IDENTITIES FOR CONJUGATION
IN THE STEENROD ALGEBRA

PHILIP D. STRAFFIN, JR.

ABSTRACT. Let $\chi$ be the canonical conjugation in the Steenrod algebra $\mathcal{A}_2$. I prove the identity

$$Sq^{2n} + \chi(Sq^n) = Sq^{2n-1} \chi(Sq^{2n-1})$$

and generalizations of this identity both in $\mathcal{A}_2$ and in $\mathcal{A}_p$ where $p$ is an odd prime.

The canonical conjugation $\chi$ in the mod 2 Steenrod algebra $\mathcal{A}_2$ can be defined by Thom's recursion formula

$$\sum_{i=0}^{n} Sq^i \chi(Sq^{n-i}) = 0$$

together with the stipulation that $\chi: \mathcal{A}_2 \rightarrow \mathcal{A}_2$ be an anti-isomorphism [3]. Since the elements $Sq^{2n}$ multiplicatively generate $\mathcal{A}_2$, we can calculate $\chi$ if we can calculate $\chi(Sq^{2n})$ for all $n$. The above recursion formula is unnecessarily cumbersome for this goal. In fact, the recursion can be shortened considerably by use of the following interesting

Identity. $Sq^{2n} + \chi(Sq^n) = Sq^{2n-1} \chi(Sq^{2n-1})$ for all positive integers $n$.

Applying the identity recursively we obtain the

Formula.

$$\chi(Sq^{2n}) = Sq^{2n} + \sum_{i=1}^{n-1} \left( \prod_{j=1}^{i} Sq^{2n-j} \right) Sq^{2n-i}.$$ 

For example,

$$\chi(Sq^{16}) = Sq^{16} + Sq^8Sq^8 + Sq^8Sq^4Sq^4 + Sq^8Sq^4Sq^2.$$ 

In this paper, I will prove a theorem which will imply the above identity, and which also yields results about the mod $p$ Steenrod algebra $\mathcal{A}_p$ when $p$ is an odd prime. The technique is to use Milnor's calculation of $\chi$ in the

Received by the editors March 25, 1974.


Key words and phrases. Steenrod algebra, conjugation, Milnor basis, binomial coefficients mod $p$. 

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
Milnor basis for $\mathbb{Q}_p$ [2], together with properties of binomial coefficients mod $p$. This technique was noticed independently by Donald Davis, who used it to prove other identities involving $\chi$ in $\mathbb{Q}_p$ [1].

Let $p$ be a fixed prime. Let $R = (r_1, r_2, \ldots)$ be a sequence of non-negative integers with only a finite number of nonzero terms. For each such $R$ there is an element $\beta^R$ in the Milnor basis for $\mathbb{Q}_p$, of degree $\sum_{i \geq 1} 2(p^i - 1)r_i$ (if $p = 2$, the element is written $Sq^R$ and its degree is $\sum_{i \geq 1} (2^i - 1)r_i$). We define $|R| = \sum_{i \geq 1} p^{i-1}r_i$. Then Davis' main proposition can be written.

**Proposition 1.** $\beta^m \chi(\beta^n) = (-1)^n \sum_{R} \binom{\frac{|R|}{m}}{\beta^R}$ where the sum is taken over all $R$ such that $\beta^R$ has the proper degree, i.e. over all $R$ such that

$$\sum_{i \geq 1} (p^i - 1)r_i = (p - 1)(m + n).$$

If $p = 2$, the only necessary modification is to write $Sq$ for $\beta$. The binomial coefficient is, of course, to be interpreted mod $p$.

**Proof.** See [1]. $\Box$

The one additional fact about binomial coefficients which we will need is

**Proposition 2.** Let $a$ and $b$ be integers. If $p^a \leq r \leq p^ab$, then

$$\sum_{k=0}^{b} (-1)^k \binom{r}{p^a k} \equiv 0 \pmod{p}. $$

**Proof.** Write $r = p^a s + t$, with $1 \leq s \leq b$ and $0 \leq t < p^a$. Then

$$\binom{p^a s + t}{p^a k} \equiv \binom{s}{k} \pmod{p},$$

as is easily seen by comparing the coefficients of $x^{p^ak}$ in the congruence

$$(1 + x)^{p^a s + t} \equiv (1 + x^{p^a})^s (1 + x)^t \pmod{p}. $$

Hence the proposition follows from the well-known identity $\sum_{k=0}^{b} (-1)^k \binom{s}{k} = 0$ for $1 \leq s \leq b$. $\Box$

We can now prove our main

**Theorem.** Let $a \geq 0$ and $b > 1$ be integers. Then

$$\sum_{k=0}^{b} \beta^{p^a k} \chi(\beta^{p^a (b-k)}) = 0.$$

**Examples.** (1) If $a = 0$, we get Thom's original recursion formula in $\mathbb{Q}_p$.

(2) If $p = 2$, $a = n - 1$, $b = 2$, we get the identity at the beginning of this paper.
(3) If $p = 2$, $a = 2$, $b = 3$, we get
\[ \chi(Sq^{12}) + Sq^4 \chi(Sq^8) + Sq^8 \chi(Sq^4) + Sq^{12} = 0. \]
(4) If $p = 3$, $a = 2$, $b = 3$, we get
\[ \chi(\mathcal{P}^{27}) + \mathcal{P}^9 \chi(\mathcal{P}^{18}) + \mathcal{P}^{18} \chi(\mathcal{P}^9) + \mathcal{P}^{27} = 0. \]

**Proof of Theorem.** Consider any $R = (r_1, r_2, \ldots)$ such that
\[ \sum_{i \geq 1} (p^i - 1) r_i = (p - 1)p^a b. \]

The coefficient of $\mathcal{P}^R$ in the Milnor base expansion of the sum in the Theorem is, by Proposition 1,
\[ \sum_{k = 0}^{b} (-1)^{p^a (b - k)} \binom{|R|}{p^a k} = (-1)^b \sum_{k = 0}^{b} (-1)^k \binom{|R|}{p^a k}. \]
By Proposition 2, this coefficient is zero if $p^a \leq |R| \leq p^a b$. But (*) gives that
\[ |R| = \sum_{i \geq 1} p^{i-1} r_i = \frac{1}{p} \left( (p - 1)p^a b + \sum_{i \geq 1} r_i \right) \]
and we also have
\[ 0 \leq \sum_{i \geq 1} r_i \leq \frac{1}{p - 1} \sum_{i \geq 1} (p^i - 1) r_i = p^a b. \]
Hence $((p - 1)/p)p^a b \leq |R| \leq p^a b$; and since $b > 1$, the required inequality holds. \(\Box\)

**BIBLIOGRAPHY**


DEPARTMENT OF MATHEMATICS, BELOIT COLLEGE, BELOIT, WISCONSIN 53511