Contemporary Mathematics
Volume **00**, 0000

Q-rings and the homology of the symmetric groups

Terrence P. Bisson & André Joyal

Abstract.

The goal of this paper is to study the rich algebraic structure supported by the homology mod 2 of the symmetric groups. We propose to organise the algebra of homology operations around a single concept, that of Q-ring. We are guided by an analogy with the representation theory of the symmetric groups and the concept of λ-ring. We show that $H_*\Sigma_*$ is the free Q-ring on one generator. It is a Hopf algebra generated by its subgroup $\mathcal{K}$ of primitive elements. This subgroup is an algebra (for the composition of operations) that we call the Kudo-Araki algebra. It is closely related to the Dyer-Lashof algebra but is better behaved: the dual coalgebra is directly representing the substitution of Ore polynomials. Many results on the homology of E_∞-spaces can be expressed in the language of Q-rings. We formulate the Nishida relations by using a Q-ring structure on a semidirect extension $\mathcal{A}$ of Milnor's dual of the Steenrod algebra. We show that the Nishida relations lead to a commutation operator between $\mathcal{K}$ and $\mathcal{A}$.

Contents

0. Introduction
1. Q-rings and modules
2. The Kudo-Araki algebra $\mathcal{K}$ and its dual
3. Free Q-rings
4. The extended Milnor coalgebra $\mathcal{A}$
5. The Nishida relations
6. Q-coalgebras
Appendix A
Appendix B
Appendix C
References

1991 *Mathematics Subject Classification.* Primary 55S05; Secondary 55S12, 20B30, 20J06.
Key words and phrases. symmetric groups, homology, Steenrod algebra.
Support for this work was provided by the Canadian NSERC and by the Quebec FCAR

0. INTRODUCTION

This paper is partly expository and wholly algebraic. Our goal is to study the rich algebraic structure supported by the homology mod 2 of the symmetric groups. We propose to organise the algebra of homology operations around a single concept, that of Q-ring. We are guided by an analogy with the representation theory of the symmetric groups and the concept of λ-ring. Recall that the direct sum $R(\Sigma_*) = \oplus_n R(\Sigma_n)$ of the character groups of the symmetric groups is the free λ-ring on one generator. It is also a self-dual Hopf algebra isomorphic to the ring of symmetric functions. For the direct sum $H_*\Sigma_* = \oplus_n H_*\Sigma_n$ of the mod 2 homology of the symmetric groups there is a similar pattern. We show that $H_*\Sigma_*$ is the free Q-ring on one generator. It is a Hopf algebra generated by its subgroup $\mathcal{K}$ of primitive elements. This subgroup is an algebra (for the composition of operations) that we call the Kudo-Araki algebra. It is closely related to the Dyer-Lashof algebra but is better behaved: the dual coalgebra is directly representing substitution of Ore polynomials.

Many results on the homology of E_∞-spaces can be expressed in the language of Q-rings. For example, if $E_\infty(X)$ is the free E_∞-space generated by a space X then $H_*E_\infty(X)$ is the free Q-ring generated by H_*X.

We formulate the Nishida relations by using a Q-ring structure on a semidirect extension $\mathcal{A}$ of Milnor's dual of the Steenrod algebra. We introduce an abstract concept of commutation operator between an algebra and a coalgebra and show that the Nishida relations lead to a commutation operator between the algebra $\mathcal{K}$ and the coalgebra (opposite to) $\mathcal{A}$.

The present work was inspired by our work on geometric Dyer-Lashof operations in unoriented cobordism, as sketched in Bisson, Joyal [1995a,b]; this geometric underpinning will be presented in a sequel. In the present paper we do not discuss distributivity relations between different Q-ring structures, such as occur in the homology of E_∞-ring spaces. We leave this for a sequel, together with an extension of our theory to mod p homology. We view our contribution to many of the results presented here as one of conceptualisation and simplification. We hope that our approach will shed new light on the work done in the field during the last forty years.

We now present a more detailed description of the paper. Except for this introduction all discussions relating our work to homology are reserved to Addenda placed at the end of each section. Throughout, Z_2 denotes the integers mod 2.

A Q-*ring* is a commutative ring R with a ring homomorphism $Q_t : R \to R[[t]]$ called the *total square*, satisfying the following conditions:

(i) $Q_0(a) = a^2$ for every a in R
(ii) $Q_t \circ Q_s$ is symmetric in t and s
where Q_t is extended to $R[[s]]$ by $Q_t(s) = s(s+t)$.

If we put $Q_t(x) = \sum_{n\geq 0} q_n(x)t^n$ then we obtain a sequence of operations $q_n : R \to R$ called the *individual squares*. The q_n were introduced by Kudo and Araki; they generate an algebra under composition that we call the *Kudo-Araki algebra* and denote by $\mathcal{K}$.

A Q-ring is *graded* when R is Z-graded and $\text{grade}(q_n(a)) = 2 \cdot \text{grade}(a) + n$ for homogeneous a. The mod 2 cohomology $H^*(X)$ of any space has a graded

Q-ring structure obtained from the Steenrod operations $Sq^i : H^*(X) \to H^{*+i}(X)$. If $x \in H^r(X)$ we have $q_i(x) = Sq^{r-i}(x)$ for $0 \leq i \leq r$, and $q_i(x) = 0$ for $r < i$. For this structure the group $H^n(X)$ is homogeneous of grade $-n$. The mod 2 homology H_*X of an E_∞-space X has a graded Q-ring structure classically expressed in terms of Dyer-Lashof operations $Q^i : H_*(X) \to H_{*+i}(X)$. If $x \in H_r(X)$ then $q_n(x) = Q^{r+n}(x)$. The Dyer-Lashof operations Q^i are obtained by reorganising the graded components of the q_i's so as to form homogeneous operations. They generate an algebra called the Dyer-Lashof algebra that is *not* isomorphic to the Kudo-Araki algebra. Here we stress the importance and naturality of $\mathcal{K}$. The concept of Q-ring provides an alternative way of handling Dyer-Lashof operations. For example, let BO_* denote the disjoint union, for $n \geq 0$, of the spaces BO_n which classify n-dimensional real vector bundles. Then BO_* has an E_∞-structure obtained from the Whitney sum of vector bundles, and the ring H_*BO_* is isomorphic to $Z_2[\beta_0, \beta_1, \dots]$ where $\beta_n \in H_*BO_1 = H_*RP^\infty$ is the nonzero element of dimension n. The Q-structure on H_*BO_* is characterized by the identity

$$Q_t(\beta)(x(x+t)) = \beta(x)\beta(x+t)$$

where $\beta(x) = \sum \beta_i x^i$.

The classifying space $B\mathcal{C}$ of any symmetric monoidal category is an E_∞-space. Its homology $H_*\mathcal{C} = H_*B\mathcal{C}$ is a Q-ring. For example, the category of finite sets and bijections has a monoidal structure given by disjoint union. It is equivalent to the disjoint union Σ_* of the symmetric groups Σ_n. Hence $H_*\Sigma_*$, the direct sum of the homology of the symmetric groups, is a Q-ring. It is $Q\langle x\rangle$, the free Q-ring on one generator.

The mod 2 homology H_*S of a spectrum S is a Q-ring. For example, the homology of the sphere spectrum $S^0 = \Omega^\infty S^\infty$ is $\{x\}^{-1}Q\langle x\rangle = Q\langle x, x^{-1}\rangle$, the free Q-ring on an invertible generator x. The homology of the representing spectrum KO of real K-theory is $Z_2[\beta_0, \beta_0^{-1}, \beta_1, \dots]$ with the Q-structure given as above. When X is a finite cell complex we have $H^n(X) = H_{-n}(X')$ where X' is the Spanier-Whitehead dual of X in the category of spectra. The Q-ring structure on the cohomology of X is isomorphic to the Q-ring structure on the homology of X' (as learned in a conversation with H. Miller).

Let $Q\langle V\rangle$ denote the free Q-ring generated by a Z_2-vector space V. For any space X the canonical map

$$Q\langle H_*X\rangle \to H_*E_\infty(X)$$

is an isomorphism, where $E_\infty(X)$ is the E_∞-space freely generated by X. If V is a coalgebra then so is $Q\langle V\rangle$; the coproduct $Q\langle V\rangle \to Q\langle V\rangle \otimes Q\langle V\rangle$ is the map of Q-rings which extends the coproduct $\delta : V \to V \otimes V$ (here we use that the tensor product $R \otimes S$ of two Q-rings is a Q-ring). For instance, the homology of any space X has a coalgebra structure obtained from the diagonal $X \to X \times X$. When $V = H_*X$ the diagonal structure on $H_*E_\infty(X) = Q\langle H_*X\rangle$ is obtained from the diagonal structure on H_*X. In particular, the diagonal structure on $H_*\Sigma_* = Q\langle x\rangle$ is given by the unique map of Q-rings $Q\langle x\rangle \to Q\langle x\rangle \otimes Q\langle x\rangle$ such that $\delta(x) = x \otimes x$.

We introduce a linear version of the concept of Q-ring called *Q-module*. It is a Z_2-vector space M equipped with an additive map $Q_t : M \to M[[t]]$ such that

$Q_t \circ Q_s$ is symmetric in t and s. A Q-module is the same thing as a left module over the Kudo-Araki algebra $\mathcal{K}$. The tensor product $M \otimes N$ of two Q-modules is a Q-module with operations given by the Cartan formula $q_n(x \otimes y) = \sum q_i(x) \otimes q_{n-i}(y)$. So $\mathcal{K}$ has a coalgebra structure defined by the map of algebras $\delta : \mathcal{K} \to \mathcal{K} \otimes \mathcal{K}$ such that $\delta(q_n) = \sum q_i \otimes q_{n-i}$. Hence (like the Steenrod algebra) $\mathcal{K}$ is a cocommutative bialgebra. The dual coalgebra $\mathcal{K}' = \mathcal{W}$ splits as a direct sum

$$\mathcal{W} = \bigoplus_n \mathcal{W}(n)$$

of polynomial algebras. Here $\mathcal{W}(n)$ is the algebra $Z_2[w_0, \dots, w_{n-1}]$ of Dickson invariants; it is generated by the coefficients of the generic Ore polynomial

$$W_n(x) = x^{2^n} + \sum_{i=0}^{n-1} w_i \, x^{2^i}.$$

There is a coalgebra structure Δ on $\mathcal{W}$ representing the operation of substitution of Ore polynomials. By definition, the map $\Delta : \mathcal{W}(m+n) \to \mathcal{W}(m) \otimes \mathcal{W}(n)$ is the ring homomorphism such that

$$\Delta(W_{m+n}) = (W_m \otimes 1) \circ (1 \otimes W_n).$$

We prove that the Kudo-Araki algebra is anti-isomorphic to the dual algebra $\mathcal{W}'$.

To construct the free Q-ring on one generator we use the *enveloping algebra* $\tilde{\Lambda} M = \tilde{\Lambda}(M, q_0)$ of an endomorphism $q_0 : M \to M$ of a Z_2-vector space. By definition, $\tilde{\Lambda}(M, q_0)$ is the quotient of the symmetric algebra $S(M)$ by the ideal generated by the relation $x^2 = q_0(x)$ for $x \in M$. When $q_0 = 0$ the enveloping algebra is the exterior algebra ΛM. If M is a Q-module then $\tilde{\Lambda} M$ is a Q-ring. The free Q-ring on one generator $Q\langle x \rangle$ is $\tilde{\Lambda}\mathcal{K}$. We have $\mathcal{K} = Z_2[q_0] \otimes \mathcal{K}^\flat$ for a subgroup $\mathcal{K}^\flat \subset \mathcal{K}$ and it follows that $Q\langle x \rangle$ is the symmetric algebra on $\mathcal{K}^\flat$. Any enveloping algebra $\tilde{\Lambda}(M, q_0)$ has a Hopf algebra structure with comultiplication given by $\sigma(x) = x \otimes 1 + 1 \otimes x$ for $x \in M$. For this structure the subgroup of primitive elements is M. In particular, $Q\langle x \rangle$ is a Hopf algebra with comultiplication the map of Q-rings $\sigma : Q\langle x \rangle \to Q\langle x \rangle \otimes Q\langle x \rangle$ such that $\sigma(x) = x \otimes 1 + 1 \otimes x$. For this structure the subgroup of primitive elements is $\mathcal{K}$.

To formulate the Nishida relations we use right comodules over the *extended Milnor coalgebra* $\mathcal{A} = Z_2[a_0^{-1}, a_0, a_1, \dots]$. The comultiplication $\Delta : \mathcal{A} \to \mathcal{A} \otimes \mathcal{A}$ is given by

$$\Delta(a) = (a \otimes 1) \circ (1 \otimes a)$$

where $\circ$ represents composition of formal power series and where $a(x) = \sum a_i x^{2^i}$. We refer to a right $\mathcal{A}$-comodule M as a *Milnor coaction* and will denote the coaction map by $\psi : M \to M \otimes \mathcal{A}$. We also introduce the *positive bialgebra* $\mathcal{A}^+$ and show that $\mathcal{K}$ is anti-isomorphic to a subalgebra of the convolution algebra $[\mathcal{A}^+, Z_2]$. The homology of any space has an $\mathcal{A}^+$-coaction which determines the action of the Steenrod operations. There is a unique Q-structure on the algebra $\mathcal{A}$ such that

$$Q_t(a)(x(x+t)) = a(x)a(x+t).$$

If M is a Q-module then "change of parameters" gives a certain natural Q-structure Q'_t on $M \otimes \mathcal{A}$; if $x \in M$ and $r \in \mathcal{A}$ then we have $Q'_t(x \otimes r) = Q_{a(t)}(x) Q_t(r)$. We say that the *Nishida relations* hold for a Q-module M if the coaction $\psi : M \to M \otimes \mathcal{A}$

is a map of Q-modules where $M \otimes \mathcal{A}$ is equipped with Q'_t. If E is an E_∞-space then H_*E is a Q-ring with a Milnor ring coaction, and the Nishida relations hold for H_*E. If M is an $\mathcal{A}$-comodule then there is a unique Milnor ring coaction on $Q\langle M\rangle$ extending the given coaction on M and satisfying the Nishida relations. It follows that for any space X the Milnor coaction on $H_*E_\infty(X)$ is obtained from the coaction on $H_*(X)$. In particular, this determines the Milnor coaction on $H_*\Sigma_* = Q\langle x\rangle$.

To study the Nishida relations we use an abstract theory of commutation operators between an algebra and a coalgebra, as sketched in appendix C. The *Nishida operator* is a commutation operator

$$\tilde{\rho} : \mathcal{K} \otimes \mathcal{A} \to \mathcal{A} \otimes \mathcal{K}$$

between $\mathcal{K}$ and the coalgebra $(\mathcal{A}, \Delta^o, \epsilon)$ opposite to $\mathcal{A}$. We use the operator in the form of a commutation operator ρ between a monad and a comonad. An action by $\mathcal{K}$ *ρ-commutes* with a coaction by $\mathcal{A}$ iff the Nishida relations are satisfied.

We would like to thank André Lebel for reading the manuscript and Paul Libbrecht for the typography.

Addendum to Section 0.

The homology of the symmetric groups has a rich history of which we can only sketch the chronology. It begins with Steenrod's description of cohomology operations obtained from elements in $H_*(\Sigma_*)$ (expressed most simply in Steenrod [1953] and [1957]); see also Steenrod, Epstein [1962] or May [1970], for instance. The homology and cohomology of symmetric products of spaces attracted considerable interest during the next few years; see Nakaoka [1957] and Dold [1958], for instance. The full computation of the homology of the symmetric groups was achieved in Nakaoka [1960]; he showed that the homology of the infinite symmetric group has the structure of a commutative Hopf algebra and proved that it is a polynomial algebra.

Kudo and Araki [1956] used a variant of Steenrod's methods to define operations on the homology of H_n-spaces. Applications of these operations were developed in Browder [1960], Dyer, Lashof [1962], Milgram [1965], Barratt, Kahn, Priddy [1971], May [1971], and Priddy [1972], for instance, especially in connection with the homology of iterated loop spaces.

Connections between homology operations and Dickson invariants appear in Madsen [1975] and Mui [1975]. Some good sources for background on E_∞-spaces and some indications of the history and applications of Dyer-Lashof operations are May [1977b], Adams [1978], and Madsen, Milgram [1979]. The construction of an E_∞-space from a symmetric monoidal category appears in Segal [1974].

Some good sources for background on λ-rings, the representation theory of the symmetric group, and symmetric functions are Grothendieck [1958], Atiyah [1966], Knutson [1973], Hoffman [1979], and Macdonald [1979]. For background on Hopf algebras and their comodules see Sweedler [1969].

1. Q-rings and modules.

We formally introduce the concept of Q-ring and Q-module and give a few basic algebraic examples.

Definition 1. A *Q-ring* is a commutative ring R together with a ring homomorphism $Q_t : R \to R[[t]]$ called the *total square*, satisfying the following conditions for every a in R:

i) $Q_0(a) = a^2$;

ii) $Q_t \circ Q_s(a)$ is symmetric in s and t in $R[[s,t]]$, where Q_t is extended to $R[[s]]$ by $Q_t(s) = s(s+t)$.

A Q-ring is always a Z_2-algebra since i) implies that the map $a \mapsto a^2$ is a ring homomorphism. If we put $Q_t(a) = \sum_{n\geq 0} q_n(a)t^n$ we obtain a sequence of operations $q_n : R \to R$ $(n \geq 0)$ called the *individual squares*. A *map of Q-rings* is a ring homomorphism preserving the operations q_n. The fact that Q_t is a ring homomorphism means that the Cartan formula holds; for all $a, b \in R$

$$q_n(ab) = \sum_{i+j=n} q_i(a)q_j(b).$$

We shall use upper and lower indexing $M_n = M^{-n}$ for Z-graded vector spaces and say that $x \in M_n$ is of dimension n and that $x \in M^n$ is of codimension n. A Q-ring is *graded* when R is graded and $\dim(q_n(a)) = 2 \cdot \dim(a) + n$. Notice that if t is given codimension 1 then the total square $Q_t(a)$ is a formal power series homogeneous of dimension $2 \cdot \dim(a)$ for homogeneous a.

For any Z_2-vector space M we shall denote by $M[[t]]$ the set of formal power series in t with coefficients in M. It is a module over the power series ring $Z_2[[t]]$. There is a substitution $u(f(t))$ for formal power series $u(t) \in M[[t]]$ and $f(t) \in tZ_2[[t]]$. These ideas apply also to the set $M[[s,t]]$ of power series in s and t.

Definition 2. A *Q-module* is a Z_2-vector space M together with an additive map $Q_t : M \to M[[t]]$ called the *total square*, such that $Q_t \circ Q_s$ is symmetric in t and s, where Q_t is extended to a map $Q_t : M[[s]] \to M[[s,t]]$ by putting $Q_t(s) = s(s+t)$ and $Q_t(\sum_i a_i s^i) = \sum_i Q_t(a_i)Q_t(s)^i$. A Q-module is *graded* when M is Z-graded and $\dim(q_n(a)) = 2 \cdot \dim(a) + n$ for homogeneous a.

The symmetry condition on $Q_t \circ Q_s$ is equivalent to a set of relations (called the Adem relations) on the q_n's. Let $\mathcal{K}$ denote the associative algebra generated by the q_n's subject to the Adem relations; we will call it the *Kudo-Araki algebra*. A Q-module is the same thing as a left $\mathcal{K}$-module; the free Q-module generated by a Z_2-vector space V is equal to $\mathcal{K} \otimes V$. Here is an explicit description of the Adem relations.

Proposition 1. *A sequence of additive operations $q_n : M \to M$ defines a Q-module structure on M iff the q_n satisfy the following Adem relation for all $a \in M$:*

$$q_m(q_n(a)) = \sum_i \binom{i-n-1}{2i-m-n} q_{m+2n-2i}(q_i(a)).$$

Proof. By definition we have

$$Q_t(Q_s(a)) = Q_t(\sum q_n(a)s^n) = \sum Q_t(q_n(a))Q_t(s)^n = \sum q_m(q_n(a))t^m[s(s+t)]^n.$$

The symmetry condition can be expressed as

$$\sum Q_t(q_n(a))[s(s+t)]^n = \sum q_j(q_i(a))s^j[t(t+s)]^i.$$

Thus we can compute $Q_t(q_n(a))$ by expanding the right hand side as a power series in $u = s(s+t)$. Observe that the change of parameter $u = st + s^2$ from s to u has a composition inverse if t is formally inverted (in the ring of Laurent series in t). Thus we can expand the right hand side of the equality as a power series in $u = s(s+t)$. We shall use residues to compute the coefficient of u^n in this expansion. Recall that if $f(u)$ is a Laurent series in u then the residue of $f(u)du$ is the coefficient of u^{-1} in $f(u)$; the coefficient of u^n is the residue of $f(u)u^{-n-1}du$. In our case $du = tds$ since we are working mod 2. Hence the coefficient of u^n in the right side of the equality is

$$\sum_{j,i\geq 0} q_j(q_i(a))\mathrm{Res}\left(\frac{s^j t^i (t+s)^i}{s^{n+1}(s+t)^{n+1}} tds\right) = \sum_{j,i\geq 0} q_j(q_i(a))t^{2i-2n+j}\binom{i-n-1}{n-j}.$$

Thus the symmetry condition can be expressed as

$$Q_t(q_n(a)) = \sum_{j,i\geq 0} q_j(q_i(a))t^{2i-2n+j}\binom{i-n-1}{n-j}.$$

The Adem relations are obtained by equating the coefficients of the two sides. QED

The next few propositions describe algebraic constructions of Q-modules and rings. We use the obvious product $M[[t]] \otimes N[[t]] \to (M\otimes N)[[t]]$; if the context is clear the product of $f(t) \in M[[t]]$ with $g(t) \in M[[t]]$ will be denoted by $f(t)\cdot g(t)$.

Proposition 2. *If M and N are (graded) Q-modules (resp. Q-rings) then so is their tensor product $M \otimes N$ with $q_n(a\otimes b) = \sum_{i+j=n} q_i(a)\otimes q_j(b)$.*

Proof. By definition we have $Q_t(a\otimes b) = Q_t(a)\cdot Q_t(b)$ with the notation introduced above. It is easy to see that $Q_t \circ Q_s(a\otimes b) = Q_t(Q_s(a))\cdot Q_t(Q_s(b))$ and it follows that $Q_t\circ Q_s$ is symmetric in s,t. If M and N are graded and a and b are homogeneous then

$$\dim(q_i(a)\otimes q_j(b)) = 2\dim(a) + i + 2\dim(b) + j = 2\dim(a\otimes b) + n.$$

Hence $M\otimes N$ is a graded Q-module. It is obvious that $Q_t : M\otimes N \to M\otimes N[[t]]$ is a ring homomorphism if M and N are Q-rings. Moreover, in this case $Q_0(a\otimes b) = Q_0(a)\otimes Q_0(b) = a^2\otimes b^2 = (a\otimes b)^2$. QED

If R is a Q-ring then the product map $R\otimes R\to R$ is a Q-module map. If an R-module M is also a Q-module and the structure map $R\otimes M \to M$ is a Q-module map then we shall say that M is a *QR-module.* It is easy to see that $R\otimes \mathcal{K}$ is the free QR-module on one generator, hence it is an algebra. A QR-module is the same thing as a left module over $R\otimes\mathcal{K}$ (see Example 3 of appendix C).

Proposition 3. *If R is a Q-ring then so are the polynomial ring $R[x_1,\dots,x_n]$ and the formal power series ring $R[[x_1,\dots,x_n]]$ if we put $Q_t(x_i) = x_i(x_i+t)$ for every $1\leq i\leq n$. Moreover, these Q-rings are graded if R is graded and codim$(x_i) = 1$. The same result is true for Q-modules instead of Q-rings.*

Proof. Let us verify that $Z_2[x]$ is a Q-ring if we put $Q_t(x) = x(x+t)$. Obviously, $Q_0(x) = x^2$. For the symmetry we have

$$\begin{aligned} Q_t \circ Q_s(x) &= Q_t(x(x+s)) = Q_t(x)(Q_t(x) + Q_t(s)) \\ &= x(x+t)(x(x+t) + s(s+t)) = x(x+t)(x+s)(x+s+t) \end{aligned}.$$

This proves that $Z_2[x]$ is a Q-ring. If $\mathrm{codim}(x) = 1$ then $x(x+t)$ is homogeneous of codimension 2 when $\mathrm{codim}(t) = 1$. It follows that $Z_2[x]$ is a graded Q-ring. According to Proposition 2, $R[x] = R \otimes Z_2[x]$ is a Q-ring. By continuity of Q_t it follows that $R[[x]]$ is also a Q-ring. It follows by induction on n that $R[x_1, \ldots, x_n]$ and $R[[x_1, \ldots, x_n]]$ are Q-rings. If M is a Q-module then according to Proposition 2, $M[x_1, \ldots, x_n] = M \otimes Z_2[x_1, \ldots, x_n]$ is a Q-module. It follows by continuity of Q_t that $M[[x_1, \ldots, x_n]]$ is a Q-module. The statement about gradings is easily checked. QED

Let us denote by $Z_2[\beta_*]$ the polynomial ring $Z_2[\beta_0, \beta_1, \ldots]$.

Proposition 4. *There is a unique Q-structure on the polynomial ring $Z_2[\beta_*]$ such that $Q_t(\beta)(x(x+t)) = \beta(x)\beta(x+t)$ where $\beta(x) = \sum_i \beta_i x^i$. This is a graded Q-ring if we take dim$(\beta_i) = i$. We have the explicit formula*

$$q_r(\beta_n) = \sum_i \binom{r+i-1}{i} \beta_{n-i}\beta_{r+n+i}.$$

Proof. For simplicity let us put $Z_2[\beta_*] = R$. The series $\beta(x)\beta(y)$ is symmetric in x and y. It follows that it can be expanded as a series in the elementary symmetric functions $t = x+y$ and $v = xy = x(x+t)$. This proves the existence and uniqueness of a power series $h(t,v)$ in $R[[t,v]]$ such that $h(t, x(x+t)) = \beta(x)\beta(x+t)$. Let $Q_t : R \to R[[t]]$ be the unique ring homomorphism such that $Q_t(\beta)(v) = h(t,v)$. Then $Q_t(\beta)(x(x+t)) = \beta(x)\beta(x+t)$. Putting $t = 0$ yields $Q_0(\beta)(x^2) = \beta(x)^2$; hence $Q_0(\beta_i) = \beta_i^2$ for every $i \geq 0$. It follows that $Q_t(x) = x^2$ for every $x \in R$ since the β_i's generate R as a ring. In order to prove the symmetry in s, t of $(Q_t \circ Q_s)(\beta)$ we first extend $Q_t : R \to R[[t]]$ to $R[[x]]$ by putting $Q_t(x) = x(x+t)$. Then we have $Q_t(\beta(x)) = Q_t(\beta)(x(x+t)) = \beta(x)\beta(x+t)$. Assuming that $Q_t(s) = s(s+t)$ we obtain $(Q_t \circ Q_s)(x) = x(x+t)(x+s)(x+s+t)$. Hence $(Q_t \circ Q_s)(x)$ is symmetric in s, t. Thus, we can prove the symmetry of $(Q_t \circ Q_s)(\beta)$ by proving the symmetry of $(Q_t \circ Q_s)(\beta(x))$. We have

$$\begin{aligned} Q_t(\beta(x+s)) &= Q_t(\beta)(Q_t(x+s)) = Q_t(\beta)((x+s)(x+s+t)) \\ &= \beta(x+s)\beta(x+s+t) \end{aligned}.$$

Thus

$$\begin{aligned} (Q_t \circ Q_s)(\beta(x)) =& Q_t(\beta(x)\beta(x+s)) = Q_t(\beta(x))Q_t(\beta(x+s)) \\ =& \beta(x)\beta(x+t)\beta(x+s)\beta(x+s+t) \end{aligned}$$

is symmetric in s, t. This finishes the proof that $(Q_t \circ Q_s)(\beta)$ is symmetric. It follows that $(Q_t \circ Q_s)(y)$ is symmetric for every $y \in R$ since the coefficients of β generate R. This finishes the proof that $Z_2[\beta_*]$ is a Q-ring. We next compute $Q_t(\beta_n)$ by the method of residues. The identity $Q_t(\beta)(x(x+t)) = \beta(x)\beta(x+t)$ means that

$Q_t(\beta_n)$ is the coefficient of $v = x(x+t)$ in $\beta(x)\beta(x+t)$. We have $dv = tdx$ and $Q_t(\beta_n)$ is equal to

$$\begin{aligned}\text{Res } \frac{\beta(x)\beta(x+t)}{x^{n+1}(x+t)^{n+1}}tdx &= \sum_{i,j}\beta_i\beta_j\text{Res } \frac{x^i(x+t)^j}{x^{n+1}(x+t)^{n+1}}tdx \\ &= \sum_{i,j}\beta_i\beta_j\binom{j-n-1}{n-i}t^{i+j-2n}\end{aligned}.$$

The formula for $q_r(\beta_n)$ is the coefficient of t^r in this series. The formula shows that $q_r(\beta_n)$ is homogeneous of dimension $2n+r$ if $\dim(b_n) = n$. It then follows by the Cartan formula that $q_r(\beta_{n_1}\cdots\beta_{n_k})$ is homogeneous of dimension $2(n_1+\cdots n_k)+r$. This proves that $Z_2[\beta_*]$ is a graded Q-ring. QED

Recall that for any ring R and any subset $S \subseteq R$ there is a fraction ring $S^{-1}R$ obtained by formally inverting the elements in S. Let $j : R \to S^{-1}R$ be the canonical map.

Proposition 5. *If R is a Q-ring then so is the fraction ring $S^{-1}R$ and the canonical map $j : R \to S^{-1}R$ is a map of Q-rings.*

Proof. For any $x \in R$ let us put $h(x) = \sum_n j(q_n(x))t^n$. This defines a ring homomorphism $h : R \to S^{-1}R[[t]]$. The constant term of the formal power series $h(x)$ is $j(q_0(x)) = j(x)^2$. Hence $h(x)$ has a multiplicative inverse when $x \in S$. It follows that there is a unique ring homomorphism $Q_t : S^{-1}R \to S^{-1}R[[t]]$ such that $Q_t(j(x)) = h(x)$ for $x \in R$. By definition, $Q_t(x/y) = Q_t(x)/Q_t(y)$ for any fraction $x/y \in S^{-1}R$. Hence $Q_0(x/y) = (x/y)^2$. The symmetry in s,t of $Q_t(Q_s(x/y))$ is obvious from the formula $Q_t(Q_s(x/y)) = Q_t(Q_s(x))/Q_t(Q_s(y))$. QED

The fraction ring $Z_2[b_0^{-1}, b_*] = \{b_0\}^{-1}Z_2[b_0, b_1, \ldots]$ supports a Hopf algebra structure called the *Fa di Bruno Hopf algebra*; we shall denote it by $\mathcal{B}$. By definition, the comultiplication is the map $\Delta : \mathcal{B} \to \mathcal{B}\otimes\mathcal{B}$ such that

$$\Delta(b) = (b\otimes 1)\circ(1\otimes b)$$

where $b(x) = \sum_i b_i x^{i+1}$. The counit $\epsilon : \mathcal{B} \to Z_2$ is the map such that $\epsilon(b)(x) = x$. The power series $b(x)$ has a composition inverse $\overline{b}(x)$ since b_0 is invertible in $\mathcal{B}$. The antipode is the algebra map $\mathcal{B} \to \mathcal{B}$ such that $b(x) \mapsto \overline{b}(x)$.

Corollary. *The Fa di Bruno algebra $\mathcal{B}$ has a unique Q-ring structure such that $Q_t(b)(x(x+t)) = b(x)b(x+t)$ where $b(x) = \sum_i b_i x^{i+1}$. This is a graded Q-ring if we take dim$(b_i) = i$.*

Proof. Let $\beta(x) = \sum_i b_i x^i$. By Proposition 4 there is a unique Q-structure on $Z_2[b_*] = Z_2[b_0, b_1, \ldots]$ such that $Q_t(\beta)(x(x+t)) = \beta(x)\beta(x+t)$. We have $b(x) = x\beta(x)$. Hence

$$Q_t(b)(x(x+t)) = x(x+t)\beta(x)\beta(x+t) = b(x)b(x+t).$$

The result then follows from Proposition 5 since $\mathcal{B} = \{b_0\}^{-1}Z_2[b_*]$. QED

Recall that a formal power series $a(x)$ with coefficients in a Z_2-algebra R is *additive* if $a(x+y) = a(x)+a(y)$; this happens iff $a(x)$ has the form $a(x) = \sum a_i x^{2^i}$. If a_0 has an inverse then $a(x)$ has an additive composition inverse $\overline{a}(x)$. It follows that the algebra $Z_2[a_0^{\pm}, a_1, \dots] = \{a_0\}^{-1}Z_2[a_0, a_1, \dots]$ supports a Hopf algebra structure that we call the *extended Milnor Hopf algebra*; we shall denote it by $\mathcal{A}$. The comultiplication is the map $\Delta : \mathcal{A} \to \mathcal{A} \otimes \mathcal{A}$ such that

$$\Delta(a) = (a \otimes 1) \circ (1 \otimes a)$$

where $a(x) = \sum_i a_i x^{2^i}$.

Proposition 6. *The extended Milnor algebra $\mathcal{A}$ has a unique Q-ring structure such that $Q_t(a)(x(x+t)) = a(x)a(x+t)$, where $a(x) = \sum_i a_i x^{2^i}$. This is a graded Q-ring if we take dim$(a_n) = 2^n - 1$. We have the explicit formula*

$$Q_t(a_n) = a_n^2 + t^{-2^{n+1}}(\sum_{k=0}^{n} a_k t^{2^k})(\sum_{i=n+1}^{\infty} a_i t^{2^i}).$$

Proof. Let us first prove the result for the ring $R = Z_2[a_0, a_1, \dots]$. The result for $\mathcal{A}$ will follow by inverting a_0. As in the proof of Proposition 4 there is a power series $h(t,v)$ in $R[[t,v]]$ such that $h(t, x(x+t)) = a(x)a(x+t)$. Let us see that $h(t,x)$ is additive. The series $tx + x^2$ has a composition inverse in the ring $R[t^{-1}, t][[x]]$. Its inverse $r(x)$ is additive since $tx+x^2$ is additive. It follows that $h(t,x)$ is additive since $h(t, x(x+t)) = a(x)^2 + a(x)a(t)$ is additive and additive series are closed under composition. Hence there is a unique ring homomorphism $Q_t : R \to R[[t]]$ such that $Q_t(a)(v) = h(t,v)$. That this is a Q-structure is proved as in Proposition 4. We justify the explicit formula as follows. We note that $Q_t(a)(x(x+t)) = a(x)a(x+t)$ iff

$$\sum Q_t(a_n)(x^2 + tx)^{2^n} = a(x)^2 + a(x)a(t).$$

By looking at the x and the $x^{2^{n+1}}$ terms here, we see that the identity holds iff

$$Q_t(a_0)t = a_0 a(t), \text{ and } Q_t(a_n) + Q_t(a_{n+1})t^{2^{n+1}} = a_n^2 + a_{n+1}a(t).$$

By multiplying both sides by $t^{2^{n+1}}$, we see that the second equation holds iff

$$Q_t(a_n)t^{2^{n+1}} + Q_t(a_{n+1})t^{2^{n+2}} = (a_n t^{2^n})^2 + (a_{n+1}t^{2^{n+1}})a(t).$$

This is essentially a recursive equation, and one can check directly that its (unique) solution is given by

$$Q_t(a_n)t^{2^{n+1}} = a_n^2 t^{2^{n+1}} + (\sum_{k=0}^{n} a_k t^{2^k})(\sum_{i=n+1}^{\infty} a_i t^{2^i})$$

as claimed. That $\mathcal{A}$ is graded if we take dim$(a_n) = 2^n - 1$ is proved as in Proposition 4. QED

Remark. In particular we have

$$Q_t(a_0) = \sum_{0}^{\infty} a_0 a_i t^{2^i - 1}.$$

This shows that the Q-structure on $\mathcal{A}$ cannot survive if we insist that $a_0 = 1$.

Addendum to Section 1.

Nature supplies us with many examples of Q-rings through the cohomology of topological spaces and the homology of E_∞-spaces. Note that in this paper, homology and cohomology are always taken with coeficients in Z_2.

It is standard that the cohomology H^*X of a topological space X is a graded ring with natural Steenrod operations Sq^i for $i \geq 0$; see Steenrod, Epstein [1962], for instance. For $x \in H^nX$, we define $q_i(x) = Sq^{n-i}(x)$ for $0 \leq i \leq n$, and $q_i(x) = 0$ for $n < i$; then $R = H^*X$ is a graded Q-ring with elements of $H^n(X)$ having degree $-n$ (grading by codimension). For example, the Steenrod operations on $H^*RP^\infty = Z_2[x]$ are given by $Sq^0(x) = x$, $Sq^1(x) = x^2$ and $Sq^i(x) = 0$ for $i > 1$. Hence $Q_t(x) = x(x+t)$; thus if $X = RP^\infty \times \dots RP^\infty$ (n copies) then $H^*X = Z_2[x_1, \dots, x_n]$ is the Q-ring described in Proposition 3.

It is also standard that if E is an E_∞-space then H_*E is a graded ring with Dyer-Lashof operations Q^j for $j \geq 0$. See May [1971], for instance, for a description of the properties of these operations. The operation $q_i : H_nE \to H_{2n+i}E$ is the Dyer-Lashof operation Q^{n+i}. In fact the operations q_i were explicitely used and studied in Kudo, Araki [1956]. The usual properties of Dyer-Lashof operations translate into the statement that H_*E is a graded Q-ring with $Q_t = \sum q_i t^i$. For example, the homology of the classifying space BO_* for real vector bundles is the polynomial ring $Z_2[\beta_*]$ where $\beta_0, \beta_1, \dots$ is a basis of $H_*BO_1 = H_*RP^\infty$. It supports the generic power series $\beta(x) = \sum \beta_i x^i$ which arises in the theory of characteristic classes; see Milnor, Stasheff [1974], for instance. The Whitney sum of vector bundles gives BO_* the structure of an E_∞-space. The resulting Q-ring structure on $Z_2[\beta_*]$ is the one described in Proposition 4; the explicit formula derived there is equivalent to one in Priddy [1975]. We will give another direct geometric proof of this result in a sequel to this paper.

For the standard Dyer-Lashof algebra (and some indications of its history) see May [1971], Madsen [1975], and May [1976], for instance.

The Fa di Bruno Hopf algebra $\mathcal{B} = Z_2[b_0^{-1}, b_0, b_1, \dots]$ is studied in combinatorics; see Joni, Rota [1982] for instance. It is closely related to the dual of the Landweber-Novikov algebra; see Landweber [1967], Quillen [1971], Adams [1974], or Morava [1985], for instance.

The Adem relations are due to Adem [1957]. The idea of writing Adem relations via generating series occurs in Bisson [1977] and in Bullett, MacDonald [1982] (extended by Steiner [1984]). For an early application of the method of formal residues in algebraic toplogy, see the brief discussion on page 65 of Adams [1974].

2. The Kudo-Araki algebra $\mathcal{K}$ and its dual

Here we show that the coalgebra dual to $\mathcal{K}$ is exactly representing substitution of Ore polynomials. We consequently obtain two explicit basis of $\mathcal{K}$.

Recall that if M and N are Q-modules then so is $M \otimes N$, with the operation q_n defined by the Cartan formula:

$$q_n(x \otimes y) = \sum_{i+j=n} q_i(x) \otimes q_j(y).$$

Abstractly this defines a symmetric tensor product on the category of left $\mathcal{K}$-modules. It follows that $\mathcal{K}$ is a cocommutative bialgebra. More precisely, the comultiplication $\delta : \mathcal{K} \to \mathcal{K} \otimes \mathcal{K}$ can be defined as the unique Q-module map such that $\delta(1) = 1 \otimes 1$; the counit of $\mathcal{K}$ as the unique Q-module map $\epsilon : \mathcal{K} \to Z_2$ such that $\epsilon(1) = 1$ (here Z_2 has its unique Q-ring structure). From the relation $\delta(q_n(1)) = q_n(\delta(1))$ it follows that

$$\delta(q_n) = \sum_{i+j=n} q_i \otimes q_j.$$

From the relation $\epsilon(q_n(1)) = q_n(\epsilon(1))$ it follows that

$$\epsilon(q_n) = \begin{cases} 1 & \text{if } n = 0 \\ 0 & \text{otherwise.} \end{cases}$$

We will give a description of the graded dual $\mathcal{K}'$ of $\mathcal{K}$. First, let us see that $\mathcal{K}$ splits as a direct sum of coalgebras. The Adem relations are homogeneous of degree 2 since they only involve words $q_i q_j$ of length 2 on the generators. It follows that $\mathcal{K}$ is a graded ring, graded by "length of words", which we call the *exponent*. We shall denote by $\mathcal{K}(n)$ the homogeneous component of exponent n. It is clear from the Cartan formula that δ is mapping $\mathcal{K}(n)$ into $\mathcal{K}(n) \otimes \mathcal{K}(n)$. Hence $\mathcal{K}(n)$ is a coalgebra and we have a decomposition of $\mathcal{K}$ as a direct sum of coalgebras:

$$\mathcal{K} = \bigoplus_n \mathcal{K}(n).$$

We shall describe the graded dual of each coalgebra $\mathcal{K}(n)$; for this we need the *dimension grading* on $\mathcal{K}(n)$. It is the unique grading which makes $\mathcal{K}$ a graded Q-module and has $dim(1) = 0$. In order to prove its existence we can associate to the generator q_i the affine transformation $\alpha_i : N \to N$ given by $\alpha_i(x) = 2x + i$; this is recording the behavior of q_i on the dimensions of elements in any graded Q-module. Then to each word $q_{i_1} \cdots q_{i_n}$ we associate the affine transformation $\alpha_{i_1} \circ \cdots \alpha_{i_n}$. The Adem relations in Proposition 1 §1 express the word $q_m q_n$ in terms of the words $q_{m+2n-2i} q_i$. This is compatible with the identity $\alpha_m \circ \alpha_n = \alpha_{m+2n-2i} \circ \alpha_i$ satisfied by the affine transformations. It follows that $\mathcal{K}$ has a grading over the monoid of affine transformations $\{2^n x + d : n, d \geq 0\}$. If $y \in \mathcal{K}$ has "degree" $2^n x + d$ then we say that y is homogeneous of *dimension* d and exponent n (or $y \in \mathcal{K}(n)$). In order to study $\mathcal{K}(n)$ we need a good basis and we shall obtain one by studying the n-fold iterated total square.

For a Q-module M, the *n-fold iterated total square* $Q^{(n)} = Q_{t_n, \ldots, t_1} : M \to M[[t_1, \ldots, t_n]]$ is defined inductively by

$$Q^{(n)}(x) = Q_{t_n}(Q^{(n-1)}(x)),$$

where Q_{t_n} is extended to $M[[t_1, \ldots, t_{n-1}]]$ by putting $Q_{t_n}(t_i) = t_i(t_i + t_n)$ for every $i < n$.

The 2-fold total square $Q_{t,s} = Q_t \circ Q_s : M \to M[[s,t]]$ is symmetric in s, t. It is also invariant under the automorphism σ of $M[[s,t]]$ defined by the substitution $s \mapsto s + t$ and $t \mapsto t$, since $\sigma(s(s+t)) = \sigma(s)(\sigma(s) + \sigma(t)) = (s+t)t$. It follows that $Q_{t,s}$ is invariant under the full group $GL(2, Z_2)$ of linear substitutions since this group is generated by σ and the transposition (s,t). In order to develop an expansion of the iterated total operations that takes the symmetry into account, we need to recall the theory of Dickson invariants. If R is a Z_2-algebra, we shall say that a polynomial $p(x) = \sum_{i=0}^{n} c_i \; x^{2^i}$ with coefficients in R is an *Ore polynomial of exponent* $\leq n$; see Ore [1933], Rota [1971]. From the identity $(x+y)^2 = x^2 + y^2$ it follows that $p(x+y) = p(x) + p(y)$; hence an Ore polynomial is additive. The set of roots of $p(x)$ is closed under addition and hence forms a Z_2-vector space. Generically, the appropriate symmetry group for the set of roots is the general linear group $GL(n) = GL(n, Z_2)$. Let us make this more precise. The group $GL(n)$ is acting by linear substitutions on the polynomial ring $Z_2[t_1, \dots , t_n]$; according to Dickson, the subring of invariants is the polynomial algebra $Z_2[t_1, \dots , t_n]^{GL(n)} = Z_2[w_0, \dots , w_{n-1}]$, where

$$W_n(x) = x^{2^n} + \sum_{i=0}^{n-1} w_i \; x^{2^i} = \prod_{v \in \langle t_1, \dots , t_n \rangle} (x + v)$$

and $\langle t_1, \dots , t_n \rangle$ is the Z_2-vector space generated by $t_1, \dots , t_n$. We shall denote the ring of Dickson invariants $Z_2[w_0, \dots , w_{n-1}]$ by $\mathcal{W}(n)$. Note that w_i is a homogeneous polynomial of degree $2^n - 2^i$ (in $Z_2[t_1, \dots , t_n]$). For any Z_2-vector space M we have

$$M[t_1, \dots , t_n]^{GL(n)} = M[w_0, \dots , w_{n-1}] \quad \text{and}$$
$$M[[t_1, \dots , t_n]]^{GL(n)} = M[[w_0, \dots , w_{n-1}]].$$

These are graded by *codimension*, where by definition $\operatorname{codim}(w_i) = 2^n - 2^i$.

Lemma 1. *If M is a Q-module then $Q^{(n)} : M \to M[[t_1, \dots , t_n]]$ takes its values in $M[[w_0, \dots , w_{n-1}]]$. Hence there is an expansion*

$$Q^{(n)}(x) = \sum_{l(R)=n} q_R(x) w^R$$

with $q_R \in \mathcal{K}(n)$ and $w^R = w_0^{r_0} \cdots w_{n-1}^{r_{n-1}}$ for $R = (r_0, \dots , r_{n-1})$.

Proof. It suffices to show that $Q_{t_n,\dots,t_1}$ is invariant under the action of $GL(n)$. But this group is generated by the transpositions $(t_i, t_{i+1}) \mapsto (t_{i+1}, t_i)$ $(1 \leq i < n)$ and the linear substitution σ such that $(t_{n-1}, t_n) \mapsto (t_{n-1} + t_n, t_n)$. If we apply the case $n = 2$ to the Q-module $M[[t_1, \dots , t_{n-2}]]$ with $s = t_{n-1}$ and $t = t_n$ we obtain that $Q_{t_n,\dots,t_1}$ is invariant under the action by σ and the transposition $(t_{n-1}, t_n) \mapsto (t_n, t_{n-1})$. But $Q_{t_n,\dots,t_1} = Q_{t_n} \circ Q_{t_{n-1},\dots,t_1}$ is invariant under the transpositions $(t_i, t_{i+1}) \mapsto (t_{i+1}, t_i)$ for $1 \leq i < n-1$ since by the inductive hypothesis $Q_{t_{n-1},\dots,t_1}$ is invariant under $GL(n-1)$. This proves the result. QED

Notice that if M is graded and $x \in M$ is homogeneous then $Q^{(n)}(x)$ is homogeneous of dimension $2^n \dim(x)$, when $\operatorname{codim}(t_i) = 1$. Applying this observation to the case $M = \mathcal{K}$ and $x = 1$ we obtain that $\dim(q_R) = \operatorname{codim}(w^R)$. We shall prove that the q_R's form a basis of $\mathcal{K}(n)$. We first show that they linearly span $\mathcal{K}(n)$.

The polynomial $W_n(x)$ is related to the polynomial $W_{n-1}(x)$ by the formula $W_n(x) = W_{n-1}(x)W_{n-1}(x + t_n)$, or equivalently by $W_n(x) = W_{n-1}(x)(W_{n-1}(x) + W_{n-1}(t_n))$ since $W_{n-1}(x)$ is additive. This can be written as $W_n = V_n \circ W_{n-1}$, where $V_n(x) = x(x + u_n)$ and $u_n = W_{n-1}(t_n)$. Iterating, we obtain that $W_n = V_n \circ \cdots \circ V_1$ where $V_i(x) = x(x + u_i)$ and $u_i = W_{i-1}(t_i)$ for $1 \leq i \leq n$. We have

$$Z_2[w_0, \dots , w_{n-1}] \subseteq Z_2[u_1, \dots , u_n] \subseteq Z_2[t_1, \dots , t_n]$$

and the polynomials $u_1, \dots, u_n$ are algebraically independent. Let us put $u^K = u_1^{k_1} \cdots u_n^{k_n}$ and $q^K = q_{k_1} \cdots q_{k_n}$ for $K = (k_1, \dots, k_n) \in N^n$.

Lemma 2. *The total square of order n has an expansion*

$$(*) \qquad Q^{(n)}(x) = \sum_{l(K)=n} q^K(x) u^K.$$

Proof. Let us first verify by induction on n that if y is an element in a Q-ring such that $Q_t(y) = y(y+t)$ then $Q^{(n)}(y) = W_n(y)$. This is obvious for $n = 1$. Supposing that $Q^{(n-1)}(y) = W_{n-1}(y)$ we obtain

$$\begin{aligned} Q^{(n)}(y) =& Q_{t_n}(Q^{(n-1)}(y)) = Q_{t_n}(W_{n-1}(y)) = \prod_{v \in \langle t_1, \dots, t_{n-1} \rangle} Q_{t_n}(y+v) \\ &= \prod_{v \in \langle t_1, \dots, t_{n-1} \rangle} y(y+t_n) + v(v+t_n) = \prod_{v \in \langle t_1, \dots, t_{n-1} \rangle} (y+v)(y+v+t_n) \\ &= W_{n-1}(y) W_{n-1}(y+t_n) = W_n(y). \end{aligned}$$

Let us now prove by induction on n that the expansion $(*)$ is valid for every n. By symmetry we have $Q^{(n)} = Q_{t_1, \dots, t_n}$: thus $Q^{(n)}$ is the composite

$$M \xrightarrow{Q_{t_n}} M[[t_n]] \xrightarrow{Q^{(n-1)}} M[[t_1, \dots, t_n]]$$

where the Q-structure is extended to $M[[t_n]]$ by putting $Q_t(t_n) = t_n(t_n + t)$. From the result just proved it follows that $Q^{(n-1)}(t_n) = W_{n-1}(t_n) = u_n$. Assuming that the expansion $(*)$ is valid for $n-1$ we obtain

$$\begin{aligned} Q^{(n)}(x) = Q^{(n-1)}(\sum_i q_i(x) t_n^i) &= \sum_i Q^{(n-1)}(q_i(x)) u_n^i \\ &= \sum_i \sum_{l(K)=n-1} q^K(q_i(x)) u^K u_n^i = \sum_{l(K)=n-1} \sum_i q^{K,i}(x) u^{K,i} \\ &= \sum_{l(K)=n} q^K(x) u^K \end{aligned}$$

where K, i denotes the concatenation $(k_1, \dots, k_{n-1}, i)$ of $K = (k_1, \dots, k_{n-1})$ and i. QED

The equality of the two expansions

$$\sum_{l(K)=n} q^K(x) u^K = \sum_{l(R)=n} q_R(x) w^R$$

of $Q^{(n)}(x)$ shows that each q^K is a linear combination of the q_R's. But the q^K's generate $\mathcal{K}(n)$ and it follows that the q_R's generate $\mathcal{K}(n)$. We shall prove that the q_R's are linearly independent by constructing a Q-module $\mathcal{W}'$ in which their images are linearly independent.

For any Z_2-algebra R let $D_n(R)$ denote the set of monic Ore polynomials of exponent n with coefficients in R. The functor $D_n : Alg \to Sets$ is represented by the algebra $\mathcal{W}(n)$, with $W_n(x)$ as the generic element; see appendix A for this terminology. Composition of Ore polynomials defines an operation $D_m \times D_n \to$

D_{m+n} that is represented by the ring homomorphism $\Delta : \mathcal{W}(m+n) \to \mathcal{W}(m) \otimes \mathcal{W}(n)$ such that

$$\Delta(W_{m+n}) = (W_m \otimes 1) \circ (1 \otimes W_n).$$

Collecting these maps together we obtain a coalgebra structure on $\mathcal{W} = \oplus_{n \geq 0} \mathcal{W}(n)$.

Recall that each $\mathcal{W}(n) = Z_2[w_0, \dots, w_{n-1}]$ is a ring graded by codimension, where $\mathrm{codim}(w_i) = 2^n - 2^i$. Let $\theta_R : \mathcal{W}(n) \to Z_2$ be the linear form picking the coefficient of w^R. The subspace $\mathcal{W}^i(n)$ with basis $(w^R : \mathrm{codim}(w^R) = i)$ is finite dimensional. Thus the *graded dual* $\mathcal{W}'(n)$ is the linear span of the θ_R's. It is graded by *dimension* where $\dim(\theta_R) = \mathrm{codim}(w^R)$. If $\mathcal{W}'_i(n)$ denotes its component of dimension i then we have $\mathcal{W}'_i(n) = [\mathcal{W}^i(n), Z_2]$. Each $\mathcal{W}'(n)$ has a coalgebra structure (δ, ϵ) obtained by dualising the algebra structure of $\mathcal{W}(n)$. From the relation $w^I w^J = w^{I+J}$ it follows by duality that

$$\delta(\theta_K) = \sum_{I+J=K} \theta_I \otimes \theta_J.$$

The counit $\epsilon : \mathcal{W}'(n) \to Z_2$ is the evaluation at $1 \in \mathcal{W}(n)$. In this way we obtain a coalgebra structure (δ, ϵ) on the direct sum $\mathcal{W}' = \bigoplus_n \mathcal{W}'(n)$.

Proposition 1. *The graded dual $\mathcal{W}'$ is a bialgebra where the algebra structure is the convolution obtained from $\Delta : \mathcal{W} \to \mathcal{W} \otimes \mathcal{W}$ and the coalgebra structure is obtained by dualising the algebra structure on each $\mathcal{W}(n)$.*

Proof. We saw that $\mathcal{W}'$ is a coalgebra with the maps (δ, ϵ) that dualise the algebra structure on each $\mathcal{W}(n)$. Let us see that $\mathcal{W}'$ is a subalgebra of the convolution algebra $[\mathcal{W}, Z_2]$ obtained from Δ. It is easy to verify that each $\Delta : \mathcal{W}(m+n) \to \mathcal{W}(m) \otimes \mathcal{W}(n)$ preserves codimension, if codimension on $\mathcal{W}(m) \otimes \mathcal{W}(n)$ is defined by $\mathrm{codim}(x \otimes y) = 2^n \mathrm{codim}(x) + \mathrm{codim}(y)$. It follows that if $f \in \mathcal{W}'_i(m)$ and $g \in \mathcal{W}'_j(n)$ then $f \star g \in \mathcal{W}'_k(m+n)$ where $\star$ denotes the convolution product and where $k = 2^n i + j$. It remains to verify that $\mathcal{W}'$ is a bialgebra. Let us show that the convolution product $\mathcal{W}' \otimes \mathcal{W}' \to \mathcal{W}'$ and the unit $Z_2 \to \mathcal{W}'$ are coalgebra maps. It suffices to prove that each convolution product $\mathcal{W}'(m) \otimes \mathcal{W}'(n) \to \mathcal{W}'(m+n)$ and each counit $\epsilon : \mathcal{W}'(n) \to Z_2$ is a coalgebra map. But this is true by duality since each convolution product is dualising the algebra map $\Delta : \mathcal{W}(m+n) \to \mathcal{W}(m) \otimes \mathcal{W}(n)$ and each ϵ is dualising the algebra map $Z_2 \to \mathcal{W}(n)$. QED

We next exhibit a Q-module structure on $\mathcal{W}'$. For $f \in \mathcal{W}'$ let $q_i(f) = f \star \theta_i$ where $\theta_i \in \mathcal{W}'(1)$ is the basis element. With this definition we have

$$Q_t(f) = \sum_i (f \star \theta_i) t^i = f \star \sum_i \theta_i t^i.$$

Let $v_t^\dagger : \mathcal{W}(1) \to Z_2[t]$ be the ring homomorphism (it is an isomorphism) representing the Ore polynomial $v_t(x) = x^2 + tx$ (see appendix A for the notation $(\ )^\dagger$). Then we have the expansions $v_t^\dagger = \sum_i \theta_i t^i$ and $Q_t(f) = f \star v_t^\dagger$.

Lemma 3. *The operation $Q_t(f) = f \star v_t^\dagger$ defines a Q-module structure on $\mathcal{W}'$.*

Proof. We need to prove that $Q_t \circ Q_s(f)$ is symmetric in s and t. Let $h^\dagger : \mathcal{W}(1) \to Z_2[s,t]$ be the ring homomorphism representing the Ore polynomial $h(x) = x^2 + s(s+t)x$. The polynomial $(h \circ v_t)(x) = x(x+t)(x+s)(x+s+t)$ is symmetric in s and t. Hence $(f\star h^\dagger)\star v_t^\dagger = f\star(h^\dagger\star v_t^\dagger) = f\star(h\circ v_t)^\dagger$ is symmetric in s and t. Thus

$$\begin{aligned}(f\star h^\dagger)\star v_t^\dagger =&\Big(\sum_i q_i(f)(s^2+st)^i\ \Big)\star v_t^\dagger = \sum_i (q_i(f)\star v_t^\dagger)(s^2+st)^i\\ =&\sum_i Q_t(q_i(f))(s^2+st)^i = Q_t\sum_i q_i(f)s^i\\ =&Q_t\circ Q_s(f)\end{aligned}$$

is symmetric in s and t. QED

Lemma 4. *(Generalised Cartan formulas) If M and N are Q-modules then*

$$q^K(x\otimes y) = \sum_{I+J=K} q^I(x)\otimes q^J(y) \quad \textit{and} \quad q_R(x\otimes y) = \sum_{I+J=R} q_I(x)\otimes q_J(y)$$

for any $x\in M$ and $y\in N$.

Proof. If R is a Q-ring then the n-fold total square is a ring homomorphism and we have $Q^{(n)}(xy) = Q^{(n)}(x)Q^{(n)}(y)$. This proves the two identities for Q-rings. For Q-modules M and N the argument can be carried out in the "enveloping" Q-ring $R = \tilde\Lambda M\otimes\tilde\Lambda N$ introduced in the next section. QED

Let $1\in\mathcal{W}'(0)$ be the unit element for the convolution product. There is a unique map of Q-modules $i:\mathcal{K}\to\mathcal{W}'$ such that $i(1)=1$ since $\mathcal{K}$ is free as Q-module.

Theorem 1. *The map $i:\mathcal{K}\to\mathcal{W}'$ is an anti-isomorphism of algebras and an isomorphism of coalgebras. We have $i(q_R)=\theta_R$ for every R, and the operations q_R with $l(R)=n$ form a basis of $\mathcal{K}(n)$.*

Proof. Let us first verify that i is an anti-homomorphism of algebras. It is preserving the unit element since $i(1)=1$. The identity $i(xy)=i(y)\star i(x)$ will be proved if we show that it holds when x is a generator q_n of $\mathcal{K}$. We have $i(q_n\ y) = q_n(i(y)) = i(y)\star\theta_n$ since i is a map of Q-modules. It follows that $i(q_n\ y) = i(y)\star i(q_n)$ since $i(q_n)=q_n(1)=1\star\theta_n=\theta_n$. This finishes the proof that i is an anti-homomorphism of algebras. Let $V_k^\dagger:\mathcal{W}(1)\to Z_2[u_1,\dots,u_n]$ be the ring homomorphism representing the Ore polynomial $V_k(x)=x(x+u_k)$. We have an expansion $V_k^\dagger=\sum_i\theta_i\ u_k^i$. If we apply i to the power series $Q^{(n)}(x)$ and use the expansions provided by Lemma 1 and 2 we obtain

$$\sum_{l(R)=n} i(q_R)\ w^R = \sum_{l(K)=n} i(q^K)\ u^K$$

where $q^K = q_{k_1}\cdots q_{k_n}$ and $u^K = u_1^{k_1}\cdots u_n^{k_n}$. But

$$i(q^K) = i(q_{k_n})\star\cdots\star i(q_{k_1}) = \theta_{k_n}\star\cdots\star\theta_{k_1}$$

since $i(q_k)=\theta_k$ and i is anti-homomorphism. It follows that

$$\sum_{l(K)=n} i(q^K)\ u^K = V_n^\dagger\star\cdots\star V_1^\dagger = (V_n\circ\cdots\circ V_1)^\dagger = W_n^\dagger.$$

But

$$W_n^\dagger = \sum_{l(R)=n} \theta_R w^R$$

since W_n is the generic monic Ore polynomial and $W_n^\dagger : \mathcal{W}(n) \to \mathcal{W}(n)$ is the identity map. This proves that $i(q_R) = \theta_R$ for every R. It follows that the q_R's are linearly independent since the θ_R's are. Hence they form a basis and i is a linear isomorphism. It remains to show that i preserves the coalgebra structures. This follows from lemma 4 and the formula for $\delta(\theta_R)$ given above Proposition 1. QED

Proposition 2. *For each $n \geq 0$ the operations $q^K = q_{k_1} \cdots q_{k_n}$ with $k_1 \leq \cdots \leq k_n$ form a basis of $\mathcal{K}(n)$.*

Proof. For every $n \geq 0$ let us order N^n lexicographicaly. Let $J_n \subseteq N^n$ be the set of increasing sequences $k_1 \leq \cdots \leq k_n$. If $m > r$ then the Adem relations in Proposition 1 §1 give a rewrite rule that expresses $q_m q_r$ as a sum of terms $q_j q_i$ with $j < m$ on the right hand side. This is because $2i \geq m + r$, since the bottom of the binomial coefficients must be non-negative. Hence $j = m + 2r - 2i \leq r < m$. This shows that $q^K = q_{k_1} \cdots q_{k_n}$ can be rewritten as a linear combination of elements of smaller index when $K \notin J_n$. This proves that the elements q^K with $K \in J_n$ generate $\mathcal{K}(n)$. To prove they form a basis we use a counting argument for the dimension of $\mathcal{K}_m(n)$, the homogeneous component of grade m of $\mathcal{K}(n)$ (here we say grade instead of dimension to avoid confusion). The elements q^K of grade m with $K \in J_n$ generate $\mathcal{K}_m(n)$. We have $\mathrm{grade}(q^K) = k_1 + k_2 2 + \cdots + k_n 2^n$. On the other hand, the elements q_R of grade m form a basis of $\mathcal{K}_m(n)$. We have $\mathrm{grade}(q_R) = \mathrm{codim}(w^R) = r_0(2^n - 2^0) + \cdots + r_{n-1}(2^n - 2^{n-1})$. But the transformation $r_i = k_{i+1} - k_i$ (with $r_0 = k_1$) defines a bijection between these two sets of elements. It follows that the q^K's of grade m with $K \in J_n$ form a basis of $\mathcal{K}_m(n)$. QED

Addendum to Section 2.

Historically, the Dyer-Lashof algebra was modelled upon the Steenrod algebra. As we discuss in section 4, the comultiplication for the Milnor coalgebra dual to the Steenrod algebra is representing composition of additive formal power series. The existence of a dual pairing between Dyer-Lashof operations and Dickson invariants is implicit in Madsen's thesis; see Madsen [1975]. There he describes a comultiplication which is dual to the composition of "upper-indexed" Dyer-Lashof operations. Wilkerson [1983] and Morava [1991] speculate on how to derive this coproduct directly from the algebra of the Dickson invariants.

If $V = Z_2^n$ then $H^*V = Z_2[t_1, \cdots, t_n]$ and $\mathcal{W}(n) = H^*V^{GL(n)}$ is the image of the ring homomorphism $H^*\Sigma_{2^n} \to H^*V$ induced by the natural "diagonal" inclusion $Z_2^n \subseteq \Sigma_{2^n}$. See Mui [1975], Madsen, Milgram [1979], or Mann, Milgram [1982] for more discussion of this point.

An expansion of iterated total operations in terms of Dickson invariants is discussed in Mui [1983] and in Lomonaco [1992].

Some good sources for algebraic background on the Dickson invariants are Mui [1975] and Wilkerson [1983]. The original reference given there is Dickson [1911]. See also Ore [1933] and Rota [1971].

3. Free Q-rings.

In this section we show that free Q-rings are polynomial rings. The result involves an explicit construction of the Q-ring freely generated by a Q-module; we show that it is the enveloping algebra of a predetermined squaring or *Frobenius* operation. We also introduce the concept of *rank* grading on a Q-ring.

We shall denote by $Q\langle V\rangle$ the Q-ring freely generated by a Z_2-vector space V. The free Q-ring on one generator will be denoted by $Q\langle x\rangle$. To construct $Q\langle V\rangle$ the first step is to take $\mathcal{K}\otimes V$ which is the free Q-module on V. The second step is to construct a Q-ring from $\mathcal{K}\otimes V$ or more generally from a Q-module. This is done with the *enveloping algebra* $\tilde{\Lambda}M = \tilde{\Lambda}(M, q_0)$ of a vector space M equiped with an endomorphism q_0. We have $Q\langle V\rangle = \tilde{\Lambda}(\mathcal{K}\otimes V)$ and in particular, $Q\langle x\rangle = \tilde{\Lambda}\mathcal{K}$.

Recall that the *Frobenius endomorphism* of a commutative Z_2-algebra is the map $x \mapsto x^2$. For a Q-ring this is the operation q_0. We shall sometimes say that a Z_2-vector space M equipped with an arbitrary endomorphism $q_0 : M \to M$ is a *Frobenius module.* It is *graded* when M is graded and $q_0(M_n) \subseteq M_{2n}$. The forgetful functor from commutative Z_2-algebras to Frobenius modules has a left adjoint $\tilde{\Lambda}(-)$ that we now describe. If M is a Frobenius module then the ring $\tilde{\Lambda}M$ is the quotient of the symmetric algebra $S(M)$ by the ideal generated by the differences $x^2 - q_0(x)$ for $x \in M$. We shall refer to $\tilde{\Lambda}M$ as the *enveloping algebra* of (M, q_0).

Proposition 1. *If M is a Q-module, then the enveloping algebra $\tilde{\Lambda}M$ of (M, q_0) is a Q-ring. The functor $M \mapsto \tilde{\Lambda}(M)$ is left adjoint to the forgetful functor from Q-rings to Q-modules.*

Proof. There is a unique ring homomorphism $Q_t : S(M) \to S(M)[[t]]$ extending the map $Q_t : M \to M[[t]]$. The ring map $Q_t \circ Q_s : S(M) \to S(M)[[s,t]]$ is symmetric in s and t since it is extending $Q_t \circ Q_s : M \to M[[s,t]]$ and the latter is symmetric. Let $\pi : S(M) \to \tilde{\Lambda}M$ be the canonical map and let us use the same notation for its extension $S(M)[[t]] \to \tilde{\Lambda}M[[t]]$. In particular, putting $t = 0$ we obtain $Q_0 \circ Q_s = Q_s \circ Q_0$ where $Q_0(s) = s^2$. We have $\pi Q_0(x) = \pi x^2$ for any $x \in S(M)$, since this relation is true for $x \in M$ and Q_0 and $(-)^2$ are ring homomorphisms. Then for any $x \in M$ we have

$$\pi Q_t(q_0(x)) = \pi Q_t Q_0(x) = \pi Q_0 Q_t(x) = \pi Q_t(x)^2 = \pi Q_t(x^2)$$

where $Q_0(t) = t^2$. It follows from this equality that there is a unique ring map $Q_t : \tilde{\Lambda}M \to \tilde{\Lambda}M[[t]]$ such that $Q_t(\pi(x)) = \pi(Q_t(x))$ for every $x \in S(M)$. From the relation $\pi Q_0(x) = \pi x^2$ for any $x \in S(M)$ it follows that $Q_0(x) = x^2$ for every $x \in \tilde{\Lambda}M$. The symmetry in s and t of $Q_t \circ Q_s : \tilde{\Lambda}M \to \tilde{\Lambda}M[[s,t]]$ follows from the symmetry of the corresponding map on $S(M)$. This proves that $\tilde{\Lambda}M$ is a Q-ring. Let us prove that $\tilde{\Lambda}(-)$ is left adjoint to the forgetful functor from Q-rings to Q-modules. We need to prove that if R is a Q-ring and $f : M \to R$ is a map of Q-modules then there is a unique map of Q-rings $\tilde{f} : \tilde{\Lambda}M \to R$ such that $\tilde{f}(x) = f(x)$ for $x \in M$. But we have $f(q_0(x)) = q_0(f(x)) = f(x)^2$ since f is a map of Q-modules. It follows that there is a unique map of rings $\tilde{f} : \tilde{\Lambda}M \to R$ such that $\tilde{f}(x) = f(x)$ for $x \in M$. It remains to verify that $Q_t(\tilde{f}(x)) = \tilde{f}(Q_t(x))$ for every $x \in \tilde{\Lambda}M$. But it suffices to verify this equality for $x \in M$ since both sides are ring homomorphisms and M generates $\tilde{\Lambda}M$ as a ring. For every $x \in M$

$Q_t(\tilde{f}(x)) = Q_t(f(x))$ and $\tilde{f}(Q_t(x)) = f(Q_t(x))$ and also $Q_t(f(x)) = f(Q_t(x))$ since f is a map of Q-modules. QED

Corollary. *The free Q-ring on a vector space V is $\tilde{\Lambda}(\mathcal{K} \otimes V)$. In particular $Q\langle x\rangle$, the free Q-ring on one generator, is $\tilde{\Lambda}\mathcal{K}$.*

Proof. Each functor $\tilde{\Lambda}(-)$ and $\mathcal{K} \otimes (-)$ is left adjoint to the corresponding forgetful functor. The result follows from the fact that a composite of left adjoints is left adjoint to the composite; see MacLane [1971], for instance. QED

A Frobenius module is nothing but a module over the polynomial algebra $Z_2[q_0]$. Hence the free Frobenius module generated by a vector space V is $Z_2[q_0] \otimes V$. According to Proposition 2 §2 the algebra $\mathcal{K}$ has a basis $q_{i_1}q_{i_2}\cdots q_{i_n}$ where $i_1 \leq i_2 \leq \cdots \leq i_n$. But each such $q_{i_1}q_{i_2}\cdots q_{i_n}$ can be written uniquely as $q_0^r q_{i_k}\cdots q_{i_n}$ where $0 < i_k \leq \ldots \leq i_n$. It follows that $\mathcal{K} = Z_2[q_0] \otimes \mathcal{K}^\flat$ where $\mathcal{K}^\flat$ is the linear span of the elements $q_{j_1}\cdots q_{j_n}$ such that $0 < j_1 \leq \cdots \leq j_n$.

Proposition 2. *For any vector space V the free Q-ring $Q\langle V\rangle$ is isomorphic to the symmetric algebra $S(\mathcal{K}^\flat \otimes V)$. In particular, the free Q-ring on one generator $Q\langle x\rangle$ has a polynomial basis consisting of the elements $q_{i_1}\cdots q_{i_n}(x)$ where $0 < i_1 \leq \cdots \leq i_n$.*

Proof. We saw above that $\mathcal{K} = Z_2[q_0] \otimes \mathcal{K}^\flat$. Hence for any vector space V, we have

$$Q\langle V\rangle = \tilde{\Lambda}(\mathcal{K} \otimes V) = \tilde{\Lambda}(Z_2[q_0] \otimes \mathcal{K}^\flat \otimes V).$$

The result then follows from the fact that a composite of left adjoints is left adjoint to the composite. More explicitly, the first functor $Z_2[q_0] \otimes (-)$ is left adjoint to the forgetful functor from Frobenius modules to Z_2-vector spaces; the second functor $\tilde{\Lambda}(-)$ is left adjoint to the forgetful functor from Z_2-algebras to Frobenius modules. Hence their composite $\tilde{\Lambda}(Z_2[q_0] \otimes (-))$ is left adjoint to the forgetful functor from algebras to vector spaces. Hence $\tilde{\Lambda}(Z_2[q_0] \otimes V)$ is the symmetric algebra $S(V)$ for any V. Thus $S(\mathcal{K}^\flat \otimes V) = \tilde{\Lambda}(Z_2[q_0] \otimes \mathcal{K}^\flat \otimes V) = Q\langle V\rangle$ for any V. QED

Let M be a Frobenius module with a basis $(u_i : i \in I)$. Consider the family of commutative monomials $u^S = u_{i_1}\cdots u_{i_n}$ where $S = \{i_1, \ldots, i_n\}$ runs through the finite subsets of I. By using the relation $u_i^2 = q_0(u_i)$ it is easy to see that the family (u^S) generates $\tilde{\Lambda}M$. We shall prove that the family (u^S) is a basis of $\tilde{\Lambda}M$. Consider the filtration $F_0 \subseteq F_1 \subseteq \cdots$ where F_n is the linear span of the monomials u^S with S of size at most n. The subgroup F_n does not depend on the basis $(u_i : i \in I)$ since it is the linear span of all the elements that can be written as a product of at most n elements in M. We have $1 \in F_0$ and $F_nF_m \subseteq F_{n+m}$. The associated graded algebra

$$\mathrm{gr}\tilde{\Lambda}M = \bigoplus_n F_n/F_{n-1}$$

is generated by F_1/F_0. Moreover, we have $x^2 = 0$ in F_2/F_1 for every $x \in F_1/F_0$ since $x^2 = q_0(x) \in F_1$. If ΛM is the exterior algebra on M then there is an algebra map $i : \Lambda M \to \mathrm{gr}\tilde{\Lambda}M$ extending the canonical map $M \to F_1/F_0$. The map i is surjective since F_1/F_0 generates $\mathrm{gr}\tilde{\Lambda}M$.

Lemma 1. *The map $i : \Lambda M \to \mathrm{gr}\tilde{\Lambda}M$ is an isomorphism.*

Proof. A Frobenius module is the same as a module over $Z_2[q_0]$. Any module is a directed colimit of finitely presented modules. Hence it suffices to prove the result for finitely presented modules over $Z_2[q_0]$ since the functors $M \mapsto \Lambda M$ and $M \mapsto \mathrm{gr}\tilde{\Lambda}M$ are preserving directed colimits. According to an elementary theorem of algebra, every finitely presented module over $Z_2[q_0]$ is a direct sum of cyclic modules. It suffices to prove the result in the case where M is a cyclic module, since for any Frobenius modules M and N we have a commutative square of canonical maps

$$\begin{tikzcd}
\Lambda(M) \otimes \Lambda(N) \arrow[r] \arrow[d, "i \otimes i"'] & \Lambda(M \oplus N) \arrow[d, "i"'] \\
\mathrm{gr}\tilde{\Lambda}(M) \otimes \mathrm{gr}\tilde{\Lambda}(N) \arrow[r] & \mathrm{gr}\tilde{\Lambda}(M \oplus N)
\end{tikzcd}$$

in which the horizontal arrows are isomorphisms. There are two cases to consider (depending on the type of M). If M is infinite cyclic then $M = Z_2[q_0]x$ is free over a generator x. It follows that $\tilde{\Lambda}(Z_2[q_0]x)$ is freely generated by x as a Z_2-algebra. Thus $\tilde{\Lambda}M = Z_2[x]$ and the canonical map $M \to \tilde{\Lambda}M$ is the linear map $Z_2[q_0]x \to Z_2[x]$ such that $q_0^n x \mapsto x^{2^n}$. But every natural number n can be expressed uniquely as a sum of distinct powers of 2. Hence every x^n can be written uniquely as a product $q_0^{i_1}(x) \dots q_0^{i_r}(x)$ where $i_1 < \cdots < i_r$. Let us put $l(n) = r$. For any $r \geq 0$ let $B_r = \{x^n : l(n) = r\}$. Then B_1 is a basis of M and the set $B_0 \cup \cdots \cup B_r$ is a basis of F_r. It follows that B_r projects to a basis in F_r/F_{r-1} and the canonical map $\Lambda^r M \to F_r/F_{r-1}$ is bijective. This finishes the proof in the case where M is infinite cyclic. In the case where M is finite cyclic, we have $M = Z_2[q_0]x$ with x satisfying a defining relation $p(q_0)x = 0$, where

$$p(q_0) = q_0^n + a_{n-1}q_0^{n-1} + \cdots + a_1 q_0 + a_0$$

is a monic polynomial of degree n. But then ΛM has dimension 2^n since M has dimension n. We have observed that i is surjective. Thus the result will be proved if we show that $\mathrm{gr}\tilde{\Lambda}M$ has dimension 2^n. But $\mathrm{gr}\tilde{\Lambda}M$ and $\tilde{\Lambda}M$ have the same dimension since

$$\begin{aligned} \sum_{i=0}^{n} \dim(F_i/F_{i-1}) &= \sum_{i=0}^{n} \dim(F_i) - \dim(F_{i-1}) \\ &= \dim(F_n) - \dim(F_{-1}) = \dim \tilde{\Lambda}M \end{aligned} .$$

Thus it suffices to prove that $\tilde{\Lambda}M$ has dimension 2^n. By definition, $\tilde{\Lambda}M$ is generated as a ring by an element x satisfying the relation $p(q_0)x = 0$ where $q_0 x = x^2$. Equivalently, it is generated by an element x satisfying the defining relation $q(x) = 0$ where $q(x)$ is the Ore polynomial

$$q(x) = x^{2^n} + a_{n-1}x^{2^{n-1}} + \cdots + a_1 x^2 + a_0 x.$$

It follows that $\tilde{\Lambda}M = Z_2[x]/(q(x))$ has dimension 2^n. QED

THEOREM 1. *(Basis theorem) Let M be a Frobenius module and let $(u_i : i \in I)$ be a basis of M. Then the monomials $u^S = u_{i_1} \cdots u_{i_n}$ where $S = \{i_1, \ldots, i_n\}$ runs through the finite subsets of I form a linear basis of $\tilde{\Lambda}M$.*

PROOF. For any $n \geq 0$ let B_n be the family of monomials u^S where S is of size n. It follows from the lemma that B_n gives a basis of F_n/F_{n-1}. An induction on n then shows that the disjoint union $B_0 \cup \cdots \cup B_n$ is a basis of F_n. The result is then obtained by letting $n \to \infty$. QED

COROLLARY. *If M is a Frobenius module the canonical map $i : M \to \tilde{\Lambda}M$ is injective. In particular, any Q-module can be embedded in a Q-ring.*

We end this section by showing that free Q-rings are bigraded. Recall that a grading $(M_n : n \in Z)$ on a Q-module M is a *dimension grading* if $q_i : M_n \to M_{2n+i}$.

DEFINITION 1. A *rank grading* $(R[n] : n \in Z)$ on a Q-ring is a grading such that $1 \in R[0]$, $R[m]R[n] \subseteq R[n+m]$, and $q_i : R[n] \to R[2n]$. An *exponent grading* $(M(n) : n \geq 0)$ on a Q-module is a non-negative grading such that $q_i : M(n) \to M(n+1)$.

Two gradings $(V[i\ ] : i \in I)$ and $(V_j : j \in J)$ on a vector space V are *compatible* if every homogeneous component for one is graded with respect to the other. Then the two gradings have a common double refinement $(V[i\ ]_j : (i,j) \in I \times J)$, so that

$$V[i\ ] = \bigoplus_{j \in J} V[i\ ]_j \quad \text{and} \quad V_j = \bigoplus_{i \in I} V[i\ ]_j.$$

EXAMPLES. The Q-ring $Z_2[\beta_*]$ of Proposition 4 §1 has compatible dimension and rank gradings with $\dim(\beta_i) = i$ and with $\text{rank}(\beta_i) = 1$. The Q-module $\mathcal{K}$ has an exponent grading $(\mathcal{K}(n) : n \geq 0)$.

If V is a graded vector space then the Q-module $\mathcal{K} \otimes V$ has compatible rank and dimension gradings; we have $\dim(q \otimes x) = 2^n \dim(x) + i$ and $\exp(q \otimes x) = n$ for $q \in \mathcal{K}(n)_i$ and homogeneous x.

PROPOSITION 3. *If a Q-module M has compatible exponent and dimension gradings then its enveloping algebra $\tilde{\Lambda}M$ has compatible rank and dimension gradings.*

PROOF. By construction $\tilde{\Lambda}M$ is the quotient of $S(M)$ by the ideal J generated by the elements $x^2 + q_0(x)$ where x runs through M. If $\dim(x) = n$ then $x^2 + q_0(x)$ is homogeneous of dimension $2n$ since $\dim(q_0 x) = 2n + 0 = 2n$. If $x \in M$ is homogeneous of exponent n let us say that it is of *rank* 2^n. Then $x^2 + q_0(x)$ is homogeneous of rank 2^{n+1} since $\exp(q_0 x) = 1 + \exp(x)$. Thus the ring $\tilde{\Lambda}M = S(M)/J$ has two compatible gradings, one extending the dimension grading of M and the other extending its rank grading. It remains to prove that $\dim(q_i(x)) = 2\dim(x) + i$ and $\text{rank}(q_i(x)) = 2\dim(x)$ for homogeneous $x \in \tilde{\Lambda}M$. But this is true for homogeneous $x \in M$ and the general case follows from the Cartan formula. QED

Corollary. *The free Q-ring $Q\langle V\rangle$ generated by a graded vector space V has compatible rank and dimension gradings.*

Proof. The free Q-module on V is $\mathcal{K}\otimes V$. We saw above that it has compatible dimension and exponent gradings. The result then follows from the equality $Q\langle V\rangle = \tilde{\Lambda}(\mathcal{K}\otimes V)$. QED

Addendum to Section 3.

The results proved in this section are very close to results stated in section 2 of May [1976]. Our graded Q-modules correspond to the "allowable left modules" over the Dyer-Lashof algebra $\mathcal{R}$ used by May there.

The Q-ring $H_*(BO_*) = Z_2[\beta_*]$ is graded by dimension and rank as shown in the above example, and $H_m(BO_r)$ is the component with rank r and dimension m.

For any space X let $E_\infty(X)$ denote the free E_∞-space generated by X. From results in May [1976] (which extend the results in Dyer, Lashof [1962] for the case where X is a point) it follows that $H_*E_\infty(X) = Q\langle H_*X\rangle$, the free Q-ring generated by H_*X. Let $\Sigma_n X$ denote the space $E[n]\times_{\Sigma_n} X^n$, where $E[n]$ is a contractible space on which Σ_n acts freely. Then we have

$$E_\infty(X) = \sum_n E[n]\times_{\Sigma_n} X^n$$

and we have $H_*\Sigma_n X = Q\langle H_*X\rangle[n]$, the component of rank n. In particular, $H_*\Sigma_n = Q\langle x\rangle[n]$.

4. The extended Milnor coalgebra $\mathcal{A}$.

In order to discuss the Nishida relations in the next section we need to use the *extended Milnor Hopf algebra* $\mathcal{A} = Z_2[a_0^{-1}, a_0, a_1, \ldots]$. We also introduce the *positive bialgebra* $\mathcal{A}^+$ and show that $\mathcal{K}$ is anti-isomorphic to a subalgebra of the convolution algebra $[\mathcal{A}^+, Z_2]$. A detailed discussion relating coactions by $\mathcal{A}$ and by the standard Milnor Hopf algebra $\mathcal{S}_*$ can be found in appendix B.

In this section *Alg* denotes the category of commutative Z_2-algebras, *Mon* the category of monoids and *Grp* the category of groups. Most bialgebras (resp. Hopf algebras) will be defined by specifying the functors $Alg \to Mon$ (resp. $Alg \to Grp$) that they represent (see appendix A).

We say that a formal power series $f(x)$ with coefficients in a Z_2-algebra R is *additive* if $f(x+y) = f(x)+f(y)$; this happens iff $f(x)$ has the form $f(x) = \sum f_i x^{2^i}$. The set of all additive series in $xR[[x]]$ is a monoid under composition that we shall denote by $A^+(R)$. If an additive f has a composition inverse then the inverse is also additive; this happens iff f_0 has an inverse. The set of all such additive invertible series forms a group $A(R) \subseteq A^+(R)$. The functor A^+ is represented by the polynomial ring $\mathcal{A}^+ = Z_2[a_0, a_1, \ldots]$, with $a(x) = \sum_i a_i x^{2^i}$ as the generic element. The coproduct $\Delta : \mathcal{A}^+ \to \mathcal{A}^+ \otimes \mathcal{A}^+$ is given by

$$\Delta(a) = (a\otimes 1)\circ(1\otimes a).$$

In this way, $\mathcal{A}^+$ is a bialgebra with no antipode. The functor A is represented by $\mathcal{A} = Z_2[a_0^{\pm}, a_1, \ldots]$. It is a Hopf algebra that we call the *extended Milnor Hopf algebra*. The antipode $\chi : \mathcal{A} \to \mathcal{A}$ takes $a(x)$ to its composition inverse.

A right $\mathcal{A}$-comodule V comes equipped with a structure map $\psi : V \to V \otimes \mathcal{A}$ which we may refer to as an $\mathcal{A}$-*coaction* or as a *Milnor coaction*. A *ring coaction* is a Z_2-algebra R for which the coaction $\psi : R \to R \otimes \mathcal{A}$ is a ring homomorphism.

Suppose a coaction $\psi : V \to V \otimes \mathcal{A}$ actually lands in $V \otimes \mathcal{A}^+$ (so that no negative power of a_0 is involved). In this case we shall say that ψ is *positive*, so that a positive coaction is the same as a right $\mathcal{A}^+$-comodule.

Example. A Milnor ring coaction is always representing an action by the functor A. For example, for any $R \in Alg$ let $F(R)$ denote the set of all power series with coefficients in R. The functor F is represented by the algebra $Z_2[\beta_*] = Z_2[\beta_0, \beta_1, \dots]$ with generic element $\beta(x) = \sum \beta_i x^i$. There is an action on the right $F(R) \times A(R) \to F(R)$ given by $(g(x), f(x)) \mapsto g(f(x))$, and it determines a (positive) Milnor ring coaction on $Z_2[\beta_*]$ with $(\not\beta\ \ )(x) = \beta(a(x))$. More explicitly,

$$\sum_i \psi(\beta_i)\ x^i = \sum_i \beta_i\ a(x)^i.$$

Observe that this coaction is rank preserving, where $\operatorname{rank}(\beta_i) = 1$ for every $i \geq 0$. It follows that for each n, the homogeneous component of rank n of $Z_2[\beta_*]$ is a comodule over $\mathcal{A}$.

The monomials $a^R = a_0^{r_0} a_1^{r_1} \cdots$ with $R = (r_0, r_1, \dots)$ form a basis of $\mathcal{A}$ (notice that $r_0 \in Z$). Any coaction $\psi : V \to V \otimes \mathcal{A}$ has a formal expansion

$$\psi(y) = \sum_R \psi_R(y) \otimes a^R$$

for $y \in V$. This expansion determines natural operations ψ_R on Milnor comodules. Recall that any linear form $f \in [\mathcal{A}, Z_2]$ gives a natural operation $y \mapsto f \bullet y$ (see appendix A). This is the left action of the convolution algebra $[\mathcal{A}, Z_2]$ on $\mathcal{A}$-comodules. For any linear form $f \in [\mathcal{A}, Z_2]$ we shall denote by $\langle f, r \rangle$ its value at $r \in \mathcal{A}$ and reserve the notation $f(y)$ for $f \bullet y$. For each monomial $a^R \in \mathcal{A}$ let ψ_R denote the linear form $\mathcal{A} \to Z_2$ which picks out the coefficient of a^R. Then $\psi_R(y) = \psi_R \bullet y$.

For any Milnor coaction $\psi : V \to V \otimes \mathcal{A}$, the specialization $a(x) \mapsto v_t(x) = tx + x^2$ determines a total operation $Q_t^* : V \to V[t^\pm]$ taking values in Laurent polynomials with coefficients in V. The formal expansion

$$Q_t^*(y) = \sum_n q_n^*(y) t^n$$

for $y \in V$ determines a collection of linear operations $q_n^* : V \to V$, where n ranges over the *integers.*

Equivalently, if $v_t^\dagger : \mathcal{A} \to Z_2[t^\pm]$ is the ring homomorphism determined by the specialization $a(x) \mapsto v_t(x)$ then $Q_t^*(y) = v_t^\dagger \bullet y$, and the Laurent expansion $v_t^\dagger = \sum_n q_n^* t^n$ determines linear forms $q_n^* : \mathcal{A} \to Z_2$ with $q_n^*(y) = q_n^* \bullet y$ for $y \in V$.

Proposition 1. *A coaction $\psi : V \to V \otimes \mathcal{A}$ is positive iff $Q_t^* : V \to V[t^{\pm}]$ actually lands in $V[t]$. In this case the operations $(x, q_n) \mapsto q_n^*(x)$ define a right $\mathcal{K}$-module structure on V.*

Proof. It is obvious that Q_t^* lands in $V[t]$ when ψ is positive. Conversely, let us suppose that Q_t^* lands in $V[t]$. Recall the formula $Q_t^*(x) = v_t^\dagger \bullet x$ for $x \in V$ where $v_t^\dagger$ is the map $\mathcal{A}_* \to Z_2[t^{\pm}]$ representing the polynomial $v_t(x) = tx + x^2$. Let $W_n(x)$ be the Ore polynomial of exponent n used in §2. For any $y \in V$ let us put $Q^{*(n)}(y) = W_n^\dagger \bullet y$ where $W_n^\dagger : \mathcal{A} \to \mathcal{W}(n)[w_0^{-1}]$ is the map representing $W_n(x)$. Let us prove that $Q^{*(n)}$ actually lands in $V \otimes \mathcal{W}(n)$. Recall from lemma 2 §2 that $Z_2[w_0, \dots, w_{n-1}] \subseteq Z_2[u_1, \dots, u_n]$ where $W_n = V_n \circ \cdots \circ V_1$ and $V_i(x) = x(x + u_i)$. Let us put $R = Z_2[u_1^{\pm}, \dots, u_n^{\pm}]$ and for every $1 \leq i \leq n$ let $V_i^\dagger$ be the map $\mathcal{A}_* \to R$ representing the polynomial $V_i(x)$. We have

$$Q^{*(n)}(y) = W_n^\dagger \bullet y = (V_n \circ \cdots \circ V_1)^\dagger \bullet y = V_n^\dagger \bullet \cdots \bullet V_1^\dagger \bullet y = Q^*_{u_n} \circ \cdots \circ Q^*_{u_1}(y)$$

and this shows that $Q^{*(n)}(y)$ lands in $V[u_1, \dots, u_n]$. Observe now that the ring $Z_2[u_1, \dots, u_n]$ is an integral extension of $Z_2[w_0, \dots, w_{n-1}]$ since from §2 we have

$$Z_2[w_0, \dots, w_{n-1}] \subseteq Z_2[u_1, \dots, u_n] \subseteq Z_2[t_1, \dots, t_n]$$

where $W_n(t_i) = 0$ and $u_i = W_{i-1}(t_i)$. Hence

$$Z_2[w_0, \dots, w_{n-1}] = Z_2[w_0^{-1}, w_0, \dots, w_{n-1}] \cap Z_2[u_1, \dots, u_n]$$

since $Z_2[w_0, \dots, w_{n-1}]$ is integrally closed. Thus

$$V[w_0, \dots, w_{n-1}] = V[w_0^{-1}, w_0, \dots, w_{n-1}] \cap V[u_1, \dots, u_n]$$

and it follows that $Q^{*(n)}(y)$ lands in $V \otimes \mathcal{W}(n)$. It follows from this that $\psi(y)$ lands in $V \otimes \mathcal{A}$ since a monomial $a^R = a_0^{r_0} a_1^{r_1} \cdots$ with $R = (r_0, r_1, \dots, r_{n-1}, 0, \dots)$ belongs to $\mathcal{A}^+$ iff the monomial $W_n^\dagger(a^R) = w^R$ belongs to $\mathcal{W}(n)$. This finishes the proof of the first part. It remains to prove the last statement. If $h(x) = s(s+t)x + x^2$ then $h^\dagger \bullet y = \sum_n q_n^*(y))(s^2 + st)^n$. The polynomial $(h \circ v_t)(x) = x(x+t)(x+s)(x+s+t)$ is symmetric in s and t. Hence also $h^\dagger \bullet (v_t^\dagger \bullet y) = (h \circ v_t)^\dagger \bullet y$. Thus

$$h^\dagger \bullet (v_t^\dagger \bullet y) = h^\dagger \bullet \sum_n q_n^*(y) t^n = \sum_n (h^\dagger \bullet q_n^*(y)) t^n = \sum_n \sum_r q_r^*(q_n^*(y)) t^n (s^2 + st)^r$$

is symmetric in s and t. But this relation is formally the transpose of the Adem relations (Proposition 1 §1) between the q_n's. QED

From any coaction $\psi : V \to V \otimes \mathcal{A}$ we extract a grading $(V_n : n \in Z)$ by specialising the generic additive series $a(x)$ to ux. More precisely, the grading coaction $\gamma : V \to V \otimes Z_2[u^{\pm}]$ is obtained by putting $a_0 = u$ and $a_i = 0$ for $i > 0$ in the expansion of ψ (see appendix B).

The *graded dual* V' of a graded vector space V is the direct sum of the dual spaces $V'^n = [V_n, Z_2]$ for $n \in Z$. If we think of V as graded by dimension, then we shall say that $z \in V'^n$ is of *codimension n*. For any coaction $\psi : V \to V \otimes \mathcal{A}$ we shall denote by $q_n : V' \to V'$ the transpose of the operation q_n^*, and define $Q_t : V' \to V'[t^{\pm}]$ by $Q_t = \sum q_n t^n$. Then $q_n(z) = z \star q_n^*$ and $Q_t(z) = z \star v_t^\dagger$ for $z \in V'$ where $v_t(x) = tx + x^2$. If $\psi : V \to V \otimes \mathcal{A}$ is positive then Q_t involves only positive powers of t.

Corollary. *If $\psi : V \to V \otimes \mathcal{A}$ is a positive coaction then the operation $Q_t : V' \to V'[t]$ defines a left $\mathcal{K}$-module structure on V'.*

Proof. This is obtained by duality from the proposition above. It also follows directly by using the formula $Q_t(z) = z \star v_t^\dagger$. QED

Remark. The Q-modules that appear as the graded dual of some positive Milnor comodule are rather special: they are negatively graded in dimension since they are positively graded in codimension; also the formal power series $Q_t(z)$ is a polynomial of degree $\leq n$ for $z \in V'^n$ and $q_n(z) = z$.

The operations Q_t^* and Q_t on a Milnor comodule and its graded dual correspond to *Steenrod operations.* Precisely, the *total Steenrod square $Sq_t^* : V \to V[t]$* in a Milnor comodule V is given by $Sq_t^*(y) = S_t^\dagger \bullet y$ where S_t is the polynomial $x + tx^2$. There is an expansion $Sq_t(y) = \sum_{n\geq 0} Sq_*^n(y)t^n$ where $Sq_*^n : V \to V$ is homogeneous of degree $-n$. The *total Steenrod square $Sq_t : V' \to V'[t]$* on the graded dual V' is given by $Sq_t(z) = z \star S_t^\dagger$. There is an expansion $Sq_t(z) = \sum_{n\geq 0} Sq^n(z)t^n$ where $Sq^n : V' \to V'$ is homogeneous of degree n. The operations Sq_i^* and Sq_i are transpose to each other. We have $\langle Sq^i(z), y\rangle = \langle z, Sq_i^*(y)\rangle$ for every z in V' and every y in V.

Here are some formulas for translating between the operations q_n^* and Sq_*^n in a Milnor comodule V and similarly for the operations q_n and Sq^n in the graded dual V'. Recall that $Q_t^* : V \to V[t^\pm]$ is given by $Q_t^*(y) = v_t^\dagger \bullet y$ for $y \in V$ where v_t is the polynomial $tx + x^2$. Also, $Q_t : V' \to V'[t^\pm]$ is given by $Q_t(z) = z \star v_t$ for $z \in V'$. From the identity $tx + x^2 = t(x + t^{-1}x^2)$ it follows that for and $y \in V_n$ and $z \in V'^n$ we have

$$Q_t^*(y) = \sum Sq_r^*(y)t^{n-2r} \quad \text{and} \quad Q_t(z) = \sum Sq^r(z)t^{n-r}.$$

Combined with Proposition 1, these formulas show that a coaction is positive iff $Sq_r^* = 0$ on V_n when $2r > n$; equivalently, iff $Sq^r = 0$ on V'^n when $r > n$.

Every positive comodule has the structure of a left module over the convolution algebra $[\mathcal{A}^+, Z_2]$. The proposition above shows that every positive comodule has also a natural right $\mathcal{K}$-module structure. This indicates that the map $q_n \mapsto q_n^*$ gives an anti-homomorphism of algebras $j : \mathcal{K} \to [\mathcal{A}^+, Z_2]$. The first statement of the following proposition uses the duality $\mathcal{K}(n) \simeq \mathcal{W}'(n)$.

Proposition 2. *The restriction of j to $\mathcal{K}(n)$ is dual to the map $W_n^\dagger : \mathcal{A}^+ \to \mathcal{W}(n)$ for which $a(x) \mapsto W_n(x)$. The map j is injective, so that j gives an anti-isomorphism between $\mathcal{K}$ and a subalgebra of $[\mathcal{A}^+, Z_2]$.*

Proof. Let us prove the first statement. For each $n \geq 0$ the map $W_n^\dagger : \mathcal{A}^+ \to \mathcal{W}(n)$ represents the inclusion $D_n \subset A^+$, where D_n is the functor which associates to each $R \in Alg$ the set $D_n(R)$ of monic Ore polynomials of exponent n in $R[x]$. Consider the following squares:

$$\begin{tikzcd}
D_m \times D_n \arrow[r] \arrow[d, hook] & D_{m+n} \arrow[d, hook] \\
A^+ \times A^+ \arrow[r] & A^+
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathcal{W}(m) \otimes \mathcal{W}(n) \arrow[r, dash, "\Delta"] & \mathcal{W}(n+m) \\
\mathcal{A}^+ \otimes \mathcal{A}^+ \arrow[r, dash, "\Delta"] \arrow[u, "W_m^\dagger \otimes W_n^\dagger"] & \mathcal{A}^+. \arrow[u, "W_{n+m}^\dagger"']
\end{tikzcd}$$

The first one commutes since the horizontal arrows represent the composition of polynomials or power series. Hence also the second. Let $h_n : \mathcal{W}'(n) \to [\mathcal{A}^+, Z_2]$ denote the transpose of $W_n^\dagger$. Taking duals we obtain a commutative square

$$\begin{tikzcd}
\mathcal{W}'(m) \otimes \mathcal{W}'(n) \arrow[r, "\star"] \arrow[d, "h_m \otimes h_m"'] & \mathcal{W}'(n+m) \arrow[d, "h_{n+m}"] \\
{[\mathcal{A}^+, Z_2] \otimes [\mathcal{A}^+, Z_2]} \arrow[r, "\star"] & {[\mathcal{A}^+, Z_2].}
\end{tikzcd}$$

where $\star$ represents convolution. This shows that by collecting the maps h_n together we have an algebra map $h : \mathcal{W}' \to [\mathcal{A}^+, Z_2]$ (modulo the verification that h preserves the unit elements). Let us see that $j = hi$ where i is the anti-isomorphism $i : \mathcal{K} \simeq \mathcal{W}'$ described in Theorem 1 §2. For this it suffices to verify the equality $j(x) = hi(x)$ for elements $x \in \mathcal{K}(1)$, since $\mathcal{K}(1)$ generates $\mathcal{K}$ and the maps j and hi are (anti)-homomorphisms of algebras. We have $\sum_n h(\theta_n) w_0^n = W_1^\dagger$ since h is transpose to $W_1^\dagger$. According to Theorem 1 §2 we have $i(q_n) = \theta_n$ for every $n \geq 0$. But $W_1^\dagger = \sum_n q_n^* w_0^n$ since $W_1(x) = x^2 + w_0 x$. Hence $W_1^\dagger = \sum_n j(q_n) w_0^n$ since $j(q_n) = q_n^*$. Combining these equalities together we obtain that $h(i(q_n)) = j(q_n)$. This finishes the proof of the first statement. It remains to show that j is injective, or equivalently that h is injective. We shall use the basis (θ_K) of $\mathcal{W}'(n)$ dual to the monomial basis (w^K) (as discussed in §2). For every $K = (k_0, \dots, k_{n-1})$ and $i \geq 0$ let us put $K, i = (k_0, \dots, k_{n-1}, i, 0, \dots)$. A direct computation shows that

$$\langle h_n(\theta_K), w^R \rangle = \langle \theta_K, W_n^\dagger(w^R) \rangle = \begin{cases} 1 & \text{if } R = K, i \text{ for some } i \geq 0 \\ 0 & \text{otherwise .} \end{cases}$$

Thus

$$h_n(\theta_K) = \sum_i \psi_{K,i}.$$

But the family $(\psi_{K,1} : n \geq 0, K \in N^n)$ is linearly independent. Hence also the family $(h_n(\theta_K) : n \geq 0, K \in N^n)$. This proves that h transforms a basis of $\mathcal{W}'$ into a linearly independent family. QED

Addendum to Section 4.

The idea of expressing the theory of Steenrod operations in terms of comodules over a Hopf algebra was introduced in Milnor [1958]. The method is explained in the setting of generalized cohomology theories in Adams [1974], for instance.

The extended Milnor Hopf algebra is implicit in Wilson [1980] (in connection with unstable operations and the Hopf ring of Eilenberg-MacLane spaces) and in in Kuhn [1994] (in connection with "generic modular representations"). There is a discussion of an extended Landweber-Novikov Hopf algebra in Morava [1985].

A Milnor coaction is positive (in our sense) iff its graded dual is an *unstable* module over the Steenrod algebra; see Steenrod, Epstein [1962], for the background. The homology of any topological space X is equipped with a natural (positive) Milnor coaction $\psi : H_*X \to H_*X \otimes \mathcal{A}$ which by duality determines the Steenrod operations on cohomology.

The total Steenrod operation Sq_t is used to great effect in Milnor, Stasheff [1974].

The coaction on $H_*(BO_*) = Z_2[\beta_*]$ is determined by $(\not\beta\ \ )(x) = \beta(a(x))$ as in Example 1; see Adams [1974] or Switzer [1973], for instance. For each $n \geq 0$ the component of rank n in $Z_2[\beta_*]$ is a Milnor comodule isomorphic to $H_*(BO_n)$. For instance, $H_*(BO_1)$ is isomorphic to $Z_2\langle\beta_*\rangle$ and $H_*(BO_n)$ is isomorphic to the n^{th} symmetric power of $Z_2\langle\beta_*\rangle$.

There have been years of work on the Steenrod algebra, including surprising recent quantum-leaps. We have not tried to encompass that work here. Some recent guides to the literature are Miller [1986], Lannes [1995], Schwartz [1994], and Wood [1995].

5. The Nishida relations

We give a description of the theory of Nishida relations based on the concept of Q-module and that of commutation operator between an algebra and a coalgebra, or equivalently between a monad and a comonad. A key ingredient is the Q-ring structure on the extended Milnor Hopf algebra $\mathcal{A}$. We show that a coaction $V \to V \otimes \mathcal{A}$ can be extended uniquely to a ring coaction $Q\langle V\rangle \to Q\langle V\rangle \otimes \mathcal{A}$ satisfying the Nishida relations.

Definition 1. Suppose that (R, Q_t) is a Q-ring. A *Q-parameter* is an additive power series $f(x) \in R[[x]]$ such that $Q_t(f)(x(x+t)) = f(x)f(x+t)$. We shall sometimes say that f is a *parameter for Q_t*.

For any vector space V the vector space $(V \otimes R)[[t]]$ is a module over the ring $R[[t]]$. If the context is clear we shall denote by $f(t)g(t)$ the product between a power series $f(t)$ in $(V \otimes R)[[t]]$ and a power series $g(t)$ in $R[[t]]$.

Proposition 1. *Let $f(x)$ be a Q-parameter in a Q-ring R. If M is a Q-module then so is $M \otimes R$ with $Q'_t(x \otimes r) = Q_{f(t)}(x)Q_t(r)$ for $x \in M$ and $r \in R$.*

Proof. We shall show that $Q'_tQ'_s : M \otimes R \to M \otimes R[[s,t]]$ is symmetric in s and t. We have $Q'_tQ'_s(x \otimes r) = Q'_t(Q'_s(x))Q_t(Q_s(r))$ since $Q'_t(x \otimes r) = Q'_t(x)Q_t(r)$ for $x \in M$ and $r \in R$; hence it suffices to verify the symmetry of $Q'_t(Q'_s(x))$ for $x \in M$. From the relations $Q_t(f(s)) = Q_t(f)(Q_t(s)) = Q_t(f)(s(s+t)) = f(s)(f(s)+f(t))$ it follows that

$$\begin{aligned} Q'_tQ'_s(x) = Q'_tQ_{f(s)}(x) =& Q'_t\sum_i q_i(x)f(s)^i = \sum_i Q'_t(q_i(x))Q_t(f(s))^i \\ =& \sum_i Q_{f(t)}(q_i(x))[f(s)(f(s)+f(t))]^i. \end{aligned}$$

But this last expression can be obtained by replacing s by $f(s)$ and t by $f(t)$ in the expression $\sum_i Q_t(q_i(x))(s(s+t))^i = Q_tQ_s(x)$. Hence the symmetry of $Q'_tQ'_s(x)$ follows from the symmetry of $Q_tQ_s(x)$. QED

Sometimes we shall denote by Q^f the Q-structure Q'_t obtained from a Q-parameter f. We shall often use the following principle whose proof is immediate: if $\alpha : R \to S$ is a map of Q-rings and $g = \alpha(f)$ then $M \otimes \alpha : M \otimes R \to M \otimes S$ is a map of Q-modules, where $M \otimes R$ and $M \otimes S$ are respectively equipped with Q^f and Q^g.

Recall from section 1 that the Q-ring structure on $\mathcal{A}$ is determined by the identity $Q_t(a)(x(x+t)) = a(x)a(x+t)$; hence $a(x)$ is a Q-parameter. Thus, if (M, Q_t) is a Q-module then $(M \otimes \mathcal{A}, Q'_t)$ is a Q-module.

Definition 2. Let M have a Q-structure Q_t and a Milnor coaction $\psi : M \to M \otimes \mathcal{A}$; the *Nishida relations hold* for the pair (Q_t, ψ) if ψ is a Q-module map where $M \otimes \mathcal{A}$ is equipped with Q'_t.

We shall sometimes say that the Nishida relations *hold between* Q_t and ψ if they hold for the pair (Q_t, ψ).

Example. The ring $Z_2[\beta_*] = Z_2[\beta_0, \beta_1, \ldots]$ has a Q-structure determined by the identity $Q_t(\beta)(x(x+t)) = \beta(x)\beta(x+t)$ where $\beta(x) = \sum_i \beta_i x^i$. It has also a Milnor coaction $\psi : Z_2[\beta_*] \to Z_2[\beta_*] \otimes \mathcal{A}$ determined by the identity $\psi(\beta)(x) = \beta(a(x))$. Let us see that the Nishida relations hold. To prove that ψ is a map of Q-rings it suffices to show that $Q'_t(\beta')(x(x+t)) = \beta'(x)\beta'(x+t)$ where $\beta'(x) = \beta(a(x))$. We have

$$\begin{aligned} Q'_t(\beta')(x(x+t)) &= Q'_t(\beta \circ a)(x(x+t)) = Q'_t(\beta) \circ Q_t(a)(x(x+t)) \\ &= Q'_t(\beta)(a(x)a(x+t)) = Q_{a(t)}(\beta)(a(x)(a(x)+a(t))) \end{aligned}$$

But by substituting $t \mapsto a(t)$ and $x \mapsto a(x)$ in the relation $Q_t(\beta)(x(x+t)) = \beta(x)\beta(x+t)$ we obtain

$$Q_{a(t)}(\beta)(a(x)(a(x)+a(t))) = \beta(a(x))\beta(a(x)+a(t)) = \beta'(x)\beta'(x+t).$$

By combining these equalitites we obtain the result:

Proposition 2. *If the Nishida relations hold between Q_t and ψ then the following two conditions are satisfied:*

(i) *(M, Q_t) is a graded Q-module if M is given the grading from ψ*

(ii) $\sum_j q_i^*(q_j(x))s^i t^j = \sum_{r,k} q_k(q_r^*(x))t^k s^r (s+t)^{k+r}$.

Proof. Let us suppose that ψ is a Q-module map. To prove (i) consider the map $u^\dagger : \mathcal{A} \to Z_2[u^\pm]$ such that $a(x) \mapsto ux$. There is a Q-structure on $Z_2[u^\pm]$ such that $Q_t(u) = u^2$. For this structure ux is a Q-parameter and it follows that $u^\dagger$ is a map of Q-rings. Hence $M \otimes Z_2[u^\pm]$ has a Q-structure Q'_t and $M \otimes u^\dagger : M \otimes \mathcal{A} \to M \otimes Z_2[u^\pm]$ preserves Q'_t. It follows that the grading coaction $\gamma = (M \otimes u^\dagger)\psi : M \to M \otimes Z_2[u^\pm]$ is a Q-module map. Thus $\gamma(Q_t(x)) = Q'_t(\gamma(x))$ for every $x \in M$. If $x \in M_n$ then $\gamma(x) = xu^n$ and $Q'_t(\gamma(x)) = Q'_t(xu^n) = Q_{ut}(x)u^{2n}$. The equality $\gamma(Q_t(x)) = Q'_t(\gamma(x))$ becomes

$$\sum_i \gamma(q_i(x))t^i = \sum_i \gamma(q_i(x))(ut)^i u^{2n}.$$

Equating the coefficients of t^i we obtain $\gamma(q_i(x)) = q_i(x)u^{2n+i}$, hence $q_i(x) \in M_{2n+i}$. This proves that M is a graded Q-module. Let us prove condition (ii). Let $v_s^\dagger$ be the map $\mathcal{A} \to Z_2[s^\pm]$ such that $a(x) \mapsto v_s(x) = sx + x^2$. There is a Q-structure on $Z_2[s^\pm]$ such that $Q_t(s) = s(s+t)$. For this structure $v_s(x) = x(x+s)$ is a Q-parameter and it follows that $v_s^\dagger : \mathcal{A} \to Z_2[s^\pm]$ is a map of Q-rings. Hence the composite $Q_s^* = (M \otimes v_s^\dagger)\psi : M \to M \otimes Z_2[s^\pm]$ is a Q-module map. Thus $Q_s^* Q_t(x) = Q'_t Q_s^*(x)$. But we have

$$Q_s^* Q_t(x) = Q_s^* \sum_j q_j(x)t^j = \sum_j Q_s^*(q_j(x))t^j = \sum_j q_i^*(q_j(x))s^i t^j \quad \text{and}$$

$$\begin{aligned} Q'_t Q^*_s(x) &= Q'_t \sum_r q^*_r(x) s^r = \sum_r Q'_t(q^*_r(x))(Q_t(s))^r \\ &= \sum_r Q_{v_s(t)}(q^*_r(x))(s(s+t))^r = \sum_{r,k} q_k(q^*_r(x))(t(t+s))^k(s(s+t))^r \\ &= \sum_{r,k} q_k(q^*_r(x)) t^k s^r (s+t)^{k+r}. \end{aligned}$$

QED

Later (in Proposition 8) we shall prove a converse to this proposition.

Remark. If we select the coefficient of $s^i t^j$ on each side of the equation $Q^*_s Q_t(x) = Q'_t Q^*_s(x)$ then we obtain the following relation (*):

$$q^*_i q_j(x) = \begin{cases} \sum_{k=0}^{j} \binom{\alpha}{j-k} q_k q^*_{\alpha-k}(x) & \text{if } i+j = 2\alpha \text{ is even} \\ 0 & \text{if } i+j \text{ is odd} \end{cases}$$

This is completely equivalent to the classical Nishida relations; see the addendum to this section.

There is a more general form of the Nishida relations which involves iterates of q_i's. We first compute the iterated total square ${Q'}^{(n)} : M \otimes R \to M \otimes R[[t_1, \dots, t_n]]$ of the Q-structure Q'_t on $M \otimes R$, when $f(x)$ is a Q-parameter in a Q-ring R. Let us denote by F the endomorphism of $R[[t_1, \dots, t_n]]$ that is obtained from the substitution $t_i \mapsto f(t_i)$. The endomorphism F commutes with the action of $GL(n)$ since f is additive. Hence F induces an endomorphism of $R[[w_0, \dots, w_{n-1}]]$, the subring of Dickson invariants. The image by F of the generic Ore polynomial $W_n(x)$ is given by

$$F(W_n)(x) = x^{2^n} + \sum_{i=0}^{n-1} F(w_i) x^{2^i} = \prod_{v \in \langle t_1, \dots, t_n \rangle} x + f(v) \quad .$$

For $x \in M$, let us put

$$Q_F^{(n)}(x) = \sum_{l(K)=n} q_K(x) F(w)^K$$

where $F(w)^K$ denotes $F(w^K)$.

Lemma 1. *We have* ${Q'}^{(n)}(xr) = Q_F^{(n)}(x) Q^{(n)}(r)$ *for* $x \in M$ *and* $r \in R$.

Proof. From the formula $Q'_t(xr) = Q'_t(x) Q_t(r)$ it follows by induction on n that ${Q'}^{(n)}(xr) = {Q'}^{(n)}(x) Q^{(n)}(r)$. Hence it suffices to prove that ${Q'}^{(n)}(x) = Q_F^{(n)}(x)$ for $x \in M$. Let $M \otimes F$ denote the endomorphism of $M \otimes R[[t_1, \dots, t_n]]$ that is obtained from the substitution $t_i \mapsto f(t_i)$ and let F_M denote its composite with the inclusion $\imath : M[[t_1, \dots, t_n]] \hookrightarrow M \otimes R[[t_1, \dots, t_n]]$. By definition we have $Q_F^{(n)} = F_M \circ Q^{(n)}$ where $Q^{(n)}$ is the n-fold iteration of Q_t on M. We shall prove by induction on n that ${Q'}^{(n)}(x) = F_M \circ Q^{(n)}(x)$ for every $x \in M$. This is clear for

$n = 0$ (and for $n = 1$). If $n > 0$ then consider the diagram

$$\begin{tikzcd}
M \arrow[r, "Q^{(n-1)}"] \arrow[d, "\imath"'] & M[[t_1, \dots, t_{n-1}]] \arrow[r, "Q_{t_n}"] \arrow[d, "F_M"'] & M[[t_1, \dots, t_n]] \arrow[d, "F_M"] \\
M \otimes R \arrow[r, "Q'^{(n-1)}"] & M \otimes R[[t_1, \dots, t_{n-1}]] \arrow[r, "Q'_{t_n}"] & M \otimes R[[t_1, \dots, t_n]].
\end{tikzcd}$$

The composite of the top (resp. bottom) horizontal arrows is $Q^{(n)}$ (resp. $Q'^{(n)}$). Let us suppose as induction hypothesis that the left hand square commutes. The result will be proved if we show that the right hand square commutes. It suffices to verify the commutativity for $x \in M$, and for $x = t_i$ for every $i < n$. But if $x \in M$ then we have

$$Q'_{t_n}(F_M(x)) = Q'_{t_n}(x) = Q_{f(t_n)}(x) = F_M(Q_{t_n}(x)).$$

If $x = t_i$ and $i < n$ then we have

$$Q'_{t_n}(F_M t_i) = Q'_{t_n}(f(t_i)) = Q_{t_n}(f)(t_i(t_i + t_n)) = f(t_i)(f(t_i) + f(t_n)).$$

But this equals $F_M(Q_{t_n}(t_i))$ since $Q_{t_n}(t_i) = Q'_{t_n}(t_i) = t_i(t_i + t_n)$. QED

In the case where $R = \mathcal{A}$ and $f = a$ we obtain an endomorphism $F = A$ of the algebra $\mathcal{A}[[w_0, \dots, w_{n-1}]]$. Observe that $M \otimes \mathcal{A}[[w_0, \dots, w_{n-1}]]$ is a module over the ring $\mathcal{A}[[w_0, \dots, w_{n-1}]]$.

Proposition 3. *If the Nishida relations hold between Q_t and ψ then for each $n \geq 0$ and $x \in M$ we have an equality of generating series*

$$\sum_{l(K)=n} \sum_R \psi_R(q_K(x))\ a^R\ w^K = \sum_{l(K)=n} \sum_R q_K(\psi_R(x))\ Q^{(n)}(a)^R\ A(w)^K$$

where $A(w)^K$ denotes $A(w^K)$ and $Q^{(n)}(a)^R$ denotes $Q^{(n)}(a^R)$.

Proof. By hypothesis, $\psi : M \to M \otimes \mathcal{A}$ is a map of Q-modules. Hence $\psi(Q^{(n)}(x)) = Q'^{(n)}(\psi(x))$ for every $n \geq 0$ and every $x \in M$. But we have

$$\psi(Q^{(n)}(x)) = \sum_{l(K)=n} \psi(q_K(x))\ w^K = \sum_{l(K)=n} \sum_R \psi_R(q_K(x))\ a^R\ w^K$$

and the lemma shows that

$$\begin{aligned} Q'^{(n)}(\psi(x)) =& Q'^{(n)} \sum_R \psi_R(x)\ a^R = \sum_R Q_A^{(n)}(\psi_R(x))\ Q^{(n)}(a^R) \\ =& \sum_{l(K)=n} \sum_R q_K(\psi_R(x))\ A(w)^K\ Q^{(n)}(a)^R. \end{aligned}$$

QED

For any Z_2-vector space V the vector spaces $\mathcal{K} \otimes (V \otimes \mathcal{A})$ and $(\mathcal{K} \otimes V) \otimes \mathcal{A}$ are canonically isomorphic, but they support different Q-structures. The first is the free Q-module on $(V \otimes \mathcal{A})$ and the second has the Q-structure Q'_t. There is a unique Q-module map

$$\rho_V : \mathcal{K} \otimes (V \otimes \mathcal{A}) \to (\mathcal{K} \otimes V) \otimes \mathcal{A}$$

such that $\rho_V(1 \otimes x \otimes r) = 1 \otimes x \otimes r$, since the domain is free. This yields a natural transformation

$$\rho : KA \to AK$$

where K and A are the functors $K, A : Vect \to Vect$ given respectively by $K(V) = \mathcal{K} \otimes V$ and $A(V) = V \otimes \mathcal{A}$. We shall say that ρ is the *Nishida commutation operator*. The basic theory of commutation operators is given in appendix C.

Proposition 4. *For each $n \geq 0$, $x \in V$ and $r \in \mathcal{A}$ there is an equality of generating series*

$$\sum_{l(K)=n} \rho_V(q_K \otimes x \otimes r)\ w^K = \sum_{l(K)=n} q_K \otimes x \otimes Q^{(n)}(r)\ A(w)^K.$$

In particular, the Nishida operator ρ_V is preserving the decomposition $\mathcal{K} \otimes V \otimes \mathcal{A} = \bigoplus_n \mathcal{K}(n) \otimes V \otimes \mathcal{A}$.

Proof. The left hand side of this equality is an expansion of $\rho_V Q^{(n)}(1 \otimes x \otimes r)$. But $\rho_V Q^{(n)} = {Q'}^{(n)} \rho_V$ since ρ_V is a Q-module map. Moreover, ${Q'}^{(n)} \rho_V(1 \otimes x \otimes r) = {Q'}^{(n)}(1 \otimes x \otimes r) = Q_A^{(n)}(1 \otimes x) Q^{(n)}(r)$ by lemma 1. If we expand the last term of this equality we obtain the equality of generating series. The last statement is obvious from this equality. QED

The endofunctor K has a monad structure $m : KK \to K$, $u : I \to K$ obtained from the algebra structure on $\mathcal{K}$. An action $q : K(V) \to V$ by this monad is equivalent to a left $\mathcal{K}$-module structure on V, which is precisely a Q-module structure on V. Similarly, the functor A has a comonad structure $\Delta : A \to AA$, $\epsilon : A \to I$ obtained from the coalgebra structure on $\mathcal{A}$. A coaction $\psi : V \to A(V)$ by this comonad is equivalent to a right $\mathcal{A}$-comodule structure on V.

Theorem 1. *The Nishida operator $\rho : KA \to AK$ respects the monad structure of K and the comonad structure of A. The Nishida relations hold for an action $q : K(M) \to M$ and a coaction and $\psi : M \to A(M)$ iff the pair (q, ψ) is ρ-commuting.*

Remark. The theorem could be formulated in terms of a commutation operator between an algebra and a coalgebra rather than between a monad and a comonad. For this we need to use the operator

$$\tilde{\rho} : \mathcal{K} \otimes \mathcal{A} \to \mathcal{A} \otimes \mathcal{K}$$

obtained by postcomposing $\rho_{Z_2} : \mathcal{K} \otimes \mathcal{A} \to \mathcal{K} \otimes \mathcal{A}$ with the symmetry isomorphism $\mathcal{K} \otimes \mathcal{A} \simeq \mathcal{A} \otimes \mathcal{K}$. Note that the theorem would then say that $\tilde{\rho}$ is respecting the *opposite coalgebra structure* (Δ^o, ϵ) of $\mathcal{A}$ (and the algebra structure of $\mathcal{K}$). We have chosen the monadic formulation only for expository reasons. See the remark after Proposition 5 Appendix C.

Proof. Let us first see that for any action $q : K(V) \to V$ the composite

$$KA(V) \xrightarrow{\rho_V} AK(V) \xrightarrow{A(q)} A(V)$$

is the action $q' : KA(V) \to A(V)$ defining the Q-structure Q'_t on $A(V)$. In the usual notation this composite is

$$\mathcal{K} \otimes (V \otimes \mathcal{A}) \xrightarrow{\rho_V} (\mathcal{K} \otimes V) \otimes \mathcal{A} \xrightarrow{q \otimes \mathcal{A}} V \otimes \mathcal{A}.$$

But ρ_V and $q \otimes \mathcal{A}$ are Q-module maps; hence so is their composite $(q \otimes \mathcal{A})\rho_V$. Moreover, $(q \otimes \mathcal{A})\rho_V(1 \otimes x \otimes r) = (q \otimes \mathcal{A})(1 \otimes x \otimes r) = x \otimes r$. This proves that $(q \otimes \mathcal{A})\rho_V = q'$. Applying Proposition 2 of appendix C, we see that ρ commutes with the monad structure of K. Let us prove that ρ respects the comonad structure of A. For this we need the following lemma.

Lemma 2. *If $f(x)$ and $g(x)$ are Q-parameters in Q-rings R and S, respectively, then so is $f \circ g$ in $R \otimes S$ for $Q'_t = Q^g$. Moreover, for any Q-module M we have $Q^{f \circ g} = (Q^f)^g$ in $M \otimes R \otimes S$.*

Proof. From the relation $Q_t(f)(s(s+t)) = f(s)f(s+t)$ it follows by substituting $t \mapsto g(t)$ and $s \mapsto g(s)$ that $Q_{g(t)}(f)(g(s)(g(s)+g(t))) = f(g(s))f(g(s)+g(t))$. Hence

$$\begin{aligned} Q'_t(f \circ g)(s(s+t)) &= Q_{g(t)}(f) \circ Q_t(g)(s(s+t)) = Q_{g(t)}(f)(g(s)(g(s)+g(t)) \\ &= f(g(s))f(g(s+t)) \end{aligned}$$

and the first statement is proved. For the second statement we have

$$\begin{aligned} (Q^f)^g(x \otimes r \otimes s) &= (Q^f)_{g(t)}(x \otimes r)Q_t(s) = Q_{f(g(t))}(x)Q_{g(t)}(r)Q_t(s) \\ &= Q_{f \circ g(t)}(x)Q'_t(r \otimes s) = Q^{f \circ g}(x \otimes r \otimes s) \end{aligned}$$

for any $x \in M$, $r \in R$ and $s \in S$. QED

We can now continue the proof of Theorem 1. If we apply Proposition 3 of appendix C we see that it is enough to prove that the maps $V \otimes \Delta : V \otimes \mathcal{A} \to V \otimes \mathcal{A} \otimes \mathcal{A}$ and $M \otimes \epsilon : V \otimes \mathcal{A} \to V$ are Q-module maps for any Q-module V. Here $(V \otimes \mathcal{A}) \otimes \mathcal{A}$ has the Q-structure Q''_t obtained by successive applications of Proposition 1. By definition $Q''_t = (Q^f)^g$, where $f(t)$ and $g(t)$ are respectively denoting the power series $(a \otimes 1)(t)$ and $(1 \otimes a)(t)$. We have $\Delta(a) = f \circ g$ and the lemma shows that $\Delta(a)$ is a change of parameter for the Q-structure Q'_t on $\mathcal{A} \otimes \mathcal{A}$. It follows that Δ is a map of Q-rings if $\mathcal{A} \otimes \mathcal{A}$ has the Q-structure Q'_t. Hence $M \otimes \Delta$ is a Q-module map if $(V \otimes \mathcal{A}) \otimes \mathcal{A}$ has the Q-structure $Q^{\Delta(a)}$. But the lemma shows that $Q^{\Delta(a)} = (Q^f)^g = Q''_t$, and this shows $M \otimes \Delta$ is a Q-module map if $(V \otimes \mathcal{A}) \otimes \mathcal{A}$ has the Q-structure Q''_t. The proof that $V \otimes \epsilon : V \otimes \mathcal{A} \to V$ is a Q-module map is immediate. Let us prove the last statement. Let $q : K(V) \to V$ be an action and $\psi : V \to A(V)$ a coaction. According to Proposition 4 appendix C the pair (q, ψ) is ρ-commuting iff ψ is a $\mathcal{K}$-module map. QED

Corollary. *The unique Q-module map $\psi' : \mathcal{K} \otimes V \to (\mathcal{K} \otimes V) \otimes \mathcal{A}$ extending a coaction $\psi : V \to V \otimes \mathcal{A}$ is a coaction. If V is a Q-module with structure map $q : \mathcal{K} \otimes V \to V$ then the Nishida relations hold between q and ψ iff q is a comodule map, where $\mathcal{K} \otimes V$ has the coaction ψ'.*

Proof. The map ψ' is equal to the composite

$$\mathcal{K}\otimes V \xrightarrow{\mathcal{K}\otimes\psi} \mathcal{K}\otimes(V\otimes\mathcal{A}) \xrightarrow{\rho_V} (\mathcal{K}\otimes V)\otimes\mathcal{A}$$

since this composite is a Q-module map extending ψ. The Theorem shows that ρ respects the comonad structure of A. Hence by the dual of Proposition 2 appendix C the map ψ' is a coaction. Let us prove the last statement. According to the Theorem 1 the Nishida relations hold for (q,ψ') iff the pair (q,ψ') is ρ-commuting. The result then follows from Proposition 4 appendix C. QED

Definition 3. The *natural extension* $\psi' : \mathcal{K}\otimes V \to (\mathcal{K}\otimes V)\otimes\mathcal{A}$ of a coaction $\psi : V \to V\otimes\mathcal{A}$ is the unique Q-module map extending ψ.

Let us calculate the grading that is obtained from the coaction ψ' on $\mathcal{K}\otimes V$. Observe first that the inclusion $V\subset\mathcal{K}\otimes V$ is homogeneous of degree 0 since ψ' extends ψ. Hence $\dim(1\otimes x) = \dim(x)$ for any homogeneous $x\in V$. Observe also that the Nishida relations hold since ψ' is a Q-module map. Hence, according to Proposition 2, $\mathcal{K}\otimes V$ is a graded Q-module with the grading induced from ψ'. This shows in particular that $\dim(q_n\otimes x) = 2\dim(1\otimes x)+n = 2\dim(x)+n$ for any homogeneous $x\in V$. More information about ψ' is contained in the following proposition.

Proposition 5. *Let $\psi' : \mathcal{K}\otimes V \to (\mathcal{K}\otimes V)\otimes\mathcal{A}$ be the natural extension of a coaction. Then for every $n\geq 0$ and $x\in V$ we have an equality of generating series*

$$\sum_{l(K)=n} \psi'(q_K\otimes x)\ w^K = \sum_i \sum_{l(K)=n} q_K\otimes x_i\otimes Q^{(n)}(r_i)\ A(w)^K$$

where $\psi(x) = \sum_i x_i\otimes r_i$. In particular, ψ' preserves the decomposition $\mathcal{K}\otimes V = \bigoplus_n \mathcal{K}(n)\otimes V$, and ψ' is positive when ψ is.

Proof. If $x\in V$ and $\psi(x) = \sum_i x_i\otimes r_i$ then

$$\sum_{l(K)=n} \psi'(q_K\otimes x)\ w^K = \sum_{l(K)=n} \rho_V(q_K\otimes x_i\otimes r_i)\ w^K$$

since $\psi' = \rho_V(\mathcal{K}\otimes\psi)$. The formula then follows from Proposition 4. The second statement is clear from the formula. If ψ is positive then $\psi(x) = \sum_i x_i\otimes r_i$ where $r_i\in\mathcal{A}^+$. But then $Q^{(n)}(r_i)\in\mathcal{A}^+$ since $\mathcal{A}^+$ is a sub-Q-ring of $\mathcal{A}$. The formula then shows that ψ' is positive. QED

The natural extension of the trivial coaction on Z_2 is the unique Q-module map $\psi' : \mathcal{K}\to\mathcal{K}\otimes\mathcal{A}$ such that $\psi'(1) = 1$. We shall say that this is the *natural coaction* on $\mathcal{K}$ and denote it by ψ.

Corollary. *The natural coaction $\psi : \mathcal{K}\to\mathcal{K}\otimes\mathcal{A}$ is positive and preserves the decomposition $\mathcal{K} = \oplus_n\mathcal{K}(n)$. For each $n\geq 0$ we have an equality of generating series*

$$\sum_{l(K)=n} \psi(q_K)w^K = \sum_{l(K)=n} q_K A(w)^K.$$

Proof. It suffices to specialise the formula of the proposition in the case where $x = 1$ and $\psi(1) = 1 \otimes 1$. QED

It follows from this corollary that each natural coaction $\psi : \mathcal{K}(n) \to \mathcal{K}(n) \otimes \mathcal{A}$ is positive. By the corollary to Proposition 1 §4 there is a corresponding Q-structure on the graded dual $\mathcal{K}'(n) = \mathcal{W}(n)$.

Proposition 6. *The Q-structure on $\mathcal{W}(n)$ is a Q-ring structure. It is determined by the identity $Q_t(W_n)(x(x+t)) = W_n(x)W_n(x+t)$ where $W_n(x)$ is the generic Ore polynomial. $\mathcal{W}(n)$ is a graded Q-ring with codim$(w_i) = 2^n - 2^i$.*

Proof. The family of elements $(q_K : l(K) = n)$ forms a basis of $\mathcal{K}(n)$ which is dual to the monomial basis $(w^K : l(K) = n)$ of $\mathcal{W}(n)$. By definition, the operation Q_t on $\mathcal{W}(n)$ is obtained by transposing the operation Q_t^* on $\mathcal{K}(n)$. Hence

$$\sum_{l(K)=n} q_K Q_t(w^K) = \sum_{l(K)=n} Q_t^*(q_K) w^K.$$

By definition, Q_t^* is obtained by specialising ψ with $a(x) \mapsto xt + x^2$. This means that we have

$$\sum_{l(K)=n} Q_t^*(q_K) w^K = \sum_{l(K)=n} q_K A(w)^K$$

where the endomorphism A is defined by $a(x) = xt + x^2$. Combining these equalities, we have that $Q_t(w^R) = A(w)^R$ for every R and this proves that $Q_t = A$ if $a(x) = xt + x^2$. By definition of the endomorphism A we have

$$\begin{aligned} A(W_n)(x(x+t)) &= \prod_{v \in \langle t_1, \dots, t_n \rangle} x(x+t) + a(v) = \prod_{v \in \langle t_1, \dots, t_n \rangle} x(x+t) + v(v+t) \\ &= \prod_{v \in \langle t_1, \dots, t_n \rangle} (x+v)(x+v+t) = W_n(x)W_n(x+t). \end{aligned}$$

In particular $q_0(W_n) = Q_0(W_n) = W_n^2$, and it follows that q_0 is the Frobenius endomorphism of $\mathcal{W}(n)$. This finishes the proof that $\mathcal{W}(n)$ is a Q-ring. The grading on $\mathcal{W}(n)$ is exactly dual to the dimension grading of $\mathcal{K}(n)$. QED

Let Vect^K denote the category of Q-modules and let Vect^A denote the category of Milnor comodules. We shall denote by Vect^{KA} the category of vector spaces equipped with a pair (Q_t, ψ) for which the Nishida relations hold.

Proposition 7.

(i) *The functor $M \mapsto M \otimes \mathcal{A}$ is right adjoint to the forgetful functor Vect$^{KA} \to$ Vect^K, where $M \otimes \mathcal{A}$ has the Q-structure Q_t'.*

(ii) *The functor $V \mapsto \mathcal{K} \otimes V$ is left adjoint to the forgetful functor Vect$^{KA} \to$ Vect^A, where $\mathcal{K} \otimes V$ has Milnor coaction ψ'.*

Proof. This follows directly from Proposition 5 of appendix C. QED

We shall now prove a converse to Proposition 2. We need the following result.

Lemma 3. *Let $f : U \to V$ be a linear map homogeneous of degree* 0 *between two $\mathcal{A}$-comodules. Then f is a comodule map iff f commutes with Q_t^*.*

Proof. The implication $\Rightarrow$ is trivial. Let us suppose that $f \circ q_n^* = q_n^* \circ f$ for every $n \in Z$. It follows from the discussion above Proposition 2 §4 that $f(Sq_*^n(x)) = Sq_*^n(f(x))$ for every $n \geq 0$ and $x \in U$. Hence f is a map of $\mathcal{S}_*$-comodules, since it is a classical result that the Sq_*^n's generate; see Milnor [1958], for instance. Thus f is a map of $\mathcal{A}$-comodules by Proposition 2, appendix B. QED

Proposition 8. *If conditions (i) and (ii) of Proposition 2 are satisfied for (M, Q_t, ψ) then the Nishida relations hold.*

Proof. We must show that $\psi : M \to M \otimes \mathcal{A}$ is a Q-module map. We shall use the fact that the following diagram commutes

$$\begin{tikzcd}
\mathcal{K} \otimes M \arrow[r, "\psi'"] \arrow[d, "\mathcal{K} \otimes \psi"'] \arrow[dr, phantom, "\rho_M"] & (\mathcal{K} \otimes M) \otimes \mathcal{A} \arrow[d, "q \otimes \mathcal{A}"] \\
\mathcal{K} \otimes (M \otimes \mathcal{A}) \arrow[r, "q'"'] & M \otimes \mathcal{A}
\end{tikzcd}$$

where q is the structure map of the Q-module M, q' is the structure map of $\mathcal{K} \otimes M$ equipped with Q_t' and ψ' is the natural extension of ψ (the commutativity is clear from the proofs of Theorem 1 and its corollary; see also Proposition 4 appendix C). Let us now suppose that conditions (i) and (ii) are satisfied for (M, Q_t, ψ). According to Proposition 5, the map ψ' induces a coaction $\psi'(1)$ on $\mathcal{K}(1) \otimes M$. We shall begin by proving that the restriction $q(1)$ of q to $\mathcal{K}(1) \otimes M$ is a comodule map. For this we shall use the lemma above with $f = q(1)$. Let us first see that f is homogeneous of degree 0. We saw above Proposition 5 that $\dim(q_n \otimes x) = 2\dim(x) + n$ for homogeneous $x \in M$. But $\dim(q_n(x)) = 2\dim(x) + n$ by condition (i). Thus f is homogeneous of degree 0 since $f(q_n \otimes x) = q_n(x)$. It remains to verify that f preserves the operation Q_t^*. We shall show that $f({Q'}_s^*(y)) = Q_s^*(f(y))$ for every $y = q_n \otimes x \in \mathcal{K}(1) \otimes M$. If we specialise the formula of Proposition 5 with $n = 1$ and $a(x) \mapsto v_s(x) = x(x+s)$ we obtain that

$$\sum_n {Q'}_s^*(q_n \otimes x) t^n = \sum_i \sum_n q_n \otimes q_i^*(x)(s^2 + st)^i (t^2 + st)^n$$

for every $x \in M$ since $Q_s^*(x) = \sum_i q_i^*(x) s^i$ and $Q_t(s) = s^2 + st$. Hence

$$\begin{aligned}\sum_n f({Q'}_s^*(q_n \otimes x)) t^n &= \sum_i \sum_n f(q_n \otimes q_i^*(x))(s^2 + st)^i (t^2 + st)^n \\ &= \sum_i \sum_n q_n(q_i^*(x))(s^2 + st)^i (t^2 + st)^n\end{aligned}$$

for every $x \in M$. On the other hand

$$\sum_n Q_s^*(f(q_n \otimes x)) t^n = \sum_n Q_s^*(q_n(x)) t^n$$

and this shows that the equality $f(Q'^*_s(q_n \otimes x)) = Q^*_s(f(q_n \otimes x))$ follows from condition (ii). We have proved that $q(1)$ is a comodule map. From the observation made at the beginning of the proof, the diagram

$$\begin{tikzcd}
\mathcal{K}(1) \otimes M \arrow[r, "\psi'(1)"] \arrow[d, "\mathcal{K}(1) \otimes \psi"'] \arrow[dr, phantom, "\rho_M(1)"] & (\mathcal{K}(1) \otimes M) \otimes \mathcal{A} \arrow[d, "q(1) \otimes \mathcal{A}"] \\
\mathcal{K}(1) \otimes (M \otimes \mathcal{A}) \arrow[r, "q'(1)"'] & M \otimes \mathcal{A}
\end{tikzcd}$$

commutes, where $q'(1)$ denotes the restriction of q' and $\rho_M(1)$ denotes the restriction of $\rho_M(1)$ (which exists by Proposition 4). Hence if one of the following two squares commutes then so does the other:

$$\begin{tikzcd}
\mathcal{K}(1) \otimes M \arrow[r, "\mathcal{K}(1) \otimes \psi"] \arrow[d, "q(1)"'] & \mathcal{K}(1) \otimes (M \otimes \mathcal{A}) \arrow[d, "q'(1)"] & \mathcal{K}(1) \otimes M \arrow[r, "\psi'(1)"] \arrow[d, "q(1)"'] & (\mathcal{K}(1) \otimes M) \otimes \mathcal{A} \arrow[d, "q(1) \otimes \mathcal{A}"] \\
M \arrow[r, "\psi"'] & M \otimes \mathcal{A} & M \arrow[r, "\psi"'] & M \otimes \mathcal{A}.
\end{tikzcd}$$

But the second square commutes since we have shown that $q(1)$ is a comodule map. Hence also the first. But this means that ψ is a Q-module map since $\mathcal{K}(1)$ generates $\mathcal{K}$. QED

Proposition 9. *If M and N are Q-modules with Milnor coactions for which the Nishida relations hold then so is $M \otimes N$.*

Proof. According to Proposition 8, it suffices to show that the conditions (i) and (ii) of Proposition 2 are satisfied. This is clear for (i) since the grading on $M \otimes N$ is compatible with the Q-structure. For condition (ii) we need to verify that

$$Q^*_s Q_t(x \otimes y) = \sum_{r,k} q_k(q^*_r(x \otimes y))(t^2 + st)^k(s^2 + st)^r$$

for $x \otimes y \in M \otimes N$. But this follows directly from the Cartan formula for the q_k's and the q^*_j's. QED

We end this section with a few propositions about extending Milnor coactions from modules to rings so as to satisfy the Nishida relations.

If M is a Frobenius module (see §2 for this concept) then so is $M \otimes \mathcal{A}$ with $q_0(x \otimes r) = q_0(x) \otimes r^2$. We shall say that a coaction $\psi : M \to M \otimes \mathcal{A}$ *commutes* with a Frobenius endomorphism $q_0 : M \to M$ if the relation $\psi(q_0(x)) = q_0(\psi(x))$ holds. This is certainly the case when q_0 is obtained from a Q-structure Q_t and the Nishida relations hold. Recall that a Q-structure on M extends to a Q-ring structure on $\tilde{\Lambda}M$ (Proposition 1 §3).

Proposition 10. *If a coaction $\psi : M \to M \otimes \mathcal{A}$ commutes with a Frobenius endomorphism $q_0 : M \to M$ then it has a unique extension $\psi : \tilde{\Lambda}M \to \tilde{\Lambda}M \otimes \mathcal{A}$ as* *a ring coaction. Moreover, if q_0 is obtained from a Q-structure Q_t and the Nishida relations hold for (Q_t, ψ) then they also hold for their ring extension to $\tilde{\Lambda}M$.*

Proof. Let us suppose that ψ commutes with q_0. Then

$$\psi(q_0(x)) = q_0(\psi(x)) = \sum_R q_0(\psi_R(x)) \otimes a^{2R}$$

for any $x \in M$. Let $f : M \to \tilde{\Lambda}M \otimes \mathcal{A}$ be the composite $(i \otimes \mathcal{A})\psi$ where $i : M \to \tilde{\Lambda}M$ is the inclusion. Then $i(q_0(x)) = i(x)^2$ and it follows from the equality above that $f(q_0(x)) = f(x)^2$. Hence by the universal property of $\tilde{\Lambda}M$ there is a unique ring homomorphism $\overline{\psi} : \tilde{\Lambda}M \to \tilde{\Lambda}M \otimes \mathcal{A}$ extending f. The coassociativity of $\overline{\psi}$ follows from the coassociativity of ψ together with the fact that M generates $\tilde{\Lambda}M$ as a ring. For the counit the proof is similar. This finishes the proof of the first statement. Let us now suppose that q_0 is obtained from a Q-structure Q_t and that the Nishida relations hold for (Q_t, ψ). Then f is a Q-module map since ψ and i are. Hence $\overline{\psi}$ is a Q-ring map since $\tilde{\Lambda}M$ is freely generated by M as a Q-ring (Proposition 1 §3). This proves that the Nishida relations hold for $(\overline{Q}_t, \overline{\psi})$; where $\overline{Q}_t$ denotes the ring extension of Q_t to $\tilde{\Lambda}M$. QED

Corollary. *Let $Q\langle V\rangle$ be the Q-ring freely generated by a Milnor comodule (V, ψ). Then the coaction $\psi : V \to V \otimes \mathcal{A}$ has a unique extension $\psi' : Q\langle V\rangle \to V\langle M\rangle \otimes \mathcal{A}$ as ring coaction for which the Nishida relations hold.*

Proof. The uniqueness of ψ' is clear since $Q\langle V\rangle$ is free over V as a Q-ring and since ψ' is a map of Q-rings if it is a ring coaction satisfying the Nishida relations. To prove its existence it suffices to take for ψ' the Q-module map extending ψ. We then have to prove that ψ' is a coaction. This can be proved directly or can be seen by applying the proposition to the natural extension $\psi' : \mathcal{K} \otimes V \to \mathcal{K} \otimes V \otimes \mathcal{A}$ since $Q\langle V\rangle = \tilde{\Lambda}(\mathcal{K} \otimes V)$. QED

Addendum to Section 5.

Suppose that X is an E_∞-space. The *classical Nishida relations* describe how the operations Sq^*_i commute with the Dyer-Lashof operations. The relations are expressed as an equality

$$Sq^a_* Q^b(x) = \sum_c \binom{b-a}{a-2c} Q^{b+c-a} Sq^c_*(x)$$

where Q^b is the Dyer-Lashof operation; see Nishida [1968] or May [1971], for instance. Let us show that these are equivalent to the relation (*) in the remark following Proposition 2. By definition, $Q^b(x) = q_{b-n}(x)$ if $x \in H_n(X)$ and $b \geq n$, and $Q^b(x) = 0$ otherwise. Recall that if $x \in H_n(X)$ then we have $Sq^c_*(x) = q^*_{n-2c}(x)$ and $q^*_i(x) = 0$ unless $i + n$ is even. Supposing that $x \in H_n(X)$ we have $Sq^a_* Q^b(x) = q^*_i q_j(x)$ where $i = b + n - 2a$ and $j = b - n$. The relation (*) then gives $Sq^a_* Q^b(x) = \sum_k \binom{b-a}{b-n-k} q_k q^*_{b-a-k}(x)$. Half of the terms in the sum are null since $q^*_{b-a-k}(x) = 0$ when $b - a - k + n$ is odd. If we write $k = b + 2c - a - n$ then we have $q_k q^*_{b-a-k}(x) = Q^{b+c-a} Sq^c_*(x)$ and $b - n - k = a - 2c$. This proves the claim. It follows that the classical Nishida relations are equivalent to condition (ii) of Proposition 2. Hence, by Proposition 8, our Nishida relations hold for H_*X.

In a sequel to this paper, we will use cobordism theory to give a direct geometric proof that our Nishida relations hold for the homology of an E_∞-space.

6. Q-coalgebras.

In this section we study some natural coalgebra structures on Q-modules and rings.

Definition 1. A *Q-coalgebra* is a Q-module with coalgebra structure (M, δ, ϵ) such that $\delta : M \to M \otimes M$ and $\epsilon : M \to Z_2$ are Q-module maps. If in addition M is a Q-ring and a bialgebra we shall say that it is a *Q-bialgebra*.

The Kudo-Araki algebra $\mathcal{K}$ is an example of a Q-coalgebra. Many of the usual constructions with coalgebras and algebras can be done with Q-coalgebras and Q-rings. For example, if C is a Q-coalgebra and R is a Q-ring then the set of Q-module maps $C \to R$ is a subalgebra of the convolution algebra $[C, R]$. If C is a Q-bialgebra then the set of Q-ring maps $C \to R$ is a monoid for the convolution product. Conversely, if a functor from Q-rings to monoids is representable by a Q-ring then this Q-ring has a Q-bialgebra structure. If a Q-bialgebra has an antipode then this antipode is a map of Q-rings.

Example 1. Consider the functor $R \mapsto E(R)$ which associates to a Q-ring R the set $E(R)$ of elements $u \in R$ such that $Q_t(u) = u(u + t)$. This functor is representable by the Q-ring $Z_2[x]$ with Q-structure given by $Q_t(x) = x(x + t)$. The functor E has a group structure since $E(R)$ is closed under addition. We obtain a Q-bialgebra structure on $Z_2[x]$ with $\delta : Z_2[x] \to Z_2[x] \otimes Z_2[x]$ given by $\delta(x) = x \otimes 1 + 1 \otimes x$.

Example 2. Consider the functor $R \mapsto F(R)$ which associates to a Q-ring R the set of formal power series $f(x) \in R[[x]]$ satisfying $Q_t(f)(x(x+t)) = f(x)f(x+t)$. This functor is representable by the Q-ring $Z_2[\beta_*] = Z_2[\beta_0, \beta_1, \dots]$ of Proposition 4 §1. The generic formal power series is $\beta(x) = \sum_i \beta_i x^i$. If $f \in F(R)$ and $g \in F(R)$ then

$$\begin{aligned} Q_t(fg)(x(x+t)) &= Q_t(f)(x(x+t))Q_t(g)(x(x+t)) \\ &= f(x)f(x+t)g(x)g(x+t) = (fg)(x)(fg)(x+t). \end{aligned}$$

It follows that $F(R)$ has a monoid structure. The map $\delta : Z_2[\beta_*] \to Z_2[\beta_*] \otimes Z_2[\beta_*]$ such that $\delta(\beta) = \beta \otimes \beta$ is representing the product of the monoid F. It follows that δ is a map of Q-rings. Hence we have described a Q-bialgebra structure on $Z_2[\beta_*]$.

Example 3. The Q-ring $Q\langle x\rangle$ is a Q-bialgebra in two ways. Since $Q\langle x\rangle$ is free, a Q-ring map $Q\langle x\rangle \to R$ is determined by its values at x. Thus $Q\langle x\rangle$ is representing the forgetful functor U from Q-rings to Sets. The functor U has also an algebra structure since $U(R) = R$ is an algebra. It follows that U has two monoid structures, one obtained from the multiplication and the other from the addition. The multiplication is represented by the map of Q-rings $\delta : Q\langle x\rangle \to Q\langle x\rangle \otimes Q\langle x\rangle$ such that $\delta(x) = x \otimes x$. The addition is represented by the map of Q-rings $\sigma : Q\langle x\rangle \to Q\langle x\rangle \otimes Q\langle x\rangle$ such that $\sigma(x) = x \otimes 1 + 1 \otimes x$. Put together, these two comultiplications are giving $Q\langle x\rangle$ the structure of a (dual) Hopf ring (see the remark below).

Example 4. The Q-ring $Q\langle x, x^{-1}\rangle = \{x\}^{-1}Q\langle x\rangle$ is representing the functor which associates to a Q-ring R its group $\mu(R)$ of invertible elements. Hence $Q\langle x, x^{-1}\rangle$ is an Hopf algebra.

Let $C = (C, \delta, \epsilon)$ be a coalgebra. Let us denote by $\delta : Q\langle C\rangle \to Q\langle C\rangle \otimes Q\langle C\rangle$ and $\epsilon : Q\langle C\rangle \to Z_2$ the Q-ring maps respectively extending $\delta : C \to C \otimes C$ and $\epsilon : C \to Z_2$.

Proposition 1. *If C is a coalgebra then $Q\langle C\rangle$ is a Q-bialgebra with δ and ϵ.*

Proof. For any Q-ring R the set $F(R)$ of Q-ring maps $Q\langle C\rangle \to R$ is in natural one to one correspondence with the set $[C, R]$ of linear maps $C \to R$ since $Q\langle C\rangle$ is free on C. But $[C, R]$ is a monoid for the convolution product defined from the coalgebra structure on C. Hence $F(R)$ has a natural monoid structure which must correspond to a coalgebra structure on $Q\langle C\rangle$. The verification that this coalgebra structure is represented by δ and ϵ is straightforward. QED

Remark. The proof of the proposition shows that if C is a coalgebra then $Q\langle C\rangle$ is a (dual) *Hopf ring* (a ring object in the category opposite to algebras). This is because the functor $R \mapsto [C, R]$ which it represents has an algebra structure (the convolution algebra). The multiplicative structure is represented by δ; the additive structure is represented by the map σ studied in Proposition 2 below.

Corollary. *The coalgebra structure on $Q\langle x\rangle$ defined by the Q-ring maps such that $\delta(x) = x \otimes x$ and $\epsilon(x) = 1$ restricts to induce the the coalgebra structure on $\mathcal{K}$.*

Proof. We have to verify that the square

$$\begin{tikzcd}
\mathcal{K} \arrow[r, "j"] \arrow[d, "\delta"'] & Q\langle x\rangle \arrow[d, "\delta"'] \\
\mathcal{K} \otimes \mathcal{K} \arrow[r, "j \otimes j"] & Q\langle x\rangle \otimes Q\langle x\rangle
\end{tikzcd}$$

commutes. But the four sides are Q-module maps and the square commutes on the generator $1 \in \mathcal{K}$ since $j(1) = x$, $\delta(1) = 1 \otimes 1$ and $\delta(x) = x \otimes x$. QED

For any Frobenius module M let $\sigma : \tilde{\Lambda}M \to \tilde{\Lambda}M \otimes \tilde{\Lambda}M$ and $\nu : \tilde{\Lambda}M \to Z_2$ be the ring maps such that $\sigma(x) = x \otimes 1 + 1 \otimes x$ and $\epsilon(x) = 0$ for $x \in V$. Recall that an element x of a bialgebra is *primitive* if $\delta(x) = x \otimes 1 + 1 \otimes x$.

Lemma 1. *For any Frobenius module M the maps σ and ν define a commutative Hopf algebra structure on $\tilde{\Lambda}M$. The subgroup of primitive elements of $\tilde{\Lambda}M$ is $M \subset \Lambda M$.*

Proof. The first statement is easily proved using representable functors. By definition, $\sigma(x) = x \otimes 1 + 1 \otimes x$ for every $x \in M$ and this means that every element of M is primitive. Conversely, let us prove that every primitive element of $\tilde{\Lambda}M$ belongs to M. If $q_0 = 0$ then $\tilde{\Lambda}M$ is the exterior algebra ΛM and this is a classical result. We shall reduce the general problem to this case. Let $F_0 \subseteq F_1 \subseteq \cdots$ be the filtration of $\tilde{\Lambda}M$ used in Lemma 1 §3. According to this lemma $\mathrm{gr}\tilde{\Lambda}M = \Lambda M$. Suppose now that $x \in \tilde{\Lambda}M$ is a non-zero primitive element and let $n \geq 0$ be the smallest integer such that $x \in F_n$. Then the corresponding element $\overline{x}$ in $F_n/F_{n-1} = \Lambda^n M$ is primitive and it follows that $n = 1$. This shows that $x \in F_1$. It remains to prove that $x \in M$. Using the basis Theorem 1 §3 it is easy to see that an element $x \in F_1$

belongs to M iff $\epsilon(x)=0$. But $\epsilon(x)=0$ since ϵ preserves primitive elements and 0 is the only primitive element of Z_2. This proves that $x \in M$. QED

Proposition 2. *For any vector space V let $\sigma : Q\langle V\rangle \to Q\langle V\rangle \otimes Q\langle V\rangle$ and $\nu : Q\langle V\rangle \to Z_2$ be the Q-ring maps such that $\sigma(x) = x \otimes 1 + 1 \otimes x$ and $\epsilon(x) = 0$ for $x \in V$. Then σ and ν are defining a commutative Hopf algebra structure on $Q\langle V\rangle$. For this structure, the subgroup of primitive elements is $\mathcal{K} \otimes V \subset Q\langle V\rangle$.*

Proof. To prove that $Q\langle V\rangle$ is a commutative Hopf algebra it suffices to show that the functor F it represents has a natural abelian group structure. But for any Q-ring R the set $F(R)$ is in natural bijection with the set $[V,R]$ of linear maps $V \to R$. Addition gives this set an abelian group structure. The verification that the structure is represented by σ and ν is straightforward. It remains to prove the second part. But this is a direct consequence of the preceding lemma applied to the case where $M = \mathcal{K} \otimes V$. QED

Corollary. *The Kudo-Araki algebra $\mathcal{K}$ is the subgroup of primitive elements of $Q\langle x\rangle$ with the Hopf algebra structure defined by σ and ν.*

Remark. Here is another proof of the corollary. According to Proposition 2 §3 we have $Q\langle x\rangle = S(\mathcal{K}^\flat)$. For any vector space U the symmetric algebra $S(U)$ has a Hopf algebra structure obtained from the addition operation on U. It is easy to see that the subgroup of primitive elements of $S(U)$ is the closure cl U of $U \subset S(U)$ under the Frobenius automorphism of $S(U)$. If $U = \mathcal{K}^\flat$ then the set of primitive element of $S(\mathcal{K}^\flat)$ is cl $\mathcal{K}^\flat = \mathcal{K}$.

Addendum to Section 6.

The homology of any space X has a coalgebra structure $\delta : H_*X \to H_*X \otimes H_*X$ obtained from the diagonal $X \to X \times X$. If X is an E_∞-space then H_*X is a Q-bialgebra; it is a Hopf algebra if X is group-like. For example the homology of BO_* (which is the classifying space for real vector bundles) is the Q-bialgebra $Z_2[\beta_*]$ considered in example 2. As another example, the homology of $\Omega^\infty S^\infty$ (which is the classifying space of cohomotopy) is the Hopf algebra $Q\langle x, x^{-1}\rangle$ considered in example 4.

If $E_\infty(X)$ is the free E_∞-space generated by a space X then $H_*E_\infty(X)$ is the free Q-ring generated by H_*X. Our Proposition 1 relates the diagonal structure on $H_*E_\infty(X) = Q\langle H_*X\rangle$ with the diagonal structure on H_*X. In particular, the diagonal $H_*\Sigma_* \to H_*\Sigma_* \otimes H_*\Sigma_*$ is given by the map of Q-rings $\delta : Q\langle x\rangle \to Q\langle x\rangle \otimes Q\langle x\rangle$ such that $\delta(x) = x \otimes x$.

The algebra $Q\langle x\rangle$ becomes a Hopf algebra when equipped with the map $\sigma : Q\langle x\rangle \to Q\langle x\rangle \otimes Q\langle x\rangle$ such that $\delta(x) = x \otimes 1 + 1 \otimes x$. Here is the “geometric” origin of this map. The ring structure on $H_*\Sigma = H_*B\Sigma_*$ is derived from the map $\alpha : B\Sigma_* \times B\Sigma_* \to B\Sigma_*$ induced by the subgroup inclusions $\Sigma_m \times \Sigma_n \to \Sigma_{n+m}$. It follows that α has the homotopy type of a finite covering space. By transfer we obtain a map $\alpha^! : H_*\Sigma_* \to H_*\Sigma_* \otimes H_*\Sigma_*$. This is σ.

A good source for coalgebras is Sweedler [1969]. For background on Hopf rings, see Ravenel, Wilson [1977], for instance. For some Hopf ring calculations directly related to our work here, see Turner [1996].

Appendix A

We recall a few basic algebraic facts about representable functors, Hopf algebras and convolution products.

Let *Alg* be the category of (commutative) Z_2-algebras. Recall that a set valued functor $F : Alg \to Sets$ is *represented* by a pair (a, A), where $A \in Alg$ and $a \in F(A)$, if for any Z_2-algebra R and any $b \in F(R)$ there is a unique algebra map $f : A \to R$ such that $F(f)(a) = b$. The element $a \in F(A)$ is said to be *universal* or *generic* in F. An element $b \in F(R)$ is then a *specialisation* of a; if $F(f)(a) = b$ we say that f is representing b and we shall write $f = b^\dagger$. Thus $b = F(b^\dagger)(a)$ and $f = F(f)(a)^\dagger$. Notice that for any $b \in F(R)$ and any map $g : R \to S$ we have $F(g)(b)^\dagger = g \circ b^\dagger$. Notice also that $a^\dagger$ is the identity map $A \to A$.

If G is another functor represented by (b, B) we say that a natural transformation $t : F \to G$ is *represented* by a map $f : B \to A$ if $G(f)(b) = t_A(a)$. The product functor $F \times G$ is then represented by $((a \otimes 1, 1 \otimes b), A \otimes B)$, where $a \otimes 1 \in F(A \otimes B)$ denotes the image of a along the canonical map $A \to A \otimes B$ and similarly for $1 \otimes b$.

For any pair U and V of Z_2-vector spaces we shall denote by $[U, V]$ the vector space of linear maps $U \to V$. Recall that if $\mathcal{C}$ is a coalgebra and R is an algebra then $[\mathcal{C}, R]$ is an associative algebra for the convolution product. More generally, let $\phi : M \to M \otimes \mathcal{C}$ be a right comodule over $\mathcal{C}$. The *convolution* of $f \in [M, R]$ with $g \in [\mathcal{C}, R]$ is the element $f \star g \in [M, R]$ obtained by composing

$$M \xrightarrow{\phi} M \otimes \mathcal{C} \xrightarrow{f \otimes g} R \otimes R \xrightarrow{m} R$$

where m is multiplication. The convolution product gives $[M, R]$ the structure of a right module over $[\mathcal{C}, R]$.

Recall that for any $g \in [\mathcal{C}, R]$ the *dot product* $g \bullet (-) : M \otimes R \to M \otimes R$ is the R-linear extension of the composite

$$M \xrightarrow{\phi} M \otimes \mathcal{C} \xrightarrow{M \otimes g} M \otimes R.$$

The dot product gives $M \otimes R$ the structure of a left module over $[\mathcal{C}, R]$. For any $f \in [M, R]$, $g \in [\mathcal{C}, R]$ and $x \in M \otimes R$ we have the identity

$$\langle f, g \bullet x \rangle = \langle f \star g, x \rangle$$

where $\langle -, - \rangle$ denotes the natural pairing $[M, R] \otimes (M \otimes R) \to R$. If $\mathcal{C}$ is a bialgebra representing a functor G and $\alpha \in G(\mathcal{C})$ is the generic element then $\alpha \bullet x = \phi(x)$ for every $x \in M$.

If a pair $(a, \mathcal{G})$ represents a monoid-valued functor G then $\mathcal{G}$ is a bialgebra with coproduct $\Delta : \mathcal{G} \to \mathcal{G} \otimes \mathcal{G}$ representing the multiplication $G \times G \to G$, and with the augmentation $\epsilon : \mathcal{G} \to Z_2$ representing the unit element $1 \to G$. If $u, v \in G(R)$ are represented by algebra maps $f, g : \mathcal{G} \to R$, then the convolution product $f \star g$ represents the product $uv \in G(R)$. This can be expressed by the identity $(uv)^\dagger = u^\dagger \star v^\dagger$. If G is group-valued then $\mathcal{G}$ is a Hopf algebra with the antipode $\chi : \mathcal{G} \to \mathcal{G}$ representing the inverse operation $G \to G$. If $u \in G(R)$ is represented by $f : \mathcal{G} \to R$ then u^{-1} is represented by $f \circ \chi : \mathcal{G} \to R$.

A good source for representable functors is MacLane [1971]. For Hopf algebras and convolution algebras see Sweedler [1969] or Joyal, Street [1991c], for instance.

Appendix B

In this appendix we relate comodules over the extended Milnor coalgebra $\mathcal{A}$ to graded comodules over the standard Milnor coalgebra $\mathcal{S}_*$.

The vector space $Z_2\langle I\rangle$ freely generated by a set I has a coalgebra structure with comultiplication obtained from the diagonal $I \to I \times I$ and counit obtained from the map $I \to 1$. We shall say that it is a *diagonal coalgebra.* A coaction $\gamma : V \to V \otimes Z_2\langle I\rangle$ is equivalent to a grading $(V_i : i \in I)$ on V. More precisely, from a grading $(V_i : i \in I)$ we obtain a coaction $\gamma(x) = \sum_i \gamma_i(x) \otimes i$ where $\gamma_i : V \to V_i$ is the projection operator; conversely, from a coaction γ we obtain a grading with $x \in V_i$ iff $\gamma(x) = x \otimes i$.

For any Z_2-algebra R let $\mu(R)$ be the group of invertible elements of R. The functor $\mu : Alg \to Grp$ is represented by the algebra $Z_2[u^{\pm}] = Z_2[u^{-1}, u]$ of Laurent polynomials, with u as the generic element and with coproduct given by $\delta(u) = u \otimes u$. It is a diagonal coalgebra since $\delta(u^n) = u^n \otimes u^n$ for every $n \in Z$. It follows that a coaction $\gamma : V \to V \otimes Z_2[u^{\pm}]$ is equivalent to a Z-grading on V. We have $x \in V_n$ iff $\gamma(x) = x \otimes u^n$.

Recall the discussion of the extended Milnor coalgebra $\mathcal{A} = Z_2[a_0^{\pm}, a_1, \dots]$ in §4. The coalgebra $\mathcal{A}$ is representing the functor $A : Alg \to Grp$ which associates to each R the group $A(R)$ of invertible additive power series in $xR[[x]]$. Let us introduce two gradings on $\mathcal{A}$, each obtained from an action of the multiplicative group μ on A. The action by conjugation $(f(x), r) \mapsto r^{-1}f(rx)$ gives the *dimension grading*, for which $\dim(a_i) = 2^i - 1$. The action on the left $(r, f(x)) \mapsto rf(x)$ gives the *rank grading*, for which $\mathrm{rank}(a_i) = 1$. The monomials $a^R = a_0^{r_0}a_1^{r_1}\cdots$ with $R = (r_0, r_1, \dots)$ form a basis of $\mathcal{A}$ (notice that $r_0 \in Z$). For any $R = (r_0, r_1, \dots)$ (with $r_0 \in Z$) we have $\dim(a^R) = r_1(2^1 - 1) + r_2(2^2 - 1) + \cdots$ and $\mathrm{rank}(a^R) = r_0 + r_1 + \cdots$. We shall write $\dim(a^R) = \dim(R)$ and $\mathrm{rank}(a^R) = \mathrm{rank}(R)$.

Recall that a coaction $\psi : V \to V \otimes \mathcal{A}$ has a formal expansion

$$\psi(y) = \sum_R \psi_R(y) \otimes a^R$$

for $y \in V$; this determines natural operations ψ_R on Milnor comodules.

From any coaction $\psi : V \to V \otimes \mathcal{A}$ we can extract a grading $(V_n : n \in Z)$ by specialising the generic additive series $a(x)$ to ux. More precisely, the grading coaction $\gamma : V \to V \otimes Z_2[u^{\pm}]$ is obtained by putting $a_0 = u$ and $a_i = 0$ for $i > 0$ in the expansion of ψ. Hence

$$\gamma(y) = \sum_n \psi_{(n,0,\dots)}(y)u^n$$

for $y \in V$, and this means that $\psi_{(n,0,\dots)}$ is the projection operator $V \to V_n$. Notice that $\gamma(y) = u^\dagger \bullet y$ where $u^\dagger$ is the ring homomorphism $\mathcal{A} \to Z_2[u^{\pm}]$ such that $a(x) \mapsto ux$.

Proposition 1. *Each ψ_R is an operation $\psi_R : V_{n+r} \to V_r$, where $n = dim(R)$ and $r = rank(R)$; $\psi_R = 0$ on V_m for $m \neq n + r$. In particular, $\psi : V \to V \otimes \mathcal{A}$ is preserving the (total) dimension.*

Proof. Notice the identity $(ua)^R = a^R u^{\mathrm{rank}R}$ where $(ua)(x) = u(a(x))$. From the associativity of ψ we obtain that

$$\sum \gamma(\psi_R(y))\ a^R = \sum \psi_R(y)\ (ua)^R = \sum \psi_R(y)\ a^R\ u^{\mathrm{rank}R}.$$

Hence $\gamma(\psi_R(y)) = \psi_R(y)u^{\mathrm{rank}R}$ and this proves that $\psi_R(y)$ is of dimension $\mathrm{rank}(R)$. Let us prove that ψ_R is 0 on V_m except when $m = \dim(R) + \mathrm{rank}(R)$. Notice the identity $(au)^R = a^R u^{\dim R + \mathrm{rank}R}$ where $(au)(x) = a(ux)$. From the associativity of ψ we obtain that

$$\sum_m \psi(\gamma_m(y))u^m = \sum \psi_R(y)\ (au)^R = \sum \psi_R(y)\ a^R\ u^{\dim R+\mathrm{rank}R}.$$

By equating the coefficient of u^m on each side of this equality we obtain the result. This proves also that ψ_R is lowering dimension by an amount equal to $\dim(R) = \dim(a^R)$. Hence ψ is homogeneous of degree 0. QED

The classical Milnor coalgebra $\mathcal{S}_*$ is representing the functor $S : Alg \to Grp$ which associates to $R \in Alg$ the group of additive power series $f(x) = \sum f_i x^{2^i}$ with $f_0 = 1$ (it is a group for the operation of substitution). We have $\mathcal{S}_* = Z_2[\xi_1, \xi_2, \dots]$, where $\xi(x) = x + \sum_{i>0} \xi_i\ x^{2^i}$ is the generic series. The coproduct $\Delta : \mathcal{S}_* \to \mathcal{S}_* \otimes \mathcal{S}_*$ is given by

$$\Delta(\xi) = (\xi \otimes 1) \circ (1 \otimes \xi).$$

The monomials $\xi^K = \xi_1^{k_1}\xi_2^{k_2}\cdots$ with $K = (k_1, k_2, \dots)$ form a basis of $\mathcal{S}_*$. An $\mathcal{S}_*$-coaction $\phi : V \to V \otimes \mathcal{S}_*$ has a formal expansion

$$\phi(x) = \sum_K \phi_K(x) \otimes \xi^K.$$

The *dimension grading* on $\mathcal{S}_*$ is given by $\dim(\xi_i) = 2^i - 1$. We say that a comodule $\phi : V \to V \otimes \mathcal{S}_*$ is *graded* if V is graded by dimension and ϕ preserves dimension. Suppose now that $\psi : V \to V \otimes \mathcal{A}$ is a coaction. Then V has a grading obtained from the specialisation $a(x) \mapsto ux$. Also, V has a coaction $\phi : V \to V \otimes \mathcal{S}_*$ obtained from the specialisation $a(x) \mapsto \xi(x)$. The coaction ϕ is preserving dimension since ψ and the specialisation $a(x) \mapsto \xi(x)$ are both dimension preserving. We have

$$\phi(x) = \sum_K \phi_K(x)\xi^K = \sum_K \sum_n \psi_{n,K}(x)\xi^K$$

where $n, K = (n, k_1, k_2, \dots)$ for $n \in Z$ and $K = (k_1, k_2, \dots)$. More precisely, for any $R = (r_0, r_1, \dots)$ we have

$$\psi_R(x) = \begin{cases} \phi_K(x) & \text{if } x \in V_n \\ 0 & \text{otherwise} \end{cases}.$$

where $K = (r_1, r_2, \dots)$ and $n = \dim(R) + \mathrm{rank}(R)$. The following result is easy to prove:

Proposition 2. *The specialisations $a(x) \mapsto \xi(x)$ and $a(x) \mapsto ux$ induce a one-to-one correspondence $\psi \mapsto \phi$ between the $\mathcal{A}$-coactions and the graded $\mathcal{S}_*$-coactions.*

Remark. The above result depends on the fact that $\mathcal{A}$ is the semi-direct (tensor) product $Z_2[u^{\pm}] \otimes \mathcal{S}_*$ (see examples 1 and 3 of appendix C). The functorial group A is a semi-direct product $\mu \times S$ since the projection $f \mapsto f_0$ is a split homomorphism $A(R) \to \mu(R)$ with kernel $S(R)$.

Warning. The traditional Milnor Hopf algebra is actually the opposite Hopf algebra $(\mathcal{S}_*, \Delta^o, \epsilon)$, with comultiplication Δ^o given by $\Delta^o(\xi) = (1 \otimes \xi) \circ (\xi \otimes 1)$. The comultiplication Δ^o is therefore representing composition of power series in the reverse order. The antipode is an isomorphism between $(\mathcal{S}_*, \Delta, \epsilon)$. and $(\mathcal{S}_*, \Delta^o, \epsilon)$. Right comodules over one may be regarded as left comodules over the other. Following Milnor [1958] most authors work with the corresponding *left* coaction over the Hopf algebra $(\mathcal{S}_*, \Delta^o, \epsilon)$. There is an intricate discussion of questions relating to left and right coactions in Boardman [1982].

Appendix C

The purpose of this appendix is to sketch an abstract theory of commutation operators.

Recall that a *monoidal or tensor category* is a category $\mathcal{C}$ equipped with a (tensor) product functor $\otimes : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ and a unit object $I \in \mathcal{C}$ together with natural associativity and unit isomorphisms, $A \otimes (B \otimes C) \simeq (A \otimes B) \otimes C$ and $A \otimes I \simeq A \simeq I \otimes A$, satisfying standard coherence conditions (see MacLane [1971]). A tensor category is *strict* if the associativity and unit isomorphisms are identity maps. We shall use MacLane's coherence theorem. For all practical purpose it says that we can safely identify all the objects obtained by multiplying a given sequence of objects according to various bracketing patterns. One version of the theorem says that any tensor category is equivalent to a strict one. The tensor power $A^{\otimes n} = A^n$ of an object is defined inductively: $A^0 = I$ and $A^{n+1} = A \otimes A^n = A^n \otimes A$.

Definition 1. Let $\mathcal{C}$ be a tensor category. A *commutation operator* between two objects A, B in $\mathcal{C}$ is an arrow $\rho : A \otimes B \to B \otimes A$.

The *powers* ${}^q\rho^p : A^p \otimes B^q \to B^q \otimes A^p$ of a commutation operator are easily defined with symbolic planar representations (Joyal, Street [1991b]). The diagram defining ${}^q\rho^p$ is a $p \times q$ diamond grid. For example, in the 3×4 case it is:

The powers ρ^p and ${}^q\rho$ can be defined by induction: $\rho^0 : B \to B$ is the identity map and ρ^{p+1} is the composite

$$A^{p+1} \otimes B \xrightarrow{A \otimes \rho^p} A \otimes B \otimes A^p \xrightarrow{\rho \otimes A^p} B \otimes A^{p+1};$$

and similarly for ${}^q\rho$. We have ${}^q\rho^p = {}^q(\rho^p) = ({}^q\rho)^p$.

Definition 2. Let $\mathcal{C}$ be a tensor category. We shall say that a commutation operator $\rho : A \otimes B \to B \otimes A$ *respects* an arrow $f : A^p \to A^q$, or that f *is (left) compatible with* ρ, if the square

$$\begin{tikzcd}
A^p \otimes B \arrow[r, "f \otimes B"] \arrow[d, "\rho^p"'] & A^q \otimes B \arrow[d, "\rho^q"] \\
B \otimes A^p \arrow[r, "B \otimes f"] & B \otimes A^q
\end{tikzcd}$$

commutes. There is a similar concept of (right) compatibility for an arrow $g : B^p \to B^q$.

Example. A Yang-Baxter operator $R : A \otimes A \to A \otimes A$ is a self-respecting commutation operator (Joyal, Street [1991a]).

Proposition 1. *If $\rho : A \otimes B \to B \otimes A$ respects $f : A^p \to A^q$ and $g : A^k \to A^r$ the it respects their tensor product $f \otimes g : A^{p+k} \to A^{q+r}$, and their composite $gf : A^p \to A^r$ if $q = r$. If $f : A^p \to A^q$ is respected by ρ then it is respected by ${}^r\rho : A \otimes B^r \to B^r \otimes A$ for any $r \geq 0$.*

Proof. These results are obvious with planar diagram representations. We leave their verification to the reader. QED

Recall that a *monoid* in a tensor category $\mathcal{C}$ is a triple $K = (K, m, u)$ where $m : K \otimes K \to K$ and the $u : I \to K$, and such that the following associativity and unit diagrams commute:

$$\begin{tikzcd}
K \otimes K \otimes K \arrow[r, "K \otimes m"] \arrow[d, "m \otimes K"'] & K \otimes K \arrow[d, "m"] & K \arrow[r, "u \otimes K"] \arrow[dr, "K"'] & K \otimes K \arrow[d, "m"] & K \arrow[r, "K \otimes u"] \arrow[dr, "K"'] & K \otimes K \arrow[d, "m"] \\
K \otimes K \arrow[r, "m"] & K & & K & & K.
\end{tikzcd}$$

As for ordinary monoids, the unit for a given m is unique when it exists. A monoid structure (m, u) is thus determined by m. Recall that a (left)*action* of K on an object S is an arrow $q : K \otimes S \to S$ such that the following associativity and unit diagrams commute:

$$\begin{tikzcd}
K \otimes K \otimes S \arrow[r, "K \otimes q"] \arrow[d, "m \otimes S"'] & K \otimes S \arrow[d, "q"] & S \arrow[r, "u \otimes S"] \arrow[dr, "S"'] & K \otimes S \arrow[d, "q"] \\
K \otimes S \arrow[r, "q"] & S & & S.
\end{tikzcd}$$

We also say that $S = (S, q)$ is an K-*object*. If S and T are K-objects we say that a map $f : S \to T$ is an K-*map* if it respects the actions.

Recall that a *comonoid* $A = (A, \Delta, \epsilon)$ in a tensor category $\mathcal{C}$ is a monoid in the opposite category. The *comultiplication* $\Delta : A \to A \otimes A$ and the *counit* satisfy dual conditions expressed by the coassociativity and counit diagrams. A *(left) coaction* $\psi : A \to A \otimes S$ of A on S is defined dualy. We shall say that $S = (S, \psi)$ is an A-*object*. There is also the concept of A-maps between A-objects.

Definition 3. We shall say that a commutation operator $\rho : K \otimes A \to A \otimes K$ *respects a monoid structure* (K, m, u) if it respects m and u. A commutation operator ρ can similarly respect a (co)monoid structure on A, or on K.

Suppose that a commutation operator $\rho : K \otimes A \to A \otimes K$ respects the monoid structures (K, m, u) and (A, n, v). Then the composite

$$A \otimes K \otimes A \otimes K \xrightarrow{A \otimes \rho \otimes K} A \otimes A \otimes K \otimes K \xrightarrow{n \otimes m} A \otimes K.$$

is a monoid structure on $A \otimes K$. We shall sometime denote this monoid by $A \otimes_\rho K$. An action by $A \otimes_\rho K$ can be analysed in terms of a pair of ρ-*commuting* actions by A and K. Two actions $q : K \otimes S \to S$ and $r : A \otimes S \to S$ are said to ρ-*commute* if the following diagram commutes:

$$\begin{tikzcd}
K \otimes A \otimes S \arrow[rr, "\rho \otimes S"] \arrow[d, "K \otimes r"'] & & A \otimes K \otimes S \arrow[d, "A \otimes q"] \\
K \otimes S \arrow[r, "q"] & S \arrow[r, dash, "r"] & A \otimes S;
\end{tikzcd}$$

In this case the composite

$$A \otimes K \otimes S \xrightarrow{A \otimes q} A \otimes S \xrightarrow{r} S$$

is an action by $A \otimes_\rho K$. This defines a one to one correspondence between the actions by $A \otimes_\rho K$ and the pairs (q, r) of ρ-commuting actions.

Example 1. Let G be a group and $H, K \subseteq G$ be subgroups. Let us suppose that the map $H \times K \to G$ given by $(x, y) \to xy$ is bijective. Then for any $(x, y) \in K \times H$ there is a unique pair $(u, v) \in H \times K$ such that $xy = uv$. If we put $\rho(x, y) = (u, v)$ then we obtain a commutation operator $\rho : K \times H \to H \times K$ (in the category *Sets* of sets). It is easy to see that ρ respects the group structures of H and K. A simple example of such a pair (H, K) is given by a semidirect decomposition $G = H \times K$. We then have $\rho(x, y) = (xyx^{-1}, x)$ if K is the normal subgroup. By duality we obtain examples with Hopf algebras. From appendix B we know that the extended coalgebra $\mathcal{A}$ is a semidirect (tensor) product $Z_2[u^{\pm}] \otimes \mathcal{S}_*$ since the functorial group A which it represents is a semi-direct product $\mu \times S$.

Example 2. For any vector space V (over a field k) let $T(V)$ be the tensor algebra of V. If S is a vector space then a linear map $\alpha : V \otimes S \to S \otimes T(V)$ has a unique extension $\rho : T(V) \otimes S \to S \otimes T(V)$ as an operator respecting the algebra structure of $T(V)$. In particular, any linear map $\alpha : S \to S \otimes k[x]$ has a unique extension $\rho : k[x] \otimes S \to S \otimes k[x]$ as an operator respecting the algebra structure of $k[x]$. Suppose now that S is an algebra and that $\alpha(s) = \alpha_0(s) \otimes 1 + \alpha_1(s) \otimes x$

for some linear maps $\alpha_0, \alpha_1 : S \to S$. In this case ρ is respecting the algebra structure of S iff α_0 is an algebra endomorphism and α_1 is an α_0-derivation (that is $\alpha_1(st) = \alpha_1(s)t + \alpha_0(s)\alpha_1(t)$ for any $s, t \in S$). We then obtain an algebra structure on $S[x] = S \otimes k[x] = S \otimes_\rho k[x]$ that is called an *Ore extension* of S. For example, if $k = Z_2$ and S is commutative we can take $\alpha_0(s) = s^2$ and $\alpha_1 = 0$. Then the Ore extension $S[x]$ is isomorphic to the algebra of Ore polynomials with coefficients in S, with the operation of substitution as multiplication.

Example 3. If R is a Q-ring then $R \otimes \mathcal{K}$ is a Q-module and there is a unique Q-module map $\rho : \mathcal{K} \otimes R \to R \otimes \mathcal{K}$ such that $\rho(1 \otimes x) = x \otimes 1$. The operator ρ respects the algebra structures of R and $\mathcal{K}$. It follows that $R \otimes \mathcal{K}$ has an algebra structure obtained from ρ. A module over this algebra is the same as a QR-module. This example is a special case of the general concept of semi-direct product between a bialgebra and an algebra. If B is a bialgebra then the tensor product of two (left) B-modules has a B-module structure derived from the comultiplication of B. If N is a B-module then $N \otimes B$ is a B-module and there is a unique B-module map $\rho : B \otimes N \to N \otimes B$ such that $\rho(1 \otimes x) = x \otimes 1$. It is easy to see that ρ respects the algebra structure of B. If N has an algebra structure for which multiplication $N \otimes N \to N$ and units $I \to B$ are B-modules maps then this structure is respected by ρ. In this case there is a semi-direct product algebra $N \otimes B$. A module V over $N \otimes B$ is the same thing as a module V over N in the category of B-modules (this means that V is a B-module and that the structure map $N \otimes M \to M$ is a B-module map). There is a dual result with comodules and coalgebras. For example, if $B = Z_2[u^{\pm}]$ then a comodule over $Z_2[u^{\pm}]$ is a graded vector spaces. The coalgebra $\mathcal{S}_*$ is graded, it is thus a coalgebra in the category of comodules over $Z_2[u^{\pm}]$. Hence there is a commutation operator $\rho : \mathcal{S}_* \otimes Z_2[u^{\pm}] \to Z_2[u^{\pm}] \otimes \mathcal{S}_*$ and a corresponding semi-direct product $\mathcal{A} = Z_2[u^{\pm}] \otimes \mathcal{S}_*$. It follows that a comodule over $\mathcal{A}$ is the same as a graded comodule over $\mathcal{S}_*$ (see Proposition 2 appendix B).

Example 4. The category $[\mathcal{C}, \mathcal{C}]$ of endofunctors of a category $\mathcal{C}$ is monoidal with composition for the tensor product. A monoid (K, m, u) in this category is called a *monad* (MacLane [1971]). The concept of commutation operator $\rho : KM \to MK$ respecting two monads is due to Jon Beck [1969] and it is called a *Beck distributive law* by category theorists.

Proposition 2. *Let $K = (K, m, u)$ be a monoid and let $\rho : K \otimes A \to A \otimes K$ be a commutation operator. Then the following two conditions are equivalent:*
(i) *ρ respects (K, m, u);*
(ii) *for any action $q : K \otimes S \to S$ the composite*

$$K \otimes A \otimes S \xrightarrow{\rho \otimes S} A \otimes K \otimes S \xrightarrow{A \otimes q} A \otimes S$$

is an action $q' : K \otimes A \otimes S \to A \otimes S$.

Proof. The implication (i) $\Rightarrow$ (ii) is left to the reader. We sketch the proof of (ii) $\Rightarrow$ (i). If we take $S = K$ and $q = m$ the map q' is the composite

$$K \otimes A \otimes K \xrightarrow{\rho \otimes K} A \otimes K \otimes K \xrightarrow{A \otimes m} A \otimes K.$$

By hypothesis q' is a coaction. If we precompose the associativity diagram for q' with the arrow $K \otimes K \otimes A \otimes u : K \otimes K \otimes A \to K \otimes K \otimes A \otimes K$ and simplify we obtain the compatibility diagram of m with ρ. The compatibility diagram of u with ρ is obtained similarly but with the unit diagram of q' instead. QED

Proposition 3. *Let $K = (K, m, u)$ be a monoid and $A = (A, \Delta, \epsilon)$ be a comonoid. If a commutation operator $\rho : K \otimes A \to A \otimes K$ respects (K, m, u) then the following two conditions are equivalent:*

(i) *ρ respects (A, Δ, ϵ);*

(ii) *for any action $q : K \otimes S \to S$ the maps $\epsilon \otimes S : A \otimes S \to S$ and $\Delta \otimes S : A \otimes S \to A \otimes A \otimes S$ are K-maps.*

Proof. The implication (i) ⇒ (ii) is left to the reader. We sketch the proof of (ii) ⇒ (i). If $S = K$ and $q = m$ the arrow q' is the composite

$$K \otimes A \otimes K \xrightarrow{\rho \otimes K} A \otimes K \otimes K \xrightarrow{A \otimes m} A \otimes K$$

and q'' is the composite

$$K \otimes A \otimes A \otimes K \xrightarrow{{}^2\rho \otimes K} A \otimes A \otimes K \otimes K \xrightarrow{A \otimes m} A \otimes A \otimes K.$$

If we precompose with $K \otimes A \otimes u$ the diagram expressing that $\Delta \otimes K$ is an K-map and simplify we obtain the compatibility diagram of Δ with ρ. The compatibility of ϵ with ρ is obtained similarly but by using $\epsilon \otimes K$ instead of $\Delta \otimes K$. QED

Suppose now that $\rho : K \otimes A \to A \otimes K$ respects the monoid structure $K = (K, m, u)$ and the comonoid structure $A = (A, \Delta, \epsilon)$. We shall say that an action $q : K \otimes S \to S$ and a coaction $\psi : S \to A \otimes S$ *ρ-commute* if the following diagram commutes:

$$\begin{tikzcd}
K \otimes S \arrow[r, "q"] \arrow[d, "K \otimes \psi"'] & S \arrow[r, "\psi"] & A \otimes S \\
K \otimes A \otimes S \arrow[rr, "\rho \otimes S"] & & A \otimes K \otimes S. \arrow[u, "A \otimes q"']
\end{tikzcd}$$

Definition 4. A *ρ-biaction* is a ρ-commuting pair (q, ψ) of an action $q : K \otimes S \to S$ and a coaction $\psi : S \to A \otimes S$.

Example. Let $Z_2[q_0]$ be the polynomial ring and let $Z_2[u^{\pm}]$ be the ring of Laurent polynomials with its bialgebra structure given by $\delta(u) = u \otimes u$. Then the commutation operator $\rho : Z_2[q_0] \otimes Z_2[u^{\pm}] \to Z_2[u^{\pm}] \otimes Z_2[q_0]$ given by $\rho(q_0^r \otimes u^n) = u^{2^r n} \otimes q_0$ respects the algebra structure of $Z_2[q_0]$ and the coalgebra structure of $Z_2[u^{\pm}]$. A ρ-biaction is a graded module M equipped with a Frobenius operator $q_0 : M \to M$ doubling the dimension. Perhaps a more interesting example is the commutation operator $\rho : \mathcal{K} \otimes Z_2[u^{\pm}] \to Z_2[u^{\pm}] \otimes \mathcal{K}$ defined as follow: consider the Q-structure on $Z_2[u^{\pm}] \otimes \mathcal{K}$ that is given by

$$Q_t(u^n \otimes x) = u^{2n} Q_{ut}(x) = u^{2n} \sum_i u^i \otimes q_n(x) t^i.$$

The vector space $\mathcal{K} \otimes Z_2[u^{\pm}]$ is free as a Q-module over $Z_2[u^{\pm}]$. By definition, ρ is the unique Q-module map such that $\rho(1 \otimes u^n) = u^n \otimes 1$. A ρ-biaction is a graded

Q-module M. These two examples are special case of a more general commutation operator $\tilde{\rho} : \mathcal{K} \otimes \mathcal{A} \to \mathcal{A} \otimes \mathcal{K}$ that is playing a central role in our theory of the Nishida relations in §5.

By the dual of Proposition 2 for any coaction $\psi : S \to A \otimes S$ the composite

$$K \otimes S \xrightarrow{K \otimes \psi} K \otimes A \otimes S \xrightarrow{\rho} A \otimes K \otimes S$$

is a coaction $\psi' : K \otimes S \to A \otimes K \otimes S$.

Proposition 4. *Suppose that $\rho : K \otimes A \to A \otimes K$ respects the monoid structure of K and the comonoid structure of A. If $q : K \otimes S \to S$ is an action and $\psi : S \to A \otimes A$ is a coaction then the following three conditions are equivalent:*

(i) *the pair (q, ψ) ρ-commutes;*
(ii) *ψ is an K-map;*
(iii) *q is an A-map.*

Proof. By definition of q' and ψ' the following diagram commutes:

$$\begin{tikzcd}
K \otimes S \arrow[r, "\psi'"] \arrow[d, "\mathcal{K} \otimes \psi"'] & A \otimes K \otimes S \arrow[d, "A \otimes q"] \\
K \otimes A \otimes S \arrow[r, "q'"] \arrow[ur, "\rho \otimes S"] & A \otimes S
\end{tikzcd}$$

This shows that the pair (q, ψ) is ρ-commuting iff one of the following two squares commute

$$\begin{tikzcd}
K \otimes S \arrow[r, "K \otimes \psi"] \arrow[d, "q"'] & K \otimes A \otimes S \arrow[d, "q'"] & K \otimes S \arrow[r, "\psi'"] \arrow[d, "q"'] & A \otimes K \otimes S \arrow[d, "A \otimes q"] \\
S \arrow[r, "\psi"] & A \otimes S & S \arrow[r, "\psi"] & A \otimes S.
\end{tikzcd}$$

But the left hand side square commutes iff ψ is an K-map and the right hand square commutes iff q is an A-map. QED

Let $\mathcal{C}^K$ and $\mathcal{C}^A$ be the categories of K-actions and A-coactions respectively. Let $\mathcal{C}^{KA}$ be the category of ρ-biactions (with maps respecting both action and coaction). We have the following proposition whose verification is left to the reader.

Proposition 5. *Suppose that $\rho : K \otimes A \to A \otimes K$ respects the monoid structure $K = (K, m, u)$ and the comonoid structure $A = (A, \Delta, \epsilon)$.*

(i) *For any coaction $\psi : S \to A \otimes S$ the pair $(m \otimes S, \psi')$ is a ρ-biaction on $K \otimes S$. The functor $S \mapsto K \otimes S$ is left adjoint to the forgetful functor $\mathcal{C}^{KA} \to \mathcal{C}^A$.*
(ii) *For any action $q : K \otimes S \to S$ the pair $(q', \Delta \otimes S)$ is a ρ-biaction on $A \otimes S$. The functor $S \mapsto A \otimes S$ is right adjoint to the forgetful functor $\mathcal{C}^{KA} \to \mathcal{C}^K$.*

Remark. The theory of commutation operator presented here must be slightly reformulated in the case of the the monoidal category $[\mathcal{C},\mathcal{C}]$ of endofunctor of a category $\mathcal{C}$. In this case the K-objects of a monoid (i.e. of a monad on $\mathcal{C}$) should be taken in $\mathcal{C}$ rather than in $[\mathcal{C},\mathcal{C}]$. Recall that an action by K on an object $S \in \mathcal{C}$ is a map $q : K(S) \to S$ for which the following associativity and unit diagrams commute:

$$\begin{tikzcd}
KK(S) \arrow[r, "K(q)"] \arrow[d, "m_S"'] & K(S) \arrow[d, "q"] & S \arrow[r, "u_S"] \arrow[dr, "1_S"'] & K(S) \arrow[d, "q"] \\
K(S) \arrow[r, "q"] & S & & S.
\end{tikzcd}$$

These K-objects are called K-algebras by category theorists (MacLane [1971]). Similarly, the A-objects of a comonad are called A-coalgebras. Let $\rho : KA \to AK$ be a commutation operator respecting the monad structure of K and the comonad structure of A. We say that an action $q : K(S) \to S$ and a coaction $\psi : S \to A(S)$ *ρ-commute* if the following diagram commutes:

$$\begin{tikzcd}
K(S) \arrow[r, "q"] \arrow[d, "K(\psi)"'] & S \arrow[r, "\psi"] & A(S) \\
KA(S) \arrow[rr, "\rho_S"] & & AK(S). \arrow[u, "A(q)"']
\end{tikzcd}$$

We say that (S, q, ψ) is a *ρ-bialgebra*. All the results of this appendix are valid when properly formulated for K-algebras, A-coalgebras in $\mathcal{C}$ instead of K-objects and A-objects in $[\mathcal{C},\mathcal{C}]$.

This paper was prepared using Paul Taylor's Diagram package of macros for TEX and with the AMS-TEXformat.

References

[1974] J.F. Adams, *Stable homotopy and generalized homology*, University of Chicago Press, 1974.

[1978] J.F. Adams, *Infinite loop spaces*, vol. 90, Ann. of Math. Studies, Princeton, 1978.

[1957] J. Adem, *The relations on Steenrod powers of cohomology classes*, Algebraic Geometry and Topology, Princeton University Press, 1957, pp. 191-238.

[1956] S. Araki & T. Kudo, *Topology of H_n-spaces and H_n-squaring operations*, Mem. Fac. Sci. Kyusyu Univ. Ser. A **10** (1956), 85-120.

[1966] M.F. Atiyah, *Power operations in K-theory*, Quart. J. Math. Oxford (2) **17** (1966), 165-193, reprinted in Atiyah, *K-theory*, Benjamin, 1967.

[1971] M. Barratt, D. Kahn & S.Priddy, *On $\Omega^\infty S^\infty$ and the infinite symmetric group*, Proc. of Sympos. Pure Math. **22** (1971), A.M.S..

[1969] J. Beck, *Distributive laws, Seminar on Triple and Categorical Homology Theory*, Lecture Notes in Mathematics, vol. 80, Springer Verlag, 1969.

[1977] T.P. Bisson, *Divided sequences and bialgebras of homology operations*, Ph.D. Thesis, Duke, 1977.

[1995a] T.P. Bisson & A. Joyal, *The Dyer-Lashof algebra in bordism*, extended abstract, C.R. Math. Rep. Acad. Sci. Canada **17** (1995), 135-140.

[1995b] ———, *Nishida relations in bordism and homology*, extended abstract, C.R. Math. Rep. Acad. Sci. Canada **17** (1995), 141-146.

[1982] J.M. Boardman, *The eightfold way to BP operations*, Can. Math. Soc. Conf. Proc. **2** (1982), no. 1.

[1960] W. Browder, *Homology operations and loop spaces*, Illinois J. Math. (1960), 347-357.

[1982] S.R. Bullett & I.G. Macdonald, *On the Adem relations*, Topology **21** (1982), 329-332.

[1911] L.E. Dickson, *A fundamental system of invariants of the general modular linear group with a solution of the form problem*, Trans. A.M.S. **12** (1911), 75-98.

[1958] A. Dold, *Homology of the symmetric products and other functors of complexes*, Ann. of Math. **68** (1958), 54-80.

[1962] E. Dyer & R.K. Lashof, *Homology of iterated loop spaces*, Amer. J. Math. **84** (1962), 35-88.

[1958] A. Grothendieck, *La théorie des classes de Chern*, Bull. Soc. Math. France **86** (1958), 137-154.

[1979] P. Hoffman, *τ-Rings and Wreath Product Representations*, Lect. Notes in Math., vol. 746, Springer-Verlag, 1979.

[1982] S.A. Joni & G.-C. Rota, *Coalgebras and bialgebras in combinatorics*, Umbral Calculus and Hopf Algebra, Contemporary Mathematics, vol. 6, A.M.S., 1982, pp. 1-47.

[1991a] A. Joyal & R. Street, *Tortile Yang Baxter operators in tensor categories*, J. of Pure and Applied Algebra **71** (1991), 43-51.

[1991b] ———, *The geometry of tensor calculus I*, Advances in Mathematics **88** (1991), no. 1, 55-112.

[1991c] ———, *An introduction to Tannaka duality and quantum groups*, Category Theory Proceedings: Como 1990, Lecture Notes in Math., vol. 1488, Springer-Verlag, 1991, pp. 411-492.

[1973] D. Knutson, *λ-Rings and the Representation Theory of the Symmetric Group*, Lecture Notes in Mathematics, vol. 308, Springer Verlag, 1973.

[1994] N. Kuhn, *Generic representations of the finite general linear groups and the Steenrod algebra*, Am. J. Math. **116** (1994), 327-360.

[1967] P. Landweber, *Cobordism operations and Hopf algebras*, Trans. A.M.S. **27** (1967), 94-110.

[1995] J. Lannes, *Applications dont la source est un classifiant*, Proceedings of the International Congress of Mathematicans: Zurich, 1994, pp. p566-573.

[1992] L. Lomonaco, *Normalized operations in cohomology*, 1990 Barcelona Conference on Algebraic Topology (J. Aguadé, M. Castellet & F.R. Cohen, eds.), Lecture Notes in Mathematics, vol. 1509, Springer-Verlag, 1992, pp. p240-249.

[1971] S. MacLane, *Categories for the Working Mathematician*, Springer Verlag, 1971.

[1979] I.G. Macdonald, *Symmetric Functions and Hall Polynomials*, Oxford Univ. Press, Oxford, 1979.

[1982] B.M. Mann & R.J. Milgram, *On the Chern classes of the regular representations of some finite groups*, Proc. of the Edinburgh Math. Soc. **25** (1982), 259-268.

[1975] I. Madsen, *On the action of the Dyer-Lashof algebra in $H_*(G)$*, Pacific J. Math. **60** (1975), 235-275.

[1979] I. Madsen & R. J. Milgram, *The classifying spaces for surgery and cobordism of manifolds*, Ann. of Math. Studies, vol. 92, Princeton 1979.

[1970] J.P. May, *A general algebraic approach to Steenrod operations*, Lecture Notes in Math., vol. 168, Springer-Verlag, 1970, pp. 153-231.

[1971] J.P. May, *Homology operations on infinite loop spaces*, Proc. Symp. Pure Math. (A. Liulevicius, ed.), vol. XXII, A.M.S., 1971, pp. 171-185.

[1976] J.P. May, *The homology of E_∞-spaces*, The homology of iterated loop spaces (F.R. Cohen, T. J. Lada & J.P. May, eds.), Lecture Notes in Math., vol. 533, Springer, 1976, pp. 1-68.

[1965] R.J. Milgram, *Iterated Loop spaces*, Ann. of Math. **84** (1966), 386-403.

[1987] H. Miller, *The Sullivan conjecture and homotopical representation theory*, Proc. Int. Cong. of Math. 1986: Berkeley, Calif. (A.M. Gleason, ed.), A.M.S., 1987, pp. 580-589.

[1958] J.W. Milnor, *The Steenrod algebra and its dual*, Ann. Math. **67** (1958), 150-171.

[1974] J.W. Milnor & J.D. Stasheff, *Characteristic Classes*, Princeton University Press, 1974.

[1985] J. Morava, *Noetherian localization of categories of cobordism comodules*, Ann. Math. **121** (1985), 1-39.

[1993] J. Morava, *Some examples of Hopf algebras and Tannakian categories*, Contemp. Math. (M.C. Tangora., ed.), Algebraic Topology, Oaxtepec 1991, vol. 146, A.M.S., 1993, pp. 349-359.

[1975] H. Mui, *Modular invariant theory and the cohomology algebras of symmetric spaces*, J. Fac. Sci. Univ. Tokyo **22** (1975), 319-369.

[1983] ———, *Dickson invariants and Milnor basis of the Steenrod algebra*, Eger International Colloquium in Topology, 1983.

[1984] ———, *Homology operations derived from modular coinvariants*, Algebraic topology, Göttingen (L Smith, ed.), Lecture Notes in Math., vol. 1172, 1984, pp. 85-115.

[1957] M. Nakaoka, *Cohomology of symmetric products*, J. Inst. Polyt. **7** (1957), Osaka City Univ., 121-144.

[1960] ———, *Decomposition theorem for homology groups of symmetric groups*, Ann. of Math. **71** (1960), no. 1, 16-42.

[1961] ———, *Homology of the infinite symmetric group*, Ann. of Math. **73** (1961), no. 2, 229-257.

[1982] W. Nichols & M.E. Sweedler, *Hopf algebras and combinatorics*, Umbral Calculus and Hopf Algebra, Contemporary Mathematics, vol. 6, A.M.S., 1982.

[1968] G. Nishida, *Cohomology operations in iterated loopspaces*, Proc. Japan Acad. **44** (1968), 104-109.

[1933] O. Ore, *On a special class of polynomials*, Trans. A.M.S. **35** (1933), 559-584; Correction Trans. A.M.S. **36** (1934), p. 275.

[1972] S. Priddy, *Transfer, symmetric groups, and stable homotopy theory*, Algebraic K-theory I (H. Bass, ed.), Lecture Notes in Math., vol. 341, Springer-Verlag, 1972, pp. 244-255.

[1975] ———, *Dyer-Lashof operations for the classifying spaces of certain matrix groups*, Quart. J. Math. Oxford (3) **26** (1975), 179-193.

[1971] D.G. Quillen, *Elementary proofs of some results of cobordism theory using Steenrod operations*, Adv. in Math. **7** (1971), 29-56.

[1977] D.C. Ravenel & W.S. Wilson, *The Hopf ring for complex cobordism*, J. of Pure and Applied Algebra **9** (1977), 241-280.

[1971] G.C. Rota, *Combinatorial Theory and Invariant Theory*, Notes by L. Guibas, (Summer 1971), Bowdoin College, Maine.

[1994] L. Schwartz, *Unstable modules over the Steenrod algebra and Sullivan's fixed point set conjecture*, U. of Chicago Press, 1994.

[1974] G. Segal, *Categories and cohomology theories*, Topology **13** (1974), 293-312.

[1972] N.E. Steenrod, *Cohomology operations and obstruction to extending continuous functions*, (lectures given in 1957), Adv. in Math. **8** (1972).

[1953] ———, *Homology groups of symmetric groups and reduced power operations*, Proc. Nat. Can. Sci. **39** (1953).

[1957] ———, *Cohomology operations derived from the symmetric groups*, Comment. Math. Helv. **31** (1957), 195-218.

[1962] N.E. Steenrod & D.B.A. Epstein, *Cohomology Operations*, Ann. of Math. Studies, vol. 50, Princeton University Press, 1962.

[1984] R. Steiner, *Homology operations and power series*, Glasgow Math. J. **24** (1984), 161-168.

[1969] M.E. Sweedler, *Hopf Algebras*, W.A. Benjamin, New York, 1969.

[1973] R.M. Switzer, *Homology comodules*, Invent. Math. **20** (1973), 97-102.

[1996] P.R. Turner, *Dickson Coinvariants and the homology of QS^0*, Math. Zeit. (to appear).

[1983] C. Wilkerson, *A primer on the Dickson invariants*, Contemporary Math. (H.R.Miller & S.B.Priddy, eds.), Proc. of the Northwestern homotopy theory conference: 1982, vol. 19, 1983; a revised version of this paper is available on WWW at hopf.math.purdue.edu.

[1980] W.S. Wilson, *Brown-Peterson homology-an introduction and sampler*, A.M.S. Regional Conference Series in Mathematics, vol. 48, 1982.

[1995] R.W. Wood, *Differential operators and the Steenrod algebra*, submitted to London Math. Soc.; See also: *An introduction to the Steenrod algebra through differential operators*, preprint 1995, available at www.LeHigh.edu, the archive of the Lehigh Algebraic Topology Discussion List.

Canisius College, Buffalo, N.Y. (U.S.A).
E-mail address: bisson@canisius.edu

Departement de Mathematiques, UQAM, Montreal, Quebec H3C 3P8
E-mail address: joyal@math.uqam.ca