Witt vectors. Part 1
Michiel Hazewinkel
Sidenotes by Darij Grinberg

Witt#2: Polynomials that can be written as w_n
[version 1.0 (15 April 2013), completed, sloppily proofread]

This is an addendum to section 5 of [1]. We recall the definition of the p-adic Witt polynomials:

> **Definition.** Let p be a prime. For every $n \in \mathbb{N}$ (where $\mathbb{N}$ means $\{0, 1, 2, ...\}$), we define a polynomial $w_n \in \mathbb{Z}[X_0, X_1, X_2, ..., X_n]$ by
>
> $$w_n(X_0, X_1, ..., X_n) = X_0^{p^n} + pX_1^{p^{n-1}} + p^2 X_2^{p^{n-2}} + ... + p^{n-1} X_{n-1}^p + p^n X_n = \sum_{k=0}^{n} p^k X_k^{p^{n-k}}.$$
>
> Since $\mathbb{Z}[X_0, X_1, X_2, ..., X_n]$ is a subring of the ring $\mathbb{Z}[X_0, X_1, X_2, ...]$ (this is the polynomial ring over $\mathbb{Z}$ in the countably many indeterminates X_0, X_1, X_2, ...), this polynomial w_n can also be considered as an element of $\mathbb{Z}[X_0, X_1, X_2, ...]$. Regarding w_n this way, we have
>
> $$w_n(X_0, X_1, X_2, ...) = \sum_{k=0}^{n} p^k X_k^{p^{n-k}}.$$
>
> We will often write X for the sequence $(X_0, X_1, X_2, ...)$. Thus, $w_n(X) = \sum\limits_{k=0}^{n} p^k X_k^{p^{n-k}}$.
>
> These polynomials $w_0(X)$, $w_1(X)$, $w_2(X)$, ... are called the *p-adic Witt polynomials.*[1]

A property of these polynomials has not been recorded in the text:

> **Theorem 1.** Let $\tau \in \mathbb{Z}[X_0, X_1, X_2, ...]$ be a polynomial. Let $n \in \mathbb{N}$. Then, the following two assertions $\mathcal{A}$ and $\mathcal{B}$ are equivalent:
>
> *Assertion $\mathcal{A}$:* There exist polynomials τ_0, τ_1, ..., τ_n in $\mathbb{Z}[X_0, X_1, X_2, ...]$ such that
>
> $$\tau(X) = w_n(\tau_0(X), \tau_1(X), ..., \tau_n(X)).$$
>
> *Assertion $\mathcal{B}$:* We have $\dfrac{\partial}{\partial X_i}(\tau(X)) \in p^n \mathbb{Z}[X_0, X_1, X_2, ...]$ for every $i \in \mathbb{N}$.

[1] *Caution:* These polynomials are referred to as w_0, w_1, w_2, ... in Sections 5-8 of [1]. However, beginning with Section 9 of [1], Hazewinkel uses the notations w_1, w_2, w_3, ... for some *different* polynomials (the so-called big Witt polynomials, defined by formula (9.25) in [1]), which are *not the same as our polynomials* w_1, w_2, w_3, ... (though they are related to them: in fact, the polynomial w_k that we have just defined here is the same as the polynomial which is called w_{p^k} in [1] from Section 9 on, up to a change of variables; however, the polynomial which is called w_k from in [1] from Section 9 on is totally different and has nothing to do with our w_k).

Proof of Theorem 1. Proof of the implication $\mathcal{A} \Longrightarrow \mathcal{B}$: Assume that Assertion $\mathcal{A}$ holds, i. e., that there exist polynomials τ_0, τ_1, ..., τ_n in $\mathbb{Z}[X_0, X_1, X_2, ...]$ such that

$$\tau(X) = w_n(\tau_0(X), \tau_1(X), ..., \tau_n(X)).$$

Then,

$$\tau(X) = w_n(\tau_0(X), \tau_1(X), ..., \tau_n(X)) = \sum_{k=0}^{n} p^k (\tau_k(X))^{p^{n-k}},$$

so that every $i \in \mathbb{N}$ satisfies

$$\frac{\partial}{\partial X_i}(\tau(X)) = \frac{\partial}{\partial X_i} \sum_{k=0}^{n} p^k (\tau_k(X))^{p^{n-k}} = \sum_{k=0}^{n} p^k \underbrace{\frac{\partial}{\partial X_i}(\tau_k(X))^{p^{n-k}}}_{\substack{=p^{n-k}(\tau_k(X))^{p^{n-k}-1}\cdot\frac{\partial}{\partial X_i}(\tau_k(X)) \\ \text{(by the chain rule, since} \\ \frac{\partial}{\partial Y}\left(Y^{p^{n-k}}\right)=p^{n-k}Y^{p^{n-k}-1})}}$$

$$= \sum_{k=0}^{n} \underbrace{p^k p^{n-k}}_{=p^n} (\tau_k(X))^{p^{n-k}-1} \cdot \frac{\partial}{\partial X_i}(\tau_k(X)) = p^n \underbrace{\sum_{k=0}^{n} (\tau_k(X))^{p^{n-k}-1} \cdot \frac{\partial}{\partial X_i}(\tau_k(X))}_{\in\mathbb{Z}[X_0,X_1,X_2,...]}$$

$$\in p^n \mathbb{Z}[X_0, X_1, X_2, ...],$$

and thus Assertion $\mathcal{B}$ holds. This proves the implication $\mathcal{A} \Longrightarrow \mathcal{B}$.

Proof of the implication $\mathcal{B} \Longrightarrow \mathcal{A}$: Proving the implication $\mathcal{B} \Longrightarrow \mathcal{A}$ is equivalent to proving the following fact:

Lemma: Let $\tau \in \mathbb{Z}[X_0, X_1, X_2, ...]$ be a polynomial. Let $n \in \mathbb{N}$. If $\frac{\partial}{\partial X_i}(\tau(X)) \in p^n \mathbb{Z}[X_0, X_1, X_2, ...]$ for every $i \in \mathbb{N}$, then there exist polynomials τ_0, τ_1, ..., τ_n in $\mathbb{Z}[X_0, X_1, X_2, ...]$ such that

$$\tau(X) = w_n(\tau_0(X), \tau_1(X), ..., \tau_n(X)).$$

Proof of the Lemma: We will prove the Lemma by induction over n. For $n = 0$, the Lemma is trivial (just set $\tau_0 = \tau$ and use $w_0(X) = X_0$). Now to the induction step: Given some $n \in \mathbb{N}$ such that $n \geq 1$, we want to prove the Lemma for this n, and we assume that it is already proven for $n - 1$ instead of n. So let $\tau \in \mathbb{Z}[X_0, X_1, X_2, ...]$ be a polynomial such that $\frac{\partial}{\partial X_i}(\tau(X)) \in p^n \mathbb{Z}[X_0, X_1, X_2, ...]$ for every $i \in \mathbb{N}$. We must find polynomials τ_0, τ_1, ..., τ_n in $\mathbb{Z}[X_0, X_1, X_2, ...]$ such that

$$\tau(X) = w_n(\tau_0(X), \tau_1(X), ..., \tau_n(X)).$$

Let $\mathbb{N}^{\mathbb{N}}_{\text{fin}}$ denote the set $\left\{(j_0, j_1, j_2, ...) \in \mathbb{N}^{\mathbb{N}} \mid \text{only finitely many } k \in \mathbb{N} \text{ satisfy } j_k \neq 0\right\}$. Then, τ has a unique representation in the form $\tau(X) = \sum_{(j_0,j_1,j_2,...)\in\mathbb{N}^{\mathbb{N}}_{\text{fin}}} t_{(j_0,j_1,j_2,...)} X_0^{j_0} X_1^{j_1} X_2^{j_2} ...$ with $t_{(j_0,j_1,j_2,...)} \in \mathbb{Z}$ for every $(j_0, j_1, j_2, ...) \in \mathbb{N}^{\mathbb{N}}_{\text{fin}}$ (in fact, every polynomial in $\mathbb{Z}[X_0, X_1, X_2, ...]$

has a unique representation of this kind). Every $i \in \mathbb{N}$ satisfies

$$\begin{aligned}
\frac{\partial}{\partial X_i}\left(\tau\left(X\right)\right) &= \frac{\partial}{\partial X_i}\left(\sum_{(j_0,j_1,j_2,\ldots)\in\mathbb{N}^{\mathbb{N}}_{\text{fin}}} t_{(j_0,j_1,j_2,\ldots)} X_0^{j_0} X_1^{j_1} X_2^{j_2} \ldots\right) \\
&= \sum_{(j_0,j_1,j_2,\ldots)\in\mathbb{N}^{\mathbb{N}}_{\text{fin}}} t_{(j_0,j_1,j_2,\ldots)} X_0^{j_0} X_1^{j_1} X_2^{j_2} \ldots X_{i-1}^{j_{i-1}} \left(\frac{\partial}{\partial X_i} X_i^{j_i}\right) X_{i+1}^{j_{i+1}} \ldots \\
&= \sum_{(j_0,j_1,j_2,\ldots)\in\mathbb{N}^{\mathbb{N}}_{\text{fin}}} t_{(j_0,j_1,j_2,\ldots)} X_0^{j_0} X_1^{j_1} X_2^{j_2} \ldots X_{i-1}^{j_{i-1}} \left(j_i X_i^{j_i-1}\right) X_{i+1}^{j_{i+1}} \ldots \\
&= \sum_{(j_0,j_1,j_2,\ldots)\in\mathbb{N}^{\mathbb{N}}_{\text{fin}}} j_i t_{(j_0,j_1,j_2,\ldots)} X_0^{j_0} X_1^{j_1} X_2^{j_2} \ldots X_{i-1}^{j_{i-1}} X_i^{j_i-1} X_{i+1}^{j_{i+1}} \ldots .
\end{aligned}$$

Hence, for every $(j_0, j_1, j_2, \ldots) \in \mathbb{N}^{\mathbb{N}}_{\text{fin}}$, the coefficient of the polynomial $\dfrac{\partial}{\partial X_i}\left(\tau\left(X\right)\right)$ before the monomial $X_0^{j_0} X_1^{j_1} X_2^{j_2} \ldots X_{i-1}^{j_{i-1}} X_i^{j_i-1} X_{i+1}^{j_{i+1}} \ldots$ is $j_i t_{(j_0,j_1,j_2,\ldots)}$. Therefore, $\dfrac{\partial}{\partial X_i}\left(\tau\left(X\right)\right) \in p^n \mathbb{Z}\left[X_0, X_1, X_2, \ldots\right]$ rewrites as $j_i t_{(j_0,j_1,j_2,\ldots)} \in p^n\mathbb{Z}$ for every $(j_0, j_1, j_2, \ldots) \in \mathbb{N}^{\mathbb{N}}_{\text{fin}}$ (because a polynomial in $\mathbb{Z}\left[X_0, X_1, X_2, \ldots\right]$ lies in $p^n \mathbb{Z}\left[X_0, X_1, X_2, \ldots\right]$ if and only if each of its coefficients lies in $p^n\mathbb{Z}$). In particular, this yields that

$$\text{for every } (j_0, j_1, j_2, \ldots) \in \mathbb{N}^{\mathbb{N}}_{\text{fin}} \text{ satisfying } p \nmid t_{(j_0,j_1,j_2,\ldots)}, \text{ we have } j_i / p^n \in \mathbb{Z} \text{ for every } i \in \mathbb{N} \tag{1}$$

(because $j_i t_{(j_0,j_1,j_2,\ldots)} \in p^n\mathbb{Z}$ and $p \nmid t_{(j_0,j_1,j_2,\ldots)}$ lead to $j_i \in p^n\mathbb{Z}$, since p is a prime).

We also notice that

$$a \equiv a^{p^n} \operatorname{mod} p \qquad \text{for every } a \in \mathbb{Z} \tag{2}$$

(since Fermat's Little Theorem yields $a^{p^k} \equiv \left(a^{p^k}\right)^p = a^{p^{k+1}} \operatorname{mod} p$ for every $k \in \mathbb{N}$, and thus by induction we get $a^{p^0} \equiv a^{p^n} \operatorname{mod} p$).

Now, define a polynomial $\rho \in \mathbb{Z}\left[X_0, X_1, X_2, \ldots\right]$ by

$$\rho\left(X\right) = \sum_{\substack{(j_0,j_1,j_2,\ldots)\in\mathbb{N}^{\mathbb{N}}_{\text{fin}};\\ p\nmid t_{(j_0,j_1,j_2,\ldots)}}} t_{(j_0,j_1,j_2,\ldots)} X_0^{j_0/p^n} X_1^{j_1/p^n} X_2^{j_2/p^n} \ldots$$

(this is actually a polynomial because of (1)). Then,

$$\begin{aligned}
\tau(X) &= \sum_{(j_0,j_1,j_2,\ldots)\in\mathbb{N}^{\mathbb{N}}_{\text{fin}}} t_{(j_0,j_1,j_2,\ldots)} X_0^{j_0} X_1^{j_1} X_2^{j_2} \ldots \\
&= \sum_{\substack{(j_0,j_1,j_2,\ldots)\in\mathbb{N}^{\mathbb{N}}_{\text{fin}};\\ p\mid t_{(j_0,j_1,j_2,\ldots)}}} \underbrace{t_{(j_0,j_1,j_2,\ldots)}}_{\substack{\equiv 0 \bmod p\text{, since}\\ p\mid t_{(j_0,j_1,j_2,\ldots)}}} X_0^{j_0} X_1^{j_1} X_2^{j_2} \ldots + \sum_{\substack{(j_0,j_1,j_2,\ldots)\in\mathbb{N}^{\mathbb{N}}_{\text{fin}};\\ p\nmid t_{(j_0,j_1,j_2,\ldots)}}} t_{(j_0,j_1,j_2,\ldots)} X_0^{j_0} X_1^{j_1} X_2^{j_2} \ldots \\
&\equiv \underbrace{\sum_{\substack{(j_0,j_1,j_2,\ldots)\in\mathbb{N}^{\mathbb{N}}_{\text{fin}};\\ p\mid t_{(j_0,j_1,j_2,\ldots)}}} 0 X_0^{j_0} X_1^{j_1} X_2^{j_2} \ldots}_{=0} + \sum_{\substack{(j_0,j_1,j_2,\ldots)\in\mathbb{N}^{\mathbb{N}}_{\text{fin}};\\ p\nmid t_{(j_0,j_1,j_2,\ldots)}}} t_{(j_0,j_1,j_2,\ldots)} X_0^{j_0} X_1^{j_1} X_2^{j_2} \ldots \\
&= \sum_{\substack{(j_0,j_1,j_2,\ldots)\in\mathbb{N}^{\mathbb{N}}_{\text{fin}};\\ p\nmid t_{(j_0,j_1,j_2,\ldots)}}} \underbrace{t_{(j_0,j_1,j_2,\ldots)}}_{\substack{\equiv t^{p^n}_{(j_0,j_1,j_2,\ldots)} \bmod p,\\ \text{due to (2)}}} \underbrace{X_0^{j_0} X_1^{j_1} X_2^{j_2} \ldots}_{\substack{=\left(X_0^{j_0/p^n} X_1^{j_1/p^n} X_2^{j_2/p^n} \ldots\right)^{p^n}\\ \text{(this makes sense because } j_i/p^n\in\mathbb{Z} \text{ for every } i\in\mathbb{N}\\ \text{(by (1), since } p\nmid t_{(j_0,j_1,j_2,\ldots)}))}} \\
&\equiv \sum_{\substack{(j_0,j_1,j_2,\ldots)\in\mathbb{N}^{\mathbb{N}}_{\text{fin}};\\ p\nmid t_{(j_0,j_1,j_2,\ldots)}}} t^{p^n}_{(j_0,j_1,j_2,\ldots)} \left(X_0^{j_0/p^n} X_1^{j_1/p^n} X_2^{j_2/p^n} \ldots\right)^{p^n} \\
&= \sum_{\substack{(j_0,j_1,j_2,\ldots)\in\mathbb{N}^{\mathbb{N}}_{\text{fin}};\\ p\nmid t_{(j_0,j_1,j_2,\ldots)}}} \left(t_{(j_0,j_1,j_2,\ldots)} X_0^{j_0/p^n} X_1^{j_1/p^n} X_2^{j_2/p^n} \ldots\right)^{p^n} \\
&\equiv \left(\underbrace{\sum_{\substack{(j_0,j_1,j_2,\ldots)\in\mathbb{N}^{\mathbb{N}}_{\text{fin}};\\ p\nmid t_{(j_0,j_1,j_2,\ldots)}}} t_{(j_0,j_1,j_2,\ldots)} X_0^{j_0/p^n} X_1^{j_1/p^n} X_2^{j_2/p^n} \ldots}_{=\rho(X)}\right)^{p^n} \\
&\qquad \left(\begin{array}{c}\text{since } \sum\limits_{s\in S} a_s^{p^n} \equiv \left(\sum\limits_{s\in S} a_s\right)^{p^n} \bmod p \text{ for any family}\\ (a_s)_{s\in S} \text{ of elements of any commutative ring}\end{array}\right) \\
&= (\rho(X))^{p^n} \bmod p
\end{aligned}$$

(where "$\bmod p$" is shorthand for "$\bmod p\mathbb{Z}[X_0, X_1, X_2, \ldots]$"). Hence, $\tau(X) - (\rho(X))^{p^n} \in p\mathbb{Z}[X_0, X_1, X_2, \ldots]$. Therefore, we can define a polynomial $\widetilde{\tau} \in \mathbb{Z}[X_0, X_1, X_2, \ldots]$ by

$$\tau(X) - (\rho(X))^{p^n} = p\widetilde{\tau}(X).$$

For every $i \in \mathbb{N}$, we have

$$\begin{aligned}
p\frac{\partial}{\partial X_i}\left(\widetilde{\tau}\left(X\right)\right) &= \frac{\partial}{\partial X_i}\left(\underbrace{p\widetilde{\tau}\left(X\right)}_{=\tau(X)-(\rho(X))^{p^n}}\right) = \frac{\partial}{\partial X_i}\left(\tau\left(X\right)-\left(\rho\left(X\right)\right)^{p^n}\right) \\
&= \frac{\partial}{\partial X_i}\left(\tau\left(X\right)\right) - \underbrace{\frac{\partial}{\partial X_i}\left(\left(\rho\left(X\right)\right)^{p^n}\right)}_{\substack{=p^n(\rho(X))^{p^n-1}\frac{\partial}{\partial X_i}(\rho(X)) \\ \left(\text{by the chain rule, since } \frac{\partial}{\partial Y}\left(Y^{p^n}\right)=p^nY^{p^n-1}\right)}} \\
&= \underbrace{\frac{\partial}{\partial X_i}\left(\tau\left(X\right)\right)}_{\in p^n\mathbb{Z}[X_0,X_1,X_2,...]} - p^n \underbrace{\left(\rho\left(X\right)\right)^{p^n-1}\frac{\partial}{\partial X_i}\left(\rho\left(X\right)\right)}_{\in\mathbb{Z}[X_0,X_1,X_2,...]} \\
&\in p^n\mathbb{Z}\left[X_0,X_1,X_2,...\right] - p^n\mathbb{Z}\left[X_0,X_1,X_2,...\right] \\
&\subseteq p^n\mathbb{Z}\left[X_0,X_1,X_2,...\right] \qquad \left(\text{since } p^n\mathbb{Z}\left[X_0,X_1,X_2,...\right] \text{ is a } \mathbb{Z}\text{-module}\right),
\end{aligned}$$

so that

$$\frac{\partial}{\partial X_i}\left(\widetilde{\tau}\left(X\right)\right) \in \frac{1}{p}p^n\mathbb{Z}\left[X_0,X_1,X_2,...\right] = p^{n-1}\mathbb{Z}\left[X_0,X_1,X_2,...\right].$$

Therefore, we can apply the Lemma with $n-1$ instead of n and with $\widetilde{\tau}$ instead of τ (in fact, the Lemma with $n-1$ instead of n is guaranteed to hold by our induction assumption), and we obtain that there exist polynomials $\widetilde{\tau}_0$, $\widetilde{\tau}_1$, ..., $\widetilde{\tau}_{n-1}$ in $\mathbb{Z}\left[X_0,X_1,X_2,...\right]$ such that

$$\widetilde{\tau}\left(X\right) = w_{n-1}\left(\widetilde{\tau}_0\left(X\right),\widetilde{\tau}_1\left(X\right),...,\widetilde{\tau}_{n-1}\left(X\right)\right).$$

In other words,

$$\widetilde{\tau}\left(X\right) = w_{n-1}\left(\widetilde{\tau}_0\left(X\right),\widetilde{\tau}_1\left(X\right),...,\widetilde{\tau}_{n-1}\left(X\right)\right) = \sum_{k=0}^{n-1} p^k \left(\widetilde{\tau}_k\left(X\right)\right)^{p^{(n-1)-k}}.$$

Now, define polynomials τ_0, τ_1, ..., τ_n in $\mathbb{Z}\left[X_0,X_1,X_2,...\right]$ by

$$\left(\tau_k = \begin{cases} \rho, \text{ if } k=0; \\ \widetilde{\tau}_{k-1}, \text{ if } k>0 \end{cases} \qquad \text{for every } k \in \left\{0,1,...,n\right\}\right).$$

Then,

$$w_n\left(\tau_0\left(X\right),\tau_1\left(X\right),...,\tau_n\left(X\right)\right)$$
$$=\sum_{k=0}^{n}p^k\left(\tau_k\left(X\right)\right)^{p^{n-k}}=\underbrace{p^0}_{=1}\left(\underbrace{\tau_0}_{=\rho}\left(X\right)\right)^{p^{n-0}}+\sum_{k=1}^{n}\underbrace{p^k}_{=pp^{k-1}}\left(\underbrace{\tau_k}_{=\widetilde{\tau}_{k-1}}\left(X\right)\right)^{p^{n-k}}$$
$$=\left(\rho\left(X\right)\right)^{p^{n-0}}+\sum_{k=1}^{n}pp^{k-1}\underbrace{\left(\widetilde{\tau}_{k-1}\left(X\right)\right)^{p^{n-k}}}_{=\left(\widetilde{\tau}_{k-1}(X)\right)^{p^{(n-1)-(k-1)}}}$$
$$=\left(\rho\left(X\right)\right)^{p^{n-0}}+\sum_{k=1}^{n}pp^{k-1}\left(\widetilde{\tau}_{k-1}\left(X\right)\right)^{p^{(n-1)-(k-1)}}$$
$$=\left(\rho\left(X\right)\right)^{p^{n-0}}+\sum_{k=0}^{n-1}pp^{k}\left(\widetilde{\tau}_{k}\left(X\right)\right)^{p^{(n-1)-k}}\qquad\text{(here we substituted } k \text{ for } k-1 \text{ in the sum)}$$
$$=\left(\rho\left(X\right)\right)^{p^{n}}+p\underbrace{\sum_{k=0}^{n-1}p^{k}\left(\widetilde{\tau}_{k}\left(X\right)\right)^{p^{(n-1)-k}}}_{=\widetilde{\tau}(X)}=\left(\rho\left(X\right)\right)^{p^{n}}+\underbrace{p\widetilde{\tau}\left(X\right)}_{=\tau(X)-(\rho(X))^{p^n}}=\tau\left(X\right).$$

This proves our Lemma (i. e., the induction is complete), and thus, the implication $\mathcal{B}\Longrightarrow\mathcal{A}$ is established.

Altogether, we have proven the implications $\mathcal{A}\Longrightarrow\mathcal{B}$ and $\mathcal{B}\Longrightarrow\mathcal{A}$. Consequently, Assertions $\mathcal{A}$ and $\mathcal{B}$ are equivalent. Theorem 1 is now proven.

Remark: While it is tempting to believe that our Theorem 1 yields Theorem 5.2 from [1], this doesn't seem to be the case.[2]

References

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

---

[2] In fact, our Theorem 1 yields that for every $n\in\mathbb{N}$ and every polynomial φ, there exist polynomials φ_0, φ_1, ..., φ_n satisfying

$$w_n\left(\varphi_0\left(X;Y;Z\right),...,\varphi_n\left(X;Y;Z\right)\right)=\varphi\left(w_n\left(X\right),w_n\left(Y\right),w_n\left(Z\right)\right)$$

(see Theorem 5.2 in [1] for details), but Theorem 5.2 from [1] additionally claims that each of these polynomials is independent of n, which does not follow from our Theorem 1.