N. SPALTENSTEIN

Polynomials over local fields, nilpotent orbits and conjugacy classes in Weyl groups

Astérisque, tome 168 (1988), p. 191-217
<http://www.numdam.org/item?id=AST_1988__168__191_0>

Société Mathématique de France
Astérisque 168 (1988), p.191-217.

Polynomials over local fields, nilpotent orbits and conjugacy classes in Weyl groups

N. Spaltenstein*

There are remarkable similarities between the nilpotent orbits in a semisimple complex Lie algebra $\mathfrak{g}$ under the action of its adjoint group G and the conjugacy classes in the Weyl group W of $\mathfrak{g}$. The most striking example is that of the regular nilpotent orbit in $\mathfrak{g}$ and the Coxeter class in W, as is made clear in the work of Kostant [5]. For $\mathfrak{g} = \mathfrak{sl}_n$ both the nilpotent orbits in $\mathfrak{g}$ and the conjugacy classes in W are parametrized by partitions of n. A partition λ corresponds to the nilpotent elements which have Jordan blocks of dimension λ_1, λ_2, ..., and to the permutations which are products of disjoint cycles of length λ_1, λ_2, ... For type A there is therefore an obvious bijection between nilpotent orbits in $\mathfrak{g}$ and conjugacy classes in W, but this construction does not carry over to other types. The problem of the existence of a natural map between nilpotent orbits in $\mathfrak{g}$ and conjugacy classes in W is raised by Carter as a concluding remark in [1], based on the similarity between the parametrization of nilpotent orbits and his own parametrization of conjugacy classes in Weyl groups. Later, Carter and Elkington [2] and Springer [7] succeed in relating a few particular nilpotent orbits in $\mathfrak{g}$ to conjugacy classes in W. The problem of defining a natural map $x \mapsto (\sigma_x)$ from nilpotent orbits in $\mathfrak{g}$ to conjugacy classes in W has now been solved by Kazhdan and Lusztig [3, 9.1] in the following way.

Let $A = \mathbf{C}[\![\varepsilon]\!]$ be the ring of complex power series in ε, $\mathfrak{m}$ its maximal ideal, $F = \mathbf{C}((\varepsilon))$ its field of fractions, $\mathfrak{g}_F = \mathfrak{g} \otimes_{\mathbf{C}} F$. The definition of the map from nilpotent orbits in $\mathfrak{g}$ to conjugacy classes in W rests on the following two facts.

(a) For every nilpotent element x in $\mathfrak{g}$, there exists a dense open subset U of $x+\mathfrak{m}\mathfrak{g}$ such that all elements of U are regular semisimple and their centralizers in $\mathfrak{g}_F$ are all $G(F)$-conjugate [3, prop. 6.1].

(b) The conjugacy classes of Cartan subalgebras in $\mathfrak{g}_F$ under the action of $G(F)$ are parametrized by the conjugacy classes in W [3, lemma 1.1].

* Supported in part by the National Science Foundation, grant # DMS-8701771

Thus by (a) we can associate to the orbit of a nilpotent element $x \in \boldsymbol{g}$ a $G(F)$-conjugacy class of Cartan subalgebras of $\boldsymbol{g}_F$, and hence by (b) a conjugacy class (σ_x) in W. Kazhdan and Lusztig show also that for semi-regular elements this map agrees with those defined in [2] and [7], that it coincides with the obvious one given by the parametrizations for $\boldsymbol{sl}_n$, and they work out a few other examples. The aim of this paper is to give a combinatorial description of this map for the orthogonal and symplectic Lie algebras.

Let now $N \in \{2n, 2n+1\}$ and let $\boldsymbol{g}$ be one of the Lie algebras $\boldsymbol{sp}_N$ or $\boldsymbol{o}_N$. For $\boldsymbol{sp}_N$ we require of course N to be even. Let also G be Sp_N if $\boldsymbol{g} = \boldsymbol{sp}_N$ and O_N if $\boldsymbol{g} = \boldsymbol{o}_N$. Then every nilpotent orbit in $\boldsymbol{g}$ under the action of G is the intersection with $\boldsymbol{g}$ of some nilpotent SL_N-orbit in $\boldsymbol{sl}_N$. They are thus parametrized by partitions of N. Moreover the partitions of N which arise in this way for $\boldsymbol{sp}_N$ (resp. $\boldsymbol{o}_N$) are precisely those which for each odd (resp. even) integer $\ell > 0$ have an even number of parts equal to ℓ [8, IV.2.15].

Notice here that we have departed from the earlier definition of G. As far as the parametrization of nilpotent orbits in $\boldsymbol{g}$ is concerned, this has an influence only for $\boldsymbol{o}_N$ when N is a multiple of 4. In this case the nilpotent O_N-orbit corresponding to a partition λ of N which has even parts only is the union of two SO_N-orbits.

Let $E = \{1, -1, \ldots, n, -n\}$ and let W_0 be the permutation group of E. For $\boldsymbol{sp}_N$ the Weyl group W can be identified with $\{w \in W_0 \,|\, w(-i) = -w(i) \text{ for each } i\}$. We attach to each element $w \in W$ two partitions α and β defined as follows. Let X be a $<w>$-orbit in E. Then $-X$ is also a $<w>$-orbit. If $X \neq -X$, then α gets one part $\alpha_i = |X|$ for the pair of orbits X, $-X$. If $X = -X$, then $|X|$ is even, and β gets one part $\beta_i = |X|/2$ for the orbit X. The pair of partitions (α, β) characterizes completely the conjugacy class of w in W, and the pairs of partitions (α, β) which arise in this way are exactly those such that $\sum \alpha_i + \sum \beta_i = n$.

Theorem A. *Let $\boldsymbol{g} = \boldsymbol{sp}_{2n}$ and let the class of the nilpotent element x of $\boldsymbol{g}$ correspond to the partition λ of $2n$. Let α be the partition which has one part α_i for each pair of equal odd parts of λ of size α_i, and let β be the partition which has one part β_i for each even part of λ of size $2\beta_i$. Then (σ_x) is the conjugacy class in W which corresponds to (α, β).*

Let now $\boldsymbol{g} = \boldsymbol{o}_N$. If N is odd, then the Weyl group of $\boldsymbol{g}$ is the same as that of $\boldsymbol{sp}_{N-1}$ and the conjugacy classes in W are therefore also parametrized by pairs of partitions. For N even, we can embed W in a Weyl group $\tilde{W}$ of type B_n. The conjugacy class of $\tilde{W}$ corresponding to the pair of partitions (α, β) is contained in W if β has an even number of parts and is disjoint from W otherwise. Moreover, if it is contained in W then it is a single conjugacy class in W, unless β is the empty partition and all the parts of α are even, in which case it splits into two classes.

Theorem B. *Let $g = o_N$ and let the class of the nilpotent element x of g correspond to the partition λ of N. Let λ^{even} and λ^{odd} be the partitions which consist respectively of the even parts and of the odd parts of λ, written as decreasing sequences. Define partitions α and β as follows.*

(a) *For each even i such that $\lambda_i^{\text{even}} \neq 0$, if the number of odd parts of λ larger than λ_i^{even} is even, then α has one part equal to λ_i^{even}, and otherwise β has two parts equal to $\lambda_i^{\text{even}}/2$.*

(b) *For each odd i such that $\lambda_i^{\text{odd}} = \lambda_{i+1}^{\text{odd}} \neq 0$, α has one part equal to λ_i^{odd}.*

(c) *For each odd i such that $\lambda_i^{\text{odd}} \neq \lambda_{i+1}^{\text{odd}} \neq 0$, β has one part equal to $(\lambda_i^{\text{odd}} - 1)/2$ and one part equal to $(\lambda_{i+1}^{\text{odd}} + 1)/2$.*

(d) *For each odd i such that $\lambda_i^{\text{odd}} \neq \lambda_{i+1}^{\text{odd}} = 0$, β has one part equal to $(\lambda_i^{\text{odd}} - 1)/2$.*

Then (α, β) is the pair of partitions which corresponds to the conjugacy class (σ_x) in W.

When N is a multiple of 4 this theorem does not describe completely the map $x \mapsto (\sigma_x)$. If x has only even dimensional Jordan blocks, then it tells only that (σ_x) is one of the two conjugacy classes in W corresponding to the pair of partitions $(\alpha, \emptyset)$ with $\alpha_i = \lambda_{2i}$ $(i \geq 1)$.

Theorems A and B follow respectively from 5.2 and 6.4 which describe generic factorization patterns for the characteristic polynomials of certain families of infinitesimal symplectic or orthogonal transformations.

The construction of the pair of partitions (α, β) associated to an orthogonal partition in theorem B is described in a slightly different way in 6.3. There a symplectic partition μ is first constructed, together with a function which allows to distinguish two types of even parts for μ. This construction is the same as that used in [6, III.7.2 and III.8.2] to relate unipotent classes of orthogonal groups in characteristic 0 and in characteristic 2. That the combinatorial map defined in [loc. cit.] might be relevant to the description of the map $x \mapsto (\sigma_x)$ was first pointed out by George Lusztig. A similar combinatorial relation for unipotent orbits in the symplectic groups in characteristic 0 and in positive characteristic is also defined in [loc.cit.]. It is however much simpler than for the orthogonal group, in the same way as the statement of theorem A is simpler than that of theorem B. Whether this relation between the Kazhdan-Lusztig map and unipotent orbits in bad characteristic has a geometric meaning is not clear.

0. Notation

0.1. We consider a discrete valuation ring R, its field of fractions F, its maximal ideal m and its valuation $v : F \to \mathbf{Z} \cup \{\infty\}$. We assume that R is complete and that the quotient field $k = R/\boldsymbol{m}$ is algebraically closed. We shall also assume that a fixed uniformizing element ε has been chosen, so that we have a well-defined isomorphism $\mathrm{Gr}(R) \cong k[\varepsilon]$.

Most of the results in section 1 hold actually under weaker assumptions on R. This is briefly discussed in 1.11.

0.2. Let M be a finitely generated R-module. Topological terms are often useful to describe subsets of M defined by congruences. More precisely for $n \in \mathbf{N}$ let $\mathcal{P}_n(M)$ be the R-algebra of $R/\boldsymbol{m}^n$-valued functions generated by $\mathrm{Hom}_R(M, R/\boldsymbol{m}^n)$. We consider on M the coarsest topology for which all the subsets $f^{-1}(0)$ with $f \in \mathcal{P}_n(M)$ and $n \in \mathbf{N}$ are closed. Closed subsets are thus finite unions of arbitrary intersections of such subsets, and open subsets are the complements of closed subsets. If $\boldsymbol{m}M = 0$, this topology is the Zariski topology on M considered as a finite dimensional k-vector space. Every submodule M' of M is closed for this topology, and if M is free, then the topology of M' coincides with that induced from M. It should be noted that these definitions differ from those in [3, 6.1-2].

Suppose now that M is free. The R-valued functions on M which are polynomials in linear forms are called polynomial functions on M. The polynomial functions on a subset X of M are those generated by the restrictions to X of polynomial functions on M, the following operations being allowed beside the addition and multiplication. If $f : X \to R$ is such that $f(X) \subset \boldsymbol{m}$, then $\varepsilon^{-1}f$ is a polynomial function on X. If $f(X) \subset R \setminus \boldsymbol{m}$, then $1/f$ is a polynomial function on X. For $n \in \mathbf{N}$ let $\mathcal{P}_n(X)$ denote the algebra of all $R/\boldsymbol{m}^n$-valued functions on X which are polynomial functions in this sense.

Let N be a second finitely generated free R-module, Y a subset of N, and consider a map $f : X \to Y$. We say that f is analytic if composition with f induces a map from $\mathcal{P}_n(Y)$ to $\mathcal{P}_n(X)$ for every $n \in \mathbf{N}$. Analytic maps are continuous. Polynomial maps are analytic.

1. Newton polygons

1.1. Newton polygons are known to be useful in the study of polynomials with coefficients in a valuation ring (see e.g. [4]). In this paper a subset Γ of $\mathbf{R}^2$ is called a *Newton polygon* if it satisfies the following three conditions.

(NP1) Γ is the convex hull of some subset of $\mathbf{N}^2$.

(NP2) $\mathrm{pr}_1(\Gamma)$ is compact.

(NP3) If $(x, y) \in \Gamma$ and $y' \geq y$, then $(x, y') \in \Gamma$.

For example, given a polynomial $A = \sum a_i X^i \in R[X]$, there is a smallest Newton polygon Γ_A containing $\left\{ (i, v(a_i)) \,\middle|\, a_i \neq 0 \right\}$. If Γ is a Newton polygon, it is clear that $V_\Gamma = \{ A \in R[X] \mid \Gamma_A \subset \Gamma \}$ is an R-submodule of $R[X]$. If Γ is non-empty, let $m = \max(\mathrm{pr}_1(\Gamma))$, $n = \min\{ j \mid (m,j) \in \Gamma \}$, and define also

$$V_\Gamma^1 = \Big\{ A = \sum a_i X^i \in V_\Gamma \;\Big|\; a_m = \varepsilon^n \Big\}.$$

If Γ and Δ are Newton polygons, then so is also $\Gamma + \Delta = \{ \gamma + \delta \mid \gamma \in \Gamma,\ \delta \in \Delta \}$. If A, $B \in R[X]$, then $\Gamma_{AB} = \Gamma_A + \Gamma_B$. It follows that $V_\Gamma V_\Delta \subset V_{\Gamma+\Delta}$, where $V_\Gamma V_\Delta = \{ AB \mid A \in V_\Gamma,\ B \in V_\Delta \}$.

1.2. Let Γ be a non-empty Newton polygon. For $q = r/s \in \mathbf{Q}$, with $(r,s) = 1$ and $s > 0$, define $\ell_{\Gamma,q} : \mathbf{R} \times \big(\mathbf{R} \cup \{\infty\}\big) \to \mathbf{R} \cup \{\infty\}$ by

$$\ell_{\Gamma,q}(x,y) = y - qx - \min\{ y' - qx' \mid (x',y') \in \Gamma \}.$$

This function takes only non-negative values on Γ, and $\ell_{\Gamma,q}(\mathbf{N}^2) \subset (1/s)\mathbf{Z}$ is a discrete subset of $\mathbf{R}$. Moreover

$$\Gamma = \{ \gamma \in \mathbf{R}^2 \mid \ell_{\Gamma,q}(\gamma) \geq 0 \text{ for every } q \in \mathbf{Q} \}.$$

Let

$$I_{\Gamma,q} = \Big\{ A \in V_\Gamma \;\Big|\; \ell_{\Gamma,q}\big(i, v(a_i)\big) > 0 \text{ for all } i \in \mathbf{N} \Big\} \tag{1.2.1}$$

and

$$I_\Gamma = \Big\{ A = \sum a_i X^i \in R[X] \;\Big|\; \ell_{\Gamma,q}\big(i, v(a_i)\big) > 0 \text{ for every } q \in \mathbf{Q},\ i \in \mathbf{N} \Big\} = \bigcap_{q \in \mathbf{Q}} I_{\Gamma,q}.$$

Then $I_{\Gamma,q}$ and I_Γ are R-submodules of V_Γ, $\overline{V}_\Gamma = V_\Gamma / I_\Gamma$ is a finite dimensional vector space over k, and $\overline{V}_\Gamma^1 = V_\Gamma^1 / I_\Gamma$ is an affine subspace of $\overline{V}_\Gamma$.

It is clear that if Δ is a second non-empty Newton polygon, then

$$I_{\Gamma,q} V_\Delta \subset I_{\Gamma+\Delta,q} \quad (q \in \mathbf{Q}), \qquad \text{and} \quad I_\Gamma V_\Delta \subset I_{\Gamma+\Delta}.$$

It follows that the multiplication of polynomials induces a natural map $\overline{V}_\Gamma \times \overline{V}_\Delta \to \overline{V}_{\Gamma+\Delta}$, which we refer to as the product map.

It is convenient to interpret the image in $V_\Gamma / I_{\Gamma,q}$ of $A = \sum a_i X^i \in V_\Gamma$ as the polynomial

$$\mathrm{Gr}_{\Gamma,q}(A) = \sum_{\substack{(i,j) \in \Gamma \cap \mathbf{N}^2 \\ \ell_{\Gamma,q}(i,j) = 0}} (a_i + \boldsymbol{m}^{j+1}) X^i \in \mathrm{Gr}(R)[X].$$

Notice that the condition $\ell_{\Gamma,q}(i,j) = 0$ in the definition of $\mathrm{Gr}_{\Gamma,q}(A)$ means that as an element of $k[\varepsilon, Y]$ this polynomial is homogeneous of degree $\ell_{\Gamma,q}(0,0)s$ if we assign the weight r to X and the weight $-s$ to the natural graduation of $\mathrm{Gr}(R)$. It is easily checked that if $B \in V_\Delta$, then $\mathrm{Gr}_{\Gamma+\Delta,q}(AB) = \mathrm{Gr}_{\Gamma,q}(A)\mathrm{Gr}_{\Delta,q}(B)$ for all $q \in \mathbf{Q}$.

The collection $\mathrm{Gr}_\Gamma(A) = \big(\mathrm{Gr}_{\Gamma,q}(A)\big)_{q\in\mathbf{Q}}$ describes completely the image in $\overline{V}_\Gamma$ of $A \in V_\Gamma$, and the product $\overline{V}_\Gamma \times \overline{V}_\Delta \to \overline{V}_{\Gamma+\Delta}$ corresponds to $\mathrm{Gr}_\Gamma(A)\mathrm{Gr}_\Delta(B) = \mathrm{Gr}_{\Gamma+\Delta}(AB)$ $(A \in V_\Gamma,\ B \in V_\Delta)$, where the multiplication is performed indexwise.

1.3. In the above it is usually not necessary to consider all values of $q \in \mathbf{Q}$. Let Γ be a non-empty Newton polygon and $q = r/s \in \mathbf{Q}$ with $(r,s) = 1$ and $s > 0$. Then

$$\big\{\,(i,j) \in \Gamma \cap \mathbf{N}^2 \;\big|\; \ell_{\Gamma,q}(i,j) = 0\,\big\} \;=\; \big\{\,(i_{\Gamma,q} + ms, j_{\Gamma,q} + mr) \;\big|\; 0 \le m \le d_{\Gamma,q}\,\big\}$$

for some uniquely defined integers $i_{\Gamma,q}$, $j_{\Gamma,q}$ and $d_{\Gamma,q} \in \mathbf{N}$. If Δ is a second non-empty Newton polygon, we have

$$i_{\Gamma+\Delta,q} = i_{\Gamma,q} + i_{\Delta,q}, \qquad j_{\Gamma+\Delta,q} = j_{\Gamma,q} + j_{\Delta,q}, \qquad d_{\Gamma+\Delta,q} = d_{\Gamma,q} + d_{\Delta,q}. \tag{1.3.1}$$

We say that q is a *slope* of Γ if $d_{\Gamma,q} \neq 0$. By (1.3.1), the set of all slopes of $\Gamma + \Delta$ is the union of the corresponding sets for Γ and Δ. Each Newton polygon has only finitely many slopes. If $\mathrm{pr}_1(\Gamma)$ is not reduced to a single point, then for $A \in V_\Gamma$ the family of polynomials $\mathrm{Gr}_\Gamma(A)$ can be recovered from the knowledge of the polynomials $\mathrm{Gr}_{\Gamma,q}(A)$ with q a slope of Γ.

1.4. Let Γ be a non-empty Newton polygon, $A \in V_\Gamma$ and $q = r/s \in \mathbf{Q}$ with $(r,s) = 1$ and $s > 0$. We take now advantage of the isomorphism $\mathrm{Gr}(R) \cong k[\varepsilon]$ to rewrite the polynomial $\mathrm{Gr}_{\Gamma,q}(A)$ of 1.2 as a polynomial with coefficients in k. More precisely, let

$$\mathrm{gr}_{\Gamma,q}(A) = \sum_{h=0}^{d_{\Gamma,q}} \big(\varepsilon^{-(j_{\Gamma,q}+hr)} a_{i_{\Gamma,q}+hs} + \boldsymbol{m}\big) Y^h.$$

Then $\mathrm{gr}_{\Gamma,q}(A) \in k[Y]$, and the polynomials $\mathrm{Gr}_{\Gamma,q}(A)$ and $\mathrm{gr}_{\Gamma,q}(A)$ determine each other completely. The assignment $A \mapsto \mathrm{gr}_{\Gamma,q}(A)$ defines an isomorphism between $V_\Gamma / I_{\Gamma,q}$ and $\big\{\,P \in k[Y] \;\big|\; \deg(P) \le d_{\Gamma,q}\,\big\}$. Moreover, if Δ is a second non-empty Newton polygon and $B \in V_\Delta$, then

$$\mathrm{gr}_{\Gamma+\Delta,q}(AB) = \mathrm{gr}_{\Gamma,q}(A)\mathrm{gr}_{\Delta,q}(B) \ \text{ for every } q \in \mathbf{Q}. \tag{1.4.1}$$

Letting $\mathrm{gr}_\Gamma(A)$ denote the collection $\big(\mathrm{gr}_{\Gamma,q}(A)\big)_{q\in\mathbf{Q}}$, (1.4.1) can be written as $\mathrm{gr}_{\Gamma+\Delta}(AB) = \mathrm{gr}_\Gamma(A)\mathrm{gr}_\Delta(B)$.

1.5. Let E be a field. For $n \in \mathbf{N}$, let $E[X]_n = \big\{\,P \in E[X] \;\big|\; \deg(P) \le n\,\big\}$ and $E[X]^1_n = \big\{\,P \in E[X]_n \;\big|\; P \text{ is monic}\,\big\}$. It is well-known that for $A \in E[X]_m$ and $B \in E[X]_n$ the map

$$\begin{array}{ccc} E[X]_m \oplus E[X]_n & \to & E[X]_{m+n} \\ (U,V) & \mapsto & BU + AV \end{array}$$

is surjective if and only if the following two conditions are satisfied.

(a) A and B are relatively prime.

(b) $\deg(A) = m$ or $\deg(B) = n$.

Moreover, if these conditions hold, then so does

(c) The map

$$\begin{array}{ccc} E[X]_{m-1} \oplus E[X]_{n-1} & \to & E[X]_{m+n-1} \\ (U,V) & \mapsto & BU + AV \end{array}$$

is bijective.

Let now Γ and Δ be non-empty Newton polygons, $A \in V_\Gamma$ and $B \in V_\Delta$. The differential at (A,B), or more precisely at $(A + I_\Gamma, B + I_\Delta)$, of the product map $\overline{V}_\Gamma \times \overline{V}_\Delta \to \overline{V}_{\Gamma+\Delta}$ corresponds to $\big(\mathrm{gr}_\Gamma(U), \mathrm{gr}_\Delta(V)\big) \mapsto \mathrm{gr}_\Delta(B)\mathrm{gr}_\Gamma(U) + \mathrm{gr}_\Gamma(A)\mathrm{gr}_\Delta(V)$. It follows that it is surjective precisely when for each $q \in \mathbf{Q}$ the following two conditions are fulfilled.

(a) $\mathrm{gr}_{\Gamma,q}(A)$ and $\mathrm{gr}_{\Delta,q}(B)$ are relatively prime.

(b) $\deg\big(\mathrm{gr}_{\Gamma,q}(A)\big) = d_{\Gamma,q}$ or $\deg\big(\mathrm{gr}_{\Delta,q}(B)\big) = d_{\Delta,q}$.

1.6. Let Γ be a non-empty Newton polygon. In the next section we shall use submodules of V_Γ defined as follows. Let $q, e \in \mathbf{Q}$. Then $I_{\Gamma,q,e}$ is the set of all polynomials $A = \sum a_i X^i \in V_\Gamma$ whose coefficients satisfy the following two conditions.

(a) $\ell_{\Gamma,q'}\big(i, v(a_i)\big) > e$ for all $i \in \mathbf{N}$ and all $q' \geq q$.

(b) $\ell_{\Gamma,q'}\big(i, v(a_i)\big) \geq e$ for all $i \in \mathbf{N}$ and all $q' < q$.

It is clear that $I_{\Gamma,q,e} \subset I_{\Gamma,q',e'}$ if $e > e'$, or if $e = e'$ and $q < q'$. If Δ is a second non-empty Newton polygon, then $I_{\Gamma,q,e} V_\Delta \subset I_{\Gamma+\Delta,q,e}$.

Proposition 1.7. *Let Γ and Δ be non-empty Newton polygons. Let also $A \in V_\Gamma^1$, $B \in V_\Delta$ and $P \in V_{\Gamma+\Delta}$ satisfy $AB \equiv P \pmod{I_{\Gamma+\Delta}}$. Assume moreover that the differential at (A,B) of the product map $\overline{V}_\Gamma^1 \times \overline{V}_\Delta \to \overline{V}_{\Gamma+\Delta}$ is surjective. Then there exist a unique $A' \in V_\Gamma^1$ and a unique $B' \in V_\Delta$ such that $A' \equiv A \pmod{I_\Gamma}$, $B' \equiv B \pmod{I_\Delta}$ and $P = A'B'$.*

Proof. We construct A' and B' as limits of suitable sequences in V_Γ and V_Δ respectively. Let $S = \{q_0, \dots, q_m\}$, where q_1, ..., q_m are the slopes of $\Gamma + \Delta$ and $q_0 > q_i$ for $1 \leq i \leq m$. Choose then $t \in \mathbf{N}^*$ in such a way that $tS \subset \mathbf{Z}$. Order the set

$$\Omega = \Big(S \times (1/t)\mathbf{N}^*\Big) \cup \Big\{ \big(\min(S), 0\big) \Big\}$$

by $(x,y) < (x',y')$ if $y < y'$, or if $y = y'$ and $x > x'$. The smallest element of Ω is thus $\omega_0 = \big(\min(S), 0\big)$. If $\omega = (q,e) \in \Omega$, write $I_{\Gamma,\omega}$ for $I_{\Gamma,q,e}$.

To prove the existence of the polynomials A' and B', it is sufficient to construct by induction on $\omega \in \Omega$ sequences $(A_\omega)_{\omega\in\Omega}$ in V_Γ^1 and $(B_\omega)_{\omega\in\Omega}$ in V_Δ, with $A_{\omega_0} = A$ and $B_{\omega_0} = B$, in such a way that for each ω the following conditions hold.

(1) If ω is the successor in Ω of some element ω', then $A_\omega \equiv A_{\omega'} \pmod{I_{\Gamma,\omega'}}$ and $B_\omega \equiv B_{\omega'} \pmod{I_{\Delta,\omega'}}$.

(2) $A_\omega B_\omega \equiv P \pmod{I_{\Gamma+\Delta,\omega}}$.

We show moreover that A_ω and B_ω are unique mod $I_{\Gamma,\omega}$ and $I_{\Delta,\omega}$ respectively, proving thus simultaneously the uniqueness of A' and B'.

Notice that for ω_0 (1) is empty and (2) holds since $I_{\Gamma,\omega_0} = I_\Gamma$, $I_{\Delta,\omega_0} = I_\Delta$ and $I_{\Gamma+\Delta,\omega_0} = I_{\Gamma+\Delta}$. Let now $\omega = (q,e) \in \Omega$ have predecessor ω', and write $q = r/s$ with $(r,s) = 1$ and $s > 0$. If $se \notin \mathbf{N}$, then $I_{\Gamma+\Delta,\omega} = I_{\Gamma+\Delta,\omega'}$, and we take $A_\omega = A_{\omega'}$ and $B_\omega = B_{\omega'}$. If $se \in \mathbf{N}$ and $q = q_0$, then $d_{\Gamma+\Delta,q} = 0$ and we are dealing with the coefficients of maximal possible degree of A_ω and B_ω. As the leading coefficient of A_ω is imposed, the result is obvious in this case. Suppose now that $se \in \mathbf{N}$ and $q \neq q_0$. We write then $A_\omega = A_{\omega'} + M$, with $M \in I_{\Gamma,\omega'}$ such that $\deg(M) < \deg(A)$, and $B_\omega = B_{\omega'} + N$, with $N \in I_{\Gamma,\omega'}$, and we must show that (2) holds for some suitable choice of M and N. Now

$$A_\omega B_\omega \equiv A_{\omega'} B_{\omega'} + A_{\omega'} N + B_{\omega'} M \pmod{I_{\Gamma+\Delta,\omega}},$$

and we must thus solve

$$A_{\omega'} N + B_{\omega'} M \equiv P - A_{\omega'} B_{\omega'} \pmod{I_{\Gamma+\Delta,\omega}}. \tag{1.7.1}$$

By (1.6)

$$V_\Gamma I_{\Delta,\omega} + V_\Delta I_{\Gamma,\omega} \subset I_{\Gamma+\Delta,\omega},$$

and since ω is the successor of ω' we also have

$$I_{\Gamma,q} I_{\Delta,\omega'} + I_{\Delta,q} I_{\Gamma,\omega'} \subset I_{\Gamma+\Delta,\omega},$$

where $I_{\Gamma,q}$ and $I_{\Delta,q}$ are defined as in (1.2). Thus for the evaluation mod $I_{\Gamma+\Delta,\omega}$ of $A_{\omega'}N + B_{\omega'}M$ we may replace $A_{\omega'}$ and $B_{\omega'}$ by their respective images in $V_\Gamma^1/I_{\Gamma,q}$ and $V_\Delta/I_{\Delta,q}$, or more conveniently by $\mathrm{Gr}_{\Gamma,q}(A_{\omega'}) = \mathrm{Gr}_{\Gamma,q}(A)$ and $\mathrm{Gr}_{\Delta,q}(B_{\omega'}) = \mathrm{Gr}_{\Delta,q}(B)$. A similar operation can be performed for M, N, $A_{\omega'}N + B_{\omega'}M$ and $P - A_{\omega'}B_{\omega'}$. The spaces $I_{\Gamma,\omega'}/I_{\Gamma,\omega}$, $I_{\Delta,\omega'}/I_{\Delta,\omega}$ and $I_{\Gamma+\Delta,\omega'}/I_{\Gamma+\Delta,\omega}$ have respective dimensions $d_{\Gamma,q}$, $d_{\Delta,q}$ and $d_{\Gamma+\Delta,q}$, and they too can be thought of as subspaces of $\mathrm{Gr}(R)[X]$. Using a transformation similar to that used in 1.3, these polynomials can be replaced in turn by polynomials in $k[Y]$. The existence of a suitable choice for M and N, and their uniqueness mod $I_{\Gamma,\omega}$ and $I_{\Delta,\omega}$ respectively, follow now from the bijectivity of the map

$$\begin{array}{ccc} k[Y]_{d_{\Gamma,q}-1} \oplus k[Y]_{d_{\Delta,q}-1} & \to & k[Y]_{d_{\Gamma+\Delta,q}-1} \\ (U,V) & \mapsto & \mathrm{gr}_{\Gamma,q}(A)U + \mathrm{gr}_{\Delta,q}(B)V \end{array}$$

which in turn is a consequence of the surjectivity at (A,B) of the differential of the product map $\overline{V}_\Gamma^1 \times \overline{V}_\Delta \to \overline{V}_{\Gamma+\Delta}$ (1.5). This proves the proposition.

Corollary 1.8. *For every $A \in R[X]$ the following hold.*

(a) *If Γ_A has exactly one slope q and $\mathrm{gr}_{\Gamma_A,q}(A)$ has degree 1, then A is irreducible in $F[X]$.*

(b) *If A is irreducible in $F[X]$, of positive degree and prime to X, then Γ_A has exactly one slope q, and $\mathrm{gr}_{\Gamma_A,q}(A) = c(Y+a)^{d_{\Gamma_A,q}}$ for some a, $c \in k$.*

Proof. (b) follows from the proposition and the assumption that the residue field k is algebraically closed, and (a) is a consequence of (1.4.1).

Corollary 1.9. *Let $(V_\Gamma^1 \times V_\Delta)^0$ be the inverse image in $V_\Gamma^1 \times V_\Delta$ of the set of all points in $\overline{V}_\Gamma^1 \times \overline{V}_\Delta$ where the differential of the product map is surjective. Then the map*

$$(V_\Gamma^1 \times V_\Delta)^0 \;/\; \boldsymbol{m}(V_\Gamma \times V_\Delta) \mapsto V_{\Gamma+\Delta}/\boldsymbol{m}V_{\Gamma+\Delta} \tag{1.9.1}$$

induced by multiplication is etale.

Proof. This is actually a corollary to the proof of 1.7. As the algebraic varieties in (1.9.1) are smooth, we need only to check that the differential is bijective at every point. The proof of 1.7 gives in particular a finite filtration of the tangent spaces involved, and the corresponding graded maps are all isomorphisms. The result follows.

Proposition 1.10. *Let Γ and Δ be non-empty Newton polygons which do not have any common slope. Then the product map induces an analytic isomorphism (in the sense of 0.2)*

$$p_0 : \{\, A \in V_\Gamma^1 \mid \Gamma_A = \Gamma \,\} \times \{\, B \in V_\Delta \mid \Gamma_B = \Delta \,\} \to \{\, P \in V_{\Gamma+\Delta} \mid \Gamma_P = \Gamma + \Delta \,\}. \tag{1.10.1}$$

Proof. Let $\bar{p}_0$ be the restriction of the product map $\overline{V}_\Gamma^1 \times \overline{V}_\Delta \to \overline{V}_{\Gamma+\Delta}$ to the images of the subsets considered in (1.10.1). Using the fact that Γ and Δ have no common slope, it is easily checked that $\bar{p}_0$ has a surjective differential at every point. We check now that $\bar{p}_0$ is bijective.

As in the proof of 1.7, let $q_1 > \ldots > q_m$ be the slopes of $\Gamma + \Delta$, and let $q_0 > q_1$. For $0 \le h \le m$ let

$$i'_h = i_{\Gamma,q_h}, \quad i''_h = i_{\Delta,q_h}, \quad i_h = i_{\Gamma+\Delta,q_h},$$

$$j'_h = j_{\Gamma,q_h}, \quad j''_h = j_{\Delta,q_h}, \quad j_h = j_{\Gamma+\Delta,q_h},$$

$$d'_h = d_{\Gamma,q_h}, \quad d''_h = d_{\Delta,q_h}, \quad d_h = d_{\Gamma+\Delta,q_h}.$$

Let $P = \sum c_h X^h$ satisfy $\Gamma_P = \Gamma + \Delta$. Define polynomials A_r and B_r, depending on P, by induction on $r \le m$. We take $A_0 = \varepsilon^{j'_0} X^{i'_0}$ and $B_0 = \varepsilon^{-j'_0} c_{i_0} X^{i''_0}$. Suppose now that $1 \le h \le m$ and write q_h in the form r/s with $s > 0$ and $(r,s) = 1$. If q_h is a slope of Γ, let β be the coefficient of $X^{i''_{h-1}}$ in B_{h-1}, and let

$$A_h = A_{h-1} + \sum_{0 \le e < d'_h} (\varepsilon^{-j''_{h-1}}\beta)^{-1} \varepsilon^{-j''_{h-1}} c_{i_h+es} X^{i'_h+es}, \quad B_h = B_{h-1}.$$

If q_h is a slope of Δ, let α be the coefficient of $X^{i'_{h-1}}$ in A_{h-1}, and let

$$A_h = A_{h-1}, \quad B_h = B_{h-1} + \sum_{0 \leq e < d''_h} (\varepsilon^{-j'_{h-1}}\alpha)^{-1}\varepsilon^{-j'_{h-1}} c_{i_h+es} X^{i''_h+es}.$$

It should be noted here that the use of negative powers of ε and inverses in these formulas conforms to the definitions in 0.2. Let then $A(P) = A_m$, $B(P) = B_m$. Then $\Gamma_{A(P)} = \Gamma$ and $\Gamma_{B(P)} = \Delta$, $P \mapsto \bigl(A(P), B(P)\bigr)$ is a polynomial map, and it induces the inverse of $\bar{p}_0$. It follows that $\bar{p}_0$ is bijective, and by 1.7 so is therefore p_0. It remains to check that p_0^{-1} is analytic. In the proof of 1.7, the polynomials A' and B' such that $p_0(A', B') = P$ are constructed as limits of converging sequences $(A_\omega)_{\omega\in\Omega}$ and $(B_\omega)_{\omega\in\Omega}$ starting with polynomials A and B such that $AB \equiv P \pmod{I_{\Gamma+\Delta}}$. We need only to check that starting from $A = A(P)$ and $B = B(P)$ the construction of the sequences $(A_\omega)_{\omega\in\Omega}$ and $(B_\omega)_{\omega\in\Omega}$ uses only polynomial functions in $A \in \bigl\{ X \in V_\Gamma^1 \bigm| \Gamma_X = \Gamma \bigr\}$, $B \in \bigl\{ X \in V_\Delta \bigm| \Gamma_X = \Delta \bigr\}$ and $P \in \bigl\{ X \in V_{\Gamma+\Delta} \bigm| \Gamma_X = \Gamma + \Delta \bigr\}$ in the sense of 0.2. The only delicate point in this construction is the choice of the solution to (1.7.1). But in the special case under consideration we can find an explicit solution. If the slope $q = q_h$ under consideration in (1.7.1) is a slope of Γ, let β be the coefficient of $X^{i''_h}$ in B. Then we can take $M = (\varepsilon^{-j''_h}\beta)^{-1}\varepsilon^{-j''_h}(P - A_{\omega'}B_{\omega'})$ and $N = 0$. If q is a slope of Δ, let α be the coefficient of $X^{i'_h}$ in A. Then we can take $M = 0$ and $N = (\varepsilon^{-j'_h}\alpha)^{-1}\varepsilon^{-j'_h}(P - A_{\omega'}B_{\omega'})$. In both cases we are dealing with polynomial functions as defined in 0.2.

1.11. Some of the results in section 1 hold under weaker assumptions on R. For example 1.1 to 1.3 hold with minor modifications for a ring R filtered by a decreasing family of ideals $(\boldsymbol{m}_i)_{i\in\mathbf{N}}$ satisfying $\boldsymbol{m}_0 = R$ and $\boldsymbol{m}_i\boldsymbol{m}_j \subset \boldsymbol{m}_{i+j}$ $(i, j \in \mathbf{N})$. In particular the formula $\Gamma_{AB} = \Gamma_A + \Gamma_B$ must be replaced by $\Gamma_{AB} \subset \Gamma_A + \Gamma_B$, with equality if $\mathrm{Gr}(R)$ is a domain. For 1.4 and 1.9 it is enough that in addition the corresponding graded ring $\mathrm{Gr}(R)$ be a polynomial ring in one variable of degree 1. Finally 1.7 and 1.10 hold for any complete discrete valuation ring.

2. Polynomials and partitions

2.1. By a partition λ of an integer $n \in \mathbf{N}$, we mean a sequence $\lambda_1 \geq \lambda_2 \geq \ldots$ of integers such that $\sum_i \lambda_i = n$, and we write $|\lambda| = n$. The non-zero λ_i's are called the parts of λ. The partition of n dual to λ is denoted λ^*. The number of parts of λ equal to $j \in \mathbf{N}^*$ is thus $\lambda_j^* - \lambda_{j+1}^*$.

The partition $n \geq 0 \geq \ldots$ is denoted (n), and (0) is also denoted $\emptyset$.

2.2. For an integer $m \in \mathbf{N}$ let $\Gamma_{(m)}$ be the smallest Newton polygon which contains $(0,1)$ and $(m,0)$. If λ is a partition of $n \in \mathbf{N}$, define

$$\Gamma_\lambda = \sum_i \Gamma_{(\lambda_i)}.$$

We have

$$\Gamma_\lambda \cap \mathbf{N}^2 = \Big\{ (i,j) \in \mathbf{N}^2 \;\Big|\; i \le n \text{ and } \sum_{h \le j} \lambda_h \ge n - i \Big\}.$$

Let

$$V_\lambda = V_{\Gamma_\lambda} = \Big\{ A = \sum_{i \le n} a_i X^i \;\Big|\; \sum_{h \le v(a_i)} \lambda_h \ge n - i \Big\} \tag{2.2.1}$$

and

$$V_\lambda^{\mathrm{reg}} = \big\{ A \in R[X] \;\big|\; \Gamma_A = \Gamma_\lambda \text{ and } \mathrm{gr}_{\Gamma_\lambda, q}(A) \text{ is multiplicity free for all } q \in \mathbf{Q} \big\}.$$

It is clear that V_λ^{reg} is a dense open subset of V_λ, and it follows from 1.7 that its elements are precisely the polynomials $A = \sum_{i=0}^{n} a_i X^i \in R[X]$ which have a decomposition $A = \prod_i P_i$ satisfying the following three conditions.

(a) $\deg(P_i) = \lambda_i$.

(b) The leading coefficient b_i of P_i is not contained in $\boldsymbol{m}$, but all the others are contained in $\boldsymbol{m}$.

(c) The constant term c_i of P_i is not contained in $\boldsymbol{m}^2$. Moreover, if $i \ne j$ and $\lambda_i = \lambda_j$, then $c_i b_j \not\equiv c_j b_i \pmod{\boldsymbol{m}^2}$.

Notice that the conditions above imply in particular that the polynomials P_i are prime. Notice also that (a), (b) and the first part of (c) are equivalent to $\Gamma_{P_i} = \Gamma_{(\lambda_i)}$.

2.3. Consider a polynomial $A = \sum_i a_i X^i \in R[X]$ of degree n. It can be written as a product of irreducible polynomials P_1, P_2, ..., of respective degrees $\lambda_1 \ge \lambda_2 \ge \dots$, and λ_1, λ_2, ... form a partition $\lambda = \pi(A)$ of n.

If moreover A is monic and $a_i \in \boldsymbol{m}$ for $i < n$, then the leading coefficients of the P_i's are the only ones which are not contained in $\boldsymbol{m}$, as is easily seen by reduction mod $\boldsymbol{m}$. It follows in this case that $P_i \in V_{(\lambda_i)}$, and therefore $A \in V_\lambda$.

The results in 2.2 provide a partial converse to this. Namely, if $A \in V_\lambda^{\mathrm{reg}}$, then $\pi(A) = \lambda$.

3. Selfdual polynomials and pairs of partitions

In this section it is assumed that $\mathrm{char}(k) \ne 2$.

3.1. For a polynomial $A \in R[X]$, let $A^* = A(-X) \in R[X]$. We say that $A \in R[X]$ is selfdual if $A^* = \pm A$, or equivalently if the subscheme of $\mathbf{A}^1_F$ defined by A is invariant under the involution $x \mapsto -x$. There are three types of irreducible polynomials which can occur as prime factors of a selfdual polynomial A.

(0) the irreducible polynomial X and its non-zero scalar multiples. They are the only irreducible selfdual polynomials of odd degree, and correspond to the only fixed geometric point of the involution $x \mapsto -x$.

(+) irreducible factors P with $P^* \neq \pm P$. Then P^* is also a factor of A, with the same multiplicity.

(−) irreducible factors P prime to X such that $P^* = \pm P$. Such factors always have even degree.

Let $A \in F[X]$ be selfdual. If moreover A is separable, then X occurs with multiplicity 1 if the degree of A is odd, and it does not occur as a factor if the degree is even. Notice that for each odd integer m, the partition $\lambda = \pi(A)$ has an even number of parts equal to m, except maybe for $m = 1$, depending on the multiplicity of the factor X. A partition which has this property for all odd integers, including 1, is called a *symplectic* partition. In addition to λ, we can associate to A a pair of partitions (α, β) defined as follows. The partition α has one part α_i for each pair $\{P, P^*\}$ of factors of type (+) of common degree α_i, and β has one part β_i for each factor of type (−) of degree $2\beta_i$. Define $\pi_+(A) = \alpha$, $\pi_-(A) = \beta$ and $\pi_\pm(A) = (\alpha, \beta)$.

Let P be a prime factor of A of type (+) or (−), and let $q = r/s$ be the unique slope of Γ_P, with $(r, s) = 1$ and $s > 0$. Then $\deg(P) = s d_{\Gamma_P, q}$. Thus if P is of type (−) and s is odd, then $d_{\Gamma_P, q}$ is even. Suppose now that P is of type (+). As P^* is also a factor of A, $\mathrm{gr}_{\Gamma_A, q}(A)$ is a multiple of $\mathrm{gr}_{\Gamma_P, q}(P)\mathrm{gr}_{\Gamma_{P^*}, q}(P^*)$. It follows in particular that if s is odd, then $\mathrm{gr}_{\Gamma_A, q}(A)$ has even degree. On the other hand, it is easily seen that $\mathrm{gr}_{\Gamma_P, q}(P) = \mathrm{gr}_{\Gamma_{P^*}, q}(P^*)$ if s is even. Therefore $\mathrm{gr}_{\Gamma_A, q}(A)$ has a square factor for each pair of prime factors of type (+) corresponding to a slope with even denominator.

3.2. For simplicity we shall now consider polynomials of even degree. If α and β are partitions, and λ is the symplectic partition of $2(|\alpha| + |\beta|)$ which has two parts of size m for each part of α of size m and one part of size $2m$ for each part of β of size m, let

$$U_\lambda = \{\, A \in V_\lambda \mid A^* = A \,\}$$

and let $U_{\alpha,\beta}$ be the closure in U_λ of

$$\{\, A \in U_\lambda \mid \Gamma_A = \Gamma_\lambda \text{ and } \mathrm{gr}_{\Gamma_\lambda, -1/s}(A) \text{ has at least } \alpha_s^* - \alpha_{s+1}^* \text{ double roots for each } s \in 2\mathbb{N}^* \,\},$$

where α^* is the partition dual to α. Then U_λ and $U_{\alpha,\beta}$ are irreducible closed subsets of V_λ. If $A \in U_\lambda$ is such that $\pi_\pm(A) = (\alpha, \beta)$, then $A \in U_{\alpha,\beta}$. Our aim is to show that there exists a dense open subset $U_{\alpha,\beta}^{\mathrm{reg}}$ of $U_{\alpha,\beta}$ on which $\pi_\pm$ takes the constant value (α, β).

Remark. If in the setting of 3.2 the partition α has no even part, then we can take

$$U^{\mathrm{reg}}_{\alpha,\beta} = U_{\alpha,\beta} \cap V^{\mathrm{reg}}_{\lambda}.$$

This special case is sufficient for the intended application to nilpotent orbits in the case of the symplectic Lie algebras.

3.3. Consider first the case where $\beta = \emptyset$ and $\alpha = (m)$ with m even. Then λ has just two parts, both equal to m. As we are seeking some non-empty open subset of $U_{\alpha,\beta}$, we may restrict our attention to $U^0_{\alpha,\beta} = \{B \in U_{\alpha,\beta} \mid \Gamma_B = \Gamma_\lambda\}$. The elements of $U^0_{\alpha,\beta}$ are the polynomials of the form $B = \sum_{i=0}^{m} b_{2i}X^{2i} \in V_\lambda$ with $b_{2m} \notin \boldsymbol{m}$, $b_0 \notin \boldsymbol{m}^3$ and

$$b_m^2 - 4b_0b_{2m} \equiv 0 \pmod{\boldsymbol{m}^3}. \tag{3.3.1}$$

We must solve the equation $AA^* = B$ with $A = \sum_{i=0}^{m} a_iX_i \in R[X]$. We must have in particular $\Gamma_B = \Gamma_A + \Gamma_A$. It follows that $a_m \notin \boldsymbol{m}$, $a_i \in \boldsymbol{m}$ for $i \neq m$ and $a_0 \notin \boldsymbol{m}^2$, and A is therefore irreducible.

If $m = 2$, we get the system of equations

$$a_0^2 = b_0, \qquad 2a_0a_2 - a_1^2 = b_2, \qquad a_2^2 = b_4.$$

Without loss of generality we may assume that both A and B are monic. The third equation is then satisfied. The assumptions on the valuation of b_0 imply that the first equation can be solved in R. Since $b_2^2 \equiv 4b_0 \pmod{\boldsymbol{m}^3}$, a_0 can moreover be chosen in such a way that $2a_0 \equiv b_2 \pmod{\boldsymbol{m}^2}$. The second equation can then be solved with $a_1 \in R$ at least if $2a_0 - b_2 \notin \boldsymbol{m}^3$, or equivalently if

$$b_2^2 - 4b_0b_4 \not\equiv 0 \pmod{\boldsymbol{m}^4}. \tag{3.3.2}$$

We can therefore use (3.3.2) to define $U^{\mathrm{reg}}_{\alpha,\beta} \subset U^0_{\alpha,\beta}$ in this case. Notice that this condition implies $a_1 \neq 0$, ensuring that A and A^* are relatively prime. Notice also that if x, y, $-x$ and $-y$ are the four roots of B, then $b_2^2 - 4b_0b_4 = b_4^2(x^2-y^2)^2$, so that for $B \in U^0_{\alpha,\beta}$ (3.3.2) is equivalent to $\delta(B) = 8$, where δ is the discriminant.

Suppose now that $m \geq 4$. In this case we claim that we can take for $U^{\mathrm{reg}}_{\alpha,\beta}$ the subset of $U^0_{\alpha,\beta}$ defined by the condition

$$2b_2b_{2m} - b_mb_{m+2} \not\equiv 0 \pmod{\boldsymbol{m}^3}. \tag{3.3.3}$$

Without loss of generality we may assume that both A and B are monic. The equation $AA^* = B$ is then a system of m equations, one for each b_{2j}, $0 \leq j < m$, with m unknowns $(a_j)_{0 \leq j < m}$. Label (j) the equation involving b_{2j}. For $i \in \mathbf{N}$ we consider these equations mod various powers of $\boldsymbol{m}$. More precisely, the equation (j) is taken mod $\boldsymbol{m}^{i+3}$ if $j = 0$, mod $\boldsymbol{m}^{i+2}$ if $0 < j \leq m/2$, and mod $\boldsymbol{m}^{i+1}$ if $m/2 < j < m$. We show by induction on i that this new system can be used to determine $a_0 \bmod \boldsymbol{m}^{i+2}$ and $a_j \bmod \boldsymbol{m}^{i+1}$ for $0 < j < m$.

For $i = 0$ we know already that $a_i \in \boldsymbol{m}$ for $0 \le i < m$. The equations are then all trivial except (0) and $(m/2)$ which become

$$a_0^2 \equiv b_0 \pmod{\boldsymbol{m}^3}, \qquad 2a_0 \equiv b_m \pmod{\boldsymbol{m}^2}.$$

The second equation gives $a_0 \bmod \boldsymbol{m}^2$, with $a_0 \notin \boldsymbol{m}^2$, and the first is then fulfilled by (3.3.1).

For $i > 0$, using the results obtained for $i-1$, the equation (0) is used first to find $a_0 \bmod \boldsymbol{m}^{i+2}$. Then the equations $\big((m/2)+j\big)$ with $0 < j < m/2$ are used to work out $a_{2j} \bmod \boldsymbol{m}^{i+1}$, and finally the equations (j) with $0 < j \le m/2$ can be used successively to find $a_{2j-1} \bmod \boldsymbol{m}^{i+1}$. It should be noted here that when $i = 1$ the equation (1),

$$2a_0a_2 - a_1^2 \equiv b_2 \pmod{\boldsymbol{m}^3},$$

in which $2a_0 \equiv b_m \pmod{\boldsymbol{m}^2}$ and $2a_2 \equiv b_{m+2} \pmod{\boldsymbol{m}^2}$, can be solved for $a_1 \pmod{\boldsymbol{m}^2}$ because of the assumption (3.3.3), and that $a_1 \notin \boldsymbol{m}^2$.

Since R is complete, this shows that the equation $AA^* = B$ with $B \in U^0_{\alpha,\beta}$ can be solved under the assumption (3.3.3). Moreover A and A^* are relatively prime. Thus (3.3.3) can be used to define $U^{\mathrm{reg}}_{\alpha,\beta} \subset U^0_{\alpha,\beta}$ in this case. Notice also that conversely if $B = AA^*$ with $A = \sum a_i X^i \in V^{\mathrm{reg}}_\lambda$ such that $a_1 \notin \boldsymbol{m}^2$, then (3.3.3) holds, i.e. $B \in U^{\mathrm{reg}}_{\alpha,\beta}$.

Proposition 3.4. *Let α and β be partitions, λ the partition of $2(|\alpha| + |\beta|)$ which has two parts of size m for each part of α of size m and one part of size $2m$ for each part of β of size m, and let $U^{\mathrm{reg}}_{\alpha,\beta}$ be the set of all polynomials $A \in R[X]$ satisfying the following three conditions.*

(i) $\Gamma_A = \Gamma_\lambda$.

(ii) *For each even integer $s \ge 2$, the polynomial $\mathrm{gr}_{\Gamma_\lambda,-1/s}(A)$ has exactly $\alpha^*_s - \alpha^*_{s+1}$ double roots.*

(iii) *A has a decomposition $A = \left(\prod_{i=1}^{\alpha_1^*} P_i P_i^*\right)\left(\prod_{i=1}^{\beta_1^*} Q_i\right)$, with $\Gamma_{P_i} = \Gamma_{(\alpha_i)}$ for each i and $\Gamma_{Q_j} = \Gamma_{(2\beta_j)}$ for each j, and moreover in each P_i the coefficient of X is not contained in $\boldsymbol{m}^2$ $(1 \le i \le \alpha_1^*)$.*

Then $U^{\mathrm{reg}}_{\alpha,\beta}$ is a dense open subset of $U_{\alpha,\beta}$ on which $\pi_\pm$ takes the constant value (α,β).

Proof. It is clear that $\pi_\pm(A) = (\alpha,\beta)$ for every polynomial $A \in R[X]$ which satisfies (iii). We need therefore only to prove that $U^{\mathrm{reg}}_{\alpha,\beta}$ is a non-empty open subset of $U_{\alpha,\beta}$. Let $U^0_{\alpha,\beta}$ be the set of all $A \in U_{\alpha,\beta}$ which satisfy (i) and (ii). Then $U^0_{\alpha\beta}$ is a dense open subset of $U_{\alpha,\beta}$. It follows from 1.7 that every $A \in U^0_{\alpha,\beta}$ can be written as a product $(\prod_i B_i)(\prod_j Q_j)$, with $\Gamma_{B_i} = \Gamma_{(\alpha_i)} + \Gamma_{(\alpha_i)}$ for each i and $\Gamma_{Q_j} = \Gamma_{(2\beta_j)}$

for each j. So for $A \in U^0_{\alpha,\beta}$, (iii) is equivalent to the requirement that the B_i's be of the form $P_i P_i^*$ with the coefficients of X in the P_i's not contained in $\boldsymbol{m}^2$. We must show that this is an open condition in $U^0_{\alpha,\beta}$. By 1.10 it is enough to prove this in the case where Γ_λ has only one slope, that is, when all the parts of λ are equal to the same number m. If m is odd the condition is empty. Let thus m be even. If $m \geq 4$, then 1.9 and (3.3.3) show that $U^{\mathrm{reg}}_{\alpha,\beta}$ is the intersection of $U^0_{\alpha,\beta}$ with the inverse image of a Zariski open subset of $U_\lambda/\boldsymbol{m}U_\lambda$. We are thus left with the case $m = 2$. Let δ be the discriminant. We may assume that $\delta(A) \neq 0$. Then A has $N = |\lambda|$ distinct roots $x_1, \ldots, x_N$, and for $i \neq j$ we have $v(x_i - x_j) = 1/2$, with the following exceptions. For each factors B_i of A, the contribution to the discriminant coming from the 12 pairs of distinct roots of B_i is at least 8, instead of 6, with equality if and only B_i satisfies (3.3.2). Thus $\delta(A) \geq N(N-1)/2 + 2\alpha_1^*$, with equality if and only if (3.3.2) holds for each B_i $(1 \leq i \leq \alpha_1^*)$. Thus in this case also $U^{\mathrm{reg}}_{\alpha,\beta}$ is open.

4. Characteristic polynomials

4.1. Let $n \in \mathbf{N}$. The $n{\times}n$ identity matrix is denoted $\mathbf{I}_n$, and the characteristic polynomial of an $n{\times}n$-matrix x is $\operatorname{char pol}(x) = \det(X\mathbf{I}_n - x)$. For $x \in \mathbf{M}_n(R)$, let $\bar{x}$ be the image of x in $\mathbf{M}_n(k)$. Then $v(\det(x)) \geq n - \operatorname{rank}(\bar{x})$. Equivalently, $v(\det(x))$ is not smaller than the number of nilpotent Jordan blocks of $\bar{x}$.

If D is a subset of $\{1,2,\ldots,n\}$ consisting of $|D| = d$ elements and x is an $n{\times}n$-matrix, let x_D denote the $d{\times}d$-matrix formed by the entries of A indexed by the elements of $D \times D$.

4.2. Given $m \in \mathbf{N}^*$ and $c \in R$, let $N_{m,c}$ be the matrix $(a_{i,j}) \in \mathbf{M}_m(R)$ defined by

$$a_{i,j} = \begin{cases} 1 & \text{if } 1 \leq i = j-1 < m, \\ c & \text{if } i = m \text{ and } j = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Then $\operatorname{char pol}(N_{m,c}) = X^m - c$.

Proposition 4.3. *Let $x \in \mathbf{M}_n(R)$ be such that $\bar{x} \in \mathbf{M}_n(k)$ is nilpotent with Jordan blocks of dimension $\lambda_1 \geq \lambda_2 \geq \ldots$. Then the following hold.*

(a) *For every $y \in x + \boldsymbol{m}\mathbf{M}_n(R)$, $\operatorname{char pol}(y) \in V_\lambda$.*

(b) *There is a dense open subset U of $x + \boldsymbol{m}\mathbf{M}_n(R)$ such that $\operatorname{char pol}(y) \in V_\lambda^{\mathrm{reg}}$ for every $y \in U$. In particular the degrees of the irreducible factors of the characteristic polynomial of y are $\lambda_1, \lambda_2, \ldots$.*

Proof. We may assume that $\bar{x}$ is in Jordan normal form. The coefficient a_i of X^i in the characteristic polynomial of y is

$$a_i = (-1)^{n-i} \sum_{\substack{D \subset \{1,\ldots,n\} \\ |D| = n-i}} \det(y_D). \tag{4.3.1}$$

The Jordan blocks of $\bar{y}_D$ are obtained by truncating and partitionning those of $\bar{y} = \bar{x}$. It follows that for every subset D of $\{1, \dots, n\}$ consisting of $n-i$ elements we have

$$v(\det(y_D)) \geq \min\left\{ j \in \mathbf{N} \;\middle|\; \sum_{h \leq j} \lambda_h \geq n-i \right\},$$

and therefore

$$\sum_{h \leq v(a_i)} \lambda_h \geq n-i,$$

which by (2.2.1) shows that $\operatorname{char pol}(y) \in V_\lambda$. This is (a).

Let now $U = \{ y \in x + \boldsymbol{m}\,\mathrm{M}_n(R) \mid \operatorname{char pol}(y) \in V_\lambda^{\mathrm{reg}} \}$. Then U is an open subset of $x + \boldsymbol{m}\,\mathrm{M}_n(R)$. For each part λ_i of λ choose $c_i \in \boldsymbol{m}$ in such a way that $c_i \notin \boldsymbol{m}^2$ and $c_i \not\equiv c_j \pmod{\boldsymbol{m}^2}$ when $\lambda_i = \lambda_j$ with $i \neq j$. Taking y with a block decomposition in which the diagonal blocks are the matrices N_{λ_i, c_i} defined in 4.2 and the other blocks are zero, we have $y \in U$. Thus U is non-empty. This proves (b).

4.4. *Remark.* Let $\Gamma = \Gamma_\lambda$, $\ell \in \mathbf{N}^*$. Suppose that λ has exactly d parts equal to ℓ and that the nilpotent matrix $\bar{y} \in \mathrm{M}_n(k)$ is in Jordan canonical form. Then in order to compute the coefficient of Y^i in $\mathrm{gr}_{\Gamma,-1/\ell}(\operatorname{char pol}(y))$, it is sufficient in the sum (4.3.1) to take those subsets D of $\{1, \dots, n\}$ which capture all the Jordan blocks of $\bar{y}$ of size larger than ℓ and exactly $d-i$ Jordan blocks of size ℓ.

5. Characteristic polynomials of infinitesimal symplectic transformations

In this section it is assumed that $\operatorname{char}(k) \neq 2$.

5.1. Given a commutative ring A and $n \in \mathbf{N}^*$, we have a symplectic Lie algebra

$$\boldsymbol{sp}_{2n}(A) = \{ X \in \mathrm{M}_{2n}(A) \mid {}^tX J_{2n} + J_{2n} X = 0 \},$$

which is acted on by the symplectic group

$$Sp_{2n}(A) = \{ X \in \mathrm{M}_{2n}(A) \mid {}^tX J_{2n} X = J_{2n} \},$$

where the matrix $J_{2n} \in \mathrm{M}_{2n}(A)$ is defined by

$$(J_{2n})_{i,j} = \begin{cases} 1 & \text{if } i+j = 2n+1 \text{ and } i \leq n, \\ -1 & \text{if } i+j = 2n+1 \text{ and } i > n, \\ 0 & \text{otherwise.} \end{cases}$$

Let $x \in \boldsymbol{sp}_{2n}(k)$ be nilpotent. The orbit of x under the action of $Sp_{2n}(k)$ is characterized by the partition λ whose parts are the dimensions of the Jordan blocks of

x. Moreover λ is a symplectic partition, that is, odd parts come in pairs, and every symplectic partition of $2n$ arises in this way.

5.2. For $m \in \mathbf{N}^*$ and $c \in R$ define $A_{2m,c} \in \mathrm{M}_{2m}(R)$ to be the matrix which has a block decomposition with $N_{m,c}$ and $-N_{m,c}$ as diagonal blocks and zeroes as non-diagonal blocks, and let $B_{2m,c} \in \mathrm{M}_{2m}(R)$ have coefficients $b_{i,j}$ defined by

$$b_{i,j} = \begin{cases} 1 & \text{if } 1 \le i = j-1 \le m, \\ -1 & \text{if } m < i = j-1 < 2m, \\ c & \text{if } i = 2m \text{ and } j = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Then both $A_{2m,c}$ and $B_{2m,c}$ belong to $\boldsymbol{sp}_{2m}(R)$. Moreover

$$\operatorname{char\,pol}(A_{2m,c}) = \begin{cases} (X^m - c)^2 & \text{if } m \text{ is even,} \\ X^{2m} - c^2 & \text{if } m \text{ is odd,} \end{cases}$$

and

$$\operatorname{char\,pol}(B_{2m,c}) = X^{2m} + (-1)^m c.$$

Proposition 5.2. *Let $x \in \boldsymbol{sp}_{2n}(R)$ be such that $\bar{x} \in \boldsymbol{sp}_{2n}(k)$ is nilpotent with Jordan blocks of size $\lambda_1 \ge \lambda_2 \ge \dots$. Let α be the partition which has one part α_i for each pair of odd parts of λ of size α_i, and let β be the partition which has one part β_i for each even part of λ of size $2\beta_i$. Then the following hold.*

(a) *For every $y \in x + \boldsymbol{m}\,\boldsymbol{sp}_{2n}(R)$, $\operatorname{char\,pol}(y) \in U_{\alpha,\beta}$.*

(b) *There is a dense open subset U of $x + \boldsymbol{m}\,\boldsymbol{sp}_{2n}(R)$ such that $\operatorname{char\,pol}(y) \in U^{\mathrm{reg}}_{\alpha,\beta}$ for every $y \in U$. In particular the characteristic polynomial of y has one irreducible selfdual factor of degree $2\beta_i$ for each part β_i of β, and one pair of dual irreducible factors of degree α_i for each part α_i of α.*

Proof. The polynomial $\operatorname{char\,pol}(y)$ is selfdual since $y \in \boldsymbol{sp}_{2n}(R)$, and by 4.3(a) we know already that this polynomial belongs to V_λ. Thus $\operatorname{char\,pol}(y) \in U_\lambda$. As α has no even part we have $U_\lambda = U_{\alpha,\beta}$. This proves (a).

Let now $U = \{ y \in x + \boldsymbol{m}\,\boldsymbol{sp}_{2n}(R) \mid \operatorname{char\,pol}(y) \in U^{\mathrm{reg}}_{\alpha,\beta} \}$. Then U is open in $x + \boldsymbol{m}\,\boldsymbol{sp}_{2n}(R)$, and we need only to check that $U \neq \emptyset$. Choose coefficients $c_i \in \boldsymbol{m} \setminus \boldsymbol{m}^2$, one for each part α_i of α, and $d_i \in \boldsymbol{m} \setminus \boldsymbol{m}^2$, one for each part β_i of β, such that $c_i^2 \not\equiv c_j^2 \pmod{\boldsymbol{m}^3}$ when $\alpha_i = \alpha_j$ with $i \neq j$, and $d_i \not\equiv d_j \pmod{\boldsymbol{m}^2}$ when $\beta_i = \beta_j$ with $i \neq j$. Let $y \in \mathrm{M}_{2n}$ (resp. $J \in \mathrm{M}_{2n}$) be the matrix which has a block decomposition with one diagonal block $A_{2\alpha_i,c_i}$ (resp $J_{2\alpha_i}$) for each part α_i of α, one diagonal block $B_{2\beta_i,d_i}$ (resp $J_{2\beta_i}$) for each part β_i of β, and in which all other blocks are zero. Then ${}^t yJ + Jy = 0$, the dimensions of the Jordan blocks of y are given by the parts of λ, and $\operatorname{char\,pol}(y) \in U^{\mathrm{reg}}_{\alpha,\beta}$. As J and J_{2n} define equivalent bilinear forms and the nilpotent

$Sp_{2n}(k)$-orbits in $\boldsymbol{sp}_{2n}(k)$ are characterized by the dimensions of the Jordan blocks of their elements, it follows that U is non-empty. This proves (b).

6. Characteristic polynomials of infinitesimal orthogonal transformations

As in section 5, it is assumed that $\operatorname{char}(k) \neq 2$.

6.1. Given a commutative ring A in which 2 is invertible and $N \in \mathbf{N}^*$, we have an orthogonal Lie algebra

$$\boldsymbol{o}_N(A) = \{\, X \in \mathbf{M}_N(A) \mid {}^tXK_N + K_NX = 0 \,\}$$

acted on by the orthogonal group

$$O_N(A) = \{\, X \in \mathbf{M}_N(A) \mid {}^tXK_NX = K_N \,\},$$

where the matrix $K_N \in \mathbf{M}_N(A)$ is defined by

$$(K_N)_{i,j} = \begin{cases} 1 & \text{if } i+j = N+1, \\ 0 & \text{otherwise.} \end{cases}$$

If $N = N_1 + N_2$ with $N_1 > N_2$ both odd, let also $K_{N_1,N_2} \in \mathbf{M}_N(R)$ be the matrix which has a block decomposition with K_{N_1} and K_{N_2} as diagonal blocks and zeroes as non-diagonal blocks. It is clear that the bilinear forms defined by K_N and K_{N_1,N_2} are equivalent.

Let $x \in \boldsymbol{o}_N(k)$ be nilpotent. The orbit of x under the adjoint action of $O_N(k)$ is characterized by the partition λ whose parts are the dimensions of the Jordan blocks of x. Moreover λ is an orthogonal partition, that is, even parts come in pairs of equal parts, and every orthogonal partition of N arises in this way.

The characterisic polynomial of $x \in \boldsymbol{o}_N$ is a selfdual polynomial. If N is odd, it is therefore a multiple of X. Instead of the characteristic polynomial, it will be convenient to use the polynomial

$$\operatorname{char pol}^{\sim}(x) = \begin{cases} \operatorname{char pol}(x) & \text{if } N \text{ is even,} \\ X^{-1}\operatorname{char pol}(x) & \text{if } N \text{ is odd,} \end{cases}$$

which is also selfdual.

We must thus relate orthogonal and symplectic partitions in this case, and more combinatorics will be needed than for the symplectic case.

6.2. For $m \in \mathbf{N}^*$ odd and $c \in R$ define $A_{2m,c} \in \mathbf{M}_{2m}(R)$ to be the matrix which has a block decomposition with $N_{m,c}$ and $-N_{m,c}$ as diagonal blocks and zeroes as non-diagonal blocks. Then $A_{2m,c} \in \boldsymbol{o}_{2m}(R)$, and as in 5.2 $\operatorname{char pol}(A_{2m,c}) = X^{2m} - c^2$. If

m is even, let $A_{2m,c} \in \mathbf{M}_{2m}(R)$ be the matrix with coefficients $a_{i,j}$ defined as follows.

$$a_{i,j} = \begin{cases} 1 & \text{if } 1 \leq i = j-1 < m, \\ -1 & \text{if } m < i = j-1 < 2m, \\ c & \text{if } i = m \text{ and } j = 1, \\ -c & \text{if } i = 2m \text{ and } j = m+1, \\ \varepsilon & \text{if } i = m-1 \text{ and } j = 1, \\ -\varepsilon & \text{if } i = 2m \text{ and } j = m+2, \\ 0 & \text{otherwise.} \end{cases}$$

Then $\operatorname{char\,pol}(A_{2m,c}) = X^{2m} - 2cX^m - \varepsilon^2 X^2 + c^2$.

Let $B_{2m+1,c} \in \mathbf{M}_{2m+1}(R)$ have coefficients $b_{i,j}$ defined by

$$b_{i,j} = \begin{cases} 1 & \text{if } 1 \leq i = j-1 \leq m, \\ -1 & \text{if } m < i = j-1 \leq 2m, \\ c & \text{if } i = 2m \text{ and } j = 1, \\ -c & \text{if } i = 2m+1 \text{ and } j = 2, \\ 0 & \text{otherwise.} \end{cases}$$

Then $B_{2m+1,c} \in \mathfrak{o}_{2m+1}(R)$ and

$$\operatorname{char\,pol}(B_{2m+1,c}) = X^{2m+1} + (-1)^m 2cX.$$

Let also $B_{1,c} = 0 \in \mathbf{M}_1(R)$. Then $\operatorname{char\,pol}(B_{1,c}) = X$.

Let now $N = N_1 + N_2$ with $N_1 > N_2$ both odd, and c, $c' \in R$, and let $B^{(2)}_{N_1,N_2,c,c'} \in \mathbf{M}_N(R)$ have coefficients $b^{(2)}_{i,j}$ defined by

$$b^{(2)}_{i,j} = \begin{cases} 1 & \text{if } 1 \leq i = j-1 < N_1/2 \text{ or } N_1 < i = j-1 < N_1 + N_2/2, \\ -1 & \text{if } N_1/2 < i = j-1 < N_1 \text{ or } N_1 + N_2/2 < i = j-1 < N, \\ c & \text{if } i = N_1 - 1 \text{ and } j = 1, \\ -c & \text{if } i = N_1 \text{ and } j = 2, \\ -c' & \text{if } i = N_1 \text{ and } j = N_1 + 1, \\ c' & \text{if } i = N \text{ and } j = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Then $B^{(2)}_{N_1,N_2,c,c'}$ belongs to $\{ A \in \mathbf{M}_N \mid {}^t A K_{N_1,N_2} + K_{N_1,N_2} A = 0 \}$. Moreover

$$\operatorname{char\,pol}(B_{N_1,N_2,c,c'}) = X^N + (-1)^{(N_1-1)/2} 2cX^{N_2+1} - (-1)^{N/2} c'^2.$$

6.3. Let λ be an orthogonal partition of $N \in \mathbf{N}^*$. We define a symplectic partition $\mu = \sigma(\lambda)$ as follows.

$$\mu_i = \begin{cases} \lambda_i - 1 & \text{if } \lambda_i \text{ is odd, } i \text{ is odd and } \lambda_i \neq \lambda_{i+1}, \\ \lambda_i + 1 & \text{if } \lambda_i \text{ is odd, } i \text{ is even and } \lambda_i \neq \lambda_{i-1}, \\ \lambda_i & \text{otherwise.} \end{cases}$$

If $N \in \{2n, 2n+1\}$, with $n \in \mathbf{N}$, then μ is a symplectic partition of $2n$.

Define also a function $\tau_\lambda : \mathbf{N}^* \to \{\pm 1\}$ by setting $\tau_\lambda(\ell) = -1$ if ℓ is a part μ_i of μ and at least one of the following two conditions is fulfilled.

(a) $\mu_i \neq \lambda_i$, or

(b) $\sum_{j\leq i} \mu_j < \sum_{j\leq i} \lambda_j$.

Otherwise set $\tau_\lambda(\ell) = 1$. Notice that $\tau_\lambda(\ell) = 1$ when ℓ is odd, and that if $\tau_\lambda(\ell) = 1$, then μ has an even number of parts equal to ℓ.

Let now α be the partition which has one part α_i for each pair of parts of μ of size α_i when $\tau_\lambda(\alpha_i) = 1$, and let β be the partition which has one part β_i for each even part of μ of size $2\beta_i$ when $\tau_\lambda(2\beta_i) = -1$. Then $|\alpha| + |\beta| = n$, and we write $(\alpha, \beta) = \pi_\pm(\lambda)$.

Proposition 6.4. *Let $x \in o_N(R)$ be such that $\bar{x} \in o_N(k)$ is nilpotent with Jordan blocks of dimension $\lambda_1 \geq \lambda_2 \geq \dots$. Let also $n \in \mathbf{N}$ be such that $N \in \{2n, 2n+1\}$, and let $(\alpha,\beta) = \pi_\pm(\lambda)$ be defined as in 6.3. Then the following hold.*

(a) *For every $y \in x + \boldsymbol{m}\, o_N(R)$, $\operatorname{char pol}^\sim(y) \in U_{\alpha,\beta}$.*

(b) *There is a dense open subset U of $x + \boldsymbol{m}\, o_N(R)$ such that $\operatorname{char pol}^\sim(y) \in U^{\mathrm{reg}}_{\alpha,\beta}$ for every $y \in U$. In particular, for $y \in U$ we have $\pi_\pm(\operatorname{char pol}^\sim(y)) = (\alpha,\beta)$, or equivalently the characteristic polynomial of y has one pair of dual irreducible factors of degree α_i for each part α_i of α, and one irreducible selfdual factor of degree $2\beta_i$ for each part β_i of β.*

Proof. Let the partition μ of $2n$ and the map $\tau_\lambda : \mathbf{N}^* \to \{\pm 1\}$ be defined as in 6.3. This notation and that introduced in the statement of the proposition are in force for the remaining part of this paragraph which is devoted to the proof of the following claims, the combination of which implies the proposition.

Claim 1. There exists $y \in x + \boldsymbol{m}\, o_N(R)$ such that $\Gamma_{\operatorname{char pol}^\sim(y)} = \Gamma_\mu$.

Claim 2. The element y in claim 1 can be chosen in such a way that for each odd integer ℓ the polynomial $\operatorname{gr}_{\Gamma_\mu,-1/\ell}(\operatorname{char pol}^\sim(y))$ is square free.

Claim 3. The element y in claim 1 can be chosen in such a way that for each even integer $\ell > 0$ such that $\tau_\lambda(\ell) = 1$, the polynomial $\operatorname{gr}_{\Gamma_\mu,-1/\ell}(\operatorname{char pol}^\sim(y))$ is the square of some square free polynomial, and moreover the corresponding factors of degree 2ℓ of $\operatorname{char pol}^\sim(y)$ satisfy the condition (3.3.2) (for $\ell = 2$) or (3.3.3) (for $\ell > 2$).

Claim 4. For every $y \in x + \boldsymbol{m}\, o_N(R)$, $\operatorname{char pol}^\sim(y) \in V_\mu$.

Claim 5. If $\tau_\lambda(\ell) = 1$ and $\ell > 0$ is even, then for every $y \in \boldsymbol{m}\, o_N(R)$ the polynomial $\operatorname{gr}_{\Gamma_\mu,-1/\ell}(\operatorname{char pol}^\sim(y))$ is a square.

Claim 6. Let $\ell > 0$ be an even integer such that $\tau_\lambda(\ell) = -1$. Then the element y in claim 1 can be chosen so that $\operatorname{gr}_{\Gamma_\mu,-1/\ell}(\operatorname{char pol}^\sim(y))$ is square free.

6.5. Let λ^{even} (resp. λ^{odd}) be the partition which consists of all the even (resp. odd) parts of λ. Choose elements $c_i \in \boldsymbol{m} \setminus \boldsymbol{m}^2$, one for each even i such that $\lambda_i^{\mathrm{even}} \neq 0$

and one for each odd i such that $\lambda_i^{\mathrm{odd}} \neq 0$. For each odd i such that $\lambda_i^{\mathrm{odd}} \neq \lambda_{i+1}^{\mathrm{odd}} \neq 0$, choose also an element $c_i' \in \boldsymbol{m} \setminus \boldsymbol{m}^2$. Let then $y \in \mathbf{M}_N(R)$ (resp. $K \in \mathbf{M}_N(R)$) be the matrix which has a block decomposition in which the non-diagonal blocks are all zero and the diagonal ones are defined as follows.

(a) For each even i such that $\lambda_i^{\mathrm{even}} \neq 0$, there is a diagonal block $A_{2\lambda_i^{\mathrm{even}},c_i}$ (resp. $K_{2\lambda_i^{\mathrm{even}}}$).

(b) For each odd i such that $\lambda_i^{\mathrm{odd}} = \lambda_{i+1}^{\mathrm{odd}} \neq 0$, there is a diagonal block $A_{2\lambda_i^{\mathrm{odd}},c_i}$ (resp. $K_{2\lambda_i^{\mathrm{odd}}}$).

(c) For each odd i such that $\lambda_i^{\mathrm{odd}} \neq \lambda_{i+1}^{\mathrm{odd}} \neq 0$, there is a diagonal block $B^{(2)}_{\lambda_i^{\mathrm{odd}},\lambda_{i+1}^{\mathrm{odd}},c_i,c_i'}$ (resp. $K_{\lambda_i^{\mathrm{odd}},\lambda_{i+1}^{\mathrm{odd}}}$).

(d) For each odd i such that $\lambda_i^{\mathrm{odd}} \neq \lambda_{i+1}^{\mathrm{odd}} = 0$, there is a diagonal block $B_{\lambda_i^{\mathrm{odd}},c_i}$ (resp. $K_{\lambda_i^{\mathrm{odd}}}$).

Then ${}^t yK + Ky = 0$, the bilinear form defined by K is equivalent to that defined by K_N, and by reduction mod $\boldsymbol{m}$, y becomes a nilpotent matrix which has Jordan blocks of dimension λ_1, λ_2, ... Moreover the characteristic polynomial of y is the product of the characteristic polynomials of the diagonal blocks, and these are computed in 6.2. It follows immediately that $\Gamma_{\mathrm{char\,pol}^\sim(y)} = \Gamma_\mu$. This proves claim 1. By choosing carefully the coefficients c_i and c_i', we can also prove claim 2 and claim 3. For claim 2, notice that if ℓ is odd, then the irreducible factors of degree ℓ of $\mathrm{char\,pol}^\sim(y)$ arise from (b) above with $\lambda_i^{\mathrm{odd}} = \ell$, and each such occurence gives one factor $X^\ell - c_i$ and one factor $X^\ell + c_i$. If the c_i's are such that $c_i \not\equiv \pm c_j \pmod{\boldsymbol{m}^2}$ when $\lambda_i = \lambda_j$ with $i \neq j$, the element y satisfies therefore the requirements of claim 2. Similarly, if ℓ is even and $\tau_\lambda(\ell) = 1$, then the factors of degree ℓ of $\mathrm{char\,pol}^\sim(y)$ arise from (a) above with $\lambda_i = \ell$ and each such occurence gives a block whose characteristic polynomial is $X^{2\ell} - 2c_iX^\ell - \varepsilon^2X^2 + c_i^2$, for which (3.3.2) or (3.3.3) holds. This proves claim 3.

6.6. In this section we prove claim 4. That is, we show that for every $y \in x + \boldsymbol{m}\,\boldsymbol{o}_N(R)$ we have $\mathrm{char\,pol}^\sim(y) \in V_\mu$. It is actually sufficient to prove this for y in some non-empty open subset of $x + \boldsymbol{m}\,\boldsymbol{o}_N(R)$. By claim 1, which has been established in the previous section, we may therefore assume that $\Gamma_{\mathrm{char\,pol}^\sim(y)} \supset \Gamma_\mu$.

If N is odd, let $\Gamma = (1,0) + \Gamma_\mu$, and otherwise let $\Gamma = \Gamma_\mu$. Let also $\mathrm{char\,pol}(y) = A = \sum_{i=0}^N a_iX^i$. Claim 4 is equivalent to the assertion that $\Gamma_A \subset \Gamma$. By 4.3(a), we know already that $A \in V_\lambda$, and we must prove that if $(d,e) \in (\mathbf{N}^2 \cap \Gamma_\lambda) \setminus \Gamma$, then $v(a_d) \neq e$. If N is odd, then there are such points with $d = 0$, and in this case we know already that $a_0 = 0$. The remaining such points (d,e) are exactly those of the form $(N - \sum_{j\leq e}\lambda_j, e)$ for integers $e < \lambda_1^*$ such that $\sum_{j\leq e}\lambda_j > \sum_{j\leq e}\mu_j$. If $\Gamma_A \not\subset \Gamma$, then there is a smallest $e \in \mathbf{N}$ such that $v(a_d) = e$ with $N - d = \sum_{j\leq e}\lambda_j > \sum_{j\leq e}\mu_j$. Then μ_e is even. Let $\ell = \mu_e$, e' the smallest integer such that $\mu_{e'+1} = \ell$, and $q =$

$(e'-e)\,/\big((e-e')\ell+1\big)$. By minimality of e and since $\Gamma_A \supset \Gamma$, q is a slope of Γ_A, and

$$d_{\Gamma_A,q} = \begin{cases} 1 & \text{if } \lambda_e = \ell, \\ \mu^*_{\ell+1} - \mu^*_{\ell+2} + 1 & \text{if } \lambda_e = \ell + 1. \end{cases}$$

As μ is a symplectic partition and ℓ is even, $\mathrm{gr}_{\Gamma_A,q}(A)$ is therefore a polynomial of odd degree. But the denominator of q is also an odd number, and as noted in 3.1 this forces $\mathrm{gr}_{\Gamma_A,q}(A)$ to have even degree, a contradiction. Thus $\Gamma_A \subset \Gamma$, and claim 4 is proved.

6.7. In this section we prove claim 5. Let ℓ be some even part of λ and assume that $\tau_\lambda(\ell) = 1$. We must show that $\mathrm{gr}_{\Gamma_\mu,-1/\ell}(\mathrm{char\,pol}^\sim(y))$ is a square. The assumption on $\tau_\lambda(\ell)$ implies that $\mathrm{gr}_{\Gamma_\mu,-1/\ell}(\mathrm{char\,pol}^\sim(y)) = \mathrm{gr}_{\Gamma_\lambda,-1/\ell}(\mathrm{char\,pol}(y))$, and as in (4.3.1) the coefficient a_i of $\mathrm{char\,pol}(y) = \sum_{i=0}^N a_i X^i$ is

$$a_i = (-1)^{N-i} \sum_{\substack{D \subset \{1,\dots,N\} \\ |D| = N-i}} \det(y_D). \tag{6.7.1}$$

We are therefore in a position to use 4.4, which we shall use first to reduce the problem to the case where $\ell = 2$ and all the parts of λ are equal to 2, and then to settle this special case. Before doing this, it is however convenient to reformulate the problem with another bilinear form and another element x to make the Jordan blocks apparent.

Instead of working with the bilinear form defined by K_N, we may also use the form defined by the matrix $K \in \mathrm{M}_N(R)$ which has one diagonal block K_{λ_i} for each odd part λ_i of λ, one diagonal block $K_{2\lambda_i}$ for each pair of even parts of λ equal to λ_i, and in which the non-diagonal blocks are zero. This bilinear form defines an orthogonal Lie algebra $\boldsymbol{o}(R) = \{ X \in \mathrm{M}_N(R) \mid {}^tXK + KX = 0 \}$. We may then take for x the matrix which has a similar block decomposition in which the non-diagonal blocks are zero, with one diagonal block $B_{\lambda_i,0}$ for each odd part λ_i of λ, and one diagonal block

$$\begin{pmatrix} N_{\lambda_i,0} & 0 \\ 0 & -N_{\lambda_i,0} \end{pmatrix} \tag{6.7.2}$$

for each pair of even parts of λ equal to λ_i. Taking into account the further block decomposition provided by (6.7.2), we can refine the given block decompositions of K and x to decompositions in which the (i,j)-block is a $\lambda_i \times \lambda_j$-matrix $(1 \le i,j \le \lambda_1^*)$. We have thus a map $\pi : \{1,\dots,N\} \to \{1,\dots,\lambda_1^*\}$ such that $\pi^{-1}(i) \times \pi^{-1}(j)$ consists precisely of the $\lambda_i\lambda_j$ pairs of indices corresponding to the (i,j)-block of the matrix x.

When looking at $\mathrm{gr}_{\Gamma_\lambda,-1/\ell}(\mathrm{char\,pol}(y))$, for $y \in x + \boldsymbol{m}\,\boldsymbol{o}(R)$, we use the same block decomposition for y. Let $z \in \mathrm{M}_{\lambda_1^*}(k)$ be the matrix such that $z_{i,j}$ is the image in k of ε^{-1} times the $(\lambda_i,1)$-coefficient of the (i,j)-block of y. We use now (6.7.1) and 4.4 to compute the coefficients of $\mathrm{gr}_{\Gamma_\lambda,-1/\ell}(\mathrm{char\,pol}(y))$. Let $m = \lambda^*_{\ell+1}$ be the number of parts of λ which are strictly larger than ℓ and $d = \lambda^*_\ell - \lambda^*_{\ell+1}$ the number of parts equal to ℓ. Then for $0 \leq i \leq d$, the coefficient b_i of Y^i in $\mathrm{gr}_{\Gamma_\lambda,-1/\ell}(\mathrm{char\,pol}(y)) \in k[X]$ is $\varepsilon^{-m-d+i}a_{i\Gamma_\lambda,q+\ell i} + \boldsymbol{m} \in k$. Now 4.4 says that in order to compute b_i we need only to consider the subsets D of $\{1,\ldots,N\}$ which are of the form $D = \pi^{-1}(D^*)$ with $|D^*| = m+d-i$. Moreover y_D contributes by $\pm\det(z_{D^*})$ to b_i, where the sign depends only on the number of parts of λ which are larger than ℓ and congruent to 3 mod 4.

It follows easily that we may successively assume the following:

(a) The only non-zero coefficients of $y - x$ are those appearing in z.

(b) λ has no part smaller than ℓ.

(c) $\ell = 2$.

(d) The odd parts of λ are all equal to 3.

The assumption on $\tau_\lambda(\ell)$ means that λ has an even number of odd parts larger than ℓ. Thus λ has now an even number of parts equal to 3. We can therefore repeat the construction above for K and x, but taking the odd parts in pairs and treating them in the same way as pairs of equal even parts. This time we see that for all pairs of equal parts of λ larger than ℓ the actual size is irrelevant. We may thus as well assume that all the parts of λ are equal to 2 or 4.

We want actually to reduce further to the case where all the parts of λ are equal to 2. The only difference between the parts of size 4 and those of size 2 in the formation of the coefficients of $\mathrm{gr}_{\Gamma_\lambda,-1/2}(\mathrm{char\,pol}(y))$ is that we consider only subsets D^* of $\{1,\ldots,\lambda_1^*\}$ which contain every integer i such that $\lambda_i = 4$. This constraint can be lifted as follows. Introduce a new variable T, and multiply the coefficients of the matrix $y - x$ by 1, T, or T^2 depending on whether they are in a $2{\times}2$-block, a $2{\times}4$ or a $4{\times}2$-block, or a $4{\times}4$-block. This gives a new matrix $\tilde{y} \in \mathbf{M}_N(R[T])$. Then ${}^t\tilde{y}K + K\tilde{y} = 0$ and we get also a corresponding new matrix $\tilde{z} \in \mathbf{M}_{\lambda_1^*}(k[T])$. Now up to sign b_i is the coefficient of T^{2m} in

$$\sum_{\substack{D^* \subset \{1,\ldots,\lambda_1^*\} \\ |D^*| = m+d-i}} \det(\tilde{z}_{D^*}).$$

Filtering $R[T]$ by the powers of $\boldsymbol{m}\,R[T]$, we get a polynomial $\mathrm{gr}_{\Gamma_\lambda,-1/2}(\mathrm{char\,pol}(\tilde{y})) \in k[Y,T]$. As the leading coefficient of the square of a polynomial in $(k[Y])[T]$ is itself a square in $k[Y]$, it is thus enough to handle the case where all the parts of λ are equal to 2.

So let all the part of λ be equal to 2, and let $n = N/4$. We use now the quadratic form defined by K_N. Using 4.4 again, we may assume that y has a block decomposition

$$y = \begin{pmatrix} 0 & 0 & \mathbf{I}_n & 0 \\ 0 & 0 & 0 & -\mathbf{I}_n \\ A & B & 0 & 0 \\ C & D & 0 & 0 \end{pmatrix} \tag{6.7.3}$$

where A, B, C and D are $n \times n$-matrices with coefficients in $\mathfrak{m}$ such that

$$ {}^tAK_n + K_nD = {}^tBK_n + K_nB = {}^tCK_n + K_nC = 0, \tag{6.7.4} $$

and we must show that $\mathrm{gr}_{\Gamma_\lambda,-1/2}(\mathrm{char\,pol}(y))$ is a square. This actually holds since in this case $\mathrm{char\,pol}(y)$ is a square, as we show now.

Let E be an algebraically closed field and let V be the set of all matrices $y \in \mathrm{M}_N(E)$ which have a block decomposition as in (6.7.3) and for which (6.7.4) holds. It is enough to prove that $\mathrm{char\,pol}(y)$ is a square for y in some dense open subset V^0 of V.

Suppose first that $B = 0$. Then $\mathrm{char\,pol}(y) = \mathrm{char\,pol}(y_1)\mathrm{char\,pol}(y_2)$ where

$$ y_1 = \begin{pmatrix} 0 & \mathbf{I}_n \\ A & 0 \end{pmatrix}, \quad y_2 = \begin{pmatrix} 0 & -\mathbf{I}_n \\ D & 0 \end{pmatrix}. $$

Since ${}^tAK_n + K_nD = 0$, $\mathrm{char\,pol}(y_1) = \mathrm{char\,pol}(y_2)$, and the result follows. For the general case, let

$$ a = \begin{pmatrix} \mathbf{I}_n & M & 0 & 0 \\ 0 & \mathbf{I}_n & 0 & 0 \\ 0 & 0 & \mathbf{I}_n & -M \\ 0 & 0 & 0 & \mathbf{I}_n \end{pmatrix} $$

with $K_nM = {}^tMK_n$. Then ${}^taK_Na = K_N$, and aya^{-1} has a block decomposition similar to that of y with A, B, C and D replaced by $A' = A - MC$, $B' = B - AM - MD + MCM$, $C' = C$ and $D' = D - CM$. We need only to prove that for y in some dense open subset of V we can find M such that $B' = 0$, and for this it is enough to show that for some $y \in V$ the differential at 0 of the map

$$ \begin{array}{ccc} \{ M \in M_n(E) \mid K_nM = {}^tMK_n \} & \to & \{ B' \in M_n(E) \mid {}^tB'K_n + K_nB' = 0 \} \\ M & \mapsto & B - AM - MD + MCM \end{array} $$

is surjective. This differential is $M \mapsto -AM - MD = K({}^tD(K_nM) - (K_nMD))$. Now the requirement on M is that K_nM be a symmetric matrix, and the requirement on B' is that K_nB' be an alternating matrix. It is therefore sufficient to take an element $y \in V$ such that D is a diagonal matrix with n distinct eigenvalues, since in this case $\dim\{ Z \in \mathrm{M}_n(E) \mid DZ = ZD \} = n$. This proves claim 5.

Lemma 6.8. *Let* $n \in \mathbf{N}$. *For* $x = (x_0, \dots, x_n) \in k^{n+1}$ *and* $y = (y_1, \dots, y_n) \in k^n$ *let*

$$ P_T(x,y) = \prod_{i=1}^{n}(T - x_i)^2 + \sum_{j=1}^{n} y_j \prod_{i \notin \{0,j\}} (T - x_i)^2, $$

$$ Q_T(x,y) = (T - x_0)\prod_{i=1}^{n}(T - x_i)^2 + \sum_{j=1}^{n} y_j \prod_{i \notin \{0,j\}} (T - x_i)^2. $$

Then the following hold.

(a) $\{ P_T(x,y) \mid x \in k^{n+1},\ y \in k^n \}$ *contains a dense open subset of* $k[T]^1_{2n}$.

(b) $\{ Q_T(x,y) \mid x \in k^{n+1},\ y \in k^n \}$ *contains a dense open subset of* $k[T]^1_{2n+1}$.

Proof. Consider for example (b). It is clear that $Q_T(x,y)$ is a monic polynomial of degree $2n+1$. At $(x,0)$, the partial derivatives of $Q_T(x,y)$ with respect to x_i and y_i are

$$\begin{aligned} \partial Q_T/\partial x_0 &= -\prod_{j=1}^{n}(T-x_j)^2, \\ \partial Q_T/\partial x_i &= -2(T-x_0)(T-x_i)\prod_{j\notin\{0,i\}}(T-x_j)^2 \quad (i\neq 0), \\ \partial Q_T/\partial y_i &= \prod_{j\notin\{0,i\}}(T-x_j)^2. \end{aligned}$$

In order to prove (b), it is enough to show that if the x_i's are distinct, then these polynomials span $k[T]_{2n}$. We prove this by induction on n. The result is obvious for $n=0$. So let $n>0$. Assuming that the result holds for $n-1$, the derivatives other than $\partial Q_T/\partial x_n$ and $\partial Q_T/\partial y_n$ span the space of all multiples of $(T-x_n)^2$ in $k[T]_{2n}$. Adding a polynomial which is prime to $T-x_n$ and one which contains this factor exactly once, we span the whole of $k[T]_{2n}$. This proves (b). The proof of (a) is similar.

6.9. We prove now claim 6. It is enough to consider the special case where λ consists only of one odd part $\lambda_1 = 2m+1$, an even number $2r$ of equal even parts $\lambda_2 = \dots = \lambda_{2r+1} = 2\ell$, and possibly an odd part $\lambda_{2r+2} = 2\ell-1$. Here $m \geq \ell \geq 1$ and $r \geq 0$. The general case follows indeed easily by taking suitable orthogonal direct sums. We construct a matrix y which depends on parameters $c_0, \dots, c_r$ and $d_1, \dots, d_{r+1} \in \boldsymbol{m}$, with $c_0 = \varepsilon$ if $m > \ell$. The parameter d_{r+1} is used only in the case where λ has $2r+2$ parts. Let also $x_i = \varepsilon^{-1}c_i + \boldsymbol{m}$ $(0 \leq i \leq r)$, $y_i = \varepsilon^{-1}d_i + \boldsymbol{m}$ $(1 \leq i \leq r)$, and $y_{r+1} = \varepsilon^{-2}d_{r+1}^2 + \boldsymbol{m}$.

Consider first the case where λ has $2r+1$ parts. Instead of the bilinear form defined by K_N we use that defined by the matrix K obtained by taking the direct sum of K_{2m+1} and r copies of $K_{4\ell}$, and take for y the matrix which has a block decomposition $(Y_{i,j})_{0\leq i,j\leq r}$ corresponding to that of K and whose blocks are defined as follows. The diagonal block $Y_{0,0}$ is $B_{2m+1,c_0/2}$, and for $1 \leq i \leq r$ let $Y_{i,i} = A$ have itself a block decompositon

$$Y_{i,i} = \begin{pmatrix} N_{2\ell,c_i} & D_i \\ 0 & -N_{2\ell,c_i} \end{pmatrix},$$

where D_i is a matrix in which the $(2\ell-1,1)$ and $(2\ell,2)$ coefficients are respectively $d_i/2$ and $-d_i/2$ and all the other coefficients are 0. For $i \neq j$, all the coefficients of $Y_{i,j}$ are 0, with the following exceptions. For $1 \leq i \leq r$, the $(2\ell,1)$-coefficient of $Y_{i,0}$ is ε and the $(2m+1,1)$-coefficient of $Y_{0,i}$ is $-\varepsilon$.

The characteristic polynomial of y can be computed by expanding the appropriate determinant along the first column. It is worth here to note that for $1 \leq i \leq r$, the minor corresponding to the coefficient ε of $Y_{i,0}$ can easily be expanded further to get rid of all the coefficients of $Y_{0,0}$. What is then left is a matrix whose first line consists of the lines $2m+1$ of the matrices $Y_{0,j}$, $1 \leq j \leq r$, and each of these lines contains one coefficient $-\varepsilon$. Expanding along this line, we can get a non-zero contribution only from the coefficient $-\varepsilon$ coming from $Y_{0,i}$, and the remaining determinant breaks up into a product of smaller determinants. The actual computation gives

$$\operatorname{char pol}^{\sim}(y) = \big(X^{2m} + (-1)^m c_0\big) \prod_{i=1}^{r} (X^{2\ell} - c_i)^2 \; - \; (-1)^m \varepsilon^2 \sum_{j=1}^{r} d_j \prod_{i \notin \{0,j\}} (X^{2\ell} - c_i)^2 .$$

If $m > \ell$ we have then

$$\operatorname{gr}_{\Gamma_\mu, -1/2\ell}\big(\operatorname{char pol}^{\sim}(y)\big) = (-1)^m \prod_{i=1}^{r} (Y - x_i)^2 \; - \; (-1)^m \sum_{j=1}^{r} y_j \prod_{i \notin \{0,j\}} (Y - x_i)^2,$$

and by 6.8(a) the coefficients can be chosen in such a way that we get a square-free polynomial. If $m = \ell$, then

$$\operatorname{gr}_{\Gamma_\mu, -1/2\ell}\big(\operatorname{char pol}^{\sim}(y)\big) = \big(Y + (-1)^m x_0\big) \prod_{i=1}^{r} (Y - x_i)^2 \; - \; (-1)^m \sum_{j=1}^{r} y_j \prod_{i \notin \{0,j\}} (Y - x_i)^2,$$

and 6.8(b) allows to conclude.

When λ has $2r+2$ parts, let λ' be the partition whose parts are the first $2r+1$ parts of λ. Using the construction above for λ', we get two matrices K' and y' in $\mathrm{M}_{N-2\ell+1}(R)$. Let then K be the direct sum of K' and $K_{2\ell-1}$, and let y have a block decomposition

$$y = \begin{pmatrix} y' & -K_{N-2\ell+1}{}^t E K_{2\ell-1} \\ E & B_{2\ell-1,0} \end{pmatrix},$$

where the $(2\ell-1,1)$-coefficient of E is d_{r+1} and all the other coefficients are zero. Then in the same way as above we find

$$\begin{aligned} \operatorname{char pol}(y) = \big(X^{2m} + (-1)^m c_0\big) X^{2\ell} \prod_{i=1}^{r} (X^{2\ell} - c_i)^2 \; - \; (-1)^m \varepsilon^2 X^{2\ell} \sum_{j=1}^{r} d_j \prod_{i \notin \{0,j\}} (X^{2\ell} - c_i)^2 \\ - (-1)^m d_{r+1}^2 \prod_{i=1}^{r} (X^{2\ell} - c_i)^2 . \end{aligned}$$

If $m > \ell$ we have then

$$\begin{aligned} \operatorname{gr}_{\Gamma_\mu, -1/2\ell}\big(\operatorname{char pol}(y)\big) = (-1)^m Y \prod_{i=1}^{r} (Y - x_i)^2 \; - \; (-1)^m Y \sum_{j=1}^{r} y_j \prod_{i \notin \{0,j\}} (Y - x_i)^2 \\ - \; (-1)^m y_{r+1} \prod_{i=1}^{r} (Y - x_i)^2 . \end{aligned}$$

Considering first the polynomials obtained with $y_{r+1} = 0$, there exists by 6.8(a) a dense open subset of $Yk[Y]^1_{2r} \subset k[Y]^1_{2r+1}$ which consists of polynomials obtained in this way. Allowing then y_{r+1} to take arbitrary values, we find that the set of all polynomials $\mathrm{gr}_{\Gamma_\mu,-1/2\ell}(\mathrm{char\,pol}(y))$ with y as above contains a dense open subset of $k[Y]^1_{2r+1}$, and in particular we can arrange to get a square-free polynomial. If $m = \ell$, then

$$\mathrm{gr}_{\Gamma_\mu,-1/2\ell}(\mathrm{char\,pol}(y)) = (Y + (-1)^m x_0)Y\prod_{i=1}^{r}(Y - x_i)^2 - (-1)^m Y\sum_{j=1}^{r} y_j \prod_{i\notin\{0,j\}}(Y - x_i)^2 - (-1)^m y_{r+1}\prod_{i=1}^{r}(Y - x_i)^2,$$

and using 6.8(b) we conclude as above. This proves claim 6, and completes the proof of 6.4.

References

1. R. Carter: Conjugacy classes in the Weyl group. In: A. Borel et al., Seminar on algebraic groups and related finite groups. Lecture Notes in Math. 131. Springer-Verlag, Berlin-Heidelberg-New York 1969.
2. R.W. Carter, G.B. Elkington: A note on the parametrization of conjugacy classes. J. Alg. 20 (1972), 350-354.
3. D. Kazhdan, G. Lusztig: Fixed point varieties on affine flag manifolds. Preprint.
4. N. Koblitz: p-adic numbers, p-adic analysis, and zeta-functions. Graduate Texts in Math. 58. Springer-Verlag, Berlin-Heidelberg-New York 1977.
5. B. Kostant: The principal three-dimensional subgroup and the Betti numbers of a complex simple group. Amer. J. Math 81 (1959), 973-1032.
6. N. Spaltenstein: Classes unipotentes et sous-groupes de Borel. Lecture Notes in Math. 946. Springer-Verlag, Berlin-Heidelberg-New York 1982.
7. T.A. Springer: Regular elements of finite reflection groups. Invent. Math. 25 (1974), 159-198.
8. T.A. Springer, R. Steinberg: Conjugacy classes. In: A. Borel et al., Seminar on algebraic groups and related finite groups. Lecture Notes in Math. 131. Springer-Verlag, Berlin-Heidelberg-New York 1969.

Nicolas Spaltenstein
University of Oregon,
Eugene, OR 97403,
USA