The nilpotence degree of torsion elements in lambda–rings

F.J.-B.J. Clauwens

April 7, 2010

1 Introduction.

If $A$ is a $\lambda$-ring then for each prime number $p$ one has a map $\theta^p : A \to A$ such that

- The map $\psi^p : A \to A$ defined by $\psi^p(a) = a^p - p\theta^p(a)$ is a ring homomorphism.
- The following formulas hold for all $a, b \in A$:
  \[
  \theta^p(1) = 0
  \]
  \[
  \theta^p(a + b) = \theta^p(a) + \theta^p(b) + \sum_{j=1}^{p-1} \binom{p}{j} a^j b^{p-j}
  \]
  \[
  \theta^p(ab) = \theta^p(a)\psi^p(b) + a^p \theta^p(b)
  \]
  \[
  \theta^p \psi^p(a) = \psi^p \theta^p(a)
  \]

Moreover the maps $\psi^p$ and $\theta^r$ commute also for $r \neq p$. Conversely if a commutative ring $A$ is equipped with maps $\psi^p$ and $\theta^p$ satisfying the above identities then $A$ has a unique structure of $\lambda$-ring such that the $\psi^p$ are the associated Adams operations. We refer to [1] for generalities about $\lambda$-rings.

In [2] it is shown that a torsion element in a $\lambda$-ring is nilpotent. The purpose of this note is to give a sharp estimate of the nilpotence degree.

Let us call a ring $A$ equipped with one operation $\theta^p$ satisfying the above conditions a $\theta^p$-ring. We will prove that if $A$ is a $\theta^p$-ring and $a \in A$ satisfies $p^e a = 0$ then $a^{p^e + p^{e-1}} = 0$. In order to show that this estimate is sharp we exhibit a $\lambda$-ring $A$ and an element $a \in A$ such that $p^e a = 0$ but $a^{p^e + p^{e-1}} \neq 0$.

If $a$ is an element of a $\lambda$-ring $A$ and $na = 0$ for some $n \in \mathbb{Z}$ then by the above theorem we have

\[
(n p^{-e})^{p^e + p^{e-1}} a^{p^e + p^{e-1}} = 0
\]

where $p^e$ is the highest power of $p$ dividing $n$. Since the greatest common divisor of the numbers $(np^{-e})^{p^e + p^{e-1}}$ is 1 it follows that

\[
a^E = 0, \text{ where } E = \max\{p^e + p^{e-1} ; p^e \text{ divides } n\}
\]
2 The nilpotency estimate.

In this section $A$ is a $\lambda$-ring at $p$, and $a \in A$ satisfies $p^e a = 0$ for some $e > 0$. We will write $\psi^p$ for the $e$-fold iterate of $\psi^p$.

**Proposition 1.** For any $b \in A$ one has $\theta^p(pb) = p^{e-1}b^p - \psi^p(b)$.

*Proof.* By definition of $\lambda$-ring at $p$ one has $\theta^p(pb) = \theta^p(p)b^p + \psi^p(p)\theta^p(b)$. Now substitute $\psi^p(p) = p$, $\theta^p(p) = p^{e-1} - 1$ and $p\theta^p(b) = b^p - \psi^p(b)$. \qed

**Proposition 2.** For $0 \leq k \leq e$ one has $p^{e-k}\psi^k(a) = 0$.

*Proof.* By induction on $k$. For $k = 0$ the conclusion $p^e a = 0$ is given. Now assume the statement is true for $k = m$. Then by the last proposition one has

$$0 = \theta^p(0) = \theta^p(p \cdot p^{e-m-1}\psi^m(a))$$

$$= p^{e-1}(p^{e-m-1}\psi^m(a))p - \psi^p(p^{e-m-1}\psi^m(a))$$

$$= -\psi^p(p^{e-m-1}\psi^m(a)) = p^{e-m-1}\psi^{m+1}(a)$$

since $(p - 1) + (e - m - 1) \geq e - m$ for $m < e$. \qed

**Proposition 3.** For $0 \leq k \leq e - 1$ one has $a^{e+p-1} = \psi^k(a^{e-k} + p^{e-k-1})$.

*Proof.* By induction on $k$. For $k = 0$ both sides are identical. Assume that the statement is true for $k = m < e - 1$. Then one has

$$a^{e+p-1} = (\psi^m(a)p)^{e-m-2}(p+1)$$

$$= (\psi^m(a) + p\theta^p\psi^m(a))^{e-m-2}(p+1)$$

$$= \sum_i \binom{e-m-2}{i}(p\theta^p\psi^m(a))^i\psi^{m+1}(a)^{e-m-2(p+1)-i}$$

If $0 < i < p^{e-m-2}(p+1)$ then the number of factors $p$ in the corresponding term is

$$i + v_p\left(p^{e-m-2}(p+1)\right) \geq i + v_p(p^{e-m-2}(p+1)) - v_p(i)$$

$$\geq i + (e + m - 2) - (i - 1) = e + m - 1$$

and it also contains a factor $\psi^{m+1}(a)$. Hence by Proposition 2 it vanishes.

If $i = p^{e-m-2}(p+1)$ then the term is a multiple of $p^{e+1-m}\theta^p\psi^m(a)$, since $p^j(p+1) \geq j + 3$ for all $j \geq 0$. But this expression equals

$$p^{e+1-m}\psi^m(a)\theta^p(a) = p^{e-m}\psi^m(a^p - \psi^p(a)) =$$

$$p^{e-m}\psi^m(a)p - \psi^p(p^{e-m}\psi^m(a)) = 0 - 0 = 0$$

by Proposition 2.

Thus only the term with $i = 0$ remains, which proves the statement for $k = m + 1$. \qed
Theorem 1. \( a^{p^e + p^{e-1}} = 0 \).

Proof. By the last Proposition we have

\[
\begin{align*}
a^{p^e + p^{e-1}} &= \psi^{p^{e-1}}(a^{p^e + 1}) \\
&= \psi^{p^{e-1}}(a)\psi^{p^{e-1}}(a^p) \\
&= \psi^{p^{e-1}}(a)\psi^{p^e}(a) + p\psi^{p^{e-1}}(a)\psi^{p^{e-1}}(a)
\end{align*}
\]

which vanishes since \( \psi^{p^e}(a) = 0 \) and \( p\psi^{p^{e-1}}(a) = 0 \) by Proposition 2.

\[\Box\]

3 The example ring.

We write \( K \) for the localization \( \mathbb{Z}_{(p)} \) of the ring of ordinary integers at \( p \), in which every prime \( r \neq p \) is invertible. It carries a unique structure of \( \lambda \)-ring such that all Adams operations \( \psi^q \) coincide with the identity map.

We write \( R \) for the polynomial ring \( K[x, y] \), and \( \phi: R \to R \) for the homomorphism given by \( \phi(x) = x^p - py, \phi(y) = y^p \).

Proposition 4. For every \( f \in R \), one has \( \phi(f) = f^p \) mod \( pR \).

Proof. The statement is obviously true if \( f \in K \) or \( f = x \) or \( f = y \). Moreover if it is true for \( f \) and \( g \) then it is also true for \( f + g \) and \( fg \).

The Proposition tells us that we can define a \( \theta^p \)-structure on \( R \) by putting \( \psi^p(f) = \phi(f) \) and \( \theta^p(f) = p^{-1}(f^p - \phi(f)) \). One can extend this to a structure of \( \lambda \)-ring by declaring \( \psi^r(x) = 0 \) and \( \psi^r(y) = 0 \) for primes \( r \) different from \( p \).

Definition 1. \( F_n \in \mathbb{Z}[s, t] \) is defined recursively by:

\[
F_0(s, t) = s, \quad F_n(s, t) = F_{n-1}(s, t)^p - pF_{n-1}(t, 0)
\]

Lemma 1. One has

\[
F_n(s, t) = F_{n-1}(s^p - pt, t^p)
\]

Proof. By induction. For \( n = 1 \) both sides read \( s^p - pt \). If the statement is true for \( n \) then \( F_{n+1}(s, t) = F_n(s, t)^p - pF_n(t, 0) = F_{n-1}(s^p - pt, t^p) - pF_{n-1}(t^p, 0) = F_n(s^p - pt, t^p) \).

The point of this definition is that

\[
\psi^p F_n(x, y) = F_n(\psi^p(x), \psi^p(y)) = F_n(x^p - py, y^p) = F_{n+1}(x, y)
\]

Definition 2. The ideal \( J \) of \( R \) is the one generated by the \( p^{e-n} F_n(x, y) \) for \( 0 \leq n \leq e \) and by \( y^p \).

Proposition 5. The ideal \( J \) is stable under \( \theta^p \).
Proof. From the formulas for $\theta^p$ of a sum and $\theta^p$ of a product it follows that is sufficient to check that the generators of $J$ are mapped to $J$. For $n < \varepsilon$ we have

\[
\theta^p(p^{\varepsilon-n}F_n(x,y)) = p^{-1}\left((p^{\varepsilon-n}F_n(x,y))^p - \psi^p(p^{\varepsilon-n}F_n(x,y))\right)
\]

\[
= p^{(\varepsilon-n)p-1}F_n(x,y) - p^{\varepsilon-n-1}F_{n+1}(x,y)
\]

where the second term is obviously in $J$ and the first term is in $J$ since $(\varepsilon - n)p - 1 \geq \varepsilon - n$. Furthermore

\[
\theta^p(F_e(x,y)) = p^{-1}(F_e(x,y)^p - F_e(x^p - py, y^p))
\]

\[
= p^{-1}(F_e(x,y)^p - F_{e+1}(x,y))
\]

\[
= p^{-1}(pF_e(y,0)) = f_e(y,0) = y^\psi
\]

and finally $\theta^p(y^\psi) = 0$ since $\psi^p(y) = y^p$. □

The Proposition tells us that the quotient ring $A = R/J$ inherits a structure of $\theta^p$-ring, and in fact a structure of $\lambda$-ring. We will show now that the class $a$ of $x$ in $R/J$ satisfies $\sigma^{p^k+p^{k-1}-1} \neq 0$.

The main ingredient for proving this is the following elementary Proposition:

**Proposition 6.** Let $k$ be a commutative ring. Let $\rho: k[\xi, \eta] \to k[x, y]$ be the homomorphism given by $\rho(\xi) = x^p$, $\rho(\eta) = y^p$. Let $M$ be an ideal of $k[\xi, \eta]$ with generators $g_j$, and let $N$ be the ideal of $k[x, y]$ generated by $\rho(g_j)$. Then $k[x, y]/N$ is a free module over $k[\xi, \eta]/M$ via $\rho$ with basis the classes of the $x^k y^m$ for $0 \leq k, m < p$.

In particular if the class of $\xi^a$ is nonzero in $k[\xi, \eta]/M$ then the class of $x^m y^m$ is nonzero in $k[x, y]/N$.

**Proof.** If $b \in k[x, y]/N$ then it is the class $[f]$ of a certain $f \in k[x, y]$. Now $f \in k[x, y]$ can be written uniquely as $\sum_{0 \leq k, m < p} x^k y^m \rho(f_{km})$ for certain $f_{km} \in k[\xi, \eta]$, and therefore $b = \sum_{k, m} [x^k y^m] \rho(f_{km})$.

On the other hand if $\sum_{k, m} [x^k y^m] \rho(f_{km}) = 0$ then there must be $h_j \in k[x, y]$ such that $\sum_{k, m} x^k y^m \rho(f_{km}) = \sum h_j \rho(g_j)$. Moreover each $h_j$ can be written as $\sum_{k, m} x^k y^m \rho(h_{jkm})$. Therefore

\[
\sum_{k, m} x^k y^m \rho(f_{km}) = \sum_{k, m} x^k y^m \rho(\sum_j g_j h_{jkm})
\]

By uniqueness this implies $f_{km} = \sum_j g_j h_{jkm}$. This means that $[f_{km}] = 0$. □

In order to apply this in an induction to prove the main theorem we need another property of the $F_n$:

**Lemma 2.** If $n > 0$ then $F_n(s, t) = F_{n-1}(s^p, t^p) \mod p^n$. 

4
Proof. If \( n = 1 \) this reads \( s^p - pt = s^p \mod p \). If the statement is true for \( n \) then

\[
F_{n+1}(s,t) = F_n(s,t)^p - pF_n(t,0)
= (F_{n-1}(s^p,t^p) \mod p^n)^p - p(F_{n-1}(t^p,0) \mod p^n)
= F_{n-1}(s^p,t^p)^p - pF_{n-1}(t^p,0) \mod p^{n+1}
= F_n(s^p,t^p)
\]

Here we used the fact that \( u = v \mod p^n \) implies \( u^p = v^p \mod p^{n+1} \). □

In order to show that \( a^{s^e+p^{e-1}-1} \) is nonzero in \( A = K[x,y]/J \) we prove that is even nonzero in \( A/p^{e+1} \) (which is of course not a \( \theta^e \)-ring):

**Theorem 2.** The class of \( x^{p^e+p^{e-1}-1} \) is nonzero in \( \mathbb{Z}/p^{e+1}[x,y] \) modulo the ideal generated by the \( p^{e-n}F_n(x,y) \) for \( 0 \leq n \leq e \) and by \( y^{p^{e+1}} \).

**Proof.** We use induction in \( e \). For \( e = 1 \) the statement says that \( x^p \neq 0 \) in \( \mathbb{Z}/p^2[x,y]/(px, x^p - py, yp) \). This is obvious by inspection.

If the statement is true for certain \( e \) then by Proposition 6 the class of \( x^{p^e+p^{e-1}-1} \) is nonzero in \( \mathbb{Z}/p^{e+1}[x,y] \) modulo the ideal generated by the \( p^{e-n}F_n(x,y) \) for \( 0 \leq n \leq e \) and by \( y^{p^{e+1}} \). By Lemma 2 this ideal coincides with the ideal generated by the \( p^{e-n}F_{n+1}(x,y) \) for \( 0 \leq n \leq e \) and by \( y^{p^{e+1}} \).

A fortiori the class of \( x^{p^{e+1}+p^{e-1}} \) is nonzero in \( \mathbb{Z}/p^{e+2}[x,y] \) modulo the ideal generated by the same polynomials and \( p^{e+1}F_0(x,y) \). But this is just the statement for \( e + 1 \). □

**References**
