i})(q) \quad \textit{and} \quad |\mathfrak{g} : (\mathbf{h}(\boldsymbol{i}))^\sigma| = q^{2\deg \omega(\boldsymbol{i})}.$$
Moreover, in this case, $\deg \omega(\boldsymbol{i}) = \frac{1}{2}\left(|\Phi| - |\Sigma|\right)$.

4. *There exist maps $\mathcal{T}_G, \mathcal{T}_{\mathfrak{g}} : \mathcal{I} \to \mathbb{Q}_c[t]$ such that, for any $\boldsymbol{i} \in \mathcal{I}$,*
$$val_{\Gamma_G}(\boldsymbol{i}) = \mathcal{T}_G(\boldsymbol{i})(q) \quad \textit{and} \quad val_{\Gamma_{\mathfrak{g}}}(\boldsymbol{i}) = \mathcal{T}_{\mathfrak{g}}(\boldsymbol{i})(q).$$
Moreover, given $\boldsymbol{i} = (\kappa, \Sigma)$, the following holds.

   (a) *If Σ is parabolic then $\deg \mathcal{T}_{\mathfrak{g}}(\boldsymbol{i}) = \deg \mathcal{T}_G(\boldsymbol{i}) = \mathrm{rk}(\mathbf{G}) - |S_\Sigma|$, where S_Σ is a base of Σ.*

   (b) *Otherwise, if Σ is locally isolated, then $\mathcal{T}_{\mathfrak{g}}(\boldsymbol{i}) = 0$ and either $\mathcal{T}_G(\boldsymbol{i}) = 0$ or $\deg \mathcal{T}_G(\boldsymbol{i}) = \deg \mathcal{T}_G(\boldsymbol{i}^P)$, where $\boldsymbol{i}^P = (\kappa, \Sigma^P)$, with Σ^P the unique parabolic subsystem of Φ such that Σ is isolated in Σ^P.*

5. *There exists maps $d_G, d_{\mathfrak{g}} : \mathcal{I} \to \mathbb{N} \cap [1, c]$ such that*
$$val_{\Gamma_G}([g]) = d_G(\boldsymbol{i}) \quad \textit{and} \quad val_{\Gamma_{\mathfrak{g}}}([x]) = d_{\mathfrak{g}}(\boldsymbol{i}),$$
whenever $[g] \in \mathrm{Ad}(G)\backslash G_{\mathrm{ss}}$ is adjacent to $\boldsymbol{i} \in \mathcal{I}$ in Γ_G and $[x]$ is adjacent to $\boldsymbol{i}$ in $\Gamma_{\mathfrak{g}}$.

The proofs of Assertions (1)-(5) of Proposition 7.1.3 are given in § 7.2.1-7.2.4 below. For each of the assertions we will find a constant c_i, for which the specific assertion holds. Once the value p_0 is fixed, the proposition eventually follows, simply by letting c be the product of these constants. In order to facilitate the analysis by excluding some special cases where $\mathrm{char}(\boldsymbol{k})$ is small, throughout this section we will make the assumption that $\mathrm{char}(\boldsymbol{k})$ is not a torsion prime for Φ (see [57, 1.3]). By [57], this is equivalent to requiring that p is greater than the height (see § 8.0.1) of all highest roots of the simple components of Φ, which are given in Corollary 1.13 of *loc cit.* Our ultimate value of p_0 is determined in the proof of Assertion (4) (page 101).

As a corollary of Proposition 7.1.3, we obtain the following reformulations of (5.4) and (5.3) as sums over the common index set $\mathcal{I}^P \subseteq \mathcal{I}_{\Phi,\phi_\sigma}$.

Definition 7.1.4. Given $\boldsymbol{i} = (\lambda, \Psi), \boldsymbol{j} = (\kappa, \Sigma) \in \mathcal{I}_{\Phi,\phi_\sigma}$, we write $\boldsymbol{j} \prec^{\mathrm{isol}} \boldsymbol{i}$ if $\kappa = \lambda$ and if Σ is an isolated subsystem of Ψ.

Corollary 7.1.5. *Let* $\mathbf{G}$ *be a simply-connected semisimple group, as above, with Steinberg endomorphism* σ *and let* $(\mathbf{G}^*, \sigma^*)$ *be the dual algebraic group. Put* $G^* = (\mathbf{G}^*)^{\sigma^*}$. *Let* $\mathcal{I}^P \subseteq \mathcal{I}_{\Phi,\phi_\sigma}$ *denote the set of pairs* $\boldsymbol{i} = (\kappa, \Sigma)$ *in which* Σ *is parabolic. Then, assuming* $p = \mathrm{char}(\boldsymbol{k}) > p_0$,

$$\epsilon_{\mathfrak{g}}(s) = \sum_{\boldsymbol{i} \in \mathcal{I}^P} \frac{\mathcal{T}_{\mathfrak{g}}(\boldsymbol{i})(q)}{d_{\mathfrak{g}}(\boldsymbol{i})} \cdot q^{-\deg \omega(\boldsymbol{i}) \cdot s} \cdot \epsilon^{\mathrm{nil}}_{\mathbf{h}(\boldsymbol{i})^\sigma}(s), \tag{7.1}$$

and

$$\zeta_{G^*}(s) = \sum_{\boldsymbol{i} \in \mathcal{I}^P} \left(\frac{\mathcal{T}_G(\boldsymbol{i})(q)}{d_G(\boldsymbol{i})} \cdot \omega(\boldsymbol{i})(q)^{-s} \cdot \zeta^{\mathrm{unip}}_{\mathbf{H}(\boldsymbol{i})^\sigma}(s) \right.$$
$$\left. + \sum_{\substack{\boldsymbol{j} \in \mathcal{I} \\ \boldsymbol{j} \prec^{\mathrm{isol}} \boldsymbol{i}}} \frac{\mathcal{T}_G(\boldsymbol{j})(q)}{d_G(\boldsymbol{j})} \cdot \omega(\boldsymbol{j})(q)^{-s} \cdot \zeta^{\mathrm{unip}}_{\mathbf{H}(\boldsymbol{j})^\sigma}(s) \right). \tag{7.2}$$

Proof. Both (7.2) and (7.1) follow from Proposition 7.1.3, by applying Lemma 7.1.6 to the graphs $\Gamma_{\mathfrak{g}}$ and Γ_G, with $B = \mathcal{I}^P$ in the former case and $B = \mathcal{I}$ in the latter, A the set of semisimple classes, and C the vector space of finite Dirichlet series in s. The equalities (7.2) and (7.1) follow by taking $f([x]) = |\mathfrak{g} : \mathbf{C}_{\mathfrak{g}}(x)|^{-s} \cdot \epsilon^{\mathrm{nil}}_{\mathbf{C}_{\mathfrak{g}}(x)}(s)$ in the former case, and $f([g]) = \left(\frac{\left|(\mathbf{G}^*)^{\sigma^*}\right|_{p'}}{|\mathbf{C}_G(g)|_{p'}} \right)^{-s} \cdot \zeta^{\mathrm{unip}}_{\mathbf{C}_G(g)}(s)$ in the latter (note that $\left|(\mathbf{G}^*)^{\sigma^*}\right| = |G|$; see [13, Proposition 4.4.4]). $\square$

Lemma 7.1.6. *Let* Γ *be a bipartite graph with a finite vertex set* $A \sqcup B$, *such that all vertices in* A *have positive valency. Let* C *be a vector space over* $\mathbb{Q}$, *and* $f : A \to C$ *a function. Suppose there exist*

1. *a function* $g : B \to C$ *such that* $f(a) = g(b)$ *whenever* $a \in A$ *and* $b \in B$ *are adjacent; and*

2. *a map* $d : B \to \mathbb{N}$ *such that* $val_\Gamma(a) = d(b)$ *whenever* $a \in A$ *is adjacent to* $b \in B$.

Then

$$\sum_{a \in A} f(a) = \sum_{b \in B} \frac{val_\Gamma(b)}{d(b)} g(b).$$

Proof. Let E denote the set of edges of Γ. Since, by definition, a vertex $v \in A \sqcup B$ appears in exactly $val_\Gamma(v)$ many edges, by assumption, it holds that

$$\sum_{a\in A} f(a) = \sum_{\{a,b\}\in E} \frac{1}{val_\Gamma(a)} f(a) = \sum_{\{a,b\}\in E} \frac{1}{d(b)} g(b) = \sum_{b\in B} \frac{val_\Gamma(b)}{d(b)} g(b).$$

□

7.1.1 The adjacency relation in Γ_G and $\Gamma_{\mathfrak{g}}$

Lemma 7.1.7. *1. Assume $g \in \mathbf{T}$ and $w \in W$ are such that ${}^{w}(\sigma(g)) = g$. Then $\Delta(g, \mathbf{T})$ is stable under the automorphism $w \circ \phi_\sigma^{-1} \in \mathrm{Aut}(X)$.*

2. Assume $x \in \mathbf{t}$ and $w \in W$ are such that ${}^{w}(\sigma(x)) = x$. Then $\Delta(x, \mathbf{t})$ is stable under the automorphism $w \circ \phi_\sigma^{-1} \in \mathrm{Aut}(X)$.

In particular, under these assumptions, if $w = w_\kappa$ for some $\kappa \in H^1(\sigma, W)$, then the pairs $(\kappa, \Delta(g, \mathbf{T}))$ and $(\kappa, \Delta(x, \mathbf{t}))$ are elements of $\mathcal{I}_{\Phi,\phi_\sigma}$.

Proof. 1. By definition of the maps $u_\alpha : \mathbb{G}_a \to \mathbf{G}$ (see § 6.2.3) it holds that $\alpha \in \Delta(g, \mathbf{T})$ if and only if $\mathrm{Ad}(g)u_\alpha(\xi) = u_\alpha(\alpha(g)\xi) = u_\alpha(\xi)$, for all $\xi \in \mathbb{G}_a$. The assumption ${}^{w}\sigma(g) = g$ implies that

$$\begin{aligned}\mathrm{Ad}(g)u_{w\circ\phi_\sigma^{-1}(\alpha)}(\xi) &= \mathrm{Ad}(n_w) \circ \sigma\left(\mathrm{Ad}(g)\sigma^{-1}\left(\mathrm{Ad}(n_w^{-1})u_{w\circ\phi_\sigma^{-1}(\alpha)}(\xi)\right)\right)\\ &= \mathrm{Ad}(n_w) \circ \sigma\left(\mathrm{Ad}(g)u_\alpha(\xi)\right)\\ &= \mathrm{Ad}(n_w) \circ \sigma\left(u_\alpha(\xi)\right) = u_{w\circ\phi_\sigma^{-1}(\alpha)}(\xi),\end{aligned}$$

for any $\xi \in \mathbb{G}_a$.

2. The second assertion follows similarly, noting that the map $d\alpha$ satisfies the condition $\mathrm{ad}(x)u = d\alpha(x) \cdot u$ for any $u \in \mathbf{u}_\alpha = \mathrm{Lie}(\mathbf{U}_\alpha)$, and that $\alpha \in \Delta(x, \mathbf{t})$ if and only if $\mathbf{u}_\alpha \subseteq \mathbf{C}_{\mathfrak{G}}(x) = \mathrm{Ker}(\mathrm{ad}(x))$.

□

It is also useful to have the following definition.

Definition 7.1.8 (Witnesses of adjacency). Fix $\boldsymbol{i} = (\kappa, \Sigma) \in \mathcal{I}$. An element $g \in \mathbf{T}$ is said to be a *witness of adjacency* to $\boldsymbol{i}$ if ${}^{w_\kappa}\sigma(g) = g$ and if $\Delta(g, \mathbf{T}) = \Sigma$. Note that this implies that any σ-stable $\mathrm{Ad}(G)$-class in $\mathrm{Ad}(\mathbf{G})g$ is adjacent to $\boldsymbol{i}$ in Γ_G.

Similarly, $x \in \mathbf{t}$ is a witness of adjacency to $\boldsymbol{i}$ is ${}^{w_\kappa}\sigma(x) = x$ and $\Delta(x, \mathbf{t}) = \Sigma$.

Example 7.1.9. The graph Γ_G, associated to $\mathbf{G} = \mathrm{GL}_2(\boldsymbol{k})$ and $\mathbf{G} = \mathrm{GL}_3(\boldsymbol{k})$, with their Frobenius endomorphism F_q, are outlined in Figure 7.1 and Figure 7.2. The circles on the left hand side

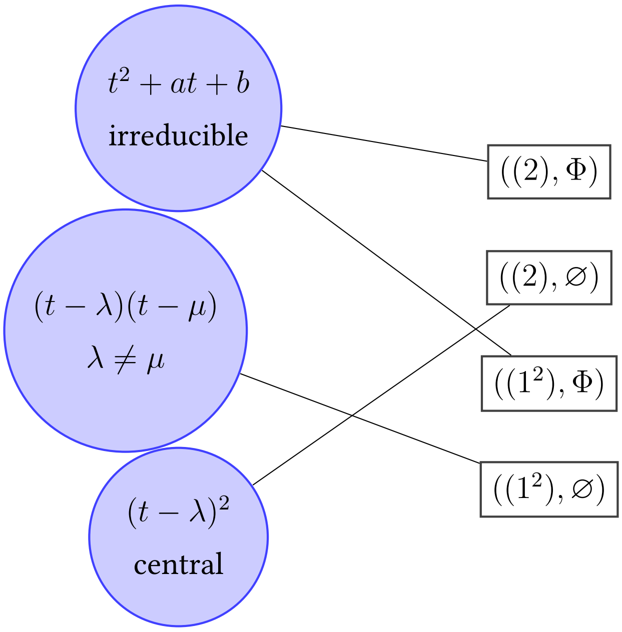


Figure 7.1: The graph Γ_G, for $\mathbf{G} = \mathrm{GL}_2(\boldsymbol{k})$ and $\sigma = F_q$

of the figures represent a partition of $\mathrm{Ad}(G)\backslash G_{\mathrm{ss}}$ with respect to the type of characteristic polynomials of elements of the class. Note that, as seen in Example 6.2.7, the map σ acts trivially on the $W_{\mathrm{GL}_n(\boldsymbol{k})}(\mathbf{T}) \simeq \mathfrak{S}_n$, and thus $H^1(\sigma, \mathfrak{S}_n)$ are conjugacy classes and therefore parametrized by partitions.

7.2 Proof of Proposition 7.1.3

In this section we prove Proposition 7.1.3. The proof is divided into subsections, whereby Assertions (1) and (2) are proved in § 7.2.1, and Assertions (3),(4) and (5) are proved in § 7.2.2, § 7.2.3 and § 7.2.4, respectively. To begin with, let us define an important set of polynomials which will appear in our computation.

Definition 7.2.1. Given $n, r, c \in \mathbb{N}$ let $\mathsf{Cyc}_{n,r,c} \subseteq \mathbb{Q}[t]$ be the set of polynomial of degree lesser or equal to n which are of the form $\sum_{j=1}^{r} a_j \Psi_j(t)$, where $a_1, \ldots, a_r \in \frac{1}{c}\mathbb{Z} \cap [-c, c]$ and the polynomial Ψ_j are products of cyclotomic polynomials and non-negative powers of t.

Note that the set $\mathsf{Cyc}_{n,r,c}$ is finite, for any given $r, n, c \in \mathbb{N}$, and in particular, there exists $c' \in \mathbb{N}$ such that $\mathsf{Cyc}_{n,r,c} \subseteq \mathbb{Q}_{c'}[t]$.

7.2.1 Centralizers of semisimple elements in G and $\mathfrak{S}$

In order to prove the first and second assertions of Proposition 7.1.3, we recall a well-known result regarding the centralizers of semisimple elements in semisimple algebraic groups. The proof of the

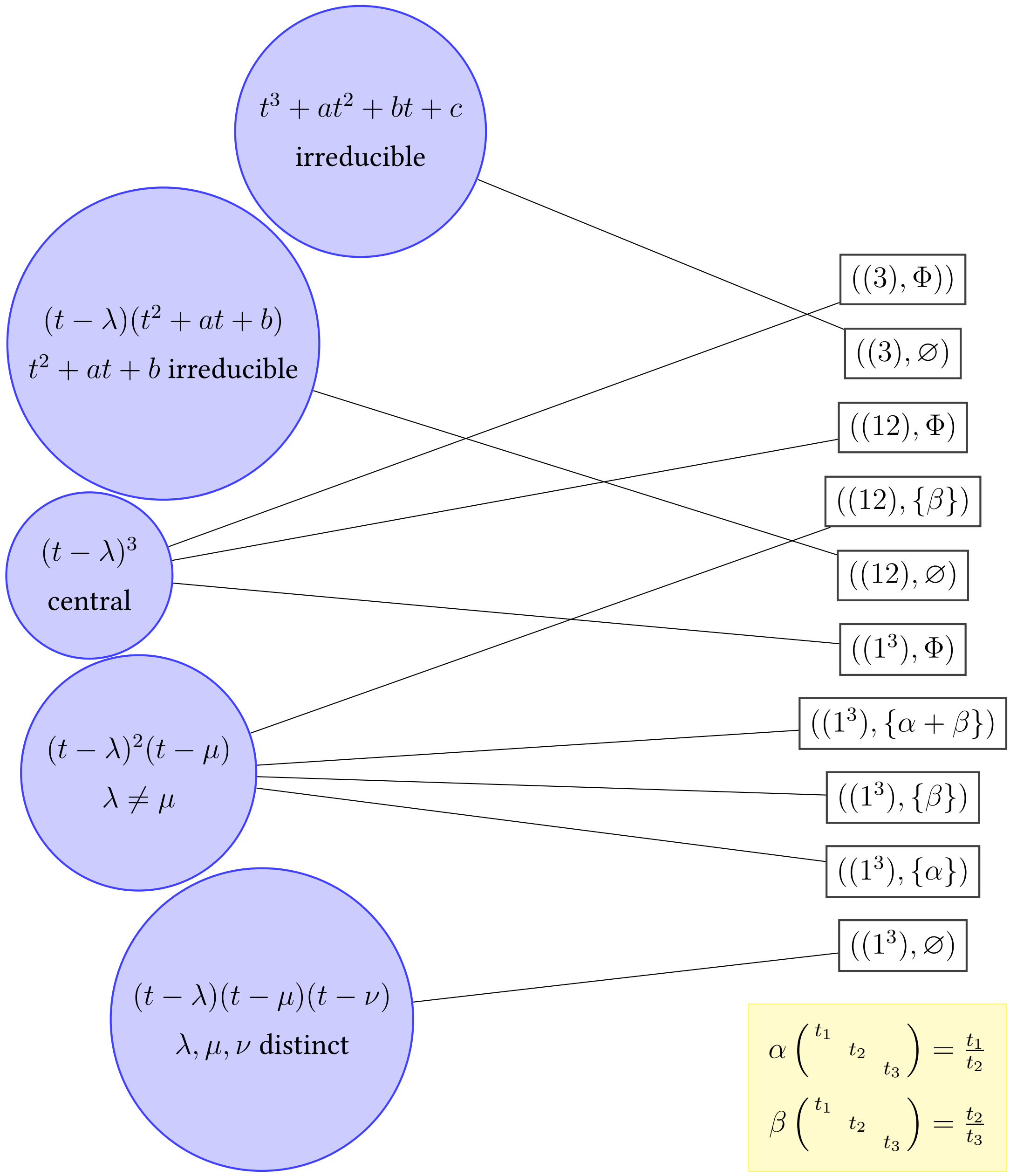


Figure 7.2: The graph Γ_G, for $\mathbf{G} = \mathrm{GL}_3(\boldsymbol{k})$ and $\sigma = F_q$.

result may be found in [51, II, 4.1].

Proposition 7.2.2. *Let* $\mathbf{G}$ *be semisimple with maximal torus* $\mathbf{S}$*, not necessarily* σ*-stable, and* $g \in \mathbf{S}$*. Let* $\Sigma = \Delta(g, \mathbf{S}) \subseteq \Phi(\mathbf{G}, \mathbf{S})$ *be as in Definition 7.1.1.*

1. *The centralizer* $\mathbf{C}_{\mathbf{G}}(g)$ *is generated by* $\mathbf{S}$*, the root subgroup* $\mathbf{U}_\alpha$ *for all* $\alpha \in \Sigma$*, and the coset representatives* n_w *of Weyl group elements* $w \in W_{\mathbf{G}}(\mathbf{S})$ *which commute with* g*.*

2. *The connected centralizer* $\mathbf{C}_{\mathbf{G}}(g)^\circ$ *is generated by* $\mathbf{S}$ *and the root subgroups* $\mathbf{U}_\alpha$ *such that* $\alpha \in \Sigma$*. In particular* $\mathbf{C}_{\mathbf{G}}(g)^\circ$ *is connected and reductive with root system* Σ *with respect to* $\mathbf{S}$*.*

Moreover, in the case where $\mathbf{G}$ is simply connected (as is assumed in Proposition 7.1.3), Steinberg's Connectedness Theorem [55, Corollary 9.9] states that the centralizer of any semisimple element of $\mathbf{G}$ is connected. In this case it holds that

$$W_{\mathbf{C}_{\mathbf{G}}(g)}(\mathbf{S}) = \mathbf{C}_{W_{\mathbf{G}}(\mathbf{S})}(g),$$

where the centralizer on the left hand side is with respect to the action of $W = W_{\mathbf{G}}(\mathbf{S})$ on $\mathbf{S}$ by conjugation. Moreover, considering $W_{\mathbf{C}_{\mathbf{G}}(g)}(\mathbf{S})$ as a subgroup of $\mathrm{Aut}(X(\mathbf{S}))$, it holds that $W_{\mathbf{C}_{\mathbf{G}}(g)}(\mathbf{S}) = \langle s_\alpha : \alpha \in \Sigma \rangle$.

The corresponding situation in the setting of the adjoint action of a semisimple group on its Lie-algebra is somewhat simpler, provided that the characteristic of the ground field is sufficiently large.

Proposition 7.2.3 ([57, Theorem 3.14])**.** *Let* $\mathbf{G}$ *be a semisimple algebraic group over* $\boldsymbol{k}$ *and let* $x \in \mathfrak{s} = \mathrm{Lie}(\mathbf{S})$*, for* $\mathbf{S} \subseteq \mathbf{G}$*, a maximal torus. Then* $\mathbf{C}_{\mathbf{G}}(x)$*, the centralizer of* x *under the adjoint action of* $\mathbf{G}$ *on* $\mathfrak{G}$*, is a connected reductive group if and only if* $p = \mathrm{char}(\boldsymbol{k})$ *is not a torsion prime for* $\mathbf{G}$*.*

Moreover, under the assumption that p is not a torsion prime, it follows that $\mathbf{C}_{\mathbf{G}}(x)$ is generated by the maximal torus $\mathbf{S}$ (which acts trivially on $\mathfrak{s}$) and the root subgroups $\mathbf{U}_\alpha$, for all $\alpha \in \Delta(x, \mathfrak{s})$. As above, the Weyl group of $\mathbf{C}_{\mathbf{G}}(x)$ is equal to the centralizer of x under the adjoint action of $W_{\mathbf{G}}(\mathbf{S})$, and is generated by the reflections $s_\alpha \in \mathrm{Aut}(X(\mathbf{S}))$ with respect to the roots $\alpha \in \Delta(x, \mathbf{t})$.

Finally, we consider the *infinitesimal centralizer* $\mathbf{C}_{\mathfrak{G}}(x)$ of $x \in \mathfrak{s}$, i.e. the set of elements of $\mathfrak{G}$ which commute with x.[1] In this situation, as mentioned in the proof Lemma 7.1.7, the root space decomposition implies that the operator $\mathrm{ad}(x)$ is diagonalizable on $\mathfrak{G}$, and acts as zero on $\mathfrak{s}$ and as the scalar $d\alpha(x)$ on the root subspaces $\mathbf{u}_\alpha$, for any $\alpha \in \Phi(\mathbf{G}, \mathbf{S})$. In particular,

$$\mathbf{C}_{\mathfrak{G}}(x) = \mathrm{Ker}(\mathrm{ad}(x)) = \mathfrak{s} \oplus \bigoplus_{\alpha \in \Delta(x, \mathfrak{s})} \mathbf{u}_\alpha. \tag{7.3}$$

[1]This terminology is based on [30].

Proof of Proposition 7.1.3.(1) and (2). Let $[g] \in \mathrm{Ad}(G)\backslash G_{\mathrm{ss}}$ and $\boldsymbol{i} = (\kappa, \Sigma) \in \mathcal{I}$ be adjacent in Γ_G. Let $g \in [g]$ be a representative and let $\widetilde{g} \in \mathrm{Ad}(\mathbf{G})g \cap \mathbf{T}$ be a witness of adjacency to $\boldsymbol{i}$. By Definition 7.1.8 and the proof of Lemma 6.3.3, it follows that the element $h = \mathrm{Ad}(g_\kappa)\widetilde{g}$ lies in $\mathbf{T}_\kappa^\sigma$, and, in particular, is a σ-fixed $\mathrm{Ad}(\mathbf{G})$-conjugate of g. Here g_κ is such that $\mathsf{L}(g_\kappa) = n_{w_\kappa}$ (see Table 6.1). By Steinberg's Connectedness Theorem and Lemma 6.1.4, it follows that g and h are in fact $\mathrm{Ad}(G)$-conjugate.

Since $\Delta(\widetilde{g}, \mathbf{T}) = \Sigma$ and $h = \mathrm{Ad}(g_\kappa)\widetilde{g}$, it follows that $\Sigma_\kappa = \{\alpha \circ \mathrm{Ad}(g_\kappa) : \alpha \in \Sigma\}$ is precisely the set of roots of $\mathbf{G}$ with respect to $\mathbf{T}_\kappa$ which vanish on h. By Proposition 7.2.2 and the definition of $\mathbf{H}(\boldsymbol{i})$ (Definition 6.4.4), it follows that

$$\mathbf{C}_{\mathbf{G}}(g) = \langle \mathbf{T}_\kappa, \mathbf{U}_{\kappa,\alpha} : \alpha \in \Sigma \rangle = \mathbf{H}(\boldsymbol{i}).$$

Since this is a bona fide equality, rather than an isomorphism, the σ-fixed points of the two groups are also equal. The first assertion now follows, since $\mathbf{C}_{\mathbf{G}}(g)$ and $\mathbf{C}_{\mathbf{G}}(h)$ are conjugate by an element of G, and in particular, have isomorphic σ-fixed subgroups.

The proof of the second assertion follows similarly, under the assumption that $\mathrm{char}(\boldsymbol{k})$ is not a torsion prime of Φ. We review it briefly. Let $[x] \in \mathrm{Ad}(G)\backslash \mathfrak{g}_{\mathrm{ss}}$ and $\boldsymbol{i} = (\kappa, \Sigma) \in \mathcal{I}$ be adjacent. Applying the argument of assertion (1), supplementing Steinberg's Connectedness Theorem with Proposition 7.2.3, there exists an $\mathrm{Ad}(G)$-conjugate $y \in \mathbf{t}_\kappa$ of x, such that $\Sigma_\kappa = \{\alpha \circ \mathrm{Ad}(g_\kappa^{-1}) : \alpha \in \Sigma\}$ is the set of roots of $\mathbf{G}$ with respect to $\mathbf{T}_\kappa$ such that $d\alpha(y) = 0$. By (7.3) and the definition of $\mathbf{h}(\boldsymbol{i})$, it follows that

$$\mathbf{C}_{\mathfrak{G}}(y) = \mathbf{t}_\kappa \oplus \bigoplus_{\alpha \in \Sigma} \mathbf{u}_{\kappa,\alpha} = \mathbf{h}(\boldsymbol{i}).$$

Finally, since x and y lie in the same $\mathrm{Ad}(G)$-conjugacy class, their infinitesimal centralizers are $\mathrm{Ad}(G)$-conjugate, and hence so are their subalgebras of σ-fixed points. $\square$

7.2.2 The finite groups $\mathbf{H}(\boldsymbol{i})^\sigma$

Fix a vertex $\boldsymbol{i} = (\kappa, \Sigma) \in \mathcal{I}$, and write $\mathbf{h} = \mathbf{h}(\boldsymbol{i})$ and $\mathbf{H} = \mathbf{H}(\boldsymbol{i})$. By Proposition 6.4.5 we known that $\dim_{\boldsymbol{k}} \mathbf{h} = \dim_{\boldsymbol{k}} \mathbf{t}_\kappa + \sum_{\alpha \in \Sigma} \dim_{\boldsymbol{k}} \mathbf{u}_{\kappa,\alpha}$. Since the spaces $\mathbf{u}_{\kappa,\alpha}$ are one-dimensional (see [41, Theorem 8.17]), it follows that $\dim_{\boldsymbol{k}} \mathbf{h} = \mathrm{rk}(\mathbf{G}) + |\Sigma|$. Additionally, for the case of $\boldsymbol{j} = ([1], \Phi)$, we have that $\mathbf{h}(\boldsymbol{j}) = \mathbf{C}_{\mathfrak{G}}(0) = \mathfrak{G}$ and $\dim_{\boldsymbol{k}} \mathfrak{G} = \dim_{\boldsymbol{k}} \mathbf{h}(\boldsymbol{j}) = \mathrm{rk}(\mathbf{G}) + |\Phi|$. Consequently, since both $\mathfrak{G}$ and $\mathbf{h}$ are σ-stable, the quotient space $\mathfrak{G}/\mathbf{h}$ is a σ-stable $\boldsymbol{k}$-vector space of dimension $|\Phi| - |\Sigma|$. By Hilbert's Theorem 90, applied for $\mathrm{Aut}(\mathfrak{G}/\mathbf{h}) \simeq \mathrm{GL}_{|\Phi|-|\Sigma|}(\boldsymbol{k})$ (see [61, 17.6 Corollary]; also [19, Example 3.7]) this space admits a basis defined over $\mathbb{F}_q$, and hence

$$|\mathfrak{g} : \mathbf{h}^\sigma| = |(\mathfrak{G}/\mathbf{h})^\sigma| = q^{|\Phi|-|\Sigma|}. \tag{7.4}$$

As noted in Proposition 6.4.5, the group $\mathbf{H}$ is connected reductive, σ-stable and of maximal rank $\mathrm{rk}(\mathbf{G})$. By Lemma 6.1.5, $\mathbf{H}$ contains a maximally split maximal torus $\mathbf{S}$. The root system $\Phi(\mathbf{H}, \mathbf{S})$ of

$\mathbf{H}$ with respect to $\mathbf{S}$ is $\mathrm{Ad}(\mathbf{H})$-conjugate to Σ, and hence $|\Phi(\mathbf{H},\mathbf{S})| = |\Sigma|$. By [19, Proposition 3.19], it follows that

$$|\mathbf{H}^\sigma| = q^{\frac{1}{2}|\Sigma|}\,|\mathbf{S}^\sigma| \sum_{w\in W_{\mathbf{H}}(\mathbf{S})^\sigma} q^{\ell(w)},$$

where $W_{\mathbf{H}}(\mathbf{S})^\sigma$ is the group of σ-fixed points in the Weyl group of $\mathbf{H}$ with respect to $\mathbf{S}$, and $\ell(w) = |\{\alpha \in \Phi(\mathbf{H},\mathbf{S})^+ : w\alpha \notin \Phi(\mathbf{H},\mathbf{S})^+\}|$ is the length function of $W_{\mathbf{H}}(\mathbf{S})$, restricted to its subgroup of σ-fixed elements. Also, note that the polynomial $\varphi_1(t) = \sum_{w\in W_{\mathbf{H}}(\mathbf{S})^\sigma} t^{\ell(w)}$ has constant term 1, corresponding to the unique element of length 0 in $W_{\mathbf{H}}(\mathbf{S})^\sigma$ (viz. the identity), and is of degree $|\Phi(\mathbf{H},\mathbf{S})^+| = \frac{1}{2}|\Sigma|$, corresponding to the longest element of $W_{\mathbf{H}}(\mathbf{S})$, which is σ-stable and maps all positive roots to negative roots. The coefficients of φ_1 are non-negative integers, bounded above by $|W_{\mathbf{H}}(\mathbf{S})| \leq |W|$.

By [41, Proposition 25.2], there exists an operator $\psi_\sigma \in \mathrm{Aut}(X(\mathbf{S}))$ of finite order, determined by the action of σ on $X(\mathbf{S})$ as in Proposition 6.2.8, such that

$$|\mathbf{S}^\sigma| = \det_{X(\mathbf{S})\otimes_{\mathbb{Z}}\mathbb{R}}(q - \psi_\sigma^{-1}).$$

Thus, there exists a polynomial $\varphi_2(t) \in \mathsf{Cyc}_{\mathrm{rk}(\mathbf{G}),1,1}$ (see Definition 7.2.1) such that $|\mathbf{S}^\circ| = \varphi_2(q)$. Since $\varphi_2(0) = \det(-\psi_\sigma^{-1}) = \pm 1$, it follows that $|\mathbf{H}^\sigma|_{p'} = \varphi_1(q)\varphi_2(q)$.

Applying the same argument for $\mathbf{G}$, with respect to the maximally split maximal torus $\mathbf{T}$, we obtain two polynomials $\theta_1, \theta_2 \in \mathbb{Z}[t]$ such that

$$\theta_1(t) = \sum_{w\in W_{\mathbf{G}}(\mathbf{T})^\sigma} t^{\ell(w)} \quad \text{and} \quad \theta_2(t) = \det_{X(\mathbf{T})\otimes_{\mathbb{Z}}\mathbb{R}}(t - \phi_\sigma^{-1}) \in \mathsf{Cyc}_{\mathrm{rk}(\mathbf{G}),1,1},$$

with $\deg\theta_1\cdot\theta_2 = \mathrm{rk}(\mathbf{G}) + \frac{1}{2}|\Phi(\mathbf{G},\mathbf{T})|$ and with $|G|_{p'} = \theta_1(q)\theta_2(q)$.

Proof of Proposition 7.1.3.(3). Let $\boldsymbol{i} = (\kappa,\Sigma)$, and, in the notation introduced above, put

$$\omega(\boldsymbol{i})(t) = \frac{\theta_1(t)\theta_2(t)}{\varphi_1(t)\varphi_2(t)}.$$

Then $\omega(\boldsymbol{i})$ is a rational function of degree $\frac{1}{2}(|\Phi| - |\Sigma|)$ and, by (7.4), it holds that $|\mathfrak{g} : \mathbf{h}^\sigma| = q^{2\deg\omega(\boldsymbol{i})}$. In fact, the map $\omega(\boldsymbol{i})$ is polynomial with integer coefficients, as the value $\omega(\boldsymbol{i})(q^j)$ is the p'-part of the index of some σ-stable connected reductive group within another σ-stable connected reductive group, hence integral, for any $j \in \mathbb{N}$ (cf. [41, Exercise 30.10]). It remains to find a bound for the coefficients of $\omega(\boldsymbol{i})$ which is independent of q.

Let c' be such that $\mathsf{Cyc}_{\mathrm{rk}(\mathbf{G}),1,1} \subseteq \mathbb{Q}_{c'}[t]$. As noted above, the coefficients of θ_1, φ_1 are integers no greater than $|W|$, and θ_2, φ_2 ares the characteristic polynomials of operators of finite order, and hence $\varphi_1,\varphi_2,\theta_1,\theta_2 \in \mathbb{Q}_{c'\cdot|W|}[t]$. Moreover, since the degrees of $\varphi_1,\varphi_2,\theta_1,\theta_2$ are all bounded above by $\dim(\mathbf{G})$, by Lemma 6.7.1.(1), there exists $c'' = (\dim\mathbf{G}+1)!\cdot c'$ such that $\theta_1\cdot\theta_2, \varphi_1\cdot\varphi_2 \in \mathbb{Q}_{c''}[t]$. Finally, since $|\varphi_1(0)\varphi_2(0)| = 1$ and since $\omega(\boldsymbol{i})$ is a polynomial, by Lemma 6.7.1.(2) and using the notation of the lemma, there exists a natural number $c_1 = a_1\cdots a_{\dim\mathbf{G}}\cdot c'' \in \mathbb{N}$, dependent only on $\mathrm{rk}(\mathbf{G})$ and $\dim(\mathbf{G})$, both of which may be deduced from the root datum of $\mathbf{G}$, and independent of q, such that $\omega(\boldsymbol{i}) \in \mathbb{Q}_{c_1}[t]$. $\square$

7.2.3 The valency of $\boldsymbol{i}$

Let $\boldsymbol{i} \in \mathcal{I}$. In order to compare the valencies of $\boldsymbol{i}$, considered as a vertex of Γ_G and $\Gamma_{\mathfrak{g}}$, we proceed in two steps. To begin with, instead of computing the number of $\mathrm{Ad}(G)$-classes of semisimple elements in G, resp. $\mathfrak{g}$, which are adjacent, we compute the total number of elements of $\mathbf{T}$, resp. $\mathbf{t}$, which witness the adjacency to $\boldsymbol{i}$ (see Definition 7.1.2). As we shall see shortly, this number may be obtained by counting the number of $\mathbb{F}_q$-rational points in certain subvarieties of $\mathbf{T}$ and $\mathbf{t}$, respectively, and described using parallel formulae, determined by $\boldsymbol{i}$; see Lemma 7.2.12 below. Following this step, in order to account for multiple counting of $\mathrm{Ad}(\mathbf{G})$-conjugate witnesses of $\boldsymbol{i}$, we compute the number of $\mathrm{Ad}(\mathbf{G})$-conjugates of a given witness of adjacency of $\boldsymbol{i}$ in $\mathbf{T}$ and $\mathbf{t}$. As it turns out, the semisimplicity of $\mathbf{G}$ implies that this number is dependent only on $\boldsymbol{i}$, and not on the chosen witness. With the information gathered up to this point, we then compute the valency of $\boldsymbol{i}$.

The number of witnesses of adjacency to $\boldsymbol{i}$

Definition 7.2.4. Given $\Psi \subseteq \Phi$ an arbitrary subset, put

$$\mathbf{T}_\Psi = \bigcap_{\alpha\in\Psi} \mathrm{Ker}(\alpha) \quad \text{and} \quad \mathbf{t}_\Psi = \bigcap_{\alpha\in\Psi} \mathrm{Ker}(d\alpha).$$

Note that the $\mathbf{t}_\Psi$ are toric subalgebras of $\mathbf{t} \subseteq \mathfrak{G}$. The groups $\mathbf{T}_\Psi$ are abelian and diagonalizable, but may fail to be connected; e.g. $\mathbf{T}_\Phi = \bigcap_{\alpha\in\Phi} \mathrm{Ker}(\alpha) = \mathbf{Z}(\mathbf{G})$ is the center of $\mathbf{G}$, which is disconnected if $\mathbf{G}$ is not of adjoint type. However, we do have the following.

Lemma 7.2.5. *Let $n = \mathrm{rk}(\mathbf{G})$. There exists a constant $\mathbf{\Lambda}(n)$ dependent only on the rank of $\mathbf{G}$, such that $|\mathbf{T}_\Sigma : \mathbf{T}_\Sigma^\circ|$ divides $\mathbf{\Lambda}(n)$, for any closed subsystem $\Sigma \subseteq \Phi$.*

Proof. Consider the group $\mathbf{H}_\Sigma$ generated by $\mathbf{T}$ and the root subgroups $\mathbf{U}_\alpha$, for all $\alpha \in \Sigma$. As mentioned in Proposition 6.4.5, the group $\mathbf{H}_\Sigma$ is connected reductive and of maximal rank, with root system Σ. In particular, by Definition 7.2.4, $\mathbf{T}_\Sigma = \bigcap_{\alpha\in\Sigma} \mathrm{Ker}(\alpha) = \mathbf{Z}(\mathbf{H}_\Sigma)$ and $\mathbf{T}_\Sigma^\circ$ is its radical $R(\mathbf{H}_\Sigma)$. In particular, it holds that $|\mathbf{T}_\Sigma : \mathbf{T}_\Sigma^\circ| = |\mathbf{Z}(\mathbf{H}_\Sigma/R(\mathbf{H}_\Sigma))|$. Since $\mathbf{H}_\Sigma^{\mathrm{ss}} = \mathbf{H}_\Sigma/R(\mathbf{H}_\Sigma)$ is semisimple of rank lesser or equal to n, its center has order no greater than the cardinality of the fundamental group of $\mathbf{H}_\Sigma^{\mathrm{ss}}$ (see [41, Definition 9.14]). A constant $\mathbf{\Lambda}(n) > 0$ which is divisible by the order of all fundamental groups of semisimple algebraic groups over $\boldsymbol{k}$ of rank $\leq n$ can be easily computed; for example, from [41, Table 9.2] it follows that one may take

$$\mathbf{\Lambda}(n) = 3^{\lfloor n/6\rfloor} 4^{\lfloor n/2\rfloor} \cdot \prod_{\substack{\lambda_1+\cdots+\lambda_r=n \\ r>0,\lambda_1,\ldots,\lambda_i\in\mathbb{N}}} (\lambda_i + 1).$$

□

Lemma 7.2.6. *Let $\boldsymbol{i} = (\kappa, \Sigma) \in \mathcal{I}$ and let $S \subseteq \Sigma$ be a base.*

1. $|\{x \in \mathbf{t}_\Sigma : {}^{w_\kappa}\sigma(x) = x\}| = q^{\mathrm{rk}\mathbf{G}-|S|}$; and

2. There exist an integer $d_{\boldsymbol{i}}$, dividing the constant $\boldsymbol{\Lambda}(\mathrm{rk}(\mathbf{G}))$ of Lemma 7.2.5, and a monic polynomial $\vartheta_{\boldsymbol{i}} \in \mathsf{Cyc}_{\mathrm{rk}(\mathbf{G})-|S|,1,1}$, such that $|\{g \in \mathbf{T}_\Sigma : {}^{w_\kappa}\sigma(g) = g\}| = d_{\boldsymbol{i}} \cdot \vartheta_{\boldsymbol{i}}(q)$.

Proof. 1. First note that $\dim_{\boldsymbol{k}} \mathbf{t}_\Sigma = \mathrm{rk}(\mathbf{G}) - |S|$. Indeed, we have a linear map $x \mapsto (d\alpha(x))_{\alpha\in\Sigma} : \mathbf{t} \to \mathbb{G}_a^{|\Sigma|}$ which, upon selection of coordinates on $\mathbf{t}$ and $\mathbb{G}_a^{|\Sigma|}$, may be represented by a matrix $A \in \mathrm{M}_{|\Sigma|\times\mathrm{rk}(\mathbf{G})}(\boldsymbol{k})$ whose rows represent the functionals $d\alpha : \mathbf{t} \to \mathbb{G}_a$ in the given coordinates on $\mathbf{t}$, for all $\alpha \in \Sigma$. Since a maximal independent subset of Σ is of size $|S|$, by the assumption that p is not a torsion prime, it follows that this matrix has rank $|S|$. By rank-nullity, $\dim_{\boldsymbol{k}} \mathbf{t}_\Sigma = \dim_{\boldsymbol{k}} \mathrm{Ker}(A) = \mathrm{rk}(\mathbf{G}) - |S|$. Assertion (1) now follows, noting that ${}^{w_\kappa}\sigma$ is a Steinberg endomorphism of $\mathbf{G}$ and that $\mathbf{t}_\Sigma$ is a stable $\boldsymbol{k}$-vector space under this endomorphism (see [19, Example 3.7]).

2. Let $X_\Sigma = \mathrm{Span}_{\mathbb{Z}}\,\Sigma \subseteq X$. Note that, in the notation of [41, Definition 3.7], it holds that $\mathbf{T}_\Sigma = \bigcap_{\alpha\in X_\Sigma} \mathrm{Ker}(\alpha) = X_\Sigma^\perp$. Additionally, since $\Sigma \subseteq \mathrm{Span}_{\mathbb{Z}}\, S$, and S is $\mathbb{Z}$-linearly independent, it holds that X_Σ is free of rank $|S|$. By [41, Proposition 3.8], it holds that

$$X(\mathbf{T}_\Sigma) = X(\mathbf{T})/T_\Sigma^\perp = X(\mathbf{T})/X_\Sigma^{\perp\perp},$$

where $X_\Sigma^{\perp\perp}$ is the subgroup of $X(\mathbf{T})$, of characters vanishing on $X_\sigma^\perp$. Since $X_\Sigma^{\perp\perp}/X_\Sigma$ is a finite p-group, it follows that $X_\Sigma^{\perp\perp}$ and X_Σ are $\mathbb{Z}$-modules of the same rank, and hence $X(\mathbf{T}_\Sigma)$ has free-rank $\mathrm{rk}(\mathbf{G}) - |S|$.

Consider the connected component $\mathbf{T}_\Sigma^\circ$ of $\mathbf{T}_\Sigma$. Recall that $d_{\boldsymbol{i}} = |\mathbf{T}_\Sigma : \mathbf{T}_\Sigma^\circ|$ divides the constant $\boldsymbol{\Lambda}(\mathrm{rk}(\mathbf{G}))$, by Lemma 7.2.5. Note that $X(\mathbf{T}_\Sigma^\circ)$, the character lattice of the torus $\mathbf{T}_\Sigma^\circ$, is free and of the same free rank as $\mathbf{T}_\Sigma$. In particular $\dim_{\mathbb{R}} X(\mathbf{T}_\Sigma^\circ) \otimes_{\mathbb{Z}} \mathbb{R} = \mathrm{rk}(\mathbf{G}) - |S|$.

Since $\boldsymbol{i} = (\kappa, \Sigma) \in \mathfrak{I}$, the subsystem $\Sigma \subseteq \Phi$ is stable under the action of $w_\kappa \circ \phi_\sigma^{-1}$. In particular, given $g \in \mathbf{T}_\Sigma$, and $\alpha \in \Sigma$ we have that

$$\alpha({}^{w_\kappa}\sigma(g)) = (w_\kappa^{-1}\alpha)(\sigma(g)) = (q\phi_\sigma \circ w_\kappa^{-1})(\alpha)(g) = \alpha'(g)^q = 1,$$

where $\alpha' = \phi_\sigma \circ w_\kappa^{-1}(\alpha) \in \Sigma$ (see Remark 6.4.2). In particular, since $\mathbf{T}_\Sigma^\circ$ is characteristic in $\mathbf{T}_\Sigma$, it holds that $\mathbf{T}_\Sigma^\circ$ is stable under the map ${}^{w_\kappa}\sigma$. Applying the argument of [41, Proposition 25.3], and taking note of Lemma 6.2.9, we deduce that

$$\left|(\mathbf{T}_\Sigma^\circ)^{{}^{w}\sigma}\right| = \left|\det_{X(\mathbf{T}_\Sigma^\circ)\otimes_{\mathbb{Z}}\mathbb{R}}(w_\kappa \circ \sigma - 1)\right| = \det_{X(\mathbf{T}_\Sigma^\circ)\otimes_{\mathbb{Z}}\mathbb{R}}(q - (w_\kappa \circ \phi_\sigma)^{-1}).$$

Since $\omega_\kappa \circ \phi_\sigma$ is an operator of finite order, its characteristic polynomial $\vartheta_{\boldsymbol{i}}(t)$ is of degree $\mathrm{rk}(\mathbf{G}) - |S|$ and given as the product of cyclotomic polynomials; that is, $\vartheta_{\boldsymbol{i}}$ is an element of $\mathsf{Cyc}_{\mathrm{rk}(\mathbf{G})-|S|,1,1}$. It follows that the set $\{g \in \mathbf{T}_\Sigma : {}^{w_\kappa}\sigma(g) = g\}$ has cardinality $d_{\boldsymbol{i}} \cdot \vartheta_{\boldsymbol{i}}(q)$.

□

In order to compute the number of witnesses of adjacency of a given pair $\boldsymbol{i} = (\kappa, \Sigma)$, we now introduce an algebraic subset of $\mathbf{T}$ which will be essential in the computation.

Definition 7.2.7. Given $\Sigma \subseteq \Phi$, a closed subsystem, define

$$\mathsf{Witn}(\Sigma, \mathbf{T}) = \{g \in \mathbf{T} : \Delta(g, \mathbf{T}) = \Sigma\}, \qquad \text{and}$$
$$\mathsf{Witn}(\Sigma, \mathbf{t}) = \{x \in \mathbf{t} : \Delta(x, \mathbf{t}) = \Sigma\}.$$

Note that $\mathsf{Witn}(\Sigma, \mathbf{T})$ and $\mathsf{Witn}(\Sigma, \mathbf{t})$ are constructible algebraic subsets of $\mathbf{T}$ and $\mathbf{t}$, respectively. In fact, it clearly holds that

$$\mathsf{Witn}(\Sigma, \mathbf{T}) = \mathbf{T}_\Sigma \smallsetminus \bigcup_{\Sigma \subsetneq \Psi \subseteq \Phi} \mathbf{T}_\Psi \quad \text{and} \quad \mathsf{Witn}(\Sigma, \mathbf{t}) = \mathbf{t}_\Sigma \smallsetminus \bigcup_{\Sigma \subsetneq \Psi \subseteq \Phi} \mathbf{t}_\Psi. \tag{7.5}$$

Furthermore, in the case where Σ is part of a pair $\boldsymbol{i} = (\kappa, \Sigma) \in \mathcal{I}$, it holds that $\mathsf{Witn}(g, \mathbf{T})$ and $\mathsf{Witn}(x, \mathbf{t})$ are stable under the endomorphism ${}^{w_\kappa}\sigma$. In this case, the number of witnesses of adjacency to $\boldsymbol{i}$ in $\mathbf{T}$ and $\mathbf{t}$ is precisely the number ${}^{w_\kappa}\sigma$-fixed points of $\mathsf{Witn}(\Sigma, \mathbf{T})$ and $\mathsf{Witn}(\Sigma, \mathbf{t})$, respectively. In order to compute this number, we will reformulate the equalities in (7.5) as sums over closed subsystems of Φ which are stable under $w_\kappa \circ \phi_\sigma^{-1}$. Before doing so, we require two simple lemmas, the first of which will be further explicated in Lemma 7.2.12 below.

Lemma 7.2.8. *Let $w \in W$ and $\Psi \subseteq \Phi$ be a parabolic subsystem (cf. Definition 6.2.1), stable under $w \circ \phi_\sigma^{-1}$. There exists $p_0 = p_0(\Phi)$ such that $\mathsf{Witn}(\Psi, \mathbf{T})^{{}^w\sigma}$ is not empty whenever $p > p_0$.*

Proof. As mentioned in the previous paragraph, the set $\mathsf{Witn}(\Psi, \mathbf{T})$ is ${}^w\sigma$-stable, and may be written as $\mathbf{T}_\Psi \smallsetminus \bigcup_{\Psi \subsetneq \Psi' \subseteq \Phi} \mathbf{T}_{\Psi'}$. Let S be a base for Ψ. Then by Lemma 7.2.6, $\left|\mathbf{T}_\Psi^{{}^w\sigma}\right|$ is given by evaluation at q of a polynomial of degree $\mathrm{rk}(\mathbf{G}) - |S|$. Furthermore, by Lemma 6.2.3, given a closed subsystem $\Psi' \supsetneq \Psi$, with base S', it necessarily holds that $|S'| > |S|$ and $\left|\mathbf{T}_{\Psi'}^{{}^w\sigma}\right|$ is given by evaluation at q of a polynomial of degree $\mathrm{rk}(\mathbf{G}) - |S'|$. It follows that the order of $\mathsf{Witn}(\Psi, \mathbf{T})^{{}^w\sigma}$ is given by evaluation at q of a polynomial of degree $\mathrm{rk}(\mathbf{G}) - |S|$, whose coefficients are bounded by a constant c' determined by Φ. Letting $p_0 > 2c'^2 + 1$ and assuming $p = \mathrm{char}(\boldsymbol{k}) > p_0$, such a polynomial cannot vanish at q; see Lemma 6.7.2. □

Remark 7.2.9. Lemma 7.2.8 may also be deduced from Direziotis' Criterion [30, § 2.15]. In the proof above we opted to use a more self-contained argument.

Definition 7.2.10. Given $w \in W$ and a subset $\Sigma \subseteq \Phi$ which is stable under $w \circ \phi_\sigma^{-1}$, put $\mathrm{cl}_w(\Sigma) = \bigcap \Delta(g, \mathbf{T})$, where the intersection ranges over all $g \in (\mathbf{T}_\Sigma)^{{}^w\sigma}$.

Note that $\mathrm{cl}_w(\Sigma)$ is the intersection of of closed subsystems, all of which are stable under the automorphism $w \circ \phi_\sigma^{-1}$, and hence closed and $w \circ \phi_\sigma^{-1}$-stable as well.

Lemma 7.2.11. *Let $w \in W$, and assume $p > p_0$ as defined in Lemma 7.2.8.*

1. *Let $g \in \mathbf{T}$ (resp $x \in \mathbf{t}$) be such that ${}^w\sigma(g) = g$ (resp. ${}^w\sigma(x) = x$). There exists a closed subsystem $\Sigma \subseteq \Phi$, stable under the operator $w \circ \phi_\sigma^{-1}$, such that $g \in \mathbf{T}_\Sigma$ (resp. $x \in \mathbf{t}_\Sigma$).*

2. *For $\Sigma \subseteq \Psi \subseteq \Phi$, arbitrary subsets, it holds that $\mathbf{T}_\Psi \subseteq \mathbf{T}_\Sigma$.*

3. *For $\Sigma, \Psi \subseteq \Phi$, arbitrary subsets, $\mathbf{T}_\Psi \cap \mathbf{T}_\Sigma = \mathbf{T}_{\Psi\cup\Sigma}$.*

4. *Let $\Sigma \subseteq \Phi$ be a subset which is stable under $w \circ \phi_\sigma^{-1}$, and let $\mathrm{cl}_w(\Sigma)$ be as in Definition 7.2.10. Then $\Sigma \subseteq \mathrm{cl}_w(\Sigma) \subseteq \Phi \cap \mathrm{Span}_\mathbb{R}\,\Sigma$.*

5. *In the setting of Assertion (4), $(\mathbf{T}_\Sigma)^{^w\sigma} = (\mathbf{T}_{\mathrm{cl}_w(\Sigma)})^{^w\sigma}$ and $(\mathbf{t}_\Sigma)^{^w\sigma} = (\mathbf{t}_{\mathrm{cl}_w(\Sigma)})^{^w\sigma}$.*

Proof. 1. Take $\Sigma = \Delta(g, \mathbf{T})$ (resp. $\Sigma = \Delta(x, \mathbf{t})$). By Lemma 7.1.7, it holds that Σ is stable under $w \circ \phi_\sigma^{-1}$, and clearly $g \in \mathbf{T}_\Sigma$ (resp. $x \in \mathbf{t}_\Sigma$).

2. and 3. Immediate from Definition 7.2.4.

4. Given $\alpha \in \Sigma$, it holds that $\alpha(g) = 1$ for all $g \in \mathbf{T}_\Sigma$, and hence $\alpha \in \bigcap_{g\in\mathbf{T}_\Sigma} \Delta(g, \mathbf{T}) \subseteq \mathrm{cl}_w(\Sigma)$. Furthermore, noting that $\Psi = \Phi\cap\mathrm{Span}_\mathbb{R}\,\Sigma$ is closed and $w\circ\phi_\sigma$-stable, the inclusion $\Sigma \subseteq \Psi$ implies the inclusion

$$\mathrm{cl}_w(\Sigma) = \bigcap_{g\in(\mathbf{T}_\Sigma)^{^w\sigma}} \Delta(g, \mathbf{T}) \subseteq \bigcap_{g\in(\mathbf{T}_\Psi)^{^w\sigma}} \Delta(g, \mathbf{T}).$$

Since Ψ is parabolic, by Lemma 7.2.8, there necessarily exists $g \in (\mathbf{T}_\Psi)^{^w\sigma}$ with $\Delta(g, \mathbf{T}) = \Psi$, and hence the rightmost intersection above equals Ψ and $\mathrm{cl}_w(\Sigma) \subseteq \Psi$.

5. The inclusion $\Sigma \subseteq \mathrm{cl}_w(\Sigma)$ implies that $\mathbf{T}_{\mathrm{cl}_w(\Sigma)} \subseteq \mathbf{T}_\Sigma$, and hence the inclusion also holds for their $^w\sigma$-fixed subgroups. Conversely, if $g \in \mathbf{T}_\Sigma^{^w\sigma}$ then, by definition, we have that $g \in \mathbf{T}_{\Delta(g,\mathbf{T})} \subseteq \mathbf{T}_{\mathrm{cl}_w(\Sigma)}$, whence the equality.

Finally, to show that $(\mathbf{t}_\Sigma)^{^w\sigma} = (\mathbf{t}_{\mathrm{cl}_w(\Sigma)})^{^w\sigma}$, it suffices to prove that the trivial inclusion $\mathbf{t}_{\mathrm{cl}_w(\sigma)} \subseteq \mathbf{t}_\Sigma$ is (recall Definition 7.2.4) actually an equality. Note that, by the argument of Lemma 7.2.6, the $\boldsymbol{k}$-dimension of $\mathbf{t}_\Sigma$ is equal to the size of a maximal linearly independent subset of Σ, which equals the size of any base of Ψ. Let S_Ψ be such a base, and let $S_{\mathrm{cl}_w(\Sigma)}$ be a base for $\mathrm{cl}_w(\Sigma)$. The inclusion $\mathrm{cl}_w(\Sigma) \subseteq \Psi$ implies that $\dim \mathbf{t}_{\mathrm{cl}_w(\Sigma)} = \mathrm{rk}(\mathbf{G}) - \left|S_{\mathrm{cl}_w(\Sigma)}\right| \geq \mathrm{rk}(\mathbf{G}) - |S_\Psi| = \dim \mathbf{t}_\Psi = \dim \mathbf{t}_\Sigma$, and hence the equality.

□

We are now ready to reformulate the equalities of (7.5) in a manner which will be suitable for our proof of Proposition 7.1.3.(4).

Lemma 7.2.12. *Let $\boldsymbol{i} = (\kappa, \Sigma) \in \mathfrak{I}$, and let $\Psi_1, \ldots, \Psi_N$ be all $w_\kappa \circ \phi_\sigma^{-1}$-stable closed subsystems of Φ which properly contain Σ. Then*

$$\left|\mathsf{Witn}(\Sigma, \mathbf{T})^{^{w_\kappa}\sigma}\right| = d_{\boldsymbol{i}}\vartheta_{\boldsymbol{i}}(q) + \sum_{I\subseteq\{1,\ldots,N\}} (-1)^{|I|} d_{(\kappa,\mathrm{cl}_{w_\kappa}(\bigcup_{j\in I}\Psi_j))}\vartheta_{(\kappa,\mathrm{cl}_{w_\kappa}(\bigcup_{j\in I}\Psi_j))}(q),$$

and

$$\left|\mathsf{Witn}(\Sigma, \mathbf{t})^{^{w_\kappa}\sigma}\right| = q^{\deg\vartheta_{\boldsymbol{i}}} + \sum_{I\subseteq\{1,\ldots,N\}} (-1)^{|I|} q^{\deg\vartheta_{(\kappa,\mathrm{cl}_{w_\kappa}(\bigcup_{j\in I}\Psi_j))}}$$

where $\vartheta_{(\kappa,\mathrm{cl}_w(\Psi))}$ *is the polynomial defined in Lemma 7.2.6, and* $\mathrm{cl}_w(\Psi)$ *is the* $w \circ \phi_\sigma^{-1}$*-stable closed subsystem of Definition 7.2.10.*

In particular, there exist polynomials $\Theta_{\mathbf{T}}(\boldsymbol{i})(t), \Theta_{\mathbf{t}}(\boldsymbol{i})(t) \in \mathsf{Cyc}_{\mathrm{rk}(\mathbf{G}),2^{2^{|\Phi|}}+1,\mathbf{\Lambda}(\mathrm{rk}(\mathbf{G}))}$*, with* $\mathbf{\Lambda}(\mathrm{rk}(\mathbf{G}))$ *as in Lemma 7.2.5, such that*

$$\left|\mathsf{Witn}(\Sigma, \mathbf{T})^{w_\kappa \sigma}\right| = \Theta_{\mathbf{T}}(\boldsymbol{i})(q) \quad \textit{and} \quad \left|\mathsf{Witn}(\Sigma, \mathbf{t})^{w_\kappa \sigma}\right| = \Theta_{\mathbf{t}}(\boldsymbol{i})(q).$$

Proof. From (7.5), we have that

$$\left|\mathsf{Witn}(\Sigma, \mathbf{T})^{w_\kappa \sigma}\right| = \left|\mathbf{T}_\Sigma^{w_\kappa \sigma}\right| - \left|\left(\bigcup_{\Sigma \subsetneq \Psi \subseteq \Phi} \mathbf{T}_\Psi\right)^{w_\kappa \sigma}\right|. \tag{7.6}$$

Furthermore, $\left|\mathbf{T}_\Sigma^{w_\kappa \sigma}\right| = d_{\boldsymbol{i}} \cdot \vartheta_{\boldsymbol{i}}(q)$, by Lemma 7.2.6.

Note that any ${}^{w_\kappa}\sigma$-fixed element $g \in \mathbf{T}_{\Sigma \cup \{\alpha\}}$ ($\alpha \in \Phi \smallsetminus \Sigma$) is included in a $w_\kappa \circ \phi_\sigma^{-1}$-stable closed subsystem of Φ, namely, the set $\Delta(g, \mathbf{T})$. In particular, the union on the right-hand side of (7.6) may be taken on $w_\kappa \circ \phi_\sigma^{-1}$-stable closed supersystems of Σ, rather than arbitrary supersets. By inclusion-exclusion, we have that

$$\begin{aligned}
\left|\left(\bigcup_{\Sigma \subsetneq \Psi \subseteq \Phi} \mathbf{T}_\Psi\right)^{w_\kappa \sigma}\right| &= \left|\bigcup_{i=1}^{N} (\mathbf{T}_{\Psi_i})^{w_\kappa \sigma}\right| \\
&= \sum_{I \subseteq \{1,\dots,N\}} (-1)^{|I|-1} \left|\bigcap_{j \in I} (\mathbf{T}_{\Psi_j})^{w_\kappa \sigma}\right| \\
&= \sum_{I \subseteq \{1,\dots,N\}} (-1)^{|I|-1} \left|\left(\mathbf{T}_{\mathrm{cl}_{w_\kappa}(\bigcup_{j \in I} \Psi_j)}\right)^{w_\kappa \sigma}\right| && \text{(Lemma 7.2.11)} \\
&= \sum_{I \subseteq \{1,\dots,N\}} (-1)^{|I|-1} d_{(\kappa,\mathrm{cl}_w(\bigcup_{j \in I} \Psi_j))} \vartheta_{(\kappa,\mathrm{cl}_w(\bigcup_{j \in I} \Psi_j))}(q). && \text{(Lemma 7.2.6)}
\end{aligned}$$

The formula for $\left|\mathsf{Witn}(\Sigma, \mathbf{T})^{w_\kappa \sigma}\right|$ follows. The formula for $\left|\mathsf{Witn}(\Sigma, \mathbf{t})^{w_\kappa \sigma}\right|$ follows by a completely parallel argument.

Finally, put

$$\Theta_{\mathbf{T}}(\boldsymbol{i})(t) = d_{\boldsymbol{i}} \vartheta_{\boldsymbol{i}}(t) + \sum_{I \subseteq \{1,\dots,N\}} (-1)^{|I|} d_{(\kappa,\mathrm{cl}_{w_\kappa}(\bigcup_{j \in I} \Psi_j))} \vartheta_{(\kappa,\mathrm{cl}_{w_\kappa}(\bigcup_{j \in I} \Psi_j))}(t), \tag{7.7}$$

and

$$\Theta_{\mathbf{t}}(\boldsymbol{i})(t) = t^{\deg \vartheta_{\boldsymbol{i}}} + \sum_{I \subseteq \{1,\dots,N\}} (-1)^{|I|} t^{\deg \vartheta_{(\kappa,\mathrm{cl}_{w_\kappa}(\bigcup_{j \in I} \Psi_j))}}. \tag{7.8}$$

By Lemma 7.2.6, the polynomials $\vartheta_{\boldsymbol{j}}$ and $t^{\deg \vartheta_{\boldsymbol{j}}}$ are products of cyclotomic polynomials and non-negative powers of t, and of degree lesser or equal to $\mathrm{rk}(\mathbf{G})$. Also, the coefficients $d_{\boldsymbol{j}}$ occurring in $\Theta_{\mathbf{T}}(\boldsymbol{i})$ are elements of $\frac{1}{\mathbf{\Lambda}(\mathrm{rk}(\mathbf{G}))}\mathbb{Z} \cap [-\mathbf{\Lambda}(\mathrm{rk}(\mathbf{G})), \mathbf{\Lambda}(\mathrm{rk}(\mathbf{G}))]$. Finally, since $\Psi_1, \dots, \Psi_N$ are all subsets of Φ, it trivially holds that $N \leq 2^{|\Phi|}$, and hence the summation in the above presentation of $\Theta_{\mathbf{T}}(\boldsymbol{i})$ and $\Theta_{\mathbf{t}}(\boldsymbol{i})$ is of no more than $2^{2^{|\Phi|}} + 1$ terms. Thus, by Definition 7.2.1, $\Theta_{\mathbf{T}}(\boldsymbol{i}), \Theta_{\mathbf{t}}(\boldsymbol{i}) \in \mathsf{Cyc}_{\mathrm{rk}(\mathbf{G}),2^{2^{|\Phi|}}+1,\mathbf{\Lambda}(\mathrm{rk}(\mathbf{G}))}$. ∎

Lemma 7.2.13. *In the notation set up in Lemma 7.2.12, assume $\boldsymbol{i} = (\kappa, \Sigma)$ is such that Σ is parabolic. Then*

$$\deg \Theta_{\mathbf{T}}(\boldsymbol{i}) = \deg \Theta_{\mathbf{t}}(\boldsymbol{i}) = \mathrm{rk}(\mathbf{G}) - |S_\Sigma| \,.$$

where S_Σ is a base of Σ.

Proof. The assumption that Σ is parabolic implies that all closed subsystems $\Psi_j \supsetneq \Sigma$ necessarily have bases strictly larger than that of Σ (see Lemma 6.2.3). In particular, by Lemma 7.2.6, the polynomials $\vartheta_{(\kappa, \mathrm{cl}_{w_\kappa}(\bigcup_{j \in I} \Psi_j))}$ in (7.7) have degrees strictly smaller than $\deg \vartheta_{\boldsymbol{i}} = \mathrm{rk}(\mathbf{G}) - |S_\Sigma|$. □

Auxiliary remarks on isolated subsystems

In this subsection we investigate the relation between pairs $\boldsymbol{i} = (\kappa, \Sigma)$ and $\boldsymbol{i}^P = (\kappa, \Sigma^P)$, where Σ is locally isolated and Σ^P is the unique parabolic subsystem of Φ in which Σ is isolated, considered as vertices in $\mathcal{I}$. Note that, by the construction of Lemma 6.2.3, it holds that Σ^P is stable under $w_\kappa \circ \phi_\sigma^{-1}$ whenever Σ is. Thus $\boldsymbol{i} \in \mathcal{I}$ indeed implies that $\boldsymbol{i}^P \in \mathcal{I}$. To begin with, let us consider the witness set of $\boldsymbol{i}$ in $\Gamma_{\mathfrak{g}}$.

Lemma 7.2.14. *Let $\Sigma \subseteq \Phi$ be a locally isolated closed subsystem. Then* $\mathsf{Witn}(\Sigma, \mathbf{t}) = \varnothing$.

Proof. Let $\Psi \subseteq \Phi$ be a closed parabolic subsystem, such that Σ is isolated in Ψ (see Lemma 6.2.3). Clearly, $\mathbf{t}_\Psi \subseteq \mathbf{t}_\Sigma$. Moreover, as seen in the proof of Lemma 7.2.6 and by definition of an isolated subsystem, $\mathbf{t}_\Sigma$ and $\mathbf{t}_\Psi$ are vector spaces of the same dimension. In particular, $\mathsf{Witn}(\sigma, \mathbf{t}) \subseteq \mathbf{t}_\Sigma \smallsetminus \mathbf{t}_\Psi = \varnothing$. □

In contrast, we have the following.

Lemma 7.2.15. *Assume $\boldsymbol{i}, \boldsymbol{i}^P \in \mathcal{I}$ are as above. Let c' be such that $\Theta(\boldsymbol{i}) \in \mathbb{Q}_{c'}[t]$ for all $\boldsymbol{i} \in \mathcal{I}$, and assume $p > p_0 = 2c'^2 + 1$. Then either $\Theta_{\mathbf{T}}(\boldsymbol{i}) = 0$, or*

$$\deg \Theta_{\mathbf{T}}(\boldsymbol{i}) = \deg \Theta_{\mathbf{T}}(\boldsymbol{i}^P).$$

Proof. Put $\Psi = \Sigma^P$, and let $\mathbf{H}_\Psi$ be the subgroup of generated by $\mathbf{T}$ and the root subgroups $\mathbf{U}_\alpha$ and $\alpha \in \Psi$. Recall the notation of $\mathbf{T}_\Sigma$ and $\mathbf{T}_\Psi$ from Definition 7.2.4, and that $\mathbf{T}_\Psi = \bigcap_{\alpha \in \Psi} \mathrm{Ker}(\alpha) = \mathbf{Z}(\mathbf{H}_\Psi)$. Furthermore, the proof of Lemma 7.2.6.(2) shows that the inclusion $\mathbf{T}_\Psi \subseteq \mathbf{T}_\Sigma$ restricts to an equality of their connected components, as both are connected and of dimension $\mathrm{rk}(\mathbf{G}) - |S|$, where S is some base of Ψ (cf. [19, Lemma 14.11]). In particular the quotient $\mathbf{T}_\Sigma / \mathbf{T}_\Psi$ is finite of size no greater than $|\mathbf{T}_\Sigma / \mathbf{T}_\Sigma^\circ| = d_{\boldsymbol{i}} < \boldsymbol{\Lambda}(\mathrm{rk}(\mathbf{G}))$ (see Lemma 7.2.6).

Consider the “restricted” witness set of Σ over Ψ

$$\mathsf{Witn}(\Sigma \mid \Psi, \mathbf{T}) = \{g \in \mathbf{T} : \Delta(g, \mathbf{T}) \cap \Psi = \Sigma\} \tag{7.9}$$

This set is obviously included in $\mathbf{T}_\Sigma \setminus \mathbf{T}_\Psi$ and is invariant under multiplication by elements of $\mathbf{T}_\Psi$. Thus, it is a union of cosets of $\mathbf{T}_\Sigma/\mathbf{T}_\Psi$ and there exist $h_1, \ldots, h_{r_{\boldsymbol{i}}} \in \mathbf{T}_\Sigma$, with $0 \le r_{\boldsymbol{i}} < d_{\boldsymbol{i}}$, such that

$$\mathsf{Witn}(\Sigma \mid \Psi, \mathbf{T}) = \bigsqcup_{j=1}^{r_{\boldsymbol{i}}} h_j \mathbf{T}_\Psi \subseteq \mathbf{T}_\Sigma.$$

Furthermore, $\mathsf{Witn}(\Sigma \mid \Psi, \mathbf{T})^{w_\kappa \sigma} = \bigsqcup_{\substack{j=1,\ldots,r_{\boldsymbol{i}} \\ w_\kappa\sigma(h_j)=h_j}} h_j \mathbf{T}_\Psi^{w_\kappa\sigma}$, and hence there exists $r'_{\boldsymbol{i}} \le r_{\boldsymbol{i}} < d_{\boldsymbol{i}}$ such that

$$\left|\mathsf{Witn}(\Sigma \mid \Psi, \mathbf{T})^{w_\kappa \sigma}\right| = r'_{\boldsymbol{i}} \left|\mathbf{T}_\Psi^{w_\sigma}\right| = r'_{\boldsymbol{i}} d_{\boldsymbol{i}^P} \cdot \vartheta_{\boldsymbol{i}^P}(q),$$

with $\deg \vartheta_{\boldsymbol{i}^P} = \mathrm{rk}(\mathbf{G}) - |S|$ (see Lemma 7.2.6). Note that $r'_{\boldsymbol{i}} = 0$ is possible, e.g. if $\mathsf{Witn}(\Sigma \mid \Psi, \mathbf{T})$ is empty.

Finally, we have that

$$\mathsf{Witn}(\Sigma, \mathbf{T}) = \{g \in \mathbf{T} : \Delta(g, \mathbf{T}) = \Sigma\} = \mathsf{Witn}(\Sigma \mid \Psi, \mathbf{T}) \setminus \bigcup_{\substack{\Sigma \subsetneq \Psi' \\ \Psi' \cap \Psi = \Sigma}} \mathbf{T}_{\Psi'}$$

where the union on the right hand side ranges over all closed subsystems of Φ which properly contain Σ and meet Ψ at Σ. Note that this union is properly included in $\mathsf{Witn}(\Sigma \mid \Psi, \mathbf{T})$. Since Σ is isolated, any closed subsystem which contains it and is not contained in Ψ necessarily spans a real vector space properly containing $\mathrm{Span}_{\mathbb{R}} \Sigma$. In particular, any base S' of Ψ has cardinality greater than $|S|$, and hence the size of $\mathbf{T}_{\Psi'}^{w_\kappa \sigma}$ is given by evaluation at q of a polynomials of degree strictly smaller than $\mathrm{rk}(\mathbf{G}) - |S|$. Using inclusion-exclusion, and applying a similar argument to Lemma 7.2.12, it follows that

$$\left|\mathsf{Witn}(\Sigma, \mathbf{T})^{w_\kappa \sigma}\right| = r'_{\boldsymbol{i}} d_{\boldsymbol{i}^P} \cdot \vartheta_{\boldsymbol{i}^P}(q) - \tau_{\boldsymbol{i}}(q),$$

for $\tau_{\boldsymbol{i}} \in \mathsf{Cyc}_{\mathrm{rk}(\mathbf{G}), 2^{2^{|\Phi|}}+1, \boldsymbol{\Lambda}(\mathrm{rk}(\mathbf{G}))}$ of degree strictly smaller than $\deg \vartheta_{\boldsymbol{i}^P}$, if $r'_{\boldsymbol{i}} \neq 0$, and $\left|\mathsf{Witn}(\Sigma, \mathbf{T})^{w_\kappa \sigma}\right| = 0$ otherwise. By Lemma 6.7.2 and the assumption $p > p_0$, it follows that either $\Theta_{\mathbf{T}}(\boldsymbol{i}) = 0$ or

$$\deg \Theta_{\mathbf{T}}(\boldsymbol{i}) = \deg \vartheta_{\boldsymbol{i}^P} = \deg \Theta_{\mathbf{T}}(\boldsymbol{i}^P).$$

□

The number of witnesses of adjacency in an $\mathrm{Ad}(\mathbf{G})$-class

To complete the preparations for the proof of Proposition 7.1.3.(4), we now consider the number elements within the $\mathrm{Ad}(\mathbf{G})$-conjugacy class of an element $g \in \mathbf{T}$ which witnesses the adjacency to the vertex $\boldsymbol{i} \in \mathcal{I}$. Our main lemma for this subsection shows that this number is in fact dependent only on the vertex $\boldsymbol{i}$, and not on the element g.

Let us fix some notation.

Notation 7.2.16. Given a subset $\Psi \subseteq \Phi$ let W_Ψ denote the subgroup of W, generated by all reflections with respect to roots in Ψ.

Recall that, by the discussion following Proposition 7.2.2 and the assumption of simply-connectedness of $\mathbf{G}$, the centralizer of a semisimple element $g \in \mathbf{T}$ equals $W_{\Delta(g,\mathbf{T})}$. Similarly, by Proposition 7.2.3 and the succeeding discussion, it also holds that $\mathbf{C}_W(x) = W_{\Delta(x,\mathbf{t})}$, for any semisimple $x \in \mathbf{t}$.

Fix $\boldsymbol{i} = (\kappa, \Sigma) \in \mathcal{I}$. Let $g \in \mathbf{T}$ and $x \in \mathbf{t}$ witness the adjacency to $\boldsymbol{i}$, that is, ${}^{w_\kappa}\sigma(g) = g$, ${}^{w_\kappa}\sigma(x) = x$ and $\Delta(g,\mathbf{T}) = \Delta(x,\mathbf{t}) = \Sigma$. Recall that, by [51, II, 3.1], any $\mathrm{Ad}(\mathbf{G})$-conjugate of g in $\mathbf{T}$ is also $\mathrm{Ad}(W)$-conjugate to it. An alternative proof of this fact (see [30, Proposition 3.1]) generalizes easily to the analogous statement for $\mathrm{Ad}(\mathbf{G})$-conjugates of x in $\mathbf{t}$.

In light of these facts, our next goal is to show that the number of $\mathrm{Ad}(W)$-conjugates of g and of x which are witnesses of adjacency is determined by $\boldsymbol{i}$.

Put

$$\begin{aligned} \mathcal{E}_G(g,\boldsymbol{i}) &= \left\{ w \in W : {}^w g \text{ is a witness of adjacency to } \boldsymbol{i} \right\}, \qquad \text{and} \\ \mathcal{E}_{\mathfrak{g}}(x,\boldsymbol{i}) &= \left\{ w \in W : {}^w x \text{ is a witness of adjacency to } \boldsymbol{i} \right\}. \end{aligned}$$

Note that it is not true in general that $\mathcal{E}_G(g,\boldsymbol{i})$ and $\mathcal{E}_{\mathfrak{g}}(x,\boldsymbol{i})$ are subgroups of W. However, they are clearly the union of left cosets of $W/\mathbf{C}_W(g)$ and $W/\mathbf{C}_W(x)$, respectively.

Lemma 7.2.17. *Let $\boldsymbol{i} = (\kappa, \Sigma) \in \mathcal{I}$ and let $g \in \mathbf{T}$ and $x \in \mathbf{t}$ be witnesses of adjacency to $\boldsymbol{i}$. Then*

$$\mathcal{E}_G(g,\boldsymbol{i}) = \mathcal{E}_{\mathfrak{g}}(x,\boldsymbol{i}) = \left\{ w \in \mathrm{Stab}_W(\Sigma) : w^{-1} w_\kappa \sigma(w) w_\kappa^{-1} \in W_\Sigma \right\}, \tag{7.10}$$

where $\mathrm{Stab}_W(\Sigma) = \{ w \in W : w\alpha \in \Sigma$ *for all* $\alpha \in \Sigma \}$.

Proof. As already mentioned, and by the assumption $\Delta(g,\mathbf{T}) = \Sigma$, we have that

$$\mathbf{C}_W(g) = W_{\Delta(g,\mathbf{T})} = W_\Sigma.$$

Let $w \in \mathcal{E}_G(g,\boldsymbol{i})$, i.e. ${}^w g$ is also a witness of adjacency to $\boldsymbol{i}$. In particular, this means that

$$\Sigma = \Delta(wg,\mathbf{T}) = w\Delta(g,\mathbf{T}) = w\Sigma$$

so that $w \in \mathrm{Stab}_W(\Sigma)$. Furthermore, being witnesses of adjacency, we have that $g = {}^{w_\kappa}\sigma(g)$ and ${}^w g = {}^{w_\kappa}\sigma({}^w g)$ and hence

$$g = {}^{w^{-1} w_\kappa \sigma(w)}\sigma(g) = {}^{w^{-1} w_\kappa \sigma(w) w_\kappa^{-1}} g,$$

i.e. $w^{-1} w_\kappa \sigma(w) w_\kappa^{-1} \in \mathbf{C}_W(g) = W_\Sigma$. Conversely, by reversing the argument above, one verifies that any element $w \in \mathrm{Stab}_W(\Sigma)$ satisfying the equality $w^{-1} w_\kappa \sigma(w) w_\kappa^{-1} \in W_\Sigma$ is necessarily an element of $\mathcal{E}_G(g,\boldsymbol{i})$.

The proof for $\mathcal{E}_{\mathfrak{g}}(x,\boldsymbol{i})$ is completely analogous. □

Proof of Proposition 7.1.3.(4). Let $\boldsymbol{i} = (\kappa, \Sigma) \in \mathcal{I}$. We have already seen in Lemma 7.2.14 that, in the case where Σ is locally isolated, $val_{\Gamma_{\mathfrak{g}}}(\boldsymbol{i}) = 0$.

By Definition 7.1.2, it holds that

$$val_{\Gamma_G}(\boldsymbol{i}) = \left|\{[g] \in \mathrm{Ad}(G)\backslash G_{\mathrm{ss}} : \exists h \in \mathrm{Ad}(\mathbf{G})g \cap \mathbf{T},\ {}^{w_\kappa}\sigma(h) = h \text{ and } \Delta(h, \mathbf{T}) = \Sigma\}\right|.$$

Additionally, by [51, II, Corollary 3.10], the simply-connectedness of $\mathbf{G}$ implies that map $\mathrm{Ad}(G)h \mapsto \mathrm{Ad}(\mathbf{G})h$ is a bijection between the set of $\mathrm{Ad}(G)$-conjugacy classes of σ-fixed semisimple elements and the set of σ-fixed $\mathrm{Ad}(\mathbf{G})$-classes in $\mathbf{G}_{\mathrm{ss}}$. Thus

$$val_{\Gamma_G}(\boldsymbol{i}) = \left|\{[g] \in (\mathrm{Ad}(\mathbf{G})\backslash \mathbf{G}_{\mathrm{ss}})^\sigma : \exists h \in [g] \cap \mathbf{T},\ {}^{w_\kappa}\sigma(h) = h \text{ and } \Delta(h, \mathbf{T}) = \Sigma\}\right|.$$

Furthermore, [51, II, Corollary 3.1] states that the map $[g] \mapsto [g] \cap \mathbf{T}$ is a bijection between the set of $\mathrm{Ad}(\mathbf{G})$-conjugacy classes of semisimple elements of $\mathbf{G}$ and the set of $\mathrm{Ad}(W)$-orbits in $\mathbf{T}$, which maps σ-stable classes to σ-stable orbits. Thus

$$\begin{aligned} val_{\Gamma_G}(\boldsymbol{i}) &= \left|\{[g] \in (\mathrm{Ad}(W)\backslash \mathbf{T})^\sigma : \exists h \in [g],\ {}^{w_\kappa}\sigma(h) = h \text{ and } \Delta(h, \mathbf{T}) = \Sigma\}\right| \\ &= \left|\{[g] \in \mathrm{Ad}(W)\backslash \mathbf{T} : \exists h \in [g],\ {}^{w_\kappa}\sigma(h) = h \text{ and } \Delta(h, \mathbf{T}) = \Sigma\}\right| \end{aligned}$$

where the last equality holds since the condition ${}^{w_\kappa}\sigma(h) = h$ already implies that $\mathrm{Ad}(W)h = \mathrm{Ad}(W)g$ is σ-stable.

Define $\nu_G(\boldsymbol{i}) = |\mathcal{E}_G(g, \boldsymbol{i})/W_\Sigma|$, where $g \in \mathbf{T}$ is a witness of adjacency of $\boldsymbol{i}$, and $\mathcal{E}_G(g, \boldsymbol{i})$ is as in Lemma 7.2.17. Recall that the value $\nu_G(\boldsymbol{i})$ is well-defined and independent of the choice of witness g. Then

$$val_{\Gamma_G}(\boldsymbol{i}) = \frac{1}{\nu(\boldsymbol{i})}\left|\{g \in \mathbf{T} : \exists^{w_\kappa}\sigma(g) = g \text{ and } \Delta(g, \mathbf{T}) = \Sigma\}\right| = \frac{\Theta_{\mathbf{T}}(\boldsymbol{i})(q)}{\nu_G(\boldsymbol{i})},$$

with $\Theta_{\mathbf{T}}(\boldsymbol{i})$, the polynomial defined in Lemma 7.2.12.

Similarly, using the connectedness of centralizers of semisimple elements of $\mathfrak{G}$ and retracing the argument of [51, II, 3.10] for this case, the argument given above shows that

$$val_{\Gamma_{\mathfrak{g}}}(\boldsymbol{i}) = \frac{\Theta_{\mathbf{t}}(\boldsymbol{i})(q)}{\nu_{\mathfrak{g}}(\boldsymbol{i})},$$

where $\nu_{\mathfrak{g}}(\boldsymbol{i}) = |\mathcal{E}_{\mathfrak{g}}(x, \boldsymbol{i}) : W_\Sigma|$ and $x \in \mathbf{t}$ is a witness of adjacency to $\boldsymbol{i}$. Since $\nu(\boldsymbol{i})$ is no greater than $|W|$, taking

$$\mathcal{T}_G(\boldsymbol{i})(t) = \frac{\Theta_{\mathbf{T}}(\boldsymbol{i})(t)}{\nu_G(\boldsymbol{i})} \quad \text{and} \quad \mathcal{T}_{\mathfrak{g}}(\boldsymbol{i})(t) = \frac{\Theta_{\mathbf{t}}(\boldsymbol{i})(t)}{\nu_{\mathfrak{g}}(\boldsymbol{i})},$$

it holds that $\mathcal{T}_G(\boldsymbol{i}), \mathcal{T}_{\mathfrak{g}}(\boldsymbol{i}) \in \mathsf{Cyc}_{\mathrm{rk}(\mathbf{G}), |W|\cdot(2^{2^{|\Phi|}}+1), \mathbf{\Lambda}(\mathrm{rk}(\mathbf{G}))}$, and therefore there exists $c_2 \in \mathbb{N}$ such that $\mathcal{T}_{\mathbf{G}}(\boldsymbol{i}), \mathcal{T}_{\mathfrak{g}}(\boldsymbol{i}) \in \mathbb{Q}_{c_2}[t]$. Let p_0 be a prime number larger than all torsion primes of Φ and greater than $2c_2^2 + 1$. Any prime $p > p_0$ satisfies the assumptions of Lemma 7.2.8 and Lemma 7.2.15. Furthermore, the equality of degrees of $\mathcal{T}_G(\boldsymbol{i})$ and $\mathcal{T}_{\mathfrak{g}}$ in the case where Σ is parabolic is noted in Lemma 7.2.13. The complementary case, of Σ locally isolated, is discussed in Lemma 7.2.14 and Lemma 7.2.15, respectively. $\square$

7.2.4 The valencies of semisimple classes in Γ_G and $\Gamma_{\mathfrak{g}}$

Finally, in this section, we consider the valency of $\mathrm{Ad}(G)$-conjugacy classes $[g] \in \mathrm{Ad}(G)\backslash G_{\mathrm{ss}}$ and $[x] \in \mathrm{Ad}(G)\backslash \mathfrak{g}_{\mathrm{ss}}$, considered as vertices in Γ_G and $\Gamma_{\mathfrak{g}}$, respectively, and prove Assertion (5) of Proposition 7.1.3. Namely, we prove the following two facts:

1. the valency of $[g]$ (resp. of $[x]$) is bounded above by a constant determined by the root system of $\mathbf{G}$; and

2. the valency of $[g]$ (resp. of $[x]$) is determined by any vertex $\boldsymbol{i}$ which is adjacent to $[g]$ in Γ_G (resp. adjacent to $[x]$ in $\Gamma_{\mathfrak{g}}$).

We require the following lemma.

Lemma 7.2.18. *Let $g \in \mathbf{T}$ (resp. $x \in \mathbf{t}$) and $w \in W$ such that ${}^{w}\sigma(g) = g$ (resp. ${}^{w}\sigma(x) = x$). The bijections of Lemma 6.3.1 restrict to bijective maps*

$$\left\{ \begin{matrix} \mathrm{Ad}(G)\text{-classes of } \sigma\text{-stable} \\ \text{maximal tori of } \mathbf{G} \text{ containing a} \\ \sigma\text{-fixed } \mathrm{Ad}(\mathbf{G})\text{-conjugate of } g \end{matrix} \right\} \quad \overset{1-1}{\longleftrightarrow} \quad \left\{ \kappa \in H^1(\sigma, W) : \kappa \cap C_W(g)w \neq \varnothing \right\},$$

and

$$\left\{ \begin{matrix} \mathrm{Ad}(G)\text{-classes of } \sigma\text{-stable} \\ \text{maximal tori of } \mathfrak{G} \text{ containing a} \\ \sigma\text{-fixed } \mathrm{Ad}(\mathbf{G})\text{-conjugate of } x \end{matrix} \right\} \quad \overset{1-1}{\longleftrightarrow} \quad \left\{ \kappa \in H^1(\sigma, W) : \kappa \cap C_W(x)w \neq \varnothing \right\},$$

where $\mathbf{C}_W(g)w \in \mathbf{C}_W(g)\backslash W$ is the right coset of $\mathbf{C}_W(g)$ with respect to w.

Proof. We proof the lemma for the case of $g \in \mathbf{T}$. The case $x \in \mathbf{t}$ is completely parallel.

Let $\mathbf{S}$ be a σ-stable maximal torus of $\mathbf{G}$ which contains a σ-fixed $\mathrm{Ad}(\mathbf{G})$-conjugate of g. Up to conjugation by an element of G, by Lemma 6.3.1, we may assume that $\mathbf{S} = \mathbf{T}_\kappa$, for a unique $\kappa \in H^1(\sigma, W)$. Furthermore, by Lemma 6.3.3, there exists $z \in \kappa$ such that ${}^{z}\sigma(g) = g$. Together with the assumption ${}^{w}\sigma(g) = g$, it now follows that

$${}^{zw^{-1}}g = {}^{z}\sigma(g) = g,$$

and hence $z \in \mathbf{C}_W(g)w$.

In the other direction, to show that the map above is surjective, let $\kappa \in H^1(\sigma, W)$ contain an element of the right coset $\mathbf{C}_W(g)w$, say $z \in \kappa \cap \mathbf{C}_W(g)w$. Thus, ${}^{zw^{-1}}g = g$. Let $h_z \in \mathbf{G}$ be such that $\mathsf{L}(h_z) = h_z\sigma(h_z)^{-1} = n_z$, where $n_z \in \mathbf{N}_{\mathbf{G}}(\mathbf{T})$ is a coset representative of z. By the bijection of Lemma 6.3.1, the maximal torus $h_z^{-1}\mathbf{T}h_z$ is $\mathrm{Ad}(G)$-conjugate to $\mathbf{T}_\kappa$, and clearly contains the element $h_z^{-1}gh_z$. Furthermore,

$$\sigma(h_z^{-1}gh_z) = h_z^{-1}\left({}^{z}\sigma(g)\right)h_z = h_z^{-1}\left({}^{zw^{-1}}g\right)h_z = h_z^{-1}(g)h_z,$$

where the penultimate equality holds since $\sigma(g) = {}^{w^{-1}}g$ and the last equality holds by the assumption $z \in \mathbf{C}_W(g)w$. $\square$

Remark 7.2.19. Lemma 7.2.18 is closely related to [51, Corollary 3.12], which may be regarded as a stronger variant of the lemma in the case $w = 1$. The strength of the corollary is evident in the fact that it allows to classify the maximal tori containing a *specific* σ-fixed $\mathrm{Ad}(\mathbf{G})$-conjugate of g, rather then any $\mathrm{Ad}(\mathbf{G})$-conjugate of g.

Proof of Proposition 7.1.3.(5). As in the proof of Lemma 7.2.18, we consider only the valency of a vertex $[g] \in \mathrm{Ad}(G)\backslash G_{\mathrm{ss}}$ in the graph Γ_G. The analogous statements for vertices of $\Gamma_{\mathfrak{g}}$ are proved similarly.

Fix an $\mathrm{Ad}(G)$-conjugacy class $[g] \in \mathrm{Ad}(G)\backslash G_{\mathrm{ss}}$, and let $\mathcal{N}_{\Gamma_G}([g]) \subseteq \mathcal{I}$ denote the set of neighbours of $[g]$ in Γ_G. Denote $\mathbf{\Omega}_{[g]} = \mathrm{Ad}(\mathbf{G})g \cap \mathbf{T}$, for $g \in [g]$ a representative, and recall that $\mathbf{\Omega}_g$ is a complete $\mathrm{Ad}(W)$-orbit, by [51, II, 3.1], and thus $\left|\mathbf{\Omega}_{[g]}\right| \leq |W|$. For any $h \in \mathbf{\Omega}_{[g]}$, put

$$A(h) = \left\{\boldsymbol{l} = (\lambda, \Psi) \in H^1(\sigma, W) : {}^{w_\lambda}\sigma(h) = h \text{ and } \Delta(h, \mathbf{T}) = \Psi\right\}.$$

By Definition 7.1.2, it holds that

$$\mathcal{N}_{\Gamma_G}([g]) = \bigcup_{h \in \mathbf{\Omega}_{[g]}} A(h). \tag{7.11}$$

Also note that, for $h \in \mathbf{\Omega}_{[g]}$ fixed, the right coordinate of any pair $\boldsymbol{i} \in A(h)$ is determined by h and hence $|A(h)| \leq |H^1(\sigma, W)| \leq |W|$. In particular, for $c_3 = |W|^2$, we deduce that

$$val_{\Gamma_G}([g]) = |\mathcal{N}_{\Gamma_G}([g])| \leq \left|\mathbf{\Omega}_{[g]}\right| \cdot \max\left\{|A(h)| : h \in \mathbf{\Omega}_{[g]}\right\} \leq c_3.$$

This proves the boundedness of $val_{\Gamma_G}([g])$, independently of $\mathrm{char}(\boldsymbol{k})$.

To complete the proof, we now present an alternative description of the set $\mathcal{N}_{\Gamma_G}([g])$, which is completely determined by an arbitrary choice of neighbour $\boldsymbol{i} \in \mathcal{N}_{\Gamma_G}([g])$. To do so, fix $\boldsymbol{i} = (\kappa, \Sigma) \in \mathcal{N}_{\Gamma_G}([g])$ and let $h \in \mathbf{\Omega}_{[g]} \subseteq \mathbf{T}$ witness the adjacency to $\boldsymbol{i}$, i.e. ${}^{w_\kappa}\sigma(h) = h$ and $\Delta(h, \mathbf{T}) = \Sigma$. Recall that the centralizer of h in W is given by $W_\Sigma = \langle s_\alpha : \alpha \in \Sigma\rangle$, and, in particular, is determined by Σ.

Let $\{w_1, \ldots, w_r\}$ be a transversal for the left coset space W/W_Σ. Then $\mathbf{\Omega}_{[g]} = \{{}^{w_1}h, {}^{w_2}h, \ldots, {}^{w_r}h\}$ (without repetitions), and, furthermore, for any $j = 1, \ldots, r$,

1. $\Delta({}^{w_j}h, \mathbf{T}) = w_j\Sigma = \{w_j\alpha : \alpha \in \Sigma\}$, and in particular, $\mathbf{C}_W({}^{w_j}h) = W_{w_j\Sigma}$; and

2. the element $\tau_\kappa(w_j) \overset{\text{def}}{=\!=} w_j w_\kappa \sigma(w_j)^{-1} \in W$ satisfies ${}^{\tau_\kappa(w_j)}\sigma(w_j h) = h$.

In particular, by Lemma 6.3.3 and Lemma 7.2.18, for any $j = 1, \ldots, r$, the coordinate projection map $(\kappa, \Sigma) \mapsto \kappa$ defines a bijection of the set $A({}^{w_j}h)$ onto the set

$$B_{\boldsymbol{i}}(w_j) = \left\{\lambda \in H^1(\sigma, W) : \lambda \cap (W_{w_j\Sigma})\tau_\kappa(w_j) \neq \varnothing\right\}.$$

Note that the information required in order to define the sets $B_{\boldsymbol{i}}(\cdot)$ and the transversal set $\{w_1, \ldots, w_j\}$ is completely contained in $\boldsymbol{i}$, and is independent of $[g]$. Also, the inverse of the projection maps $A({}^{w_j}h) \to B_{\boldsymbol{i}}(w_j)$ is given by $\lambda \in B_{\boldsymbol{i}}(w_j) \mapsto (\lambda, w_j\Sigma) \in A({}^{w_j}h)$, and is completely determined by $\boldsymbol{i}$ and the transversal set $\{w_1, \ldots, w_r\}$. Gluing these maps, we get a surjective map

$$\bigsqcup_{j=1}^{r} B_{\boldsymbol{i}}(w_j) \to \bigcup_{j=1}^{r} A({}^{w_j}h) = \mathcal{N}_{\Gamma_G}([g]). \tag{7.12}$$

The cardinality of fibres of this map are also given in terms of the data enclosed in $\boldsymbol{i} = (\kappa, \Sigma)$; namely, given $\boldsymbol{l} = (\lambda, \Psi)$, the fibre over $\boldsymbol{l}$ is in bijection with the set

$$F_{\boldsymbol{l}} = \left\{ j \in \{1, \ldots, r\} : w_j\Sigma = \Psi \text{ and } \lambda \cap (W_{w_j\Psi})\tau_\kappa(w_j) \neq \varnothing \right\}.$$

The valency of $[g]$ may now be reformulated as

$$val_{\Gamma_G}([g]) = |\mathcal{N}_{\Gamma_G}([g])| = \sum_{\boldsymbol{l} \in \bigcup_j A({}^{w_j}h)} 1 = \sum_{j=1}^{r} \sum_{\lambda \in B_{\boldsymbol{i}}(w_j)} \frac{1}{\left|F_{(\lambda, w_j\Sigma)}\right|},$$

a quantity completely determined by $\boldsymbol{i}$, which we define to be $d_G(\boldsymbol{i})$.

Repeating the proof for the case of a vertex $[x] \in \mathrm{Ad}(G)\backslash\mathfrak{g}_{\mathrm{ss}}$ in $\Gamma_{\mathfrak{g}}$, one arrives at the same conclusion, namely, that $val_{\Gamma_{\mathfrak{g}}}([x]) = d_{\mathfrak{g}}(\boldsymbol{i})$, whenever $[x]$ and $\boldsymbol{i}$ are adjacent vertices of $\Gamma_{\mathfrak{g}}$. This computation is omitted. □

The proof of Proposition 7.1.3 is now complete, by letting $c = c_1 \cdot c_2 \cdot c_3$, where $c_1, c_2, c_3 \in \mathbb{N}$ are the constants obtained in Subsections 7.2.2, 7.2.3 and 7.2.4, respectively, and letting p_0 be the prime fixed in the proof of Assertion (4) in 7.2.4.

7.3 The Adjoint class functions of $\mathrm{Lie}(\mathbf{G})$ and $\mathrm{Lie}(\mathbf{G}^*)$

Let $(\mathbf{G}, \sigma)$ and $(\mathbf{G}^*, \sigma^*)$ a pair of dual connected semisimple algebraic groups, with $\mathbf{G}$ of adjoint type, and $\mathbf{T}, \mathbf{T}^*$ maximal σ- and σ^*-stable maximally split tori in $\mathbf{G}$ and $\mathbf{G}^*$, respectively and Φ and Φ^* their respective root systems. Let ϕ_σ and ϕ_{σ^*} denote the automorphism of $\mathrm{Aut}(X(\mathbf{T}))$ and $\mathrm{Aut}(X(\mathbf{T}^*))$ determined by the action σ and σ^* on the respective character group. Put $\mathcal{I} = \mathcal{I}_{\Phi, \phi_\sigma}$ and $\mathcal{I}^* = \mathcal{I}_{\Phi^*, \phi_{\sigma^*}}$, and $\mathcal{I}^P$ and $(\mathcal{I}^*)^P$ the sets of pairs whose root subsystem is parabolic in the ambient root system. Writing $G = \mathbf{G}^\sigma$, $G^* = (\mathbf{G}^*)^\sigma$, $\mathfrak{g}^* = \mathrm{Lie}(\mathbf{G}^*)^{\sigma^*}$, and letting $\mathbf{H}^*(\boldsymbol{j})$, for $\boldsymbol{j} = (\kappa, \Sigma) \in \mathcal{I}^*$, be the subgroup of $\mathbf{G}^*$ generated by the σ^*-stable maximal torus $\mathbf{T}^*_\kappa$ and the root subgroups $\mathbf{U}_{\alpha^*}$ for $\alpha^* \in \Sigma$, Equations (7.2) and (7.1) of Corollary 7.1.5 may be rewritten as

$$\zeta_G(s) = \sum_{\boldsymbol{i} \in (\mathcal{I}^*)^P} \left(\frac{\mathcal{T}_{G^*}(\boldsymbol{i})(q)}{d_{G^*}(\boldsymbol{i})} \cdot \omega_{G^*}(\boldsymbol{i})(q)^{-s} \cdot \zeta^{\mathrm{unip}}_{\mathbf{H}^*(\boldsymbol{i})^\sigma}(s) \right.$$
$$\left. + \sum_{\substack{\boldsymbol{j} \in \mathcal{I}^* \\ \boldsymbol{j} \prec^{\mathrm{isol}} \boldsymbol{i}}} \frac{\mathcal{T}_{G^*}(\boldsymbol{j})(q)}{d_{G^*}(\boldsymbol{j})} \cdot \omega(\boldsymbol{j})(q)^{-s} \cdot \zeta^{\mathrm{unip}}_{\mathbf{H}^*(\boldsymbol{j})^\sigma}(s) \right),$$

and

$$\epsilon_{\mathfrak{g}^*}(s) = \sum_{\boldsymbol{i}\in(\mathcal{I}^*)^P} \frac{\mathcal{T}_{\mathfrak{g}^*}(\boldsymbol{i})(q)}{d_{\mathfrak{g}^*}(\boldsymbol{i})} \cdot q^{-\deg\omega(\boldsymbol{i})\cdot s} \cdot \epsilon^{\mathrm{nil}}_{\mathrm{Lie}(\mathbf{H}^*(\boldsymbol{i}))^{\sigma^*}}(s).$$

By Proposition 7.1.3, there exists a constant $c^* \in \mathbb{N}$ and a prime p_0 such that, assuming $\mathrm{char}(\mathbb{F}_q) > p$, the polynomials $\mathcal{T}_{G^*}(\boldsymbol{j}), \omega_{G^*}(\boldsymbol{j})$ and $\mathcal{T}_{\mathfrak{g}^*}(\boldsymbol{j})$ are all elements of $\mathbb{Q}_{c^*}[t]$, and the natural numbers $d_{G^*}(\boldsymbol{j})$ and $d_{\mathfrak{g}^*}(\boldsymbol{j})$ are bounded by c^*, for any $\boldsymbol{j} \in \mathcal{I}^*$. Furthermore, $\deg \mathcal{T}_{G^*}(\boldsymbol{i}) = \deg \mathcal{T}_{\mathfrak{g}^*}(\boldsymbol{i})$ for any $\boldsymbol{i} \in (\mathcal{I}^*)^P$.

Utilizing the bijection $\boldsymbol{i} \mapsto \boldsymbol{i}^* : (\mathcal{I})^P \to (\mathcal{I}^*)^P$, defined in § 6.5.3, we now compare between the representation zeta function of G and the adjoint class function of $\mathfrak{g}$. Recall that the bijection $*$ maps a pair (κ, Σ) to (κ^*, Σ^*), where κ^* is defined as in Lemma 6.5.2 and $\Sigma^* = \{\alpha^* : \alpha \in \Sigma\}$ is a parabolic subsystem; see Lemma 6.2.6. In particular, any base of Σ is mapped bijectively by the map $\alpha \mapsto \alpha^*$ to a base of Σ^*. Increasing p_0 if necessary, assume $\mathrm{char}(\boldsymbol{k})$ is larger than p_0 and the prime attained by applying Proposition 7.1.3 to the root system Φ as well as Φ^*, with their respective Steinberg endomorphisms. We then have the following.

Lemma 7.3.1. *Retaining all notation set up thus far, let $\boldsymbol{i} \in \mathcal{I}^P$. Then*

$$\deg \mathcal{T}_{\mathfrak{g}}(\boldsymbol{i}) = \deg \mathcal{T}_{\mathfrak{g}^*}(\boldsymbol{i}^*) \quad \textit{and} \quad \deg \omega_G(\boldsymbol{i}) = \deg \omega_{G^*}(\boldsymbol{i}^*).$$

Furthermore, the pairs $(\mathbf{H}(\boldsymbol{i}), \sigma)$ and $(\mathbf{H}^*(\boldsymbol{i}^*), \sigma^*)$ are dual.

Proof. Let S_Σ be a base of Σ. Then $S^*_\Sigma = \{\alpha^* : \alpha \in S_\Sigma\}$ is a base of Σ^* of the same cardinality as S_Σ. By Proposition 7.1.3.(4).(a), $\deg \mathcal{T}_{\mathfrak{g}}(\boldsymbol{i}) = \mathrm{rk}(\mathbf{G}) - |S_\Sigma|$ which is the same as $\mathrm{rk}(\mathbf{G}^*) - |S^*_\Sigma| = \deg \mathcal{T}_{\mathfrak{g}^*}(\boldsymbol{i}^*)$ and, by Assertion (3) of the same proposition, $\deg \omega_G(\boldsymbol{i}) = \frac{1}{2}(|\Phi| - |\Sigma|) = \frac{1}{2}(|\Phi^*| - |\Sigma^*|) = \deg \omega_{G^*}(\boldsymbol{i}^*)$. The final assertion is simply Lemma 6.5.3. □

Remark 7.3.2. We note that, *a priori,* the map $\mathcal{T}_{\mathfrak{g}}$ of Lemma 7.3.1 is not well-defined, as $\mathbf{G}$ here is taken to be of adjoint type and does not necessarily satisfy the hypothesis of Proposition 7.1.3. This may be repaired by passing to the simply-connected cover $\mathbf{G}^{\mathrm{sc}}$ of $\mathbf{G}$, to which Proposition 7.1.3 applies, and noting that $\mathrm{Lie}(\mathbf{G}^{\mathrm{sc}})$ is canonically isomorphic to $\mathfrak{G}$ (see [41, Proposition 9.15]) and that the adjoint action of $\mathbf{G}^{\mathrm{sc}}$ on $\mathfrak{G}$ factors through the adjoint action of $\mathbf{G}$ on $\mathfrak{G}$.

Proposition 7.3.3. *There exist $d \in \mathbb{N}$, and, for any $\boldsymbol{i} \in \mathcal{I}$ and $\boldsymbol{j} \in \mathcal{I}^*$, polynomials $\boldsymbol{\tau}^{\boldsymbol{i}}_{\mathfrak{g}}, \boldsymbol{\tau}^{\boldsymbol{j}}_{G^*} \in \mathbb{Q}_d[t]$ such that*

1. $\deg \boldsymbol{\tau}^{\boldsymbol{i}}_{\mathfrak{g}} = \deg \boldsymbol{\tau}^{\boldsymbol{i}^*}_{G^*}$*, for any $\boldsymbol{i} \in \mathcal{I}^P$; and*
2. *for any $\boldsymbol{i} \in \mathcal{I}^P$ and $\boldsymbol{j} \in \mathcal{I}^*$ such that $\boldsymbol{j} \prec^{\mathrm{isol}} \boldsymbol{i}^*$, the polynomial $\boldsymbol{\tau}^{\boldsymbol{j}}_{G^*}$ is either zero or of degree equal to* $\deg \boldsymbol{\tau}^{\boldsymbol{i}^*}_{G^*}$.

The polynomials $\boldsymbol{\tau}_{\mathfrak{g}}^{\boldsymbol{i}}$ and $\boldsymbol{\tau}_{G^*}^{\boldsymbol{j}}$ satisfy

$$\zeta_G(s) = \sum_{\boldsymbol{i}\in\mathcal{I}^P} \Bigg(\boldsymbol{\tau}_{G^*}^{\boldsymbol{i}^*}(q) \cdot \omega_{G^*}(\boldsymbol{i}^*)(q)^{-s} \cdot \zeta^{\mathrm{unip}}_{\mathbf{H}^*(\boldsymbol{i}^*)^{\sigma^*}}(s) + \sum_{\substack{\boldsymbol{j}\in\mathcal{I}^* \\ \boldsymbol{j}\prec^{\mathrm{isol}}\boldsymbol{i}^*}} \boldsymbol{\tau}_{G^*}^{\boldsymbol{j}}(q) \cdot \omega_{G^*}(\boldsymbol{j})(q)^{-s} \cdot \zeta^{\mathrm{unip}}_{\mathbf{H}^*(\boldsymbol{j})^{\sigma^*}}(s) \Bigg) \tag{7.13}$$

and

$$\epsilon_{\mathfrak{g}}(s) = \sum_{\boldsymbol{i}\in\mathcal{I}^P} \boldsymbol{\tau}_{\mathfrak{g}}^{\boldsymbol{i}}(q) \cdot q^{-\deg \omega_{G^*}(\boldsymbol{i}^*)\cdot s} \cdot \epsilon^{\mathrm{nil}}_{\mathbf{h}(\boldsymbol{i})^{\sigma}}(s). \tag{7.14}$$

Furthermore, for any $\boldsymbol{i} \in \mathcal{I}^P$, $\mathbf{h}(\boldsymbol{i})$ is the Lie-algebra of the dual algebraic group of $\mathbf{H}^*(\boldsymbol{i}^*)$, with σ the dual Steinberg endomorphism of σ^*.

Proof. Let c and c^* be the constants obtained from Proposition 7.1.3 for the root systems Φ and Φ^* respectively, and put $d = (c \cdot c^*)^2$. For any $\boldsymbol{i} \in \mathcal{I}$ let $\boldsymbol{\tau}_{\mathfrak{g}}^{\boldsymbol{i}} = \frac{1}{d_{\mathfrak{g}}(\boldsymbol{i})}\mathcal{T}_{\mathfrak{g}}(\boldsymbol{i})$ and, for any $\boldsymbol{j} \in \mathcal{I}^*$, let $\boldsymbol{\tau}_{G^*}^{\boldsymbol{j}} = \frac{1}{d_{G^*}(\boldsymbol{j})}\mathcal{T}_{G^*}(\boldsymbol{j})$. It clearly holds that $\boldsymbol{\tau}_{\mathfrak{g}}^{i}, \boldsymbol{\tau}_{G^*}^{\boldsymbol{j}} \in \mathbb{Q}_d[t]$, and that Assertions (1) and (2) above hold, by Proposition 7.1.3.(4) and Lemma 7.3.1. Equations (7.13) and (7.14) follow directly from the discussion above. □

Proof of Theorem 7.0.1. Let $I = \mathcal{I}^P$, and take p_0 be no lesser than the primes obtained by applying Proposition 7.1.3 to both Φ and Φ^*, with their respective automorphisms induced from σ and σ^*. Let d be the constant obtained in Proposition 7.3.3. For any $\boldsymbol{i} = (\kappa, \Psi) \in \mathcal{I}^P$ let $n_{\boldsymbol{i}}$ denote the number of isolated subsystems of Ψ, and let $\boldsymbol{j}_1, \dots, \boldsymbol{j}_{n_{\boldsymbol{i}}} \in \mathcal{I}^*$ be all distinct elements such that $\boldsymbol{j}_k \prec^{\mathrm{isol}} \boldsymbol{i}^*$. The lemma follows directly from Proposition 7.3.3, by taking

$$u_1^{\mathfrak{g}} = \tau_{\mathfrak{g}}^{\boldsymbol{i}}, \quad u_{\boldsymbol{i},1}^G = \boldsymbol{\tau}_{G^*}^{\boldsymbol{i}}, \quad v_{\boldsymbol{i},1}^G = \omega_{G^*}(\boldsymbol{i}^*), \quad u_{\boldsymbol{i},k}^G = \boldsymbol{\tau}_G^{\boldsymbol{j}_k}, \quad v_{\boldsymbol{i},k}^G = \omega_{G^*}(\boldsymbol{j}),$$

for any $\boldsymbol{i} \in I$ and $k = 2, \dots, n_{\boldsymbol{i}}$. The assertion that $\deg v_{i,j} > \deg v_{1,j}$ for all $i \in I$ and $j = 1, \dots, n_j$ follows from Assertion (3) of Proposition 7.1.3 and the definition of the relation $\prec^{\mathrm{isol}}$. □

Chapter 8

Unipotent representations and nilpotent classes

Let $\mathbf{G}$ be a connected semisimple algebraic group of adjoint type over $\boldsymbol{k}$ and Steinberg endomorphism σ with respect to an $\mathbb{F}_q$-structure of $\mathbf{G}$. Let $\mathbf{G}^*$ be the dual algebraic group of $\mathbf{G}$ with σ^* a Steinberg endomorphism dual to σ (see Section 6.5), and let $\mathfrak{G}^* = \mathrm{Lie}(\mathbf{G}^*)$. Let Φ be the root system of $\mathbf{G}$ with respect to a maximally split maximal torus $\mathbf{T}$, and $\Phi^* = \Phi(\mathbf{G}^*, \mathbf{T}^*)$ the dual root system. The group $\mathbf{G}^*$ is simply connected, and the results of the previous chapter may be applied to it. In particular, by Proposition 7.3.3, there exists a finite set $\mathcal{I}^P$ consisting of pairs $(\kappa, \Sigma) \in \mathcal{I} = \mathcal{I}_{\Phi,\phi_\sigma}$ in which Σ is a parabolic subsystem of Φ, such that the representation zeta function of $G = \mathbf{G}^\sigma$ and the adjoint class function of $\mathfrak{g} = \mathfrak{G}^\sigma$ may be written as a sum of finite Dirichlet series, indexed by $\mathcal{I}^P$, of the form

$$\zeta_G(s) = \sum_{\boldsymbol{i} \in \mathcal{I}^P} \left(\boldsymbol{\tau}_{G^*}^{\boldsymbol{i}^*}(q) \cdot \omega(\boldsymbol{i}^*)(q)^{-s} \cdot \zeta^{\mathrm{unip}}_{\mathbf{H}^*(\boldsymbol{i}^*)^{\sigma^*}}(s) + \sum_{\substack{\boldsymbol{j} \in \mathcal{I}^* \\ \boldsymbol{j} \prec^{\mathrm{isol}} \boldsymbol{i}^*}} \boldsymbol{\tau}_{G^*}^{\boldsymbol{j}}(q) \omega(\boldsymbol{j})(q)^{-s} \cdot \zeta^{\mathrm{unip}}_{\mathbf{H}^*(\boldsymbol{j})^{\sigma^*}}(s) \right),$$

and

$$\epsilon_{\mathfrak{g}}(s) = \sum_{\boldsymbol{i} \in \mathcal{I}^P} \boldsymbol{\tau}_{\mathfrak{g}}^{\boldsymbol{i}}(q) \cdot q^{-\deg \omega(\boldsymbol{i}^*) \cdot s} \cdot \epsilon^{\mathrm{nil}}_{\mathbf{h}(\boldsymbol{i})^\sigma}(s).$$

where $\omega(\boldsymbol{j}) = \omega_{G^*}(\boldsymbol{j})$, $\tau_{G^*}^{\boldsymbol{j}}$ and $\tau_{\mathfrak{g}}^{\boldsymbol{i}}$ ($\boldsymbol{j} \in \mathcal{I}^*,\ \boldsymbol{i} \in \mathcal{I}$) are polynomials with coefficients in a fixed finite subset of $\mathbb{Q}$, which is determined by the root datum of $\mathbf{G}$ and the automorphism $\phi_\sigma \in \mathrm{Aut}(X)$. Furthermore $\deg(\tau_{G^*}^{\boldsymbol{i}^*}) = \deg(\tau_{\mathfrak{g}}^{\boldsymbol{i}})$ for all $\boldsymbol{i} \in \mathcal{I}^P$, and, given $\boldsymbol{i} \in \mathcal{I}^P$ and $\boldsymbol{j} \in \mathcal{I}^*$ such that $\boldsymbol{j} \prec^{\mathrm{isol}} \boldsymbol{i}^*$ (recall Definition 7.1.4), the polynomial $\boldsymbol{\tau}_{G^*}^{\boldsymbol{j}}$ is either zero or of the same degree as $\boldsymbol{\tau}_{G^*}^{\boldsymbol{i}^*}$.

It follows that, in order to prove that $\zeta_G(s) \sim_{(c,q)} \epsilon_{\mathfrak{g}}(s)$ for some $c \in \mathbb{N}$, it is sufficient to find $c_{\boldsymbol{i}}$, for any $\boldsymbol{i} \in \mathcal{I}^P$, such that

$$\epsilon^{\mathrm{nil}}_{\mathbf{h}(\boldsymbol{i})^\sigma}(s) \sim_{(c_{\boldsymbol{i}},q)} \zeta^{\mathrm{unip}}_{\mathbf{H}^*(\boldsymbol{i}^*)^{\sigma^*}}(s) + \sum_{\substack{\boldsymbol{j} \in \mathcal{I}^* \\ \boldsymbol{j} \prec^{\mathrm{isol}} \boldsymbol{i}^* \text{ and } \boldsymbol{\tau}_{G^*}^{\boldsymbol{j}} \neq 0}} \left(\frac{\omega(\boldsymbol{j})(q)}{\omega(\boldsymbol{i})(q)} \right)^{-s} \zeta^{\mathrm{unip}}_{\mathbf{H}^*(\boldsymbol{j})^{\sigma^*}}(s). \tag{8.1}$$

Note that, by the defining property of the map $\omega = \omega_{G^*}$ (see Proposition 7.1.3), it holds that $\frac{\omega(\boldsymbol{j})(q)}{\omega(\boldsymbol{i})(q)} = \left|\mathbf{H}^*(\boldsymbol{i})^{\sigma^*} : \mathbf{H}^*(\boldsymbol{j})^{\sigma^*}\right|$, whenever $\boldsymbol{j} \prec^{\mathrm{isol}} \boldsymbol{i}^*$. The question of when $\boldsymbol{\tau}_{G^*}^{\boldsymbol{j}}$ is non-zero for $\boldsymbol{j} \in \mathcal{I}$ is addressed in § 8.0.1 below.

In this chapter we prove that a formula, closely related to (8.1), does indeed hold in the case where $\mathbf{H}(\boldsymbol{i})$ is a simply-connected simple group of type A_ℓ for any $\ell \in \mathbb{N}$, or of type C_ℓ for $2 \leq \ell \leq 41$. Namely, we show the following.

Theorem 8.0.1. *Let $(\mathbf{H}, \sigma)$ be one of the following pairs of $\mathbb{F}_q$-defined simply connected simple algebraic group over $\boldsymbol{k}$ and Steinberg endomorphism of $\mathbf{H}$*

1. *$(\mathrm{SL}_{\ell+1}(\boldsymbol{k}), F_q)$, with F_q the Frobenius map with respect to an $\mathbb{F}_q$-structure on $\mathrm{SL}_{\ell+1}(\boldsymbol{k})$, and $\ell \in \mathbb{N}$.*

2. *$(\mathrm{SL}_{\ell+1}(\boldsymbol{k}), \sigma)$, with σ the twisted Steinberg endomorphism on $\mathrm{SL}_{\ell+1}(\boldsymbol{k})$, defined as in Example 6.2.7, and $\ell \in \mathbb{N}$.*

3. *$(\mathrm{Sp}_{2\ell}(\boldsymbol{k}), F_q)$, with F_q the Frobenius map with respect to an $\mathbb{F}_q$-structure on $\mathrm{Sp}_{2\ell}(\boldsymbol{k})$, and $\ell \in \mathbb{N} \cap [1, 41]$.*

Let Φ be the root system of $\mathbf{H}$ with respect to a maximally split maximal torus $\mathbf{S} \subseteq \mathbf{H}$, and $W = W_{\mathbf{H}}(\mathbf{S})$, the Weyl group. Let $\mathbf{H}^*$ be the dual algebraic group of $\mathbf{H}$, with Lie-algebra $\mathbf{h}$ and dual Steinberg endomorphism σ^*, and put $\mathfrak{h}^* = (\mathbf{h}^*)^{\sigma^*}$.

Let $\Sigma_1, \ldots, \Sigma_r$ be distinct representatives for all isolated ϕ_σ-stable subsystems of Φ such that $\boldsymbol{\tau}_H^{([\mathbf{1}],\Sigma_i)} \neq 0$, up to conjugacy by an element of W. For any $i = 1, \ldots, r$, let $\mathbf{H}_i = \mathbf{H}_{\Sigma_i}$ be the subgroup of $\mathbf{H}$ generated by $\mathbf{S}$ and the root subgroups $\mathbf{U}_\alpha$ for $\alpha \in \Sigma_i$, and put $H_i = \mathbf{H}_i^{\sigma^*}$. There exists $c \in \mathbb{N}$ and a prime number p_0 such that,

$$\epsilon_{\mathfrak{h}^*}^{\mathrm{nil}}(s) \sim_{(c,q)} \zeta_H^{\mathrm{unip}}(s) + \sum_{i=1}^{r} |H : H_i|^{-s} \, \zeta_{H_i}^{\mathrm{unip}}(s), \tag{8.2}$$

whenever $\mathrm{char}(\boldsymbol{k}) > p_0$.

In the case where $\mathbf{H} = \mathrm{SL}_{\ell+1}(\mathbb{F}_q)$, Theorem 8.0.1 reduces to the assertion that $\epsilon_{\mathfrak{h}^*}^{\mathrm{nil}} = \epsilon_{\mathfrak{h}}^{\mathrm{nil}} \sim \zeta_H^{\mathrm{unip}}$, as in this case the group $\mathbf{H}$ is self-dual, and all maximal closed subsystems of Φ are $\mathrm{Ad}(W)$-conjugate to Φ, and, in particular, Φ has no isolated subsystems. In this case, the proof may be completed using elementary combinatorial tools, and is carried out in Section 8.1. The case where $\mathbf{H} = \mathrm{Sp}_{2\ell}(\mathbb{F}_q)$ is slightly more elaborate, as in this case the root system Φ has $\lfloor \ell/2 \rfloor$ distinct isolated subsystems satisfying the condition of the theorem. The proof in this case, while still elementary in nature, is somewhat more elaborate. The restriction $\ell \leq 41$ in this case is due to a current lack of proof for a necessary combinatorial identity (see Lemma B.2.2). It is highly likely that this restriction is superfluous; see Remark 8.2.2.

8.0.1 Deriziotis's Critertion

For the following section, let $\mathbf{G}$ be a simple and simply-connected algebraic group over $\boldsymbol{k}$ with Steinberg endomorphism σ, and root system Φ with respect to a maximally split maximal torus $\mathbf{T}$. Let $W = W_{\mathbf{G}}(\mathbf{T})$ be the Weyl group of $\mathbf{G}$. Recall the notation $\Delta(g, \mathbf{T}) = \{\alpha \in \Phi : \alpha(g) = 1\}$ (Definition 7.1.1). Deriziotis's Criterion gives a very convenient characterization of the closed subsystems $\Sigma \subseteq \Phi$ for which $\Sigma = \Delta(g, \mathbf{T})$ for some $g \in \mathbf{T}$, which we now recall.

Let $S \subseteq \Phi$ be a base for Φ. By definition, any element $\beta \in \Phi$ can be written uniquely as $\beta = \sum_{\alpha \in S} c_\alpha \alpha$, with $c_\alpha \in \mathbb{Z}$, all of the same sign. The *height* of β is then defined to be the value $\sum_\alpha c_\alpha$. The root system Φ, being indecomposable, contains a unique *highest root* α_0 with respect to the base S; i.e., a root whose height is maximal.

Theorem 8.0.2 (Deriziotis's Criterion [17])**.** *Let $\Sigma \subseteq \Phi$ be a closed subsystem of $\mathbf{G}$ and let $\mathbf{H}_\Sigma$ be the connected reductive subgroup generated by $\mathbf{T}$ and the root subgroups $\mathbf{U}_\alpha$, for $\alpha \in \Sigma$. There exists a semisimple element $g \in \mathbf{T}$ such that $\mathbf{H}$ is $\mathrm{Ad}(\mathbf{G})$ conjugate to $\mathbf{C}_{\mathbf{G}}(g)$ if and only if its root system Σ has a basis which is $\mathrm{Ad}(W)$-conjugate to a proper subset of $S \cup \{-\alpha_0\}$, where α_0 is the highest root of Φ with respect to S. In this case, $\Sigma = \Delta(g, \mathbf{T})$.*

For more information regarding the criterion, as well as other relevant criteria, we refer to [30, Ch. 2].

Root subsystems satisfying Deriziotis's Criterion may be classified using the *extended Dynkin diagram* of Φ, which is formed using the ordinary construction of the Dynkin diagram, applied to the set $S \cup \{-\alpha_0\}$ (see [44, Ch. 4, § 2 and 3]). The extended diagrams of the groups which we shall consider appear in (8.3) and (8.11).

We note that the element $g \in \mathbf{T}$ such that $\Sigma = \Delta(g, \mathbf{T})$ given by Deriziotis's Criterion is not necessarily σ-stable element g. The condition that Σ is ϕ_σ-stable has already been shown to be necessary for g to be σ-stable, but *a priori* not sufficient, in Lemma 7.1.7. In order to bypass this possible issue, we will simply find a suitable σ-stable element g for which $\Sigma = \Delta(g, \mathbf{T})$ in all investigated cases. Note that the existence of such an element is equivalent, by Lemma 7.2.15 and Definition 7.1.2, to $\mathcal{T}_G([\mathbf{1}], \Sigma)$ being non-zero.

8.0.2 Families of unipotent characters

A prominent feature of the set of unipotent characters of the group $G = \mathbf{G}^\sigma$ which is central in our analysis is its decomposition into *families of unipotent characters*. Let us briefly recall the definition a family, in the case where σ is split, i.e. the maximal torus $\mathbf{T}$ may be chosen so that σ acts as F_q on it; for the general case we refer to [13, § 12.3]. In this case, one defines, for any irreducible character ϕ of W, a class function on G by

$$R_\phi = \frac{1}{|W|} \sum_{w \in W} \phi(w) R_{\mathbf{T}^\sigma_{[w]}, \mathbf{1}},$$

where $\mathbf{T}_{[w]}$ is the σ-stable maximal torus associated to the equivalence class of w in $H^1(\sigma, W)$ and $R_{\mathbf{T}^{\sigma}_{[w]},\mathbf{1}}$ is the generalized character associated to the trivial character on $\mathbf{T}_{[w]}$ (see [13, § 7.2]). Two unipotent characters χ, χ' lie in the same family if there exists a sequence

$$\chi = \chi^1, \chi^2, \ldots, \chi^r = \chi',$$

such that for any $i = 1, \ldots, r-1$, there exists $\phi \in \mathrm{Irr}(W)$ such that $[\chi_i, R_\phi] \neq 0$ and $[\chi_{i+1}, R_\phi] \neq 0$, where $[\cdot, \cdot]$ is the standard inner product of class functions on G (see e.g. Section 6.6).

Families of unipotent characters are finite and of prescribed order, and their elements are parametrized in terms of certain associated finite groups. Furthermore, given such a family $\mathbf{F} \subseteq \mathrm{Irr}(G)$, there exists a unique $\phi_{\mathbf{F}} \in \mathrm{Irr}(W)$ which satisfies the condition $[\chi, R_{\phi_{\mathbf{F}}}] > 0$ for all $\chi \in \mathbf{F}$, and the association $\mathbf{F} \mapsto \phi_{\mathbf{F}}$ defines a bijection between the collection of families of unipotent characters of G and $\mathrm{Irr}(W)$. This bijection is explicated below in Lemma 8.2.3 in the case of $G = \mathrm{Sp}_{2\ell}(\mathbb{F}_q)$. Furthermore, in the same case, we show the following.

Lemma 8.0.3. *For any $\chi \in \mathrm{Irr}(G)$ let $u_\chi \in \mathbb{Q}[t]$ be such that $\chi(1) = u_\chi(q)$. Let $\mathbf{F}$ be a family of unipotent characters and let $\mathscr{F} = \{u_\chi : \chi \in \mathbf{F}\}$. Then all polynomials in $\mathscr{F}$ have the same degree.*

It is likely that Lemma 8.0.3 may be proved directly from the properties of family (see [13, p. 380]). Nonetheless, we give an elementary and self-contained proof, assuming knowledge of the set $\mathscr{F}$ (taken from [13, § 13.8]), in Lemma 8.2.3. Lemma 8.0.3 has also been verified in a parallel project for all simple groups.

8.0.3 Partition notation

In order to formalize the comparison of unipotent representation zeta function and the nilpotent adjoint class function, we require some basic terminology regarding integer partitions, which is summarized in Table 8.1. As a matter of convention, we always write partitions in non-descending order, and Young diagrams in English notation, i.e. with the top row corresponding to the largest (that is, the last) partition part. We emphasize that, throughout this section, we consider the empty partition as a viable partition; namely, it is the unique partition of zero.

The norm notations $\|\cdot\|_1$ and $\|\cdot\|_2^2$ are also in use, more generally, for finite number sequences.

Throughout the following sections we also invoke certain partition identities, the proofs of which are deferred to Appendix B.

8.1 Groups of type $\mathsf{A}_\ell(q)$ and ${}^2\mathsf{A}_\ell(q)$

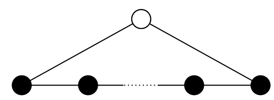
Write $n = \ell + 1$, and let $\mathbf{H} = \mathrm{SL}_n(\boldsymbol{k})$. Let $\sigma_{+1} = F_q$ be the Frobenius map on $\mathbf{H}$, and let σ_{-1} be the twisted automorphism $a \mapsto F_q(a^{-t})^{w_0}$, with $w_0 = \begin{pmatrix} & & 1 \\ & \cdot^{\cdot^{\cdot}} & \\ 1 & & \end{pmatrix} \in \mathrm{GL}_n(\boldsymbol{k})$, as in Example 6.2.7.

Symbol	Meaning
$\lambda \vdash n$	$\lambda = (\lambda_1, \ldots, \lambda_r)$ is a partition of n
$\lambda^* = (\lambda_1^*, \ldots, \lambda_m^*)$	The dual partition of λ $\lambda_i^* = \lvert\{j : \lambda_j \geq m + 1 - j\}\rvert$
$\lVert\lambda\rVert_1$	The sum of λ, $\lVert\lambda\rVert_1 = \sum_j \lambda_j$
$\lVert\lambda\rVert_2$	The 2-norm of λ, $\lVert\lambda\rVert_2 = \left(\sum_j \lambda_j^2\right)^{1/2}$
$\boldsymbol{l}(\lambda)$	The length of λ
$o(\lambda)$	Number of odd parts in λ

Table 8.1: Partition notation

For $\iota \in \{\pm 1\}$, let $H_\iota = \mathbf{H}^{\sigma_\iota}$. That is, $H_{+1} = \mathrm{SL}_n(\mathbb{F}_q)$ and $H_{-1} = \mathrm{SU}_n(\mathbb{F}_{q^2}, \mathbb{F}_q) \subseteq \mathrm{GL}_n(\mathbb{F}_{q^2})$, the special unitary group. The algebraic group $\mathbf{H}$ is self-dual, with each of the endomorphisms σ_ι being identifiable with its dual endomorphism. The Lie-algebra of $\mathbf{H}$ is $\mathbf{h} = \mathfrak{sl}_n(\boldsymbol{k})$, the Lie-algebra of traceless $n \times n$ matrices over $\mathbb{F}_q$, and its corresponding σ_ι-fixed algebras are, respectively for $\iota = +1$ and $\iota = -1$, the Lie-algebra $\mathfrak{h}_{+1} = \mathfrak{sl}_n(\mathbb{F}_q)$ of traceless $n \times n$ matrices over $\mathbb{F}_q$, and $\mathfrak{h}_{-1} = \mathfrak{su}_n(\mathbb{F}_{q^2}, \mathbb{F}_q)$ of traceless $n \times n$ matrices over $\mathbb{F}_{q^2}$ which act as anti-hermitian operators with respect to an F_q-sesquilinear form on an n-dimensional $\mathbb{F}_{q^2}$-vector space.

The extended Dynkin diagram of $\mathbf{H}$ is



(8.3)

where the hollow node corresponds to $-\alpha_0$, where $\alpha_0 = \sum_{\alpha \in S} \alpha$ is the highest root with respect to a base S of the root system Φ of $\mathbf{H}$. By Deriziotis's Criterion [30, § 2.15], up to conjugation by an element of the Weyl group W of H, all subsystems of Φ which occur as the root system of the centralizer of an element of $\mathbf{H}$ are given by choosing a base included in $S \cup \{-\alpha_0\}$. The isolated subsystems of Φ are therefore given by deletion of a single node in (8.3). In the present case all subsystems thus obtained are of type A_ℓ as well.

Consequently, our interest in this section is to compare the nilpotent adjoint class function $\epsilon^{\mathrm{nil}}_{\mathfrak{h}_\iota}$ of $\mathfrak{h}_\iota$ with the unipotent representation zeta function $\zeta^{\mathrm{unip}}_{H_\iota}$ of H_ι. Namely, we prove

Proposition 8.1.1. *There exists a natural number $c \in \mathbb{N}$ such that, for any prime p greater than n and any finite field $\mathbb{F}_q$ of characteristic p,*

$$\epsilon^{\mathrm{nil}}_{\mathfrak{sl}_n(\mathbb{F}_q)} \sim_{(c,q)} \zeta^{\mathrm{unip}}_{\mathrm{SL}_n(\mathbb{F}_q)} \quad \textit{and} \quad \epsilon^{\mathrm{nil}}_{\mathfrak{su}_n(\mathbb{F}_{q^2}, \mathbb{F}_q)} \sim_{(c,q)} \zeta^{\mathrm{unip}}_{\mathrm{SU}_n(\mathbb{F}_{q^2}, \mathbb{F}_q)}.$$

8.1.1 Nilpotent adjoint classes of $\mathfrak{h}_{\pm 1}$

The computation of nilpotent adjoint classes in $\mathfrak{h}_{\pm 1}$, as well as all other classical Lie-algebras over $\mathbb{F}_q$, was carried out in [51, Ch. 4], and, independently and in greater generality, in [60]. We briefly recall below the relevant results arising from the analysis carried out by Springer and Steinberg, in order to prove the following.

Lemma 8.1.2. *Let $\mathfrak{h}_{+1} = \mathfrak{sl}_n(\mathbb{F}_q)$ and $\mathfrak{h}_{-1} = \mathfrak{su}_n(\mathbb{F}_{q^2}, \mathbb{F}_q)$. There exist positive integers $c_\lambda^\iota \in \mathbb{N} \cap [0, n]$, for any partition $\lambda \vdash n$ and $\iota \in \{\pm 1\}$, such that*

$$\epsilon_{\mathfrak{h}_\iota}(s) = \sum_{[x] \in \mathrm{Ad}(H_\iota) \backslash \mathfrak{h}_\iota} |\mathfrak{h}_\iota : \mathbf{C}_{\mathfrak{h}_\iota}(x)|^{-s/2} = \sum_{\lambda \vdash n} c_\lambda^\iota q^{-\frac{1}{2}\left(n^2 - \|\lambda^*\|_2^2\right)s}, \quad \textit{for } \iota \in \{\pm 1\} \tag{8.4}$$

where λ^* denotes the dual partition of λ.

Proof. Fix $\iota \in \{\pm 1\}$. Let $\mathbf{V}$ be an n-dimensional vector space over $\mathbb{F}_q$ and let $x \in \mathbf{h}$ be a nilpotent element which is fixed under σ_ι, which is considered as a traceless operator on $\mathbf{V}$. Note that the assumption $p > n$ implies that x is scalar if and only if $x = 0$. Considered as a $\boldsymbol{k}[x]$-module decomposes as a direct sum $\mathbf{V} = \bigoplus_{j=1}^m \mathbf{V}_{\lambda_j}$, where $\mathbf{V}_{\lambda_j} = x^{h-\lambda_j}\mathbf{V}$ and h is minimal such that $x^h = 0$. The sequence $\lambda = (\lambda_1, \dots, \lambda_m)$ comprises a partition of n, and is determined, up to permutation, by x, and any partition of n arises in this manner from some σ_ι-nilpotent element. The centralizer of x in $\mathrm{GL}_n(\mathbb{F}_q)$ is of dimension $\|\lambda^*\|_2^2$ (see [51, IV, 1.7-1.8]) and any two nilpotent elements giving rise to the partition λ lie in the same $\mathrm{Ad}(\mathrm{GL}_n(\mathbb{F}_q))$-adjoint class, which we denote $C_\lambda \subseteq \mathbf{h}$. Restricting to $\mathbf{H}$, the centralizer of x in $\mathbf{H}$ acts transitively on the adjoint class of x, and satisfies $|\mathbf{C}_{\mathbf{H}}(x) : \mathbf{C}_{\mathbf{H}}(x)^\circ| \leq n$; see [51, IV, 1.10]. It follows, by Lemma 6.1.4, that, for any $\lambda \vdash n$, there exists $c_\lambda \in \mathbb{N} \cap [1, n]$ such that the set $(C_\lambda)^{\sigma_\iota}$ decomposes into c_λ-many $\mathrm{Ad}(H_\iota)$-classes. Finally, the centralizer of x in $\mathfrak{h}_\iota$ is an $\mathbb{F}_q$-vector space of dimension $\|\lambda^*\|_2^2 - 1$, hence $|\mathfrak{h}_\iota : \mathbf{C}_{\mathfrak{h}_\iota}(x)| = q^{n^2 - \|\lambda^*\|_2^2}$, as wanted. □

8.1.2 Unipotent characters of $H_{\pm 1}$

The unipotent characters of both H_{+1} and H_{-1} are parametrized by partitions of n, such that for any $\lambda = (\lambda_1, \dots, \lambda_r) \vdash n$ there exists a unique unipotent character $\chi_\lambda^\iota \in \mathrm{Irr}(H_\iota)$ such that $\chi_\lambda^\iota(1) = u_\lambda^\iota(q)$ for

$$u_\lambda^\iota(t) = \frac{(t-\iota)(t^2-\iota^2)\cdots(t^n-\iota^n) \cdot \prod_{1 \leq i_1 < i_2 \leq r}\left(t^{\lambda_{i_1}+i_1-1} - \iota^{\lambda_{i_1}+\lambda_{i_2}+i_1+i_2} t^{\lambda_{i_2}+i_2-1}\right)}{t^{\binom{r-1}{2}+\binom{r-2}{2}+\cdots} \prod_{i=1}^r \prod_{k=1}^{\lambda_i+i-1}(t^k - \iota^k)} \tag{8.5}$$

and all unipotent characters of H_ι are obtained in this manner (see [13, § 13.8]). Note that the rational functions u_λ^ι attain integer values at infinitely many prime powers, and, consequently, are polynomial.

In particular, we have that

$$\zeta_{H_\iota}^{\mathrm{unip}}(s) = \sum_{\lambda \vdash n} u_\lambda^\iota(q)^{-s}, \quad \text{for } \iota \in \{\pm 1\}. \tag{8.6}$$

We make the following observation.

Lemma 8.1.3. *Let* $\lambda = (\lambda_1, \dots, \lambda_r) \vdash n$ *and* $\iota \in \{\pm 1\}$. *Then* $\deg u_\lambda^\iota = \frac{1}{2}\left(n^2 - \|\lambda\|_2^2\right)$.

Proof. The proof is by direct computation, using some auxiliary lemmas. We have that

$$\deg\left((t-\iota)\cdots(t^n-\iota^n)\right) = 1+2+\cdots+n = \binom{n+1}{2} \tag{8.7}$$

$$\deg\left(t^{\binom{r-1}{2}+\binom{r-2}{2}+\cdots}\right) = \sum_{i=1}^{r}\binom{r-1}{2} = \binom{r}{3}, \tag{8.8}$$

by the hockey-stick identity, and, letting $\mu = (\mu_1, \dots, \mu_r)$ be defined by $\mu_i = \lambda_i + i - 1$,

$$\deg\left(\prod_{i=1}^{r}\prod_{k=1}^{\lambda_i+i-1}(t^k - \iota^k)\right) = \sum_{i=1}^{r}\left(\sum_{k=1}^{\mu} k\right) = \sum_{i=1}^{r}\binom{\mu_i+1}{2}. \tag{8.9}$$

Furthermore, by Lemma B.1.1, we have that

$$\deg\left(\prod_{1\le i_1<i_2\le r}\left(t^{\lambda_{i_1}+i_1-1} - \iota^{\lambda_{i_1}+\lambda_{i_2}+i_1+i_2}t^{\lambda_{i_2}+i_2-1}\right)\right) = \sum_{i=1}^{r}(i-1)\mu_i. \tag{8.10}$$

Combining equations (8.7) through (8.10) and the definition of u_λ^ι, we have that

$$\begin{aligned}
\deg u_\lambda^\iota &= \binom{n+1}{2} + \sum_{i=1}^{r}(i-1)\mu_i - \binom{r}{3} - \sum_{i=1}^{r}\binom{\mu_i+1}{2} \\
&= \binom{n+1}{2} - \binom{r}{3} - \|\mu\|_1 - \sum_{i=1}^{r}\left(\binom{\mu_i+1}{2} - i\mu_i\right) \\
&= \frac{n^2+n}{2} - \binom{r}{3} - n - \binom{r}{2} - \left(\frac{1}{2}\|\lambda\|_2^2 - \frac{n}{2} - \binom{r+1}{3}\right) \\
&= \frac{1}{2}\left(n^2 - \|\lambda\|_2^2\right),
\end{aligned}$$

where the penultimate equality is prove in Lemma B.1.3. □

Proof of Proposition 8.1.1. Let $C \subseteq \mathbb{N}$ be a finite set containing all coefficients of all polynomials u_λ^ι of (8.5) and all coefficients c_λ^ι of Lemma 8.1.2, for all $\iota \in \{\pm 1\}$ and $\lambda \vdash n$, and let $c \in \mathbb{N}$ be divisible by all elements of C. As seen in Lemma 8.1.2, for any $p > n$, it holds that

$$\epsilon_{\mathfrak{h}_\iota}(s) = \sum_{\lambda \vdash n} c_{\lambda^*}^\iota q^{-\frac{1}{2}(n^2-\|\lambda\|_2^2)}, \quad \text{for } \iota \in \{\pm 1\}.$$

Note that the replacement of λ with λ^* has no fact on the equation above. Furthermore, we have that

$$\zeta_{H_\iota}(s) = \sum_{\lambda \vdash n} u_\lambda^\iota(q)^{-s}, \quad \text{with } \deg u_\lambda^\iota = \frac{1}{2}(n^2 - \|\lambda^*\|_2^2),$$

by Lemma 8.1.3. It follows from the definition of $\mathscr{D}_{c,q}$ and the (c,q)-relation that $\zeta_{H_\iota}^{\mathrm{unip}}, \epsilon_{\mathfrak{h}_\iota}^{\mathrm{nil}} \in \mathscr{D}_{c,q}$ and

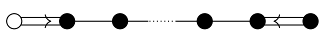
$$\epsilon_{\mathfrak{h}_\iota}^{\mathrm{nil}} \sim_{(c,q)} \zeta_{H_\iota}^{\mathrm{unip}}(s),$$

for any $\iota \in \{\pm 1\}$. □

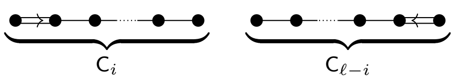
8.2 Groups of type C_ℓ

In this section we consider the group $\mathbf{H} = \mathrm{Sp}_{2\ell}(\boldsymbol{k})$ of automorphisms preserving a symplectic form on a 2ℓ-dimensional vector space with $\sigma = F_q$ the Frobenius map on $\mathbf{H}$. Then $H = \mathbf{H}^\sigma = \mathrm{Sp}_{2\ell}(\mathbb{F}_q)$ is the group of automorphism of the restriction of ambient symplectic form to a 2ℓ-dimensional $\mathbb{F}_q$-vector subspace. The dual algebraic group of $\mathbf{H}$ is $\mathbf{H}^* = \mathrm{SO}_{2\ell+1}(\boldsymbol{k})$. It is adjoint of type B_ℓ, and the dual Steinberg endomorphism σ^* of σ may be taken to be the Frobenius map on $\mathbf{H}^*$. Its Lie-algebra $\mathbf{h}^* = \mathfrak{so}_{2\ell+1}(\boldsymbol{k})$ may be identified with the Lie-algebra of antisymmetric endomorphisms with respect to a non-degenerate symmetric bilinear form on a $\boldsymbol{k}$-vector space of dimension $2\ell + 1$. The Lie-algebra $\mathfrak{h}^* = (\mathbf{h}^*)^{\sigma^*}$, of σ^*-fixed points, is $\mathfrak{so}_{2\ell+1}(\mathbb{F}_q)$, the Lie-algebra of antisymmetric endomorphisms of a $(2\ell + 1)$-dimensional vector space over $\mathbb{F}_q$.

The extended Dynkin diagram of $\mathbf{H}$ is


, (8.11)

where the hollow node represents the root $-\alpha_0$, where $\alpha_0 \in \Phi$ is the highest root respect to a fixed base S. By Deriziotis's Criterion [30, § 2.15], all subsystems of Φ which occur as the root system of a centralizer of an element of $\mathbf{H}$ admit a base which, up to conjugation by W, is a subset of $S \cup \{-\alpha_0\}$. The isolated subsystems are precisely those whose Dynkin diagram is given by deletion of a single node of (8.11), i.e. of the form



$(i = 0, \ldots, \lfloor \ell/2 \rfloor)$.

Therefore, the subgroups $\mathbf{H}_i = \mathrm{Sp}_{2i}(\boldsymbol{k}) \times \mathrm{Sp}_{2\ell-2i}(\boldsymbol{k})$ for $i = 1, \ldots, \lfloor \ell/2 \rfloor$ are representatives for the isomorphism classes of all groups $\mathbf{H}_\Sigma$ for $\Sigma \subseteq \Phi$ isolated (cf. [6, Example 4.10]).

Our interest in this section, consequently, is to compare the nilpotent adjoint zeta function $\epsilon^{\mathrm{nil}}_{\mathfrak{h}^*}$ of $\mathfrak{h}^* = \mathfrak{so}_{2\ell+1}(\mathbb{F}_q)$ with the finite Dirichlet series

$$\sum_{i=0}^{\lfloor \ell/2 \rfloor} \left(\frac{|H|_{p'}}{|H_i \times H_{\ell-i}|_{p'}} \right)^{-s} \zeta^{\mathrm{unip}}_{H_i \times H_{\ell-i}}(s) \tag{8.12}$$

where $H_i = \mathrm{Sp}_{2i}(\mathbb{F}_q) = \mathbf{H}_i^\sigma$, and H_0 is, by convention, the trivial group. Note that for any i, j, the equality $\zeta^{\mathrm{unip}}_{H_i \times H_j} = \zeta^{\mathrm{unip}}_{H_i} \cdot \zeta^{\mathrm{unip}}_{H_j}$ holds by the compatibility of unipotent characters with cartesian products (see [2, Proposition 3.5]). Also note that, is $\mathbf{H}$ is identified with the group of $2\ell \times 2\ell$ matrices over $\mathbb{F}_q$ satisfying the condition $g^t \mathbf{J} g = \mathbf{J}$, where $J = \left(\begin{smallmatrix} 0 & \mathbf{1}_\ell \\ -\mathbf{1}_\ell & 0 \end{smallmatrix} \right)$, then each of the subgroups $\mathbf{H}_i \times \mathbf{H}_{\ell-i}$ may be realized as the centralizer of the semisimple element

$$g_i = \mathrm{diag}(\underbrace{1, \ldots, 1}_{i \text{ entries}}, \underbrace{-1, \ldots, -1}_{\ell-i \text{ entries}}, \underbrace{1, \ldots, 1}_{i \text{ entries}}, \underbrace{-1, \ldots -1}_{\ell-i \text{ entries}}) \in \mathbf{H},$$

and hence the root subsystems Σ_i of the subgroups $\mathbf{H}_i \times \mathbf{H}_{\ell-i}$ are ϕ_σ-stable and $\boldsymbol{\tau}^{\boldsymbol{i}}_H \neq 0$.

This comparison is carried out in two stages. To begin with, we consider the nilpotent adjoint classes in $\mathfrak{h}^* = \mathfrak{so}_{2\ell+1}(\mathbb{F}_q)$. Such classes are naturally parametrized by partitions $\lambda \vdash 2\ell + 1$ in which each even part occurs with even multiplicity. As discussed in [13, § 13.3], such partitions are in bijection with certain ordered pairs (ξ, ν) of partitions satisfying $\|\xi\|_1 + \|\nu\|_1 = \ell$. We call the partitions lying in the image of this bijection *partitions of type* B_ℓ (see Definition 8.2.5). This explicit bijection, which we outline in § 8.2.1, is a manifestation of the Springer correspondence, which relates the set of pairs (C, ψ), with $C \subseteq \mathbf{h}$ a nilpotent conjugacy class and ψ a character of a finite group associated to C, and the set of irreducible characters of the Weyl group W of $\mathrm{SO}_{2\ell+1}(\mathbb{F}_q)$, which are known to be parametrized by such partition pairs. Using this bijection, we show the following.

Lemma 8.2.1. *Let $\mathscr{A}_\ell$ denote the set of ordered pairs of partitions (ξ, ν) such that $\|\xi\|_1 + \|\nu\|_1 = \ell$. Assume that $\ell \leq 41$. There exist positive integers $c_{(\xi,\nu)} \in \mathbb{N} \cap [1, 2^{2\ell+1}]$, for any $(\xi, \nu) \in \mathscr{A}_\ell$, such that*

$$\epsilon^{\mathrm{nil}}_{\mathfrak{h}^*} = \sum_{\substack{(\xi,\nu)\in\mathscr{A}_\ell \\ \text{of type } \mathsf{B}_\ell}} c_{(\xi,\nu)} \cdot q^{-g_\ell(\nu^*,\xi^*)s} \quad \textit{where} \quad g_\ell(\xi,\nu) = \ell^2 + \ell - \|\xi\|_1 - \|\xi\|_2^2 - \|\nu\|_2^2 .$$

Remark 8.2.2. The assumption $\ell \leq 41$ in Lemma 8.2.1 is most probably superfluous. The formula given above relies on certain combinatorial identities which, to date I have only been able to prove directly for a subset of $\mathscr{A}_\ell$, viz. *special* partition pairs (see Definition 8.2.5), for any $\ell \in \mathbb{N}$; see Lemma B.2.2 in Appendix B. Computer assisted computations have, however, demonstrated the equality to hold for *all* elements of $\mathscr{A}_\ell$ of type B_ℓ, for any $\ell \leq 41$, and it is highly likely that it holds in complete generality.

Following this step, we turn to consider the unipotent characters of the groups H_i. Recall that the dimensions of unipotent characters of a finite group of Lie-type are given by evaluation at q of certain polynomials, which, in the case of H_i are parametrized by the so-called *symbols* of rank i. Given such a symbol $\binom{\lambda}{\mu}$ (see § 8.2.2), let $u^i_{\binom{\lambda}{\mu}} \in \mathbb{Q}[t]$ denote the corresponding polynomial. In § 8.2.2 we consider the unipotent characters of the groups H_i and show that degrees of the polynomials $u^i_{\binom{\lambda}{\mu}}$ remains constant as $\binom{\lambda}{\mu}$ ranges over symbols lying in a fixed family (see [13, § 12.3]). Moreover, we prove the following.

Lemma 8.2.3. *Let $i \in \mathbb{N}$. Lusztig families of unipotent characters of $H_i = \mathrm{Sp}_{2i}(\mathbb{F}_q)$ may be parametrized by special partition pairs in $\mathscr{A}_i$ (see Definition 8.2.5), such that if $\mathbf{F}_{(\xi,\nu)}$ denotes the family associated to a special pair (ξ, ν), and $u^i_{\binom{\lambda}{\mu}} \in \mathbb{Z}[t]$ is the degree polynomial associated with a symbol $\binom{\lambda}{\mu}$ corresponding to a character $\chi = \chi_{\binom{\lambda}{\mu}} \in \mathbf{F}_{(\xi,\nu)}$, then*

$$\deg u^i_{\binom{\lambda}{\mu}} = i^2 + i - \|\xi\|_1 - \|\xi\|_2^2 - \|\nu\|_2^2 .$$

In particular

$$\zeta^{\mathrm{unip}}_{H_i}(s) = \sum_{\substack{(\xi,\nu)\in\mathscr{A}_i\\ \textit{special}}} \left(\sum_{\chi=\chi_{\binom{\lambda}{\mu}}\in\mathbf{F}_{(\xi,\nu)}} u^i_{\binom{\lambda}{\mu}}(q)^{-s} \right).$$

Note that the degree of $u^i_{\binom{\lambda}{\mu}}$ in Lemma 8.2.3 is precisely the value $g_i(\xi,\nu)$, where g_i is as defined in Lemma 8.2.1.

Using Lemma 8.2.3, and making some further observations regarding the functions $\zeta^{\mathrm{unip}}_{H_i}\cdot\zeta^{\mathrm{unip}}_{H_{\ell-i}}$, we then deduce the following.

Proposition 8.2.4. *There exist a natural number* c *and a prime* p_0 *such that, for any* $p \geq p_0$*, and any finite field* $\mathbb{F}_q$ *of characteristic* p*,*

$$\epsilon_{\mathfrak{so}^{\mathrm{nil}}_{2\ell+1}}(s) \sim_{(c,q)} \sum_{i=0}^{\lfloor \ell/2\rfloor} \left(\frac{|\mathrm{Sp}_{2\ell}(\mathbb{F}_q)|_{p'}}{\left|\mathrm{Sp}_{2i}(\mathbb{F}_q)) \times \mathrm{Sp}_{2(\ell-i)}(\mathbb{F}_q)\right|_{p'}} \right)^{-s} \zeta_{\mathrm{Sp}_{2i}(\mathbb{F}_q))\times\mathrm{Sp}_{2(\ell-i)}(\mathbb{F}_q)}(s), \tag{8.13}$$

where $\mathrm{Sp}_0(\mathbb{F}_q)$ *is, by convention, the trivial group.*

8.2.1 Nilpotent adjoint classes of $\mathfrak{h}$

Nilpotent adjoint orbits of $\mathfrak{h}^* = \mathfrak{so}_{2\ell+1}(\mathbb{F}_q)$ are classified in terms of partitions $\lambda \vdash 2\ell+1$, whereby a nilpotent adjoint class C gives rise to a partition λ if its elements, considered as endomorphisms of $V = {\mathbb{F}_q}^{2\ell+1}$, have elementary divisors given by λ, i.e. $V = \bigoplus_{j\geq 0} V_{\lambda_j}$ as an $\mathbb{F}_q[x]$-module, where the V_{λ_j} are as in Lemma 8.1.2. In this case, for any $x \in C$, the algebraic group $\mathbf{C}_{\mathbf{H}}(x)$ has dimension $\frac{1}{2}\left(\|\lambda^*\|_2^2 - o(\lambda)\right)$, where $o(\lambda)$ denotes the number of odd parts in λ (see [51, IV, 2.25 and 2.28]). Furthermore, given such $\lambda \vdash 2\ell+1$, the number of different conjugacy classes which contain an element whose elementary divisors are given by λ is bounded above by $2^{o(\lambda)}$ (see [51, IV, 2.26]). In particular, assuming that $\mathrm{char}(\mathbb{F}_q) \neq 2$ and hence $\dim \mathbf{C}_{\mathbf{H}}(x) = \dim \mathbf{C}_{\mathbf{h}}(x)$ (see [4]), we obtain

$$\epsilon^{\mathrm{nil}}_{\mathfrak{h}^*}(s) = \sum_{\substack{\lambda\vdash 2\ell+1\\ |\{j:\lambda_j=2k\}| \text{ is even}\\ \text{for all } k\in\mathbb{N}}} c_\lambda \cdot q^{\frac{1}{2}\left(2\ell^2+\ell-\frac{1}{2}(\|\lambda\|_2^2-o(\lambda))\right)s}, \tag{8.14}$$

where $c_\lambda \in \mathbb{N}\cap[1,2^{2\ell+1}]$, for any λ. Note that $2\ell^2+\ell = \dim \mathrm{SO}_{2\ell+1}(\boldsymbol{k})$.

Let us recall the bijection, described in [13, § 13.3], between partitions $\lambda \vdash 2\ell+1$ in which all even parts occur with even multiplicities and the set $\mathscr{A}_\ell$ of partition pairs (ξ,ν) with $\|\xi\|_1 + \|\nu\|_1 = \ell$. Recall that, according to the Springer correspondence [50], there exists a bijection between pairs (C,ψ), in which C is a nilpotent adjoint class in $\mathbf{h}^*$ and ψ is a character of the finite group $\mathbf{C}_{\mathbf{H}^*}(x)/\mathbf{C}_{\mathbf{H}^*}(x)^\circ$, and representations of the Weyl group W of $\mathbf{H}^*$, which are obtained from the action of W on the top-dimensional cohomologies of a variety $\mathcal{B}_x$ associated with the class C. In more matter-of-factly terms, restricting this map to the set of pairs $(C, \mathbf{1}_{\mathbf{C}_{\mathbf{H}^*}(x)/\mathbf{C}^\circ_{\mathbf{H}^*}(x)})$ and recalling that representations of W are parametrized by the elements of $\mathscr{A}_\ell$, we obtain the desired bijection.

To construct this bijection, let $\lambda = (\lambda_1, \ldots, \lambda_{2m+1}) \vdash 2\ell + 1$ have all even parts occurring with even multiplicities, and note that $\boldsymbol{l}(\lambda)$ is necessarily odd. Define a partition $\widetilde{\lambda} \vdash 2\ell + 1 + \binom{2m}{2}$ by $\widetilde{\lambda}_j = \lambda_j + (j-1)$, for $j = 1, \ldots, 2m+1$. Arguing by induction on ℓ, one verifies that $\widetilde{\lambda}$ has $m+1$ odd parts and m even parts. Let $\widetilde{x} = (\widetilde{x}_1, \ldots, \widetilde{x}_{m+1})$ and $\widetilde{y} = (\widetilde{y}_1, \ldots, \widetilde{y}_m)$ be such that the odd parts (resp. the even parts) of $\widetilde{\lambda}$ are $\{2\widetilde{x}_j + 1 : j = 1, \ldots, m+1\}$ (resp. $\{\widetilde{y}_j : j = 1, \ldots, m\}$). Define $x = (x_1, \ldots, x_{m+1})$ and $y = (y_1, \ldots, y_m)$ by $x_j = \widetilde{x}_j - (j-1)$ and $y_j = \widetilde{y}_j - (j-1)$, and let ξ and ν be the partition obtained by taking the non-zero terms of x and y, with the same multiplicities. By computing $\|\widetilde{\lambda}\|_1$ in two ways, one easily verifies that indeed $\|\xi\|_1 + \|\nu\|_1 = \ell$. Also note that the sequences x and y necessarily satisfy the inequalities

$$x_1 \leq y_1 \leq x_2 + 2 \leq y_2 + 2 \leq \ldots \leq y_m + 2(m-1) \leq x_{m+1} + 2m. \tag{8.15}$$

This condition characterizes the image of the map $\lambda \mapsto (\xi, \nu)$ just constructed; its inverse may be constructed by reversing the construction above. It is also worth noting that all other representations of W which are associated to the adjoint class corresponding to λ may also be described in terms of the sequences x and y; for further information, we refer to [13, § 13.2 and 3].

We require some definitions regarding the set $\mathscr{A}_\ell$.

Definition 8.2.5. Let $(\xi, \nu) \in \mathscr{A}_\ell$ be a partition pair.

1. We call a pair (x, y) of finite non-decreasing sequence of length $m+1$ and m, for some $m \in \mathbb{N}$ respectively, an *associated sequence pair* to (ξ, ν), if all parts of ξ (resp. of ν) occur in x (resp. in y) with the same multiplicities, and all other parts of x and y are zero.

2. The pair (ξ, ν) is said to be *of type* B_ℓ if there exists an associated sequence pair (x, y) to (ξ, ν) which satisfies the condition of (8.15).

3. The pair (ξ, ν) is said to be *special* if there exists an associated sequence pair (x, y) of (ξ, ν) such that

$$x_1 \leq y_1 \leq x_2 + 1 \leq y_1 + 1 \leq \ldots \leq y_m + (m-1) \leq x_{m+1} + m. \tag{8.16}$$

Note that special partition pairs are, in particular, of type B_ℓ. Also, note that the definitions above are independent of the choice of associated sequence (x, y). Furthermore, the discussion in the paragraph above shows that the set of partition $\lambda \vdash 2\ell + 1$ arising from nilpotent conjugacy classes of $\mathfrak{h}^*$ is in bijection with the set of partition pairs in $\mathscr{A}_\ell$ of type B_ℓ.

The set $\mathscr{A}_\ell$ is endowed with an involutive map $\dagger : \mathscr{A}_\ell \to \mathscr{A}_\ell$, defined by $(\xi, \nu)^\dagger = (\nu^*, \xi^*)$, where ν^* and ξ^* are the dual partitions of ν and ξ, respectively.

Lemma 8.2.6. *Let $(\xi, \nu) \in \mathscr{A}_\ell$. Then (ξ, ν) is special if and only if $(\xi, \nu)^\dagger = (\nu^*, \xi^*)$ is special.*

Proof. See Lemma B.2.1. $\square$

We are now ready to complete the proof of Lemma 8.2.1.

Proof of Lemma 8.2.1. By (8.14), it suffices to prove that the equality

$$\|\lambda^*\|_2^2 - o(\lambda) = 4\,\|\xi^*\|_2^2 + 4\,\|\nu^*\|_2^2 + 4\,\|\nu^*\|_1 - 2\ell \tag{8.17}$$

holds for any $\lambda \vdash 2\ell + 1$ arising from a nilpotent adjoint class, with $(\xi, \nu) \in \mathscr{A}_\ell$ the associated partition pair.

The proof of (8.17) follows in two steps. Firstly, we note the equality

$$\|\lambda^*\|_2^2 - \left(\|\lambda\|_2^2 - 4\left(\|\xi\|_2^2 + \|\nu\|_2^2 + \|\xi\|_1 - \|\nu\|_1\right)\right) = 4\,\|\xi^*\|_2^2 + 4\,\|\nu^*\|_2^2 + 4\,\|\nu^*\|_1 - 2\ell. \tag{8.18}$$

which is proved in the following paragraph. Secondly we verify that the value

$$\|\lambda\|_2^2 - 4\left(\|\xi\|_2^2 + \|\nu\|_2^2 + \|\xi\|_1 - \|\nu\|_1\right)$$

does indeed give the number of odd parts of λ. This is proved for the case where the pair (ξ, ν) is special in Lemma B.2.2, and has been verified using MathLab for all partitions in $\mathscr{A}_\ell$ of type B_ℓ, for $\ell = 1, \dots, 149$.

To prove (8.18), we compute the value of $\|\widetilde{\lambda}\|_2^2$ in two ways. We freely use the notation set up in the construction on page 116. By definition, we have that $\widetilde{\lambda} = (\widetilde{\lambda}_1, \dots, \widetilde{\lambda}_{2m+1})$, where $\widetilde{\lambda}_j = \lambda_j + (j-1)$. Thus,

$$\begin{aligned}
\|\widetilde{\lambda}\|_2^2 &= \sum_{j=1}^{2m+1} (\lambda_j + (j-1))^2 \\
&= \|\lambda\|_2^2 + 2\sum_{j=1}^{2m+1} j\lambda_j - 2\,\|\lambda\|_1 + \sum_{j=1}^{2m+1} (j-1)^2 \\
&= \|\lambda\|_2^2 - \|\lambda^*\|_2^2 + (4m+1)\cdot \underbrace{\|\lambda\|_1}_{=2\ell+1} + \frac{2m(2m+1)(4m+1)}{6},
\end{aligned} \tag{8.19}$$

where the final equality invokes Lemma B.1.2. On the other hand, we have that

$$\begin{aligned}
\|\widetilde{\lambda}\|_2^2 &= \sum_{j=1}^{m+1} (2\widetilde{x}_j + 1)^2 + \sum_{j=1}^{m} (2\widetilde{y}_j)^2 \\
&= 4\,\|\widetilde{x}\|_2^2 + 4\,\|\widetilde{x}\|_1 + (m+1) + 4\,\|\widetilde{y}\|_2^2.
\end{aligned} \tag{8.20}$$

Using the definition of the sequences x and y and of the pair (ξ, ν), we have that

$$\begin{aligned}
\|\widetilde{x}\|_2^2 = \sum_{j=1}^{m+1} (x_j + (j-1))^2 &= \|\xi\|_2^2 + 2\sum_j jx_j - 2\,\|\xi\|_1 + \sum_{j=1}^{m+1} (j-1)^2 \\
&= \|\xi\|_2^2 - \|\xi^*\|_2^2 + (2m+1)\,\|\xi\|_1 + \frac{m(m+1)(2m+1)}{6},
\end{aligned}$$

and, likewise,

$$\|\widetilde{y}\|_2^2 = \|\nu\|_2^2 - \|\nu^*\|_2^2 + (2m-1)\,\|\nu\|_1 + \frac{m(m-1)(2m-1)}{6}.$$

Moreover, $\|\widetilde{x}\|_1 = \|\xi\|_1 + \binom{m+1}{2}$. Applying the last three equations into (8.20) and comparing with (8.19), we deduce that

$$\begin{aligned}
\|\lambda\|_2^2 - \|\lambda^*\|_2^2 + (2\ell+1)\,(4m+1) + \frac{2m(2m+1)(4m+1)}{6} = \\
=&4\left(\|\xi\|_2^2 - \|\xi^*\|_2^2 + \|\nu\|_2^2 - \|\nu^*\|_2^2 + 2\,\|\xi\|_1 - \|\nu\|_1\right) + 8m\cdot\left(\|\nu\|_1 + \|\xi\|_1\right) \\
&+ m + 1 + 4\binom{m+1}{2} + 4m\frac{m(m+1)(2m+1)}{6} + 4m\frac{m(m-1)(2m-1)}{6}.
\end{aligned}$$

Comparing the right and left hands of the above equation, one easily verifies that all terms depending on m cancel out, and thus

$$\|\lambda\|_2^2 - \|\lambda^*\|_2^2 + 2\ell = 4\left(\|\xi\|_2^2 - \|\xi^*\|_2^2 + \|\nu\|_2^2 - \|\nu^*\|_2^2 + 2\,\|\xi\|_1 - \|\nu\|_1\right).$$

Rearranging the terms of the above equality, recalling that $\|\xi\|_1 + \|\nu\|_1 = \ell$, this completes the proof of Lemma 8.2.1. □

8.2.2 Unipotent characters of $\mathrm{Sp}_{2i}(\mathbb{F}_q)$

Fix $i \in \mathbb{N}$. In this section we consider the unipotent characters of $H_i = \mathrm{Sp}_{2i}(\mathbb{F}_q)$, and prove Lemma 8.2.3. As discussed in [13, § 13.8], unipotent characters of H_i are parametrized by symbols of the form

$$\binom{\lambda}{\mu} = \begin{pmatrix} \lambda_1 & & \lambda_2 & & \lambda_3 & & \dots & & \lambda_a \\ & \mu_1 & & \mu_2 & & \dots & & \mu_b & \end{pmatrix},$$

where $0 \le \lambda_1 < \lambda_2 < \ldots < \lambda_a$, $0 \le \mu_1 < \ldots < \mu_b$, $a-b$ is odd an positive, and $\{\lambda_1, \mu_1\} \neq \{0\}$. Given such a symbol, the rank of $\binom{\lambda}{\mu}$ is defined to be

$$\mathrm{rk}\binom{\lambda}{\mu} = \|\lambda\|_1 + \|\mu\|_1 - \left(\frac{a+b-1}{2}\right)^2. \tag{8.21}$$

The unipotent characters of H_i are in bijection with the set of symbols of rank i, where the dimension of the character corresponding to a symbol $\binom{\lambda}{\mu}$ is given by $u^i_{\binom{\lambda}{\mu}}(q)$, where $u^i_{\binom{\lambda}{\mu}}(t)$ is the polynomial

$$\frac{(t^2-1)(t^4-1)\cdots(t^{2i}-1)\prod_{j_1<j_2}(t^{\lambda_{j_1}} - t^{\lambda_{j_2}})\prod_{k_1<k_2}(t^{\mu_1} - t^{\mu_2})\prod_{j,k}(t^{\lambda_j} + t^{\mu_k})}{(a+b-1)t^{\binom{a+b-2}{2}+\binom{a+b-4}{2}+\cdots}\prod_j\prod_{k=1}^{\lambda_j}(t^{2k}-1)\prod_j\prod_{k=1}^{\mu_j}(t^{2k}-1)}; \tag{8.22}$$

see [13, p. 466]. As mentioned in [13, p. 468], two unipotent characters lie in the same family if and only their symbols contain the same values with the same multiplicities. In particular, it follows that any family of unipotent characters contains a *unique* character corresponding to a symbol of the form

$$\begin{pmatrix} \lambda_1 & & \lambda_2 & & \dots & & \lambda_{m+1} \\ & \mu_1 & & \dots & & \mu_m & \end{pmatrix},$$

such that $\lambda_1 \leq \mu_1 \leq \lambda_2 \leq \ldots \leq \mu_m \leq \lambda_{m+1}$. Such a symbol is called a *special* symbol. Given a special symbol $\binom{\lambda}{\mu}$ we define finite non-decreasing sequences $x = (x_1, \ldots, x_{m+1})$ and $y = (y_1, \ldots, y_m)$ by $x_j = \lambda_j - (j-1)$ and $y_j = \mu_j - (j-1)$, and let ξ and ν be the partitions defined by the non-zero parts of x and y, respectively. Note that, by (8.21),

$$\|\xi\|_1 + \|\nu\|_1 = \|\lambda\|_1 - \binom{m+1}{2} + \|\mu\|_1 - \binom{m}{2} = \operatorname{rk}\binom{\lambda}{\mu},$$

so that $(\xi, \nu) \in \mathscr{A}_i$, and, by Definition 8.2.5, (ξ, ν) is special. Conversely, given a special pair $(\xi, \nu) \in \mathscr{A}_i$, a symbol $\binom{\lambda}{\mu}$ is defined by letting (x, y) be an associated sequence pair to (ξ, ν) such that the first entries of x and y are not both zero, and define $\lambda_j = x_j + (j-1)$ and $\mu_j = y_j + (j-1)$.

Notation 8.2.7. Given a special pair $(\xi, \nu) \in \mathscr{A}_i$, we write $\mathbf{F}_{(\xi,\nu)} \subseteq \operatorname{Irr}(H^i)$ for the family of unipotent characters of H^i containing the special symbol $\binom{\lambda}{\mu}$ associated to (ξ, ν) as above.

Proof of Lemma 8.2.3. By the discussion above, to show that the degrees of the polynomials $u^i_{\binom{\lambda}{\mu}}$ are constant as $\binom{\lambda}{\mu}$ ranges over the symbols associated with characters in a given family $\mathbf{F}$, it is sufficient to show that $\deg u^i_{\binom{\lambda}{\mu}}$ is dependent only on the values occurring in the sequence $\eta = (\eta_1, \ldots, \eta_{a+b}) = (\lambda_1, \ldots, \lambda_a, \mu_1, \ldots \mu_b)$. Inspecting the expression (8.22), it is sufficient to show that the degree of the factor $\prod_{j_1<j_2}(t^{\lambda_{j_1}} - t^{\lambda_{j_2}}) \prod_{k_1<k_2}(t^{\mu_1} - t^{\mu_2}) \prod_{j,k}(t^{\lambda_j} + t^{\mu_k})$ is dependent only on the values of η and not on their order or their partition into the sub-sequences λ and μ. Indeed, applying Lemma B.1.1, we have that

$$\begin{aligned}
\deg &\left(\prod_{j_1<j_2}(t^{\lambda_{j_1}} - t^{\lambda_{j_2}}) \prod_{k_1<k_2}(t^{\mu_1} - t^{\mu_2}) \prod_{j,k}(t^{\lambda_j} + t^{\mu_k})\right) \\
&= \sum_{j=1}^{a}(j-1)\lambda_j + \sum_{k=1}^{b}(k-1)\mu_k + \sum_{j,k} \max\{\lambda_j, \mu_k\} \\
&= \sum_{1\leq j<k\leq a+b} \max\{\eta_j, \eta_k\},
\end{aligned}$$

which is clearly determined by η.

It follows that in order to compute the degrees of the polynomials $u^i_{\binom{\lambda}{\mu}}$ it is sufficient to consider the case where $\binom{\lambda}{\mu}$ is a special symbol. We first note the following equalities, which hold regardless of whether $\binom{\lambda}{\mu}$ is special.

$$\deg\left((t^2-1)(t^4-1)\cdots(t^{2i}-1)\right) = i(i+1), \tag{8.23}$$

$$\deg\left(t^{\binom{2m-1}{2}+\binom{2m-3}{2}+\cdots}\right) = \frac{m(m-1)(4m+1)}{6}, \tag{8.24}$$

and

$$\deg\left(\prod_i\prod_{k=1}^{\lambda_i}(t^{2k}-1)\prod_j\prod_{k=1}^{\mu_j}(t^{2k}-1)\right) = 2\sum_{j=1}^{m+1}\binom{\lambda_j+1}{2} + 2\sum_{j=1}^{m}\binom{\mu_j+1}{2}. \tag{8.25}$$

Also, by Lemma B.1.1,

$$\deg\left(\prod_{j_1<j_2}(t^{\lambda_{j_1}}-t^{\lambda_{j_2}})\right) = \sum_{j=1}^{m+1}(j-1)\lambda_j, \quad \text{and} \tag{8.26}$$

$$\deg\left(\prod_{j_1<j_2}(t^{\mu_{j_1}}-t^{\mu_{j_2}})\right) = \sum_{j=1}^{m}(j-1)\mu_j. \tag{8.27}$$

Furthermore, by speciality of $\binom{\lambda}{\mu}$ we have that $\lambda_1 \leq \mu_1 \leq \ldots \leq \mu_m \leq \lambda_{m+1}$, which implies that

$$\begin{aligned}\deg\left(\prod_{j,k}(t^{\lambda_j}+t^{\mu_k})\right) &= \sum_{j,k}\max\{\lambda_j,\mu_k\} = \sum_{j=1}^{m+1}\left(\sum_{k=1}^{j-1}\lambda_j + \sum_{k=j}^{m}\mu_k\right)\\ &= \sum_{j=1}^{m+1}(j-1)\lambda_j + \sum_{k=1}^{m}k\mu_k. \end{aligned}\tag{8.28}$$

Combining equations (8.23) through (8.28), and letting (ξ,ν) be the special pair associated with $\binom{\lambda}{\mu}$, the equality

$$\deg(u^i_{\binom{\lambda}{\mu}}) = i^2 + i - \|\xi\|_1 - \|\xi\|_2^2 - \|\nu\|_2^2$$

now follows by direct computation, which we omit. We remark that in order to perform the computation, one should recall the definition of the sequence pair (x,y) associated to (ξ,ν), and invokes Lemma B.1.3 in order to rewrite (8.25) in terms of ξ and ν. □

8.2.3 Proof of Proposition 8.2.4

Let us make some observations regarding the sum on the right-hand side of (8.13), in preparation for the proof of Proposition 8.2.4.

Firstly, by Proposition 7.1.3.(3), we know that, given $i \in \{0,\ldots,\lfloor \ell/2\rfloor\}$, the value $\frac{|H_\ell|_{p'}}{|H_i\times H_{\ell-i}|_{p'}}$ is given by evaluation at q of a polynomial $\omega(\boldsymbol{i}_i)$, where $\boldsymbol{i}_i = ([1],\Sigma_i) \in \mathfrak{I}$ and Σ_i is an isolated root subsystem of Φ of type $\mathsf{C}_i \times \mathsf{C}_{\ell-i}$. Furthermore, in this case,

$$\deg\omega(\boldsymbol{i}_i) = \frac{1}{2}\left(|\Phi| - |\Sigma_i|\right) = \ell^2 - i^2 - (\ell-i)^2. \tag{8.29}$$

Secondly, by Lemma 8.2.3, we have that

$$\left(\frac{|H_\ell|_{p'}}{|H_i\times H_{\ell-i}|_{p'}}\right)^{-s}\zeta^{\mathrm{unip}}_{H_i}(s)\zeta^{\mathrm{unip}}_{H_{\ell-i}}(s)$$

$$= \sum_{\substack{(\xi_1,\nu_1)\in\mathscr{A}_i \text{ special} \\ (\xi_2,\nu_2)\in\mathscr{A}_{\ell-i} \text{ special}}} \sum_{\mathbf{F}_{(\nu_1^*,\xi_1^*)}\times\mathbf{F}_{(\nu_2^*,\xi_2^*)}} \left(\omega(\boldsymbol{i}_i)(q)\cdot u^i_{\binom{\lambda_1}{\mu_1}}(q)\cdot u^{\ell-i}_{\binom{\lambda_2}{\mu_2}}(q)\right)^{-s} \tag{8.30}$$

where the final sum ranges over all pairs $(\binom{\lambda_1}{\mu_1}, \binom{\lambda_2}{\mu_2})$ corresponding to pairs of unipotent characters in the cartesian product $\mathbf{F}_{(\xi_1,\nu_1)^\dagger} \times \mathbf{F}_{(\xi_2,\nu_2)^\dagger} = \mathbf{F}_{(\nu_1^*,\xi_1^*)} \times \mathbf{F}_{(\nu_2^*,\xi_2^*)}$. Note that the passage application of $\dagger$ to the coordinates of the pair $((\xi_1,\nu_1),(\xi_2,\nu_2))$ does not affect the outcome of the product on the left-hand side of (8.30), by Lemma 8.2.6.

Finally, we note that given special partition pairs $(\xi_1,\nu_1)\in\mathscr{A}_i$ and $(\xi_2,\nu_2)\in\mathscr{A}_{\ell-i}$ and a pair of symbols $(\binom{\lambda_1}{\mu_1}, \binom{\lambda_2}{\mu_2})$ corresponding to a pair of unipotent characters in the product $\mathbf{F}_{(\nu_1^*,\xi_1^*)} \times \mathbf{F}_{(\nu_2^*,\xi_2^*)}$, by (8.29) and Lemma 8.2.3, it holds that

$$\deg(\omega(\boldsymbol{i}_i)\cdot u^i_{\binom{\lambda_1}{\mu_1}}\cdot u^{\ell-i}_{\binom{\lambda_2}{\mu_2}}) = \ell^2+\ell-\|\nu_1^*\cup\nu_2^*\|_1 - \|\nu_1^*\cup\nu_2^*\|_2^2) - \|\xi_1^*\cup\xi_2^*\|_2^2),$$

where the union of partitions is defined as on [40, p. 6]. Invoking [40, (1.8)], we have that

$$\deg(\omega(\boldsymbol{i}_i)\cdot u^i_{\binom{\lambda_1}{\mu_1}}\cdot u^{\ell-i}_{\binom{\lambda_2}{\mu_2}}) = \ell^2+\ell-\|(\nu_1\oplus\nu_2)^*\|_1 - \|(\nu_1\oplus\nu_2)^*\|_2^2 - \|(\xi_1\oplus\xi_2)^*\|_2^2,$$

where the direct sum of partition is defined by

$$(\eta_1,\dots,\eta_{m_1})\oplus(\tau_1,\dots,\tau_{m_2}) = (\eta_1,\dots\eta_{m_1-m_2},(\eta_{m_1-m_2+1}+\tau_1),\dots,(\eta_{m_1}+\tau_{m_2})),$$

assuming without loss of generality that $m_1\geq m_2$. We note that this definition coincides with the definition of sum of partitions in [40], as, by convention in *loc. cit.*, partitions are arranged in non-ascending order, rather than non-descending. Put otherwise, we have shown that

$$\deg(\omega(\boldsymbol{i}_i)\cdot u^i_{\binom{\lambda_1}{\mu_1}}\cdot u^{\ell-i}_{\binom{\lambda_2}{\mu_2}}) = g_\ell((\nu_1\oplus\nu_2)^*,(\xi_1\oplus\xi_2)^*), \tag{8.31}$$

where g_ℓ is as defined Lemma 8.2.1.

To conclude the preparations for proving Proposition 8.2.4, we require one more simple lemma.

Lemma 8.2.8.
1. *Let $r,k\in\mathbb{N}$ and let $(\xi_1,\nu_1)\in\mathscr{A}_r$ and $(\xi_2,\nu_2)\in\mathscr{A}_k$ be special partition pairs. The partition pair $(\xi_1\oplus\xi_2,\nu_1\oplus\nu_2)$ is then of type B_{r+k}.*
2. *Let $(\xi,\nu)\in\mathscr{A}_m$ be a partition pair of type B_m. There exist $r,k\in\mathbb{N}$ and special partition pairs $(\xi_1,\nu_1)\in\mathscr{A}_r$, $(\xi_2,\nu_2)\in\mathscr{A}_k$ such that $r+k=m$ and*

$$(\xi_1\oplus\xi_2,\nu_1\oplus\nu_2)=(\xi,\nu).$$

Proof. See Lemma B.2.4. □

Proof of Proposition 8.2.4. We have already seen in Lemma 8.2.1 that, assuming $p>2$, the nilpotent adjoint class function of $\mathfrak{so}_{2\ell+1(\mathbb{F}_q)}$ may be written in the form

$$\epsilon^{\mathrm{nil}}_{\mathfrak{h}^*} = \sum_{\substack{(\xi,\nu)\in\mathscr{A}_\ell \\ \text{of type } \mathsf{B}_\ell}} c_{(\xi,\nu)}\cdot q^{-g_\ell(\nu^*,\xi^*)s}, \tag{8.32}$$

with $c_{(\xi,\nu)} \in \mathbb{N} \cap [1, 2^{2\ell+1}]$ and $g_\ell(\xi,\nu) = \ell^2 + \ell - \|\xi\|_1 - \|\xi\|_2^2 - \|\nu\|_2^2$.

Furthermore, Lemma 8.2.8 implies that the map

$$\varphi = (((\xi_1,\nu_1),(\xi_2,\nu_2)) \mapsto (\xi_1 \oplus \xi_2, \nu_1 \oplus \nu_2)) : \bigsqcup_{i=0}^{\lfloor \ell/2 \rfloor} \mathscr{A}_i \times \mathscr{A}_{\ell-i} \to \mathscr{A}_\ell$$

restricts to a surjective map from the set $\bigsqcup_{i=0}^{\lfloor \ell/2 \rfloor} \mathscr{A}_i^{\mathrm{sp}} \times \mathscr{A}_{\ell-i}^{\mathrm{sp}}$ of pairs of special pairs onto the set $\mathscr{A}_\ell^{\mathsf{B}_\ell}$ of pairs of type B_ℓ. For any $(\xi,\nu) \in \mathscr{A}_\ell^{\mathsf{B}_\ell}$ let

$$A_{(\xi,\nu)} = \varphi^{-1}((\xi,\nu)) \cap \left(\bigsqcup_{i=0}^{\lfloor \ell/2 \rfloor} \mathscr{A}_i^{\mathrm{sp}} \times \mathscr{A}_{\ell-i}^{\mathrm{sp}} \right),$$

and, for any $i = 0, \ldots, \lfloor \ell/2 \rfloor$, put $A^i_{(\xi,\nu)} = A_{(\xi,\nu)} \cap (\mathscr{A}_i \times \mathscr{A}_{\ell-i})$.

Given $(\xi,\nu) \in \mathscr{A}_\ell^{\mathsf{B}_\ell}$, define

$$\mathcal{Z}_{(\xi,\nu)}(q,s) = \sum_{i=0}^{\lfloor \ell/2 \rfloor} \sum_{((\xi_1,\nu_1),(\xi_2,\nu_2)) \in A^i_{(\xi,\nu)}} \sum_{\mathbf{F}_{(\nu_1^*,\xi_1^*)} \times \mathbf{F}_{(\nu_2^*,\xi_2^*)}} \left(\omega(\boldsymbol{i}_i)(q) \cdot u^i_{\binom{\lambda_1}{\mu_1}}(q) \cdot u^{\ell-i}_{\binom{\lambda_2}{\mu_2}}(q) \right)^{-s} \tag{8.33}$$

where the innermost sum ranges over all pairs of symbols $(\binom{\lambda_1}{\mu_1}, \binom{\lambda_2}{\mu_2})$ corresponding to a pair of unipotent characters in the cartesian product $\mathbf{F}_{(\nu_1^*,\xi_1^*)} \times \mathbf{F}_{(\nu_2^*,\xi_2^*)}$ of families, as defined in Lemma 8.2.3, and $\boldsymbol{i}_i$ is as defined at the beginning of this section. Note that the summands occurring in $\mathcal{Z}_{(\xi,\nu)}$ are determined by (ξ,ν) and are independent of the value of q. In particular, their number is bounded by a function of ℓ, and is independent of q as well. Lastly, by (8.31), all polynomials $\omega(\boldsymbol{i}_i) \cdot u^i_{\binom{\lambda_1}{\mu_1}} \cdot u^{\ell-i}_{\binom{\lambda_2}{\mu_2}}$ occurring in $\mathcal{Z}_{(\xi,\nu)}$ have degree

$$g_\ell((\nu_1 \oplus \nu_2)^*, (\xi_1 \oplus \xi_2)^*) = g_\ell(\nu^*, \xi^*).$$

The sum on the right-hand side of (8.13) may now be rewritten as

$$\sum_{i=0}^{\lfloor \ell/2 \rfloor} \left(\frac{|\mathrm{Sp}_{2\ell}(\mathbb{F}_q)|_{p'}}{|\mathrm{Sp}_{2i}(\mathbb{F}_q)) \times \mathrm{Sp}_{2(\ell-i)}(\mathbb{F}_q)|_{p'}} \right)^{-s} \zeta_{\mathrm{Sp}_{2i}(\mathbb{F}_q)) \times \mathrm{Sp}_{2(\ell-i)}(\mathbb{F}_q)}(s) = \sum_{(\xi,\nu) \in \mathscr{A}_\ell^{\mathsf{B}_\ell}} \mathcal{Z}_{(\xi,\nu)}(q,s).$$

Let $C \subseteq \mathbb{N}$ be a finite set containing the following.

1. The number $c_{(\xi,\nu)}$ of (8.32), for any $(\xi,\nu) \in \mathscr{A}_\ell^{\mathsf{B}_\ell}$;

2. the number of summands in the expression (8.33) for $\mathcal{Z}_{(\xi,\nu)}$, for any $(\xi,\nu) \in \mathscr{A}_\ell^{\mathsf{B}_\ell}$; and

3. for any $i = 0, \ldots, \lfloor \ell/2 \rfloor$, any pair $((\xi_1,\nu_1),(\xi_2,\nu_2)) \in \mathscr{A}_i^{\mathrm{sp}} \times \mathscr{A}_{\ell-i}^{\mathrm{sp}}$, and any pair of symbolss $(\binom{\lambda_1}{\mu_1}, \binom{\lambda_2}{\mu_2})$ corresponding to a character pair in $\mathbf{F}_{(\xi_1,\nu_1)} \times \mathbf{F}_{(\xi_2,\nu_2)}$, all coefficients of all polynomials of the form $\omega(\boldsymbol{i}_i) \cdot u^i_{\binom{\lambda_1}{\mu_1}} \cdot u^{\ell-i}_{\binom{\lambda_2}{\mu_2}}$.

Letting $c \in \mathbb{N}$ be large enough so that it is divisible by all elements of C, one now has that

$$\sum_{\substack{(\xi,\nu)\in\mathscr{A}_\ell \\ \text{of type } \mathsf{B}_\ell}} c_{(\xi,\nu)} \cdot q^{-g_\ell(\nu^*,\xi^*)s} \sim_{c,q} \sum_{(\xi,\nu)\in\mathscr{A}_\ell^{\mathsf{B}_\ell}} \mathcal{Z}_{(\xi,\nu)}(q,s)$$

and therefore

$$\epsilon^{\mathrm{nil}}_{\mathfrak{so}_{2\ell+1}(\mathbb{F}_q)} \sim_{(c,q)} \sum_{i=0}^{\lfloor \ell/2 \rfloor} \left(\frac{|\mathrm{Sp}_{2\ell}(\mathbb{F}_q)|_{p'}}{\left|\mathrm{Sp}_{2i}(\mathbb{F}_q)) \times \mathrm{Sp}_{2(\ell-i)}(\mathbb{F}_q)\right|_{p'}} \right)^{-s} \zeta_{\mathrm{Sp}_{2i}(\mathbb{F}_q))\times \mathrm{Sp}_{2(\ell-i)}(\mathbb{F}_q)}(s),$$

Moreover, both finite Dirichlet series occurring above are elements of $\mathscr{D}_{c,q}$. □

Index of notation

General notation

Symbol	Meaning
$\mathbb{N}$, $\mathbb{N}_0$	Natural numbers, non-negative integers
$\mathbb{G}_a$	The additive group of $\boldsymbol{k}$
$\mathbb{G}_m$	The multiplicative group $\boldsymbol{k}^\times$ of $\boldsymbol{k}$
$\mathbb{A}^m_{\boldsymbol{k}}$	The m-dimensional affine space over a field $\boldsymbol{k}$

Given finite groups $H \subseteq G$ and characters θ of H and χ of G, we write χ_H for the restriction of χ to H, and θ^G for the induced character. If η is another character of G (or, more generally, for η and χ class functions), we write $[\chi, \eta] = \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\eta(g)}$ for the standard inner product of class functions of G

Notation introduced in Part I

Notation introduced in Part II

Bibliography

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

[2] Avni, N., Klopsch, B., Onn, U., and Voll, C. Arithmetic groups, base change, and representation growth. Geom. Funct. Anal. 26, 1 (2016), 67–135.

[3] Avni, N., Klopsch, B., Onn, U., and Voll, C. Similarity classes of integral $\mathfrak{p}$-adic matrices and representation zeta functions of groups of type A_2. Proc. Lond. Math. Soc. (3) 112, 2 (2016), 267–350.

[4] Bate, M., Martin, B., Röhrle, G., and Tange, R. Complete reducibility and separability. Trans. Amer. Math. Soc. 362, 8 (2010), 4283–4311.

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

[6] Bonnafé, C. Quasi-isolated elements in reductive groups. Comm. Algebra 33, 7 (2005), 2315–2337.

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

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

[9] Bourbaki, N. Éléments de mathématique. Fasc. XXVI. Groupes et algèbres de Lie. Chapitre I: Algèbres de Lie. Seconde édition. Actualités Scientifiques et Industrielles, No. 1285. Hermann, Paris, 1971.

[10] Britnell, J. R. Cycle index methods for finite groups of orthogonal type in odd characteristic. J. Group Theory 9, 6 (2006), 753–773.

[11] Bushnell, C., and Fröhlich, A. Gauss sums and p-adic division algebras. Lecture notes in mathematics. Springer, 1983.

[12] Carnevale, A., Shechter, S., and Voll, C. Enumerating traceless matrices over compact discrete valuation rings. Israel J. Math. 227, 2 (2018), 957–986.

[13] Carter, R. W. Finite groups of Lie type. Pure and Applied Mathematics (New York). John Wiley & Sons, Inc., New York, 1985. Conjugacy classes and complex characters, A Wiley-Interscience Publication.

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

[15] Conrad, B., Gabber, O., and Prasad, G. Pseudo-reductive groups, second ed., vol. 26 of New Mathematical Monographs. Cambridge University Press, Cambridge, 2015.

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

[17] Deriziotis, D. I. Centralizers of semisimple elements in a Chevalley group. Comm. Algebra 9, 19 (1981), 1997–2014.

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

[19] Digne, F., and Michel, J. Representations of finite groups of Lie type, vol. 21 of London Mathematical Society Student Texts. Cambridge University Press, Cambridge, 1991.

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

[21] Dyer, M. J., and Lehrer, G. I. Reflection subgroups of finite and affine Weyl groups. Trans. Amer. Math. Soc. 363, 11 (2011), 5971–6005.

[22] Fulman, J., and Guralnick, R. The number of regular semisimple conjugacy classes in the finite classical groups. Linear Algebra Appl. 439, 2 (2013), 488–503.

[23] Fulman, J., Neumann, P. M., and Praeger, C. E. A generating function approach to the enumeration of matrices in classical groups over finite fields. Mem. Amer. Math. Soc. 176, 830 (2005), vi+90.

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

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

[26] Hill, G. Regular elements and regular characters of $\mathrm{GL}_n(\mathfrak{O})$. Journal of Algebra 174 (1995), 610–635.

[27] Humphreys, J. Linear Algebraic Groups. Graduate Texts in Mathematics. Springer, 1975.

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

[29] Humphreys, J. E. Reflection groups and Coxeter groups, vol. 29 of Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 1990.

[30] Humphreys, J. E. Conjugacy classes in semisimple algebraic groups, vol. 43 of Mathematical Surveys and Monographs. American Mathematical Society, Providence, RI, 1995.

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

[32] Kaneda, M., and Seitz, G. M. On the Lie algebra of a finite group of Lie type. J. Algebra 74, 2 (1982), 333–340.

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

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

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

[36] Larsen, M., and Lubotzky, A. Representation growth of linear groups. J. Eur. Math. Soc. (JEMS) 10, 2 (2008), 351–390.

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

[38] Lubotzky, A., and Martin, B. Polynomial representation growth and the congruence subgroup problem. Israel J. Math. 144 (2004), 293–316.

[39] Lusztig, G. Characters of reductive groups over a finite field, vol. 107 of Annals of Mathematics Studies. Princeton University Press, Princeton, NJ, 1984.

[40] Macdonald, I. G. Symmetric functions and Hall polynomials, second ed. Oxford Classic Texts in the Physical Sciences. The Clarendon Press, Oxford University Press, New York, 2015. With contribution by A. V. Zelevinsky and a foreword by Richard Stanley, Reprint of the 2008 paperback edition [MR1354144].

[41] Malle, G., and Testerman, D. Linear algebraic groups and finite groups of Lie type, vol. 133 of Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 2011.

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

[43] Neumann, P. M., and Praeger, C. E. Cyclic matrices in classical groups over finite fields. J. Algebra 234, 2 (2000), 367–418. Special issue in honor of Helmut Wielandt.

[44] Nicolas, B. Groupes et algébres de Lie. Chapitres 4 á 6 / N. Bourbaki. Eléments de mathématique. Springer Berlin Heidelberg Springer e-books Imprint: Springer Springer e-books, Berlin, Heidelberg, 2007.

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

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

[47] Shechter, S. Regular characters of classical groups over complete discrete valuation rings. arXiv e-prints (Sept. 2017), arXiv:1709.01685.

[48] Shintani, T. On certain square integrable irreducible unitary representations of some $\mathfrak{p}$-adic linear groups. Proceedings of the Japan Academy, Series A, Mathematical Sciences 44, 1 (1968), 1–3.

[49] Springer, T. Linear algebraic groups. Progress in mathematics. Birkhäuser, 1981.

[50] Springer, T. A. A construction of representations of Weyl groups. Invent. Math. 44, 3 (1978), 279–293.

[51] Springer, T. A., and Steinberg, R. Conjugacy classes. In Seminar on Algebraic Groups and Related Finite Groups (The Institute for Advanced Study, Princeton, N.J., 1968/69), Lecture Notes in Mathematics, Vol. 131. Springer, Berlin, 1970, pp. 167–266.

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

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

[54] Stasinski, A., and Stevens, S. The regular representations of GL_N over finite local principal ideal rings. Bull. Lond. Math. Soc. 49, 6 (2017), 1066–1084.

[55] Steinberg, R. Endomorphisms of linear algebraic groups. Memoirs of the American Mathematical Society, No. 80. American Mathematical Society, Providence, R.I., 1968.

[56] Steinberg, R. Conjugacy classes in algebraic groups. Lecture notes in mathematics. Springer, 1974.

[57] Steinberg, R. Torsion in reductive groups. Advances in Math. 15 (1975), 63–92.

[58] Takase, K. Regular irreducible characters of a hyperspecial compact group and Weil representations over finite fields. arXiv e-prints (Sept. 2015), arXiv:1509.07573.

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

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

[61] Waterhouse, W. C. Introduction to affine group schemes, vol. 66 of Graduate Texts in Mathematics. Springer-Verlag, New York-Berlin, 1979.

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

[63] Wilson, R. The Finite Simple Groups. Graduate Texts in Mathematics. Springer London, 2009.

Part III

Appendices

Appendix A

The number of monic irreducible even polynomials of a given degree over $\mathbb{F}_q$

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

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

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

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

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

$\Leftarrow$ Let $\sigma \in \mathrm{Gal}(\boldsymbol{k} \mid \mathbb{F}_q)$ be the map $\sigma(y) = y^{q^m}$. Then, by the assumption $f(t) \mid t^{q^m} + t$, we have that

$$\sigma(x) = x^{q^m} = -x$$

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

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

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

□

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

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

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

$$x^{q^{2m}} = \left(x^{q^m}\right)^{q^m} = x$$

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

$$x^{q^d} = \sigma(x) = -x.$$

Lastly, we show that $r = \frac{m}{d}$ is odd. This follows since

$$-x = x^{q^m} = F^m(x) = (F^d)^r(x) = (-1)^r x,$$

and hence r is odd. □

Note that the converse of Lemma A.0.2 is true as well. Namely, if $d \mid m$ and $r = \frac{m}{d}$ is an odd integer then any non-zero $x \in \boldsymbol{k}$ which satisfies $x^{q^d} + x = F^d(x) + x = 0$ also satisfies

$$x^{q^m} + x = (F^d)^r(x) + x = (-1)^r x + x = 0.$$

Thus, we obtain the following.

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

1. *$S_d \subseteq S_m$ if and only if $d \mid m$ and $\frac{m}{d}$ is an odd integer.*

2. *The set non-zero even elements $x \in \boldsymbol{k}$ which generate an extension of $\mathbb{F}_q$ of degree $2m$ is*

$$S_m \setminus \bigcup_{d \mid m,\ \frac{m}{d} \text{ is odd}} S_d.$$

As the set S_m has cardinality $q^m - 1$ (since the field $\mathbb{F}_q$ is perfect and the roots of $t^{q^m} + t$ are all simple), by exclusion-inclusion we deduce that the non-zero even elements of $\boldsymbol{k}$ which generate a degree $2m$ extension of $\mathbb{F}_q$ is

$$\sum_{d|m\,,\;2\nmid\frac{m}{d}} \mu\left(\frac{m}{d}\right)\left(q^d - 1\right),$$

where μ is the Möbius function.

Appendix B

Some partition identities

B.1 General identities

Lemma B.1.1. *Let $n \in \mathbb{N}$ and $\mu = (\mu_1, \ldots, \mu_r) \vdash n$ with $\mu_1 < \mu_2 < \ldots < \mu_r$. Let $\iota \in \{\pm 1\}$, and define a polynomial*

$$\varphi_\mu^\iota(t) = \prod_{1 \le i_1 < i_2 \le r} \left(t^{\mu_1} - \iota^{\mu_1+\mu_2} t^{\mu_2}\right),$$

Then $\deg \varphi_\mu = \sum_{i=1}^r (i-1)\mu_i$.

Proof. By properties of the Vandermonde matrix, we have that

$$\begin{aligned}
\varphi_\mu^\iota(t) &= \prod_{1 \le i_1 < i_2 \le r} \iota^{\mu_1} \left((\iota t)^{\mu_1} - (\iota t)^{\mu_2}\right) \\
&= \iota^{\sum_{j=1}^r (r-j)\mu_j} \det \begin{pmatrix} 1 & 1 & \cdots & 1 \\ (\iota t)^{\mu_1} & (\iota t)^{\mu_2} & \cdots & (\iota t)^{\mu_r} \\ \vdots & \vdots & \ddots & \vdots \\ (\iota t)^{(r-1)\mu_1} & (\iota t)^{(r-1)\mu_2} & \cdots & (\iota t)^{(r-1)\mu_r} \end{pmatrix} \\
&= \iota^{\sum_{j=1}^r (r-j)\mu_j} \sum_{\tau \in \mathfrak{S}_r} sgn(\tau) \prod_{i=1}^r (\iota t)^{(i-1)\mu_{\tau(i)}}.
\end{aligned}$$

The fact that μ is strictly increasing implies both that this sum is non-zero, and that the maximal value of $\left\{\sum_{i=1}^r (i-1)\mu_{\tau(t)} : \tau \in \mathfrak{S}_r\right\}$ is attained if and only if $\tau = \mathbf{1}$ is the trivial permutation. Therefore

$$\deg \varphi_\mu^\iota = \deg \left(\sum_{\tau \in \mathfrak{S}_r} sgn(\tau) \prod_{i=1}^r (\iota t)^{(i-1)\mu_{\tau(i)}} \right) = \sum_{i=1}^r (i-1)\mu_i.$$

□

Lemma B.1.2. *Let $n \in \mathbb{N}$ and $\lambda = (\lambda_1, \ldots, \lambda_r) \vdash n$ and let $h = (h_1, \ldots, h_k)$ be a non-decreasing sequence, with $r \le k$ and $h_i = \lambda_{i+r-k}$ for any $i > k - r$ and $h_i = 0$ otherwise. Then*

$$\sum_{i=1}^k i h_i = \left(k + \frac{1}{2}\right) \|\lambda\|_1 - \frac{1}{2} \|\lambda^*\|_2^2.$$

Proof. We have that

$$\sum_{i=1}^{k} ih_i = k\sum_{i=1}^{k} h_i + \sum_{i=k-r+1}^{k}(i-k)\lambda_{i+r-k} = k\left\|\lambda\right\|_1 - \sum_{j=1}^{r}(r-j)\lambda_j \tag{B.1}$$

where in the final equality we made the change of index $j = i-k+r$. The value $\sum_j (r-j)\lambda_j$ may be computed analogously to [40, p. 3], recalling our convention for the order of partitions. Namely, consider the Young diagram associated to λ, and label all cells of the top row by 0, all cells of the second row by 1 et cetera. Summing along the rows we get the value $\sum_j (r-j)\lambda_j$, while by summing along columns we obtain

$$\sum_{j=1}^{l(\lambda^*)}(0+1+\ldots+\lambda_j^*) = \sum_{j=1}^{l(\lambda^*)}\binom{\lambda_j^*}{2} = \frac{1}{2}\left(\left\|\lambda^*\right\|_2^2 - \left\|\lambda^*\right\|_1\right). \tag{B.2}$$

The lemma follows from (B.1) and (B.2), noting that $\left\|\lambda^*\right\|_1 = \left\|\lambda\right\|_1$. ☐

Lemma B.1.3. *Let $n \in \mathbb{N}$ and $\lambda = (\lambda_1, \ldots, \lambda_r) \vdash n$. Define a partition $\mu = (\mu_1, \ldots, \mu_r) \vdash n + \binom{r}{2}$ by $\mu_i = \lambda_i + (i-1)$. Then*

$$\sum_{i=1}^{r}\left(\binom{\mu_i+1}{2} - i\mu_i\right) = \frac{1}{2}\left\|\lambda\right\|_2^2 - \frac{n}{2} - \binom{r+1}{3}.$$

Proof. Consider the Young table of μ, and assign values to the cells of the table in two manners. Firstly, for any $i = 1, \ldots, \mu_r$ place the value i in each of the cells of the i-th column of the table. Secondly, in a second copy of the table, for any $i = 1, \ldots, r$, place the value $r-i+1$ in each of the cells of the i-th row of the table. Summing all values in each of the tables we get $\sum_{i=1}^{r}\binom{\mu_i+1}{2}$ in the first assignment, and $\sum_{i=1}^{r} i\mu_i$ in the second.

Now, consider the Young table obtained by subtracting the second table from the first one. This table may be written as the union of the Young tables of the partition $(1, 2, \ldots, r-1)$ in which the value $i-r$ has been placed along the i-th diagonal, and the Young table of λ, in which the value j has been placed in each of the cells of the j-th column. See (B.3) for the tables thus obtained for $\lambda = (1, 2, 2)$.

$$\begin{aligned}
&\begin{ytableau} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 \\ 1 \end{ytableau} \quad - \quad \begin{ytableau} 3 & 3 & 3 & 3 \\ 2 & 2 & 2 \\ 1 \end{ytableau} \\
&\qquad = \begin{ytableau} -2 & -1 & 0 & 1 \\ -1 & 0 & 1 \\ 0 \end{ytableau} \\
&\qquad\qquad = \begin{ytableau} -2 & -1 \\ -1 \end{ytableau} \quad \cup \quad \begin{ytableau} 0 & 1 \\ 0 & 1 \\ 0 \end{ytableau}
\end{aligned} \tag{B.3}$$

Computing the sum of the last two table we obtain the value

$$-\sum_{i=1}^{r-1}\binom{i+1}{2}+\sum_{i=1}^{r}\binom{\lambda_i}{2}=-\binom{r+1}{3}+\frac{1}{2}\left\|\lambda\right\|_2^2-\frac{1}{2}\left\|\lambda\right\|_1,$$

by the Hockey-stick identity. The lemma follows. □

B.2 Special partition pairs

Lemma B.2.1. *Let $(\xi,\nu)\in\mathscr{A}_\ell$. Then (ξ,ν) is special if and only if $(\xi,\nu)^\dagger=(\nu^*,\xi^*)$ is special.*

Proof. Let (x,y) be an associated sequence pair to (ξ,ν), with $x=(x_1,\ldots,x_{m+1})$ and $y=(y_1,\ldots,y_m)$. Then the sequence pair $(y^*=(y_1^*,\ldots,y_{r+1}^*),x^*=(x_1^*,\ldots,x_r^*))$, given by

$$y_j^*=\left|\{i:y_i\geq r+2-j\}\right|\qquad\text{and}\qquad x_j^*=\left|\{i:x_i\geq r+1-j\}\right|,\tag{B.4}$$

with $r\geq\max\{x_{m+1},y_m\}$, is associated to the pair (ν^*,ξ^*).

To prove that $(\xi,\nu)^\dagger$ is special, we need to show that $y_j^*\leq x_j^*\leq y_{j+1}^*$ holds, for any $j=1,\ldots,r$. First note that the assumption $y_i\leq x_{i+1}+1$ for any $i=1,\ldots,m$, which follows from speciality of the pair (ξ,ν), implies that the map $i\mapsto i+1$ is an injection from the set $\{i:y_i\geq r+2-j\}$ into the set $\{i:x_i\geq r+1-j\}$, for any $j=1,\ldots,r$. Hence $x_j^*\geq y_j^*$. Secondly, since the equality $x_i\leq y_i$ holds for all $i=1,\ldots,m$, the condition $x_i\geq r+1-j$ implies that $y_i\geq r+2-(j+1)$ for any $i=1,\ldots,m$. In particular, the set of i's such that $x_i\geq r+2-j$ and $y_i<r+2-(j+1)$ is included in the singleton $\{m+1\}$ and hence

$$x_j^*-y_{j+1}^*\leq\left|\{m+1\}\right|=1.$$

Thus (ν^*,ξ^*) is special. The converse implication follows by duality. □

Lemma B.2.2. *Let $\lambda\vdash 2\ell+1$, have all even parts having even multiplicity, and let (ξ,ν) be the associated partition pair of ℓ, as in § 8.2.1. Assume (ξ,ν) is special. The number of odd parts in λ is*

$$\left\|\lambda\right\|_2^2-4\left\|\xi\right\|_2^2-4\left\|\nu\right\|_2^2-4\left(\left\|\xi\right\|_1-\left\|\nu\right\|_1\right).$$

To prove Lemma B.2.2, we require the following.

Lemma B.2.3. *Let $\widetilde{x}=(\widetilde{x}_1,\ldots,\widetilde{x}_{m+1})$ and $\widetilde{y}=(\widetilde{y}_1,\ldots,\widetilde{y}_m)$ be increasing sequences and assume*

$$\widetilde{x}_1\leq\widetilde{y}_1\leq\widetilde{x}_2\leq\widetilde{y}_2\leq\ldots\leq\widetilde{y}_m\leq\widetilde{x}_{m+1}.$$

Let $\widetilde{\mu}=(\widetilde{\mu}_1,\ldots\widetilde{\mu}_{2m+1})$ be the increasing sequence whose set of elements is $\{2\widetilde{x}_j+1,2\widetilde{y}_j\}$, and $\mu=(\mu_1,\ldots,\mu_{2m+1})$ be given by $\mu_i=\widetilde{\mu}_i-(i-1)$.

1. $\widetilde{\mu}_{2m+1}=2\widetilde{x}_{m+1}+1$.

2. *The equality* $\{\widetilde{\mu}_{2i-1}, \widetilde{\mu}_{2i}\} = \{2\widetilde{x}_i + 1, 2\widetilde{y}_i\}$ *holds for all* $i = 1, \ldots, m$.

3. *The part* μ_{2i} *is odd if and only if* $\widetilde{\mu}_{2i} = 2\widetilde{y}_i$*, for all* $1 \leq i \leq m$*. In this case necessarily* μ_{2i-1} *is odd as well.*

4. *If* μ_{2i} *is even then* $\mu_{2i} = \mu_{2i-1}$*, for all* $i = 1, \ldots, m$.

Proof. 1. Clearly, since $\widetilde{x}, \widetilde{y}$ and $\widetilde{\mu}$ are increasing sequences and by the definition of $\widetilde{x}$ and $\widetilde{y}$, we have that $\widetilde{\mu}_{2m+1} = \max\{2\widetilde{x}_{m+1} + 1, 2\widetilde{y}_m\}$. Also,

$$2\widetilde{y}_m \leq 2\widetilde{x}_{m+1} < 2\widetilde{x}_{m+1} + 1.$$

2. It is enough to show that for any $i = 1, \ldots, m-1$

$$\max\{2\widetilde{x}_i + 1, 2\widetilde{y}_i\} < \min\{2\widetilde{x}_{i+1} + 1, 2\widetilde{y}_{i+1}\}.$$

The inequalities $2\widetilde{x}_i + 1 < 2\widetilde{x}_{i+1} + 1$ and $2\widetilde{y}_i < 2\widetilde{y}_{i+1}$ are clear, since both $\widetilde{x}$ and $\widetilde{y}$ are increasing. Additionally, the inequality $2\widetilde{y}_i < 2\widetilde{x}_{i+1} + 1$ follows by the same argument as the case $i = m$ in the previous item. Finally, the assumption about the pair $(\widetilde{x}, \widetilde{y})$ and the fact that $\widetilde{x}$ is increasing imply that $\widetilde{x}_i < \widetilde{x}_{i+1} \leq \widetilde{y}_{i+1}$ and hence $2\widetilde{x}_i + 1 \leq 2\widetilde{y}_{i+1}$. Since the two hands of the last inequality have different parities, this inequality is strict.

3. Clearly, $\mu_{2i} = \widetilde{\mu}_{2i} - (2i-1)$ is odd if and only if $\widetilde{\mu}_{2i}$ is even, which, by the previous item, implies that $\widetilde{\mu}_{2i} = 2\widetilde{y}_i$ and $\widetilde{\mu}_{2i-1} = 2\widetilde{x}_i + 1$. Also, in this case $\mu_{2i-1} = \widetilde{\mu}_{2i-1} - (2i-2) = 2\widetilde{x}_i - (2i-3)$ is odd as well.

4. We have that μ_{2i} is even if and only if $\widetilde{\mu}_{2i} = 2\widetilde{x}_i + 1$ and $\widetilde{\mu}_{2i-1} = 2\widetilde{y}_i$, and, since $\widetilde{\mu}$ is increasing, it follows that $2\widetilde{y}_i < 2\widetilde{x}_i + 1$ and hence $\widetilde{y}_i \leq \widetilde{x}_i$. The assumption regarding the pair $(\widetilde{x}, \widetilde{y})$ implies that the converse inequality holds as well and hence $\widetilde{y}_i = \widetilde{x}_i$.

□

Proof of Lemma B.2.2. 1. Define $\mathscr{O}_\lambda = \{i \in \{1, \ldots, m\} : \lambda_{2i} \text{ is odd}\}$. Note that, since $\lambda_{2m+1} = 2\widetilde{x}_{m+1} + 1 - 2m$ is odd, the number of odd parts of λ is $2|\mathscr{O}_\lambda| + 1$. The assumption that (ξ, ν) is special implies that the pair (x, y) obtained from the odd and even parts of $\widetilde{\lambda} = (\lambda_1, \lambda_2 + 1, \ldots, \lambda_{2m+1} + 2m)$ satisfies the conditions of Lemma B.2.3.(1), with $\widetilde{\mu} = \widetilde{\lambda}$, in the notation of the lemma. Using the properties proved in Lemma B.2.3, we compute the value $\|\lambda\|_2^2$ to get

$$\begin{aligned}
\|\lambda\|_2^2 &= \sum_{j=1}^{2m+1} \left(\widetilde{\lambda}_j - (j-1)\right)^2 \\
&= \left(\widetilde{\lambda}_{2m+1} - 2m\right)^2 + \sum_{j=1}^{m} \left(\left(\widetilde{\lambda}_{2j-1} - (2j-2)\right)^2 + \left(\widetilde{\lambda}_{2j} - (2j-1)\right)^2\right)
\end{aligned}$$

$$
\begin{aligned}
&= (2\widetilde{x}_{m+1} - 2m + 1)^2 + \sum_{j \in \mathscr{O}_\lambda} \left((2\widetilde{x}_j + 1 - (2j-2))^2 + (2\widetilde{y}_j - (2j-1))^2\right) \\
&+ \sum_{j \notin \mathscr{O}_\lambda} \left((2\widetilde{y}_j - (2j-2))^2 + (2\widetilde{x}_j + 1 - (2j-1))^2\right) \\
&= (2x_{m+1} + 1)^2 + \sum_{j \in \mathscr{O}_\lambda} \left((2x_j + 1)^2 + (2y_j - 1)^2\right) + \sum_{j \notin \mathscr{O}_\lambda} \left(4y_j^2 + 4x_j^2\right) \\
&= 4\left\|\xi\right\|_2^2 + 4\left\|\nu\right\|_2^2 + 1 + x_{m+1} + \sum_{j \in \mathscr{O}_\lambda} \left(4\left(x_j - y_j\right) + 2\right) + \sum_{j \notin \mathscr{O}_\lambda} \underbrace{4\left(x_j - y_j\right)}_{=0} \\
&= 4\left\|\xi\right\|_2^2 + 4\left\|\nu\right\|_2^2 + 4\left\|\xi\right\|_1 - 4\left\|\nu\right\|_1 + 2\left|\mathscr{O}_\lambda\right| + 1
\end{aligned}
$$

The first assertion of the lemma easily follows.

2. Again, we define $\mathscr{O}_\lambda = \{i \in \{1, \ldots, m\} : \lambda_{2i} \text{ is odd}\}$, and note that in the present setting the number of odd parts of λ is $2\left|\mathscr{O}_\lambda\right|$. Let $x = (x_1, \ldots, x_m)$ and $y = (y_1, \ldots, y_m)$ be the increasing sequences determined by λ, such that ξ and ν are given by their non-zero parts. The assumption of speciality implies that the sequence pair $((0, x_1, \ldots, x_m), y)$ satisfies

$$0 \leq y_1 \leq x_1 + 1 \leq y_2 + 1 \leq x_2 + 2 \leq \ldots \leq y_m + (m-1) \leq x_m + m,$$

and hence the sequences $\widetilde{x} = (x_1, x_2{+}1, \ldots, x_m{+}(m{-}1))$, $\widetilde{y} = (y_1, y_2{+}1, \ldots, y_m{+}(m{-}1))$ satisfy the conditions of Lemma B.2.3.(2), with $\widetilde{\mu} = \widetilde{\lambda}$. Using the relevant properties we, again, compute the value $\left\|\lambda\right\|_2^2$ to get

$$
\begin{aligned}
\left\|\lambda\right\|_2^2 &= \sum_{j=1}^{2m} \left(\widetilde{\lambda}_j - (j-1)\right)^2 \\
&= \sum_{j=1}^{m} \left(\left(\widetilde{\lambda}_{2j-1} - (2j-2)\right)^2 + \left(\widetilde{\lambda}_{2j} - (2j-1)\right)^2\right) \\
&= \sum_{j \in \mathscr{O}_\lambda} \left((2\widetilde{x}_j + 1 - (2j-2))^2 + (2\widetilde{y}_j - (2j-1))^2\right) \\
&+ \sum_{j \notin \mathscr{O}_\lambda} \left((2\widetilde{y}_j - (2j-2))^2 + (2\widetilde{x}_j + 1 - (2j-1))^2\right) \\
&= \sum_{j \in \mathscr{O}_\lambda} \left((2x_j + 1)^2 + (2y_j - 1)^2\right) + \sum_{j \notin \mathscr{O}_\lambda} \left(4x_j^2 + 4y_j^2\right) \\
&= \left\|\xi\right\|_2^2 + \left\|\nu\right\|_2^2 + \sum_{j \in \mathscr{O}_\lambda} \left(4\underbrace{(x_j - y_j)}_{=-1} + 2\right) = \left\|\xi\right\|_2^2 + \left\|\nu\right\|_2^2 - 2\left|\mathscr{O}_\lambda\right|.
\end{aligned}
$$

The second assertion of the lemma is now proved.

□

Lemma B.2.4. *1. Let $r, k \in \mathbb{N}$ and let $(\xi_1, \nu_1) \in \mathscr{A}_r$ and $(\xi_2, \nu_2) \in \mathscr{A}_k$ be special partition pairs. The partition pair $(\xi_1 \oplus \xi_2, \nu_1 \oplus \nu_2)$ is then of type B_{r+k}.*

2. *Let $(\xi,\nu)\in\mathscr{A}_l$ be a partition pair of type B_l. There exists $r,k\in\mathbb{N}$ and special partition pairs $(\xi_1,\nu_1)\in\mathscr{A}_r$, $(\xi_2,\nu_2)\in\mathscr{A}_k$ such that $r+k=l$ and*

$$(\xi_1\oplus\xi_2,\nu_1\oplus\nu_2)=(\xi,\nu).$$

Proof. 1. Let (x^1,y^1) and (x^2,y^2) be associated sequence pairs to (ξ_1,ν_1) and (ξ_2,ν_2), with $x^j=(x^j_1,\dots,x^j_{m_j+1})$ and $y^j=(y^j_1,\dots,y^j_{m_j})$ for $j=1,2$. Note that, without loss of generality, up to addition of zeros at the head of x^j and y^j, we may assume that $m_1=m_2=m$. By assumption of speciality, we have that

$$x^j_1\le y^j_1\le x^j_2+1\le y^j_2+1\le\ldots\le y^j_m+(m-1)\le x^j_{m+1}+m,$$

for $j=1,2$. Furthermore, by definition of $\oplus$, it is clear that the sequence pair (x^1+x^2,y^1+y^2) is associated to the partition pair $(\xi_1\oplus\xi_2,\nu_1\oplus\nu_2)$. Writing out the inequalities obtained for (x^1+x^2,y^1+y^2), it holds that

$$(x^1_1+x^2_1)\le(y^1_1+y^2_1)\le(x^1_2+x^2_2)+2\le(y^1_2+y^2_2)+2\le\ldots\le(x^1_{m+1}+x^2_{m+1})+2m,$$

whence the first assertion.

2. Let (x,y) be a sequence pair associated to (ξ,ν) with $x=(x_1,\dots,x_{m+1})$ and $y=(y_1,\dots,y_m)$. Then, since (ξ,ν) is of type B_m, we have that

$$x_1\le y_1\le x_2+2\le y_2+2\le\ldots\le y_m+2(m-1)\le x_{m+1}+2m.$$

Let $i_0\in\{1,\dots,m+1\}$ be minimal such that $x_j=y_j$ for all $j<i_0$. Thus $x_{i_0}<y_{i_0}$. Define sequences (x^1,y^1) and (x^2,y^2) by $x^1=x$, $x^2=0$,

$$y^1_j=\begin{cases}y_j & \text{if } j<i_0\\ y_j-1 & \text{if } j\ge i_0\end{cases}\quad\text{and}\quad y^2_j=\begin{cases}0 & \text{if } j<i_0\\ 1 & \text{if } j\ge i_0\end{cases},$$

for any $j=1,\dots,m$. Note that $y^1_{i_0-1}=x^1_{i_0-1}\le x_{i_0}<y_{i_0}$ and hence $y^1_{i_0-1}\le y^1_{i_0}=y_{i_0}-1$. Consequently, y^1 is non-decreasing. Furthermore, obviously, $x^1+x^2=x$ and $y^1+y^2=y$ and the partition pair $(\xi_2,\nu_2)=(-,1^{m-i_0})$, which is associated to (x^2,y^2), is a special element of $\mathscr{A}_k$ for $k=m-i_0$. Finally, let (ξ_1,ν_1) be the partition pair associated to (x^1,y^1). Then, for any $j=1,\dots,m$ we have that $x^1_j\le y^1_j\le x^1_{j+1}+1$. Indeed, if $j<i_0$ then $x^1_jx_j=y_j=y^1_j\le x^1_{j+1}<x^1_{j+1}+1$, simply because x is non-decreasing. Otherwise, if $j\ge i_0$ then, by the assumption that (ξ,ν) is of type B_l and the minimality of i_0, we have that $x_j<y_j\le x_{j+1}+2$ and hence $x^1_j\le y^1_j=y_j-1\le x_{j+1}+2-1=x^1_{j+1}+1$. It follows easily that the sequence pair $(\xi_1,\nu_1)\in\mathscr{A}_{l-k}$ is special.

□