Factorisation of Lie resolvents

R.M. Bryant\textsuperscript{a}, Manfred Schocker\textsuperscript{b,\ast}

\textsuperscript{a} School of Mathematics, University of Manchester, PO Box 88, Manchester M60 1QD, UK
\textsuperscript{b} Department of Mathematics, University of Wales Swansea, Singleton Park, Swansea SA2 8PP, UK

Received 25 July 2005; received in revised form 14 March 2006; accepted 23 March 2006
Available online 5 June 2006
Communicated by S. Donkin

Abstract

Let $G$ be a group, $F$ a field of prime characteristic $p$, and $V$ a finite-dimensional $FG$-module. For each positive integer $r$, the $r$th homogeneous component of the free Lie algebra on $V$ is an $FG$-module called the $r$th Lie power of $V$. Lie powers are determined, up to isomorphism, by certain functions $\Phi^r$ on the Green ring of $FG$, called ‘Lie resolvents’. Our main result is the factorisation $\Phi^{pmk} = \Phi^p \circ \Phi^k$ whenever $k$ is not divisible by $p$. This may be interpreted as a reduction to the key case of $p$-power degree.

\begin{flushleft}
MSC: 17B01; 20C07; 20C20
\end{flushleft}

1. Introduction

Let $G$ be a group and $F$ a field. For any finite-dimensional $FG$-module $V$, let $L(V)$ be the free Lie algebra on $V$, regarded as an $FG$-module on which each element of $G$ acts as a Lie algebra automorphism. Each homogeneous component $L^r(V)$ is a finite-dimensional submodule, called the $r$th Lie power of $V$. When $F$ has prime characteristic $p$, we may also consider the free restricted Lie algebra $R(V)$. The homogeneous component $R^r(V)$ is called the $r$th restricted Lie power of $V$.

A general problem is to describe the modules $L^r(V)$ and $R^r(V)$ up to isomorphism. We refer to [4] and the papers cited there for a discussion of progress on $L^r(V)$. Although some use has been made of $R(V)$ in studying $L(V)$, results so far on the module structure of $R^r(V)$ are rather sparse; however, see [9,10,17].

The main result of [4] is the ‘Decomposition Theorem’: see Theorem 2.1 below. It reduces the study of arbitrary Lie powers in characteristic $p$ to the study of Lie powers of $p$-power degree. In this paper, we derive some consequences of this result.

First, in Section 2, we obtain an analogous result for restricted Lie powers. Then, in the remainder of the paper, we turn to applications of the Decomposition Theorem in the Green ring $R_{FG}$. This is the ring spanned by the isomorphism classes of finite-dimensional $FG$-modules with addition and multiplication coming from direct sums and tensor products, respectively. In Section 3, we describe a general framework which may be used to study Lie

\textsuperscript{\ast} Corresponding author. Tel.: +44 1792 602230; fax: +44 1792 295843.
\textupit{E-mail addresses:} roger.bryant@manchester.ac.uk (R.M. Bryant), m.schocker@swansea.ac.uk (M. Schocker).
powers and symmetric powers of finite-dimensional $FG$-modules. This is mainly a summary of material contained in [1]. In particular, we describe the relevance of the Adams operations and the Lie resolvents. The latter are $\mathbb{Z}$-linear maps $\Phi^r: R_{FG} \to R_{FG}$. Knowledge of these maps is essentially equivalent to knowledge of the isomorphism classes of Lie powers of finite-dimensional $FG$-modules. We also introduce certain functions $L^*$ and $S^*$ defined on formal power series in an indeterminate $t$ with coefficients from $R_{FG}$. Here, $L^*$ encodes Lie powers and $S^*$ encodes symmetric powers. Furthermore, $L^*$ and $S^*$ have properties like those of the logarithm function and exponential function, respectively.

In Section 4, we obtain the main result of the paper, called the ‘Factorisation Theorem’. It gives a ‘factorisation’ of Lie resolvents under composition: for every non-negative integer $m$ and every positive integer $k$ not divisible by $p$, $\Phi^{pmk} = \Phi^{pm} \circ \Phi^k$. The Lie resolvents $\Phi^k$ for $k$ not divisible by $p$ are comparatively well understood, so the result can be interpreted as a reduction to the case of $p$-power degree. The Factorisation Theorem was conjectured in [3] and proved in [7] in the special case of $m = 1$. It is interesting that the Witt polynomials (as used to define the operations on Witt vectors) arise here in connection with the Factorisation Theorem.

Finally, in Section 5, we describe relations between $L^*$ and $S^*$. A power series in $t$ is said to be ‘$p$-typical’ if the coefficient of $t^r$ is 0 unless $r$ is a power of $p$. We show that, in characteristic $p$, the composite function $L^* \circ S^*$ maps any $p$-typical power series to a $p$-typical power series. In characteristic zero, $L^*$ is the inverse of $S^*$.

2. Decomposition of Lie powers and restricted Lie powers

Let $V$ be a finite-dimensional $FG$-module, where $F$ is a field and $G$ is a group. We write $T(V)$ for the free associative algebra freely generated by any $F$-basis of $V$. Thus $T(V)$ has an $F$-space decomposition $T(V) = \bigoplus_{r \geq 0} T^r(V)$, where, for each $r$, $T^r(V)$ is the $r$th homogeneous component of $T(V)$. The action of $G$ on $V$ extends to $T(V)$, so that $G$ acts by algebra automorphisms. Thus $T(V)$ becomes an $FG$-module, and each $T^r(V)$ is a finite-dimensional submodule.

The algebra $T(V)$ may be made into a Lie algebra by defining $[a, b] = ab - ba$ for all $a, b \in T(V)$. If $F$ has prime characteristic $p$, then $T(V)$ may be made into a restricted Lie algebra by taking the additional powering operation $a \mapsto a^p$. The Lie subalgebra of $T(V)$ generated by $V$ is denoted by $L(V)$ and (when $F$ has characteristic $p$) the restricted Lie subalgebra of $T(V)$ generated by $V$ is denoted by $R(V)$. As is well known, $L(V)$ is a free Lie algebra and $R(V)$ is a free restricted Lie algebra, both freely generated by any basis of $V$ (see, for example, [13, Sections 1.2, 1.6.3 and 2.5.2]). For $r \geq 1$, we write $L^r(V) = T^r(V) \cap L(V)$ and $R^r(V) = T^r(V) \cap R(V)$. Thus $L(V) = \bigoplus_{r \geq 1} L^r(V)$ and $R(V) = \bigoplus_{r \geq 1} R^r(V)$. Here, $L^r(V)$ and $R^r(V)$ are $FG$-submodules of $T^r(V)$, called, respectively, the $r$th Lie power and restricted Lie power of $V$.

As observed in [4, Section 2], if $B$ is a submodule of $T^r(V)$, the associative subalgebra of $T(V)$ generated by $B$ may be identified with $T(B)$. The Lie subalgebra of $T(V)$ generated by $B$ is then the free Lie algebra $L(B)$ and the restricted Lie subalgebra of $T(V)$ generated by $B$ is the free restricted Lie algebra $R(B)$. We assume such identifications in the next two theorems. The first is [4, Theorem 4.4].

**Theorem 2.1** (Decomposition Theorem). Let $F$ be a field of prime characteristic $p$. Let $G$ be a group and $V$ a finite-dimensional $FG$-module. For each positive integer $r$, there is a submodule $B_r$ of $L^r(V)$ such that $B_r$ is a direct summand of $T^r(V)$ and, for $k$ not divisible by $p$ and $m \geq 0$,

$$L^{pkm}(V) = L^{pm}(B_k) \oplus L^{pm-1}(B_{pk}) \oplus \cdots \oplus L^1(B_{pk^m}). \quad (2.1)$$

We use this to prove a similar result for restricted Lie powers.

**Theorem 2.2.** In the notation of Theorem 2.1,

$$R^{pkm}(V) = R^{pm}(B_k) \oplus R^{pm-1}(B_{pk}) \oplus \cdots \oplus R^1(B_{pk^m}).$$

**Proof.** For any subset $S$ of $L(V)$ and $i \geq 0$, we write $S^{[p^i]}$ for the set $\{s^{p^i} : s \in S\}$. We shall use the fact that, if $X$ is any basis of $L(V)$, then the elements $x^{p^i}$ with $x \in X$ and $i \geq 0$ are distinct and form a basis of $R(V)$: they are linearly independent by the Poincaré–Birkhoff–Witt Theorem and it is easy to see that they span $R(V)$.
For each non-negative integer $i$ and each positive integer $k$ not divisible by $p$, let $\mathcal{X}(i, k)$ be a basis of $L^{p^i k}(V)$. Hence $\bigcup_{i, k} \mathcal{X}(i, k)$ is a basis of $L(V)$. Here, and in the remainder of the proof, all unions are unions of disjoint sets. Furthermore, write

$$\widehat{\mathcal{X}}(i, k) = \mathcal{X}(0, k)^{p^i} \cup \mathcal{X}(1, k)^{p^{i-1}} \cup \cdots \cup \mathcal{X}(i, k)^{[1]}.$$ (2.2)

Considerations of degree in the basis of $R(V)$ obtained from $\bigcup_{i, k} \mathcal{X}(i, k)$ show that $\widehat{\mathcal{X}}(i, k)$ is a basis of $R^{p^i k}(V)$.

For each triple $(i, j, k)$ where $i$ and $j$ are non-negative integers and $k$ is a positive integer not divisible by $p$, let $\mathcal{Y}(i, j, k)$ be any basis of $L^{p^i}(B_{p^j k})$ and write

$$\mathcal{Y}(i, j, k) = \mathcal{Y}(0, j, k)^{p^i} \cup \mathcal{Y}(1, j, k)^{p^{i-1}} \cup \cdots \cup \mathcal{Y}(i, j, k)^{[1]}.$$ (2.3)

Thus $\mathcal{Y}(i, j, k)$ is a basis of $R^{p^i}(B_{p^j k})$.

By the Decomposition Theorem, we can choose the basis $\mathcal{X}(i, k)$ of $L^{p^i k}(V)$ to satisfy

$$\mathcal{X}(i, k) = \mathcal{Y}(i, 0, k) \cup \mathcal{Y}(i - 1, 1, k) \cup \cdots \cup \mathcal{Y}(0, i, k).$$ (2.4)

Let $m$ be a non-negative integer. It is easily verified from (2.2) and (2.4) that $\widehat{\mathcal{X}}(m, k)$ is the union of the sets $\mathcal{Y}(i, j, k)^{p^i}$ with $i + j + r = m$. Hence, by (2.3),

$$\widehat{\mathcal{X}}(m, k) = \mathcal{Y}(m, 0, k) \cup \mathcal{Y}(m - 1, 1, k) \cup \cdots \cup \mathcal{Y}(0, m, k).$$

Since $\widehat{\mathcal{X}}(m, k)$ spans $R^{p^m k}(V)$ and $\mathcal{Y}(i, m - i, k)$ spans $R^{p^i}(B_{p^{m-i} k})$, we obtain the required result. □

### 3. Symmetric powers and Lie powers

The underlying ideas that we use are described in [1]. However, we shall make the treatment here as self-contained as possible. We also formulate some of the ideas in a slightly new way, in order to emphasise the analogies between symmetric powers and Lie powers. Let $G$ be a group and $F$ a field. Let $\text{Mod}(FG)$ be the class of all finite-dimensional $FG$-modules and let $R_{FG}$ be the associated Green ring (or representation ring), as defined in Section 1.

The $\mathbb{Q}$-algebra $\mathbb{Q} \otimes_{\mathbb{Z}} R_{FG}$ will be denoted by $\Gamma_{FG}$ and we regard $R_{FG}$ as a subring of $\Gamma_{FG}$. (In [1], $\mathbb{C}$ was used instead of $\mathbb{Q}$. But, for what is needed here, $\mathbb{Q}$ works as well as $\mathbb{C}$.)

Let $\Pi$ denote the power series ring over $\Gamma_{FG}$ in an indeterminate $t$; that is, $\Pi = \Gamma_{FG}[[t]]$. Thus $t \Pi$ and $1 + t \Pi$ are the subsets consisting of all power series with constant terms 0 and 1, respectively. There are mutually inverse functions $\exp : t \Pi \to 1 + t \Pi$ and $\log : 1 + t \Pi \to t \Pi$ such that, for $f \in t \Pi$ and $g \in 1 + t \Pi$,

$$\exp(f) = 1 + f + f^2/2! + f^3/3! + \cdots$$

and

$$\log(g) = (g - 1) - (g - 1)^2/2 + (g - 1)^3/3 - \cdots.$$ 

If $V \in \text{Mod}(FG)$, we also write $V$ for the element of $R_{FG}$ or $\Gamma_{FG}$ determined by $V$. Thus, for example, $T^r(V)$ as an element of $R_{FG}$ denotes the isomorphism class of the module $T^r(V)$ and it is equal to $V^r$.

We start with a discussion of symmetric powers and Adams operations. For $V \in \text{Mod}(FG)$, let $S(V)$ denote the polynomial algebra (free commutative associative algebra) over $F$ freely generated by any basis of $V$. The action of $G$ on $V$ extends to $S(V)$ so that $G$ acts by algebra automorphisms. For $r \geq 0$, the $r$th homogeneous component $S^r(V)$ is an $FG$-submodule of $S(V)$ called the $r$th symmetric power of $V$.

For $V \in \text{Mod}(FG)$, let $S(V, t) \in 1 + t \Pi$ be defined by

$$S(V, t) = 1 + S^1(V)t + S^2(V)t^2 + \cdots.$$ 

It is well known and easy to verify that, for $U, V \in \text{Mod}(FG)$, we have

$$S(U \oplus V, t) = S(U, t)S(V, t).$$

It follows that there is a $\mathbb{Q}$-linear function $\psi : \Gamma_{FG} \to t \Pi$ satisfying

$$\psi(V) = \log(S(V, t))$$ (3.1)
for all $V \in \text{Mod}(FG)$. Hence we may define a function $S^+ : t\Pi \to t\Pi$ by

$$S^+(A_1t + A_2t^2 + A_3t^3 + \cdots) = \psi(A_1) + \psi(A_2)_t + \psi(A_3)_{t^2} + \cdots,$$

(3.2)

for all $A_1, A_2, \ldots \in \Gamma_{FG}$, where the subscript $t \mapsto t^r$ denotes the operation of replacing a power series $X_1t + X_2t^2 + \cdots$ by $X_1t^r + X_2t^{2r} + \cdots$. The properties of $S^+$ given in the following lemma are readily obtained from the definition.

**Lemma 3.1.** The function $S^+$ is $\mathbb{Q}$-linear and $S^+(t^r\Pi) \subseteq t^r\Pi$, for all $r \geq 1$. For all $f \in t\Pi$ and all $r \geq 1$, $S^+(f_{t^r}) = S^+(f)_{t^r}$. If $f_i \in t\Pi$ for $i = 1, 2, \ldots$, then $S^+(\sum f_i) = \sum S^+(f_i)$.

We now define a function $S^* : t\Pi \to 1 + t\Pi$ as the composite

$$S^* = \exp \circ S^+.$$

(3.3)

It is clear from (3.1) and (3.2) that $S^*(Vt) = S(V, t)$ for all $V \in \text{Mod}(FG)$. Also, since $S^+$ is additive, $S^*(f + g) = S^*(f)S^*(g)$ for all $f, g \in t\Pi$.

For $A \in \Gamma_{FG}$, we may define $\psi^1(A), \psi^2(A), \ldots \in \Gamma_{FG}$ by the equation

$$S^+(At) = \psi(A) = \psi^1(A)t + \frac{1}{2}\psi^2(A)t^2 + \frac{1}{3}\psi^3(A)t^3 + \cdots.$$

(3.4)

Thus we obtain $\mathbb{Q}$-linear functions $\psi^r : \Gamma_{FG} \to \Gamma_{FG}$. These functions were denoted by $\psi^r$ in [1, Section 5]: they are the Adams operations on $\Gamma_{FG}$ determined by symmetric powers. (Adams operations, different in general, can also be defined using exterior powers.) By [1, Section 5], if $V \in \text{Mod}(FG)$ then $\psi^r(V) \in R_{FG}$. Thus $\psi^r$ restricts to a $\mathbb{Z}$-linear function $\psi^r : R_{FG} \to R_{FG}$.

If $V \in \text{Mod}(FG)$ then, by (3.1) and (3.4),

$$\log(S(V, t)) = \psi^1(V)t + \frac{1}{2}\psi^2(V)t^2 + \cdots.$$

This equation shows that symmetric powers may be expressed in terms of Adams operations, and vice versa. Also, by [1, Theorem 5.4], we have the following ‘factorisation’ result.

**Lemma 3.2.** If $r$ and $s$ are positive integers such that $r$ is not divisible by the characteristic of $F$, then $\psi^{rs} = \psi^r \circ \psi^s$. In particular, if $F$ has prime characteristic $p$, then $\psi^{p^mk} = \psi^k \circ \psi^p$ for all non-negative integers $m$ and all positive integers $k$ not divisible by $p$.

All the results stated above for symmetric powers have analogues for exterior powers. However, we shall not need exterior powers for the applications in this paper.

We now turn to Lie powers and Lie resolvents. The theory is based on a function $L_{FG} : t\Pi \to t\Pi$ called the Lie module function. When $F$ and $G$ are understood, we write $L$ instead of $L_{FG}$. The properties of this function are described in [1, Sections 2 and 3]. In particular, by [1, Lemma 3.1],

$$L(Vt) = L^1(V)t + L^2(V)t^2 + \cdots,$$

(3.5)

for all $V \in \text{Mod}(FG)$ and $r \geq 1$, and

$$L(f) + L(g) = L(f + g - fg),$$

(3.6)

for all $f, g \in t\Pi$.

There are advantages in considering a modification of $L$, namely the function $L^* : 1 + t\Pi \to t\Pi$ defined by

$$L^*(f) = -L(1 - f)$$

(3.7)

for all $f \in 1 + t\Pi$. It follows from (3.5), (3.6) and (3.7) that

$$-L^*(1 - Vt) = L^1(V)t + L^2(V)t^2 + \cdots,$$

for all $V \in \text{Mod}(FG)$, and $L^*(fg) = L^*(f) + L^*(g)$, for all $f, g \in 1 + t\Pi$. 
We may define a function $L^+: t\Pi \to t\Pi$ by $L^+ = L^* \circ \exp$. Thus $L^+$ is additive and

$$L^* = L^+ \circ \log.$$  

(3.8)

Let $\text{Exp}: t\Pi \to t\Pi$ be defined by $\text{Exp}(f) = 1 - \exp(-f)$ for all $f \in t\Pi$. Since

$$L^+(f) = -L^+(-f) = -L^*(\exp(-f)) = \mathcal{L}(1 - \exp(-f)),$$

we obtain

$$L^+ = \mathcal{L} \circ \text{Exp}.$$  

(3.9)

Additional properties of $L^+$ are given in [1, Section 3], where $L^+$ is denoted by $F_{FG}$. These properties yield the following result.

Lemma 3.3. The function $L^+$ has the properties of $S^+$ stated in Lemma 3.1.

In particular, $L^+$ is $\mathbb{Q}$-linear.

For $A \in \Gamma_{FG}$, we may define $\Phi_1(A), \Phi_2(A), \ldots \in \Gamma_{FG}$ by the equation

$$L^+(At) = \Phi_1(A)t + \frac{1}{2} \Phi_2(A)t^2 + \frac{1}{3} \Phi_3(A)t^3 + \cdots.$$  

(3.10)

Thus we obtain $\mathbb{Q}$-linear functions $\Phi^r: \Gamma_{FG} \to \Gamma_{FG}$. These functions were considered in [1], where they were written $\Phi^r_{FG}$ and called the Lie resolvents for $G$ over $F$. They restrict to $\mathbb{Z}$-linear functions $\Phi^r: R_{FG} \to R_{FG}$. Lie powers may be expressed in terms of Lie resolvents and vice versa by means of the following expressions given in [1, Corollary 3.3]: for all $V \in \text{Mod}(FG)$ and every positive integer $r$,

$$L^r(V) = \frac{1}{r} \sum_{d|r} \Phi^d(V^{r/d})$$  

and

$$\Phi^r(V) = \sum_{d|r} \mu(r/d)dL^d(V^{r/d}),$$

where $\mu$ denotes the Möbius function. Also, by [1, Corollary 6.2],

$$\Phi^r = \mu(r)\psi^r \quad \text{if char}(F) \nmid r.$$  

(3.13)

We conclude this section with one further lemma.

Lemma 3.4. Let $f \in t\Pi$, where $f = A_1t + A_2t^2 + \cdots$. Then

$$L^+(f) = \sum_{r \geq 1} \left( \sum_{d|r} \frac{1}{d} \Phi^d(A_{r/d}) \right) t^r$$

and

$$S^+(f) = \sum_{r \geq 1} \left( \sum_{d|r} \frac{1}{d} \Phi^d(A_{r/d}) \right) t^r.$$  

Proof. By (3.10) and (3.4), and in the terminology of [1, Section 2], the functions $\frac{1}{r} \Phi^r$ and $\frac{1}{r} \psi^r$ are the ‘components’ of $L^+$ and $S^+$, respectively. Hence the result follows from [1, (2.5)]. \qed

4. The Factorisation Theorem

Let $F$ be an infinite field and $n$ a positive integer. We write $G(n) = GL(n, F)$. We require some facts about polynomial modules and their characters. Most of these have already been collected in [1, Section 5], so we use this as
a convenient reference: but see also [8]. As in [1, Section 5], let $R_{FG(n)}^{\text{poly}}$ denote the subring of the Green ring $R_{FG(n)}$ spanned by all the isomorphism classes of finite-dimensional polynomial modules. It is clear from (3.12) that, for each $r$, the Lie resolvent $\Phi^r$ restricts to a map $\Phi^r : R_{FG(n)}^{\text{poly}} \to R_{FG(n)}^{\text{poly}}$.

Let $t_1, \ldots, t_n$ be indeterminates and let $\Delta$ be the subring of $\mathbb{Z}[t_1, \ldots, t_n]$ consisting of all symmetric polynomials. For each positive integer $r$, the endomorphism of $\mathbb{Z}[t_1, \ldots, t_n]$ satisfying $t_i \mapsto t_i^r$ for all $i$ restricts to an endomorphism of $\Delta$, which we denote by $\chi^r$. As explained in [1, Section 5], there is a ring homomorphism $\text{ch} : R_{FG(n)}^{\text{poly}} \to \Delta$ such that, for every finite-dimensional polynomial $FG(n)$-module $U$, $\text{ch}(U)$ is the formal character of $U$.

As stated in [6, Section 3.2], if $V$ is the natural $FG(n)$-module, then

$$\text{ch}(L^r(V)) = \frac{1}{r} \sum_{d|r} \mu(d)(t_1^d + \cdots + t_n^d)^{r/d}$$.  \hspace{1cm} (4.1)$$

Suppose that $U$ is a finite-dimensional polynomial $FG(n)$-module. Then we may write $\text{ch}(U) = w_1 + \cdots + w_m$, where $m = \dim U$ and $w_1, \ldots, w_m$ are monomials in $t_1, \ldots, t_n$. We may choose a basis of $U$ consisting of elements from weight spaces. Then every diagonal element of $G(n)$ is represented on $U$ by a diagonal element of $GL(m, F)$. By (4.1) with $m$ instead of $n$, we obtain

$$\text{ch}(L^r(U)) = \frac{1}{r} \sum_{d|r} \mu(d)(w_1^d + \cdots + w_m^d)^{r/d}.$$ 

Hence

$$\text{ch}(L^r(U)) = \frac{1}{r} \sum_{d|r} \mu(d) \chi^d(\text{ch}(U)^{r/d})).$$ \hspace{1cm} (4.2)$$

**Lemma 4.1.** Let $U$ be a finite-dimensional polynomial $FG(n)$-module.

(i) For all $r \geq 1$, $\text{ch}(\Phi^r(U)) = \mu(r) \chi^r(\text{ch}(U))$.

(ii) If $(r, s) = 1$, then $\text{ch}(\Phi^r(U)) = \text{ch}(\Phi^s(U))$.

**Proof.** By (3.11),

$$\text{ch}(L^r(U)) = \frac{1}{r} \sum_{d|r} \text{ch}(\Phi^d(U)^{r/d})).$$

Comparing this with (4.2) and using induction on $r$ gives (i). Hence, for all $W \in R_{FG(n)}^{\text{poly}}$,

$$\text{ch}(\Phi^r(W)) = \mu(r) \chi^r(\text{ch}(W)).$$ \hspace{1cm} (4.3)$$

Therefore

$$\text{ch}(\Phi^r(\Phi^s(U))) = \mu(r) \chi^r(\text{ch}(\Phi^s(U))) = \mu(r) \chi^r(\mu(s) \chi^s(\text{ch}(U))).$$

However, $\chi^r \circ \chi^s = \chi^{rs}$ and, if $r$ and $s$ are coprime, $\mu(r) \mu(s) = \mu(rs)$. Therefore

$$\text{ch}(\Phi^r(\Phi^s(U))) = \mu(rs) \chi^{rs}(\text{ch}(U)).$$

Hence, by (4.3), $\text{ch}(\Phi^r(\Phi^s(U))) = \text{ch}(\Phi^{rs}(U))$, as required for (ii). \hspace{1cm} $\square$

We recall the Decomposition Theorem (Theorem 2.1). The submodules $B_r$ are not uniquely determined by $V$, as easy examples show. However, it follows from the family of equations (2.1), by induction, that the $B_r$ are uniquely determined up to isomorphism. Thus they give uniquely determined elements of $R_{FG}$. We shall deduce the following result from the Decomposition Theorem.

**Theorem 4.2** (Factorisation Theorem). Let $F$ be a field of prime characteristic $p$. Let $G$ be a group. For every non-negative integer $m$ and every positive integer $k$ not divisible by $p$,

$$\Phi^{p^m} \circ \Phi^k = \Phi^{p^m k}$$ \hspace{1cm} (4.4)
and, for every finite-dimensional $FG$-module $V$, the elements $B_{\nu}$ of $RG$ obtained from the Decomposition Theorem satisfy

$$p^m B_{\nu} = p^{m-1} B_{\nu^{p^{-1}}} + \cdots + p B_{\nu^{p}} + B_{\nu} = L^k(V^{p^m}). \quad (4.5)$$

**Proof.** When we wish to show the dependence on $V$ on $E$, we write $B_{\nu}$ as $B'(V)$, and when we wish to show the role of $C$ and $D$ in $\Phi'$ we write it as $\Phi'_{FG}$. We first reduce to the case where $F$ is finite. Let $E$ be an infinite extension of $F$. Assume that the theorem holds with $E$ in place of $F$. Each $FG$-module $V$ determines an $EG$-module $E \otimes_F V$ by extension of scalars. Thus we obtain a ring homomorphism $\iota : R_{FG} \to R_{EG}$. It follows from the Noether–Deuring Theorem (see [5, (29.7)]) that $\iota$ is an embedding. By [3, Lemma 2.4], for all $r \geq 1$ and all $V \in \text{Mod}(FG)$, we have $L'(\iota(V)) = \iota(L'(V))$ and $\Phi'_{EG} \circ \iota = \iota \circ \Phi'_{FG}$. By (4.4) over $E$, $\Phi'_{EG} \circ \iota = \Phi'_{FG} \circ \iota$ and hence $\iota \circ \Phi'_{EG} = \iota \circ \Phi'_{FG}$. Since $\iota$ is an embedding, we obtain (4.4) over $F$. Let $V \in \text{Mod}(FG)$. Applying $\iota$ to the family of equations (2.1) over $F$, we find that $\iota(B'(V)) = B'(\iota(V))$ for all $r$. By (4.5) over $E$ for the module $\iota(V)$,

$$p^m B_{\nu} = p^{m-1} (B_{\nu^{p^{-1}}}(\iota(V))) + \cdots + (B_{\nu}(\iota(V)))^{p^m} = L^k(\iota(V)^{p^m}).$$

Thus

$$\iota(p^m B_{\nu}) = \iota(L^k(V^{p^m})).$$

Since $\iota$ is an embedding, we obtain (4.5) over $F$. Hence it is enough to prove the theorem over $E$. In other words, we may assume that $F$ is finite.

We use induction on $m$ and $k$. If $m = 0$, the result is clear, because $\Phi^1$ is the identity map and, for all $V$, $B_k(V) = L^k(V)$, by (2.1). Hence we may assume that $m \geq 1$ and that the result holds for $p d$ with $d$ not divisible by $p$ if $i < m$ or $i = m$ and $d < k$. Since the functions $\Phi^r$ are linear, in order to prove (4.4) it suffices to prove

$$\Phi^r_{\nu} = (\Phi^r_{\nu} \circ \Phi^k)(V) \quad (4.6)$$

for all $V \in \text{Mod}(FG)$.

Let $V \in \text{Mod}(FG)$ and $n = \dim V$. By choice of a basis of $V$, the representation of $G$ on $V$ gives a homomorphism $\theta : G \to G(n)$. Furthermore, $\theta$ induces a ring homomorphism $\theta^* : R_{FG(n)} \to R_{FG}$. We can regard $V$ as the natural module for $G(n)$, in which case we write it as $V(n)$. Thus $\theta^*(V(n)) = V$. We now show that it is enough to prove the required results for $G(n)$ and $V(n)$. Suppose that (4.6) and (4.5) hold for $G(n)$ and $V(n)$. By [3, Lemmas 2.2 and 2.3], for all $r \geq 1$ and all $U \in \text{Mod}(FG(n))$, we have $L'(\theta^*(U)) = \theta^*(L'(U))$ and $\theta^* \circ \Phi'_{FG(n)} = \Phi'_{FG} \circ \theta^*$. Thus, by applying $\theta^*$ to (4.6) for $G(n)$ and $V(n)$, we get (4.6) for $G$ and $V$. By applying $\theta^*$ to the family of equations (2.1) for $G(n)$ and $V(n)$, we get $\theta^*(B'(V(n))) = B'(V)$ for all $r$. Hence, by applying $\theta^*$ to (4.5) for $G(n)$ and $V(n)$, we get (4.5) for $G$ and $V$. Thus it remains to prove (4.6) and (4.5) for $G(n)$ and $V(n)$. To simplify the notation, write $V(n)$ for $V(n)$ and $B_r$ for $B'(V(n))$.

As in Section 3, let $\Pi = \Pi_{FG(n)}[\Pi]$. Let $\text{Log} : t \Pi \to t \Pi$ be defined by

$$\text{Log}(f) = - \log(1 - f) = f + f^2/2 + f^3/3 + \cdots$$

for all $f \in t \Pi$. Thus Log is the inverse of the function $\text{Exp}$ defined in Section 3. For $f \in t \Pi$ and $r \geq 1$, we write $f_r$ for the coefficient of $t^r$ in $f$; thus $f_r \in \text{Exp}(\Pi)$ and $f = \sum_{r \geq 1} f_r t^r$.

Let $Q' = \sum_{r \geq 0} \log(B_{r'}(t))$, $Q'' = \sum_{r \geq 0} B_{r'}(t)^{p^m} = Q - Q''$. Then it is easily calculated that $Q_{(r')} = \frac{1}{p^r} B_{r'} + \frac{1}{p^{r-1}} B_{r' - 1} + \cdots + B_{r' - k} - \frac{1}{p^r} \pi \pi (V^{p^m})$.

By the inductive hypothesis, $Q_{(r')} = 0$ for $i < m$. Hence, by Lemma 3.4, we obtain

$$Q_{(r')} = \frac{1}{p^m} B_{r'} + \frac{1}{p^{m-1}} B_{r' - 1} + \cdots + B_{r' - k} - \frac{1}{p^m} \pi \pi (V^{p^m}).$$

Thus

$$L^+(Q_{(r')}) = \Phi^1(Q_{(r')}) = Q_{(r')},$$

and

$$Q_{(r')} = \frac{1}{p^m} B_{r'} + \frac{1}{p^{m-1}} B_{r' - 1} + \cdots + B_{r' - k} - \frac{1}{p^m} \pi \pi (V^{p^m}).$$

Thus
Since $L^+$ is additive and $L^+ \circ \text{Log} = L$, by (3.9), we have

$$L^+(Q') = \sum_{i \geq 0} L(B_{p^i}t^{p^i}).$$

Thus, by (3.5),

$$L^+(Q')_{(p^m)} = L^{p^m}(B_k) + L^{p^{m-1}}(B_{pk}) + \cdots + L^1(B_{p^m_k}).$$

Therefore, by the Decomposition Theorem, $L^+(Q')_{(p^m)} = L^{p^m_k}(V)$. By Lemma 3.4,

$$L^+(Q'')_{(p^m)} = \frac{1}{p^m} \sum_{d | p^m} \Phi^d(L^k(V^{p^m/d})).$$

Hence, by (3.11),

$$L^+(Q'')_{(p^m)} = \frac{1}{p^m} \sum_{d | p^m} \Phi^d \left( \frac{1}{k} \sum_{e | k} \Phi^e(V^{p^m_k/d}) \right)
\quad = \frac{1}{p^m k} \sum_{d | p^m, e | k} (\Phi^d \circ \Phi^e)(V^{p^m_k/d}).$$

We write $\Phi^d \circ \Phi^e = \Phi^{de} = \Phi^{de}_k$ for $de < p^m$. Thus

$$L^+(Q'')_{(p^m)} = \frac{1}{p^m k} \sum_{d | p^m} \Phi^d((V^{p^m_k/d}) + \frac{1}{p^m k} (\Phi^m(\Phi^k(V)) - \Phi^{p^m_k}(V))
\quad = L^{p^m_k}(V) + \frac{1}{p^m k} (\Phi^m(\Phi^k(V)) - \Phi^{p^m_k}(V)).$$

Since $L^+(Q)_{(p^m)} = L^+(Q')_{(p^m)} - L^+(Q'')_{(p^m)}$, we obtain

$$\frac{1}{p^m} B_{p^m}^m + \frac{1}{p^m-1} B_{p^{m-1}}^m + \cdots + B_{p^m}^m - \frac{1}{p^m} L^k(V^{p^m}) = \frac{1}{p^m k} (\Phi^m(\Phi^k(V)) - \Phi^{p^m_k}(\Phi^k(V))).$$

Therefore

$$\frac{1}{k} (\Phi^{p^m_k}(V) - \Phi^{p^m}(\Phi^k(V))) = W,$$

where

$$W = p^m B_{p^m_k} + p^{m-1} B_{p^{m-1}k} + \cdots + p B_{p^m k} + B_{p^m_k} - L^k(V^{p^m}).$$

By Lemma 4.1, $\text{ch}(\Phi^{p^m_k}(V) - \Phi^{p^m}(\Phi^k(V))) = 0$. Thus $\text{ch}(W) = 0$. By the Decomposition Theorem, $B_{p^m_k}, B_{p^{m-1}k}, \ldots, B_{p^m_k}$ are isomorphic to direct summands of the tensor power $V^{p^m_k}$. Hence they are tilting modules: see [1, Section 5]. Since $p \nmid k$, $L^k(V^{p^m_k})$ is also a direct summand of $V^{p^m_k}$ (see, for example, [6, Section 3.1]). Thus, it too is a tilting module. However, tilting modules are determined up to isomorphism by their formal characters (see, for example, [6]). Since $\text{ch}(W) = 0$, it follows that $W = 0$. Thus $\Phi^{p^m_k}(V) - \Phi^{p^m}(\Phi^k(V)) = 0$. This gives (4.5) and (4.6). \qed

Note that the family of equations (4.5) gives a recursive description, within $\Gamma_{FG}$, of $B_{p^m_k}$ as a polynomial in $L^k(V), L^k(V^p), \ldots, L^k(V^{p^m})$. The polynomials in $B_k, B_{pk}, B_{p^2 k}, \ldots$ occurring on the left-hand side of (4.5) may be recognised as the Witt polynomials associated with the prime $p$: see [16, Chapter II, Section 6] or [11, Chapter 3]. Thus, in the terminology often used in relation to Witt vectors, $L^k(V), L^k(V^p), L^k(V^{p^2}), \ldots$ are the ‘ghost’ components of $(B_k, B_{pk}, B_{p^2 k}, \ldots)$. However, we have not yet been able to deduce from this more explicit information on the modules $B_{p^m_k}$.

Of particular interest is the case where $V$ is the natural module for $GL(n, F)$. Then, since the modules $B_k, B_{pk}, \ldots$ and $L^k(V), L^k(V^p), \ldots$ are direct summands of tensor powers of $V$, they are determined, up to isomorphism, by their
formal characters. We may therefore translate the equations of (4.5) into equations in symmetric functions. Closely related equations have been considered by Reutenauer [14] and Scharf and Thibon [15].

Statement (4.4) in the Factorisation Theorem is analogous to the second statement of Lemma 3.2 for Adams operations. The Factorisation Theorem and (3.13) reduce the study of Lie resolvents to the study of Adams operations and $p$-power Lie resolvents.

5. Symmetric powers and Lie powers revisited

Let $F$ be a field and $G$ a group. For each positive integer $r$, we may define a function $\rho^r : \Gamma_{FG} \to \Gamma_{FG}$ by

$$\rho^r = \frac{1}{r} \sum_{d|r} \phi^d \circ \psi^{r/d}. \quad (5.1)$$

Thus, since $\psi^1$ is the identity map, the Lie resolvents $\phi^r$ may be expressed recursively in terms of the functions $\rho^r$ and the Adams operations. Hence, if we assume the Adams operations, knowledge of the functions $\rho^r$ is equivalent to knowledge of the Lie resolvents.

**Theorem 5.1.** Let $G$ be a group and $F$ a field of prime characteristic $p$. Then $\rho^r = 0$, unless $r$ is a power of $p$.

**Proof.** Write $r = p^m k$, where $m \geq 0$ and $k$ is not divisible by $p$. By (5.1) and the Factorisation Theorem,

$$\rho^r = \frac{1}{r} \sum_{d|r} \phi^d \circ \psi^{r/d} \phi^{p^m k/e} \circ \psi^{p^m k/e}$$

Hence, by (3.13) and Lemma 3.2,

$$\rho^r = \frac{1}{r} \sum_{0 \leq i \leq m} \mu(e) (\phi^d \circ \psi^{e} \circ \psi^{p^m k/e}) = \frac{1}{r} \sum_{0 \leq i \leq m} \mu(e) (\phi^d \circ \psi^{p^m k/e}).$$

If $r$ is not a power of $p$, then $k > 1$ and so $\sum_{e|k} \mu(e) = 0$, which gives $\rho^r = 0$. □

**Lemma 5.2.** We have $L^* \circ S^* = L^+ \circ S^+$ and, for all $A \in \Gamma_{FG}$,

$$(L^* \circ S^*)(A) = \rho^1(A)t + \rho^2(A)t^2 + \cdots.$$

**Proof (See also [2, Lemma 4.1]).** By (3.3) and (3.8), $L^* \circ S^* = L^+ \circ S^+$. Also, by (3.4) and Lemma 3.4,

$$L^+(S^+(A)) = L^+ \left( \psi^1(A)t + \frac{1}{2}\psi^2(A)t^2 + \cdots \right)$$

$$= \sum_{r \geq 1} \left( \sum_{d|r} \frac{1}{d} \phi^d ((d/r)\psi^{r/d}(A)) \right) t^r.$$

Hence, by the linearity of $\phi^d$ and (5.1),

$$(L^* \circ S^*)(A) = (L^+ \circ S^+)(A) = \sum_{r \geq 1} \rho^r(A)t^r. \quad \Box$$

Recall that $II = \Gamma_{FG}[[t]]$. An element of $tII$ is said to be $p$-typical if, for every positive integer $r$, the coefficient of $t^r$ is zero unless $r$ is a power of $p$. 

Theorem 5.3. Let $G$ be a group and $F$ a field of prime characteristic $p$. Then $(L^* \circ S^*)(f)$ is $p$-typical for every $p$-typical element $f$ of $t \Pi$.

Proof. By Lemma 5.2, $L^* \circ S^* = L^+ \circ S^+$. By Theorem 5.1 and Lemma 5.2, $(L^+ \circ S^+)(A \tau) = p$-typical for all $A \in tFG$. By Lemmas 3.1 and 3.3, $L^+ \circ S^+$ has the properties of $S^+$ stated in Lemma 3.1. It follows that $(L^+ \circ S^+)(f)$ is $p$-typical for every $p$-typical element $f$ of $t \Pi$. □

The functions $\rho^r$ seem to have some importance in the study of Lie powers. As we have already seen, they may be used instead of the Lie resolvents, but, on the available evidence, their properties seem to be smoother. Theorem 5.1 shows that $\rho^r = 0$, unless $r$ is a power of $p$. It is remarkable also that, in the cases which have so far been calculated, even the functions $\rho^1$, $\rho^p$, $\rho^{p^2}$, ... are well behaved. Of course, $\rho^1$ is the identity function. It follows from [2, Corollary 4.5 and Lemma 4.6] that, if $G$ is cyclic of order $p$ (and $F$ has characteristic $p$), then $\rho^{p^m} = 0$ for all $m > 1$. In fact, from the results in [2] and [3], it is not difficult to deduce the same fact for every finite group $G$ such that $p^m > |G|$. It is interesting to speculate on how far this generalises to other groups: perhaps, if $G$ is finite, we have $\rho^{p^m} = 0$ for all sufficiently large $m$.

We conclude with a few remarks about the easier case where $F$ has characteristic 0. In this case, by (3.13), $\phi^r = \mu(r)\psi^r$ for all $r$. By a simplified version of the calculation of Theorem 5.1 we obtain $\rho^r = 0$ for all $r > 1$.

Thus, by Lemma 5.2, $(L^+ \circ S^+)(A \tau) = A \tau$ for all $A \in tFG$. By the properties of $S^+$ and $L^+$, it follows that $L^+ \circ S^+$ is the identity function on $t \Pi$. A similar calculation shows that $S^* \circ L^+$ is the identity function. However, $L^* \circ S^* = L^+ \circ S^+$ and

$$S^* \circ L^* = \exp \circ S^+ \circ L^+ \circ \log.$$  

Thus we have the following result, closely related to results of Joyal [12] and Reutenauer [14].

Theorem 5.4. Let $G$ be a group and $F$ a field of characteristic 0. Then $L^* \circ S^*$ is the identity function on $t \Pi$ and $S^* \circ L^*$ is the identity function on $1 + t \Pi$.

Recall that, by (3.7), $L^*(f) = -L(1 - f)$ for all $f \in 1 + t \Pi$. Since $S^* \circ L^*$ is the identity function in characteristic 0, it follows easily that

$$S^*\left(L(g)\right) = (1 - g)^{-1} = 1 + g + g^2 + \cdots$$

for all $g \in t \Pi$. This may be regarded as a version of the Poincaré–Birkhoff–Witt Theorem (by taking $g = Vt$) and it is similar to a result of Joyal [12, Chapter 4, Proposition 1] (see also [14, Lemma 3.2]). Similarly, the fact that $L^* \circ S^*$ is the identity function is a version of a result of Reutenauer [14, Theorem 3.1].

Acknowledgement

The second author was supported by Deutsche Forschungsgemeinschaft (DFG-Scho 799).

References