Witt vectors. Part 1

Michiel Hazewinkel
Sidenotes by Darij Grinberg

Witt#5a: Polynomials that can be written as big w_n

[completed, not proofread]

The point of this note is to generalize the property of p-adic Witt polynomials that appeared as Theorem 1 in [2] to big Witt polynomials.

First, let us introduce the notation that we are going to use.

Definition 1. Let $\mathbb{P}$ denote the set of all primes. (A *prime* means an integer $n > 1$ such that the only divisors of n are n and 1. The word "divisor" means "positive divisor".)

Definition 2. We denote the set $\{0, 1, 2, ...\}$ by $\mathbb{N}$, and we denote the set $\{1, 2, 3, ...\}$ by $\mathbb{N}_+$. (Note that our notations conflict with the notations used by Hazewinkel in [1]; in fact, Hazewinkel uses the letter $\mathbb{N}$ for the set $\{1, 2, 3, ...\}$, which we denote by $\mathbb{N}_+$.)

Definition 3. 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). [1]. For any $n \in \mathbb{N}$, let Ξ^n mean the family of the n-th powers of all elements of our family Ξ (considered as elements of $\mathbb{Z}[\Xi]$) [2]. (Therefore, whenever $P \in \mathbb{Q}[\Xi]$ is a polynomial, then $P(\Xi^n)$ is the polynomial obtained from P after replacing every indeterminate by its n-th power.[3])

Note that if Ξ is the empty family, then $\mathbb{Q}[\Xi]$ simply is the ring $\mathbb{Q}$, and $\mathbb{Z}[\Xi]$ simply is the ring $\mathbb{Z}$.

Definition 4. For any integer m, the set $\{n \in \mathbb{N}_+ \mid (n \mid m)\}$ will be denoted by $\mathbb{N}_{|m}$. This set $\mathbb{N}_{|m}$ is the set of all divisors of m.

Definition 5. If N is a set, we shall denote by X_N the family $(X_n)_{n \in N}$ of distinct symbols. Hence, $\mathbb{Z}[X_N]$ is the ring $\mathbb{Z}\left[(X_n)_{n \in N}\right]$ (this is the polynomial ring over $\mathbb{Z}$ in $|N|$ indeterminates, where the indeterminates are labelled X_n, where n runs through the elements of the set N). For instance, $\mathbb{Z}\left[X_{\mathbb{N}_+}\right]$ is the polynomial ring $\mathbb{Z}[X_1, X_2, X_3, ...]$ (since $\mathbb{N}_+ = \{1, 2, 3, ...\}$), and $\mathbb{Z}\left[X_{\{1,2,3,5,6,10\}}\right]$ is the polynomial ring $\mathbb{Z}[X_1, X_2, X_3, X_5, X_6, X_{10}]$.

If A is a commutative ring with unity, if N is a set, if $(x_d)_{d \in N} \in A^N$ is a family of elements of A indexed by elements of N, and if $P \in \mathbb{Z}[X_N]$, then

[1] 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 $\mathbb{Z}[X_0, X_1, X_2, ...; Y_0, Y_1, Y_2, ...; Z_0, Z_1, Z_2, ...]$.

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

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

we denote by $P\left(\left(x_d\right)_{d\in N}\right)$ the element of A that we obtain if we substitute x_d for X_d for every $d \in N$ into the polynomial P. (For instance, if $N = \{1, 2, 5\}$ and $P = X_1^2 + X_2X_5 - X_5$, and if $x_1 = 13$, $x_2 = 37$ and $x_5 = 666$, then $P\left(\left(x_d\right)_{d\in N}\right) = 13^2 + 37 \cdot 666 - 666$.)

Definition 6. For any $n \in \mathbb{N}_+$, we define a polynomial $w_n \in \mathbb{Z}\left[X_{\mathbb{N}_{|n}}\right]$ by

$$w_n = \sum_{d|n} dX_d^{n/d}.$$

Hence, for every commutative ring A with unity, and for any family $(x_k)_{k\in\mathbb{N}_{|n}} \in A^{\mathbb{N}_{|n}}$ of elements of A, we have

$$w_n\left(\left(x_k\right)_{k\in\mathbb{N}_{|n}}\right) = \sum_{d|n} dx_d^{n/d}.$$

The polynomials w_1, w_2, w_3, ... are called the *big Witt polynomials* or, simply, the *Witt polynomials*.

Caution: These polynomials w_1, w_2, w_3, ... are referred to as w_1, w_2, w_3, ... most of the time in [1] (beginning with Section 9). However, in Sections 5-8 of [1], Hazewinkel uses the notations w_1, w_2, w_3, ... for some *different* polynomials (the so-called p-adic Witt polynomials, defined by formula (5.1) in [1]), which are *not the same as our polynomials* w_1, w_2, w_3, ... (though they are related to them: namely, the polynomial denoted by w_k in Sections 5-8 of [1] is the polynomial that we are denoting by w_{p^k} here *after a renaming of variables*; on the other hand, the polynomial that we call w_k here is something completely different).

Definition 7. Let $n \in \mathbb{Z} \setminus \{0\}$. Let $p \in \mathbb{P}$. We denote by $v_p(n)$ the largest nonnegative integer m satisfying $p^m \mid n$. Clearly, $p^{v_p(n)} \mid n$ and $v_p(n) \geq 0$. Besides, $v_p(n) = 0$ if and only if $p \nmid n$.
We also set $v_p(0) = \infty$; this way, our definition of $v_p(n)$ extends to all $n \in \mathbb{Z}$ (and not only to $n \in \mathbb{Z} \setminus \{0\}$).

Definition 8. Let $n \in \mathbb{N}_+$. We denote by $\operatorname{PF} n$ the set of all prime divisors of n. By the unique factorization theorem, the set $\operatorname{PF} n$ is finite and satisfies $n = \prod_{p\in\operatorname{PF} n} p^{v_p(n)}$.

Let us now formulate our main result:

Theorem 1. Let Ξ be a family of symbols. Let $\tau \in \mathbb{Z}[\Xi]$ be a polynomial. Let $m \in \mathbb{N}$. Then, the following two assertions $\mathcal{A}$ and $\mathcal{B}$ are equivalent:

Assertion $\mathcal{A}$: There exists a family $(\tau_d)_{d\in\mathbb{N}_{|m}} \in (\mathbb{Z}[\Xi])^{\mathbb{N}_{|m}}$ such that $\tau = w_m\left(\left(\tau_d\right)_{d\in\mathbb{N}_{|m}}\right)$.

Assertion $\mathcal{B}$: We have $\dfrac{\partial}{\partial\xi}\tau \in m\mathbb{Z}[\Xi]$ for every $\xi \in \Xi$.

Remarks: **1)** Here, $\dfrac{\partial}{\partial \xi}\tau$ means the derivative of the polynomial $\tau \in \mathbb{Z}\left[\Xi\right]$ with respect to the variable ξ.

2) Theorem 1 makes sense even in the case when Ξ is the empty family (in this case, the Assertion $\mathcal{B}$ is vacuously true (since no $\xi \in \Xi$ exists), and therefore Theorem 1 claims that in this case Assertion $\mathcal{A}$ is true as well; see Corollary 3 for details).

Before we come to proving this theorem, let us remark why exactly this Theorem 1 generalizes the Theorem 1 of [2]. In fact, if p is a prime and $n \in \mathbb{N}$, then the big Witt polynomial w_{p^n} (the one that we have defined above, not the one called w_{p^n} in [2]) is

$$\begin{aligned} w_{p^n} &= \sum_{d \mid p^n} d X_d^{p^n/d} = \sum_{d \in \mathbb{N}_{\mid p^n}} d X_d^{p^n/d} \\ &= \sum_{k=0}^{n} p^k X_{p^k}^{p^n/p^k} \qquad \left(\text{since } \mathbb{N}_{\mid p^n} = \left\{p^0, p^1, ..., p^n\right\} \text{ (because } p \text{ is a prime)}\right) \\ &= \sum_{k=0}^{n} p^k X_{p^k}^{p^{n-k}} \qquad \left(\text{since } p^n/p^k = p^{n-k}\right), \end{aligned}$$

and therefore this polynomial w_{p^n} is equal to the polynomial denoted by w_n in [2][4], up to a renaming of variables (in fact, if we rename the variable X_{p^k} as X_k for every $k \in \mathbb{N}$, then $w_{p^n} = \sum_{k=0}^{n} p^k X_{p^k}^{p^{n-k}}$ becomes $w_{p^n} = \sum_{k=0}^{n} p^k X_k^{p^{n-k}}$, which is exactly the formula defining w_n in [2]). Hence, in the case when $m = p^n$ for a prime p and an integer $n \in \mathbb{N}$, and when $\Xi = (X_0, X_1, X_2, ...)$, the Assertions $\mathcal{A}$ and $\mathcal{B}$ of our Theorem 1 are identical with the Assertions $\mathcal{A}$ and $\mathcal{B}$ of the Theorem 1 in [2], and therefore our Theorem 1 yields the Theorem 1 in [2].

Before we come to the proof of Theorem 1, let us state a simple fact: If Ξ is a family of symbols, then

$$\frac{\partial}{\partial \xi} P^g = g P^{g-1} \cdot \left(\frac{\partial}{\partial \xi} g\right) \tag{1}$$

for every $\xi \in \Xi$, every $P \in \mathbb{Z}\left[\Xi\right]$ and every positive integer g. (This can be proven either using the chain rule for differentiation, or by induction on g using the Leibniz rule.)

Proof of Theorem 1. Proof of the implication $\mathcal{A} \Longrightarrow \mathcal{B}$: Assume that the Assertion $\mathcal{A}$ holds. Then, there exists a family $(\tau_d)_{d \in \mathbb{N}_{\mid m}} \in \left(\mathbb{Z}\left[\Xi\right]\right)^{\mathbb{N}_{\mid m}}$ such that $\tau = w_m\left((\tau_d)_{d \in \mathbb{N}_{\mid m}}\right)$. Hence,

$$\tau = w_m\left((\tau_d)_{d \in \mathbb{N}_{\mid m}}\right) = \sum_{d \mid m} d \tau_d^{m/d},$$

[4]Let us remind ourselves once again that this is *not* the polynomial that we call w_n *in this present note.*

and thus every $\xi \in \Xi$ satisfies

$$\frac{\partial}{\partial \xi}\tau = \frac{\partial}{\partial \xi}\sum_{d\mid m} d\tau_d^{m/d} = \sum_{d\mid m} d \underbrace{\frac{\partial}{\partial \xi}\tau_d^{m/d}}_{\substack{=(m/d)\tau_d^{m/d-1}\cdot\left(\frac{\partial}{\partial\xi}\tau_d\right) \\ \text{(by (1), applied to } P=\tau_d \text{ and } g=m/d)}} = \sum_{d\mid m} \underbrace{d\,(m/d)}_{=m} \tau_d^{m/d-1}\cdot\left(\frac{\partial}{\partial\xi}\tau_d\right)$$

$$= m \underbrace{\sum_{d\mid m} \tau_d^{m/d-1}\cdot\left(\frac{\partial}{\partial\xi}\tau_d\right)}_{\in\mathbb{Z}[\Xi]} \in m\mathbb{Z}\left[\Xi\right],$$

so that Assertion $\mathcal{B}$ holds. Thus, we have shown that whenever Assertion $\mathcal{A}$ holds, Assertion $\mathcal{B}$ must hold as well. This proves the implication $\mathcal{A} \Longrightarrow \mathcal{B}$.

Proof of the implication $\mathcal{B} \Longrightarrow \mathcal{A}$: Let us assume that Assertion $\mathcal{B}$ holds. Thus, we have $\dfrac{\partial}{\partial\xi}\tau \in m\mathbb{Z}\left[\Xi\right]$ for every $\xi \in \Xi$. If we rename ξ as η here, this rewrites as follows: We have $\dfrac{\partial}{\partial\eta}\tau \in m\mathbb{Z}\left[\Xi\right]$ for every $\eta \in \Xi$.

Let us introduce some notation:

For every family $j \in \mathbb{N}^{\Xi}$ and every $\xi \in \Xi$, let us denote by j_ξ the ξ-th member of the family j. Then, every family $j \in \mathbb{N}^{\Xi}$ satisfies $j = (j_\xi)_{\xi\in\Xi}$.

Let $\mathbb{N}^{\Xi}_{\text{fin}}$ denote the set $\left\{j \in \mathbb{N}^{\Xi} \mid \text{only finitely many } \xi \in \Xi \text{ satisfy } j_\xi \neq 0\right\}$. For every $j \in \mathbb{N}^{\Xi}_{\text{fin}}$, let Ξ^j denote the monomial $\prod\limits_{\xi\in\Xi} \xi^{j_\xi}$. For every polynomial $P \in \mathbb{Z}\left[\Xi\right]$, let $\operatorname{coeff}_j P$ denote the coefficient of P before this monomial Ξ^j. Then, every polynomial $P \in \mathbb{Z}\left[\Xi\right]$ satisfies

$$P = \sum_{j\in\mathbb{N}^{\Xi}_{\text{fin}}} \operatorname{coeff}_j P \cdot \Xi^j. \tag{2}$$

(This sum $\sum\limits_{j\in\mathbb{N}^{\Xi}_{\text{fin}}} \operatorname{coeff}_j P \cdot \Xi^j$ has only finitely many nonzero summands, since every polynomial has only finitely many nonzero coefficients.)

For every $n \in \mathbb{N}$ and every $j \in \mathbb{N}^{\Xi}_{\text{fin}}$, let us denote by $nj \in \mathbb{N}^{\Xi}_{\text{fin}}$ the family $(nj_\xi)_{\xi\in\Xi}$. Clearly, $1j = (1j_\xi)_{\xi\in\Xi} = (j_\xi)_{\xi\in\Xi} = j$.

If $k \in \mathbb{N}^{\Xi}_{\text{fin}}$ and $n \in \mathbb{N}$, then we write $n \mid k$ if and only if ($n \mid k_\xi$ for every $\xi \in \Xi$). If $k \in \mathbb{N}^{\Xi}_{\text{fin}}$ and $n \in \mathbb{N}$ are such that $n \mid k$, then we can define a family $k/n \in \mathbb{N}^{\Xi}_{\text{fin}}$ by $k/n = \left(\dfrac{k_\xi}{n}\right)_{\xi\in\Xi}$ (indeed, $\dfrac{k_\xi}{n} \in \mathbb{N}$ for every $\xi \in \Xi$, since $n \mid k$ yields $n \mid k_\xi$). This family k/n clearly satisfies $n\,(k/n) = \left(n\dfrac{k_\xi}{n}\right)_{\xi\in\Xi} = (k_\xi)_{\xi\in\Xi} = k$. Also, it is obvious that $k/1 = \left(\dfrac{k_\xi}{1}\right)_{\xi\in\Xi} = (k_\xi)_{\xi\in\Xi} = k$.

Now, according to (2), our polynomial τ satisfies $\tau = \sum\limits_{j\in\mathbb{N}^{\Xi}_{\text{fin}}} \operatorname{coeff}_j \tau \cdot \Xi^j$. Thus, for

every $\eta \in \Xi$, we have

$$\frac{\partial}{\partial \eta}\tau = \frac{\partial}{\partial \eta}\sum_{j\in\mathbb{N}_{\text{fin}}^{\Xi}} \text{coeff}_j\,\tau \cdot \Xi^j = \sum_{j\in\mathbb{N}_{\text{fin}}^{\Xi}} \text{coeff}_j\,\tau \cdot \frac{\partial}{\partial \eta}\Xi^j = \sum_{j\in\mathbb{N}_{\text{fin}}^{\Xi}} \text{coeff}_j\,\tau \cdot \frac{\partial}{\partial \eta}\left(\eta^{j_\eta}\prod_{\xi\in\Xi\setminus\{\eta\}}\xi^{j_\xi}\right)$$

$$\left(\text{since } \Xi^j = \prod_{\xi\in\Xi}\xi^{j_\xi} = \eta^{j_\eta}\prod_{\xi\in\Xi\setminus\{\eta\}}\xi^{j_\xi}\right)$$

$$= \sum_{j\in\mathbb{N}_{\text{fin}}^{\Xi}} \text{coeff}_j\,\tau \cdot \underbrace{\left(\frac{\partial}{\partial \eta}\eta^{j_\eta}\right)}_{=\begin{cases} j_\eta\eta^{j_\eta-1}, \text{ if } j_\eta > 0; \\ 0, \text{ if } j_\eta = 0 \end{cases}} \prod_{\xi\in\Xi\setminus\{\eta\}}\xi^{j_\xi} = \sum_{j\in\mathbb{N}_{\text{fin}}^{\Xi}} \text{coeff}_j\,\tau \cdot \begin{cases} j_\eta\eta^{j_\eta-1}, \text{ if } j_\eta > 0; \\ 0, \text{ if } j_\eta = 0 \end{cases} \prod_{\xi\in\Xi\setminus\{\eta\}}\xi^{j_\xi}$$

$$= \sum_{\substack{j\in\mathbb{N}_{\text{fin}}^{\Xi}; \\ j_\eta>0}} \text{coeff}_j\,\tau \cdot \underbrace{\begin{cases} j_\eta\eta^{j_\eta-1}, \text{ if } j_\eta > 0; \\ 0, \text{ if } j_\eta = 0 \end{cases}}_{=j_\eta\eta^{j_\eta-1}, \text{ since } j_\eta>0} \prod_{\xi\in\Xi\setminus\{\eta\}}\xi^{j_\xi} + \sum_{\substack{j\in\mathbb{N}_{\text{fin}}^{\Xi}; \\ j_\eta=0}} \text{coeff}_j\,\tau \cdot \underbrace{\begin{cases} j_\eta\eta^{j_\eta-1}, \text{ if } j_\eta > 0; \\ 0, \text{ if } j_\eta = 0 \end{cases}}_{=0, \text{ since } j_\eta=0} \prod_{\xi\in\Xi\setminus\{\eta\}}\xi^{j_\xi}$$

$$= \sum_{\substack{j\in\mathbb{N}_{\text{fin}}^{\Xi}; \\ j_\eta>0}} \text{coeff}_j\,\tau \cdot j_\eta\eta^{j_\eta-1} \prod_{\xi\in\Xi\setminus\{\eta\}}\xi^{j_\xi} + \underbrace{\sum_{\substack{j\in\mathbb{N}_{\text{fin}}^{\Xi}; \\ j_\eta=0}} \text{coeff}_j\,\tau \cdot 0 \prod_{\xi\in\Xi\setminus\{\eta\}}\xi^{j_\xi}}_{=0} = \sum_{\substack{j\in\mathbb{N}_{\text{fin}}^{\Xi}; \\ j_\eta>0}} \text{coeff}_j\,\tau \cdot j_\eta\eta^{j_\eta-1} \prod_{\xi\in\Xi\setminus\{\eta\}}\xi^{j_\xi}. \tag{3}$$

Now, define a map

$$F : \left\{j \in \mathbb{N}_{\text{fin}}^{\Xi} \mid j_\eta > 0\right\} \to \mathbb{N}_{\text{fin}}^{\Xi} \qquad \text{defined by}$$

$$F(j) = \left(\begin{cases} j_\xi, \text{ if } \xi \neq \eta; \\ j_\eta - 1, \text{ if } \xi = \eta \end{cases}\right)_{\xi\in\Xi} \qquad \text{for every } j \in \mathbb{N}_{\text{fin}}^{\Xi} \text{ satisfying } j_\eta > 0.$$

This map F is a bijection (in fact, this map leaves all members of the family j fixed, except of the η-th member, which is reduced by 1). By the definition of F, every $j \in \mathbb{N}_{\text{fin}}^{\Xi}$ satisfying $j_\eta > 0$ is mapped to $F(j) = \left(\begin{cases} j_\xi, \text{ if } \xi \neq \eta; \\ j_\eta - 1, \text{ if } \xi = \eta \end{cases}\right)_{\xi\in\Xi}$. Hence, for every $\xi \in \Xi$, we have $(F(j))_\xi = \begin{cases} j_\xi, \text{ if } \xi \neq \eta; \\ j_\eta - 1, \text{ if } \xi = \eta \end{cases}$. In other words, $(F(j))_\xi = j_\xi$ if

$\xi \neq \eta$, and $\left(F\left(j\right)\right)_\eta = j_\eta - 1$ (since $\eta = \eta$). Using these two equations, (3) becomes

$$\begin{aligned}
\frac{\partial}{\partial \eta}\tau &= \sum_{\substack{j \in \mathbb{N}_{\text{fin}}^{\Xi}; \\ j_\eta > 0}} \underbrace{\operatorname{coeff}_j \tau}_{=\operatorname{coeff}_{F^{-1}(F(j))}\tau} \cdot \underbrace{j_\eta}_{\substack{=(j_\eta - 1)+1 \\ =\left(F(j)\right)_\eta + 1}} \underbrace{\eta^{j_\eta - 1}}_{\substack{=\eta^{\left(F(j)\right)_\eta} \\ (\text{since } \left(F(j)\right)_\eta = j_\eta - 1)}} \prod_{\xi \in \Xi \setminus \{\eta\}} \underbrace{\xi^{j_\xi}}_{\substack{=\xi^{\left(F(j)\right)_\xi} \\ (\text{since } \xi \in \Xi \setminus \{\eta\} \\ \text{yields } \xi \neq \eta \text{ and thus} \\ \left(F(j)\right)_\xi = j_\xi)}} \\
&= \sum_{\substack{j \in \mathbb{N}_{\text{fin}}^{\Xi}; \\ j_\eta > 0}} \operatorname{coeff}_{F^{-1}(F(j))}\tau \cdot \left(\left(F\left(j\right)\right)_\eta + 1\right) \eta^{\left(F(j)\right)_\eta} \prod_{\xi \in \Xi \setminus \{\eta\}} \xi^{\left(F(j)\right)_\xi} \\
&= \sum_{j \in \mathbb{N}_{\text{fin}}^{\Xi}} \operatorname{coeff}_{F^{-1}(j)}\tau \cdot \left(j_\eta + 1\right) \underbrace{\eta^{j_\eta} \prod_{\xi \in \Xi \setminus \{\eta\}} \xi^{j_\xi}}_{=\prod_{\xi \in \Xi} \xi^{j_\xi} = \xi^j} \qquad \left(\begin{array}{c} \text{here we substituted } F\left(j\right) \text{ for } j \text{ in the sum,} \\ \text{since the map } F \text{ is a bijection} \end{array}\right) \\
&= \sum_{j \in \mathbb{N}_{\text{fin}}^{\Xi}} \operatorname{coeff}_{F^{-1}(j)}\tau \cdot \left(j_\eta + 1\right) \xi^j.
\end{aligned}$$

Hence, for every $j \in \mathbb{N}_{\text{fin}}^{\Xi}$, we have $\operatorname{coeff}_j\left(\dfrac{\partial}{\partial \eta}\tau\right) = \operatorname{coeff}_{F^{-1}(j)}\tau \cdot \left(j_\eta + 1\right)$. But we must have $\operatorname{coeff}_j\left(\dfrac{\partial}{\partial \eta}\tau\right) \in m\mathbb{Z}$ (since $\dfrac{\partial}{\partial \eta}\tau \in m\mathbb{Z}\left[\Xi\right]$). Thus,

$$\operatorname{coeff}_{F^{-1}(j)}\tau \cdot \left(j_\eta + 1\right) \in m\mathbb{Z} \qquad \text{for every } j \in \mathbb{N}_{\text{fin}}^{\Xi}. \tag{4}$$

Thus, every $j \in \mathbb{N}_{\text{fin}}^{\Xi}$ and every $\eta \in \Xi$ satisfy

$$\operatorname{coeff}_j \tau \cdot j_\eta \in m\mathbb{Z} \tag{5}$$

(since (4), applied to $F\left(j\right)$ instead of j, yields $\operatorname{coeff}_{F^{-1}(F(j))}\tau \cdot \left(\left(F\left(j\right)\right)_\eta + 1\right) \in m\mathbb{Z}$, which simplifies to $\operatorname{coeff}_j \tau \cdot j_\eta \in m\mathbb{Z}$ because $F^{-1}\left(F\left(j\right)\right)$ and because $\underbrace{\left(F\left(j\right)\right)_\eta}_{=j_\eta - 1} + 1 = \left(j_\eta - 1\right) + 1 = j_\eta$).

Now we recall the following result from [4]:

Theorem 2. Let Ξ be a family of symbols. Let N be a nest[5], and let $\left(b_n\right)_{n \in N} \in \left(\mathbb{Z}\left[\Xi\right]\right)^N$ be a family of polynomials in the indeterminates Ξ. Then, the two following assertions $\mathcal{C}_\Xi$ and $\mathcal{D}_\Xi$ are equivalent:

Assertion $\mathcal{C}_\Xi$: Every $n \in N$ and every $p \in \operatorname{PF} n$ satisfies

$$b_{n/p}\left(\Xi^p\right) \equiv b_n \bmod p^{v_p(n)}\mathbb{Z}\left[\Xi\right].$$

Assertion $\mathcal{D}_\Xi$: There exists a family $\left(x_n\right)_{n \in N} \in \left(\mathbb{Z}\left[\Xi\right]\right)^N$ of elements of $\mathbb{Z}\left[\Xi\right]$ such that

$$\left(b_n = w_n\left(\left(x_k\right)_{k \in N}\right) \text{ for every } n \in N\right).$$

[5]We refer to [4] (Definition 5) for the definition of a nest. For our aims, it is only important to know that $\mathbb{N}_{|m}$ is a nest.

This Theorem 2 is part of Theorem 13 in [4] (which claims that the assertions $\mathcal{C}_\Xi$, $\mathcal{D}_\Xi$, $\mathcal{D}'_\Xi$, $\mathcal{E}_\Xi$, $\mathcal{E}'_\Xi$, $\mathcal{F}_\Xi$, $\mathcal{G}_\Xi$ and $\mathcal{H}_\Xi$ are equivalent, where $\mathcal{C}_\Xi$ and $\mathcal{D}_\Xi$ are our assertions $\mathcal{C}_\Xi$ and $\mathcal{D}_\Xi$, while $\mathcal{D}'_\Xi$, $\mathcal{E}_\Xi$, $\mathcal{E}'_\Xi$, $\mathcal{F}_\Xi$, $\mathcal{G}_\Xi$ and $\mathcal{H}_\Xi$ are some other assertions). Hence, for the proof of Theorem 2, we refer the reader to [4].

Now, let us continue with the proof of Theorem 1:

Let $N = \mathbb{N}_{|m}$. Then, every element n of N is a divisor of m, and hence $m/n \in \mathbb{N}$ for every $n \in N$.

We are going to apply Theorem 2 to the family $(b_n)_{n\in N} \in (\mathbb{Z}[\Xi])^N$ defined by

$$b_n = \sum_{\substack{j\in\mathbb{N}_{\text{fin}}^{\Xi};\\ (m/n)\mid j}} \operatorname{coeff}_j \tau \cdot \Xi^{j/(m/n)} \qquad \text{for every } n \in N.$$

Let $n \in N$ and every $p \in \operatorname{PF} n$. The polynomial $b_{n/p}(\Xi^p)$ is the polynomial obtained from $b_{n/p}$ after replacing every indeterminate by its n-th power. Since

$$b_{n/p} = \sum_{\substack{j\in\mathbb{N}_{\text{fin}}^{\Xi};\\ (m/(n/p))\mid j}} \operatorname{coeff}_j \tau \cdot \underbrace{\Xi^{j/(m/(n/p))}}_{=\prod_{\xi\in\Xi}\xi^{(j/(m/(n/p)))\xi}} = \sum_{\substack{j\in\mathbb{N}_{\text{fin}}^{\Xi};\\ (m/(n/p))\mid j}} \operatorname{coeff}_j \tau \cdot \prod_{\xi\in\Xi} \xi^{(j/(m/(n/p)))_\xi},$$

it must therefore be

$$\begin{aligned} b_{n/p}(\Xi^p) &= \sum_{\substack{j\in\mathbb{N}_{\text{fin}}^{\Xi};\\ (m/(n/p))\mid j}} \operatorname{coeff}_j \tau \cdot \prod_{\xi\in\Xi} (\xi^p)^{(j/(m/(n/p)))_\xi} = \sum_{\substack{j\in\mathbb{N}_{\text{fin}}^{\Xi};\\ (m/(n/p))\mid j}} \operatorname{coeff}_j \tau \cdot \prod_{\xi\in\Xi} \underbrace{(\xi^p)^{j_\xi n/(mp)}}_{=\xi^{p\cdot j_\xi n/(mp)}=\xi^{j_\xi n/m}} \\ &\qquad \left(\text{since } (j/(m/(n/p)))_\xi = \frac{j_\xi}{(m/n)/p} = j_\xi n/(mp)\right) \\ &= \sum_{\substack{j\in\mathbb{N}_{\text{fin}}^{\Xi};\\ (m/(n/p))\mid j}} \operatorname{coeff}_j \tau \cdot \prod_{\xi\in\Xi} \xi^{j_\xi n/m} = \sum_{\substack{j\in\mathbb{N}_{\text{fin}}^{\Xi};\\ (pm/n)\mid j}} \operatorname{coeff}_j \tau \cdot \prod_{\xi\in\Xi} \xi^{j_\xi n/m} \end{aligned} \tag{6}$$

(since $m/(n/p) = pm/n$). Now, let us prove that

$$\text{every } j \in \mathbb{N}_{\text{fin}}^{\Xi} \text{ which satisfies } (m/n) \mid j \text{ and } (pm/n) \nmid j \text{ must satisfy } \operatorname{coeff}_j \tau \equiv 0 \bmod p^{v_p(n)}\mathbb{Z}[\Xi]. \tag{7}$$

In fact, let $j \in \mathbb{N}_{\text{fin}}^{\Xi}$ be such that $(m/n) \mid j$ and $(pm/n) \nmid j$. We have to prove that $\operatorname{coeff}_j \tau \equiv 0 \bmod p^{v_p(n)}\mathbb{Z}[\Xi]$. Assume, for the sake of contradiction, that the opposite holds, i. e. that $\operatorname{coeff}_j \tau \not\equiv 0 \bmod p^{v_p(n)}\mathbb{Z}[\Xi]$. Then, $p^{v_p(n)} \nmid \operatorname{coeff}_j \tau$, so that $v_p(\operatorname{coeff}_j \tau) < v_p(n)$. Hence, $v_p(\operatorname{coeff}_j \tau) \leq v_p(n) - 1$ (since $v_p(\operatorname{coeff}_j \tau)$ and $v_p(n)$ are integers). But for every $\eta \in \Xi$, the relation (5) yields $m \mid \operatorname{coeff}_j \tau \cdot j_\eta$ and thus

$$v_p(m) \leq v_p(\operatorname{coeff}_j \tau \cdot j_\eta) = \underbrace{v_p(\operatorname{coeff}_j \tau)}_{\leq v_p(n)-1} + v_p(j_\eta) \leq (v_p(n) - 1) + v_p(j_\eta),$$

[6]Here, $w_n((x_k)_{k\in N})$ means $w_n\left((x_k)_{k\in\mathbb{N}_{|n}}\right)$ (because $\mathbb{N}_{|n}$ is a subset of N, since $n \in N$ and since n is a nest).

so that

$$v_p(j_\eta) \geq \underbrace{v_p(m)}_{\substack{=v_p((m/n)\cdot n)\\ =v_p(m/n)+v_p(n)}} - (v_p(n)-1) = v_p(m/n)+1,$$

and thus $p^{v_p(m/n)+1} \mid j_\eta$. On the other hand, $m/n \mid j_\eta$ (since $m/n \mid j$). Thus, $\operatorname{lcm}\left(p^{v_p(m/n)+1}, m/n\right) \mid j_\eta$. But $\operatorname{lcm}\left(p^{v_p(m/n)+1}, m/n\right) = pm/n$ (in fact, $\gcd\left(p^{v_p(m/n)+1}, m/n\right) = p^{v_p(m/n)}$ [7], and thus the formula $\operatorname{lcm}(a,b) = \dfrac{ab}{\gcd(a,b)}$ (which holds for any two positive integers a and b) yields $\operatorname{lcm}\left(p^{v_p(m/n)+1}, m/n\right) = \dfrac{p^{v_p(m/n)+1}\cdot m/n}{p^{v_p(m/n)}} = pm/n$). Hence, $(pm/n) \mid j_\eta$. Since this holds for any $\eta \in \Xi$, we have thus shown that $(pm/n) \mid j$, contradicting our assumption that $(pm/n) \nmid j$. This contradiction shows that our assumption that $\operatorname{coeff}_j \tau \not\equiv 0 \bmod p^{v_p(n)}\mathbb{Z}[\Xi]$ was wrong. Thus, (7) is proven.

Now, every $n \in N$ and every $p \in \operatorname{PF} n$ satisfy

$$\begin{aligned}
b_n &= \sum_{\substack{j\in\mathbb{N}_{\text{fin}}^{\Xi};\\ (m/n)\mid j}} \operatorname{coeff}_j \tau \cdot \Xi^{j/(m/n)} = \sum_{\substack{j\in\mathbb{N}_{\text{fin}}^{\Xi};\\ (m/n)\mid j;\\ (pm/n)\mid j}} \operatorname{coeff}_j \tau \cdot \Xi^{j/(m/n)} + \sum_{\substack{j\in\mathbb{N}_{\text{fin}}^{\Xi};\\ (m/n)\mid j;\\ (pm/n)\nmid j}} \underbrace{\operatorname{coeff}_j \tau}_{\substack{\equiv 0 \bmod p^{v_p(n)}\mathbb{Z}[\Xi]\\ \text{(by (7))}}} \cdot \Xi^{j/(m/n)} \\
&\equiv \sum_{\substack{j\in\mathbb{N}_{\text{fin}}^{\Xi};\\ (m/n)\mid j;\\ (pm/n)\mid j}} \operatorname{coeff}_j \tau \cdot \Xi^{j/(m/n)} + \underbrace{\sum_{\substack{j\in\mathbb{N}_{\text{fin}}^{\Xi};\\ (m/n)\mid j;\\ (pm/n)\nmid j}} 0 \cdot \Xi^{j/(m/n)}}_{=0} = \sum_{\substack{j\in\mathbb{N}_{\text{fin}}^{\Xi};\\ (m/n)\mid j;\\ (pm/n)\mid j}} \operatorname{coeff}_j \tau \cdot \Xi^{j/(m/n)} \\
&= \sum_{\substack{j\in\mathbb{N}_{\text{fin}}^{\Xi};\\ (pm/n)\mid j}} \operatorname{coeff}_j \tau \cdot \underbrace{\Xi^{j/(m/n)}}_{=\prod_{\xi\in\Xi}\xi^{(j/(m/n))_\xi}} \\
&\qquad \left(\begin{array}{c} \text{since for every } j \in \mathbb{N}_{\text{fin}}^{\Xi}, \text{ the conditions } ((m/n) \mid j \text{ and } (pm/n) \mid j) \text{ are} \\ \text{equivalent, because if } (pm/n) \mid j, \text{ then } (m/n) \mid j \end{array} \right) \\
&= \sum_{\substack{j\in\mathbb{N}_{\text{fin}}^{\Xi};\\ (pm/n)\mid j}} \operatorname{coeff}_j \tau \cdot \prod_{\xi\in\Xi} \xi^{(j/(m/n))_\xi} \\
&= \sum_{\substack{j\in\mathbb{N}_{\text{fin}}^{\Xi};\\ (pm/n)\mid j}} \operatorname{coeff}_j \tau \cdot \prod_{\xi\in\Xi} \xi^{j_\xi n/m} \qquad \left(\text{since } (j/(m/n))_\xi = \frac{j_\xi}{m/n} = j_\xi n/m\right) \\
&= b_{n/p}\left(\Xi^p\right) \bmod p^{v_p(n)}\mathbb{Z}[\Xi] \qquad \text{(by (6))}.
\end{aligned}$$

Hence, we have shown that every $n \in N$ and every $p \in \operatorname{PF} n$ satisfies $b_{n/p}\left(\Xi^p\right) \equiv b_n \bmod p^{v_p(n)}\mathbb{Z}[\Xi]$. Thus, Assertion $\mathcal{C}_\Xi$ of Theorem 2 holds for our family $(b_n)_{n\in N} \in (\mathbb{Z}[\Xi])^N$. Consequently, Assertion $\mathcal{D}_\Xi$ of Theorem 2 also holds for this family (since

[7] In fact, the number $\gcd\left(p^{v_p(m/n)+1}, m/n\right)$ must be a power of p (since it is a divisor of $p^{v_p(m/n)+1}$, and p is a prime) and a divisor of m/n, so it must be a power of p which divides m/n, and thus it must be p^κ for some integer κ satisfying $0 \leq \kappa \leq v_p(m/n)$. Thus, $\gcd\left(p^{v_p(m/n)+1}, m/n\right) = p^\kappa \mid p^{v_p(m/n)}$ (since $\kappa \leq v_p(m/n)$). On the other hand, $p^{v_p(m/n)} \mid \gcd\left(p^{v_p(m/n)+1}, m/n\right)$ (since $p^{v_p(m/n)}$ is a common divisor of $p^{v_p(m/n)+1}$ and m/n). Hence, $\gcd\left(p^{v_p(m/n)+1}, m/n\right) = p^{v_p(m/n)}$, qed.

Theorem 2 states that assertions $\mathcal{C}_\Xi$ and $\mathcal{D}_\Xi$ are equivalent). In other words, there exists a family $(x_n)_{n\in N} \in (\mathbb{Z}[\Xi])^N$ of elements of $\mathbb{Z}[\Xi]$ such that

$$\left(b_n = w_n\left((x_k)_{k\in N}\right) \text{ for every } n \in N\right).$$

Applying this to $n = m$, we obtain $b_m = w_m\left((x_k)_{k\in N}\right) = w_m\left((x_k)_{k\in \mathbb{N}_{|m}}\right)$. Renaming the family $(x_k)_{k\in \mathbb{N}_{|m}}$ as $(\tau_d)_{d\in \mathbb{N}_{|m}}$, we can rewrite this as $b_m = w_m\left((\tau_d)_{d\in \mathbb{N}_{|m}}\right)$. Since

$$\begin{aligned} b_m &= \sum_{\substack{j\in \mathbb{N}_{\text{fin}}^{\Xi}; \\ (m/m)|j}} \operatorname{coeff}_j \tau \cdot \underbrace{\Xi^{j/(m/m)}}_{=\Xi^{j/1}=\Xi^j} = \sum_{\substack{j\in \mathbb{N}_{\text{fin}}^{\Xi}; \\ (m/m)|j}} \operatorname{coeff}_j \tau \cdot \Xi^j = \sum_{j\in \mathbb{N}_{\text{fin}}^{\Xi}} \operatorname{coeff}_j \tau \cdot \Xi^j \\ &\qquad \left(\text{since every } j \in \mathbb{N}_{\text{fin}}^{\Xi} \text{ satisfies } (m/m) \mid j, \text{ because } m/m = 1\right) \\ &= \tau \qquad \text{(by (2))}, \end{aligned}$$

this rewrites as $\tau = w_m\left((\tau_d)_{d\in \mathbb{N}_{|m}}\right)$. Thus, Assertion $\mathcal{A}$ holds. Hence, we have derived Assertion $\mathcal{A}$ from Assertion $\mathcal{B}$. This proves the implication $\mathcal{B} \Longrightarrow \mathcal{A}$.

Altogether we have now proven the implications $\mathcal{A} \Longrightarrow \mathcal{B}$ and $\mathcal{B} \Longrightarrow \mathcal{A}$. We can thus conclude that the assertions $\mathcal{A}$ and $\mathcal{B}$ are equivalent. This proves Theorem 1.

We notice a trivial corollary from Theorem 1:

Corollary 3. Let $\tau \in \mathbb{Z}$ be an integer. Let $m \in \mathbb{N}$. Then, there exists a family $(\tau_d)_{d\in \mathbb{N}_{|m}} \in \mathbb{Z}^{\mathbb{N}_{|m}}$ of integers such that $\tau = w_m\left((\tau_d)_{d\in \mathbb{N}_{|m}}\right)$.

Proof of Corollary 3. Let Ξ be the empty family. Then, $\mathbb{Z}[\Xi] = \mathbb{Z}$ (in fact, $\mathbb{Z}[\Xi]$ is the ring of all polynomials in the indeterminates Ξ over $\mathbb{Z}$, but Ξ is the empty family, and polynomials in an empty family of indeterminates over $\mathbb{Z}$ are the same as integers). Clearly, our "polynomial" $\tau \in \mathbb{Z}[\Xi]$ satisfies Assertion $\mathcal{B}$ of Theorem 1 (in fact, Ξ is the empty family, so that there exists no $\xi \in \Xi$, and thus Assertion $\mathcal{B}$ of Theorem 1 is vacuously true). Hence, it also satisfies Assertion $\mathcal{A}$ of Theorem 1 (because Theorem 1 states that assertions $\mathcal{A}$ and $\mathcal{B}$ are equivalent). In other words, there exists a family $(\tau_d)_{d\in \mathbb{N}_{|m}} \in (\mathbb{Z}[\Xi])^{\mathbb{N}_{|m}}$ such that $\tau = w_m\left((\tau_d)_{d\in \mathbb{N}_{|m}}\right)$. Since $\mathbb{Z}[\Xi] = \mathbb{Z}$, this yields the assertion of Corollary 3. Thus, Corollary 3 is proven.

References

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

[2] Darij Grinberg, *Witt#2: Polynomials that can be written as w_n.* `http://www.cip.ifi.lmu.de/~grinberg/algebra/witt2.pdf`

[3] Darij Grinberg, *Witt#3: Ghost component computations.* `http://www.cip.ifi.lmu.de/~grinberg/algebra/witt3.pdf`

[4] Darij Grinberg, *Witt#5: Around the integrality criterion 9.93.* `http://www.cip.ifi.lmu.de/~grinberg/algebra/witt5.pdf`