Witt vectors. Part 1

Michiel Hazewinkel
Sidenotes by Darij Grinberg

Witt#5b: Some divisibilities for big Witt polynomials

[not completed, not proofread]

In this note, we are going to verify a few properties of big Witt polynomials. First, the relevant definitions:

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. If m and n are two integers, then we write $m \perp n$ if and only if m is coprime to n. If m is an integer and S is a set, then we write $m \perp S$ if and only if ($m \perp n$ for every $n \in S$).

Definition 5. A *nest* means a nonempty subset N of $\mathbb{N}_+$ such that for every element $d \in N$, every divisor of d lies in N.

Here are some examples of nests: For instance, $\mathbb{N}_+$ itself is a nest. For every prime p, the set $\{1, p, p^2, p^3, ...\}$ is a nest; we denote this nest by $p^{\mathbb{N}}$. For any integer m, the set $\{n \in \mathbb{N}_+ \mid n \perp m\}$ is a nest; we denote this nest by $\mathbb{N}_{\perp m}$. For any positive integer m, the set $\{n \in \mathbb{N}_+ \mid n \leq m\}$ is a nest; we denote this nest by $\mathbb{N}_{\leq m}$. For any integer m, the set $\{n \in \mathbb{N}_+ \mid (n \mid m)\}$ is

[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 $P(\Xi^n) = (X_0^n + X_1^n)^2 - 2X_3^n + 1$.

a nest; we denote this nest by $\mathbb{N}_{|m}$. Another example of a nest is the set $\{1, 2, 3, 5, 6, 10\}$.

Clearly, every nest N contains the element 1 [4].

Definition 6. If N is a set[5], 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 we denote by $P\left((x_d)_{d \in N}\right)$ 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 $P = X_1^2 + X_2 X_5 - X_5$, and if $x_1 = 13$, $x_2 = 37$ and $x_5 = 666$, then $P\left((x_d)_{d \in N}\right) = 13^2 + 37 \cdot 666 - 666$.)

We notice that whenever N and M are two sets satisfying $N \subseteq M$, then we canonically identify $\mathbb{Z}[X_N]$ with a subring of $\mathbb{Z}[X_M]$. In particular, when $P \in \mathbb{Z}[X_N]$ is a polynomial, and A is a commutative ring with unity, and $(x_m)_{m \in M} \in A^M$ is a family of elements of A, then $P\left((x_m)_{m \in M}\right)$ means $P\left((x_m)_{m \in N}\right)$. (Thus, the elements x_m for $m \in M \setminus N$ are simply ignored when evaluating $P\left((x_m)_{m \in M}\right)$.) In particular, if $N \subseteq \mathbb{N}_+$, and $(x_1, x_2, x_3, ...) \in A^{\mathbb{N}_+}$, then $P(x_1, x_2, x_3, ...)$ means $P\left((x_m)_{m \in N}\right)$.

Definition 7. For any $n \in \mathbb{N}_+$, we define a polynomial $w_n \in \mathbb{Z}\left[X_{\mathbb{N}_{|n}}\right]$ by

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

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

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

As explained in Definition 6, if N is a set containing $\mathbb{N}_{|n}$, if A is a commutative ring with unity, and $(x_k)_{k \in N} \in A^N$ is a family of elements of A, then $w_n\left((x_k)_{k \in N}\right)$ means $w_n\left((x_k)_{k \in \mathbb{N}_{|n}}\right)$; in other words,

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

[4] In fact, there exists some $n \in N$ (since N is a nest and thus nonempty), and thus $1 \in N$ (since 1 is a divisor of n, and every divisor of n must lie in N because N is a nest).

[5] We will use this notation only for the case of N being a nest. However, it equally makes sense for any arbitrary set N.

The polynomials w_1, w_2, w_3, ... are called the *big Witt polynomials* or, simply, the *Witt polynomials*.[6]

Definition 8. 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 9. 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 $n = \prod_{p \in \operatorname{PF} n} p^{v_p(n)}$.

Definition 10. An Abelian group A is called *torsionfree* if and only if every element $a \in A$ and every $n \in \mathbb{N}_+$ such that $na = 0$ satisfy $a = 0$.

A ring R is called *torsionfree* if and only if the Abelian group $(R, +)$ is torsionfree.

Definition 11. Let μ denote the Möbius function $\mu : \mathbb{N}_+ \to \mathbb{Z}$ defined by

$$\mu(n) = \begin{cases} (-1)^{|\operatorname{PF} n|}, & \text{if } (v_p(n) \leq 1 \text{ for every } p \in \operatorname{PF} n) \\ 0, & \text{otherwise} \end{cases} \qquad \text{for every } n \in \mathbb{N}_+.$$

Let ϕ denote the Euler phi function $\phi : \mathbb{N}_+ \to \mathbb{Z}$ defined by

$$\phi(n) = |\{m \in \{1, 2, ..., n\} \mid m \perp n\}| \qquad \text{for every } n \in \mathbb{N}_+.$$

We recall one of the results of [4]:

Theorem 1. Let N be a nest. Let A be a torsionfree Abelian group (written additively). For every $n \in N$, let $\varphi_n : A \to A$ be an endomorphism of the group A such that

$$(\varphi_1 = \mathrm{id}) \qquad \text{and} \tag{1}$$

$$(\varphi_n \circ \varphi_m = \varphi_{nm} \text{ for every } n \in N \text{ and every } m \in N \text{ satisfying } nm \in N). \tag{2}$$

Let $(b_n)_{n \in N} \in A^N$ be a family of elements of A. Then, the following assertions $\mathcal{C}$, $\mathcal{E}$, $\mathcal{E}'$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ are equivalent:

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

$$\varphi_p(b_{n/p}) \equiv b_n \bmod p^{v_p(n)} A. \tag{3}$$

[6] *Caution:* These polynomials 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).

Assertion $\mathcal{E}$: There exists a family $(y_n)_{n\in N} \in A^N$ of elements of A such that

$$\left(b_n = \sum_{d|n} d\varphi_{n/d}\left(y_d\right) \text{ for every } n \in N \right).$$

Assertion $\mathcal{E}'$: There exists *one and only one* family $(y_n)_{n\in N} \in A^N$ of elements of A such that

$$\left(b_n = \sum_{d|n} d\varphi_{n/d}\left(y_d\right) \text{ for every } n \in N \right).$$

Assertion $\mathcal{F}$: Every $n \in N$ satisfies

$$\sum_{d|n} \mu(d)\, \varphi_d\left(b_{n/d}\right) \in nA.$$

Assertion $\mathcal{G}$: Every $n \in N$ satisfies

$$\sum_{d|n} \phi(d)\, \varphi_d\left(b_{n/d}\right) \in nA.$$

Assertion $\mathcal{H}$: Every $n \in N$ satisfies

$$\sum_{i=1}^{n} \varphi_{n/\gcd(i,n)}\left(b_{\gcd(i,n)}\right) \in nA.$$

We won't prove this theorem here, because it is identical with Theorem 7 in [4], and thus we refer to [4] for its proof.

Our main result is the following:

Theorem 2. Consider the polynomial ring $\mathbb{Z}\left[X_{\mathbb{N}_+}\right] = \mathbb{Z}\left[X_1, X_2, X_3, ...\right]$. Let A be the Abelian group $\left(\mathbb{Z}\left[X_{\mathbb{N}_+}\right]\right)^{\mathbb{N}_+}$ (this is the Abelian group of all sequences of elements of $\mathbb{Z}\left[X_{\mathbb{N}_+}\right]$, with componentwise addition and zero $(0)_{n\in\mathbb{N}_+}$).

For every $n \in \mathbb{N}_+$, define an endomorphism $\varphi_n : A \to A$ of the group A by

$$\varphi_n\left(\left(x_k\right)_{k\in\mathbb{N}_+}\right) = \left(x_{nk}\right)_{k\in\mathbb{N}_+} \qquad \text{for every } \left(x_k\right)_{k\in\mathbb{N}_+} \in A. \tag{4}$$

We define a family $(b_n)_{n\in\mathbb{N}_+} \in A^{\mathbb{N}_+}$ of elements of A by

$$b_n = \left(w_k^n\right)_{k\in\mathbb{N}_+} \qquad \text{for every } n \in \mathbb{N}_+.$$

(a) The group A is torsionfree, and the endomorphisms φ_n satisfy (1) and (2).

(b) The family $(b_n)_{n\in\mathbb{N}_+}$ satisfies the Assertions $\mathcal{C}$, $\mathcal{E}$, $\mathcal{E}'$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ of Theorem 1 for $N = \mathbb{N}_+$.

Before we come to the proof of this fact, we recall some lemmata:

Lemma 3. Let B be a commutative ring with unity, and $p \in \mathbb{N}$ be a nonnegative integer[7]. Let $k \in \mathbb{N}$ and $\ell \in \mathbb{N}$ be such that $k > 0$. Let $u \in B$ and $v \in B$. If $u \equiv v \bmod p^k B$, then $u^{p^\ell} \equiv v^{p^\ell} \bmod p^{k+\ell} B$.

This is Lemma 3 in [3] (with slightly different notations: our B, u and v were called A, a and b in [3]). This lemma yields:

Lemma 4. Let B be a commutative ring with unity. Let $n \in \mathbb{N}_+$ and $p \in \operatorname{PF} n$. Let $u \in B$ and $v \in B$. If $u \equiv v \bmod pB$, then $u^{n/p} \equiv v^{n/p} \bmod p^{v_p(n)} B$.

Proof of Lemma 4. Since $p \in \operatorname{PF} n$, we have $p \mid n$ and thus $v_p(n) \geq 1$. In other words, $v_p(n) - 1 \geq 0$.

Set $k = 1$ and $\ell = v_p(n) - 1$. Then, $k + \ell = 1 + (v_p(n) - 1) = v_p(n)$. Note that $\ell \in \mathbb{N}$, since $\ell = v_p(n) - 1 \geq 0$. Also, note that $u \equiv v \bmod p^k B$ (this follows from $u \equiv v \bmod pB$, because $k = 1$).

Since $p^{v_p(n)} \mid n$, there exists some $\gamma \in \mathbb{N}_+$ such that $n = \gamma p^{v_p(n)}$. Consider this γ. Since $n = \gamma p^{v_p(n)}$, we have $n/p = \gamma p^{v_p(n)}/p = \gamma p^{v_p(n)-1}$. Now, applying Lemma 3, we obtain $u^{p^\ell} \equiv v^{p^\ell} \bmod p^{k+\ell} B$. Since $k+\ell = v_p(n)$, this rewrites as $u^{p^\ell} \equiv v^{p^\ell} \bmod p^{v_p(n)} B$. But $n/p = \gamma p^{v_p(n)-1} = \gamma p^\ell$ (since $v_p(n) - 1 = \ell$), so that $u^{n/p} = u^{\gamma p^\ell}$ and $v^{n/p} = v^{\gamma p^\ell}$. Therefore,

$$\begin{aligned} u^{n/p} = u^{\gamma p^\ell} &= \left(u^{p^\ell}\right)^\gamma \equiv \left(v^{p^\ell}\right)^\gamma \qquad \left(\text{since } u^{p^\ell} \equiv v^{p^\ell} \bmod p^{v_p(n)} B\right) \\ &= v^{\gamma p^\ell} = v^{n/p} \bmod p^{v_p(n)} B, \end{aligned}$$

and Lemma 4 is proven.

Another easy lemma:

Lemma 5. Let $k \in \mathbb{N}_+$ and $p \in \mathbb{P}$. Then, $w_{pk} \equiv w_k^p \bmod p\mathbb{Z}\left[X_{\mathbb{N}_+}\right]$. (Remember that $\mathbb{Z}\left[X_{\mathbb{N}_+}\right] = \mathbb{Z}\left[X_1, X_2, X_3, ...\right]$).

Proof of Lemma 5. We notice that

$$\sum_{\substack{d \mid pk; \\ d \nmid k}} d X_d^{pk/d} \equiv 0 \bmod p\mathbb{Z}\left[X_{\mathbb{N}_+}\right], \tag{5}$$

since every divisor d of pk which satisfies $d \nmid k$ must satisfy $dX_d^{pk/d} \equiv 0 \bmod p\mathbb{Z}\left[X_{\mathbb{N}_+}\right]$ [8]. Now, comparing

$$w_{pk} = \sum_{d \mid pk} dX_d^{pk/d} = \sum_{\substack{d \mid pk; \\ d \mid k}} dX_d^{pk/d} + \underbrace{\sum_{\substack{d \mid pk; \\ d \nmid k}} dX_d^{pk/d}}_{\substack{\equiv 0 \bmod p\mathbb{Z}\left[X_{\mathbb{N}_+}\right] \\ \text{(by (5))}}} \equiv \underbrace{\sum_{\substack{d \mid pk; \\ d \mid k}} dX_d^{pk/d}}_{= \sum_{d \mid k}} = \sum_{d \mid k} dX_d^{pk/d} \bmod p\mathbb{Z}\left[X_{\mathbb{N}_+}\right]$$

[7] Though we call it p, we do not require it to be a prime in this lemma!

[8] In fact, if d is a divisor of pk which satisfies $d \nmid k$, then d cannot be coprime to p (since otherwise, $d \mid pk$ would yield $d \mid k$, contradicting to $d \nmid k$), and thus d must be divisible by p (since p is a prime), so that $d \equiv 0 \bmod p\mathbb{Z}\left[X_{\mathbb{N}_+}\right]$ and thus $dX_d^{pk/d} \equiv 0 \bmod p\mathbb{Z}\left[X_{\mathbb{N}_+}\right]$.

with

$$w_k^p = \left(\sum_{d|k} d X_d^{k/d}\right)^p \qquad \left(\text{since } w_k = \sum_{d|k} d X_d^{k/d}\right)$$

$$\equiv \sum_{d|k} \left(d X_d^{k/d}\right)^p$$

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

$$= \sum_{d|k} \underbrace{d^p}_{\substack{\equiv d \bmod p\mathbb{Z}\left[X_{\mathbb{N}_+}\right] \\ (\text{since } d^p \equiv d \bmod p\mathbb{Z} \\ \text{by Fermat's Little Theorem})}} \underbrace{\left(X_d^{k/d}\right)^p}_{=X_d^{k/d\cdot p} = X_d^{pk/d}} \equiv \sum_{d|k} d X_d^{pk/d} \bmod p\mathbb{Z}\left[X_{\mathbb{N}_+}\right],$$

we obtain $w_{pk} \equiv w_k^p \bmod p\mathbb{Z}\left[X_{\mathbb{N}_+}\right]$, and thus Lemma 5 is proven.

A conclusion from Lemmata 4 and 5:

Lemma 6. Let $k \in \mathbb{N}_+$. Let $n \in \mathbb{N}_+$ and $p \in \operatorname{PF} n$. Then, $w_{pk}^{n/p} \equiv w_k^n \bmod p^{v_p(n)}\mathbb{Z}\left[X_{\mathbb{N}_+}\right]$. (Remember that $\mathbb{Z}\left[X_{\mathbb{N}_+}\right] = \mathbb{Z}\left[X_1, X_2, X_3, ...\right]$).

Proof of Lemma 6. Lemma 5 yields $w_{pk} \equiv w_k^p \bmod p\mathbb{Z}\left[X_{\mathbb{N}_+}\right]$ (since $p \in \mathbb{P}$ due to $p \in \operatorname{PF} n$). Lemma 4 (applied to $B = \mathbb{Z}\left[X_{\mathbb{N}_+}\right]$, $u = w_{pk}$ and $v = w_k^p$) now yields $w_{pk}^{n/p} \equiv \left(w_k^p\right)^{n/p} \bmod p^{v_p(n)}\mathbb{Z}\left[X_{\mathbb{N}_+}\right]$. Since $\left(w_k^p\right)^{n/p} = w_k^n$, this rewrites as $w_{pk}^{n/p} \equiv w_k^n \bmod p^{v_p(n)}\mathbb{Z}\left[X_{\mathbb{N}_+}\right]$, and thus Lemma 6 is proven.

Proof of Theorem 2. Let N be the nest $\mathbb{N}_+$. Then, $A = \left(\mathbb{Z}\left[X_{\mathbb{N}_+}\right]\right)^{\mathbb{N}_+} = \left(\mathbb{Z}\left[X_{\mathbb{N}_+}\right]\right)^N$, and the equation (4) rewrites as

$$\varphi_n\left((x_k)_{k\in N}\right) = (x_{nk})_{k\in N} \qquad \text{for every } (x_k)_{k\in N} \in A \tag{6}$$

(since $\mathbb{N}_+ = N$).

(a) Clearly, the group A is torsionfree (since $A = \left(\mathbb{Z}\left[X_{\mathbb{N}_+}\right]\right)^{\mathbb{N}_+}$, and since the group $\mathbb{Z}\left[X_{\mathbb{N}_+}\right]$ is torsionfree). Besides, every $(x_k)_{k\in N} \in A$ satisfies

$$\varphi_1\left((x_k)_{k\in N}\right) = (x_{1k})_{k\in N} \qquad \text{(by (6), applied to } n = 1)$$
$$= (x_k)_{k\in N},$$

and thus $\varphi_1 = \mathrm{id}$. Hence, (1) holds. Finally, for every $n \in N$ and $m \in N$, every $(x_k)_{k\in N} \in A$ satisfies

$$\left(\varphi_n \circ \varphi_m\right)\left((x_k)_{k\in N}\right) = \varphi_n\left(\varphi_m\left((x_k)_{k\in N}\right)\right) = \varphi_n\left((x_{mk})_{k\in N}\right)$$
$$\left(\text{since } \varphi_m\left((x_k)_{k\in N}\right) = (x_{mk})_{k\in N} \text{ by (6) (applied to } m \text{ instead of } n)\right)$$
$$= (x_{mnk})_{k\in N} \qquad \left(\text{by (6) (applied to } (x_{mk})_{k\in N} \text{ instead of } (x_k)_{k\in N}\right))$$
$$= (x_{nmk})_{k\in N} = \varphi_{nm}\left((x_k)_{k\in N}\right) \qquad \text{(by (6) (applied to } nm \text{ instead of } n)),$$

and thus $\varphi_n \circ \varphi_m = \varphi_{nm}$. Hence, (2) holds. This completes the proof of Theorem 2 **(a)**.

(b) Every $n \in N$ and every $p \in \operatorname{PF} n$ satisfies

$$\begin{aligned}
\varphi_p\left(b_{n/p}\right) &= \varphi_p\left(\left(w_k^{n/p}\right)_{k\in N}\right) && \left(\text{since } b_{n/p} \text{ is defined as } \left(w_k^{n/p}\right)_{k\in N}\right) \\
&= \left(w_{pk}^{n/p}\right)_{k\in N} && \left(\text{by (6) (applied to } p \text{ and } \left(w_k^{n/p}\right)_{k\in N} \text{ instead of } n \text{ and } \left(x_k\right)_{k\in N}\right)\right) \\
&\equiv \left(w_k^n\right)_{k\in N} && \left(\text{since Lemma 6 says that } w_{pk}^{n/p} \equiv w_k^n \bmod p^{v_p(n)}\mathbb{Z}\left[X_{\mathbb{N}_+}\right] \text{ for every } k \in \mathbb{N}_+\right) \\
&= b_n \bmod p^{v_p(n)} A.
\end{aligned}$$

Thus, Assertion $\mathcal{C}$ of Theorem 1 is true for our family $\left(b_n\right)_{n\in N}$. Since the Assertions $\mathcal{C}$, $\mathcal{E}$, $\mathcal{E}'$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ of Theorem 1 are equivalent (according to Theorem 1, which we can apply because of Theorem 2 **(a)**), this yields that the Assertions $\mathcal{E}$, $\mathcal{E}'$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ must be true as well. This proves Theorem 2 **(b)**.

Now that Theorem 2 is proven, let us explicitly write down what the assertions $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ of Theorem 1 mean for our family $\left(b_n\right)_{n\in N}$:

Theorem 7. Consider the polynomial ring $\mathbb{Z}\left[X_{\mathbb{N}_+}\right] = \mathbb{Z}\left[X_1, X_2, X_3, ...\right]$.

(a) Every $n \in \mathbb{N}_+$ satisfies

$$\sum_{d|n} \mu\left(d\right) w_{dk}^{n/d} \in n\mathbb{Z}\left[X_{\mathbb{N}_{|kn}}\right] \qquad \text{for every } k \in \mathbb{N}_+.$$

(b) Every $n \in \mathbb{N}_+$ satisfies

$$\sum_{d|n} \phi\left(d\right) w_{dk}^{n/d} \in n\mathbb{Z}\left[X_{\mathbb{N}_{|kn}}\right] \qquad \text{for every } k \in \mathbb{N}_+.$$

(c) Every $n \in \mathbb{N}_+$ satisfies

$$\sum_{i=1}^{n} w_{n/\gcd(i,n)\cdot k}^{\gcd(i,n)} \in n\mathbb{Z}\left[X_{\mathbb{N}_{|kn}}\right] \qquad \text{for every } k \in \mathbb{N}_+.$$

9

Proof of Theorem 7. Let us invoke Theorem 2. So let us define the nest $N = \mathbb{N}_+$, the Abelian group A, the endomorphisms $\varphi_n : A \to A$ and the family $\left(b_n\right)_{n\in\mathbb{N}_+} \in A^{\mathbb{N}_+}$ as in Theorem 2. Then, Theorem 2 **(b)** states that the family $\left(b_n\right)_{n\in N}$ satisfies the Assertions $\mathcal{C}$, $\mathcal{E}$, $\mathcal{E}'$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ of Theorem 1.

(a) Assertion $\mathcal{F}$ of Theorem 1 states that every $n \in N$ satisfies

$$\sum_{d|n} \mu\left(d\right) \varphi_d\left(b_{n/d}\right) \in nA.$$

[9] *Remark on notation:* Here and in the following, $\alpha/\beta\cdot\gamma$ means $(\alpha/\beta)\cdot\gamma$ and not $\alpha/(\beta\cdot\gamma)$.

Since this assertion is satisfied, we thus have $\sum_{d|n} \mu(d)\, \varphi_d(b_{n/d}) \in nA$ for every $n \in N$.

Since

$$\sum_{d|n} \mu(d)\, \varphi_d(b_{n/d}) = \sum_{d|n} \mu(d)\, \underbrace{\varphi_d\left(\left(w_k^{n/d}\right)_{k\in\mathbb{N}_+}\right)}_{=\left(w_{dk}^{n/d}\right)_{k\in\mathbb{N}_+} \text{ (by the definition of } \varphi_d)} \qquad \left(\text{since } b_{n/d} \text{ is defined as } \left(w_k^{n/d}\right)_{k\in\mathbb{N}_+}\right)$$

$$= \sum_{d|n} \mu(d) \left(w_{dk}^{n/d}\right)_{k\in\mathbb{N}_+} = \left(\sum_{d|n} \mu(d)\, w_{dk}^{n/d}\right)_{k\in\mathbb{N}_+}$$

(since addition in A is componentwise),

this becomes $\left(\sum_{d|n} \mu(d)\, w_{dk}^{n/d}\right)_{k\in\mathbb{N}_+} \in nA$. In other words, there exists a sequence $(u_k)_{k\in\mathbb{N}_+} \in A$ such that $\left(\sum_{d|n} \mu(d)\, w_{dk}^{n/d}\right)_{k\in\mathbb{N}_+} = n\,(u_k)_{k\in\mathbb{N}_+}$. Thus, $\left(\sum_{d|n} \mu(d)\, w_{dk}^{n/d}\right)_{k\in\mathbb{N}_+} = n\,(u_k)_{k\in\mathbb{N}_+} = (nu_k)_{k\in\mathbb{N}_+}$. Hence, for every $k \in \mathbb{N}_+$, we have $\sum_{d|n} \mu(d)\, w_{dk}^{n/d} = nu_k \in n\mathbb{Z}\left[X_{\mathbb{N}_+}\right]$. In other words, $\frac{1}{n}\sum_{d|n} \mu(d)\, w_{dk}^{n/d} \in \mathbb{Z}\left[X_{\mathbb{N}_+}\right]$.

On the other hand, $\frac{1}{n}\sum_{d|n} \mu(d)\, w_{dk}^{n/d} \in \mathbb{Q}\left[X_{\mathbb{N}_{|kn}}\right]$, since every $d \mid n$ satisfies $w_{dk} \in \mathbb{Q}\left[X_{\mathbb{N}_{|dk}}\right] \subseteq \mathbb{Q}\left[X_{\mathbb{N}_{|kn}}\right]$ (since $d \mid n$ yields $dk \mid nk = kn$ and thus $\mathbb{N}_{|dk} \subseteq \mathbb{N}_{|kn}$). Hence, $\frac{1}{n}\sum_{d|n} \mu(d)\, w_{dk}^{n/d} \in \mathbb{Q}\left[X_{\mathbb{N}_{|kn}}\right] \cap \mathbb{Z}\left[X_{\mathbb{N}_+}\right]$ (because $\frac{1}{n}\sum_{d|n} \mu(d)\, w_{dk}^{n/d} \in \mathbb{Q}\left[X_{\mathbb{N}_{|kn}}\right]$ and $\frac{1}{n}\sum_{d|n} \mu(d)\, w_{dk}^{n/d} \in \mathbb{Z}\left[X_{\mathbb{N}_+}\right]$).

Now, as was shown in the proof of Theorem 25 **(b)** in [4], we have

$$\mathbb{Q}[U] \cap \mathbb{Z}[V] = \mathbb{Z}[U]$$

whenever U and V are two sets of symbols such that $U \subseteq V$. Applying this to $U = X_{\mathbb{N}_{|kn}}$ and $V = X_{\mathbb{N}_+}$ (which satisfy $U \subseteq V$ since $X_{\mathbb{N}_{|kn}} \subseteq X_{\mathbb{N}_+}$, since $\mathbb{N}_{|kn} \subseteq \mathbb{N}_+$), we obtain

$$\mathbb{Q}\left[X_{\mathbb{N}_{|kn}}\right] \cap \mathbb{Z}\left[X_{\mathbb{N}_+}\right] = \mathbb{Z}\left[X_{\mathbb{N}_{|kn}}\right]. \tag{7}$$

Thus, $\frac{1}{n}\sum_{d|n} \mu(d)\, w_{dk}^{n/d} \in \mathbb{Q}\left[X_{\mathbb{N}_{|kn}}\right] \cap \mathbb{Z}\left[X_{\mathbb{N}_+}\right]$ becomes $\frac{1}{n}\sum_{d|n} \mu(d)\, w_{dk}^{n/d} \in \mathbb{Z}\left[X_{\mathbb{N}_{|kn}}\right]$. In other words, $\sum_{d|n} \mu(d)\, w_{dk}^{n/d} \in n\mathbb{Z}\left[X_{\mathbb{N}_{|kn}}\right]$. This proves Theorem 7 **(a)**.

(b) The proof of Theorem 7 **(b)** is the same as the proof of Theorem 7 **(a)** that we have just done; we just have to replace every μ by ϕ and use Assertion $\mathcal{G}$ instead of Assertion $\mathcal{F}$.

(c) Assertion $\mathcal{H}$ of Theorem 1 states that every $n \in N$ satisfies

$$\sum_{i=1}^{n} \varphi_{n/\gcd(i,n)}\left(b_{\gcd(i,n)}\right) \in nA.$$

Since this assertion is satisfied, we thus have $\sum_{i=1}^{n} \varphi_{n/\gcd(i,n)}\left(b_{\gcd(i,n)}\right) \in nA$ for every $n \in N$. Since

$$\begin{aligned}
\sum_{i=1}^{n} \varphi_{n/\gcd(i,n)}\left(b_{\gcd(i,n)}\right) &= \sum_{i=1}^{n} \underbrace{\varphi_{n/\gcd(i,n)}\left(\left(w_k^{\gcd(i,n)}\right)_{k\in\mathbb{N}_+}\right)}_{=\left(w^{\gcd(i,n)}_{n/\gcd(i,n)\cdot k}\right)_{k\in\mathbb{N}_+}} \\
&\qquad \left(\text{by the definition of } \varphi_{n/\gcd(i,n)}\right) \\
&\qquad \left(\text{since } b_{\gcd(i,n)} \text{ is defined as } \left(w_k^{\gcd(i,n)}\right)_{k\in\mathbb{N}_+}\right) \\
&= \sum_{i=1}^{n} \left(w^{\gcd(i,n)}_{n/\gcd(i,n)\cdot k}\right)_{k\in\mathbb{N}_+} = \left(\sum_{i=1}^{n} w^{\gcd(i,n)}_{n/\gcd(i,n)\cdot k}\right)_{k\in\mathbb{N}_+} \\
&\qquad \left(\text{since addition in } A \text{ is componentwise}\right),
\end{aligned}$$

this rewrites as $\left(\sum_{i=1}^{n} w^{\gcd(i,n)}_{n/\gcd(i,n)\cdot k}\right)_{k\in\mathbb{N}_+} \in nA$. In other words, there exists a sequence $(v_k)_{k\in\mathbb{N}_+} \in A$ such that $\left(\sum_{i=1}^{n} w^{\gcd(i,n)}_{n/\gcd(i,n)\cdot k}\right)_{k\in\mathbb{N}_+} = n\,(v_k)_{k\in\mathbb{N}_+}$. Thus, $\left(\sum_{i=1}^{n} w^{\gcd(i,n)}_{n/\gcd(i,n)\cdot k}\right)_{k\in\mathbb{N}_+} = n\,(v_k)_{k\in\mathbb{N}_+} = (nv_k)_{k\in\mathbb{N}_+}$. Hence, for every $k \in \mathbb{N}_+$, we have $\sum_{i=1}^{n} w^{\gcd(i,n)}_{n/\gcd(i,n)\cdot k} = nv_k \in n\mathbb{Z}\left[X_{\mathbb{N}_+}\right]$. In other words, $\frac{1}{n}\sum_{i=1}^{n} w^{\gcd(i,n)}_{n/\gcd(i,n)\cdot k} \in \mathbb{Z}\left[X_{\mathbb{N}_+}\right]$.

On the other hand, $\frac{1}{n}\sum_{i=1}^{n} w^{\gcd(i,n)}_{n/\gcd(i,n)\cdot k} \in \mathbb{Q}\left[X_{\mathbb{N}_{|kn}}\right]$, since every $i \in \{1,2,...,n\}$ satisfies $w_{n/\gcd(i,n)\cdot k} \in \mathbb{Q}\left[X_{\mathbb{N}_{|n/\gcd(i,n)\cdot k}}\right] \subseteq \mathbb{Q}\left[X_{\mathbb{N}_{|kn}}\right]$ (since $(n/\gcd(i,n)) \mid n$ yields $n/\gcd(i,n)\cdot k \mid nk = kn$ and thus $\mathbb{N}_{|n/\gcd(i,n)\cdot k} \subseteq \mathbb{N}_{|kn}$). Hence, $\frac{1}{n}\sum_{i=1}^{n} w^{\gcd(i,n)}_{n/\gcd(i,n)\cdot k} \in \mathbb{Q}\left[X_{\mathbb{N}_{|kn}}\right] \cap \mathbb{Z}\left[X_{\mathbb{N}_+}\right]$ (because $\frac{1}{n}\sum_{i=1}^{n} w^{\gcd(i,n)}_{n/\gcd(i,n)\cdot k} \in \mathbb{Q}\left[X_{\mathbb{N}_{|kn}}\right]$ and $\frac{1}{n}\sum_{i=1}^{n} w^{\gcd(i,n)}_{n/\gcd(i,n)\cdot k} \in \mathbb{Z}\left[X_{\mathbb{N}_+}\right]$). Due to (7), this becomes $\frac{1}{n}\sum_{i=1}^{n} w^{\gcd(i,n)}_{n/\gcd(i,n)\cdot k} \in \mathbb{Z}\left[X_{\mathbb{N}_{|kn}}\right]$. In other words, $\sum_{i=1}^{n} w^{\gcd(i,n)}_{n/\gcd(i,n)\cdot k} \in n\mathbb{Z}\left[X_{\mathbb{N}_{|kn}}\right]$. This proves Theorem 7 **(c)**.

Actually, Theorem 2 generalizes:

Theorem 8. Let B be a commutative ring with unity.

Let A be the Abelian group $B^{\mathbb{N}_+}$ (this is the Abelian group of all sequences of elements of B, with componentwise addition and zero $(0)_{n\in\mathbb{N}_+}$).

For every $n \in \mathbb{N}_+$, define an endomorphism $\varphi_n : A \to A$ of the group A by

$$\varphi_n\left((x_k)_{k\in\mathbb{N}_+}\right) = (x_{nk})_{k\in\mathbb{N}_+} \qquad \text{for every } (x_k)_{k\in\mathbb{N}_+} \in A.$$

Let $(\beta_n)_{n\in\mathbb{N}_+} \in B^{\mathbb{N}_+}$ be a family of elements which satisfies

$$\left(\beta_{n/p}^p \equiv \beta_n \bmod pB \text{ for every } n \in \mathbb{N}_+ \text{ and every } p \in \operatorname{PF} n\right). \tag{8}$$

We define a family $(b_n)_{n\in\mathbb{N}_+} \in A^{\mathbb{N}_+}$ of elements of A by

$$b_n = (\beta_k^n)_{k\in\mathbb{N}_+} \qquad \text{for every } n \in \mathbb{N}_+.$$

(a) The endomorphisms φ_n satisfy (1) and (2).

(b) The family $(b_n)_{n\in\mathbb{N}_+}$ satisfies the Assertions $\mathcal{C}$, $\mathcal{E}$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ of Theorem 1 for $N = \mathbb{N}_+$.

(c) If the ring B is torsionfree, then the family $(b_n)_{n\in\mathbb{N}_+}$ satisfies the Assertions $\mathcal{C}$, $\mathcal{E}$, $\mathcal{E}'$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ of Theorem 1 for $N = \mathbb{N}_+$.

Remarks: **1)** Note that Theorem 2 is a particular case of Theorem 8 for the ring $B = \mathbb{Z}\left[X_{\mathbb{N}_+}\right]$ (this ring is torsionfree) and the family $(\beta_n)_{n\in\mathbb{N}_+} \in B^{\mathbb{N}_+}$ defined by $\beta_n = w_n$ for every $n \in \mathbb{N}_+$. (That this family $(\beta_n)_{n\in\mathbb{N}_+}$ satisfies (8) follows from Lemma 5, applied to $k = n/p$.)

2) If $B = \mathbb{Z}$, then the condition (8) is equivalent to the condition

$$\left(\beta_{n/p} \equiv \beta_n \bmod pB \text{ for every } n \in \mathbb{N}_+ \text{ and every } p \in \operatorname{PF} n\right),$$

because $\beta_{n/p}^p \equiv \beta_{n/p} \bmod pB$ if $B = \mathbb{Z}$ (by Fermat's Little Theorem).

Now we are going to prove Theorem 8 in all its generality. First, let us formulate the part of Theorem 1 that holds without requiring A to be torsionfree:

Theorem 9. Let N be a nest. Let A be a Abelian group (written additively). For every $n \in N$, let $\varphi_n : A \to A$ be an endomorphism of the group A such that (1) and (2) hold.

Let $(b_n)_{n\in N} \in A^N$ be a family of elements of A. Then, the assertions $\mathcal{C}$, $\mathcal{E}$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ of Theorem 1 are equivalent.

This Theorem 9 is Theorem 5 in [4], so we don't need to prove it here.

Proof of Theorem 8. Let N be the nest $\mathbb{N}_+$.

(a) The proof of Theorem 8 **(a)** is completely analogous to the corresponding part of the proof of Theorem 2 **(a)**.

(b) For every $n \in N$, every $p \in \operatorname{PF} n$ and every $k \in N$, we have $\beta_{pk} \equiv \beta_k^p \bmod pB$ (since $\beta_k^p = \beta_{pk/p}^p \equiv \beta_{pk} \bmod pB$ by (8) (applied to pk instead of n)). Thus, Lemma 4 (applied to $u = \beta_{pk}$ and $v = \beta_k^p$) yields that $\beta_{pk}^{n/p} \equiv \left(\beta_k^p\right)^{n/p} \bmod p^{v_p(n)}B$. Since $\left(\beta_k^p\right)^{n/p} = \beta_k^n$, this simplifies to $\beta_{pk}^{n/p} \equiv \beta_k^n \bmod p^{v_p(n)}B$.

Every $n \in N$ and every $p \in \operatorname{PF} n$ satisfies

$$\begin{aligned}
\varphi_p\left(b_{n/p}\right) &= \varphi_p\left(\left(\beta_k^{n/p}\right)_{k\in N}\right) && \left(\text{since } b_{n/p} \text{ is defined as } \left(\beta_k^{n/p}\right)_{k\in N}\right) \\
&= \left(\beta_{pk}^{n/p}\right)_{k\in N} && \left(\text{by (6) (applied to } p \text{ and } \left(\beta_k^{n/p}\right)_{k\in N} \text{ instead of } n \text{ and } (x_k)_{k\in N}\right) \\
&\equiv (\beta_k^n)_{k\in N} && \left(\text{since } \beta_{pk}^{n/p} \equiv \beta_k^n \bmod p^{v_p(n)}B\right) \\
&= b_n \bmod p^{v_p(n)}A.
\end{aligned}$$

Thus, Assertion $\mathcal{C}$ of Theorem 1 is true for our family $(b_n)_{n\in N}$. Since the Assertions $\mathcal{C}$, $\mathcal{E}$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ of Theorem 1 are equivalent (according to Theorem 9, which we can apply because of Theorem 8 **(a)**), this yields that the Assertions $\mathcal{E}$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ must be true as well. This proves Theorem 8 **(b)**.

(c) Assume that the ring B is torsionfree. Then, the Abelian group A is torsionfree as well (since $A = B^{\mathbb{N}_+}$). Due to this fact, and due to Theorem 8 **(a)**, we can apply Theorem 1 to our situation, and Theorem 1 yields that the Assertions $\mathcal{C}$, $\mathcal{E}$, $\mathcal{E}'$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ of Theorem 1 are equivalent. Since the Assertion $\mathcal{C}$ is true (as we have shown above), we can therefore conclude that all the Assertions $\mathcal{C}$, $\mathcal{E}$, $\mathcal{E}'$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ are true, and thus Theorem 8 **(c)** is proven.

The following is a kind of generalization of Theorem 7:

Theorem 10. Let B be a commutative ring with unity. Let $(\beta_n)_{n\in\mathbb{N}_+} \in B^{\mathbb{N}_+}$ be a family of elements which satisfies (8).

(a) Every $n \in \mathbb{N}_+$ satisfies

$$\sum_{d|n} \mu(d)\, \beta_{dk}^{n/d} \in nB \qquad \text{for every } k \in \mathbb{N}_+.$$

(b) Every $n \in \mathbb{N}_+$ satisfies

$$\sum_{d|n} \phi(d)\, \beta_{dk}^{n/d} \in nB \qquad \text{for every } k \in \mathbb{N}_+.$$

(c) Every $n \in \mathbb{N}_+$ satisfies

$$\sum_{i=1}^{n} \beta_{n/\gcd(i,n)\cdot k}^{\gcd(i,n)} \in nB \qquad \text{for every } k \in \mathbb{N}_+.$$

Proof of Theorem 10. Let N be the nest $\mathbb{N}_+$. Let us invoke Theorem 8. So let us define the Abelian group A, the endomorphisms $\varphi_n : A \to A$ and the family $(b_n)_{n\in\mathbb{N}_+} \in A^{\mathbb{N}_+}$ as in Theorem 8. Then, Theorem 8 **(b)** states that the family $(b_n)_{n\in\mathbb{N}_+}$ satisfies the Assertions $\mathcal{C}$, $\mathcal{E}$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ of Theorem 1.

(a) Assertion $\mathcal{F}$ of Theorem 1 states that every $n \in N$ satisfies

$$\sum_{d|n} \mu(d)\, \varphi_d(b_{n/d}) \in nA.$$

Since this assertion is satisfied, we thus have $\sum_{d|n} \mu(d)\, \varphi_d(b_{n/d}) \in nA$ for every $n \in N$.

Since

$$\sum_{d|n} \mu(d)\, \varphi_d(b_{n/d}) = \sum_{d|n} \mu(d)\, \underbrace{\varphi_d\left(\left(\beta_k^{n/d}\right)_{k\in\mathbb{N}_+}\right)}_{=\left(\beta_{dk}^{n/d}\right)_{k\in\mathbb{N}_+} \text{ (by the definition of } \varphi_d)} \qquad \left(\text{since } b_{n/d} \text{ is defined as } \left(\beta_k^{n/d}\right)_{k\in\mathbb{N}_+}\right)$$

$$= \sum_{d|n} \mu(d) \left(\beta_{dk}^{n/d}\right)_{k\in\mathbb{N}_+} = \left(\sum_{d|n} \mu(d)\, \beta_{dk}^{n/d}\right)_{k\in\mathbb{N}_+}$$

(since addition in A is componentwise),

this becomes $\left(\sum_{d\mid n}\mu(d)\,\beta_{dk}^{n/d}\right)_{k\in\mathbb{N}_+} \in nA$. In other words, there exists a sequence $(u_k)_{k\in\mathbb{N}_+}\in A$ such that $\left(\sum_{d\mid n}\mu(d)\,\beta_{dk}^{n/d}\right)_{k\in\mathbb{N}_+} = n\,(u_k)_{k\in\mathbb{N}_+}$. Thus, $\left(\sum_{d\mid n}\mu(d)\,\beta_{dk}^{n/d}\right)_{k\in\mathbb{N}_+} = n\,(u_k)_{k\in\mathbb{N}_+} = (nu_k)_{k\in\mathbb{N}_+}$. Hence, for every $k\in\mathbb{N}_+$, we have $\sum_{d\mid n}\mu(d)\,\beta_{dk}^{n/d} = nu_k \in nB$. This proves Theorem 10 **(a)**.

(b) The proof of Theorem 10 **(b)** is the same as the proof of Theorem 10 **(a)** that we have just done; we just have to replace every μ by ϕ and use Assertion $\mathcal{G}$ instead of Assertion $\mathcal{F}$.

(c) Assertion $\mathcal{H}$ of Theorem 1 states that every $n\in N$ satisfies

$$\sum_{i=1}^{n}\varphi_{n/\gcd(i,n)}\left(b_{\gcd(i,n)}\right)\in nA.$$

Since this assertion is satisfied, we thus have $\sum_{i=1}^{n}\varphi_{n/\gcd(i,n)}\left(b_{\gcd(i,n)}\right)\in nA$ for every $n\in N$. Since

$$\begin{aligned}\sum_{i=1}^{n}\varphi_{n/\gcd(i,n)}\left(b_{\gcd(i,n)}\right) &= \sum_{i=1}^{n}\underbrace{\varphi_{n/\gcd(i,n)}\left(\left(\beta_k^{\gcd(i,n)}\right)_{k\in\mathbb{N}_+}\right)}_{=\left(\beta^{\gcd(i,n)}_{n/\gcd(i,n)\cdot k}\right)_{k\in\mathbb{N}_+}}\\ &\qquad\qquad\left(\text{by the definition of }\varphi_{n/\gcd(i,n)}\right)\\ &\qquad\qquad\left(\text{since } b_{\gcd(i,n)} \text{ is defined as } \left(\beta_k^{\gcd(i,n)}\right)_{k\in\mathbb{N}_+}\right)\\ &= \sum_{i=1}^{n}\left(\beta^{\gcd(i,n)}_{n/\gcd(i,n)\cdot k}\right)_{k\in\mathbb{N}_+} = \left(\sum_{i=1}^{n}\beta^{\gcd(i,n)}_{n/\gcd(i,n)\cdot k}\right)_{k\in\mathbb{N}_+}\\ &\qquad\qquad\left(\text{since addition in } A \text{ is componentwise}\right),\end{aligned}$$

this rewrites as $\left(\sum_{i=1}^{n}\beta^{\gcd(i,n)}_{n/\gcd(i,n)\cdot k}\right)_{k\in\mathbb{N}_+}\in nA$. In other words, there exists a sequence $(v_k)_{k\in\mathbb{N}_+}\in A$ such that $\left(\sum_{i=1}^{n}\beta^{\gcd(i,n)}_{n/\gcd(i,n)\cdot k}\right)_{k\in\mathbb{N}_+} = n\,(v_k)_{k\in\mathbb{N}_+}$. Thus, $\left(\sum_{i=1}^{n}\beta^{\gcd(i,n)}_{n/\gcd(i,n)\cdot k}\right)_{k\in\mathbb{N}_+} = n\,(v_k)_{k\in\mathbb{N}_+} = (nv_k)_{k\in\mathbb{N}_+}$. Hence, for every $k\in\mathbb{N}_+$, we have $\sum_{i=1}^{n}\beta^{\gcd(i,n)}_{n/\gcd(i,n)\cdot k} = nv_k \in nB$. This proves Theorem 10 **(c)**.

We can generalize Theorem 10 even further, replacing some of the $\mathbb{N}_+$ by an arbitrary nest N:

Theorem 11. Let N be a nest. Let B be a commutative ring with unity.

Let $(\beta_n)_{n\in N}\in B^N$ be a family of elements which satisfies

$$\left(\beta^p_{n/p}\equiv\beta_n \bmod pB \text{ for every } n\in N \text{ and every } p\in \operatorname{PF} n\right). \tag{9}$$

(a) Every $n \in N$ satisfies

$$\sum_{d|n} \mu(d)\, \beta_{dk}^{n/d} \in nB \qquad \text{for every } k \in N \text{ satisfying } nk \in N.$$

(b) Every $n \in N$ satisfies

$$\sum_{d|n} \phi(d)\, \beta_{dk}^{n/d} \in nB \qquad \text{for every } k \in N \text{ satisfying } nk \in N.$$

(c) Every $n \in N$ satisfies

$$\sum_{i=1}^{n} \beta_{n/\gcd(i,n)\cdot k}^{\gcd(i,n)} \in nB \qquad \text{for every } k \in N \text{ satisfying } nk \in N.$$

Remarks: **1)** In the particular case $N = \mathbb{N}_+$, Theorem 11 yields Theorem 10.
2) If $B = \mathbb{Z}$, then the condition (9) is equivalent to the condition

$$\left(\beta_{n/p} \equiv \beta_n \bmod pB \text{ for every } n \in N \text{ and every } p \in \operatorname{PF} n\right),$$

because $\beta_{n/p}^{p} \equiv \beta_{n/p} \bmod pB$ if $B = \mathbb{Z}$ (by Fermat's Little Theorem).

For the proof of Theorem 11, we will need a consequence of the Chinese Remainder Theorem:

Lemma 12. Let B be an Abelian group (written additively). Let $P \subseteq \mathbb{P}$ be a finite set of primes. Let $(c_p)_{p\in P} \in B^P$ be a family of elements of B. Then, there exists an element m of B such that

$$\left(c_p \equiv m \bmod pB \text{ for every } p \in P\right).$$

This Lemma 12 is Corollary 3 in [5] (with M renamed as B), so we won't give the proof of Lemma 12 here.

Proof of Theorem 11. We would like to apply Theorem 10, but we cannot do this directly, since we only have a family $(\beta_n)_{n\in N} \in B^N$, while Theorem 10 requires a family $(\beta_n)_{n\in\mathbb{N}_+} \in B^{\mathbb{N}_+}$. So let us extend our family $(\beta_n)_{n\in N} \in B^N$ to a family $(\beta_n)_{n\in\mathbb{N}_+} \in B^{\mathbb{N}_+}$. In other words, we are going to define an element $\beta_n \in B$ for every $n \in \mathbb{N}_+ \setminus N$ such that the resulting family $(\beta_n)_{n\in\mathbb{N}_+} \in B^{\mathbb{N}_+}$ (which consists of the already known elements β_n for $n \in N$ and the newly constructed elements β_n for $n \in \mathbb{N}_+ \setminus N$) satisfies (8).

This construction will be done by strong induction over n. So fix some $n \in \mathbb{N}_+ \setminus N$, and let us construct an element $\beta_n \in B$, assuming that we have already constructed an element $\beta_m \in B$ for every $m \in \mathbb{N}_+ \setminus N$ satisfying $m < n$.

Actually, an element $\beta_m \in B$ is defined for every $m \in \mathbb{N}_+$ satisfying $m < n$ (in fact, if $m \in N$, then β_m is defined by the condition of Theorem 11, and if $m \in \mathbb{N}_+ \setminus N$, then β_m has already been constructed by our induction assumption). Consequently, an element $\beta_{n/p} \in B$ is defined for every $p \in \operatorname{PF} n$ (because $n/p < n$). Now, let $P = \operatorname{PF} n$, and define a family $(c_p)_{p\in P} \in B^P$ by $c_p = \beta_{n/p}^{p}$ for every $p \in P$. Then, Lemma 12 states that there exists an element m of B such that $\left(c_p \equiv m \bmod pB \text{ for every } p \in P\right)$.

Now, define an element $\beta_n \in B$ by $\beta_n = m$ for this element m. Then, for every $p \in P$, we have

$$\beta_{n/p}^p = c_p \equiv m = \beta_n \bmod pB.$$

Thus, we have shown that

$$\left(\beta_{n/p}^p \equiv \beta_n \bmod pB \text{ for every } p \in \operatorname{PF} n\right). \tag{10}$$

Hence, we can recursively define elements $\beta_n \in B$ for all $n \in \mathbb{N}_+ \setminus N$, and these elements satisfy (10) for every $n \in \mathbb{N}_+ \setminus N$.

This construction gives us a family $(\beta_n)_{n \in \mathbb{N}_+} \in B^{\mathbb{N}_+}$ which satisfies (8) (in fact, (8) is satisfied, because for each $n \in \mathbb{N}_+$ and each $p \in \operatorname{PF} n$, we have $\beta_{n/p}^p \equiv \beta_n \bmod pB$ [10]). Thus, Theorem 10 can be applied to this family $(\beta_n)_{n \in \mathbb{N}_+} \in B^{\mathbb{N}_+}$, and the assertions of Theorem 10 **(a)**, Theorem 10 **(b)** and Theorem 10 **(c)** yield the assertions of Theorem 11 **(a)**, Theorem 11 **(b)** and Theorem 11 **(c)**, respectively. This proves Theorem 11.

Now let us extend Theorem 2 and Theorem 7 a bit further. In fact, if we trace back our proof of Theorem 2, we notice that the only property of the Witt polynomials w_n which we used is Lemma 5, which relied chiefly on the fact that $dX_d^{pk/d} \equiv 0 \bmod p\mathbb{Z}\left[X_{\mathbb{N}_+}\right]$ for every $d \in \mathbb{N}_+$, $k \in \mathbb{N}_+$ and $p \in \operatorname{PF} d$ satisfying $d \nmid k$. This is an almost trivial fact, which can be easily weakened using the notion of the *radical* of a positive integer:

Definition 12. We define a function $\operatorname{rad} : \mathbb{N}_+ \to \mathbb{N}_+$ by

$$\operatorname{rad} n = \prod_{p \in \operatorname{PF} n} p \qquad \text{for any } n \in \mathbb{N}_+.$$

For any $n \in \mathbb{N}_+$, we denote the number $\operatorname{rad} n$ as the *radical* of n.

Here are some very basic properties of rad: Clearly, every $n \in \mathbb{N}_+$ satisfies $\operatorname{rad} n \mid n$ [11]. The number $\operatorname{rad} n$ is the greatest squarefree divisor of n. Also notice that

$$p \mid \operatorname{rad} n \text{ for every } n \in \mathbb{N}_+ \text{ and every } p \in \operatorname{PF} n. \tag{11}$$

[12]

Using this notion, we can define so-called *radical Witt polynomials*, which mimic the Witt polynomials but tend to have smaller coefficients:

[10] In fact, we must have either $n \in N$ or $n \in \mathbb{N}_+ \setminus N$. But in both of these cases, we have $\beta_{n/p}^p \equiv \beta_n \bmod pB$ (in fact, in the case $n \in N$, this follows from (9), and in the case $n \in \mathbb{N}_+ \setminus N$, this follows from (10)). Hence, $\beta_{n/p}^p \equiv \beta_n \bmod pB$ always holds.

[11] *Proof.* Let $n \in \mathbb{N}_+$. Every $p \in \operatorname{PF} n$ satisfies $p \mid n$ and thus $v_p(n) \geq 1$, so that $p \mid p^{v_p(n)}$. Hence, $\prod_{p \in \operatorname{PF} n} p \mid \prod_{p \in \operatorname{PF} n} p^{v_p(n)}$. But now, we have $\operatorname{rad} n = \prod_{p \in \operatorname{PF} n} p \mid \prod_{p \in \operatorname{PF} n} p^{v_p(n)} = n$, qed.

[12] *Proof of (11):* Let $n \in \mathbb{N}_+$. Then, every $q \in \operatorname{PF} n$ satisfies $q \mid \prod_{p \in \operatorname{PF} n} p = \operatorname{rad} n$. If we rename q as p in this result, we obtain the following: Every $p \in \operatorname{PF} n$ satisfies $p \mid \operatorname{rad} n$. This proves (11).

Definition 13. For any $n \in \mathbb{N}_+$, we define a polynomial $\sqrt[\infty]{w}_n \in \mathbb{Z}\left[X_{\mathbb{N}_{|n}}\right]$ (note that $\sqrt[\infty]{w}$ is considered to be a single symbol here; it's not a "root of w" or anything like that) by

$$\sqrt[\infty]{w}_n = \sum_{d|n} (\operatorname{rad} d)\, X_d^{n/d}.$$

The polynomials $\sqrt[\infty]{w}_1$, $\sqrt[\infty]{w}_2$, $\sqrt[\infty]{w}_3$, ... will be called the *big radical Witt polynomials* or, simply, the *radical Witt polynomials*.[13]

These polynomials are studied in [6]. Here comes an analogue of Theorem 2 for these radical Witt polynomials:

Theorem 13. Consider the polynomial ring $\mathbb{Z}\left[X_{\mathbb{N}_+}\right] = \mathbb{Z}\left[X_1, X_2, X_3, ...\right]$. Let A be the Abelian group $\left(\mathbb{Z}\left[X_{\mathbb{N}_+}\right]\right)^{\mathbb{N}_+}$ (this is the Abelian group of all sequences of elements of $\mathbb{Z}\left[X_{\mathbb{N}_+}\right]$, with componentwise addition and zero $(0)_{n\in\mathbb{N}_+}$).

For every $n \in \mathbb{N}_+$, define an endomorphism $\varphi_n : A \to A$ of the group A as in Theorem 2.

We define a family $(b_n)_{n\in\mathbb{N}_+} \in A^{\mathbb{N}_+}$ of elements of A by

$$b_n = \left(\sqrt[\infty]{w}_k^n\right)_{k\in\mathbb{N}_+} \qquad \text{for every } n \in \mathbb{N}_+.$$

(Of course, this family $(b_n)_{n\in\mathbb{N}_+}$ is **not** the family $(b_n)_{n\in\mathbb{N}_+}$ from Theorem 2.)

(a) The group A is torsionfree, and the endomorphisms φ_n satisfy (1) and (2).

(b) The family $(b_n)_{n\in\mathbb{N}_+}$ satisfies the Assertions $\mathcal{C}$, $\mathcal{E}$, $\mathcal{E}'$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ of Theorem 1 for $N = \mathbb{N}_+$.

And the corresponding analogue of Theorem 7 says:

Theorem 14. Consider the polynomial ring $\mathbb{Z}\left[X_{\mathbb{N}_+}\right] = \mathbb{Z}\left[X_1, X_2, X_3, ...\right]$.

(a) Every $n \in \mathbb{N}_+$ satisfies

$$\sum_{d|n} \mu(d)\ \sqrt[\infty]{w}_{dk}^{n/d} \in n\mathbb{Z}\left[X_{\mathbb{N}_{|kn}}\right] \qquad \text{for every } k \in \mathbb{N}_+.$$

(b) Every $n \in \mathbb{N}_+$ satisfies

$$\sum_{d|n} \phi(d)\ \sqrt[\infty]{w}_{dk}^{n/d} \in n\mathbb{Z}\left[X_{\mathbb{N}_{|kn}}\right] \qquad \text{for every } k \in \mathbb{N}_+.$$

(c) Every $n \in \mathbb{N}_+$ satisfies

$$\sum_{i=1}^{n} \sqrt[\infty]{w}_{n/\gcd(i,n)\cdot k}^{\gcd(i,n)} \in n\mathbb{Z}\left[X_{\mathbb{N}_{|kn}}\right] \qquad \text{for every } k \in \mathbb{N}_+.$$

[13] These radical Witt polynomials $\sqrt[\infty]{w}_1$, $\sqrt[\infty]{w}_2$, $\sqrt[\infty]{w}_3$, ... are somewhat similar to the big Witt polynomials w_1, w_2, w_3, ... defined in [4]. Exploiting this similarity is the purpose of this paper.

We will not prove Theorems 13 and 14 directly, but rather extend them even further. In order to do so, we define a more general ilk of Witt polynomials:

Definition 14. Let $F : \mathbb{P} \times \mathbb{N} \to \mathbb{N}$ be a map. We denote by $\widetilde{F} : \mathbb{N}_+ \to \mathbb{N}_+$ the map defined by

$$\widetilde{F}(n) = \prod_{p \in \mathrm{PF}\, n} p^{F(p, v_p(n))} \qquad \text{for every } n \in \mathbb{N}_+.$$

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

$$w_{F,n} = \sum_{d|n} \widetilde{F}(d)\, X_d^{n/d}.$$

The polynomials $w_{F,1}$, $w_{F,2}$, $w_{F,3}$, ... will be called the *big F-Witt polynomials* or, simply, the *F-Witt polynomials*.

Note that the notions $\widetilde{F}$ and $w_{F,n}$ which we have just defined are exactly identical with the notions $\widetilde{F}$ and $w_{F,n}$ defined in [7], but in [7] they were only defined for *pseudo-monotonous* maps $F : \mathbb{P} \times \mathbb{N} \to \mathbb{N}$ (we refer to Definition 9 of [7] for the meaning of "pseudo-monotonous"), while here we have defined them for arbitrary F.

However, these F-Witt polynomials don't yet have to satisfy analogues of Theorems 2 and 7. We need an additional condition to ensure that:

Definition 15. A map $F : \mathbb{P} \times \mathbb{N} \to \mathbb{N}$ is said to be *superradical* if it satisfies

$$\left(F(p, a) > 0 \qquad \text{for every } p \in \mathbb{P} \text{ and } a \in \mathbb{N}_+\right). \tag{12}$$

Before we continue, let us give two example of superradical maps:

Example 1: Define the map $\mathrm{pr}_{\mathbb{N}} : \mathbb{P} \times \mathbb{N} \to \mathbb{N}$ by

$$\mathrm{pr}_{\mathbb{N}}(p, k) = k \qquad \text{for every } p \in \mathbb{P} \text{ and } k \in \mathbb{N}.$$

Then, $\mathrm{pr}_{\mathbb{N}}$ is a superradical map (this is very easy to check), and $\widetilde{\mathrm{pr}_{\mathbb{N}}} = \mathrm{id}$ (since every $n \in \mathbb{N}_+$ satisfies $\widetilde{\mathrm{pr}_{\mathbb{N}}}(n) = \prod_{p \in \mathrm{PF}\, n} \underbrace{p^{\mathrm{pr}_{\mathbb{N}}(p, v_p(n))}}_{\substack{= p^{v_p(n)} \\ (\text{since } \mathrm{pr}_{\mathbb{N}}(p, v_p(n)) = v_p(n))}} = \prod_{p \in \mathrm{PF}\, n} p^{v_p(n)} = n$). Hence, every $n \in \mathbb{N}_+$ satisfies $w_{\mathrm{pr}_{\mathbb{N}}, n} = \sum_{d|n} \underbrace{\widetilde{\mathrm{pr}_{\mathbb{N}}}(d)}_{= \mathrm{id}(d) = d} X_d^{n/d} = \sum_{d|n} d X_d^{n/d} = w_n$.

Example 2: Define the map $\mathrm{prad} : \mathbb{P} \times \mathbb{N} \to \mathbb{N}$ by

$$\mathrm{prad}(p, k) = \begin{cases} 0, & \text{if } k = 0; \\ 1, & \text{if } k > 0 \end{cases} \qquad \text{for every } p \in \mathbb{P} \text{ and } k \in \mathbb{N}.$$

Then, prad is a superradical map[14], and the map $\widetilde{\operatorname{prad}}$ is identic with the map rad : $\mathbb{N}_+ \to \mathbb{N}_+$ defined by $\operatorname{rad} n = \prod_{p \in \operatorname{PF} n} p$ for every $n \in \mathbb{N}_+$ (since every $n \in \mathbb{N}_+$ satisfies

$$\widetilde{\operatorname{prad}}(n) = \prod_{p \in \operatorname{PF} n} \underbrace{p^{\operatorname{prad}(p, v_p(n))}}_{\substack{=p \text{ (since } p \in \operatorname{PF} n \text{ yields} \\ p \mid n \text{ and thus } v_p(n) > 0, \\ \text{so that } \operatorname{prad}(p, v_p(n)) = 1 \\ \text{and thus } p^{\operatorname{prad}(p, v_p(n))} = p^1 = p)}} = \prod_{p \in \operatorname{PF} n} p = \operatorname{rad} n$$

). Hence, every $n \in \mathbb{N}_+$ satisfies

$$w_{\operatorname{prad},n} = \sum_{d \mid n} \underbrace{\widetilde{\operatorname{prad}}(d)}_{=\operatorname{rad} d} X_d^{n/d} = \sum_{d \mid n} (\operatorname{rad} d) X_d^{n/d} = \sqrt[\infty]{w}_n. \tag{14}$$

We now state the generalization of Theorem 2:

Theorem 15. Consider the polynomial ring $\mathbb{Z}\left[X_{\mathbb{N}_+}\right] = \mathbb{Z}\left[X_1, X_2, X_3, ...\right]$. Let A be the Abelian group $\left(\mathbb{Z}\left[X_{\mathbb{N}_+}\right]\right)^{\mathbb{N}_+}$ (this is the Abelian group of all sequences of elements of $\mathbb{Z}\left[X_{\mathbb{N}_+}\right]$, with componentwise addition and zero $(0)_{n \in \mathbb{N}_+}$).

Let $F : \mathbb{P} \times \mathbb{N} \to \mathbb{N}$ be a superradical map.

For every $n \in \mathbb{N}_+$, define an endomorphism $\varphi_n : A \to A$ of the group A as in Theorem 2.

We define a family $(b_n)_{n \in \mathbb{N}_+} \in A^{\mathbb{N}_+}$ of elements of A by

$$b_n = \left(w_{F,k}^n\right)_{k \in \mathbb{N}_+} \qquad \text{for every } n \in \mathbb{N}_+.$$

(Of course, this family $(b_n)_{n \in \mathbb{N}_+}$ is **not** the family $(b_n)_{n \in \mathbb{N}_+}$ from Theorem 2.)

(a) The group A is torsionfree, and the endomorphisms φ_n satisfy (1) and (2).

(b) The family $(b_n)_{n \in \mathbb{N}_+}$ satisfies the Assertions $\mathcal{C}$, $\mathcal{E}$, $\mathcal{E}'$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ of Theorem 1 for $N = \mathbb{N}_+$.

The corresponding generalization of Theorem 7 now claims:

[14] *Proof.* By the definition of "superradical", the map prad is superradical if and only if it satisfies

$$(\operatorname{prad}(p, a) > 0 \qquad \text{for every } p \in \mathbb{P} \text{ and } a \in \mathbb{N}_+). \tag{13}$$

Since the map prad does satisfy (13) (because for every $p \in \mathbb{P}$ and $a \in \mathbb{N}_+$, we have

$$\begin{aligned} \operatorname{prad}(p, a) &= \begin{cases} 0, & \text{if } a = 0; \\ 1, & \text{if } a > 0 \end{cases} \qquad \text{(by the definition of prad)} \\ &= 1 \qquad \text{(since } a > 0 \text{ (because } a \in \mathbb{N}_+)) \\ &> 0 \end{aligned}$$

), this yields that the map prad is superradical, qed.

Theorem 16. Consider the polynomial ring $\mathbb{Z}\left[X_{\mathbb{N}_+}\right] = \mathbb{Z}\left[X_1, X_2, X_3, ...\right]$.

Let $F : \mathbb{P} \times \mathbb{N} \to \mathbb{N}$ be a superradical map.

(a) Every $n \in \mathbb{N}_+$ satisfies

$$\sum_{d \mid n} \mu(d)\, w_{F,dk}^{n/d} \in n\mathbb{Z}\left[X_{\mathbb{N}_{\mid kn}}\right] \qquad \text{for every } k \in \mathbb{N}_+.$$

(b) Every $n \in \mathbb{N}_+$ satisfies

$$\sum_{d \mid n} \phi(d)\, w_{F,dk}^{n/d} \in n\mathbb{Z}\left[X_{\mathbb{N}_{\mid kn}}\right] \qquad \text{for every } k \in \mathbb{N}_+.$$

(c) Every $n \in \mathbb{N}_+$ satisfies

$$\sum_{i=1}^{n} w_{F,n/\gcd(i,n)\cdot k}^{\gcd(i,n)} \in n\mathbb{Z}\left[X_{\mathbb{N}_{\mid kn}}\right] \qquad \text{for every } k \in \mathbb{N}_+.$$

We now come to proving these theorems. First, a simple remark:

Lemma 17. Let $F : \mathbb{P} \times \mathbb{N} \to \mathbb{N}$ be a superradical map. Then, $p \mid \widetilde{F}(n)$ for every $n \in \mathbb{N}_+$ and $p \in \operatorname{PF} n$.

Proof of Lemma 17. According to Definition 15, we know that the map F is superradical if and only if it satisfies (12). Since we know that F is superradical, we thus conclude that F satisfies (12).

Every $n \in \mathbb{N}_+$ satisfies $\widetilde{F}(n) = \prod_{p \in \operatorname{PF} n} p^{F(p, v_p(n))} = \prod_{q \in \operatorname{PF} n} q^{F(q, v_q(n))}$ (here, we renamed the index p as q in the product).

Now, let $n \in \mathbb{N}_+$ and $p \in \operatorname{PF} n$. Since $p \in \operatorname{PF} n$, we know that p is prime and satisfies $p \mid n$. Thus, $v_p(n) \geq 1$. In other words, $v_p(n) \in \mathbb{N}_+$.

Since p is prime, we have $p \in \mathbb{P}$. Hence, applying (12) to $a = v_p(n)$, we obtain $F(p, v_p(n)) > 0$ (since $v_p(n) \in \mathbb{N}_+$), so that $F(p, v_p(n)) \geq 1$. Hence,

$$p \mid p^{F(p, v_p(n))} \mid \prod_{q \in \operatorname{PF} n} q^{F(q, v_q(n))} \qquad (\text{since } p \in \operatorname{PF} n)$$
$$= \widetilde{F}(n).$$

This proves Lemma 17.

Next, we show an analogue of Lemma 5:

Lemma 18. Let $k \in \mathbb{N}_+$ and $p \in \mathbb{P}$. Let $F : \mathbb{P} \times \mathbb{N} \to \mathbb{N}$ be a superradical map. Then, $w_{F,pk} \equiv w_{F,k}^p \bmod p\mathbb{Z}\left[X_{\mathbb{N}_+}\right]$. (Remember that $\mathbb{Z}\left[X_{\mathbb{N}_+}\right] = \mathbb{Z}\left[X_1, X_2, X_3, ...\right]$).

Proof of Lemma 18. For every divisor d of pk which satisfies $d \nmid k$, we have $\widetilde{F}(d) X_d^{pk/d} \equiv 0 \bmod p\mathbb{Z}\left[X_{\mathbb{N}_+}\right]$ [15]. Thus,

$$\sum_{\substack{d \mid pk; \\ d \nmid k}} \underbrace{\widetilde{F}(d) X_d^{pk/d}}_{\equiv 0} \equiv \sum_{\substack{d \mid pk; \\ d \nmid k}} 0 = 0 \bmod p\mathbb{Z}\left[X_{\mathbb{N}_+}\right]. \tag{15}$$

Now, comparing

$$\begin{aligned} w_{F,pk} &= \sum_{d \mid pk} \widetilde{F}(d) X_d^{pk/d} = \sum_{\substack{d \mid pk; \\ d \mid k}} \widetilde{F}(d) X_d^{pk/d} + \underbrace{\sum_{\substack{d \mid pk; \\ d \nmid k}} \widetilde{F}(d) X_d^{pk/d}}_{\substack{\equiv 0 \bmod p\mathbb{Z}\left[X_{\mathbb{N}_+}\right] \\ \text{(by (15))}}} \\ &\equiv \underbrace{\sum_{\substack{d \mid pk; \\ d \mid k}}}_{= \sum_{d \mid k}} \widetilde{F}(d) X_d^{pk/d} = \sum_{d \mid k} \widetilde{F}(d) X_d^{pk/d} \bmod p\mathbb{Z}\left[X_{\mathbb{N}_+}\right] \end{aligned}$$

with

$$\begin{aligned} w_{F,k}^p &= \left(\sum_{d \mid k} \widetilde{F}(d) X_d^{k/d} \right)^p \qquad \left(\text{since } w_{F,k} = \sum_{d \mid k} \widetilde{F}(d) X_d^{k/d} \right) \\ &\equiv \sum_{d \mid k} \left(\widetilde{F}(d) X_d^{k/d} \right)^p \\ &\qquad \left(\text{since } \left(\sum_{s \in S} a_s \right)^p \equiv \sum_{s \in S} a_s^p \bmod pK \text{ for any family } (a_s)_{s \in S} \text{ of elements of a commutative ring } K \right) \\ &= \sum_{d \mid k} \underbrace{\left(\widetilde{F}(d) \right)^p}_{\substack{\equiv \widetilde{F}(d) \bmod p\mathbb{Z}\left[X_{\mathbb{N}_+}\right] \\ \text{(since } \left(\widetilde{F}(d)\right)^p \equiv \widetilde{F}(d) \bmod p\mathbb{Z} \\ \text{by Fermat's Little Theorem)}}} \underbrace{\left(X_d^{k/d} \right)^p}_{= X_d^{k/d \cdot p} = X_d^{pk/d}} \equiv \sum_{d \mid k} \widetilde{F}(d) X_d^{pk/d} \bmod p\mathbb{Z}\left[X_{\mathbb{N}_+}\right], \end{aligned}$$

we obtain $w_{F,pk} \equiv w_{F,k}^p \bmod p\mathbb{Z}\left[X_{\mathbb{N}_+}\right]$, and thus Lemma 18 is proven.

A conclusion from Lemmata 4 and 18:

Lemma 19. Let $k \in \mathbb{N}_+$. Let $n \in \mathbb{N}_+$ and $p \in \operatorname{PF} n$. Let $F : \mathbb{P} \times \mathbb{N} \to \mathbb{N}$ be a superradical map. Then, $w_{F,pk}^{n/p} \equiv w_{F,k}^n \bmod p^{v_p(n)}\mathbb{Z}\left[X_{\mathbb{N}_+}\right]$. (Remember that $\mathbb{Z}\left[X_{\mathbb{N}_+}\right] = \mathbb{Z}\left[X_1, X_2, X_3, ...\right]$).

Proof of Lemma 19. Lemma 18 yields $w_{F,pk} \equiv w_{F,k}^p \bmod p\mathbb{Z}\left[X_{\mathbb{N}_+}\right]$ (since $p \in \mathbb{P}$ due to $p \in \operatorname{PF} n$). Lemma 4 (applied to $B = \mathbb{Z}\left[X_{\mathbb{N}_+}\right]$, $u = w_{F,pk}$ and $v = w_{F,k}^p$) now

[15] *Proof.* Let d be a divisor of pk which satisfies $d \nmid k$. Then, d cannot be coprime to p, (since otherwise, from $d \mid pk$ we could conclude that $d \mid k$, contradicting to $d \nmid k$), and thus d must be divisible by p (since p is a prime). Thus, p is a divisor of d. Since p is prime, this yields that p is a prime divisor of d, so that $p \in \operatorname{PF} d$. Hence, Lemma 17 (applied to d instead of n) yields $p \mid \widetilde{F}(d)$. Hence, $\widetilde{F}(d) \equiv 0 \bmod p\mathbb{Z}\left[X_{\mathbb{N}_+}\right]$, so that $\widetilde{F}(d) X_d^{pk/d} \equiv 0 \bmod p\mathbb{Z}\left[X_{\mathbb{N}_+}\right]$, qed.

yields $w_{F,pk}^{n/p} \equiv \left(w_{F,k}^{p}\right)^{n/p} \bmod p^{v_p(n)}\mathbb{Z}\left[X_{\mathbb{N}_+}\right]$. Since $\left(w_{F,k}^{p}\right)^{n/p} = w_{F,k}^{n}$, this rewrites as $w_{F,pk}^{n/p} \equiv w_{F,k}^{n} \bmod p^{v_p(n)}\mathbb{Z}\left[X_{\mathbb{N}_+}\right]$, and thus Lemma 19 is proven.

Proof of Theorem 15. Let N be the nest $\mathbb{N}_+$. Then, $A = \left(\mathbb{Z}\left[X_{\mathbb{N}_+}\right]\right)^{\mathbb{N}_+} = \left(\mathbb{Z}\left[X_{\mathbb{N}_+}\right]\right)^{N}$. Just as in the proof of Theorem 2, we can see that (6) holds.

(a) Theorem 15 **(a)** is identical with Theorem 2 **(a)**, and thus needs not be proven again.

(b) Every $n \in N$ and every $p \in \operatorname{PF} n$ satisfies

$$\begin{aligned}
\varphi_p\left(b_{n/p}\right) &= \varphi_p\left(\left(w_{F,k}^{n/p}\right)_{k\in N}\right) && \left(\text{since } b_{n/p} \text{ is defined as } \left(w_{F,k}^{n/p}\right)_{k\in N}\right) \\
&= \left(w_{F,pk}^{n/p}\right)_{k\in N} && \left(\text{by (6) (applied to } p \text{ and } \left(w_{F,k}^{n/p}\right)_{k\in N} \text{ instead of } n \text{ and } \left(x_k\right)_{k\in N}\right)\right) \\
&\equiv \left(w_{F,k}^{n}\right)_{k\in N} && \left(\text{since Lemma 19 says that } w_{F,pk}^{n/p} \equiv w_{F,k}^{n} \bmod p^{v_p(n)}\mathbb{Z}\left[X_{\mathbb{N}_+}\right] \text{ for every } k \in \mathbb{N}_+\right) \\
&= b_n \bmod p^{v_p(n)} A.
\end{aligned}$$

Thus, Assertion $\mathcal{C}$ of Theorem 1 is true for our family $\left(b_n\right)_{n\in N}$. Since the Assertions $\mathcal{C}$, $\mathcal{E}$, $\mathcal{E}'$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ of Theorem 1 are equivalent (according to Theorem 1, which we can apply because of Theorem 15 **(a)**), this yields that the Assertions $\mathcal{E}$, $\mathcal{E}'$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ must be true as well. This proves Theorem 15 **(b)**.

Theorem 15 is now proven. We are now going to derive Theorem 16 from it:

Proof of Theorem 16. Let us invoke Theorem 15. So let us define the nest $N = \mathbb{N}_+$, the Abelian group A, the endomorphisms $\varphi_n : A \to A$ and the family $\left(b_n\right)_{n\in\mathbb{N}_+} \in A^{\mathbb{N}_+}$ as in Theorem 15. Then, Theorem 15 **(b)** states that the family $\left(b_n\right)_{n\in N}$ satisfies the Assertions $\mathcal{C}$, $\mathcal{E}$, $\mathcal{E}'$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ of Theorem 1.

(a) Assertion $\mathcal{F}$ of Theorem 1 states that every $n \in N$ satisfies

$$\sum_{d|n} \mu\left(d\right) \varphi_d\left(b_{n/d}\right) \in nA.$$

Since this assertion is satisfied, we thus have $\sum_{d|n} \mu\left(d\right) \varphi_d\left(b_{n/d}\right) \in nA$ for every $n \in N$.

Since

$$\sum_{d|n} \mu\left(d\right) \varphi_d\left(b_{n/d}\right) = \sum_{d|n} \mu\left(d\right) \underbrace{\varphi_d\left(\left(w_{F,k}^{n/d}\right)_{k\in\mathbb{N}_+}\right)}_{\substack{=\left(w_{F,dk}^{n/d}\right)_{k\in\mathbb{N}_+} \\ \text{(by the definition of } \varphi_d\text{)}}} \qquad \left(\text{since } b_{n/d} \text{ is defined as } \left(w_{F,k}^{n/d}\right)_{k\in\mathbb{N}_+}\right)$$

$$= \sum_{d|n} \mu\left(d\right) \left(w_{F,dk}^{n/d}\right)_{k\in\mathbb{N}_+} = \left(\sum_{d|n} \mu\left(d\right) w_{F,dk}^{n/d}\right)_{k\in\mathbb{N}_+}$$

$$\text{(since addition in } A \text{ is componentwise)},$$

this becomes $\left(\sum_{d|n} \mu\left(d\right) w_{F,dk}^{n/d}\right)_{k\in\mathbb{N}_+} \in nA$. In other words, there exists a sequence $\left(u_k\right)_{k\in\mathbb{N}_+} \in A$ such that $\left(\sum_{d|n} \mu\left(d\right) w_{F,dk}^{n/d}\right)_{k\in\mathbb{N}_+} = n\left(u_k\right)_{k\in\mathbb{N}_+}$. Thus, $\left(\sum_{d|n} \mu\left(d\right) w_{F,dk}^{n/d}\right)_{k\in\mathbb{N}_+} =$

$n\left(u_k\right)_{k\in\mathbb{N}_+} = \left(nu_k\right)_{k\in\mathbb{N}_+}$. Hence, for every $k \in \mathbb{N}_+$, we have $\sum\limits_{d\mid n} \mu\left(d\right) w_{F,dk}^{n/d} = nu_k \in n\mathbb{Z}\left[X_{\mathbb{N}_+}\right]$. In other words, $\dfrac{1}{n}\sum\limits_{d\mid n} \mu\left(d\right) w_{F,dk}^{n/d} \in \mathbb{Z}\left[X_{\mathbb{N}_+}\right]$.

On the other hand, $\dfrac{1}{n}\sum\limits_{d\mid n} \mu\left(d\right) w_{F,dk}^{n/d} \in \mathbb{Q}\left[X_{\mathbb{N}_{\mid kn}}\right]$, since every $d \mid n$ satisfies $w_{F,dk} \in \mathbb{Q}\left[X_{\mathbb{N}_{\mid dk}}\right] \subseteq \mathbb{Q}\left[X_{\mathbb{N}_{\mid kn}}\right]$ (since $d \mid n$ yields $dk \mid nk = kn$ and thus $\mathbb{N}_{\mid dk} \subseteq \mathbb{N}_{\mid kn}$). Hence, $\dfrac{1}{n}\sum\limits_{d\mid n} \mu\left(d\right) w_{F,dk}^{n/d} \in \mathbb{Q}\left[X_{\mathbb{N}_{\mid kn}}\right] \cap \mathbb{Z}\left[X_{\mathbb{N}_+}\right]$ (because $\dfrac{1}{n}\sum\limits_{d\mid n} \mu\left(d\right) w_{F,dk}^{n/d} \in \mathbb{Q}\left[X_{\mathbb{N}_{\mid kn}}\right]$ and $\dfrac{1}{n}\sum\limits_{d\mid n} \mu\left(d\right) w_{F,dk}^{n/d} \in \mathbb{Z}\left[X_{\mathbb{N}_+}\right]$).

Now, as was shown in the proof of Theorem 7, we have (7). Thus, $\dfrac{1}{n}\sum\limits_{d\mid n} \mu\left(d\right) w_{F,dk}^{n/d} \in \mathbb{Q}\left[X_{\mathbb{N}_{\mid kn}}\right] \cap \mathbb{Z}\left[X_{\mathbb{N}_+}\right]$ becomes $\dfrac{1}{n}\sum\limits_{d\mid n} \mu\left(d\right) w_{F,dk}^{n/d} \in \mathbb{Z}\left[X_{\mathbb{N}_{\mid kn}}\right]$. In other words, $\sum\limits_{d\mid n} \mu\left(d\right) w_{F,dk}^{n/d} \in n\mathbb{Z}\left[X_{\mathbb{N}_{\mid kn}}\right]$. This proves Theorem 16 **(a)**.

(b) The proof of Theorem 16 **(b)** is the same as the proof of Theorem 16 **(a)** that we have just done; we just have to replace every μ by ϕ and use Assertion $\mathcal{G}$ instead of Assertion $\mathcal{F}$.

(c) Assertion $\mathcal{H}$ of Theorem 1 states that every $n \in N$ satisfies

$$\sum_{i=1}^{n} \varphi_{n/\gcd(i,n)}\left(b_{\gcd(i,n)}\right) \in nA.$$

Since this assertion is satisfied, we thus have $\sum\limits_{i=1}^{n} \varphi_{n/\gcd(i,n)}\left(b_{\gcd(i,n)}\right) \in nA$ for every $n \in N$. Since

$$\begin{aligned}
\sum_{i=1}^{n} \varphi_{n/\gcd(i,n)}\left(b_{\gcd(i,n)}\right) &= \sum_{i=1}^{n} \underbrace{\varphi_{n/\gcd(i,n)}\left(\left(w_{F,k}^{\gcd(i,n)}\right)_{k\in\mathbb{N}_+}\right)}_{\substack{=\left(w_{F,n/\gcd(i,n)\cdot k}^{\gcd(i,n)}\right)_{k\in\mathbb{N}_+} \\ \left(\text{by the definition of } \varphi_{n/\gcd(i,n)}\right)}} \\
&\qquad \left(\text{since } b_{\gcd(i,n)} \text{ is defined as } \left(w_{F,k}^{\gcd(i,n)}\right)_{k\in\mathbb{N}_+}\right) \\
&= \sum_{i=1}^{n} \left(w_{F,n/\gcd(i,n)\cdot k}^{\gcd(i,n)}\right)_{k\in\mathbb{N}_+} = \left(\sum_{i=1}^{n} w_{F,n/\gcd(i,n)\cdot k}^{\gcd(i,n)}\right)_{k\in\mathbb{N}_+} \\
&\qquad \left(\text{since addition in } A \text{ is componentwise}\right),
\end{aligned}$$

this rewrites as $\left(\sum\limits_{i=1}^{n} w_{F,n/\gcd(i,n)\cdot k}^{\gcd(i,n)}\right)_{k\in\mathbb{N}_+} \in nA$. In other words, there exists a sequence $\left(v_k\right)_{k\in\mathbb{N}_+} \in A$ such that $\left(\sum\limits_{i=1}^{n} w_{F,n/\gcd(i,n)\cdot k}^{\gcd(i,n)}\right)_{k\in\mathbb{N}_+} = n\left(v_k\right)_{k\in\mathbb{N}_+}$. Thus, $\left(\sum\limits_{i=1}^{n} w_{F,n/\gcd(i,n)\cdot k}^{\gcd(i,n)}\right)_{k\in\mathbb{N}_+} = n\left(v_k\right)_{k\in\mathbb{N}_+} = \left(nv_k\right)_{k\in\mathbb{N}_+}$. Hence, for every $k \in \mathbb{N}_+$, we have $\sum\limits_{i=1}^{n} w_{F,n/\gcd(i,n)\cdot k}^{\gcd(i,n)} = nv_k \in$

$n\mathbb{Z}\left[X_{\mathbb{N}_+}\right]$. In other words, $\frac{1}{n}\sum\limits_{i=1}^{n} w_{F,n/\gcd(i,n)\cdot k}^{\gcd(i,n)} \in \mathbb{Z}\left[X_{\mathbb{N}_+}\right]$.

On the other hand, $\frac{1}{n}\sum\limits_{i=1}^{n} w_{F,n/\gcd(i,n)\cdot k}^{\gcd(i,n)} \in \mathbb{Q}\left[X_{\mathbb{N}_{|kn}}\right]$, since every $i \in \{1,2,...,n\}$ satisfies $w_{F,n/\gcd(i,n)\cdot k} \in \mathbb{Q}\left[X_{\mathbb{N}_{|n/\gcd(i,n)\cdot k}}\right] \subseteq \mathbb{Q}\left[X_{\mathbb{N}_{|kn}}\right]$ (since $(n/\gcd(i,n)) \mid n$ yields $n/\gcd(i,n)\cdot k \mid nk = kn$ and thus $\mathbb{N}_{|n/\gcd(i,n)\cdot k} \subseteq \mathbb{N}_{|kn}$). Hence, $\frac{1}{n}\sum\limits_{i=1}^{n} w_{F,n/\gcd(i,n)\cdot k}^{\gcd(i,n)} \in \mathbb{Q}\left[X_{\mathbb{N}_{|kn}}\right] \cap \mathbb{Z}\left[X_{\mathbb{N}_+}\right]$ (because $\frac{1}{n}\sum\limits_{i=1}^{n} w_{F,n/\gcd(i,n)\cdot k}^{\gcd(i,n)} \in \mathbb{Q}\left[X_{\mathbb{N}_{|kn}}\right]$ and $\frac{1}{n}\sum\limits_{i=1}^{n} w_{F,n/\gcd(i,n)\cdot k}^{\gcd(i,n)} \in \mathbb{Z}\left[X_{\mathbb{N}_+}\right]$). Due to (7), this becomes $\frac{1}{n}\sum\limits_{i=1}^{n} w_{F,n/\gcd(i,n)\cdot k}^{\gcd(i,n)} \in \mathbb{Z}\left[X_{\mathbb{N}_{|kn}}\right]$. In other words, $\sum\limits_{i=1}^{n} w_{F,n/\gcd(i,n)\cdot k}^{\gcd(i,n)} \in n\mathbb{Z}\left[X_{\mathbb{N}_{|kn}}\right]$. This proves Theorem 16 **(c)**.

We can now get Theorems 13 and 14 as particular cases of Theorems 15 and 16:

Proof of Theorem 13. We know that prad is a superradical map. Hence, we can apply Theorem 15 to $F = \mathrm{prad}$, and obtain the following result:

> **Theorem 15a.** Consider the polynomial ring $\mathbb{Z}\left[X_{\mathbb{N}_+}\right] = \mathbb{Z}\left[X_1, X_2, X_3, ...\right]$. Let A be the Abelian group $\left(\mathbb{Z}\left[X_{\mathbb{N}_+}\right]\right)^{\mathbb{N}_+}$ (this is the Abelian group of all sequences of elements of $\mathbb{Z}\left[X_{\mathbb{N}_+}\right]$, with componentwise addition and zero $(0)_{n\in\mathbb{N}_+}$).
>
> For every $n \in \mathbb{N}_+$, define an endomorphism $\varphi_n : A \to A$ of the group A as in Theorem 2.
>
> We define a family $(b_n)_{n\in\mathbb{N}_+} \in A^{\mathbb{N}_+}$ of elements of A by
>
> $$b_n = \left(w_{\mathrm{prad},k}^{n}\right)_{k\in\mathbb{N}_+} \qquad \text{for every } n \in \mathbb{N}_+.$$
>
> (Of course, this family $(b_n)_{n\in\mathbb{N}_+}$ is **not** the family $(b_n)_{n\in\mathbb{N}_+}$ from Theorem 2.)
>
> **(a)** The group A is torsionfree, and the endomorphisms φ_n satisfy (1) and (2).
>
> **(b)** The family $(b_n)_{n\in\mathbb{N}_+}$ satisfies the Assertions $\mathcal{C}$, $\mathcal{E}$, $\mathcal{E}'$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ of Theorem 1 for $N = \mathbb{N}_+$.

Now, Theorem 13 is obtained from Theorem 15a by replacing $w_{\mathrm{prad},k}$ by $\sqrt[\infty]{w}_k$. Since this replacement doesn't change the validity of this theorem (because

$$w_{\mathrm{prad},k} = \sqrt[\infty]{w}_k \qquad \text{(by (14), applied to } k \text{ instead of } n)$$

), this yields that Theorem 13 is equivalent to Theorem 15a. Thus, Theorem 13 holds (since we know that Theorem 15 holds).

Proof of Theorem 16. We know that prad is a superradical map. Hence, we can apply Theorem 16 to $F = \mathrm{prad}$.

(a) Let $n \in \mathbb{N}_+$ and $k \in \mathbb{N}_+$. We have $w_{\mathrm{prad},dk} = \sqrt[\infty]{w}_{dk}$ for every divisor d of n (by (14), applied to dk instead of n). Thus,

$$\sum_{d\mid n} \mu(d) \underbrace{\sqrt[\infty]{w}_{dk}}_{=w_{\mathrm{prad},dk}}^{n/d} = \sum_{d\mid n} \mu(d)\, w_{\mathrm{prad},dk}^{n/d} \in n\mathbb{Z}\left[X_{\mathbb{N}_{|kn}}\right]$$

(by Theorem 14 **(a)**, applied to $F = \operatorname{prad}$). This proves Theorem 16 **(a)**.

(b) Let $n \in \mathbb{N}_+$ and $k \in \mathbb{N}_+$. We have $w_{\operatorname{prad},dk} = \sqrt[\infty]{w}_{dk}$ for every divisor d of n (by (14), applied to dk instead of n). Thus,

$$\sum_{d|n} \phi(d) \underbrace{\sqrt[\infty]{w}_{dk}}_{=w_{\operatorname{prad},dk}}{}^{n/d} = \sum_{d|n} \phi(d)\, w_{\operatorname{prad},dk}^{n/d} \in n\mathbb{Z}\left[X_{\mathbb{N}_{|kn}}\right]$$

(by Theorem 14 **(b)**, applied to $F = \operatorname{prad}$). This proves Theorem 16 **(b)**.

(c) Let $n \in \mathbb{N}_+$ and $k \in \mathbb{N}_+$. We have $w_{\operatorname{prad},n/\gcd(i,n)\cdot k} = \sqrt[\infty]{w}_{n/\gcd(i,n)\cdot k}$ for every $i \in \{1, 2, ..., n\}$ (by (14), applied to $n/\gcd(i,n) \cdot k$ instead of n). Thus,

$$\sum_{i=1}^{n} \underbrace{\sqrt[\infty]{w}_{n/\gcd(i,n)\cdot k}}_{=w_{\operatorname{prad},n/\gcd(i,n)\cdot k}}{}^{\gcd(i,n)} = \sum_{i=1}^{n} w_{\operatorname{prad},n/\gcd(i,n)\cdot k}^{\gcd(i,n)} \in n\mathbb{Z}\left[X_{\mathbb{N}_{|kn}}\right]$$

(by Theorem 14 **(c)**, applied to $F = \operatorname{prad}$). This proves Theorem 16 **(c)**.

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.*

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

[4] Darij Grinberg, *Witt#5: Around the integrality criterion 9.93.*

[5] Darij Grinberg, *Witt#5c: The Chinese Remainder Theorem for Modules.*

[6] Darij Grinberg, *Witt#5d: Analoga of integrality criteria for radical Witt polynomials.*

[7] Darij Grinberg, *Witt#5e: Generalizing integrality theorems for ghost-Witt vectors.*