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 $\Xi$ be a family of symbols. We consider the polynomial ring $\mathbb{Q}[\Xi]$ (this is the polynomial ring over $\mathbb{Q}$ in the indeterminates $\Xi$; in other words, we use the symbols from $\Xi$ as variables for the polynomials) and its subring $\mathbb{Z}[\Xi]$ (this is the polynomial ring over $\mathbb{Z}$ in the indeterminates $\Xi$). For any $n \in \mathbb{N}$, let $\Xi^n$ mean the family of the $n$-th powers of all elements of our family $\Xi$ (considered as elements of $\mathbb{Z}[\Xi]$). 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.

Note that if $\Xi$ 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 $\mathbb{Z}[(X_n)_{n \in N}]$ (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, $\mathbb{Z}[X_{\mathbb{N}_+}]$ is the polynomial ring $\mathbb{Z}[X_1, X_2, X_3, ...]$ (since $\mathbb{N}_+ = \{1, 2, 3, ...\}$), and $\mathbb{Z}[X_{\{1,2,3,5,6,10\}}]$ 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, $\Xi$ can be $(X_0, X_1, X_2, ...)$, in which case $\mathbb{Z}[\Xi]$ means $\mathbb{Z}[X_0, X_1, X_2, ...]$. Or, $\Xi$ 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 $\Xi^n$ as $(\xi_i^n)_{i \in I}$. For instance, if $\Xi = (X_0, X_1, X_2, ...)$, then $\Xi^n = (X_0^n, X_1^n, X_2^n, ...)$.

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 $P\left((x_d)_{d\in\mathbb{N}}\right)$ the element of $A$ that we obtain if we substitute $x_d$ for $X_d$ for every $d \in \mathbb{N}$ 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 $P\left((x_d)_{d\in\mathbb{N}}\right) = 13^2 + 37 \cdot 666 - 666$.)

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

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

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

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

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

**Caution:** These polynomials $w_1, w_2, w_3, \ldots$ are referred to as $w_1, w_2, w_3, \ldots$ most of the time in [1] (beginning with Section 9). However, in Sections 5-8 of [1], Hazewinkel uses the notations $w_1, w_2, w_3, \ldots$ 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 $w_1, w_2, w_3, \ldots$ (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 $\text{PF} n$ the set of all prime divisors of $n$. By the unique factorization theorem, the set $\text{PF} n$ is finite and satisfies

$$n = \prod_{p \in \text{PF} n} p^{v_p(n)}.$$ 

Let us now formulate our main result:

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

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

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


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

2) Theorem 1 makes sense even in the case when $\Xi$ is the empty family (in this case, the Assertion $B$ is vacuously true (since no $\xi \in \Xi$ exists), and therefore Theorem 1 claims that in this case Assertion $A$ 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 $w_{pn}$ (the one that we have defined above, not the one called $w_{pn}$ in [2]) is

$$w_{pn} = \sum_{d \mid p^n} dX_{d}^{p^n/d} = \sum_{d \in \mathbb{N}_{p^n}} dX_{d}^{p^n/d}$$

$$= \sum_{k=0}^{n} p^k X_{p^k}^{p^n/p^k} \quad \text{(since $\mathbb{N}_{p^n} = \{p^0, p^1, \ldots, p^n\}$ (because $p$ is a prime))}$$

$$= \sum_{k=0}^{n} p^k X_{p^k}^{p^{n-k}} \quad \text{(since $p^n/p^k = p^{n-k}$)},$$

and therefore this polynomial $w_{pn}$ is equal to the polynomial denoted by $w_n$ in [2] 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 $w_{pn} = \sum_{k=0}^{n} p^k X_{p^k}^{p^{n-k}}$ becomes $w_{pn} = \sum_{k=0}^{n} p^k X_{k}^{p^{n-k}}$, 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 $\Xi = (X_0, X_1, X_2, \ldots)$, the Assertions $A$ and $B$ of our Theorem 1 are identical with the Assertions $A$ and $B$ 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 $\Xi$ is a family of symbols, then

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

(1)

for every $\xi \in \Xi$, every $P \in \mathbb{Z}[\Xi]$ 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 $A \implies B$: Assume that the Assertion $A$ holds. Then, there exists a family $(\tau_d)_{d \in \mathbb{N}_{m}} \in (\mathbb{Z}[\Xi])^{\mathbb{N}_{m}}$ such that $\tau = w_m \left( (\tau_d)_{d \in \mathbb{N}_{m}} \right)$. Hence,

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

\footnote{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

$$
\frac{\partial}{\partial \xi} \tau = \frac{\partial}{\partial \xi} \sum_{d|m} d^{m/d} \cdot \sum_{d|m} \frac{\partial}{\partial d} \tau_d^{m/d} = \sum_{d|m} d^{(m/d)} \tau_d^{m/d-1} \cdot \left( \frac{\partial}{\partial \tau_d} \right)
$$

(by \ref{eq:tau}, applied to $P = \tau_d$ and $g = m/d$)

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

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

**Proof of the implication $B \implies A$:** Let us assume that Assertion $B$ holds. Thus, we have $\frac{\partial}{\partial \xi} \tau \in m\mathbb{Z}[\Xi]$ for every $\xi \in \Xi$. If we rename $\xi$ as $\eta$ here, this rewrites as follows:

We have $\frac{\partial}{\partial \eta} \tau \in m\mathbb{Z}[\Xi]$ 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 $j_\xi$ the $\xi$-th member of the family $j$. Then, every family $j \in \mathbb{N}^\Xi$ satisfies $j = (j_\xi)_{\xi \in \Xi}$.

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

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

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

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

Clearly, $1j = (1j_\xi)_{\xi \in \Xi} = (j_\xi)_{\xi \in \Xi} = j$.

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

Now, according to (2), our polynomial $\tau$ satisfies $\tau = \sum_{j \in \mathbb{N}_n^\Xi} \text{coeff}_j \tau \cdot \Xi^j$. Thus, for
every $\eta \in \Xi$, we have

\[
\frac{\partial}{\partial \eta} \tau = \sum_{j \in \mathbb{N}^\Xi_{\text{fin}}} \text{coeff}_j \tau \cdot \Xi^j = \sum_{j \in \mathbb{N}^\Xi_{\text{fin}}} \text{coeff}_j \tau \cdot \frac{\partial}{\partial \eta} \Xi^j = \sum_{j \in \mathbb{N}^\Xi_{\text{fin}}} \text{coeff}_j \tau \cdot \frac{\partial}{\partial \eta} \left( \eta^j \prod_{\xi \in \Xi \setminus \{\eta\}} \xi^j \right)
\]

\[
= \sum_{j \in \mathbb{N}^\Xi_{\text{fin}}; \ j_\eta > 0} \text{coeff}_j \tau \cdot \eta^{j_\eta} \prod_{\xi \in \Xi \setminus \{\eta\}} \xi^j = \sum_{j \in \mathbb{N}^\Xi_{\text{fin}}; \ j_\eta > 0} \text{coeff}_j \tau \cdot \eta^{j_\eta - 1} \prod_{\xi \in \Xi \setminus \{\eta\}} \xi^j + \sum_{j \in \mathbb{N}^\Xi_{\text{fin}}; \ j_\eta = 0} \text{coeff}_j \tau \cdot \prod_{\xi \in \Xi \setminus \{\eta\}} \xi^j
\]

(3)

Now, define a map

\[
F : \{ j \in \mathbb{N}^\Xi_{\text{fin}} \mid j_\eta > 0 \} \to \mathbb{N}^\Xi_{\text{fin}} \quad \text{defined by}
\]

\[
F (j) = \left( \begin{cases} 
\jmath_\xi, & \text{if } \xi \neq \eta; \\
\jmath_\eta - 1, & \text{if } \xi = \eta
\end{cases} \right)_{\xi \in \Xi}
\]

for every $j \in \mathbb{N}^\Xi_{\text{fin}}$ 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 $\eta$-th member, which is reduced by 1). By the definition of $F$, every $j \in \mathbb{N}^\Xi_{\text{fin}}$ satisfying $j_\eta > 0$ is mapped to $F (j) = \left( \begin{cases} 
\jmath_\xi, & \text{if } \xi \neq \eta; \\
\jmath_\eta - 1, & \text{if } \xi = \eta
\end{cases} \right)_{\xi \in \Xi}$. Hence, for every $\xi \in \Xi$, we have $(F (j))_\xi = \begin{cases} 
\jmath_\xi, & \text{if } \xi \neq \eta; \\
\jmath_\eta - 1, & \text{if } \xi = \eta
\end{cases}$. In other words, $(F (j))_\xi = \jmath_\xi$ if
\[ \xi \neq \eta, \text{ and } (F(\eta))_\eta = j_\eta - 1 \text{ (since } \eta = \eta) \). Using these two equations, Equation 3 becomes

\[
\frac{\partial}{\partial \eta} \tau = \sum_{j \in \mathbb{N}^e_{\text{fin}}} \text{coeff}_{F^{-1}(F(\eta))} \tau \cdot j_\eta \prod_{\xi \in \Xi \setminus \{\eta\}} \eta^{j_\eta - 1} \prod_{\xi \in \Xi \setminus \{\eta\}} \xi^{j_\xi} = \prod_{\xi \in \Xi \setminus \{\eta\}} \xi^{F(\eta)}
\]

\[
= \sum_{j \in \mathbb{N}^e_{\text{fin}}} \text{coeff}_{F^{-1}(F(\eta))} \tau \cdot (j_\eta + 1) \prod_{\xi \in \Xi \setminus \{\eta\}} \xi^{j_\xi} \quad \text{(here we substituted } F(\eta) \text{ for } j \text{ in the sum, since the map } F \text{ is a bijection)}
\]

\[
= \sum_{j \in \mathbb{N}^e_{\text{fin}}} \text{coeff}_{F^{-1}(\eta)} \tau \cdot (j_\eta + 1) \xi^j.
\]

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

\[
\text{coeff}_{F^{-1}(\eta)} \tau \cdot (j_\eta + 1) \in m\mathbb{Z} \quad \text{for every } j \in \mathbb{N}^e_{\text{fin}}.
\]

Thus, every \( j \in \mathbb{N}^e_{\text{fin}} \) and every \( \eta \in \Xi \) satisfy

\[
\text{coeff}_j \tau \cdot j_\eta \in m\mathbb{Z} \quad \text{(5)}
\]

(since (4), applied to \( F(\eta) \) instead of \( j \), yields \( \text{coeff}_{F^{-1}(\eta)} \tau \cdot (F(\eta))_\eta + 1 \in m\mathbb{Z} \),

which simplifies to \( \text{coeff}_j \tau \cdot j_\eta \in m\mathbb{Z} \) because \( F^{-1}(F(\eta)) \) and because \( (F(\eta))_\eta + 1 = (j_\eta - 1) + 1 = j_\eta \).)

Now we recall the following result from [4]:

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

**Assertion \( C_\Xi \):** Every \( n \in N \) and every \( p \in PF n \) satisfies

\[ b_{n/p}(\Xi^p) \equiv b_n \mod p^{v_p(n)}\mathbb{Z}[\Xi]. \]

**Assertion \( D_\Xi \):** There exists a family \((x_n)_{n \in N} \in (\mathbb{Z}[\Xi])^N \) of elements of \( \mathbb{Z}[\Xi] \) such that

\[ (b_n = w_n((x_k)_{k \in N}) \text{ for every } n \in N). \]

\(^5\)We refer to [4] (Definition 5) for the definition of a nest. For our aims, it is only important to know that \( \mathbb{N}_{\text{fin}} \) is a nest.
This Theorem 2 is part of Theorem 13 in [4] (which claims that the assertions \( C_\Xi, D_\Xi, D'_\Xi, E_\Xi, E'_\Xi, F_\Xi, G_\Xi \) and \( H_\Xi \) are equivalent, where \( C_\Xi \) and \( D_\Xi \) are our assertions \( C_\Xi \) and \( D_\Xi \), while \( D'_\Xi, E_\Xi, E'_\Xi, F_\Xi, G_\Xi \) and \( H_\Xi \) 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 \( (b_n)_{n \in N} \in (\mathbb{Z} \left[ \Xi \right])^N \) defined by

\[
b_n = \sum_{j \in \mathbb{N}^\Xi_{\text{fin}}; (m/n)|j} \text{coeff}_j \tau \cdot \Xi^{j/(m/n)} \quad \text{for every } n \in N.
\]

Let \( n \in N \) and every \( p \in \text{PF}_n \). 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

\[
b_{n/p}(\Xi^p) = \sum_{j \in \mathbb{N}^\Xi_{\text{fin}}; (m/(n/p))|j} \text{coeff}_j \tau \cdot \Xi^{j/(m/(n/p))} = \sum_{\xi \in \Xi} \text{coeff}_j \tau \cdot \prod_{\xi \in \Xi} \xi^{(j/(m/(n/p)))\xi} \tag{6}
\]

it must therefore be

\[
b_{n/p}(\Xi^p) = \sum_{j \in \mathbb{N}^\Xi_{\text{fin}}; (m/(n/p))|j} \text{coeff}_j \tau \cdot \prod_{\xi \in \Xi} \xi^{j/(m/(n/p))} = \sum_{\xi \in \Xi} \text{coeff}_j \tau \cdot \prod_{\xi \in \Xi} \xi^{(j/(m/(n/p)))\xi} \tag{6}
\]

(since \( (j/(m/(n/p)))\xi = \frac{j \xi}{j m p} = (j \xi m p) \)).

(7)

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

\[
v_p(m) \leq v_p(\text{coeff}_j \tau \cdot j_\eta) = v_p(\text{coeff}_j \tau) + v_p(j_\eta) \leq (v_p(n) - 1) + v_p(j_\eta), \tag{6}
\]

Here, \( w_n((x_k)_{k \in N}) \) means \( w_n((x_k)_{k \in N}) \) (because \( \mathbb{N}_{n} \) is a subset of \( N \), since \( n \in N \) and since \( n \) is a nest).
so that
\[ v_p(j_\eta) \geq \frac{v_p(m)}{v_p((m/n)_n)} - (v_p(n) - 1) = v_p(m/n) + 1, \]
and thus \(p^{v_p(m/n)+1} | j_\eta\). On the other hand, \(m/n | j_\eta\) (since \(m/n | j\)). Thus, \(\text{lcm} (p^{v_p(m/n)+1}, m/n) | j_\eta\). But \(\text{lcm} (p^{v_p(m/n)+1}, m/n) = pm/n\) (in fact, \(\gcd (p^{v_p(m/n)+1}, m/n) = p^{v_p(m/n)}\)) and thus the formula \(\text{lcm} (a, b) = \frac{ab}{\gcd (a, b)}\) (which holds for any two positive integers \(a\) and \(b\)) yields \(\text{lcm} (p^{v_p(m/n)+1}, m/n) = \frac{p^{v_p(m/n)+1} \cdot m/n}{p^{v_p(m/n)}} = pm/n\).

Hence, \((pm/n) | j_\eta\). Since this holds for any \(\eta \in \Xi\), we have thus shown that \((pm/n) | j\), contradicting our assumption that \((pm/n) \not| j\). This contradiction shows that our assumption that \(\text{coeff}_j \tau \not\equiv 0 \mod p^{v_p(n)}Z[\Xi]\) was wrong. Thus, (7) is proven.

Now, every \(n \in N\) and every \(p \in \text{PF}_n\) satisfy
\[
b_n = \sum_{j \in \mathbb{N}_0^\Xi \cap (m/n)} \text{coeff}_j \tau \cdot \Xi^{j/(m/n)} = \sum_{j \in \mathbb{N}_0^\Xi \cap (m/n)} \text{coeff}_j \tau \cdot \Xi^{j/(m/n)} + \sum_{j \in \mathbb{N}_0^\Xi \cap (m/n) \setminus \Xi^{j/(m/n) \equiv 0 \mod p^{v_p(n)}Z[\Xi]}} \text{coeff}_j \tau \cdot \Xi^{j/(m/n)}
\]
\[
= \sum_{j \in \mathbb{N}_0^\Xi \cap (m/n) \setminus \Xi^{j/(m/n)}} \text{coeff}_j \tau \cdot \Xi^{j/(m/n)} = \prod_{\xi \in \Xi} \xi^{j/(m/n)}
\]
\[(\text{since for every } j \in \mathbb{N}_0^\Xi \cap (m/n), \text{the conditions } ((m/n) | j \text{ and } (pm/n) | j) \text{ are equivalent, because if } (pm/n) | j, \text{ then } (m/n) | j)\]
\[
= \sum_{j \in \mathbb{N}_0^\Xi \cap (m/n)} \text{coeff}_j \tau \cdot \prod_{\xi \in \Xi} \xi^{j/(m/n)}
\]
\[
= \sum_{j \in \mathbb{N}_0^\Xi \cap (m/n)} \text{coeff}_j \tau \cdot \prod_{\xi \in \Xi} \xi^{j \eta / m}
\]
\[(\text{since } j/(m/n) = j \xi / m = j \xi n / m)\]
\[
= b_{n/p}(\Xi^p) \mod p^{v_p(n)}Z[\Xi] \quad \text{(by (6))}.
\]
Hence, we have shown that every \(n \in N\) and every \(p \in \text{PF}_n\) satisfies \(b_{n/p}(\Xi^p) \equiv b_n \mod p^{v_p(n)}Z[\Xi]\). Thus, Assertion \(C_\Xi\) of Theorem 2 holds for our family \((b_n)_{n \in N} \in (Z[\Xi])^N\). Consequently, Assertion \(D_\Xi\) of Theorem 2 also holds for this family (since

\[\text{In fact, the number } \gcd (p^{v_p(m/n)+1}, m/n) \text{ must be a power of } p \text{ (since it is a divisor of } p^{v_p(m/n)+1}, \text{ and } p \text{ is a prime) and a divisor of } m/n, \text{ so it must be a power of } p \text{ which divides } m/n, \text{ and thus it must be } p^\kappa \text{ for some integer } \kappa \text{ satisfying } 0 \leq \kappa \leq v_p(m/n). \text{ Thus, } \gcd (p^{v_p(m/n)+1}, m/n) = p^\kappa \mid p^{v_p(m/n)} \text{ (since } \kappa \leq v_p(m/n)). \text{ On the other hand, } p^{v_p(m/n)} \mid \gcd (p^{v_p(m/n)+1}, m/n) \text{ (since } p^{v_p(m/n)} \text{ is a common divisor of } p^{v_p(m/n)+1} \text{ and } m/n). \text{ Hence, } \gcd (p^{v_p(m/n)+1}, m/n) = p^{v_p(m/n)}, \text{ qed.} \]
Theorem 2 states that assertions \( C_\Xi \) and \( D_\Xi \) are equivalent. In other words, there exists a family \( (x_n)_{n \in \mathbb{N}} \in (\mathbb{Z}[\Xi])^\mathbb{N} \) of elements of \( \mathbb{Z}[\Xi] \) such that

\[
(b_n = w_n ((x_k)_{k \in \mathbb{N}}) \text{ for every } n \in \mathbb{N}).
\]

Applying this to \( n = m \), we obtain

\[
b_m = w_m ((x_k)_{k \in \mathbb{N}}) = w_m ((x_k)_{k \in \mathbb{N} \setminus \{m\}}).
\]

Renaming the family \( (x_k)_{k \in \mathbb{N} \setminus \{m\}} \) as \( (\tau_d)_{d \in \mathbb{N} \setminus \{m\}} \), we can rewrite this as

\[
b_m = w_m ((\tau_d)_{d \in \mathbb{N} \setminus \{m\}}).
\]

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

Altogether we have now proven the implications \( \mathcal{A} \implies \mathcal{B} \) and \( \mathcal{B} \implies \mathcal{A} \). 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 \( (\tau_d)_{d \in \mathbb{N} \setminus \{m\}} \in \mathbb{Z}^{|\mathbb{N} \setminus \{m\}|} \) of integers such that \( \tau = w_m ((\tau_d)_{d \in \mathbb{N} \setminus \{m\}}) \).

**Proof of Corollary 3.** Let \( \Xi \) be the empty family. Then, \( \mathbb{Z}[\Xi] = \mathbb{Z} \) (in fact, \( \mathbb{Z}[\Xi] \) is the ring of all polynomials in the indeterminates \( \Xi \) over \( \mathbb{Z} \), but \( \Xi \) 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, \( \Xi \) 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 \( (\tau_d)_{d \in \mathbb{N} \setminus \{m\}} \in (\mathbb{Z}[\Xi])^{|\mathbb{N} \setminus \{m\}|} \) such that \( \tau = w_m ((\tau_d)_{d \in \mathbb{N} \setminus \{m\}}) \). Since \( \mathbb{Z}[\Xi] = \mathbb{Z} \), this yields the assertion of Corollary 3. Thus, Corollary 3 is proven.

**References**

[2] Darij Grinberg, *Witt#2: Polynomials that can be written as \( w_n \).*

http://www.cip.ifi.lmu.de/~grinberg/algebra/witt2.pdf


http://www.cip.ifi.lmu.de/~grinberg/algebra/witt5.pdf