Inventiones math. 37, 109 – 120 (1976)

Inventiones mathematicae

The Structure of Morava Stabilizer Algebras

Douglas C. Ravenel*

Department of Mathematics, Columbia University, New York, N.Y. 10027, USA

§0. Introduction

The purpose of this note is to prove some general theorems which will facilitate the computation of $\mathrm{Ext}^*_{BP_*BP}(BP_*, v_n^{-1} BP_*/I_n)$, where $I_n=(p, v_1, \ldots, v_{n-1})$ is the n-th invariant prime ideal in BP_*. Specific calculations and applications to the Novikov spectral sequence will be exposed in [8] and [13].

This paper is a sequel to [4] in that we reprove some results of Morava ([10] and [11]) with more conventional algebraic topological methods. Our approach differs from those of Morava and Johnson-Wilson in that no use is made of any cohomology theories other than Brown-Peterson theory. Our results have the advantage of being more directly applicable to homotopy theoretic computations than Morava's were.

Although none of his results are actually used here, this paper owes its existence to many inspiring and invaluable conversations with Jack Morava. I would also like to thank Haynes Miller, John Moore, Robert Morris, and Steve Wilson for their interest and help.

In §1 we use the change of rings theorem of [7] to show that computing the above mentioned Ext group is equivalent to computing the cohomology of a certain Hopf algebra $S(n)$, which we call the Morava stabilizer algebra. We describe it explicitly using the results of [12].

In §2 we describe the relation of $S(n)$ to a certain compact p-adic Lie group S_n which Morava called the stabilizer group, as it was the isotropy group of a certain point in a scheme with a certain group action in [10]. This group has been studied to some extent by number theorists but we do not exploit this fact. Its basic cohomological properties were originally found by Morava and the author (very likely not for the first time) by application of the results of Lazard [5]. The results of §3, however, make no use of [5] or even of the existence of S_n, and §3 is independent of §2. We do however use this group theoretic interpretation to get a certain splitting (Theorem (2.12)) of $S(n)$ when p does not divide n.

* Supported in part by NSF grant MPS72 05055 A02

** Current address: Department of Mathematics, University of Washington, Seattle, WA 98195, USA

In § 3 we define a certain filtration of $S(n)$ and describe the associated graded Hopf algebra $E_0 S(n)$ as the enveloping algebra of a restricted Lie algebra. Hence the machinery of [6] may be applied to the computation of $H^* E_0 S(n)$ and $H^* S(n)$. This will be done in a subsequent paper.

§ 1. The Definition and Structure of $S(n)$

Let $K(n)_* = \mathbb{F}_p[v_n, v_n^{-1}]$ and regard it as a BP_*-algebra via the ring homomorphism sending v_i to 0 for $i \neq n$. Let

$$K(n)_* K(n) = K(n)_* \otimes_{BP_*} BP_* BP \otimes_{BP_*} K(n)_*.$$

Then by the main result of [7] we have

(1.1) **Theorem.**

$$\mathrm{Ext}^*_{BP_* BP}(BP_*, v_n^{-1} BP_*/I_n) \cong \mathrm{Ext}^*_{K(n)_* K(n)}(K(n)_*, K(n)_*). \quad \square$$

Since v_n is invariant under $BP_* BP$ modulo I_n, $K(n)_* K(n)$ is a commutative biassociative Hopf algebra over $K(n)_*$.

Now $K(n)_*$ is a graded field in the sense that every graded module over it is free. (If M is such a module, then M_i is canonically isomorphic to $M_{i+2(p^n-1)}$ since $\dim v_n = 2(p^n-1)$.) Hence the category of graded $K(n)_*$-modules is equivalent to that of $\mathbb{F}_p$-modules graded over $\mathbb{Z}/2(p^n-1)$. We define

$$S(n)_* = K(n)_* K(n) \otimes_{K(n)_*} \mathbb{F}_p$$

where $K(n)_*$ and $K(n)_* K(n)$ are here regarded as graded over $\mathbb{Z}/2(p^n-1)$ and $\mathbb{F}_p$ is a $K(n)_*$-algebra via the map sending v_n to 1.

$S(n)$ will denote the linear dual of $S(n)_*$, but some care is required for its definition. We can regard $BP_* BP$ as $\varinjlim BP_* BP^i$ where $BP_* BP^i = BP_*[t_1 \dots t_i] \subset BP_* BP$. We define $K(n)_* K(n)^i$ and $S(n)^i_*$ accordingly, so $S(n)_* = \varinjlim S(n)^i_*$ with the discrete topology. It will follow from Proposition (1.3) below that $S(n)^i_*$ is finite dimensional so we define $S(n)^i = \mathrm{Hom}(S(n)^i_*, \mathbb{F}_p)$ and $S(n) = \varprojlim S(n)^i$. $S(n)$ is compact and complete in the inverse limit topology. $S(n)$ is also equipped with a completed cocommutative coproduct, i.e. a map

$$\hat{\Delta}: S(n) \to S(n) \hat{\otimes} S(n) = \varprojlim \mathrm{Hom}(S(n)^i_* \otimes S(n)^j_*, \mathbb{F}_p).$$

Hence $S(n)$ could be called a cocommutative profinite Hopf algebra.

The category of graded $K(n)_* K(n)$-comodules is equivalent to that of cyclically graded $S(n)_*$-comodules, so we have

(1.2) **Proposition.**

$$\mathrm{Ext}_{K(n)_* K(n)}(K(n)_*, K(n)_*) \otimes_{K(n)_*} \mathbb{F}_p \cong \mathrm{Ext}_{S(n)_*}(\mathbb{F}_p, \mathbb{F}_p). \quad \square$$

The latter group will be denoted by $H^* S(n)$. For the algebra structures of $S(n)_*$ and $K(n)_* K(n)$ we have

(1.3) **Proposition.** *As algebras*

$$K(n)_* K(n) \cong K(n)_*[t_1, t_2, \dots]/(v_n t_i^{p^n} - v_n^{p^i} t_i)$$

and

$$S(n)_* \cong \mathbb{F}_p[t_1, t_2 \ldots]/(t_i^{p^n} - t_i)$$

where $\dim t_i = 2(p^i - 1)$.

Proof. We have

$$\begin{aligned} K(n)_* K(n) &= K(n)_* \otimes_{BP_*} BP_* BP \otimes_{BP_*} K(n) \\ &= K(n)_*[t_1, t_2 \ldots] \otimes_{BP_*} K(n)_* \\ &= K(n)_*[t_1, t_2 \ldots]/(\eta_R v_{n+i}). \end{aligned}$$

Now it follows from Theorem 1 of [12] that in $K(n)_*[t_1, t_2 \ldots]$,

$$\eta_R v_{n+i} \equiv v_n t_i^{p^n} - v_n^{p^i} t_i \bmod (\eta_R v_{n+1}, \ldots, \eta_R v_{n+i-1})$$

and the result follows. □

The coproduct and conjugation of $S(n)_*$ are essentially those inherited from $BP_* BP$. In order to give precise formulae we need some more notation. Let $\tilde{K}(n)_* = \mathbb{Z}_{(p)}[v_n]$ and $\tilde{\tilde{K}}(n)_* = \mathbb{Q}[v_n]$. Let

$$\tilde{\tilde{K}}(n)_*[[x]] \ni \log x = \sum_{i \geq 0} v_n^{a_i} \frac{x^{p^{in}}}{p^i}$$

where $a_i = (p^{in} - 1)/(p^n - 1)$. Then define $\tilde{F}(x, y) \in \tilde{\tilde{K}}(n)_*[[x, y]]$ by $\log \tilde{F}(x, y) = \log x + \log y$.

Then we have

(1.4) **Theorem.** *$\tilde{F}(x, y)$ is a commutative formal group law over $\tilde{K}(n)_*$, i.e.*

$$\tilde{F}(x, y) \in \tilde{K}(n)_*[[x, y]] \quad \tilde{F}(x, 0) = \tilde{F}(0, x) = x,$$

$$\tilde{F}(x, y) = \tilde{F}(y, x) \quad \text{and} \quad \tilde{F}(\tilde{F}(x, y), z) = \tilde{F}(x, \tilde{F}(y, z)).$$

Proof. This is a consequence of Hazewinkel's theorem ([3], 1.2). □

Hence $\tilde{F}(x, y)$ has a mod p reduction which we denote by $F(x, y) \in K(n)_*[[x, y]]$. As in [12] we define $\sum_{i=1}^{m}{}^F x_i \in K(n)_*[[x_1, \ldots, x_m]]$ inductively by

$$\sum_{i=1}^{m}{}^F x_i = F\left(\sum_{i=1}^{m-1}{}^F x_i, x_m\right).$$

Now the coproduct Δ and conjugation c are those inherited from $BP_* BP$ and are given by

$$(1.5) \quad \sum_{i \geq 0}{}^F \Delta(t_i) = \sum_{i, j \geq 0}{}^F t_i \otimes t_j^{p^i}$$

and

$$(1.6) \quad \sum_{i, j \geq 0}{}^F t_i c(t_j)^{p^i} = 1, \quad \text{where } t_0 = 1.$$

These occur as formulae (17) and (19) of [12], where it is observed that they can be regarded as structure formulae for $BP_* BP$.

In order to get a more explicit formula for the coproduct in $K(n)_* K(n)$ we need the following

(1.7) **Lemma.** *In $\tilde{K}(n)_*[[x_1, \ldots, x_m]]$ there are unique symmetric homogeneous polynomials $w_{j,n}(x_1 \ldots x_m)$ of degree p^{nj} such that*

$$\sum_i^F x_i = \sum_{j \geqq 0}^F v_n^{a_j} w_{j,n}(x_1 \ldots x_m)$$

where $a_j = (p^{nj}-1)/(p^n-1)$ and $w_{0,n}(x_1 \ldots x_m) = \sum x_i$.

Proof. If we take the log of both sides we get

$$\sum_{\substack{k \geqq 0 \\ i}} v_n^{a_k} \frac{x_i^{p^{nk}}}{p^k} = \sum_{k,j \geqq 0} v_n^{a_{k+j}} \frac{w_{j,n}(x_1 \ldots x_m)^{p^{nk}}}{p^k}$$

which in degree p^{nk} gives us

$$(1.71) \quad \sum x_i^{p^{nk}} = w_{0,n}(x_1^{p^{nk}}, \ldots, x_m^{p^{nk}}) = \sum_{j \geqq 0} p^j w_{j,n}(x_1, \ldots, x_m)^{p^{n(k-j)}}.$$

We can use this to define $w_{k,n}$ inductively if we can show that

$$w_{0,n}(x_1^{p^k}, \ldots, x_m^{p^k}) \equiv \sum_{0 \leqq j < k} p^j w_{j,n}(x_1 \ldots x_m)^{p^{n(k-j)}} \bmod p^k$$

or equivalently

$$(1.72) \quad w_{0,n}(x_1^{p^{(k+1)n}}, \ldots, x_m^{p^{(k+1)n}}) \equiv \sum_{0 \leqq j \leqq k} p^j w_{j,n}(x_1, \ldots, x_m)^{p^{n(1+k-j)}} \bmod p^{k+1}.$$

We will do this inductively, deriving (1.72) from (1.71) and observing that the statement is trivially true for $k=0$.

Now it follows from the binomial theorem that $f \equiv g \bmod p$ implies $f^{p^{ni}} \equiv g^{p^{ni}} \bmod p^{i+1}$ for any f and g. We also have

$$w(x_1^{p^n} \ldots x_m^{p^n}) \equiv w(x_1, \ldots, x_m)^{p^n} \bmod p,$$

so

$$p^j w_{j,n}(x_1^{p^n} \ldots x_m^{p^n})^{p^{n(k-j)}} \equiv p^j w_{j,n}(x_1, \ldots, x_m)^{p^{n(1+k-j)}} \bmod p^{k+1}.$$

This enables us to derive (1.72) from (1.71) by replacing x_i by $x_i^{p^n}$. □

For $n=1$, this Lemma is essentially due to Witt (see [1], Lemma 3).

Lemma (1.7) enables us to give a recursive formula for the coproduct in $S(n)_*$. Let M_i denote the $(i+1)$-ple of elements in $S(n)_* \otimes S(n)_*$, $(t_k \otimes t_{i-k}^{p^k})$ with $0 \leqq k \leqq i$. Let $i = jn+l$ with $0 < l \leqq n$ and define the $(2j)$-ple Δ_i recursively by

$$\Delta_i = (w_{0,n}(M_i), w_{1,n}(M_{i-n})), \ldots, w_{j,n}(M_l),$$

$$w_{1,n}(\Delta_{i-n}), \quad w_{2,n}(\Delta_{i-2n}) \ldots w_{j-1,n}(\Delta_{n+l})$$

and $\Delta_i = \phi$ (the empty set) for $j=0$.

Then we have

(1.8) **Theorem.** *The coproduct in $S(n)_*$ is given by*

$$\Delta(t_i) = \begin{cases} w_{0,n}(M_i) & \text{for } i \leqq n \\ w_{0,n}(\Delta_i) & \text{for } i > n. \end{cases}$$

Proof. This follows by straightforward iterated application of Lemma (1.7) to (1.5). □

Remark. It is immediate that $w_{1,n}(x_i) = -C_{p^n}(x_i) = p^{-1}(\sum(x_i^{p^n}) - (\sum x_i)^{p^n})$, so Theorem (1.8) gives an expression for $\Delta(t_i)$ for $i \leqq 2n$ analogous to Theorem 8 of [12].

§ 2. The Algebra $S(n)$ and the Group S_n

Our purpose in this section is to show that $S(n) \otimes \mathbb{F}_{p^n}$, regarded as an ungraded profinite Hopf algebra, is isomorphic to the $\mathbb{F}_{p^n}$ group algebra of a certain profinite group S_n. In proving this result we essentially recompute the endomorphism ring of a formal group over $\mathbb{F}_{p^n}$ of height n (see [2], III § 2). Most of the argument is well known but as far as we know it has not appeared in a form suitable for our purposes, so we find it convenient to give a detailed proof.

We will show how the cyclic grading on $S(n) \otimes \mathbb{F}_{p^n}$ can be recovered from an eigenspace decomposition associated with an action of $\mathbb{F}_{p^n}^\times$. Finally we will describe a representation of S_n which will lead to a splitting of $S(n)$ when n is not divisible by p.

Throughout this section we set $q = p^n$. We will make extensive use of the formal group law $F(x, y)$ over $K(n)_*$ defined in (1.4), its reduction to $\mathbb{F}_p$ (by sending v_n to $1 \in \mathbb{F}_p$), and the extension of the latter to $\mathbb{F}_q$. The same notation will be used for all three as the ground ring will be clear from the context. $\mathbb{Z}_p$ will denote the ring of p-adic integers and $W(\mathbb{F}_q)$ the Witt ring of $\mathbb{F}_q$, i.e. the extension of $\mathbb{Z}_p$ obtained by adjoining $(q-1)$-th roots of unity. We will use the following well-known facts about $W(\mathbb{F}_q)$.

(2.1) **Lemma.** a) *$W(\mathbb{F}_q)$ is a complete local ring with maximal ideal (p) and residue field $\mathbb{F}_q$.*

b) *Its group of units $W(\mathbb{F}_q)^\times$ is $\mathbb{F}_q^\times \otimes W(\mathbb{F}_q)$, for $p > 2$, where $\mathbb{F}_q^\times \cong \mathbb{Z}/(q-1)$, and $Z/2 \oplus \mathbb{F}_q^\times \oplus W(\mathbb{F}_q)$ for $p = 2$.*

c) *$W(\mathbb{F}_q)$ is a free $\mathbb{Z}_p$-module of rank n.*

d) *Any element $w \in W(\mathbb{F}_q)$ can be expressed uniquely as $w = \sum_{i \geqq 0} w_i p^i$ where each w_i satisfies $w_i^q = w_i$.*

e) *The Galois group of $W(\mathbb{F}_q)$ over $\mathbb{Z}_p$ is cyclic of order n and generated by the Frobenius automorphism $(\cdot)^\sigma$ given by $w^\sigma = \sum_{i \geqq 0} w_i^p p^i$ in the notation of* d).

Proof. See [1] or [14]. □

Let $E_n = W(\mathbb{F}_q)\langle\langle S \rangle\rangle / (S^n - p)$ where S is a noncommuting power series indeterminate with $Sw = w^\sigma S$. The following properties of E_n are immediate.

(2.2) **Proposition.** a) *E_n is a $\mathbb{Z}_p$-algebra of rank n^2.*

b) *E_n is generated as a $\mathbb{Z}_p$-algebra by S and a primitive $(q-1)$-th root of unity $\omega \in W(\mathbb{F}_q)$; the relations $S\omega = \omega^p S$ and $S^n = p$ completely determine the structure of E_n.*

c) *$E_n \otimes \mathbb{Q}_p$ is a division algebra over $\mathbb{Q}_p$ (the p-adic numbers) with Hasse invariant $1/n$.* □

(2.2)c) will not be used here. For literature on division algebras over $\mathbb{Q}_p$, see [15].

We now define $S_n \subset E_n$ to be the group of units congruent to one modulo (S). Then the main result of this section is

(2.3) **Theorem.** *$S(n) \otimes \mathbb{F}_q \cong \mathbb{F}_q[S_n]$ as profinite Hopf algebras, where we disregard the grading on $S(n)$.*

Proof. We will state several Lemmas as needed and prove them below.

Our first task is to show that $S(n) \otimes \mathbb{F}_q$ is a group algebra. A cocommutative Hopf algebra is a group algebra iff it has a basis $\{x_i\}$ of group like elements (i.e. $\Delta(x_i) = x_i \otimes x_i$) (see [16], Proposition 3.2.1). This is equivalent to the existence of a dual basis $\{y_i\}$ with $y_i^2 = y_i$ and $y_i y_j = 0$ for $i \neq j$. Since $S(n)_* \otimes \mathbb{F}_q$ is a tensor product of algebras isomorphic to $R = \mathbb{F}_q[t]/(t^q - t)$, it suffices to produce such a basis for R. Let $a \in \mathbb{F}_q^\times$ be a generator and let

$$r_i = \begin{cases} -\sum\limits_{0<j<q} (a^i t)^j & \text{for } 0 < i < q \\ 1 - t^{q-1} & \text{for } i = 0. \end{cases}$$

Then $\{r_i\}$ is such a basis, so $S(n) \otimes \mathbb{F}_q$ is a group algebra.

For the moment let $G(n)$ denote the corresponding group. We will now define a left action of $G(n)$ on the algebra $\mathbb{F}_q[[x]]$ by defining a completed left comodule structure of $\mathbb{F}_q[[x]]$ over $S(n)_* \otimes \mathbb{F}_q$. We will need

(2.4) **Lemma.** *For any $a \in \mathbb{F}_q$, $F(ax, ay) = aF(x, y)$.* □

We now define the comodule structure map $\psi: \mathbb{F}_q[[x]] \to S(n)_* \hat{\otimes} \mathbb{F}_q[[x]]$ to be an algebra homomorphism given by

$$\psi(x) = \sum_{i \geq 0}^F t_i \otimes x^{p^i}$$

where $t_0 = 1$ as usual. To verify that this makes sense we must show that the following diagram commutes.

$$\begin{array}{ccc} \mathbb{F}_q[[x]] & \xrightarrow{\psi} & S(n)_* \hat{\otimes} \mathbb{F}_q[[x]] \\ \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \Delta \otimes 1} \\ S(n)_* \hat{\otimes} \mathbb{F}_q[[x]] & \xrightarrow{1 \otimes \psi} & S(n)_* \hat{\otimes} S(n)_* \hat{\otimes} \mathbb{F}_q[[x]] \end{array}$$

for which we have

$$\begin{aligned} (\Delta \otimes 1)\psi(x) &= (\Delta \otimes 1) \sum_{i \geq 0}^F t_i \otimes x^{p^i} \\ &= \sum_{i \geq 0}^F \Big(\sum_{j+k=i}^F t_j \otimes t_k^{p^j} \Big) \otimes x^{p^i} \\ &= \sum_{j,k \geq 0}^F t_j \otimes t_k^{p^j} \otimes x^{p^{j+k}}. \end{aligned}$$

This can be seen by inserting x as a dummy variable in (1.5). We also have

$$\begin{aligned}(1\otimes\psi)\psi(x)&=(1\otimes\psi)\Big(\sum_{j\geqq 0}^{F} t_i\otimes x^{p^i}\Big)\\&=\sum_{i\geqq 0}^{F} t_i\otimes\Big(\sum_{j\geqq 0}^{F} t_j\otimes x^{p^j}\Big)^{p^i}\\&=\sum_{i,j\geqq 0}^{F} t_i\otimes t_j^{p^i}\otimes x^{p^{i+j}}.\end{aligned}$$

The last equality follows from the fact that $F(x^p, y^p)=F(x, y)^p$. The linearity of ψ follows from Lemma (2.4), so ψ defines an $S(n)_*\otimes\mathbb{F}_q$-comodule structure on $\mathbb{F}_q[[x]]$.

We can regard the t_i as continuous $\mathbb{F}_q$-valued functions on $G(n)$ and define an action of $G(n)$ on the algebra $\mathbb{F}_q[[x]]$ by

$$g(x)=\sum_{i\geqq 0}^{F} t_i(g)\, x^{p^i}$$

for $g\in G(n)$. Hence $g(x)=x$ iff $g=1$, so our representation is faithful.

We can embed $G(n)$ in the set $A(n)$ of all power series of the form $a(x)=\sum_{i\geqq 0}^{F} a_i x^{p^i}$ where $a_i\in\mathbb{F}_q$. We will show now that $A(n)$ can be given the structure of a $\mathbb{Z}_p$-algebra, which will turn out to be isomorphic to E_n. We will need

(2.5) **Lemma.** *If $a, b\in A(n)$ then $F(a, b)\in A(n)$.* □

Hence we can define $F(a, b)$ to be the sum of a and b in $A(n)$. We define the multiplication to be composition of power series. The right and left distributive laws follow immediately with the help of Lemma (2.4).

The ring homomorphism $\mathbb{Z}\to A(n)$ is given by $n\to[n](x)$ where $[1](x)=x$, $[-1](x)$ is the inverse in the formal group law, and for

$$n>1,\quad [n](x)=F(x,[n-1](x)).$$

We have

(2.6) **Lemma.** $[p](x)=x^q$. □

From this result it is evident that $[n](x)$ can be defined for $n\in\mathbb{Z}_p$ and that $A(n)$ is torsion-free as a $\mathbb{Z}_p$-module.

We can define a $\mathbb{Z}_p$-algebra homomorphism $h: E_n\to A(n)$ by $h(S)=x^p$ and $h(\omega)=\bar{\omega}x$, where $\bar{\omega}$ is the mod p reduction of ω (see Proposition (2.2)).

To see that h is an isomorphism, observe that by Lemma (2.1) d) any element $e\in E_n$ can be written uniquely as $e=\sum_{i\geqq 0} e_i S^i$ where $e_i\in W(\mathbb{F}_q)$ satisfies $e_i^q=e_i$, so $h(e)=\sum_{i\geqq 0}^{F}\bar{e}_i x^{p^i}$ where $\bar{e}_i$ is the mod p reduction of e_i. Since $S_n=\{e\in E_n: e_0=1\}$ and $G(n)=\{a\in A(n): a_0=1\}$, this completes the proof of Theorem (2.3). □

We remark that $A(n)$ is actually the endomorphism ring of the formal group law F defined over $\mathbb{F}_q$, and $S(n)_*$ represents the étale algebraic group which assigns to an $\mathbb{F}_p$-algebra A the automorphism group of F over A. These facts are essential in Morava's exposition [10] but are not needed here.

(2.7) **Corollary.** $H^*(S(n)) \otimes \mathbb{F}_q \cong H^*(S_n; \mathbb{F}_q)$, *the continuous cohomology of* S_n *with coefficients in the trivial module* $\mathbb{F}_q$. □

To recover the grading on $S(n)_* \otimes \mathbb{F}_q$, we have an action of the cyclic group of order $q-1$ generated by ω via conjugation in E_n.

(2.8) **Proposition.** *The eigenspace of* $S(n)_* \otimes \mathbb{F}_q$ *with eigenvalue* $\bar{\omega}^i$ *is the component* $S(n)_{2i} \otimes \mathbb{F}_q$ *of degree* $2i$.

Proof. The eigenspace decomposition is multiplicative in the sense that if x and y are in the eigenspaces with eigenvalues $\bar{\omega}^i$ and $\bar{\omega}^j$ respectively, then xy is in the eigenspace with eigenvalue $\bar{\omega}^{i+j}$. Hence it suffices to show that t_k is in the eigenspace with eigenvalue $\bar{\omega}^{p^k-1}$.

To see this we compute the conjugation of $t_k S^k \in E_n$ by ω and we have $\omega^{-1}(t_k S^k)\omega = \omega^{-1} t_k \omega^{p^k} S^k = \omega^{p^k-1} t_k S^k$. □

We now turn to the proofs of Lemmas (2.4)–(2.6).

Proof of Lemma (2.4). We can redefine the formal group law $F(x, y)$ over $\mathbb{F}_q$ as the mod p reduction of $\tilde{F}(x, y) \in W(\mathbb{F}_q)[[x, y]]$ defined by

$$\log \tilde{F}(x, y) = \log x + \log y \in (Q \otimes W(\mathbb{F}_q))[[x, y]]$$

where $\log x = \sum_{i \geq 0} \frac{x^{q^i}}{p^i}$. Now let $a \in W(\mathbb{F}_q)$ be a $(q-1)$th root of unity. Then $\log ax = a \log x$ so $\tilde{F}(ax, ay) = a\tilde{F}(x, y)$ and $F(\bar{a}x, \bar{a}y) = \bar{a}F(x, y)$, where $\bar{a}$ is the mod p reduction of a. Since any nonzero element of $\mathbb{F}_q$ is the reduction of a root of unity, this completes the proof. □

Proof of Lemma (2.5). We need to show that given $a_i, b_i \in \mathbb{F}_q$ for $i \geq 0$, we can find $c_i \in \mathbb{F}_q$ such that

$$\sum_{i \geq 0}^F c_i x^{p^i} = F\Big(\sum_{i \geq 0}^F a_i x^{p^i}, \sum_{i \geq 0}^F b_i x^{p^i}\Big) = \sum_{i \geq 0} F(a_i x^{p^i}, b_i x^{p^i}).$$

By Lemma (1.7) we can find $d_{i,j} \in \mathbb{F}_q$ for $0 \leq i \leq j$ such that

$$F(a_0 x, b_0 x) = \sum_{j \geq 0}^F d_{0,j} x^{p^j}$$

and for $i > 0$

$$F\Big(F(a_i x^{p^i}, b_i x^{p^i}), \sum_{0 \leq h < i}^F d_{h,i} x^{p^i}\Big) = \sum_{i \leq j}^F d_{i,j} x^{p^j}.$$

We can then set $c_i = d_{i,i}$. □

Proof of Lemma (2.6). We can lift $[p](x) \in \mathbb{F}_p[[x]]$ to $Z_{(p)}[[x]]$ by defining if with

$$\log [p](x) = p \log x \in Q[[x]]$$

which gives

$$\log [p](x) = px + \log x^q$$
$$[p](x) = \tilde{F}(\exp px, x^q).$$

But $\exp px \equiv 0 \bmod p$ by Lemma 2 of [12], so $[p](x) \equiv x^q \bmod p$. □

We now describe a matrix representation of E_n over $W(\mathbb{F}_q)$.

(2.9) **Proposition.** *Let* $e = \sum_{0 \leqq i < n} e_i S^i$ *with* $e_i \in W(\mathbb{F}_q)$ *be an element of* E_n. *Define an* $n \times n$ *matrix* (e_{ij}) *over* $W(\mathbb{F}_q)$ *by*

$$e_{i+1,j+1} = \begin{cases} e_{j-i}^{\sigma^i} & \text{for } i \leqq j \\ p e_{j+n-i}^{\sigma^i} & \text{for } i > j. \end{cases}$$

Then a) *this defines a faithful representation of* E_n;

b) *the determinant* $|e_{ij}|$ *lies in* $\mathbb{Z}_p$.

Proof. a) is straightforward. For b) it suffices to check that ω and S give determinants in $\mathbb{Z}_p$. □

We can now define homomorphisms $c: \mathbb{Z}_p \to S_n$ and $d: S_n \to \mathbb{Z}_p$ for $p > 2$, and $c: \mathbb{Z}_2^\times \to S_n$ and $d: S_n \to \mathbb{Z}_2^\times$ for $p = 2$ by identifying S_n with the appropriate matrix group. ($\mathbb{Z}_p$ is to be regarded here as a subgroup of $\mathbb{Z}_p^\times$.) Let d be the determinant for all primes. For $p > 2$ let $c(x) = (\exp px)I$ where I is the $n \times n$ identity matrix and $x \in Z_p$; for $p = 2$ let $c(x) = xI$ for $x \in Z_2^\times$.

(2.10) **Theorem.** *Let* $S_n^1 = \ker d$.

a) *If* $p > 2$ *and* $p \nmid n$ *then* $S_n \cong Z_p \oplus S_n^1$.

b) *If* $p = 2$ *and* n *is odd then* $S_n \cong S_n^1 \oplus Z_2^\times$.

Proof. In both cases one sees that Im c lies in the center of S_n (in fact Im c is the center of S_n) and is therefore a normal subgroup. The composition dc is multiplication by n which is an isomorphism for $p \nmid n$, so we have the desired splitting. □

We now describe an analogous splitting for $S(n)_*$. Let $A = \mathbb{F}_p[\mathbb{Z}_p]$ for $p > 2$ and $A = \mathbb{F}_2[\mathbb{Z}_2^\times]$ for $p = 2$. Let A_* be the continuous linear dual of A.

(2.11) **Proposition.** *As an algebra* $A_* = \mathbb{F}_p[u_1, u_2 \ldots]/(u_i - u_i^p)$. *The coproduct* Δ *is given by*

$$\sum_{i \geqq 0}^{G} \Delta(u_i) = \sum_{i,j \geqq 0}^{G} u_i \otimes u_j$$

where $u_0 = 1$ and G *is the formal group law with*

$$\log_G(x) = \sum x^{p^i}/p^i. \quad \square$$

Proof. Since $A \cong \mathbb{F}_p[S_1]$, this follows immediately from Theorem (2.3). □

We can define Hopf algebra homomorphisms $c_*: S(n)_* \otimes \mathbb{F}_q \to A_* \otimes \mathbb{F}_q$ and $d_*: A_* \otimes \mathbb{F}_q \to S(n)_* \otimes \mathbb{F}_q$ dual to the group homomorphisms c and d defined above.

(2.12) **Theorem.** *There exist maps* $c_*: S(n)_* \to A_*$ *and* $d_*: A_* \to S(n)_*$ *corresponding to those defined above, and for* $p \nmid n$, $S(n)_* \cong A_* \otimes B_*$ *where* $B_* \otimes \mathbb{F}_q$ *is the continuous linear dual of* $\mathbb{F}_q[S_n^1]$.

Proof. We can define c_* explicitly by

$$c_* t_i = \begin{cases} u_{i/n} & \text{if } n|i \\ 0 & \text{otherwise.} \end{cases}$$

It is straightforward to check that this is a homomorphism corresponding to the c_* defined above. In lieu of defining d_* explicitly we observe that the determinant of $\sum_{i \geqq 0} t_i S^i$, where $t_i \in W(\mathbb{F}_q)$ and $t_i = t_i^q$, is a power series in p whose coefficients are polynomials in the t_i over $\mathbb{Z}_p$. It follows that d_* can be defined over $\mathbb{F}_p$. The splitting then follows as in Theorem (2.10). □

§ 3. A Filtration of $S(n)$

Our object in this section is to define an increasing filtration of $S(n)_*$ which will be dual to a decreasing filtration of $S(n)$. We will then describe the associated graded Hopf algebras $E^0 S(n)_*$ and its dual $E_0 S(n)$. This filtration was originally motivated by filtration of the algebra E_n of § 2 by powers of (S). It is not the same as the filtration of $S(n)$ by powers of the augmentation ideal, but $E_0 S(n)$ is nevertheless primitively generated. In [13] we will show that $S(n)_*$ has other primitives besides the usual $t_1^{p^i}$. These elements will have filtration degree greater than one in our filtration, which we find more convenient for understanding the structure of $S(n)$.

(3.1) **Theorem.** *Let*

$$d_i = \begin{cases} 0 & \text{for } i \leqq 0 \\ \max(i, p d_{i-n}) & \text{for } i > 0. \end{cases}$$

Then there is a unique increasing Hopf algebra filtration on $S(n)_*$ with $t_i^{p^j} \in F_{d_i} S(n)_*$ and $t_i^{p^j} \notin F_{d_i - 1} S(n)_*$.

Before proving this result we need

(3.2) **Lemma.** *Let $w_{j,n}$ be the polynomials defined in Lemma* (1.7). *Then $w_{j,n}(x_i) \equiv w_{j,1}(x_i^{p^{(n-1)j}}) \bmod p$.*

Proof. The $w_{j,n}$ are defined by

$$\sum_i \frac{x_i^{p^{nj}}}{p^j} = \sum_{0 \leqq k \leqq j} \frac{w_{k,n}(x_i)^{p^{n(j-k)}}}{p^{j-k}}. \tag{3.21}$$

We will argue by induction on j, the statement being trivial for $j=0$. If $w_{k,n}(x_i) \equiv w_{k,1}(x_i^{p^{nk-k}}) \bmod p$, then

$$w_{k,n}(x_i)^{p^{m(j-k)}} \equiv w_{k,1}(x_i^{p^{nk-k}})^{p^{m(j-k)}} \bmod p^{1+j-k}$$

for $m > 0$. Hence (3.21) can be rewritten

$$\begin{aligned} \sum_i \frac{(x_i^{p^{nj-j}})^{p^j}}{p^j} &\equiv w_{j,n}(x_i) + \sum_{k<j} \frac{w_{k,1}(x_i^{p^{nk-k}})^{p^{n(j-k)}}}{p^{j-k}} \\ &\equiv w_{j,n}(x_i) + \sum_{k<j} \frac{w_{k,1}(x_i^{p^{nj-j}})^{p^{j-k}}}{p^{j-k}} \bmod p. \end{aligned}$$

If we replace $w_{j,n}(x_i)$ by $w_{1,n}(x_i^{p^{nj-j}})$ we obtain the definition of the latter, so $w_{j,n}(x_i) \equiv w_{j,1}(x_i^{p^{nj-j}}) \bmod p$. □

We now prove Theorem (3.1) by showing that all terms in the coproduct of $t_i^{p^j}$ have degree $\leqq d_i$ by induction on i. We use the notation of Theorem (1.8). It follows from Lemma (3.2) that the polynomial $w_{j,n}$ increases degree by a factor of at most p^j. Clearly M_i has degree d_i so it follows Δ_i has degree d_i. □

We now describe $E^0 S(n)_*$. Let $t_{i,j}$, $M_{i,j}$ and $\Delta_{i,j}$ denote the elements in the appropriate graded object corresponding to $t_i^{p^j}$, $M_i^{p^j}$ and $\Delta_i^{p^j}$, respectively, where multiplication of vectors is componentwise, $j \in \mathbb{Z}/(n)$, $v_n = 1$ and $p = 0$ since we are now working in $S(n)_*$. Then we have

(3.3) **Theorem.** a) *As an algebra* $E^0 S(n)_* = \mathbb{F}_p[t_{i,j}]/(t_{i,j}^p)$ *with* $t_{i,j} \in E_{d_i}^0 S(n)_*$, $i > 0$, $j \in \mathbb{Z}/(n)$.

b) $$M_{i,j} = \begin{cases} (1 \otimes t_{i,j}, t_{1,j} \otimes t_{i-1,j+1}, t_{2,j} \otimes t_{i-2,j+2}, \ldots, t_{i,j} \otimes 1) & \text{for } i \leqq m \\ (t_{i,j} \otimes 1, 1 \otimes t_{i,j}) & \text{for } i > m \end{cases}$$

where $m = pn/(p-1)$.

c) *Let* $i = kn + l$ *with* $0 < l \leqq n$ *and* $w_h = w_{h,1}$. *Then*

$$\Delta_{i,j} = (w_0(M_{i,j}), w_1(M_{i-n,j-1}), \ldots w_k(M_{l,j-k}),$$
$$w_1(\Delta_{i-n,j-1}), w_2(\Delta_{i-2n,j-2}), \ldots w_{k-1}(\Delta_{n+l,j+1-k}).$$

d) *The coproduct in* $E^0 S(n)_*$ *is given by*

$$\Delta(t_{i,j}) = \begin{cases} w_0(M_{i,j}) & \text{for } i \leqq n \\ w_0(\Delta_{i,j}) & \text{for } i > n. \end{cases}$$

Proof. a) and b) are trivial, c) follows by applying Lemma (3.2) to the definition of $\Delta_{i,j}$, and d) follows from Theorem (1.8). □

We now turn our attention to $E_0 S(n)$. Let $x_{i,j} \in E_0 S(n)$ be the dual of $t_{i,j}$ with respect to the monomial basis.

(3.4) **Theorem.** $E_0 S(n)$ *is the enveloping algebra of the restricted Lie algebra with basis* $\{x_{i,j}\}$, *bracket*

$$[x_{i,j}, x_{k,l}] = \begin{cases} \delta_{i+j}^l x_{i+k,j} - \delta_{k+l}^j x_{i+k,l} & \text{for } i+k \leqq m \\ 0 & \text{otherwise} \end{cases}$$

(*where* $\delta_t^s = 1$ iff $s \equiv t \bmod n$ *and* $\delta_t^s = 0$ *otherwise*), *and restriction*

$$\xi(x_{i,j}) = \begin{cases} 0 & \text{if } i \leqq n/(p-1) \\ -x_{i+n,j+1} & \text{otherwise.} \end{cases}$$

Proof. Since $t_{i,j}^p = 0$ for all i, j, $E_0 S(n)$ is primitively generated with primitives $x_{i,j}$ ([16], Proposition 13.2.3). Hence by a theorem of Milnor-Moore ([9], Theorem 6.11) it is the enveloping algebra of the restricted Lie algebra of primitives. The bracket and restriction can be read off from Theorem (3.3). □

Now let $L(n)$ be the Lie algebra (without restriction) on the primitives $x_{i,j}$ for $m-n<i\leqq m$ and let $UL(n)$ be its enveloping algebra. Let $T(n)$ be the quotient of $E_0S(n)$ by the subalgebra generated by $x_{i,j}$ for $i>m-n$.

(3.5) **Corollary.** *$E_0S(n)$ is given as an extension of cocommutative Hopf algebras which is trivial as an extension of coalgebras*

$$\mathbb{F}_p \to UL(n) \to E_0S(n) \to T(n) \to \mathbb{F}_p$$

and $T(n)$ is a restricted enveloping algebra with trivial restriction. In particular $E_0S(n) \cong UL(n)$ for $n<p-1$. □

References

1. Bergman, G.M.: Ring schemes: the Witt scheme. In: Lectures on curves on an algebraic surface, (D. Mumford, Ed.). Annals Studies No. **59**, 1966
2. Fröhlich, A.: Formal Groups. Lecture Notes in Math. **74.** Berlin-Heidelberg-New York: Springer 1968
3. Hazewinkel, M.: Constructing formal groups I Over $\mathbb{Z}_{(p)}$-algebras, Report 7119, Netherlands School of Economics, Econometric Institute, 1971
4. Johnson, D.C., Wilson, W.S.: BP operations and Morava's extraordinary K-theory. Math. Z. **144**, 55–75 (1975)
5. Lazard, M.: Groupes analytiques p-adiques. IHES Pub. Math. No. **26** (1965)
6. May, J.P.: The cohomology of restricted Lie algebras and of Hopf algebras. J. of Algebra **3**, 123–146 (1966)
7. Miller, H.R., Ravenel, D.C.: Morava stabilizer algebras and the localization of Novikov's E_2-term. To appear
8. Miller, H.R., Ravenel, D.C., Wilson, W.S.: Periodic phenomena in the Novikov spectral sequence. To appear
9. Milnor, J., Moore, J.C.: On the structure of Hopf algebras. Ann. Math. **81**, 211–264 (1965)
10. Morava, J.: Structure theorems for cobordism comodules. To appear
11. Morava, J.: Private communication
12. Ravenel, D.C.: The structure of BP_*BP modulo an invariant prime ideal. Topology **15**, 149–153 (1976)
13. Ravenel, D.C.: The cohomology of the Morava stabilizer algebras. To appear
14. Serre, J-P.: Corps locaux. Paris: Hermann 1962
15. Serre, J-P.: Local class field theory. In: Algebraic number theory, (J.W.S. Cassels and A. Frolich, Eds.), pp. 128–161. New York-London: Academic Press 1967
16. Sweedler, M.: Hopf algebras. Amsterdam: Benjamin 1969

Received December 10, 1975