An Algebraic Introduction to the Steenrod Algebra
Summer School
Interactions Between Invariant Theory and Algebraic Topology
Ioannina, Greece, June 26 – June 30, 2000

Larry Smith

AG-Invariantentheorie

PRELIMINARY

MATHEMATICS SUBJECT CLASSIFICATION : 13A50 Invariant Theory

Typeset by $\mathcal{LS}$TEX

During the month of June 2000 Fred Cohen (University of Rochester, USA) and I, directed, and lectured to, a summer school at the University of Ioannina in Greece. The purpose of the summer school was to make some of the recent developments on the interface of invariant theory and algabraic topology accesible to students. This proved not to be an easy undertaking, and in the year before the summer school, Fred and I spent many hours discussing in person, and weeks exchanging `e-mail` mesages, the problems connected with organizing a coherent program, i.e., selecting from the material with which we were familiar to create a program that hung together well.

One topic that seemed central to our planning was the Steenrod algebra. Beginning with the paper of J. F. Adams and C. W. Wilkerson [1], it has had a significant influence on the development of invariant theory (see e.g. [21], [22], [18], and [17] and their reference lists). This presented us with the problem of explaining the Steenrod algebra to non algebraic topologists in a concise, motivated, and nontechnical[1] algebraic manner. A decade ago at Yale I was confronted with the same problem when teaching a course on invariant theory to an audience consisting primarily of algbraicists, group theorists, and number theorists. I explained how I did this to Fred: the basic idea was to regard the total Steenrod operation as a perturbation of the Frobenius map, and to define the Steenrod algebra as a subalgebra of the endomorphisms of a certain functor gotten from this perturbation.

This got Fred to thinking about some things he was familiar with, which had a similar nature. These he explained to me. In the course of doing so, we found that a common, but not well brought out theme, in many of the topics we felt to be relevent for the summer school, was the structure of a subgroup, or subalgebra, of automorphisms of a functor: generally a simple and easily understood functor, where the subgroup, or subalgebra, had a natural origin. We decided to organize the summer school around this theme.

The purpose of these notes is to provide an introduction to the Steenrod algebra in this manner, i.e., presented as a subalgebra of the algebra of endomorphisms of a functor. The functor assigns to a vector space over a Galois field the algebra of polynomial functions on that vector space, and the subalgebra is specified by means of the Frobenius map.

The material presented here is not new: in fact most of the ideas go back to the middle of the last century, and are to be found in papers of H. Cartan [6], [7], J.-P. Serre [19], R. Thom [28] and Wu-Wen Tsün [33], with one key ingrediant being supplied by S. Bullet and I. Macdonald [5] (see also T.P. Bisson [3]). My contribution, if there is one, is to reorganize the presentation of this material so that no algebraic topology is used, nor is it necessary to assume that the ground field is the prime field. This way of presenting things appeared in print spread through Chapters 10 and 11 of[2] [21]. (See also [20].) For the summer school I collected all this, stripped it of the applications to algebraic topology, and expanded it to include the Hopf algebra structure of the Steenrod algebra due to J.W. Milnor [13] for the prime field.

I have kept these notes to a minimum, and can only encourage the reader to consult the vast literature on the Steenrod algebra. For orientation in this morass the reader can do no better than to consult the excellent survey artical [31]. In addition to the references already mentioned, the course notes from the lectures of Prof. R. Wood at the Summer School [32] in Ioannina provide an excellent list of accesible papers and problems (sic!).

In what follows we adhere to the notations and terminology of [21] and [18]. In particular,

[1] No Eilenberg-MacLane spaces, no $\cup_1$ products, etc.

[2] The emphasis in Chapter 10 of [21] is on certain topological applications: in these notes, and at the summer school in Ioannina, I replaced this with some examples from invariant theory.

if $\mathbb{F}$ is a field and $V = \mathbb{F}^n$ is an n-dimenaional vector space over $\mathbb{F}$, then $\mathbb{F}[V]$ denotes the graded algebra of polynomial functions on V. This may be regarded as the symmetric algebra on the dual vector space V^* of V, where the elements of V^*, the linear forms, have degree 1. Note carefully we ignore the usual topological sign conventions, since graded commutation rules play no role here. (For a discussion of gradings see e.g., [18] Appendix A Section 1.) The correspondence $V \rightsquigarrow \mathbb{F}[V]$ defines a contravariant functor from vector spaces over $\mathbb{F}$ to graded connected algebras, which is at the center of what follows.

§1. The Steenrod Algebra

We fix once and for all a Galois field $\mathbb{F}_q$ of characteristic p containing $q = p^\nu$ elements. Denote by $\mathbb{F}_q[V][[\xi]]$ the power series ring over $\mathbb{F}_q[V]$ in an additional variable ξ, and set $\deg(\xi) = 1 - q$. Define an $\mathbb{F}_q$-algebra homomorphism of degree zero

$$P(\xi) : \mathbb{F}_q[V] \longrightarrow \mathbb{F}_q[V][[\xi]],$$

by requiring

$$P(\xi)(\ell) = \ell + \ell^q \xi \in \mathbb{F}_q[V][[\xi]], \quad \forall \text{ linear forms } \ell \in V^*.$$

For an arbitrary polynomial $f \in \mathbb{F}_q[V]$, we have after separating out homogeneous components, [3]

$$(\star) \qquad P(\xi)(f) = \begin{cases} \sum_{i=0}^{\infty} \mathcal{P}^i(f)\xi^i & \text{if } p \text{ is odd,} \\ \sum_{i=0}^{\infty} \mathrm{Sq}^i(f)\xi^i & \text{if } p = 2. \end{cases}$$

This defines $\mathcal{P}^i$, resp. Sq^i, as $\mathbb{F}_q$-linear maps

$$\mathcal{P}^i, \mathrm{Sq}^i : \mathbb{F}_q[V] \longrightarrow \mathbb{F}_q[V].$$

These maps are functorial in V. The operations $\mathcal{P}^i$, respectively Sq^i, are called **Steenrod reduced power operations**, respectively **Steenrod squaring operations**, or collectively, **Steenrod operations**. In order to avoid a separate notation for the case $p = 2$, with the indulgence of topologists, [4] we set $\mathrm{Sq}^i = \mathcal{P}^i$ for all $i \in \mathbb{N}_0$.

The sums appearing in $(\star)$ are actually finite. In fact $P(\xi)(f)$ is a *polynomial* in ξ of degree $\deg(f)$ with leading coefficient f^q. This means the Steenrod operations acting on $\mathbb{F}_q[V]$ satisfy the **unstability condition**

$$\mathcal{P}^i(f) = \begin{cases} f^q & \text{if } i = \deg(f), \\ 0 & \text{if } i > \deg(f), \end{cases} \quad \forall f \in \mathbb{F}_q[V].$$

Note that these conditions express both a triviality condition, viz., $\mathcal{P}^i(f) = 0$ for all $i > \deg(f)$, and, a nontriviality condition, viz., $\mathcal{P}^{\deg(f)}(f) = f^q$. It is the interplay of these two requirements that seems to endow the unstability condition with the power to yield unexpected consequences.

Next, observe that the multiplicativity of the operator $P(\xi)$ leads to the formulae:

$$\mathcal{P}^k(f'f'') = \sum_{i+j=k} \mathcal{P}^i(f')\mathcal{P}^j(f''), \quad \forall f', f'' \in \mathbb{F}_q[V].$$

These are called the **Cartan formulae** for the Steenrod operations. (N.b., in field theory, a family of operators satisfying these formulae is called a **higher order derivation**. See, e.g., [12] Chapter 4, Section 9.)

---

3 Let me emphasize here, that we will have no reason to consider nonhomogeneous polynomials, and implicitly, we are always assuming, unless the contrary is stated, that all algebras are graded, and if nonnegatively graded, also connected. The algebra $\mathbb{F}[V][[\xi]]$ is graded, but no longer connected.

4 This is **not** the usual topological convention, which would be to set $\mathcal{P}^i = \mathrm{Sq}^{2i}$. This is only relevant for this algebraic approach when it is necessary to bring in a Bockstein operation.

As a simple example of how one can compute with these operations consider the quadratic form

$$Q = x^2 + xy + y^2 \in \mathbb{F}_2[x, y].$$

Let us compute how the Steenrod operations Sq^i act on Q by using linearity, the Cartan formula, and unstability.

$$\begin{aligned}
\mathrm{Sq}^1(Q) &= \mathrm{Sq}^1(x^2) + \mathrm{Sq}^1(xy) + \mathrm{Sq}^1(y^2) \\
&= 2x\mathrm{Sq}^1(x) + \mathrm{Sq}^1(x)\cdot y + x \cdot \mathrm{Sq}^1(y) + 2y\mathrm{Sq}^1(y) \\
&= 0 + x^2y + xy^2 + 0 = x^2y + xy^2, \\
\mathrm{Sq}^2(Q) &= Q^2 = x^4 + x^2y^2 + y^4, \\
\mathrm{Sq}^i(Q) &= 0 \text{ for } i > 2.
\end{aligned}$$

Since the Steenrod operations are natural with respect to linear transformations between vector spaces they induce endomorphisms of the functor

$$\mathbb{F}_q[-] : \mathcal{V}ect_{\mathbb{F}_q} \longrightarrow \mathcal{A}lg_{\mathbb{F}_q}$$

from $\mathbb{F}_q$-vector spaces to commutative graded $\mathbb{F}_q$-algebras. They therefore commute with the action of $\mathrm{GL}(V)$ on $\mathbb{F}_q[V]$. If $G \hookrightarrow \mathrm{GL}(n, \mathbb{F}_q)$ is a faithful representation of a finite group G then the Steenrod operations restrict to the ring of invariants $\mathbb{F}_q[V]^G$, i.e., map invariant forms to invariant forms. Hence they can be used to produce new invariants from old ones. This is a new feature of invariant theory over finite fields as opposed to arbitrary fields (but do see in this connection [10]). Here is an example to illustrate this. It is based on a result, and the methods of [23].

EXAMPLE 1: Let $\mathbb{F}_q$ be the Galois field with q elements of odd characteristic p, and consider the action of the group $\mathrm{SL}(2, \mathbb{F}_q)$ on the space of binary quadratic forms over $\mathbb{F}_q$ by change of variables. A typical such form is $Q(x, y) = ax^2 + 2bxy + cy^2$.

$$\mathbf{T}_Q = \begin{bmatrix} a & b \\ b & c \end{bmatrix}$$

The space of such forms can be identified with the vector space $\mathrm{Mat}^{\mathrm{sym}}_{2,2}(\mathbb{F}_q)$ of 2×2 symmetric matrices over $\mathbb{F}_q$. Under this identification the form Q corresponds to the matrix $\mathbf{T}_Q$ at the left, and the action of $\mathrm{SL}(2, \mathbb{F}_q)$ is given by $\mathbf{T}_Q \longmapsto \mathbf{S}\mathbf{T}_Q\mathbf{S}^{\mathrm{tr}}$, where $\mathbf{S} \in \mathrm{SL}(2, \mathbb{F}_q)$, with $\mathbf{S}^{\mathrm{tr}}$ the transpose of $\mathbf{S}$. The element $-\mathbf{I} \in \mathrm{SL}(2, \mathbb{F}_q)$ acts trivially. By dividing out the subgroup it generates, we receive a faithful representation of $\mathrm{PSL}(2, \mathbb{F}_q) = \mathrm{SL}(2, \mathbb{F}_q)/\{\pm\mathbf{I}\}$ on the space of binary quadratic forms. This group has order $q(q^2-1)/2$.

The action of $\mathrm{PSL}(2, \mathbb{F}_q)$ on $\mathrm{Mat}^{\mathrm{sym}}_{2,2}(\mathbb{F}_q)$ preserves the quadratic form $\det : \mathrm{Mat}^{\mathrm{sym}}_{2,2}(\mathbb{F}_q) \longrightarrow \mathbb{F}_q$ and since there is only one, up to isomorphism, nonsingular quadratic form in 3 variables over $\mathbb{F}_q$ (cf., [9] §169–173), we receive an unambiguous faithful representation $\rho : \mathrm{PSL}(2, \mathbb{F}_q) \hookrightarrow \mathbb{O}(3, \mathbb{F}_q)$. Denote by

$$\begin{bmatrix} x & y \\ y & z \end{bmatrix} \in \mathrm{Mat}^{\mathrm{sym}}_{2,2}(\mathbb{F}_q)^*$$

a generic linear form on the dual space of the 2×2 symmetric matrices over $\mathbb{F}_q$. Per definition the quadratic form

$$\det = xz - y^2 \in \mathbb{F}_q[\mathrm{Mat}^{\mathrm{sym}}_{2,2}(\mathbb{F}_q)] = \mathbb{F}_q[x, y, z]$$

is $\mathbb{O}(3, \mathbb{F}_q)$-invariant. If we apply the first Steenrod operation to this form we receive the new invariant form of degree $q+1$, viz.,

$$\mathcal{P}^1(\det) = x^qz + xz^q - 2y^{q+1} \in \mathbb{F}_q[x, y, z]^{\mathbb{O}(3,\mathbb{F}_q)}.$$

The full ring of invariants of the orthogonal group $\mathbb{O}(3, \mathbb{F}_q)$ is known (see, e.g., [8] or [23]). To wit

$$\mathbb{F}_q[x, y, z]^{\mathbb{O}(3,\mathbb{F}_q)} \cong \mathbb{F}_q[\det, \mathcal{P}^1(\det), \mathbf{E}_{\det}].$$

Here $\mathbf{E}_{\det}$ is the Euler class (see e.g. [26] or [18] Chapter 4) associated to the configuration of linear forms defining the set of external lines to the projective variety $\mathfrak{X}_{\det}$ in the projective plane $\mathbb{PF}_q(2)$ over $\mathbb{F}_q$ defined by the vanishing of the determinant [5] (see [11] Section 8.2 and [23]). The form $\mathbf{E}_{\det}$ has degree $q(q-1)$. The three forms det, $\mathcal{P}^1(\det)$, $\mathbf{E}_Q \in \mathbb{F}_q[x, y, z]^{\mathbb{O}(3,\mathbb{F}_q)}$ are a system of parameters [23].. Since the product of their degrees is $|\mathbb{O}(3, \mathbb{F}_q)|$ it follows from [21] Proposition 5.5.5 that $\mathbb{F}_q[x, y, z]^{\mathbb{O}(3,\mathbb{F}_q)}$ must be a polynomial algebra as stated.

The pre-Euler class $\mathbf{e}_{\det}$ of the set of external projective lines to $\mathfrak{X}_{\det}$ is an $\mathbb{O}(3, \mathbb{F}_q)$ det-relative invariant, so is $\mathbb{SO}(3, \mathbb{F}_q)$-invariant. It has degree $\binom{q}{2}$, and together with the forms det and $\mathcal{P}^1(\det)$ it forms a system of parameters for $\mathbb{F}_q[x, y, z]^{\mathbb{SO}(3,\mathbb{F}_q)}$, so again we may apply Proposition 5.5.5 and conclude that $\mathbb{F}_q[x, y, z]^{\mathbb{SO}(3,\mathbb{F}_q)}$ is a polynomial algebra, viz., $\mathbb{F}_q[x, y, z]^{\mathbb{SO}(3,\mathbb{F}_q)} = \mathbb{F}_q[\det, \mathcal{P}^1(\det), \mathbf{e}_{\det}]$.

Finally, $\mathrm{PSL}(2, \mathbb{F}_q)$ is the commutator subgroup of $\mathbb{SO}(3, \mathbb{F}_q)$ and has index 2 in $\mathbb{SO}(3, \mathbb{F}_q)$, so by a Proposition in [25] the ring of invariants of $\mathrm{PSL}(2, \mathbb{F}_q)$ acting on the space of binary quadratic forms is a hypersurface. It has generators det, $\mathcal{P}^1(\det)$, $\mathbf{e}_{\det}$ and a certain form ω which satisfies a monic quadratic equation over the subalgebra generated by the first three. A choice for ω is the pre-Euler class of the configuration of interior projective lines to the variety $\mathfrak{X}_{\det} \subset \mathbb{PF}(3)$.

The Steenrod operations can be collected together to form an algebra, in fact a Hopf algebra (see Section 4), over the Galois field $\mathbb{F}_q$.

DEFINITION: The **Steenrod algebra** $\mathcal{P}^*(\mathbb{F}_q)$ is the $\mathbb{F}_q$-subalgebra of the endomorphism algebra of the functor $\mathbb{F}_q[-]$, generated by $\mathcal{P}^0 = 1, \mathcal{P}^1, \mathcal{P}^2, \ldots$

NOTATION: In most situations, such as here, the ground field $\mathbb{F}_q$ is fixed at the outset, and we therefore abreviate $\mathcal{P}^*(\mathbb{F}_q)$ to $\mathcal{P}^*$.

The next sections develop the basic algebraic structure of the Steenrod algebra

§2. The Adem-Wu Relations

The Steenrod algebra is by no means freely generated by the Steenrod reduced powers. For example, when $p=2$ it is easy to check that $\mathrm{Sq}^1\mathrm{Sq}^1=0$ by verifying this is the case for monomials $z^E = z_1^{e_1}, \ldots, z_n^{e_n}$: to do so one needs the formula, valid for any linear form, $\mathrm{Sq}^1(z^k) = kz^{k+1}$, which follows by induction immediately from the Cartan formula. [6]

Traditionally, relations between the Steenrod operations are expressed as commutation rules for $\mathcal{P}^i\mathcal{P}^j$, respectively $\mathrm{Sq}^i\mathrm{Sq}^j$. These commutation relations are called **Adem-Wu relations.** In the case of the prime field $\mathbb{F}_p$ they were originally conjectured by Wu Wen-Tsün based on his study of the mod p cohomology of Grassmann manifolds [33] and proved by J. Adem in [2], H. Cartan in [6], and for $p = 2$ by J.-P. Serre in [19]. These relations are usually written as follows:

$$\mathcal{P}^i\mathcal{P}^j = \sum_{k=0}^{[i/q]}(-1)^{i-qk}\binom{(q-1)(j-k)-1}{i-qk}\mathcal{P}^{i+j-k}\mathcal{P}^k \quad \forall\, i, j \geq 0,\, i < qj.$$

Note for any Galois field $\mathbb{F}_q$ the coefficients are still elements in the prime subfield $\mathbb{F}_p$ of $\mathbb{F}_q$.

The proof of these relations is greatly simplified by the **Bullett-Macdonald identity**, which provides us with a well-wrapped description of the relations among the Steenrod operations, [5]. To describe this identity, as in [5], extend $P(\xi)$ to a ring homomorphism $P(\xi)$:

---

5 The projective plane of $\mathbb{F}_q$ is defined by $\mathbb{PF}_q(2) = (\mathbb{F}_q^3 \setminus \{0\})^{\mathbb{F}^\times}$ where $\mathbb{F}^\times$ acts via scalar multiplication on the vectors of $\mathbb{F}_q^3$ In this discussion we are identifying $\mathbb{F}_q^3$ with $\mathrm{Mat}_{2,2}^{\mathrm{sym}}(\mathbb{F}_q)$, so this is the same as the set of lines through the origin in $\mathrm{Mat}_{2,2}^{\mathrm{sym}}$. The pre-Euler class $\mathbf{e}_{\det}$ may be taken to be the product of a set of linear forms $\{\ell_L\}$, indexed by the $\binom{q}{2}$ external lines $\{L\}$ to $\mathfrak{X}_{\det}$, and satisfying $\ker(\ell_L) = L$. The Euler class $\mathbf{E}_{\det}$ is its square.

6 In fact every element in the Steenrod algebra is nilpotent: but the index of nilpotence is known only in a few cases, see e.g. [15], [16], [29], [30] and [31] for a resumé of what is known.

$\mathbb{F}[V][\eta] \longrightarrow \mathbb{F}[V][\eta][\xi]$ by setting $P(\xi))(\eta) = \eta$. Next, set $u = (1-t)^{q-1} = 1 + t + \cdots + t^{q-1}$ and $s = tu$. Then the Bullet-Macdonald identity is

$$P(s) \circ P(1) = P(u) \circ P(t^q).$$

Since $P(\xi)$ is additive and multiplicative, it is enough to check this equation for the basis elements of V^*, which is indeed a short calculation. Rumor says, Macdonald, like most of us, could not remember the coefficients that appear in the Adem relations, so devised this identity so that he could derive them on the spot when J. F. Adams came to talk with him.

REMARK: For $p = 2$ T.P. Bisson has pointed out (see [4]) that the Bullet-Macdonald may be viewed as a commutation rule, viz., $P(\xi)P(\eta) = P(\eta)P(\xi)$. For a general Galois $\mathbb{F}_q$, one needs to demand $\mathrm{GL}(2, \mathbb{F}_q)$-invariance of $P(\zeta)$, where $\zeta \in \mathrm{Span}_{\mathbb{F}_q}\{\xi, \eta\}$.

To derive the Adem-Wu relations we provide details for the residue computation [7] sketched in [5]. First of all, direct calculation gives:

$$P(s)P(1) = \sum_{a,\, k} s^a \wp^a \wp^k$$

$$P(u)P(t^q) = \sum_{a,\, b,\, j} u^{a+b-j} t^{qj} \wp^{a+b-j} \wp^j$$

which the Bullett-Macdonald identity says are equal. Recall from complex analysis that

$$\frac{1}{2\pi i} \oint_\gamma z^m dz = \begin{cases} 1 & m = -1 \\ 0 & \text{otherwise} \end{cases}$$

where γ is a small circle around $0 \in \mathbb{C}$. Therefore we obtain

$$\begin{aligned}
\sum_k \wp^a \wp^k &= \frac{1}{2\pi i} \oint_\gamma \frac{P(s)P(1)}{s^{a+1}} ds \\
&= \frac{1}{2\pi i} \oint_\gamma \frac{P(u)P(t^q)}{s^{a+1}} ds \\
&= \frac{1}{2\pi i} \sum_{a,\, b,\, j} \oint_\gamma \frac{u^{a+b-j} t^{qj}}{s^{a+1}} ds \wp^{a+b-j} \wp^j
\end{aligned}$$

The formula $s = t(1-t)^{q-1}$ gives $ds = (1-t)^{q-2}(1-qt)dt$, so substituting gives

$$\begin{aligned}
\frac{u^{a+b-j} t^{qj}}{s^{a+1}} ds &= \frac{(1-t)^{(q-1)(a+b-j)} t^{qj} (1-t)^{q-2}(1-qt)}{\left[t(1-t)^{q-1}\right]^{a+1}} dt \\
&= (1-t)^{(b-j-1)(q-1)+(q-2)} t^{qj-a-1}(1-qt)dt \\
&= (1-t)^{((b-j)(q-1)-1)} t^{qj-a-1}(1-qt)dt \\
&= \left[\sum_k (-1)^k \binom{(b-j)(q-1)-1}{k} t^k\right] t^{qj-a-1}(1-qt)dt \\
&= \sum_k (-1)^k \binom{(b-j)(q-1)-1}{k} \left[t^{k+qj-a-1} - qt^{k+qj-a}\right] d\,t.
\end{aligned}$$

Therefore

$$\begin{aligned}
\wp^a \wp^b &= \sum_j \left[\frac{1}{2\pi i} \oint_\gamma \frac{u^{a+b-j} t^{qj}}{s^{a+1}} ds\right] \wp^{a+b-j} \wp^j \\
&= \sum_j \frac{1}{2\pi i} \oint \sum_k (-1)^k \binom{(b-j)(q-1)-1}{k} \left[t^{k+qj-a-1} - qt^{k+qj-a}\right] dt \wp^{a+b-j} \wp^j.
\end{aligned}$$

[7] The following discussion is based on conversations with E.H. Brown Jr. I do hope I have come close to getting the indices correct for once.

Only the terms where

$$k + qj - a - 1 = -1 \quad (k = a - qj)$$
$$k + qj - a = -1 \quad (k = a - qj - 1)$$

contribute anything to the sum, so

$$\mathcal{P}^a \mathcal{P}^b = \sum_j \left[(-1)^{a-qj)} \binom{(b-j)(q-1)-1}{a-qj} + (-1)^{a-qj-1} q \binom{(b-j)(q-1)-1}{a-qj-1} \right] \mathcal{P}^{a+b-j}\mathcal{P}^j$$

and since

$$\binom{(b-j)(q-1)-1}{a-qj} - q\binom{(b-j)(q-1)-1}{a-qj-1} \equiv \binom{(b-j)(q-1)-1}{a-qj} \bmod p$$

we conclude

$$\mathcal{P}^a \mathcal{P}^b = \sum_j (-1)^{a-qj} \binom{(b-j)(q-1)-1}{a-qj} \mathcal{P}^{a+b-j}\mathcal{P}^j.$$

Thus there is a surjective map from the free associative algebra with 1 generated by the Steenrod operations modulo the ideal generated by the Adem-Wu relations,

$$\mathcal{P}^a \mathcal{P}^b - \sum_j (-1)^{a-qj} \binom{(b-j)(q-1)-1}{a-qj} \mathcal{P}^{a+b-j}\mathcal{P}^j \quad a, b \in \mathbb{N} \text{ and } a < qb,$$

onto the Steenrod algebra. Denote this quotient algebra by $\mathcal{B}^*$. In fact, this map, $\mathcal{B}^* \longrightarrow \mathcal{P}^*$ is an isomorphism, so the Adem-Wu relations are a complete set of defining relations for the Steenrod algebra. The proof of this, and some of its consequences, is the subject of the next section.

§3. The Basis of Admissible Monomials

In this section we show that the relations between Steenrod operations that are universally valid all follow from the Adem-Wu relations. To do so we extend some theorems of of H. Cartan, [6], J.-P. Serre, [19], and Wu Wen Tsün, [33] from the case of the prime field to arbitrary Galois fields. We also rearrange their proofs so that they do not make any direct use of topology.

An **index sequence** is a sequence $I = (i_1, i_2, \ldots, i_k, \ldots)$ of nonnegative integers, almost all of which are zero. If I is an index sequence we denote by $\mathcal{P}^I \in \mathcal{P}^*$ the monomial $\mathcal{P}^{i_1} \cdot \mathcal{P}^{i_2} \ldots \mathcal{P}^{i_k} \ldots$ in the Steenrod operations $\mathcal{P}^i$, with the convention that trailing 1s are ignored. The degree of the element $\mathcal{P}^I$ is $(q-1)(j_1 + j_2 + \cdots + j_k + \cdots)$. These iterations of Steenrod operations are called **basic monomials**. An index sequence I is called **admissible** if $i_s \geq q i_{s+1}$ for $s = 1, \ldots$. We call k the **length** of I if $i_k \neq 0$ but $i_s = 0$ for $s > k$. Write $\ell(I)$ for the length of I. It is often convenient to treat an index sequence as a finite sequence of nonnegative integers by truncating it to $\ell(I)$ entries.

A basic monomial is defined to be **admissible** if the corresponding index sequence is admissible. The strategy of H. Cartan and J.-P. Serre to show that the Adem-Wu relations are a complete set of defining relations for the Steenrod algebra is to prove that the admissible monomials are an $\mathbb{F}_q$ basis for $\mathcal{P}^*$.

Recall that $\mathcal{B}^*$ denotes the free, graded, associative algebra generated by the symbols $\mathcal{P}^k$ modulo the ideal spanned by the Adem-Wu relations. We have a surjective map $\mathcal{B}^* \longrightarrow \mathcal{P}^*$, and so with his notation our goal is to prove:

THEOREM 3.1: *The admissible monomials span $\mathcal{B}^*$ as an $\mathbb{F}_p$-vector space. The images of the admissible monomials in the Steenrod algebra are linearly independent.*

PROOF: We begin by showing that the admissible monomials span $\mathscr{B}^*$.

For a sequence $I = (i_1, i_2, \ldots, i_k)$, the **moment** of I, denoted by $m(I)$, is defined by $m(I) = \sum_{s=1}^{k} s \cdot i_s$. We first show that an inadmissible monomial is a sum of monomials of smaller moment. Granted this it follows by induction over the moment that the admissible monomials span $\mathscr{B}^*$.

Suppose that $\wp^I$ is an inadmissible monomial. Then there is a smallest s such that $i_s < q i_{s+1}$, i.e.,

$$\wp^I = \mathscr{Q}' \wp^{i_s} \wp^{i_{s+1}} \mathscr{Q}''$$

where $\mathscr{Q}'$, $\mathscr{Q}''$ are basic monomials, and $\mathscr{Q}'$ is admissible. It is therefore possible to apply an Adem-Wu relation to $\wp^I$ to obtain

$$\wp^I = \sum_j a_j \mathscr{Q}' \wp^{i_s + i_{s+1} - j} \wp^j \mathscr{Q}''$$

for certain coefficients $a_j \in \mathbb{F}_p$. The terms on the right hand side all have smaller moment than $\wp^I$, and so, by induction on s we may express $\wp^I$ as a sum of admissible monomials. (N.b. The admissible monomials are *reduced* in the sense that no Adem-Wu relation can be applied to them.)

We next show that the admissible monomials are linearly independent as elements of the Steenrod algebra $\mathscr{P}^*$. This we do by adapting an argument of J.-P. Serre [19] and H. Cartan [6] which makes use of a formula of Wu Wen-Tsün.

Let $e_n = x_1 x_2 \cdots x_n \in \mathbb{F}_q[x_1, \ldots, x_n]$ be the n-th elementary symmetric function. Then,

$$\begin{aligned} P(\xi)(e_n) &= P(\xi)(\prod_{i=1}^{n} x_i) = \prod_{i=1}^{n} P(\xi)(x_i) \\ &= \prod_{i=1}^{n}(x_i + x_i^q \xi) = \prod_{i=1}^{n} x_i \cdot \prod_{i=1}^{n}(1 + x_i^{q-1}\xi) \\ &= e_n(x_1, \ldots, x_n) \cdot \left(\sum_{i=1}^{n} e_i(x_1^{p-1}, \ldots, x_n^{q-1})\xi^i \right), \end{aligned}$$

where $e_i(x_1, \ldots, x_n)$ denotes the i-th elementary symmetric polynomial in $x_1, \ldots, x_n$. So we have obtained a formula of Wu Wen-Tsün:

$$\wp^i(e_n) = e_n \cdot e_i(x_1^{p-1}, \ldots, x_n^{q-1}).$$

We claim that the monomials

$$\left\{ \wp^I \mid \wp^I \text{ admissible and } \deg(\wp^I) \leq 2n \right\}$$

are linearly independent in $\mathbb{F}_q[x_1, \ldots, x_n]$. To see this note that in case $\ell(I) \leq n$, each entry in I is at most n (so the following formula makes sense), and

$$\wp^I(e_n) = e_n \cdot \prod_{j=1}^{s} e_{i_j}(x_1^{q-1}, \ldots, x_n^{q-1}) + \ldots$$

where $I = (i_1, \ldots, i_s)$, $\wp^I = \wp^{i_1} \cdots \wp^{i_s}$ and the remaining terms are lower in the lexicographic ordering on monomials. So $e_n \cdot \prod_{j=1}^{s} e_{i_j}(x_1^{q-1}, \ldots, x_n^{q-1})$ is the largest monomial in $\wp^I(e_n)$ in the lexicographic order. Thus

$$\left\{ \wp^I(e_n) \mid \wp^I \text{ admissible and } \deg(\wp^I) \leq 2n \right\},$$

have distinct largest monomials, so are linearly independent.

By letting $n \longrightarrow \infty$ we obtain the assertion, completing the proof. □

Thus the Steenrod algebra may be regarded (this is one traditional definition) as the graded free associative algebra with 1 generated by the Sq^i respectively $\mathcal{P}^i$ modulo the ideal generated by the Adem-Wu relations. This means we have proven:

THEOREM 3.2: *The Steenrod algebra $\mathcal{P}^*$ is the free associative $\mathbb{F}_q$-algebra generated by the reduced power operations $\mathcal{P}^0, \mathcal{P}^1, \mathcal{P}^2, \ldots$ modulo the Adem-Wu relations.* □

COROLLARY 3.3: *The admissible monomials are an $\mathbb{F}_q$-basis for the Steenrod algebra $\mathcal{P}^*$.* □

Since the coefficients of the Adem-Wu relations lie in the prime field $\mathbb{F}_p$, the operations $\mathcal{P}^{p^i}$ for $i \geq 0$ are indecomposables in $\mathcal{P}^*$. In particular, over the Galois field $\mathbb{F}_q$, the Steenrod algebra $\mathcal{P}^*$ is **not** generated by the operations $\mathcal{P}^{q^i}$ for $i \geq 0$: one needs all $\mathcal{P}^{p^i}$ for $i \geq 0$. This will become even clearer after we have developed the Hopf algebra structure of $\mathcal{P}^*$ in the next section.

EXAMPLE 1: Consider the polynomial algebra $\mathbb{F}_2[Q, T]$ over the field with 2 elements, where the indeterminate Q has degree 2 and T has degree 3. If the Steenrod algebra were to act unstably on this algebra then the unstability condition would determine $\mathrm{Sq}^i(Q)$ and $\mathrm{Sq}^j(T)$ apart from $i = 1$ and $j = 1$ and 2. If we specify these as follows

$$\mathrm{Sq}^1(Q) = T, \quad \mathrm{Sq}^1(T) = 0, \quad \mathrm{Sq}^2(T) = QT,$$

and demand that the Cartan formula hold, then using these formulae we can compute Sq^k on any monomial, and hence by linearity, on any polynomial in Q and T. For example

$$\mathrm{Sq}^1(QT) = \mathrm{Sq}^1(Q) \cdot T + Q \cdot \mathrm{Sq}^1(T) = T^2 + 0 = T^2,$$

and so on. Note that since $\mathrm{Sq}^1 \cdot \mathrm{Sq}^1 = 0$ is an Adem-Wu relation, $\mathrm{Sq}^1(T) = 0$ is forced from $\mathrm{Sq}^1(Q) = T$. To verify the unstability conditions, suppose that

$$\mathrm{Sq}^a \mathrm{Sq}^b = \sum_{c=0}^{[\frac{a}{2}]} \binom{b-1-c}{a-2c} \mathrm{Sq}^{a+b-c}\mathrm{Sq}^c, \qquad 0 < a < 2b,$$

is an Adem-Wu relation. We need to show that

$$\left(\mathrm{Sq}^a \mathrm{Sq}^b - \sum_{c=0}^{[\frac{a}{2}]} \binom{b-1-c}{a-2c} \mathrm{Sq}^{a+b-c}\mathrm{Sq}^c \right) (Q^i T^j) = 0$$

for all $i, j \in \mathbb{N}_0$. By a simple argument using the Cartan formulae, see, e.g., [27] Lemma 4.1, it is enough to verify that these hold for the generators Q and T, and this is routine. It is a bit more elegant to identify Q with $x^2 + xy + y^2$ and T with $x^2y + xy^2 \in \mathbb{F}_2[x, y]$. The action of the Steenrod operations on Q and T then coincides with the restriction of the action from $\mathbb{F}_2[x, y]$. This way, it is then clear that $\mathbb{F}_2[Q, T]$ is an unstable algebra over the Steenrod algebra, because with some topological background we recognize this as just $H^*(B\mathbb{SO}(3); \mathbb{F}_2)$.

§4. The Hopf Algebra Structure of the Steenrod Algebra

Our goal in this section is to complete the traditional picture of the Steenrod algebra by proving that $\mathcal{P}^*(\mathbb{F}_q)$ is a Hopf algebra [8] and extending Milnor's Hopf algebra [13] structure theorems from the prime field $\mathbb{F}_p$ to an arbitrary Galois field. It should be emphasized that this requires no new ideas, only a careful redoing of Milnor's proofs avoiding reference to algebraic topology and cohomology operations, and carefully replacing p by q where appropriate.

[8] One quick way to do this is to write down as comultiplication map

$$\nabla(\mathcal{P}^k) = \sum_{i+j=k} \mathcal{P}^i \otimes \mathcal{P}^j, \quad k = 1, 2, \ldots,$$

and verify that it is compatible with the Bullett-Macdonald identity, and hence also with the Adem-Wu relations.

PROPOSITION 4.1: *Let p be a prime integer, $q = p^{\nu}$ a power of p, and $\mathbb{F}_q$ the Galois field with q elements. Then the Steenrod algebra of $\mathbb{F}_q$ is a cocommutative Hopf algebra over $\mathbb{F}_q$ with respect to the coproduct*

$$\nabla : \mathscr{P}^* \longrightarrow \mathscr{P}^* \otimes \mathscr{P}^*$$

defined by the formulae

$$\nabla(\mathcal{P}^k) = \sum_{i+j=k} \mathcal{P}^i \otimes \mathcal{P}^j, \quad k = 1, 2, \ldots .$$

PROOF: Consider the functor $V \rightsquigarrow \mathbb{F}_q[V] \otimes \mathbb{F}_q[V]$ that assigns to a finite dimensional vector space V over $\mathbb{F}_q$ the commutative graded algebra $\mathbb{F}_q[V] \otimes \mathbb{F}_q[V]$ over $\mathbb{F}_q$. There is a natural map of algebras

$$\mathscr{P}^* \otimes \mathscr{P}^* \longrightarrow \mathrm{End}(V \rightsquigarrow \mathbb{F}_q[V] \otimes \mathbb{F}_q[V])$$

given by the tensor product of endomorphisms. Since there is an isomorphism $\mathbb{F}_q[V] \otimes \mathbb{F}_q[V] \cong \mathbb{F}_q[V \oplus V]$, that is natural in V, the functor $\mathrm{End}(V \rightsquigarrow \mathbb{F}_q[V] \otimes \mathbb{F}_q[V])$ is a subfunctor of the functor $\mathrm{End}(V \rightsquigarrow \mathbb{F}_q[V])$ that assigns to a finite dimensional vector space V over $\mathbb{F}_q$ the polynomial algebra $\mathbb{F}_q[V]$. Hence restriction defines a map of algebras

$$\mathscr{P}^* \longrightarrow \mathrm{End}(V \rightsquigarrow \mathbb{F}_q[V] \otimes \mathbb{F}_q[V])$$

and we obtain a diagram of algebra homomorphisms

$$\begin{array}{ccc} & & \mathscr{P}^* \otimes \mathscr{P}^* \\ & \nearrow & \downarrow \tau \\ \mathscr{P}^* & \xrightarrow{\rho} & \mathrm{End}(V \rightsquigarrow \mathbb{F}_q[V] \otimes \mathbb{F}_q[V]) \end{array}$$

What we need to show is that $\mathrm{Im}(\rho) \subseteq \mathrm{Im}(\tau)$, for since τ is monic $\nabla = \tau^{-1}\rho$ would define the desired coproduct. Since $\mathcal{P}^k$ for $k = 1, 2, \ldots,$ generate $\mathscr{P}^*$ it is enough to check that $\rho(\mathcal{P}^k) \in \mathrm{Im}(\tau)$ for $k = 1, 2, \ldots,$. But this is immediate from the Cartan formula. Since ∇ is a map of algebras the Hopf condition is satisfied, so $\mathscr{P}^*$ is a Hopf algebra. $\square$

If J is an admissible index sequence then

$$e(J) = \sum_{s=1}^{\infty} (j_s - q j_{s+1})$$

is called the **excess** of J. For example, the sequences

$$M_k = (q^{k-1}, \ldots, q, 1), \quad k = 1, 2, \ldots$$

are all the admissible sequences of excess zero. Note that

$$\deg(\mathcal{P}^{M_k}) = \sum_{j=1}^{k} q^{k-j}(q-1) = q^k - 1, \quad \text{for } k = 1, 2, \ldots .$$

Recall by Corollary 3.3 that the admissible monomials are an $\mathbb{F}_q$-vector space basis for $\mathscr{P}^*$. Let $\mathscr{P}_*(\mathbb{F}_q)$ denote the Hopf algebra dual to the Steenrod algebra $\mathscr{P}^*(\mathbb{F}_q)$. We define $\xi_k \in \mathscr{P}_*(\mathbb{F}_q)$ to be dual to the monomial $\mathcal{P}^{M_k} = \mathcal{P}^{q^{k-1}} \cdots \mathcal{P}^q \cdot \mathcal{P}^1$ with respect to the basis of admissible monomials for $\mathscr{P}^*$. This means that we have:

$$<\mathcal{P}^J \mid \xi_k> = \begin{cases} 1 & \text{if } J = M_k, \\ 0 & \text{otherwise,} \end{cases}$$

where we have written $<\mathcal{P} \mid \xi>$ for the value of an element $\mathcal{P} \in \mathscr{P}^*(\mathbb{F}_q)$ on an element $\xi \in \mathscr{P}_*(\mathbb{F}_q)$. Note that $\deg(\xi_k) = q^k - 1$ for $k = 1, \ldots,$.

If $I = (i_1, i_2, \ldots, i_k, \ldots)$ is an index sequence we call ℓ the **length** of I, denoted by $\ell(I)$, if $i_k = 0$ for $k > \ell$, but $i_\ell \neq 0$. We associate to an index sequence $I = (i_1, i_2, \ldots, i_k, \ldots)$ the element $\xi^I = \xi_1^{i_1} \cdot \xi_2^{i_2} \cdots \xi_\ell^{i_\ell} \in \mathscr{P}_*(\mathbb{F}_q)$, where $\ell = \ell(I)$. Note that

$$\deg(\xi^I) = \sum_{s=1}^{\ell(I)} i_s(q^s - 1).$$

To an index sequence $I = (i_1, i_2, \ldots, i_k, \ldots)$ we also associate an admissible sequence $J(I) = (j_1, j_2, \ldots, j_k, \ldots)$ defined by

$$(\circledast) \qquad j_1 = \sum_{s=1}^{\infty} i_s q^{s-1}, \quad j_2 = \sum_{s=2}^{\infty} i_s q^{s-2}, \ldots, \quad j_k = \sum_{s=k}^{\infty} i_s q^{s-k}, \ldots.$$

It is easy to verify that as I runs over all index sequences that $J(I)$ runs over all admissible sequences. Finally, note that $\deg(\mathscr{P}^{J(I)}) = \deg(\xi^I)$ for any index sequence I.

The crucial observation used by Milnor to prove the structure theorem of $\mathscr{P}_*(\mathbb{F}_q)$ is that the pairing of the admissible monomial basis for $\mathscr{P}^*(\mathbb{F}_q)$ against the monomials in the ξ_k is upper triangular. To formulate this precisely we order the index sequences lexicographically from the right, so for example $(1, 2, 0, \ldots) \prec (0, 0, 1, \ldots)$.

LEMMA 4.2 (J. W. Milnor): *With the preceding notations we have that the inner product matrix* $<\mathscr{P}^{J(I)} \mid \xi^K>$ *is upper triangular with* 1*s on the diagonal, i.e.,*

$$<\mathscr{P}^{J(I)} \mid \xi^K> = \begin{cases} 1 & \text{if } I = K, \\ 0 & \text{if } I < K. \end{cases}$$

PROOF: Let the length of K be ℓ and define $K' = (k_1, k_2, \ldots, k_{\ell-1})$, so

$$\xi^K = \xi^{K'} \cdot \xi_\ell \in \mathscr{P}_*(\mathbb{F}_q).$$

If ∇ denotes the coproduct in $\mathscr{P}^*(\mathbb{F}_q)$, then we have the formula

$$(\div) \qquad <\mathscr{P}^{J(I)} \mid \xi^K> = <\mathscr{P}^{J(I)} \mid \xi^{K'} \cdot \xi_\ell> = <\nabla(\mathscr{P}^{J(I)}) \mid \xi^{K'} \otimes \xi_\ell>$$

If $J(I) = (j_1, j_2, \ldots, j_k, \ldots)$ then one easily checks that

$$\nabla(\mathscr{P}^{J(I)}) = \sum_{J'+J''=J(I)} \mathscr{P}^{J'} \otimes \mathscr{P}^{J''}.$$

Substituting this into $(\div)$ gives

$$(\boxplus) \qquad <\mathscr{P}^{J(I)} \mid \xi^K> = \sum_{J'+J''=J(I)} <\mathscr{P}^{J'} \mid \xi^{K'}> \cdot <\mathscr{P}^{J''} \mid \xi_\ell>.$$

By the definition of ξ_ℓ we have

$$<\mathscr{P}^{J''} \mid \xi_\ell> = \begin{cases} 1 & \text{if } J'' = M_\ell, \\ 0 & \text{otherwise.} \end{cases}$$

If $J'' = M_\ell$ then unravelling the definitions shows that $J' = J(I')$, for a suitable I', so if K and I have the same length ℓ, we have shown

$$<\mathscr{P}^{J(I)} \mid \xi^K> = <\mathscr{P}^{J(I')} \mid \xi^{K'}>,$$

and hence it follows from induction over the degree that

$$<\mathscr{P}^{J(I)} \mid \xi^K> = \begin{cases} 1 & \text{if } I = K, \\ 0 & \text{if } I < K. \end{cases}$$

If, on the other hand, $\ell(I) < \ell$ then all the terms

$$<\mathscr{P}^{J''} \mid \xi_\ell>$$

in the sum $(\boxplus)$ are zero and hence that $<\mathscr{P}^{J(I)} \mid \xi^K> = 0$ as required. □

THEOREM 4.3: *Let p be a prime integer, $q = p^\nu$ a power of p, and $\mathbb{F}_q$ the Galois field with q elements. Let $\mathscr{P}_*(\mathbb{F}_q)$ denote the dual Hopf algebra to the Steenrod algebra of the Galois field $\mathbb{F}_q$. Then, as an algebra*

$$\mathscr{P}_* \cong \mathbb{F}_q[\xi_1, \ldots, \xi_k, \ldots],$$

where $\deg(\xi_k) = q^k - 1$ for $k \in \mathbb{N}$. The coproduct is given by the formula

$$\nabla_*(\xi_k) = \sum_{i+j=k} \xi_i^{q^j} \otimes \xi_j, \quad k = 1, 2, \ldots.$$

PROOF: By Milnor's Lemma (Lemma 4.2) the monomials $\{\xi^I\}$ where I ranges over all index sequences are linearly independent in $\mathscr{P}_*(\mathbb{F}_q)$. Hence $\mathbb{F}_q[\xi_1, \ldots, \xi_k, \ldots] \subseteq \mathscr{P}_*(\mathbb{F}_q)$. But $\mathscr{P}_*(\mathbb{F}_q)$ and $\mathbb{F}_q[\xi_1, \ldots, \xi_k, \ldots]$ have the same Poincaré series, since $\deg(\mathscr{P}^{J(I)}) = \deg(\xi^I)$ for all index sequences I, and the admissible moniomials $\mathscr{P}^{J(I)}$ are an $\mathbb{F}_q$-vector space basis for $\mathscr{P}^*(\mathbb{F}_q)$. So $\mathbb{F}_q[\xi_1, \ldots, \xi_k, \ldots] = \mathscr{P}_*(\mathbb{F}_q)$, and it remains to verify the formula for the coproduct.

To this end we use the test algebra $\mathbb{F}_q[u]$, the polynomial algebra on one generator, as in [13]. Note that for admissible sequences we have

$$(\bigstar) \qquad \mathscr{P}^J(u) = \begin{cases} u^{q^k} & \text{if } J = M_k, \\ 0 & \text{otherwise.} \end{cases}$$

Define the map

$$\lambda^* : \mathbb{F}_q[u] \longrightarrow \mathbb{F}_q[u] \otimes \mathscr{P}_*$$

by the formula

$$\lambda^*(u^i) = \sum \mathscr{P}^{J(I)}(u^i) \otimes \xi^I$$

where the sum is over all index sequences I. Note that in any given degree the sum is finite and that λ^* is a map of algebras. Moreover

$$(\lambda^* \otimes 1)\lambda^*(u) = (1 \otimes \nabla_*)\lambda^*(u),$$

i.e., the following diagram

$$☯ \qquad \begin{array}{ccc} \mathbb{F}_q[u] \otimes \mathscr{P}_*(\mathbb{F}_q) \otimes \mathscr{P}_*(\mathbb{F}_q) & \xleftarrow{1 \otimes \nabla_*} & \mathbb{F}_q[u] \otimes \mathscr{P}_* \\ \uparrow{\scriptstyle \lambda^* \otimes 1} & & \uparrow{\scriptstyle \lambda^*} \\ \mathbb{F}_q[u] \otimes \mathscr{P}_* & \xleftarrow{\lambda^*} & \mathbb{F}_q[u] \end{array}$$

is commutative.

From $(\bigstar)$ it follows that

$$\lambda^*(u) = \sum u^{q^k} \otimes \xi_k$$

which when raised to the q^r-th power gives

$$\lambda^*(u^r) = \sum u^{q^{k+r}} \otimes \xi_k^{q^r},$$

and leads to the formula

$$(\lambda^* \otimes 1)(\lambda^*(u)) = (\lambda^* \otimes 1)\Big(\sum_k u^{q^k} \otimes \xi_k\Big) = \sum_r \sum_k u^{q^{k+r}} \otimes \xi_r^{q^k} \otimes \xi_k.$$

Whereas, the other way around the diagram ☯ leads to

$$(1 \otimes \nabla_*)(\lambda^*(u)) = \sum_j u^{q^j} \otimes \nabla_*(\xi_k),$$

and equating these two expressions leads to the asserted formula for the coproduct. □

As remarked at the end of the previous Section the operations $\mathcal{P}^{p^i}$ for $i>0$ are indecomposables in $\mathcal{P}^*$, so $\mathcal{P}^*$ is not generated by the operations $\mathcal{P}^{q^i}$ for $i \geq 0$; we need all the $\mathcal{P}^{p^i}$ for $i>0$. This can be readily seen on hand from the dual Hopf algebra, where, since $\mathbb{F}_q$ has characteristic p, the elements $\xi_1^{p^i}$ for $i \geq 0$ are all primitive, [14]. The following Corollary also indicates that passing from the prime field $\mathbb{F}_p$ to a general Galois field $\mathbb{F}_q$ is not just a simple substitution of q for p.

COROLLARY 4.4: *Let p be a prime integer, $q = p^\nu$ a power of p, and $\mathbb{F}_q$ the Galois field with q elements. The indecomposable module $Q(\mathcal{P}^*)$ of the Steenrod algebra of $\mathbb{F}_q$ has a basis consisting of the elements $\mathcal{P}^{p^i}$ for $i \in \mathbb{N}_0$, and the primitive elements $P(\mathcal{P}^*)$ has a basis consisting of the elements $\mathcal{P}^{\Delta_k}$ for $k \in \mathbb{N}$, where, for $k \in \mathbb{N}$, $\mathcal{P}^{\Delta_k}$ is dual to ξ_k with respect to the monomial basis for $\mathcal{P}_*$.* □

§5. The Milnor Basis and Embedding one Steenrod Algebra in Another

If $I = (i_1, i_2, \ldots, i_k, \ldots)$ is an index sequence we denote by $\mathcal{P}(I) \in \mathcal{P}^*(\mathbb{F}_q)$ the element in the Steenrod algebra that is dual to the corresponding monomial ξ^I in $\mathcal{P}_*(\mathbb{F}_q)$ with respect to the monomial basis for $\mathcal{P}_*(\mathbb{F}_q)$. This is not the same as the monomial $\mathcal{P}^I = \mathcal{P}^{i_1} \cdot \mathcal{P}^{i_2} \cdots \mathcal{P}^{i_k} \cdots$, these two elements do not even have the same degrees. As I ranges over all index sequences the collection $\mathcal{P}(I)$ ranges over an $\mathbb{F}_q$-basis for $\mathcal{P}^*(\mathbb{F}_q)$ called the **Milnor basis.**

To give some examples of elements written in the Milnor basis introduce the index sequence Δ_k which has a 1 in the k-th position and otherwise 0s. Then $\mathcal{P}^k$ is $\mathcal{P}(k\Delta_1)$, and, as noted at the end of Section 4, **the Milnor primitive elements** $\mathcal{P}^{\Delta_k} = \mathcal{P}(\Delta_k)$, for $k>0$, form a basis for the subspace of all primitive elements. In terms of the reduced power operations these elements can also be defined by the inductive formulae

$$\mathcal{P}^{\Delta_k} = \begin{cases} \mathcal{P}^1 & \text{if } k=1 \\ [\mathcal{P}^{q^{k-1}}, \mathcal{P}^{\Delta_k}] & \text{for } k>0, \end{cases}$$

where $[\mathcal{P}', \mathcal{P}'']$ denotes the commutator $\mathcal{P}' \cdot \mathcal{P}'' - \mathcal{P}'' \cdot \mathcal{P}'$ of $\mathcal{P}'$ and $\mathcal{P}''$. In Milnor's paper one can also find a formula for the product $\mathcal{P}(I) \cdot \mathcal{P}(J)$ of two elements in the Milnor basis. The basis transformation matrix from the admissible to the Milnor basis and its inverse is quite complicated, so we will say nothing more about it.

To each index sequence I we can make correspond both an admissible sequence over $\mathbb{F}_p$ and one over $\mathbb{F}_q$ via the equations (e) from the previous Section. This correspondence gives us a map $\vartheta : \mathcal{P}^*(\mathbb{F}_q) \longrightarrow \mathcal{P}^*(\mathbb{F}_p) \otimes_{\mathbb{F}_p} \mathbb{F}_q$.

THEOREM 5.1: *Let p be a prime integer, $q = p^\nu$ a power of p, and $\mathbb{F}_q$ the Galois field with q elements. The map*

$$\vartheta : \mathcal{P}^*(\mathbb{F}_q) \longrightarrow \mathcal{P}^*(\mathbb{F}_p) \otimes_{\mathbb{F}_p} \mathbb{F}_q$$

embeds the Steenrod algebra $\mathcal{P}^*(\mathbb{F}_q)$ of $\mathbb{F}_q$ as a Hopf subalgebra in the Steenrod algebra of $\mathbb{F}_p$ extended from $\mathbb{F}_p$ up to $\mathbb{F}_q$.

PROOF: It is much easier to verify that the dual map

$$\vartheta_* : \mathcal{P}_*(\mathbb{F}_p) \otimes_{\mathbb{F}_p} \mathbb{F}_q \longrightarrow \mathcal{P}_*(\mathbb{F}_q),$$

which is defined by the requirement that it be a map of algebras, and take the values

$$\vartheta_*(\xi_k(p) \otimes 1) = \begin{cases} \xi_m(q) & \text{if } k = m\nu \text{ (so } p^k - 1 = q^m - 1) \\ 0 & \text{otherwise,} \end{cases}$$

on algbera generators, is in fact a map of Hopf algebras. This is a routine computation. □

The Steenrod algebra over the prime field $\mathbb{F}_p$ has a well known interpretation as the mod p cohomology of the Eilenberg - MacLane spectrum. By flat base change $\mathcal{P}^*(\mathbb{F}_p) \otimes_{\mathbb{F}_p} \mathbb{F}_q$ may be regarded as the $\mathbb{F}_q$-cohomology of the same. By including the Eilenberg - MacLane spectrum $\mathbf{K}(\mathbb{F}_p)$ for the prime field into the Eilenberg - MacLane spectrum $\mathbf{K}(\mathbb{F}_q)$ we may view the elements of $\mathscr{P}^*(\mathbb{F}_p) \otimes_{\mathbb{F}_p} \mathbb{F}_q$ as defining stable cohomology operations in $\mathbb{F}_q$-cohomology. By Theorem 5.1 this also allows us to interpret elements of $\mathscr{P}^*(\mathbb{F}_q)$ as stable cohomology operations acting on the $\mathbb{F}_q$-cohomology of a topological space. Which elements appear in this way is described in cohomological terms in [24].

§6. Closing Comments

Algebraic topologists will of course immediately say *"but that isn't the Steenrod algebra, it is only the algebra of reduced power operations; there is no Bockstein operator unless* $q = 2$*."* This is correct, the full Steenrod algebra, with the Bockstein, has not yet played a significant role in invariant theory, so I have not treated it here. But, if one wishes to have a definition for the full Steenrod algebra in the same style as the one presented here, all one needs to do for $q \neq 2$ is to replace the functor $V \rightsquigarrow \mathbb{F}[V]$ with the functor $V \rightsquigarrow H(V)$, where $H(V)$ is defined to be $H(V) = \mathbb{F}[V] \otimes E[V]$, with $E[V]$ the exterior algebra on the dual vector space V^* of V. Since V^* occurs *twice* as a subspace of $H(V)$, once as $V^* \otimes \mathbb{F} \subset \mathbb{F}[V] \otimes \mathbb{F}$ and once as $\mathbb{F} \otimes V^* \subset E[V]$, we need a way to distinguish these two copies. One way to do this is to write z for a linear form $z \in V^*$ when it is to be regarded as a polynomial function, and dz for the same linear form when it is to be regarded as an alternating linear form. This amounts to identifying $H(V)$ with the algebra of polynomial differential forms on V.

Next introduce the Bockstein operator $\beta : H(V) \longrightarrow H(V)$ by requiring it to be the derivation where, for an alternating linear form dz one has $\beta(dz) = z$, where z is the corresponding polynomial linear form, and for any polynomial linear form z one has $\beta(z) = 0$. The operators $\mathcal{P}^k$ for $k \in \mathbb{N}_0$ together with β generate a subalgebra of the algebra of endomorphisms of the functor $V \rightsquigarrow H(V)$, and this subalgebra is the full Steenrod algebra of the Galois field $\mathbb{F}_q$.

Finally, at the summer school T.P. Bisson spoke about his work with A. Joyal on a universal algebra approach to both the Dyer-Lashof algebra and the Steenrod algebra [4]. The interested reader should consult this paper which contains many informative facts.

References

[1] J. F. Adams and C.W. Wilkerson, *Finite H-spaces and Algebras over the Steenrod Algebra,* Annals of Math. 111 (1980), 95–143.

[2] J. Adem, *The Relations on Steenrod Powers of Cohomology Classes,* in: Algebraic Geometry and Toplogy, Edited by, R.H. Fox, D.C. Spencer and A.W. Tucker, Princeton Umiv. Press 1957.

[3] T. P. Bisson, *Divided Sequences and Bialgebras of Homology Operations,* PhD Thesis, Duke University, 1977.

[4] T. P. Bisson and A. Joyal, *Q-Rings and the Homology of the Symmetric Group,* Contemp. Math. 202 (1997), 235–286.

[5] S. R. Bullett and I. G. Macdonald, *On the Adem Relations,* Topology 21 (1982), 329–332.

[6] H. Cartan, *Sur l'Iteration des Opérations de Steenrod,* Comment. Math. Helv. 29 (1955), 40–58.

[7] H. Cartan, *Algèbres d'Eilenberg-Mac Lane et Homotopie,* Séminaire Henri Cartan, 1954/55, W. A. Benjamin, New York 1967.

[8] S. D. Cohen, *Rational Functions Invariant under an Orthogonal Group,* Bull. London Math. Soc. 22 (1990), 217 – 221.

[9] L. E. Dickson, *Linear Groups,* Dover Publications Inc., New York 1958.

[10] O. E. Glenn, *Modular Invariant Processes,* Bull. of the Amer. Math. Soc. 21 (1914-15), 167 – 173.

[11] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields,* Oxford Mathematical Monographs, Oxford Science Publications, Oxford 1998 second edition.

[12] N. Jacobson, *Lectures in Abstract Algebra* III *Theory of Fields and Galois Theory,* Springer-Verlag, Heidelberg, Berlin, New York, 1975.

[13] J. W. Milnor, *The Steenrod algebra and its Dual,* Annals of Math. (2) 67 (1958), 150–171.

[14] J. W. Milnor and J. C. Moore, *The Structure of Hopf Algebras,* Ann. of Math. 81 (1965), 211–265.

[15] K.G. Monks, *Nilpotence in the Steenrod Algebra,* Bol. Soc. Mat. Mexicana (2) (1992), 401–416.

[16] K.G. Monks, *The Nilpotence Height of* P^s_t, Proc. of the Amer. Math. Soc. 124 (1996), 1297–1303.

[17] M. D. Neusel, *Inverse Invariant Theory and Steenrod Operations,* Memoirs of the Amer. Math. Soc. No. 692 Vol.146, AMS, Providence RI 2000.

[18] M. D. Neusel and L. Smith, *Polynomial Invariants of Finite Groups,* Springer-Verlag, Heidelberg, Berlin, Encyclopedea of Mathematics (to appear).

[19] J.-P. Serre, *Cohomologie modulo 2 des complexes d'Eilenberg-Mac Lane,* Comment. Math. Helv. 27 (1953), 198–232.

[20] L. Smith, *$\mathcal{P}^*$-Invariant Ideals in Rings of Invariants,* Forum Mathematicum 8 (1996), 319–342.

[21] L. Smith, *Polynomial Invariants of Finite Groups,* A.K. Peters, Ltd., Wellesley, MA, 1995, second printing 1997.

[22] L. Smith, *Polynomial Invariants of Finite Groups: A Survey of Recent Developments,* Bull. of the Amer. Math. Soc. 34 (1997), 211–250.

[23] L. Smith, *The Ring of Invariants of* $O(3, \mathbb{F}_q)$, Finite Fields and their Applications 5 (1999), 96–101.

[24] L. Smith, *Cohomology Automorphisms over Galois Fields and Group-Like Elements in the Steenrod Algebra,* Preprint, AG-Invariantentheorie, 2000.

[25] L. Smith, *Invariants of* 2×2 *Matrices over Finite Fields,* AG-Invariantentheorie, Preprint 2000.

[26] L. Smith and R. E. Stong, *On the Invariant Theory of Finite Groups: Orbit Polynomials, Chern Classes and Splitting Principles,* J. of Algebra 109 (1987), 134–157.

[27] N. E. Steenrod, *Polynomial Algebras over the Algebra of Cohomology Operations,* in: *H-Spaces, Actes de la reunion de Neuchâtel (Suisse), Auot 1970*, Lecture Notes in Math. 196, Springer-Verlag, Heidelberg, Berlin, New York 1971.

[28] R. Thom, *Quelques propriétés globales des variétés différentiables,* Comm. Math. Helv. 28 (1954), 17–86.

[29] G. Walker and R. Wood, *The Nilpotence Height of* Sq^{2^n}, Proc. of the Amer. Math. Soc. 124 (1996), 1291–1295.

[30] G. Walker and R. Wood, *The Nilpotence Height of* $\mathcal{P}^{p^n}$, Math. Proc. Camb. Phil. Soc. 123 (1998), 85–93.

[31] R. Wood, *Problems in the Steenrod Algebra,* Bull. London Math. Soc. 30 (1998), 449–517.

[32] R. Wood, *Hit Problems and the Steenrod Algebra,* Notes from a Lecture Course at the University of Ioannina, june 2000.

[33] Wu Wen-Tsün, *Sur les puissance de Steenrod,* Colloque de Topologie de Strasbourg, 1951.

Larry Smith
AG-Invariantentheorie
Mittelweg 3
D 37133 Friedland
Federal Republic of Germany
e-mail: LARRY@SUNRISE.UNI-MATH.GWDG.DE

$\mathbb{F}_q[V][[\xi]]$ 2
$\mathbf{e}_{\det}$ 4
$\mathbf{E}_{\det}$ 4
$\mathcal{P}^i(-)$ 2
$CGA_{\mathbb{F}_q}$ 3
$Sq^i(-)$ 2
$Vect_{\mathbb{F}_q}$ 3

Adem-Wu relations 4
admissible monomial 6
algebra of polynomial functions 2

basic monomials 6
Bullett-Macdonald identity 5

Cartan formulae 2

Euler class 4
Example $\mathbb{O}(3, \mathbb{F}_q)$ 3
Example, $H^*(B\mathbb{SO}(3); \mathbb{F}_2)$ 8
Example, $\mathbb{SO}(3, \mathbb{F}_q)$ 4
Example, $PSL(2, \mathbb{F}_q)$ 3
Example, $SL(2, \mathbb{F})$ 3
excess 9

higher order derivation 3
Hopf algebra 4

index sequence 6

length 6
linear forms 2

Milnor basis 12
Milnor primitive elements 12
moment 7

pre-Euler class 4

Steenrod algebra 2, 3, 4
Steenrod operations 2
Steenrod reduced power operations 2
Steenrod squaring operations 2

unstability condition 2