Centralisers in the unit group of the Steenrod algebra

Sandling, Robert

2011

MIMS EPrint: **2011.105**

Manchester Institute for Mathematical Sciences
School of Mathematics

The University of Manchester

Reports available from: http://eprints.maths.manchester.ac.uk/
And by contacting: The MIMS Secretary
School of Mathematics
The University of Manchester
Manchester, M13 9PL, UK

ISSN 1749-9097

Centralisers in the unit group of the Steenrod algebra

Robert Sandling
School of Mathematics
University of Manchester

1. Introduction

The unit group of an algebra is often an important object in its own right. The general linear group, for example, is the group of units of the algebra of matrices. For all the interest shown over the years in the Steenrod algebra, remarkably little attention has been paid to its group of units. Here we present results arising from an attempt to redress the balance for the most classical Steenrod algebra, that over the field of two elements. Our object is to develop approaches which might lead to insights about the Steenrod algebra itself available from a novel point of view.

Our main result states that the centraliser of a non-identity element of the unit group of the Steenrod algebra is of infinite index. It is equivalent to say that every non-identity conjugacy class of the unit group is infinite, or that every non-identity normal subgroup is infinite. These results have virtual extensions in the group-theoretic sense of the term, e.g., no subgroup of finite index has non-identity finite normal subgroups. The result has consequences within the Steenrod algebra itself: its centre is trivial; the centraliser of a non-scalar element is of infinite codimension.

Our main technique is refinement of the Adem-Wu relations to capture more information from the reduction of a monomial in the Steenrod squares into the canonical form afforded by these relations, that is, its decomposition in the basis of admissible monomials. This is applied by giving precise descriptions of the annihilators of the augmentation ideals of the finite subalgebras introduced by Milnor. We show in particular that such an annihilator has a basis of admissibles.

The paper concludes with diverse remarks and results about the group of units, most exploiting its key feature, local finiteness. They complement the discussion in Sect. 9 of the survey article [Wo98]. The fact that the composition of the antipode with inversion is an outer automorphism of the unit group is proved here.

Notation. The Steenrod algebra over the Galois field $\mathbf{F}_2$ is denoted by A, and its augmentation ideal by A^+; U denotes the *Steenrod group*, the unit group of A, so that $U = 1 + A^+$. For $n \geq 0$, $A(n)$ denotes the unital subalgebra generated by the Steenrod squares $Sq^{2^m}, 0 \leq m \leq n$, (equivalently, generated by $Sq^i, 0 \leq i \leq 2^{n+1} - 1$). Further, $A(n)^+$ denotes its augmentation ideal, spanned as subspace by its monomials of positive grading, and $U(n) = 1 + A(n)^+$, the

unit group of $A(n)$. For standard results on the Steenrod algebra we refer the reader to [SE62, Wo98].

A typical monomial in the Steenrod squares is denoted as $Sq^{\mathbf{x}}$, where $\mathbf{x} = (x_1, x_2, \ldots), x_i \geq 0$, with only finitely many non-zero entries; thus, $Sq^{\mathbf{x}} = \prod_i Sq^{x_i} = Sq^{x_1}Sq^{x_2}\ldots$. To avoid ambiguity of representation, we assume that $\mathbf{x}$ is normalised in the sense that, if $x_k \neq 0$, then $x_i \neq 0$ for $1 \leq i \leq k$. We write $|\mathbf{x}|$ for the sum of the entries of $\mathbf{x}$ and set $|Sq^{\mathbf{x}}| := |\mathbf{x}|$ if $Sq^{\mathbf{x}} \neq 0$ in which case $|Sq^{\mathbf{x}}|$ is called the *degree*, or *grading*, of the monomial $Sq^{\mathbf{x}}$. The *length* of $Sq^{\mathbf{x}}$, denoted $\ell(Sq^{\mathbf{x}})$ or $\ell(\mathbf{x})$, is the number of non-zero entries of $\mathbf{x}$. We write $\mathbf{x}' = (x_2, x_3, \ldots)$ and so on. A monomial $Sq^{\mathbf{a}}$ is called *admissible* if $a_i \geq 2a_{i+1}$ for all i; in these circumstances we also refer to $\mathbf{a}$ as admissible. The admissible elements of A comprise a basis for A. The Steenrod algebra is the free algebra generated by the Steenrod squares $Sq^\alpha, \alpha \geq 0$, subject to the Adem-Wu relations which state that, if $2\beta > \alpha$, then

$$Sq^\alpha Sq^\beta = \sum \epsilon_\kappa Sq^{\alpha+\beta-\kappa}Sq^\kappa$$

for certain coefficients ϵ_κ. Specifically,

$$\epsilon_\kappa = \binom{\beta - \kappa - 1}{\alpha - 2\kappa}$$

but the specific values are not always needed. The antipode, or conjugation, of A as Hopf algebra is denoted by χ; it is an anti-automorphism of A and of U.

2. Centralisers and annihilators

For our purposes the admissible basis of the Steenrod algebra has proved to be the most useful because of the way in which the Adem-Wu relations enable an arbitrary monomial to be straightened into the canonical form this basis provides. We begin with a lemma which establishes certain features obtainable by this straightening process. That the grading of a monomial remains unchanged on passing to its admissible expression, and that its length cannot increase, are familiar features immediate from the nature of the Adem-Wu relations. The point of our lemma is its specification of conditions under which the superfix of the leading factor of an admissible appearing in the expression exceeds the superfixes of the factors of the original monomial.

2.1 Lemma *Let $Sq^{\mathbf{x}} = \sum_{\mathbf{a}\in\mathbf{A}} Sq^{\mathbf{a}}$ be the decomposition of the non-zero monomial $Sq^{\mathbf{x}}$ in the admissible basis. Then, for $\mathbf{a} \in \mathbf{A}$, $|\mathbf{a}| = |\mathbf{x}|, \ell(\mathbf{a}) \leq \ell(\mathbf{x})$ and $a_1 \geq x_i$ for all i; if $x_1 < 2x_j$ for an index $j, j > 1$, then $a_1 > x_i$ for all i.*

Proof. The proof proceeds by induction on $d := |\mathbf{x}|$. We may assume that $d > 1$. If $|\mathbf{x}| = d$, then $d \geq x_1$ so that we may induct in reverse on the value of

x_1 among all $\mathbf{x}$ for which $|\mathbf{x}| = d$ and $Sq^{\mathbf{x}} \neq 0$. As the case $x_1 = d$ is trivial, we assume that $x_1 < d$.

By the induction on d, we know that $Sq^{\mathbf{x}'}$ is a sum of admissibles $Sq^{\mathbf{a}}$ for which $|\mathbf{a}| = d - x_1, \ell(\mathbf{a}) \leq \ell - 1$ and $a_1 \geq x_i$ for all $i \geq 2$. It suffices to show that each non-zero element $Sq^{x_1}Sq^{\mathbf{a}}$ has the desired expression. For economy of notation, we take $\mathbf{x}'$ to be admissible and return our attention to $Sq^{\mathbf{x}}$. If $\mathbf{x}$ is itself admissible, we are done as then $x_1 \geq 2x_2 > x_i$ for $i \geq 2$. If not, then $x_1 < 2x_2$ so that, by the Adem-Wu relations,

$$Sq^{x_1}Sq^{x_2} = \sum \epsilon_\kappa Sq^{x_1+x_2-\kappa}Sq^{\kappa}.$$

On substituting, we see that $Sq^{\mathbf{x}}$ is a sum of monomials $Sq^{x_1+x_2-\kappa}Sq^{\kappa}Sq^{\mathbf{x}''}$ with $x_1 \geq 2\kappa$. Thus $x_1 + x_2 - \kappa > x_1$ so that, by induction on x_1, such a monomial, not equal to zero, is a sum of admissibles of the required form. As, in addition, $x_1 + x_2 - \kappa > x_2 \geq x_i$ for $i \geq 2$ because of the assumption that $\mathbf{x}'$ is admissible, the final assertion of the lemma follows. □

We pause at this point to deduce the triviality of the centre of U (cf. [Wo98, p. 455]). While this is an immediate consequence of our main result as all elements of U have finite order so that a non-identity central element would generate a non-trivial finite normal subgroup, much less is required for its proof.

2.2 Theorem *The centre of the Steenrod algebra is the base field; the centre of its group of units is trivial.*

Proof. (Wood) Suppose that A has a non-scalar central element z. In the expression $z = \sum_{\mathbf{a}\in\mathbf{A}} Sq^{\mathbf{a}}$ in the admissible basis, let a be maximal among the values a_1 for $\mathbf{a} \in \mathbf{A}$.

Then $Sq^{2a}z$ is a sum of admissibles, each of which has leading factor Sq^{2a}. On the other hand, by the lemma, zSq^{2a} is a sum of admissibles, each of which has leading factor Sq^{ℓ} with $\ell > 2a$. Thus, $Sq^{2a}z \neq zSq^{2a}$, a contradiction.

The result for U follows immediately as a central element of U is of the form $1 + z$, where z is a central element of A. □

The proof which we provide for our main result relies upon a detailed description of the right annihilator $\mathrm{ra}(A(n)^+)$ of the augmentation ideal of $A(n)$. As $A(n)$ is a Poincaré duality algebra [Ma83, p. 188], its subspace of highest grading is one-dimensional. Its generator is a monomial, indeed an admissible, the necessarily unique admissible of highest degree in $A(n)$. This element is called the top element; we denote it as t_n. As illustrations, $t_0 = Sq^1$, $t_1 = Sq^5Sq^1$ and $t_2 = Sq^{17}Sq^5Sq^1$. Because of its maximal degree in $A(n)$, $t_n \in \mathrm{ra}(A(n)^+)$, so that t_nA, the principal right ideal generated by t_n, is contained in $\mathrm{ra}(A(n)^+)$. It is known that the two coincide. We offer a proof for this fact based on the themes introduced here. The general formula for t_n is

$$t_n = Sq^{\mathbf{a}}, a_i = 1 + (n + 1 - i)2^{n+2-i}, 1 \leq i \leq n + 1$$

(cf. [Wo98, pp. 478-481]). Thus, $t_n = Sq^{1+n2^{n+1}} t_{n-1}$, a form by which t_n could be defined inductively and one which is itself useful for inductive proofs. For example, it can be used to deduce directly the fact that $t_n \in \mathrm{ra}(A(n)^+)$, the only aspect of the conceptual definition of the top element which is used here.

The ideal $\mathrm{ra}(A(n)^+)$ is unusual in having a basis of admissible elements, as we show. Members of this basis are used in the proof of our main result. We approach the topic through two subspaces which contain t_n and whose definitions mimic the form of t_n.

2.3 Definition Let $n \geq 0$. Let V_n be the subspace of A spanned by all monomials $Sq^{\mathbf{x}}$ with $x_i \equiv 1 \bmod 2^{n+2-i}$ if $1 \leq i \leq n+1$. Let V_n^{adm} be the analogous subspace in which $\mathbf{x}$ is additionally required to be admissible.

While it is clear that V_n is a right ideal, it is much less clear that the subspace V_n^{adm} is as well. In fact, both subspaces coincide with $t_n A$ so that all of their elements have t_n as initial factor. We prove the coincidence of the subspaces $t_n A$, V_n^{adm} and V_n through a sequence of technical lemmas.

2.4 Lemma *Let q be a power of 2, $q \geq 1$. Suppose that $\alpha \equiv 1 \bmod 2q$, $\beta \equiv 1 \bmod q$ and that $Sq^\alpha Sq^\beta \neq 0$. Let $Sq^{\alpha'} Sq^{\beta'}$ be a term in the expression for $Sq^\alpha Sq^\beta$ in the admissible basis. Then $\alpha' \equiv 1 \bmod 2q$ and $\beta' \equiv 1 \bmod q$; further, if $\alpha' \neq \alpha$, then $\alpha' > \alpha$.*

Proof. We may assume that $2\beta > \alpha$. By the Adem-Wu relations,

$$Sq^\alpha Sq^\beta = \sum \binom{\beta - \kappa - 1}{\alpha - 2\kappa} Sq^{\alpha+\beta-\kappa} Sq^\kappa$$

in the admissible basis. If $\binom{\beta-\kappa-1}{\alpha-2\kappa} \neq 0$, then $\alpha + \beta - \kappa > \alpha$, as needed for the last point of the statement.

Write q as $2^m, m \geq 0$. If $m = 0$, the hypothesis states that α is odd and the conclusion required is that α' is odd. But, if α is odd, then $\alpha - 2\kappa$ is odd so that, if

$$\binom{\beta - \kappa - 1}{\alpha - 2\kappa} \equiv 1 \bmod 2,$$

then $\beta - \kappa - 1$ must also be odd whence $\alpha + \beta - \kappa$ is odd as required.

Assume then that $m \geq 1$. Write the dyadic expansions of the various quantities as follows:

$$\alpha = \sum \alpha_i 2^i, \beta = \sum \beta_i 2^i, \kappa = \sum \kappa_i 2^i,$$

$$\beta - \kappa - 1 = \sum \gamma_i 2^i, \alpha - 2\kappa = \sum \delta_i 2^i.$$

By hypothesis, $\alpha_0 = \beta_0 = 1, \alpha_i = 0, 1 \leq i \leq m$, and $\beta_i = 0, 1 \leq i \leq m-1$.

Let κ be such that $\binom{\beta-\kappa-1}{\alpha-2\kappa} \equiv 1 \bmod 2$. We show that $\kappa \equiv 1 \bmod 2^m$ and that $\alpha+\beta-\kappa \equiv 1 \bmod 2^{m+1}$. By a standard congruence [AS72, 24.1.1],

$$\binom{\beta-\kappa-1}{\alpha-2\kappa} \equiv \prod \binom{\gamma_i}{\delta_i} \bmod 2,$$

we see that $\binom{\gamma_i}{\delta_i} \equiv 1$ for all i, that is, if $\delta_i = 1$, then $\gamma_i = 1$. As $\alpha - 2\kappa$ is odd, $\delta_0 = 1$ and so $\gamma_0 = 1$. As before, $\beta - \kappa - 1$ is odd so that κ is as well whence $\kappa_0 = 1$.

The next conclusions are obtained by working modulo 2^{m+1} and so congruences are to be interpreted modulo this number. Now $\beta \equiv 1 + \beta_m 2^m$ so that

$$\begin{aligned}\beta - \kappa - 1 \equiv \beta_m 2^m - \kappa &= -\sum_{0\le i\le m-1} \kappa_i 2^i + (\beta_m - \kappa_m)2^m \\ &\equiv 1 + (2^{m+1}-1) - \sum_{0\le i\le m-1} \kappa_i 2^i + (\beta_m - \kappa_m)2^m \\ &= 1 + \sum_{0\le i\le m-1} (1-\kappa_i)2^i + (1+\beta_m-\kappa_m)2^m.\end{aligned}$$

Thus, $\gamma_i = 1 - \kappa_i$ if $0 \le i \le m-1$ while $\gamma_m \equiv 1 + \beta_m - \kappa_m \bmod 2$. Further, $\alpha \equiv 1$ so that

$$\alpha - 2\kappa \equiv 1 - \sum_{1\le i\le m} \kappa_{i-1} 2^i \equiv 1 + 2 + \sum_{2\le i\le m} (1-\kappa_{i-1})2^i$$

as $\kappa_0 = 1$. Thus, $\delta_1 = 1$ and $\delta_i = 1 - \kappa_{i-1} = \gamma_{i-1}$ if $2 \le i \le m$.

It follows by induction that $\gamma_i = 1 = \delta_i$ if $0 \le i \le m$, that is, $\kappa_i = 0$ if $0 \le i \le m-1$ so that $\kappa \equiv 1 \bmod 2^m$ as required. Finally, from $\gamma_m = 1$, we see that $\beta_m = \kappa_m$ and so $\alpha + \beta - \kappa \equiv 1 \bmod 2^{m+1}$. □

The first consequence which we draw from this result bounds the superfixes of the non-zero elements of V_n in terms of the superfixes of t_n.

2.5 Lemma *Suppose that* $\mathbf{x}$ *satisfies the conditions for a generator of* V_n *so that* $x_i = 1 + m_i 2^{n+2-i}$ *for integers* $m_i \ge 0$ *if* $1 \le i \le n+1$. *If* $Sq^{\mathbf{x}} \ne 0$, *then* $m_i \ge n+1-i$ *if* $1 \le i \le n+1$.

Proof. The proof proceeds by induction on n. The result is clear for $n = 0$. For $n > 0$, the induction hypothesis, applied to $\mathbf{x}'$, implies the result for all i strictly greater than 1. We may assume that $\mathbf{x}$ is inadmissible. It remains to show that $m_1 \ge n$. Suppose that $m := m_1 < n$. Again, $x_2 \equiv 1 \bmod 2^n$ so that, by Lemma 2.4 and the Adem-Wu relations,

$$Sq^{1+m2^{n+1}} Sq^{x_2} = \sum \epsilon_\kappa Sq^{1+m2^{n+1}+x_2-\kappa} Sq^\kappa,$$

where $\kappa \equiv 1 \bmod 2^n$ and $\kappa \le m2^n$. Thus, we need only sum over those $\kappa = 1 + \ell 2^n$ for ℓ such that $0 \le \ell \le m-1$. As $m - 1 \le n - 1$, by the induction

hypothesis $Sq^{1+\ell 2^n}Sq^{\mathbf{x}''} = 0$ and so $Sq^{\mathbf{x}} = Sq^{1+m2^{n+1}}Sq^{x_2}Sq^{\mathbf{x}''} = 0$, contrary to hypothesis. □

A particularly simple case in which an $\mathbf{x}$ satisfies the defining conditions for a generator of V_n but not the conclusions of this lemma, and so in which we can conclude that $Sq^{\mathbf{x}} = 0$, is that in which the degree of $\mathbf{x}$ is too small. By the lemma the non-zero element of smallest degree in V_n is t_n, whose degree is $6 + (n-1)(1+2^{n+2})$. Thus, for example, $Sq^9Sq^9Sq^3 = 0$.

Another consequence of Lemma 2.4 is the fact that V_n^{adm} is a right ideal.

2.6 Lemma *For $n \geq 0$, V_n^{adm} coincides with V_n and is a right ideal.*

Proof. Since V_n^{adm} is clearly a subspace of V_n and since V_n is a right ideal, it remains to show that $V_n \leq V_n^{\mathrm{adm}}$. We prove this by induction on n. To avoid repetition, we start the induction at $n = -1$. Stretched to this case the definition gives $V_{-1} = V_{-1}^{\mathrm{adm}} = A$ (with $A(-1) := \mathbf{F}_2$, we get the correct description of the right annihilator in this case). We may then take $n \geq 0$.

Fix a positive integer d for which there is an $\mathbf{x}$ satisfying $|\mathbf{x}| = d$ and for which $Sq^{\mathbf{x}}$ is a non-zero generator of V_n. As before, among all such generators of V_n, there are vectors $\mathbf{x}$ for which x_1 is maximal. We show that $Sq^{\mathbf{x}} \in V_n^{\mathrm{adm}}$ by reverse induction on x_1.

To start the induction, take $\mathbf{x}$ as above with x_1 maximal. Then $Sq^{\mathbf{x}'} \in V_{n-1}$. By the induction on n, $Sq^{\mathbf{x}'} \in V_{n-1}^{\mathrm{adm}}$. As in the proof of Lemma 2.1, we assume that $\mathbf{x}'$ is admissible and then show that $\mathbf{x}$ is admissible.

If $\mathbf{x}$ is not admissible, then $2x_2 > x_1$. Now $x_1 \equiv 1 \bmod 2^{n+1}$ and $x_2 \equiv 1 \bmod 2^n$ so that, by the previous lemma, $Sq^{x_1}Sq^{x_2}$ is a sum of admissibles of the form $Sq^{y_1}Sq^{y_2}$ with $y_1 \equiv 1 \bmod 2^{n+1}$ and $y_2 \equiv 1 \bmod 2^n$ and $y_1 > x_1$. But then $Sq^{y_1}Sq^{y_2}Sq^{\mathbf{x}''} \in V_n$, a contradiction.

We may now turn to a non-zero generator $Sq^{\mathbf{x}}$ of V_n with $|\mathbf{x}| = d$ but x_1 not maximal. We assume that $\mathbf{x}$ is not admissible. As in the previous paragraph, we find that $Sq^{\mathbf{x}}$ is a sum of monomials $Sq^{y_1}Sq^{y_2}Sq^{\mathbf{x}''}$, each a generator of V_n and in each of which $y_1 > x_1$. By the induction on the first superfix, we conclude that the monomials are in V_n^{adm} whence $Sq^{\mathbf{x}}$ is as well. □

It remains to show that each generator of V_n has t_n as initial factor. This is done explicitly; the main identity required is given in the next lemma. As with $A(-1)$, it is convenient to extend the definition of t_n to the case $n = -1$, namely, by setting $t_{-1} := 1$.

2.7 Lemma *Let $x \geq 0$. If 2^{n+1} divides x, then $t_nSq^x = Sq^{1+n2^{n+1}+x}t_{n-1}$; otherwise, $t_nSq^x = 0$.*

Proof. For $n = 0$ the result is immediate, and we finish the proof by use of induction. Assume then that $n \geq 1$ and that $x = u2^{n+1}$, where $u \geq 1$. Then

$$t_nSq^x = Sq^{1+n2^{n+1}}t_{n-1}Sq^{(2u)2^n},$$

which, by the induction hypothesis, is

$$Sq^{1+n2^{n+1}}Sq^{1+(n-1+2u)2^n}t_{n-2}.$$

By Lemma 2.4, the product of the first two factors is

$$\sum \epsilon_\kappa Sq^{1+n2^{n+1}+1+(n-1+2u)2^n-\kappa}Sq^\kappa,$$

where $\kappa \equiv 1 \bmod 2^n$ and $\kappa \leq n2^n$. Thus, we need only sum over those κ of the form $\kappa = 1 + \ell 2^n$, $0 \leq \ell \leq n-1$. If $\ell \leq n-2$, the product $Sq^{1+\ell 2^n}t_{n-2} = 0$ by Lemma 2.5. For $\ell = n-1$, the binomial coefficient

$$\epsilon_{1+(n-1)2^n} = \binom{2u2^n - 1}{2^{n+1} - 1},$$

which is odd. This leaves

$$t_nSq^{u2^{n+1}} = Sq^{1+(n+u)2^{n+1}}Sq^{1+(n-1)2^n}t_{n-2} = Sq^{1+(n+u)2^{n+1}}t_{n-1},$$

as required.

Now assume that $x = 2^e y$, where y is odd and $n \geq e \geq 0$. Since $t_nA(n) = 0$, it suffices to show that $Sq^{\mathbf{x}} \in A(e)A$. We prove this by induction on e. We may assume that $e \geq 1$ and also that $y \geq 3$. By the Adem-Wu relations,

$$Sq^{2^e}Sq^{2^e(y-1)} = \sum \epsilon_\kappa Sq^{2^e y-\kappa}Sq^\kappa,$$

where $0 \leq \kappa \leq 2^{e-1}$. If $\kappa \geq 1$, the highest power of 2 which can divide $2^e y - \kappa$ is 2^{e-1} so that, by the induction hypothesis, $Sq^{2^e y-\kappa}Sq^\kappa \in A(e)A$. But the binomial coefficient ϵ_0 is odd. Thus, $Sq^{2^e y} \equiv Sq^{2^e}Sq^{2^e(y-1)} \bmod A(e)A$, that is, $Sq^{2^e y} \in A(e)A$. □

The following corollary is suggested by the proof. It follows with the further observation that the algebra $A(n)$ is generated by all Sq^{2^m}, where $0 \leq m \leq n$.

2.8 Corollary *The right ideal $A(n)A$ is the linear subspace spanned by all $Sq^{\mathbf{x}}$ for which x_1 is not divisible by 2^{n+1}.*

2.9 Proposition *For $n \geq 0$, the right annihilator of $A(n)^+$ is the principal right ideal generated by the top element t_n of $A(n)$ and coincides with the subspaces V_n and V_n^{adm}.*

Proof. We show first that the ideals t_nA, V_n^{adm} and V_n coincide. We know from the definition of V_n that t_nA is contained in V_n and from Lemma 2.6 that $V_n^{\mathrm{adm}} = V_n$. We next show that V_n is contained in t_nA.

Let $Sq^{\mathbf{x}}$ be a generator of V_n. We may assume that $x_i = 0$ if $i > n+1$ so that $Sq^{\mathbf{x}} = Sq^{x_1} \cdots Sq^{x_{n+1}}$ with $x_i \geq 1 + (n+1-i)2^{n+2-i}$ by Lemma 2.5. The result then follows from the identity

$$Sq^{\mathbf{x}} = t_n \prod_{1 \leq i \leq n+1} Sq^{x_i-(1+(n+1-i)2^{n+2-i})}.$$

This identity is proved by induction in which the induction step is provided by Lemma 2.7. Thus, $V_n \subseteq t_n A$ as required.

We have already remarked that $t_n A$ is contained in $\mathrm{ra}(A(n)^+)$ so that V_n^{adm} is contained in $\mathrm{ra}(A(n)^+)$. We complete the proof of the remaining part of the proposition, the first assertion, by showing, via induction, that $\mathrm{ra}(A(n)^+)$ is contained in V_n^{adm}.

To begin we establish by induction the technical fact that, if the admissible $Sq^{\mathbf{a}}$ lies in V_{n-1}^{adm}, then no superfix of an admissible in the expansion of $Sq^{2^n}Sq^{\mathbf{a}}$ is strictly greater than $a_1 + 2^n$. We may assume that $a_1 > 2^{n-1}$. Recall our conventions $V_{-1}^{\mathrm{adm}} = A$ and $A(-1) = \mathbf{F}_2$. For $n = 0$, either $Sq^1Sq^{\mathbf{a}}$ vanishes or has leading superfix $a_1 + 1$.

Let $n \geq 1$. Let $Sq^{\mathbf{a}}$ be an admissible of V_{n-1}^{adm}. Thus, $Sq^{\mathbf{a}'} \in V_{n-2}^{\mathrm{adm}}$ so that $Sq^{\kappa}Sq^{\mathbf{a}'} = 0$ for all κ, $1 \leq \kappa \leq 2^{n-1} - 1$, because the Steenrod squares Sq^{κ} belong to $A(n-2)^+$. Further, by the Adem-Wu relations,

$$Sq^{2^n}Sq^{a_1} = \sum_{0 \leq \kappa \leq 2^{n-1}} \binom{a_1 - \kappa - 1}{2^n - 2\kappa} Sq^{2^n + a_1 - \kappa}Sq^{\kappa}.$$

Thus,

$$Sq^{2^n}Sq^{\mathbf{a}} = \binom{a_1 - 1}{2^n} Sq^{a_1 + 2^n}Sq^{\mathbf{a}'} + Sq^{a_1 + 2^{n-1}}Sq^{2^{n-1}}Sq^{\mathbf{a}'}.$$

By the induction hypothesis, the largest superfix in the admissible expansion of $Sq^{2^{n-1}}Sq^{\mathbf{a}'}$ is less than or equal to $a_2 + 2^{n-1}$. By the admissibility of $\mathbf{a}$, $a_1 \geq 2a_2$ so that, by consideration of the residues modulo 2^n, we conclude that $a_1 + 2^{n-1} \geq 2(a_2 + 2^{n-1})$. Thus, if $Sq^{2^{n-1}}Sq^{\mathbf{a}'}$ has admissible decomposition $\sum_{\mathbf{e} \in \mathbf{E_a}} Sq^{\mathbf{e}}$, then

$$Sq^{a_1 + 2^{n-1}}Sq^{2^{n-1}}Sq^{\mathbf{a}'} = \sum_{\mathbf{e} \in \mathbf{E_a}} Sq^{a_1 + 2^{n-1}}Sq^{\mathbf{e}}$$

is the admissible decomposition of the product. Consequently, $Sq^{2^n}Sq^{\mathbf{a}}$ decomposes admissibly as

$$\binom{a_1 - 1}{2^n} Sq^{a_1 + 2^n}Sq^{\mathbf{a}'} + \sum_{\mathbf{e} \in \mathbf{E_a}} Sq^{a_1 + 2^{n-1}}Sq^{\mathbf{e}},$$

which visibly has no superfix greater than $a_1 + 2^n$.

We can now show by induction that $\mathrm{ra}(A(n)^+)$ is contained in V_n^{adm}. For $n = 0$, $A(0)^+$ is spanned by Sq^1, its top element. It is an immediate consequence of the Adem-Wu relations that $\mathrm{ra}(A(0)^+) = \mathrm{ra}(Sq^1)$ is spanned by all $Sq^{\mathbf{x}}$ with x_1 odd. Thus, $\mathrm{ra}(A(0)^+) = V_0 = V_0^{\mathrm{adm}}$.

Let $n \geq 1$. As an ideal in $A(n)$, $A(n)^+$ is generated by Sq^{2^m} for all m, $0 \leq m \leq n$, and so an element r of A is in $\mathrm{ra}(A(n)^+)$ if and only if $Sq^{2^m}r = 0$ for these m. By the induction hypothesis, this is then equivalent to the conditions $Sq^{2^n}r = 0$ and $r \in \mathrm{ra}(A(n-1)^+) = V_{n-1}^{\mathrm{adm}}$.

Let r be a non-zero element of $\mathrm{ra}(A(n)^+)$. We may then write $r = \sum_{\mathbf{a}\in\mathbf{A}} Sq^{\mathbf{a}}$ as a sum of admissibles of V_{n-1}^{adm}. Thus, for each $\mathbf{a}$, $a_i \equiv 1 \bmod 2^{n+1-i}$ if $1 \leq i \leq n$. In order to prove that $r \in V_n^{\mathrm{adm}}$, we must show that, for each $\mathbf{a} \in \mathbf{A}$, $a_i \equiv 1 \bmod 2^{n+2-i}$ if $1 \leq i \leq n+1$.

The role of the technical fact is to supply the admissible decomposition of $Sq^{2^n} r$, namely, there are sets $\mathbf{E_a}$ of admissibles for which

$$Sq^{2^n} r = \sum_{\mathbf{a}\in\mathbf{A}} \binom{a_1 - 1}{2^n} Sq^{a_1+2^n} Sq^{\mathbf{a}'} + \sum_{\mathbf{a}\in\mathbf{A}} \sum_{\mathbf{e}\in\mathbf{E_a}} Sq^{a_1+2^{n-1}} Sq^{\mathbf{e}}$$

is a sum of admissibles. As, by hypothesis, $Sq^{2^n} r = 0$, binomial coefficients must vanish or terms must cancel or both.

Fix $\mathbf{a}$. We show first that $a_1 \equiv 1 \bmod 2^{n+1}$, or, equivalently, that $\binom{a_1-1}{2^n} \equiv 0$ since, by the induction hypothesis, $a_1 = 1 + x2^n$ for an integer x. Assume that $a_1 \not\equiv 1 \bmod 2^{n+1}$, i.e., that x is odd so that $a_1 = 1 + 2^n + \frac{x-1}{2} 2^{n+1}$. The admissible term $Sq^{a_1+2^n} Sq^{\mathbf{a}'}$ in the expansion of $Sq^{2^n} r$ given above must then cancel with another term. It is clear that it cannot cancel with another of the first type. Suppose then that it cancels with an admissible of the second type corresponding to an admissible $\mathbf{b}$, say, so that $a_1 + 2^n = b_1 + 2^{n-1}$ and $\mathbf{a}' = \mathbf{e}$ for an admissible $\mathbf{e} \in \mathbf{E_b}$. Write $b_1 = 1 + y2^n$. Note that $a_1 + 2^n \equiv 1 \bmod 2^{n+1}$. If y is even, then $b_1 + 2^{n-1} \equiv 1 + 2^{n-1} \bmod 2^{n+1}$, a contradiction. If y is odd, then $b_1 + 2^{n-1} \equiv 1 + 2^{n-1} + 2^n \bmod 2^{n+1}$, again a contradiction. Thus, $a_1 \equiv 1 \bmod 2^{n+1}$ for all $\mathbf{a}$ in $\mathbf{A}$ as required. Moreover there are no terms of the first type appearing in the expansion given for $Sq^{2^n} r$.

As to the second type of term, let a be one of the values occurring among the a_1, and let $\mathbf{A}_a$ be the set of those $\mathbf{a} \in \mathbf{A}$ for which $a_1 = a$. As cancellation of terms corresponding to $\mathbf{a} \in \mathbf{A}_a$ can only occur with other such terms,

$$0 = \sum_{\mathbf{a}\in\mathbf{A}_a} \sum_{\mathbf{e}\in\mathbf{E_a}} Sq^{a+2^{n-1}} Sq^{\mathbf{e}} = Sq^{a+2^{n-1}} \sum_{\mathbf{a}\in\mathbf{A}_a} \sum_{\mathbf{e}\in\mathbf{E_a}} Sq^{\mathbf{e}}.$$

By admissibility, it follows that

$$0 = \sum_{\mathbf{a}\in\mathbf{A}_a} \sum_{\mathbf{e}\in\mathbf{E_a}} Sq^{\mathbf{e}} = \sum_{\mathbf{a}\in\mathbf{A}_a} Sq^{2^{n-1}} Sq^{\mathbf{a}'}.$$

With $s = \sum_{\mathbf{a}\in\mathbf{A}_a} Sq^{\mathbf{a}'}$, we see that $Sq^{2^{n-1}} s = 0$. The induction hypothesis implies that $s \in \mathrm{ra}(A(n-2)^+) = V_{n-2}^{\mathrm{adm}}$ and so $s \in \mathrm{ra}(A(n-1)^+)$. But then, for each $\mathbf{a} \in \mathbf{A}$, $Sq^{\mathbf{a}'} \in \mathrm{ra}(A(n-1)^+)$ and so $a_i \equiv 1 \bmod 2^{n+1-(i-1)} = 2^{n+2-i}$ if $2 \leq i \leq n+1$, which is the final fact needed to show that the admissible $Sq^{\mathbf{a}}$ belongs to V_n^{adm}. □

We turn now to the application of these technical results to the unit group of A. Before leaving them, we remark that the result $V_n^{\mathrm{adm}} = V_n = t_n A$ and the identities involving t_n are not isolated phenomena but rather one extreme of a range of similar results [Sa07]. At the other extreme lie analogous results

centred on the Milnor basis elements $Sq(1, \cdots, 1)$; compare, for example, the identities in Sect. 5.2 of [Wo98].

2.10 Lemma *Let $n \geq 0$. Then there is an involution t in U for which $A(n) \cap A(n)^t = \mathbf{F}_2$.*

Proof. It suffices to show that $A(n)^+ \cap A(n)^{+t} = 0$. Choose m such that, for each admissible $\mathbf{a}$ for which $Sq^{\mathbf{a}}$ occurs in the expression of an element of $A(n)$ in the admissible basis, $2^m \geq 2a_1$.

Let $r = Sq^{\mathbf{x}} Sq^{2^m}$ with

$$x_i = 1 + (m + 1 - i + 2^m)2^{m+2-i}, 1 \leq i \leq m + 1,$$

and $x_i = 0$ otherwise (r is the admissible of smallest degree in V_m^{adm} for which the $(m + 2)$nd superfix is 2^m). By the proposition, $r \in \mathrm{ra}(A(m)^+)$. Since $Sq^{2^m} \in A(m)^+$, it follows that $r^2 = 0$ so that $t := 1 + r$ is an involution.

Let $s \in A(n)^+, s \neq 0$. Then $s^t := t^{-1}st = (1+r)s(1+r) = (1+r)s = s+rs$ since $m \geq n$. With s expressed as $\sum Sq^{\mathbf{a}}$ in the admissible basis, we see that $rSq^{\mathbf{a}}$ is also admissible because of the choice of m. Again by the definition of m, $rSq^{\mathbf{a}}$ does not occur in the expression of an element of $A(n)$ in the admissible basis so that $rs \notin A(n)$. Thus, $s^t \notin A(n)^+$, as required. □

The group U acts on the algebra A by conjugation so that, for $r \in A$, the standard centraliser notation $C_U(r)$ is meaningful. The centraliser of r in A itself, $C_A(r)$, is simply $\mathbf{F}_2 + C_U(r)$, while, for $u \in U$, $C_U(u) = 1 + C_{A^+}(u)$.

2.11 Theorem *Let u be a non-identity element in the unit group U of the Steenrod algebra A and let r be a non-scalar element of A. Then $C_U(u)$ is of infinite index in U and $C_A(r)$ is of infinite codimension in A. Both $C_U(u)$ and $C_A(r)$ are infinite.*

Proof. It is convenient to approach these results through one of the equivalent formulations mentioned in the introduction. That the first result is equivalent to the statement that every non-identity conjugacy class of the unit group is infinite is a standard argument in group theory: the size of the conjugacy class of an element is the index of the centraliser of the element in the whole group. That this statement is equivalent to saying that every non-identity normal subgroup is infinite, is easy to see in a locally finite group from the facts that a normal subgroup is a union of conjugacy classes and that the subgroup generated by a conjugacy class is normal. We take the conjugacy class approach.

Suppose that $C := u^U$, the conjugacy class of u in U, is finite. As A is locally finite, C is contained in $A(n)$ for some n. By the lemma, there is a unit t for which $A(n) \cap A(n)^t = \mathbf{F}_2$ so that $C = C^t \subseteq \mathbf{F}_2$, whence $C = \{1\}$, a contradiction.

For the second statement, if $r \in U$, then $C_A(r)$ is of finite codimension in A if and only if $C_U(r)$ is of finite index in U. If $r \notin U$, then $r \in A^+$ so that $1 + r \in U$ and $C_A(r) = C_A(1 + r)$.

For the last statement, suppose that $r \in A(n)$. From the description of $t_n A$ as V_n^{adm}, it is clear that there are infinitely many admissibles of the form $Sq^{\mathbf{x}} t_n$, where $Sq^{\mathbf{x}}$ is in V_n^{adm}. Thus, the subalgebra $t_n A t_n$ is infinite, and each of its elements centralises r. □

The result generalises from individual elements to finite subsets in two ways, to centralisers and to normalisers. The centraliser $C_U(R)$ of a subset R of A is defined as $\{u \in U \,|\, r^u = r \text{ for all } r \in R\}$, while its normaliser $N_U(R)$ is $\{u \in U \,|\, r^u \in R \text{ for all } r \in R\}$. The generalisations are straightforward corollaries of 2.11 and its proof.

2.12 Corollary *Let R be a finite subset of the Steenrod algebra A not contained in the base field. Then both $C_U(R)$ and $N_U(R)$ are infinite and of infinite index in U.*

The admissible basis can also be used to prove a result of the same type about A, without the intervention of group theory, namely, the fact that ideals are infinite. For two-sided ideals, however, this fact is an immediate consequence of one of the versions of 2.11, the fact that non-identity normal subgroups are infinite. To see this, note that, if I is a two-sided ideal of A, $I \neq A$, then $I \subseteq A^+$, the unique maximal ideal of A, and $1 + I$ is a subgroup of U, necessarily normal.

2.13 Proposition *Every non-zero ideal of A is infinite-dimensional.*

Proof. Because of the existence of the antipode χ [Wo98], it suffices to prove the result for left ideals. Further, we need only consider principal ideals. Let $r \in A, r \neq 0$, and write r as the sum of admissibles $Sq^{\mathbf{a}}$. Suppose that m is such that $2^m \geq 2a_1$ for each $\mathbf{a}$ which appears. Then $Sq^{2^m} r = \sum Sq^{2^m} Sq^{\mathbf{a}}$ is also a sum of admissibles. If n is another such integer, $n \neq m$, then $Sq^{2^n} r \neq Sq^{2^m} r$; this gives infinitely many elements of the principal ideal Ar. □

The group U also acts on the vector space A by right multiplication and by left multiplication. Properties of one of these actions are related to those of the other via the antipode so we focus just on right multiplication. One common convention in a group action is to denote the stabiliser in U of an element r of A by $C_U(r)$, that is, in this context $C_U(r) = \{u \in U \,|\, ru = r\}$. Note that, if $r \neq 0$, then the stabiliser $C_A(r)$ of r in the right action of A on itself is $C_U(r)$. As in Theorem 2.11 which implies that the orbits of non-central elements of A under the conjugation action of U are infinite, so are the orbits of right multiplication; we state this result in its stabiliser form.

2.14 Theorem *The stabiliser of a non-zero element of the Steenrod algebra in the action of the unit group by either right or left multiplication is infinite and of infinite index.*

Proof. It is easy to check that, if $r \neq 0$, then the right annihilator $\mathrm{ra}(r) = 1 + C_U(r)$, and so, by 2.13, is infinite. Again by the previous proposition,

$A/\mathrm{ra}(r) \approx rA$ is infinite-dimensional whence $\mathrm{ra}(r)$ is of infinite codimension and $C_U(r)$ of infinite index. □

3. Other results

With the recognition of U as a locally finite 2-group, the hope arises that the long-established theory of locally finite groups might provide insights into U and A which had not been made before. We report in this section results in this direction.

One of the few results about infinite locally finite groups which apply in full generality is the fact that such a group contains an infinite abelian subgroup. This is a substantial theorem in the general case but the proof in the p-group case is an exercise [Ro96, Exer. 14.3.8, p. 436]. It has long been known, however, that A contains infinite commutative subalgebras, for example, the exterior algebra of countable dimension; it follows that U contains the corresponding infinite abelian subgroup. Explicit examples of infinite commutative subalgebras appear in the proof of 2.11, namely, the subspaces t_nAt_n for $n \geq 0$. These are nilsubalgebras, i.e., all products vanish, and so commutative. Each is contained in the first, Sq^1ASq^1, a subalgebra which can be viewed as comprising roughly a quarter of the Steenrod algebra (e.g., by dimension as degree increases). The subalgebra $\mathbf{F}_2Sq^1 + Sq^1ASq^1$ is a maximal nilsubalgebra as it is the intersection of $\mathrm{ra}(Sq^1) = Sq^1A$ and the left annihilator $\mathrm{la}(Sq^1) = ASq^1$.

The outer automorphisms of infinite locally finite groups have also been much studied (an outer automorphism of a group G is one which is not induced by conjugation by an element of G, an inner automorphism). In this regard the situation in the Steenrod group is favourable. We have seen in the main theorem of the previous section that the group $\mathrm{Inn}(U)$ of inner automorphisms of U is isomorphic to U as, for any group G, $\mathrm{Inn}(G) \approx G/\zeta(G)$. Thus, to show that U has infinitely many outer automorphisms, it suffices to find a single such automorphism: its composites with inner automorphisms would all be outer. This can be accomplished constructively in U by using the antipode. Note that, on U, the antipode commutes with the inversion anti-automorphism of U.

3.1 Proposition *The composition of the antipode with inversion in U is an outer automorphism of U.*

Proof. The antipode χ sends A^+ to itself and induces an anti-automorphism of U. Define the automorphism ϕ of U by $\phi(u) = \chi(u^{-1}) = \chi(u)^{-1}$. We show that ϕ is outer.

Let I_n be the subspace of A spanned by monomials of degree greater than or equal to n. Then I_n is a two-sided ideal of A and so $1 + I_n$ is a normal subgroup of U. As χ preserves degree, ϕ leaves $1 + I_n$ invariant and so acts on the associated graded Lie algebra $\bigoplus(1+I_n)/(1+I_{n+1})$. Note that, because the exponent of $(1 + I_n)/(1 + I_{n+1})$ is 2, the action of ϕ on it is just that of χ.

Moreover, this action is not trivial. For example, ϕ sends the coset of $1+Sq^3$ to that of $1+Sq^2Sq^1$ and these cosets are not equivalent modulo $1+I_4$ because Sq^3 is not equivalent to Sq^2Sq^1 modulo I_4 as both monomials are admissibles.

The conjugation action of U on $\bigoplus(1+I_n)/(1+I_{n+1})$ is trivial, however. To see this, take $r \in I_n$ and $u = 1+s \in U$. Then

$$(1+r)^u = 1 + (\sum s^i)r(1+s) = 1 + r + q,$$

where $q \in I_{n+1}$. But $1+r+q = (1+r)(1+(1+r)^{-1}q)$ which is equivalent to $1+r$ modulo $1+I_{n+1}$. $\square$

For locally finite p-groups which are countably infinite, such as U, a stronger result is known, namely, that such a group has an uncountably infinite outer automorphism group [Pu92, Theorem 2]. We do not know how to prove this for U independently, nor whether such a result holds for A.

Because of the importance and ubiquity of the Steenrod algebra, it seems desirable to learn more about its group of units in its own right. Even elementary facts about its group theory are unexplored. Its local finiteness is obtained by realising it as the union of the canonical finite subgroups $U(n)$. The nature of these subgroups is unclear. The group $U(1)$ is small enough to study exhaustively; results about it, mainly due to Donald Coleman, are reported in [Wo98]. These groups grow rapidly with n however.

Acknowledgements. This work was prompted and guided by Reg Wood.

References

[AS72] Abramowitz, M.; Stegun, I.A. (eds.) (1972): Handbook of mathematical functions. New York: Dover 1972

[Ma83] Margolis, H.R.: Spectra and the Steenrod algebra. Amsterdam: Elsevier 1983

[Pu92] Puglisi, O.: A note on the automorphism group of a locally finite p-group Bull. London Math. Soc. **24**, 437-441 (1992)

[Ro96] Robinson, D.J.S.: A course in the theory of groups. Second edition. (Graduate Texts in Mathematics **80**) New York: Springer 1996

[Sa07] Sandling, R.: The lattice of column 2-regular partitions in the Steenrod algebra.

[SE62] Steenrod, N.E., Epstein, D.B.A.: Cohomology operations. (Ann. Math. Stud. **50**) Princeton: Princeton University Press 1962

[Wo98] Wood, R.M.W.: Problems in the Steenrod algebra. Bull. London Math. Soc. **30**, 449–517 (1998)