TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 352, Number 2, Pages 901–934
S 0002-9947(99)02369-7
Article electronically published on October 6, 1999

ON THE MODULE STRUCTURE OF FREE LIE ALGEBRAS

R. M. BRYANT AND RALPH STÖHR

Abstract. We study the free Lie algebra L over a field of non-zero characteristic p as a module for the cyclic group of order p acting on L by cyclically permuting the elements of a free generating set. Our main result is a complete decomposition of L as a direct sum of indecomposable modules.

1. Introduction and statement of results

For a group G, a field K (or, more generally, a commutative ring with identity), and a KG-module V, let $L(V)$ denote the free Lie algebra on V. For each positive integer n, let $L_n(V)$ be the homogeneous component of $L(V)$ of degree n. Then $L(V)$ and $L_n(V)$ are themselves KG-modules, and these modules have been studied intensively over the past 50 years. We mention the pioneering work of Thrall [12], Brandt [2] and Wever [14], and for an account of some of the later work we refer to [9]. Most of the results on the module structure of $L(V)$ are concerned with the case where K is a field of characteristic zero, and very little seems to be known for prime characteristic. In fact, many of the methods used in characteristic zero fail in the modular case. In a recent paper, Donkin and Erdmann [5] studied $L(V)$ as a module for $GL(V)$ over an infinite field of prime characteristic p. They obtained a formula for the multiplicities of the indecomposable components of $L_n(V)$ for values of n not divisible by p. Their results also confirm that considerable difficulties arise when p divides n. In this paper we study the case where G is the cyclic group of order p, K is an arbitrary field of characteristic p and V is a free KG-module. Let IG denote the augmentation ideal of KG. Note that IG is an indecomposable KG-module of dimension $p-1$. For a given positive integer m, and for $n \geq 1$, let

$$a(n) = -\frac{1}{n} \sum_{\substack{d \\ p|d|n}} \mu(d) m^{n/d}, \tag{1.1}$$

where the sum ranges over all divisors d of n which are multiples of p, and where μ is the Möbius function. Our main result reads as follows.

Theorem 1. *Let p be a prime, G the cyclic group of order p, K a field of characteristic p and V a free KG-module of finite dimension m. Then $L_n(V)$ is a direct sum of a free KG-module and $a(n)$ isomorphic copies of IG.*

Thus we obtain a complete decomposition of $L_n(V)$ into indecomposable KG-modules. The non-trivial part of Theorem 1 is in the case where p divides n. If $(n, p) = 1$, we have $a(n) = 0$ and thus $L_n(V)$ is a free KG-module. This is, in fact,

Received by the editors August 20, 1997.
1991 *Mathematics Subject Classification.* Primary 17B01, Secondary 20C20.

not hard to show, and will be established in Section 2 (Corollary 2.2). For $p = 2$, Theorem 1 was proved in our earlier paper [4]. An easy consequence of the theorem is the following result (derived in Section 6).

Corollary 1. *The dimension of the fixed point subspace $L_n(V)^G$ is given by*

$$\dim L_n(V)^G = \frac{1}{pn} \sum_{\substack{d\mid n\\(d,p)=1}} \mu(d)m^{n/d},$$

where the sum runs over all divisors d of n which are coprime to p.

In the case where $m = p$, the dimension formula in Corollary 1 was conjectured by Short [10]. Another consequence of Theorem 1 concerns the module structure of the free Lie ring.

Corollary 2. *Let V be a free $\mathbb{Z}G$-module of finite rank. Then the free Lie ring $L(V)$, regarded as a $\mathbb{Z}G$-module, has no non-zero direct summand upon which G acts trivially, and*

$$L(V)^G = L(V)(1 + g + \ldots + g^{p-1}),$$

where g is a generator of G.

Theorem 1 will be deduced from Theorem 2 below, which gives additional insight into the structure of the free Lie algebra on an arbitrary (not necessarily finite dimensional) free KG-module V. To state it, we need to introduce some more notation. Let $A(p)$ denote the free associative ring on free generators $x_1, x_2, \ldots , x_p$ and take the usual Lie bracket operation defined by $[a, b] = ab-ba$ for all $a, b \in A(p)$. Define a word w by

$$w = w(x_1, \ldots , x_p) = \frac{1}{p}\left(\sum_{\pi} x_{\pi(1)} \cdots x_{\pi(p)} - \sum_{\kappa}[x_1, x_{\kappa(2)}, \ldots , x_{\kappa(p)}]\right),$$

where π runs over all permutations of $\{1, 2, \ldots , p\}$, κ runs over all permutations of $\{2, \ldots , p\}$ and the terms in the second sum are left-normed Lie products. It turns out that the expression within parentheses belongs to $pA(p)$; hence $w \in A(p)$. For a KG-module V, let $A(V)$ denote the free associative algebra on V. Thus $A(V)$ is the universal enveloping algebra of $L(V)$ and, with $A(V)$ regarded as a KG-module, $L(V)$ is a submodule. For arbitrary elements $u_1, \ldots , u_p$ of $A(V)$ we may take the corresponding value $w(u_1, \ldots , u_p)$ of the word w.

Theorem 2. *Let G be the cyclic group of order p, g a generator of G, K a field of characteristic p and V a free KG-module. Then there exists a set $\mathcal{L}$ of homogeneous elements of $L(V)$ such that the elements u, ug, ug^2, $\ldots$, ug^{p-1}, for $u \in \mathcal{L}$, together with the elements*

$$w(u^{p^\alpha}, (u^{p^\alpha})g, \ldots , (u^{p^\alpha})g^{p-1})(1 - g^j), \tag{1.2}$$

for $u \in \mathcal{L}$, $\alpha \geq 0$, $1 \leq j \leq p - 1$, form a basis of $L(V)$.

The basis elements (1.2) are, as written, elements of the enveloping algebra $A(V)$, but they turn out to be elements of $L(V)$ itself. In Section 7 we obtain an explicit expression for such a basis element as an element of $L(V)$, that is, as a linear combination of Lie products of the elements $u, ug, \ldots, ug^{p-1}$.

Our approach to Theorem 2 is based on the following strategy. Write $A(V) = \bigoplus_{n\geq 0} A_n(V)$, where $A_n(V)$ is the n-th homogeneous component of $A(V)$. We introduce a Lie subalgebra L^* of $A(V)$ which is, in many ways, close to $L(V)$: for example, $L^* \cap A_n(V) = L(V) \cap A_n(V)$ for all n except $n = 1$ and $n = p$. A crucial point about L^* is that it is a free Lie algebra with a free generating set $\mathcal{W}$ which consists of homogeneous elements of degree at least 2 (as elements of $A(V)$). Furthermore G acts freely on this set $\mathcal{W}$: thus L^* is the free Lie algebra on the free KG-module with basis $\mathcal{W}$. The free generating set $\mathcal{W}$ provides L^* with a grading of its own, and, by construction, elements of degree n with respect to $\mathcal{W}$ have degree at least $2n$ with respect to the original free generating set of $A(V)$. This enables us to obtain information about the homogeneous components of $L(V)$ from homogeneous components of L^* which are of smaller degree (with respect to $\mathcal{W}$). In other words, it opens the way for an inductive proof.

In addition to the free Lie and associative algebras, some other free algebras play an important role in this paper. These are the free restricted Lie algebra, the free metabelian Lie algebra and the symmetric algebra (that is, the free commutative associative algebra). In Section 2 we assemble some facts about these free algebras which will be assumed later in the paper. Most of this material is well known and we record it without giving a particular reference (useful general references, however, are [1], [6] and [9]). Specific references are given for a few facts thought to be less familiar.

In Section 3 we examine symmetric powers of the regular module KG (in other words, the homogeneous components of the symmetric algebra on KG) and prove that certain submodules of these symmetric powers are free. In Section 4 the free metabelian Lie algebra $M(V)$ is used to obtain the structure of $L_n(V)$ in the special but seminal case where $n = p$. Since $M(V)$ is isomorphic to a quotient algebra of $L(V)$, there is a module homomorphism ν from $L_p(V)$ on to $M_p(V)$, the homogeneous component of degree p in $M(V)$. We use the word w, introduced above, to construct a right inverse of ν. Then we are able to use a direct sum decomposition of $M_p(V)$ to obtain a direct sum decomposition of $L_p(V)$.

Free restricted Lie algebras and symmetric powers are crucial components in the implementation of our proof strategy. They play a major role in Section 5, which is entirely devoted to the proof of the key technical result of this paper, Proposition 5.2. In particular, the results of Section 3 are used in this proof. In Section 6 we exploit Proposition 5.2 to carry out the proof strategy outlined above. This culminates in Theorem 6.4, from which the main results are easily deduced. With a view to further applications ([7] in particular) we also include a modification of Theorem 6.4 (namely Proposition 6.5) which refers to the Lie powers of projective modules for the normalizer of a p-cycle in the symmetric group of degree p.

We are deeply grateful to L. G. Kovács for many helpful discussions about this paper. We are also indebted to G. E. Wall for pointing out the relevance of the word w, which had an invaluable impact on our progress, and to M. R. Vaughan-Lee for helpful comments regarding the calculation in Section 7. Part of this work was carried out while the second author was visiting the Australian National University, Canberra. Financial support for this visit from the Royal Society and from the ANU is gratefully acknowledged.

2. Notation and preliminaries

Throughout this paper p will be a prime number and G will be a cyclic group of order p with generator g. Also, K will be a field of characteristic p. We shall require some notation and simple facts about Lie algebras and other algebras over both K and $\mathbb{Z}$. In order to cover both cases we temporarily work with a coefficient ring J which is an arbitrary commutative ring with identity. We shall use vector space terminology to describe J-modules, in conformity with the special case $J = K$.

Let JG be the group algebra of G over J and let V be a (right) JG-module which is free as a J-module. We write $L(V)$ for the free Lie algebra on V: thus $L(V)$ is the free Lie algebra over J with the property that $L(V)$ contains V as a subspace (that is, J-submodule) and every basis of V (that is, free generating set for V as J-module) is a free generating set of $L(V)$. The action of G on V extends uniquely to $L(V)$ subject to $L(V)$ becoming a JG-module on which the elements of G act as algebra automorphisms. For $n \geq 1$, the n-th homogeneous component $L_n(V)$ of $L(V)$ is called the n-th Lie power of V: it is the subspace of $L(V)$ spanned by all left-normed Lie products $[v_1, v_2, \ldots, v_n]$ with $v_1, \ldots, v_n \in V$, and it is a JG-submodule of $L(V)$. Thus $L(V)$ is a graded module with a direct decomposition

$$L(V) = \bigoplus_{n \geq 1} L_n(V).$$

If V has finite dimension (that is, J-rank) m, the dimension of $L_n(V)$ is given by Witt's formula:

$$\dim L_n(V) = \frac{1}{n} \sum_{d \mid n} \mu(d) m^{n/d},$$

where d ranges over all positive divisors of n and μ is the Möbius function.

In an analogous way we obtain the free associative algebra $A(V)$, the symmetric algebra (or free commutative associative algebra) $S(V)$ and the free metabelian Lie algebra $M(V)$, where $M(V)$ is identified with the quotient of $L(V)$ by its second derived subalgebra $L(V)''$. All these algebras will be regarded as graded JG-modules in the obvious way, and their homogeneous components $A_n(V)$ (for $n \geq 0$), $S_n(V)$ (for $n \geq 0$) and $M_n(V)$ (for $n \geq 1$) will be called, respectively, the n-th free associative power, n-th symmetric power and n-th free metabelian Lie power of V.

We regard $A(V)$ as a Lie algebra under the Lie bracket operation given by $[a, b] = ab - ba$ for all $a, b \in A(V)$. If $u_1, \ldots, u_n$ are (not necessarily distinct) elements of $A(V)$, then by a Lie product of $u_1, \ldots, u_n$ we mean u_1 itself in the case $n = 1$ and, inductively, for $n > 1$, any Lie product $[u, v]$, where u is a Lie product of $u_1, \ldots, u_k$ and v is a Lie product of $u_{k+1}, \ldots, u_n$ for some k with $1 \leq k < n$.

We shall frequently make use of ordered bases and ordered free generating sets. By an ordering, in this connection, we always mean a total ordering. If $\mathcal{V}$ is an ordered basis of V, then the monomials $b_1 b_2 \cdots b_n$, with $b_1, \ldots, b_n \in \mathcal{V}$, form a basis of $A_n(V)$, the monomials $b_1 b_2 \cdots b_n$, with $b_1, \ldots, b_n \in \mathcal{V}$ and $b_1 \leq b_2 \leq \ldots \leq b_n$, form a basis of $S_n(V)$, and the left-normed Lie products $[b_1, b_2, \ldots, b_n]$, with $b_1, \ldots, b_n \in \mathcal{V}$ and $b_1 > b_2 \leq b_3 \leq \ldots \leq b_n$, form a basis of $M_n(V)$ (see [1], Section 4.7, for the last result).

We note that, in the free metabelian Lie algebra $M(V)$, left-normed Lie products $[u_1, u_2, u_3, \ldots, u_k]$ with $u_1, \ldots, u_k \in M(V)$ are symmetric with respect to the entries $u_3, \ldots, u_k$. This follows immediately from the Jacobi identity and the fact that $M(V)'' = 0$.

An easy induction shows that, for $u, u_1, u_2, \dots , u_k \in A(V)$,

$$u_1u_2\cdots u_ku = uu_1u_2\cdots u_k - \sum_{i=0}^{k-1}\sum_{\omega} u_{\omega(1)}\cdots u_{\omega(i)}[u, u_{\omega(i+1)}, \dots , u_{\omega(k)}], \tag{2.1}$$

where the inner sum ranges over all permutations ω of $\{1, 2, \dots , k\}$ such that $\omega(1) < \dots < \omega(i)$ and $\omega(i + 1) < \dots < \omega(k)$.

We now take J to be our field K of characteristic p and we consider restricted Lie algebras over K (see [1], [6], [9]). We write $R(V)$ for the free restricted Lie algebra on V, regarded as a graded KG-module. Its homogeneous component $R_n(V)$ is called the n-th restricted Lie power of V. It is well known that $A(V)$ becomes a restricted Lie algebra under the Lie bracket operation together with the unary operation given by $a^{[p]} = a^p$ for all $a \in A(V)$. Then $R(V)$ can be identified with the restricted Lie subalgebra of $A(V)$ generated by V, and $L(V)$ can be identified with the Lie subalgebra generated by V. Making these identifications, we have $L(V) \subseteq R(V) \subseteq A(V)$ and $L_1(V) = R_1(V) = A_1(V) = V$. Also, $L_n(V) = A_n(V) \cap L(V)$ and $R_n(V) = A_n(V) \cap R(V)$ for all $n \geq 1$.

For all $a, b \in R(V)$ we have

$$[a, b] \in L(V), \tag{2.2}$$

and therefore $[R(V), R(V)] \subseteq L(V)$. There is an element $v(x_1, x_2)$ of the p-th homogeneous component of the free Lie algebra on x_1 and x_2 such that, for all $a, b \in A(V)$,

$$(a + b)^p = a^p + b^p + v(a, b). \tag{2.3}$$

By (2.2), if $a, b \in R(V)$ then $v(a, b) \in L(V)$.

If $\mathcal{U}$ is a subset of $A(V)$ then it is easily verified that the restricted Lie subalgebra of $A(V)$ generated by $\mathcal{U}$ is spanned by all elements which have the form v^{p^α}, where v is a Lie product of elements from $\mathcal{U}$ and α is a non-negative integer.

If $\mathcal{B}$ is a basis of $L(V)$, then the elements b^{p^α}, where $b \in \mathcal{B}$ and $\alpha \geq 0$, form a basis $\mathcal{B}^{[p]}$ of $R(V)$, and, if $\mathcal{R}$ is an ordered basis of $R(V)$, then the elements

$$b_1^{\alpha_1}b_2^{\alpha_2}\cdots b_k^{\alpha_k}, \tag{2.4}$$

where $b_1, \dots , b_k \in \mathcal{R}$, $b_1 < b_2 < \dots < b_k$, $k \geq 0$ and $\alpha_1, \dots , \alpha_k \in \{1, \dots , p - 1\}$, form a basis of $A(V)$ (see [9], page 51, or [6], Chapter 5, for the latter result). Thus any basis $\mathcal{B}$ of $L(V)$ together with an ordering of $\mathcal{B}^{[p]}$ gives rise to a basis $\mathcal{B}(A(V))$ of $A(V)$ consisting of the elements (2.4) in the case $\mathcal{R} = \mathcal{B}^{[p]}$.

By a well known theorem of Witt [15], every subalgebra of a free restricted Lie algebra is itself a free restricted Lie algebra. Let R^* be a subalgebra of $R(V)$ and let $\mathcal{U}$ be a free generating set for R^*. We can then identify R^* with $R(U)$, where U is the subspace spanned by $\mathcal{U}$. Clearly the Lie subalgebra of R^* generated by $\mathcal{U}$ is freely generated by $\mathcal{U}$ and may be identified with $L(U)$. We claim also that *the associative subalgebra of $A(V)$ generated by R^* is freely generated by $\mathcal{U}$*: thus it may be identified with $A(U)$, the free associative algebra on U. To see this, let $\mathcal{R}$ be an ordered basis of $R(V)$ chosen so that $\mathcal{R} \cap R^*$ is a basis of R^*. Since $A(U)$ is freely generated by $\mathcal{U}$, there is a homomorphism of associative algebras $\phi : A(U) \to A(V)$ which extends the inclusion map $\mathcal{U} \to A(V)$. The products in $A(U)$ which have the form (2.4) with $b_1, \dots , b_k \in \mathcal{R} \cap R^*$ form a basis of $A(U)$, and these products are mapped under ϕ to the corresponding products in $A(V)$. But the latter products form part of a basis of $A(V)$: thus ϕ is an embedding. The image of ϕ is clearly the associative subalgebra of $A(V)$ generated by R^*, and, since ϕ is an embedding, this subalgebra is freely generated by $\mathcal{U}$.

Now we return to the case of a general coefficient ring J. For a subset $\mathcal{U}$ of a G-module, we write $\mathcal{U}G$ for the set defined by

$$\mathcal{U}G = \{ug^i : u \in \mathcal{U},\, 0 \leq i \leq p-1\}.$$

Note that if V is a free JG-module, and if $\mathcal{X}$ is a free generating set of V, then $\mathcal{X}G$ is a G-free basis of V, that is, a basis of V on which G acts freely. Conversely, if $\mathcal{V}$ is a G-free basis of V, then any G-transversal $\mathcal{X}$ of $\mathcal{V}$ is a free generating set of V as a JG-module, and $\mathcal{V} = \mathcal{X}G$. Clearly, a JG-module is free if and only if it has a G-free basis.

Let V be a JG-module which is free as a J-module. Let $\mathcal{V}$ be a (fixed) basis of V, and hence a free generating set of the Lie algebra $L(V)$. By a monomial in $L(V)$ we mean a non-zero Lie product of elements of $\mathcal{V}$. Every monomial of $L(V)$ has a multidegree with respect to $\mathcal{V}$: this is the sequence which lists, for each element b of $\mathcal{V}$, the multiplicity with which b occurs in the monomial. The same applies to the algebras $A(V)$, $S(V)$ and $M(V)$. It will be convenient to label multidegrees by elements of the standard basis of $S(V)$. Let $<$ be an arbitrary ordering of $\mathcal{V}$ and denote by $\mathcal{C}_n$ the basis of $S_n(V)$ consisting of the monomials $b_1b_2\cdots b_n$ with $b_1, \ldots, b_n \in \mathcal{V}$ and $b_1 \leq b_2 \leq \ldots \leq b_n$. Clearly, the multidegrees with total degree n are in one-to-one correspondence with the elements of $\mathcal{C}_n$. For $P \in \{A, L, S, M\}$ and $c \in \mathcal{C}_n$ we let $P_{n,c}(\mathcal{V})$ denote the span in $P_n(V)$ of all monomials of multidegree c. Then it is easily verified that $P_n(V)$ is the direct sum of its subspaces $P_{n,c}(\mathcal{V})$.

Now assume that $\mathcal{V}$ is G-free. We call a monomial of $P(V)$ balanced (with respect to $\mathcal{V}$) if all the elements within each G-orbit of $\mathcal{V}$ occur with the same multiplicity; otherwise the monomial is said to be unbalanced. We write $\mathcal{C}_n^b$ for the set of all balanced elements of $\mathcal{C}_n$, and $\mathcal{C}_n^u$ for the set of all unbalanced elements of $\mathcal{C}_n$. Then we define

$$P_n^b(\mathcal{V}) = \bigoplus_{c \in \mathcal{C}_n^b} P_{n,c}(\mathcal{V}), \qquad P_n^u(\mathcal{V}) = \bigoplus_{c \in \mathcal{C}_n^u} P_{n,c}(\mathcal{V}).$$

In the case where $J = K$ we define $R_{n,c}(\mathcal{V}) = A_{n,c}(\mathcal{V}) \cap R(V)$ for each $c \in \mathcal{C}_n$. We also define $R_n^b(\mathcal{V}) = A_n^b(\mathcal{V}) \cap R(V)$ and $R_n^u(\mathcal{V}) = A_n^u(\mathcal{V}) \cap R(V)$.

Lemma 2.1. *Let V be a free JG-module and $\mathcal{V}$ a G-free basis of V. Let $P \in \{A, L, S, M, R\}$, where $P = R$ applies only in the case $J = K$. Then, for all $n \geq 1$, $P_n^b(\mathcal{V})$ and $P_n^u(\mathcal{V})$ are submodules of $P_n(V)$, and $P_n(V) = P_n^b(\mathcal{V}) \oplus P_n^u(\mathcal{V})$. Moreover, $P_n^u(\mathcal{V})$ is a free JG-module, and $P_n^b(\mathcal{V})$ has a module direct decomposition*

$$P_n^b(\mathcal{V}) = \bigoplus_{c \in \mathcal{C}_n^b} P_{n,c}(\mathcal{V}).$$

Proof. First we consider the case $P = S$, using the basis $\mathcal{C}_n$ of $S_n(V)$. It is easily verified that G acts freely on $\mathcal{C}_n^u$ and trivially on each element of $\mathcal{C}_n^b$. The result in this case follows immediately. Now let $P \in \{A, L, M, R\}$. For each c take a basis $\mathcal{B}_{n,c}$ of $P_{n,c}(\mathcal{V})$. Note that for $i = 0, 1, \ldots, p-1$ we have $P_{n,c}(\mathcal{V})g^i = P_{n,cg^i}(\mathcal{V})$. It follows that $P_n(V)$ is the direct sum of its submodules $P_n^b(\mathcal{V})$ and $P_n^u(\mathcal{V})$. Moreover, since g^i acts as an automorphism, $\mathcal{B}_{n,c}g^i$ is a basis of $P_{n,cg^i}(\mathcal{V})$. Consequently, if I_n is a G-transversal of the G-free set $\mathcal{C}_n^u$, then $\bigcup_{c \in I_n} \mathcal{B}_{n,c}G$ is a G-free basis of $P_n^u(\mathcal{V})$.

Thus $P_n^u(\mathcal{V})$ is a free JG-module. Finally, it is clear that $P_n^b(\mathcal{V})$ is the direct sum of its submodules $P_{n,c}(\mathcal{V})$ with $c \in \mathcal{C}_n^b$. □

Corollary 2.2. *Let V be a free JG-module and let $P \in \{A, L, S, M, R\}$, where $P = R$ applies only in the case $J = K$. Then $P_n(V)$ is a free JG-module for all n such that $(n,p) = 1$.*

Proof. Let $\mathcal{V}$ be a G-free basis of V. Since the degree of any balanced monomial is divisible by p, if $(n,p) = 1$ then $P_n^b(\mathcal{V}) = 0$ and hence $P_n(V) = P_n^u(\mathcal{V})$. □

Remark. In the case where $P = A$ we can do better: the free associative powers $A_n(V)$ of a free JG-module V are free JG-modules for all $n \geq 1$. Indeed, one can easily check that G acts freely on the set of all monomials of degree n.

For a free JG-module V, the module structure of the free metabelian Lie powers $M_n(V)$ is straightforward. Let $\mathcal{X}$ be an ordered free generating set for V, and write $\mathcal{V} = \mathcal{X}G$. Thus $\mathcal{V}$ is a G-free basis of V. We extend the order of $\mathcal{X}$ to $\mathcal{V}$ by setting $x < xg < \ldots < xg^{p-1}$ for all $x \in \mathcal{X}$ and by setting $xg^{p-1} < y$ for all $x, y \in \mathcal{X}$ such that $x < y$ in the order of $\mathcal{X}$. If u is an element of the derived algebra $M(V)'$ and b is a monomial of $S(V)$, where $b = b_1 \cdots b_k$ with $b_1, \ldots, b_k \in \mathcal{V}$, we write $u \circ b$ for the element $[u, b_1, \ldots, b_k]$ of $M(V)'$. (This notation reflects the fact that there is a natural way in which $M(V)'$ can be regarded as a module for $S(V)$.) As before, let $\mathcal{C}_n^b$ denote the set of all balanced monomials of degree n in $S(V)$ derived from the ordered basis $\mathcal{V}$ of V. For $n = pq$ (where $q \geq 1$), the elements of $\mathcal{C}_{pq}^b$ have the form

$$c = x_1^{q_1}(x_1g)^{q_1} \cdots (x_1g^{p-1})^{q_1} \cdots x_k^{q_k}(x_kg)^{q_k} \cdots (x_kg^{p-1})^{q_k}, \tag{2.5}$$

where $k \geq 1$, $x_1, \ldots, x_k \in \mathcal{X}$, $x_1 < x_2 < \ldots < x_k$, $q_i \geq 1$ (for $i = 1, \ldots, k$) and $q_1 + q_2 + \ldots + q_k = q$. If c is given by (2.5), and if $i \in \{1, 2, \ldots, k\}$ and $j \in \{0, 1, \ldots, p-1\}$ where $(i,j) \neq (1,0)$, it will be convenient to write $\hat{c}(i,j)$ for the element of degree $pq - 2$ obtained from c by replacing the exponents of x_1 and x_ig^j by $q_1 - 1$ and $q_i - 1$, respectively.

Lemma 2.3. *Let V, $\mathcal{X}$ and $\mathcal{V}$ be as above. Then $M_n(V)$ is a free JG-module for all n with $(n,p) = 1$, and, for $n = pq$ where $q \geq 1$, there is a module direct decomposition*

$$M_{pq}(V) = M_{pq}^f(\mathcal{V}) \oplus \bigoplus_{c \in \mathcal{C}_{pq}^b} M_{pq,c}^a(\mathcal{V}),$$

where $M_{pq}^f(\mathcal{V})$ is a free JG-module and, for all $c \in \mathcal{C}_{pq}^b$, $M_{pq,c}^a(\mathcal{V})$ is isomorphic to the augmentation ideal $J(G-1)$. Moreover, for c as in (2.5), the elements $[x_1g^j, x_1] \circ \hat{c}(1,j)$ with $1 \leq j \leq p-1$ form a basis of $M_{pq,c}^a(\mathcal{V})$.

Proof. Corollary 2.2 gives the case where $(n,p) = 1$. For $n = pq$, Lemma 2.1 tells us that $M_{pq}(V)$ is a direct sum of the free JG-module $M_{pq}^u(\mathcal{V})$ and the modules $M_{pq,c}(\mathcal{V})$, where $c \in \mathcal{C}_{pq}^b$. For c as in (2.5), $M_{pq,c}(\mathcal{V})$ has a basis consisting of the elements

$$[x_ig^j, x_1] \circ \hat{c}(i,j), \tag{2.6}$$

where $i = 1, 2, \ldots, k$, $j = 0, 1, \ldots, p-1$ and $(i,j) \neq (1,0)$. Let $M_{pq,c}^a(\mathcal{V})$ denote the span of the elements (2.6) with $i = 1$ and $j = 1, 2, \ldots, p-1$. It is easily checked that the J-space isomorphism $J(G-1) \to M_{pq,c}^a(\mathcal{V})$ given by $1 - g^j \mapsto [x_1g^j, x_1] \circ \hat{c}(1,j)$ for $j = 1, 2, \ldots, p-1$ is, in fact, a JG-module isomorphism, and that G acts freely modulo $M^a_{pq,c}(\mathcal{V})$ on the remaining basis elements (2.6). The lemma now follows. □

Remark. In the case $n = p$, the set $\mathcal{C}^b_p$ consists of the elements $x(xg)\cdots(xg^{p-1})$ where $x \in \mathcal{X}$. Hence $M^a_{p,c}(\mathcal{V}) = M_{p,c}(\mathcal{V})$ for all c. Thus $M^b_p(\mathcal{V})$ is the direct sum of the modules $M^a_{p,c}(\mathcal{V})$ and has a basis consisting of the elements

$$[xg^j, x, xg, \dots, xg^{j-1}, xg^{j+1}, \dots, xg^{p-1}], \tag{2.7}$$

for $x \in \mathcal{X}$, $j = 1, 2, \dots, p-1$. Furthermore, the complement $M^f_p(\mathcal{V})$ may be taken to be $M^u_p(\mathcal{V})$.

The elements $1, g, \dots, g^{p-1}$ of the cyclic group G form a G-free basis of the regular module KG. When working in the symmetric algebra $S(KG)$ we write g_i instead of g^i, for $i = 0, 1, \dots, p-1$. Then we identify $S(KG)$ with the polynomial algebra $K[g_0, g_1, \dots, g_{p-1}]$ and write monomials in this algebra in the form $g_0^{\alpha_0} g_1^{\alpha_1} \cdots g_{p-1}^{\alpha_{p-1}}$ (where $\alpha_0, \dots, \alpha_{p-1} \geq 0$), thus avoiding confusion with the group element $1^{\alpha_0} g^{\alpha_1} \cdots g^{(p-1)\alpha_{p-1}}$. (Note, in particular, that g_0 is not the identity element of $S(KG)$.) Similarly, when working in $S(IG)$, where IG is the augmentation ideal of KG, we write a_j instead of $1 - g^j$, for $j = 1, \dots, p-1$. The original multiplication of G should be forgotten in $S(KG)$ and $S(IG)$. All we should remember is the action of G on these algebras: namely, g acts on $S(KG)$ by $g_0 \mapsto g_1 \mapsto \dots \mapsto g_{p-1} \mapsto g_0$ and g acts on $S(IG)$ by $a_j \mapsto a_j - a_1$, for $j < p-1$, and $a_{p-1} \mapsto -a_1$. Identifying a_j with $g_0 - g_j$ for $j = 1, \dots, p-1$, we have

$$S(IG) = K[a_1, \dots, a_{p-1}] \subseteq K[g_0, \dots, g_{p-1}] = S(KG).$$

3. On symmetric powers of KG

In this section we examine certain submodules of the symmetric powers of the regular module KG.

For each positive integer r with $2 \leq r \leq p$ let V_r be the KG-module with basis $\{x_1, \dots, x_r\}$ such that $x_i g = x_i + x_{i+1}$ for $i = 1, \dots, r-1$ and $x_r g = x_r$. Note that V_p is a regular KG-module. We identify $S(V_r)$ with the polynomial algebra $K[x_1, \dots, x_r]$ in the obvious way. Thus $K[x_1, \dots, x_r]$ becomes a KG-module. For each positive integer n let $V(n, r)$ be the subspace of $K[x_1, \dots, x_r]$ spanned by the monomials $x_1^{\alpha_1} \cdots x_r^{\alpha_r}$ such that $\alpha_1 + \dots + \alpha_r = n$ and $\alpha_1 \leq p-1$. It is easily verified that $V(n, r)$ is a submodule of $K[x_1, \dots, x_r]$. Note that $V(n, r)$ is defined for all pairs (n, r) satisfying $n \geq 1$ and $2 \leq r \leq p$.

Lemma 3.1. (i) *$V(n, p)$ is a free KG-module whenever $1 \leq n \leq p-1$.*

(ii) *$V(n, 2)$ is a regular KG-module whenever $n \geq p-1$.*

(iii) *For $n \geq 2$ and $3 \leq r \leq p$, if any two of the KG-modules $V(n-1, r)$, $V(n, r-1)$ and $V(n, r)$ are free, then the third is also free.*

Proof. (i) For $1 \leq n \leq p-1$, $V(n, p) = S_n(V_p)$. Since V_p is free the result follows from Corollary 2.2.

(ii) Note that $V(n, 2)$ has dimension p because it has basis

$$\{x_2^n, x_1 x_2^{n-1}, \dots, x_1^{p-1} x_2^{n-p+1}\}.$$

Let c be the element $(1-g)^{p-1}$ of KG. To show that $V(n, 2)$ is regular it suffices to show that $V(n, 2)c \neq 0$, because this shows that $V(n, 2)$ is indecomposable. Since

$c = 1 + g + \ldots + g^{p-1}$, we have

$$(x_1^{p-1} x_2^{n-p+1})c = (x_1^{p-1})c \cdot x_2^{n-p+1}$$

$$= (x_1^{p-1} + (x_1 + x_2)^{p-1} + (x_1 + 2x_2)^{p-1} + \ldots + (x_1 + (p-1)x_2)^{p-1})x_2^{n-p+1}.$$

The coefficient of x_2^n in this expression (over our field of characteristic p) is given by

$$1^{p-1} + 2^{p-1} + \ldots + (p-1)^{p-1} = 1 + 1 + \ldots + 1 = p - 1.$$

Thus $(x_1^{p-1} x_2^{n-p+1})c \neq 0$, which gives the required result.

(iii) Let $\theta : V(n-1, r) \to V(n, r)$ be the map defined by $\theta(v) = vx_r$ for all $v \in V(n-1, r)$, and let $\phi : V(n, r) \to V(n, r-1)$ be the map induced from the homomorphism $K[x_1, \ldots, x_r] \to K[x_1, \ldots, x_{r-1}]$ in which $x_i \mapsto x_i$ for $i < r$ and $x_r \mapsto 0$. It is easily verified that

$$0 \longrightarrow V(n-1, r) \xrightarrow{\theta} V(n, r) \xrightarrow{\phi} V(n, r-1) \longrightarrow 0$$

is a short exact sequence of KG-modules. This gives the required result. □

Proposition 3.2. *$V(n, r)$ is a free KG-module whenever $n + r \geq p + 1$. In particular, $V(n, p)$ is free for all $n \geq 1$.*

Proof. Define sets of ordered pairs of positive integers by

$$\Gamma = \{(n, r) : 1 \leq n \leq p-1,\ 2 \leq r \leq p,\ n + r \geq p + 1\}$$

and $\Delta = \{(n, r) : n \geq p - 1,\ 2 \leq r \leq p\}$. Thus Γ can be thought of as the set of integral points of a triangular region in the plane, and Δ as the set of integral points of a semi-infinite horizontal strip.

We first claim that $V(n, r)$ is free for all $(n, r) \in \Gamma$. If not, then choose $(n, r) \in \Gamma$ with r maximal so that $V(n, r)$ is not free. By Lemma 3.1(i), $r < p$. Thus $(n, r+1)$ and $(n-1, r+1)$ belong to Γ. Thus, by maximality, $V(n, r+1)$ and $V(n-1, r+1)$ are free. Thus, by Lemma 3.1(iii), $V(n, r)$ is free—a contradiction.

Now we claim that $V(n, r)$ is free for all $(n, r) \in \Delta$. If not, then choose $(n, r) \in \Delta$ with $n + r$ minimal so that $V(n, r)$ is not free. By Lemma 3.1(ii), $r > 2$. By the result for Γ, $n > p - 1$. Thus $(n-1, r)$ and $(n, r-1)$ belong to Δ. Thus, by minimality, $V(n-1, r)$ and $V(n, r-1)$ are free. Thus, by Lemma 3.1(iii), $V(n, r)$ is free—a contradiction.

The result follows since $\Gamma \cup \Delta = \{(n, r) : n \geq 1,\ 2 \leq r \leq p,\ n + r \geq p + 1\}$. □

We now interpret this result in $S(KG)$. As noted above, V_p is a regular module. Indeed, there is a KG-module isomorphism from V_p to KG given by $x_1 \mapsto 1$, $x_2 \mapsto g - 1, \ldots, x_p \mapsto (g-1)^{p-1}$. (Note that $g - 1, \ldots, (g-1)^{p-1}$ span the augmentation ideal IG, which is also spanned by $1 - g,\ 1 - g^2, \ldots, 1 - g^{p-1}$.) We use the induced isomorphism from $S(V_p)$ to $S(KG)$, and in $S(KG)$ we write g_i instead of g^i and a_j instead of $1 - g^j$, as explained in Section 2. It is easy to check that, under this induced isomorphism, $V(n, p)$ is mapped to the submodule $\tilde{S}_n(KG)$ of $S_n(KG)$ which is spanned over K by all elements of the form $g_0^{\alpha_0} a_1^{\alpha_1} \cdots a_{p-1}^{\alpha_{p-1}}$, where $0 \leq \alpha_0 \leq p - 1$ and $\alpha_0 + \alpha_1 + \ldots + \alpha_{p-1} = n$.

From Proposition 3.2 we therefore obtain the following result.

Corollary 3.3. *$\tilde{S}_n(KG)$ is a free KG-module for all $n \geq 1$.*

We shall also need to use some other submodules of $S_n(KG)$. For n satisfying $0 \leq n \leq p(p-1)$, let $\hat{S}_n(KG)$ denote the span in $S_n(KG)$ of all monomials $g_0^{\alpha_0} g_1^{\alpha_1} \cdots g_{p-1}^{\alpha_{p-1}}$ where $\alpha_0+\alpha_1+\ldots+\alpha_{p-1} = n$ and $0 \leq \alpha_i \leq p-1$ for $i = 0, \ldots, p-1$. Clearly these monomials form a basis for $\hat{S}_n(KG)$. Let $\hat{S}_n^u(KG)$ denote the span of all unbalanced monomials of this kind; that is, monomials in which $\alpha_0, \alpha_1, \ldots, \alpha_{p-1}$ are not all equal. If $p \,|\, n$ let $\hat{S}_n^b(KG)$ denote the subspace spanned by the element $g_0^{\alpha} g_1^{\alpha} \cdots g_{p-1}^{\alpha}$, where $\alpha = n/p$. By arguments similar to those in Section 2 we obtain the following result.

Proposition 3.4. *Suppose* $0 \leq n \leq p(p-1)$.

(i) *If n is not divisible by p, then $\hat{S}_n(KG) = \hat{S}_n^u(KG)$, and $\hat{S}_n(KG)$ is a free KG-module.*

(ii) *If $p \,|\, n$, then $\hat{S}_n(KG) = \hat{S}_n^u(KG) \oplus \hat{S}_n^b(KG)$, where $\hat{S}_n^u(KG)$ is a free KG-module and $\hat{S}_n^b(KG)$ is a one-dimensional trivial KG-module.*

4. The p-th Lie power of a free G-module

In this section we shall initially work with integer coefficients. Let $L(p)$, $A(p)$ and $M(p)$ denote, respectively, the free Lie ring, the free associative ring and the free metabelian Lie ring on free generators $x_1, x_2, \ldots, x_p$, and identify $L(p)$ with the Lie subring of $A(p)$ generated by $x_1, \ldots, x_p$. We denote by ν the natural surjection $\nu : L(p) \to M(p)$.

Consider the element

$$\sum_{\pi} x_{\pi(1)} \cdots x_{\pi(p)} - \sum_{\kappa} [x_1, x_{\kappa(2)}, \ldots, x_{\kappa(p)}]$$

of $A(p)$, in which π and κ range over all permutations of $\{1, 2, \ldots, p\}$ and $\{2, \ldots, p\}$, respectively. It follows from [13] (Lemma 1 on page 677) that this element belongs to $pA(p)$. Thus the element defined by

$$\begin{aligned} w &= w(x_1, \ldots, x_p) \\ &= \frac{1}{p}\left(\sum_{\pi} x_{\pi(1)} \cdots x_{\pi(p)} - \sum_{\kappa} [x_1, x_{\kappa(2)}, \ldots, x_{\kappa(p)}]\right) \end{aligned} \tag{4.1}$$

is an element of $A(p)$. Note that w is symmetric in the variables $x_2, \ldots, x_p$. Let

$$\begin{aligned} \hat{w} = \hat{w}(x_1, \ldots, x_p) &= w(x_2, x_1, x_3, \ldots, x_p) - w(x_1, x_2, x_3, \ldots, x_p) \\ &= \frac{1}{p}\left(\sum_{\kappa} [x_1, x_{\kappa(2)}, \ldots, x_{\kappa(p)}] - \sum_{\lambda} [x_2, x_{\lambda(1)}, \ldots, x_{\lambda(p)}]\right), \end{aligned}$$

where the range of κ is as before and λ ranges over all permutations of $\{1, 3, \ldots, p\}$. Since $p\hat{w} \in L(p)$ and $L(p)$ is a direct summand of $A(p)$, it follows that $\hat{w} \in L(p)$; that is, $\hat{w}$ is a Lie element. However w is not a Lie element because, using the natural surjection $\delta : A(p) \to \mathbb{Z}[x_1, \ldots, x_p]$, we have

$$\delta(w) = (p-1)!\, x_1 x_2 \cdots x_p, \tag{4.2}$$

and this is a non-zero element of $\mathbb{Z}[x_1, \ldots, x_p]$.

We shall now calculate the image $\nu(\hat{w})$ in the free metabelian Lie ring $M(p)$. Recall that a left-normed Lie product $[u_1, u_2, u_3, \ldots, u_p]$ in $M(p)$ is symmetric with respect to the entries $u_3, \ldots, u_p$. Thus

$$\begin{aligned}\nu(\hat{w}) &= \frac{1}{p}\left(\sum_{\kappa}[x_1, x_{\kappa(2)}, \ldots, x_{\kappa(p)}] - \sum_{\lambda}[x_2, x_{\lambda(1)}, \ldots, x_{\lambda(p)}]\right) \\ &= \frac{(p-2)!}{p}\left([x_1, x_2, x_3, \ldots, x_p] + \sum_{i=3}^{p}[x_1, x_i, x_2, \ldots]\right. \\ &\qquad \left. - [x_2, x_1, x_3, \ldots, x_p] - \sum_{i=3}^{p}[x_2, x_i, x_1, \ldots]\right).\end{aligned}$$

But, by the Jacobi identity,

$$\begin{aligned}\sum_{i=3}^{p}[x_1, x_i, x_2, \ldots] - \sum_{i=3}^{p}[x_2, x_i, x_1, \ldots] &= \sum_{i=3}^{p}[x_1, x_2, x_i, \ldots] \\ &= (p-2)[x_1, x_2, \ldots, x_p].\end{aligned}$$

Hence

$$\nu(\hat{w}) = (p-2)![x_1, x_2, \ldots, x_p]. \tag{4.3}$$

Now suppose that the cyclic group G acts on the free generators $x_1, \ldots, x_p$ via $x_i g = x_{i+1}$ (subscripts modulo p). Then $A(p)$, $L(p)$ and $M(p)$ become $\mathbb{Z}G$-modules. Observe that $w(g-1) = \hat{w}$. Thus w has the property that, although it is not itself a Lie element, it becomes one when it is acted on by any element of the augmentation ideal of $\mathbb{Z}G$.

For any associative algebra A on which G acts by algebra automorphisms, and for any element u of A, we write $w(u)$ for the value of w at the elements of the G-orbit of u in A; that is,

$$w(u) = w(u, ug, \ldots, ug^{p-1}).$$

It follows that

$$w(u)(g-1) = \hat{w}(u, ug, \ldots, ug^{p-1}). \tag{4.4}$$

Now let V be a $\mathbb{Z}G$-module which is free as a $\mathbb{Z}$-module. We consider the $\mathbb{Z}$-algebras $L(V)$, $A(V)$, $S(V)$ and $M(V)$. It is easy to verify that there is a $\mathbb{Z}G$-module map $M_p(V) \to V \otimes S_{p-1}(V)$ such that

$$[v_1, v_2, \ldots, v_p] \mapsto v_1 \otimes (v_2 v_3 \cdots v_p) - v_2 \otimes (v_1 v_3 \cdots v_p)$$

for all $v_1, \ldots, v_p \in V$. Furthermore, there is a $\mathbb{Z}G$-module map

$$V \otimes S_{p-1}(V) \to A_p(V)$$

such that, for all $v_1, \ldots, v_p \in V$,

$$v_1 \otimes (v_2 v_3 \cdots v_p) \mapsto v_1 \left(\sum_{\kappa} v_{\kappa(2)} v_{\kappa(3)} \cdots v_{\kappa(p)}\right),$$

where κ ranges over all permutations of $\{2, 3, \ldots, p\}$. Also, there is a $\mathbb{Z}G$-module map $A_p(V) \to L_p(V)$ such that, for all $v_1, \ldots, v_p \in V$,

$$v_1 v_2 \cdots v_p \mapsto [v_1, v_2, \ldots, v_p].$$

The composite of these three maps is a $\mathbb{Z}G$-module map $M_p(V) \to L_p(V)$ such that, for all $v_1, \dots, v_p \in V$,

$$[v_1, v_2, \dots, v_p] \mapsto p\hat{w}(v_1, v_2, \dots, v_p).$$

Since $L_p(V)$ is torsion-free as a $\mathbb{Z}$-module, we finally obtain a $\mathbb{Z}G$-module homomorphism $\psi : M_p(V) \to L_p(V)$ such that

$$\psi([v_1, v_2, \dots, v_p]) = \hat{w}(v_1, v_2, \dots, v_p)$$

for all $v_1, \dots, v_p \in V$.

Remark. The definition of the homomorphism ψ does not depend upon G being cyclic of prime order. In fact, it can be defined for $\mathbb{Z}$-free modules for an arbitrary group.

Suppose that V is a free $\mathbb{Z}G$-module. Then it follows from [11] (Lemma 3.4 combined with Theorem 3.11) that $L_p(V) \cap L(V)''$ has a finite filtration with quotients which are free $\mathbb{Z}G$-modules. Hence $L_p(V) \cap L(V)''$ is itself a free $\mathbb{Z}G$-module.

We now consider algebras over K. Suppose that V is a free KG-module with a free generating set $\mathcal{X}$, and take the basis $\mathcal{V}$ defined by $\mathcal{V} = \mathcal{X}G$. The natural surjection $\nu : L_p(V) \to M_p(V)$ is a KG-module homomorphism with kernel $L_p(V) \cap L(V)''$. Since V can be obtained from a free $\mathbb{Z}G$-module by tensoring with K, while $L(V)$ is obtained in the same way from the corresponding Lie algebra over $\mathbb{Z}$, the result stated above in the integral case implies that $L_p(V) \cap L(V)''$ is a free KG-module.

By Lemma 2.3 (with $n = p$) and the remark after it, $M_p(V)$ has a direct sum decomposition

$$M_p(V) = M_p^u(\mathcal{V}) \oplus M_p^b(\mathcal{V}),$$

where $M_p^b(\mathcal{V})$ is a direct sum of isomorphic copies of IG (one for each $x \in \mathcal{X}$). Let $\varepsilon : M_p(V) \to M_p^b(\mathcal{V})$ be the projection map. Thus the kernel of the composite map $\varepsilon\nu : L_p(V) \to M_p^b(\mathcal{V})$ is an extension of $L_p(V) \cap L(V)''$ by a module isomorphic to $M_p^u(\mathcal{V})$, and hence is a free KG-module. We denote this module by $L_p^f(V)$. Clearly it is spanned by $L_p(V) \cap L(V)''$ and $L_p^u(\mathcal{V})$.

Since $L(V)$ and $M(V)$ can be obtained from the corresponding algebras over $\mathbb{Z}$ by tensoring with K, the map ψ defined above in the integral case yields a KG-module homomorphism $\psi : M_p(V) \to L_p(V)$ such that

$$\psi([v_1, v_2, \dots, v_p]) = \hat{w}(v_1, v_2, \dots, v_p)$$

for all $v_1, \dots, v_p \in V$. In view of (4.3) and the fact that $(p-2)! = 1$ in K, the composite map $\nu\psi : M_p(V) \to M_p(V)$ is the identity map. Hence the restriction $\psi : M_p^b(\mathcal{V}) \longrightarrow L_p(V)$ is a right inverse of $\varepsilon\nu$. Write $L_p^a(V) = \psi(M_p^b(\mathcal{V}))$. Then it follows that $L_p(V)$ is the direct sum of $L_p^a(V)$ and the kernel $L_p^f(V)$ of $\varepsilon\nu$. By Lemma 2.3 and the remark after it, the balanced Lie products (2.7) form a basis of $M_p^b(\mathcal{V})$. By the definitions of ψ, w and $\hat{w}$, and exploiting the symmetry of w in $x_2, \dots, x_p$, we have

$$\begin{aligned}
\psi([xg^j, x, \dots, xg^{p-1}]) &= \hat{w}(xg^j, x, \dots, xg^{p-1}) \\
&= w(x, \dots) - w(xg^j, \dots) \\
&= w(x) - w(xg^j) \\
&= w(x)(1 - g^j).
\end{aligned}$$

Since ψ is an embedding, the elements $w(x)(1-g^j)$ (for $x \in \mathcal{X}$, $1 \leq j \leq p-1$) are distinct and form a basis of $L_p^a(V)$. Thus we have proved the following result.

Proposition 4.1. *Let V be a free KG-module with free generating set $\mathcal{X}$ and basis $\mathcal{V}$, where $\mathcal{V} = \mathcal{X}G$. Then, with $L_p^f(V)$ and $L_p^a(V)$ as defined above,*

$$L_p(V) = L_p^f(V) \oplus L_p^a(V),$$

$L_p^f(V)$ is a free KG-module, and $L_p^a(V)$ is a direct sum of isomorphic copies of IG, one for each element of $\mathcal{X}$. Moreover, $L_p^f(V)$ is spanned by $L_p(V) \cap L(V)''$ and $L_p^u(\mathcal{V})$. Furthermore, the elements $w(x)(1-g^j)$, where $x \in \mathcal{X}$ and $1 \leq j \leq p-1$, are distinct and form a basis of $L_p^a(V)$.

5. The associative algebra

As before, let V be a free KG-module with free generating set $\mathcal{X}$ and basis $\mathcal{V}$, where $\mathcal{V} = \mathcal{X}G$. We write $L = L(V)$, $R = R(V)$, $A = A(V)$, $L_n = L_n(V)$, and so on. Thus, in relation to Proposition 4.1, we write $L_p^f = L_p^f(V)$ and $L_p^a = L_p^a(V)$. Note that $\mathcal{V}$ is a free generating set of each of the algebras L, R and A. For a subset $\mathcal{U}$ of a K-space, we write $\langle \mathcal{U} \rangle$ for the subspace spanned by $\mathcal{U}$.

Let $\mathcal{B}$ be a basis of L which has the form $\mathcal{B} = \bigcup_{i \geq 1} \mathcal{B}_i$, where $\mathcal{B}_i \subseteq L_i$ for each i and $\mathcal{B}_p = \mathcal{B}_p^f \cup \mathcal{B}_p^a$ with $\mathcal{B}_p^f \subseteq L_p^f$ and $\mathcal{B}_p^a \subseteq L_p^a$. Furthermore, we take $\mathcal{B}_1 = \mathcal{V}$ and

$$\mathcal{B}_p^a = \{w(x)(1-g^j) : x \in \mathcal{X},\ j = 1, \ldots, p-1\}.$$

For each $x \in \mathcal{X}$, write $g_i(x) = xg^i$ for $i = 0, 1, \ldots, p-1$ and $a_j(x) = w(x)(1-g^j)$ for $j = 1, \ldots, p-1$. These elements $g_i(x)$ and $a_j(x)$ will be called *x-factors*: the $g_i(x)$ will be called *free x-factors* and the $a_j(x)$ will be called *augmentation x-factors.* By an *$\mathcal{X}$-factor* we mean an x-factor for some $x \in \mathcal{X}$. Thus $\mathcal{B}_1$ consists of all free $\mathcal{X}$-factors and $\mathcal{B}_p^a$ consists of all augmentation $\mathcal{X}$-factors.

Let $\mathcal{R} = \mathcal{B}^{[p]}$, where $\mathcal{B}^{[p]} = \{b^{p^\alpha} : b \in \mathcal{B},\ \alpha \geq 0\}$. Thus $\mathcal{R}$ is a basis of R. We write $\mathcal{R} = \mathcal{R}^\sharp \cup \mathcal{R}^*$, where $\mathcal{R}^\sharp = \mathcal{B}_1 \cup (\mathcal{B}_p^a)^{[p]}$ and

$$\mathcal{R}^* = \mathcal{R} \setminus \mathcal{R}^\sharp = (\mathcal{B}_1^{[p]} \setminus \mathcal{B}_1) \cup \mathcal{B}_2^{[p]} \cup \ldots \cup \mathcal{B}_{p-1}^{[p]} \cup (\mathcal{B}_p^f)^{[p]} \cup \mathcal{B}_{p+1}^{[p]} \cup \ldots .$$

Thus $\mathcal{R}^\sharp$ consists of all free $\mathcal{X}$-factors and all p-power powers of augmentation $\mathcal{X}$-factors.

Note that $\langle x^p : x \in \mathcal{V} \rangle$ and L_p^f span their direct sum in R_p. Let $R_p^* = \langle x^p : x \in \mathcal{V} \rangle \oplus L_p^f$ and let R^* be the restricted Lie subalgebra of R which is generated by $L_2, \ldots, L_{p-1}, R_p^*, L_{p+1}, \ldots$.

Lemma 5.1. *The restricted Lie algebra R^* has basis $\mathcal{R}^*$.*

Proof. Clearly $\mathcal{R}^*$ generates R^*, and the elements of $\mathcal{R}^*$ are linearly independent because $\mathcal{R}^* \subseteq \mathcal{R}$. Thus it suffices to verify that the subspace $\langle \mathcal{R}^* \rangle$ is a restricted Lie algebra.

For all $d, e \in \mathcal{R}^*$ we have $[d, e] \in L$ by (2.2), and so $[d, e] \in L_n$ for some $n \geq 2$. If $n \neq p$ then $[d, e] \in \langle \mathcal{B}_n \rangle \subseteq \langle \mathcal{R}^* \rangle$. But if $n = p$ then both d and e must belong to $\mathcal{B}_2 \cup \ldots \cup \mathcal{B}_{p-1}$, and so $[d, e] \in L_p \cap L'' \subseteq L_p^f = \langle \mathcal{B}_p^f \rangle \subseteq \langle \mathcal{R}^* \rangle$. Thus $\langle \mathcal{R}^* \rangle$ is a Lie algebra.

By its definition, the set $\mathcal{R}^*$ is closed under the unary operation $u \mapsto u^p$. In view of (2.3) and the fact that $\langle \mathcal{R}^* \rangle$ is a Lie algebra, it follows that $\langle \mathcal{R}^* \rangle$ is closed under this unary operation. Hence $\langle \mathcal{R}^* \rangle$ is a restricted Lie algebra. □

Since R^* is a subalgebra of R, it is a free restricted Lie algebra, by Witt's Theorem. Let A^* be the associative subalgebra of A generated by R^*; that is, A^* is the associative subalgebra generated by $L_2, \dots, L_{p-1}, R_p^*, L_{p+1}, \dots$. As shown in Section 2 (see the paragraph after (2.4)), A^* is a free associative algebra, freely generated as associative algebra by any free generating set of R^*. For each $k \geq 0$ write $A_k^* = A^* \cap A_k$. Then it is easily verified that $A^* = A_0^* \oplus A_1^* \oplus \dots$, and A^* is a KG-submodule of A. The main result of this section is as follows.

Proposition 5.2. *For each $k \geq 1$, A_k^* is a free KG-module.*

A product $e_1 e_2 \cdots e_m$ of $\mathcal{X}$-factors $e_1, \dots, e_m$ will be called an *$\mathcal{X}$-product* if, for every free $\mathcal{X}$-factor b, the number of values of i for which $e_i = b$ does not exceed $p-1$. The *free degree* of an $\mathcal{X}$-product $e_1 \cdots e_m$ is the number of values of i for which e_i is a free $\mathcal{X}$-factor.

Let $x \in \mathcal{X}$. An $\mathcal{X}$-product $e_1 \cdots e_m$ in which each e_i is an x-factor is called an *x-product.* An *x-block* is an x-product $e_1 \cdots e_m$ such that $e_1 \leq e_2 \leq \dots \leq e_m$ in the ordering of x-factors given by

$$g_0(x) < \dots < g_{p-1}(x) < a_1(x) < \dots < a_{p-1}(x).$$

Thus every x-block has the form

$$u(x) = g_0(x)^{\alpha_0} \cdots g_{p-1}(x)^{\alpha_{p-1}} a_1(x)^{\beta_1} \cdots a_{p-1}(x)^{\beta_{p-1}}, \tag{5.1}$$

where $\alpha_0, \dots, \alpha_{p-1} \in \{0, 1, \dots, p-1\}$ and $\beta_1, \dots, \beta_{p-1} \geq 0$. Note that $\alpha_0 + \dots + \alpha_{p-1}$ is the free degree of $u(x)$, and this is bounded above by $p(p-1)$.

We next define an ordering on the whole of $\mathcal{R}$. In this ordering every element of $\mathcal{R}^\sharp$ is taken to precede every element of $\mathcal{R}^*$, while $\mathcal{R}^*$ is ordered arbitrarily and $\mathcal{R}^\sharp$ is ordered as follows. For each $x \in \mathcal{X}$ the powers of x-factors which lie in $\mathcal{R}^\sharp$ are ordered by

$$\begin{aligned} g_0(x) < \dots < g_{p-1}(x) < a_1(x) < a_1(x)^p < \dots < a_2(x) < a_2(x)^p \\ < \dots < a_{p-1}(x) < a_{p-1}(x)^p < \dots . \end{aligned}$$

Then we order $\mathcal{X}$ arbitrarily and complete the definition of the ordering by taking all powers of x-factors lying in $\mathcal{R}^\sharp$ to precede all powers of y-factors lying in $\mathcal{R}^\sharp$ whenever $x, y \in \mathcal{X}$ and $x < y$.

Since $\mathcal{R}$ is a basis of R it follows (see Section 2) that A has a basis $\mathcal{B}(A)$ consisting of all products of the form

$$c_1^{\alpha_1} c_2^{\alpha_2} \cdots c_n^{\alpha_n}, \tag{5.2}$$

where $c_1, \dots, c_n \in \mathcal{R}$, $c_1 < \dots < c_n$ and $\alpha_1, \dots, \alpha_n \in \{1, \dots, p-1\}$. (The empty product, with $n = 0$, is allowed.) Let $\mathcal{B}(A^*)$ be the subset of $\mathcal{B}(A)$ consisting of all products (5.2) in which $c_1, \dots, c_n \in \mathcal{R}^*$. By Lemma 5.1, $\mathcal{R}^*$ is a basis of R^*. Since A^* is the free associative algebra freely generated by a free generating set of R^*, $\mathcal{B}(A^*)$ is a basis of A^*. It is easily verified from the definitions made above that $\mathcal{B}(A)$ consists of all elements which can be written in the form

$$v = u(x_1) u(x_2) \cdots u(x_n) z, \tag{5.3}$$

where $x_1, \dots, x_n \in \mathcal{X}$, $x_1 < \dots < x_n$, $u(x_i)$ is an x_i-block for $i = 1, \dots, n$, and $z \in \mathcal{B}(A^*)$.

Note that, for each non-negative integer k, the elements of $\mathcal{B}(A)$ which have degree k form a basis of A_k and the elements of $\mathcal{B}(A^*)$ which have degree k form a basis of A_k^*. Recall from Section 2 the definition of a Lie product of elements $u_1, \dots, u_n$ of A.

Lemma 5.3. *Let v be a Lie product of $\mathcal{X}$-factors $e_1, \dots, e_n$, where $n \geq 2$. If $v \notin A^*$ then $n = p$, $\{e_1, \dots, e_p\} = \{g_0(x), \dots, g_{p-1}(x)\}$ for some $x \in \mathcal{X}$, and v may be written as a linear combination of $a_1(x), \dots, a_{p-1}(x)$ together with elements of A_p^* which are Lie products of elements in $\{g_0(x), \dots, g_{p-1}(x)\}$.*

Proof. Suppose $v \notin A^*$. Clearly $v \in L_m$ for some $m \geq 2$. But $L_m \subseteq A^*$ for all $m \geq 2$ except $m = p$. Thus $v \in L_p$. Hence each e_i is a free $\mathcal{X}$-factor, and $n = p$. All unbalanced monomials of degree p belong to L_p^f, by Proposition 4.1, and $L_p^f \subseteq A^*$. Thus v is balanced. Hence $\{e_1, \dots, e_p\} = \{g_0(x), \dots, g_{p-1}(x)\}$ for some $x \in \mathcal{X}$. By Proposition 4.1 applied to the subalgebra L_x of L generated by $\{e_1, \dots, e_p\}$ we see that v is a linear combination of $a_1(x), \dots, a_{p-1}(x)$ together with elements of $L_p^f \cap L_x$. This gives the result. □

For $l = 0, 1, \dots, k$, where $k \geq 1$, let $A_{k,l}$ denote the span in A_k of all basis elements (5.3) of degree k such that $\deg(z) \geq l$. Clearly

$$A_k^* = A_{k,k} \leq A_{k,k-1} \leq \dots \leq A_{k,1} \leq A_{k,0} = A_k.$$

We shall now prove that each $A_{k,l}$ is a submodule of A_k (by submodule we always mean KG-submodule).

Lemma 5.4. (i) *Let v be an $\mathcal{X}$-product and let z be an element of $\mathcal{B}(A^*)$ such that $\deg(vz) = k$ and $\deg(z) \geq l$. Then $vz \in A_{k,l}$.*

(ii) *$A_{k,l}$ is a submodule of A_k.*

Proof. (i) Write $v = e_1 \cdots e_m$, where each e_i is an $\mathcal{X}$-factor. There is a permutation π of $\{1, \dots, m\}$ such that $e_{\pi(1)} \cdots e_{\pi(m)} z$ has the form (5.3) and so belongs to $A_{k,l}$. Thus we may assume that $m \geq 2$ and, by a suitable induction, it suffices to prove that the element $e_1 \cdots e_{s-1}[e_s, e_{s+1}]e_{s+2} \cdots e_m z$ belongs to $A_{k,l}$ when $1 \leq s < m$. Using the identity (2.1), we can write this element as a linear combination of elements of the form $e_1 \cdots e_{s-1} b_s \cdots b_t c z$, where $(b_s, \dots, b_t)$ is a subsequence of $(e_{s+2}, \dots, e_m)$ and c is a Lie product of e_s, e_{s+1} and elements of $\{e_{s+2}, \dots, e_m\}$. By Lemma 5.3, each such c is a linear combination of augmentation $\mathcal{X}$-factors and elements of A^*. It follows that $e_1 \cdots e_{s-1}[e_s, e_{s+1}]e_{s+2} \cdots e_m z$ is a linear combination of elements of degree k of the form $v'z'$, where v' is an $\mathcal{X}$-product with fewer than m factors, $z' \in \mathcal{B}(A^*)$, and $\deg(z') \geq l$. The result follows by induction on m.

(ii) Consider a basis element (5.3) of degree k such that $\deg(z) \geq l$. It suffices to show that

$$(u(x_1)g) \cdots (u(x_n)g)(zg) \in A_{k,l}.$$

Note that the action of g permutes the free x_i-factors for each i, and that if b is an augmentation x_i-factor then bg is a linear combination of augmentation x_i-factors. It follows easily that $(u(x_1)g) \cdots (u(x_n)g)$ is a linear combination of $\mathcal{X}$-products of the same degree as $u(x_1) \cdots u(x_n)$. Also, zg is a linear combination of elements of $\mathcal{B}(A^*)$ of the same degree as z. Thus $(u(x_1)g) \cdots (u(x_n)g)(zg)$ is a linear combination of elements which belong to $A_{k,l}$ by (i). The result follows. □

For $x \in \mathcal{X}$ we write $P(x)$ for the subspace of A spanned by all x-products (including the empty product 1). For each $k \geq 1$ we write $P_k(x)$ for the subspace spanned by all x-products of degree k, and $B_k(x)$ for the subspace spanned by all

x-blocks of degree k. We write $A^*(x)$ for the subspace of A^* spanned by all elements of A^* which are Lie products of $\mathcal{X}$-factors at least one of which is an x-factor. Note that $A^*(x) \subseteq A_1^* \oplus A_2^* \oplus \dots$.

Lemma 5.5. (i) *For $k \geq 1$ and $x \in \mathcal{X}$,*

$$P_k(x) \subseteq B_k(x) + P(x)A^*(x).$$

(ii) *For $x, y \in \mathcal{X}$ with $x \neq y$,*

$$A^*(x)P(y) \subseteq P(y)A^*(x).$$

Proof. (i) Let $e_1 \cdots e_m$ be an x-product of degree k (where each e_i is an x-factor). There is a permutation π of $\{1, \dots, m\}$ such that $e_{\pi(1)} \cdots e_{\pi(m)} \in B_k(x)$. Thus we may assume that $m \geq 2$ and, by a suitable induction, it suffices to prove that

$$e_1 \cdots e_{s-1}[e_s, e_{s+1}]e_{s+2} \cdots e_m \in B_k(x) + P(x)A^*(x)$$

when $1 \leq s < m$. By the argument used in the proof of Lemma 5.4, the element $e_1 \cdots e_{s-1}[e_s, e_{s+1}]e_{s+2} \cdots e_m$ is a linear combination of elements of degree k of the form $e_1 \cdots e_{s-1}b_s \cdots b_t c$, where $(b_s, \dots, b_t)$ is a subsequence of $(e_{s+2}, \dots, e_m)$ and c is a linear combination of augmentation x-factors and elements of $A^*(x)$. The result follows by induction on m.

(ii) Let u be one of the Lie products spanning $A^*(x)$, according to its definition above, and let $e_1 \cdots e_m$ be a y-product (of y-factors $e_1, \dots, e_m$). By (2.1), we can write $ue_1 \cdots e_m = e_1 \cdots e_m u + v$, where v is a linear combination of elements of the form $b_1 \cdots b_t c$, where $(b_1, \dots, b_t)$ is a subsequence of $(e_1, \dots, e_m)$, and where c is a Lie product of u and one or more elements of $\{e_1, \dots, e_m\}$. Since c can be written as a Lie product of $\mathcal{X}$-factors including both an x-factor and a y-factor, Lemma 5.3 gives $c \in A^*$. Hence $c \in A^*(x)$, and the result follows. □

It is clear that, for $l < k$, $A_{k,l}/A_{k,l+1}$ has a basis consisting of all elements of the form $v + A_{k,l+1}$, where v is as in (5.3) with $\deg(v) = k$ and $\deg(z) = l$. Suppose that $k_1, \dots, k_n$ are positive integers such that $k_1 + \dots + k_n = k - l$. Let $x_1, \dots, x_n \in \mathcal{X}$ with $x_1 < \dots < x_n$. We write $V(l)^{k_1,\dots,k_n}_{x_1,\dots,x_n}$ for the subspace of $A_{k,l}/A_{k,l+1}$ spanned by all those basis elements $u(x_1) \cdots u(x_n)z + A_{k,l+1}$ of $A_{k,l}/A_{k,l+1}$, where $\deg(u(x_i)) = k_i$ for $i = 1, \dots, n$ and $\deg(z) = l$. Then, clearly, $A_{k,l}/A_{k,l+1}$ is the direct sum of the subspaces $V(l)^{k_1,\dots,k_n}_{x_1,\dots,x_n}$, where the sum is taken over all choices of $x_1, \dots, x_n, k_1, \dots, k_n$ satisfying the given conditions. We shall aim to prove that these subspaces are submodules of $A_{k,l}/A_{k,l+1}$ and that they are free KG-modules.

Lemma 5.6. *Each $V(l)^{k_1,\dots,k_n}_{x_1,\dots,x_n}$ is a submodule of $A_{k,l}/A_{k,l+1}$ and, as KG-modules,*

$$V(l)^{k_1,\dots,k_n}_{x_1,\dots,x_n} \cong V(0)^{k_1}_{x_1} \otimes \cdots \otimes V(0)^{k_n}_{x_n} \otimes A_l^*.$$

Proof. As stated above, $V(l)^{k_1,\dots,k_n}_{x_1,\dots,x_n}$ has a basis consisting of the elements $u(x_1) \cdots u(x_n)z + A_{k,l+1}$ with $\deg(u(x_i)) = k_i$ and $\deg(z) = l$. The tensor product in the statement of the lemma has a basis consisting of corresponding elements

$$(u(x_1) + A_{k_1,1}) \otimes \cdots \otimes (u(x_n) + A_{k_n,1}) \otimes z.$$

Let θ be the vector space isomorphism from $V(l)^{k_1,\dots,k_n}_{x_1,\dots,x_n}$ to the tensor product which maps basis element to corresponding basis element.

For $i = 1, \dots , n$, $u(x_i)g$ is a linear combination of x_i-products of degree k_i, and so, by Lemma 5.5(i), we can write $u(x_i)g = b_i + c_i$ where $b_i \in B_{k_i}(x_i)$ and $c_i \in P(x_i)A^*(x_i)$. Hence

$$(u(x_1) \cdots u(x_n)z)g = b_1 \cdots b_n(zg) + v,$$

where v is a linear combination of elements of the form $d_1 \cdots d_n(zg)$, where, for each i, $d_i \in B_{k_i}(x_i)$ or $d_i \in P(x_i)A^*(x_i)$, and where $d_i \in P(x_i)A^*(x_i)$ for at least one value of i. Recall that $A^*(x_i) \subseteq A^*_1 \oplus A^*_2 \oplus \dots$. By repeated use of Lemma 5.5(ii) we get

$$d_1 \cdots d_n(zg) \in P(x_1) \cdots P(x_n)(A^*_1 \oplus A^*_2 \oplus \dots)(zg).$$

Thus

$$v \in P(x_1) \cdots P(x_n)(A^*_{l+1} \oplus A^*_{l+2} \oplus \dots).$$

Since v has degree k it follows that v is a linear combination of elements of degree k of the form $v'z'$ where v' is an $\mathcal{X}$-product, $z' \in \mathcal{B}(A^*)$ and $\deg(z') \geq l + 1$. Thus, by Lemma 5.4, $v \in A_{k,l+1}$. Therefore

$$(u(x_1) \cdots u(x_n)z)g + A_{k,l+1} = b_1 \cdots b_n(zg) + A_{k,l+1}.$$

It follows that $V(l)^{k_1,\dots,k_n}_{x_1,\dots,x_n}$ is a submodule of $A_{k,l}/A_{k,l+1}$.

A similar result holds for each $V(0)^{k_i}_{x_i}$, and we have

$$u(x_i)g + A_{k_i,1} = b_i + A_{k_i,1}.$$

Hence

$$\begin{aligned}\theta((u(x_1) \cdots u(x_n)z + A_{k,l+1})g) &= (b_1 + A_{k_1,1}) \otimes \cdots \otimes (b_n + A_{k_n,1}) \otimes zg \\ &= (u(x_1) + A_{k_1,1})g \otimes \cdots \otimes (u(x_n) + A_{k_n,1})g \otimes zg \\ &= (\theta(u(x_1) \cdots u(x_n)z + A_{k,l+1}))g.\end{aligned}$$

Thus θ is a module isomorphism. □

Note that, for each $x \in \mathcal{X}$ and $k \geq 1$, $V(0)^k_x$ is a submodule of $A_k/A_{k,1}$. Our main task now will be the proof of the following result.

Proposition 5.7. *For $x \in \mathcal{X}$ and $k \geq 1$, $V(0)^k_x$ is a free KG-module.*

Before starting on the proof we show that this result yields Proposition 5.2, the main result of this section.

Suppose, then, that Proposition 5.7 has been proved. By Lemma 5.6 it follows that each module $V(l)^{k_1,\dots,k_n}_{x_1,\dots,x_n}$ is free. Since $A_{k,l}/A_{k,l+1}$ is a direct sum of modules of this sort, it also is free. This holds for $l = 0, \dots , k - 1$, and so $A_{k,0}/A_{k,k}$ is free. But $A_{k,0} = A_k$ and $A_{k,k} = A^*_k$. Since A_k is free for all $k \geq 1$ (see the remark after Corollary 2.2) it follows that A^*_k is free for all $k \geq 1$. This gives Proposition 5.2.

The rest of this section will be devoted to the proof of Proposition 5.7. We make use of the modules $\tilde{S}_n(KG)$, $\hat{S}_n(KG)$ and $\hat{S}^u_n(KG)$ considered in Section 3.

We fix $x \in \mathcal{X}$ and $k \geq 1$, and write $V(0)^k_x = X/A_{k,1}$, where $A_{k,1} \leq X \leq A_k$. Thus $X/A_{k,1}$ has a basis consisting of all elements $u + A_{k,1}$, where u is an x-block of degree k.

Write $k = qp + r$, where $0 \leq r < p$. Then any x-block of degree k can be written in the form

$$u = g_0(x)^{\alpha_0} \cdots g_{p-1}(x)^{\alpha_{p-1}} a_1(x)^{\beta_1} \cdots a_{p-1}(x)^{\beta_{p-1}}, \tag{5.4}$$

where $\alpha_0, \dots, \alpha_{p-1} \in \{0, 1, \dots, p-1\}$ and

$$\alpha_0 + \dots + \alpha_{p-1} + p(\beta_1 + \dots + \beta_{p-1}) = k = qp + r.$$

Recall that $\alpha_0 + \dots + \alpha_{p-1}$ is the free degree of u. This free degree cannot exceed $p(p-1)$. Therefore it takes one of the values $r, p+r, \dots, lp+r$, where $l = \min(q, [p-1-(r/p)])$.

Every x-product of degree k is obtained by permuting the factors of an x-block of degree k, so its free degree also takes one of the values $jp+r$ for $j = 0, 1, \dots, l$.

For $j = 0, 1, \dots, l$, let X_j be the subspace of X spanned by $A_{k,1}$ together with all x-blocks of degree k and free degree not exceeding $jp+r$. Also, put $X_{-1} = A_{k,1}$. Thus

$$A_{k,1} = X_{-1} \leq X_0 \leq \dots \leq X_l = X. \tag{5.5}$$

Note that, for $j = 0, \dots, l$, X_j/X_{j-1} has a basis consisting of all elements $u + X_{j-1}$ where u is an x-block of degree k and free degree $jp+r$.

Lemma 5.8. *Let $j \in \{0, 1, \dots, l\}$.*

(i) *The subspace X_j contains every x-product of degree k and free degree $jp+r$.*

(ii) *Let $e_1 \cdots e_m$ be an x-product of degree k and free degree $jp+r$ (where each e_i is an x-factor). Suppose $m \geq 2$ and $1 \leq s < m$. Then*

$$e_1 \cdots e_{s-1} e_s e_{s+1} e_{s+2} \cdots e_m + X_{j-1} = e_1 \cdots e_{s-1} e_{s+1} e_s e_{s+2} \cdots e_m + X_{j-1}.$$

Furthermore, if e_s or e_{s+1} is an augmentation factor, then

$$e_1 \cdots e_{s-1} e_s e_{s+1} e_{s+2} \cdots e_m + A_{k,1} = e_1 \cdots e_{s-1} e_{s+1} e_s e_{s+2} \cdots e_m + A_{k,1}.$$

Proof. (i) Every x-product of degree k and free degree $jp+r$ can be obtained by permuting the factors of an x-block of degree k and free degree $jp+r$. The latter belongs to X_j. Thus (i) follows from (ii).

(ii) It suffices to show that the element $e_1 \cdots e_{s-1}[e_s, e_{s+1}]e_{s+2} \cdots e_m$ belongs to X_{j-1}, and that if e_s or e_{s+1} is an augmentation factor then this element belongs to $A_{k,1}$. As in the proofs of Lemmas 5.4 and 5.5, $e_1 \cdots e_{s-1}[e_s, e_{s+1}]e_{s+2} \cdots e_m$ is a linear combination of elements of the form $e_1 \cdots e_{s-1} b_s \cdots b_t c$, where $(b_s, \dots, b_t)$ is a subsequence of $(e_{s+2}, \dots, e_m)$ and c is a Lie product of e_s, e_{s+1} and elements of $\{e_{s+2}, \dots, e_m\}$. By Lemma 5.3, c is a linear combination of augmentation x-factors and elements of $A^*(x)$. In the special case where e_s or e_{s+1} is an augmentation factor, Lemma 5.3 shows that $c \in A^*(x)$. In this special case we get

$$e_1 \cdots e_{s-1}[e_s, e_{s+1}]e_{s+2} \cdots e_m \in A_{k,1},$$

by Lemma 5.4(i). In the general case, $e_1 \cdots e_{s-1}[e_s, e_{s+1}]e_{s+2} \cdots e_m$ is a linear combination of elements of $A_{k,1}$ and x-products of degree k and free degree smaller than $jp+r$. The result therefore follows by induction on j. □

Note that Lemma 5.8 shows, roughly speaking, that the x-factors commute in X_j/X_{j-1}.

Lemma 5.9. *For $j = 0, 1, \dots, l$, X_j is a submodule of X and there is a KG-module isomorphism*

$$X_j/X_{j-1} \cong \hat{S}_{jp+r}(KG) \otimes S_{q-j}(IG).$$

Proof. Since $X_{-1} = A_{k,1}$, we may use induction on j and assume that X_{j-1} is a submodule of X.

There is a vector space isomorphism χ from X_j/X_{j-1} to $\hat{S}_{jp+r}(KG) \otimes S_{q-j}(IG)$ given on each basis element $u + X_{j-1}$, where

$$u = g_0(x)^{\alpha_0} \cdots g_{p-1}(x)^{\alpha_{p-1}} a_1(x)^{\beta_1} \cdots a_{p-1}(x)^{\beta_{p-1}},$$

by

$$\chi(u + X_{j-1}) = g_0^{\alpha_0} \cdots g_{p-1}^{\alpha_{p-1}} \otimes a_1^{\beta_1} \cdots a_{p-1}^{\beta_{p-1}}.$$

Recall that when working in $S(KG)$ and $S(IG)$ we write g_i instead of g^i and a_i instead of $1 - g^i$. Note that the map $g_i(x) \mapsto g^i$ (for $i = 0, \ldots, p-1$) extends to a KG-module isomorphism from $\langle g_0(x), \ldots, g_{p-1}(x) \rangle$ to KG, while the map $a_i(x) \mapsto 1 - g^i$ (for $i = 1, \ldots, p-1$) extends to a KG-module isomorphism from $\langle a_1(x), \ldots, a_{p-1}(x) \rangle$ to IG. With u as above, we have

$$(\chi(u + X_{j-1}))g \in \hat{S}_{jp+r}(KG) \otimes S_{q-j}(IG),$$

since the tensor product is a KG-module. Using Lemma 5.8 and the KG-module isomorphisms with KG and IG described above, we calculate that

$$\chi^{-1}((\chi(u + X_{j-1}))g) = ug + X_{j-1}. \tag{5.6}$$

We deduce that $ug \in X_j$. Since X_{j-1} is a submodule of X it follows that X_j is a submodule of X. Furthermore, equation (5.6) shows that χ is a KG-module isomorphism. □

We can now prove Proposition 5.7 in the case where $r \neq 0$.

Lemma 5.10. *Let $k = qp + r$, where $0 \leq r < p$. If $r \neq 0$, then $V(0)_x^k$ is a free KG-module.*

Proof. Suppose that $r \neq 0$. Then the modules $\hat{S}_{jp+r}(KG)$ are free modules, by Proposition 3.4. Hence, by Lemma 5.9, each module X_j/X_{j-1} is free. Thus, in view of (5.5), $X/A_{k,1}$ is free; that is, $V(0)_x^k$ is free. □

So, from now on, we assume that $r = 0$. Since the modules $\hat{S}_{jp}(KG)$ are not free—see Proposition 3.4—the method of Lemma 5.10 fails in this case.

Because $r = 0$ we have $k = qp$. The free degree of an x-block of degree k takes one of the values $0, p, \ldots, lp$, where $l = \min(q, p-1)$.

Let $\mathcal{E}$ be the set of all x-blocks of degree k. Thus $\{u + A_{k,1} : u \in \mathcal{E}\}$ is a basis of $X/A_{k,1}$. An element u of $\mathcal{E}$ will be said to be *balanced* if it has the form

$$u = g_0(x)^j g_1(x)^j \cdots g_{p-1}(x)^j a_1(x)^{\beta_1} \cdots a_{p-1}(x)^{\beta_{p-1}} \tag{5.7}$$

for some $j \in \{0, 1, \ldots, l\}$. Note that the element (5.7) belongs to X_j.

Let $\mathcal{E}_0$ be the set of balanced elements of $\mathcal{E}$, and let $\mathcal{E}_1 = \mathcal{E} \setminus \mathcal{E}_0$. For $u \in \mathcal{E}_0$ as in (5.7), write

$$\overline{u} = w(x)^j a_1(x)^{\beta_1} \cdots a_{p-1}(x)^{\beta_{p-1}}. \tag{5.8}$$

From the definitions of $w(x)$ and w it follows that $w(x)^j$ can be written as a linear combination of terms of the form $g_{i_1}(x) \cdots g_{i_{jp}}(x)$ with each of $g_0(x), \ldots, g_{p-1}(x)$ occurring exactly j times as a factor. But, by Lemma 5.8,

$$g_{i_1}(x) \cdots g_{i_{jp}}(x) a_1(x)^{\beta_1} \cdots a_{p-1}(x)^{\beta_{p-1}} + X_{j-1} = u + X_{j-1}.$$

Thus $\overline{u}+X_{j-1}$ is a scalar multiple of $u+X_{j-1}$. Calculating as in (4.2) and noting that $(p-1)!=-1$ in K, we see that $\overline{u}+X_{j-1}=(-1)^j u+X_{j-1}$. Let $\overline{\mathcal{E}}_0=\{\overline{u}:u\in\mathcal{E}_0\}$. Then it follows by a simple induction on j that

$$\{v+A_{k,1}:v\in\overline{\mathcal{E}}_0\cup\mathcal{E}_1\}$$

is a basis of $X/A_{k,1}$. Let $\overline{X}$ be the subspace of X such that $A_{k,1}\leq\overline{X}\leq X$ and $\overline{X}/A_{k,1}$ has basis $\{\overline{u}+A_{k,1}:\overline{u}\in\overline{\mathcal{E}}_0\}$.

Lemma 5.11. *Let $e_1,\dots,e_m\in\{w(x),a_1(x),\dots,a_{p-1}(x)\}$, where $e_1\cdots e_m$ has degree k and where there are at most l values of i for which $e_i=w(x)$.*

(i) *$e_1\cdots e_m\in\overline{X}$.*

(ii) *If $m\geq 2$ and $1\leq s<m$, then*

$$e_1\cdots e_{s-1}e_se_{s+1}e_{s+2}\cdots e_m+A_{k,1}=e_1\cdots e_{s-1}e_{s+1}e_se_{s+2}\cdots e_m+A_{k,1}.$$

Proof. (i) Since $e_1\cdots e_m$ can be obtained by permuting the factors of an element of $\overline{X}$, (i) follows from (ii).

(ii) If $e_s=e_{s+1}=w(x)$, the result is trivial. Thus, without loss of generality, we may assume that $e_s\in\{a_1(x),\dots,a_{p-1}(x)\}$. We rewrite each e_i with $e_i=w(x)$ according to its definition as a linear combination of terms of the form $g_{\pi(0)}(x)\cdots g_{\pi(p-1)}(x)$, where π is a permutation of $\{0,\dots,p-1\}$. Since $w(x)$ occurs with multiplicity at most l (and since $l\leq p-1$), this rewriting process applied to $e_1\cdots e_{s-1}e_se_{s+1}e_{s+2}\cdots e_m$ gives a linear combination of x-products of degree k. The same process applied to $e_1\cdots e_{s-1}e_{s+1}e_se_{s+2}\cdots e_m$ gives a linear combination of x-products which differ from the x-products for $e_1\cdots e_{s-1}e_se_{s+1}e_{s+2}\cdots e_m$ only in the position occupied by e_s. Since e_s is an augmentation factor, Lemma 5.8 shows that e_s may be repositioned in the x-products without affecting their values modulo $A_{k,1}$. The result therefore follows. □

Note that Lemma 5.11 shows, roughly speaking, that the factors $w(x)$, $a_1(x)$, $\dots$, $a_{p-1}(x)$ commute in $\overline{X}/A_{k,1}$.

Lemma 5.12. *$\overline{X}$ is a submodule of X, and $\overline{X}/A_{k,1}\cong\tilde{S}_q(KG)$.*

Proof. Note that, if $\overline{u}$ is as in (5.8), then $j,\beta_1,\dots,\beta_{p-1}$ satisfy the conditions $j+\beta_1+\ldots+\beta_{p-1}=q$ and $0\leq j\leq l=\min(q,p-1)$. These conditions are equivalent to $j+\beta_1+\ldots+\beta_{p-1}=q$ and $0\leq j\leq p-1$. Thus there is a vector space isomorphism ξ from $\overline{X}/A_{k,1}$ to $\tilde{S}_q(KG)$ given on each basis element $\overline{u}+A_{k,1}$, where

$$\overline{u}=w(x)^ja_1(x)^{\beta_1}\cdots a_{p-1}(x)^{\beta_{p-1}},$$

by

$$\xi(\overline{u}+A_{k,1})=g_0^ja_1^{\beta_1}\cdots a_{p-1}^{\beta_{p-1}}.$$

Since $a_i(x)=w(x)(1-g^i)$, the map $w(x)\mapsto 1$, $a_i(x)\mapsto 1-g^i$ for $i=1,\dots,p-1$, extends to a KG-module isomorphism from $\langle w(x),a_1(x),\dots,a_{p-1}(x)\rangle$ to KG. With $\overline{u}$ as above, $(\xi(\overline{u}+A_{k,1}))g$ belongs to $\tilde{S}_q(KG)$ because $\tilde{S}_q(KG)$ is a KG-module. Using Lemma 5.11 and the KG-module isomorphism with KG described above, we calculate that

$$\xi^{-1}((\xi(\overline{u}+A_{k,1}))g)=\overline{u}g+A_{k,1}.$$

Hence $\overline{u}g\in\overline{X}$, $\overline{X}$ is a submodule of X, and ξ is a KG-module isomorphism. □

We can now prove Proposition 5.7 in the remaining case, where $r = 0$.

Lemma 5.13. *Suppose that k is divisible by p and let $k = qp$. Then $V(0)^k_x$ is a free KG-module.*

Proof. Consider the chain of submodules

$$A_{k,1} \le \overline{X} = X_{-1} + \overline{X} \le X_0 + \overline{X} \le \ldots \le X_l + \overline{X} = X.$$

We wish to show that $X/A_{k,1}$ is free. By Lemma 5.12 and Corollary 3.3, $\overline{X}/A_{k,1}$ is free. Thus it suffices to show that $(X_j + \overline{X})/(X_{j-1} + \overline{X})$ is free for $j = 0, 1, \ldots, l$. It is easily verified that $(X_j + \overline{X})/(X_{j-1} + \overline{X})$ has a basis consisting of all elements of the form $u + (X_{j-1} + \overline{X})$, where $u \in \mathcal{E}_1$ and the free degree of u is jp. By the argument used in the proof of Lemma 5.9 we find that

$$(X_j + \overline{X})/(X_{j-1} + \overline{X}) \cong \hat{S}^u_{jp}(KG) \otimes S_{q-j}(IG).$$

But $\hat{S}^u_{jp}(KG)$ is free, by Proposition 3.4. Therefore $(X_j + \overline{X})/(X_{j-1} + \overline{X})$ is free, as required. □

6. Main results

We continue to use the notation of Section 5. In what follows we make use of various gradings of the free algebra A and its submodules. For most of the results it would be sufficient to use the natural grading by multidegree (with respect to a free generating set) as introduced in the paragraphs preceding Lemma 2.1 in Section 2. However, for Proposition 6.5 we require a different grading. For that reason we prove the results in this section for the more general notion of a ρ-grading as defined below.

For each $x \in \mathcal{V}$ and each monomial u of A, where $u = x_1 \cdots x_r$ with $x_1, \ldots, x_r \in \mathcal{V}$, we write $\deg_x(u)$ for the degree of u in x, that is, the number of values of i for which $x_i = x$. Let ρ be an equivalence relation on $\mathcal{V}$ and suppose that ρ is G-*invariant*; that is, for all $x_1, x_2 \in \mathcal{V}$, we have $(x_1, x_2) \in \rho$ if and only if $(x_1g, x_2g) \in \rho$. Let Φ be the set of all functions $\phi : \mathcal{V}/\rho \to \{0, 1, 2, \ldots\}$ with finite support. For $\phi \in \Phi$ let A_ϕ denote the subspace of A spanned by all monomials u such that $\sum_{x \in E} \deg_x(u) = \phi(E)$ for each equivalence class E. We say that an element of A is ρ-*homogeneous* if it belongs to A_ϕ for some ϕ. Clearly $A = \bigoplus_{\phi \in \Phi} A_\phi$. Furthermore $A_\phi \subseteq A_n$, where $n = \sum_E \phi(E)$. Thus ρ-homogeneous elements are homogeneous.

A subspace B of A is said to be ρ-*graded* if $B = \bigoplus_{\phi \in \Phi} B_\phi$, where $B_\phi = B \cap A_\phi$. The subspaces B_ϕ are called the ρ-homogeneous components of B. (Note that, in the case where the equivalence relation ρ is simply equality, the ρ-homogeneous components are just the ordinary multihomogeneous components.) It is easily seen that a subspace B of A is ρ-graded if and only if it is spanned by a set of ρ-homogeneous elements. Furthermore, if B and C are ρ-graded subspaces, then so are $B \cap C$ and $B + C$. Clearly each A_n is ρ-graded.

Since G acts on $\mathcal{V}$ and ρ is G-invariant, there is an induced action of G on $\mathcal{V}/\rho$. Thus G also acts on Φ; the action of g is given by $\phi \mapsto \phi g$ where $(\phi g)(E) = \phi(Eg^{-1})$ for each $E \in \mathcal{V}/\rho$. Clearly, if u is ρ-homogeneous, then so is ug. In fact, for each $\phi \in \Phi$, $(A_\phi)g = A_{\phi g}$. Thus G permutes the ρ-homogeneous components B_ϕ of any ρ-graded KG-submodule B of A.

In this section we shall be concerned with direct decompositions of KG-modules which may have infinite dimension. It is a straightforward exercise to verify that every KG-module is a direct sum of finite-dimensional indecomposables. It follows that a direct summand of a free KG-module is free.

Lemma 6.1. (i) *Let B be a ρ-graded free KG-submodule of A. Then B has a G-free basis $\mathcal{S}$ where each element of $\mathcal{S}$ is ρ-homogeneous.*

(ii) *Let B and C be ρ-graded KG-submodules of A such that $C \leq B$ and B/C is a free KG-module. Then there exists a ρ-graded free KG-submodule U of B such that $B = C \oplus U$.*

Proof. Let Ω be the set of all G-orbits in the action of G on Φ.

(i) For $I \in \Omega$ let $B_I = \bigoplus_{\phi \in I} B_\phi$. Thus we have a module decomposition $B = \bigoplus_{I \in \Omega} B_I$. Hence each B_I is free, and it suffices to consider the case where $B = B_I$ for some I. If I is a singleton, $I = \{\phi\}$, then the result is clear. If I contains p elements, $I = \{\phi, \phi g, \dots, \phi g^{p-1}\}$, then we can take a basis $\mathcal{S}_\phi$ of B_ϕ to obtain a G-free basis $\mathcal{S}$ of B, where $\mathcal{S} = \mathcal{S}_\phi G$.

(ii) Clearly $C_\phi \subseteq B_\phi$ for each $\phi \in \Phi$. For $I \in \Omega$ define B_I and C_I as in (i). Then $B/C \cong \bigoplus_{I \in \Omega} B_I/C_I$. Thus each B_I/C_I is free. When $I = \{\phi\}$ let U_I be any submodule of B_I such that $B_I = C_I \oplus U_I$. Clearly U_I is free. When $I = \{\phi, \phi g, \dots, \phi g^{p-1}\}$ let $\{u_\lambda : \lambda \in \Lambda\}$ be a subset of B_ϕ such that $\{u_\lambda + C_\phi : \lambda \in \Lambda\}$ is a basis of B_ϕ/C_ϕ, and let U_I be the subspace of B_I with basis $\{u_\lambda : \lambda \in \Lambda\}G$. Then it is easily verified that U_I is a ρ-graded free submodule of B_I such that $B_I = C_I \oplus U_I$. To complete the proof we define $U = \bigoplus_{I \in \Omega} U_I$. □

It is easy to see that L, R and L_p^f are ρ-graded. Recall from Section 5 that R^* is the restricted Lie algebra generated by $L_2, \dots, L_{p-1}, R_p^*, L_{p+1}, \dots,$ where $R_p^* = \langle x^p : x \in \mathcal{V} \rangle \oplus L_p^f$. Recall also that R^* is free. Since R^* is generated by (and hence spanned by) ρ-homogeneous elements, it follows that R^* is ρ-graded.

If $\mathcal{S}$ is a set of homogeneous elements of R, we say that $\mathcal{S}$ is *reduced* if no element of $\mathcal{S}$ belongs to the restricted Lie algebra generated by the other elements of $\mathcal{S}$. In the proof of the next proposition we use the result that every reduced set freely generates the restricted Lie algebra that it generates: see Kukin [8].

Proposition 6.2. *Let ρ be a G-invariant equivalence relation on $\mathcal{V}$. The free restricted Lie algebra R^* has a G-free free generating set $\mathcal{W}$ consisting of ρ-homogeneous elements such that $\mathcal{W} = \bigcup_{n \geq 2} \mathcal{W}_n$ with $\mathcal{W}_n \subseteq L_n$ for $n \neq p$, and $\mathcal{W}_p = \mathcal{W}_p^f \cup \{x^p : x \in \mathcal{V}\}$ with $\mathcal{W}_p^f \subseteq L_p^f$.*

Proof. For each $n \geq 2$ let $R^*(n)$ denote the subalgebra of R^* defined as follows: for $2 \leq n < p$, let $R^*(n)$ be generated by $L_2, \dots, L_n$; let $R^*(p)$ be generated by $L_2, \dots, L_{p-1}, R_p^*$; and, for $n > p$, let $R^*(n)$ be generated by $L_2, \dots, L_{p-1}, R_p^*, L_{p+1}, \dots, L_n$. Note that each $R^*(n)$ is ρ-graded, since it is generated by (and hence spanned by) ρ-homogeneous elements. We shall define sets $\mathcal{W}_n$ inductively for $n \geq 2$ with the following properties: each $\mathcal{W}_n$ is G-free and consists of ρ-homogeneous elements; $\mathcal{W}_n \subseteq L_n$ for $n \neq p$; $\mathcal{W}_p = \mathcal{W}_p^f \cup \{x^p : x \in \mathcal{V}\}$ with $\mathcal{W}_p^f \subseteq L_p^f$; and each set $\mathcal{W}_2 \cup \ldots \cup \mathcal{W}_n$ is reduced and generates $R^*(n)$. These properties imply that, for all $n \geq 2$, the set $\mathcal{W}_2 \cup \ldots \cup \mathcal{W}_n$ is a free generating set for $R^*(n)$, so that $\bigcup_{n \geq 2} \mathcal{W}_n$ is a free generating set for R^*. Thus we shall have proved the proposition.

We first find the sets $\mathcal{W}_n$ for $2 \leq n < p$. (This is only relevant when $p > 2$.) If $p > 2$ then, by Corollary 2.2, L_2 is a free KG-module. Since L_2 is ρ-graded, Lemma 6.1 shows that this module has a G-free basis $\mathcal{W}_2$ which consists of ρ-homogeneous elements. Since L_2 generates $R^*(2)$, so does $\mathcal{W}_2$. Clearly $\mathcal{W}_2$ is reduced.

Suppose next that $3 \leq n < p$ and that suitable sets $\mathcal{W}_2, \dots, \mathcal{W}_{n-1}$ have been obtained in relation to $R^*(2), \dots, R^*(n-1)$. We write $R^*(n-1)_{(i)}$ for the i-th homogeneous component of $R^*(n-1)$ as a free restricted Lie algebra on $\mathcal{W}_2 \cup \ldots \cup \mathcal{W}_{n-1}$. Then each $R^*(n-1)_{(i)}$ is ρ-graded. In particular,

$$R^*(n-1) = \bigoplus_{i,k} (R^*(n-1)_{(i)} \cap A_k).$$

By consideration of the degrees of the elements of $\mathcal{W}_2 \cup \ldots \cup \mathcal{W}_{n-1}$,

$$R^*(n-1) \cap A_n = (R^*(n-1)_{(2)} \cap A_n) \oplus \ldots \oplus (R^*(n-1)_{(n-1)} \cap A_n).$$

For $i = 1, \dots, p-1$, $R^*(n-1)_{(i)}$ is a free KG-module, by Corollary 2.2. Hence the modules $R^*(n-1)_{(2)} \cap A_n, \dots, R^*(n-1)_{(n-1)} \cap A_n$ are free (since they are direct summands of the $R^*(n-1)_{(i)}$). Hence $R^*(n-1) \cap A_n$ is free. Since $\mathcal{W}_2 \cup \ldots \cup \mathcal{W}_{n-1} \subseteq L$, we have $R^*(n-1)_{(i)} \subseteq L$ for $i < p$. Thus $R^*(n-1) \cap A_n \subseteq L_n$. Since L_n and $R^*(n-1) \cap A_n$ are free, $L_n/(R^*(n-1) \cap A_n)$ is free. Thus, since L_n and $R^*(n-1) \cap A_n$ are ρ-graded, Lemma 6.1 yields a ρ-graded free module U_n such that $L_n = (R^*(n-1) \cap A_n) \oplus U_n$, together with a G-free basis $\mathcal{W}_n$ for U_n which consists of ρ-homogeneous elements. Since $R^*(n)$ is generated by $R^*(n-1)$ and L_n, it is generated by $\mathcal{W}_2 \cup \ldots \cup \mathcal{W}_n$. It is easily verified that this set is reduced.

We now consider $n = p$. Suppose then that we have found $\mathcal{W}_2, \dots, \mathcal{W}_{p-1}$. We take the notational convention that $\mathcal{W}_2 \cup \ldots \cup \mathcal{W}_{p-1} = \emptyset$ and $R^*(p-1) = 0$ for $p = 2$. Just as in the previous case,

$$R^*(p-1) \cap A_p = (R^*(p-1)_{(2)} \cap A_p) \oplus \ldots \oplus (R^*(p-1)_{(p-1)} \cap A_p)$$

and $R^*(p-1) \cap A_p$ is free. Also, $\mathcal{W}_2 \cup \ldots \cup \mathcal{W}_{p-1} \subseteq [L, L]$. Hence $R^*(p-1)_{(i)} \subseteq L''$ for $2 \leq i \leq p-1$. Thus

$$R^*(p-1) \cap A_p \subseteq L'' \cap A_p \subseteq L_p^f.$$

Since L_p^f and $R^*(p-1) \cap A_p$ are ρ-graded and free, Lemma 6.1 yields a ρ-graded free module U_p such that $L_p^f = (R^*(p-1) \cap A_p) \oplus U_p$, together with a G-free basis $\mathcal{W}_p^f$ of U_p which consists of ρ-homogeneous elements. Let $\mathcal{W}_p = \mathcal{W}_p^f \cup \{x^p : x \in \mathcal{V}\}$. Since $R^*(p)$ is generated by $R^*(p-1)$ and R_p^*, it is generated by $\mathcal{W}_2 \cup \ldots \cup \mathcal{W}_p$. It is easily verified that this set is reduced.

Finally, suppose that $n > p$ and that we have found $\mathcal{W}_2, \dots, \mathcal{W}_{n-1}$. Let $A^*(n-1)$ be the associative subalgebra of A generated by $R^*(n-1)$. Thus $A^*(n-1)$ is ρ-graded. Moreover (see Section 2), $A^*(n-1)$ is a free associative algebra with $\mathcal{W}_2 \cup \ldots \cup \mathcal{W}_{n-1}$ as a free generating set. Since this generating set is G-free, the homogeneous components $A^*(n-1)_{(i)}$ are free KG-modules for $i \geq 1$. Thus $A^*(n-1) \cap A_n$ is also a free module, since it is a direct sum of summands of the $A^*(n-1)_{(i)}$. Recall from Section 5 that A^* is the associative algebra generated by $L_2, \dots, L_{p-1}, R_p^*, L_{p+1}, \dots$. Hence A^* is generated by $R^*(n-1) \cup L_n \cup L_{n+1} \cup \ldots$, and so by $\mathcal{W}_2 \cup \ldots \cup \mathcal{W}_{n-1} \cup L_n \cup L_{n+1} \cup \ldots$. Therefore $A^* \cap A_n$ is spanned by all products of degree n formed from this last generating set. It follows that $A^* \cap A_n = (A^*(n-1) \cap A_n) + L_n$. By Proposition 5.2, $A^* \cap A_n$ is free. Since $A^*(n-1) \cap A_n$ is free, so also is

$$((A^*(n-1) \cap A_n) + L_n)/(A^*(n-1) \cap A_n).$$

Thus $L_n/(A^*(n-1)\cap L_n)$ is free. Since L_n and $A^*(n-1)\cap L_n$ are ρ-graded, Lemma 6.1 yields a ρ-graded free module U_n such that $L_n=(A^*(n-1)\cap L_n)\oplus U_n$, together with a G-free basis $\mathcal{W}_n$ of U_n which consists of ρ-homogeneous elements.

Let $L^*(n-1)$ be the Lie subalgebra of $R^*(n-1)$ generated by $\mathcal{W}_2\cup\ldots\cup\mathcal{W}_{n-1}$. Thus $L^*(n-1)$ is a free Lie algebra, with free generating set $\mathcal{W}_2\cup\ldots\cup\mathcal{W}_{n-1}$. Since $L^*(n-1)\subseteq R^*\subseteq R$, we have $[L^*(n-1),L^*(n-1)]\subseteq L$. It follows easily that

$$L^*(n-1)=\langle x^p : x\in\mathcal{V}\rangle\oplus(L^*(n-1)\cap L).$$

Let $\mathcal{F}$ be any basis of L which includes both $\mathcal{V}$ and a basis $\mathcal{F}_0$ of $L^*(n-1)\cap L$. Let $\mathcal{F}_1=\{x^p : x\in\mathcal{V}\}\cup\mathcal{F}_0$. Thus $\mathcal{F}_1$ is a basis of $L^*(n-1)$. Take an arbitrary ordering of $\mathcal{F}^{[p]}$, where $\mathcal{F}^{[p]}=\{b^{p^\alpha} : b\in\mathcal{F},\,\alpha\geq 0\}$. Since $\mathcal{F}_1^{[p]}\subseteq\mathcal{F}^{[p]}$, there is an induced ordering of $\mathcal{F}_1^{[p]}$. Let $\mathcal{F}(A)$ and $\mathcal{F}_1(A^*(n-1))$ be the bases of A and $A^*(n-1)$, respectively, obtained from $\mathcal{F}^{[p]}$ and $\mathcal{F}_1^{[p]}$ as in Section 2. Clearly $\mathcal{F}_1(A^*(n-1))\subseteq\mathcal{F}(A)$, $\mathcal{F}\subseteq\mathcal{F}(A)$, and $\mathcal{F}_1(A^*(n-1))\cap\mathcal{F}=\mathcal{F}_0$. Thus the intersection of the subspaces of A spanned by $\mathcal{F}_1(A^*(n-1))$ and $\mathcal{F}$ is equal to the subspace spanned by $\mathcal{F}_0$. In other words, $A^*(n-1)\cap L=L^*(n-1)\cap L$.

It follows that $A^*(n-1)\cap L=R^*(n-1)\cap L$, and so, by the choice of U_n, $L_n=(R^*(n-1)\cap L_n)\oplus U_n$. Since $R^*(n)$ is generated by $R^*(n-1)$ and L_n, it is generated by $\mathcal{W}_2\cup\ldots\cup\mathcal{W}_n$. It is easily verified that this set is reduced. This completes the proof. □

Lemma 6.3. *Let L^* be the Lie subalgebra of R^* generated by $\mathcal{W}$, where $\mathcal{W}$ is as in Proposition 6.2. Then L^* is a free Lie algebra with free generating set $\mathcal{W}$. Furthermore,*

$$L^*=L_2\oplus\ldots\oplus L_{p-1}\oplus R_p^*\oplus L_{p+1}\oplus\ldots.$$

For each $i\geq 1$, let L_i^* be the i-th homogeneous component of L^* with respect to the free generating set $\mathcal{W}$. Then $L_i^*\cap A_n=L_i^*\cap L_n$ for all $i,n\geq 1$ except for the case $i=1$, $n=p$. Also, we have

$$L_n=(L_1^*\cap A_n)\oplus\ldots\oplus(L_{n-1}^*\cap A_n)\quad \textit{for } n\geq 2,\ n\neq p,$$

and

$$L_p^f=(L_1^*\cap L_p)\oplus\ldots\oplus(L_{p-1}^*\cap L_p).$$

Proof. Clearly L^* is a free Lie algebra with free generating set $\mathcal{W}$. Since $L^*\subseteq R$ we have $[L^*,L^*]\subseteq L$. It follows easily that $L^*=\langle x^p : x\in\mathcal{V}\rangle\oplus(L^*\cap L)$. Recall that A^* is the associative algebra generated by R^*. By the same argument as was used to prove that $A^*(n-1)\cap L=L^*(n-1)\cap L$ in the proof of Proposition 6.2, we obtain $A^*\cap L=L^*\cap L$. Therefore

$$L_2\oplus\ldots\oplus L_{p-1}\oplus L_p^f\oplus L_{p+1}\oplus\ldots\subseteq A^*\cap L\subseteq L^*\cap L.$$

But $L^*\cap L\subseteq L_2\oplus\ldots\oplus L_{p-1}\oplus L_p\oplus L_{p+1}\oplus\ldots$. Thus

$$L^*\cap L=L_2\oplus\ldots\oplus L_{p-1}\oplus(L^*\cap L_p)\oplus L_{p+1}\oplus\ldots,$$

where $L_p^f\subseteq L^*\cap L_p$.

Each element u of $[L^*,L^*]$ can be written as a linear combination of Lie monomials of length at least 2 in the elements of $\mathcal{W}$. If $u\in[L^*,L^*]\cap A_p$, then only elements of $\mathcal{W}_2\cup\ldots\cup\mathcal{W}_{p-1}$ are needed, and these belong to $[L,L]$. Thus

$[L^*, L^*] \cap A_p \subseteq L'' \cap A_p \subseteq L_p^f$. Since the elements of $\mathcal{W}$ are homogeneous in $\mathcal{V}$, we have

$$L^* \cap A_p = (L_1^* \cap A_p) \oplus ([L^*, L^*] \cap A_p) \subseteq (L_1^* \cap A_p) + L_p^f.$$

Thus $L^* \cap L_p = (L_1^* \cap L_p) + L_p^f$. But $L_1^* \cap L_p \subseteq L_p^f$. Thus $L^* \cap L_p = L_p^f$. It follows that

$$L^* \cap L = L_2 \oplus \ldots \oplus L_{p-1} \oplus L_p^f \oplus L_{p+1} \oplus \ldots ,$$

and so

$$L^* = L_2 \oplus \ldots \oplus L_{p-1} \oplus R_p^* \oplus L_{p+1} \oplus \ldots .$$

Since $[L^*, L^*] \subseteq L$, we have $L_i^* \cap L_n = L_i^* \cap A_n$ for all n and all $i \geq 2$. Also, for $n \neq p$, $L_1^* \cap A_n \subseteq L$, so $L_1^* \cap L_n = L_1^* \cap A_n$.

Since each element of $\mathcal{W}$ has degree at least 2 in $\mathcal{V}$,

$$L^* \cap A_n = (L_1^* \cap A_n) \oplus \ldots \oplus (L_{n-1}^* \cap A_n)$$

for all $n \geq 2$. For $n \geq 2$ with $n \neq p$ we have $L^* \cap A_n = L_n$, and so

$$L_n = (L_1^* \cap A_n) \oplus \ldots \oplus (L_{n-1}^* \cap A_n).$$

For $n = p$, since $[L^*, L^*] \cap A_p \subseteq L_p^f \subseteq L^* \cap A_p$, we have

$$L_p^f = (L_1^* \cap L_p^f) \oplus (L_2^* \cap A_p) \oplus \ldots \oplus (L_{p-1}^* \cap A_p).$$

But $L_1^* \cap L_p^f = L_1^* \cap L_p$, and $L_i^* \cap A_p = L_i^* \cap L_p$ for $i \geq 2$. Hence

$$L_p^f = (L_1^* \cap L_p) \oplus \ldots \oplus (L_{p-1}^* \cap L_p).$$

□

Our strategic aim, as outlined in the Introduction, has been achieved in the previous lemma. This result provides a direct decomposition of L_n into a sum of modules which can be found as direct summands of homogeneous components of L^* of degree (in L^*) smaller than n. The fact that L_n is a direct sum of isomorphic copies of KG and IG can now be established by a straightforward induction. We omit the details because we shall obtain the indecomposables of L_n together with their multiplicities (when $\mathcal{V}$ is finite) as a consequence of the much stronger Theorem 2, which is proved later in this section. In fact, Theorem 2 follows immediately from our next result.

Theorem 6.4. *Let L be the free Lie algebra on a G-free free generating set $\mathcal{V}$, with L regarded as a KG-module. Let ρ be any G-invariant equivalence relation on $\mathcal{V}$. Then there exist subsets $\mathcal{L}_1, \mathcal{L}_2, \ldots$ of L such that, for all $n \geq 1$, the union of*

$$\{ug^i : u \in \mathcal{L}_n,\ i = 0, 1, \ldots, p-1\}$$

and

$$\bigcup_{\substack{\alpha \geq 1 \\ p^\alpha | n}} \{w(u^{p^{\alpha-1}})(1 - g^j) \ :\ u \in \mathcal{L}_{n/p^\alpha},\ j = 1, \ldots, p-1\}$$

is a basis of L_n. Furthermore, the elements of this basis are distinct, as written, and each set $\mathcal{L}_n$ consists of elements which are ρ-homogeneous.

Proof. If L is a free Lie algebra over K with a G-free free generating set $\mathcal{V}$, where $\mathcal{V} = \mathcal{X}G$, with G-transversal $\mathcal{X}$, and if ρ is a G-invariant equivalence relation on $\mathcal{X}G$, then, for the purposes of this proof, let us say that $(L, \mathcal{X}, \rho)$ is a G-triple.

For a G-triple $(L, \mathcal{X}, \rho)$ let R^* be defined as in Section 5, and let $\mathcal{W}$ be a free generating set for R^* with the properties given in Proposition 6.2. Choose a G-transversal $\mathcal{Y}$ of $\mathcal{W}$ such that $\{x^p : x \in \mathcal{X}\} \subseteq \mathcal{Y}$. Thus $\mathcal{W} = \mathcal{Y}G$. Each element of $\mathcal{Y}G$ is ρ-homogeneous. Thus we can define an equivalence relation σ on $\mathcal{Y}G$ by taking $(y_1, y_2) \in \sigma$ (for $y_1, y_2 \in \mathcal{Y}G$) if and only if both y_1 and y_2 belong to the same ρ-homogeneous component of A. It is easy to verify that σ is G-invariant. Let L^* be the free Lie algebra with free generating set $\mathcal{Y}G$ as described in Lemma 6.3. It follows that $(L^*, \mathcal{Y}, \sigma)$ is a G-triple. Define a function μ on G-triples by $\mu(L, \mathcal{X}, \rho) = (L^*, \mathcal{Y}, \sigma)$. (Although there were choices made in the construction of $\mathcal{Y}$ from $(L, \mathcal{X}, \rho)$, we simply make arbitrary choices in order to define $\mu(L, \mathcal{X}, \rho)$.)

By an inductive definition we can define, for every G-triple $(L, \mathcal{X}, \rho)$, subsets $\eta_1(L, \mathcal{X}, \rho), \eta_2(L, \mathcal{X}, \rho), \dots$ of L satisfying $\eta_1(L, \mathcal{X}, \rho) = \mathcal{X}$ and, for all $n \geq 2$,

$$\eta_n(L, \mathcal{X}, \rho) = \bigcup_{i=1}^{n-1} (\eta_i(\mu(L, \mathcal{X}, \rho)) \cap L_n).$$

For a fixed G-triple $(L, \mathcal{X}, \rho)$ we shall write, as before, A for the free associative algebra on $\mathcal{X}G$ and $(L^*, \mathcal{Y}, \sigma) = \mu(L, \mathcal{X}, \rho)$. Furthermore, we write $\mathcal{L}_n = \eta_n(L, \mathcal{X}, \rho)$ and $\mathcal{M}_n = \eta_n(L^*, \mathcal{Y}, \sigma)$ for all $n \geq 1$. Thus $\mathcal{L}_1 = \mathcal{X}$, $\mathcal{M}_1 = \mathcal{Y}$ and

$$\mathcal{L}_n = \bigcup_{i=1}^{n-1} (\mathcal{M}_i \cap L_n) \quad \text{for all} \quad n \geq 2. \tag{6.1}$$

We now prove that the elements of $\mathcal{L}_n$ are ρ-homogeneous for all $n \geq 1$. This is clear for $n = 1$. Arguing by induction on n for all G-triples, we may assume that $n > 1$ and that the elements of $\mathcal{M}_1, \dots, \mathcal{M}_{n-1}$ are σ-homogeneous. But $\mathcal{Y}G$ consists of elements which are ρ-homogeneous. It follows easily that the elements of $\mathcal{M}_1, \dots, \mathcal{M}_{n-1}$ are ρ-homogeneous. Thus, by (6.1), the elements of $\mathcal{L}_n$ are ρ-homogeneous. This completes the induction.

Note that the argument in the preceding paragraph also shows that the elements of each $\mathcal{M}_n$ are ρ-homogeneous. Thus, writing $\mathcal{M}_{i,n} = \mathcal{M}_i \cap A_n$ for all $i, n \geq 1$, we have $\mathcal{M}_i = \bigcup_{n \geq 1} \mathcal{M}_{i,n}$. By Lemma 6.3, $\mathcal{M}_i \cap L_n = \mathcal{M}_{i,n}$ except when $i = 1$, $n = p$. Thus, by (6.1),

$$\mathcal{L}_n = \bigcup_{i=1}^{n-1} \mathcal{M}_{i,n} \quad \text{for all} \quad n \geq 2 \quad \text{with} \quad n \neq p. \tag{6.2}$$

Also, $(\mathcal{M}_1 \cap L_p) \cup \{x^p : x \in \mathcal{X}\} = \mathcal{M}_{1,p}$. Thus, by (6.1),

$$\mathcal{L}_p \cup \{x^p : x \in \mathcal{X}\} = \bigcup_{i=1}^{p-1} \mathcal{M}_{i,p}. \tag{6.3}$$

For any subset $\mathcal{S}$ of A and $\alpha \geq 0$ we write $\mathcal{S}^{p^\alpha} = \{u^{p^\alpha} : u \in \mathcal{S}\}$ and

$$\zeta(\mathcal{S}) = \{w(u)(1 - g^j) : u \in \mathcal{S},\ j = 1, \dots, p-1\}.$$

It is easy to verify that, if $\mathcal{S}$ consists of ρ-homogeneous elements of A, then $\mathcal{S}^{p^\alpha}$ and $\zeta(\mathcal{S})$ have the same property.

For each $n \geq 1$ we define

$$\mathcal{B}(L_n) = \mathcal{L}_n G \cup \bigcup_{\substack{\alpha \geq 1 \\ p^\alpha | n}} \zeta(\mathcal{L}_{n/p^\alpha}^{p^{\alpha-1}}) \tag{6.4}$$

and

$$\mathcal{B}(L_n^*) = \mathcal{M}_n G \cup \bigcup_{\substack{\alpha \geq 1 \\ p^\alpha | n}} \zeta(\mathcal{M}_{n/p^\alpha}^{p^{\alpha-1}}). \tag{6.5}$$

Clearly all elements of $\mathcal{B}(L_n)$ and $\mathcal{B}(L_n^*)$ are ρ-homogeneous. By (6.1), $\mathcal{L}_n G \subseteq L_n$ for all n. Thus $\mathcal{L}_{n/p^\alpha} \subseteq L_{n/p^\alpha}$, and it follows easily from (4.4) and (2.2) that $\zeta(\mathcal{L}_{n/p^\alpha}^{p^{\alpha-1}}) \subseteq L_n$. Hence $\mathcal{B}(L_n) \subseteq L_n$. Similarly, $\mathcal{B}(L_n^*) \subseteq L_n^*$.

We shall prove that $\mathcal{B}(L_n)$ is a basis of L_n, for all $n \geq 1$. This is clear for $n = 1$ because $\mathcal{L}_1 G = \mathcal{X} G$. Arguing by induction on n for all G-triples, we may assume that $n > 1$ and that $\mathcal{B}(L_i^*)$ is a basis of L_i^* for $i = 1, \ldots, n-1$. So, from now on, n is fixed with these properties.

By our assumptions, $\mathcal{B}(L_i^*) \cap A_n$ is a basis for $L_i^* \cap A_n$ for $i = 1, \ldots, n-1$ (since elements of $\mathcal{B}(L_i^*)$ are ρ-homogeneous). But, if $n \neq p$,

$$L_n = (L_1^* \cap A_n) \oplus \ldots \oplus (L_{n-1}^* \cap A_n)$$

by Lemma 6.3. Thus

$$\bigcup_{i=1}^{n-1} (\mathcal{B}(L_i^*) \cap A_n) \quad \text{is a basis of} \quad L_n \quad \text{if} \quad n \neq p. \tag{6.6}$$

For $i > 1$, $L_i^* \cap L_p = L_i^* \cap A_p$ by Lemma 6.3. Thus, if $n = p$, $\mathcal{B}(L_i^*) \cap L_p$ is a basis for $L_i^* \cap L_p$ for $i > 1$. Also, since $\mathcal{B}(L_1^*) = \mathcal{Y} G$, it is easy to check that $\mathcal{B}(L_1^*) \cap L_p$ is a basis for $L_1^* \cap L_p$. By Lemma 6.3,

$$L_p^f = (L_1^* \cap L_p) \oplus \ldots \oplus (L_{p-1}^* \cap L_p).$$

Thus

$$\bigcup_{i=1}^{p-1} (\mathcal{B}(L_i^*) \cap L_p) \quad \text{is a basis of} \quad L_p^f \quad \text{if} \quad n = p. \tag{6.7}$$

To prove that $\mathcal{B}(L_n)$ is a basis of L_n we first consider the case $n = p$. Then, by (6.4) and (6.1),

$$\begin{aligned} \mathcal{B}(L_p) &= \mathcal{L}_p G \cup \zeta(\mathcal{L}_1) \\ &= \bigcup_{i=1}^{p-1} (\mathcal{M}_i G \cap L_p) \cup \{w(x)(1 - g^j) : x \in \mathcal{X},\ j = 1, \ldots, p-1\}. \end{aligned}$$

But, for $i < p$, $\mathcal{M}_i G \cap L_p = \mathcal{B}(L_i^*) \cap L_p$. Therefore, by (6.7), $\bigcup_{i=1}^{p-1} (\mathcal{M}_i G \cap L_p)$ is a basis of L_p^f. Hence, by Proposition 4.1, $\mathcal{B}(L_p)$ is a basis of L_p.

Now suppose that $n \neq p$. By (6.6), it suffices to prove that $\bigcup_{i=1}^{n-1}(\mathcal{B}(L_i^*) \cap A_n) = \mathcal{B}(L_n)$. By (6.5) and (6.2),

$$\begin{aligned}\bigcup_{i=1}^{n-1}(\mathcal{B}(L_i^*) \cap A_n) &= \bigcup_{i=1}^{n-1}(\mathcal{M}_i G \cap A_n) \cup \bigcup_{i=1}^{n-1} \bigcup_{\substack{\alpha \geq 1 \\ p^\alpha \mid i}} (\zeta(\mathcal{M}_{i/p^\alpha}^{p^{\alpha-1}}) \cap A_n) \\ &= \bigcup_{i=1}^{n-1} \mathcal{M}_{i,n} G \cup \bigcup_{i=1}^{n-1} \bigcup_{\substack{\alpha \geq 1 \\ p^\alpha \mid (i,n)}} \zeta((\mathcal{M}_{i/p^\alpha, n/p^\alpha})^{p^{\alpha-1}}) \\ &= \mathcal{L}_n G \cup \bigcup_{\substack{\alpha \geq 1 \\ p^\alpha \mid n}} \bigcup_{t=1}^{(n/p^\alpha)-1} \zeta((\mathcal{M}_{t, n/p^\alpha})^{p^{\alpha-1}}).\end{aligned}$$

By comparison with (6.4) we see that it suffices to prove

$$\bigcup_{\substack{\alpha \geq 1 \\ p^\alpha \mid n}} \bigcup_{t=1}^{(n/p^\alpha)-1} (\mathcal{M}_{t, n/p^\alpha})^{p^{\alpha-1}} = \bigcup_{\substack{\alpha \geq 1 \\ p^\alpha \mid n}} \mathcal{L}_{n/p^\alpha}^{p^{\alpha-1}}. \tag{6.8}$$

For α such that $n/p^\alpha \notin \{1, p\}$ we have, by (6.2),

$$\bigcup_{t=1}^{(n/p^\alpha)-1} \mathcal{M}_{t, n/p^\alpha} = \mathcal{L}_{n/p^\alpha}.$$

Thus, for these values of α, the terms on the two sides of (6.8) are equal. To prove (6.8) we need only compare the terms corresponding to values of α for which $n/p^\alpha \in \{1, p\}$. These only occur when n is a power of p, $n = p^\beta$ (where $\beta \geq 2$ since $n \geq 2$ and $n \neq p$). In this case it remains to prove

$$\bigcup_{\alpha \in \{\beta-1, \beta\}} \bigcup_{t=1}^{(n/p^\alpha)-1} (\mathcal{M}_{t, n/p^\alpha})^{p^{\alpha-1}} = \bigcup_{\alpha \in \{\beta-1, \beta\}} \mathcal{L}_{n/p^\alpha}^{p^{\alpha-1}}. \tag{6.9}$$

The term on the left hand side with $\alpha = \beta$ is empty. Evaluation of the other term on the left gives, by (6.3),

$$\bigcup_{t=1}^{p-1} (\mathcal{M}_{t,p})^{p^{\beta-2}} = \mathcal{L}_p^{p^{\beta-2}} \cup \{x^p : x \in \mathcal{X}\}^{p^{\beta-2}} = \mathcal{L}_p^{p^{\beta-2}} \cup \mathcal{L}_1^{p^{\beta-1}},$$

which establishes equality with the right hand side of (6.9).

We have now proved that $\mathcal{B}(L_n)$ is a basis of L_n for all n. To complete the proof of the theorem we must show that the basis elements are distinct as written in the statement of the theorem.

Let $\mathcal{L} = \bigcup_{n \geq 1} \mathcal{L}_n$ and $\mathcal{M} = \bigcup_{n \geq 1} \mathcal{M}_n$. For $i = 0, 1, \ldots, p-1$ define $\kappa_i : A \to A$ by $\kappa_i(u) = ug^i$ for all $u \in A$. For $j = 1, \ldots, p-1$ and $\alpha = 1, 2, 3, \ldots$ define $\lambda_{j,\alpha} : A \to A$ by $\lambda_{j,\alpha}(u) = w(u^{p^{\alpha-1}})(1 - g^j)$. Let Δ be the set of all the functions κ_i and $\lambda_{j,\alpha}$. We must prove that the elements $\delta(u)$ for $u \in \mathcal{L}$, $\delta \in \Delta$, are distinct. It is clearly sufficient to show that, for each n, the elements $\delta(u)$ which belong to L_n are distinct.

The elements $\delta(u)$ which belong to L_1 are the elements xg^i for $x \in \mathcal{X}$ and $i = 0, 1, \ldots, p-1$. Since $\mathcal{X}$ is a G-transversal of $\mathcal{X}G$, the result is true for $n = 1$.

Working by induction on n over all G-triples, we may assume that $n \geq 2$ and that those elements $\delta(u)$, with $u \in \mathcal{M}$, $\delta \in \Delta$, which belong to $L_1^* \cup \ldots \cup L_{n-1}^*$ are distinct.

Suppose first that $n = p$. The elements $\delta(u)$ which belong to L_p are the elements ug^i for $u \in \mathcal{L}_p$, $i = 0, 1, \ldots, p-1$, and the elements $w(x)(1 - g^j)$ for $x \in \mathcal{X}$, $j = 1, \ldots, p-1$. Now $\mathcal{L}_p = \bigcup_{i=1}^{p-1}(\mathcal{M}_i \cap L_p)$, so the elements ug^i are distinct by the inductive hypothesis. The elements $w(x)(1 - g^j)$ are distinct and belong to L_p^a by Proposition 4.1. But the elements ug^i belong to L_p^f by (6.7), and $L_p = L_p^f \oplus L_p^a$ by Proposition 4.1. Thus the result follows in this case.

Suppose now that $n \neq p$. Let $\delta(u) \in L_n$ where $u \in \mathcal{L}$, $\delta \in \Delta$. If $u \in \mathcal{L}_i$ with $i > 1$, then $u \in \mathcal{M}_1 \cup \ldots \cup \mathcal{M}_{i-1}$ by (6.1), and hence $\delta(u) \in L_1^* \cup \ldots \cup L_{n-1}^*$. But, if $u \in \mathcal{L}_1$, then $\delta = \lambda_{j,\alpha}$ for some j and α with $\alpha > 1$ (since $n \neq p$): in this case we have $\delta(u) = \lambda_{j,\alpha-1}(u^p)$, where $u^p \in \mathcal{M}_1$ and $\lambda_{j,\alpha-1}(u^p) \in L_1^* \cup \ldots \cup L_{n-1}^*$. Hence the result follows by the inductive hypothesis. □

With a view to future applications we now briefly describe a version of Theorem 6.4 in which the sets $\mathcal{L}_n$ may be chosen to have an additional property.

Identify the group G with a Sylow p-subgroup of the symmetric group of degree p, and let N be the normalizer of G in this symmetric group. Thus N has order $p(p-1)$, and it is the semidirect product of G by a cyclic group H of order $p-1$. Let h be a generator of H. Suppose that V is a KN-module such that the restriction $V{\downarrow_G}$ is a free KG-module. Note that $V(IG)$ is a KN-submodule of V. Since K contains a primitive $(p-1)$-th root of unity, there is a KH-submodule X of V such that $V = V(IG) \oplus X$, and X has a basis $\mathcal{X}$ which consists of eigenvectors of h. It is not difficult to see that $\mathcal{X}$ is a free generating set for $V{\downarrow_G}$. Thus V has a G-free basis $\mathcal{X}G$ with a G-transversal $\mathcal{X}$ which consists of eigenvectors of h. Note that H permutes the set of all scalar multiples of elements of $\mathcal{X}G$.

The free associative algebra A generated by V is naturally a KN-module, and the restriction from N to G gives, of course, the KG-module structure that we have already been using. Clearly, the algebras L and R are KN-submodules of A, and it is easily verified that the algebra R^* is also a KN-submodule.

Take any equivalence relation ρ on $\mathcal{X}G$ such that $(x, xg) \in \rho$ for all $x \in \mathcal{X}G$. Thus ρ is G-invariant, and each ρ-homogeneous component A_ϕ is a KN-submodule of A. In order to obtain a version of Proposition 6.2 and hence the desired version of Theorem 6.4, we require a variant of Lemma 6.1. Suppose that B is any ρ-graded KN-submodule of A such that $B{\downarrow_G}$ is free. Then each ρ-homogeneous component B_ϕ of B is a KN-submodule such that $B_\phi{\downarrow_G}$ is free. Hence (as already noted for V) the module B_ϕ has a G-free basis $\mathcal{S}_\phi$ with a G-transversal $\mathcal{T}_\phi$ consisting of eigenvectors of h. By taking the union over ϕ we obtain a G-free basis $\mathcal{S}$ of B which consists of ρ-homogeneous elements and which has a G-transversal $\mathcal{T}$ consisting of eigenvectors of h. This is the required variant of Lemma 6.1(i). Suppose now that B and C are ρ-graded KN-submodules of A such that $C \leq B$ and $(B/C){\downarrow_G}$ is free. Then each $(B_\phi/C_\phi){\downarrow_G}$ is free, and so (since G is a Sylow p-subgroup of N) each B_ϕ/C_ϕ is projective. Hence we easily obtain a ρ-graded KN-submodule U of B such that $U{\downarrow_G}$ is free and $B = C \oplus U$. This is the required variant of Lemma 6.1(ii).

It is easily checked that all the KG-modules considered in the proof of Proposition 6.2 are KN-modules. Hence, by use of the above variant of Lemma 6.1, we can choose the sets $\mathcal{W}_n$ to have the extra property that each $\mathcal{W}_n$ has a G-transversal

$\mathcal{Y}_n$ consisting of eigenvectors of h. Thus $\mathcal{W}$ has a G-transversal $\mathcal{Y}$ consisting of eigenvectors of h, and clearly we can take $\{x^p : x \in \mathcal{X}\} \subseteq \mathcal{Y}$. Note also that $\langle \mathcal{W} \rangle$ is a KN-module.

Now let L^* and σ be as defined in the proof of Theorem 6.4. Then it is easily checked that $(y, yg) \in \sigma$ for all $y \in \mathcal{W} = \mathcal{Y}G$. Thus in the proof of Theorem 6.4 we may restrict consideration to G-triples $(L, \mathcal{X}, \rho)$ where $(x, xg) \in \rho$ for all $x \in \mathcal{X}G$ and where $\mathcal{X}$ consists of eigenvectors of h. The sets $\mathcal{L}_n$ defined inductively by means of $\mathcal{L}_1 = \mathcal{X}$ and equation (6.1) then consist of eigenvectors of h.

Proposition 6.5. *In the case described above, in which $\mathcal{V} = \mathcal{X}G$, where $\mathcal{X}$ consists of eigenvectors of h and $(x, xg) \in \rho$ for all $x \in \mathcal{V}$, the sets $\mathcal{L}_n$ of Theorem* 6.4 *may be chosen to have the additional property that they consist of eigenvectors of h.*

We can now prove our main results, as stated in Section 1.

Proof of Theorem 2. Theorem 2 follows immediately from Theorem 6.4 on putting $\mathcal{L} = \bigcup_{n \geq 1} \mathcal{L}_n$. □

Remark. By choosing ρ to be the relation of equality, we see that the elements of $\mathcal{L}$ in Theorem 2 may be taken to be multihomogeneous.

Proof of Theorem 1. We derive Theorem 1 from Theorem 2, writing $\mathcal{L}_n = \mathcal{L} \cap L_n$ in accordance with Theorem 6.4. The fact that L_n is a direct sum of a free module and modules isomorphic to IG follows from Theorem 2, since for each $u \in \mathcal{L}_n$ the elements $u, ug, \ldots, ug^{p-1}$ span a regular submodule of L_n, and for each $u \in \mathcal{L}_{n/p^\alpha}$ with $\alpha \geq 1$ and $p^\alpha \,|\, n$ the elements $w(u^{p^{\alpha-1}})(1 - g^j)$, for $j = 1, \ldots, p-1$, span a submodule of L_n that is isomorphic to IG. It remains to verify the formula for the number of copies of IG. We do this by induction on n. Let $f(n)$ and $a(n)$ denote, respectively, the multiplicity of the regular module and the multiplicity of IG when L_n is written as a direct sum of indecomposables. Note that, by Theorem 2, $f(n)$ is equal to the number of elements of $\mathcal{L}_n$. We need to verify that $a(n)$ satisfies formula (1.1). Clearly,

$$\dim(L_n) = p\,f(n) + (p-1)a(n).$$

Hence

$$f(n) = \frac{1}{p}(\dim(L_n) - (p-1)a(n)).$$

It follows from Theorem 2 that

$$a(n) = f(n/p) + f(n/p^2) + f(n/p^3) + \ldots\,,$$

where $f(r)$ is interpreted as 0 when r is not an integer. If $(n, p) = 1$ then $a(n) = 0$, which gives (1.1) in this case. In particular we have the basis of our induction. If $p \,|\, n$, then we have

$$\begin{aligned} a(n) &= f(n/p) + a(n/p) \\ &= \frac{1}{p}(\dim(L_{n/p}) + a(n/p)). \end{aligned} \tag{6.10}$$

Witt's formula and the inductive hypothesis give

$$\begin{aligned} a(n) &= \frac{1}{p}\left(\frac{1}{n/p}\sum_{d|(n/p)}\mu(d)m^{n/pd} - \frac{1}{n/p}\sum_{\substack{d\\ p|d|(n/p)}}\mu(d)m^{n/pd}\right) \\ &= \frac{1}{n}\sum_{\substack{d|(n/p)\\ (d,p)=1}}\mu(d)m^{n/pd} \qquad (6.11) \\ &= -\frac{1}{n}\sum_{\substack{d\\ p|d|n}}\mu(d)m^{n/d}. \end{aligned}$$

This completes the proof of Theorem 1. □

Proof of Corollary 1. Clearly $\dim (L_n)^G = f(n) + a(n)$. By (6.10), $f(n) + a(n) = a(pn)$. Hence the result follows from (6.11) with pn in place of n. □

Proof of Corollary 2. In the case where V is a regular $\mathbb{Z}G$-module, Corollary 2 follows from Corollary 1 and the results of [3]. The general case is obtained in the same way, by means of a straightforward generalisation of the results of [3]. □

7. On the basis elements of L

In this final section we obtain an identity which allows us to express basis elements of the form (1.2) in Theorem 2 explicitly as elements of $L(V)$.

We define numbers $\beta_{n,k}$, for all non-negative integers n, k, by setting $\beta_{0,0} = 2$, $\beta_{n,0} = 1$ for all $n \geq 1$, and

$$\beta_{n,k} = (-1)^k \frac{n}{k}\binom{n-k-1}{k-1}$$

for all n, k with $k \geq 1$, where the binomial coefficient is taken to be 0 if $n-k-1 < 0$, $k-1 < 0$ or $n-k-1 < k-1$. It is straightforward to verify that

$$\beta_{n,k} = \beta_{n-1,k} - \beta_{n-2,k-1} \qquad (7.1)$$

for all $n \geq 2$ and all $k \geq 1$. Hence each $\beta_{n,k}$ is an integer. Using (7.1), we obtain

$$-\beta_{n,k+1} = \sum_{i=0}^{n-2}\beta_{i,k} \qquad (7.2)$$

for all $n \geq 2$ and all $k \geq 0$.

For elements x and y of any Lie ring, define the elements $[x, y^k]$ inductively, for each non-negative integer k, by $[x, y^0] = x$ and $[x, y^k] = [[x, y^{k-1}], y]$ for $k > 0$. In the next two lemmas, x, y and z are arbitrary elements of a Lie ring.

Lemma 7.1. *For all $n \geq 0$,*

$$[x, z^n, y] - [y, z^n, x] = \sum_{k=0}^{[n/2]}\beta_{n,k}[[x, z^k], [y, z^k], z^{n-2k}].$$

Proof. The result is easy to verify for $n = 0$ and $n = 1$. We proceed by induction on n and assume $n \geq 2$. Then

$$\begin{aligned}
&[x, z^n, y] - [y, z^n, x] \\
&\quad = \quad [x, z^{n-1}, y, z] - [y, z^{n-1}, x, z] + [x, z^{n-1}, [z, y]] - [y, z^{n-1}, [z, x]] \\
&\quad = \quad [[x, z^{n-1}, y] - [y, z^{n-1}, x], z] - \big([[x, z], z^{n-2}, [y, z]] - [[y, z], z^{n-2}, [x, z]]\big)\,.
\end{aligned}$$

Using the inductive hypothesis for $n - 1$ and $n - 2$, the right hand side can be rewritten as

$$\begin{aligned}
&\sum_{k=0}^{[(n-1)/2]} \beta_{n-1,k}[[x, z^k], [y, z^k], z^{n-2k-1}, z] \\
&\quad - \sum_{k=0}^{[(n-2)/2]} \beta_{n-2,k}[[x, z, z^k], [y, z, z^k], z^{n-2k-2}] \\
&\quad = \quad \beta_{n-1,0}[x, y, z^n] + \sum_{k=1}^{[n/2]} (\beta_{n-1,k} - \beta_{n-2,k-1})[[x, z^k], [y, z^k], z^{n-2k}].
\end{aligned}$$

The lemma follows by (7.1) and the fact that $\beta_{n-1,0} = \beta_{n,0}$. □

Lemma 7.2. *For all $n \geq 2$,*

$$\begin{aligned}
&\sum_{i=0}^{n-2}([x, z^i, y, z^{n-i-2}] - [y, z^i, x, z^{n-i-2}]) \\
&\qquad = \sum_{k=0}^{[(n-2)/2]} -\beta_{n,k+1}[[x, z^k], [y, z^k], z^{n-2k-2}].
\end{aligned}$$

Proof. For $i = 0, \ldots, n - 2$ let u_i be the summand indexed by i on the left hand side. By Lemma 7.1,

$$\begin{aligned}
u_i \quad &= \quad [[x, z^i, y] - [y, z^i, x], z^{n-i-2}] \\
&= \quad \sum_{k=0}^{[i/2]} \beta_{i,k}[[x, z^k], [y, z^k], z^{i-2k}, z^{n-i-2}] \\
&= \quad \sum_{k=0}^{[i/2]} \beta_{i,k}[[x, z^k], [y, z^k], z^{n-2k-2}].
\end{aligned}$$

Summing from $i = 0$ to $i = n-2$, and then changing the order of summation, gives

$$\sum_{i=0}^{n-2} u_i = \sum_{k=0}^{[(n-2)/2]} \left(\sum_{i=0}^{n-2} \beta_{i,k}\right) [[x, z^k], [y, z^k], z^{n-2k-2}],$$

and, in view of (7.2), this is equal to the right hand side of the equation in the lemma. □

Proposition 7.3. *Let $\hat{w}$ be as defined in Section 4. Then*

$$\hat{w} = \sum_{k,\pi} \gamma_{p,k}[[x_1, x_{\pi(3)}, \ldots, x_{\pi(k+2)}], [x_2, x_{\pi(k+3)}, \ldots, x_{\pi(2k+2)}], x_{\pi(2k+3)}, \ldots, x_{\pi(p)}],$$

where k runs from 0 *to* $\left[\frac{p-2}{2}\right]$*,* π *ranges over all permutations of* $\{3, 4, \dots, p\}$*, and each* $\gamma_{p,k}$ *is an integer given by*

$$\gamma_{p,k} = (-1)^k \frac{1}{k+1} \binom{p-k-2}{k}.$$

Proof. We apply the equation of Lemma 7.2, with $n = p$, to the free Lie ring on free generators $x_1, x_2, \dots, x_p$, as in Section 4. Put $x = x_1$, $y = x_2$ and $z = x_3 + x_4 + \dots + x_p$. We expand both sides of the equation and compare the multilinear parts (consisting of the terms with degree 1 in each generator $x_1, \dots, x_p$). The multilinear part on the left hand side is

$$\sum_{\kappa} [x_1, x_{\kappa(2)}, \dots, x_{\kappa(p)}] - \sum_{\lambda} [x_2, x_{\lambda(1)}, \dots, x_{\lambda(p)}]$$

where κ and λ range over all permutations of $\{2, 3, \dots, p\}$ and $\{1, 3, \dots, p\}$, respectively. But this is equal to $p\,\hat{w}$. The multilinear part on the right hand side is

$$\sum_{k,\pi} -\beta_{p,k+1} [[x_1, x_{\pi(3)}, \dots, x_{\pi(k+2)}], [x_2, x_{\pi(k+3)}, \dots, x_{\pi(2k+2)}], x_{\pi(2k+3)}, \dots, x_{\pi(p)}],$$

with k and π as in the proposition. It is easily verified that $\beta_{p,k+1}$ is divisible by p for all $k \geq 0$. Hence the result follows on dividing through by p. □

Let $\mathcal{L}$ be as in Theorem 2 and take $u \in \mathcal{L}$ and $\alpha \geq 0$. Then, by (4.4) and Proposition 7.3, we may write $w(u^{p^\alpha})(g-1)$ as a linear combination of Lie products of elements from $\{u^{p^\alpha}, (u^{p^\alpha})g, \dots, (u^{p^\alpha})g^{p-1}\}$. These Lie products may be written as Lie products of elements from $\{u, ug, \dots, ug^{p-1}\}$, because $(u^{p^\alpha})g^i = (ug^i)^{p^\alpha}$ and, over a field of characteristic p, the value of $[x, y^{p^\alpha}]$ is given by

$$[x, y^{p^\alpha}] = xy^{p^\alpha} - y^{p^\alpha}x = [x, \underbrace{y, y, \dots, y}_{p^\alpha}].$$

References

[1] Yu. A. Bakhturin, *Identical Relations in Lie Algebras*, Nauka, Moscow, 1985 (Russian). English translation: VNU Science Press, Utrecht, 1987. MR **88f:**17032

[2] A. Brandt, '*The free Lie ring and Lie representations of the full linear group*', Trans. Amer. Math. Soc., 56 (1944), 528–536. MR **6:**146d

[3] R. M. Bryant, '*Cyclic groups acting on free Lie algebras*', in P. H. Kropholler, G. A. Niblo and R. Stöhr (editors) 'Geometry and Cohomology in Group Theory', London Mathematical Society Lecture Note Series, 252, Cambridge University Press, Cambridge, 1998, pp. 39–44.

[4] R. M. Bryant and R. Stöhr, '*Fixed points of automorphisms of free Lie algebras*', Arch. Math., 67 (1996), 281–289. MR **97m:**17008

[5] S. Donkin and K. Erdmann, '*Tilting modules, symmetric functions and the module structure of the free Lie algebra*', J. Algebra, 203 (1998), 69–90. MR **99e:**20056

[6] N. Jacobson, *Lie Algebras*, Interscience, New York, 1962. MR **26:**1345

[7] L. G. Kovács and R. Stöhr, '*Lie powers of the natural module for GL*(2)', J. Algebra, to appear.

[8] G. P. Kukin, '*The subalgebras of free Lie p-algebras*', Algebra i Logika, 11 (1972), 535–550. MR **47:**6798

[9] C. Reutenauer, *Free Lie Algebras*, Clarendon Press, Oxford, 1993. MR **94j:**17002

[10] M. W. Short, '*A conjecture about free Lie algebras*', Commun. Algebra, 23 (1995), 3051–3057. MR **96c:**17007

[11] R. Stöhr, '*On torsion in free central extensions of some torsion-free groups*', J. Pure Appl. Algebra, 46 (1987), 249–289. MR **88j:**20032

[12] R. M. Thrall, '*On symmetrized Kronecker powers and the structure of the free Lie ring*', Amer. J. Math., 64 (1942), 371–388. MR **3:**262d

[13] G. E. Wall, '*On the Lie ring of a group of prime exponent*', in 'Proc. Second Internat. Conf. Theory of Groups, Canberra, 1973', Lecture Notes in Mathematics, 372, Springer, Berlin, etc., 1974, pp. 667–690. MR **50:**10098

[14] F. Wever, '*Über Invarianten von Lieschen Ringen*', Math. Annalen, 120 (1949), 563–580. MR **10:**676e

[15] E. Witt, '*Die Unterringe der freien Lieschen Ringe*', Math. Z., 64 (1956), 195–216. MR **17:**1050a

Department of Mathematics, UMIST, Manchester M60 1QD, United Kingdom
E-mail address: bryant@umist.ac.uk

E-mail address: r.stohr@umist.ac.uk