Witt vectors. Part 1

Michiel Hazewinkel
Sidenotes by Darij Grinberg

Witt#3: Ghost component computations

[version 1.0 (21 April 2013), completed, not proofread]

This is an addendum to section 5 of [1]. We are going to explicitly state and prove the general principle on which the proofs of 5.2, 5.25, 5.27 and 5.40 of [1] are based - the "method of ghost component equations".

We recall the definition of the p-adic Witt polynomials:

Definitions. (a) 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 family $(X_0, X_1, X_2, ...)$. Thus, $w_n(X) = \sum_{k=0}^{n} p^k X_k^{p^{n-k}}$.

These polynomials $w_0(X)$, $w_1(X)$, $w_2(X)$, ... are called the *p-adic Witt polynomials*.[1]

Remark. It is sometimes useful to additionally define a Witt polynomial $w_{-1} \in \mathbb{Z}$ (that's right, a polynomial in 0 indeterminates) by $w_{-1} = 0$. This agrees with the definition of w_n by $w_n(X_0, X_1, ..., X_n) = \sum_{k=0}^{n} p^k X_k^{p^{n-k}}$, because for $n = -1$, the sum $\sum_{k=0}^{n} p^k X_k^{p^{n-k}}$ is an empty sum and thus to be

[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).

understood as 0. While this polynomial w_{-1} does not store any interesting information, it sometimes helps to have it defined[2].

(b) Let Ξ be a family of symbols. We consider the polynomial ring $\mathbb{Q}[\Xi]$ (this is the polynomial ring over $\mathbb{Q}$ in the indeterminates Ξ; in other words, we use the symbols from Ξ as variables for the polynomials) and its subring $\mathbb{Z}[\Xi]$ (this is the polynomial ring over $\mathbb{Z}$ in the indeterminates Ξ) [3]. Let Ξ^p mean the family of the p-th powers of all elements of our family Ξ (considered as elements of $\mathbb{Z}[\Xi]$) [4]. (Therefore, whenever $P \in \mathbb{Q}[\Xi]$ is a polynomial, $P(\Xi^p)$ is the polynomial obtained from P after replacing every indeterminate by its p-th power.[5])

We will now show two theorems:

Theorem 1 (Working with ghost components I).

(a) Let $(f_0, f_1, f_2, ...) \in (\mathbb{Q}[\Xi])^{\mathbb{N}}$ and $(g_0, g_1, g_2, ...) \in (\mathbb{Q}[\Xi])^{\mathbb{N}}$ be two families of polynomials. Then,

$$(f_n = g_n \qquad \text{for every } n \in \mathbb{N}) \tag{1}$$

if and only if

$$(w_n(f_0, f_1, ..., f_n) = w_n(g_0, g_1, ..., g_n) \qquad \text{for every } n \in \mathbb{N}). \tag{2}$$

(b) Let $(f_0, f_1, f_2, ...) \in (\mathbb{Q}[\Xi])^{\mathbb{N}}$ be a family of polynomials. Then,

$$(f_n \in \mathbb{Z}[\Xi] \qquad \text{for every } n \in \mathbb{N}) \tag{3}$$

if and only if

$$(w_n(f_0, f_1, ..., f_n) - w_{n-1}(f_0(\Xi^p), f_1(\Xi^p), ..., f_{n-1}(\Xi^p)) \in p^n \mathbb{Z}[\Xi] \qquad \text{for every } n \in \mathbb{N}). \tag{4}$$

Theorem 2 (Working with ghost components II).

Let $(p_0, p_1, p_2, ...) \in (\mathbb{Q}[\Xi])^{\mathbb{N}}$ be a family of polynomials.

(a) Then, there exists one and only one family $(f_0, f_1, f_2, ...) \in (\mathbb{Q}[\Xi])^{\mathbb{N}}$ of polynomials such that

$$(w_n(f_0, f_1, ..., f_n) = p_n \qquad \text{for every } n \in \mathbb{N}). \tag{5}$$

[2]For instance, the formula (5.26) of [1] simplifies to

$$w_n(\mathbf{V}_p) = p w_{n-1} \qquad \text{for } \textit{all } n \in \mathbb{N}$$

when we use the convention $w_{-1} = 0$.

[3]For instance, Ξ can be $(X_0, X_1, X_2, ...)$, in which case $\mathbb{Z}[\Xi]$ means $\mathbb{Z}[X_0, X_1, X_2, ...]$. Or, Ξ can be $(X_0, X_1, X_2, ...; Y_0, Y_1, Y_2, ...; Z_0, Z_1, Z_2, ...)$, in which case $\mathbb{Z}[\Xi]$ means $\mathbb{Z}[X_0, X_1, X_2, ...; Y_0, Y_1, Y_2, ...; Z_0, Z_1, Z_2, ...]$.

[4]In other words, if $\Xi = (\xi_i)_{i \in I}$, then we define Ξ^p as $(\xi_i^p)_{i \in I}$. For instance, if $\Xi = (X_0, X_1, X_2, ...)$, then $\Xi^p = (X_0^p, X_1^p, X_2^p, ...)$. If $\Xi = (X_0, X_1, X_2, ...; Y_0, Y_1, Y_2, ...; Z_0, Z_1, Z_2, ...)$, then $\Xi^p = (X_0^p, X_1^p, X_2^p, ...; Y_0^p, Y_1^p, Y_2^p, ...; Z_0^p, Z_1^p, Z_2^p, ...)$.

[5]For instance, if $\Xi = (X_0, X_1, X_2, ...)$ and $P(\Xi) = (X_0 + X_1)^2 - 2X_3 + 1$, then $P(\Xi^p) = (X_0^p + X_1^p)^2 - 2X_3^p + 1$.

(b) The family $(f_0, f_1, ..., f_n)$ defined in Theorem 2 **(a)** satisfies $f_n \in \mathbb{Q}[p_0, p_1, ..., p_n]$ (where $\mathbb{Q}[p_0, p_1, ..., p_n]$ means the sub-$\mathbb{Q}$-algebra of $\mathbb{Q}[\Xi]$ generated by the polynomials p_0, p_1, ..., p_n) for every $n \in \mathbb{N}$.

(c) This family $(f_0, f_1, ..., f_n)$ defined in Theorem 2 **(a)** satisfies $(f_0, f_1, f_2, ...) \in (\mathbb{Z}[\Xi])^{\mathbb{N}}$ if and only if

$$(p_n - p_{n-1}(\Xi^p) \in p^n \mathbb{Z}[\Xi] \qquad \text{for every } n \in \mathbb{N}). \tag{6}$$

Here, p_{-1} denotes the zero polynomial.

Before we prove these theorems, let us explain their use: Theorem 2 **(a)** says that we can define a family $(f_0, f_1, f_2, ...) \in (\mathbb{Q}[\Xi])^{\mathbb{N}}$ of polynomials uniquely using "ghost component equations" (i. e., by defining $w_n(f_0, f_1, ..., f_n)$ for every $n \in \mathbb{N}$ instead of directly defining f_n for every $n \in \mathbb{N}$). These polynomials need not necessarily come out integral when defined this way, but Theorem 2 **(c)** yields a handy way to check whether they are. Moreover, Theorem 2 **(b)** shows that the polynomial f_n lies - at least, over $\mathbb{Q}$ - in the subalgebra generated by p_0, p_1, ..., p_n, so it cannot have variables that don't occur in any of p_0, p_1, ..., p_n. Theorem 1 is more or less a reformulation of Theorem 2 that makes it easier for us to prove it.

We are now going to prove Theorems 1 and 2. First, a lemma:

Lemma 3. Let A be a commutative ring with unity, and $p \in \mathbb{N}$ be a nonnegative integer[6]. Let $k \in \mathbb{N}$ and $\ell \in \mathbb{N}$ be such that $k > 0$. Let $a \in A$ and $b \in A$. If $a \equiv b \bmod p^k A$, then $a^{p^\ell} \equiv b^{p^\ell} \bmod p^{k+\ell} A$.

Proof of Lemma 3. We will show Lemma 3 by induction over ℓ. For $\ell = 0$, the assertion of Lemma 3 is trivial. Now, for the induction step, we assume that $a^{p^\ell} \equiv b^{p^\ell} \bmod p^{k+\ell} A$ for some $\ell \in \mathbb{N}$, and we want to show that $a^{p^{\ell+1}} \equiv b^{p^{\ell+1}} \bmod p^{k+\ell+1} A$. In fact, we have $a \equiv b \bmod pA$ (because $a \equiv b \bmod p^k A$ yields $a - b \in p^k A \subseteq pA$, since $k > 0$) and thus

$$\sum_{i=0}^{p-1} \left(a^{p^\ell}\right)^i \left(b^{p^\ell}\right)^{p-1-i} \equiv \sum_{i=0}^{p-1} \left(b^{p^\ell}\right)^i \left(b^{p^\ell}\right)^{p-1-i} = \sum_{i=0}^{p-1} \left(b^{p^\ell}\right)^{p-1} = p \left(b^{p^\ell}\right)^{p-1} \equiv 0 \bmod pA,$$

so that $\sum_{i=0}^{p-1} \left(a^{p^\ell}\right)^i \left(b^{p^\ell}\right)^{p-1-i} \in pA$. Hence,

$$a^{p^{\ell+1}} - b^{p^{\ell+1}} = \left(a^{p^\ell}\right)^p - \left(b^{p^\ell}\right)^p = \underbrace{\left(a^{p^\ell} - b^{p^\ell}\right)}_{\substack{\in p^{k+\ell} A, \text{ since} \\ a^{p^\ell} \equiv b^{p^\ell} \bmod p^{k+\ell} A}} \cdot \underbrace{\sum_{i=0}^{p-1} \left(a^{p^\ell}\right)^i \left(b^{p^\ell}\right)^{p-1-i}}_{\in pA} \in p^{k+\ell+1} A,$$

so that $a^{p^{\ell+1}} \equiv b^{p^{\ell+1}} \bmod p^{k+\ell+1} A$, and the induction step is complete. Thus, Lemma 3 is proven.

As a consequence of Lemma 3, we can establish the following fact (which is Lemma 5.4 in [1]):

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

Lemma 4. Let $\psi \in \mathbb{Z}[\Xi]$ be a polynomial. Let p be a prime.

(a) Then,

$$\psi\left(\Xi^p\right) \equiv \psi^p \bmod p\mathbb{Z}[\Xi].$$

(b) For every $\ell \in \mathbb{N}$, we have

$$\left(\psi\left(\Xi^p\right)\right)^{p^\ell} \equiv \psi^{p^{\ell+1}} \bmod p^{\ell+1}\mathbb{Z}[\Xi].$$

Proof of Lemma 4. **(a)** Every element $\mathbf{n} \in \mathbb{N}^\Xi$ is a family of elements of $\mathbb{N}$ indexed by elements of Ξ. For every $\xi \in \Xi$, we will denote by $\mathbf{n}_\xi$ the ξ-th component of this family $\mathbf{n}$. (Thus, every $\mathbf{n} \in \mathbb{N}^\Xi$ satisfies $\mathbf{n} = (\mathbf{n}_\xi)_{\xi\in\Xi}$.)

Let $\mathbb{N}^\Xi_{\text{fin}}$ denote the set

$$\left\{\mathbf{n} \in \mathbb{N}^\Xi \ \mid \ \text{only finitely many } \xi \in \Xi \text{ satisfy } \mathbf{n}_\xi \neq 0\right\}.$$

Then, the polynomial ψ has (like any polynomial in $\mathbb{Z}[\Xi]$) a representation in the form $\psi = \sum\limits_{\mathbf{n}\in\mathbb{N}^\Xi_{\text{fin}}} a_{\mathbf{n}} \prod\limits_{\xi\in\Xi} \xi^{\mathbf{n}_\xi}$, where $a_{\mathbf{n}}$ is an element of $\mathbb{Z}$ for every $\mathbf{n} \in \mathbb{N}^\Xi_{\text{fin}}$. Obviously, $\psi\left(\Xi^p\right) = \sum\limits_{\mathbf{n}\in\mathbb{N}^\Xi_{\text{fin}}} a_{\mathbf{n}} \prod\limits_{\xi\in\Xi} \left(\xi^p\right)^{\mathbf{n}_\xi}$. But

$$\psi^p = \left(\sum_{\mathbf{n}\in\mathbb{N}^\Xi_{\text{fin}}} a_{\mathbf{n}} \prod_{\xi\in\Xi} \xi^{\mathbf{n}_\xi}\right)^p \equiv \sum_{\mathbf{n}\in\mathbb{N}^\Xi_{\text{fin}}} \left(a_{\mathbf{n}} \prod_{\xi\in\Xi} \xi^{\mathbf{n}_\xi}\right)^p$$

$$\left(\text{since } \left(\sum_{s\in S} a_s\right)^p \equiv \sum_{s\in S} a_s^p \bmod pA \text{ for any family } \left(a_s\right)_{s\in S} \text{ of elements of a commutative ring } A\right)$$

$$= \sum_{\mathbf{n}\in\mathbb{N}^\Xi_{\text{fin}}} \underbrace{a_{\mathbf{n}}^p}_{\substack{\equiv a_{\mathbf{n}} \bmod p\mathbb{Z}[\Xi], \\ \text{because } a_{\mathbf{n}}^p \equiv a_{\mathbf{n}} \bmod p \text{ in } \mathbb{Z} \\ \text{(by Fermat's Little Theorem)}}} \prod_{\xi\in\Xi} \underbrace{\left(\xi^{\mathbf{n}_\xi}\right)^p}_{=\left(\xi^p\right)^{\mathbf{n}_\xi}} \equiv \sum_{\mathbf{n}\in\mathbb{N}^\Xi_{\text{fin}}} a_{\mathbf{n}} \prod_{\xi\in\Xi} \left(\xi^p\right)^{\mathbf{n}_\xi} = \psi\left(\Xi^p\right) \bmod p\mathbb{Z}[\Xi].$$

This proves Lemma 4 **(a)**.

(b) Lemma 4 **(b)** follows from Lemma 4 **(a)** using Lemma 3 (applied to $A = \mathbb{Z}[\Xi]$, $k = 1$, $a = \psi\left(\Xi^p\right)$ and $b = \psi^p$).

This completes the proof of Lemma 4.

Proof of Theorem 1. **(a)** We have to prove that (1) is equivalent to (2). In fact, it is clear that (1) yields (2), so it only remains to prove that (2) yields (1). So, let us assume that (2) holds. We want to prove that (1) holds as well. In other words, we have to prove that $f_n = g_n$ for every $n \in \mathbb{N}$. We will prove this by strong induction over n; this means that we fix some $n \in \mathbb{N}$, and our goal is to show that $f_n = g_n$ assuming that $f_k = g_k$ is already proven for each $k \in \mathbb{N}$ satisfying $k < n$. Now,

$$w_n\left(f_0, f_1, ..., f_n\right) = \sum_{k=0}^{n} p^k f_k^{p^{n-k}} = \sum_{k=0}^{n-1} p^k f_k^{p^{n-k}} + p^n \underbrace{f_n^{p^{n-n}}}_{=f_n^{p^0}=f_n} = \sum_{k=0}^{n-1} p^k f_k^{p^{n-k}} + p^n f_n \qquad \text{and similarly}$$

$$w_n\left(g_0, g_1, ..., g_n\right) = \sum_{k=0}^{n-1} p^k g_k^{p^{n-k}} + p^n g_n.$$

Thus, (2) yields

$$\sum_{k=0}^{n-1} p^k f_k^{p^{n-k}} + p^n f_n = \sum_{k=0}^{n-1} p^k g_k^{p^{n-k}} + p^n g_n.$$

Subtracting $\sum_{k=0}^{n-1} p^k f_k^{p^{n-k}} = \sum_{k=0}^{n-1} p^k g_k^{p^{n-k}}$ (which is because $f_k = g_k$ for each $k \in \mathbb{N}$ satisfying $k < n$, by the induction assumption) from this equation, we obtain $p^n f_n = p^n g_n$. Hence, $f_n = g_n$ (because p^n is not a zero divisor in the ring $(\mathbb{Q}[\Xi])^{\mathbb{N}}$). This completes the induction, and thus (1) is proven. This completes the proof of Theorem 1 **(a)**.

(b) Obviously,

$$w_n(f_0, f_1, ..., f_n) = \sum_{k=0}^{n} p^k f_k^{p^{n-k}} = p^n f_n^{p^{n-n}} + \sum_{k=0}^{n-1} p^k f_k^{p^{n-k}} \tag{7}$$

and

$$w_{n-1}(f_0(\Xi^p), f_1(\Xi^p), ..., f_{n-1}(\Xi^p)) = \sum_{k=0}^{n-1} p^k (f_k(\Xi^p))^{p^{(n-1)-k}}. \tag{8}$$

Now, we have to prove that (3) is equivalent to (4). We will do this in two steps: First, we will show that (3) implies (4), and then we will establish the converse.

Step 1: Proof that (3) implies (4): Assume that (3) holds. We have to prove (4) then, i. e., we have to prove that

$$w_n(f_0, f_1, ..., f_n) - w_{n-1}(f_0(\Xi^p), f_1(\Xi^p), ..., f_{n-1}(\Xi^p)) \in p^n \mathbb{Z}[\Xi] \qquad \text{for every } n \in \mathbb{N}.$$

In fact, let us first notice that $f_k \in \mathbb{Z}[\Xi]$ for every $k \in \mathbb{N}$ (since (3) was assumed to hold). Thus, in particular, $f_k \in \mathbb{Z}[\Xi]$ for every $k \in \mathbb{N}$ satisfying $k < n$. Hence, for every $k \in \mathbb{N}$ satisfying $k < n$, Lemma 4 **(b)** (applied to $\psi = f_k$) yields that

$$(f_k(\Xi^p))^{p^\ell} \equiv f_k^{p^{\ell+1}} \bmod p^{\ell+1}\mathbb{Z}[\Xi] \qquad \text{for every } \ell \in \mathbb{N}. \tag{9}$$

Now,

$$\begin{aligned}\sum_{k=0}^{n-1} p^k f_k^{p^{n-k}} - \sum_{k=0}^{n-1} p^k (f_k(\Xi^p))^{p^{(n-1)-k}} &= \sum_{k=0}^{n-1} p^k \underbrace{\left(f_k^{p^{n-k}} - (f_k(\Xi^p))^{p^{(n-1)-k}}\right)}_{\substack{\in p^{n-k}\mathbb{Z}[\Xi], \text{ because} \\ (f_k(\Xi^p))^{p^{(n-1)-k}} \equiv f_k^{p^{n-k}} \bmod p^{n-k}\mathbb{Z}[\Xi] \\ \text{(by (9), applied to } \ell=(n-1)-k)}} \\ &\in \sum_{k=0}^{n-1} \underbrace{p^k p^{n-k}\mathbb{Z}[\Xi]}_{=p^n\mathbb{Z}[\Xi]} \subseteq p^n\mathbb{Z}[\Xi]. \end{aligned} \tag{10}$$

Hence,

$$\begin{aligned}
&w_n\left(f_0, f_1, ..., f_n\right) - w_{n-1}\left(f_0\left(\Xi^p\right), f_1\left(\Xi^p\right), ..., f_{n-1}\left(\Xi^p\right)\right) \\
&= \left(p^n f_n^{p^{n-n}} + \sum_{k=0}^{n-1} p^k f_k^{p^{n-k}}\right) - \sum_{k=0}^{n-1} p^k \left(f_k\left(\Xi^p\right)\right)^{p^{(n-1)-k}} \qquad \text{(by (7) and (8))} \\
&= p^n f_n^{p^{n-n}} + \underbrace{\left(\sum_{k=0}^{n-1} p^k f_k^{p^{n-k}} - \sum_{k=0}^{n-1} p^k \left(f_k\left(\Xi^p\right)\right)^{p^{(n-1)-k}}\right)}_{\in p^n \mathbb{Z}[\Xi] \text{ by (10)}} \\
&\in p^n \underbrace{f_n^{p^{n-n}}}_{\in \mathbb{Z}[\Xi]} + p^n \mathbb{Z}\left[\Xi\right] \qquad (11) \\
&\subseteq p^n \mathbb{Z}\left[\Xi\right] + p^n \mathbb{Z}\left[\Xi\right] \subseteq p^n \mathbb{Z}\left[\Xi\right] \qquad \text{(since } \mathbb{Z}\left[\Xi\right] \text{ is a } \mathbb{Z}\text{-module)}.
\end{aligned}$$

Thus, (4) is proven, i. e., we have shown that (3) implies (4).

Step 2: Proof that (4) implies (3): Assume that (4) holds. We have to prove (3) then, i. e., we have to prove that $f_n \in \mathbb{Z}\left[\Xi\right]$ for every $n \in \mathbb{N}$. We will prove this by strong induction over n; this means that we fix some $n \in \mathbb{N}$, and our goal is to show that $f_n \in \mathbb{Z}\left[\Xi\right]$, assuming that $f_k \in \mathbb{Z}\left[\Xi\right]$ is already proven for each $k \in \mathbb{N}$ satisfying $k < n$.

As in Step 1, we can prove (11) (because our proof of (11) in Step 1 only used that $f_k \in \mathbb{Z}\left[\Xi\right]$ for every $k \in \mathbb{N}$ satisfying $k < n$; it did not use that $f_k \in \mathbb{Z}\left[\Xi\right]$ for *all* $k \in \mathbb{N}$). Hence,

$$w_n\left(f_0, f_1, ..., f_n\right) - w_{n-1}\left(f_0\left(\Xi^p\right), f_1\left(\Xi^p\right), ..., f_{n-1}\left(\Xi^p\right)\right) \in p^n \underbrace{f_n^{p^{n-n}}}_{=f_n^{p^0}=f_n} + p^n \mathbb{Z}\left[\Xi\right] = p^n f_n + p^n \mathbb{Z}\left[\Xi\right],$$

so that

$$\begin{aligned}
p^n f_n &\in \underbrace{\left(w_n\left(f_0, f_1, ..., f_n\right) - w_{n-1}\left(f_0\left(\Xi^p\right), f_1\left(\Xi^p\right), ..., f_{n-1}\left(\Xi^p\right)\right)\right)}_{\in p^n \mathbb{Z}[\Xi] \text{ by (4)}} - p^n \mathbb{Z}\left[\Xi\right] \\
&\subseteq p^n \mathbb{Z}\left[\Xi\right] - p^n \mathbb{Z}\left[\Xi\right] = p^n \mathbb{Z}\left[\Xi\right].
\end{aligned}$$

Hence, $f_n = \dfrac{1}{p^n} p^n f_n \in \dfrac{1}{p^n} p^n \mathbb{Z}\left[\Xi\right] = \mathbb{Z}\left[\Xi\right]$. This completes our induction step. Therefore, (3) is proven, i. e., we have shown that (4) implies (3).

Altogether, we now know that (3) implies (4) and that (4) implies (3). This proves that (3) and (4) are equivalent. Theorem 1 **(b)** is now proven.

Proof of Theorem 2. **(a)** The uniqueness of the family $(f_0, f_1, f_2, ...) \in \left(\mathbb{Q}\left[\Xi\right]\right)^{\mathbb{N}}$ satisfying (5) immediately follows from Theorem 1 **(a)**, so it only remains to prove the existence of a family $(f_0, f_1, f_2, ...) \in \left(\mathbb{Q}\left[\Xi\right]\right)^{\mathbb{N}}$ satisfying (5). We will do this by constructing it recursively: Let $N \in \mathbb{N}$. Assume that the polynomials f_0, f_1, ..., f_{N-1} are already constructed, and that (5) holds for all $n < N$. Then, we define a polynomial $f_N \in \mathbb{Q}\left[\Xi\right]$ by

$$f_N = \frac{1}{p^N}\left(p_N - \sum_{k=0}^{N-1} p^k f_k^{p^{N-k}}\right). \qquad (12)$$

Then, (5) holds for $n = N$ as well, since

$$\begin{aligned} w_N(f_0, f_1, ..., f_N) &= \sum_{k=0}^{N} p^k f_k^{p^{N-k}} = \sum_{k=0}^{N-1} p^k f_k^{p^{N-k}} + p^N \underbrace{f_N^{p^{N-N}}}_{=f_N^{p^0}=f_N} = \sum_{k=0}^{N-1} p^k f_k^{p^{N-k}} + p^N f_N \\ &= \sum_{k=0}^{N-1} p^k f_k^{p^{N-k}} + p^N \cdot \frac{1}{p^N} \left(p_N - \sum_{k=0}^{N-1} p^k f_k^{p^{N-k}} \right) \qquad \text{(by (12))} \\ &= \sum_{k=0}^{N-1} p^k f_k^{p^{N-k}} + \left(p_N - \sum_{k=0}^{N-1} p^k f_k^{p^{N-k}} \right) = p_N. \end{aligned}$$

Thus, the family $(f_0, f_1, f_2, ...) \in (\mathbb{Q}[\Xi])^{\mathbb{N}}$ that we recursively construct this way will satisfy (5) for all $n \in \mathbb{N}$. This proves the existence of such a family $(f_0, f_1, f_2, ...) \in (\mathbb{Q}[\Xi])^{\mathbb{N}}$. Thus, the proof of Theorem 2 **(a)** is complete.

(b) We have to prove that $f_n \in \mathbb{Q}[p_0, p_1, ..., p_n]$ for all $n \in \mathbb{N}$. We will prove this by strong induction over n; this means that we fix some $N \in \mathbb{N}$, and our goal is to show that $f_N \in \mathbb{Q}[p_0, p_1, ..., p_N]$, assuming that $f_k \in \mathbb{Q}[p_0, p_1, ..., p_k]$ is already proven for each $k \in \mathbb{N}$ satisfying $k < N$.

Looking back at our construction of the family $(f_0, f_1, f_2, ...) \in (\mathbb{Q}[\Xi])^{\mathbb{N}}$ (during the proof of Theorem 2 **(a)**), we see that $f_N \in \mathbb{Q}[p_N, f_0, f_1, ..., f_{N-1}]$ (because of (12)). But $\mathbb{Q}[p_N, f_0, f_1, ..., f_{N-1}] \subseteq \mathbb{Q}[p_0, p_1, ..., p_N]$ (because $p_N \in \mathbb{Q}[p_0, p_1, ..., p_N]$ and because our induction assumption yields $f_k \in \mathbb{Q}[p_0, p_1, ..., p_k] \subseteq \mathbb{Q}[p_0, p_1, ..., p_N]$ for each $k < N$). Hence, $f_N \in \mathbb{Q}[p_0, p_1, ..., p_N]$. This concludes our induction, and thus, Theorem 2 **(b)** is proven.

(c) For each $n \in \mathbb{N}$, we have

$$w_{n-1}(f_0, f_1, ..., f_{n-1}) = p_{n-1} \tag{13}$$

[7], and thus

$$w_{n-1}(f_0(\Xi^p), f_1(\Xi^p), ..., f_{n-1}(\Xi^p)) = p_{n-1}(\Xi^p) \tag{14}$$

[8].

We have to prove that $(f_0, f_1, f_2, ...) \in (\mathbb{Z}[\Xi])^{\mathbb{N}}$ if and only if (6). But clearly, $(f_0, f_1, f_2, ...) \in (\mathbb{Z}[\Xi])^{\mathbb{N}}$ is equivalent to (3), while (6) is equivalent to (4) (because (5) yields $w_n(f_0, f_1, ..., f_n) = p_n$, and (14) yields $w_{n-1}(f_0(\Xi^p), f_1(\Xi^p), ..., f_{n-1}(\Xi^p)) = p_{n-1}(\Xi^p)$). Hence, it remains to show that (3) is equivalent to (4). But this follows from Theorem 1 **(b)**. Thus, Theorem 2 **(c)** is proven.

Now, both Theorems 1 and 2 are completely proven, and we can come to their applications.

Our first application will be a proof of the following fact, which is Theorem 5.2 in [1]:

> **Theorem 5.** Let Ξ denote the family $(X_0, X_1, X_2, ...; Y_0, Y_1, Y_2, ...; Z_0, Z_1, Z_2, ...)$ of symbols. We abbreviate its subfamilies $(X_0, X_1, X_2, ...)$, $(Y_0, Y_1, Y_2, ...)$,

[7] *Proof of (13):* Let $n \in \mathbb{N}$. If $n = 0$, then (13) follows from $w_{n-1} = w_{-1} = 0$ and $p_{n-1} = p_{-1} = 0$. Thus, we WLOG assume that $n \neq 0$. Hence, $n \geq 1$, so that $n - 1 \in \mathbb{N}$. Therefore, (13) follows from (5) (applied to $n - 1$ instead of n).

[8] This follows by evaluating the identity (13) at Ξ^p.

$(Z_0, Z_1, Z_2, ...)$ by X, Y, Z, respectively. (Thus, as usual, if $P \in \mathbb{Z}[X_0, X_1, X_2, ...]$ is a polynomial, then $P(X)$ will mean $P(X_0, X_1, X_2, ...)$ (which is the same as P), while $P(Y)$ will mean $P(Y_0, Y_1, Y_2, ...)$, and $P(Z)$ will mean $P(Z_0, Z_1, Z_2, ...)$.)

Let $f \in \mathbb{Z}[\alpha; \beta; \gamma]$ be a polynomial in three variables.

(a) Then, there exists one and only one family $(f_0, f_1, f_2, ...) \in (\mathbb{Q}[\Xi])^{\mathbb{N}}$ of polynomials such that

$$(w_n(f_0, f_1, ..., f_n) = f(w_n(X); w_n(Y); w_n(Z)) \qquad \text{for every } n \in \mathbb{N}). \tag{15}$$

(b) This family $(f_0, f_1, f_2, ...) \in (\mathbb{Q}[\Xi])^{\mathbb{N}}$ satisfies $f_n \in \mathbb{Z}[X_0, X_1, ..., X_n; Y_0, Y_1, ..., Y_n; Z_0, Z_1, ..., Z_n]$ for every $n \in \mathbb{N}$.

Before we prove this theorem, an easy lemma:

Lemma 6. Every $n \geq 1$ satisfies

$$w_n(X) - w_{n-1}(X^p) = p^n X_n.$$

(Here, X means the family of indeterminates $(X_0, X_1, X_2, ...)$, and X^p means the family of the p-th powers of all indeterminates from the family X; in other words, $X^p = (X_0^p, X_1^p, X_2^p, ...)$.)

Proof of Lemma 6. Subtracting the equality

$$w_{n-1}(X^p) = \sum_{k=0}^{n-1} p^k (X_k^p)^{p^{(n-1)-k}} = \sum_{k=0}^{n-1} p^k X_k^{p \cdot p^{(n-1)-k}} = \sum_{k=0}^{n-1} p^k X_k^{p^{n-k}}$$

from the equality

$$w_n(X) = \sum_{k=0}^{n} p^k X_k^{p^{n-k}} = \sum_{k=0}^{n-1} p^k X_k^{p^{n-k}} + p^n X_n^{p^{n-n}},$$

we obtain

$$w_n(X) - w_{n-1}(X^p) = p^n \underbrace{X_n^{p^{n-n}}}_{=X_n^{p^0}=X_n} = p^n X_n.$$

Lemma 6 is proven.

Proof of Theorem 5. Define a family $(p_0, p_1, p_2, ...) \in (\mathbb{Q}[\Xi])^{\mathbb{N}}$ by $p_k = f(w_k(X); w_k(Y); w_k(Z))$ for every $k \in \mathbb{N}$. Then, Theorem 5 **(a)** immediately results from Theorem 2 **(a)**. It now remains to prove Theorem 5 **(b)**, i. e. to prove that $f_n \in \mathbb{Z}[X_0, X_1, ..., X_n; Y_0, Y_1, ..., Y_n; Z_0, Z_1, ..., Z_n]$ for every $n \in \mathbb{N}$.

Theorem 2 **(b)** yields that $f_n \in \mathbb{Q}[p_0, p_1, ..., p_n]$. But all the polynomials p_0, p_1, ..., p_n lie in

$$\mathbb{Q}[w_0(X), w_1(X), ..., w_n(X); w_0(Y), w_1(Y), ..., w_n(Y); w_0(Z), w_1(Z), ..., w_n(Z)]$$

(because $p_k = f\left(w_k\left(X\right); w_k\left(Y\right); w_k\left(Z\right)\right)$ for every $k \in \mathbb{N}$, with f being a polynomial). Hence,

$$\mathbb{Q}\left[p_0, p_1, ..., p_n\right] \subseteq \mathbb{Q}\left[w_0\left(X\right), w_1\left(X\right), ..., w_n\left(X\right); w_0\left(Y\right), w_1\left(Y\right), ..., w_n\left(Y\right); w_0\left(Z\right), w_1\left(Z\right), ..., w_n\left(Z\right)\right].$$

Besides, for every $k \in \{0, 1, ..., n\}$, the polynomials $w_k\left(X\right)$, $w_k\left(Y\right)$, and $w_k\left(Z\right)$ all lie in $\mathbb{Q}\left[X_0, X_1, ..., X_n; Y_0, Y_1, ..., Y_n; Z_0, Z_1, ..., Z_n\right]$ (because

$$\begin{aligned} w_k\left(X\right) &= w_k\left(X_0, X_1, ..., X_k\right) \in \mathbb{Q}\left[X_0, X_1, ..., X_k\right] \subseteq \mathbb{Q}\left[X_0, X_1, ..., X_n\right] \\ &\subseteq \mathbb{Q}\left[X_0, X_1, ..., X_n; Y_0, Y_1, ..., Y_n; Z_0, Z_1, ..., Z_n\right] \end{aligned}$$

and similarly for $w_k\left(Y\right)$ and $w_k\left(Z\right)$). Hence,

$$\begin{aligned} &\mathbb{Q}\left[w_0\left(X\right), w_1\left(X\right), ..., w_n\left(X\right); w_0\left(Y\right), w_1\left(Y\right), ..., w_n\left(Y\right); w_0\left(Z\right), w_1\left(Z\right), ..., w_n\left(Z\right)\right] \\ &\subseteq \mathbb{Q}\left[X_0, X_1, ..., X_n; Y_0, Y_1, ..., Y_n; Z_0, Z_1, ..., Z_n\right]. \end{aligned}$$

Combining these results, we see that

$$\begin{aligned} f_n &\in \mathbb{Q}\left[p_0, p_1, ..., p_n\right] \\ &\subseteq \mathbb{Q}\left[w_0\left(X\right), w_1\left(X\right), ..., w_n\left(X\right); w_0\left(Y\right), w_1\left(Y\right), ..., w_n\left(Y\right); w_0\left(Z\right), w_1\left(Z\right), ..., w_n\left(Z\right)\right] \\ &\subseteq \mathbb{Q}\left[X_0, X_1, ..., X_n; Y_0, Y_1, ..., Y_n; Z_0, Z_1, ..., Z_n\right]. \end{aligned} \tag{16}$$

On the other hand, Lemma 6 yields $w_n\left(X\right) - w_{n-1}\left(X^p\right) = p^n X_n \in p^n \mathbb{Z}\left[\Xi\right]$, so that $w_n\left(X\right) \equiv w_{n-1}\left(X^p\right) \bmod p^n \mathbb{Z}\left[\Xi\right]$, and similarly $w_n\left(Y\right) \equiv w_{n-1}\left(Y^p\right) \bmod p^n \mathbb{Z}\left[\Xi\right]$ and $w_n\left(Z\right) \equiv w_{n-1}\left(Z^p\right) \bmod p^n \mathbb{Z}\left[\Xi\right]$. Thus,

$$p_n = f\left(w_n\left(X\right); w_n\left(Y\right); w_n\left(Z\right)\right) \equiv f\left(w_{n-1}\left(X^p\right); w_{n-1}\left(Y^p\right); w_{n-1}\left(Z^p\right)\right) \bmod p^n \mathbb{Z}\left[\Xi\right].$$

On the other hand, evaluating the polynomial identity $p_{n-1} = f\left(w_{n-1}\left(X\right); w_{n-1}\left(Y\right); w_{n-1}\left(Z\right)\right)$ at Ξ^p yields

$$p_{n-1}\left(\Xi^p\right) = f\left(w_{n-1}\left(X^p\right); w_{n-1}\left(Y^p\right); w_{n-1}\left(Z^p\right)\right).$$

Hence,

$$p_n \equiv f\left(w_{n-1}\left(X^p\right); w_{n-1}\left(Y^p\right); w_{n-1}\left(Z^p\right)\right) = p_{n-1}\left(\Xi^p\right) \bmod p^n \mathbb{Z}\left[\Xi\right],$$

so that

$$p_n - p_{n-1}\left(\Xi^p\right) \in p^n \mathbb{Z}\left[\Xi\right] \qquad \text{for every } n \in \mathbb{N}.$$

Therefore, Theorem 2 **(c)** yields that $\left(f_0, f_1, f_2, ...\right) \in \left(\mathbb{Z}\left[\Xi\right]\right)^{\mathbb{N}}$. In other words, $f_n \in \mathbb{Z}\left[\Xi\right]$ for every $n \in \mathbb{N}$. Combining this with (16), we see that

$$\begin{aligned} f_n &\in \mathbb{Z}\left[\Xi\right] \cap \mathbb{Q}\left[X_0, X_1, ..., X_n; Y_0, Y_1, ..., Y_n; Z_0, Z_1, ..., Z_n\right] \\ &= \mathbb{Z}\left[X_0, X_1, ..., X_n; Y_0, Y_1, ..., Y_n; Z_0, Z_1, ..., Z_n\right]. \end{aligned}$$

This proves Theorem 5 **(b)**. Thus, the proof of Theorem 5 is complete.

As another application of Theorems 1 and 2, we can prove the main result of [1], 5.25, namely that the map $\mathbf{V}_p$ defined in [1], 5.25 is a functorial group endomorphism of the Witt vectors. This will follow from the following result:

Theorem 7. Define the polynomials s_0, s_1, s_2, ... and the polynomials m_0, m_1, m_2, ... as in [1], 5.9. Define the family $(v_0, v_1, v_2, ...) \in (\mathbb{Z}[X])^{\mathbb{N}}$ by $v_0(X) = 0$ and $v_n(X) = X_{n-1}$ for every $n \geq 1$ (where X means the family $(X_0, X_1, X_2, ...)$).

Then,

$$\begin{aligned} &v_n(s_0(X;Y), s_1(X;Y), s_2(X;Y), ...) \\ &= s_n(v_0(X), v_1(X), v_2(X), ...; v_0(Y), v_1(Y), v_2(Y), ...) \end{aligned}$$

for every $n \in \mathbb{N}$.

Proof of Theorem 7. Let Ξ denote the family $(X_0, X_1, X_2, ...; Y_0, Y_1, Y_2, ...)$ of symbols. Define two families $(f_0, f_1, f_2, ...) \in (\mathbb{Q}[\Xi])^{\mathbb{N}}$ and $(g_0, g_1, g_2, ...) \in (\mathbb{Q}[\Xi])^{\mathbb{N}}$ by

$$\begin{aligned} f_k &= v_k(s_0(X;Y), s_1(X;Y), s_2(X;Y), ...) \qquad \text{and} \\ g_k &= s_k(v_0(X), v_1(X), v_2(X), ...; v_0(Y), v_1(Y), v_2(Y), ...) \end{aligned}$$

for every $n \in \mathbb{N}$. Then, we wish to prove that

$$(f_n = g_n \qquad \text{for every } n \in \mathbb{N}).$$

According to Theorem 1 **(a)**, this will immediately follow once we can show that

$$(w_n(f_0, f_1, ..., f_n) = w_n(g_0, g_1, ..., g_n) \qquad \text{for every } n \in \mathbb{N}). \tag{17}$$

So it remains to prove (17).

We have

$$\begin{aligned} w_n(f_0, f_1, ..., f_n) &= \sum_{k=0}^{n} p^k f_k^{p^{n-k}} = \sum_{k=0}^{n} p^k \left(v_k(s_0(X;Y), s_1(X;Y), s_2(X;Y), ...)\right)^{p^{n-k}} \\ &\qquad (\text{since } f_k = v_k(s_0(X;Y), s_1(X;Y), s_2(X;Y), ...)) \\ &= p^0 \underbrace{\left(v_0(s_0(X;Y), s_1(X;Y), s_2(X;Y), ...)\right)^{p^{n-0}}}_{\substack{=0 \\ (\text{since } v_0=0 \text{ and } p^{n-0}>0)}} \\ &\qquad + \sum_{k=1}^{n} \underbrace{p^k}_{=pp^{k-1}} \left(\underbrace{v_k(s_0(X;Y), s_1(X;Y), s_2(X;Y), ...)}_{\substack{=s_{k-1}(X;Y), \text{ since} \\ v_k(X)=X_{k-1}}} \right)^{p^{n-k}} \\ &= \underbrace{p^0 0}_{=0} + \sum_{k=1}^{n} pp^{k-1} \left(s_{k-1}(X;Y)\right)^{p^{n-k}} = p \sum_{k=1}^{n} p^{k-1} \left(s_{k-1}(X;Y)\right)^{p^{n-k}} \\ &= p \underbrace{\sum_{k=0}^{n-1} p^k \left(s_k(X;Y)\right)^{p^{(n-1)-k}}}_{=w_{n-1}(s_0(X;Y), s_1(X;Y), ..., s_{n-1}(X;Y))} \qquad \text{(here we substituted } k \text{ for } k-1 \text{ in the sum)} \\ &= p \underbrace{w_{n-1}(s_0(X;Y), s_1(X;Y), ..., s_{n-1}(X;Y))}_{\substack{=w_{n-1}(X)+w_{n-1}(Y) \\ (\text{by [1], (5.10), applied to } n-1 \text{ instead of } n)}} = pw_{n-1}(X) + pw_{n-1}(Y). \end{aligned}$$

On the other hand,

$$\begin{aligned}
&w_n\left(v_0\left(X\right), v_1\left(X\right), v_2\left(X\right), ...\right) \\
&= \sum_{k=0}^{n} p^k \left(v_k\left(X\right)\right)^{p^{n-k}} = p^0 \underbrace{\left(v_0\left(X\right)\right)^{p^{n-0}}}_{\substack{=0 \\ \text{(since } v_0=0 \text{ and } p^{n-0}>0\text{)}}} + \sum_{k=1}^{n} \underbrace{p^k}_{=pp^{k-1}} \left(v_k\left(X\right)\right)^{p^{n-k}} \\
&= \underbrace{p^0 0}_{=0} + \sum_{k=1}^{n} pp^{k-1} \left(v_k\left(X\right)\right)^{p^{n-k}} = p\sum_{k=1}^{n} p^{k-1} \left(\underbrace{v_k\left(X\right)}_{=X_{k-1}}\right)^{p^{n-k}} \\
&= p\sum_{k=1}^{n} p^{k-1} \underbrace{X_{k-1}^{p^{n-k}}}_{=X_{k-1}^{p^{(n-1)-(k-1)}}} = p\sum_{k=1}^{n} p^{k-1} X_{k-1}^{p^{(n-1)-(k-1)}} \\
&= p \underbrace{\sum_{k=0}^{n-1} p^k X_k^{p^{(n-1)-k}}}_{\substack{=w_{n-1}(X_0,X_1,...,X_{n-1}) \\ =w_{n-1}(X)}} \qquad \text{(here we substituted } k \text{ for } k-1 \text{ in the sum)} \\
&= pw_{n-1}\left(X\right)
\end{aligned}$$

and similarly $w_n\left(v_0\left(Y\right), v_1\left(Y\right), v_2\left(Y\right), ...\right) = pw_{n-1}\left(Y\right)$. Thus,

$$\begin{aligned}
w_n\left(g_0, g_1, ..., g_n\right) &= w_n\left(s_0\left(v_0\left(X\right), v_1\left(X\right), v_2\left(X\right), ...; v_0\left(Y\right), v_1\left(Y\right), v_2\left(Y\right), ...\right),\right. \\
&\qquad s_1\left(v_0\left(X\right), v_1\left(X\right), v_2\left(X\right), ...; v_0\left(Y\right), v_1\left(Y\right), v_2\left(Y\right), ...\right), \\
&\qquad \left. s_2\left(v_0\left(X\right), v_1\left(X\right), v_2\left(X\right), ...; v_0\left(Y\right), v_1\left(Y\right), v_2\left(Y\right), ...\right), ...\right) \\
&= \underbrace{w_n\left(v_0\left(X\right), v_1\left(X\right), v_2\left(X\right), ...\right)}_{=pw_{n-1}(X)} + \underbrace{w_n\left(v_0\left(Y\right), v_1\left(Y\right), v_2\left(Y\right), ...\right)}_{=pw_{n-1}(Y)} \\
&\qquad \left(\begin{array}{c} \text{this follows from the polynomial identity} \\ w_n\left(s_0\left(X;Y\right), s_1\left(X;Y\right), s_2\left(X;Y\right), ...\right) = w_n\left(X\right) + w_n\left(Y\right) \\ \text{upon substitution of} \\ \left(v_0\left(X\right), v_1\left(X\right), v_2\left(X\right), ...; v_0\left(Y\right), v_1\left(Y\right), v_2\left(Y\right), ...\right) \text{ for } \left(X;Y\right) \end{array}\right) \\
&= pw_{n-1}\left(X\right) + pw_{n-1}\left(Y\right) = w_n\left(f_0, f_1, ..., f_n\right),
\end{aligned}$$

so that (17) is proven (this argument even makes sense for $n = 0$ if we define the polynomial w_{-1} by $w_{-1}\left(X\right) = 0$, which agrees with the formula $w_n\left(X\right) = \sum_{k=0}^{n} p^k X_k^{p^{n-k}}$ because empty sums are understood to have the value 0). This completes the proof of Theorem 7.

Now, using Theorem 7, it is easy to verify the main claim of [1], 5.25 - namely, the claim that the map $\mathbf{V}_p$ defined in [1], 5.25 is a functorial group endomorphism of the Witt vectors. In fact, this follows from the following fact:

Corollary 8. For every commutative ring A with unity, the map $\mathbf{V}_p : W_{p^\infty}\left(A\right) \to W_{p^\infty}\left(A\right)$ defined by

$$\mathbf{V}_p a = \left(v_0\left(a\right), v_1\left(a\right), v_2\left(a\right), ...\right) \qquad \text{for every } a \in W_{p^\infty}\left(A\right)$$

is a group endomorphism of the additive group of $W_{p^\infty}(A)$.

Proof of Corollary 8. Any $a \in W_{p^\infty}(A)$ and $b \in W_{p^\infty}(A)$ satisfy

$$\mathbf{V}_p(a +_W b) = (v_0(a +_W b), v_1(a +_W b), v_2(a +_W b), ...)$$

and

$$\mathbf{V}_p a +_W \mathbf{V}_p b = (s_0(\mathbf{V}_p a; \mathbf{V}_p b), s_1(\mathbf{V}_p a; \mathbf{V}_p b), s_2(\mathbf{V}_p a; \mathbf{V}_p b), ...).$$

But for any $n \in \mathbb{N}$, we have

$$\begin{aligned} v_n(a +_W b) &= v_n(s_0(a;b), s_1(a;b), s_2(a;b), ...) \\ &= s_n(v_0(a), v_1(a), v_2(a), ...; v_0(b), v_1(b), v_2(b), ...) \qquad \text{(by Theorem 7)} \\ &= s_n(\mathbf{V}_p a; \mathbf{V}_p b). \qquad (18) \end{aligned}$$

Hence,

$$\begin{aligned} \mathbf{V}_p(a +_W b) &= (v_0(a +_W b), v_1(a +_W b), v_2(a +_W b), ...) \\ &= (s_0(\mathbf{V}_p a; \mathbf{V}_p b), s_1(\mathbf{V}_p a; \mathbf{V}_p b), s_2(\mathbf{V}_p a; \mathbf{V}_p b), ...) \qquad \text{(by (18))} \\ &= \mathbf{V}_p a +_W \mathbf{V}_p b. \end{aligned}$$

Thus, $\mathbf{V}_p(a +_W b) = \mathbf{V}_p a +_W \mathbf{V}_p b$ holds for any $a \in W_{p^\infty}(A)$ and $b \in W_{p^\infty}(A)$. This yields that $\mathbf{V}_p$ is a group endomorphism of the additive group of $W_{p^\infty}(A)$. Corollary 8 is proven.

Our next application is a proof of part of [1], 5.27 (namely, of the integrality of f_n and of (5.30)). This comes down to showing the following fact:

Theorem 9. **(a)** There exists one and only one family $(f_0, f_1, f_2, ...) \in (\mathbb{Q}[X])^{\mathbb{N}}$ of polynomials such that

$$(w_n(f_0, f_1, ..., f_n) = w_{n+1} \qquad \text{for every } n \in \mathbb{N}). \qquad (19)$$

(b) This family $(f_0, f_1, f_2, ...) \in (\mathbb{Q}[X])^{\mathbb{N}}$ satisfies $f_n \in \mathbb{Z}[X_0, X_1, ..., X_{n+1}]$ for every $n \in \mathbb{N}$.

(c) This family $(f_0, f_1, f_2, ...) \in (\mathbb{Q}[X])^{\mathbb{N}}$ satisfies $f_n \equiv X_n^p \bmod p\mathbb{Z}[X_0, X_1, ..., X_{n+1}]$ for every $n \in \mathbb{N}$.

Proof of Theorem 9. Define a family $(p_0, p_1, p_2, ...) \in (\mathbb{Q}[X])^{\mathbb{N}}$ by $p_k = w_{k+1}$ for all $k \in \mathbb{N}$. Then, Theorem 2 **(a)** (applied to $\Xi = X$) yields that there exists one and only one family $(f_0, f_1, f_2, ...) \in (\mathbb{Q}[\Xi])^{\mathbb{N}}$ of polynomials such that

$$(w_n(f_0, f_1, ..., f_n) = p_n \qquad \text{for every } n \in \mathbb{N}).$$

This is exactly the statement of Theorem 9 **(a)** (because $p_n = w_{n+1}$). Thus, Theorem 9 **(a)** is proven.

Theorem 2 **(b)** (applied to $\Xi = X$) yields that this family $(f_0, f_1, f_2, ...) \in (\mathbb{Q}[X])^{\mathbb{N}}$ satisfies $f_n \in \mathbb{Q}[p_0, p_1, ..., p_n]$ for every $n \in \mathbb{N}$. But recall that $p_k = w_{k+1}$ for all $k \in \mathbb{N}$. Thus,

$$\mathbb{Q}[p_0, p_1, ..., p_n] = \mathbb{Q}[w_1, w_2, ..., w_{n+1}] \subseteq \mathbb{Q}[X_0, X_1, ..., X_{n+1}]$$

(since the Witt polynomials w_1, w_2, ..., w_{n+1} all lie in $\mathbb{Q}[X_0, X_1, ..., X_{n+1}]$). Hence, $f_n \in \mathbb{Q}[p_0, p_1, ..., p_n] = \mathbb{Q}[X_0, X_1, ..., X_{n+1}]$ for every $n \in \mathbb{N}$.

Theorem 2 **(c)** (applied to $\Xi = X$) yields that our family $(f_0, f_1, f_2, ...) \in (\mathbb{Q}[X])^{\mathbb{N}}$ satisfies $(f_0, f_1, f_2, ...) \in (\mathbb{Z}[X])^{\mathbb{N}}$ if and only if

$$(p_n - p_{n-1}(X^p) \in p^n \mathbb{Z}[X] \qquad \text{for every } n \in \mathbb{N}). \tag{20}$$

But (20) does hold, since

$$\begin{aligned} p_n - p_{n-1}(X^p) &= w_{n+1} - w_n(X^p) && \text{(since } p_k = w_{k+1} \text{ for all } k \in \mathbb{N}) \\ &= w_{n+1}(X) - w_n(X^p) \\ &= p^{n+1} X_{n+1} && \text{(by Lemma 6, applied to } n+1 \text{ instead of } n) \\ &\in p^n \mathbb{Z}[X] \end{aligned}$$

for every $n \in \mathbb{N}$. Thus, $(f_0, f_1, f_2, ...) \in (\mathbb{Z}[X])^{\mathbb{N}}$. In other words, $f_n \in \mathbb{Z}[X]$ for every $n \in \mathbb{N}$.

Altogether, we now know that $f_n \in \mathbb{Q}[X_0, X_1, ..., X_{n+1}]$ and $f_n \in \mathbb{Z}[X]$ for every $n \in \mathbb{N}$. Hence,

$$f_n \in \mathbb{Q}[X_0, X_1, ..., X_{n+1}] \cap \mathbb{Z}[X] = \mathbb{Z}[X_0, X_1, ..., X_{n+1}]$$

for every $n \in \mathbb{N}$. This proves Theorem 9 **(b)**.

It remains to verify Theorem 9 **(c)**. This will be done by strong induction over n: We let n be some nonnegative integer, and we wish to prove that

$$f_n \equiv X_n^p \bmod p\mathbb{Z}[X_0, X_1, ..., X_{n+1}],$$

assuming that we have already shown that

$$f_k \equiv X_k^p \bmod p\mathbb{Z}[X_0, X_1, ..., X_{k+1}] \qquad \text{for all } k < n. \tag{21}$$

On the one hand,

$$\begin{aligned} w_{n+1} &= w_n(f_0, f_1, ..., f_n) && \text{(by (19))} \\ &= \sum_{k=0}^{n} p^k f_k^{p^{n-k}} = \sum_{k=0}^{n-1} p^k f_k^{p^{n-k}} + p^n \underbrace{f_n^{p^{n-n}}}_{= f_n^{p^0} = f_n} = \sum_{k=0}^{n-1} p^k f_k^{p^{n-k}} + p^n f_n, \end{aligned}$$

but on the other hand

$$\begin{aligned} w_{n+1} &= \sum_{k=0}^{n+1} p^k X_k^{p^{(n+1)-k}} = \sum_{k=0}^{n-1} p^k X_k^{p^{(n+1)-k}} + p^n \underbrace{X_n^{p^{(n+1)-n}}}_{= X_n^{p^1} = X_n^p} + p^{n+1} \underbrace{X_{n+1}^{p^{(n+1)-(n+1)}}}_{= X_{n+1}^{p^0} = X_{n+1}} \\ &= \sum_{k=0}^{n-1} p^k X_k^{p^{(n+1)-k}} + p^n X_n^p + p^{n+1} X_{n+1}. \end{aligned}$$

Thus,

$$\sum_{k=0}^{n-1} p^k f_k^{p^{n-k}} + p^n f_n = \sum_{k=0}^{n-1} p^k X_k^{p^{(n+1)-k}} + p^n X_n^p + p^{n+1} X_{n+1}. \tag{22}$$

Now, for every $k < n$, we have $f_k \equiv X_k^p \bmod p\mathbb{Z}[X_0, X_1, ..., X_{n+1}]$ (this follows from (21) since $p\mathbb{Z}[X_0, X_1, ..., X_{k+1}] \subseteq p\mathbb{Z}[X_0, X_1, ..., X_{n+1}]$) and thus

$$f_k^{p^{n-k}} \equiv \left(X_k^p\right)^{p^{n-k}} \bmod p^{1+n-k}\mathbb{Z}[X_0, X_1, ..., X_{n+1}]$$

(by Lemma 3, applied to $\mathbb{Z}[X_0, X_1, ..., X_{n+1}]$, f_k, X_k^p, 1 and $n-k$ instead of A, a, b, k and ℓ, respectively), and multiplication by p^k yields

$$p^k f_k^{p^{n-k}} \equiv p^k \left(X_k^p\right)^{p^{n-k}} \bmod \underbrace{p^{(1+n-k)}p^k}_{=p^{(1+n-k)+k}=p^{1+n}=p^{n+1}} \mathbb{Z}[X_0, X_1, ..., X_{n+1}]. \tag{23}$$

Thus,

$$\sum_{k=0}^{n-1} p^k f_k^{p^{n-k}} \equiv \sum_{k=0}^{n-1} p^k \underbrace{\left(X_k^p\right)^{p^{n-k}}}_{=X_k^{pp^{n-k}}=X_k^{p^{n-k+1}}=X_k^{p^{(n+1)-k}}} = \sum_{k=0}^{n-1} p^k X_k^{p^{(n+1)-k}} \bmod p^{n+1}\mathbb{Z}[X_0, X_1, ..., X_{n+1}].$$

Subtracting this congruence from the equation (22), we obtain

$$p^n f_n \equiv p^n X_n^p + p^{n+1} X_{n+1} \bmod p^{n+1}\mathbb{Z}[X_0, X_1, ..., X_{n+1}].$$

Since $p^{n+1}X_{n+1} \equiv 0 \bmod p^{n+1}\mathbb{Z}[X_0, X_1, ..., X_{n+1}]$, this simplifies to

$$p^n f_n \equiv p^n X_n^p \bmod p^{n+1}\mathbb{Z}[X_0, X_1, ..., X_{n+1}].$$

Dividing this congruence by p^n, we obtain

$$f_n \equiv X_n^p \bmod p\mathbb{Z}[X_0, X_1, ..., X_{n+1}],$$

and this completes our induction step. Thus, Theorem 9 **(c)** is proven.

Thus, two of the statements in [1], 5.27 are proven. Proving the remaining statements is left to the reader (hint: [1], (5.31) follows from Theorem 9 **(c)**, and the statement that $\mathbf{f}_p$ is an endomorphism of the unital ring $W_{p^\infty}(A)$ is proven similarly to our proof of Corollary 8).[9]

As a final application of Theorem 1, we will prove the main claim of [1], 5.40. This claim says that:

> **Theorem 10.** Let A be a commutative ring with unity. Let $a = (a_0, a_1, a_2, ...) \in W_{p^\infty}(A)$ and $b = (b_0, b_1, b_2, ...) \in W_{p^\infty}(A)$ be such that for every $n \in \mathbb{N}$, at least one of a_n and b_n is zero. Then, $a +_W b = (a_0 + b_0, a_1 + b_1, a_2 + b_2, ...)$.

[9] As a side-note to [1], 5.27, let me remark that there seems to be some confusion in literature regarding the name "Frobenius". While [1] denotes the map

$$\mathbf{f}_p : W_{p^\infty}(A) \to W_{p^\infty}(A),$$
$$a \mapsto (f_0(a), f_1(a), f_2(a), ...)$$

as "Frobenius", some other sources (like [2]) denote the map

$$W_{p^\infty}(A) \to W_{p^\infty}(A),$$
$$(a_0, a_1, a_2, ...) \mapsto (a_0^p, a_1^p, a_2^p, ...)$$

as "Frobenius". These two maps are, in general, different (though they are equal if $p \cdot 1_A = 0$ in A).

We will derive this fact from the following lemma:

Lemma 11. Let $f : \mathbb{N} \to \{0,1\}$ and $g : \mathbb{N} \to \{0,1\}$ be two functions such that for every $n \in \mathbb{N}$, at least one of $f(n)$ and $g(n)$ is zero. Then,

$$s_n(f(0)X_0, f(1)X_1, f(2)X_2, ...; g(0)X_0, g(1)X_1, g(2)X_2, ...) = (f(n) + g(n))X_n$$

for every $n \in \mathbb{N}$.

Proof of Lemma 11. Let us first notice that

$$(f(k))^j + (g(k))^j = (f(k) + g(k))^j \tag{24}$$

for every positive integer j and every $k \in \mathbb{N}$ [10].

Define two families $(f_0, f_1, f_2, ...) \in (\mathbb{Q}[X])^{\mathbb{N}}$ and $(g_0, g_1, g_2, ...) \in (\mathbb{Q}[X])^{\mathbb{N}}$ by

$$f_n = s_n(f(0)X_0, f(1)X_1, f(2)X_2, ...; g(0)X_0, g(1)X_1, g(2)X_2, ...) \quad \text{for every } n \in \mathbb{N}, \quad \text{and}$$
$$g_n = (f(n) + g(n))X_n \quad \text{for every } n \in \mathbb{N}.$$

Theorem 1 **(a)** (applied to $\Xi = X$) yields that (1) if and only if (2). But (2) holds, since for every $n \in \mathbb{N}$, we have

$$\begin{aligned}
w_n(f_0, f_1, ..., f_n) &= w_n(s_0(f(0)X_0, f(1)X_1, f(2)X_2, ...; g(0)X_0, g(1)X_1, g(2)X_2, ...), \\
&\qquad s_1(f(0)X_0, f(1)X_1, f(2)X_2, ...; g(0)X_0, g(1)X_1, g(2)X_2, ...), \\
&\qquad s_2(f(0)X_0, f(1)X_1, f(2)X_2, ...; g(0)X_0, g(1)X_1, g(2)X_2, ...), \\
&\qquad ...) \\
&= w_n(f(0)X_0, f(1)X_1, f(2)X_2, ...) + w_n(g(0)X_0, g(1)X_1, g(2)X_2, ...) \\
&\qquad \left(\begin{array}{c} \text{this follows from the polynomial identity} \\ w_n(s_0(X;Y), s_1(X;Y), s_2(X;Y), ...) = w_n(X) + w_n(Y) \\ \text{upon substitution of} \\ (f(0)X_0, f(1)X_1, f(2)X_2, ...; g(0)X_0, g(1)X_1, g(2)X_2, ...) \text{ for } (X;Y) \end{array} \right) \\
&= \sum_{k=0}^{n} p^k (f(k)X_k)^{p^{n-k}} + \sum_{k=0}^{n} p^k (g(k)X_k)^{p^{n-k}} \qquad \text{(by the definition of } w_n\text{)} \\
&= \sum_{k=0}^{n} p^k \underbrace{\left((f(k))^{p^{n-k}} + (g(k))^{p^{n-k}}\right)}_{\substack{=(f(k)+g(k))^{p^{n-k}} \\ \text{(by (24), applied to } j=p^{n-k}\text{)}}} X_k^{p^{n-k}} \\
&= \sum_{k=0}^{n} p^k (f(k) + g(k))^{p^{n-k}} X_k^{p^{n-k}} = \sum_{k=0}^{n} p^k \left(\underbrace{(f(k) + g(k))X_k}_{=g_k}\right)^{p^{n-k}} \\
&= \sum_{k=0}^{n} p^k g_k^{p^{n-k}} = w_n(g_0, g_1, ..., g_n).
\end{aligned}$$

[10] *Proof of (24):* Let j be a positive integer, and let $k \in \mathbb{N}$.

We know that $f(k) \in \{0,1\}$ (since f is a map $\mathbb{N} \to \{0,1\}$) and $g(k) \in \{0,1\}$ (for similar reasons). Furthermore, we know that at least one of $f(k)$ and $g(k)$ is zero. Hence, we are in one of the following three cases:

Case 1: We have $f(k) = 0$ and $g(k) = 0$.

Case 2: We have $f(k) = 0$ and $g(k) = 1$.

Case 3: We have $f(k) = 1$ and $g(k) = 0$.

But (24) can be straightforwardly verified in each of these three cases.

Thus, (1) holds as well, so that $f_n = g_n$ for every $n \in \mathbb{N}$. But recalling the definitions of f_n and g_n, we notice that this is exactly the claim of Lemma 11. Thus, Lemma 11 is proven.

Proof of Theorem 10. Define two functions $f : \mathbb{N} \to \{0,1\}$ and $g : \mathbb{N} \to \{0,1\}$ by $f(n) = \begin{cases} 1, & \text{if } a_n \neq 0; \\ 0, & \text{if } a_n = 0 \end{cases}$ and $g(n) = \begin{cases} 1, & \text{if } b_n \neq 0; \\ 0, & \text{if } b_n = 0 \end{cases}$ for every $n \in \mathbb{N}$. Then, for every $n \in \mathbb{N}$, at least one of $f(n)$ and $g(n)$ is zero (since at least one of a_n and b_n is zero). Hence, Lemma 11 yields

$$s_n(f(0) X_0, f(1) X_1, f(2) X_2, ...; g(0) X_0, g(1) X_1, g(2) X_2, ...) = (f(n) + g(n)) X_n$$

for every $n \in \mathbb{N}$. Evaluating this polynomial identity at $(X_0, X_1, X_2, ...) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, ...)$, we get

$$\begin{aligned} &s_n(f(0)(a_0+b_0), f(1)(a_1+b_1), f(2)(a_2+b_2), ...; g(0)(a_0+b_0), g(1)(a_1+b_1), g(2)(a_2+b_2), ...) \\ &= (f(n) + g(n))(a_n + b_n) \end{aligned} \tag{25}$$

for every $n \in \mathbb{N}$.

Besides, for every $n \in \mathbb{N}$, we have

$$f(n) a_n = \begin{cases} 1, & \text{if } a_n \neq 0; \\ 0, & \text{if } a_n = 0 \end{cases} \cdot a_n = \begin{cases} a_n, & \text{if } a_n \neq 0; \\ 0, & \text{if } a_n = 0 \end{cases} = a_n;$$

$$f(n) b_n = \begin{cases} 1, & \text{if } a_n \neq 0; \\ 0, & \text{if } a_n = 0 \end{cases} \cdot b_n = \begin{cases} b_n, & \text{if } a_n \neq 0; \\ 0, & \text{if } a_n = 0 \end{cases} = 0 \qquad \left(\begin{array}{c} \text{since } b_n = 0 \text{ if } a_n \neq 0, \\ \text{because at least one of } a_n \text{ and } b_n \text{ is zero} \end{array} \right);$$

$$g(n) a_n = \begin{cases} 1, & \text{if } b_n \neq 0; \\ 0, & \text{if } b_n = 0 \end{cases} \cdot a_n = \begin{cases} a_n, & \text{if } b_n \neq 0; \\ 0, & \text{if } b_n = 0 \end{cases} = 0 \qquad \left(\begin{array}{c} \text{since } a_n = 0 \text{ if } b_n \neq 0, \\ \text{because at least one of } a_n \text{ and } b_n \text{ is zero} \end{array} \right);$$

$$g(n) b_n = \begin{cases} 1, & \text{if } b_n \neq 0; \\ 0, & \text{if } b_n = 0 \end{cases} \cdot b_n = \begin{cases} b_n, & \text{if } b_n \neq 0; \\ 0, & \text{if } b_n = 0 \end{cases} = b_n,$$

and therefore

$$\begin{aligned} f(n)(a_n + b_n) &= f(n) a_n + f(n) b_n = a_n + 0 = a_n; \\ g(n)(a_n + b_n) &= g(n) a_n + g(n) b_n = 0 + b_n = b_n, \end{aligned}$$

so that

$$(f(n) + g(n))(a_n + b_n) = f(n)(a_n + b_n) + g(n)(a_n + b_n) = a_n + b_n.$$

Now, $f(n)(a_n + b_n) = a_n$ for every $n \in \mathbb{N}$, and therefore

$$\begin{aligned} &(f(0)(a_0+b_0), f(1)(a_1+b_1), f(2)(a_2+b_2), ...) \\ &= (a_0, a_1, a_2, ...) = a. \end{aligned} \tag{26}$$

Similarly,

$$(g(0)(a_0+b_0), g(1)(a_1+b_1), g(2)(a_2+b_2), ...) = b. \tag{27}$$

Now,

$$a +_W b = (s_0(a;b), s_1(a;b), s_2(a;b), ...) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, ...),$$

because every $n \in \mathbb{N}$ satisfies

$$
\begin{aligned}
&s_n(a;b) \\
&= s_n\left(f(0)(a_0+b_0), f(1)(a_1+b_1), f(2)(a_2+b_2), ...; g(0)(a_0+b_0), g(1)(a_1+b_1), g(2)(a_2+b_2), ...\right) \\
&\qquad \left(\begin{array}{c} \text{since } a = (f(0)(a_0+b_0), f(1)(a_1+b_1), f(2)(a_2+b_2), ...) \text{ by (26)} \\ \text{and } b = (g(0)(a_0+b_0), g(1)(a_1+b_1), g(2)(a_2+b_2), ...) \text{ by (27)} \end{array} \right) \\
&= (f(n)+g(n))(a_n+b_n) \qquad \text{(by (25))} \\
&= \underbrace{f(n)(a_n+b_n)}_{=a_n} + \underbrace{g(n)(a_n+b_n)}_{=b_n} = a_n + b_n.
\end{aligned}
$$

This proves Theorem 10.

References

[1] Michiel Hazewinkel, *Witt vectors. Part 1*, revised version: 20 April 2008. `https://arxiv.org/abs/0804.3888v1`

[2] Siegfried Bosch, *Algebra*, Sechste Auflage, Springer-Verlag 2006.