ADVANCES IN MATHEMATICS 111, 195 207 (1995)

A Generalization of Rota's NBC Theorem

BRUCE E. SAGAN

Department of Mathematics, Michigan State University, East Lansing, Michigan 48824-1027

We generalize Rota's theorem characterizing the Möbius function of a geometric lattice in terms of subsets of atoms containing no broken circuit and give applications to the weak Bruhat order of a finite Coxeter group and the Tamari lattices. We also give a direct proof of the fact that in the geometric case any total order of the atoms can be used. Simple involutions are used in both proofs. Finally, we show how involutions can be used in similar situations, specifically in a special case of Rota's Crosscut Theorem as well as in related proofs of Walker on Hall's Theorem and Reiner on characteristic and Poincaré polynomials.

1. ROTA'S THEOREM AND ITS GENERALIZATION

One of the most beautiful and useful theorems in algebraic combinatorics is Rota's theorem [12] characterizing the Möbius function of a geometric lattice in terms of subsets of atoms which are NBC, i.e., contain no broken circuit. In this note we will generalize Rota's theorem to any lattice satisfying a simple condition and give applications to the weak Bruhat order of a Coxeter group and the Tamari lattices. The proof of Rota's theorem is an easy application of the simplest version of the Involution Principle of Garsia and Milne [5]. We also use an involution to show directly that in the geometric case the number of NBC sets is the same for any total ordering of the atoms. Finally we discuss a related proof for a special case of Rota's Crosscut Theorem as well as proofs of Walker concerning the Möbius function as a reduced Euler characteristic and of Reiner connecting characteristic and Poincaré polynomials.

We first review Rota's original theorem. Let L be a finite poset with minimal element $\hat{0}$. The *Möbius function* of L is the function $\mu: L \to \mathbf{Z}$ ($\mathbf{Z}$ being the integers) which is uniquely defined by

$$\sum_{y \leq x} \mu(y) = \delta_{\hat{0}x}, \tag{1}$$

where the right side is the Kronecker delta. In particular, if L is the lattice of divisors of an integer than μ is the number-theoretic Möbius function.

0001-8708/95 $9.00

Suppose that L is a lattice and let $\wedge$ and $\vee$ denote the meet (greatest lower bound) and join (least upper bound) operations, respectively. Let $\mathscr{A}(L)$ be the set of *atoms* of L, i.e., all $a \neq \hat{0}$ such that there is no $x \in L$ with $\hat{0} < x < a$. We say that L is atomic if every $x \in L$ is a join of atoms.

Assume further that L is *ranked* with rank function ρ, which means that for all $x \in L$ the quantity

$$\rho(x) = \text{length of a maximal } \hat{0} \text{ to } x \text{ chain}$$

is well defined (independent of the chain). Such a lattice is *semimodular* if

$$\rho(x \wedge y) + \rho(x \vee y) \leqslant \rho(x) + \rho(y)$$

for all $x, y \in L$. It is easy to prove, using this inequality and induction, that if $B \subseteq \mathscr{A}(L)$ then $\rho(\bigvee B) \leqslant |B|$ where the vertical bars denote cardinality. So define B to be *independent* if $\rho(\bigvee B) = |B|$ and *dependent* otherwise. If B is independent then we say it is a *base* for $x = \bigvee B$. If C is a minimal (with respect to inclusion) dependent set then we say that C is a *circuit*. Now put a total order on $\mathscr{A}(L)$ which we will denote $\trianglelefteq$ to distinguish it from the partial order $\leq$ in L. A circuit C has corresponding *broken circuit* $\bar{C} = C \backslash c$ where c is the smallest atom in C. Finally, $B \subseteq \mathscr{A}(L)$ is NBC if it contains no broken circuit. Note that such a set must be independent. Rota's theorem can now be stated.

THEOREM 1.1 (Rota). *Let L be a geometric (i.e., atomic and semimodular) lattice. Then for any total ordering of $\mathscr{A}(L)$ we have*

$$\mu(x) = (-1)^{\rho(x)} (\textit{number of NBC bases of } x). \tag{2}$$

To generalize this result to lattices, we first need to redefine some terms since L may no longer be ranked. Call $B \subseteq \mathscr{A}(L)$ *independent* if $\bigvee \bar{B} < \bigvee B$ for any proper subset $\bar{B}$ of B. Thus if C is dependent then $\bigvee \bar{C} = \bigvee C$ for some $\bar{C} \subset C$. Note that it follows directly from the definitions that a superset of a dependent set is dependent, or equivalently that a subset of an independent set is independent. The definitions of base, circuit and broken circuit can now be kept as before. If C is a circuit, it will be convenient to adopt the notation $\bar{C} = C \backslash c$ for the corresponding broken circuit. This done, our generalization is as follows.

THEOREM 1.2. *Let L be a finite lattice. Let $\trianglelefteq$ be any total ordering of $\mathscr{A}(L)$ such that for all broken circuits $\bar{C} = C \backslash c$ we have*

$$\bigvee \bar{C} = \bigvee C.$$

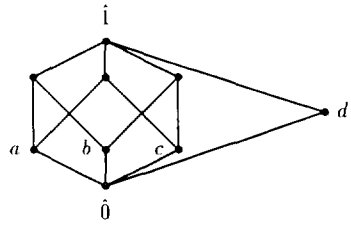

FIG. 1. An example lattice L.

Then for all $x \in L$ *we have*

$$\mu(x) = \sum_{B} (-1)^{|B|} \tag{3}$$

where the sum is over all NBC *bases* B *of* x.

Before presenting the proof, let us do an example. Consider the lattice L in Fig. 1 with the atoms ordered $a \lhd b \lhd c \lhd d$. The circuits of L are $\{a, b, d\}$, $\{a, c, d\}$ and $\{b, c, d\}$ with corresponding broken circuits $\{b, d\}$ and $\{c, d\}$. It is easy to verify that these circuits satisfy the hypothesis of Theorem 1.2. Also, the element $x = \hat{1}$ has two NBC bases, namely $\{a, d\}$ and $\{a, b, c\}$. It follows that

$$\mu(\hat{1}) = (-1)^2 + (-1)^3 = 0$$

which is readily checked from the definition of the Möbius function.

Proof (of Theorem 1.2). Let

$$\tilde{\mu}(x) = \sum_{B} (-1)^{|B|}.$$

Then since (1) uniquely defines μ, it suffices to show that $\sum_{y \leqslant x} \tilde{\mu}(y) = \delta_{\hat{0}x}$. If $x = \hat{0}$ then both sides of this equation are clearly equal to 1. So we assume that $x > \hat{0}$ and show that

$$\sum_{y \leqslant x} \tilde{\mu}(y) = 0. \tag{4}$$

Consider the set

$$\mathscr{S} = \{B: B \text{ is a base for some } y \leqslant x\}$$

with sign function

$$\varepsilon(B) = (-1)^{|B|}.$$

Clearly $\sum_{B \in \mathscr{S}} \varepsilon(B)$ is the left side of (4), so to prove this identity it suffice to find a sign-reversing involution on $\mathscr{S}$.

Let a_0 be the smallest atom under x. Define a map $\iota: \mathscr{S} \to \mathscr{S}$ by

$$\iota(B) = B \triangle a_0,$$

where $\triangle$ is the symmetric difference operator. This is clearly a sign-reversing involution as long as it is well-defined, i.e., as long as B NBC implies $\iota(B)$ NBC.

There are now two cases. If $\iota(B) = B \backslash a_0$ then $\iota(B)$ is still NBC because it is a subset of B. Otherwise let $\bar{B} := \iota(B) = B \cup a_0$ and suppose $\bar{B}$ contains broken circuit $\bar{C} = C \backslash c$. If $a_0 \notin \bar{C}$ then $\bar{C} \subseteq B$ contradicting B being NBC. If $a_0 \in \bar{C}$ then we must have

$$c \lhd a_0 \tag{5}$$

because of the way circuits are broken. But now, using the theorem's hypothesis,

$$c \leqslant \bigvee C = \bigvee \bar{C} \leqslant \bigvee \bar{B} \leqslant x.$$

Thus $c \trianglerighteq a_0$ since a_0 is the last atom under x, contradicting (5). ∎

Note that when L is geometric, then all NBC bases of a given $x \in L$ have the same number of elements, namely $\rho(x)$. Thus the right sides of (2) and (3) do really coincide in this case. Furthermore, the hypothesis of Theorem 1.2 explains why any ordering of $\mathscr{A}(L)$ works in Rota's Theorem: $\bigvee \bar{C} = \bigvee C$ for any $\bar{C}$ obtained by removing a single atom from the circuit C. On the other hand, it would be nice to have a direct proof of this fact using involutions, which we present next.

PROPOSITION 1.3. *Let L be a geometric lattice and let $\mathscr{O}_1$ and $\mathscr{O}_2$ be two total orderings of $\mathscr{A}(L)$. Then for all $x \in L$ we have*

$$\textit{number of NBC bases of } x \textit{ in } \mathscr{O}_1 = \textit{number of NBC bases of } x \textit{ in } \mathscr{O}_2. \tag{6}$$

Proof. It is enough to prove the proposition in the case where $\mathscr{O}_2$ is obtained from $\mathscr{O}_1$ by transposing the order of two atoms $c \lhd_1 d$ adjacent in $\mathscr{O}_1$. For $i = 1, 2$ let $\mathscr{BO}_i$ (respectively, $\mathscr{NBO}_i$) be the set of broken circuits (respectively, NBC bases of x) in the two orders. If C is any circuit containing both c, d and no a smaller than both then

$$\bar{C}^1 = C \backslash c \in \mathscr{BO}_1 \qquad \text{and} \qquad \bar{C}^2 = C \backslash d \in \mathscr{BO}_2. \tag{7}$$

Any other circuit gives rise to

$$\bar{C} = C \backslash a \in \mathscr{BC}_1 \cap \mathscr{BC}_2. \tag{8}$$

Now define a map $f: .1\,\mathscr{BC}_1 \backslash .1\,\mathscr{BC}_2 \to .1\,\mathscr{BC}_2 \backslash .1\,\mathscr{BC}_1$ by

$$f(B) = B \triangle \{c, d\}.$$

We must show that f is well-defined.

First note that B cannot contain any broken circuit of the form (8) since $B \in .1\,\mathscr{BC}_1$, but it must contain one of the form (7) since $B \notin .1\,\mathscr{BC}_2$. So for some circuit C we have $B \supseteq \bar{C}^2$ but $B \not\supseteq \bar{C}^1$, since $B \in .1\,\mathscr{BC}_1$. Thus we must have $c \in B$ and $d \notin B$ and so

$$f(B) = (B \backslash c) \cup d = \bar{B} \cup d, \tag{9}$$

where $\bar{B} = B \backslash c$.

We claim that $f(B) \notin .1\,\mathscr{BC}_1$. Indeed $\bar{C}^1 = (\bar{C}^2 \backslash c) \cup d$ and $\bar{C}^2 \subseteq B$. Thus Eq. (9) yields $\bar{C}^1 \subseteq f(B)$.

Now we claim that $f(B) \in .1\,\mathscr{BC}_2$. Suppose not. But $f(B)$ can not contain a broken circuit of the form (7) since $c \notin f(B)$ and $c \in \bar{C}^2$ for all C of this type. Thus $f(B)$ must contain a broken circuit of type (8), say $f(B) \supseteq \bar{D}$. However, $B \not\supseteq \bar{D}$ and so by (9) we can write

$$\bar{D} = D' \cup d,$$

where $D' \subseteq B$. Also $\bar{D} = D \backslash a$ where $a \lhd d$ (in both orders) since $d \in \bar{D}$. In fact a is smaller than every atom in C since no element of C is smaller than c, d. Write

$$D = D' \cup a \cup d \qquad \text{and} \qquad C = \bar{C}^2 \cup d,$$

where the unions are disjoint. The fact that L is geometric implies that there exists a circuit $E \subset C \cup D$ which does not contain $d \in C \cap D$. Now if $a \notin E$ then

$$E \subseteq D' \cup \bar{C}^2 \subseteq B$$

which contradicts $B \in .1\,\mathscr{BC}_1$. On the other hand, if $a \in E$ then $\bar{E} = E \backslash a$ since a is minimal in $C \cup D$. But then $\bar{E} \subseteq B$ contradicting $B \in .1\,\mathscr{BC}_1$ again. This final contradiction finishes the proof that $f(B) \in .1\,\mathscr{BC}_2$ and that f is well-defined.

Using precisely the same reasoning, one shows that f has a well-defined inverse $f^{-1}: .1\,\mathscr{BC}_2 \backslash .1\,\mathscr{BC}_1 \to .1\,\mathscr{BC}_1 \backslash .1\,\mathscr{BC}_2$ given by

$$f^{-1}(B') = B' \triangle \{c, d\} = (B' \backslash d) \cup c.$$

Thus f is a bijection and this proves the theorem. Of course, this could also be expressed in terms of an involution $\iota: \mathcal{A}\mathcal{B}\mathcal{C}_1 \triangle \mathcal{A}\mathcal{B}\mathcal{C}_2 \to \mathcal{A}\mathcal{B}\mathcal{C}_1 \triangle \mathcal{A}\mathcal{B}\mathcal{C}_2$ where $\iota(B) = B \triangle \{c, d\}$. ∎

A related result is the fact that the Tutte polynomial [13] as defined by external and internal activities is order-independent. Tutte's original proof of this fact in the paper just cited is quite involved. It would be interesting to find an easier proof using involutions.

2. Applications

We now give two examples of lattices which are not geometric, but whose Möbius functions can be computed using Theorem 1.2. We first note a general result that follows from our main theorem.

Corollary 2.1. *Let L be a finite lattice such that $\mathcal{A}(L)$ is independent. Then the Möbius values of L are all 0 or ± 1. Specifically, if $x \in L$ then*

$$\mu(x) = \begin{cases} (-1)^{|B|} & \text{if } x = \bigvee B \text{ for some } B \subseteq \mathcal{A}(L), \\ 0 & \text{else.} \end{cases}$$

Proof. If $\mathcal{A}(L)$ is independent then so is any $B \subseteq \mathcal{A}(L)$. Furthermore, there are no circuits so any such B is NBC. Finally, independence of $\mathcal{A}(L)$ implies that $\bigvee B \neq \bigvee B'$ for any $B \neq B'$. The corollary now follows from Theorem 1.2. ∎

We note that Corollary 2.1 also follows easily from a special case of Rota's Crosscut Theorem [12], proved by involutions in Section 3.

We now derive the Möbius function of the weak Bruhat order of a Coxeter group which is a result of Björner [2]. (We do not consider the strong ordering because it is not a lattice in general.) Any terminology from the theory of Coxeter groups not defined here can be found in Humphreys' book [9]. Let (W, S) be a finite Coxeter system so that W is a finite Coxeter group and S is a set of simple generators of W. The *length of* $w \in W$, $l(w)$, is the smallest l such that

$$w = s_1 s_2 \cdots s_l, \tag{10}$$

where $s_i \in S$. If $v, w \in W$ then we write $v \geqslant w$ if there is an $s \in S$ with $v = ws$ and $l(v) = l(w) + 1$. (It is easy to see that $l(v) = l(ws) = l(w) \pm 1$, cf. Lemma 3.3.) Extending this relation by transitive closure, we obtain the weak Bruhat poset P_W on W. Equivalently, this is the partial order obtained from the Cayley graph of W with respect to S by directing edges away from the identity element.

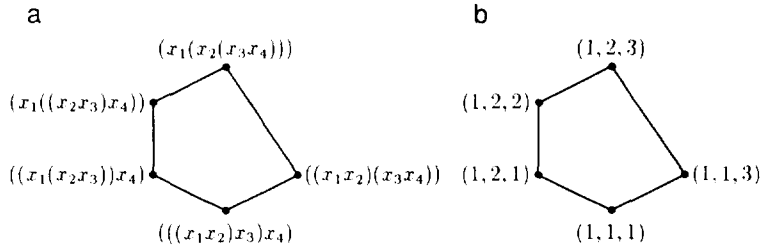

FIG. 2. The Tamari lattice T_3. (a) Parenthesized version. (b) Left bracket version.

The atoms of P_W are just the elements of S. The $\hat{1}$ of P_W is the element of maximum length, $w_0 = \bigvee S$. If $J \subset S$ is any proper subset, then these elements generate a corresponding parabolic subgroup W_J which is a proper subgroup of W. So none of the elements $w_0(J) = \bigvee J$ is equal to w_0 and so $S = \mathscr{A}(W_P)$ is independent. Thus Corollary 2.1 applies and we have proved the following result.

PROPOSITION 2.2 (Björner). *Let (W, S) be a Coxeter system and let P_W be the corresponding weak Bruhat order. Then for $w \in W$ we have*

$$\mu(w) = \begin{cases} (-1)^{|J|} & \text{if } w = w_0(J) \text{ for some } J \subseteq S, \\ 0 & \text{else.} \end{cases}$$

Björner actually derives the Möbius function from any interval $[v, w]$ in P_W. But this follows easily from the preceding proposition since there is a poset isomorphism $[v, w] \equiv [\hat{0}, v^{-1}w]$.

Next we consider the Tamari lattices [4, 6, 8]. Consider the set of all proper parenthesizations of the word $x_1x_2 \cdots x_{n+1}$. It is well known that the number of such is the Catalan number $C_n = \binom{2n}{n}/(n+1)$. Partially order this set by saying that π is covered by σ if

$$\pi = \cdots((AB)C)\cdots \qquad \text{and} \qquad \sigma = \cdots(A(BC))\cdots$$

for some subwords A, B, C. This poset is the *Tamari lattice* T_n and T_3 is illustrated in Fig. 2a.

A *left bracket vector*, $(v_1, \ldots, v_n)$, is an integer vector satisfying the conditions

1. $1 \leqslant v_i \leqslant i$ for all i and
2. if we let $S_i = \{v_i, v_i + 1, \ldots, i\}$ then for any pair S_i, S_j either one set contains the other or $S_i \cap S_j = \varnothing$.

The number of left bracket vectors with n components is also C_n. In fact given any parenthesized word π we have an associated left bracket vector

$v(\pi) = (v_1, \ldots, v_n)$ defined as follows. To calculate v_i, start at x_i in π and move to the left, counting the number of x's and the number of left parentheses you meet until these two numbers are equal. Then $v_i = j$ where x_j is the last x which is passed before the numbers balance. It is not hard to show that this gives a bijection between parenthesizations and left bracket vectors, thus inducing a partial order on the latter. This version of T_5 is shown in Fig. 2b.

We will need the following result which is proved (in a dual version) in [8].

PROPOSITION 2.3 (Huang and Tamari). *The poset T_n is a lattice. In fact, if $v(\pi) = (v_1, \ldots, v_n)$ and $v(\sigma) = (w_1, \ldots, w_n)$ then*

$$v(\pi \vee \sigma) = (\max\{v_1, w_1\}, \ldots, \max\{v_n, w_n\}).$$

We can now calculate the Möbius function of the Tamari lattice.

PROPOSITION 2.4. *Let $\pi \in T_n$ have vector $v(\pi) = (v_1, \ldots, v_n)$. Then*

$$\mu(\pi) = \begin{cases} (-1)^t & \text{if } v_i \in \{1, i\} \text{ for all } i \\ 0 & \text{else,} \end{cases}$$

where t is the number of $v_i = i \neq 1$. In particular

$$\mu(T_n) = (-1)^{n-1}.$$

Proof. Note that T_n has $n-1$ atoms $a_2, \ldots, a_n$ where $v(a_i)$ has $v_i = i$ and all other $v_j = 1$. From Proposition 2.3 we see that the atom set is independent. Thus Corollary 2.1 applies and the given formulae follow easily. ∎

3. Crosscuts, Euler Characteristics, and Characteristic Polynomials

We now present some proofs of related results using involutions. The following is a special case of Rota's Crosscut Theorem [12].

THEOREM 3.1 (Rota). *If L is a finite lattice and $x \in L$ then define*

$$a_i(x) = \text{number of sets of } i \text{ atoms whose join is } x.$$

We have

$$\mu(x) = a_0 - a_1 + a_2 - \cdots.$$

Proof. The proof follows the same lines as that of Theorem 1.2. In this case the set is

$$\mathscr{S} = \left\{ A : A \subseteq \mathscr{A}(L) \text{ and } \bigvee A \leqslant x \right\}$$

with sign function

$$\varepsilon(A) = (-1)^{|A|}.$$

Given any fixed atom $a \leqslant x$ we define the involution

$$\iota(A) = A \triangle a.$$

This is clearly well-defined and the proof follows. ∎

It would be interesting to find of a proof of the Crosscut Theorem in its full generality using involutions. The stumbling block is that to apply this method one would need to have a crosscut C such that for every $x \in L$ not covering $\hat{0}$ we have $C \cap [\hat{0}, x]$ is a crosscut of that interval. But this condition forces C to be the set of atoms.

The Möbius function of any partially ordered set L can be viewed as a reduced Euler characteristic. If $x \in L$ then a *chain of length i in the open interval* $(\hat{0}, x)$ is

$$c : x_0 < x_1 < \cdots < x_i,$$

where $\hat{0} < x_j < x$ for all j. Let

$$c_i(x) = \text{number of chains of length } i \text{ in } (\hat{0}, x).$$

Note that if $x > \hat{0}$ then $c_{-1}(x) = 1$ because of the empty chain. Walker [14, Theorem 1.6] notes that the following result, usually known as Philip Hall's Theorem [7, 12], can be proved using involutions.

THEOREM 3.2 (Hall). *If L is any partially ordered set with a $\hat{0}$ and $x \in L$, then*

$$\mu(x) = \begin{cases} 1 & \text{if } x = \hat{0} \\ -c_{-1}(x) + c_0(x) - c_1(x) + \cdots & \text{else.} \end{cases} \tag{11}$$

Proof. Again, the proof follows the lines of Theorem 1.2. Let

$$\mathscr{S} = \{\hat{0}\} \cup \{(c, y) : c \text{ is a chain in } (\hat{0}, y), \hat{0} < y \leqslant x\}$$

with sign function

$$\varepsilon(\hat{0}) = 1 \qquad \text{and} \qquad \varepsilon(c, y) = (-1)^{l(c)},$$

where $l(c)$ is the length of the chain. The involution ι is defined by

$$\hat{0} \overset{\iota}{\longleftrightarrow} (\varnothing, x)$$

and for $(c, y) \in \mathscr{L} \setminus \{\hat{0}, (\varnothing, x)\}$ let

$$\iota(c, y) = \begin{cases} (c \setminus c', c') & \text{if } y = x, \\ (c < y, x) & \text{else,} \end{cases}$$

where c' is the largest element of c, and $c < y$ is the chain formed by adjoining y to c. The fact that this is a sign-reversing involution can now be used to show that the right side of (11) satisfies the same recursion as $\mu(x)$. ∎

If a geometric lattice comes from a hyperplane arrangement, even more can be said about its Möbius function. Any terms in the following discussion which are not defined can be found in the book of Orlik and Terao [10]. Let W be a finite Euclidean reflection group acting on a vector space V. Let $\mathscr{A}_W$ be the corresponding hyperplane arrangement with intersection lattice L_W; i.e., L_W is the set of all subspaces of V that can be obtained as intersections of hyperplanes in $\mathscr{A}_W$ ordered by *reverse* inclusion.

Define the *absolute length of* $w \in W$, $\hat{l}(w)$, to be the smallest l such that w can be written as

$$w = t_1 t_2 \cdots t_l \tag{12}$$

with the t_i coming from the set of all reflections $T \subseteq W$. This differs from the definition of ordinary length given in (10) in that one is not restricted to a set S of simple reflections. An expression of the form (12) will be called *absolutely reduced*. We will need the following result about absolute length.

LEMMA 3.3. *Let W be a finite reflection group and consider $w \in W$. If $t \in W$ is any reflection then*

$$\hat{l}(wt) = \hat{l}(w) \pm 1.$$

Proof. If $w = t_1 t_2 \cdots t_k$ is an absolutely reduced expression then $wt = t_1 \cdots t_k t$ so that $\hat{l}(wt) \leqslant \hat{l}(w) + 1$. Now replacing w by wt in the last inequality yields $\hat{l}(wt) \geqslant \hat{l}(w) - 1$. Finally, we cannot have $\hat{l}(wt) = \hat{l}(w)$ since $\det(wt) = -\det(w)$ and $\det(u) = (-1)^{\hat{l}(u)}$ for any $u \in W$. ∎

For any element $w \in W$ let

$$V^w = \{v \in V : w(v) = v\}.$$

It follows from an easy-to-prove result of Carter [3] that if $V^w = X$ for some subspace $X \in L_W$ then $\hat{l}(w) = \operatorname{codim} X$. This makes the statement of the following theorem unambiguous.

THEOREM 3.4. *Let W be a finite reflection group with corresponding intersection lattice L_W. Then for any $X \in L_W$ we have*

$$\mu(X) = (-1)^{\hat{l}} (\text{number of } w \in W \text{ with } V^w = X), \tag{13}$$

where $\hat{l} = \hat{l}(w)$ of some (any) w with $V^w = X$.

Proof. This proof was discovered by Victor Reiner (personal communication) using the ideas in our proof of Theorem 1.2. I thank him for letting me reproduce it here.

If $X = \hat{0} = V$ then both sides of (13) are clearly 1. If $X > \hat{0}$ then consider the set

$$W' = \{w \in W: V^w \supseteq X\}$$

with sign function

$$\varepsilon(w) = (-1)^{\hat{l}(w)}.$$

Clearly the right side of (13) is given by $\sum_{w \in W'} \varepsilon(w)$. But W' is just the stabilizer of X, and so is a non-trivial reflection group in its own right. Let t be any fixed reflection in W' and define an involution $\iota: W' \to W'$ by

$$\iota(w) = wt.$$

By Lemma 3.3 this is sign-reversing and so we are done. ∎

We should note that there is a direct connection between absolutely reduced expressions and NBC bases. Specifically, in [1] Barcelo and Goupil show that if $H_1, \ldots, H_m$ is an NBC base of $\mathscr{A}_W$ then the corresponding product of reflections $r_{H_1} \cdots r_{H_m}$ is totally reduced and this gives a bijection between NBC bases and W.

We end by showing how Theorem 3.4 relates the characteristic polynomial of L_W to the Poincaré polynomial of W. The *characteristic polynomial* of L_W is the generating function for its Möbius function:

$$\chi(L_W, t) = \sum_{X \in L_W} \mu(X)\, t^{\dim X}.$$

The *Poincaré polynomial* of W is the generating function for its elements by absolute length:

$$\pi(W, t) = \sum_{w \in W} t^{\hat{l}(w)}.$$

THEOREM 3.5. *Let W be a finite reflection group in V, $\dim V = n$, with corresponding intersection lattice L_W. Then*

$$\pi(W, t) = (-t)^n \chi(L_W, -1/t).$$

Proof. Using Theorem 3.4 and the lemma of Carter cited previously, we have the following series of equalities

$$\begin{aligned}(-t)^n \chi(L_W, -1/t) &= \sum_{X \in L_W} \mu(X)(-t)^{\operatorname{codim} X} \\ &= \sum_{w \in W} t^{\tilde{h}(w)} \\ &= \pi(W, t). \quad \blacksquare\end{aligned}$$

ACKNOWLEDGMENTS

I thank Victor Reiner for many helpful discussions and in particular for posing the problem of finding an involution proof of the Crosscut Theorem. Anders Björner suggested considering the lattices discussed in Section 2 as applications. Finally, I thank Christian Krattenthaler and Gian-Carlo Meloni who independently asked for a combinatorial explanation of the arbitrariness of the atom ordering in the geometric case.

REFERENCES

1. H. BARCELO AND A. GOUPIL, Non-broken circuits of reflection groups and their factorization in D_n, preprint.
2. A. BJÖRNER, Orderings of Coxeter groups, *Contemp. Math.* **34** (1984), 175–195.
3. R. CARTER, Conjugacy classes in the Weyl group, *Compositio Math.* **25** (1972), 1–59.
4. H. FRIEDMAN AND D. TAMARI, Problèmes d'associativité: Une treillis finis induite par une loi demi-associative, *J. Combin. Theory* **2** (1967), 215–242.
5. A. M. GARSIA AND S. C. MILNE, A Rogers-Ramanujan bijection, *J. Combin. Theory Ser. A* **31** (1981), 289–339.
6. G. GRÄTZER, "Lattice Theory," pp. 17–18, problems 26–36, Freeman, San Francisco, 1971.
7. P. HALL, A contribution to the theory of groups of prime power order, *Proc. London Math. Soc. (2)* **36** (1932), 39–95.
8. S. HUANG AND D. TAMARI, Problems of associativity: A simple proof for the lattice property of systems ordered by a semi-associative law, *J. Combin. Theory Ser. A* **13** (1972), 7–13.
9. J. E. HUMPHREYS, "Reflection Groups and Coxeter Groups," Cambridge Studies in Advanced Mathematics, Cambridge Univ. Press, Cambridge, 1990.
10. P. ORLIK AND H. TERAO, "Arrangements of Hyperplanes," Grundlehren, Vol. 300, Springer-Verlag, New York, 1992.
11. J. G. OXLEY, "Matroid Theory," Oxford Univ. Press, New York, 1992.

12. G.-C. ROTA, On the foundations of combinatorial theory I. Theory of Möbius functions, *Z. Wahrscheinlichkeitstheorie* **2** (1964), 340–368.
13. W. T. TUTTE, A contribution to the theory chomatic polynomials, *Canad. J. Math.* **6** (1953), 80–91.
14. J. WALKER, "Topology and Combinatorics of Ordered Sets," Ph.D. thesis, Massachusetts Institute of Technology, Cambridge, MA, 1981.

ADVANCES IN MATHEMATICS 111, 208–226 (1995)

A Rigidity Theorem for Finite Group Actions on Enveloping Algebras of Semisimple Lie Algebras

JACQUES ALEV

Université de Reims, UFR des Sciences, Département de Mathématiques, Moulin de la Housse, BP 347, 51062 Reims Cedex, France

AND

PATRICK POLO

URA 747 du CNRS, Université Pierre et Marie Curie, BP 191, 4, place Jussieu, 75252 Paris Cedex 05, France

Let $\mathbf{g}$ denote a semisimple Lie algebra over an algebraically closed field k of characteristic zero and G, a finite group of k-automorphisms of the enveloping algebra U of $\mathbf{g}$. In this paper, it is proved that, if the subalgebra U^G is k-isomorphic to an enveloping algebra, then G is trivial. A similar result for Weyl algebras over k is also obtained. © 1995 Academic Press, Inc.

INTRODUCTION

Let k denote an algebraically closed field of characteristic zero. A well-known theorem of Shephard Todd and Chevalley asserts that, if G is a finite group of automorphisms of a finite dimensional vector space V over k, then the algebra of invariants of G acting in the symmetric algebra of V is a polynomial algebra over k if and only if G is generated by pseudoreflections. In searching for eventual noncommutative analogues of this result, the following rigidity property is observed to hold for certain strongly structured algebras such as enveloping algebras of semisimple Lie algebras and Weyl algebras:

> For any k-algebra A of either kind above and any non-trivial finite group G of k-automorphisms of A, the subalgebra A^G of fixed points is not k-isomorphic to A; we shall say that A does not admit Galois embeddings into itself.

Note that this property also holds when A is the tensor algebra of a finite dimensional vector space V and G is a finite subgroup of $GL(V)$. Indeed, in that case, by [Kar] the algebra of invariants is also a tensor algebra, whereas, by [Di Fo], it is finitely generated if and only if G consists of

0001-8708/95 $9.00

scalar multiples of the identity, in which case it is isomorphic to the tensor algebra of $V^{\otimes |G|}$; in particular, the algebra of invariants is isomorphic to the initial tensor algebra if and only if G is trivial. On the other hand, in [A-H-V] a complete classification of finite group actions in the first Weyl algebra and of their invariants is given; in particular, one can observe that the first Weyl algebra admits no Galois embedding into itself. Finally, in [Smi] and later in [Mo-Gu] in a more general form, it is shown that the first Weyl algebra never appears as the invariant subalgebra of a non-perfect finite group of automorphism of *any* k-algebra without zero-divisors. The case of a simple group seems still open. In this paper, we establish the following two theorems.

THEOREM 1. *Let G be a finite group of k-automorphisms of the enveloping algebra $U(\mathbf{g})$ of a semisimple Lie algebra $\mathbf{g}$ over k; if $U(\mathbf{g})^G$ is k-isomorphic to the enveloping algebra of some Lie algebra $\mathbf{g}'$, then $\mathbf{g}' \simeq \mathbf{g}$ and G is trivial. In particular, $U(\mathbf{g})$ does not admit any Galois embedding into itself.*

THEOREM 2. *Let G be a finite group of k-automorphisms of the nth Weyl algebra $A_n(k)$; if $A_n(k)^G$ is k-isomorphic to $A_n(k)$, then G is trivial. In other words, $A_n(k)$ does not admit any Galois embedding into itself.*

We could remark that no linearity is assumed on the action of G; indeed, the usual filtrations of $U(\mathbf{g})$ and $A_n(k)$ are not supposed to be preserved by G and this forces to look for finer automorphism invariants of these algebras. On the one hand, both proofs use general results relating the structure of a ring R to the structure of the fixed subring R^G of a finite automorphism group G. On the other hand, the proof of Theorem 1 is based on very precise information available about primitive ideals of $U(\mathbf{g})$, whereas the proof of Theorem 2 goes by reduction to positive characteristic.

The paper is organized as follows: Theorem 1 is proved in Section 1, whereas Section 2 contains a proof of Theorem 2 as stated above, as well as a shorter proof in the case of a linear action.

We thank M. Van den Bergh for allowing the publication of Theorem 2, which was elaborated jointly with the first author. Also, the first author would like to thank M. Chamarie, S. Donkin, H. Kraft, and M. Lazarus for various helpful discussions.

1. ENVELOPING ALGEBRAS OF SEMISIMPLE LIE ALGEBRAS

1.1. Throughout this section, let k denote an algebraically closed field of characteristic zero, $\mathbf{g}$ a semisimple Lie algebra over k, $U = U(\mathbf{g})$ its enveloping algebra, and G a finite subgroup of $\mathrm{Aut}_k\, U(\mathbf{g})$. We shall then prove the following.

THEOREM 1. *Assume that $U(\mathbf{g})^G$ is k-isomorphic to the enveloping algebra of some Lie algebra $\mathbf{g}'$; then $\mathbf{g}' \simeq \mathbf{g}$ and G is trivial. In particular, $U(\mathbf{g})$ does not admit any Galois embedding into itself.*

1.2. During the Oberwolfach conference on "Noncommutative Algebra and Representation Theory" (August 16–21, 1993), L. Small informed the first author of some results in the forthcoming paper [Kr–Sm], which imply in particular that the subalgebra of invariants of $U(\mathbf{sl}_2)$ under a non-trivial finite cyclic subgroup of the adjoint group is not even a quotient of the enveloping algebra of any semisimple Lie algebra. This issue was further discussed with L. Le Bruyn, and we would like to thank them both for their interest, which led us to observe that our proof gives, in fact, a stronger result in the case of a subgroup of the adjoint group. Namely, one has the following.

PROPOSITION. *Keep notation as in* 1.1 *and assume further that G fixes pointwise the center of U (which is the case if G is conjugate in $\mathrm{Aut}_k\, U(\mathbf{g})$ to a subgroup of the adjoint group). Then, unless G is trivial, U^G is not even a quotient of the enveloping algebra of any semisimple Lie algebra.*

1.3. Consider the following assertions:

(A) Every irreducible finite dimensional $U(\mathbf{g})$-module remains irreducible by restriction to $U(\mathbf{U})^G$.

(B) The annihilator of each irreducible finite dimensional $U(\mathbf{g})$-module is G-invariant.

Then one has the following.

PROPOSITION. *Assume that assertions* (A) *and* (B) *hold. Then $G = \{1\}$.*

Proof. Let $u \in U$ and $g \in G$. Consider an arbitrary irreducible finite dimensional $U(\mathbf{g})$-module E. Since E remains irreducible by restriction to $U(\mathbf{g})^G$ then, by Jacobson's density theorem, the map $U(\mathbf{g})^G \to \mathrm{End}_k(E)$ is surjective. Therefore there exists $x \in U(\mathbf{g})^G$ such that $u - x \in \mathrm{Ann}\, E$. Since $\mathrm{Ann}\, E$ is G-invariant and x a fixed point of G one obtains $gu - x \in \mathrm{Ann}\, E$, hence $u - gu \in \mathrm{Ann}\, E$. Since E was arbitrary and since the intersection of the annihilators of all irreducible finite dimensional $U(\mathbf{g})$-modules is reduced to $\{0\}$ by a theorem of Harish-Chandra, together with Weyl's complete reducibility theorem (see [Dix, 2.5.7 and 1.6.3]), it follows that $u = gu$. This proves that $G = \{1\}$.

Remark. Note that the finiteness of G was not used in this subsection. Also, let us mention that Theorem 1 was first proved for $\mathbf{g} = \mathbf{sl}_2$ by

M. Chamarie and the first author (unpublished), by using the above argument.

1.4. Let us denote by $Z(A)$ the center of a ring A. Then we have the following.

PROPOSITION. $Z(U^G) = Z(U)^G$.

Proof. First, recall the definition of X-inner automorphisms of a (semiprime) ring; see [Mo 1, Chap. 3]. Then, by [*loc. cit.*, 6.17], the proposition will follow if one checks that $U(\mathbf{g})$ has no X-inner automorphism but the identity. So, let τ be an X-inner automorphism of $U(\mathbf{g})$. Then, by [Mo 2, Proposition 1], τ preserves the canonical filtration of $U(\mathbf{g})$, and induces the identity on the associated graded ring. Hence, there exists a linear form λ on $\mathbf{g}$ such that $\tau(x) = x + \lambda(x)$ for all $x \in \mathbf{g}$, and λ satisfies $\lambda([\mathbf{g}, \mathbf{g}]) = 0$. Indeed, if $x, y \in \mathbf{g}$ then

$$\tau([x, y]) = \tau(xy - yx) = \tau(x)\,\tau(y) - \tau(y)\,\tau(x) = xy - yx = [x, y];$$

hence $\lambda([x, y]) = 0$. But $\mathbf{g} = [\mathbf{g}, \mathbf{g}]$ since $\mathbf{g}$ is semisimple; hence $\lambda = 0$ and $\tau = \mathrm{id}$. This proves the proposition.

1.5. In this subsection we record several facts about finite dimensional irreducible U-modules and their central characters. For short, we denote the center of U simply by Z. Recall first that, since k is algebraically closed, any maximal ideal of Z is the kernel of a (unique) k-algebra homomorphism $Z \to k$, and such a homomorphism is called a central character. Hence there is a bijection between the set $\mathrm{Max}\, Z$ of maximal ideals of Z, and the set $\mathrm{Char}\, Z$ of central characters of Z. Also, any $z \in Z$ can be regarded as a regular function on the affine variety $\mathrm{Max}\, Z$. Moreover, if $\chi \in \mathrm{Char}\, Z$, and $m = \mathrm{Ker}\, \chi$ then $\chi(z)$ is precisely the value of z on the point m. For this reason, we shall denote $\chi(z)$ by $\langle z, \chi \rangle$ or $\langle z, m \rangle$.

Now, a U-module is said to admit a central character χ if it is annihilated by the (maximal) ideal $\mathrm{Ker}\, \chi$ of Z. By Schur's lemma, every (finite dimensional) irreducible U-module E admits a central character, denoted by χ_E. Let us denote by $\mathscr{I}'(\mathbf{g})$ the set of isomorphy classes of irreducible finite dimensional U-modules, and by Γ the set of all χ_E's, as E varies through $\mathscr{I}'(\mathbf{g})$. Then one has the following.

PROPOSITION. (a) *For any $\chi \in \Gamma$, there exists a unique element of $\mathscr{I}'(\mathbf{g})$, denoted by $E(\chi)$, whose central character is χ.*

(b) *The set* $\{\operatorname{Ker}\chi \mid \chi \in \Gamma\}$ *is dense in* $\operatorname{Max} Z$, *for the Zariski topology.*

(c) *There exists a (unique) element* D *of* Z *such that, for all* $\chi \in \Gamma$,

$$\langle D, \chi \rangle = (\dim_k E(\chi))^2.$$

Proof. This is well known: parts (a) and (b) can be found in [Bou, VIII, Section 8, No. 5, Théorème 2 et Corollaires]; part (c) in [*loc. cit.*, Section 9, Exercice 2].

1.6. Recall the definition of Gelfand Kirillov dimension, see [Kr Le], which we shall denote by $d(?)$. Then, for future use, we record here the following.

LEMMA. *Let* A *be a noetherian* k*-algebra,* H *a finite group of automorphisms of* A, *and* J *a two-sided ideal of* A. *Then,* $d(A^H/A^H \cap J) = d(A/J)$.

Proof. This follows from [Mo 1, 5.9; Kr Le, 5.5].

1.7. From now on, we assume that $U(\mathbf{g})^G$ is k-isomorphic to the enveloping algebra of some Lie algebra $\mathbf{g}'$. Then, by the previous lemma, $d(U(\mathbf{g}')) = d(U(\mathbf{g}))$, and by [Kr Le, 6.5 6.9], it follows that $\mathbf{g}'$ is finite dimensional and $\dim_k(\mathbf{g}') = \dim_k(\mathbf{g})$. Moreover, $\mathbf{g}'$ is semisimple, as it follows from the lemma.

LEMMA. *Every finite dimensional* $U(\mathbf{g}')$*-module is the restriction of a finite dimensional* $U(\mathbf{g})$*-module and is, therefore, semisimple. As a consequence,* $\mathbf{g}'$ *is semisimple.*

Proof. Set $U' = U(\mathbf{g})^G \simeq U(\mathbf{g}')$ and let M' be a finite dimensional U'-module. First, since $\operatorname{char}(k) = 0$, then, as a U'-bimodule, U' is a direct summand of U. Namely, one has $U = U' \oplus \operatorname{Ker} p$, where p is the projector $p = |G|^{-1} \sum_{g \in G} g$. It follows that M' is a U'-submodule of $M|_{U'}$, where M denotes the left U-module $U \otimes_{U'} M'$. Moreover, a result of Farkas and Snider [Mo 1, 5.9] asserts that U is a finite right U'-module. This gives that M is a finite dimensional, hence completely reducible, U-module. Then, by a result of Lorenz and Passman [*loc. cit.*, 7.6(4)], $M|_{U'}$ is a completely reducible U'-module, and so is its submodule M'. The lemma is proved.

1.8. *Proof of assertion* (A). From now on, we denote $U(\mathbf{g})^G \simeq U(\mathbf{g}')$ simply by U', its center by Z', and introduce notations $\mathcal{I}'(\mathbf{g}')$ and Γ' similar to those for $\mathbf{g}$. Applying Proposition 1.5 to $\mathbf{g}'$ instead of $\mathbf{g}$, we

denote, for every $\chi' \in \Gamma'$, by $E'(\chi')$ the corresponding element of $\mathscr{I}'(\mathbf{g}')$. Also, let D' denote the unique element of Z', similar to the element D of Z.

Now, let $\chi \in \Gamma$ and let $E(\chi)$ be the corresponding element of $\mathscr{I}'(\mathbf{g})$. Since $Z' \subseteq Z$, by Proposition 1.4, then $E(\chi)$, regarded as a U'-module, admits the central character $\chi' = \chi|_{Z'}$. On the other hand, by Weyl's complete reducibility theorem, $E(\chi)|_{U'}$ is a direct sum of (finite dimensional) irreducible U'-modules, and each of these admits the central character χ'. Hence $\chi' \in \Gamma'$, and $E(\chi)|_{U'}$ is a direct sum of copies of $E'(\chi')$. Let $m(\chi)$ denote the multiplicity of $E'(\chi')$ in $E(\chi)|_{U'}$. Then:

$$\langle D, \chi \rangle = (\dim_k E(\chi))^2 = m(\chi)^2 (\dim_k E'(\chi'))^2 = m(\chi)^2 \langle D', \chi' \rangle. \qquad (*)$$

Also, $\chi' = \chi|_{Z'}$; hence $\langle D', \chi' \rangle$ is nothing but $\langle D', \chi \rangle$. Moreover, $m(\chi)$ is the length of $E(\chi)$ as a $U' = U^G$-module, and by a result of Lorentz and Passmann [Mo 1, Theorem 7.6(3)], one has for all $\chi \in \Gamma$,

$$m(\chi) = \text{length}_{U'}(E(\chi)|_{U'}) \leqslant |G| \text{ length}_U(E(\chi)) = |G|.$$

Hence, $m(\chi) \in \{1, ..., |G|\}$ for all $\chi \in \Gamma$. Thus, the element $P = \prod_{i=1}^{|G|} (D - i^2 D')$ of Z satisfies $\langle P, \text{Ker } \chi \rangle = \langle P, \chi \rangle = 0$ for all $\chi \in \Gamma$. Since $\{\text{Ker } \chi \mid \chi \in \Gamma\}$ is a dense subset of Max Z, then P vanishes identically on Max Z, and since the latter is irreducible (Z being a domain), some factor of P also vanishes identically. Hence $D = i^2 D'$ for some $i \in \{1, ..., |G|\}$. Consider now the one-dimensional represenation of U. It certainly restricts to a one-dimensional representation of U', and this gives $i = 1$; hence $D = D'$. It then follows from $(*)$ that $m(\chi) = 1$ for all $\chi \in \Gamma$. This proves assertion (A).

1.9. *Proof of Proposition* 1.2. First, it is easy to see that, if U^G is only assumed to be a quotient of $U(\mathbf{g}')$, with $\mathbf{g}'$ semisimple, then the argument of the previous subsection applies just as well and gives that assertion (A) also holds in this case. Second, under the hypothesis that G fixes pointwise the center of U, it is immediate that assertion (B) is satisfied, since every finite dimensional irreducible U-module is determined by its central character. This proves Proposition 1.2.

1.10. *Towards the proof of assertion* (B). For each $d \in \mathbf{N}^+$, set $\mathscr{I}'_d(\mathbf{g}) = \{E \in \mathscr{I}'(\mathbf{g}) \mid \dim_k E = d\}$, define $\mathscr{I}'_d(\mathbf{g}')$ similarly, and, taking the truth of assertion (A) into account, denote by ϕ_d the map from the former into the latter, which takes $E \in \mathscr{I}'_d(\mathbf{g})$ to $\phi_d(E) := E|_{U'} \in \mathscr{I}'_d(\mathbf{g}')$. It is clear from the proof of Lemma 1.7 that every ϕ_d is surjective. For future use, we record this fact as the:

COROLLARY. *ϕ_d is surjective, for every $d \in \mathbf{N}^+$.*

Also, observe that there is a natural action of G on $\mathscr{I}'(\mathbf{g})$. Indeed, if $E \in \mathscr{I}'(\mathbf{g})$ and $g \in G$, define the twisted module ${}^gE$ to be the vector space E with the U-module structure given by $u \cdot e = g^{-1}(u)e$, for all $u \in U$, $e \in E$. Then note, on the one hand, that $\operatorname{Ann}{}^gE = g(\operatorname{Ann} E)$, and, on the other hand, that $\phi_d({}^gE) = \phi_d(E)$, where $d = \dim_k E$. Therefore, assertion (B) would follow from the injectivity of the ϕ_d. But it is well known that $\mathscr{I}'_d(\mathbf{g})$ and $\mathscr{I}'_d(\mathbf{g}')$ are finite sets (see Lemma 1.16 below); therefore, in view of the previous corollary, injectivity will follow if we prove that, for every $d \in \mathbf{N}^+$, $\mathscr{I}'_d(\mathbf{g})$ and $\mathscr{I}'_d(\mathbf{g}')$ have the same cardinality. It is certainly enough to prove that $\mathbf{g} \simeq \mathbf{g}'$, and this is what we shall do.

1.11. Let $\mathbf{h}$ be a Cartan subalgebra of $\mathbf{g}$, R the root system of $(\mathbf{g}, \mathbf{h})$, Δ a basis of R, and define $\mathbf{h}' \subset \mathbf{g}'$, R', and Δ' similarly. Then one has the lemma.

LEMMA. (a) $\dim_k \mathbf{g} = d(U) = d(U') = \dim_k \mathbf{g}'$

(b) $|\Delta| = d(Z) = d(Z') = |\Delta'|$

(c) $|R| = |R'|$.

Proof. Since $\dim_k \mathbf{g} = |\Delta| + |R|$, and similarly for $\mathbf{g}'$, assertion (c) is a consequence of assertions (a) and (b), which themselves follow from Lemma 1.6, together with [Kr-Le, 6.9; Dix, 7.3.8].

1.12. *Primitive ideals.* Keep the notations of 1.11, and, in addition, introduce: $\mathbf{g} = \mathbf{h} \oplus (\bigoplus_{\alpha \in R} \mathbf{g}_\alpha)$ the corresponding weight space decompositon, $R^\vee = \{H_\alpha \mid \alpha \in R\} \subset \mathbf{h}$ the set of coroots, W the Weyl group, $R^+ = R \cap \mathbf{N}\Delta$ the set of positive roots corresponding to Δ, ρ the half-sum of the elements of R^+, and w_0 the unique element of W such that $w_0(R^+) = -R^+$. Recall that to each $\alpha \in \Delta$ is associated an element of W, the reflection s_α. Then, for each subset S of Δ, set $R_S = R \cap \mathbf{Z}S$, $R_S^+ = R_S \cap R^+$, let W_S be the subgroup of W generated by the reflections s_α, where $\alpha \in S$, and let w_S denote the unique element of W_S such that $w_S(R_S^+) = -R_S^+$.

Now, set $\mathbf{n} = \bigoplus_{\alpha \in R^+} \mathbf{g}_\alpha$ and $\mathbf{b} = \mathbf{h} \oplus \mathbf{n}$. Then $\mathbf{b}$ is a Borel subalgebra of $\mathbf{g}$ and $\mathbf{n}$ an ideal of $\mathbf{b}$. Let $\lambda \in \mathbf{h}^*$. Then λ defines a one-dimensional representation of $\mathbf{h}$. Since $\mathbf{b}/\mathbf{n} \simeq \mathbf{h}$, then λ also defines a one-dimensional representation of $\mathbf{b}$, which we shall denote by k_λ. One then defines the Verma module $M(\lambda) = U(\mathbf{g}) \otimes_{U(\mathbf{b})} k_\lambda$. By [Dix, 7.1.11–7.1.13], $M(\lambda)$ has a unique simple quotient, denoted by $L(\lambda)$, and $L(\lambda)$ is characterized by the existence of a non-zero vector $v \in L(\lambda)$ such that $\mathbf{n}v = 0$ and $(h - \lambda(h))v = 0$ for all $h \in \mathbf{h}$. (Beware the change of notation: our $M(\lambda)$ is denoted $M(\lambda + \rho)$

in *loc. cit.*). Since the unique one-dimensional $\mathbf{g}$-module is annihilated by $[\mathbf{g}, \mathbf{g}] = \mathbf{g}$, and in particular by $\mathbf{b}$, this module is indeed $L(0)$. Also, for every $\lambda \in \mathbf{h}^*$, set $I(\lambda) = \mathrm{Ann}_U L(\lambda)$. Recall the definition of the dot-action of W on $\mathbf{h}^*$: for any $w \in W$, $\lambda \in \mathbf{h}^*$, $w \cdot \lambda = w(\lambda + \rho) - \rho$. Then one has the following.

PROPOSITION. *Let χ_0 denote the central character of $L(0)$, and set $I = U(\mathrm{Ker}\, \chi_0)$. Then*:

(a) *I is left invariant by every automorphism of U.*

(b) *I is completely prime, and $I = I(w_0 \cdot 0)$.*

(c) *The prime ideals of U, minimal among those strictly containing I, are exactly the $I(s_\alpha w_0 \cdot 0) := I_\alpha$, where $\alpha \in \Delta$.*

(d) *For any subset S of Δ, one has $\sum_{\alpha \in S} I(s_\alpha w_0 \cdot 0) = I(w_S w_0 \cdot 0) := I_S$; this ideal is completely prime, and $d(U/I_S) = |R| - |R_S|$. Also, $d(U/I) = |R|$.*

Proof. Since $\mathbf{g}$ has a unique one-dimensional representation, then U has a unique two-sided ideal of codimension one, which we shall denote by U_+. Clearly, U_+ is left invariant by every automorphism of U; hence so is $\mathrm{Ker}\, \chi_0 = U_+ \cap Z$. This proves assertion (a). Assertion (b) follows from [Dix, 8.4.3–8.4.4, 7.4.7, and 7.6.24]. Assertion (c) and the first part of assertion (d) follow from [Duf, Corollaire 2 de la Proposition 10, Proposition 12]. The second part of assertion (d) follows from [Jan, 15.3(5) and 15.6]. Finally, the assertions concerning Gelfand–Kirillov dimension follow from [*loc. cit.*, 15.3(1) and 10.9].

1.13. Set $\chi_0' = \chi_0|_{Z'}$, and $I' = U'(\mathrm{Ker}\, \chi_0')$. Since χ_0' is the central character of $L(0)|_{U'}$, the unique one-dimensional U'-module, then Proposition 1.12 also applies to I'. In particular, the prime ideals of U', minimal among those strictly containing I', are denoted by $I'_{\alpha'}$, where α' runs through Δ'. Then we have the following.

PROPOSITION. (a) $I \cap U' = I'$.

(b) *There exists a bijection $\varphi: \Delta \to \Delta'$ such that, for all $\alpha \in \Delta$, $I_\alpha \cap U' = I'_{\varphi(\alpha)}$.*

(c) *I_α is G-invariant, for every $\alpha \in \Delta$.*

Proof. Clearly, $(I \cap U') \supseteq I'$. Moreover, by 1.6, 1.11(c), and the last assertion of 1.12 applied to both U and U', one has

$$d(U'/U' \cap I) = d(U/I) = |R| = |R'| = d(U'/I').$$

Since U'/I' is prime noetherian, this gives $U' \cap I = I'$, by [Kr–Le, 3.15] together with Goldie's theorem (see, e.g., [Dix, 3.5.10]). Thus, since I is

G-stable by Proposition 1.12(a), setting $A = U/I$ and $A' = U'/I'$ one then has $A'' = A'$. Recall then that, by a result of Montgomery [Mo 3, 4.2 and 3.6], there exists a bijective, order preserving, correspondence between G-orbits in Spec A and certain equivalence classes in Spec A'. In our case, a part of this correspondence can be expressed in a simple manner, since some equivalence classes in Spec A' are trivial. Indeed, for every minimal non-zero prime ideal J of A, the ideal $J \cap A'$ is completely prime since J is so. It then follows from [*loc. cit.*] that the map $\phi : J \mapsto J \cap A'$ is a surjective map from the set of minimal non-zero primes of A onto the set of minimal non-zero primes of A', and every fiber of ϕ is a G-orbit. But we saw already that A and A' have the same number of minimal non-zero prime ideals, namely $|\Delta| = |\Delta'|$. This simultaneously gives that ϕ is bijective and hence induces a bijection $\varphi : \Delta \to \Delta'$ such that $U' \cap I_\alpha = I'_{\varphi(\alpha)}$ for all $\alpha \in \Delta$, and that all I_α, where $\alpha \in \Delta$, are G-invariant. The proposition is proved.

1.14. *Coxeter graphs.* For any pair α, β of elements of Δ, denote by $m_{\alpha\beta}$ the order of the element $s_\alpha s_\beta$ of W. Then recall (see [Bou, IV, Section 1, No. 9]) that the Coxeter graph of $\mathbf{g}$ is the labelled graph defined as follows: its set of vertices is Δ, and $\{\alpha, \beta\}$ is an edge if and only if $m_{\alpha\beta} \geq 3$, in which case the edge $\{\alpha, \beta\}$ carries the label $m_{\alpha\beta}$.

LEMMA. *One has* $2m_{\alpha\beta} = |R_{\{\alpha,\beta\}}|$, *for every pair of elements* α, β *in* Δ.

Proof. Let $W_{\{\alpha,\beta\}}$ be the subgroup of W generated by s_α and s_β. Recall that the length $l(w)$ of an element $w \in W_{\{\alpha,\beta\}}$ is the smallest integer $q \geq 0$ such that w can be written as a product of q elements of the set $\{s_\alpha, s_\beta\}$. By [Bou, IV, Section 1, No. 2, Remarque], $W_{\{\alpha,\beta\}}$ contains a unique element of maximal length, denoted by $w_{\{\alpha,\beta\}}$, and $l(w_{\{\alpha,\beta\}}) = m_{\alpha\beta}$. On the other hand, by [Bou, VI, Section 1, No. 6, Corollaire 3 de la Proposition 17], one has $l(w_{\{\alpha,\beta\}}) = |R^+_{\{\alpha,\beta\}}|$. The lemma follows.

PROPOSITION. *The bijection* $\varphi : \Delta \to \Delta'$ *of Proposition* 1.13(b) *is an isomorphism of Coxeter graphs.*

Proof. Let $\{\alpha, \beta\}$ be a pair of elements of Δ. Since I_α and I_β are G-stable by Proposition 1.13 and since the functor $M \mapsto M^G$ is exact (recall $\mathrm{char}(k) = 0$) one has $(I_\alpha + I_\beta)^G = I_\alpha^G + I_\beta^G = I'_{\varphi(\alpha)} + I'_{\varphi(\beta)}$. Therefore, by Lemma 1.6 and by Proposition 1.12(d) applied to U and to U', we obtain

$$|R| - |R_{\{\alpha,\beta\}}| = d\left(\frac{U}{I_\alpha + I_\beta}\right)$$

$$= d\left(\frac{U'}{I'_{\varphi(\alpha)} + I'_{\varphi(\beta)}}\right) = |R'| - |R'_{\{\varphi(\alpha),\varphi(\beta)\}}|.$$

Since $|R| = |R'|$ by Lemma 1.11, it follows that $|R_{\{\alpha,\beta\}}| = |R'_{\{\varphi(\alpha),\varphi(\beta)\}}|$. Applying the previous lemma on both sides, we obtain $m_{\alpha\beta} = m_{\varphi(\alpha)\varphi(\beta)}$. This proves the proposition.

1.15. Recall (see, e.g., [Bou, VIII, Section 4, No. 4, Théorème 2(iii)]) that a semisimple Lie algebra over an algebraically closed field of characteristic zero is determined up to isomorphism by its Dynkin graph (defined, e.g., in [*loc. cit.*, VI, Section 4, No. 2]). In particular, the latter determines the Coxeter graph. Conversely, it is well known (see, e.g., [*loc. cit.*, Section 4, Théorèmes 1 and 3]) that two connected Dynkin graphs having the same Coxeter graph are isomorphic, unless they are of types B_n and C_n, for some $n \geqslant 3$. This leads us to introduce the following notations. First, denote by $\mathscr{D}(\mathbf{g})$ the Dynkin graph of $\mathbf{g}$ and by X the set of connected components of $\mathscr{D}(\mathbf{g})$. Then recall (see [*loc. cit.*]) that the set of vertices of $\mathscr{D}(\mathbf{g})$ may be identified with Δ, the set of simple roots. Making this identification, let us then denote, for every $\mathscr{C} \in X$, by $\mathbf{g}_{\mathscr{C}}$ the subalgebra of $\mathbf{g}$ generated by the subspaces $\mathbf{g}_{\pm\alpha}$, where $\alpha \in \mathscr{C}$. Then $\mathbf{g}_{\mathscr{C}}$ is a simple Lie algebra, and $\mathscr{C}$ is its Dynkin graph. Moreover, $\mathbf{g}$ is the direct product of the $\mathbf{g}_{\mathscr{C}}$, as $\mathscr{C}$ runs through X. Define similarly X', and the subalgebras $\mathbf{g}'_{\mathscr{C}'}$ of $\mathbf{g}'$, for $\mathscr{C}' \in X'$. Also, for every integer $n \geqslant 3$, let us denote by:

$\mathbf{b}_n$ (resp. $\mathbf{c}_n$) the simple Lie algebra of type B_n (resp. C_n).

r_n (resp. s_n) the number of connected components of $\mathscr{D}(\mathbf{g})$ of type B_n (resp. C_n).

$X_{\leqslant n}$ (resp. X_n) the set of connected components of $\mathscr{D}(\mathbf{g})$ which are of type B_p or C_p, with $p \geqslant n$ (resp. $p = n$).

$$\mathbf{p}_n = \prod_{\mathscr{C} \notin X_{\leqslant n}} \mathbf{g}_{\mathscr{C}},\quad \mathbf{g}_n = \prod_{\mathscr{C} \in X_n} \mathbf{g}_{\mathscr{C}},\quad \mathbf{q}_n = \prod_{\mathscr{C} \in X_{\leqslant n+1}} \mathbf{g}_{\mathscr{C}}.$$

Then, one has $\mathbf{g} \simeq \mathbf{p}_n \times \mathbf{g}_n \times \mathbf{q}_n$ and $\mathbf{g}_n \simeq (\mathbf{b}_n)^{r_n} \times (\mathbf{c}_n)^{s_n}$.

Define similarly r'_n, s'_n, $\mathbf{p}'_n, \mathbf{g}'_n$, and $\mathbf{q}'_n$. Then, with these notations, Proposition 1.14 has the following consequence.

COROLLARY. *One has* $\mathbf{p}_3 \simeq \mathbf{p}'_3$, *and* $r_n + s_n = r'_n + s'_n$ *for every* $n \geqslant 3$.

By induction on n, we are going to prove that $\mathbf{p}_n \simeq \mathbf{p}'_n$, for all $n \geqslant 3$. We shall need several lemmas.

1.16. Set $\mathscr{P}^+ = \{\lambda \in \mathbf{h}^* \mid \lambda(H_\alpha) \in \mathbf{N}\ \forall \alpha \in \Delta\}$, and let $\{\omega_\alpha\}_{\alpha \in \Delta}$ denote the basis of $\mathbf{h}^*$ dual to the basis $\{H_\alpha\}_{\alpha \in \Delta}$ of $\mathbf{h}$; the ω_α are called the fundamental weights, they form an $\mathbf{N}$-basis of $\mathscr{P}^+$. Indeed, for any $\lambda \in \mathscr{P}^+$ and $\alpha \in \Delta$, set $\lambda_\alpha = \lambda(H_\alpha) \in \mathbf{N}$; then $\lambda = \sum_{\alpha \in \Delta} \lambda_\alpha \omega_\alpha$. Define a partial order $\leqslant$ on $\mathscr{P}^+$ as follows: $\lambda \leqslant \mu$ if and only if $\lambda_\alpha \leqslant \mu_\alpha$ for all $\alpha \in \Delta$. Also, set $\lambda < \mu$ if $\lambda \leqslant \mu$ and $\lambda \neq \mu$. Then, one has the following.

LEMMA. (a) *The map* $\lambda \mapsto [L(\lambda)]$ *is a bijection from* $\mathscr{P}^+$ *to* $\mathscr{I}'(\mathbf{g})$.

(b) $\mathscr{I}'_d(\mathbf{g})$ *is a finite set, for every* $d \in \mathbf{N}^+$.

(c) *Let* $\lambda, \mu \in \mathscr{P}^+$. *If* $\lambda \prec \mu$, *then* $\dim_k L(\lambda) < \dim_k L(\mu)$.

Proof. Assertion (a) follows from [Dix, 7.2.6], whereas assertions (b) and (c) will follow from the Weyl character formula: for all $\lambda \in \mathscr{P}^+$,

$$\dim_k L(\lambda) = \prod_{\alpha \in R^+} \frac{(\rho + \lambda)(H_\alpha)}{\rho(H_\alpha)}.$$

Indeed, recall first that $\rho(H_\alpha) = 1$ for all $\alpha \in \Delta$, whence $\rho(H_\alpha)$ and $(\lambda + \rho)(H_\alpha)$ are positive integers for all $\alpha \in R^+$. Now, if $\dim_k L(\lambda) = d$, then $\prod_{\alpha \in R^+} (\rho + \lambda)(H_\alpha) = d \prod_{\alpha \in R^+} \rho(H_\alpha) := d' \in \mathbf{N}^+$. This gives, for instance, that $\lambda_\alpha \leqslant d' - 1$ for all $\alpha \in \Delta$, and assertion (b) follows.

Cosider now assertion (c). First, for every $\beta \in R^+$, one has $H_\beta = \sum_{\alpha \in \Delta} c_{\beta\alpha} H_\alpha$ for some $c_{\beta\alpha} \in \mathbf{N}$; hence, if $\lambda, \mu \in \mathscr{P}^+$ and $\lambda \leqslant \mu$ then

$$(\rho + \lambda)(H_\beta) = \sum_{\alpha \in \Delta} c_{\beta\alpha}(\rho_\alpha + \lambda_\alpha) \leqslant \sum_{\alpha \in \Delta} c_{\beta\alpha}(\rho_\alpha + \mu_\alpha) = (\rho + \mu)(H_\beta).$$

Moreover, if $\lambda \prec \mu$ then the above inequality is strict for at least one $\beta \in \Delta$, and assertion (c) follows.

1.17. LEMMA. *Let* $n \geqslant 3$. *Then*:

(a) *Every non-trivial irreducible representation of* $\mathbf{b}_n$ *has dimension* $\geqslant 2n + 1$, *and there is a unique, up to isomorphism, such representation of dimension* $2n + 1$.

(b) *Every non-trivial irreducible representation of* $\mathbf{c}_n$ *has dimension* $\geqslant 2n$, *and there is a unique, up to isomorphism, such representation of dimension* $2n$, *but none of dimension* $2n + 1$.

Proof. In both cases, we fix numberings $\alpha_1, \ldots, \alpha_n$ and, correspondingly, $\omega_1, \ldots, \omega_n$ of the simple roots and fundamental weights, as in [Bou, VI, Planches II III]. Then, one has $\dim_k L(\omega_1) = 2n + 1$ for $\mathbf{b}_n$, whereas $\dim_k L(\omega_1) = 2n$ for $\mathbf{c}_n$. Hence, by Lemma 1.16, it is enough to prove, in both cases, that $\dim_k L(\lambda) \geqslant 2n + 2$ when λ is either $2\omega_1$, or ω_i for some $i \geqslant 2$.

Consider $\mathbf{b}_n$. By [Bou, VIII, Section 13, No. 2], one has $L(\omega_i) \simeq \bigwedge^i L(\omega_1)$ for $2 \leqslant i \leqslant n - 1$, and $\dim_k L(\omega_n) = 2^n$. Hence, one has

$$\dim_k L(\omega_i) = \binom{2n+1}{i} > 2n + 1 \qquad \text{for} \quad 2 \leqslant i \leqslant n - 1.$$

Taking the hypothesis $n \geqslant 3$ into account, one also obtains

$$\dim_k L(\omega_n) = 2^n = \sum_{j=0}^{n} \binom{n}{j} \geqslant 1 + n + \binom{n}{2} + 1 \geqslant 2n + 2.$$

Also, direct computations, using Weyl's character formula, together with the lists of positive roots in [Bou, VI, Planches II–III], give, on the one hand, that

$$\dim_k L(2\omega_1) = \begin{cases} n(2n+3) & \text{for } \mathbf{b}_n \\ n(2n+1) & \text{for } \mathbf{c}_n \end{cases}$$

and, on the other hand, that, for $\mathbf{c}_n$ and any $i \in \{2, \ldots, n\}$,

$$\dim_k L(\omega_i) = (2n+1) \times \prod_{j=0}^{i-3} \frac{2n-j}{2n-j-i} \times \frac{1}{2n+1-i} \binom{2n+1-i}{i}$$

with the convention that the factor in the middle equals 1 if the indexing set is empty, that is, if $i = 2$. Otherwise, if $i \geqslant 3$, this factor is a rational number > 1. Moreover, since binomial coefficients are unimodal, then the last factor is also a rational number > 1, unless $i = 2n - i$, that is, unless $i = n$. Since $n \geqslant 3$, the conditions $i = 2$ and $i = n$ cannot simultaneously be realized, hence $\dim_k L(\omega_i) > 2n + 1$. The lemma is proved.

1.18. For each $\mathscr{C} \in X$, the linear span of the H_α, where $\alpha \in \mathscr{C}$, is a Cartan subalgebra of $\mathbf{g}_\mathscr{C}$, denoted by $\mathbf{h}_\mathscr{C}$; we set $\mathscr{P}_\mathscr{C}^+ = \{\lambda \in \mathbf{h}_\mathscr{C}^* \mid \lambda(H_\alpha) \in \mathbf{N}\ \forall \alpha \in \mathscr{C}\}$. Then $\mathbf{h}, \mathbf{h}^*$, and $\mathscr{P}^+$ are respectively the direct product of the $\mathbf{h}_\mathscr{C}$, $\mathbf{h}_\mathscr{C}^*$, and $\mathscr{P}_\mathscr{C}^+$, as $\mathscr{C}$ runs through X.

Now, consider $\lambda = (\lambda_\mathscr{C})_{\mathscr{C} \in X}$ in $\mathbf{h}^*$. For every $\mathscr{C} \in X$, one defines the irreducible $U(\mathbf{g}_\mathscr{C})$-module $L_\mathscr{C}(\lambda_\mathscr{C})$ as in 1.12. Moreover, if $\lambda \in \mathscr{P}^+$ then every $\lambda_\mathscr{C}$ belongs to $\mathscr{P}_\mathscr{C}^+$, so that $L_\mathscr{C}(\lambda_\mathscr{C})$ is finite dimensional, by Lemma 1.16(a) applied to $\mathbf{g}_\mathscr{C}$. Finally, since $\mathbf{g} = \prod_\mathscr{C} \mathbf{g}_\mathscr{C}$, then every $L_\mathscr{C}(\lambda_\mathscr{C})$ is a $\mathbf{g}$-module and so is their tensor product. Then one has the following (well-known) lemma (see, e.g., [Bou, VIII, Section 7, Exercice 2]).

LEMMA. *For every $\lambda = (\lambda_\mathscr{C})_{\mathscr{C} \in X}$ in $\mathscr{P}^+$, one has $L(\lambda) \simeq \bigotimes_{\mathscr{C} \in X} L_\mathscr{C}(\lambda_\mathscr{C})$.*

Proof. Set $M = \bigotimes_\mathscr{C} L_\mathscr{C}(\lambda_\mathscr{C})$. Clearly, M contains a non-zero vector annihilated by $\mathbf{n}$ and by $h - \lambda(h)$, for all $h \in \mathbf{h}$. Hence, by [Dix, 7.1.13], it is enough to check that M is irreducible. Since M is finite dimensional, as we already observed, it is completely reducible. Therefore, irreducibility will follow if we check that $\mathrm{End}_\mathbf{g} M = k$. But, since each $\mathbf{g}_\mathscr{C}$ acts trivially on all factors of the tensor product, except the one corresponding to $\mathscr{C}$, it easily follows that $\mathrm{End}_\mathbf{g} M \simeq \bigotimes_\mathscr{C} \mathrm{End}_{\mathbf{g}_\mathscr{C}} L_\mathscr{C}(\lambda_\mathscr{C}) \simeq k$. This proves the lemma.

1.19. *Completion of the proof.* We can now finish the proof of Theorem 1. Recall the notations of Subsection 1.15 and let $n \geqslant 3$. By induction hypothesis, we may assume that $\mathbf{p}_n \simeq \mathbf{p}'_n$. If follows from Lemmas 1.18 and 1.17 that

$$|\mathscr{I}'_{2n}(\mathbf{g})| = |\mathscr{I}'_{2n}(\mathbf{p}_n)| + |\mathscr{I}'_{2n}(\mathbf{g}_n)| = |\mathscr{I}'_{2n}(\mathbf{p}_n)| + s_n$$

and

$$|\mathscr{I}'_{2n+1}(\mathbf{g})| = |\mathscr{I}'_{2n+1}(\mathbf{p}_n)| + |\mathscr{I}'_{2n+1}(\mathbf{g}_n)| = |\mathscr{I}'_{2n+1}(\mathbf{p}_n)| + r_n.$$

Similarly,

$$|\mathscr{I}'_{2n}(\mathbf{g}')| = |\mathscr{I}'_{2n}(\mathbf{p}'_n)| + s'_n, \qquad |\mathscr{I}'_{2n+1}(\mathbf{g}')| = |\mathscr{I}'_{2n+1}(\mathbf{p}'_n)| + r_n.$$

On the other hand, by Corollary 1.10, one has $|\mathscr{I}'_d(\mathbf{g})| \geqslant |\mathscr{I}'_d(\mathbf{g}')|$ for all $d \in \mathbf{N}^*$ and, in particular, for $d = 2n$ and $2n+1$. Taking the isomorphism $\mathbf{p}_n \simeq \mathbf{p}'_n$ into account, one therefore obtains $s_n \geqslant s'_n$ and $r_n \geqslant r'_n$. Since $r_n + s_n = r'_n + s'_n$ by Corollary 1.15, this gives $s_n = s'_n$ and $r_n = r'_n$; hence $\mathbf{p}_{n+1} \simeq \mathbf{p}'_{n+1}$. Since $\mathbf{g} = \mathbf{p}_t$ and $\mathbf{g}' = \mathbf{p}'_t$ for t large enough, one therefore obtains $\mathbf{g} \simeq \mathbf{g}'$. As noted in Subsection 1.10, this completes the proof of Theorem 1.

2. Weyl Algebras

2.1. In this section, let K denote a field of characteristic zero, and let G be a finite group of K-automorphisms of the nth Weyl algebra $A_n(K)$. We shall then prove the following.

Theorem 2. *If $A_n(K)^G$ is K-isomorphic to $A_n(K)$, then G is trivial. In other words, $A_n(K)$ does not admit any Galois embedding into itself.*

2.2. Recall that the nth Weyl algebra $A_n(K)$ is the K-algebra with generators $p_1, q_1, \ldots, p_n, q_n$ and relations: $[p_i, p_j] = [q_i, q_j] = 0$, and $[p_i, q_j] = \delta_{ij}$. It is a simple noetherian domain, and its only units are the non-zero elements of K (see, e.g., [Dix, 4.6.3–4.6.6]).

2.3. *Separability.* Consider an inclusion of rings $R \subset S$. After [L V V, II.5.1], one says that S is separable over R if the S-bimodule map $S \otimes_R S \to S$, $s \otimes s' \mapsto ss'$, admits a splitting. This generalizes the classical notion of separable extension when R is commutative (see, e.g., [De In]).

2.4. Let S be a ring, H a finite group of automorphisms of S, and $R = S^H$. For every $h \in H$, there exists an S-bimodule map $\varphi_h : S \otimes_R S \to {}_hS_1$, $s \otimes s' \mapsto h(s)s'$, where ${}_hS_1$ denotes S, regarded as a S-bimodule for the actions: $s \cdot t = h(s)t$ and $t \cdot s' = ts'$ for all $s, s' \in S$, $t \in {}_hS_1$. Note that φ_1 is precisely the map considered in the previous subsection. Then, one has the following.

PROPOSITION. *Keep the above notations and assume that there exist elements $a_1, b_1, \ldots, a_m, b_m$ in S such that $\sum_{i=1}^m g(a_i)\, h(b_i) = \delta_{g,h}$ for all $g, h \in H$. Then the map $\bigoplus_h \varphi_h$: $S \otimes_R S \to \bigoplus_h {}_hS_1$ is an isomorphism of S-bimodules. In particular, S is separable over R.*

Proof. Set $\phi = \bigoplus_h \varphi_h$. It is clear that ϕ is an homomorphism of S-bimodules. On the other hand, define $\psi : \bigoplus_h {}_hS_1 \to S \otimes_R S$ as follows: if $u_h \in {}_hS_1$ then $\psi(u_h) = \sum_{i=1}^m a_i \otimes h(b_i) u_h$. One then checks that

$$(\phi \circ \psi)(u_h) = \sum_{g \in H} \sum_i g(a_i)\, h(b_i)\, u_h = \sum_g \delta_{g,h} u_h = u_h$$

and also, if $x, y \in S$,

$$\begin{aligned}
(\psi \circ \phi)(x \otimes y) &= \psi\left(\sum_{h \in H} h(x)y\right) \\
&= \sum_h \sum_i a_i \otimes h(b_i)\, h(x)y \\
&= \sum_i a_i \otimes \sum_h h(b_i x)y \\
&= \sum_i a_i \left(\sum_h h(b_i x)\right) \otimes y \qquad \left(\text{since } \sum_h h(b_i x) \in R\right) \\
&= \sum_h \sum_i a_i h(b_i)\, h(x) \otimes y \\
&= \sum_h \delta_{1,h} h(x) \otimes y \\
&= x \otimes y.
\end{aligned}$$

Therefore ψ is the inverse of ϕ. This proves the proposition.

2.5. Now, set $A = A_n(K)$, and recall that G is a finite group of K-automorphisms of A. Then, one has the following.

PROPOSITION. *There exist elements $a_1, b_1, \ldots, a_m, b_m$ in A such that $\sum_{i=1}^m g(a_i)\, h(b_i) = \delta_{g,h}$ for all $g, h \in G$.*

Proof. Since the only invertible elements of A are the nonzero scalars, which are central, then A has no inner automorphism, but the identity. Therefore, it follows from [Mo1, 2.3] that the skew group ring $S = A * G$ is a simple ring. Recall that S is a free left A-module with basis e_g, for $g \in G$, and multiplication is given by $(ae_g)(a'e_h) = ag^{-1}(a')e_{gh}$ for all $a, a' \in A$, $g, h \in G$. Now, consider the element $f = \sum_h e_h$ of S. Note that $e_g f = fe_g = f$ for all $g \in G$; hence $SfS = AfA$. Therefore, since $f \neq 0$ and S is simple, there exist elements $a_1, b_1, \ldots, a_m, b_m$ in A such that $\sum_{i=1}^{m} a_i f b_i = 1$. Then

$$1 = \sum_i \sum_h a_i e_h b_i = \sum_i \sum_h a_i h^{-1}(b_i) e_h = \sum_h \left(\sum_i a_i h^{-1}(b_i) \right) e_h$$

and, therefore, $\sum_i a_i h^{-1}(b_i) = \delta_{1,h}$; applying another element $g \in G$ to this equality, we get $\sum_i g(a_i)\, gh^{-1}(b_i) = \delta_{1,h} = \delta_{g,gh^{-1}}$. Up to the change of variables $h' = gh^{-1}$, this is the sought for equality.

2.6. From now on, we make the assumption that $A_n(K)^G \simeq A_n(K)$, and we shall obtain the conclusion that $|G| = 1$ by carrying the whole situation over a finite field. First, one has the following.

PROPOSITION. *There exists a finitely generated* **Z***-subalgebra A of K, such that, first the subalgebra $A_n(A)$ of $A_n(K)$ is G-invariant and, second, for any maximal ideal m of A, with residue field $k = A/m$, the following hold:*

(a) *The action of G on $A_n(A)/mA_n(A) \simeq A_n(k)$ is faithful.*

(b) *$A_n(k)$ is separabe over $A_n(k)^G$.*

(c) *$A_n(k)^G$ is k-isomorphic to $A_n(k)$.*

Proof. Being finitely generated over K, $A_n(K)$ is the union of its subalgebras $A_n(A)$, where A runs through the finitely generated subrings of K. Since G is finite, it follows that there exists a subring A_0 as above, such that $A_n(A_0)$ is G-stable. Up to enlarging A_0, we may assume that the elements a_i, b_i of 2.5 belong to A_0, and also that $|G|^{-1} \in A_0$. Thanks to the latter assumption, one can consider the projector $p = |G|^{-1} \sum_g g$, and this has the consequence that, for any over-ring A of A_0, one has

$$A_n(A)^G = p(A_n(A)) = p(AA_n(A_0)) = Ap(A_n(A_0)) = AA_n(A_0)^G. \qquad (*)$$

Moreover, under the same assumption, $A_n(A_0)^G$ is a finitely generated A_0-algebra, by [Mo Sm, Theorem 1]. On the other hand, by our main assumption, $A_n(K)^G$ is also a Weyl algebra, say with generators P_i, Q_i; hence there exists a finitely generated subring A of K, containing A_0, such

that the generators of $A_n(\Lambda_0)^G$ belongs to the subalgebra $\Lambda\{P_i, Q_i\}$. Taking (*) into account, one then obtains that $A_n(\Lambda)^G$ equals $\Lambda\{P_i, Q_i\}$ and is, therefore, Λ-isomorphic to $A_n(\Lambda)$.

Let now $m \in \operatorname{Max} \Lambda$ and set $k = \Lambda/m$. Then $A_n(\Lambda)/mA_n(\Lambda) \simeq A_n(k)$; also, $mA_n(\Lambda)$ is G-stable and, since $|G|^{-1} \in \Lambda$, then

$$A_n(k)^G \simeq (A_n(\Lambda)/mA_n(\Lambda))^G \simeq A_n(\Lambda)^G/mA_n(\Lambda)^G$$
$$\simeq A_n(\Lambda)/mA_n(\Lambda) \simeq A_n(k).$$

Finally, the identities $\sum_i g(\bar{a}_i)\, h(\bar{b}_i) = \delta_{g,h}$ in $A_n(k)$ give both the faithfulness of the action of G and the separability over $A_n(k)^G$.

2.7. From now on, we fix a maximal ideal m of Λ and set $k = \Lambda/m$. Then k is a finite field, say of characteristic l. Note that l is prime to $|G|$, since $|G|^{-1} \in \Lambda$. Set $A_n(k) = B$ and $A_n(k)^G = B'$ and denote by Z and Z' their respective centers. Then, one has the following.

PROPOSITION. *G acts faithfully on Z.*

Proof. Denote by $\bar{k}$ the algebraic closure of k, set $\bar{B} = B \otimes_k \bar{k}$, and define $\bar{Z}$ and $\bar{B}'$ similarly. Then $\bar{B} \simeq A_n(\bar{k})$; its center is $\bar{Z}$. The action of G extends to $\bar{B}$, and $\bar{B}^G$ equals $\overline{B'}$, hence is $\bar{k}$-isomorphic to $\bar{B}$. Now, by [Rev], $\bar{B}$ is an Azumaya algebra, of rank l^{4n} over its center $\bar{Z}$; in particular, every simple quotient algebra of $\bar{B}$ has dimension l^{4n} over $\bar{k}$, and the same is true for $\overline{B'}$, which is $\bar{k}$-isomorphic to $\bar{B}$. It follows that, for every maximal ideal J of $\bar{B}$, the inclusion $\bar{B}^G/(\bar{B}^G \cap J) \subsetneq \bar{B}/J$ is in fact an equality.

Assume now that $\sigma \in G$ acts trivially on Z, and let $\bar{\sigma} = \sigma \otimes 1$ denote its extension to $\bar{B}$. Let $J \in \operatorname{Max} \bar{B}$; since $\bar{B}$ is Azumaya, J is generated by its intersection with $\bar{Z}$ and is, therefore, $\bar{\sigma}$-stable. Hence $\bar{\sigma}$ acts on $\bar{B}/J$, and this action is trivial, since $\bar{B}/J = \bar{B}^G/(\bar{B}^G \cap J)$. Therefore, for every $b \in \bar{B}$, $b - \bar{\sigma}(b) \in J$. Since J is arbitrary and since the intersection of all maximal ideals of $\bar{B}$ is reduced to $\{0\}$, this gives $\bar{\sigma} = \mathrm{id}$. It follows that $\sigma = \mathrm{id}$; the proposition is proved.

COROLLARY. *One has $Z' = Z^G$.*

Proof. Certainly, any X-inner automorphism of B acts trivially on Z; therefore the previous proposition says that B has no such automorphism but the identity. The corollary then follows from [Mo 1, 6.17].

2.8. Combining 2.6 and 2.7, we are now able to obtain the following.

PROPOSITION. (a) *Z is separable over Z'.*

(b) *For every $m \in \operatorname{Max} Z$ of codimension 1, the orbit Gm has cardinality $|G|$.*

Proof. By Proposition 2.6(b), B is separable over B', whereas B' is separable over Z' by [Rev]. By transitivity of separability [L V–V, II.5.1.2], B is separable over Z'. Then, by [De–In, II.3.8], so is Z.

Consider now assertion (b). First, denote by F and F' the fraction fields of Z and Z'. One has $F' = F^G$ and, since G acts faithfully on Z, then $\dim_{F'} F = |G|$. As is well known, it follows from Nakayama's lemma that, for every maximal ideal m' of Z', one has

$$\dim_{Z'/m'} Z/m'Z \geqslant \dim_{F'} F = |G|. \qquad (**)$$

Now, let m be a maximal ideal of Z of codimension 1, and $m' = m \cap Z$. Then the maximal ideals of Z containing $m'Z$ are precisely the G-conjugates of m, say $m = m_1, \ldots, m_t$, where $t = |Gm|$; they have codimension 1 as well. On the other hand, since Z is separable over Z', then $Z/m'Z$ is separable over $Z'/m' = k$ by [De–In, II.1.7]. Hence, by [*loc. cit.*, II.2.4], the finite dimensional k-algebra $Z/m'Z$ has zero radical. It follows that $Z/m'Z$ is the direct product of the Z/m_i, where $1 \leqslant i \leqslant t$; hence has dimension t. Together with (**), this gives $t = |G|$. The proposition is proved.

2.9. *Completion of the proof.* We can now conclude as follows. It is well known and easy to see that Z is a polynomial algebra over k in $2n$ variables; therefore the set of maximal ideals of Z of codimension 1 is in bijection with the affine space k^{2n}. Proposition 2.8(b) then implies that $|G|$ divides $|k^{2n}|$, which is a power of l. Since, on the other hand, our construction was made so that l is prime to $|G|$, this gives $|G| = 1$. The proof of Theorem 2 is complete.

2.10. *Linear actions.* Recall the notations and hypotheses of Theorem 2; in particular, K denotes a field of characteristic zero. For the sake of completeness, we shall give a shorter proof, under the additional hypothesis that the action of G is linearizable; which means that some conjugate of G in $\operatorname{Aut}_K A_n(K)$ preserves the natural filtration of $A_n(K)$. Namely, let us prove the following.

PROPOSITION. *Let G be a finite group of K-automorphisms of $A_n(K)$; assume that the action of G is linearizable, then $K_0(A_n(K)^G) \simeq \mathbf{Z}^{\operatorname{irr}_K(G)}$, where $\operatorname{irr}_K(G)$ denotes the number of irreducible representations of G over K. In particular, if $A_n(K)^G$ is K-isomorphic to $A_n(K)$, then G is trivial.*

Proof. Set $A_n(K) = A$. Firstly, note that $K_0(A) \simeq \mathbf{Z}$ by Quillen's theorem [Qui, Section 6, Theorem 7]. Second, since conjugate subgroups have isomorphic algebras of invariants, we may assume that G itself preserves the canonical filtration of A. Then, as observed in [A–H–V, Theorem 2.1], it also follows from Quillen's theorem that $K_0(A * G) \simeq K_0(KG)$, and the latter is isomorphic to $\mathbf{Z}^{\mathrm{irr}_K(G)}$. On the other hand, since the only invertible elements of A are the nonzero scalars, which are central, then A has no nontrivial inner automorphism. Therefore, it follows from [Mo 1, 2.5–2.6] that $A * G$ and A^G are Morita equivalent; thus $K_0(A^G) \simeq K_0(A * G) \simeq \mathbf{Z}^{\mathrm{irr}_K(G)}$.

Assume now that $A^G \simeq A$. Since $K_0(A) \simeq \mathbf{Z}$, it follows $\mathrm{irr}_K(G) = 1$; hence G has only one irreducible representation over K, the trivial one. But, since KG is semisimple, the sum of all its irreducible representations is faithful; it follows that G is trivial.

REFERENCES

[A–H–V] J. ALEV, T. J. HODGES, AND J.-D. VELEZ, Fixed rings of the Weyl algebra $A_1(\mathbf{C})$, *J. Algebra* **130** (1990), 83–96.

[Bou] N. BOURBAKI, "Groupes et algèbres de Lie," Chaps. IV–VI, VII–VIII, Hermann, Paris, 1968, 1975.

[De–In] F. DEMEYER AND E. INGRAHAM, "Separable Algebras over Commutative Rings," Lect. Notes in Math., Vol. 181, Springer-Verlag, Berlin/Heidelberg/New York, 1971.

[Di–Fo] W. DICKS AND E. FORMANEK, Poincaré series and a problem of S. Montgomery, *Linear Multilinear Algebra* **12** (1982), 21–30.

[Dix] J. DIXMIER, "Algèbres Enveloppantes," Gauthier-Villars, Paris/Bruxelles/Montréal, 1974.

[Duf] M. DUFLO, Idéaux primitifs dans les algèbres enveloppantes, *Ann. of Math.* **105** (1977), 107–120.

[Jan] J. C. JANTZEN, "Einhüllende Algebren halbeinfacher Lie-Algebren," Springer-Verlag, Berlin/Heidelberg/New York, 1983.

[Kar] V. K. KARCHENKO, Algebras of invariants of free algebras, *Algebra and Logic* **17** (1978), 316–321.

[Kr–Sm] H. KRAFT AND L. SMALL, Invariant algebras and completely reducible representations, *Math. Research Letters* **1** (1994), 297–307.

[Kr–Le] G. KRAUSE AND T. LENAGAN, "Growth of Algebras and Gelfand–Kirillov Dimension," Res. Notes in Math., Vol. 116, Pitman, Boston/London, 1985.

[Mo 1] S. MONTGOMERY, "Fixed Rings of Finite Automorphisms Groups of Associative Rings," Lect. Notes in Math., Vol. 818, Springer-Verlag, Berlin/Heidelberg/New York, 1980.

[Mo 2] S. MONTGOMERY, X-inner automorphisms of filtered algebras, *Proc. Amer. Math. Soc.* **83** (1981), 263–268.

[Mo 3] S. MONTGOMERY, Prime ideals in fixed rings, *Comm. Algebra* **9** (1981), 423–449.

[Mo–Gu] S. MONTGOMERY AND R. M. GURALNICK, On invertible bimodules and automorphisms of noncommutative rings, *Trans. Amer. Math. Soc.*

[Mo–Sm] S. MONTGOMERY AND L. SMALL, Fixed rings of noetherian rings, *Bull. London Math. Soc.* **13** (1981), 33–38.

[L V V] L. Le Bruyn, M. Van den Bergh, and F. Van Oystaeyen, "Graded Orders," Birkhäuser, Boston/Basel, 1988.

[Qui] D. Quillen, Higher algebraic K-thery, *in* "Algebraic K-Theory" (H. Bass, Ed.), Lect. Notes in Math., Vol. 341, Springer-Verlag, Berlin Heidelberg/New York, 1973.

[Rev] P. Revoy, Algèbres de Weyl en caractéristique *p*, *C. R. Acad. Sci. Paris* **276** (1973), 225–228.

[Smi] P. Smith, Can the Weyl algebra be a fixed ring?, *Proc. Amer. Math. Soc.* **107** (1989), 587–589.