Witt vectors. Part 1

Michiel Hazewinkel

Sidenotes by Darij Grinberg

Witt#0: Teichmüller representatives

[not completed, not proofread]

The purpose of this note is to correct the results from section 4 of [1] and to give detailed proofs for them.

First, section 4 of [1] has four mistakes. Let us correct them:

- "The ring of power series $k((T))$" should be "The ring of power series $k[[T]]$".
- The map σ is never defined. It should be defined by $\sigma = \mathbf{f}_p$.
- In the sentence directly following (4.1), the term $\sigma^{-1}(x)$ should be $\sigma^{-r}(x)$ instead.
- We need to suppose that A is not only complete, but also separated (i. e., Hausdorff) in the $\mathfrak{m}$-adic topology. (Otherwise, at least some of the results stated in section 4 of [1] become false.)

Now it is time to formulate the main results of section 4 of [1]. But first we introduce a notation:

Definition. Let A be a ring, and $p \in \mathbb{N}$ a prime. An element $a \in A$ is said to be *p-ancient* if and only if

$$\left(\text{for every } \mu \in \mathbb{N}, \text{ there exists some } b \in A \text{ such that } b^{p^\mu} = a\right).$$

With this definition, we can notice that for any commutative ring A with unity,

- $$\text{the element } 0 \in A \text{ is } p\text{-ancient}$$
  (since $0 = 0^{p^\mu}$ for every $\mu \in \mathbb{N}$);
- $$\text{the element } 1 \in A \text{ is } p\text{-ancient}$$
  (since $1 = 1^{p^\mu}$ for every $\mu \in \mathbb{N}$);
- $$\text{if two elements } a \text{ and } a' \text{ of } A \text{ are } p\text{-ancient, then their product } aa' \text{ is } p\text{-ancient as well} \tag{1}$$
  (since for every $\mu \in \mathbb{N}$, there exists some $b \in A$ such that $b^{p^\mu} = a$ (since a is p-ancient), and there exists some $b' \in A$ such that $(b')^{p^\mu} = a'$ (since a' is p-ancient), and hence $(bb')^{p^\mu} = b^{p^\mu}(b')^{p^\mu} = aa'$, which shows that aa' is p-ancient as well);

•

$$\text{if } p\cdot 1_A = 0 \text{ in } A\text{, and if two elements } a \text{ and } a' \text{ of } A \text{ are } p\text{-ancient, then their sum } a+a' \text{ is } p\text{-ancient as well} \qquad (2)$$

(since for every $\mu \in \mathbb{N}$, there exists some $b \in A$ such that $b^{p^\mu} = a$ (since a is p-ancient), and there exists some $b' \in A$ such that $(b')^{p^\mu} = a'$ (since a' is p-ancient), and hence

$$(b+b')^{p^\mu} = \underbrace{b^{p^\mu}}_{=a} + \underbrace{(b')^{p^\mu}}_{=a'} \qquad \text{(by the Idiot's Binomial Formula, since } p\cdot 1_A = 0 \text{ in } A)$$
$$= a + a',$$

which shows that $a+a'$ is p-ancient as well);

Now come the (corrected) main assertions of section 4 of [1]:

Theorem 1. Let A be a commutative ring with unity, and let $\mathfrak{m}$ be an ideal[1] of A. Let $p \in \mathbb{N}$ be a prime such that $p \cdot 1_k = 0$ in the ring $k = A \diagup \mathfrak{m}$. Assume that the ring homomorphism

$$\sigma : k \to k \text{ defined by } \sigma(x) = x^p \text{ for every } x \in k$$

is bijective[2]. Suppose, further, that the ring A is complete and separated in the $\mathfrak{m}$-adic topology.

For every element u of A, we let $\overline{u}$ denote the canonical projection of u onto the factor ring $A \diagup \mathfrak{m}$.

(a) For every $x \in k$, there exists one and only one p-ancient element a of A such that $\overline{a} = x$.

We will denote this element a by $t(x)$. Clearly, $\overline{t(x)} = x$ for every $x \in k$.

Thus, we have defined a map $t : k \to A$.

(b) We have $t(0) = 0$, $t(1) = 1$ and $t(xx') = t(x)\,t(x')$ for any two elements x and x' of k.

(c) If $p \cdot 1_A = 0$ in A, then $t(x+x') = t(x) + t(x')$ for any two elements x and x' of k.

(d) If $t' : k \to A$ is a map such that

$$(t'(xx') = t'(x)\,t'(x') \text{ for any two elements of } x \text{ and } x' \text{ of } k) \qquad (3)$$

and

$$\left(\overline{t'(x)} = x \text{ for every } x \in k\right), \qquad (4)$$

then $t' = t$.

[1]not necessarily a maximal ideal, despite the label $\mathfrak{m}$ being mostly used for maximal ideals in literature

[2]This map $\sigma : k \to k$ is indeed a ring homomorphism, since $p \cdot 1_k = 0$ in the ring k. It is the so-called *Frobenius endomorphism* of the ring k.

(e) If $t' : k \to A$ is a map such that

$$\left(t'(x^p) = (t'(x))^p \text{ for any } x \in k\right) \tag{5}$$

and

$$\left(\overline{t'(x)} = x \text{ for every } x \in k\right), \tag{6}$$

then $t' = t$.

Note that for every $x \in k$, the element $t(x)$ is called the *Teichmüller representative* of x in A. Theorem 1 **(a)** characterizes this Teichmüller representative $t(x)$ as the only p-ancient element of A whose residue class modulo $\mathfrak{m}$ is x. Theorem 1 **(b)** shows that the Teichmüller system of representatives is multiplicative and respects 0 and 1. Roughly speaking, Theorem 1 **(d)** says that it is actually the only multiplicative system of representatives, and Theorem 1 **(e)** says that it is the only system of representatives that commutes with taking the p-th power.

Before we start proving Theorem 1, a lemma (generalizing Lemma 3 in [2]):

Lemma 2. Let A be a commutative ring with unity, and $p \in \mathbb{N}$ be a nonnegative integer[3]. Let $\mathfrak{m} \subseteq A$ be an ideal such that $p \cdot 1_A \in \mathfrak{m}$. Let $k \in \mathbb{N}$ and $\ell \in \mathbb{N}$ be such that $k > 0$. Let $a \in A$ and $b \in A$. If $a \equiv b \bmod \mathfrak{m}^k$, then $a^{p^\ell} \equiv b^{p^\ell} \bmod \mathfrak{m}^{k+\ell}$.

Proof of Lemma 2. Assume that $a \equiv b \bmod \mathfrak{m}^k$. We need to show that every $\ell \in \mathbb{N}$ satisfies $a^{p^\ell} \equiv b^{p^\ell} \bmod \mathfrak{m}^{k+\ell}$.

We will show this by induction over ℓ. For $\ell = 0$, the claim that $a^{p^\ell} \equiv b^{p^\ell} \bmod \mathfrak{m}^{k+\ell}$ is true (because it is equivalent to $a \equiv b \bmod \mathfrak{m}^k$). Now, for the induction step, we assume that $a^{p^\ell} \equiv b^{p^\ell} \bmod \mathfrak{m}^{k+\ell}$ for some $\ell \in \mathbb{N}$, and we want to show that $a^{p^{\ell+1}} \equiv b^{p^{\ell+1}} \bmod \mathfrak{m}^{k+\ell+1}$. In fact, we have $a \equiv b \bmod \mathfrak{m}$ (because $a \equiv b \bmod \mathfrak{m}^k$ yields $a - b \in \mathfrak{m}^k \subseteq \mathfrak{m}$ (since $k > 0$)) and thus

$$\sum_{k=0}^{p-1} \left(a^{p^\ell}\right)^k \left(b^{p^\ell}\right)^{p-1-k} \equiv \sum_{k=0}^{p-1} \underbrace{\left(b^{p^\ell}\right)^k \left(b^{p^\ell}\right)^{p-1-k}}_{=\left(b^{p^\ell}\right)^{p-1}} = \sum_{k=0}^{p-1} \left(b^{p^\ell}\right)^{p-1} = p\left(b^{p^\ell}\right)^{p-1} \equiv 0 \bmod \mathfrak{m}$$

(since $p \cdot 1_A \in \mathfrak{m}$ yields $p \cdot 1_A \equiv 0 \bmod \mathfrak{m}$), so that $\sum\limits_{k=0}^{p-1} \left(a^{p^\ell}\right)^k \left(b^{p^\ell}\right)^{p-1-k} \in \mathfrak{m}$. Hence,

$$\begin{aligned} a^{p^{\ell+1}} - b^{p^{\ell+1}} &= \left(a^{p^\ell}\right)^p - \left(b^{p^\ell}\right)^p = \underbrace{\left(a^{p^\ell} - b^{p^\ell}\right)}_{\substack{\in \mathfrak{m}^{k+\ell}\text{, since} \\ a^{p^\ell} \equiv b^{p^\ell} \bmod \mathfrak{m}^{k+\ell}}} \cdot \underbrace{\sum_{k=0}^{p-1} \left(a^{p^\ell}\right)^k \left(b^{p^\ell}\right)^{p-1-k}}_{\in \mathfrak{m}} \\ &\qquad \left(\text{since } x^q - y^q = (x-y) \cdot \sum_{k=0}^{q-1} x^k y^{q-1-k} \text{ for any } q \in \mathbb{N}\text{, any } x \in A \text{ and any } y \in A\right) \\ &\in \mathfrak{m}^{k+\ell} \cdot \mathfrak{m} = \mathfrak{m}^{k+\ell+1}, \end{aligned}$$

[3] Though we call it p, we do not require it to be a prime!

so that $a^{p^{\ell+1}} \equiv b^{p^{\ell+1}} \operatorname{mod} \mathfrak{m}^{k+\ell+1}$, and the induction step is complete. Thus, Lemma 2 is proven.

Proof of Theorem 1. Before we start proving Theorem 1, we notice three trivial things: First,

$$\overline{0} = 0, \qquad \overline{1} = 1, \qquad \overline{xy} = \overline{x} \cdot \overline{y}, \qquad \overline{x+y} = \overline{x} + \overline{y}, \qquad \overline{x^n} = \overline{x}^n$$

for any $x \in A$, $y \in A$ and $n \in \mathbb{N}$. This is all because the canonical projection $A \to A/\mathfrak{m}$ is a ring homomorphism.

Besides,

$$y^{p^s} = \sigma^s(y) \qquad \text{for every } y \in k \text{ and } s \in \mathbb{N}. \tag{7}$$

(This follows by induction over s from the fact that $x^p = \sigma(x)$ for every $x \in k$).

Finally, since the canonical projection $A \to A/\mathfrak{m}$ is a ring homomorphism, we have $\overline{p \cdot 1_A} = p \cdot 1_k = 0$. Thus, $p \cdot 1_A \in \mathfrak{m}$.

(a) In order to prove Theorem 1 **(a)**, we have two prove two assertions:

Assertion 1: For every $x \in k$, there exists at least one p-ancient element a of A such that $\overline{a} = x$.

Assertion 2: For every $x \in k$, there exists at most one p-ancient element a of A such that $\overline{a} = x$.

Once these two Assertions are proven, Theorem 1 **(a)** will immediately follow.

Proof of Assertion 1. Let $x \in k$. For every $r \in \mathbb{N}$, let y_r be an element of A satisfying $\overline{y_r} = \sigma^{-r}(x)$. (Such a y_r clearly exists.) First, we are going to prove that

$$\text{for every } \mu \in \mathbb{N}, \text{ the sequence } \left(y_{r+\mu}^{p^r}\right)_{r\in\mathbb{N}} \text{ is a Cauchy sequence with respect to the } \mathfrak{m}\text{-adic topology.} \tag{8}$$

In fact, this requires proving that for every $\nu \in \mathbb{N}$, there exists some $N \in \mathbb{N}$ such that $y_{i+\mu}^{p^i} \equiv y_{j+\mu}^{p^j} \operatorname{mod} \mathfrak{m}^\nu$ for every $i \geq N$ and every $j \geq N$. We will prove this for $N = \max\{\nu-1, 0\}$. Namely, if $i \geq \max\{\nu-1, 0\}$ and $j \geq \max\{\nu-1, 0\}$, then $i-(\nu-1) \geq 0$ (since $i \geq \max\{\nu-1, 0\} \geq \nu-1$) and $j-(\nu-1) \geq 0$ (similarly), so that

$$\begin{aligned}\overline{y_{i+\mu}^{p^{i-(\nu-1)}}} &= \overline{y_{i+\mu}}^{p^{i-(\nu-1)}} = \underbrace{\left(\sigma^{-(i+\mu)}(x)\right)^{p^{i-(\nu-1)}}}_{\substack{=\sigma^{i-(v-1)}\left(\sigma^{-(i+\mu)}(x)\right)\\ \text{by (7)}}} \\ &\qquad \left(\text{since } \overline{y_{i+\mu}} = \sigma^{-(i+\mu)}(x) \text{ by the definition of } y_{i+\mu}\right) \\ &= \sigma^{i-(\nu-1)}\left(\sigma^{-(i+\mu)}(x)\right) = \sigma^{i-(\nu-1)-(i+\mu)}(x) = \sigma^{-(\nu-1)-\mu}(x)\end{aligned}$$

and

$$\begin{aligned}\overline{y_{j+\mu}^{p^{j-(\nu-1)}}} &= \overline{y_{j+\mu}}^{p^{j-(\nu-1)}} = \underbrace{\left(\sigma^{-(j+\mu)}(x)\right)^{p^{j-(\nu-1)}}}_{\substack{=\sigma^{j-(v-1)}\left(\sigma^{-(j+\mu)}(x)\right)\\ \text{by (7)}}} \\ &\qquad \left(\text{since } \overline{y_{j+\mu}} = \sigma^{-(j+\mu)}(x) \text{ by the definition of } y_{j+\mu}\right) \\ &= \sigma^{j-(v-1)}\left(\sigma^{-(j+\mu)}(x)\right) = \sigma^{j-(\nu-1)-(j+\mu)}(x) = \sigma^{-(\nu-1)-\mu}(x),\end{aligned}$$

so that $\overline{y_{i+\mu}^{p^{i-(\nu-1)}}} = \overline{y_{j+\mu}^{p^{j-(\nu-1)}}}$ and thus $y_{i+\mu}^{p^{i-(\nu-1)}} \equiv y_{j+\mu}^{p^{j-(\nu-1)}} \operatorname{mod} \mathfrak{m}$, so that Lemma 2 (applied to $a = y_{i+\mu}^{p^{i-(\nu-1)}}$, $b = y_{j+\mu}^{p^{j-(\nu-1)}}$, $k = 1$ and $\ell = \nu - 1$) yields $\left(y_{i+\mu}^{p^{i-(\nu-1)}}\right)^{p^{\nu-1}} \equiv \left(y_{j+\mu}^{p^{j-(\nu-1)}}\right)^{p^{\nu-1}} \operatorname{mod} \mathfrak{m}^\nu$, what rewrites as $y_{i+\mu}^{p^i} \equiv y_{j+\mu}^{p^j} \operatorname{mod} \mathfrak{m}^\nu$ (since $\left(y_{i+\mu}^{p^{i-(\nu-1)}}\right)^{p^{\nu-1}} = y_{i+\mu}^{p^i}$ and $\left(y_{j+\mu}^{p^{j-(\nu-1)}}\right)^{p^{\nu-1}} = y_{j+\mu}^{p^j}$). Thus, the sequence $\left(y_{r+\mu}^{p^r}\right)_{r\in\mathbb{N}}$ is a Cauchy sequence with respect to the $\mathfrak{m}$-adic topology. This proves (8).

Since the ring A is complete in the $\mathfrak{m}$-adic topology, every Cauchy sequence with respect to the $\mathfrak{m}$-adic topology has a limit in A. Thus, by (8), for every $\mu \in \mathbb{N}$, the sequence $\left(y_{r+\mu}^{p^r}\right)_{r\in\mathbb{N}}$ has a limit $\lim\limits_{r\to\infty} y_{r+\mu}^{p^r} \in A$. In particular, for $\mu = 0$, this means that the sequence $\left(y_r^{p^r}\right)_{r\in\mathbb{N}}$ has a limit $\lim\limits_{r\to\infty} y_r^{p^r} \in A$. We denote this limit by a; thus, $a = \lim\limits_{r\to\infty} y_r^{p^r}$.

Now, we are going to prove that the element $a \in A$ is p-ancient and satisfies $\overline{a} = x$. Once this is proven, Assertion 1 will immediately follow.

The element a is p-ancient, since for every $\mu \in \mathbb{N}$, there exists some $b \in A$ such that $b^{p^\mu} = a$ (in fact, take $b = \lim\limits_{r\to\infty} y_{r+\mu}^{p^r}$; then,

$$\begin{aligned} b^{p^\mu} &= \left(\lim_{r\to\infty} y_{r+\mu}^{p^r}\right)^{p^\mu} = \lim_{r\to\infty} \left(\underbrace{\left(y_{r+\mu}^{p^r}\right)^{p^\mu}}_{=y_{r+\mu}^{p^r p^\mu} = y_{r+\mu}^{p^{r+\mu}}} \right) \qquad \text{(since the map } A \to A,\ u \mapsto u^{p^\mu} \text{ is continuous)} \\ &= \lim_{r\to\infty} y_{r+\mu}^{p^{r+\mu}} = \lim_{r\to\infty} y_r^{p^r} \qquad \text{(here we substituted } r \text{ for } r+\mu \text{ in the limit)} \\ &= a \end{aligned}$$

). Besides, the canonical projection from A to $A/\mathfrak{m}$ is continuous (where the ring A is given the $\mathfrak{m}$-adic topology, and the ring $A/\mathfrak{m}$ is given the discrete topology), so that

$$\overline{\lim_{r\to\infty} y_r^{p^r}} = \lim_{r\to\infty} \underbrace{\overline{y_r^{p^r}}}_{\substack{=\overline{y_r}^{p^r} \\ =\left(\sigma^{-r}(x)\right)^{p^r}}} = \lim_{r\to\infty} \underbrace{\left(\sigma^{-r}(x)\right)^{p^r}}_{\substack{=\sigma^r\left(\sigma^{-r}(x)\right) \\ \text{by (7)}}} = \lim_{r\to\infty} \sigma^r\left(\sigma^{-r}(x)\right) = \lim_{r\to\infty} x = x.$$

Since $\lim\limits_{r\to\infty} y_r^{p^r} = a$, this rewrites as $\overline{a} = x$. Hence, we have shown that a is p-ancient and satisfies $\overline{a} = x$. This proves Assertion 1.

Proof of Assertion 2. Let a_1 and a_2 be two p-ancient elements of A such that $\overline{a_1} = x$ and $\overline{a_2} = x$. We are going to prove that $a_1 = a_2$.

We will first prove that $a_1 - a_2 \in \mathfrak{m}^s$ for every $s \in \mathbb{N}$.

In fact, for every $\mu \in \mathbb{N}$, there exists some $b \in A$ such that $b^{p^\mu} = a_1$ (since a_1 is p-ancient). Applied to $\mu = s$, this yields that there exists some $b \in A$ such that $b^{p^s} = a_1$. Denote this b by b_1; thus we have found some $b_1 \in A$ such that $b_1^{p^s} = a_1$.

Similarly, we can find some $b_2 \in A$ such that $b_2^{p^s} = a_2$. Now,

$$\sigma^s\left(\overline{b_1 - b_2}\right) = \sigma^s\left(\overline{b_1} - \overline{b_2}\right) = \underbrace{\sigma^s\left(\overline{b_1}\right)}_{\substack{=\overline{b_1}^{p^s} \\ \text{by (7)}}} - \underbrace{\sigma^s\left(\overline{b_2}\right)}_{\substack{=\overline{b_2}^{p^s} \\ \text{by (7)}}} \qquad \text{(since } \sigma^s \text{ is a ring homomorphism)}$$
$$= \overline{b_1}^{p^s} - \overline{b_2}^{p^s} = \underbrace{\overline{b_1^{p^s}}}_{=\overline{a_1}=x} - \underbrace{\overline{b_2^{p^s}}}_{=\overline{a_2}=x} = 0,$$

so that $\overline{b_1 - b_2} = 0$ (since $\sigma : k \to k$ is bijective, and thus $\sigma^s : k \to k$ is bijective as well). Therefore, $b_1 - b_2 \in \mathfrak{m}$ and thus $b_1 \equiv b_2 \mod \mathfrak{m}$. Consequently, Lemma 2 (applied to b_1, b_2, 1 and s instead of a, b, k and ℓ) yields $b_1^{p^s} \equiv b_2^{p^s} \mod \mathfrak{m}^{s+1}$ for every $s \in \mathbb{N}$. Thus, for every $s \in \mathbb{N}$, we have $b_1^{p^s} - b_2^{p^s} \in \mathfrak{m}^{s+1} = \mathfrak{m} \cdot \mathfrak{m}^s \subseteq \mathfrak{m}^s$ (since $\mathfrak{m}^s$ is an ideal). Since $b_1^{p^s} = a_1$ and $b_2^{p^s} = a_2$, this rewrites as follows: For every $s \in \mathbb{N}$, we have $a_1 - a_2 \in \mathfrak{m}^s$. Hence, $a_1 - a_2 \in \bigcap_{s \in \mathbb{N}} \mathfrak{m}^s$. But $\bigcap_{s \in \mathbb{N}} \mathfrak{m}^s = 0$, since the ring A is separated in the $\mathfrak{m}$-adic topology. Thus, $a_1 - a_2 \in 0$. In other words, $a_1 - a_2 = 0$, so that $a_1 = a_2$.

Hence, for any two p-ancient elements a_1 and a_2 of A such that $\overline{a_1} = x$ and $\overline{a_2} = x$, we have proven that $a_1 = a_2$. In other words, we have shown that any two p-ancient elements a of A such that $\overline{a} = x$ must be equal. Thus, Assertion 2 is proven.

Now that both Assertions 1 and 2 are proven, Theorem 1 **(a)** becomes obvious.

(b) The element $t(0)$ is defined as the only p-ancient element a of A such that $\overline{a} = 0$. Hence, $t(0) = 0$ (because 0 is a p-ancient element of A and satisfies $\overline{0} = 0$).

The element $t(1)$ is defined as the only p-ancient element a of A such that $\overline{a} = 1$. Hence, $t(1) = 1$ (because 1 is a p-ancient element of A and satisfies $\overline{1} = 1$).

Now, let x and x' be two elements of k. We want to prove that $t(xx') = t(x)t(x')$. We know that $t(x)$ is a p-ancient element of A and that $\overline{t(x)} = x$. We also know that $t(x')$ is a p-ancient element of A and that $\overline{t(x')} = x'$. Now, the element $t(xx')$ is defined as the only p-ancient element a of A such that $\overline{a} = xx'$. Hence, $t(xx') = t(x)t(x')$ (because $t(x)t(x')$ is a p-ancient element of A [4] and satisfies $\overline{t(x)t(x')} = \underbrace{\overline{t(x)}}_{=x} \underbrace{\overline{t(x')}}_{=x'} = xx'$).

Thus, Theorem 1 **(b)** is completely proven.

(c) Assume (for the duration of the proof of Theorem 1 **(c)**) that $p \cdot 1_A = 0$ in A. Let x and x' be two elements of k. We want to prove that $t(x + x') = t(x) + t(x')$. We know that $t(x)$ is a p-ancient element of A and that $\overline{t(x)} = x$. We also know that $t(x')$ is a p-ancient element of A and that $\overline{t(x')} = x'$. Now, the element $t(x + x')$ is defined as the only p-ancient element a of A such that $\overline{a} = x + x'$. Hence, $t(x + x') = t(x) + t(x')$ (because $t(x) + t(x')$ is a p-ancient element of A [5] and satisfies $\overline{t(x) + t(x')} = \underbrace{\overline{t(x)}}_{=x} + \underbrace{\overline{t(x')}}_{=x'} = x + x'$). This proves Theorem 1 **(c)**.

(e) We can easily see that

$$t'\left(y^{p^\mu}\right) = \left(t'(y)\right)^{p^\mu} \text{ for any } y \in k \text{ and any } \mu \in \mathbb{N} \tag{9}$$

[4] by (1), since $t(x)$ and $t(x')$ are p-ancient

[5] by (2), since $t(x)$ and $t(x')$ are p-ancient

[6]. Hence,

$$t'(x) = \left(t'\left(\sigma^{-\mu}(x)\right)\right)^{p^\mu} \text{ for any } y \in k \text{ and any } \mu \in \mathbb{N} \qquad (10)$$

[7]. Thus, for every $x \in k$, the element $t'(x) \in A$ is p-ancient (in fact, for every $\mu \in \mathbb{N}$, there exists some $b \in A$ such that $b^{p^\mu} = t'(x)$, namely $b = t'(\sigma^{-\mu}(x))$). Besides, this element $t'(x)$ satisfies $\overline{t'(x)} = x$ (by (6)). On the other hand, we know that the only p-ancient element $a \in A$ that satisfies $\overline{a} = x$ is $t(x)$. Thus, $t'(x) = t(x)$. We have proven this for every $x \in k$; hence, $t' = t$. Thus, Theorem 1 **(e)** is proven.

(d) By induction, (3) yields (5). Also, clearly, (4) is equivalent to (6). Thus, (5) and (6) hold, and therefore, Theorem 1 **(e)** yields that $t' = t$. This proves Theorem 1 **(d)**.

Now, the proof of Theorem 1 is complete.

References

[1] Michiel Hazewinkel, *Witt vectors. Part 1*, revised version: 20 April 2008.

[2] Darij Grinberg, *Witt#3: Ghost component computations.*

---

[6] *Proof of (9) by induction over μ:*

Induction base: For $\mu = 0$, the equation (9) is trivially true.

Induction step: Assume that some given $\mu \in \mathbb{N}$ satisfies

$$t'\left(y^{p^\mu}\right) = (t'(y))^{p^\mu} \text{ for any } y \in k.$$

Then,

$$t'\left(y^{p^{\mu+1}}\right) = (t'(y))^{p^{\mu+1}} \text{ for any } y \in k,$$

because

$$\begin{aligned} t'\left(y^{p^{\mu+1}}\right) &= t'\left(y^{p^\mu p}\right) = t'\left(\left(y^{p^\mu}\right)^p\right) = \left(t'\left(y^{p^\mu}\right)\right)^p && \left(\text{by (5), applied to } x = y^{p^\mu}\right) \\ &= \left((t'(y))^{p^\mu}\right)^p && (\text{by the induction assumption}) \\ &= (t'(y))^{p^\mu p} = (t'(y))^{p^{\mu+1}}, \end{aligned}$$

and the induction step is complete. Thus, (9) is proven.

[7] since

$$t'(x) = t'\left(\underbrace{\sigma^\mu\left(\sigma^{-\mu}(x)\right)}_{\substack{=\left(\sigma^{-\mu}(x)\right)^{p^\mu} \\ \text{by (7)}}}\right) = t'\left(\left(\sigma^{-\mu}(x)\right)^{p^\mu}\right) = \left(t'\left(\sigma^{-\mu}(x)\right)\right)^{p^\mu}$$

(by (9), applied to $y = \sigma^{-\mu}(x)$)