Invariant polynomial functions on the Poisson algebra in characteristic p

Serge Skryabin

Classical results of Chevalley and Harish-Chandra describe the ring of invariant polynomial functions $k[\mathfrak{g}]^{\mathfrak{g}}$ on a complex semisimple Lie algebra $\mathfrak{g}$ and the center Z of the universal enveloping algebra $U(\mathfrak{g})$. If now $\mathfrak{g}$ is a finite dimensional Lie algebra over an algebraically closed field k of characteristic $p > 0$ then both $k[\mathfrak{g}]^{\mathfrak{g}}$ and Z are essentially bigger than in the complex case. Indeed, $k[\mathfrak{g}]^{\mathfrak{g}}$ always contains the subalgebra $k[\mathfrak{g}]^{(p)}$ consisting of the powers φ^p of all functions $\varphi \in k[\mathfrak{g}]$ and, similarly, Z contains the so-called p-center Z_p over which $U(\mathfrak{g})$ is a finite module (see [25]). However, if $\mathfrak{g}$ is the Lie algebra of a semisimple algebraic group G then, under some restrictions on p, there are precise analogs of classical results for the subrings of G-invariants $k[\mathfrak{g}]^G$ and Z^G, as was shown by Veldkamp [21], and Kac and Weisfeiler [5]. Furthermore, $k[\mathfrak{g}]^{\mathfrak{g}} = k[\mathfrak{g}]^{(p)} \cdot k[\mathfrak{g}]^G$ and $Z = Z_p \cdot Z^G$ (see also [3]).

There is another big class of simple finite dimensional Lie algebras over k called the Lie algebras of Cartan type, for which the situation with the invariants is very little understood until now. A significant progress was earlier achieved only in one case by Premet [15] who completely described the ring of invariants $k[\mathfrak{g}]^G$ where $\mathfrak{g} = W_n$ is the Jacobson-Witt algebra and G its automorphism group. Premet established analogs of many classical results, although G has a big unipotent radical and the Lie algebra of G is a proper subalgebra of $\mathfrak{g}$. One no longer has an invariant bilinear form on $\mathfrak{g}$, and so one cannot pass to invariants in the symmetric algebra $S(\mathfrak{g})$, all the more to the central elements in $U(\mathfrak{g})$. From the viewpoint of invariant theory the coadjoint $\mathfrak{g}$-module looks very much different from the adjoint module. As follows from computations of Krylyuk [8], the stabilizers of generic linear functions on $\mathfrak{g}$ have big $[p]$-nilpotent parts whose dimension grows exponentially when n increases.

In the present paper I consider another class of Lie algebras over k. Denote by $B_{2n} = k[x_1, \ldots, x_{2n}]$, $x_i^p = 0$, the commutative associative algebra of truncated polynomials in $2n$ variables. The Poisson bracket defined by the formula

$$[f, g] = \sum_{i=1}^{n} \big(\partial_i(f)\partial_{n+i}(g) - \partial_{n+i}(f)\partial_i(g)\big), \qquad f, g \in B_{2n},$$

where $\partial_1, \ldots, \partial_{2n}$ denote the partial derivatives in $x_1, \ldots, x_{2n}$ gives a Lie algebra structure on B_{2n}. The resulting Lie algebra has a center coinciding with the scalars k, and the factor algebra B_{2n}/k is isomorphic to a certain Hamiltonian Lie algebra L whose commutator subalgebra $[L, L]$ is simple (with an exception for $p = 2$, $n = 1$) and nonclassical (with an exception for $p = 2$, $n = 2$ or $p = 3$, $n = 1$). The Lie algebras appearing here are rather special in the whole class of Hamiltonian algebras (see [4], [11], [23]). In fact these algebras admit a $[p]$-map which makes them into p-Lie algebras or restricted Lie algebras, as defined by Jacobson [1]. The

$[p]$-structure turns out to be essential for the construction of invariants. The reason that I work with the Poisson algebra B_{2n} rather than with L is that the results are stated nicer in this case.

The main results are as follows. Denote by G the group of Poisson automorphisms of B_{2n}, i.e., invertible transformations preserving both the associative and the Lie algebra structures. Let $G_{[p]} \subset G$ be the subgroup whose elements respect the $[p]$-map as well. Consider also the action of L on B_{2n} induced by the adjoint action of B_{2n}. Theorem 3.4 states that $k[B_{2n}]^L$ is generated over $k[B_{2n}]^{(p)}$ by certain $G_{[p]}$-invariant functions $\varphi_1, \ldots, \varphi_{p^n}$. Moreover, $k[B_{2n}]^L$ is free over $k[B_{2n}]^{(p)}$ and is a locally complete intersection ring. In Theorem 5.2 I prove that $k[B_{2n}]^{G_{[p]}}$ and $k[B_{2n}]^G$ are polynomial rings generated by $p^n + n$ and p^n elements, respectively. Moreover, there are affine subspaces $S, S_0 \subset B_{2n}$ such that the restriction of functions gives isomorphisms $k[B_{2n}]^G \cong k[S_0]$ and $k[B_{2n}]^{G_{[p]}} \cong k[S]$. Clearly, S, S_0 are analogs of Kostant's transversal plane to a principal nilpotent element in the classical settings [10]. The subsets S, S_0 give a full system of representatives for the $G_{[p]}$- (respectively G-) conjugacy classes on a Zariski open subset $U \subset B_{2n}$ whose elements are "regular" for the results of the present paper. In particular, the Lie centralizers $\mathfrak{z}(f)$ of elements $f \in U$ all have dimension p^n (see Proposition 2.2). To prove that the invariants separate the orbits on U I need Theorem 4.3 which ensures that every $[p]$-compatible isomorphism of Lagrangian subalgebras of B_{2n} (see section 1 for the definition) admits an extension to an element of G.

In Theorem 6.4 I prove that the cone $\mathcal{N}$ of $[p]$-nilpotent elements in B_{2n} is an irreducible normal complete intersection of codimension n. This is again an analog of Kostant's results. It should be mentioned for comparison that in case of W_n the singular locus of the nilpotent cone has codimension 1 in $\mathcal{N}$, and therefore $\mathcal{N}$ is not normal, as was proved by Premet [15]. In [14] Premet conjectured that the nilpotent cone $\mathcal{N}$ is irreducible for any p-Lie algebra, and proved under this assumption that $\mathcal{N}$ is a set-theoretic complete intersection (apparently the irreducibility assumption can be removed here). The available information suggests that $\mathcal{N}$ is always a strict complete intersection. There are still certain classical facts which do not carry over to the Poisson algebra. The nilpotent cone does not contain a dense orbit, and $k[B_{2n}]$ is a free module neither over $k[B_{2n}]^{G_{[p]}}$ nor over $k[B_{2n}]^G$, at least when either p or n is big enough. It seems that these deviations are related somehow to the fact that the generic centralizers $\mathfrak{z}(f)$ are not $[p]$-semisimple, and the $[p]$-semisimple elements are not dense in B_{2n}.

Luckily enough, an invariant bilinear form on B_{2n} does exist, yielding a G- and L-equivariant isomorphism $S(B_{2n}) \cong k[B_{2n}]$. Denote by $\varphi_1^\vee, \ldots, \varphi_{p^n}^\vee \in S(B_{2n})$ the images of the invariant functions $\varphi_1, \ldots, \varphi_{p^n}$ mentioned before. Then $\varphi_a^\vee$ is homogeneous of degree a. Consider the canonical increasing filtration $U_m(B_{2n})$, $m \geq 0$, in the universal enveloping algebra. If $0 < a < p^n$ and $a \not\equiv 0 \pmod{p}$, Theorem 7.2 ensures the existence of a $G_{[p]}$-invariant element $z_a \in Z \cap U_a(B_{2n})$ whose image in $S^a(B_{2n})$ coincides with $\varphi_a^\vee$. The major unsolved problem is to verify this property for the remaining invariants in the symmetric algebra. I will explain briefly the construction of z_a. If $a \not\equiv 0 \pmod{p}$ then $\varphi_a^\vee$ is an element of an L-submodule, call it $V \subset S^a(B_{2n})$, which is induced from a onedimensional L_0-submodule, call it $V_0 \subset S^a(B_{2n})$, where L_0 is a subalgebra of codimension $2n$ in L. It turns out that $V_0 \subset S(I)$ where $I \subset B_{2n}$ is an abelian Lie subalgebra. As $U(I) \cong S(I)$, we can generate by V_0 an L-submodule $V' \subset U_a(B_{2n})$. The latter is mapped isomorphically onto V under the projection $U_a(B_{2n}) \to S^a(B_{2n})$. So we can find z_a inside V'.

1. Preliminaries

Denote by $B_n = k[x_1, \dots, x_n]$, $x_i^p = 0$, the truncated polynomial algebra in n variables where k is an algebraically closed field of characteristic $p > 0$. One has $f^p \in k$ for all $f \in B_n$, and so B_n is local with the maximal ideal $\mathfrak{n}$ consisting of those $f \in B_n$ for which $f^p = 0$. Any minimal system of generators of B_n consists of n elements $y_1, \dots, y_n$ which are linearly independent modulo $k + \mathfrak{n}^2$. One has then $y_i^p = \alpha_i$ for some $\alpha_1, \dots, \alpha_n \in k$ and the monomials $y_1^{r_1} \cdots y_{2n}^{r_n}$ with $0 \le r_i < p$ constitute a basis for B_n over k. If $z_1, \dots, z_n$ is another minimal system of generators with $z_i^p = \beta_i$ then there exists an automorphism $\theta \in \operatorname{Aut} B_n$ sending each y_i to z_i if and only if $\alpha_i = \beta_i$ for all i. The derivation algebra $W_n = \operatorname{Der} B_n$ is a Lie algebra called the *Jacobson-Witt algebra*. Note that W_n is a free B_n-module with a basis consisting of the partial derivatives $\partial_1, \dots, \partial_n$ in $x_1, \dots, x_n$.

If C is a commutative, associative and unital algebra, then a *Poisson bracket* on C is a Lie algebra structure satisfying the identity $[f, gh] = [f, g]h + [f, h]g$ where $f, g, h \in C$. This identity means that the linear transformations $\mathcal{D}_f : C \to C$ given by $\mathcal{D}_f(g) = [f, g]$ are derivations of C. The algebra C together with a fixed Poisson bracket on it is called a *Poisson algebra*. We will be considering the truncated polynomial algebra B_{2n} in $2n$ variables $x_1, \dots, x_{2n}$ as a Poisson algebra using the Poisson bracket explicitly written out in the introduction. Thus $[f, g] = \mathcal{D}_f(g)$ where

$$\mathcal{D}_f = \sum_{i=1}^{n} \big(\partial_i(f)\partial_{n+i} - \partial_{n+i}(f)\partial_i\big) \in W_{2n}.$$

The assignment $f \mapsto \mathcal{D}_f$ gives a Lie algebra homomorphism $B_{2n} \to W_{2n}$. Its image $L = \{\mathcal{D}_f \mid f \in B_{2n}\}$ is therefore a Lie subalgebra in W_{2n} (it is an ideal in the Hamiltonian Lie algebra H_{2n} consisting of all $D \in W_{2n}$ such that $D\omega = 0$ where $\omega = dx_1 \wedge dx_{n+1} + \ldots + dx_n \wedge dx_{2n}$ is a Hamiltonian differential form). Taking $f = x_1, \dots, x_{2n}$ in the formula for $\mathcal{D}_f$, one sees that $\partial_1, \dots, \partial_{2n} \in L$. It is immediate thereof that the Lie center $\{f \in B_{2n} \mid [f, B_{2n}] = 0\}$ coincides with k, and $L \cong B_{2n}/k$. Denote by $\mathfrak{m}$ the maximal associative ideal of B_{2n}, and put $L_0 = \{\mathcal{D}_f \mid f \in \mathfrak{m}^2\}$, which is a subalgebra of L.

It is well known that $D^p \in L$ for all $D \in L$. Hence one can define on B_{2n} a $[p]$-*map* $f \mapsto f^{[p]}$ satisfying the identities

$([p]_1)$ $\quad \mathcal{D}_f^p = \mathcal{D}_{f^{[p]}}$,

$([p]_2)$ $\quad (\lambda f)^{[p]} = \lambda^p f^{[p]}$,

$([p]_3)$ $\quad (f+g)^{[p]} = f^{[p]} + \sum_{l=1}^{p-1} s_l(f, g) + g^{[p]}$

where $f, g \in B_{2n}$, $\lambda \in k$ and $l s_l(f, g)$ is equal to the coefficient of t^{l-1} in the expansion of the expression $(\mathcal{D}_f + t\mathcal{D}_g)^{p-1}(g)$ with t a scalar indeterminate (see [2], [19]). Because of a nontrivial center the $[p]$-map on B_{2n} is not determined uniquely. Since L_0 coincides with the stabilizer of $\mathfrak{m}$ in L, we have $D^p \in L_0$ for all $D \in L_0$. We can therefore specify the $[p]$-map on $k + \mathfrak{m}^2$ by the requirement that $1^{[p]} = 0$ and $f^{[p]} \in \mathfrak{m}^2$ for all $f \in \mathfrak{m}^2$. Any $[p]$-structure with this property will be called *normalized*. Denote by G the group of automorphisms of both the associative and the Lie algebra structures on B_{2n}.

Lemma 1.1. *Any two normalized $[p]$-structures on B_{2n} are transformed to one another by an element of G.*

Proof. Since the derivations $\partial_1, \ldots, \partial_{2n}$ have zero $[p]$-power, $x_i^{[p]} = \alpha_i \in k$ for all i. Given $1 \le j \le 2n$, we put $j' = j+n$ if $j \le n$ and $j' = j-n$ if $j > n$. Let $y_i = x_i$ for $i \ne j$ and $y_j = x_j - \lambda x_{j'}^{p-1}$ where $\lambda \in k$. There exists $\theta \in \operatorname{Aut} B_{2n}$ sending each x_i to y_i. In fact $\theta \in G$ since $[y_i, y_j] = [x_i, x_j]$ for all $i \ne j$. If $p > 2$ then $\left(x_{j'}^{p-1}\right)^{[p]} = 0$ and the terms $s_l(x_j, x_{j'}^{p-1})$ in the formula ($[p]_3$) likewise vanish for $1 < l < p$. We get then $y_j^{[p]} = x_j^{[p]} - \mathcal{D}_{x_j}^{p-1}(\lambda x_{j'}^{p-1}) = \alpha_j + \lambda$. If $p = 2$ then $y_j^{[2]} = \alpha_j + \lambda + \lambda^2 \alpha_{j'}$. In any case we can find λ such that $y_j^{[p]}$ takes any given value in k. Repeating this procedure successively for $j = 1, \ldots, 2n$, we get the required element in G. □

From now on we fix a normalized $[p]$-structure on B_{2n} and denote by $G_{[p]} \subset G$ the subgroup of automorphisms commuting with the $[p]$-map.

Remark. In this paper we don't use the structural properties of G. It can be shown that G coincides with the group of those $\theta \in \operatorname{Aut} B_{2n}$ which stabilize the Hamiltonian form ω, and this group was studied in [22]. In particular, G is a semidirect product of Sp_{2n} and the unipotent radical of G. The Lie algebra of G coincides with the stabilizer of $\mathfrak{m}$ in H_{2n}, and it can be shown that the Lie algebra of $G_{[p]}$ is L_0 for any normalized $[p]$-map.

We call an associative subalgebra $B \subset B_{2n}$ (respectively an associative ideal $I \subset B_{2n}$) *Lagrangian* if it is generated by n elements $y_1, \ldots, y_n \in \mathfrak{m}$ which are linearly independent modulo $\mathfrak{m}^2$ and $[B, B] = 0$ (respectively $[I, I] \subset I$). Since $y_1, \ldots, y_n$ can be included in a minimal system of generators for B_{2n}, it is clear that $B \cong B_n$ and B_{2n} is free over B (respectively $B_{2n}/I \cong B_n$) in this case. We state below a few simple properties of Lagrangian subalgebras and ideals.

Lemma 1.2. *Suppose that $B \subset B_{2n}$ is a Lagrangian subalgebra generated by $y_1, \ldots, y_n \in \mathfrak{m}$. Then:*

(1) *$\mathcal{D}_{y_1}, \ldots, \mathcal{D}_{y_n}$ are a basis for $\operatorname{Der}_B B_{2n} \subset W_{2n}$, the subalgebra of B-linear derivations, as a B_{2n}-module.*

(2) *The Lie centralizer $\mathfrak{z}(B) = \{g \in B_{2n} \mid [g, B] = 0\}$ coincides with B. In particular, $B^{[p]} \subset B$. If $f \in \mathfrak{m}_B^2$ where $\mathfrak{m}_B = \mathfrak{m} \cap B$ then $f^{[p]} = 0$.*

(3) *There exists a Lagrangian ideal $I \subset B_{2n}$ such that $I^{[p]} \subset I$ and $B_{2n} = B \oplus I$.*

Proof. Define $\kappa : B_{2n} \to k$ by $\kappa(\lambda + f) = \lambda$ for $\lambda \in k$ and $f \in \mathfrak{m}$. The formula $(g, h) = \kappa([g, h])$ where $g, h \in B_{2n}$ gives an alternating bilinear form on B_{2n}. Since $[\mathfrak{m}^2, B_{2n}] \subset \mathfrak{m} = \ker \kappa$, the subspace $\mathfrak{m}^2$ is contained in the kernel of this bilinear form. On the other hand, $(x_i, x_j) \ne 0$ precisely when $j - i = \pm n$. It follows that the induced bilinear form on the factor space $\mathfrak{m}/\mathfrak{m}^2$ is nondegenerate.

Since $y_1, \ldots, y_n \in \mathfrak{m}$ are linearly independent modulo $\mathfrak{m}^2$, we can find elements $z_1, \ldots, z_n \in \mathfrak{m}$ such that $[y_i, z_j] \equiv \delta_{ij} \pmod{\mathfrak{m}}$ for $1 \le i, j \le n$. Then $y_1, \ldots, y_n$, $z_1, \ldots, z_n$ form a minimal system of generators for B_{2n}. It follows that the monomials $z_1^{r_1} \cdots z_n^{r_n}$ with $0 \le r_j < p$ give a basis for B_{2n} as a module over B. It is now clear that the B_{2n}-module $\operatorname{Der}_B B_{2n}$ is free with a basis consisting of the derivations $D_1, \ldots, D_n \in W_{2n}$ such that $D_i(y_j) = 0$ and $D_i(z_j) = \delta_{ij}$. The derivations $\mathcal{D}_{y_i}$ are B-linear as $[B, B] = 0$. Write $\mathcal{D}_{y_i} = \sum_{j=1}^n h_{ij} D_j$ with $h_{ij} \in B_{2n}$. Then

$h_{ij} = \mathcal{D}_{y_i}(z_j) \equiv \delta_{ij} \pmod{\mathfrak{m}}$. Hence the $n \times n$ matrix with entries h_{ij} is invertible, yielding (1).

Suppose $g \in \mathfrak{z}(B)$. Then $\mathcal{D}_{y_i}(g) = 0$, and by (1) $D_i(g) = 0$, for all i. Expressing g as a B-linear combination of monomials in z's, we deduce that the coefficients of monomials of positive degree have to be zero. Thus $\mathfrak{z}(B) = B$. Suppose that $f = gh$ where $g, h \in \mathfrak{m}_B$. Then $\mathcal{D}_f^p = (g\mathcal{D}_h + h\mathcal{D}_g)^p = g^p\mathcal{D}_h^p + h^p\mathcal{D}_g^p = 0$ as $g^p = h^p = 0$. It follows that $\mathcal{D}_f^p = 0$ for any $f \in \mathfrak{m}_B^2$. Since $f^{[p]} \in \mathfrak{m}^2$ is a unique element such that $([p]_1)$ holds, we get $f^{[p]} = 0$.

Let $J \subset \{1, \ldots, 2n\}$ be a maximal subset subject to the two conditions:

(a) for each $i \in \{1, \ldots, n\}$ the indices i and $i + n$ are not both in J,

(b) the elements $\{y_1, \ldots, y_n\} \cup \{x_i \mid i \in J\}$ are linearly independent modulo $\mathfrak{m}^2$.

Note that (a) means that $[x_i, x_j] = 0$ for all $i, j \in J$. We claim that J has cardinality n. Suppose the contrary. Then there exists $j \in \{1, \ldots, n\}$ such that $j \notin J$ and $j + n \notin J$. Since neither $J \cup \{j\}$ nor $J \cup \{j + n\}$ is an admissible subset, we must have $x_j \equiv u_1 + v_1$ and $x_{j+n} \equiv u_2 + v_2 \pmod{\mathfrak{m}^2}$ where u_1, u_2 are linear combinations of elements $y_1, \ldots, y_n$ and v_1, v_2 are linear combinations of elements $\{x_i \mid i \in J\}$. Since both $J \cup \{j\}$ and $J \cup \{j + n\}$ satisfy (1), we see that the three commutators $[v_1, v_2]$, $[x_j, v_2]$, $[v_1, x_{j+n}]$ all vanish. Then $[u_1, v_2] = [v_1, u_2] = 0$ as well. We have also $[u_1, u_2] = 0$ since $u_1, u_2 \in B$. It follows $[x_j, x_{j+n}] = 0$, a contradiction.

Denote by $I \subset B_{2n}$ the associative ideal generated by n elements $\{x_i \mid i \in J\}$. Then (a) ensures that $[I, I] \subset I$. As $\{y_1, \ldots, y_n\} \cup \{x_i \mid i \in J\}$ is a minimal system of generators for B_{2n}, we get also $B_{2n} = B \oplus I$. In view of lemma 1.1 we may assume, adjusting the generators $x_1, \ldots, x_{2n}$ if necessary, that $x_i^{[p]} = 0$ for all $1 \le i \le 2n$. It will follow then from the next lemma that $I^{[p]} \subset I$. □

Lemma 1.3. *Suppose that $I \subset B_{2n}$ is a Lagrangian ideal generated by elements $y_1, \ldots, y_n \in \mathfrak{m}$. For each $f \in I$ denote by $\overline{\mathcal{D}}_f$ the derivation of the factor algebra $\overline{B} = B_{2n}/I$ induced by $\mathcal{D}_f$. Then:*

(1) *$\overline{\mathcal{D}}_{y_1}, \ldots, \overline{\mathcal{D}}_{y_n}$ are a basis for $\operatorname{Der} \overline{B}$ as a $\overline{B}$-module.*

(2) *The Lie normalizer $\mathfrak{n}(I) = \{g \in B_{2n} \mid [g, I] \subset I\}$ coincides with $k + I$. In particular, $I^{[p]} \subset k + I$. If $y_i^{[p]} \in I$ for all i then $I^{[p]} \subset I$.*

(3) *There exists a Lagrangian subalgebra $B \subset B_{2n}$ such that $B_{2n} = B \oplus I$.*

Proof. Let $y_1, \ldots, y_n, z_1, \ldots, z_n \in \mathfrak{m}$ be a minimal system of generators for B_{2n} such that $[y_i, z_j] \equiv \delta_{ij} \pmod{\mathfrak{m}}$. Then $\overline{B}$ has a basis consisting of the monomials $\overline{z}_1^{r_1} \cdots \overline{z}_n^{r_n}$ with $0 \le r_i < p$ where $\overline{z}_i$ denotes the image of z_i in $\overline{B}$. Furthermore, $\overline{z}_i^p = 0$ for all i. The $\overline{B}$-module $\operatorname{Der} \overline{B}$ has a basis consisting of the derivations $D_1, \ldots, D_n$ such that $D_i(\overline{z}_j) = \delta_{ij}$. Write $\overline{\mathcal{D}}_{y_i} = \sum_{j=1}^n h_{ij} D_j$ with $h_{ij} \in \overline{B}$. Then $h_{ij} = \overline{\mathcal{D}}_{y_i}(\overline{z}_j) \equiv \delta_{ij}$ modulo the maximal ideal $\mathfrak{m}/I$ of $\overline{B}$. Hence the $n \times n$ matrix with entries h_{ij} is invertible, and (1) is immediate.

Suppose that $g \in \mathfrak{n}(I)$. Then $\mathcal{D}_{y_i}(g) \in I$, and therefore $\overline{\mathcal{D}}_{y_i}(\overline{g}) = 0$ for all i, where $\overline{g}$ denotes the image of g in $\overline{B}$. It follows from (1) that $\overline{g} \in k$, i.e., $g \in k + I$. For every $f \in I \cap \mathfrak{m}^2$ we have $f^{[p]} \in (k + I) \cap \mathfrak{m}^2 \subset I$. Now $I = ky_1 + \ldots + ky_n + I \cap \mathfrak{m}^2$. If $y_i^{[p]} \in I$ for all i, we get $f^{[p]} \in I$ for every $f \in I$ applying the formula $([p]_3)$.

Let $J \subset \{1, \dots, 2n\}$ be a subset constructed as in the proof of lemma 1.2 with respect to $y_1, \dots, y_n$. Then the associative subalgebra $B \subset B_{2n}$ generated by elements $\{x_i \mid i \in J\}$ is Lagrangian and satisfies (3). $\square$

Given two vector spaces V, W over k, denote by $\mathrm{Pol}(V, W)$ the vector space of all polynomial maps $V \to W$. If $\varphi \in \mathrm{Pol}(V, W)$ and $u, v \in V$ then there is an expansion as a power series in $t \in k$,

$$\varphi(v + tu) = \varphi(v) + t\varphi'(v, u) + t^m\text{-terms with } m \geq 2.$$

Here $\varphi'(v, u)$ is polynomial in v and linear in u. The differential of φ at v is the linear map $(d\varphi)_v : V \to W$ given by $u \mapsto \varphi'(v, u)$. If V, W are modules over a Lie algebra $\mathfrak{g}$ or rational modules over an algebraic group then $\mathrm{Pol}(V, W)$ inherits the same structure, which comes in fact from a linear isomorphism $\mathrm{Pol}(V, W) \cong S(V^*) \otimes W$ where $S(V^*)$ is the symmetric algebra of the dual space V^*. If $D \in \mathfrak{g}$ then $(D\varphi)(v) = D\big(\varphi(v)\big) - \varphi'(v, Dv)$. In the special case where $W = k$ we denote by $k[V] = \mathrm{Pol}(V, k)$ the algebra of polynomial functions on V.

Suppose that $\mathfrak{g}$ is a p-Lie algebra operating on V via a p-representation. Put $\mathfrak{g}_v = \{D \in \mathfrak{g} \mid Dv = 0\}$ for $v \in V$, and

$$c_{\mathfrak{g}}(V) = \max_{v \in V} \operatorname{codim}_{\mathfrak{g}} \mathfrak{g}_v.$$

The maximal ideal $\mathfrak{m}_v = \{\varphi \in k[V] \mid \varphi(v) = 0\}$ of the function algebra is generated by functions $\xi - \xi(v)1$ with $\xi \in V^*$. Hence $\mathfrak{m}_v$ is stable under $D \in \mathfrak{g}$ if and only if $(D\xi)(v) = -\xi(Dv) = 0$ for all ξ, if and only if $D \in \mathfrak{g}_v$. Denote by $k[V]^{(p)} \subset k[V]$ the subalgebra consisting of pth powers φ^p of functions $\varphi \in k[V]$. We can now state a special case of [18], theorem 5.4:

Theorem 1.4. *Suppose that $\varphi_1, \dots, \varphi_m \in k[V]^{\mathfrak{g}}$ are $\mathfrak{g}$-invariant polynomial functions where $m = \dim V - c_{\mathfrak{g}}(V)$. Suppose also that their differentials are linearly independent at all points of an open subset $U \subset V$ whose complement has codimension at least 2 in V. Then $k[V]^{\mathfrak{g}} = k[V]^{(p)}[\varphi_1, \dots, \varphi_m]$. Moreover, $k[V]^{\mathfrak{g}}$ is free of rank p^m over $k[V]^{(p)}$ and is a locally complete intersection ring.*

The arguments used by Kostant to prove the normality of nilpotent cones in complex semisimple Lie algebras work equally well in our case. For convenience we state below a lemma which incorporates several standard facts from algebraic geometry.

Lemma 1.5. *Let $N \subset V$ be the zero set of homogeneous polynomial functions $\varphi_1, \dots, \varphi_m \in k[V]$. Suppose that $U \subset V$ is an open subset and $E \subset V$ a vector subspace such that $E \cap N \subset \{0\} \cup U$ and $(d\varphi_1)_u, \dots, (d\varphi_m)_u$ are linearly independent at all points $u \in U$.*

(1) *If $\dim E \geq m + 1$ then N is a complete intersection of codimension m in V and the ideal $I_N = \{\varphi \in k[V] \mid \varphi(N) = 0\}$ is generated by $\varphi_1, \dots, \varphi_m$.*

(2) *If $\dim E \geq m + 2$ then N is normal and irreducible.*

Proof. Denote by X the closed subset of those $u \in N$ for which $(d\varphi_1)_u, \dots, (d\varphi_m)_u$ are linearly dependent. Since $\varphi_1, \dots, \varphi_m$ are homogeneous, X is conical, and by the hypotheses $E \cap X = \{0\}$. Since every irreducible component of X meets E

at 0, the theorem on dimensions of intersections in an affine space ensures that $\operatorname{codim}_V X \ge \dim E \ge m+1$. Now N is a fiber of the morphism $\pi : V \to \mathbb{A}^m$ given by functions $\varphi_1, \ldots, \varphi_m$. By the theorem on dimension of fibers $\operatorname{codim}_V Z \le m$, and so $Z \not\subset X$, for each irreducible component Z of N. If $u \in Z \smallsetminus X$, then $(d\pi)_u$ is surjective, whence π is smooth at u. This shows, in particular, that $\operatorname{codim}_V Z = m$. Furthermore, each $u \in N \smallsetminus X$ is a nonsingular point of N, and the kernel of the canonical homomorphism of local rings $\mathcal{O}_{V,u} \to \mathcal{O}_{N,u}$ is generated by $\varphi_1, \ldots, \varphi_m$. Let I be the ideal of $k[V]$ generated by $\varphi_1, \ldots, \varphi_m$. The ring $A = k[V]/I$ is Cohen-Macaulay by [13], (16.A), (16.B). Each minimal prime ideal $\mathfrak{p} \subset A$ corresponds to some Z above, and if $\mathfrak{m} \subset A$ is the maximal ideal corresponding to $u \in Z \smallsetminus X$, then the local ring $A_\mathfrak{m} \cong \mathcal{O}_{N,u}$ is regular and, in particular, integral. It follows that $A_\mathfrak{p}$ is integral and artinian, i.e., a field. If now $a \in A$ is nilpotent, then its annihilator ideal $\operatorname{ann}(a)$ is not contained in any such $\mathfrak{p}$. As the set of zero divisors in a Cohen-Macaulay ring coincides with the union of minimal primes [13], (16.C), $\operatorname{ann}(a)$ contains a regular element, which means $a = 0$. Thus A is reduced, and (1) is proved. Under assumptions of (2), $\operatorname{codim}_Z Z \cap X \ge 2$ for each irreducible component Z of N. Then N is smooth in codimension 1, whence N is normal by Serre's criterion [13], (17.I). As N is a disjoint union of its irreducible components, each of which has to contain 0, the variety N is irreducible. $\square$

2. The open set of regular elements

Given $f \in B_{2n}$, we define $f^{[1]} = f$ and, inductively, $f^{[p^i]} = \big(f^{[p^{i-1}]}\big)^{[p]}$ for $i > 0$. For each integer $a \ge 0$ denote by $a_0, a_1, a_2, \ldots$ the coefficients in the p-adic expansion $a = \sum_{i\ge0} a_i p^i$ with $0 \le a_i < p$, and put

$$f^{[a]} = \prod_{i\ge0} \big(f^{[p^i]}\big)^{a_i} \in B_{2n}.$$

Denote also

$$U = \{f \in B_{2n} \mid f, f^{[p]}, \ldots, f^{[p^{n-1}]} \text{ are linearly independent modulo } k + \mathfrak{m}^2\}$$

where $\mathfrak{m}$ is the maximal ideal of B_{2n}. The elements in U are *regular* in as much as our further results are concerned. Because the term "regular" has so many different meanings, the reader is warned that its usage here is limited to the specific context of the present paper.

Lemma 2.1. *Let $T_{\mathbb{F}_p} \subset B_{2n}$ be the $\mathbb{F}_p$-linear span of elements $t_1, \ldots, t_n$ where $t_i = (1 + x_i)x_{n+i}$ and $\mathbb{F}_p \subset k$ the prime subfield. Then every $\mathbb{F}_p$-linear invertible transformation τ of $T_{\mathbb{F}_p}$ extends to an automorphism $\theta \in G$ such that $\theta(V) = V$ where $V = k + kx_1 + \ldots + kx_n + \mathfrak{m}^2$.*

Proof. Put $y_i = 1 + x_i$ for $i = 1, \ldots, n$. The elements $t_1, \ldots, t_n, y_1, \ldots, y_n$ form a minimal system of generators for B_{2n} and satisfy the relations $t_i^p = 0$, $y_i^p = 1$, $[t_i, t_j] = [y_i, y_j] = 0$, $[y_j, t_i] = \delta_{ij} y_j$.

Denote $X = \operatorname{Hom}_{\mathbb{F}_p}(T_{\mathbb{F}_p}, \mathbb{F}_p)$, and let $B \subset B_{2n}$ be the Lagrangian subalgebra generated by $x_1, \ldots, x_n$. For each $\alpha \in X$ the algebra B contains a unique element y_α such that $y_\alpha^p = 1$ and $[y_\alpha, t] = \alpha(t) y_\alpha$ for all $t \in T_{\mathbb{F}_p}$. In fact $y_\alpha = y_1^{r_1} \cdots y_n^{r_n}$ where $r_i \in \mathbb{Z}$ are such that $\alpha(t_i) = r_i 1$. We have $y_\alpha y_\beta = y_{\alpha+\beta}$ for $\alpha, \beta \in X$ so that B is isomorphic with the group algebra of the additive group X.

Put $t'_i = \tau(t_i)$. Then $t'_1, \ldots, t'_n$ are a basis for $T_{\mathbb{F}_p}$ over $\mathbb{F}_p$. Denote by $\varepsilon'_1, \ldots, \varepsilon'_n$ the elements of the dual basis of X, and put $y'_i = y_{\varepsilon'_i}$. Then $y'_1, \ldots, y'_n$ generate the algebra B, whence $t'_1, \ldots, t'_n, y'_1, \ldots, y'_n$ is a minimal system of generators for B_{2n}. We have the relations ${t'_i}^p = 0$, ${y'_i}^p = 1$, $[t'_i, t'_j] = [y'_i, y'_j] = 0$, $[y'_j, t'_i] = \delta_{ij} y'_j$. Now the assignments $t_i \mapsto t'_i$, $y_i \mapsto y'_i$ define an automorphism $\theta \in \operatorname{Aut} B_{2n}$. Furthermore, $\theta([f,g]) = [\theta(f), \theta(g)]$ for all $f, g \in B_{2n}$ since it suffices to verify this identity on a set of generators for B_{2n}. Thus $\theta \in G$. By construction $\theta(B) = B$. Since $V = B + \mathfrak{m}^2$ and $\mathfrak{m}^2$ is stable under automorphisms, we get $\theta(V) = V$. $\square$

Proposition 2.2. (1) *The subset U is nonempty, Zariski open in B_{2n} and stable under G. Its complement $B_{2n} \smallsetminus U$ has codimension at least 2 in B_{2n}.*

(2) *For each $f \in U$ its centralizer $\mathfrak{z}(f) = \{g \in B_{2n} \mid [f,g] = 0\}$ is a Lagrangian subalgebra with basis elements $f^{[a]}$, $0 \le a < p^n$. In particular, $\dim \mathfrak{z}(f) = p^n$.*

(3) *The subset $U_s = \{f \in B_{2n} \mid f_s \in U\}$, where f_s denotes the $[p]$-semisimple component of f, is nonempty, Zariski open in B_{2n} and G-stable. Furthermore, $U_s \subset U$ and $\mathfrak{z}(f) = \mathfrak{z}(f_s)$ for every $f \in U_s$.*

(4) *$f^{[p]} \in U_s$ if and only if $f \in U_s$.*

Proof. (1) If $\theta \in G$ then $\theta(f^{[p]}) \equiv \theta(f)^{[p]} \pmod{k}$, whence $\theta(f^{[p^i]}) \equiv \theta(f)^{[p^i]} \pmod{k}$ for all $f \in B_{2n}$ and $i \ge 0$ by induction on i. Since $k + \mathfrak{m}^2$ is stable under θ, it is immediate that so is U too.

Suppose that V is a vector subspace of codimension n in B_{2n} such that $V \supset k + \mathfrak{m}^2$. Let $e_1, \ldots, e_n$ be a basis for a complement of V in B_{2n}. For each i we can write $f^{[p^i]} \equiv \sum_{j=1}^n \lambda_{ij}(f) e_j \pmod{V}$ where λ_{ij} are homogeneous polynomial functions of degree p^i on B_{2n}. Denote by $\Delta(f)$ the determinant of the square matrix $[\lambda_{ij}(f)]_{j=1,\ldots,n}^{i=0,\ldots,n-1}$. Then Δ is a homogeneous polynomial function of degree $(p^n-1)/(p-1)$ on B_{2n}. Note that $\Delta(f) \ne 0$ if and only if $f, f^{[p]}, \ldots, f^{[p^{n-1}]}$ are linearly independent modulo V. It is clear that $f \in U$ if and only if f lies in the open subset $\{f \in B_{2n} \mid \Delta(f) \ne 0\}$ defined with respect to a suitable subspace V as above. Hence U is open.

We take now V as in lemma 2.1 and put $Z = \{f \in B_{2n} \mid \Delta(f) = 0\}$, so that $B_{2n} \smallsetminus U \subset Z$. Let t_i, y_i, $T_{\mathbb{F}_p}$, X have the same meaning as in lemma 2.1. Extend each $\alpha \in X$ to a linear function on $T = kT_{\mathbb{F}_p}$. Note that the monomial $y_1^{r_1} \cdots y_n^{r_n} t_1^{s_1} \cdots t_n^{s_n}$ is an eigenvector for $\mathcal{D}_{t_i}$ with eigenvalue $-r_i 1$. Thus $\mathcal{D}_{t_i}$ is a diagonalizable linear transformation of B_{2n} with all eigenvalues in $\mathbb{F}_p$, that is, $\mathcal{D}_{t_i}^p = \mathcal{D}_{t_i}$. We see that $\mathcal{D}_{t_1}, \ldots, \mathcal{D}_{t_n}$ span an n-dimensional torus. If $t \in T$ then $t \in Z$ if and only if $\mathcal{D}_t$ generates a torus of dimension less than n, which means that $t \in T_\alpha = \ker \alpha$ for some $0 \ne \alpha \in X$. There are $p^n - 1$ nonzero elements in X, hence $(p^n-1)/(p-1)$ distinct hyperplanes $T_\alpha \subset T$. It follows that the restriction of Δ to T coincides up to a scalar multiple with the product of $(p^n-1)/(p-1)$ nonproportional elements of X.

Put $G_V = \{\theta \in G \mid \theta(V) = V\}$. If $\theta \in G_V$ then clearly $\Delta(\theta f) = \det(\theta_V)\Delta(f)$ where θ_V is the invertible linear transformation of the vector space B_{2n}/V induced by θ. Hence Z is stable under G_V, and G_V permutes the irreducible components of Z. Let $Z_1, \ldots, Z_m$ be all irreducible components of Z which are G_V-conjugate to one chosen irreducible component. Then $Z_1 \cup \ldots \cup Z_m$ is the zero locus of a polynomial function Δ' on B_{2n} which divides Δ. Now $\Delta'|_T$ is up to a scalar multiple a product of some $\alpha \in X$. Suppose that $0 \ne \alpha \in X$ occurs as a factor of

$\Delta'|_T$, and let $0 \neq \beta \in X$ be any element. Both T_α and T_β are spanned by elements from $T_{\mathbb{F}_p}$. Hence there exists an invertible linear transformation $\tau : T \to T$ such that $\tau(T_{\mathbb{F}_p}) = T_{\mathbb{F}_p}$ and $\tau(T_\alpha) = T_\beta$. By lemma 2.1 τ extends to an automorphism $\theta \in G_V$. Since T_α is contained in a G_V-stable set $Z_1 \cup \ldots \cup Z_m$, the same is valid for T_β as well. In other words, β divides $\Delta'|_T$. It follows that $\deg \Delta' = \deg \Delta$, and $\Delta' = \Delta$ up to a scalar multiple. Thus all irreducible components of Z are conjugate to each other with respect to G_V. If one of the components were contained in $B_{2n} \smallsetminus U$, we would get $B_{2n} \smallsetminus U = Z$. This is, however, impossible. Indeed, consider the linear span T' of $t'_1, \ldots, t'_n$ where $t'_i = x_i(1 + x_{n+i})$. As $T' \cap (k + \mathfrak{m}^2) = 0$ and $\mathcal{D}_{t'_1}, \ldots, \mathcal{D}_{t'_n}$ span an n-dimensional torus, we have $T' \cap U \neq \varnothing$. On the other hand $T' \subset V \subset Z$ by construction. Thus no irreducible component of $B_{2n} \smallsetminus U$ has codimension 1 in B_{2n}.

(2) Assume $f \in U$. Denote by $B \subset B_{2n}$ the associative subalgebra generated by $f, f^{[p]}, \ldots, f^{[p^{n-1}]}$. Then B is Lagrangian by the definition of U, and so the elements $f^{[a]}$ with $0 \le a < p^n$ form a basis for B. Note that $\mathfrak{z}(f) = \mathfrak{z}(B)$ where $\mathfrak{z}(B) = B$ by lemma 1.2.

(3) and (4) If $\theta \in G$ then $\theta \circ \mathcal{D}_f \circ \theta^{-1} = \mathcal{D}_{\theta f}$ for all $f \in B_{2n}$. If $f = f_s + f_n$ is the Jordan-Chevalley decomposition then we deduce that $\mathcal{D}_{\theta f} = \mathcal{D}_{\theta f_s} + \mathcal{D}_{\theta f_n}$ where $\mathcal{D}_{\theta f_s}$ is semisimple, $\mathcal{D}_{\theta f_n}$ nilpotent, and $[\theta f_s, \theta f_n] = 0$. It follows that $\mathcal{D}_{(\theta f)_s} = \mathcal{D}_{\theta f_s}$, i.e., $(\theta f)_s \equiv \theta f_s \pmod k$. Since U is G-stable, it is immediate now that so is U_s too. Let T be as in the proof of (1). As we have seen, $T \cap U \neq \varnothing$. Take $f \in T \cap U$. Since $\mathcal{D}_f$ is diagonalizable, we have $f \equiv f_s$ modulo k. It follows $f_s \in U$, and so $U_s \neq \varnothing$.

Given $f \in B_{2n}$, let $m \ge 0$ be the largest integer such that $f, f^{[p]}, \ldots, f^{[p^{m-1}]}$ are linearly independent modulo $k + \mathfrak{m}^2$. Since $k + \mathfrak{m}^2$ is a p-Lie subalgebra in B_{2n}, we deduce that $f^{[p^i]}$ is a linear combination of $f, f^{[p]}, \ldots, f^{[p^{m-1}]}$ modulo $k + \mathfrak{m}^2$ for all $i \ge m$. Hence $f \in U$ if and only if $\dim \mathfrak{g}(f)/\mathfrak{g}(f) \cap (k + \mathfrak{m}^2) \ge n$ where $\mathfrak{g}(f) \subset B_{2n}$ denotes the linear span of all elements $f^{[p^i]}$ with $i \ge 0$. Since $f_s \in \mathfrak{g}(f)$, we have $\mathfrak{g}(f_s) \subset \mathfrak{g}(f)$, and so $f_s \in U$ implies $f \in U$. Thus $U_s \subset U$.

Since $\mathfrak{g}(f_s) = \mathfrak{g}(f_s^{[p]})$, our previous observations show that $f_s \in U$ if and only if $f_s^{[p]} \in U$. This gives (4) since $f_s^{[p]}$ is the semisimple component of $f^{[p]}$. There exists $r > 0$ such that $f^{[p^r]}$ is semisimple for every $f \in B_{2n}$. Then $f \in U_s$ if and only if $f^{[p^r]} \in U$. In other words, $U_s = q^{-1}(U)$ where $q : B_{2n} \to B_{2n},\ f \mapsto f^{[p^r]}$, is a polynomial map. Since U is open, so is U_s too.

Obviously, $\mathfrak{z}(f) \subset \mathfrak{z}(f_s)$. If $f \in U_s$ then $\dim \mathfrak{z}(f) = \dim \mathfrak{z}(f_s)$ in view of (2), whence $\mathfrak{z}(f) = \mathfrak{z}(f_s)$. □

Remark. Krylyuk [7] computed the dimensions of generic centralizers and stabilizers of generic linear functions in the Hamiltonian algebras related to the Poisson algebra B_{2n} using essentially the open subset U_s.

3. Construction of invariants

Lemma 3.1. *The assignment $f \mapsto f^{[a]}$ defines a homogeneous of degree a polynomial map $B_{2n} \to B_{2n}$ which is $G_{[p]}$-invariant and L-invariant. If t is a scalar indeterminate and $f, g \in B_{2n}$ then*

$$(f + tg)^{[a]} = f^{[a]} + t \sum_{\{i \ge 0 \mid p^i \le a\}} a_i f^{[a - p^i]} \mathcal{D}_f^{p^i - 1}(g) + \text{terms divisible by } t^2.$$

Proof. The homogeneity and invariance are immediately derived from the special case of $a = p$. The formula ($[p]_3$) from section 1 gives $(f+tg)^{[p]} \equiv f^{[p]} + t\mathcal{D}_f^{p-1}(g)$, and by iteration $(f+tg)^{[p^i]} \equiv f^{[p^i]} + t\mathcal{D}_f^{p^i-1}(g) \pmod{t^2}$ for all $i \ge 0$. The formula for $(f+tg)^{[a]}$ is also immediate now. □

Proposition 3.2. (1) *There are uniquely determined polynomial functions φ_1, $\dots, \varphi_{p^n}$ on B_{2n} such that the following relation holds true for all $f \in B_{2n}$:*

$$f^{[p^n]} + \sum_{a=1}^{p^n} \varphi_a(f) f^{[p^n-a]} = 0. \tag{$*$}$$

(2) *The functions φ_a are $G_{[p]}$-invariant and L-invariant. Furthermore, φ_a is homogeneous of degree a.*

(3) $a\varphi_a(f) = \varphi_1(f^{[a]})$ *for $0 \le a < p^n$ with the convention that $\varphi_0(f) = 1$.*

(4) $\varphi_a'(f,g) = \varphi_1(f^{[a-1]}g)$ *for $0 < a \le p^n$.*

(5) *φ_1 is a nonzero linear function such that* $\ker\varphi_1 = [B_{2n}, B_{2n}]$.

(6) *The symmetric bilinear form $\beta(f,g) = \varphi_1(fg)$ defined on B_{2n} is nondegenerate. If $f \in U_s$ then the restriction of β to $\mathfrak{z}(f)$ is nondegenerate.*

Proof. Clearly, $f^{[p^n]} \in \mathfrak{z}(f)$. If $f \in U$ then it follows from the description of $\mathfrak{z}(f)$ in proposition 2.2 that $f^{[p^n]}$ is a uniquely determined linear combination of the elements $f^{[a]}$ with $0 \le a < p^n$. Hence we can define the functions φ_a on U so that $(*)$ is fulfilled for all $f \in U$.

We claim that the functions φ_a are regular on U. Suppose that $V \subset B_{2n}$ is a subspace of codimension p^n. Put $U_V = \{f \in U \mid B_{2n} = \mathfrak{z}(f) \oplus V\}$, and choose elements e_b, $1 \le b \le p^n$, such that $B_{2n} = ke_1 \oplus \dots \oplus ke_{p^n} \oplus V$. We can write $f^{[a]} \equiv \sum_{b=1}^{p^n} \lambda_{ab}(f) e_b \pmod V$ where λ_{ab} are polynomial functions on B_{2n}. Then U_V consists precisely of those $f \in U$ for which the square matrix $[\lambda_{ab}(f)]_{b=1,\dots,p^n}^{a=0,\dots,p^n-1}$ is invertible. In particular, U_V is an open subset of U. For $f \in U_V$ we have an expression $e_b \equiv \sum_{a=0}^{p^n-1} \mu_{ba}(f) f^{[a]} \pmod V$ where μ_{ba} are regular functions on U_V. Now

$$f^{[p^n]} \equiv \sum_{b=1}^{p^n} \sum_{a=0}^{p^n-1} \lambda_{p^n,b}(f)\mu_{ba}(f) f^{[a]} \pmod V.$$

Since $\mathfrak{z}(f) \cap V = 0$, we get $f^{[p^n]} = \sum_{b=1}^{p^n} \sum_{a=0}^{p^n-1} \lambda_{p^n,b}(f)\mu_{ba}(f) f^{[a]}$. It follows that $\varphi_a(f) = -\sum_{b=1}^{p^n} \lambda_{p^n,b}(f)\mu_{ba}(f)$, which is a regular function on U_V. Clearly U is the union of its open subsets U_V defined for different V. Hence φ_a is regular on U.

Now φ_a are rational functions on B_{2n}. Since $B_{2n} \setminus U$ has no irreducible components of codimension 1, the φ_a's extend to polynomial functions on the whole B_{2n}. Since $(*)$ is fulfilled on an open subset of B_{2n}, it is fulfilled everywhere. That completes the proof of (1).

We may always assume that $f \in U$ when verifying that two polynomial functions in f coincide. Recall that $1, f, \dots, f^{[p^n-1]}$ are linearly independent under this assumption. Multiplying $(*)$ by λ^{p^n}, where $\lambda \in k$, and noting that $(\lambda f)^{[c]} = \lambda^c f^{[c]}$ for all $c \ge 0$, we deduce $\varphi_a(\lambda f) = \lambda^a \varphi_a(f)$. Similarly, applying $\theta \in G_{[p]}$ to $(*)$, we get $\varphi_a(\theta f) = \varphi_a(f)$ since $\theta(f^{[c]}) = (\theta f)^{[c]}$.

We put formally $\varphi_0(f)=1$. Then $(*)$ is rewritten as $\sum_{b+c=p^n}\varphi_b(f)f^{[c]}=0$. Let $f,g,h\in B_{2n}$. Now substitute $f+tg$ for f in $(*)$ where t is a scalar indeterminate and compare the coefficients of t. Using lemma 3.1, we get

$$\sum_{b+c=p^n}\Bigl(\varphi_b'(f,g)f^{[c]}+\varphi_b(f)\sum_{\{i\ge 0\,|\,p^i\le c\}}c_if^{[c-p^i]}\mathcal{D}_f^{p^i-1}(g)\Bigr)=0. \qquad (**)$$

Substitute here $\mathcal{D}_f(g)$ for g. We have $\sum_{\{i\ge 0|p^i\le c\}}c_if^{[c-p^i]}\mathcal{D}_f^{p^i}(g)=[f^{[c]},g]$, and $\sum_{b+c=p^n}\varphi_b(f)[f^{[c]},g]=0$ in view of $(*)$. Hence $\sum_{b+c=p^n}\varphi_b'(f,[f,g])f^{[c]}=0$. This is a linear combination of $1,f,\ldots,f^{[p^n-1]}$ since $\varphi_0'=0$. It follows $\varphi_a'(f,[f,g])=0$, i.e., $\mathcal{D}_g\varphi_a=0$ for all a. That completes the proof of (2).

Suppose now $g\in\mathfrak{z}(f)$. Then $\mathcal{D}_f^{p^i-1}(g)=0$ for all $i>0$, and $(**)$ reduces to the equality

$$\begin{aligned}\sum_{b+c=p^n}\varphi_b'(f,g)f^{[c]}&+\sum_{b+c=p^n,\ c>0}c_0\varphi_b(f)f^{[c-1]}g\\ &=\sum_{b+c=p^n}\varphi_b'(f,g)f^{[c]}-\sum_{b+c=p^n-1}b\varphi_b(f)f^{[c]}g=0\end{aligned}$$

since $c_0\equiv c\equiv -b\pmod p$ in the left hand sum. Take $g=f^{[a]}$ where $0\le a<p^n$. Note that $f^{[c]}f^{[a]}=\lambda f^{[d]}$ where $\lambda\in k$ and d is an integer, $0\le d<p^n$, such that $d_i=c_i+a_i$ or $d_i=c_i+a_i-p$ for each $i=0,\ldots,n-1$ depending on whether $c_i+a_i<p$ or not. We have $d_i<p-1$ in all cases except when $c_i+a_i=p-1$. Hence $d<p^n-1$ in all cases except when $c+a=p^n-1$. Note also that $\varphi_1'(f,g)=\varphi_1(g)$ since φ_1 is a linear function. Thus the coefficient of $f^{[p^n-1]}$ in the displayed equation above equals $\varphi_1(f^{[a]})-a\varphi_a(f)$. If $f\in U$, then $1,f,\ldots,f^{[p^n-1]}$ are linearly independent, whence $\varphi_1(f^{[a]})=a\varphi_a(f)$. Since both sides of the last equality are polynomial functions on B_{2n}, it is fulfilled everywhere. We get (3).

We now prove (5). The L-invariance of the linear function φ_1 means that φ_1 vanishes on $[B_{2n},B_{2n}]$. Suppose that $\varphi_1=0$. Then $\varphi_a=0$ for all $a\not\equiv 0\pmod p$ according to (3). By $(*)$ $f^{[p^n]}$ is a linear combination of elements $f^{[c]}$ with $c<p^n$, $c\equiv 0\pmod p$. Any such $f^{[c]}$ is, modulo $k+\mathfrak{m}^2$, a linear combination of elements $f^{[p^i]}$ with $0<i<n$. Thus $f^{[p]},\ldots,f^{[p^{n-1}]},f^{[p^n]}$ are linearly dependent modulo $k+\mathfrak{m}^2$, and so $f^{[p]}\notin U$ for every $f\in B_{2n}$. But this contradicts proposition 2.2(4). Thus $\varphi_1\ne 0$. As is easily checked straightforwardly, $[B_{2n},B_{2n}]$ is a subspace of codimension 1 in B_{2n} spanned by the monomials $x_1^{r_1}\cdots x_{2n}^{r_{2n}}$ with $r_i<p-1$ for at least one i. It follows $\ker\varphi_1=[B_{2n},B_{2n}]$.

The kernel of β coincides with the largest associative ideal of B_{2n} contained in $\ker\varphi_1$. Any nonzero associative ideal of B_{2n} contains the element $y=x_1^{p-1}\cdots x_{2n}^{p-1}$. Since $y\notin[B_{2n},B_{2n}]$, the bilinear form is nondegenerate. Suppose that $f\in U_s$ so that $\mathfrak{z}(f)=\mathfrak{z}(f_s)$ by proposition 2.2. We have then $B_{2n}=\mathfrak{z}(f)\oplus[f_s,B_{2n}]$ and $\varphi_1(u[f_s,v])=\varphi_1([f_s,uv])=0$ for all $u\in\mathfrak{z}(f)$, $v\in B_{2n}$. As $\mathfrak{z}(f)$ is orthogonal to $[f_s,B_{2n}]$ with respect to β, the second assertion in (6) is clear.

Now multiply $(**)$ by $h\in\mathfrak{z}(f)$ and apply φ_1 to both sides of the equality obtained. Since $hf^{[c-p^i]}\mathcal{D}_f^{p^i-1}(g)=\mathcal{D}_f^{p^i-1}(ghf^{[c-p^i]})\subset[B_{2n},B_{2n}]=\ker\varphi_1$ for all $i>0$, we get

$$\varphi_1\Big(\sum_{b+c=p^n}\varphi'_b(f,g)f^{[c]}h\Big) = -\varphi_1\Big(\sum_{b+c=p^n,\ c>0} c_0\varphi_b(f)f^{[c-1]}gh\Big)$$
$$= \sum_{b+c=p^n-1}\varphi_1(f^{[b]})\varphi_1(f^{[c]}gh)$$

where we first used the equality $-c_0\varphi_b(f) = b\varphi_b(f) = \varphi_1(f^{[b]})$ for $c > 0$ and then substituted $c+1$ for c. We claim that

$$\sum_{b+c=p^n-1}\varphi_1(f^{[b]})\varphi_1(f^{[c]}gh) = \sum_{b+c=p^n-1}\varphi_1(f^{[b]}h)\varphi_1(f^{[c]}g)$$

when $h = f^{[a]}$ with $0 \le a < p^n$. In fact both left and right sides can be rewritten as

$$\sum_{\substack{0\le d<p^n,\quad 0\le e<p^n,\\ d_i+e_i\equiv a_i-1 \pmod p \text{ for } i=0,\ldots,n-1}} \lambda_{de}\varphi_1(f^{[d]})\varphi_1(f^{[e]}g)$$

with $\lambda_{de} = \prod_{i\in I_{de}}\big(f^{[p^i]}\big)^p \in k$ where $I_{de} \subset \{0,1,\ldots,n-1\}$ is the subset consisting of those i for which $e_i < a_i$ in one case and $d_i < a_i$ in the other. Note that for any pair of indices d, e occurring in the sum we have either $d_i + e_i = a_i - 1$ or $d_i + e_i = a_i + p - 1$. One sees that each of the two conditions $e_i < a_i$ and $d_i < a_i$ is equivalent to $d_i + e_i = a_i - 1$. Thus the subsets I_{de} are the same in both cases. We now arrive at the equality

$$\varphi_1\Big(\sum_{b+c=p^n}\varphi'_b(f,g)f^{[c]}h\Big) = \sum_{b+c=p^n-1}\varphi_1(f^{[b]}h)\varphi_1(f^{[c]}g)$$
$$= \varphi_1\Big(\sum_{b+c=p^n-1}\varphi_1(f^{[c]}g)f^{[b]}h\Big)$$

when $h = f^{[a]}$. Suppose that $f \in U_s$. Then $\mathfrak{z}(f)$ is spanned by the elements $f^{[a]}$ with $0 \le a < p^n$, so that the equality above holds for all $h \in \mathfrak{z}(f)$. Applying (6), we get

$$\sum_{b+c=p^n}\varphi'_b(f,g)f^{[c]} = \sum_{b+c=p^n-1}\varphi_1(f^{[c]}g)f^{[b]}$$

Extracting the coefficients of $f^{[p^n-a]}$, we deduce (4). $\square$

Remark. Assertions (3) and (5) show that $f^{[a]} \in [B_{2n}, B_{2n}]$ whenever $0 \le a < p^n$ and $p|a$.

Denote by $\kappa : B_{2n} \to k$ the homomorphism of associative algebras with kernel $\mathfrak{m}$. Put $\kappa_i(f) = \kappa(f^{[p^i]})$. Thus κ_i is a homogeneous polynomial function of degree p^i on B_{2n}. It is $G_{[p]}$-invariant and L_0-invariant. We mention also that $\kappa = \kappa_0$ is a G-invariant function.

Lemma 3.3. *The differentials of $p^n + n$ functions $\varphi_1, \ldots, \varphi_{p^n}, \kappa_0, \ldots, \kappa_{n-1}$ are linearly independent at all $f \in U$.*

Proof. For $g \in B_{2n}$ we have $(d\varphi_a)_f(g) = \varphi'_a(f,g) = \beta(f^{[a-1]}, g)$ by proposition 3.2, and $(d\kappa_i)_f(g) = \kappa'_i(f,g) = \kappa\big(\mathcal{D}_f^{p^i-1}(g)\big)$ in view of lemma 3.1. Since $1, \ldots, f^{[p^n-1]}$

are linearly independent and β is nondegenerate, $(d\varphi_1)_f, \ldots, (d\varphi_{p^n})_f$ are linearly independent. It remains to show that the linear functions $(d\kappa_0)_f, \ldots, (d\kappa_{n-1})_f$ have linearly independent restrictions to the subspace $V = \bigcap_{a=1}^{p^n} \ker(d\varphi_a)_f$. Note that V is the orthogonal complement of $\mathfrak{z}(f)$ with respect to β. Since β is L-invariant, $\mathfrak{z}(f)$ coincides with the orthogonal complement of the subspace $[f, B_{2n}]$. It follows $V = [f, B_{2n}]$. Now $(d\kappa_i)_f([f,g]) = \kappa([f^{[p^i]}, g])$. The elements $y_i = f^{[p^i]} - \kappa(f^{[p^i]})$ with $0 \le i < n$ lie in $\mathfrak{m}$ and generate the Lagrangian subalgebra $\mathfrak{z}(f)$. As we have seen in the proof of lemma 1.2 there exist elements $z_0, \ldots, z_{n-1} \in \mathfrak{m}$ such that $[f^{[p^i]}, z_j] = [y_i, z_j] \equiv \delta_{ij} \pmod{\mathfrak{m}}$ for all $0 \le i, j < n$. Then $[f, z_j] \in V$ and $(d\kappa_i)_f([f, z_j]) = \delta_{ij}$. Thus we are done. $\square$

Theorem 3.4. *The algebra of invariants $k[B_{2n}]^L$ (respectively $k[B_{2n}]^{L_0}$) is generated over $k[B_{2n}]^{(p)}$ by $\varphi_1, \ldots, \varphi_{p^n}$ (respectively by $\varphi_1, \ldots, \varphi_{p^n}, \kappa_0, \ldots, \kappa_{n-1}$). Both algebras are free over $k[B_{2n}]^{(p)}$ and are locally complete intersection rings.*

Proof. Apply theorem 1.4 for $V = B_{2n}$ and $\mathfrak{g} = B_{2n}$ or $\mathfrak{g} = \mathfrak{m}^2$ operating on V via the homomorphism $\mathfrak{g} \to L$. Since $\dim \mathfrak{z}(f) = p^n$ for all f in an open subset of B_{2n}, we have $c_{\mathfrak{g}}(V) = p^{2n} - p^n$ in case of $\mathfrak{g} = B_{2n}$. If $f \in U$ then $\mathfrak{z}(f)$ is a Lagrangian subalgebra, whence $\dim \mathfrak{z}(f) \cap \mathfrak{m}^2 = p^n - n - 1$. Now $\dim \mathfrak{m}^2 = p^{2n} - 2n - 1$, and it follows that $c_{\mathfrak{g}}(V) = \operatorname{codim}_{\mathfrak{m}^2} \mathfrak{z}(f) \cap \mathfrak{m}^2 = p^{2n} - p^n - n$ in case of $\mathfrak{g} = \mathfrak{m}^2$. Thus we have the correct number of invariant functions $m = p^n$ (respectively $m = p^n + n$). Lemma 3.3 and proposition 2.2 show that the hypotheses of theorem 1.4 are fulfilled. $\square$

In order to get the G-invariant functions we need to modify our construction slightly. For $a \ge 0$ put

$$f^{\langle a \rangle} = \prod_{i \ge 0} \left(f^{[p^i]} - \kappa_i(f)\right)^{a_i}.$$

Thus $f^{\langle p^i \rangle} = f^{[p^i]} - \kappa_i(f)$ is the unique element $g \in \mathfrak{m}$ such that $\mathcal{D}_g = \mathcal{D}_f^{p^i}$. It is clear that the polynomial map $B_{2n} \to B_{2n}$ given by assignment $f \mapsto f^{\langle a \rangle}$ is G-invariant and homogeneous of degree a.

Proposition 3.5. (1) *There are uniquely determined polynomial functions $\widetilde{\varphi}_1, \ldots, \widetilde{\varphi}_{p^n-1}$ on B_{2n} such that the following relation holds true for all $f \in B_{2n}$:*

$$f^{\langle p^n \rangle} + \sum_{a=1}^{p^n-1} \widetilde{\varphi}_a(f) f^{\langle p^n - a \rangle} = 0.$$

(2) *The functions $\widetilde{\varphi}_a$ are G-invariant and homogeneous with* $\deg \widetilde{\varphi}_a = a$.

(3) $\widetilde{\varphi}_a(f) = \sum_{b=1}^{a} (-1)^{a-b} \binom{a-1}{b-1} \kappa(f^{[a-b]}) \varphi_b(f)$ *for all $f \in B_{2n}$ and $0 < a < p^n$.*

(4) $\varphi_a(f) = \sum_{b=1}^{a} \binom{a-1}{b-1} \kappa(f^{[a-b]}) \widetilde{\varphi}_b(f)$ *for all $f \in B_{2n}$ and $0 < a < p^n$.*

(5) $\varphi_{p^n}(f) = -\kappa_n(f) - \sum_{b=1}^{p^n-1} (-1)^b \kappa(f^{[p^n-b]}) \widetilde{\varphi}_b(f)$ *for all $f \in B_{2n}$.*

(6) *The differentials of p^n+n functions $\widetilde\varphi_1,\dots,\widetilde\varphi_{p^n-1},\kappa_0,\dots,\kappa_n$ are linearly independent at all $f\in U$.*

Proof. If $f\in U$ then the elements $f^{\langle p^i\rangle}$ with $0\le i<n$ are linearly independent modulo $\mathfrak m^2$, whence the elements $f^{\langle a\rangle}$ with $0\le a<p^n$ form a basis for $\mathfrak z(f)$. In particular, the equality in (1) characterizes the $\widetilde\varphi_a$'s uniquely. Now note that

$$f^{[a]}=\sum_{\substack{b_0+c_0=a_0,\\ b_1+c_1=a_1,\dots}}\ \prod_{i\ge0}\binom{a_i}{c_i}\kappa\big(f^{[p^i]}\big)^{b_i}\big(f^{\langle p^i\rangle}\big)^{c_i}=\sum_{b+c=a}\binom{a}{c}\kappa(f^{[b]})f^{\langle c\rangle}.$$

as $\binom{a}{c}\equiv\prod\binom{a_i}{c_i}\pmod p$. By proposition 3.2

$$0=\sum_{b+c=p^n}\varphi_b(f)f^{[c]}=\sum_{b+d+e=p^n}\binom{d+e}{e}\varphi_b(f)\kappa(f^{[d]})f^{\langle e\rangle}=\sum_{a+e=p^n}\widetilde\varphi_a(f)f^{\langle e\rangle}$$

where we put $\widetilde\varphi_a(f)=\sum_{b+d=a}\binom{p^n-b}{p^n-a}\varphi_b(f)\kappa(f^{[d]})$ for $a=0,\dots,p^n$. Here $\widetilde\varphi_0=1$. If $0<a<p^n$, then $\binom{p^n}{p^n-a}\equiv0$ and $\binom{p^n-b}{p^n-a}\equiv(-1)^{a-b}\binom{a-1}{b-1}\pmod p$ for $b>0$, so that the $\widetilde\varphi_a$'s are given by the formula in (3). Note that $f^{\langle0\rangle}=1$ and $f^{\langle e\rangle}\in\mathfrak m$ whenever $e>0$. It follows from the displayed equality above that $\widetilde\varphi_{p^n}=0$, and we come to (1). Assertion (2) is a consequence of properties of maps $f\mapsto f^{\langle a\rangle}$.

Using the relation $f^{\langle a\rangle}=\sum_{b+c=a}(-1)^b\binom{a}{c}\kappa(f^{[b]})f^{[c]}$, we deduce similarly

$$0=\sum_{b+c=p^n}\widetilde\varphi_b(f)f^{\langle c\rangle}=\sum_{b+d+e=p^n}(-1)^d\binom{d+e}{e}\widetilde\varphi_b(f)\kappa(f^{[d]})f^{[e]},$$

which proves (4) and (5). For each $a=1,\dots,p^n$ the function φ_a is expressed as a polynomial in $\widetilde\varphi_1,\dots,\widetilde\varphi_{p^n-1},\kappa_0,\dots,\kappa_n$. Hence $(d\varphi_a)_f$ is a linear combination of $(d\widetilde\varphi_1)_f,\dots,(d\widetilde\varphi_{p^n-1})_f,(d\kappa_0)_f,\dots,(d\kappa_n)_f$. Now (6) follows from lemma 3.3. □

Corollary 3.6. *One has $\varphi_1=\widetilde\varphi_1$. The bilinear form β on B_{2n} is L-invariant and G-invariant.*

We will use the notations $\widetilde\varphi_0=1$ and $\widetilde\varphi_{p^n}=0$ for consistency reasons. If $\lambda\in k$ then $(f+\lambda)^{\langle a\rangle}=f^{\langle a\rangle}$ for all a, whence also $\widetilde\varphi_a(f+\lambda)=\widetilde\varphi_a(f)$ for all a. This shows that $\widetilde\varphi_a$ induces a G-invariant polynomial function on $L\cong B_{2n}/k$.

4. A universal construction and automorphisms

With each Lagrangian subalgebra $B\subset B_{2n}$ we will associate a Poisson algebra $F(B)$. The latter is attached to B in a canonical way in the sense that every isomorphism of Lagrangian subalgebras $\tau:B\to B'$ compatible with the $[p]$-map induces an isomorphism of Poisson algebras $\tau_*:F(B)\to F(B')$. We will show that $B_{2n}\cong F(B)$, although this isomorphism depends on additional data. This will enable us to prove that any isomorphism τ above extends to an element of the group G of Poisson automorphisms of B_{2n}.

We first recall one construction (see [20], Theorem 2.2, for a more general treatment). Suppose that $\mathfrak g$ is a p-Lie algebra and A an arbitrary algebra over k. Put $F(\mathfrak g,A)=\operatorname{Hom}\big(u(\mathfrak g),A\big)$ where $u(\mathfrak g)$ is the restricted universal enveloping algebra of $\mathfrak{g}$. With each $x \in \mathfrak{g}$ we associate a linear transformation D_x of $F(\mathfrak{g}, A)$ defined by the rule $(D_x f)(u) = f(ux)$ for $f \in F(\mathfrak{g}, A)$ and $u \in u(\mathfrak{g})$. This makes $F(\mathfrak{g}, A)$ into a restricted $\mathfrak{g}$-module. Define a linear map $\pi : F(\mathfrak{g}, A) \to A$ by the rule $\pi(f) = f(1)$. Then for every $u(\mathfrak{g})$-module M and a linear map $\xi : M \to A$ there exists a unique $\mathfrak{g}$-module homomorphism $\eta : M \to F(\mathfrak{g}, A)$ such that $\xi = \pi \circ \eta$. Explicitly, $\eta(m)(u) = \xi(u \cdot m)$. In particular, if η satisfies $\pi \circ \eta = 0$ then necessarily $\eta = 0$. This shows also that $\ker \pi$ contains no nonzero $\mathfrak{g}$-invariant subspaces.

Using the universality property above, one sees easily that $F(\mathfrak{g}, A)$ has a unique $\mathfrak{g}$-invariant multiplication such that π is an algebra homomorphism. The explicit formula involves the comultiplication in $u(\mathfrak{g})$ but we will not need it. Now $\mathfrak{g}$ operates on $F(\mathfrak{g}, A)$ as a p-Lie algebra of derivations. Considering next the trivial $\mathfrak{g}$-module k, we see that for every element $a \in A$ there exists a unique $\mathfrak{g}$-module homomorphism $\eta : k \to F(\mathfrak{g}, A)$ such that $\pi(\eta(1)) = a$. In other words π maps the subalgebra of $\mathfrak{g}$-invariants $F(\mathfrak{g}, A)^{\mathfrak{g}}$ isomorphically onto A. We will identify A with $F(\mathfrak{g}, A)^{\mathfrak{g}}$ by means of this isomorphism. After this identification we have $D_x(a) = 0$ for all $x \in \mathfrak{g}$ and $a \in A$. In our application A will be commutative, associative and unital. Then $F(\mathfrak{g}, A)$ inherits the same properties.

Suppose that $B \subset B_{2n}$ is a Lagrangian subalgebra. By (2) of lemma 1.2 B is a p-Lie subalgebra containing the Lie center k of B_{2n}. We apply the previous construction taking $\mathfrak{g} = B/k$ and $A = B$ considered as an algebra with respect to the associative multiplication. We thus obtain a commutative, associative and unital algebra $F(\mathfrak{g}, B)$ and a homomorphism of algebras $\pi : F(\mathfrak{g}, B) \to B$. With each $f \in B$ we have associated a derivation D_f of $F(\mathfrak{g}, B)$ which depends only on the coset of f modulo k, so that $D_1 = 0$. Furthermore, B is identified with the subalgebra of elements $g \in F(\mathfrak{g}, B)$ such that $D_f(g) = 0$ for all $f \in B$. We have $\pi(g) = g$ for all $g \in B$. Put

$$F(B) = \{h \in F(\mathfrak{g}, B) \mid D_{fg}(h) = fD_g(h) + gD_f(h) \text{ for all } f, g \in B\}.$$

Clearly $F(B)$ is a subalgebra of $F(\mathfrak{g}, B)$ and $B \subset F(B)$. Since the Lie multiplication in B is abelian, the B-submodule of $\operatorname{Der} F(\mathfrak{g}, B)$ generated by all derivations D_f with $f \in B$ is an abelian Lie algebra too. It is immediate thereof that $F(B)$ is stable under all derivations D_f.

Proposition 4.1. *There exists a unique Poisson bracket on $F(B)$ such that the following identities hold for all $f \in B$ and $g, h \in F(B)$:*

(1) $D_f([g, h]) = [D_f(g), h] + [g, D_f(h)]$.

(2) $[f, g] = D_f(g)$.

(3) $\pi([g, h]) = 0$ *whenever* $\pi(g) = 0$ *and* $\pi(h) = 0$.

Proof. Put $J = \{g \in F(B) \mid \pi(g) = 0\}$. Then $F(B) = B \oplus J$ and J is an ideal of $F(B)$. Define a linear map $\xi : F(B)^{\otimes 2} \to B$ setting

$$\xi(g \otimes h) = \begin{cases} 0 & \text{when } g, h \in J, \\ \pi\big(D_g(h)\big) & \text{when } g \in B, \\ -\pi\big(D_h(g)\big) & \text{when } h \in B, \end{cases}$$

Note that $D_g(h) = 0 = D_h(g)$ when $g, h \in B$, so that ξ is well defined. If the required Poisson bracket on $F(B)$ exists then the formula $\eta(g \otimes h) = [g, h]$ defines a $\mathfrak{g}$-module homomorphism $\eta : F(B)^{\otimes 2} \to F(B)$ satisfying $\pi \circ \eta = \xi$. However, by the universality property of $F(\mathfrak{g}, B)$ there exists a unique $\mathfrak{g}$-module homomorphism $\eta : F(B)^{\otimes 2} \to F(\mathfrak{g}, B)$ such that $\pi \circ \eta = \xi$. We put $[g, h] = \eta(g \otimes h) \in F(\mathfrak{g}, B)$ for $g, h \in F(B)$. We will have yet to check that η takes values in $F(B)$.

Identities (1) and (3) in the statement of the proposition are immediate from the definition of η. The linear map $\alpha : B \otimes F(B) \to F(B)$ defined by the rule $\alpha(f \otimes h) = D_f(h)$ is clearly a $\mathfrak{g}$-module homomorphism and $\pi \circ \alpha = \xi$. Then α coincides with the restriction of η by the universality property of $F(\mathfrak{g}, B)$. Hence (2) is also fulfilled.

We will construct several other $\mathfrak{g}$-module homomorphisms to obtain the necessary identities. Consider first $\beta : F(B)^{\otimes 2} \to F(\mathfrak{g}, B)$ such that $\beta(g \otimes h) = [g, h] + [h, g]$. Then $\pi \circ \beta = 0$, whence $\beta = 0$. Note that $[f, f] = D_f(f) = 0$ for all $f \in B$. If $g \in J$ then $\pi([g, g]) = 0$ by (3) and $D_f([g, g]) = [D_f(g), g] + [g, D_f(g)] = \beta(D_f(g) \otimes g) = 0$ for all $f \in B$, whence $[g, g] \in F(\mathfrak{g}, B)^{\mathfrak{g}} = B$. It follows that $[g, g] = 0$ for all $g \in F(B)$.

Consider next $\gamma : F(B)^{\otimes 3} \to F(\mathfrak{g}, B)$, $\gamma(f \otimes g \otimes h) = [fg, h] - f[g, h] - g[f, h]$ for $f, g, h \in F(B)$. If $h \in B$ then, using (2) and the anticommutativity, we can rewrite the value of γ as $-D_h(fg) + fD_h(g) + gD_h(f)$. As D_h is a derivation, we get $\gamma(f \otimes g \otimes h) = 0$ in this case. The same is true whenever $f, g \in B$ as is immediate from (2) and the definition of $F(B)$. If now $h \in J$ and either $f \in J$ or $g \in J$ then $\pi([fg, h] - f[g, h] - g[f, h]) = 0$ because J is an ideal and $\pi([J, J]) = 0$ by (3). It follows that $\pi \circ \gamma = 0$, and then $\gamma = 0$.

We can now show that $[h, h'] \in F(B)$ for all $h, h' \in F(B)$. If $f, g \in B$ then

$$\begin{aligned} fD_g([h, h']) &= f[D_g(h), h'] + f[h, D_g(h')] \\ &= [fD_g(h), h'] - D_g(h)[f, h'] + [h, fD_g(h')] - [h, f]D_g(h') \\ &= [fD_g(h), h'] - D_g(h)D_f(h') + [h, fD_g(h')] + D_f(h)D_g(h'). \end{aligned}$$

Setting $D_{f,g} = D_{fg} - fD_g - gD_f$, we deduce

$$D_{f,g}([h, h']) = [D_{f,g}(h), h'] + [h, D_{f,g}(h')] = 0,$$

as desired.

Finally, consider the $\mathfrak{g}$-module homomorphism $\delta : F(B)^{\otimes 3} \to F(B)$ such that $\delta(f \otimes g \otimes h) = [f, [g, h]] - [[f, g], h] - [g, [f, h]]$. If $f \in B$ then $\delta(f \otimes g \otimes h) = 0$ as this equality reduces to (1). Since δ is skewsymmetric in its arguments, the same is valid when either $g \in B$ or $h \in B$. Now (3) means that $[J, J] \subset J$, and therefore $\delta(f \otimes g \otimes h) \in J$ whenever $f, g, h \in J$. It follows that $\pi \circ \delta = 0$, and $\delta = 0$. All necessary identities are now checked. $\square$

Let C be an arbitrary Poisson algebra over k. Suppose that $C = C' \oplus I$ where C' is an associative subalgebra and I an associative ideal of C such that $[C', C'] = 0$ and $[I, I] \subset I$. Suppose also that C' is endowed with a p-semilinear transformation $f \mapsto f^{[p]}$ such that $1^{[p]} = 0$ and $\mathcal{D}_f^p = \mathcal{D}_{f^{[p]}}$ for all $f \in C'$, where $\mathcal{D}_f \in \operatorname{Der} C$ denotes the adjoint derivation.

Proposition 4.2. (1) *Under the above hypotheses every isomorphism of algebras $\tau : C' \to B$ such that $\tau(f^{[p]}) \equiv \tau(f)^{[p]} \pmod{k}$ for all $f \in C'$ extends in a unique way to a homomorphism of Poisson algebras $\sigma : C \to F(B)$ such that $\sigma(I) \subset \ker \pi$.*

(2) *If $C = B_{2n}$, $C' = B$ and $\tau = \mathrm{id}_B$ then the homomorphism σ in* (1) *is an isomorphism.*

Proof. We may regard C' as an abelian p-Lie algebra which operates on C by means of the representation $f \mapsto \mathcal{D}_f$. Since $[k, C] = 0$, there is the induced action of the factor algebra C'/k on C. Now τ induces an isomorphism of p-Lie algebras $C'/k \to B/k$, and so the p-Lie algebra $\mathfrak{g} = B/k$ operates on C via the inverse isomorphism. Let $\pi_C : C \to C'$ be the projection with respect to the decomposition $C = C' \oplus I$. There exists then a unique $\mathfrak{g}$-module homomorphism $\sigma : C \to F(\mathfrak{g}, B)$ such that $\pi \circ \sigma = \tau \circ \pi_C$. It is immediate that $\sigma(I) \subset \ker \pi$ and $\pi \circ \sigma|_{C'} = \tau = \pi \circ \tau$. Hence $\sigma|_{C'} = \tau$ by the uniqueness property for $\mathfrak{g}$-module homomorphisms into $F(\mathfrak{g}, B)$.

Consider the $\mathfrak{g}$-module homomorphism $\alpha : C \otimes C \to F(\mathfrak{g}, B)$ defined by the rule $\alpha(g \otimes h) = \sigma(gh) - \sigma(g)\sigma(h)$ for $g, h \in C$. Since $\pi \circ \sigma = \tau \circ \pi_C$ is a homomorphism of associative algebras, we get $\pi \circ \alpha = 0$, whence $\alpha = 0$. Thus σ is a homomorphism of associative algebras.

Note that the $\mathfrak{g}$-invariance of σ means that $D_{\tau(g)}\big(\sigma(h)\big) = \sigma\big(\mathcal{D}_g(h)\big)$ for $g \in C'$ and $h \in C$. If $f, g \in C'$ and $h \in C$ then

$$\Big(D_{\tau(f)\tau(g)} - \tau(f)D_{\tau(g)} - \tau(g)D_{\tau(f)}\Big)\sigma(h) = \sigma\Big((\mathcal{D}_{fg} - f\mathcal{D}_g - g\mathcal{D}_f)(h)\Big) = 0$$

by the properties of Poisson brackets. Since $\tau(C') = B$, we deduce $\sigma(h) \in F(B)$.

Consider the $\mathfrak{g}$-module homomorphism $\beta : C \otimes C \to F(B)$ defined by the rule $\beta(g \otimes h) = \sigma([g,h]) - [\sigma(g), \sigma(h)]$ for $g, h \in C$. If $g \in C'$ then $\beta(g \otimes h) = 0$ in view of the $\mathfrak{g}$-invariance of σ. By anticommutativity $\beta(g \otimes h) = 0$ when $h \in C'$ as well. If $g, h \in I$ then $\beta(g \otimes h) \in \ker \pi$. Thus $\pi \circ \beta = 0$, and so $\beta = 0$. In other words, $\sigma : C \to F(B)$ respects the Poisson brackets.

Clearly $\ker \sigma$ is an associative and a Lie ideal of C such that $\ker \sigma \subset I$. Under the assumptions of (2) $\ker \sigma$ is stable under $\partial_1, \ldots, \partial_{2n} \in L$. It is easy to see that B_{2n} contains no nonzero proper associative ideals stable under $\partial_1, \ldots, \partial_{2n}$. It follows $\ker \sigma = 0$.

Denote by $T \subset \operatorname{End}_k F(B)$ the associative subalgebra generated by all derivations D_f with $f \in B$ and all operators of associative multiplications by elements $f \in B$. Clearly T is commutative. We may identify B with the subalgebra of associative multiplication operators in T. It is immediate from the identity $D_{fg} = fD_g + gD_f$ that T is generated as an algebra over B by $D_{y_1}, \ldots, D_{y_n}$ where $y_1, \ldots, y_n \in \mathfrak{m}$ is any minimal system of generators for B. Since $D_f^p = D_{f^{[p]}}$ is a B-linear combination of derivations $D_{y_1}, \ldots, D_{y_n}$ for every $f \in B$, we see that T is generated as a module over B by p^n elements $D_{y_1}^{r_1}, \ldots, D_{y_n}^{r_n}$ where $0 \le r_i < p$. Now define a linear map $\lambda : F(B) \to \operatorname{Hom}_B(T, B)$ setting $\lambda(h)(\psi) = \pi\big(\psi(h)\big)$ for $h \in F(B)$ and $\psi \in T$. Then $\ker \lambda$ is the largest T-invariant subspace contained in $\ker \pi$. As we know, $\ker \pi$ contains no nonzero $\mathfrak{g}$-invariant subspaces, whence $\ker \lambda = 0$. We conclude

$$\dim F(B) \le \dim \operatorname{Hom}_B(T, B) \le p^n \dim B = p^{2n} = \dim B_{2n}.$$

Comparing of dimensions yields $\sigma(B_{2n}) = F(B)$, i.e., σ is an isomorphism. □

Theorem 4.3. *Suppose $B, B' \subset B_{2n}$ are Lagrangian subalgebras and $I, I' \subset B_{2n}$ Lagrangian ideals such that $B_{2n} = B \oplus I = B' \oplus I'$, Then every isomorphism of associative algebras $\tau : B \to B'$ satisfying $\tau(f^{[p]}) \equiv \tau(f)^{[p]} \pmod{k}$ for all $f \in B$ extends uniquely to an automorphism $\theta \in G$ such that $\theta(I) = I'$. If, moreover,*

$\tau(f^{[p]}) = \tau(f)^{[p]}$ *for all* $f \in B$ *and both* I *and* I' *are closed under the* $[p]$*-map then* $\theta \in G_{[p]}$.

Proof. By proposition 4.2 we have a commutative diagram

$$\begin{array}{ccccccc} B_{2n} & \xrightarrow{\sigma} & F(B) & \xrightarrow{\tau_*} & F(B') & \xleftarrow{\sigma'} & B_{2n} \\ \uparrow\downarrow & & \uparrow\downarrow & & \uparrow\downarrow & & \uparrow\downarrow \\ B & \xrightarrow{\mathrm{id}} & B & \xrightarrow{\tau} & B' & \xleftarrow{\mathrm{id}} & B' \end{array}$$

where the upward arrows are the inclusion maps, the downward arrows on the sides of the diagram are retractions with kernel I and I', respectively, the downward arrows in the middle are canonical retractions, and the arrows in the top row are the homomorphisms of Poisson algebras induced by the respective algebra homomorphisms in the bottom row. Both σ and σ' are isomorphisms by proposition 4.2. The isomorphism τ^{-1} induces $\tau_*^{-1} : F(B') \to F(B)$, and it is clear that $\tau_*^{-1} \circ \tau_*$ and $\tau_* \circ \tau_*^{-1}$ are both identity maps by the uniqueness property. Hence τ_* is also an isomorphism. Now $\theta = \sigma'^{-1} \circ \tau_* \circ \sigma$ is the required element of G, and the uniqueness is also clear.

Suppose that τ commutes with the $[p]$-map and both I and I' are closed under the $[p]$-map. Given $g \in I$, consider the element $h = (\tau_* \circ \sigma)(g^{[p]}) - \sigma'((\theta g)^{[p]}) \in F(B')$. We have $\pi(h) = 0$ and

$$\begin{aligned} [\tau(f), h] &= (\tau_* \circ \sigma)([f, g^{[p]}]) - \sigma'([\theta(f), (\theta g)^{[p]}]) \\ &= -(\tau_* \circ \sigma)\big((\mathcal{D}_g^p(f)\big) + (\sigma' \circ \theta)\big((\mathcal{D}_g^p(f)\big) = 0 \end{aligned}$$

for all $f \in B$. It follows that $[B', h] = 0$, whence $h \in B' \cap \ker \pi = 0$. We deduce that $\theta(g^{[p]}) = \theta(g)^{[p]}$ for all $g \in I$. We have $\theta(f^{[p]}) = \theta(f)^{[p]}$ for all $f \in B$ since $\theta|_B = \tau$. By the Jacobson p-th power formula the equality $\theta(f^{[p]}) = \theta(f)^{[p]}$ holds then for all $f \in B_{2n}$. Thus $\theta \in G_{[p]}$. □

Remark. In this section we never used an explicit expression for the Poisson bracket on B_{2n}. The only properties actually needed are:

(a) there exists a $[p]$-map making B_{2n} into a p-Lie algebra,

(b) B_{2n} contains no nonzero proper associative ideals which are stable under all $\mathcal{D}_f$.

One can strengthen theorem 4.3 as follows. Given two Poisson brackets satisfying (a) and (b), a Lagrangian pair B, I with respect to the first bracket and a Lagrangian pair B', I' with respect to the second bracket, every $[p]$-compatible isomorphism $\tau : B \to B'$ extends to an automorphism $\theta \in \operatorname{Aut} B_{2n}$ which transforms one Poisson bracket to another. Given a Poisson bracket satisfying (a) and (b), there exist two n-dimensional tori $T_1, T_2 \subset B_{2n}$ such that $T_1, T_2 \subset \mathfrak{m}$ and $B_{2n} = k \oplus T_1 \oplus T_2 \oplus \mathfrak{m}^2$. In fact, it is easy to ascertain the existence of an n-dimensional torus $T_0 \in \mathfrak{m}^2$ as $\mathfrak{m}^2/\mathfrak{m}^3$ is a p-Lie algebra operating faithfully on $V = \mathfrak{m}/\mathfrak{m}^2$ as $\mathrm{sp}(V)$ when $p > 2$ and as the commutant of $\mathrm{sp}(V)$ when $p = 2$. To obtain T_1 and T_2 one has to apply Winter's switchings of tori (see [24]) taking a certain amount of care. Now T_1 generates a Lagrangian subalgebra B and T_2 a Lagrangian ideal I such that $B_{2n} = B \oplus I$. If T_1', T_2' and B', I' are constructed similarly with respect to a second Poisson bracket satisfying (a) and (b) then an isomorphism of tori $T_1 \cong T_1'$ extends to a $[p]$-compatible isomorphism $\tau : B \to B'$. It follows that any two

Poisson brackets satisfying (a) and (b) are conjugate with respect to $\operatorname{Aut} B_{2n}$. This can be also derived from the known results. A Poisson bracket satisfying (a) and (b) corresponds to a Hamiltonian form on W_{2n} which has to be exact by [17], Th. 2.2. According to the classification of Hamiltonian forms on W_{2n} [12], the exact Hamiltonian forms belong to a single orbit with respect to $\operatorname{Aut} B_{2n}$.

5. Cross section of regular classes

In the construction of cross sections in theorem 5.2 we assume that $x_i^{[p]} = 0$ for all $i = 1, \dots, 2n$ (see lemma 1.1).

Lemma 5.1. *Suppose $f, h \in B_{2n}$ and $g \in \mathfrak{m}$ satisfy $[f,g] = 1$ and $[f,h] \in g^{p-1}B_{2n}$. If $p = 2$ assume also that $g^{[2]} = 0$. Then*

$$(f + g^{p-1}h)^{[p]} = f^{[p]} - h + g^{p-1}h[g,h].$$

Proof. We will need a precise computation of terms occurring in the formula $([p]_3)$ from section 1. Put $y = g^{p-1}h$. As $g^p = 0$, we have $\mathcal{D}_f^i(y) = (-1)^i i! g^{p-1-i}h$ for $i < p$. Now $s_1(f,y) = \mathcal{D}_f^{p-1}(y) = -h$. Note that $[y, \mathcal{D}_f^i(y] \in [g^{p-1}B_{2n}, g^2B_{2n}] = 0$ for $i < p-2$. In particular, $s_l(f,y) = 0$ for $2 < l \le p-1$. If $p > 2$ then

$$2s_2(f,y) = [y, \mathcal{D}_f^{p-2}(y)] = [g^{p-1}h, -gh] = (2-p)g^{p-1}h[g,h].$$

We see also by induction on i that $\mathcal{D}_y^i(B_{2n}) \subset g^{i(p-2)}B_{2n}$. If $p > 2$ then $y^{[p]} = 0$ as $y \in \mathfrak{m}^2$ and $\mathcal{D}_y^3 = 0$. Suppose $p = 2$. We have

$$\begin{aligned}
\mathcal{D}_{gh}^2 = (g\mathcal{D}_h + h\mathcal{D}_g)^2 &= (g\mathcal{D}_h)^2 + [g\mathcal{D}_h, h\mathcal{D}_g] + (h\mathcal{D}_g)^2 \\
&= g^2\mathcal{D}_h^2 + g[h,g]\mathcal{D}_h + gh\mathcal{D}_{[h,g]} + h^2\mathcal{D}_g^2 + h[g,h]\mathcal{D}_g \\
&= \mathcal{D}_{gh[g,h]}
\end{aligned}$$

since $g^2 = 0$ and $\mathcal{D}_g^2 = 0$ by the assumptions on g. If $h \in \mathfrak{m}$ then $(gh)^{[2]} \in \mathfrak{m}^2$, whence $(gh)^{[2]} = gh[g,h]$. In general, let $h = \lambda + h'$ where $\lambda \in k$ and $h' \in \mathfrak{m}$. Then

$$(gh)^{[2]} = (\lambda g + gh')^{[2]} = \lambda^2 g^{[2]} + \lambda g[g,h'] + gh'[g,h'] = gh[g,h]. \qquad \square$$

We adopt the convention that the product over an empty set is equal to 1. For $\lambda = (\lambda_1, \dots, \lambda_n) \in \mathbb{A}^n$ and $h \in k[x_1, \dots, x_n] \subset B_{2n}$ define an element

$$u_{\lambda,h} = \sum_{i=1}^{n} \Big((-1)^{i-1}(\lambda_i + x_i) \prod_{j=1}^{i-1} x_{n+j}^{p-1} \Big) + (-1)^{n-1} h \prod_{j=1}^{n} x_{n+j}^{p-1} \in B_{2n}$$

and consider the following affine subspaces of dimension $p^n + n$ and p^n in B_{2n}:

$$\begin{aligned}
S &= \{\, u_{\lambda,h} \mid \lambda \in \mathbb{A}^n \text{ and } h \in k[x_1, \dots, x_n] \,\}, \\
S_0 &= \{\, u_{\lambda,h} \mid \lambda_2 = \ldots = \lambda_n = 0 \text{ and } h \in \mathfrak{m} \cap k[x_1, \dots, x_n] \,\}.
\end{aligned}$$

Theorem 5.2. (1) *The invariant functions $\varphi_1, \dots, \varphi_{p^n}, \kappa_0, \dots, \kappa_{n-1}$ (respectively $\widetilde{\varphi}_1, \dots, \widetilde{\varphi}_{p^n-1}, \kappa$) separate the $G_{[p]}$-orbits (respectively G-orbits) on U.*

(2) *The morphisms of algebraic varieties* $\varphi : S \to \mathbb{A}^{p^n+n}$ *and* $\widetilde{\varphi} : S_0 \to \mathbb{A}^{p^n}$ *given by functions* $\varphi_1, \ldots, \varphi_{p^n}, \kappa_0, \ldots, \kappa_{n-1}$ *and* $\widetilde{\varphi}_1, \ldots, \widetilde{\varphi}_{p^n-1}, \kappa$*, respecctively, are isomorphisms.*

(3) *One has* $S \subset U$*, and each* $G_{[p]}$*-orbit (respectively* G*-orbit) on* U *meets* S *(respectively* S_0*) at a single point.*

(4) *The algebra of invariants* $k[B_{2n}]^{G_{[p]}}$ *(respectively* $k[B_{2n}]^G$*) is generated by functions* $\varphi_1, \ldots, \varphi_{p^n}, \kappa_0, \ldots, \kappa_{n-1}$ *(respectively* $\widetilde{\varphi}_1, \ldots, \widetilde{\varphi}_{p^n-1}, \kappa$*) which are algebraically independent.*

Proof. Let $f, g \in U$. Suppose $\kappa(f) = \kappa(g)$ and $\widetilde{\varphi}_a(f) = \widetilde{\varphi}_a(g)$ for all $1 \le a < p^n$. The elements $f^{\langle p^i \rangle}$ (respectively $g^{\langle p^i \rangle}$) with $0 \le i < n$ lie in $\mathfrak{m}$ and generate the Lagrangian subalgebra $\mathfrak{z}(f)$ (respectively $\mathfrak{z}(g)$). It follows that there exists an isomorphism of associative algebras $\tau : \mathfrak{z}(f) \to \mathfrak{z}(g)$ such that $f^{\langle p^i \rangle} \mapsto g^{\langle p^i \rangle}$ for each $0 \le i < n$. We have $\tau(f^{\langle a \rangle}) = g^{\langle a \rangle}$ for all $a < p^n$. Put

$$V = \{h \in \mathfrak{z}(f) \mid \tau(h^{\langle p \rangle}) = (\tau h)^{\langle p \rangle}\}.$$

The assignment $h \mapsto h^{[p]}$ is a p-semilinear map on every Lagrangian subalgebra. The same is true then for the map $h \mapsto h^{\langle p \rangle}$. Hence V is a subspace of $\mathfrak{z}(f)$. If $h = f^{\langle p^i \rangle}$ where $i < n$ then $h^{\langle p \rangle} = f^{\langle p^{i+1} \rangle}$ and $\tau(h)^{\langle p \rangle} = g^{\langle p^{i+1} \rangle}$. Hence $f^{\langle p^i \rangle} \in V$ for $i < n-1$ by the construction of τ. Next,

$$\tau(f^{\langle p^n \rangle}) = \tau\Big(-\sum_{a=1}^{p^n-1} \widetilde{\varphi}_a(f) f^{\langle p^n - a \rangle}\Big) = -\sum_{a=1}^{p^n-1} \widetilde{\varphi}_a(g) g^{\langle p^n - a \rangle} = g^{\langle p^n \rangle},$$

which shows that $f^{[p^{n-1}]} \in V$ too. If $h \in \big(\mathfrak{m} \cap \mathfrak{z}(f)\big)^2$ then $h^{\langle p \rangle} = 0$ and $\tau(h)^{\langle p \rangle} = 0$ by lemma 1.2. Finally, $1 \in V$ since $1^{\langle p \rangle} = 0$. Thus $V = \mathfrak{z}(f)$. As $h^{[p]} = h^{\langle p \rangle} + \kappa_1(h)$, we get $\tau(h^{[p]}) \equiv (\tau h)^{[p]} \pmod k$ for all $h \in \mathfrak{z}(f)$. In view of lemma 1.2 there exist Lagrangian ideals $I, I' \subset B_{2n}$ such that for $B = \mathfrak{z}(f)$ and $B' = \mathfrak{z}(g)$ we meet the hypotheses of theorem 4.3. The extension $\theta \in G$ of τ satisfies $\theta(f) = \theta\big(f^{\langle 1 \rangle} + \kappa(f)\big) = g^{\langle 1 \rangle} + \kappa(g) = g$. Thus f and g are G-conjugate.

Suppose now that $\varphi_a(f) = \varphi_a(g)$ for all $1 \le a \le p^n$ and $\kappa_i(f) = \kappa_i(g)$ for all $0 \le i < n$. According to proposition 3.5 $\widetilde{\varphi}_a$ belongs to the subalgebra generated by $\varphi_1, \ldots, \varphi_{p^n}, \kappa_0, \ldots, \kappa_{n-1}$. Hence $\widetilde{\varphi}_a(f) = \widetilde{\varphi}_a(g)$ for all $1 \le a < p^n$, and we can apply our previous construction of θ. Note that $\kappa_n(f) = \kappa_n(g)$ by (5) of proposition 3.5. Hence $\tau\big(f^{[p^i]}\big) = \tau\big(f^{\langle p^i \rangle} + \kappa_i(f)\big) = g^{\langle p^i \rangle} + \kappa_i(g) = g^{[p^i]}$ for $0 \le i \le n$. This means that the equality $\tau(h^{[p]}) = (\tau h)^{[p]}$ holds for $h = f^{[p^i]}$ with $0 \le i < n$. As it holds also for $h \in \big(\mathfrak{m} \cap \mathfrak{z}(f)\big)^2$ by lemma 1.2 and for $h = 1$ since $1^{[p]} = 0$, it is fulfilled on the whole $\mathfrak{z}(f)$. Since I and I' can be chosen closed under the $[p]$-map, we get $\theta \in G_{[p]}$ by theorem 4.3. Thus f and g are $G_{[p]}$-conjugate, which completes the proof of (1).

Consider the element $u = u_{\lambda,0} \in S$. We prove by induction on r that

$$u^{[p^r]} = \sum_{i=r+1}^{n} \Big((-1)^{i-1-r}(\lambda_i + x_i) \prod_{j=r+1}^{i-1} x_{n+j}^{p-1}\Big) \qquad \text{for all } r = 0, \ldots, n$$

(note that for $r = n$ the formula should be understood as $u^{[p^n]} = 0$). Denote by w_r the right hand side of the formula. If $r > 0$ then $w_{r-1} = f - g^{p-1} w_r$ where

$f = \lambda_r + x_r$ and $g = x_{n+r}$. Note that f, g together with $h = -w_r$ satisfy the hypotheses of lemma 5.1, and furthermore $[f,h] = [g,h] = 0$ in this case. Hence $w_{r-1}^{[p]} = w_r$, as required.

An arbitrary element $v = u_{\lambda,h} \in S$ can be written as

$$v = u + (-1)^{n-1} h \prod_{j=1}^{n} x_{n+j}^{p-1} \qquad \text{where } h \in k[x_1, \ldots, x_n].$$

Put $I = x_{n+1}B_{2n} + \ldots + x_{2n}B_{2n}$. From the computations above we see at once that $u^{[p^{r-1}]} \equiv \lambda_r + x_r \pmod{I}$ for each $r = 1, \ldots, n$. In particular, $u^{[p^{r-1}]} - \lambda_r \in \mathfrak{m}$. Denote by

$$h^u = h(u - \lambda_1, u^{[p]} - \lambda_2, \ldots, u^{[p^{n-1}]} - \lambda_n) \in k[u, u^{[p]}, \ldots, u^{[p^{n-1}]}]$$

the image of h under the algebra homomorphism $k[x_1, \ldots, x_n] \to B_{2n}$ such that $x_i \mapsto u^{[p^{i-1}]} - \lambda_i$ for all $i = 1, \ldots, n$. We claim that

$$v^{[p^r]} = u^{[p^r]} + (-1)^{n-1-r} h^u \prod_{j=r+1}^{n} x_{n+j}^{p-1} \qquad \text{for all } r = 0, \ldots, n-1.$$

When $r = 0$, the formula follows from the fact that $h^u \equiv h \pmod{I}$. Suppose that the formula is valid for $r = s-1$ where $0 < s < n$. Thus

$$v^{[p^{s-1}]} = u^{[p^{s-1}]} + x_{n+s}^{p-1} h' \qquad \text{where } h' = (-1)^{n-s} h^u \prod_{j=s+1}^{n} x_{n+j}^{p-1}.$$

Apply lemma 5.1 with $f = u^{[p^{s-1}]}$, $g = x_{n+s}$ and h' in place of h. By our previous calculations $f = \lambda_s + x_s + g^{p-1}w$ where w lies in the associative subalgebra of B_{2n} generated by the elements x_i, x_{n+i} with $i > s$. It follows $[f,g] = [x_s, x_{n+s}] = 1$ and $[f, x_{n+j}] = g^{p-1}[w, x_{n+j}]$ for $j > s$. As $[f, h^u] = 0$, we get $[f, h'] \in g^{p-1}B_{2n}$. Thus the hypotheses of the lemma are fulfilled, and so

$$v^{[p^s]} = u^{[p^s]} - h' + h' x_{n+s}^{p-1}[x_{n+s}, h']. \tag{$*$}$$

Observe that $h' \in x_{2n}^{p-1}B_{2n}$, whence $[x_{n+s}, h'] \in x_{2n}^{p-1}B_{2n}$, and $h'[x_{n+s}, h'] = 0$. It follows $v^{[p^s]} = u^{[p^s]} - h'$, which is the required formula for $v^{[p^r]}$ with $r = s$.

For $s = n$ we can repeat the arguments above until the formula $(*)$ is reached. In this case $h' = h^u$. Since $u^{[p^n]} = 0$, we deduce $v^{[p^n]} \equiv -h^u \equiv -h \pmod{I}$.

We have $v^{[p^{r-1}]} \equiv u^{[p^{r-1}]} \equiv \lambda_r + x_r \pmod{I}$ for each $r = 1, \ldots, n$. In particular, $v, v^{[p]}, \ldots, v^{[p^{n-1}]}$ are linearly independent modulo $k + \mathfrak{m}^2$, and so $v \in U$. By proposition 2.2 $\mathfrak{z}(v)$ coincides with the associative subalgebra of B_{2n} generated by $v, v^{[p]}, \ldots, v^{[p^{n-1}]}$. Let $\pi : B_{2n} \to k[x_1, \ldots, x_n]$ be the retraction with kernel I. It is clear that π maps $\mathfrak{z}(v)$ isomorphically onto $k[x_1, \ldots, x_n]$. Denote by

$$h^v = h(v - \lambda_1, v^{[p]} - \lambda_2, \ldots, v^{[p^{n-1}]} - \lambda_n) \in \mathfrak{z}(v)$$

the image of h under the algebra homomorphism $k[x_1,\dots,x_n]\to B_{2n}$ such that $x_i\mapsto v^{[p^{i-1}]}-\lambda_i$ for all $i=1,\dots,n$. Then $\pi(h^v)=h$. As $v^{[p^n]}\in\mathfrak{z}(v)$ and $\pi(v^{[p^n]})=-h$, we conclude that $v^{[p^n]}+h^v=0$.

By the above calculations $\kappa_{i-1}(v)=\lambda_i$ for $i=1,\dots,n$ and $\varphi_a(v)$ is equal to the coefficient of $v^{[p^n-a]}$ in the expansion of h^v for $a=1,\dots,p^n$. Given $(\mu_1,\dots,\mu_n)\in\mathbb{A}^n$ and $(\nu_1,\dots,\nu_{p^n})\in\mathbb{A}^{p^n}$, there exists a unique $v\in S$ such that $\kappa_{i-1}(v)=\mu_i$ for all $i=1,\dots,n$ and $\varphi_a(v)=\nu_a$ for all $a=1,\dots,p^n$. In fact we must take $\mu_i=\lambda_i$ and $h=\sum_{a+b=p^n,a>0}\nu_a\prod_{i=1}^n(x_i+\lambda_i)^{b_i}$ (recall that we denote by b_i the p-adic coefficients of b). Thus φ is bijective, and the inverse map $\mathbb{A}^{p^n+n}\to S$ is a morphism of algebraic varieties.

We have $v^{\langle p^{i-1}\rangle}=v^{[p^{i-1}]}-\lambda_i$ for $i=1,\dots,n$. If $h\in\mathfrak{m}$, then $h^v\in\mathfrak{m}$, and it follows that $v^{\langle p^n\rangle}=v^{[p^n]}$, so that $v^{\langle p^n\rangle}+h^v=0$. Hence $\widetilde{\varphi}_a(v)$ is the coefficient of $v^{\langle p^n-a\rangle}$ in the expansion of h^v as a linear combination of $v^{\langle b\rangle}$ with $0<b<p^n$. We conclude as before that $\widetilde{\varphi}$ is an isomorphism. The proof of (2) is complete.

We have checked already that $S\subset U$. The remainder of (3) is immediate from (1) and (2). Let $k[U]$ be the algebra of regular functions on U. The restriction homomorphisms $k[U]^G\to k[S_0]$ and $k[U]^{G_{[p]}}\to k[S]$ are injective by (3) and surjective by (2). Since $B_{2n}\smallsetminus U$ has codimension at least 2 in B_{2n}, there is an equality $k[B_{2n}]=k[U]$. That gives (4). $\square$

Remark. If N denotes the null fiber of the morphism $B_{2n}\to\mathbb{A}^{p^n+n}$ (respectively $B_{2n}\to\mathbb{A}^{p^n}$) given by invariant functions of theorem 5.2, then it can be shown that the codimension of $N\cap\mathfrak{m}^3$ in B_{2n} is less than p^n+n (respectively p^n) provided that either p or n is big enough. This means that $k[B_{2n}]$ is a free module neither over $k[B_{2n}]^{G_{[p]}}$ nor over $k[B_{2n}]^G$.

Corollary 5.3. *If $y=x_1^{p-1}\cdots x_{2n}^{p-1}$ then $\varphi_1(y)=(-1)^{n-1}$ and $\varphi_a(y)=0$ for $a>1$.*

Proof. Let $v=u_{0,\,th}\in S$ where $t\in k$ and $h=x_1^{p-1}\cdots x_n^{p-1}$. Then $v=u+(-1)^{n-1}ty$ where $u=u_{0,0}$. By calculations in the proof of the theorem $\varphi_a(v)$ is equal to the coefficient of $v^{[p^n-a]}$ in the expansion of $th^v=t\prod_{i=0}^{n-1}\big(v^{[p^i]}\big)^{p-1}=tv^{[p^n-1]}$. Hence $\varphi_1(v)=t$ and $\varphi_a(v)=0$ for $a>1$. As φ_a is homogeneous of degree a, we have $\varphi_a(v)=(-1)^{(n-1)a}t^a\varphi_a(y)$ modulo a polynomial in t of degree $<a$. Comparing the coefficients of t^a, we find $\varphi_a(y)$. $\square$

We conclude this section with a result which has a bearing on the representation theory of the Poisson algebra in view of [16], Th. 5.4. I will investigate the representations more thoroughly in a forthcoming paper.

Corollary 5.4. *Suppose that $f\in U$, and let K denote the asymptotic cone of the orbit $G_{[p]}f$. Then $K\cap U$ is nonempty.*

Proof. We may assume that $f=u_{\lambda,h}\in S$. For $0\ne t\in k$ define $\theta_t\in\operatorname{Aut}B_{2n}$ setting $\theta_t(x_i)=t^{-p^{i-1}}x_i$ and $\theta_t(x_{n+i})=t^{p^{i-1}}x_{n+i}$ for $i=1,\dots,n$. One checks readily that $\theta_t\in G_{[p]}$. We have

$$\theta_t(f)=t^{-1}u+\sum_{i=1}^n\Big((-1)^{i-1}\lambda_it^{p^{i-1}-1}\prod_{j=1}^{i-1}x_{n+j}^{p-1}\Big)+(-1)^{n-1}t^{p^n-1}\theta_t(h)\prod_{j=1}^n x_{n+j}^{p-1}$$

where $u = u_{0,0} = \sum_{i=1}^{n} (-1)^{i-1} x_i \prod_{j=1}^{i-1} x_{n+j}^{p-1}$. Since $h \in k[x_1, \ldots, x_n]$, the map $t \mapsto \theta_t(h)$ is polynomial in t^{-1} of degree $< p^n$. Hence $\theta_t(f) = t^{-1}u + \psi(t)$ where $\psi(t)$ is a polynomial map in t.

Let $Z \subset B_{2n} \oplus k$ be the closure of the set of elements (tg, t) with $t \in k \setminus \{0\}$ and $g \in G_{[p]}f$. Denote by $\eta : Z \to k$ the restriction of the projection $B_{2n} \oplus k \to k$ onto the second summand. Then $K = \eta^{-1}(0)$ by [6], Ch. II, 4.2. We have $(u + t\psi(t), t) = (t\theta_t(f), t) \in Z$ for $t \neq 0$, whence $(u, 0) \in Z$ as well. It follows $u \in K$, and it remains to notice that $u \in S \subset U$. $\square$

6. Semisimple and nilpotent elements

Denote by $\mathcal{Z}_s$ the closure of the set of $[p]$-semisimple elements and by $\mathcal{N}$ the closed set of $[p]$-nilpotent elements in B_{2n}.

Lemma 6.1. (1) *$\varphi_a(f^{[p]}) = \widetilde{\varphi}_a(f^{[p]}) = \widetilde{\varphi}_a(f)^p$ if $a = p^n - p^i$, $i = 0, \ldots, n$, and $\varphi_a(f^{[p]}) = \widetilde{\varphi}_a(f^{[p]}) = 0$ otherwise.*

(2) *$f^{[p^{n+1}]}$ is $[p]$-semisimple for any $f \in B_{2n}$.*

Proof. If $c \neq 0$ and $c \neq p^i$ for $i = 0, \ldots, n$ then $f^{\langle c \rangle} \in \mathfrak{n}^2$, where $\mathfrak{n}$ is the maximal ideal of the associative subalgebra $k[f, f^{[p]}, \ldots, f^{[p^{n-1}]}] \subset B_{2n}$. We have $\left(f^{\langle c \rangle}\right)^{[p]} = 0$ for such integers c (see lemma 1.2), and it follows

$$\sum_{i=0}^{n} \widetilde{\varphi}_{p^n - p^i}(f)^p f^{[p^{i+1}]} = \Big(\sum_{b+c=p^n} \widetilde{\varphi}_b(f) f^{\langle c \rangle} \Big)^{[p]} = 0.$$

Taking the projection onto $\mathfrak{m}$ with respect to the decomposition $B_{2n} = k \oplus \mathfrak{m}$, we get a zero linear combination of $f^{\langle p \rangle}, \ldots, f^{\langle p^{n+1} \rangle}$ with the same coefficients. If $f \in U_s$ then $f^{[p]} \in U_s$ by proposition 2.2. In this case $\varphi_a(f^{[p]})$ (respectively $\widetilde{\varphi}_a(f^{[p]})$) is the coefficient of $f^{[b]}$ (respectively $f^{\langle b \rangle}$) where $b = p^{n+1} - pa$ in the above linear combinations, which yields (1). Since U_s is open in B_{2n}, (1) holds for all f.

Let i be the smallest integer among $0, \ldots, n$ such that $\widetilde{\varphi}_{p^n - p^i}(f) \neq 0$. Then $f^{[p^{i+1}]}$ is a linear combination of elements $f^{[p^{j+1}]}$ with $i < j \leq n$, and so $f^{[p^{i+1}]}$ is $[p]$-semisimple. This proves (2). $\square$

Remark. The proof of the lemma also describes the minimal p-polynomial for the Poisson algebra, as defined in [14].

Proposition 6.2. (1) *$\mathcal{Z}_s$ is an irreducible subvariety of codimension $p^n - n$ in B_{2n}.*

(2) *$\mathcal{Z}_s \cap U = \{ f \in U \mid \varphi_a(f) = 0$ for all $1 \leq a \leq p^n,\ a \neq p^n - p^i \}$.*

(3) *$\mathcal{Z}_s \cap U$ contains only nonsingular points of $\mathcal{Z}_s$.*

(4) *$f^{[p]} \in \mathcal{Z}_s$ for all $f \in B_{2n}$.*

Proof. Consider the morphism $q : B_{2n} \to B_{2n},\ f \mapsto f^{[p^r]}$, where $r > n$. Its image coincides with the set of $[p]$-semisimple elements in B_{2n}. As $q(B_{2n})$ is irreducible, so is its closure $\mathcal{Z}_s$ too. Let $f \in U_s$ and $g \in q^{-1}\big(q(f)\big)$. Then $g^{[p^r]} = f^{[p^r]} = f_s^{[p^r]}$, and so $g \in \mathfrak{z}(f_s^{[p^r]}) = \mathfrak{z}(f_s)$. By proposition 2.2 $\mathfrak{z}(f_s)$ is a Lagrangian subalgebra of B_{2n}. If $T \subset B_{2n}$ denotes the torus generated by the semisimple element f_s, then $\dim T = n$ and $\mathfrak{z}(f_s) = k + T + \mathfrak{n}^2$ where $\mathfrak{n} = \mathfrak{m} \cap \mathfrak{z}(f_s)$. By lemma 1.2 the $[p]$-map on $k + \mathfrak{n}^2$ is zero. Now $g_s \in T$. As $g_s^{[p^r]} = g^{[p^r]} = f_s^{[p^r]}$, we get $g_s = f_s$. It follows

$q^{-1}\big(q(f)\big) = f_s + k + \mathfrak{n}^2$. In particular, $\dim q^{-1}\big(q(f)\big) = p^n - n$. Since U_s is an open subset of B_{2n}, we get (1). Furthermore, (4) holds for $f \in U_s$ since $f^{[p]}$ is semisimple in this case. Then (4) is fulfilled everywhere.

Denote by Z the zero set of $p^n - n$ functions φ_a with $1 \le a \le p^n$, $a \ne p^n - p^i$. All semisimple elements are contained in Z by lemma 6.1. Hence $\mathcal{Z}_s \subset Z$. All irreducible components of Z have codimension $\le p^n - n$ in B_{2n}. If $f \in U \cap Z$ then f is a nonsingular point of Z and the irreducible component of Z containing f has codimension $p^n - n$ by lemma 3.3. Put $Z' = \{f \in Z \mid \varphi_{p^n-1}(f) = 0\}$. All irreducible components of $Z' \cap U$ have, similarly, codimension $p^n - n + 1$. Hence every irreducible component of $Z \cap U$ contains a point outside of Z'. If $f \in Z$ then $\widetilde{\varphi}_{p^n-1}(f) = \varphi_{p^n-1}(f)$ by (3) of proposition 3.5 since $\binom{p^n-2}{p^n-p^i-1} \equiv 0 \pmod p$ for $0 < i < n$. If $f \in Z \smallsetminus Z'$ then $\widetilde{\varphi}_{p^n-1}(f) \ne 0$, and (1) of proposition 3.5 shows that f is a linear combination of elements $f^{[p^i]}$ with $1 \le i \le n$, so that f is semisimple. Thus $Z \smallsetminus Z' \subset \mathcal{Z}_s$, and we conclude $Z \cap U = \mathcal{Z}_s \cap U$. $\square$

Denote by $\chi_D(t)$ the characteristic polynomial of $D \in W_{2n}$ as a linear transformation of B_{2n}. As was proved by Premet [15],

$$\chi_D(t) = t^{p^{2n}} + \sum_{i=0}^{2n-1} \psi_i(D) t^{p^i}$$

where ψ_i is a polynomial function of degree $p^{2n} - p^i$ on W_{2n}.

Lemma 6.3. *If $f \in B_{2n}$ then $\psi_i(\mathcal{D}_f) = 0$ and $\psi_{n+i}(\mathcal{D}_f) = \widetilde{\varphi}_{p^n-p^i}(f)^{p^n}$ for all $0 \le i < n$.*

Proof. It suffices to check the equalities for $f \in U$. Under this assumption $\mathfrak{z}(f) \cong B_n$ as associative algebras. Let $\mathfrak{z}(f) = J_0 \supset J_1 \supset \ldots \supset J_{p^n} = 0$ be a chain of associative ideals such that $\dim J_{a-1}/J_a = 1$ for all $a = 1, \ldots, p^n$. Then $J_a B_{2n}$ is stable under $\mathcal{D}_f$ for each a. Since $J_1 J_{a-1} \subset J_a$ and B_{2n} is a free $\mathfrak{z}(f)$-module,

$$J_{a-1}B_{2n}/J_a B_{2n} \cong J_{a-1}/J_a \otimes_{\mathfrak{z}(f)} B_{2n} \cong J_{a-1}/J_a \otimes \overline{B} \cong \overline{B}$$

where $\overline{B} = B_{2n}/J_1 B_{2n} \cong B_n$. Denote by $D \in \operatorname{Der} \overline{B} \cong W_n$ the derivation induced by $\mathcal{D}_f$. The linear transformation induced by $\mathcal{D}_f$ in $J_{a-1}B_{2n}/J_a B_{2n}$ is equivalent to D for each a. It follows $\chi_{\mathcal{D}_f}(t) = \chi_D(t)^{p^n}$ where χ_D is the characteristic polynomial of D. By Premet's result $\chi_D(t) = t^{p^n} + \sum_{i=0}^{n-1} \lambda_i t^{p^i}$ for some $\lambda_0, \ldots, \lambda_{n-1} \in k$. We have $D^{p^n} + \sum_{i=0}^{n-1} \lambda_i D^{p^i} = 0$ by Cayley-Hamilton theorem. If $0 \le c \le p^n$ and $c \ne p^i$ for $i = 0, \ldots, n$ then $f^{\langle c \rangle} \in J_1^2$, whence $[f^{\langle c \rangle}, B_{2n}] \subset J_1 B$, so that $\mathcal{D}_{f^{\langle c \rangle}}$ induces a zero derivation of $\overline{B}$. Clearly $\mathcal{D}_{f^{\langle p^i \rangle}} = \mathcal{D}_f^{p^i}$ induces D^{p^i} on $\overline{B}$. It follows now from proposition 3.5(1) that $D^{p^n} + \sum_{i=0}^{n-1} \widetilde{\varphi}_{p^n-p^i}(f) D^{p^i} = 0$. Note that $J_1 B$ is a Lagrangian ideal of B_{2n} generated by $f^{\langle 1 \rangle}, f^{\langle p \rangle}, \ldots, f^{\langle p^{n-1} \rangle}$. Hence $D, D^p, \ldots, D^{p^{n-1}}$ are linearly independent by lemma 1.3. We can conclude that $\lambda_i = \widetilde{\varphi}_{p^n-p^i}(f)$ for each i, and the required formulas are immediate. $\square$

Theorem 6.4. (1) *$\mathcal{N}$ is an irreducible normal complete intersection of codimension n in B_{2n}.*

(2) *The ideal $I = \{\varphi \in k[B_{2n}] \mid \varphi(\mathcal{N}) = 0\}$ is generated by n functions $\widetilde{\varphi}_{p^n-p^i}$ with $i = 0, \ldots, n-1$.*

(3) $\mathcal{N} \cap U$ *contains only nonsingular points of* $\mathcal{N}$ *and* $\operatorname{codim}_{\mathcal{N}} \mathcal{N} \smallsetminus U \geq 2$.

(4) $\mathcal{N} = \{f \in B_{2n} \mid f^{[p^{n+1}]} = 0\}$.

Proof. An element $f \in B_{2n}$ is $[p]$-nilpotent if and only if $\mathcal{D}_f$ is nilpotent, if and only if $\chi_{\mathcal{D}_f}(t) = t^{p^{2n}}$, if and only if $\psi_i(\mathcal{D}_f) = 0$ for all $i = 0, \ldots, 2n-1$. In view of lemma 6.3 we get

$$\mathcal{N} = \{f \in B_{2n} \mid \widetilde{\varphi}_{p^n - p^i}(f) = 0 \text{ for all } i = 0, \ldots, n-1\}.$$

The differentials of n functions $\widetilde{\varphi}_{p^n-p^i}$ with $i = 0, \ldots, n-1$ are linearly independent at all $f \in U$ by proposition 3.5, and so the points in $\mathcal{N} \cap U$ are nonsingular. We can find a linear subspace $E \subset B_{2n}$ such that $\dim E = n + 2$ and $E \cap \mathcal{N} \subset \{0\} \cup U$. Take E to be the linear span of elements $u, v, s_1, \ldots, s_n$ where

$$u = \sum_{i=1}^{n} \Big((-1)^{i-1} x_i \prod_{j=1}^{i-1} x_{n+j}^{p-1} \Big), \qquad v = \sum_{i=1}^{n} \Big((-1)^{i-1} x_{n+i} \prod_{j=1}^{i-1} x_j^{p-1} \Big),$$

and $s_i = x_i x_{n+i}$ for $i = 1, \ldots, n$. Let $T = \{\theta_t \mid t \in k^*\} \subset G_{[p]}$ be the onedimensional torus such that $\theta_t(x_i) = t^{p^{i-1}} x_i$ and $\theta_t(x_{n+i}) = t^{-p^{i-1}} x_{n+i}$ for $i = 1, \ldots, n$. Then B_{2n} decomposes as a direct sum of weight spaces $V_m = \{f \in B_{2n} \mid \theta_t(f) = t^m f\}$, $m \in \mathbb{Z}$, with respect to T. We have $f^{[p]} \in V_{pm}$ for all $f \in V_m$. Note that $u \in V_1$, $v \in V_{-1}$ and $s_i \in V_0$. Write $f \in E$ as $\lambda u + s + \mu v$ where $\lambda, \mu \in k$ and s is a linear combination of $s_1, \ldots, s_n$. Using Jacobson's formula, we deduce

$$f^{[p^r]} \equiv \lambda^{p^r} u^{[p^r]} + \mu^{p^r} v^{[p^r]} \pmod{\sum_{a=1-p^r}^{p^r-1} V_a}$$

for all $r \geq 0$. Note that $\mathfrak{m}$ and $\mathfrak{m}^2$ are stable under T, and the weights of T on $\mathfrak{m}/\mathfrak{m}^2$ are $p^{\pm i}$ with $i = 0, \ldots, n-1$. Hence $V_m \subset k + \mathfrak{m}^2$ for all other m. As we have seen in the proof of theorem 5.2, $u^{[p^r]} \equiv x_{r+1} \pmod{\mathfrak{m}^2}$ for $r = 0, \ldots, n-1$. Now $v = \tau(u)$ where $\tau \in G_{[p]}$ sends x_i to x_{n+i} and x_{n+i} to $-x_i$ for $i = 1, \ldots, n$. It follows that $v^{[p^r]} = \tau(u^{[p^r]}) \equiv x_{n+r+1} \pmod{\mathfrak{m}^2}$, and

$$f^{[p^r]} \equiv \lambda^{p^r} x_{r+1} + \mu^{p^r} x_{n+r+1} \pmod{k + \mathfrak{m}^2}.$$

If either $\lambda \neq 0$ or $\mu \neq 0$ then $f, f^{[p]}, \ldots, f^{[p^{n-1}]}$ are linearly independent modulo $k+\mathfrak{m}^2$, i.e., $f \in U$. If $\lambda = \mu = 0$ then $f = s$ is $[p]$-semisimple. Thus $E \cap \mathcal{N} \subset \{0\} \cup U$, as required. Now (1) and (2) follow from lemma 1.5. If $f \in \mathcal{N}$ then $f^{[p^{n+1}]}$ is $[p]$-nilpotent. As the latter element is $[p]$-semisimple by lemma 6.1, it has to be zero. □

7. Central elements in the universal enveloping algebra

Let $U(B_{2n})$ be the universal enveloping algebra of the Lie algebra structure on B_{2n}. It has a canonical increasing filtration $U_m(B_{2n})$, $m \geq 0$, such that $\operatorname{gr} U(B_{2n}) \cong S(B_{2n})$, the symmetric algebra of B_{2n}. Endow the center Z of $U(B_{2n})$ with the induced filtration. Then $\operatorname{gr} Z \subset S(B_{2n})^L$, the subalgebra of L-invariants in $S(B_{2n})$. The nondegenerate invariant bilinear form on B_{2n} (see corollary 3.6) yields an isomorphism of L- and G-modules $B_{2n} \cong B_{2n}^*$. Hence an L- and G-equivariant isomorphism of algebras $S(B_{2n}) \cong S(B_{2n}^*) \cong k[B_{2n}]$. Denote by $\varphi_a^\vee, \kappa_i^\vee \in S(B_{2n})$ the images of $\varphi_a, \kappa_i \in k[B_{2n}]$ under this isomorphism (see section 3). Thus each $\varphi_a^\vee$ is L- and $G_{[p]}$-invariant, and each $\kappa_i^\vee$ is L_0- and $G_{[p]}$-invariant. We are going to prove that $\varphi_a^\vee \in \operatorname{gr} Z$ whenever $a \not\equiv 0 \pmod p$, $0 < a < p^n$.

For $a \geq 0$ define $\xi_a : B_{2n} \to k[B_{2n}]$ by the formula $\xi_a(g)(f) = \varphi_1(f^{[a]}g)$ for $f, g \in B_{2n}$. Then ξ_a is a homomorphism of L-modules and $G_{[p]}$-modules. In fact

$$\operatorname{Hom}(B_{2n}, k[B_{2n}]) \cong k[B_{2n}] \otimes B_{2n}^* \cong k[B_{2n}] \otimes B_{2n} \cong \operatorname{Pol}(B_{2n}, B_{2n})$$

as L-modules and $G_{[p]}$-modules. Under this isomorphism ξ_a corresponds to the L- and $G_{[p]}$-invariant polynomial map $B_{2n} \to B_{2n}$ given by $f \mapsto f^{[a]}$.

Denote by $\xi_a^\vee : B_{2n} \to S(B_{2n})$ the composite of ξ_a and the invariant isomorphism $k[B_{2n}] \cong S(B_{2n})$ considered earlier, and put $y = x_1^{p-1} \cdots x_{2n}^{p-1}$.

Lemma 7.1. (1) $\xi_a(y) = (-1)^{n-1} \prod_{i \geq 0} \kappa_i^{a_i}$ *and* $\xi_a^\vee(y) = (-1)^{n-1} \prod_{i \geq 0} (\kappa_i^\vee)^{a_i}$.

(2) $\xi_a^\vee(y) \in S(\mathfrak{m}^{(2n-j)(p-1)})$ *when* $a < p^{j+1}$, $0 \leq j \leq 2n$.

Proof. (1) Since $\mathfrak{m}y = 0$ and $\varphi_1(y) = (-1)^{n-1}$ by corollary 5.3, we have

$$\varphi_1(f^{[a]}y) = \kappa(f^{[a]})\varphi_1(y) = (-1)^{n-1} \prod_{i \geq 0} \kappa_i(f)^{a_i},$$

which gives the first equality. Take the images in $S(B_{2n})$ to get the second one.

(2) For $r \geq 2$ we have $\mathfrak{m}^r = \{g \in \mathfrak{m}^2 \mid [g, \mathfrak{m}] \subset \mathfrak{m}^{r-1}\}$. In fact, if $g \notin \mathfrak{m}^r$ then $[g, x_i] \notin \mathfrak{m}^{r-1}$ for some $i = 1, \ldots, 2n$. If now $g \in \mathfrak{m}^r$ then $g^{[p]} \in \mathfrak{m}^2$ and $[g^{[p]}, \mathfrak{m}] \subset \mathcal{D}_g^{p-1}(\mathfrak{m}^{r-1}) \subset \mathfrak{m}^{r-1}$. Hence $\mathfrak{m}^r$ is closed under the $[p]$-map. Using Jacobson's formula, we find that $(f+g)^{[p]} \equiv f^{[p]} \pmod{\mathfrak{m}^{r-p+1}}$ whenever $g \in \mathfrak{m}^r$ and $r \geq p$. Iterating yields $(f+g)^{[p^i]} \equiv f^{[p^i]} \pmod{\mathfrak{m}^{r-i(p-1)}}$ whenever $g \in \mathfrak{m}^r$ and $r > i(p-1)$. Thus

$$\kappa_i(f+g) = \kappa((f+g)^{[p^i]}) = \kappa(f^{[p^i]}) = \kappa_i(f) \qquad \text{when } g \in \mathfrak{m}^{i(p-1)+1},$$

and so we may regard κ_i as a polynomial function on $B_{2n}/\mathfrak{m}^{i(p-1)+1}$. For each $0 \leq s \leq 2n(p-1)$ the orthogonal complement of $\mathfrak{m}^s$ with respect to the invariant bilinear form on B_{2n} coincides with $\mathfrak{m}^{2n(p-1)-s+1}$. This is clear since φ_1 vanishes on all the monomials in $x_1, \ldots, x_{2n}$ of degree less than $2n(p-1)$. Hence the isomorphism $B_{2n} \to B_{2n}^*$ maps $\mathfrak{m}^{(2n-i)(p-1)}$ onto the subspace of linear functions vanishing on $\mathfrak{m}^{i(p-1)+1}$. It follows $\kappa_i^\vee \in S(\mathfrak{m}^{(2n-i)(p-1)})$, and it remains to apply (1). $\square$

Theorem 7.2. *Let $Z^{G_{[p]}} \subset Z$ be the subalgebra of $G_{[p]}$-invariant elements. Then $\varphi_a^\vee \in \operatorname{gr} Z^{G_{[p]}}$ whenever $a \not\equiv 0 \pmod p$, $0 < a < p^n$.*

Proof. Let $u(L)$ and $u(L_0)$ be the restricted universal enveloping algebras of L and L_0, respectively. Clearly $ky = \mathfrak{m}^{2n(p-1)}$ is an L_0- and a G-submodule of B_{2n}. Consider the induced L-module $\operatorname{Ind} ky = u(L) \otimes_{u(L_0)} ky$. As G operates on L by automorphisms and L_0 is stable under G, there is a canonical action of G on $\operatorname{Ind} ky$. The embedding $ky \to B_{2n}$ extends to a homomorphism of L- and G-modules $\operatorname{Ind} ky \to B_{2n}$. As $L = L_0 + k\partial_1 + \ldots + k\partial_{2n}$, the elements $\partial_1^{r_1} \cdots \partial_{2n}^{r_{2n}} \otimes y$ with

$0 \le r_i < p$ constitute a basis for $\operatorname{Ind} ky$. Furthermore, the elements $\partial_1^{r_1} \cdots \partial_{2n}^{r_{2n}}(y)$ give all possible monomials in $x_1, \ldots, x_{2n}$. In other words, $\operatorname{Ind} ky \cong B_{2n}$.

Put $I = \mathfrak{m}^{(n+1)(p-1)}$. Then $[I,I] \subset \mathfrak{m}^{2(n+1)(p-1)-2} \subset \mathfrak{m}^{2n(p-1)}$. Since $[B_{2n}, B_{2n}]$ has zero intersection with $\mathfrak{m}^{2n(p-1)}$, we see that I is an abelian Lie subalgebra of B_{2n}. Hence there is a canonical isomorphism $U(I) \cong S(I)$ between the universal enveloping and the symmetric algebras of I. Suppose that $a < p^n$, so that $\xi_a^\vee(y)$ lies in $S(I)$ by lemma 7.1. The embedding $\xi_a^\vee : ky \to S^a(I) \hookrightarrow U_a(B_{2n})$ of L_0- and $G_{[p]}$-modules extends then to a homomorphism $B_{2n} \cong \operatorname{Ind} ky \to U_a(B_{2n})$ of L- and $G_{[p]}$-modules. Denote by z_a the image of $1 \in B_{2n}$ under this homomorphism. Clearly z_a is L- and $G_{[p]}$-invariant. In particular $z_a \in Z$. Now the composite $B_{2n} \to U_a(B_{2n}) \to S^a(B_{2n})$ is a homomorphism of L-modules extending the same embedding $ky \to S^a(B_{2n})$. It follows that this composite coincides with $\xi_a^\vee$, and so the image of z_a in $S^a(B_{2n})$ equals $\xi_a^\vee(1)$. If $a \not\equiv 0 \pmod p$ then $\xi_a(1) = a^{-1}\varphi_a$ by proposition 3.2 and the definition of ξ_a, whence $\xi_a^\vee(1) = a^{-1}\varphi_a^\vee$. $\square$

Remark. We thus have the formula $z_a = \partial_1^{p-1} \cdots \partial_{2n}^{p-1} \cdot \xi_a^\vee(y)$, computed in $U(B_{2n})$, for central elements in $U(B_{2n})$. If $a < p$ then $\xi_a^\vee(y) = (\kappa_1^\vee)^a$ where $\kappa_1^\vee = y$ as an element of $U(B_{2n})$. Other elements are much less obvious. Koreshkov [9] constructed central elements up to degree p. He wrote them up explicitly as complicated linear combinations in a PBW basis, and it is difficult to compare his elements with our z_a. Using [18], Cor. 3.4, it is possible to prove that $\operatorname{Hom}_L(B_{2n}, S(B_{2n}))$ is a free $S(B_{2n})^L$-module with basis elements $\xi_a^\vee$ where $0 \le a < p^n$. Since $\xi_a^\vee(1) = 0$ when $p|a$, the method we used cannot give the remaining hypothetical central elements in $U(B_{2n})$.

References

1. N. Jacobson, *Restricted Lie algebras of characteristic p,* Trans. Amer. Math. Soc. **50** (1941) 15–25.
2. N. Jacobson, *Lie Algebras*, Interscience Tracts in Pure and Appl. Math., Vol. 10, Interscience, New York, 1962.
3. E.M. Friedlander and B.J. Parshall, *Rational actions associated to the adjoint representation,* Ann. Sci. École Norm. Sup. **20** (1987) 215–226.
4. V.G. Kac, *Description of filtered Lie algebras with which graded Lie algebras of Cartan type are associated,* Izv. Akad. Nauk SSSR Ser. Mat. **38** (1974) 800–838 [In Russian]. Translation in Math. USSR Izv. **8** (1974) 801–835.
5. V. Kac and B. Weisfeiler, *Coadjoint action of a simple algebraic group and the center of the enveloping algebra in characteristic p,* Indag. Math. **38** (1976) 136–151.
6. H. Kraft, *Geometrische Methoden in der Invariantentheorie*, Vieweg, Braunschweig, 1984.
7. Ya.S. Krylyuk, *On the maximal dimension of irreducible representations of simple p-algebras of Cartan series S and H,* Mat. Sbornik **123** (1984) 108–119 [In Russian]. Translation in Math. USSR Sbornik **51** (1985) 107–118.
8. Ya.S. Krylyuk, *On the index of Cartan type Lie algebras in finite characteristic,* Izv. Akad. Nauk SSSR Ser. Mat. **50** (1986) 393–412 [In Russian]. Translation in Math. USSR Izv. **28** (1987) 381–399.
9. N.A. Koreshkov, *On the center of the universal enveloping algebra of the hamiltonian Lie algebra H_n,* manuscript, deposited at VINITI no. 3392 (1989) [In Russian]
10. B. Kostant, *Lie group representations on polynomial rings,* Amer. J. Math. **85** (1963) 327–404.

11. A.I. Kostrikin and I.R. Shafarevich, *Graded Lie algebras of finite characteristic,* Izv. Akad. Nauk SSSR Ser. Mat. **33** (1969) 251–322 [In Russian]. Translation in Math. USSR Izv. **3** (1969) 237–304.
12. M.I. Kuznetsov and S.A. Kirillov, *Hamiltonian differential forms over an algebra of truncated polynomials,* Uspekhi Mat. Nauk **41** no. 2 (1986) 197–198 [In Russian]. Translation in Russ. Math. Surv. **41** no. 2 (1986) 205–206.
13. H. Matsumura, *Commutative Algebra, Second Edition*, Benjamin, New York, 1980.
14. A.A. Premet, *Regular Cartan subalgebras and nilpotent elements in restricted Lie algebras,* Mat. Sbornik **180** (1989) 542–557 [In Russian]. Translation in Math. USSR Sbornik **66** (1990) 555–570.
15. A.A. Premet, *The theorem on restriction of invariants and nilpotent elements in* W_n, Mat. Sbornik **182** (1991) 746–773 [In Russian]. Translation in Math. USSR Sbornik **73** (1992) 135–159.
16. A. Premet and S. Skryabin, *Representations of restricted Lie algebras and families of associative* $\mathcal{L}$*-algebras,* J. Reine Angew. Math. **507** (1999) 189–218.
17. S. Skryabin, *Modular Lie algebras of Cartan type over algebraically non-closed fields. II,* Comm. Algebra **23** (1995) 1403–1453.
18. S. Skryabin, *Invariants of finite group schemes,* electronic version math.AG/0107019.
19. H. Strade and R. Farnsteiner, *Modular Lie Algebras and their Representations*, Marcel Dekker Textbooks and Monographs, Vol. 116, Marcel Dekker, New York, 1988.
20. H. Strade, *The classification of the Simple Lie Algebras over Fields with positive characteristic*, Hamburger Beiträge zur Mathematik, Heft 31, Hamburg, 1997.
21. F.D. Veldkamp, *The center of the universal enveloping algebra of a Lie algebra in characteristic p,* Ann. Sci. École Norm. Sup. **5** (1972) 217–240.
22. R.L. Wilson, *Automorphisms of graded Lie algebras of Cartan type,* Comm. Algebra **3** (1975) 591–613.
23. R.L. Wilson, *A structural characterization of the simple Lie algebras of generalized Cartan type over fields of prime characteristic,* J. Algebra **40** (1976) 418–465.
24. D.J. Winter, *On the toral structure of Lie p-algebras,* Acta. Math. **123** (1969) 70–81.
25. H. Zassenhaus, *The representations of Lie algebras of prime characteristic,* Proc. Glasgow Math. Assoc. **2** (1954) 1–36.