Witt vectors. Part 1

Michiel Hazewinkel
Sidenotes by Darij Grinberg

Witt#5d: Analoga of integrality criteria for radical Witt polynomials

[not completed, not proofread]

This note is about something I call "radical Witt polynomials" $\sqrt[\infty]{w}_n$. These polynomials are somewhat similar to the Witt polynomials w_n, and many of the theorems proven in [4] about the Witt polynomials w_n have analogues concerning these "radical Witt polynomials" $\sqrt[\infty]{w}_n$. We will formulate some of these analogues in this note. Most of these analogues (as well as the corresponding theorems about w_n) are particular cases of the corresponding properties of the so-called "F-Witt polynomials" (a common generalization of Witt polynomials w_n and "radical Witt polynomials" $\sqrt[\infty]{w}_n$) proven in [6], so the proofs will be simply references to [6]. However, some theorems about $\sqrt[\infty]{w}_n$ doesn't have an F-Witt counterpart and thus requires a separate proof; two such examples are Theorems 4' and 9' in this note.

I will keep the numbering of the results in this note consistent with the numbering of the results in [4] and [6], so that for instance Theorem i in this note will be the analogue of Theorem i in [4] and a particular case of Theorem i in [6] for as many i as possible.

First, let us introduce some notation[1]:

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). [2]. 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 $\mathbb{Z}[\Xi]$) [3]. (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.[4])

[1] All of the following nine definitions, except of Definitions 7, 8 and 9, are the same as the corresponding definitions in [4].

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

[3] 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 $\Xi^n = (X_0^n, X_1^n, X_2^n, ...; Y_0^n, Y_1^n, Y_2^n, ...; Z_0^n, Z_1^n, Z_2^n, ...)$.

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

Note that if Ξ is the empty family, then $\mathbb{Q}\left[\Xi\right]$ simply is the ring $\mathbb{Q}$, and $\mathbb{Z}\left[\Xi\right]$ 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 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 [5].

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

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 $P \in \mathbb{Z}\left[X_N\right]$, 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 $\mathbb{Z}\left[X_N\right]$ with a subring of $\mathbb{Z}\left[X_M\right]$. In particular, when $P \in \mathbb{Z}\left[X_N\right]$ 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 $P\left(x_1, x_2, x_3, ...\right)$ means $P\left((x_m)_{m \in N}\right)$.

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

[5] 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).

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

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

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 $\operatorname{rad} n \mid n$ [7]. The number $\operatorname{rad} n$ is the greatest squarefree divisor of n. Also notice that

$$p \mid \operatorname{rad} n \text{ for every } n \in \mathbb{N}_+ \text{ and every } p \in \operatorname{PF} n. \tag{1}$$

[8]

Definition 9. 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

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

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

$$\sqrt[\infty]{w}_n\left((x_k)_{k \in \mathbb{N}_{|n}}\right) = \sum_{d \mid n} (\operatorname{rad} d)\, x_d^{n/d}.$$

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 $\sqrt[\infty]{w}_n\left((x_k)_{k \in N}\right)$ means $\sqrt[\infty]{w}_n\left((x_k)_{k \in \mathbb{N}_{|n}}\right)$; in other words,

$$\sqrt[\infty]{w}_n\left((x_k)_{k \in N}\right) = \sum_{d \mid n} (\operatorname{rad} d)\, x_d^{n/d}.$$

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*.[9]

We start by recalling a property of primes and commutative rings:

[7] *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.

[8] *Proof of (1):* 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 (1).

[9] 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.

Theorem 1. Let A be a commutative ring with unity. Let M be an A-module. Let $N \in \mathbb{N}$. Let I_1, I_2, ..., I_N be N ideals of A such that $I_i + I_j = A$ for any two elements i and j of $\{1, 2, ..., N\}$ satisfying $i < j$. Then, $I_1 I_2 ... I_N \cdot M = I_1 M \cap I_2 M \cap ... \cap I_N M$.

This Theorem 1 is exactly the Theorem 1 of [4], so we are not proving this theorem here.

A trivial corollary from Theorem 1 that we will use is:

Corollary 2.[10] Let A be an Abelian group (written additively). Let $n \in \mathbb{N}_+$. Then, $(\operatorname{rad} n) A = \bigcap\limits_{p \in \operatorname{PF} n} (pA)$.

Proof of Corollary 2. Since $\operatorname{PF} n$ is a finite set, there exist $N \in \mathbb{N}$ and some pairwise distinct primes p_1, p_2, ..., p_N such that $\operatorname{PF} n = \{p_1, p_2, ..., p_N\}$. Thus, $\prod\limits_{i=1}^{N} p_i = \prod\limits_{p \in \operatorname{PF} n} p = \operatorname{rad} n$.

Define an ideal I_i of $\mathbb{Z}$ by $I_i = p_i \mathbb{Z}$ for every $i \in \{1, 2, ..., N\}$. Then, $I_i + I_j = \mathbb{Z}$ for any two elements i and j of $\{1, 2, ..., N\}$ satisfying $i < j$ (in fact, the integers p_i and p_j are coprime[11], and thus, by Bezout's theorem, there exist integers α and β such that $1 = p_i \alpha + p_j \beta$ in $\mathbb{Z}$, and therefore $1 = \underbrace{p_i \alpha}_{\in p_i \mathbb{Z} = I_i} + \underbrace{p_j \beta}_{\in p_j \mathbb{Z} = I_j} \in I_i + I_j$ in $\mathbb{Z}$, and thus $I_i + I_j = \mathbb{Z}$). Hence, Theorem 1 (applied to $\mathbb{Z}$ and A instead of A and M, respectively) yields $I_1 I_2 ... I_N \cdot A = I_1 A \cap I_2 A \cap ... \cap I_N A$. Since

$$I_1 I_2 ... I_N \cdot A = \prod_{i=1}^{N} \underbrace{I_i}_{= p_i \mathbb{Z}} \cdot A = \prod_{i=1}^{N} (p_i \mathbb{Z}) \cdot A = \underbrace{\left(\prod_{i=1}^{N} p_i \right)}_{= \operatorname{rad} n} \mathbb{Z} \cdot A = (\operatorname{rad} n) \mathbb{Z} \cdot A = (\operatorname{rad} n) A$$

and

$$I_1 A \cap I_2 A \cap ... \cap I_N A = \bigcap_{i=1}^{N} (I_i A) = \bigcap_{i=1}^{N} (p_i \mathbb{Z} \cdot A) = \bigcap_{i=1}^{N} (p_i A) = \bigcap_{p \in \operatorname{PF} n} (pA)$$

(since $\operatorname{PF} n = \{p_1, p_2, ..., p_N\}$), this becomes $(\operatorname{rad} n) A = \bigcap\limits_{p \in \operatorname{PF} n} (pA)$. Corollary 2 is thus proven.

Now comes our first theorem about radical Witt polynomials - the analogue of Theorem 4 in [4]:

Theorem 4. Let N be a nest. Let A be a commutative ring with unity. For every $p \in \mathbb{P} \cap N$, let $\varphi_p : A \to A$ be an endomorphism of the ring A such that

$$\left(\varphi_p (a) \equiv a^p \bmod pA \text{ holds for every } a \in A \text{ and } p \in \mathbb{P} \cap N \right). \qquad (2)$$

[10] This is an analogue of Corollary 2 in [4] (and can actually be easily derived from that Corollary 2 in [4], but here we will prove it differently).

[11] since p_i and p_j are distinct primes (because $i < j$ and since the primes p_1, p_2, ..., p_N are pairwise distinct)

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

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

$$\varphi_p\left(b_{n/p}\right) \equiv b_n \bmod pA. \tag{3}$$

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

$$\left(b_n = \sqrt[\infty]{w}_n\left((x_k)_{k \in N}\right) \text{ for every } n \in N\right).$$

We will give two proofs of this theorem. First, let us make a definition that we will use in the first proof:

Definition 10. **(a)** We are going to use the notion of *pseudo-monotonous maps*. For the definition of these maps, we refer to Definition 9 in [6]. All we need to know is that pseudo-monotonous maps are a particular kind of maps from $\mathbb{P} \times \mathbb{N}$ to $\mathbb{N}$, and each such map leads to a certain generalization of Witt polynomials. Some properties of these maps were studied in [6].

(b) For any pseudo-monotonous map $F : \mathbb{P} \times \mathbb{N} \to \mathbb{N}$, we define a map $\widetilde{F} : \mathbb{N}_+ \to \mathbb{N}_+$ by

$$\left(\widetilde{F}(n) = \prod_{p \in \operatorname{PF} n} p^{F(p, v_p(n))}\right).$$

(c) We define a map $\operatorname{prad} : \mathbb{P} \times \mathbb{N} \to \mathbb{N}$ by

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

Then, prad is a pseudo-monotonous map (as proven in [6], Example 2) and satisfies $\widetilde{\operatorname{prad}} = \operatorname{rad}$ (again, this is proven in [6], Example 2).

Notice that

$$p^{\operatorname{prad}(p, v_p(n))} = p \qquad \text{for every } n \in \mathbb{N}_+ \text{ and every } p \in \operatorname{PF} n. \tag{4}$$

[12]

(d) Let $F : \mathbb{P} \times \mathbb{N} \to \mathbb{N}$ be a pseudo-monotonous map. For any $n \in \mathbb{N}_+$, we define a polynomial $w_{F,n} \in \mathbb{Z}\left[X_{\mathbb{N}_{|n}}\right]$ by

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

[12] *Proof of (4):* Let $n \in \mathbb{N}_+$ and let $p \in \operatorname{PF} n$. Since $p \in \operatorname{PF} n$, we have $p \mid n$ and thus $v_p(n) > 0$. By the definition of $\operatorname{prad}(p, v_p(n))$, we have $\operatorname{prad}(p, v_p(n)) = \begin{cases} 0, & \text{if } v_p(n) = 0; \\ 1, & \text{if } v_p(n) > 0 \end{cases} = 1$ (since $v_p(n) > 0$). Thus, $p^{\operatorname{prad}(p, v_p(n))} = p^1 = p$. This proves (4).

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*.

We have

$$w_{\operatorname{prad},n} = \sqrt[\infty]{w_n} \qquad \text{for every } n \in \mathbb{N}_+. \tag{5}$$

(This is proven in [6], Example 2.)

Note that Definition 10 will never be used in stating theorems, but only in proving them (or, more precisely, in deducing them from results in [6]).

Proof of Theorem 4. Let us use the conventions of Definition 10. We know that prad is a pseudo-monotonous map. Hence, applying Theorem 4 in [6] to $F = \operatorname{prad}$, we conclude[13] that the following two assertions $\mathcal{C}_{\operatorname{prad}}$ and $\mathcal{D}_{\operatorname{prad}}$ are equivalent:

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

$$\varphi_p\left(b_{n/p}\right) \equiv b_n \bmod p^{\operatorname{prad}(p, v_p(n))} A.$$

Assertion $\mathcal{D}_{\operatorname{prad}}$: There exists a family $(x_n)_{n \in N} \in A^N$ of elements of A such that

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

But Assertion $\mathcal{C}_{\operatorname{prad}}$ is equivalent to Assertion $\mathcal{C}$ (since (4) yields $p^{\operatorname{prad}(p, v_p(n))} = p$ for every $n \in N$ and every $p \in \operatorname{PF} n$). Also, Assertion $\mathcal{D}_{\operatorname{prad}}$ is equivalent to Assertion $\mathcal{D}$ (because (5) yields $w_{\operatorname{prad},n} = \sqrt[\infty]{w_n}$ for every $n \in N$). So altogether we have proven the equivalences $\mathcal{C}_{\operatorname{prad}} \Longleftrightarrow \mathcal{C}$, $\mathcal{C}_{\operatorname{prad}} \Longleftrightarrow \mathcal{D}_{\operatorname{prad}}$ and $\mathcal{D}_{\operatorname{prad}} \Longleftrightarrow \mathcal{D}$. Consequently, all four assertions $\mathcal{C}$, $\mathcal{C}_{\operatorname{prad}}$, $\mathcal{D}_{\operatorname{prad}}$ and $\mathcal{D}$ are equivalent, so that, in particular, $\mathcal{C} \Longleftrightarrow \mathcal{D}$. Thus, Theorem 4 is proven.

We are going to prove many more theorems similarly to how we just verified Theorem 4. However, in the case of Theorem 4, we can actually do better: The following generalization of Theorem 4 provides a conclusion which is easily seen to be equivalent to that of Theorem 4, without requiring the endomorphisms φ_p to exist:

Theorem 4'. Let N be a nest. Let A be a commutative ring with unity.

Let $(b_n)_{n \in N} \in A^N$ be a family of elements of A. Then, the following two assertions $\mathcal{C}_{4'}$ and $\mathcal{D}$ are equivalent:

Assertion $\mathcal{C}_{4'}$: Every $n \in N$ and every $p \in \operatorname{PF} n$ satisfies

$$b_{n/p}^p \equiv b_n \bmod pA. \tag{6}$$

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

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

[13] We rename the assertions $\mathcal{C}$ and $\mathcal{D}$ of Theorem 4 in [6] as $\mathcal{C}_{\operatorname{prad}}$ and $\mathcal{D}_{\operatorname{prad}}$, respectively, because we have already used up the letters $\mathcal{C}$ and $\mathcal{D}$ for two slightly different (even if equivalent) assertions.

Note that the Assertion $\mathcal{D}$ of Theorem 4' is identical with the Assertion $\mathcal{D}$ of Theorem 4; this is why we labelled both assertions by the same letter.

Of course, Theorem 4' yields Theorem 4, because if endomorphisms $\varphi_p : A \to A$ satisfying (2) exist, then $\varphi_p(b_{n/p})$ can be replaced by $b_{n/p}^p$ in Assertion $\mathcal{C}$ (since (2) (applied to $a = b_{n/p}$) yields $\varphi_p(b_{n/p}) \equiv b_{n/p}^p \bmod pA$), and therefore Assertion $\mathcal{C}$ is equivalent to Assertion $\mathcal{C}_{4'}$.

Proof of Theorem 4'. Our goal is to show that Assertion $\mathcal{C}_{4'}$ is equivalent to Assertion $\mathcal{D}$. We will achieve this by proving the implications $\mathcal{D} \Longrightarrow \mathcal{C}_{4'}$ and $\mathcal{C}_{4'} \Longrightarrow \mathcal{D}$.

Proof of the implication $\mathcal{D} \Longrightarrow \mathcal{C}_{4'}$: Assume that Assertion $\mathcal{D}$ holds. That is, there exists a family $(x_n)_{n \in N} \in A^N$ of elements of A such that

$$\left(b_n = \sqrt[\infty]{w}_n\left((x_k)_{k \in N}\right) \text{ for every } n \in N\right). \tag{7}$$

We want to prove that Assertion $\mathcal{C}_{4'}$ holds, i. e., that every $n \in N$ and every $p \in \operatorname{PF} n$ satisfies (6). Let $n \in N$ and $p \in \operatorname{PF} n$. Then, $p \mid n$, so that $n/p \in \mathbb{N}_+$, and thus $n/p \in N$ (since n/p is a divisor of n, and every divisor of n lies in N [14]). Thus, applying (7) to n/p instead of n yields $b_{n/p} = \sqrt[\infty]{w}_{n/p}\left((x_k)_{k \in N}\right)$. But $\sqrt[\infty]{w}_{n/p}\left((x_k)_{k \in N}\right) = \sum\limits_{d \mid (n/p)} (\operatorname{rad} d)\, x_d^{(n/p)/d}$ and $\sqrt[\infty]{w}_n\left((x_k)_{k \in N}\right) = \sum\limits_{d \mid n} (\operatorname{rad} d)\, x_d^{n/d}$. Now, (7) yields

$$b_n = \sqrt[\infty]{w}_n\left((x_k)_{k \in N}\right) = \sum_{d \mid n} (\operatorname{rad} d)\, x_d^{n/d} = \sum_{\substack{d \mid n; \\ d \mid (n/p)}} (\operatorname{rad} d)\, x_d^{n/d} + \sum_{\substack{d \mid n; \\ d \nmid (n/p)}} (\operatorname{rad} d)\, x_d^{n/d}. \tag{8}$$

But for any divisor d of n, the assertions $d \nmid (n/p)$ and $p^{v_p(n)} \mid d$ are equivalent[15]. Hence, every divisor d of n which satisfies $d \nmid (n/p)$ must satisfy $\operatorname{rad} d \equiv 0 \bmod pA$ [16]. Thus,

$$\sum_{\substack{d \mid n; \\ d \nmid (n/p)}} \underbrace{(\operatorname{rad} d)}_{\equiv 0 \bmod pA} x_d^{n/d} \equiv \sum_{\substack{d \mid n; \\ d \nmid (n/p)}} 0 x_d^{n/d} = 0 \bmod pA.$$

[14] because $n \in N$ and because N is a nest

[15] In fact, we have the following chain of equivalences:

$$\begin{aligned}
(d \nmid (n/p)) &\iff \left(\frac{n/p}{d} \notin \mathbb{Z}\right) \iff \left(\frac{n/d}{p} \notin \mathbb{Z}\right) \qquad \left(\text{since } \frac{n/p}{d} = \frac{n/d}{p}\right) \\
&\iff (p \nmid (n/d)) \qquad \text{(here we use that } n/d \in \mathbb{Z}\text{, since } d \mid n\text{)} \\
&\iff (v_p(n/d) = 0) \Longleftarrow (v_p(n/d) \leq 0) \qquad \text{(since } v_p(n/d) \geq 0\text{, because } n/d \in \mathbb{Z}\text{)} \\
&\iff (v_p(n) - v_p(d) \leq 0) \qquad \text{(since } v_p(n/d) = v_p(n) - v_p(d)\text{)} \\
&\iff (v_p(n) \leq v_p(d)) \iff \left(p^{v_p(n)} \mid d\right).
\end{aligned}$$

[16] In fact, let d be a divisor of n satisfying $d \nmid (n/p)$. We have already proven that the assertions $d \nmid (n/p)$ and $p^{v_p(n)} \mid d$ are equivalent. Since we know that $d \nmid (n/p)$, we thus have $p^{v_p(n)} \mid d$. Since $p \in \operatorname{PF} n$, we have $p \mid n$ and thus $v_p(n) \geq 1$, so that $p \mid p^{v_p(n)} \mid d$, so that $p \in \operatorname{PF} d$ (because $p \in \operatorname{PF} n$, and thus p is a prime). Hence, (1) (applied to d instead of n) yields $p \mid \operatorname{rad} d$, and thus $\operatorname{rad} d \equiv 0 \bmod pA$.

Thus, (8) becomes

$$b_n = \underbrace{\sum_{\substack{d \mid n; \\ d \mid (n/p)}} (\operatorname{rad} d)\, x_d^{n/d}}_{= \sum\limits_{d \mid (n/p)}} + \underbrace{\sum_{\substack{d \mid n; \\ d \nmid (n/p)}} (\operatorname{rad} d)\, x_d^{n/d}}_{\equiv 0 \bmod pA} \equiv \sum_{d \mid (n/p)} (\operatorname{rad} d)\, x_d^{n/d} + 0$$

$$= \sum_{d \mid (n/p)} (\operatorname{rad} d)\, x_d^{n/d} \bmod pA. \tag{9}$$

On the other hand,

$$b_{n/p} = \sqrt[\infty]{w}_{n/p}\left((x_k)_{k \in N}\right) = \sum_{d \mid (n/p)} (\operatorname{rad} d)\, x_d^{(n/p)/d} \qquad \text{yields}$$

$$b_{n/p}^p = \left(\sum_{d \mid (n/p)} (\operatorname{rad} d)\, x_d^{(n/p)/d}\right)^p \equiv \sum_{d \mid (n/p)} \left((\operatorname{rad} d)\, x_d^{(n/p)/d}\right)^p$$

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

$$= \sum_{d \mid (n/p)} \underbrace{(\operatorname{rad} d)^p}_{\substack{\equiv \operatorname{rad} d \bmod pA \\ \text{(since } (\operatorname{rad} d)^p \equiv \operatorname{rad} d \bmod p\mathbb{Z} \text{ by Fermat's Little Theorem)}}} \underbrace{\left(x_d^{(n/p)/d}\right)^p}_{= x_d^{(n/p)/d \cdot p} = x_d^{n/d}} \equiv \sum_{d \mid (n/p)} (\operatorname{rad} d)\, x_d^{n/d} \equiv b_n \bmod pA$$

(by (9)). This proves (6), and thus Assertion $\mathcal{C}_{4'}$ is proven. We have therefore shown the implication $\mathcal{D} \Longrightarrow \mathcal{C}_{4'}$.

Proof of the implication $\mathcal{C}_{4'} \Longrightarrow \mathcal{D}$: Assume that Assertion $\mathcal{C}_{4'}$ holds. That is, every $n \in N$ and every $p \in \operatorname{PF} n$ satisfies (6).

We will now recursively construct a family $(x_n)_{n \in N} \in A^N$ of elements of A which satisfies the equation

$$b_m = \sum_{d \mid m} (\operatorname{rad} d)\, x_d^{m/d} \tag{10}$$

for every $m \in N$.

In fact, let $n \in N$, and assume that we have already constructed an element $x_m \in A$ for every $m \in N \cap \{1, 2, ..., n-1\}$ in such a way that (10) holds for every $m \in N \cap \{1, 2, ..., n-1\}$. Now, we must construct an element $x_n \in A$ such that (10) is also satisfied for $m = n$.

Our assumption says that we have already constructed an element $x_m \in A$ for every $m \in N \cap \{1, 2, ..., n-1\}$. In particular, this yields that we have already constructed an element $x_d \in A$ for every divisor d of n satisfying $d \neq n$ (in fact, every such divisor d of n must lie in N [17] and in $\{1, 2, ..., n-1\}$ [18], and thus it satisfies $d \in N \cap \{1, 2, ..., n-1\}$).

Let $p \in \operatorname{PF} n$. Then, $p \mid n$, so that $n/p \in \mathbb{N}_+$, and thus $n/p \in N$ (since n/p is a divisor of n, and every divisor of n lies in N [19]). Besides, $n/p \in \{1, 2, ..., n-1\}$.

[17] because $n \in N$ and because N is a nest

[18] because d is a divisor of n satisfying $d \neq n$

[19] because $n \in N$ and because N is a nest

Hence, $n/p \in N \cap \{1, 2, ..., n-1\}$. Since (by our assumption) the equation (10) holds for every $m \in N \cap \{1, 2, ..., n-1\}$, we can thus conclude that (10) holds for $m = n/p$. In other words, $b_{n/p} = \sum\limits_{d \mid (n/p)} (\operatorname{rad} d)\, x_d^{(n/p)/d}$. From this equation, we can conclude (by the same reasoning as in the proof of the implication $\mathcal{D} \Longrightarrow \mathcal{C}_{4'}$) that

$$b_{n/p}^p \equiv \sum_{d \mid (n/p)} (\operatorname{rad} d)\, x_d^{n/d} \bmod pA.$$

Comparing this with (6), we obtain

$$\sum_{d \mid (n/p)} (\operatorname{rad} d)\, x_d^{n/d} \equiv b_n \bmod pA. \tag{11}$$

However, every divisor d of n which satisfies $d \nmid (n/p)$ must satisfy $\operatorname{rad} d \equiv 0 \bmod pA$ [20]. Thus,

$$\sum_{\substack{d \mid n; \\ d \nmid (n/p); \\ d \neq n}} \underbrace{(\operatorname{rad} d)}_{\equiv 0 \bmod pA}\, x_d^{n/d} \equiv \sum_{\substack{d \mid n; \\ d \nmid (n/p); \\ d \neq n}} 0 x_d^{n/d} = 0 \bmod pA.$$

Hence,

$$\begin{aligned}
&\sum_{\substack{d \mid n; \\ d \neq n}} (\operatorname{rad} d)\, x_d^{n/d} \\
&= \underbrace{\sum_{\substack{d \mid n; \\ d \nmid (n/p); \\ d \neq n}} (\operatorname{rad} d)\, x_d^{n/d}}_{\equiv 0 \bmod pA} + \sum_{\substack{d \mid n; \\ d \mid (n/p); \\ d \neq n}} (\operatorname{rad} d)\, x_d^{n/d} \equiv \sum_{\substack{d \mid n; \\ d \mid (n/p); \\ d \neq n}} (\operatorname{rad} d)\, x_d^{n/d} = \underbrace{\sum_{\substack{d \mid n; \\ d \mid (n/p)}}}_{= \sum\limits_{d \mid (n/p)}} (\operatorname{rad} d)\, x_d^{n/d} \\
&\qquad \left(\begin{array}{c} \text{since for any divisor } d \text{ of } n, \text{ the assertions } (d \mid (n/p) \text{ and } d \neq n) \text{ and } d \mid (n/p) \\ \text{are equivalent (because if } d \mid (n/p), \text{ then } d \neq n \text{ (since } n \nmid (n/p)\text{)}) \end{array} \right) \\
&= \sum_{d \mid (n/p)} (\operatorname{rad} d)\, x_d^{n/d} \equiv b_n \bmod pA \qquad \text{(by (11))}.
\end{aligned}$$

In other words,

$$b_n - \sum_{\substack{d \mid n; \\ d \neq n}} (\operatorname{rad} d)\, x_d^{n/d} \in pA.$$

This relation holds for every $p \in \operatorname{PF} n$. Thus,

$$b_n - \sum_{\substack{d \mid n; \\ d \neq n}} (\operatorname{rad} d)\, x_d^{n/d} \in \bigcap_{p \in \operatorname{PF} n} (pA) = (\operatorname{rad} n)\, A \qquad \text{(by Corollary 2)}.$$

Hence, there exists an element x_n of A that satisfies $b_n - \sum\limits_{\substack{d \mid n; \\ d \neq n}} (\operatorname{rad} d)\, x_d^{n/d} = (\operatorname{rad} n)\, x_n$.

[20] This has already been proven during our proof of the implication $\mathcal{D} \Longrightarrow \mathcal{C}_{4'}$.

Fix such an x_n. We now claim that this element x_n satisfies (10) for $m = n$. In fact,

$$\sum_{d|n} (\operatorname{rad} d)\, x_d^{n/d} = \sum_{\substack{d|n;\\ d\neq n}} (\operatorname{rad} d)\, x_d^{n/d} + \underbrace{\sum_{\substack{d|n;\\ d=n}} (\operatorname{rad} d)\, x_d^{n/d}}_{=(\operatorname{rad} n) x_n^{n/n} = (\operatorname{rad} n) x_n^1 = (\operatorname{rad} n) x_n} = \sum_{\substack{d|n;\\ d\neq n}} (\operatorname{rad} d)\, x_d^{n/d} + (\operatorname{rad} n)\, x_n = b_n$$

(since $b_n - \sum\limits_{\substack{d|n;\\ d\neq n}} (\operatorname{rad} d)\, x_d^{n/d} = (\operatorname{rad} n)\, x_n$). Hence, (10) is satisfied for $m = n$. This shows that we can recursively construct a family $(x_n)_{n\in N} \in A^N$ of elements of A which satisfies the equation (10) for every $m \in N$. Therefore, this family satisfies

$$\begin{aligned} b_n &= \sum_{d|n} (\operatorname{rad} d)\, x_d^{n/d} \qquad \text{(by (10), applied to } m = n\text{)} \\ &= \sqrt[\infty]{w}_n \left((x_k)_{k\in N} \right) \end{aligned}$$

for every $n \in N$. So we have proven that there exists a family $(x_n)_{n\in N} \in A^N$ which satisfies $b_n = \sqrt[\infty]{w}_n \left((x_k)_{k\in N} \right)$ for every $n \in N$. In other words, we have proven Assertion $\mathcal{D}$. Thus, the implication $\mathcal{C}_{4'} \Longrightarrow \mathcal{D}$ is proven.

Now that both implications $\mathcal{D} \Longrightarrow \mathcal{C}_{4'}$ and $\mathcal{C}_{4'} \Longrightarrow \mathcal{D}$ are verified, we conclude the equivalence $\mathcal{C}_{4'} \Longleftrightarrow \mathcal{D}$. Thus, Theorem 4' is proven. With it, Theorem 4 is proven a second time (because we have shown that Theorem 4' yields Theorem 4).

Next, we will show a result similar to Theorem 4[21]:

Theorem 5. Let N be a nest. Let A be an Abelian group (written additively). For every $n \in N$, let $\varphi_n : A \to A$ be an endomorphism of the group A such that

$$(\varphi_1 = \mathrm{id}) \qquad \text{and} \tag{12}$$

$$(\varphi_n \circ \varphi_m = \varphi_{nm} \text{ for every } n \in N \text{ and every } m \in N \text{ satisfying } nm \in N)\,. \tag{13}$$

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

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

$$\varphi_p (b_{n/p}) \equiv b_n \bmod pA. \tag{14}$$

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

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

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

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

[21]Later, we will unite it with Theorem 4 into one big theorem - whose conditions, however, will include the conditions of both Theorems 4 and 5, so it does not replace Theorems 4 and 5.

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

$$\sum_{d|n} \phi(d)\, \varphi_d(b_{n/d}) \in (\operatorname{rad} n)\, A.$$

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

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

Remark: Here, μ denotes the Möbius function $\mu : \mathbb{N}_+ \to \mathbb{Z}$ defined by

$$\mu(n) = \begin{cases} (-1)^{|\operatorname{PF} n|}, & \text{if } (v_p(n) \leq 1 \text{ for every } p \in \operatorname{PF} n) \\ 0, & \text{otherwise} \end{cases}. \tag{15}$$

Besides, ϕ denotes the Euler phi function $\phi : \mathbb{N}_+ \to \mathbb{Z}$ defined by

$$\phi(n) = |\{m \in \{1, 2, ..., n\} \mid m \perp n\}|.$$

Proof of Theorem 5. Let us use the conventions of Definition 10. We know that prad is a pseudo-monotonous map. Hence, applying Theorem 5 in [6] to $F = \operatorname{prad}$, we conclude[22] that the following five assertions $\mathcal{C}_{\operatorname{prad}}$, $\mathcal{E}_{\operatorname{prad}}$, $\mathcal{F}_{\operatorname{prad}}$, $\mathcal{G}_{\operatorname{prad}}$ and $\mathcal{H}_{\operatorname{prad}}$ are equivalent:

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

$$\varphi_p(b_{n/p}) \equiv b_n \bmod p^{\operatorname{prad}(p, v_p(n))} A.$$

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

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

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

$$\sum_{d|n} \mu(d)\, \varphi_d(b_{n/d}) \in \widetilde{\operatorname{prad}}(n)\, A.$$

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

$$\sum_{d|n} \phi(d)\, \varphi_d(b_{n/d}) \in \widetilde{\operatorname{prad}}(n)\, A.$$

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

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

[22] We rename the assertions $\mathcal{C}$, $\mathcal{E}$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ of Theorem 5 in [6] as $\mathcal{C}_{\operatorname{prad}}$, $\mathcal{E}_{\operatorname{prad}}$, $\mathcal{F}_{\operatorname{prad}}$, $\mathcal{G}_{\operatorname{prad}}$ and $\mathcal{H}_{\operatorname{prad}}$, respectively, because we have already used up the letters $\mathcal{C}$, $\mathcal{E}$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ for five slightly different (even if equivalent) assertions.

Now, for every $n \in N$ and every $p \in \operatorname{PF} n$, we have $p^{\operatorname{prad}(p, v_p(n))} = p$ (by (4)). Hence, Assertion $\mathcal{C}_{\operatorname{prad}}$ is equivalent to Assertion $\mathcal{C}$. Besides, Assertion $\mathcal{E}_{\operatorname{prad}}$ is equivalent to Assertion $\mathcal{E}$ (because the equality $\widetilde{\operatorname{prad}} = \operatorname{rad}$ (which we know) yields $\widetilde{\operatorname{prad}}(d) = \operatorname{rad}(d) = \operatorname{rad} d$). Also, Assertion $\mathcal{F}_{\operatorname{prad}}$ is equivalent to Assertion $\mathcal{F}$ (because $\widetilde{\operatorname{prad}} = \operatorname{rad}$ yields $\widetilde{\operatorname{prad}}(n) = \operatorname{rad}(n) = \operatorname{rad} n$); besides, Assertion $\mathcal{G}_{\operatorname{prad}}$ is equivalent to Assertion $\mathcal{G}$ (for the same reason). Finally, Assertion $\mathcal{H}_{\operatorname{prad}}$ is equivalent to Assertion $\mathcal{H}$ (for the same reason). So altogether we have proven the equivalences $\mathcal{C}_{\operatorname{prad}} \Longleftrightarrow \mathcal{C}$, $\mathcal{E}_{\operatorname{prad}} \Longleftrightarrow \mathcal{E}$, $\mathcal{F}_{\operatorname{prad}} \Longleftrightarrow \mathcal{F}$, $\mathcal{G}_{\operatorname{prad}} \Longleftrightarrow \mathcal{G}$, $\mathcal{H}_{\operatorname{prad}} \Longleftrightarrow \mathcal{H}$ and $\mathcal{C}_{\operatorname{prad}} \Longleftrightarrow \mathcal{E}_{\operatorname{prad}} \Longleftrightarrow \mathcal{F}_{\operatorname{prad}} \Longleftrightarrow \mathcal{G}_{\operatorname{prad}} \Longleftrightarrow \mathcal{H}_{\operatorname{prad}}$. From this we can conclude that all assertions $\mathcal{C}$, $\mathcal{E}$, $\mathcal{F}$, $\mathcal{G}$, $\mathcal{H}$, $\mathcal{C}_{\operatorname{prad}}$, $\mathcal{E}_{\operatorname{prad}}$, $\mathcal{F}_{\operatorname{prad}}$, $\mathcal{G}_{\operatorname{prad}}$ and $\mathcal{H}_{\operatorname{prad}}$ are equivalent, so that, in particular, the assertions $\mathcal{C}$, $\mathcal{E}$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ are equivalent. Thus, Theorem 5 is proven.

We can slightly extend Theorem 5 if we require our group A to be *torsionfree*. First, the definition:

Definition 11. 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.

(Note that in [1], Hazewinkel calls torsionfree rings "rings of characteristic zero" - at least, if I understand him right, because he never defines what he means by "ring of characteristic zero".)

Now, here comes the extension of Theorem 5:

Theorem 7. 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 (12) and (13) hold.

Let $(b_n)_{n \in N} \in A^N$ be a family of elements of A. Then, the six assertions $\mathcal{C}$, $\mathcal{E}$, $\mathcal{E}'$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ are equivalent, where the assertions $\mathcal{C}$, $\mathcal{E}$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ are the ones stated in Theorem 5, and the assertion $\mathcal{E}'$ is the following one:

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

$$\left(b_n = \sum_{d \mid n} (\operatorname{rad} d)\, \varphi_{n/d}(y_d) \text{ for every } n \in N \right). \tag{16}$$

Obviously, most of Theorem 7 is already proven. The only thing we have to add is the following easy observation:

Lemma 8. Under the conditions of Theorem 7, there exists *at most one* family $(y_n)_{n \in N} \in A^N$ of elements of A satisfying (16).

Proof of Lemma 8. Let us use the conventions of Definition 10. We know that prad is a pseudo-monotonous map. Hence, applying Lemma 8 in [6] to $F = \operatorname{prad}$, we conclude that there exists *at most one* family $(y_n)_{n \in N} \in A^N$ of elements of A satisfying

$$\left(b_n = \sum_{d \mid n} \widetilde{\operatorname{prad}}(d)\, \varphi_{n/d}(y_d) \text{ for every } n \in N \right). \tag{17}$$

But since (17) is equivalent to (16) (because $\widetilde{\operatorname{prad}} = \operatorname{rad}$ and therefore $\widetilde{\operatorname{prad}}\,(d) = \operatorname{rad}(d) = \operatorname{rad} d$), this result can be rewritten as follows: There exists *at most one* family $(y_n)_{n\in N} \in A^N$ of elements of A satisfying (16). Hence, Lemma 8 is proven.

Now the proof of Theorem 7 is trivial:

Proof of Theorem 7. Theorem 5 yields that the five assertions $\mathcal{C}$, $\mathcal{E}$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ are equivalent. In other words, $\mathcal{C} \Longleftrightarrow \mathcal{E} \Longleftrightarrow \mathcal{F} \Longleftrightarrow \mathcal{G} \Longleftrightarrow \mathcal{H}$. Besides, it is obvious that $\mathcal{E}' \Longrightarrow \mathcal{E}$. It remains to prove the implication $\mathcal{E} \Longrightarrow \mathcal{E}'$.

Assume that Assertion $\mathcal{E}$ holds. In other words, assume that there exists a family $(y_n)_{n\in N} \in A^N$ of elements of A satisfying (16). According to Lemma 8, there exists *at most one* such family. Hence, there exists *one and only one* family $(y_n)_{n\in N} \in A^N$ of elements of A satisfying (16). In other words, Assertion $\mathcal{E}'$ holds. Hence, we have proven the implication $\mathcal{E} \Longrightarrow \mathcal{E}'$. Together with $\mathcal{E}' \Longrightarrow \mathcal{E}$, this yields $\mathcal{E} \Longleftrightarrow \mathcal{E}'$. Combining this with $\mathcal{C} \Longleftrightarrow \mathcal{E} \Longleftrightarrow \mathcal{F} \Longleftrightarrow \mathcal{G} \Longleftrightarrow \mathcal{H}$, we see that all six assertions $\mathcal{C}$, $\mathcal{E}$, $\mathcal{E}'$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ are equivalent. This proves Theorem 7.

Just as Theorem 7 strengthened Theorem 5 in the case of a torsionfree A, we can strengthen Theorem 4 in this case as well:

> **Theorem 9.** Let N be a nest. Let A be a torsionfree commutative ring with unity. For every $p \in \mathbb{P} \cap N$, let $\varphi_p : A \to A$ be an endomorphism of the ring A such that (2) holds.
>
> Let $(b_n)_{n\in N} \in A^N$ be a family of elements of A. Then, the three assertions $\mathcal{C}$, $\mathcal{D}$ and $\mathcal{D}'$ are equivalent, where the assertions $\mathcal{C}$ and $\mathcal{D}$ are the ones stated in Theorem 4, and the assertion $\mathcal{D}'$ is the following one:
>
> *Assertion $\mathcal{D}'$:* There exists *one and only one* family $(x_n)_{n\in N} \in A^N$ of elements of A such that
>
> $$\left(b_n = \sqrt[\infty]{w}_n\left((x_k)_{k\in N}\right) \text{ for every } n \in N\right). \tag{18}$$

Again, having proven Theorem 4, the only thing we need to do here is checking the following fact:

> **Lemma 10.** Let N be a nest. Let A be a torsionfree commutative ring with unity. Let $(b_n)_{n\in N} \in A^N$ be a family of elements of A. Then, there exists *at most one* family $(x_n)_{n\in N} \in A^N$ of elements of A satisfying (18).

Proof of Lemma 10. Let us use the conventions of Definition 10. We know that prad is a pseudo-monotonous map. Hence, applying Lemma 10 in [6] to $F = \operatorname{prad}$, we conclude that there exists *at most one* family $(x_n)_{n\in N} \in A^N$ of elements of A satisfying

$$\left(b_n = w_{\operatorname{prad},n}\left((x_k)_{k\in N}\right) \text{ for every } n \in N\right). \tag{19}$$

But since (19) is equivalent to (18) (because every $n \in N$ satisfies $w_{\operatorname{prad},n} = \sqrt[\infty]{w}_n$), this result can be rewritten as follows: There exists *at most one* family $(x_n)_{n\in N} \in A^N$ of elements of A satisfying (18). Hence, Lemma 10 is proven.

Proving Theorem 9 now is immediate:

Proof of Theorem 9. Theorem 4 yields that the two assertions $\mathcal{C}$ and $\mathcal{D}$ are equivalent. In other words, $\mathcal{C} \Longleftrightarrow \mathcal{D}$. Besides, it is obvious that $\mathcal{D}' \Longrightarrow \mathcal{D}$. It remains to prove the implication $\mathcal{D} \Longrightarrow \mathcal{D}'$.

Assume that Assertion $\mathcal{D}$ holds. In other words, assume that there exists a family $(x_n)_{n\in N} \in A^N$ of elements of A satisfying (18). According to Lemma 10, there exists *at most one* such family. Hence, there exists *one and only one* family $(x_n)_{n\in N} \in A^N$ of elements of A satisfying (18). In other words, Assertion $\mathcal{D}'$ holds. Hence, we have proven the implication $\mathcal{D} \Longrightarrow \mathcal{D}'$. Together with $\mathcal{D}' \Longrightarrow \mathcal{D}$, this yields $\mathcal{D} \Longleftrightarrow \mathcal{D}'$. Combining this with $\mathcal{C} \Longleftrightarrow \mathcal{D}$, we see that all three assertions $\mathcal{C}$, $\mathcal{D}$ and $\mathcal{D}'$ are equivalent. This proves Theorem 9.

However, just as Theorem 4, Theorem 9 is not the whole story, and can be strengthened in the case of radical Witt polynomials:

Theorem 9'. Let N be a nest. Let A be a torsionfree commutative ring with unity.

Let $(b_n)_{n\in N} \in A^N$ be a family of elements of A. Then, the three assertions $\mathcal{C}_{4'}$, $\mathcal{D}$ and $\mathcal{D}'$ are equivalent, where the assertions $\mathcal{C}_{4'}$ and $\mathcal{D}$ are the ones stated in Theorem 4', and the assertion $\mathcal{D}'$ is the one stated in Theorem 9.

Proof of Theorem 9'. Theorem 4' yields that the two assertions $\mathcal{C}_{4'}$ and $\mathcal{D}$ are equivalent. In other words, $\mathcal{C}_{4'} \Longleftrightarrow \mathcal{D}$. Besides, it is obvious that $\mathcal{D}' \Longrightarrow \mathcal{D}$. It remains to prove the implication $\mathcal{D} \Longrightarrow \mathcal{D}'$.

Assume that Assertion $\mathcal{D}$ holds. In other words, assume that there exists a family $(x_n)_{n\in N} \in A^N$ of elements of A satisfying (18). According to Lemma 10, there exists *at most one* such family. Hence, there exists *one and only one* family $(x_n)_{n\in N} \in A^N$ of elements of A satisfying (18). In other words, Assertion $\mathcal{D}'$ holds. Hence, we have proven the implication $\mathcal{D} \Longrightarrow \mathcal{D}'$. Together with $\mathcal{D}' \Longrightarrow \mathcal{D}$, this yields $\mathcal{D} \Longleftrightarrow \mathcal{D}'$. Combining this with $\mathcal{C}_{4'} \Longleftrightarrow \mathcal{D}$, we see that all three assertions $\mathcal{C}_{4'}$, $\mathcal{D}$ and $\mathcal{D}'$ are equivalent. This proves Theorem 9'.

For the sake of application, let us combine Theorems 4, 4' and 5:

Theorem 11'. Let N be a nest. Let A be a commutative ring with unity. For every $n \in N$, let $\varphi_n : A \to A$ be an endomorphism of the ring A such that the conditions (2), (12) and (13) are satisfied.

Let $(b_n)_{n\in N} \in A^N$ be a family of elements of A. Then, the assertions $\mathcal{C}$, $\mathcal{C}_{4'}$, $\mathcal{D}$, $\mathcal{E}$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ are equivalent, where the assertions $\mathcal{C}$ and $\mathcal{D}$ are the ones stated in Theorem 4, the assertion $\mathcal{C}_{4'}$ is the one stated in Theorem 4', and the assertions $\mathcal{E}$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ are the ones stated in Theorem 5.

Proof of Theorem 11'. According to Theorem 4, the assertions $\mathcal{C}$ and $\mathcal{D}$ are equivalent. According to Theorem 4', the assertions $\mathcal{C}_{4'}$ and $\mathcal{D}$ are equivalent. According to Theorem 5, the assertions $\mathcal{C}$, $\mathcal{E}$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ are equivalent. Combining these three observations, we conclude that the assertions $\mathcal{C}$, $\mathcal{C}_{4'}$, $\mathcal{D}$, $\mathcal{E}$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ are equivalent[23], and thus Theorem 11' is proven.

And here comes the strengthening of Theorem 11' for torsionfree rings A:

[23]Here, of course, we have used that the assertion $\mathcal{C}$ from Theorem 5 is identic with the assertion $\mathcal{C}$ from Theorem 4, and we have used that the assertion $\mathcal{D}$ from Theorem 4' is identic with the assertion $\mathcal{D}$ from Theorem 4.

Theorem 12'. Let N be a nest. Let A be a torsionfree commutative ring with unity. For every $n \in N$, let $\varphi_n : A \to A$ be an endomorphism of the ring A such that the conditions (2), (12) and (13) are satisfied.

Let $(b_n)_{n \in N} \in A^N$ be a family of elements of A. Then, the assertions $\mathcal{C}$, $\mathcal{C}_{4'}$, $\mathcal{D}$, $\mathcal{D}'$, $\mathcal{E}$, $\mathcal{E}'$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ are equivalent, where:

- the assertions $\mathcal{C}$ and $\mathcal{D}$ are the ones stated in Theorem 4,
- the assertion $\mathcal{C}_{4'}$ is the one stated in Theorem 4',
- the assertions $\mathcal{E}$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ are the ones stated in Theorem 5,
- the assertion $\mathcal{D}'$ is the one stated in Theorem 9, and
- the assertion $\mathcal{E}'$ is the one stated in Theorem 7.

Proof of Theorem 12'. According to Theorem 9, the assertions $\mathcal{C}$, $\mathcal{D}$ and $\mathcal{D}'$ are equivalent. According to Theorem 9', the assertions $\mathcal{C}_{4'}$, $\mathcal{D}$ and $\mathcal{D}'$ are equivalent. According to Theorem 7, the assertions $\mathcal{C}$, $\mathcal{E}$, $\mathcal{E}'$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ are equivalent. Combining these three observations, we conclude that the assertions $\mathcal{C}$, $\mathcal{C}_{4'}$, $\mathcal{D}$, $\mathcal{D}'$, $\mathcal{E}$, $\mathcal{E}'$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ are equivalent[24], and thus Theorem 12' is proven.

We now start specializing the above results. First, let us formulate the most important particular case of Theorem 12', namely the one where A is a ring of polynomials over $\mathbb{Z}$:

Theorem 13'. Let Ξ be a family of symbols. Let N be a nest, and let $(b_n)_{n \in N} \in (\mathbb{Z}[\Xi])^N$ be a family of polynomials in the indeterminates Ξ. Then, the following assertions $\mathcal{C}_\Xi$, $\mathcal{C}_{4'\Xi}$, $\mathcal{D}_\Xi$, $\mathcal{D}'_\Xi$, $\mathcal{E}_\Xi$, $\mathcal{E}'_\Xi$, $\mathcal{F}_\Xi$, $\mathcal{G}_\Xi$ and $\mathcal{H}_\Xi$ are equivalent:

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

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

Assertion $\mathcal{C}_{4'\Xi}$: Every $n \in N$ and every $p \in \operatorname{PF} n$ satisfies

$$b_{n/p}^p \equiv b_n \bmod p\mathbb{Z}[\Xi].$$

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

$$\left(b_n = \sqrt[\infty]{w}_n\left((x_k)_{k \in N}\right) \text{ for every } n \in N\right).$$

Assertion $\mathcal{D}'_\Xi$: There exists *one and only one* family $(x_n)_{n \in N} \in (\mathbb{Z}[\Xi])^N$ of elements of $\mathbb{Z}[\Xi]$ such that

$$\left(b_n = \sqrt[\infty]{w}_n\left((x_k)_{k \in N}\right) \text{ for every } n \in N\right).$$

[24]Here, of course, we have used that the assertion $\mathcal{C}$ from Theorem 5 is identic with the assertion $\mathcal{C}$ from Theorem 4, and we have used that the assertion $\mathcal{D}$ from Theorem 4' is identic with the assertion $\mathcal{D}$ from Theorem 4.

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

$$\left(b_n = \sum_{d|n} (\operatorname{rad} d)\, y_d\left(\Xi^{n/d}\right) \text{ for every } n \in N \right).$$

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

$$\left(b_n = \sum_{d|n} (\operatorname{rad} d)\, y_d\left(\Xi^{n/d}\right) \text{ for every } n \in N \right).$$

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

$$\sum_{d|n} \mu(d)\, b_{n/d}\left(\Xi^d\right) \in (\operatorname{rad} n)\, \mathbb{Z}[\Xi].$$

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

$$\sum_{d|n} \phi(d)\, b_{n/d}\left(\Xi^d\right) \in (\operatorname{rad} n)\, \mathbb{Z}[\Xi].$$

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

$$\sum_{i=1}^{n} b_{\gcd(i,n)}\left(\Xi^{n/\gcd(i,n)}\right) \in (\operatorname{rad} n)\, \mathbb{Z}[\Xi].$$

Before we prove this result, we need a lemma:

Lemma 14. Let $a \in \mathbb{Z}[\Xi]$ be a polynomial. Let p be a prime. Then, $a(\Xi^p) \equiv a^p \bmod p\mathbb{Z}[\Xi]$.

This lemma is Lemma 4 **(a)** in [3] (with ψ renamed as a), so we don't need to prove this lemma here.

Proof of Theorem 13'. Let A be the ring $\mathbb{Z}[\Xi]$ (this is the ring of all polynomials over $\mathbb{Z}$ in the indeterminates Ξ). Then, A is a torsionfree commutative ring with unity (torsionfree because every element $a \in \mathbb{Z}[\Xi]$ and every $n \in \mathbb{N}_+$ such that $na = 0$ satisfy $a = 0$).

For every $n \in N$, define a map $\varphi_n : \mathbb{Z}[\Xi] \to \mathbb{Z}[\Xi]$ by $\varphi_n(P) = P(\Xi^n)$ for every polynomial $P \in \mathbb{Z}[\Xi]$. It is clear that φ_n is an endomorphism of the ring $\mathbb{Z}[\Xi]$ [25]. The

[25] because $\varphi_n(0) = 0(\Xi^n) = 0$, $\varphi_n(1) = 1(\Xi^n) = 1$, and any two polynomials $P \in \mathbb{Z}[\Xi]$ and $Q \in \mathbb{Z}[\Xi]$ satisfy

$$\varphi_n(P+Q) = (P+Q)(\Xi^n) = P(\Xi^n) + Q(\Xi^n) = \varphi_n(P) + \varphi_n(Q) \quad \text{and}$$
$$\varphi_n(P \cdot Q) = (P \cdot Q)(\Xi^n) = P(\Xi^n) \cdot Q(\Xi^n) = \varphi_n(P) \cdot \varphi_n(Q).$$

condition (2) is satisfied, since $\varphi_p(a) = a(\Xi^p) \equiv a^p \bmod p\mathbb{Z}[\Xi]$ (by Lemma 14) holds for every $a \in A$. The condition (12) is satisfied as well (since $\varphi_1(P) = P(\Xi^1) = P(\Xi) = P$ for every $P \in \mathbb{Z}[\Xi]$), and the condition (13) is also satisfied (since $\varphi_n \circ \varphi_m = \varphi_{nm}$ for every $n \in N$ and every $m \in N$ satisfying $nm \in N$ [26]). Hence, the three conditions (2), (12) and (13) are satisfied. Therefore, Theorem 12' yields that the assertions $\mathcal{C}$, $\mathcal{C}_{4'}$, $\mathcal{D}$, $\mathcal{D}'$, $\mathcal{E}$, $\mathcal{E}'$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ are equivalent, where:

- the assertions $\mathcal{C}$ and $\mathcal{D}$ are the ones stated in Theorem 4,
- the assertion $\mathcal{C}_{4'}$ is the one stated in Theorem 4',
- the assertions $\mathcal{E}$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ are the ones stated in Theorem 5,
- the assertion $\mathcal{D}'$ is the one stated in Theorem 9, and
- the assertion $\mathcal{E}'$ is the one stated in Theorem 7.

Now, comparing the assertions $\mathcal{C}$, $\mathcal{C}_{4'}$, $\mathcal{D}$, $\mathcal{D}'$, $\mathcal{E}$, $\mathcal{E}'$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ with the respective assertions $\mathcal{C}_\Xi$, $\mathcal{C}_{4'\Xi}$, $\mathcal{D}_\Xi$, $\mathcal{D}'_\Xi$, $\mathcal{E}_\Xi$, $\mathcal{E}'_\Xi$, $\mathcal{F}_\Xi$, $\mathcal{G}_\Xi$ and $\mathcal{H}_\Xi$, we notice that:

- we have $\mathcal{C} \Longleftrightarrow \mathcal{C}_\Xi$ (since $A = \mathbb{Z}[\Xi]$ and $\varphi_p(b_{n/p}) = b_{n/p}(\Xi^p)$);
- we have $\mathcal{C}_{4'} \Longleftrightarrow \mathcal{C}_{4'\Xi}$ (since $A = \mathbb{Z}[\Xi]$);
- we have $\mathcal{D} \Longleftrightarrow \mathcal{D}_\Xi$ (since $A = \mathbb{Z}[\Xi]$);
- we have $\mathcal{D}' \Longleftrightarrow \mathcal{D}'_\Xi$ (since $A = \mathbb{Z}[\Xi]$);
- we have $\mathcal{E} \Longleftrightarrow \mathcal{E}_\Xi$ (since $A = \mathbb{Z}[\Xi]$ and $\varphi_{n/d}(y_d) = y_d\left(\Xi^{n/d}\right)$);
- we have $\mathcal{E}' \Longleftrightarrow \mathcal{E}'_\Xi$ (since $A = \mathbb{Z}[\Xi]$ and $\varphi_{n/d}(y_d) = y_d\left(\Xi^{n/d}\right)$);
- we have $\mathcal{F} \Longleftrightarrow \mathcal{F}_\Xi$ (since $A = \mathbb{Z}[\Xi]$ and $\varphi_d(b_{n/d}) = b_{n/d}\left(\Xi^d\right)$);
- we have $\mathcal{G} \Longleftrightarrow \mathcal{G}_\Xi$ (since $A = \mathbb{Z}[\Xi]$ and $\varphi_d(b_{n/d}) = b_{n/d}\left(\Xi^d\right)$);
- we have $\mathcal{H} \Longleftrightarrow \mathcal{H}_\Xi$ (since $A = \mathbb{Z}[\Xi]$ and $\varphi_{n/\gcd(i,n)}\left(b_{\gcd(i,n)}\right) = b_{\gcd(i,n)}\left(\Xi^{n/\gcd(i,n)}\right)$).

[26] *Proof.* Let $n \in N$ and $m \in N$ be such that $nm \in N$. Then, every $P \in \mathbb{Z}[\Xi]$ satisfies

$$(\varphi_n \circ \varphi_m)(P) = \varphi_n\left(\underbrace{\varphi_m(P)}_{=P(\Xi^m)}\right) = \varphi_n\left(P(\Xi^m)\right) = P\left(\underbrace{(\Xi^n)^m}_{=\Xi^{nm}}\right)$$
$$\left(\begin{array}{c}\text{here, } (\Xi^n)^m \text{ means the family of the } m\text{-th powers of all elements of} \\ \text{the family } \Xi^n \text{ (considered as elements of } \mathbb{Z}[\Xi]\text{)}\end{array}\right)$$
$$= P(\Xi^{nm}) = \varphi_{nm}(P).$$

Thus, $\varphi_n \circ \varphi_m = \varphi_{nm}$, qed.

Hence, the equivalence of the assertions $\mathcal{C}$, $\mathcal{C}_{4'}$, $\mathcal{D}$, $\mathcal{D}'$, $\mathcal{E}$, $\mathcal{E}'$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ yields the equivalence of the assertions $\mathcal{C}_\Xi$, $\mathcal{C}_{4'\Xi}$, $\mathcal{D}_\Xi$, $\mathcal{D}'_\Xi$, $\mathcal{E}_\Xi$, $\mathcal{E}'_\Xi$, $\mathcal{F}_\Xi$, $\mathcal{G}_\Xi$ and $\mathcal{H}_\Xi$. Thus, Theorem 13' is proven.

Theorem 13' has numerous applications, in particular the existence of "addition and multiplications" for the radical Witt vectors similar to those for normal Witt vectors. But first, let us formulate the simplest corollary of Theorem 13': namely, the one obtained for $\Xi = \varnothing$.

Theorem 15'. Let N be a nest, and let $(b_n)_{n\in N} \in \mathbb{Z}^N$ be a family of integers. Then, the following assertions $\mathcal{C}_\varnothing$, $\mathcal{C}_{4'\varnothing}$, $\mathcal{D}_\varnothing$, $\mathcal{D}'_\varnothing$, $\mathcal{E}_\varnothing$, $\mathcal{E}'_\varnothing$, $\mathcal{F}_\varnothing$, $\mathcal{G}_\varnothing$ and $\mathcal{H}_\varnothing$ are equivalent:

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

$$b_{n/p} \equiv b_n \bmod p\mathbb{Z}.$$

Assertion $\mathcal{C}_{4'\varnothing}$: Every $n \in N$ and every $p \in \operatorname{PF} n$ satisfies

$$b_{n/p}^p \equiv b_n \bmod p\mathbb{Z}.$$

Assertion $\mathcal{D}_\varnothing$: There exists a family $(x_n)_{n\in N} \in \mathbb{Z}^N$ of integers such that

$$\left(b_n = \sqrt[\infty]{w}_n\left((x_k)_{k\in N}\right) \text{ for every } n \in N\right).$$

Assertion $\mathcal{D}'_\varnothing$: There exists *one and only one* family $(x_n)_{n\in N} \in \mathbb{Z}^N$ of integers such that

$$\left(b_n = \sqrt[\infty]{w}_n\left((x_k)_{k\in N}\right) \text{ for every } n \in N\right).$$

Assertion $\mathcal{E}_\varnothing$: There exists a family $(y_n)_{n\in N} \in \mathbb{Z}^N$ of integers such that

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

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

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

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

$$\sum_{d|n} \mu(d)\, b_{n/d} \in (\operatorname{rad} n)\,\mathbb{Z}.$$

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

$$\sum_{d|n} \phi(d)\, b_{n/d} \in (\operatorname{rad} n)\,\mathbb{Z}.$$

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

$$\sum_{i=1}^{n} b_{\gcd(i,n)} \in (\operatorname{rad} n)\,\mathbb{Z}.$$

Proof of Theorem 15'. We let Ξ be the empty family. Then, $\mathbb{Z}[\Xi] = \mathbb{Z}$ (because the ring of polynomials in an empty set of indeterminates over $\mathbb{Z}$ is simply the ring $\mathbb{Z}$ itself). Every "polynomial" $a \in \mathbb{Z}$ satisfies $a(\Xi^n) = a$ for every $n \in \mathbb{N}$ [27]. Theorem 13' yields that the assertions $\mathcal{C}_\Xi$, $\mathcal{C}_{4'\Xi}$, $\mathcal{D}_\Xi$, $\mathcal{D}'_\Xi$, $\mathcal{E}_\Xi$, $\mathcal{E}'_\Xi$, $\mathcal{F}_\Xi$, $\mathcal{G}_\Xi$ and $\mathcal{H}_\Xi$ are equivalent (these assertions were stated in Theorem 13').

Now, comparing the assertions $\mathcal{C}_\Xi$, $\mathcal{C}_{4'\Xi}$, $\mathcal{D}_\Xi$, $\mathcal{D}'_\Xi$, $\mathcal{E}_\Xi$, $\mathcal{E}'_\Xi$, $\mathcal{F}_\Xi$, $\mathcal{G}_\Xi$ and $\mathcal{H}_\Xi$ with the respective assertions $\mathcal{C}_\varnothing$, $\mathcal{C}_{4'\varnothing}$, $\mathcal{D}_\varnothing$, $\mathcal{D}'_\varnothing$, $\mathcal{E}_\varnothing$, $\mathcal{E}'_\varnothing$, $\mathcal{F}_\varnothing$, $\mathcal{G}_\varnothing$ and $\mathcal{H}_\varnothing$, we notice that:

- we have $\mathcal{C}_\Xi \Longleftrightarrow \mathcal{C}_\varnothing$ (since $\mathbb{Z}[\Xi] = \mathbb{Z}$ and $b_{n/p}(\Xi^p) = b_{n/p}$);
- we have $\mathcal{C}_{4'\Xi} \Longleftrightarrow \mathcal{C}_{4'\varnothing}$ (since $\mathbb{Z}[\Xi] = \mathbb{Z}$);
- we have $\mathcal{D}_\Xi \Longleftrightarrow \mathcal{D}_\varnothing$ (since $\mathbb{Z}[\Xi] = \mathbb{Z}$);
- we have $\mathcal{D}'_\Xi \Longleftrightarrow \mathcal{D}'_\varnothing$ (since $\mathbb{Z}[\Xi] = \mathbb{Z}$);
- we have $\mathcal{E}_\Xi \Longleftrightarrow \mathcal{E}_\varnothing$ (since $\mathbb{Z}[\Xi] = \mathbb{Z}$ and $y_d\left(\Xi^{n/d}\right) = y_d$);
- we have $\mathcal{E}'_\Xi \Longleftrightarrow \mathcal{E}'_\varnothing$ (since $\mathbb{Z}[\Xi] = \mathbb{Z}$ and $y_d\left(\Xi^{n/d}\right) = y_d$);
- we have $\mathcal{F}_\Xi \Longleftrightarrow \mathcal{F}_\varnothing$ (since $\mathbb{Z}[\Xi] = \mathbb{Z}$ and $b_{n/d}\left(\Xi^d\right) = b_{n/d}$);
- we have $\mathcal{G}_\Xi \Longleftrightarrow \mathcal{G}_\varnothing$ (since $\mathbb{Z}[\Xi] = \mathbb{Z}$ and $b_{n/d}\left(\Xi^d\right) = b_{n/d}$);
- we have $\mathcal{H}_\Xi \Longleftrightarrow \mathcal{H}_\varnothing$ (since $\mathbb{Z}[\Xi] = \mathbb{Z}$ and $b_{\gcd(i,n)}\left(\Xi^{n/\gcd(i,n)}\right) = b_{\gcd(i,n)}$).

Hence, the equivalence of the assertions $\mathcal{C}_\Xi$, $\mathcal{C}_{4'\Xi}$, $\mathcal{D}_\Xi$, $\mathcal{D}'_\Xi$, $\mathcal{E}_\Xi$, $\mathcal{E}'_\Xi$, $\mathcal{F}_\Xi$, $\mathcal{G}_\Xi$ and $\mathcal{H}_\Xi$ yields the equivalence of the assertions $\mathcal{C}_\varnothing$, $\mathcal{C}_{4'\varnothing}$, $\mathcal{D}_\varnothing$, $\mathcal{D}'_\varnothing$, $\mathcal{E}_\varnothing$, $\mathcal{E}'_\varnothing$, $\mathcal{F}_\varnothing$, $\mathcal{G}_\varnothing$ and $\mathcal{H}_\varnothing$. Thus, Theorem 15' is proven.

We notice a simple corollary of Theorem 15':

Theorem 16. Let $q \in \mathbb{Z}$ be an integer. Then:

(a) There exists *one and only one* family $(x_n)_{n\in\mathbb{N}_+} \in \mathbb{Z}^{\mathbb{N}_+}$ of integers such that

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

(b) There exists *one and only one* family $(y_n)_{n\in\mathbb{N}_+} \in \mathbb{Z}^{\mathbb{N}_+}$ of integers such that

$$\left(q^n = \sum_{d|n} (\operatorname{rad} d)\, y_d \text{ for every } n \in \mathbb{N}_+\right).$$

[27] In fact, $a(\Xi^n)$ is defined as the result of replacing every indeterminate by its n-th power in the polynomial a. But since there are no indeterminates, "replacing" them by their n-th powers doesn't change anything, and thus $a(\Xi^n) = a$.

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

$$\sum_{d|n} \mu(d)\, q^{n/d} \in (\operatorname{rad} n)\, \mathbb{Z}.$$

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

$$\sum_{d|n} \phi(d)\, q^{n/d} \in (\operatorname{rad} n)\, \mathbb{Z}.$$

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

$$\sum_{i=1}^{n} q^{\gcd(i,n)} \in (\operatorname{rad} n)\, \mathbb{Z}.$$

Note that parts **(c)**, **(d)** and **(e)** of our Theorem 16 are *weaker versions* of the corresponding parts of Theorem 16 in [4], because $\operatorname{rad} n \mid n$. Still, we are going to prove the whole Theorem 16 here for the sake of completeness.

Proof of Theorem 16. First we note that every $n \in \mathbb{N}_+$ and every $p \in \operatorname{PF} n$ satisfies

$$q^{n/p} \equiv q^n \bmod p\mathbb{Z}. \tag{20}$$

[28]

Now let N be the nest $\mathbb{N}_+$. Define a family $(b_n)_{n\in N} \in \mathbb{Z}^N$ by $b_n = q^n$ for every $n \in N$. According to Theorem 15', the assertions $\mathcal{C}_\varnothing$, $\mathcal{C}_{4'\varnothing}$, $\mathcal{D}_\varnothing$, $\mathcal{D}'_\varnothing$, $\mathcal{E}_\varnothing$, $\mathcal{E}'_\varnothing$, $\mathcal{F}_\varnothing$, $\mathcal{G}_\varnothing$ and $\mathcal{H}_\varnothing$ are equivalent (these assertions were stated in Theorem 15'). Since the assertion $\mathcal{C}_\varnothing$ is true for our family $(b_n)_{n\in N} \in \mathbb{Z}^N$ (because every $n \in N$ and every $p \in \operatorname{PF} n$ satisfies

$$\begin{aligned} b_{n/p} &= q^{n/p} \equiv q^n && \text{(by (20))} \\ &= b_n \bmod p\mathbb{Z} \end{aligned}$$

), this yields that the assertions $\mathcal{C}_{4'\varnothing}$, $\mathcal{D}_\varnothing$, $\mathcal{D}'_\varnothing$, $\mathcal{E}_\varnothing$, $\mathcal{E}'_\varnothing$, $\mathcal{F}_\varnothing$, $\mathcal{G}_\varnothing$ and $\mathcal{H}_\varnothing$ must also be true for our family $(b_n)_{n\in N} \in \mathbb{Z}^N$. But for the family $(b_n)_{n\in N} \in \mathbb{Z}^N$,

- assertion $\mathcal{D}'_\varnothing$ is equivalent to Theorem 16 **(a)** (since $N = \mathbb{N}_+$ and $b_n = q^n$);
- assertion $\mathcal{E}'_\varnothing$ is equivalent to Theorem 16 **(b)** (since $N = \mathbb{N}_+$ and $b_n = q^n$);
- assertion $\mathcal{F}_\varnothing$ is equivalent to Theorem 16 **(c)** (since $N = \mathbb{N}_+$ and $b_{n/d} = q^{n/d}$);
- assertion $\mathcal{G}_\varnothing$ is equivalent to Theorem 16 **(d)** (since $N = \mathbb{N}_+$ and $b_{n/d} = q^{n/d}$);
- assertion $\mathcal{H}_\varnothing$ is equivalent to Theorem 16 **(e)** (since $N = \mathbb{N}_+$ and $b_{\gcd(i,n)} = q^{\gcd(i,n)}$).

[28] *Proof.* Let $n \in \mathbb{N}_+$ and $p \in \operatorname{PF} n$. By Fermat's little theorem, $\left(q^{n/p}\right)^p \equiv q^{n/p} \bmod p\mathbb{Z}$. Thus, $q^{n/p} \equiv \left(q^{n/p}\right)^p = q^{(n/p)\cdot p} = q^n \bmod p\mathbb{Z}$, qed.

Hence, Theorem 16 **(a)**, Theorem 16 **(b)**, Theorem 16 **(c)**, Theorem 16 **(d)** and Theorem 16 **(e)** must be true (since the assertions $\mathcal{D}'_{\varnothing}$, $\mathcal{E}'_{\varnothing}$, $\mathcal{F}_{\varnothing}$, $\mathcal{G}_{\varnothing}$ and $\mathcal{H}_{\varnothing}$ are true for the family $(b_n)_{n\in N} \in \mathbb{Z}^N$). This proves Theorem 16.

We now take on Theorem 17 of [4]. Its analogue for radical Witt polynomials is the following:

Theorem 17. In the following, for any $u \in \mathbb{Z}$ and any $r \in \mathbb{Q}$, we define the binomial coefficient $\dbinom{u}{r}$ by

$$\binom{u}{r} = \begin{cases} \dfrac{1}{r!}\prod\limits_{k=0}^{r-1}(u-k), & \text{if } r \in \mathbb{N}; \\ 0, & \text{if } r \notin \mathbb{N} \end{cases}.$$

In particular, if $r \in \mathbb{Q} \setminus \mathbb{Z}$, then $\dbinom{u}{r}$ is supposed to mean 0.

Let $q \in \mathbb{Z}$ and $r \in \mathbb{Q}$. Then:

(a) There exists *one and only one* family $(x_n)_{n\in\mathbb{N}_+} \in \mathbb{Z}^{\mathbb{N}_+}$ of integers such that

$$\left(\binom{qn}{rn} = \sqrt[\infty]{w}_n\left(\left(x_k\right)_{k\in\mathbb{N}_+}\right) \text{ for every } n \in \mathbb{N}_+\right).$$

(b) There exists *one and only one* family $(y_n)_{n\in\mathbb{N}_+} \in \mathbb{Z}^{\mathbb{N}_+}$ of integers such that

$$\left(\binom{qn}{rn} = \sum_{d\mid n}(\operatorname{rad} d)\, y_d \text{ for every } n \in \mathbb{N}_+\right).$$

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

$$\sum_{d\mid n}\mu(d)\binom{qn/d}{rn/d} \in (\operatorname{rad} n)\,\mathbb{Z}.$$

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

$$\sum_{d\mid n}\phi(d)\binom{qn/d}{rn/d} \in (\operatorname{rad} n)\,\mathbb{Z}.$$

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

$$\sum_{i=1}^{n}\binom{q\gcd(i,n)}{r\gcd(i,n)} \in (\operatorname{rad} n)\,\mathbb{Z}.$$

Just as in the case of Theorem 16, parts **(c)**, **(d)** and **(e)** of Theorem 17 tell nothing new compared to the similar parts of Theorem 17 of [4]. We will still prove them along with the rest.

Let us first quote Lemma 19 from [4]:

Lemma 19. Let $n \in \mathbb{N}_+$ and let $p \in \operatorname{PF} n$. Let $q \in \mathbb{Z}$ and $r \in \mathbb{Q}$. Then,

$$\binom{qn/p}{rn/p} \equiv \binom{qn}{rn} \bmod p^{v_p(n)}\mathbb{Z}. \tag{21}$$

For the proof of this lemma, see [4].

Proof of Theorem 17. Let us first notice that every $n \in \mathbb{N}_+$ and every $p \in \operatorname{PF} n$ satisfy

$$\binom{qn/p}{rn/p} \equiv \binom{qn}{rn} \bmod p\mathbb{Z}. \tag{22}$$

[29]

Let N be the nest $\mathbb{N}_+$. Define a family $(b_n)_{n\in N} \in \mathbb{Z}^N$ by $b_n = \binom{qn}{rn}$ for every $n \in N$. According to Theorem 15', the assertions $\mathcal{C}_\varnothing$, $\mathcal{C}_{4'\varnothing}$, $\mathcal{D}_\varnothing$, $\mathcal{D}'_\varnothing$, $\mathcal{E}_\varnothing$, $\mathcal{E}'_\varnothing$, $\mathcal{F}_\varnothing$, $\mathcal{G}_\varnothing$ and $\mathcal{H}_\varnothing$ are equivalent (these assertions were stated in Theorem 15'). Since the assertion $\mathcal{C}_\varnothing$ is true for our family $(b_n)_{n\in N} \in \mathbb{Z}^N$ (because every $n \in N$ and every $p \in \operatorname{PF} n$ satisfies

$$\begin{aligned} b_{n/p} &= \binom{qn/p}{rn/p} \equiv \binom{qn}{rn} \qquad \text{(by (22))} \\ &= b_n \bmod p\mathbb{Z} \end{aligned}$$

), this yields that the assertions $\mathcal{C}_{4'\varnothing}$, $\mathcal{D}_\varnothing$, $\mathcal{D}'_\varnothing$, $\mathcal{E}_\varnothing$, $\mathcal{E}'_\varnothing$, $\mathcal{F}_\varnothing$, $\mathcal{G}_\varnothing$ and $\mathcal{H}_\varnothing$ must also be true for our family $(b_n)_{n\in N} \in \mathbb{Z}^N$. But for the family $(b_n)_{n\in N} \in \mathbb{Z}^N$,

- assertion $\mathcal{D}'_\varnothing$ is equivalent to Theorem 17 **(a)** (since $N = \mathbb{N}_+$ and $b_n = \binom{qn}{rn}$);
- assertion $\mathcal{E}'_\varnothing$ is equivalent to Theorem 17 **(b)** (since $N = \mathbb{N}_+$ and $b_n = \binom{qn}{rn}$);
- assertion $\mathcal{F}_\varnothing$ is equivalent to Theorem 17 **(c)** (since $N = \mathbb{N}_+$ and $b_{n/d} = \binom{qn/d}{rn/d}$);
- assertion $\mathcal{G}_\varnothing$ is equivalent to Theorem 17 **(d)** (since $N = \mathbb{N}_+$ and $b_{n/d} = \binom{qn/d}{rn/d}$);
- assertion $\mathcal{H}_\varnothing$ is equivalent to Theorem 17 **(e)** (since $N = \mathbb{N}_+$ and $b_{\gcd(i,n)} = \binom{q\gcd(i,n)}{r\gcd(i,n)}$).

Hence, Theorem 17 **(a)**, Theorem 17 **(b)**, Theorem 17 **(c)**, Theorem 17 **(d)** and Theorem 17 **(e)** must be true (since the assertions $\mathcal{D}'_\varnothing$, $\mathcal{E}'_\varnothing$, $\mathcal{F}_\varnothing$, $\mathcal{G}_\varnothing$ and $\mathcal{H}_\varnothing$ are true for the family $(b_n)_{n\in N} \in \mathbb{Z}^N$). This proves Theorem 17.

Actually, we can do better than Theorem 17 in the case when r is an integer:

[29] *Proof of (22):* Let $n \in \mathbb{N}_+$ and $p \in \operatorname{PF} n$. Then, $p \mid n$ (since $p \in \operatorname{PF} n$) and thus $v_p(n) \geq 1$, so that $p \mid p^{v_p(n)}$. Hence, $p^{v_p(n)}\mathbb{Z} \subseteq p\mathbb{Z}$. But Lemma 19 yields $\binom{qn/p}{rn/p} \equiv \binom{qn}{rn} \bmod p^{v_p(n)}\mathbb{Z}$. Since $p^{v_p(n)}\mathbb{Z} \subseteq p\mathbb{Z}$, this yields $\binom{qn/p}{rn/p} \equiv \binom{qn}{rn} \bmod p\mathbb{Z}$. This proves (22).

Theorem 20. In the following, for any $u \in \mathbb{Z}$ and any $r \in \mathbb{Q}$, we define the binomial coefficient $\binom{u}{r}$ by

$$\binom{u}{r} = \begin{cases} \dfrac{1}{r!} \prod\limits_{k=0}^{r-1} (u-k), & \text{if } r \in \mathbb{N}; \\ 0, & \text{if } r \notin \mathbb{N} \end{cases}.$$

In particular, if $r \in \mathbb{Z} \setminus \mathbb{N}$, then $\binom{u}{r}$ is supposed to mean 0.

Let $q \in \mathbb{Z}$ and $r \in \mathbb{Z}$. Then:

(a) There exists *one and only one* family $(x_n)_{n \in \mathbb{N}_+} \in \mathbb{Z}^{\mathbb{N}_+}$ of integers such that

$$\left(\binom{qn-1}{rn-1} = \sqrt[\infty]{w}_n \left((x_k)_{k \in \mathbb{N}_+} \right) \text{ for every } n \in \mathbb{N}_+ \right).$$

(b) There exists *one and only one* family $(y_n)_{n \in \mathbb{N}_+} \in \mathbb{Z}^{\mathbb{N}_+}$ of integers such that

$$\left(\binom{qn-1}{rn-1} = \sum_{d \mid n} (\operatorname{rad} d)\, y_d \text{ for every } n \in \mathbb{N}_+ \right).$$

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

$$\sum_{d \mid n} \mu(d) \binom{qn/d-1}{rn/d-1} \in (\operatorname{rad} n)\, \mathbb{Z}.$$

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

$$\sum_{d \mid n} \phi(d) \binom{qn/d-1}{rn/d-1} \in (\operatorname{rad} n)\, \mathbb{Z}.$$

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

$$\sum_{i=1}^{n} \binom{q \gcd(i,n)-1}{r \gcd(i,n)-1} \in (\operatorname{rad} n)\, \mathbb{Z}.$$

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

$$\sum_{d \mid n} \mu(d) \binom{qn/d}{rn/d} \in \frac{q}{r} (\operatorname{rad} n)\, \mathbb{Z}.$$

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

$$\sum_{d \mid n} \phi(d) \binom{qn/d}{rn/d} \in \frac{q}{r} (\operatorname{rad} n)\, \mathbb{Z}.$$

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

$$\sum_{i=1}^{n} \binom{q \gcd(i,n)}{r \gcd(i,n)} \in \frac{q}{r} (\operatorname{rad} n)\, \mathbb{Z}.$$

The proof of this fact will use an analogue (and corollary) of Lemma 19:

Lemma 21. Let $n \in \mathbb{N}_+$ and let $p \in \operatorname{PF} n$. Let $q \in \mathbb{Z}$ and $r \in \mathbb{Q}$. Assume that there exist two integers α and β with $v_p(\alpha) \geq v_p(\beta)$ and $r = \dfrac{\alpha}{\beta}$. Then,

$$\binom{qn/p-1}{rn/p-1} \equiv \binom{qn-1}{rn-1} \bmod p^{v_p(n)}\mathbb{Z}. \tag{23}$$

This lemma is identic with Lemma 21 in [4], so we won't prove it here.

Proof of Theorem 20. We will use the formula

$$\binom{a}{b} = \frac{a}{b}\binom{a-1}{b-1} \tag{24}$$

for any $a \in \mathbb{Q}$ and $b \in \mathbb{Q} \setminus \{0\}$. (This formula was proven during the proof of Lemma 21 in [4].)

Let us also notice that every $n \in \mathbb{N}_+$ and every $p \in \operatorname{PF} n$ satisfy

$$\binom{qn/p-1}{rn/p-1} \equiv \binom{qn-1}{rn-1} \bmod p\mathbb{Z}. \tag{25}$$

[30]

Let N be the nest $\mathbb{N}_+$. Define a family $(b_n)_{n\in N} \in \mathbb{Z}^N$ by $b_n = \dbinom{qn-1}{rn-1}$ for every $n \in N$. According to Theorem 15', the assertions $\mathcal{C}_\varnothing$, $\mathcal{C}_{4'\varnothing}$, $\mathcal{D}_\varnothing$, $\mathcal{D}'_\varnothing$, $\mathcal{E}_\varnothing$, $\mathcal{E}'_\varnothing$, $\mathcal{F}_\varnothing$, $\mathcal{G}_\varnothing$ and $\mathcal{H}_\varnothing$ are equivalent (these assertions were stated in Theorem 15'). Since the assertion $\mathcal{C}_\varnothing$ is true for our family $(b_n)_{n\in N} \in \mathbb{Z}^N$ (because every $n \in N$ and every $p \in \operatorname{PF} n$ satisfies

$$\begin{aligned} b_{n/p} &= \binom{qn/p-1}{rn/p-1} \equiv \binom{qn-1}{rn-1} \qquad \text{(by (25))} \\ &= b_n \bmod p\mathbb{Z}, \end{aligned}$$

), this yields that the assertions $\mathcal{C}_{4'\varnothing}$, $\mathcal{D}_\varnothing$, $\mathcal{D}'_\varnothing$, $\mathcal{E}_\varnothing$, $\mathcal{E}'_\varnothing$, $\mathcal{F}_\varnothing$, $\mathcal{G}_\varnothing$ and $\mathcal{H}_\varnothing$ must also be true for our family $(b_n)_{n\in N} \in \mathbb{Z}^N$. But for the family $(b_n)_{n\in N} \in \mathbb{Z}^N$,

- assertion $\mathcal{D}'_\varnothing$ is equivalent to Theorem 20 **(a)** (since $N = \mathbb{N}_+$ and $b_n = \dbinom{qn-1}{rn-1}$);
- assertion $\mathcal{E}'_\varnothing$ is equivalent to Theorem 20 **(b)** (since $N = \mathbb{N}_+$ and $b_n = \dbinom{qn-1}{rn-1}$);

[30] *Proof of (25):* Let $n \in \mathbb{N}_+$ and $p \in \operatorname{PF} n$. Then, $p \mid n$ (since $p \in \operatorname{PF} n$) and thus $v_p(n) \geq 1$, so that $p \mid p^{v_p(n)}$. Hence, $p^{v_p(n)}\mathbb{Z} \subseteq p\mathbb{Z}$.

But clearly, there exist two integers α and β with $v_p(\alpha) \geq v_p(\beta)$ and $r = \dfrac{\alpha}{\beta}$ (namely, $\alpha = r$ and $\beta = 1$, since $\dfrac{r}{1} = 1$ and $v_p(r) \geq 0 = v_p(1)$). Thus, Lemma 21 yields $\dbinom{qn/p-1}{rn/p-1} \equiv \dbinom{qn-1}{rn-1} \bmod p^{v_p(n)}\mathbb{Z}$. Since $p^{v_p(n)}\mathbb{Z} \subseteq p\mathbb{Z}$, this yields $\dbinom{qn/p-1}{rn/p-1} \equiv \dbinom{qn-1}{rn-1} \bmod p\mathbb{Z}$. This proves (25).

- assertion $\mathcal{F}_{\varnothing}$ is equivalent to Theorem 20 **(c)** (since $N = \mathbb{N}_+$ and $b_{n/d} = \binom{qn/d-1}{rn/d-1}$);
- assertion $\mathcal{G}_{\varnothing}$ is equivalent to Theorem 20 **(d)** (since $N = \mathbb{N}_+$ and $b_{n/d} = \binom{qn/d-1}{rn/d-1}$);
- assertion $\mathcal{H}_{\varnothing}$ is equivalent to Theorem 20 **(e)** (since $N = \mathbb{N}_+$ and $b_{\gcd(i,n)} = \binom{q\gcd(i,n)-1}{r\gcd(i,n)-1}$).

Hence, Theorem 20 **(a)**, Theorem 20 **(b)**, Theorem 20 **(c)**, Theorem 20 **(d)** and Theorem 20 **(e)** must be true (since the assertions $\mathcal{D}'_{\varnothing}$, $\mathcal{E}'_{\varnothing}$, $\mathcal{F}_{\varnothing}$, $\mathcal{G}_{\varnothing}$ and $\mathcal{H}_{\varnothing}$ are true for the family $(b_n)_{n\in N} \in \mathbb{Z}^N$).

Theorem 20 **(f)** follows from Theorem 20 **(c)**, since

$$\sum_{d|n} \mu(d) \underbrace{\binom{qn/d}{rn/d}}_{=\frac{qn/d}{rn/d}\binom{qn/d-1}{rn/d-1}} = \sum_{d|n} \mu(d) \underbrace{\frac{qn/d}{rn/d}}_{=\frac{q}{r}} \binom{qn/d-1}{rn/d-1} = \frac{q}{r} \underbrace{\sum_{d|n} \mu(d) \binom{qn/d-1}{rn/d-1}}_{\in(\operatorname{rad} n)\mathbb{Z} \text{ (by Theorem 20 (c))}}$$

(by (24), applied to $a=qn/d$ and $b=rn/d$)

$$\in \frac{q}{r}(\operatorname{rad} n)\mathbb{Z}.$$

Theorem 20 **(g)** follows from Theorem 20 **(d)**, because

$$\sum_{d|n} \phi(d) \underbrace{\binom{qn/d}{rn/d}}_{=\frac{qn/d}{rn/d}\binom{qn/d-1}{rn/d-1}} = \sum_{d|n} \phi(d) \underbrace{\frac{qn/d}{rn/d}}_{=\frac{q}{r}} \binom{qn/d-1}{rn/d-1} = \frac{q}{r} \underbrace{\sum_{d|n} \phi(d) \binom{qn/d-1}{rn/d-1}}_{\in(\operatorname{rad} n)\mathbb{Z} \text{ (by Theorem 20 (d))}}$$

(by (24), applied to $a=qn/d$ and $b=rn/d$)

$$\in \frac{q}{r}(\operatorname{rad} n)\mathbb{Z}.$$

Theorem 20 **(h)** follows from Theorem 20 **(e)**, since

$$\sum_{i=1}^{n} \underbrace{\binom{q\gcd(i,n)}{r\gcd(i,n)}}_{=\frac{q\gcd(i,n)}{r\gcd(i,n)}\binom{q\gcd(i,n)-1}{r\gcd(i,n)-1}} = \sum_{i=1}^{n} \underbrace{\frac{q\gcd(i,n)}{r\gcd(i,n)}}_{=\frac{q}{r}} \binom{q\gcd(i,n)-1}{r\gcd(i,n)-1}$$

(by (24), applied to $a=q\gcd(i,n)$ and $b=r\gcd(i,n)$)

$$= \frac{q}{r} \underbrace{\sum_{i=1}^{n} \binom{q\gcd(i,n)-1}{r\gcd(i,n)-1}}_{\in(\operatorname{rad} n)\mathbb{Z} \text{ (by Theorem 20 (e))}} \in \frac{q}{r}(\operatorname{rad} n)\mathbb{Z}.$$

Thus, altogether we have now proven Theorem 20 completely.

So much for applications of Theorem 13' for the case when Ξ is the empty family (i. e. for polynomials in zero variables). We now aim to apply Theorem 13' to nonempty Ξ. However, at first, let us make a part of Theorem 13' stronger.

Theorem 22. Let Ξ be a family of symbols. Let N be a nest, and let $\left(b_n\right)_{n\in N} \in \left(\mathbb{Q}\left[\Xi\right]\right)^N$ be a family of polynomials in the indeterminates Ξ.

(a) There exists *one and only one* family $\left(x_n\right)_{n\in N} \in \left(\mathbb{Q}\left[\Xi\right]\right)^N$ of elements of $\mathbb{Q}\left[\Xi\right]$ such that

$$\left(b_n = \sqrt[\infty]{w}_n\left(\left(x_k\right)_{k\in N}\right) \text{ for every } n \in N\right).$$

We denote this family $\left(x_n\right)_{n\in N}$ by $\left(\widetilde{x}_n\right)_{n\in N}$. Then, we have $\left(\widetilde{x}_n\right)_{n\in N} \in \left(\mathbb{Q}\left[\Xi\right]\right)^N$ and

$$\left(b_n = \sqrt[\infty]{w}_n\left(\left(\widetilde{x}_k\right)_{k\in N}\right) \text{ for every } n \in N\right).$$

(b) The family $\left(\widetilde{x}_n\right)_{n\in N} \in \left(\mathbb{Q}\left[\Xi\right]\right)^N$ defined in Theorem 22 **(a)** satisfies $\widetilde{x}_n \in \mathbb{Q}\left[b_{\mathbb{N}_{|n}}\right]$ (where $\mathbb{Q}\left[b_{\mathbb{N}_{|n}}\right]$ means the sub-$\mathbb{Q}$-algebra of $\mathbb{Q}\left[\Xi\right]$ generated by the polynomials b_d for all $d \in \mathbb{N}_{|n}$) for every $n \in N$.

(c) Assume that $\left(b_n\right)_{n\in N} \in \left(\mathbb{Z}\left[\Xi\right]\right)^N$. Then, the family $\left(\widetilde{x}_n\right)_{n\in N} \in \left(\mathbb{Q}\left[\Xi\right]\right)^N$ defined in Theorem 22 **(a)** satisfies $\left(\widetilde{x}_n\right)_{n\in N} \in \left(\mathbb{Z}\left[\Xi\right]\right)^N$ if and only if every $n \in N$ and every $p \in \operatorname{PF} n$ satisfies

$$b_{n/p}\left(\Xi^p\right) \equiv b_n \bmod p\mathbb{Z}\left[\Xi\right]. \tag{26}$$

Proof of Theorem 22. Let us use the conventions of Definition 10. We know that prad is a pseudo-monotonous map. Hence, we can apply Theorem 22 in [6] to $F = \operatorname{prad}$. As a result, we obtain the following theorem:

Theorem 22a. Let Ξ be a family of symbols. Let N be a nest, and let $\left(b_n\right)_{n\in N} \in \left(\mathbb{Q}\left[\Xi\right]\right)^N$ be a family of polynomials in the indeterminates Ξ.

(a) There exists *one and only one* family $\left(x_n\right)_{n\in N} \in \left(\mathbb{Q}\left[\Xi\right]\right)^N$ of elements of $\mathbb{Q}\left[\Xi\right]$ such that

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

We denote this family $\left(x_n\right)_{n\in N}$ by $\left(\widetilde{x}_n\right)_{n\in N}$. Then, we have $\left(\widetilde{x}_n\right)_{n\in N} \in \left(\mathbb{Q}\left[\Xi\right]\right)^N$ and

$$\left(b_n = w_{\operatorname{prad},n}\left(\left(\widetilde{x}_k\right)_{k\in N}\right) \text{ for every } n \in N\right).$$

(b) The family $\left(\widetilde{x}_n\right)_{n\in N} \in \left(\mathbb{Q}\left[\Xi\right]\right)^N$ defined in Theorem 22a **(a)** satisfies $\widetilde{x}_n \in \mathbb{Q}\left[b_{\mathbb{N}_{|n}}\right]$ (where $\mathbb{Q}\left[b_{\mathbb{N}_{|n}}\right]$ means the sub-$\mathbb{Q}$-algebra of $\mathbb{Q}\left[\Xi\right]$ generated by the polynomials b_d for all $d \in \mathbb{N}_{|n}$) for every $n \in N$.

(c) Assume that $(b_n)_{n\in N} \in (\mathbb{Z}[\Xi])^N$. Then, the family $(\widetilde{x}_n)_{n\in N} \in (\mathbb{Q}[\Xi])^N$ defined in Theorem 22a **(a)** satisfies $(\widetilde{x}_n)_{n\in N} \in (\mathbb{Z}[\Xi])^N$ if and only if every $n \in N$ and every $p \in \operatorname{PF} n$ satisfies

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

But Theorem 22 can be obtained from Theorem 22a by means of replacing $w_{\operatorname{prad},n}$ by $\sqrt[\infty]{w}_n$ and replacing $p^{\operatorname{prad}(p,v_p(n))}$ by p. Since these replacements don't change the validity of the theorem (because every $n \in N$ satisfies $w_{\operatorname{prad},n} = \sqrt[\infty]{w}_n$, and because every $n \in N$ and every $p \in \operatorname{PF} n$ satisfy $p^{\operatorname{prad}(p,v_p(n))} = p$ (according to (4))), this yields that Theorem 22 is equivalent to Theorem 22a. Since we know that Theorem 22a is true, we can thus conclude that Theorem 22 is true.

Now we come to the main application of Theorem 13':

Theorem 25. Let N be a nest. Let $m \in \mathbb{N}$. Let Ξ denote the family $(X_{k,n})_{(k,n)\in\{1,2,...,m\}\times N}$ of symbols. This family is clearly the union $\bigcup_{k\in\{1,2,...,m\}} X_{k,N}$ of the families $X_{k,N}$ defined by $X_{k,N} = (X_{k,n})_{n\in N}$ for each $k \in \{1,2,...,m\}$. For each $k \in \{1,2,...,m\}$, the family $X_{k,N} = (X_{k,n})_{n\in N}$ consists of $|N|$ symbols; their union Ξ is a family consisting of $m\cdot|N|$ symbols. (Consequently, $\mathbb{Z}[\Xi] = \mathbb{Z}\left[(X_{k,n})_{(k,n)\in\{1,2,...,m\}\times N}\right]$ is a polynomial ring over $\mathbb{Z}$ in $m\cdot|N|$ indeterminates which are labelled $X_{k,n}$ for $(k,n) \in \{1,2,...,m\}\times N$.)

Let $f \in \mathbb{Z}[\alpha_1,\alpha_2,...,\alpha_m]$ be a polynomial in m variables.

(a) Then, there exists one and only one family $(x_n)_{n\in N} \in (\mathbb{Q}[\Xi])^N$ of polynomials such that

$$\left(\sqrt[\infty]{w}_n\left((x_k)_{k\in N}\right) = f\left(\sqrt[\infty]{w}_n(X_{1,N}),\ \sqrt[\infty]{w}_n(X_{2,N}),...,\ \sqrt[\infty]{w}_n(X_{m,N})\right) \quad \text{for every } n\in N\right).$$

We denote this family $(x_n)_{n\in N}$ by $(f_n)_{n\in N}$. Then, we have $(f_n)_{n\in N} \in (\mathbb{Q}[\Xi])^N$ and

$$\left(\sqrt[\infty]{w}_n\left((f_k)_{k\in N}\right) = f\left(\sqrt[\infty]{w}_n(X_{1,N}),\ \sqrt[\infty]{w}_n(X_{2,N}),...,\ \sqrt[\infty]{w}_n(X_{m,N})\right) \quad \text{for every } n\in N\right).$$

(b) This family $(f_n)_{n\in N} \in (\mathbb{Q}[\Xi])^N$ satisfies $f_n \in \mathbb{Z}\left[\Xi_{\mathbb{N}_{|n}}\right]$ (where $\mathbb{Z}\left[\Xi_{\mathbb{N}_{|n}}\right]$ means the sub-$\mathbb{Z}$-algebra of $\mathbb{Z}[\Xi]$ generated by the polynomials $X_{k,d}$ for $k \in \{1,2,...,m\}$ and $d \in \mathbb{N}_{|n}$) for every $n \in N$.

Proof of Theorem 25. Let us use the conventions of Definition 10. We know that prad is a pseudo-monotonous map. Hence, we can apply Theorem 25 in [6] to $F = \operatorname{prad}$. As a result, we obtain the following theorem:

Theorem 25a. Let N be a nest. Let $m \in \mathbb{N}$. Let Ξ denote the family $(X_{k,n})_{(k,n)\in\{1,2,...,m\}\times N}$ of symbols. This family is clearly the union $\bigcup_{k\in\{1,2,...,m\}} X_{k,N}$ of the families $X_{k,N}$ defined by $X_{k,N} = (X_{k,n})_{n\in N}$ for each $k \in \{1,2,...,m\}$. For each $k \in \{1,2,...,m\}$, the family $X_{k,N} = (X_{k,n})_{n\in N}$ consists of $|N|$ symbols; their union Ξ is a family consisting of $m\cdot|N|$ symbols. (Consequently,

$\mathbb{Z}[\Xi] = \mathbb{Z}\left[(X_{k,n})_{(k,n)\in\{1,2,...,m\}\times N}\right]$ is a polynomial ring over $\mathbb{Z}$ in $m \cdot |N|$ indeterminates which are labelled $X_{k,n}$ for $(k,n) \in \{1,2,...,m\} \times N$.)

Let $f \in \mathbb{Z}[\alpha_1, \alpha_2, ..., \alpha_m]$ be a polynomial in m variables.

(a) Then, there exists one and only one family $(x_n)_{n\in N} \in (\mathbb{Q}[\Xi])^N$ of polynomials such that

$$\left(w_{\mathrm{prad},n}\left((x_k)_{k\in N}\right) = f\left(w_{\mathrm{prad},n}\left(X_{1,N}\right), w_{\mathrm{prad},n}\left(X_{2,N}\right), ..., w_{\mathrm{prad},n}\left(X_{m,N}\right)\right) \qquad \text{for every } n \in N\right).$$

We denote this family $(x_n)_{n\in N}$ by $(f_n)_{n\in N}$. Then, we have $(f_n)_{n\in N} \in (\mathbb{Q}[\Xi])^N$ and

$$\left(w_{\mathrm{prad},n}\left((f_k)_{k\in N}\right) = f\left(w_{\mathrm{prad},n}\left(X_{1,N}\right), w_{\mathrm{prad},n}\left(X_{2,N}\right), ..., w_{\mathrm{prad},n}\left(X_{m,N}\right)\right) \qquad \text{for every } n \in N\right).$$

(b) This family $(f_n)_{n\in N} \in (\mathbb{Q}[\Xi])^N$ satisfies $f_n \in \mathbb{Z}\left[\Xi_{\mathbb{N}_{|n}}\right]$ (where $\mathbb{Z}\left[\Xi_{\mathbb{N}_{|n}}\right]$ means the sub-$\mathbb{Z}$-algebra of $\mathbb{Z}[\Xi]$ generated by the polynomials $X_{k,d}$ for $k \in \{1,2,...,m\}$ and $d \in \mathbb{N}_{|n}$) for every $n \in N$.

But Theorem 25 can be obtained from Theorem 25a by means of replacing $w_{\mathrm{prad},n}$ by $\sqrt[\infty]{w}_n$. Since this replacement doesn't change the validity of the theorem (because every $n \in N$ satisfies $w_{\mathrm{prad},n} = \sqrt[\infty]{w}_n$), this yields that Theorem 25 is equivalent to Theorem 25a. Since we know that Theorem 25a is true, we can thus conclude that Theorem 25 is true.

[...]

[define $+_W$ and $\cdot_W$ maybe]

[...]

[add stuff to witt5b]

References

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

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

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

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

[5] Darij Grinberg, *Witt#5c: The Chinese Remainder Theorem for Modules.* http://www.cip.ifi.lmu.de/~grinberg/algebra/witt5c.pdf

[6] Darij Grinberg, *Witt#5e: Generalizing integrality theorems for ghost-Witt vectors.* http://www.cip.ifi.lmu.de/~grinberg/algebra/witt5e.pdf