Witt vectors. Part 1

Michiel Hazewinkel

Sidenotes by Darij Grinberg

Witt#5e: Generalizing integrality theorems for ghost-Witt vectors

[not completed, not proofread]

In this note, we will generalize most of the results in [4], replacing the Witt polynomials w_n by the more general polynomials $w_{F,n}$ defined for any pseudo-monotonous map $F : \mathbb{P} \times \mathbb{N} \to \mathbb{N}$ (the meaning of "pseudo-monotonous" will soon be explained below). Whenever possible, the proofs will be done by simply copypasting the corresponding proofs from [4] and doing the necessary changes - which often will be trivial, though sometimes new thinking will be required. I will even try to keep the numbering of the results in this note consistent with the numbering of the results in [4], so that for instance Theorem i in this note will be the generalization of Theorem i in [4] for as many i as possible. This explains why there are gaps in the numbering: e. g., there is no numbered result between Theorem 17 and Lemma 19 in this note, because Lemma 18 of [4] was just an auxiliary result and needs not be generalized to the $w_{F,n}$.

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])

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 $\mathbb{Z}$.

[1] The first 6 of the following 10 definitions 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 $P(\Xi^n) = (X_0^n + X_1^n)^2 - 2X_3^n + 1$.

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

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

[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 9. A map $F : \mathbb{P} \times \mathbb{N} \to \mathbb{N}$ is said to be *pseudo-monotonous* if it satisfies

$$\left(F\left(p,0\right)=0 \qquad \text{for every } p\in\mathbb{P}\right) \qquad \text{and} \tag{1}$$

$$\left(F\left(p,a\right)-a\leq F\left(p,b\right)-b \qquad \text{for every } p\in\mathbb{P},\ a\in\mathbb{N} \text{ and } b\in\mathbb{N} \text{ satisfying } a\geq b\right). \tag{2}$$

If $F : \mathbb{P} \times \mathbb{N} \to \mathbb{N}$ is a pseudo-monotonous map, then we denote by $\widetilde{F} : \mathbb{N}_+ \to \mathbb{N}_+$ the map defined by

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

[7]

We note that

$$v_p\left(\widetilde{F}\left(n\right)\right)=F\left(p,v_p\left(n\right)\right) \qquad \text{for every } n\in\mathbb{N}_+ \text{ and every } p\in\operatorname{PF}n \tag{3}$$

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

$$\widetilde{F}\left(n\right)\mid\left(n/d\right)\widetilde{F}\left(d\right) \qquad \text{for every } n\in\mathbb{N}_+ \text{ and every } d\in\mathbb{N}_{|n} \tag{4}$$

[8].

[7] Note that $\widetilde{F}$ is always a multiplicative function, but not every multiplicative function from $\mathbb{N}_+$ to $\mathbb{N}_+$ can be written as $\widetilde{F}$ for some pseudo-monotonous map $F : \mathbb{P}\times\mathbb{N}\to\mathbb{N}$.

[8] In fact, we have

$$\begin{aligned}\prod_{p\in\operatorname{PF}n}p^{F\left(p,v_p\left(d\right)\right)}&=\underbrace{\prod_{p\in\operatorname{PF}d}p^{F\left(p,v_p\left(d\right)\right)}}_{\substack{=\widetilde{F}\left(d\right)\text{ (by the}\\ \text{definition of }\widetilde{F}\text{)}}}\cdot\prod_{p\in\operatorname{PF}n\setminus\operatorname{PF}d}\underbrace{p^{F\left(p,v_p\left(d\right)\right)}}_{\substack{=p^{F\left(p,0\right)}\\ \text{(since }p\in\operatorname{PF}n\setminus\operatorname{PF}d\\ \text{yields }p\notin\operatorname{PF}d\text{ and thus}\\ v_p\left(d\right)=0\text{)}}} \qquad \left(\text{since } d\mid n \text{ yields } \operatorname{PF}d\subseteq\operatorname{PF}n\right)\\ &=\widetilde{F}\left(d\right)\cdot\prod_{p\in\operatorname{PF}n\setminus\operatorname{PF}d}\underbrace{p^{F\left(p,0\right)}}_{\substack{=1\text{ (since (1) yields}\\ F\left(p,0\right)=0\text{ and thus}\\ p^{F\left(p,0\right)}=p^0=1\text{)}}}=\widetilde{F}\left(d\right)\cdot\prod_{p\in\operatorname{PF}n\setminus\operatorname{PF}d}1=\widetilde{F}\left(d\right)\end{aligned}$$

and

$$\begin{aligned}\prod_{p\in\operatorname{PF}n}p^{v_p\left(n/d\right)}&=\underbrace{\prod_{p\in\operatorname{PF}\left(n/d\right)}p^{v_p\left(n/d\right)}}_{=n/d}\cdot\prod_{p\in\operatorname{PF}n\setminus\operatorname{PF}\left(n/d\right)}\underbrace{p^{v_p\left(n/d\right)}}_{\substack{=1\\ \text{(since }p\in\operatorname{PF}n\setminus\operatorname{PF}\left(n/d\right)\\ \text{yields }p\notin\operatorname{PF}\left(n/d\right)\text{ and thus}\\ v_p\left(n/d\right)=0\text{, so that }p^{v_p\left(n/d\right)}=p^0=1\text{)}}}\\ &\qquad\left(\text{since }\left(n/d\right)\mid n\text{ yields }\operatorname{PF}\left(n/d\right)\subseteq\operatorname{PF}n\right)\\ &=n/d\cdot 1=n/d.\end{aligned}$$

Now, for every $p\in\operatorname{PF}n$, we have $v_p\left(n\right)=v_p\left(\left(n/d\right)\cdot d\right)=\underbrace{v_p\left(n/d\right)}_{\geq 0}+v_p\left(d\right)\geq v_p\left(d\right)$, and thus (2)

Definition 10. 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

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

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

$$w_{F,n}\left((x_k)_{k \in \mathbb{N}_{|n}}\right) = \sum_{d \mid n} \widetilde{F}(d) x_d^{n/d}.$$

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 $w_{F,n}\left((x_k)_{k \in N}\right)$ means $w_{F,n}\left((x_k)_{k \in \mathbb{N}_{|n}}\right)$; in other words,

$$w_{F,n}\left((x_k)_{k \in N}\right) = \sum_{d \mid n} \widetilde{F}(d) x_d^{n/d}.$$

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.*

First, here are two examples of pseudo-monotonous 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 pseudo-monotonous map, and $\widetilde{\mathrm{pr}_{\mathbb{N}}} = \mathrm{id}$ (since every $n \in \mathbb{N}_+$ satisfies $\widetilde{\mathrm{pr}_{\mathbb{N}}}(n) = \prod\limits_{p \in \mathrm{PF}\, n} \underbrace{p^{\mathrm{pr}_{\mathbb{N}}(p, v_p(n))}}_{\substack{= p^{v_p(n)} \text{ (since} \\ \mathrm{pr}_{\mathbb{N}}(p, v_p(n)) = v_p(n))}} = \prod\limits_{p \in \mathrm{PF}\, n} p^{v_p(n)} = n$). Hence, every $n \in \mathbb{N}_+$ satisfies $w_{\mathrm{pr}_{\mathbb{N}}, n} = \sum\limits_{d \mid n} \underbrace{\widetilde{\mathrm{pr}_{\mathbb{N}}}(d)}_{= \mathrm{id}(d) = d} X_d^{n/d} = \sum\limits_{d \mid n} d X_d^{n/d}$. Therefore, for every $n \in \mathbb{N}_+$, the polynomial

(applied to $a = v_p(n)$ and $b = v_p(d)$) yields

$$F(p, v_p(n)) - v_p(n) \leq F(p, v_p(d)) - v_p(d), \qquad \text{so that}$$
$$F(p, v_p(n)) \leq F(p, v_p(d)) + \underbrace{v_p(n)}_{= v_p(n/d) + v_p(d)} - v_p(d) = F(p, v_p(d)) + v_p(n/d),$$

and consequently $p^{F(p, v_p(n))} \mid p^{F(p, v_p(d)) + v_p(n/d)}$. Hence,

$$\widetilde{F}(n) = \prod_{p \in \mathrm{PF}\, n} \underbrace{p^{F(p, v_p(n))}}_{\mid p^{F(p, v_p(d)) + v_p(n/d)}} \mid \prod_{p \in \mathrm{PF}\, n} \underbrace{p^{F(p, v_p(d)) + v_p(n/d)}}_{= p^{F(p, v_p(d))} p^{v_p(n/d)}} = \underbrace{\prod_{p \in \mathrm{PF}\, n} p^{F(p, v_p(d))}}_{= \widetilde{F}(d)} \cdot \underbrace{\prod_{p \in \mathrm{PF}\, n} p^{v_p(n/d)}}_{= n/d} = \widetilde{F}(d) \cdot n/d = (n/d)\, \widetilde{F}(d).$$

$w_{\operatorname{pr}_{\mathbb{N}},n}$ is identic with the polynomial w_n defined in [4]. Because of this, all the theorems that we will prove about the polynomials $w_{F,1}$, $w_{F,2}$, $w_{F,3}$, ... will generalize the corresponding theorems about the polynomials w_1, w_2, w_3, ... in [4].

Example 2: Define the 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[9], and the map $\widetilde{\operatorname{prad}}$ is identic with the map $\operatorname{rad} : \mathbb{N}_+ \to \mathbb{N}_+$ defined by $\operatorname{rad} n = \prod\limits_{p \in \operatorname{PF} n} p$ for every $n \in \mathbb{N}_+$ (since every $n \in \mathbb{N}_+$

[9] *Proof.* By the definition of "pseudo-monotonous", the map prad is pseudo-monotonous if and only if it satisfies

$$(\operatorname{prad}(p,0) = 0 \qquad \text{for every } p \in \mathbb{P}) \qquad \text{and} \tag{5}$$

$$(\operatorname{prad}(p,a) - a \leq \operatorname{prad}(p,b) - b \qquad \text{for every } p \in \mathbb{P},\ a \in \mathbb{N} \text{ and } b \in \mathbb{N} \text{ satisfying } a \geq b). \tag{6}$$

We will now prove that it indeed satisfies these relations (5) and (6).

First of all, every $p \in \mathbb{P}$ satisfies

$$\begin{aligned} \operatorname{prad}(p,0) &= \begin{cases} 0, & \text{if } 0 = 0; \\ 1, & \text{if } 0 > 0 \end{cases} \qquad (\text{by the definition of prad}) \\ &= 0 \qquad (\text{since } 0 = 0). \end{aligned}$$

Thus, (5) is proven.

Next, let $p \in \mathbb{P}$, $a \in \mathbb{N}$ and $b \in \mathbb{N}$ be given such that $a \geq b$. We distinguish between two cases:

Case 1: We have $b = 0$.

Case 2: We have $b > 0$.

Let us consider Case 1 first. In this case, $b = 0$. By the definition of prad, we have

$$\begin{aligned} \operatorname{prad}(p,a) &= \begin{cases} 0, & \text{if } a = 0; \\ 1, & \text{if } a > 0 \end{cases} \leq \begin{cases} 0, & \text{if } a = 0; \\ a, & \text{if } a > 0 \end{cases} \qquad (\text{because } 1 \leq a \text{ in the case when } a > 0) \\ &= \begin{cases} a, & \text{if } a = 0; \\ a, & \text{if } a > 0 \end{cases} \qquad (\text{since } 0 = a \text{ in the case when } a = 0) \\ &= a, \end{aligned}$$

so that $\operatorname{prad}(p,a) - a \leq 0$. Since $b = 0$, we have $\operatorname{prad}(p,b) - b = \underbrace{\operatorname{prad}(p,0)}_{=0} - 0 = 0$. Thus, $\operatorname{prad}(p,a) - a \leq 0 = \operatorname{prad}(p,b) - b$. We have thus proven $\operatorname{prad}(p,a) - a \leq \operatorname{prad}(p,b) - b$ in Case 1.

Let us now consider Case 2. In this case, $b > 0$. Thus, the definition of prad yields $\operatorname{prad}(p,b) = \begin{cases} 0, & \text{if } b = 0; \\ 1, & \text{if } b > 0 \end{cases} = 1$ (since $b > 0$). On the other hand, $a \geq b > 0$. Hence, the definition of prad yields $\operatorname{prad}(p,a) = \begin{cases} 0, & \text{if } a = 0; \\ 1, & \text{if } a > 0 \end{cases} = 1$ (since $a > 0$). Now $\underbrace{\operatorname{prad}(p,a)}_{=1=\operatorname{prad}(p,b)} - \underbrace{a}_{\geq b} \leq \operatorname{prad}(p,b) - b$. Thus, we have proven $\operatorname{prad}(p,a) - a \leq \operatorname{prad}(p,b) - b$ in Case 2.

Hence, we have proven $\operatorname{prad}(p,a) - a \leq \operatorname{prad}(p,b) - b$ in each of the cases 1 and 2. Since these two cases cover all possibilities, this yields that $\operatorname{prad}(p,a) - a \leq \operatorname{prad}(p,b) - b$ always holds.

Now, forget that we fixed p, a and b. We thus have proven that $\operatorname{prad}(p,a) - a \leq \operatorname{prad}(p,b) - b$ for every $p \in \mathbb{P}$, $a \in \mathbb{N}$ and $b \in \mathbb{N}$ satisfying $a \geq b$. In other words, we have proven (6).

Recall that the map prad is pseudo-monotonous if and only if it satisfies the relations (5) and (6). Since we have proven that it satisfies the relations (5) and (6), we thus conclude that the map prad is pseudo-monotonous, qed.

satisfies

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

). Hence, every $n \in \mathbb{N}_+$ satisfies $w_{\text{prad},n} = \sum\limits_{d|n} \underbrace{\widetilde{\operatorname{prad}}\left(d\right)}_{=\operatorname{rad} d} X_d^{n/d} = \sum\limits_{d|n} \left(\operatorname{rad} d\right) X_d^{n/d}$. Therefore, for every $n \in \mathbb{N}_+$, the polynomial $w_{\text{prad},n}$ is identic with the polynomial $\sqrt[\infty]{w}_n$ defined in [6]. Because of this, all the theorems that we will prove about the polynomials $w_{F,1}$, $w_{F,2}$, $w_{F,3}$, ... will generalize the corresponding theorems about the polynomials $\sqrt[\infty]{w}_1$, $\sqrt[\infty]{w}_2$, $\sqrt[\infty]{w}_3$, ... in [6]. This is not to say that we will be able to generalize all results from [6] to our polynomials $w_{F,1}$, $w_{F,2}$, $w_{F,3}$, ... In fact, Theorem 4' in [6] doesn't follow from any of the theorems below.

Now, we start by recalling some properties of primes and commutative rings:

> **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, $I_1 I_2 ... I_N \cdot M = I_1 M \cap I_2 M \cap ... \cap I_N M$.

We will not prove this Theorem 1 here, since it is identic with Theorem 1 in [4] and was proven in [4].

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

> **Corollary 2.**[10] Let A be an Abelian group (written additively). Let $n \in \mathbb{N}_+$. Let $F : \mathbb{P} \times \mathbb{N} \to \mathbb{N}$ be a pseudo-monotonous map. Then, $\widetilde{F}\left(n\right) A = \bigcap\limits_{p\in\operatorname{PF}n} \left(p^{F(p,v_p(n))} A\right)$.

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, $\prod\limits_{i=1}^{N} p_i^{F\left(p_i, v_{p_i}(n)\right)} = \prod\limits_{p\in\operatorname{PF}n} p^{F(p,v_p(n))} = \widetilde{F}\left(n\right)$.

Define an ideal I_i of $\mathbb{Z}$ by $I_i = p_i^{F\left(p_i, v_{p_i}(n)\right)} \mathbb{Z}$ 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 $p_i^{F\left(p_i, v_{p_i}(n)\right)}$ and $p_j^{F\left(p_j, v_{p_j}(n)\right)}$ are coprime[11], and thus, by Bezout's theorem, there exist integers α and β such that $1 = p_i^{F\left(p_i, v_{p_i}(n)\right)} \alpha + p_j^{F\left(p_j, v_{p_j}(n)\right)} \beta$ in $\mathbb{Z}$, and therefore $1 = \underbrace{p_i^{F\left(p_i, v_{p_i}(n)\right)} \alpha}_{\in p_i^{F\left(p_i, v_{p_i}(n)\right)} \mathbb{Z} = I_i} + \underbrace{p_j^{F\left(p_j, v_{p_j}(n)\right)} \beta}_{\in p_j^{F\left(p_j, v_{p_j}(n)\right)} \mathbb{Z} = I_j} \in I_i + I_j$ in $\mathbb{Z}$, and thus $I_i + I_j = \mathbb{Z}$). Hence,

[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)

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

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

$$= \underbrace{\left(\prod_{i=1}^{N} p_i^{F\left(p_i, v_{p_i}(n)\right)} \right)}_{=\widetilde{F}(n)} \mathbb{Z} \cdot A = \widetilde{F}(n) \mathbb{Z} \cdot A = \widetilde{F}(n) A$$

and

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

(since $\operatorname{PF} n = \{p_1, p_2, ..., p_N\}$), this becomes $\widetilde{F}(n) A = \bigcap_{p \in \operatorname{PF} n} \left(p^{F(p, v_p(n))} A \right)$. Corollary 2 is thus proven.

Another fact we will use:

Lemma 3. Let A be a commutative ring with unity, and $p \in \mathbb{N}$ be a nonnegative integer[12]. Let $k \in \mathbb{N}$ and $\ell \in \mathbb{N}$ be such that $k > 0$. Let $a \in A$ and $b \in A$. If $a \equiv b \operatorname{mod} p^k A$, then $a^{p^\ell} \equiv b^{p^\ell} \operatorname{mod} p^{k+\ell} A$.

This lemma was proven in [3], Lemma 3.

The following result generalizes Theorem 4 in [4]:

Theorem 4. Let N be a nest. Let $F : \mathbb{P} \times \mathbb{N} \to \mathbb{N}$ be a pseudo-monotonous map. 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

$$\left(\varphi_p(a) \equiv a^p \operatorname{mod} pA \text{ holds for every } a \in A \text{ and } p \in \mathbb{P} \cap N \right). \qquad (7)$$

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

$$\varphi_p\left(b_{n/p}\right) \equiv b_n \operatorname{mod} p^{F(p, v_p(n))} A. \qquad (8)$$

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

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

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

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

Proof of the implication $\mathcal{D} \Longrightarrow \mathcal{C}$: 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

$$\left(b_n = w_{F,n}\left((x_k)_{k\in N}\right) \text{ for every } n \in N\right). \tag{9}$$

We want to prove that Assertion $\mathcal{C}$ holds, i. e., that every $n \in N$ and every $p \in \operatorname{PF} n$ satisfies (8). 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 [13]). Thus, applying (9) to n/p instead of n yields $b_{n/p} = w_{F,n/p}\left((x_k)_{k\in N}\right)$. But $w_{F,n/p}\left((x_k)_{k\in N}\right) = \sum\limits_{d\mid(n/p)} \widetilde{F}(d)\, x_d^{(n/p)/d}$ and $w_{F,n}\left((x_k)_{k\in N}\right) = \sum\limits_{d\mid n} \widetilde{F}(d)\, x_d^{n/d}$. Now, (9) yields

$$b_n = w_{F,n}\left((x_k)_{k\in N}\right) = \sum_{d\mid n} \widetilde{F}(d)\, x_d^{n/d} = \sum_{\substack{d\mid n;\\ d\mid(n/p)}} \widetilde{F}(d)\, x_d^{n/d} + \sum_{\substack{d\mid n;\\ d\nmid(n/p)}} \widetilde{F}(d)\, x_d^{n/d}. \tag{10}$$

But for any divisor d of n, the assertions $d \nmid (n/p)$ and $p^{v_p(n)} \mid d$ are equivalent[14]. Hence, every divisor d of n which satisfies $d \nmid (n/p)$ must satisfy $\widetilde{F}(d) \equiv 0 \bmod p^{F(p,v_p(n))}A$ [15]. Thus,

$$\sum_{\substack{d\mid n;\\ d\nmid(n/p)}} \underbrace{\widetilde{F}(d)}_{\equiv 0 \bmod p^{F(p,v_p(n))}A} x_d^{n/d} \equiv \sum_{\substack{d\mid n;\\ d\nmid(n/p)}} 0 x_d^{n/d} = 0 \bmod p^{F(p,v_p(n))}A.$$

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

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

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

[15] In fact, let d be a divisor of n satisfying $d \nmid (n/p)$. Then, $p^{v_p(n)} \mid d$ (since the assertions $d \nmid (n/p)$ and $p^{v_p(n)} \mid d$ are equivalent), so that $v_p(d) \geq v_p(n)$. Together with $v_p(d) \leq v_p(n)$ (which is because $d \mid n$ yields $\frac{n}{d} \in \mathbb{Z}$, thus $v_p\left(\frac{n}{d}\right) \geq 0$ and now $v_p(n) = v_p\left(d\frac{n}{d}\right) = v_p(d) + \underbrace{v_p\left(\frac{n}{d}\right)}_{\geq 0} \geq v_p(d)$), this becomes $v_p(d) = v_p(n)$. Hence, the equality $v_p\left(\widetilde{F}(d)\right) = F(p, v_p(d))$ (which follows from (3), applied to d instead of n) rewrites as $v_p\left(\widetilde{F}(d)\right) = F(p, v_p(n))$, so that $p^{F(p,v_p(n))} \mid \widetilde{F}(d)$, and thus $\widetilde{F}(d) \equiv 0 \bmod p^{F(p,v_p(n))}A$.

Thus, (10) becomes

$$\begin{aligned} b_n &= \underbrace{\sum_{\substack{d\mid n;\\ d\mid (n/p)}}}_{=\sum_{d\mid (n/p)}} \widetilde{F}(d)\, x_d^{n/d} + \underbrace{\sum_{\substack{d\mid n;\\ d\nmid (n/p)}} \widetilde{F}(d)\, x_d^{n/d}}_{\equiv 0 \operatorname{mod} p^{F(p,v_p(n))}A} \equiv \sum_{d\mid (n/p)} \widetilde{F}(d)\, x_d^{n/d} + 0 \\ &= \sum_{d\mid (n/p)} \widetilde{F}(d)\, x_d^{n/d} \operatorname{mod} p^{F(p,v_p(n))}A. \qquad (11) \end{aligned}$$

On the other hand,

$$b_{n/p} = w_{F,n/p}\left((x_k)_{k\in N}\right) = \sum_{d\mid (n/p)} \widetilde{F}(d)\, x_d^{(n/p)/d} \qquad \text{yields}$$

$$\varphi_p\left(b_{n/p}\right) = \varphi_p\left(\sum_{d\mid (n/p)} \widetilde{F}(d)\, x_d^{(n/p)/d}\right) = \sum_{d\mid (n/p)} \widetilde{F}(d)\left(\varphi_p(x_d)\right)^{(n/p)/d} \qquad (12)$$

(since φ_p is a ring endomorphism).

Now, let d be a divisor of n/p. Then, $d \mid (n/p) \mid n$, so that $\frac{n}{d} \in \mathbb{Z}$ and thus $v_p\left(\frac{n}{d}\right) \geq 0$. Let $\alpha = v_p((n/p)/d)$ and $\beta = v_p\left(\widetilde{F}(d)\right)$. Clearly, $v_p(n) = v_p\left(d\frac{n}{d}\right) = v_p(d) + \underbrace{v_p\left(\frac{n}{d}\right)}_{\geq 0} \geq v_p(d)$ yields $F(p, v_p(n)) - v_p(n) \leq F(p, v_p(d)) - v_p(d)$ (by (2), applied to $a = v_p(n)$ and $b = v_p(d)$), and thus $F(p, v_p(d)) \geq F(p, v_p(n)) - v_p(n) + v_p(d)$. Since $\beta = v_p\left(\widetilde{F}(d)\right) = F(p, v_p(d))$ (by (3), applied to d instead of n), this becomes

$$\beta \geq F(p, v_p(n)) - v_p(n) + v_p(d).$$

Adding the equality $\alpha = v_p((n/p)/d)$ to this inequality, we obtain

$$\begin{aligned} \alpha + \beta &\geq v_p((n/p)/d) + F(p, v_p(n)) - v_p(n) + v_p(d) \\ &= \underbrace{v_p((n/p)/d) + v_p(d)}_{=v_p(((n/p)/d)\cdot d) = v_p(n/p)} + F(p, v_p(n)) - \underbrace{v_p(n)}_{\substack{=v_p(p\cdot(n/p))\\ =v_p(p)+v_p(n/p)}} \\ &= F(p, v_p(n)) - \underbrace{v_p(p)}_{=1} = F(p, v_p(n)) - 1, \end{aligned}$$

so that $1 + \alpha + \beta \geq F(p, v_p(n))$.

Besides, $\alpha = v_p((n/p)/d)$ yields $p^\alpha \mid (n/p)/d$, so that there exists some $\nu \in \mathbb{N}$ such that $(n/p)/d = p^\alpha \nu$. Finally, $\beta = v_p\left(\widetilde{F}(d)\right)$ yields $p^\beta \mid \widetilde{F}(d)$, so that there exists some $\kappa \in \mathbb{N}$ such that $\widetilde{F}(d) = \kappa p^\beta$. Applying Lemma 3 to the values $k = 1$, $\ell = \alpha$, $a = \varphi_p(x_d)$ and $b = x_d^p$ (which satisfy $a \equiv b \operatorname{mod} p^k A$ because of (7), applied to $a = x_d$) yields $(\varphi_p(x_d))^{p^\alpha} \equiv \left(x_d^p\right)^{p^\alpha} \operatorname{mod} p^{1+\alpha}A$. Using the equation $(n/p)/d = p^\alpha \nu$, we get

$$\begin{aligned}
\left(\varphi_p\left(x_d\right)\right)^{(n/p)/d} &= \left(\varphi_p\left(x_d\right)\right)^{p^\alpha \nu} = \left(\left(\varphi_p\left(x_d\right)\right)^{p^\alpha}\right)^\nu \\
&\equiv \left(\left(x_d^p\right)^{p^\alpha}\right)^\nu \qquad \left(\text{since } \left(\varphi_p\left(x_d\right)\right)^{p^\alpha} \equiv \left(x_d^p\right)^{p^\alpha} \operatorname{mod} p^{1+\alpha} A\right) \\
&= \left(x_d^p\right)^{p^\alpha \nu} = \left(x_d^p\right)^{(n/p)/d} \qquad \left(\text{since } p^\alpha \nu = (n/p)/d\right) \\
&= \left(x_d^p\right)^{(n/d)/p} = x_d^{n/d} \operatorname{mod} p^{1+\alpha} A.
\end{aligned}$$

Multiplying this congruence with p^β, we obtain

$$p^\beta \left(\varphi_p\left(x_d\right)\right)^{(n/p)/d} \equiv p^\beta x_d^{n/d} \operatorname{mod} p^{1+\alpha+\beta} A.$$

As a consequence of this,

$$p^\beta \left(\varphi_p\left(x_d\right)\right)^{(n/p)/d} \equiv p^\beta x_d^{n/d} \operatorname{mod} p^{F(p, v_p(n))} A$$

(since $1+\alpha+\beta \geq F\left(p, v_p(n)\right)$ and hence $p^{1+\alpha+\beta} A \subseteq p^{F(p, v_p(n))} A$). Now, multiplying this congruence with κ, we get

$$\kappa p^\beta \left(\varphi_p\left(x_d\right)\right)^{(n/p)/d} \equiv \kappa p^\beta x_d^{n/d} \operatorname{mod} p^{F(p, v_p(n))} A,$$

which rewrites as

$$\widetilde{F}(d) \left(\varphi_p\left(x_d\right)\right)^{(n/p)/d} \equiv \widetilde{F}(d)\, x_d^{n/d} \operatorname{mod} p^{F(p, v_p(n))} A$$

(since $\kappa p^\beta = \widetilde{F}(d)$). Hence, (12) becomes

$$\varphi_p\left(b_{n/p}\right) = \sum_{d \mid (n/p)} \underbrace{\widetilde{F}(d) \left(\varphi_p\left(x_d\right)\right)^{(n/p)/d}}_{\equiv \widetilde{F}(d) x_d^{n/d} \operatorname{mod} p^{F(p, v_p(n))} A} \equiv \sum_{d \mid (n/p)} \widetilde{F}(d)\, x_d^{n/d} \equiv b_n \operatorname{mod} p^{F(p, v_p(n))} A$$

(by (11)). This proves (8), and thus Assertion $\mathcal{C}$ is proven. We have therefore shown the implication $\mathcal{D} \Longrightarrow \mathcal{C}$.

Proof of the implication $\mathcal{C} \Longrightarrow \mathcal{D}$: Assume that Assertion $\mathcal{C}$ holds. That is, every $n \in N$ and every $p \in \operatorname{PF} n$ satisfies (8).

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

$$b_m = \sum_{d \mid m} \widetilde{F}(d)\, x_d^{m/d} \tag{13}$$

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 (13) holds for every $m \in N \cap \{1, 2, ..., n-1\}$. Now, we must construct an element $x_n \in A$ such that (13) 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 [16] and in $\{1, 2, ..., n-1\}$ [17], 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 [18]). Besides, $n/p \in \{1, 2, ..., n-1\}$.

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

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

[18] 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 (13) holds for every $m \in N \cap \{1, 2, ..., n-1\}$, we can thus conclude that (13) holds for $m = n/p$. In other words, $b_{n/p} = \sum\limits_{d \mid (n/p)} \widetilde{F}(d)\, x_d^{(n/p)/d}$. From this equation, we can conclude (by the same reasoning as in the proof of the implication $\mathcal{D} \Longrightarrow \mathcal{C}$) that

$$\varphi_p\left(b_{n/p}\right) \equiv \sum_{d \mid (n/p)} \widetilde{F}(d)\, x_d^{n/d} \mod p^{F(p, v_p(n))} A.$$

Comparing this with (8), we obtain

$$\sum_{d \mid (n/p)} \widetilde{F}(d)\, x_d^{n/d} \equiv b_n \mod p^{F(p, v_p(n))} A. \qquad (14)$$

Now, every divisor d of n which satisfies $d \nmid (n/p)$ must satisfy $\widetilde{F}(d) \equiv 0 \mod p^{F(p, v_p(n))} A$ [19]. Thus,

$$\sum_{\substack{d \mid n; \\ d \nmid (n/p); \\ d \neq n}} \underbrace{\widetilde{F}(d)}_{\equiv 0 \mod p^{F(p, v_p(n))} A} x_d^{n/d} \equiv \sum_{\substack{d \mid n; \\ d \nmid (n/p); \\ d \neq n}} 0 x_d^{n/d} = 0 \mod p^{F(p, v_p(n))} A.$$

Hence,

$$\sum_{\substack{d \mid n; \\ d \neq n}} \widetilde{F}(d)\, x_d^{n/d} = \underbrace{\sum_{\substack{d \mid n; \\ d \nmid (n/p); \\ d \neq n}} \widetilde{F}(d)\, x_d^{n/d}}_{\equiv 0 \mod p^{F(p, v_p(n))} A} + \sum_{\substack{d \mid n; \\ d \mid (n/p); \\ d \neq n}} \widetilde{F}(d)\, x_d^{n/d} \equiv \sum_{\substack{d \mid n; \\ d \mid (n/p); \\ d \neq n}} \widetilde{F}(d)\, x_d^{n/d} = \sum_{\substack{d \mid n; \\ d \mid (n/p)}} \widetilde{F}(d)\, x_d^{n/d}$$

$$\left(\begin{array}{c} \text{since for any divisor } d \text{ of } n \text{, the assertions } (d \mid (n/p) \text{ and } d \neq n) \text{ and } d \mid (n/p) \\ \text{are equivalent, because if } d \mid (n/p)\text{, then } d \neq n \text{ (since } n \nmid (n/p)\text{)} \end{array}\right)$$

$$= \sum_{d \mid (n/p)} \widetilde{F}(d)\, x_d^{n/d} \equiv b_n \mod p^{F(p, v_p(n))} A \qquad (\text{by (14)}).$$

In other words,

$$b_n - \sum_{\substack{d \mid n; \\ d \neq n}} \widetilde{F}(d)\, x_d^{n/d} \in p^{F(p, v_p(n))} A.$$

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

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

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

Fix such an x_n. We now claim that this element x_n satisfies (13) for $m = n$. In fact,

$$\sum_{d \mid n} \widetilde{F}(d)\, x_d^{n/d} = \sum_{\substack{d \mid n; \\ d \neq n}} \widetilde{F}(d)\, x_d^{n/d} + \underbrace{\sum_{\substack{d \mid n; \\ d = n}} \widetilde{F}(d)\, x_d^{n/d}}_{= \widetilde{F}(n) x_n^{n/n} = \widetilde{F}(n) x_n^1 = \widetilde{F}(n) x_n} = \sum_{\substack{d \mid n; \\ d \neq n}} \widetilde{F}(d)\, x_d^{n/d} + \widetilde{F}(n)\, x_n = b_n$$

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

(since $b_n - \sum\limits_{\substack{d\mid n;\\ d\neq n}} \widetilde{F}(d)\, x_d^{n/d} = \widetilde{F}(n)\, x_n$). Hence, (13) 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 (13) for every $m \in N$. Therefore, this family satisfies

$$\begin{aligned} b_n &= \sum_{d\mid n} \widetilde{F}(d)\, x_d^{n/d} \qquad \text{(by (13), applied to } m = n\text{)} \\ &= w_{F,n}\left((x_k)_{k\in N}\right) \end{aligned}$$

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

Now that both implications $\mathcal{D} \Longrightarrow \mathcal{C}$ and $\mathcal{C} \Longrightarrow \mathcal{D}$ are verified, Theorem 4 is proven.

Next, we will show a result similar to Theorem 4[20]:

Theorem 5. Let N be a nest. Let $F : \mathbb{P} \times \mathbb{N} \to \mathbb{N}$ be a pseudo-monotonous map. 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

$$(\varphi_1 = \mathrm{id}) \qquad \text{and} \tag{15}$$

$$(\varphi_n \circ \varphi_m = \varphi_{nm} \text{ for every } n \in N \text{ and every } m \in N \text{ satisfying } nm \in N). \tag{16}$$

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

$$\varphi_p\left(b_{n/p}\right) \equiv b_n \mod p^{F(p, v_p(n))} A. \tag{17}$$

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

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

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

$$\sum_{d\mid n} \mu(d)\, \varphi_d\left(b_{n/d}\right) \in \widetilde{F}(n)\, A.$$

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

$$\sum_{d\mid n} \phi(d)\, \varphi_d\left(b_{n/d}\right) \in \widetilde{F}(n)\, A.$$

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

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

[20] 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.

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

$$\mu(n) = \begin{cases} (-1)^{|\operatorname{PF} n|}, \text{ if } (v_p(n) \leq 1 \text{ for every } p \in \operatorname{PF} n) \\ 0, \text{ otherwise} \end{cases}. \tag{18}$$

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

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

We will need some basic properties of the functions μ and ϕ:

Theorem 6. Any $n \in \mathbb{N}_+$ satisfies the five identities

$$\mu(n) = \begin{cases} (-1)^{|\operatorname{PF} n|}, \text{ if } n = \prod\limits_{p \in \operatorname{PF} n} p \\ 0, \text{ otherwise} \end{cases} \tag{19}$$

$$\sum_{d|n} \phi(d) = n; \tag{20}$$

$$\sum_{d|n} \mu(d) = [n = 1]; \tag{21}$$

$$\sum_{d|n} \mu(d) \frac{n}{d} = \phi(n); \tag{22}$$

$$\sum_{d|n} d\mu(d) \phi\left(\frac{n}{d}\right) = \mu(n). \tag{23}$$

Here, for any assertion $\varkappa$, we denote by $[\varkappa]$ the truth value of $\varkappa$ (defined by $[\varkappa] = \begin{cases} 1, \text{ if } \varkappa \text{ is true;} \\ 0, \text{ if } \varkappa \text{ is false} \end{cases}$).

This Theorem 6 is exactly identical to Theorem 6 in [4], and therefore we will not prove it here.

Proof of Theorem 5. First, we are going to prove the equivalence of the assertions $\mathcal{C}$ and $\mathcal{E}$. In order to do this, we will prove the implications $\mathcal{E} \Longrightarrow \mathcal{C}$ and $\mathcal{C} \Longrightarrow \mathcal{E}$.

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

$$\left(b_n = \sum_{d|n} \widetilde{F}(d) \varphi_{n/d}(y_d) \text{ for every } n \in N\right). \tag{24}$$

We want to prove that Assertion $\mathcal{C}$ holds, i. e., that every $n \in N$ and every $p \in \operatorname{PF} n$ satisfies (17). 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 [21]). Thus, applying (24) to n/p instead of n yields $b_{n/p} = \sum\limits_{d|(n/p)} \widetilde{F}(d) \varphi_{(n/p)/d}(y_d)$. Now, (24) yields

$$b_n = \sum_{d|n} \widetilde{F}(d) \varphi_{n/d}(y_d) = \sum_{\substack{d|n; \\ d|(n/p)}} \widetilde{F}(d) \varphi_{n/d}(y_d) + \sum_{\substack{d|n; \\ d\nmid(n/p)}} \widetilde{F}(d) \varphi_{n/d}(y_d). \tag{25}$$

But every divisor d of n which satisfies $d \nmid (n/p)$ must satisfy $\widetilde{F}(d) \equiv 0 \mod p^{F(p, v_p(n))} A$ [22].

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

[22] This has already been proven during our proof of Theorem 4.

Thus,

$$\sum_{\substack{d\mid n;\\ d\nmid(n/p)}} \underbrace{\widetilde{F}(d)}_{\equiv 0 \operatorname{mod} p^{F(p,v_p(n))}A} \varphi_{n/d}(y_d) \equiv \sum_{\substack{d\mid n;\\ d\nmid(n/p)}} 0\varphi_{n/d}(y_d) = 0 \operatorname{mod} p^{F(p,v_p(n))}A.$$

Thus, (25) becomes

$$b_n = \sum_{\substack{d\mid n;\\ d\mid(n/p)}} \widetilde{F}(d)\varphi_{n/d}(y_d) + \underbrace{\sum_{\substack{d\mid n;\\ d\nmid(n/p)}} \widetilde{F}(d)\varphi_{n/d}(y_d)}_{\equiv 0 \operatorname{mod} p^{F(p,v_p(n))}A} \equiv \sum_{\substack{d\mid n;\\ d\mid(n/p)}} \widetilde{F}(d)\varphi_{n/d}(y_d) + 0 = \sum_{\substack{d\mid n;\\ d\mid(n/p)}} \widetilde{F}(d)\varphi_{n/d}(y_d)$$

$$= \sum_{d\mid(n/p)} \widetilde{F}(d)\varphi_{n/d}(y_d) \operatorname{mod} p^{F(p,v_p(n))}A. \qquad (26)$$

On the other hand, $b_{n/p} = \sum\limits_{d\mid(n/p)} \widetilde{F}(d)\varphi_{(n/p)/d}(y_d)$ yields

$$\begin{aligned}\varphi_p(b_{n/p}) &= \varphi_p\left(\sum_{d\mid(n/p)} \widetilde{F}(d)\varphi_{(n/p)/d}(y_d)\right)\\ &= \sum_{d\mid(n/p)} \widetilde{F}(d)\underbrace{\varphi_p\left(\varphi_{(n/p)/d}(y_d)\right)}_{=\left(\varphi_p\circ\varphi_{(n/p)/d}\right)(y_d)} \qquad \text{(since } \varphi_p \text{ is a group endomorphism)}\\ &= \sum_{d\mid(n/p)} \widetilde{F}(d)\underbrace{\left(\varphi_p\circ\varphi_{(n/p)/d}\right)}_{=\varphi_{p\cdot(n/p)/d} \text{ (due to (16))}}(y_d)\\ &= \sum_{d\mid(n/p)} \widetilde{F}(d)\underbrace{\varphi_{p\cdot(n/p)/d}}_{=\varphi_{n/d}}(y_d) = \sum_{d\mid(n/p)} \widetilde{F}(d)\varphi_{n/d}(y_d) \equiv b_n \operatorname{mod} p^{F(p,v_p(n))}A\end{aligned}$$

(by (26)). In other words, (17) is satisfied, and thus Assertion $\mathcal{C}$ is proven. We have therefore shown the implication $\mathcal{E} \Longrightarrow \mathcal{C}$.

Proof of the implication $\mathcal{C} \Longrightarrow \mathcal{E}$*:* Assume that Assertion $\mathcal{C}$ holds. That is, every $n \in N$ and every $p \in \operatorname{PF} n$ satisfies (17).

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

$$b_m = \sum_{d\mid m} \widetilde{F}(d)\varphi_{m/d}(y_d) \qquad (27)$$

for every $m \in N$.

In fact, let $n \in N$, and assume that we have already constructed an element $y_m \in A$ for every $m \in N \cap \{1, 2, ..., n-1\}$ in such a way that (27) holds for every $m \in N \cap \{1, 2, ..., n-1\}$. Now, we must construct an element $y_n \in A$ such that (27) is also satisfied for $m = n$.

Our assumption says that we have already constructed an element $y_m \in A$ for every $m \in N \cap \{1, 2, ..., n-1\}$. In particular, this yields that we have already constructed an element $y_d \in A$ for every divisor d of n satisfying $d \neq n$ (in fact, every such divisor d of n must lie in N [23] and in $\{1,2,...,n-1\}$ [24], 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 [25]). Besides, $n/p \in \{1,2,...,n-1\}$. Hence, $n/p \in N \cap \{1,2,...,n-1\}$. Since (by our assumption) the equation (27) holds for every $m \in N \cap \{1,2,...,n-1\}$, we can thus conclude that (27) holds for $m = n/p$. In other words, $b_{n/p} = \sum\limits_{d|(m/p)} \widetilde{F}(d)\,\varphi_{(m/p)/d}(y_d)$. From this equation, we can conclude (by the same reasoning as in the proof of the implication $\mathcal{E} \Longrightarrow \mathcal{C}$) that

$$\varphi_p\left(b_{n/p}\right) = \sum_{d|(n/p)} \widetilde{F}(d)\,\varphi_{n/d}(y_d).$$

Comparing this with (17), we obtain

$$\sum_{d|(n/p)} \widetilde{F}(d)\,\varphi_{n/d}(y_d) \equiv b_n \bmod p^{F(p,v_p(n))}A. \tag{28}$$

Now, every divisor d of n which satisfies $d \nmid (n/p)$ must satisfy $\widetilde{F}(d) \equiv 0 \bmod p^{F(p,v_p(n))}A$ [26]. Thus,

$$\sum_{\substack{d|n;\\ d\nmid(n/p);\\ d\neq n}} \underbrace{\widetilde{F}(d)}_{\equiv 0 \bmod p^{F(p,v_p(n))}A} \varphi_{n/d}(y_d) \equiv \sum_{\substack{d|n;\\ d\nmid(n/p);\\ d\neq n}} 0\varphi_{n/d}(y_d) = 0 \bmod p^{F(p,v_p(n))}A.$$

Hence,

$$\begin{aligned}
&\sum_{\substack{d|n;\\ d\neq n}} \widetilde{F}(d)\,\varphi_{n/d}(y_d) = \underbrace{\sum_{\substack{d|n;\\ d\nmid(n/p);\\ d\neq n}} \widetilde{F}(d)\,\varphi_{n/d}(y_d)}_{\equiv 0 \bmod p^{F(p,v_p(n))}A} + \sum_{\substack{d|n;\\ d|(n/p);\\ d\neq n}} \widetilde{F}(d)\,\varphi_{n/d}(y_d) \equiv \sum_{\substack{d|n;\\ d|(n/p);\\ d\neq n}} \widetilde{F}(d)\,\varphi_{n/d}(y_d) \\
&= \sum_{\substack{d|n;\\ d|(n/p)}} \widetilde{F}(d)\,\varphi_{n/d}(y_d) \\
&\qquad \left(\begin{array}{c}\text{since for any divisor } d \text{ of } n\text{, the assertions } (d \mid (n/p) \text{ and } d \neq n) \text{ and } d \mid (n/p) \\ \text{are equivalent, because if } (d \mid (n/p))\text{, then } d \neq n \text{ (since } n \nmid (n/p)\text{)}\end{array}\right) \\
&= \sum_{d|(n/p)} \widetilde{F}(d)\,\varphi_{n/d}(y_d) \equiv b_n \bmod p^{F(p,v_p(n))}A \qquad \text{(by (28))}.
\end{aligned}$$

In other words,

$$b_n - \sum_{\substack{d|n;\\ d\neq n}} \widetilde{F}(d)\,\varphi_{n/d}(y_d) \in p^{F(p,v_p(n))}A.$$

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

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

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

[26] This has already been proven during our proof of Theorem 4.

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

$$b_n - \sum_{\substack{d \mid n;\\ d \neq n}} \widetilde{F}(d) \varphi_{n/d}(y_d) \in \bigcap_{p \in \operatorname{PF} n} \left(p^{F(p, v_p(n))} A \right) = \widetilde{F}(n) A \qquad \text{(by Corollary 2)}.$$

Hence, there exists an element y_n of A that satisfies $b_n - \sum\limits_{\substack{d \mid n;\\ d \neq n}} \widetilde{F}(d) \varphi_{n/d}(y_d) = \widetilde{F}(n) y_n$. Fix such a y_n. We now claim that this element y_n satisfies (27) for $m = n$. In fact,

$$\sum_{d \mid n} \widetilde{F}(d) \varphi_{n/d}(y_d) = \sum_{\substack{d \mid n;\\ d \neq n}} \widetilde{F}(d) \varphi_{n/d}(y_d) + \underbrace{\sum_{\substack{d \mid n;\\ d = n}} \widetilde{F}(d) \varphi_{n/d}(y_d)}_{\substack{= \widetilde{F}(n) \varphi_{n/n}(y_n) = \widetilde{F}(n) \varphi_1(y_n) = \widetilde{F}(n) y_n, \\ \text{due to (15)}}}$$

$$= \sum_{\substack{d \mid n;\\ d \neq n}} \widetilde{F}(d) \varphi_{n/d}(y_d) + \widetilde{F}(n) y_n = b_n$$

(since $b_n - \sum\limits_{\substack{d \mid n;\\ d \neq n}} \widetilde{F}(d) \varphi_{n/d}(y_d) = \widetilde{F}(n) y_n$). Hence, (27) is satisfied for $m = n$. This shows that we can recursively construct a family $(y_n)_{n \in N} \in A^N$ of elements of A which satisfies the equation (27) for every $m \in N$. Therefore, this family satisfies $b_n = \sum\limits_{d \mid n} \widetilde{F}(d) \varphi_{n/d}(y_d)$ for every $n \in N$ (by (27), applied to $m = n$). So we have proven that there exists a family $(y_n)_{n \in N} \in A^N$ which satisfies $b_n = \sum\limits_{d \mid n} \widetilde{F}(d) \varphi_{n/d}(y_d)$ for every $n \in N$. In other words, we have proven Assertion $\mathcal{E}$. Thus, the implication $\mathcal{C} \Longrightarrow \mathcal{E}$ is proven.

Since both implications $\mathcal{C} \Longrightarrow \mathcal{E}$ and $\mathcal{E} \Longrightarrow \mathcal{C}$ are proven now, we can conclude that $\mathcal{C} \Longleftrightarrow \mathcal{E}$. Next we are going to show that $\mathcal{E} \Longleftrightarrow \mathcal{F}$.

Proof of the implication $\mathcal{E} \Longrightarrow \mathcal{F}$: Assume that Assertion $\mathcal{E}$ holds. That is, there exists a family $(y_n)_{n \in N} \in A^N$ of elements of A such that (24) holds. Then, every $n \in N$

satisfies

$$\sum_{d\mid n}\mu(d)\,\varphi_d\left(b_{n/d}\right) = \sum_{e\mid n}\mu(e)\,\varphi_e\left(b_{n/e}\right) \qquad \text{(here we substituted e for d in the sum)}$$

$$= \sum_{e\mid n}\mu(e)\,\underbrace{\varphi_e\left(\sum_{d\mid(n/e)}\widetilde{F}(d)\,\varphi_{(n/e)/d}(y_d)\right)}_{\substack{=\sum_{d\mid(n/e)}\widetilde{F}(d)\varphi_e\left(\varphi_{(n/e)/d}(y_d)\right)\\ \text{(since φ_e is a group endomorphism)}}} \qquad \left(\begin{array}{c}\text{since } b_{n/e}=\sum\limits_{d\mid(n/e)}\widetilde{F}(d)\,\varphi_{(n/e)/d}(y_d)\\ \text{by (24) (applied to n/e instead of n)}\end{array}\right)$$

$$= \sum_{e\mid n}\mu(e)\underbrace{\sum_{d\mid(n/e)}}_{=\sum_{\substack{d\mid n;\\ d\mid(n/e)}}}\widetilde{F}(d)\,\underbrace{\varphi_e\left(\varphi_{(n/e)/d}(y_d)\right)}_{=\left(\varphi_e\circ\varphi_{(n/e)/d}\right)(y_d)} = \sum_{e\mid n}\mu(e)\sum_{\substack{d\mid n;\\ d\mid(n/e)}}\widetilde{F}(d)\left(\varphi_e\circ\varphi_{(n/e)/d}\right)(y_d)$$

$$= \underbrace{\sum_{e\mid n}\sum_{\substack{d\mid n;\\ d\mid(n/e)}}}_{=\sum_{d\mid n}\sum_{\substack{e\mid n;\\ d\mid(n/e)}}}\mu(e)\,\widetilde{F}(d)\left(\underbrace{\varphi_e\circ\varphi_{(n/e)/d}}_{\substack{=\varphi_{e\cdot(n/e)/d}\\ \text{(by (16))}}}\right)(y_d) = \sum_{d\mid n}\sum_{\substack{e\mid n;\\ d\mid(n/e)}}\mu(e)\,\widetilde{F}(d)\,\underbrace{\varphi_{e\cdot(n/e)/d}}_{=\varphi_{n/d}}(y_d)$$

$$= \sum_{d\mid n}\sum_{\substack{e\mid n;\\ d\mid(n/e)}}\mu(e)\,\widetilde{F}(d)\,\varphi_{n/d}(y_d) = \sum_{d\mid n}\underbrace{\sum_{\substack{e\mid n;\\ e\mid(n/d)}}}_{=\sum_{e\mid(n/d)}}\mu(e)\,\widetilde{F}(d)\,\varphi_{n/d}(y_d)$$

(since for any $d \mid n$ and any integer e, the assertion $d \mid (n/e)$ is equivalent to $e \mid (n/d)$)

$$= \sum_{d\mid n}\sum_{e\mid(n/d)}\mu(e)\,\widetilde{F}(d)\,\varphi_{n/d}(y_d) = \sum_{d\mid n}[n=d]\,\widetilde{F}(d)\,\varphi_{n/d}(y_d)$$

$$\left(\text{since (21) (with n and d replaced by n/d and e) yields } \sum_{e\mid(n/d)}\mu(e) = [n/d=1] = [n=d]\right)$$

$$= \sum_{\substack{d\mid n;\\ d\neq n}}\underbrace{[n=d]}_{=0 \text{ (since } d\neq n)}\widetilde{F}(d)\,\varphi_{n/d}(y_d) + \underbrace{\sum_{\substack{d\mid n;\\ d=n}}[n=d]\,\widetilde{F}(d)\,\varphi_{n/d}(y_d)}_{=[n=n]\widetilde{F}(n)\varphi_{n/n}(y_n)}$$

(since any divisor d of n satisfies either $d \neq n$ or $d = n$)

$$= \underbrace{\sum_{\substack{d\mid n;\\ d\neq n}}0\widetilde{F}(d)\,\varphi_{n/d}(y_d)}_{=0} + [n=n]\,\widetilde{F}(n)\,\varphi_{n/n}(y_n) = \underbrace{[n=n]}_{=1}\widetilde{F}(n)\,\varphi_{n/n}(y_n) = \widetilde{F}(n)\,\varphi_{n/n}(y_n) \in \widetilde{F}(n)\,A.$$

Thus, Assertion $\mathcal{F}$ is satisfied. Consequently, the implication $\mathcal{E} \Longrightarrow \mathcal{F}$ is proven.

Proof of the implication $\mathcal{F} \Longrightarrow \mathcal{E}$*:* Assume that Assertion $\mathcal{F}$ holds. That is, every

$n \in N$ satisfies

$$\sum_{d\mid n} \mu(d)\,\varphi_d\left(b_{n/d}\right) \in \widetilde{F}(n)\,A.$$

Thus, for every $n \in N$, there exists some $y_n \in A$ such that

$$\widetilde{F}(n)\,y_n = \sum_{d\mid n} \mu(d)\,\varphi_d\left(b_{n/d}\right). \tag{29}$$

Fix such a y_n for every $n \in N$. Then, every $n \in N$ satisfies

$$\sum_{d\mid n} \widetilde{F}(d)\,\varphi_{n/d}(y_d) = \sum_{e\mid n} \underbrace{\widetilde{F}(e)\,\varphi_{n/e}(y_e)}_{\substack{=\varphi_{n/e}\left(\widetilde{F}(e)y_e\right),\text{ since }\varphi_{n/e}\\ \text{is a group endomorphism}}} \qquad (\text{here we substituted } e \text{ for } d \text{ in the sum})$$

$$= \sum_{e\mid n} \varphi_{n/e}\left(\widetilde{F}(e)\,y_e\right) = \sum_{e\mid n} \underbrace{\varphi_{n/e}\left(\sum_{d\mid e} \mu(d)\,\varphi_d\left(b_{e/d}\right)\right)}_{\substack{=\sum_{d\mid e}\mu(d)\varphi_{n/e}\left(\varphi_d\left(b_{e/d}\right)\right),\text{ since }\varphi_{n/e}\\ \text{is a group endomorphism}}}$$

$$\left(\text{since } \widetilde{F}(e)\,y_e = \sum_{d\mid e} \mu(d)\,\varphi_d\left(b_{e/d}\right) \text{ by (29) (applied to } e \text{ instead of } n)\right)$$

$$= \underbrace{\sum_{e\mid n}\sum_{d\mid e}}_{=\sum_{\substack{d\mid n;\\ d\mid e}}} \mu(d)\,\underbrace{\varphi_{n/e}\left(\varphi_d\left(b_{e/d}\right)\right)}_{=\left(\varphi_{n/e}\circ\varphi_d\right)\left(b_{e/d}\right)} = \underbrace{\sum_{e\mid n}\sum_{\substack{d\mid n;\\ d\mid e}}}_{=\sum_{d\mid n}\sum_{\substack{e\mid n;\\ d\mid e}}} \mu(d) \left(\underbrace{\varphi_{n/e}\circ\varphi_d}_{\substack{=\varphi_{(n/e)\cdot d}\\ (\text{by (16)})}}\right)\left(b_{e/d}\right) = \sum_{d\mid n}\sum_{\substack{e\mid n;\\ d\mid e}} \mu(d)\,\varphi_{(n/e)\cdot d}\left(b_{e/d}\right)$$

$$= \sum_{d\mid n} \mu(d) \sum_{\substack{e\mid n;\\ d\mid e}} \varphi_{(n/e)\cdot d}\left(b_{e/d}\right). \tag{30}$$

Now, for any divisor d of n, we have

$$\underbrace{\sum_{\substack{e\mid n;\\ d\mid e}}}_{=\sum_{\substack{e\in\mathbb{N}_{\mid n};\\ d\mid e}}} \underbrace{\varphi_{(n/e)\cdot d}}_{=\varphi_{n/(e/d)}}\left(b_{e/d}\right) = \sum_{\substack{e\in\mathbb{N}_{\mid n};\\ d\mid e}} \varphi_{n/(e/d)}\left(b_{e/d}\right) = \sum_{h\in\mathbb{N}_{\mid(n/d)}} \varphi_{n/h}\left(b_h\right)$$

(here we substituted h for e/d in the sum, since the map

$$\left\{e \in \mathbb{N}_{\mid n} \;\mid\; (d \mid e)\right\} \to \mathbb{N}_{\mid(n/d)}, \qquad e \mapsto e/d$$

is a bijection). Thus, (30) becomes

$$\sum_{d\mid n}\widetilde{F}\left(d\right)\varphi_{n/d}\left(y_d\right)=\sum_{d\mid n}\mu\left(d\right)\underbrace{\sum_{\substack{e\mid n;\\ d\mid e}}\varphi_{(n/e)\cdot d}\left(b_{e/d}\right)}_{=\sum\limits_{h\in\mathbb{N}_{\mid(n/d)}}\varphi_{n/h}(b_h)}=\sum_{d\mid n}\mu\left(d\right)\underbrace{\sum_{h\in\mathbb{N}_{\mid(n/d)}}}_{=\sum\limits_{h\mid(n/d)}=\sum\limits_{\substack{h\mid n;\\ h\mid(n/d)}}}\varphi_{n/h}\left(b_h\right)$$

$$=\sum_{d\mid n}\mu\left(d\right)\sum_{\substack{h\mid n;\\ h\mid(n/d)}}\varphi_{n/h}\left(b_h\right)=\underbrace{\sum_{d\mid n}\sum_{\substack{h\mid n;\\ h\mid(n/d)}}}_{=\sum\limits_{h\mid n}\sum\limits_{\substack{d\mid n;\\ h\mid(n/d)}}}\mu\left(d\right)\varphi_{n/h}\left(b_h\right)=\sum_{h\mid n}\sum_{\substack{d\mid n;\\ h\mid(n/d)}}\mu\left(d\right)\varphi_{n/h}\left(b_h\right)$$

$$=\sum_{h\mid n}\underbrace{\sum_{\substack{d\mid n;\\ d\mid(n/h)}}}_{=\sum\limits_{d\mid(n/h)}}\mu\left(d\right)\varphi_{n/h}\left(b_h\right)\qquad\left(\begin{array}{c}\text{since for any integer } d\text{, the assertion } h\mid(n/d) \text{ is}\\ \text{equivalent to } d\mid(n/h)\end{array}\right)$$

$$=\sum_{h\mid n}\sum_{d\mid(n/h)}\mu\left(d\right)\varphi_{n/h}\left(b_h\right)=\sum_{h\mid n}\left[n=h\right]\varphi_{n/h}\left(b_h\right)$$

$$\left(\text{since (21) (applied to } n/h \text{ instead of } n\text{) yields }\sum_{d\mid(n/h)}\mu\left(d\right)=\left[n/h=1\right]=\left[n=h\right]\right)$$

$$=\sum_{\substack{h\mid n;\\ h\neq n}}\underbrace{\left[n=h\right]}_{=0\text{ (since }h\neq n)}\varphi_{n/h}\left(b_h\right)+\underbrace{\sum_{\substack{h\mid n;\\ h=n}}\left[n=h\right]\varphi_{n/h}\left(b_h\right)}_{=[n=n]\varphi_{n/n}(b_n)}$$

$$\left(\text{since any divisor } h \text{ of } n \text{ satisfies either } h\neq n \text{ or } h=n\right)$$

$$=\underbrace{\sum_{\substack{h\mid n;\\ h\neq n}}0\varphi_{n/h}\left(b_h\right)}_{=0}+\underbrace{\left[n=n\right]}_{=1}\underbrace{\varphi_{n/n}}_{\substack{=\varphi_1=\operatorname{id}\\ \text{(by (15))}}}\left(b_n\right)=0+1\operatorname{id}\left(b_n\right)=\operatorname{id}\left(b_n\right)=b_n.$$

Therefore, Assertion $\mathcal{E}$ is satisfied. We have thus shown the implication $\mathcal{F}\Longrightarrow\mathcal{E}$.

Now we have proven both implications $\mathcal{E}\Longrightarrow\mathcal{F}$ and $\mathcal{F}\Longrightarrow\mathcal{E}$. As a consequence, we now know that $\mathcal{E}\Longleftrightarrow\mathcal{F}$. Our next step will be to prove that $\mathcal{E}\Longleftrightarrow\mathcal{G}$.

Proof of the implication $\mathcal{E}\Longrightarrow\mathcal{G}$*:* Assume that Assertion $\mathcal{E}$ holds. Then, we can prove that every $n\in N$ satisfies

$$\sum_{d\mid n}\phi\left(d\right)\varphi_d\left(b_{n/d}\right)=\sum_{d\mid n}\sum_{e\mid(n/d)}\phi\left(e\right)\widetilde{F}\left(d\right)\varphi_{n/d}\left(y_d\right)$$

(this equation is proven in exactly the same way as we have shown the equation $\sum\limits_{d\mid n}\mu\left(d\right)\varphi_d\left(b_{n/d}\right)=\sum\limits_{d\mid n}\sum\limits_{e\mid(n/d)}\mu\left(e\right)\widetilde{F}\left(d\right)\varphi_{n/d}\left(y_d\right)$ in the proof of the implication $\mathcal{E}\Longrightarrow\mathcal{F}$, only with μ replaced by ϕ throughout the proof). Since every divisor d of n satisfies

$\sum\limits_{e\mid(n/d)} \phi(e) = n/d$ (by (20), with n and d replaced by n/d and e), this becomes

$$\begin{aligned}\sum_{d\mid n} \phi(d)\,\varphi_d(b_{n/d}) &= \sum_{d\mid n} \underbrace{\sum_{e\mid(n/d)} \phi(e)}_{=n/d} \widetilde{F}(d)\,\varphi_{n/d}(y_d) = \sum_{d\mid n} \underbrace{(n/d)\,\widetilde{F}(d)}_{\substack{\in \widetilde{F}(n)\mathbb{Z} \\ \text{(due to (4))}}} \varphi_{n/d}(y_d) \\ &\in \sum_{d\mid n} \widetilde{F}(n)\,\mathbb{Z}\varphi_{n/d}(y_d) = \widetilde{F}(n) \underbrace{\sum_{d\mid n} \mathbb{Z}\varphi_{n/d}(y_d)}_{\subseteq A} \subseteq \widetilde{F}(n)\,A.\end{aligned}$$

Thus, Assertion $\mathcal{G}$ is satisfied. Consequently, the implication $\mathcal{E} \Longrightarrow \mathcal{G}$ is proven.

Proof of the implication $\mathcal{G} \Longrightarrow \mathcal{E}$*:* Assume that Assertion $\mathcal{G}$ holds. That is, every $n \in N$ satisfies

$$\sum_{d\mid n} \phi(d)\,\varphi_d(b_{n/d}) \in \widetilde{F}(n)\,A.$$

Thus, for every $n \in N$, there exists some $z_n \in A$ such that

$$\widetilde{F}(n)\,z_n = \sum_{d\mid n} \phi(d)\,\varphi_d(b_{n/d}). \tag{31}$$

Fix such a z_n for every $n \in N$. For every $n \in N$, we define an element $y_n \in A$ by

$$y_n = \sum_{h\mid n} \underbrace{\frac{h\widetilde{F}(n/h)}{\widetilde{F}(n)}}_{\substack{\text{this is an integer, since } \widetilde{F}(n)\mid h\widetilde{F}(n/h) \\ \text{(in fact, (4), applied to } d=n/h\text{,} \\ \text{yields } \widetilde{F}(n)\mid(n/(n/h))\widetilde{F}(n/h)=h\widetilde{F}(n/h))}} \mu(h)\,\varphi_h(z_{n/h}).$$

Then,

$$\widetilde{F}(n)\, y_n = \widetilde{F}(n) \sum_{h|n} \frac{h\widetilde{F}(n/h)}{\widetilde{F}(n)} \mu(h)\, \varphi_h(z_{n/h}) = \sum_{h|n} \underbrace{\widetilde{F}(n)\, \frac{h\widetilde{F}(n/h)}{\widetilde{F}(n)}}_{=h\widetilde{F}(n/h)} \mu(h)\, \varphi_h(z_{n/h})$$

$$= \sum_{h|n} h\mu(h)\, \underbrace{\widetilde{F}(n/h)\, \varphi_h(z_{n/h})}_{\substack{=\varphi_h\left(\widetilde{F}(n/h) z_{n/h}\right),\text{ since} \\ n/h\in\mathbb{Z} \text{ and since } \varphi_h \text{ is} \\ \text{a group endomorphism}}} = \sum_{h|n} h\mu(h)\, \varphi_h\left(\widetilde{F}(n/h)\, z_{n/h}\right)$$

$$= \sum_{h|n} h\mu(h)\, \underbrace{\varphi_h\left(\sum_{d|(n/h)} \phi(d)\, \varphi_d\left(b_{(n/h)/d}\right)\right)}_{\substack{=\sum\limits_{d|(n/h)} \phi(d)\varphi_h\left(\varphi_d\left(b_{(n/h)/d}\right)\right),\text{ since} \\ \varphi_h \text{ is a group endomorphism}}}$$

$$\left(\begin{array}{c}\text{since the equation (31), applied to } n/h \text{ instead of } n, \\ \text{yields } \widetilde{F}(n/h)\, z_{n/h} = \sum\limits_{d|(n/h)} \phi(d)\, \varphi_d\left(b_{(n/h)/d}\right)\end{array}\right)$$

$$= \sum_{h|n} h\mu(h) \sum_{d|(n/h)} \phi(d)\, \underbrace{\varphi_h\left(\varphi_d\left(b_{(n/h)/d}\right)\right)}_{=(\varphi_h\circ\varphi_d)\left(b_{(n/h)/d}\right)} = \sum_{h|n} h\mu(h) \underbrace{\sum_{d|(n/h)}}_{=\sum\limits_{d\in\mathbb{N}_{|(n/h)}}} \phi\left(\underbrace{d}_{=\dfrac{hd}{h}}\right) \left(\underbrace{\varphi_h\circ\varphi_d}_{=\varphi_{hd}\text{ (by (16))}}\right) \left(\underbrace{b_{(n/h)/d}}_{=b_{n/(hd)}}\right)$$

$$= \sum_{h|n} h\mu(h) \sum_{d\in\mathbb{N}_{|(n/h)}} \phi\left(\frac{hd}{h}\right) \varphi_{hd}\left(b_{n/(hd)}\right).$$

Since every divisor h of n satisfies

$$\sum_{d\in\mathbb{N}_{|(n/h)}} \phi\left(\frac{hd}{h}\right) \varphi_{hd}\left(b_{n/(hd)}\right) = \sum_{\substack{e\in\mathbb{N}_{|n}; \\ h|e}} \phi\left(\frac{e}{h}\right) \varphi_e\left(b_{n/e}\right)$$

(here, we have substituted e for hd in the sum, since the map

$$\mathbb{N}_{|(n/h)} \to \left\{e\in\mathbb{N}_{|n} \mid (h \mid e)\right\},\ d\mapsto hd$$

is a bijection, because $h \mid n$), this becomes

$$\begin{aligned}
&\widetilde{F}\left(n\right) y_n \\
&= \sum_{h\mid n} h\mu\left(h\right) \underbrace{\sum_{d\in\mathbb{N}_{\mid(n/h)}} \phi\left(\frac{hd}{h}\right) \varphi_{hd}\left(b_{n/(hd)}\right)}_{=\sum\limits_{\substack{e\in\mathbb{N}_{\mid n};\\ h\mid e}} \phi\left(\frac{e}{h}\right)\varphi_e\left(b_{n/e}\right)} = \sum_{h\mid n} h\mu\left(h\right) \underbrace{\sum_{\substack{e\in\mathbb{N}_{\mid n};\\ h\mid e}}}_{=\sum\limits_{\substack{e\mid n;\\ h\mid e}}} \phi\left(\frac{e}{h}\right) \varphi_e\left(b_{n/e}\right) \\
&= \underbrace{\sum_{h\mid n} \sum_{\substack{e\mid n;\\ h\mid e}}}_{=\sum\limits_{e\mid n} \sum\limits_{\substack{h\mid n;\\ h\mid e}}} h\mu\left(h\right) \phi\left(\frac{e}{h}\right) \varphi_e\left(b_{n/e}\right) = \sum_{e\mid n} \underbrace{\sum_{\substack{h\mid n;\\ h\mid e}}}_{=\sum\limits_{h\mid e}} h\mu\left(h\right) \phi\left(\frac{e}{h}\right) \varphi_e\left(b_{n/e}\right) = \sum_{e\mid n} \underbrace{\sum_{h\mid e} h\mu\left(h\right) \phi\left(\frac{e}{h}\right)}_{\substack{=\mu(e) \text{ (by (23), with} \\ d \text{ and } n \text{ replaced by } h \text{ and } e)}} \varphi_e\left(b_{n/e}\right) \\
&= \sum_{e\mid n} \mu\left(e\right) \varphi_e\left(b_{n/e}\right) = \sum_{d\mid n} \mu\left(d\right) \varphi_d\left(b_{n/d}\right) \qquad \text{(here we substituted } d \text{ for } e \text{ in the sum)}.
\end{aligned}$$

In other words, we have proven (29). From this point, we can proceed as in the proof of the implication $\mathcal{F} \Longrightarrow \mathcal{E}$, and we arrive at Assertion $\mathcal{E}$. Hence, we have shown the implication $\mathcal{G} \Longrightarrow \mathcal{E}$.

Now we have shown both implications $\mathcal{E} \Longrightarrow \mathcal{G}$ and $\mathcal{G} \Longrightarrow \mathcal{E}$. Thus, the equivalence $\mathcal{E} \Longleftrightarrow \mathcal{G}$ must hold.

Finally, let us prove the equivalence between the assertions $\mathcal{G}$ and $\mathcal{H}$. This is very easy, since every $n \in N$ satisfies

$$\sum_{d\mid n} \phi\left(d\right) \varphi_d\left(b_{n/d}\right) = \sum_{i=1}^{n} \varphi_{n/\gcd(i,n)}\left(b_{\gcd(i,n)}\right)$$

[27]. Therefore, it is clear that $\mathcal{G} \Longleftrightarrow \mathcal{H}$.

Altogether, we have now proven the equivalences $\mathcal{C} \Longleftrightarrow \mathcal{E}$, $\mathcal{E} \Longleftrightarrow \mathcal{F}$, $\mathcal{E} \Longleftrightarrow \mathcal{G}$, and $\mathcal{G} \Longleftrightarrow \mathcal{H}$. Thus, the five assertions $\mathcal{C}$, $\mathcal{E}$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ are equivalent. This proves Theorem 5.

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:

[27] A proof of this equality can be found in [4] (more precisely, in the proof of $\mathcal{G} \Longleftrightarrow \mathcal{H}$ during the proof of Theorem 5 in [4]).

Theorem 7. Let $F : \mathbb{P} \times \mathbb{N} \to \mathbb{N}$ be a pseudo-monotonous map. 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 (15) and (16) 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

$$\left(b_n = \sum_{d\mid n} \widetilde{F}(d)\,\varphi_{n/d}(y_d) \text{ for every } n \in N\right). \tag{32}$$

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 (32).

Proof of Lemma 8. In order to prove Lemma 8, it is enough to show that if $(y_n)_{n\in N} \in A^N$ and $(y'_n)_{n\in N} \in A^N$ are two families of elements of A satisfying

$$\left(b_n = \sum_{d\mid n} \widetilde{F}(d)\,\varphi_{n/d}(y_d) \text{ for every } n \in N\right) \qquad \text{and} \tag{33}$$

$$\left(b_n = \sum_{d\mid n} \widetilde{F}(d)\,\varphi_{n/d}(y'_d) \text{ for every } n \in N\right), \tag{34}$$

then $(y_n)_{n\in N} = (y'_n)_{n\in N}$. So let us show this. Actually, let us prove that $y_m = y'_m$ for every $m \in N$. We will prove this by strong induction over m; so, we fix some $n \in N$, and try to prove that $y_n = y'_n$, assuming that $y_m = y'_m$ is already proven for every $m \in N$ such that $m < n$. But this is easy to do: We have $\sum\limits_{\substack{d\mid n;\\ d\neq n}} \widetilde{F}(d)\,\varphi_{n/d}(y_d) = \sum\limits_{\substack{d\mid n;\\ d\neq n}} \widetilde{F}(d)\,\varphi_{n/d}(y'_d)$ (because $y_d = y'_d$ holds for every divisor d of n satisfying $d \neq n$ [28]).
But (33) yields

$$b_n = \sum_{d\mid n} \widetilde{F}(d)\,\varphi_{n/d}(y_d) = \sum_{\substack{d\mid n;\\ d\neq n}} \widetilde{F}(d)\,\varphi_{n/d}(y_d) + \underbrace{\sum_{\substack{d\mid n;\\ d=n}} \widetilde{F}(d)\,\varphi_{n/d}(y_d)}_{\substack{=\widetilde{F}(n)\varphi_{n/n}(y_n)\\ =\widetilde{F}(n)\varphi_1(y_n)=\widetilde{F}(n)y_n\\ \text{(due to (15))}}} = \sum_{\substack{d\mid n;\\ d\neq n}} \widetilde{F}(d)\,\varphi_{n/d}(y_d) + \widetilde{F}(n)\,y_n$$

[28] *Proof.* Let d be a divisor of n satisfying $d \neq n$. Then, $d < n$. Moreover, every divisor of n lies in N (since $n \in N$ and since N is a nest), so that $d \in N$ (since d is a divisor of n).

Now recall our assumption that $y_m = y'_m$ is already proven for every $m \in N$ such that $m < n$. Applied to $m = d$, this yields $y_d = y'_d$ (since $d \in N$ and $d < n$).

and similarly (34) leads to

$$b_n = \sum_{\substack{d \mid n; \\ d \neq n}} \widetilde{F}(d)\, \varphi_{n/d}(y'_d) + \widetilde{F}(n)\, y'_n .$$

Thus, $\sum\limits_{\substack{d \mid n; \\ d \neq n}} \widetilde{F}(d)\, \varphi_{n/d}(y_d) + \widetilde{F}(n)\, y_n = b_n = \sum\limits_{\substack{d \mid n; \\ d \neq n}} \widetilde{F}(d)\, \varphi_{n/d}(y'_d) + \widetilde{F}(n)\, y'_n$. Subtracting the equality $\sum\limits_{\substack{d \mid n; \\ d \neq n}} \widetilde{F}(d)\, \varphi_{n/d}(y_d) = \sum\limits_{\substack{d \mid n; \\ d \neq n}} \widetilde{F}(d)\, \varphi_{n/d}(y'_d)$ from this equality, we obtain $\widetilde{F}(n)\, y_n = \widetilde{F}(n)\, y'_n$, so that $\widetilde{F}(n)(y_n - y'_n) = \underbrace{\widetilde{F}(n)\, y_n}_{=\widetilde{F}(n) y'_n} - \widetilde{F}(n)\, y'_n = 0$ and thus $y_n - y'_n = 0$ (since the group A is torsionfree), so that $y_n = y'_n$. This completes our induction. Thus, we have proven that $y_m = y'_m$ for every $m \in N$. In other words, $(y_n)_{n \in N} = (y'_n)_{n \in N}$. This completes the proof of Lemma 8.

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 (32). 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 (32). 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 $F : \mathbb{P} \times \mathbb{N} \to \mathbb{N}$ be a pseudo-monotonous map. 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 (7) 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
>
> $$\left(b_n = w_{F,n}\left((x_k)_{k \in N} \right) \text{ for every } n \in N \right). \qquad (35)$$

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

> **Lemma 10.** Let $F : \mathbb{P} \times \mathbb{N} \to \mathbb{N}$ be a pseudo-monotonous map. 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 (35).

Proof of Lemma 10. In order to prove Lemma 10, it is enough to show that if $(x_n)_{n\in N} \in A^N$ and $(x'_n)_{n\in N} \in A^N$ are two families of elements of A satisfying

$$\left(b_n = w_{F,n}\left((x_k)_{k\in N}\right) \text{ for every } n \in N\right) \qquad \text{and} \tag{36}$$
$$\left(b_n = w_{F,n}\left((x'_k)_{k\in N}\right) \text{ for every } n \in N\right), \tag{37}$$

then $(x_n)_{n\in N} = (x'_n)_{n\in N}$. So let us show this. Actually, let us prove that $x_m = x'_m$ for every $m \in N$. We will prove this by strong induction over m; so, we fix some $n \in N$, and try to prove that $x_n = x'_n$, assuming that $x_m = x'_m$ is already proven for every $m \in N$ such that $m < n$. But this is easy to prove: We have $\sum\limits_{\substack{d|n;\\ d\neq n}} \widetilde{F}(d)\, x_d^{n/d} = \sum\limits_{\substack{d|n;\\ d\neq n}} \widetilde{F}(d)\,(x'_d)^{n/d}$ (because $x_d = x'_d$ holds for every divisor d of n satisfying $d \neq n$ [29]). But (36) yields

$$b_n = w_{F,n}\left((x_k)_{k\in N}\right) = \sum_{d|n} \widetilde{F}(d)\, x_d^{n/d} = \sum_{\substack{d|n;\\ d\neq n}} \widetilde{F}(d)\, x_d^{n/d} + \underbrace{\sum_{\substack{d|n;\\ d=n}} \widetilde{F}(d)\, x_d^{n/d}}_{\substack{=\widetilde{F}(n)x_n^{n/n}\\ =\widetilde{F}(n)x_n^1=\widetilde{F}(n)x_n}} = \sum_{\substack{d|n;\\ d\neq n}} \widetilde{F}(d)\, x_d^{n/d} + \widetilde{F}(n)\, x_n$$

and similarly (37) leads to

$$b_n = \sum_{\substack{d|n;\\ d\neq n}} \widetilde{F}(d)\,(x'_d)^{n/d} + \widetilde{F}(n)\, x'_n.$$

Thus, $\sum\limits_{\substack{d|n;\\ d\neq n}} \widetilde{F}(d)\, x_d^{n/d} + \widetilde{F}(n)\, x_n = b_n = \sum\limits_{\substack{d|n;\\ d\neq n}} \widetilde{F}(d)\,(x'_d)^{n/d} + \widetilde{F}(n)\, x'_n$. Subtracting the equality $\sum\limits_{\substack{d|n;\\ d\neq n}} \widetilde{F}(d)\, x_d^{n/d} = \sum\limits_{\substack{d|n;\\ d\neq n}} \widetilde{F}(d)\,(x'_d)^{n/d}$ from this equality, we obtain $\widetilde{F}(n)\, x_n = \widetilde{F}(n)\, x'_n$, so that $\widetilde{F}(n)(x_n - x'_n) = \underbrace{\widetilde{F}(n)\, x_n}_{=\widetilde{F}(n)x'_n} - \widetilde{F}(n)\, x'_n = 0$ and thus $x_n - x'_n = 0$ (since the ring A is torsionfree), so that $x_n = x'_n$. This completes our induction. Thus, we have proven that $x_m = x'_m$ for every $m \in N$. In other words, $(x_n)_{n\in N} = (x'_n)_{n\in N}$. This completes the proof of Lemma 10.

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 (35). 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 (35). 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 $\mathcal{D} \Longleftrightarrow \mathcal{D}'$.

[29] *Proof.* Let d be a divisor of n satisfying $d \neq n$. Then, $d < n$. Moreover, every divisor of n lies in N (since $n \in N$ and since N is a nest), so that $d \in N$ (since d is a divisor of n).

Now recall our assumption that $x_m = x'_m$ is already proven for every $m \in N$ such that $m < n$. Applied to $m = d$, this yields $x_d = x'_d$ (since $d \in N$ and $d < n$).

Combining this with $\mathcal{C} \iff \mathcal{D}$, we see that all three assertions $\mathcal{C}$, $\mathcal{D}$ and $\mathcal{D}'$ are equivalent. This proves Theorem 9.

Let us record, for the sake of application, the following result, which is a trivial consequence of Theorems 4 and 5:

> **Theorem 11.** Let $F : \mathbb{P} \times \mathbb{N} \to \mathbb{N}$ be a pseudo-monotonous map. 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 (7), (15) and (16) are satisfied.
>
> Let $(b_n)_{n \in N} \in A^N$ be a family of elements of A. Then, the assertions $\mathcal{C}$, $\mathcal{D}$, $\mathcal{E}$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ are equivalent, where the assertions $\mathcal{C}$ and $\mathcal{D}$ are the ones stated in Theorem 4, 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 5, the assertions $\mathcal{C}$, $\mathcal{E}$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ are equivalent. Combining these two observations, we conclude that the assertions $\mathcal{C}$, $\mathcal{D}$, $\mathcal{E}$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ are equivalent[30], and thus Theorem 11 is proven.

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

> **Theorem 12.** Let $F : \mathbb{P} \times \mathbb{N} \to \mathbb{N}$ be a pseudo-monotonous map. 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 (7), (15) and (16) are satisfied.
>
> Let $(b_n)_{n \in N} \in A^N$ be a family of elements of A. Then, the assertions $\mathcal{C}$, $\mathcal{D}$, $\mathcal{D}'$, $\mathcal{E}$, $\mathcal{E}'$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ are equivalent, where:

- the assertions $\mathcal{C}$ and $\mathcal{D}$ are the ones stated in Theorem 4,
- the 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 7, the assertions $\mathcal{C}$, $\mathcal{E}$, $\mathcal{E}'$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ are equivalent. Combining these two observations, we conclude that the assertions $\mathcal{C}$, $\mathcal{D}$, $\mathcal{D}'$, $\mathcal{E}$, $\mathcal{E}'$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ are equivalent[31], and thus Theorem 12 is proven.

We are now going to formulate the most important particular case of Theorem 12, namely the one where A is a ring of polynomials over $\mathbb{Z}$:

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

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

Theorem 13. Let $F : \mathbb{P} \times \mathbb{N} \to \mathbb{N}$ be a pseudo-monotonous map. 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 $\mathcal{C}_\Xi$, $\mathcal{D}_\Xi$, $\mathcal{D}'_\Xi$, $\mathcal{E}_\Xi$, $\mathcal{E}'_\Xi$, $\mathcal{F}_\Xi$, $\mathcal{G}_\Xi$ and $\mathcal{H}_\Xi$ are equivalent:

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

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

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

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

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

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

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

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

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

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

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

$$\sum_{d\mid n} \mu(d)\, b_{n/d}\left(\Xi^d\right) \in \widetilde{F}(n)\,\mathbb{Z}[\Xi].$$

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

$$\sum_{d\mid n} \phi(d)\, b_{n/d}\left(\Xi^d\right) \in \widetilde{F}(n)\,\mathbb{Z}[\Xi].$$

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

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

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, $a(\Xi^p) \equiv a^p \operatorname{mod} p\mathbb{Z}[\Xi]$.

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 $\mathbb{Z}[\Xi]$ [32]. The condition (7) is satisfied, since $\varphi_p(a) = a(\Xi^p) \equiv a^p \operatorname{mod} p\mathbb{Z}[\Xi]$ (by Lemma 14) holds for every $a \in A$. The condition (15) is satisfied as well (since $\varphi_1(P) = P(\Xi^1) = P(\Xi) = P$ for every $P \in \mathbb{Z}[\Xi]$), and the condition (16) is also satisfied (since $\varphi_n \circ \varphi_m = \varphi_{nm}$ for every $n \in N$ and every $m \in N$ satisfying $nm \in N$ [33]). Hence, the three conditions (7), (15) and (16) are satisfied. Therefore, Theorem 12 yields that the assertions $\mathcal{C}$, $\mathcal{D}$, $\mathcal{D}'$, $\mathcal{E}$, $\mathcal{E}'$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ are equivalent, where:

- the assertions $\mathcal{C}$ and $\mathcal{D}$ are the ones stated in Theorem 4,
- the 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 $\mathcal{C}$, $\mathcal{D}$, $\mathcal{D}'$, $\mathcal{E}$, $\mathcal{E}'$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ with the respective assertions $\mathcal{C}_\Xi$, $\mathcal{D}_\Xi$, $\mathcal{D}'_\Xi$, $\mathcal{E}_\Xi$, $\mathcal{E}'_\Xi$, $\mathcal{F}_\Xi$, $\mathcal{G}_\Xi$ and $\mathcal{H}_\Xi$, we notice that:

- we have $\mathcal{C} \iff \mathcal{C}_\Xi$ (since $A = \mathbb{Z}[\Xi]$ and $\varphi_p(b_{n/p}) = b_{n/p}(\Xi^p)$);
- we have $\mathcal{D} \iff \mathcal{D}_\Xi$ (since $A = \mathbb{Z}[\Xi]$);
- we have $\mathcal{D}' \iff \mathcal{D}'_\Xi$ (since $A = \mathbb{Z}[\Xi]$);
- we have $\mathcal{E} \iff \mathcal{E}_\Xi$ (since $A = \mathbb{Z}[\Xi]$ and $\varphi_{n/d}(y_d) = y_d\left(\Xi^{n/d}\right)$);

[32] 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

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

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

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

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

- 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 $\varphi_{n/\gcd(i,n)}\left(b_{\gcd(i,n)}\right) = b_{\gcd(i,n)}\left(\Xi^{n/\gcd(i,n)}\right)$).

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

Theorem 13 has a number of applications, including the existence of the Witt addition and multiplication polynomials. But first we notice the simplest particular case of Theorem 13:

Theorem 15. Let $F : \mathbb{P} \times \mathbb{N} \to \mathbb{N}$ be a pseudo-monotonous map. 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 $\mathcal{C}_{\varnothing}$, $\mathcal{D}_{\varnothing}$, $\mathcal{D}'_{\varnothing}$, $\mathcal{E}_{\varnothing}$, $\mathcal{E}'_{\varnothing}$, $\mathcal{F}_{\varnothing}$, $\mathcal{G}_{\varnothing}$ and $\mathcal{H}_{\varnothing}$ are equivalent:

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

$$b_{n/p} \equiv b_n \operatorname{mod} p^{F(p,v_p(n))}\mathbb{Z}.$$

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

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

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

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

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

$$\left(b_n = \sum_{d\mid n} \widetilde{F}(d)\, y_d \text{ for every } n \in N\right).$$

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

$$\left(b_n = \sum_{d\mid n} \widetilde{F}(d)\, y_d \text{ for every } n \in N\right).$$

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

$$\sum_{d\mid n} \mu(d)\, b_{n/d} \in \widetilde{F}(n)\,\mathbb{Z}.$$

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

$$\sum_{d \mid n} \phi(d)\, b_{n/d} \in \widetilde{F}(n)\,\mathbb{Z}.$$

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

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

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 $n \in \mathbb{N}$ [34]. Theorem 13 yields that the assertions $\mathcal{C}_\Xi$, $\mathcal{D}_\Xi$, $\mathcal{D}'_\Xi$, $\mathcal{E}_\Xi$, $\mathcal{E}'_\Xi$, $\mathcal{F}_\Xi$, $\mathcal{G}_\Xi$ and $\mathcal{H}_\Xi$ are equivalent (these assertions were stated in Theorem 13).

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

- we have $\mathcal{C}_\Xi \iff \mathcal{C}_\varnothing$ (since $\mathbb{Z}[\Xi] = \mathbb{Z}$ and $b_{n/p}(\Xi^p) = b_{n/p}$);
- we have $\mathcal{D}_\Xi \iff \mathcal{D}_\varnothing$ (since $\mathbb{Z}[\Xi] = \mathbb{Z}$);
- we have $\mathcal{D}'_\Xi \iff \mathcal{D}'_\varnothing$ (since $\mathbb{Z}[\Xi] = \mathbb{Z}$);
- we have $\mathcal{E}_\Xi \iff \mathcal{E}_\varnothing$ (since $\mathbb{Z}[\Xi] = \mathbb{Z}$ and $y_d\left(\Xi^{n/d}\right) = y_d$);
- we have $\mathcal{E}'_\Xi \iff \mathcal{E}'_\varnothing$ (since $\mathbb{Z}[\Xi] = \mathbb{Z}$ and $y_d\left(\Xi^{n/d}\right) = y_d$);
- we have $\mathcal{F}_\Xi \iff \mathcal{F}_\varnothing$ (since $\mathbb{Z}[\Xi] = \mathbb{Z}$ and $b_{n/d}\left(\Xi^d\right) = b_{n/d}$);
- we have $\mathcal{G}_\Xi \iff \mathcal{G}_\varnothing$ (since $\mathbb{Z}[\Xi] = \mathbb{Z}$ and $b_{n/d}\left(\Xi^d\right) = b_{n/d}$);
- we have $\mathcal{H}_\Xi \iff \mathcal{H}_\varnothing$ (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 $\mathcal{C}_\Xi$, $\mathcal{D}_\Xi$, $\mathcal{D}'_\Xi$, $\mathcal{E}_\Xi$, $\mathcal{E}'_\Xi$, $\mathcal{F}_\Xi$, $\mathcal{G}_\Xi$ and $\mathcal{H}_\Xi$ yields the equivalence of the assertions $\mathcal{C}_\varnothing$, $\mathcal{D}_\varnothing$, $\mathcal{D}'_\varnothing$, $\mathcal{E}_\varnothing$, $\mathcal{E}'_\varnothing$, $\mathcal{F}_\varnothing$, $\mathcal{G}_\varnothing$ and $\mathcal{H}_\varnothing$. Thus, Theorem 15 is proven.

We notice a simple corollary of Theorem 15:

Theorem 16. Let $F : \mathbb{P} \times \mathbb{N} \to \mathbb{N}$ be a pseudo-monotonous map. 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

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

[34] 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 $a(\Xi^n) = a$.

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

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

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

$$\sum_{d\mid n} \mu(d)\, q^{n/d} \in \widetilde{F}(n)\,\mathbb{Z}.$$

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

$$\sum_{d\mid n} \phi(d)\, q^{n/d} \in \widetilde{F}(n)\,\mathbb{Z}.$$

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

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

Note that this Theorem 16 is a generalization of Theorem 16 in [4], but the parts **(c)**, **(d)** and **(e)** of our Theorem 16 are *not stronger* than the corresponding parts of Theorem 16 in [4], because $\widetilde{F}(n) \mid n$ (as quickly follows from (4), applied to $d = n$). 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 $q^{n/p} \equiv q^n \mod p^{v_p(n)}\mathbb{Z}$ [35]. Since $F(p, v_p(n)) \leq v_p(n)$ (because (2), applied to $a = v_p(n)$ and $b = 0$, yields $F(p, v_p(n)) - v_p(n) \leq \underbrace{F(p,0)}_{=0 \text{ (by (1))}} - 0 = 0$) yields $p^{F(p,v_p(n))} \mid p^{v_p(n)}$ and thus $p^{v_p(n)}\mathbb{Z} \subseteq p^{F(p,v_p(n))}\mathbb{Z}$, this becomes

$$q^{n/p} \equiv q^n \mod p^{F(p,v_p(n))}\mathbb{Z}. \tag{38}$$

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 $\mathcal{C}_\varnothing$, $\mathcal{D}_\varnothing$, $\mathcal{D}'_\varnothing$, $\mathcal{E}_\varnothing$, $\mathcal{E}'_\varnothing$, $\mathcal{F}_\varnothing$, $\mathcal{G}_\varnothing$ 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

$$\begin{aligned} b_{n/p} = q^{n/p} &\equiv q^n \qquad \text{(by (38))} \\ &= b_n \mod p^{F(p,v_p(n))}\mathbb{Z} \end{aligned}$$

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

[35] In fact, $p^{v_p(n)} \mid n$, and thus there exists some $u \in \mathbb{N}_+$ such that $n = p^{v_p(n)}u$. Since $v_p(n) \geq 1$ (because $p \in \operatorname{PF} n$), we have $v_p(n) - 1 \in \mathbb{N}$, and thus can define an element $\ell \in \mathbb{N}$ by $\ell = v_p(n) - 1$.

Now, Fermat's little theorem yields $q^u \equiv (q^u)^p = q^{up} \mod p\mathbb{Z}$, and thus $(q^u)^{p^\ell} \equiv (q^{up})^{p^\ell} \mod p^{1+\ell}\mathbb{Z}$ (by Lemma 3, applied to $k = 1$, $a = q^u$, $b = q^{up}$ and $A = \mathbb{Z}$). But $n/p = p^{v_p(n)}u/p = p^{v_p(n)-1}u = p^\ell u = up^\ell$ yields $q^{n/p} = q^{up^\ell} = (q^u)^{p^\ell}$, and $n = \underbrace{n/p}_{=up^\ell} \cdot p = up \cdot p^\ell$ yields $q^n = q^{up\cdot p^\ell} = (q^{up})^{p^\ell}$. Finally, $1 + \ell = 1 + (v_p(n) - 1) = v_p(n)$. Hence, $(q^u)^{p^\ell} \equiv (q^{up})^{p^\ell} \mod p^{1+\ell}\mathbb{Z}$ becomes $q^{n/p} \equiv q^n \mod p^{v_p(n)}\mathbb{Z}$ (since $q^{n/p} = (q^u)^{p^\ell}$, $q^n = (q^{up})^{p^\ell}$ and $1 + \ell = v_p(n)$), qed.

- 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 $b_{\gcd(i,n)} = q^{\gcd(i,n)}$).

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.

Now here is a less-known analogue of Theorem 16:

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 $F : \mathbb{P} \times \mathbb{N} \to \mathbb{N}$ be a pseudo-monotonous map. 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

$$\left(\binom{qn}{rn} = w_{F,n}\left((x_k)_{k\in\mathbb{N}_+}\right) \text{ for every } n \in \mathbb{N}_+\right).$$

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

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

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

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

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

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

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

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

This is the analogue of Theorem 17 of [4]. In order to prove it, we 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,

$$\binom{qn/p}{rn/p} \equiv \binom{qn}{rn} \operatorname{mod} p^{v_p(n)}\mathbb{Z}. \tag{39}$$

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

Proof of Theorem 17. 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 $\mathcal{C}_\varnothing$, $\mathcal{D}_\varnothing$, $\mathcal{D}'_\varnothing$, $\mathcal{E}_\varnothing$, $\mathcal{E}'_\varnothing$, $\mathcal{F}_\varnothing$, $\mathcal{G}_\varnothing$ 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

$$\begin{aligned} b_{n/p} &= \binom{qn/p}{rn/p} \equiv \binom{qn}{rn} \qquad \text{(by (39))} \\ &= b_n \operatorname{mod} p^{v_p(n)}\mathbb{Z}, \end{aligned}$$

and thus $b_{n/p} \equiv b_n \operatorname{mod} p^{F(p,v_p(n))}\mathbb{Z}$ because we can prove $p^{v_p(n)}\mathbb{Z} \subseteq p^{F(p,v_p(n))}\mathbb{Z}$ just as in the proof of Theorem 16), this yields that the assertions $\mathcal{D}_\varnothing$, $\mathcal{D}'_\varnothing$, $\mathcal{E}_\varnothing$, $\mathcal{E}'_\varnothing$, $\mathcal{F}_\varnothing$, $\mathcal{G}_\varnothing$ 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:

Theorem 20. 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 $r \in \mathbb{Z} \setminus \mathbb{N}$, then $\dbinom{u}{r}$ is supposed to mean 0.

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

$$\left(\binom{qn-1}{rn-1} = w_{F,n}\left((x_k)_{k\in\mathbb{N}_+} \right) \text{ for every } n \in \mathbb{N}_+ \right).$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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 $r = \frac{\alpha}{\beta}$. Then,

$$\binom{qn/p - 1}{rn/p - 1} \equiv \binom{qn-1}{rn-1} \operatorname{mod} p^{v_p(n)}\mathbb{Z}. \tag{40}$$

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

$$\binom{a}{b} = \frac{a}{b}\binom{a-1}{b-1} \tag{41}$$

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 N be the nest $\mathbb{N}_+$. Define a family $(b_n)_{n\in N} \in \mathbb{Z}^N$ by $b_n = \binom{qn-1}{rn-1}$ for every $n \in N$. According to Theorem 15, the assertions $\mathcal{C}_\varnothing$, $\mathcal{D}_\varnothing$, $\mathcal{D}'_\varnothing$, $\mathcal{E}_\varnothing$, $\mathcal{E}'_\varnothing$, $\mathcal{F}_\varnothing$, $\mathcal{G}_\varnothing$ 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

$$b_{n/p} = \binom{qn/p - 1}{rn/p - 1} \equiv \binom{qn-1}{rn-1} \qquad \left(\begin{array}{c}\text{by (40), because there exist two integers } \alpha \text{ and } \beta \text{ with} \\ v_p(\alpha) \geq v_p(\beta) \text{ and } r = \dfrac{\alpha}{\beta} \text{ (namely, } \alpha = r \text{ and } \beta = 1\text{, since} \\ \dfrac{r}{1} = 1 \text{ and } v_p(r) \geq 0 = v_p(1)\text{)}\end{array}\right)$$

$$= b_n \operatorname{mod} p^{v_p(n)}\mathbb{Z},$$

and thus $b_{n/p} \equiv b_n \operatorname{mod} p^{F(p,v_p(n))}\mathbb{Z}$ because we can prove $p^{v_p(n)}\mathbb{Z} \subseteq p^{F(p,v_p(n))}\mathbb{Z}$ just as in the proof of Theorem 16), this yields that the assertions $\mathcal{D}_\varnothing$, $\mathcal{D}'_\varnothing$, $\mathcal{E}_\varnothing$, $\mathcal{E}'_\varnothing$, $\mathcal{F}_\varnothing$, $\mathcal{G}_\varnothing$ 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 $b_n = \binom{qn-1}{rn-1}$);
- assertion $\mathcal{E}'_\varnothing$ is equivalent to Theorem 20 **(b)** (since $N = \mathbb{N}_+$ and $b_n = \binom{qn-1}{rn-1}$);
- 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 $b_{n/d} = \dbinom{qn/d-1}{rn/d-1}$);
- assertion $\mathcal{H}_\varnothing$ is equivalent to Theorem 20 **(e)** (since $N = \mathbb{N}_+$ and $b_{\gcd(i,n)} = \dbinom{q\gcd(i,n)-1}{r\gcd(i,n)-1}$).

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

$$\sum_{d\mid n}\mu(d)\underbrace{\binom{qn/d}{rn/d}}_{\substack{=\frac{qn/d}{rn/d}\binom{qn/d-1}{rn/d-1} \\ \text{(by (41), applied to} \\ a=qn/d \text{ and } b=rn/d)}} = \sum_{d\mid n}\mu(d)\underbrace{\frac{qn/d}{rn/d}}_{=\frac{q}{r}}\binom{qn/d-1}{rn/d-1} = \frac{q}{r}\underbrace{\sum_{d\mid n}\mu(d)\binom{qn/d-1}{rn/d-1}}_{\substack{\in\widetilde{F}(n)\mathbb{Z} \\ \text{(by Theorem 20 (c))}}}$$

$$\in \frac{q}{r}\widetilde{F}(n)\mathbb{Z}.$$

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

$$\sum_{d\mid n}\phi(d)\underbrace{\binom{qn/d}{rn/d}}_{\substack{=\frac{qn/d}{rn/d}\binom{qn/d-1}{rn/d-1} \\ \text{(by (41), applied to} \\ a=qn/d \text{ and } b=rn/d)}} = \sum_{d\mid n}\phi(d)\underbrace{\frac{qn/d}{rn/d}}_{=\frac{q}{r}}\binom{qn/d-1}{rn/d-1} = \frac{q}{r}\underbrace{\sum_{d\mid n}\phi(d)\binom{qn/d-1}{rn/d-1}}_{\substack{\in\widetilde{F}(n)\mathbb{Z} \\ \text{(by Theorem 20 (d))}}}$$

$$\in \frac{q}{r}\widetilde{F}(n)\mathbb{Z}.$$

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

$$\sum_{i=1}^{n}\underbrace{\binom{q\gcd(i,n)}{r\gcd(i,n)}}_{\substack{=\frac{q\gcd(i,n)}{r\gcd(i,n)}\binom{q\gcd(i,n)-1}{r\gcd(i,n)-1} \\ \text{(by (41), applied to} \\ a=q\gcd(i,n) \text{ and } b=r\gcd(i,n))}} = \sum_{i=1}^{n}\underbrace{\frac{q\gcd(i,n)}{r\gcd(i,n)}}_{=\frac{q}{r}}\binom{q\gcd(i,n)-1}{r\gcd(i,n)-1}$$

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

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 $F : \mathbb{P} \times \mathbb{N} \to \mathbb{N}$ be a pseudo-monotonous map.

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

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

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

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

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

(b) The family $(\widetilde{x}_n)_{n\in N} \in (\mathbb{Q}[\Xi])^N$ 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 $\mathbb{Q}[\Xi]$ 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 22 **(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

$$b_{n/p}(\Xi^p) \equiv b_n \operatorname{mod} p^{F(p,v_p(n))}\mathbb{Z}[\Xi]. \tag{42}$$

The proof of Theorem 22 is easy using Theorem 13; in order to formulate it, we will use a trick:

Let us replace $\mathbb{Z}$ by $\mathbb{Q}$ throughout Theorem 13. We obtain the following result[36]:

Lemma 23. Let $F : \mathbb{P} \times \mathbb{N} \to \mathbb{N}$ be a pseudo-monotonous map. Let Ξ be a family of symbols. Let N be a nest, and let $(b_n)_{n\in N} \in (\mathbb{Q}[\Xi])^N$ be a family of polynomials in the indeterminates Ξ. Then, the following assertions $\mathcal{C}_\Xi^\mathbb{Q}$, $\mathcal{D}_\Xi^\mathbb{Q}$, $\mathcal{D}_\Xi'^\mathbb{Q}$, $\mathcal{E}_\Xi^\mathbb{Q}$, $\mathcal{E}_\Xi'^\mathbb{Q}$, $\mathcal{F}_\Xi^\mathbb{Q}$, $\mathcal{G}_\Xi^\mathbb{Q}$ and $\mathcal{H}_\Xi^\mathbb{Q}$ are equivalent:

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

$$b_{n/p}(\Xi^p) \equiv b_n \operatorname{mod} p^{F(p,v_p(n))}\mathbb{Q}[\Xi].$$

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

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

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

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

[36] Don't be surprised that the assertions $\mathcal{C}_\Xi^\mathbb{Q}$, $\mathcal{F}_\Xi^\mathbb{Q}$, $\mathcal{G}_\Xi^\mathbb{Q}$ and $\mathcal{H}_\Xi^\mathbb{Q}$ are always fulfilled. I have only included them to make the similarity between Lemma 23 and Theorem 13 more evident.

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

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

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

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

Assertion $\mathcal{F}_{\Xi}^{\mathbb{Q}}$*:* Every $n \in N$ satisfies

$$\sum_{d\mid n} \mu(d)\, b_{n/d}\left(\Xi^d\right) \in \widetilde{F}(n)\,\mathbb{Q}[\Xi].$$

Assertion $\mathcal{G}_{\Xi}^{\mathbb{Q}}$*:* Every $n \in N$ satisfies

$$\sum_{d\mid n} \phi(d)\, b_{n/d}\left(\Xi^d\right) \in \widetilde{F}(n)\,\mathbb{Q}[\Xi].$$

Assertion $\mathcal{H}_{\Xi}^{\mathbb{Q}}$*:* Every $n \in N$ satisfies

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

Of course, it is obvious that the assertions $\mathcal{C}_{\Xi}^{\mathbb{Q}}$, $\mathcal{F}_{\Xi}^{\mathbb{Q}}$, $\mathcal{G}_{\Xi}^{\mathbb{Q}}$ and $\mathcal{H}_{\Xi}^{\mathbb{Q}}$ are always fulfilled (since $p^{F(p,v_p(n))}\mathbb{Q}[\Xi] = \mathbb{Q}[\Xi]$ for every $n \in N$ and every $p \in \operatorname{PF} n$, and $\widetilde{F}(n)\,\mathbb{Q}[\Xi] = \mathbb{Q}[\Xi]$ for every $n \in N$), so the actual meaning of Lemma 23 is that the assertions $\mathcal{D}_{\Xi}^{\mathbb{Q}}$, $\mathcal{D}_{\Xi}'^{\mathbb{Q}}$, $\mathcal{E}_{\Xi}^{\mathbb{Q}}$ and $\mathcal{E}_{\Xi}'^{\mathbb{Q}}$ are always fulfilled as well.

Proof of Lemma 23. In order to prove Lemma 23, it is almost enough to replace every appearance of $\mathbb{Z}$ by $\mathbb{Q}$ (and, of course, every appearance of $\mathcal{C}_{\Xi}$, $\mathcal{D}_{\Xi}$, $\mathcal{D}_{\Xi}'$, $\mathcal{E}_{\Xi}$, $\mathcal{E}_{\Xi}'$, $\mathcal{F}_{\Xi}$, $\mathcal{G}_{\Xi}$ and $\mathcal{H}_{\Xi}$ by $\mathcal{C}_{\Xi}^{\mathbb{Q}}$, $\mathcal{D}_{\Xi}^{\mathbb{Q}}$, $\mathcal{D}_{\Xi}'^{\mathbb{Q}}$, $\mathcal{E}_{\Xi}^{\mathbb{Q}}$, $\mathcal{E}_{\Xi}'^{\mathbb{Q}}$, $\mathcal{F}_{\Xi}^{\mathbb{Q}}$, $\mathcal{G}_{\Xi}^{\mathbb{Q}}$ and $\mathcal{H}_{\Xi}^{\mathbb{Q}}$, respectively) in the proof of Theorem 13. The only difference is that now, instead of Lemma 14, we need the following fact:

Lemma 24. Let $a \in \mathbb{Q}[\Xi]$ be a polynomial. Let p be a prime. Then, $a(\Xi^p) \equiv a^p \bmod p\mathbb{Q}[\Xi]$.

But this lemma is trivial, since $p\mathbb{Q}[\Xi] = \mathbb{Q}[\Xi]$. Hence, Lemma 23 is proven.

Proof of Theorem 22. **(a)** The family $(b_n)_{n\in N} \in (\mathbb{Q}[\Xi])^N$ satisfies the Assertion $\mathcal{C}_{\Xi}^{\mathbb{Q}}$ of Lemma 23 (since every $n \in N$ and every $p \in \operatorname{PF} n$ satisfies $b_{n/p}(\Xi^p) \equiv b_n \bmod p^{F(p,v_p(n))}\mathbb{Q}[\Xi]$, because $p^{F(p,v_p(n))}\mathbb{Q}[\Xi] = \mathbb{Q}[\Xi]$). Thus, it also satisfies the Assertion $\mathcal{D}_{\Xi}'^{\mathbb{Q}}$ of Lemma 23 (since Lemma 23 yields that the assertions $\mathcal{C}_{\Xi}^{\mathbb{Q}}$ and $\mathcal{D}_{\Xi}'^{\mathbb{Q}}$ are equivalent). In other words, there exists *one and only one* family $(x_n)_{n\in N} \in (\mathbb{Q}[\Xi])^N$ of elements of $\mathbb{Q}[\Xi]$ such that

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

This proves Theorem 22 **(a)**.

(b) We want to prove that $\widetilde{x}_n \in \mathbb{Q}\left[b_{\mathbb{N}_{|n}}\right]$ for every $n \in N$.

We are going to prove this by strong induction over n: Fix some $m \in N$. Assume that

$$\widetilde{x}_n \in \mathbb{Q}\left[b_{\mathbb{N}_{|n}}\right] \text{ is already proven for every } n \in N \text{ satisfying } n < m. \tag{43}$$

We want to show that $\widetilde{x}_n \in \mathbb{Q}\left[b_{\mathbb{N}_{|n}}\right]$ also holds for $n = m$.

According to Theorem 22 **(a)**, we have $b_n = w_{F,n}\left((\widetilde{x}_k)_{k\in N}\right)$ for every $n \in N$. In particular, for $n = m$, this yields

$$b_m = w_{F,m}\left((\widetilde{x}_k)_{k\in N}\right) = \sum_{d\mid m} \widetilde{F}(d)\,\widetilde{x}_d^{m/d} = \sum_{\substack{d\mid m;\\ d\neq m}} \widetilde{F}(d)\,\widetilde{x}_d^{m/d} + \underbrace{\sum_{\substack{d\mid m;\\ d=m}} \widetilde{F}(d)\,\widetilde{x}_d^{m/d}}_{=\widetilde{F}(m)\widetilde{x}_m^{m/m}=\widetilde{F}(m)\widetilde{x}_m} = \sum_{\substack{d\mid m;\\ d\neq m}} \widetilde{F}(d)\,\widetilde{x}_d^{m/d} + \widetilde{F}(m)\,\widetilde{x}_m,$$

so that $\widetilde{x}_m = \dfrac{1}{\widetilde{F}(m)}\left(b_m - \sum\limits_{\substack{d\mid m;\\ d\neq m}} \widetilde{F}(d)\,\widetilde{x}_d^{m/d}\right)$. Now, every divisor d of m satisfying $d \neq m$ must satisfy $\widetilde{F}(d)\,\widetilde{x}_d^{m/d} \in \mathbb{Q}\left[b_{\mathbb{N}_{|m}}\right]$ (in fact, $d \mid m$ and $d \neq m$ yield $d < m$, and thus (43) (applied to $n = d$) yields $\widetilde{x}_d \in \mathbb{Q}\left[b_{\mathbb{N}_{|d}}\right]$ and thus $\widetilde{x}_d \in \mathbb{Q}\left[b_{\mathbb{N}_{|m}}\right]$ (since $d \mid m$ yields $\mathbb{N}_{|d} \subseteq \mathbb{N}_{|m}$ and thus $\mathbb{Q}\left[b_{\mathbb{N}_{|d}}\right] \subseteq \mathbb{Q}\left[b_{\mathbb{N}_{|m}}\right]$), so that $\widetilde{F}(d)\,\widetilde{x}_d^{m/d} \in \mathbb{Q}\left[b_{\mathbb{N}_{|m}}\right]$), and clearly $b_m \in \mathbb{Q}\left[b_{\mathbb{N}_{|m}}\right]$. Hence, $\widetilde{x}_m = \dfrac{1}{\widetilde{F}(m)}\left(\underbrace{b_m}_{\in\mathbb{Q}\left[b_{\mathbb{N}_{|m}}\right]} - \sum\limits_{\substack{d\mid m;\\ d\neq m}} \underbrace{\widetilde{F}(d)\,\widetilde{x}_d^{m/d}}_{\in\mathbb{Q}\left[b_{\mathbb{N}_{|m}}\right]}\right) \in \mathbb{Q}\left[b_{\mathbb{N}_{|m}}\right]$.

Thus, $\widetilde{x}_n \in \mathbb{Q}\left[b_{\mathbb{N}_{|n}}\right]$ holds for $n = m$. This completes the induction step, and thus we have proven that $\widetilde{x}_n \in \mathbb{Q}\left[b_{\mathbb{N}_{|n}}\right]$ for every $n \in N$. This completes the proof of Theorem 22 **(b)**.

(c) Assume that $(b_n)_{n\in N} \in (\mathbb{Z}[\Xi])^N$. Then, we must prove that the family $(\widetilde{x}_n)_{n\in N} \in (\mathbb{Q}[\Xi])^N$ defined in Theorem 22 **(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 (42).

In order to prove this, we must show the following two assertions:

Assertion 1: If the family $(\widetilde{x}_n)_{n\in N} \in (\mathbb{Q}[\Xi])^N$ defined in Theorem 22 **(a)** satisfies $(\widetilde{x}_n)_{n\in N} \in (\mathbb{Z}[\Xi])^N$, then every $n \in N$ and every $p \in \operatorname{PF} n$ satisfies (42).

Assertion 2: If every $n \in N$ and every $p \in \operatorname{PF} n$ satisfies (42), then the family $(\widetilde{x}_n)_{n\in N} \in (\mathbb{Q}[\Xi])^N$ defined in Theorem 22 **(a)** satisfies $(\widetilde{x}_n)_{n\in N} \in (\mathbb{Z}[\Xi])^N$.

Proof of Assertion 1: Assume that the family $(\widetilde{x}_n)_{n\in N} \in (\mathbb{Q}[\Xi])^N$ defined in Theorem 22 **(a)** satisfies $(\widetilde{x}_n)_{n\in N} \in (\mathbb{Z}[\Xi])^N$. Remember that the family $(\widetilde{x}_n)_{n\in N}$ satisfies

$\left(b_n = w_{F,n}\left(\left(\widetilde{x}_k\right)_{k\in N}\right) \text{ for every } n \in N\right)$ (according to Theorem 22 **(a)**). Thus, there exists a family $\left(x_n\right)_{n\in N} \in \left(\mathbb{Z}\left[\Xi\right]\right)^N$ satisfying $\left(b_n = w_{F,n}\left(\left(x_k\right)_{k\in N}\right) \text{ for every } n \in N\right)$ (namely, the family $\left(x_n\right)_{n\in N} = \left(\widetilde{x}_n\right)_{n\in N}$). In other words, the assertion $\mathcal{D}_\Xi$ of Theorem 13 is satisfied. Hence, the assertion $\mathcal{C}_\Xi$ of Theorem 13 is also satisfied (since the assertions $\mathcal{C}_\Xi$ and $\mathcal{D}_\Xi$ are equivalent, according to Theorem 13). In other words, every $n \in N$ and every $p \in \operatorname{PF} n$ satisfies (42). Thus, Assertion 1 is proven.

Proof of Assertion 2: Assume that every $n \in N$ and every $p \in \operatorname{PF} n$ satisfies (42). Then, the assertion $\mathcal{C}_\Xi$ of Theorem 13 is fulfilled. Hence, the assertion $\mathcal{D}_\Xi$ of Theorem 13 is satisfied as well (since the assertions $\mathcal{C}_\Xi$ and $\mathcal{D}_\Xi$ are equivalent, according to Theorem 13). In other words, there exists a family $\left(x_n\right)_{n\in N} \in \left(\mathbb{Z}\left[\Xi\right]\right)^N$ of elements of $\mathbb{Z}\left[\Xi\right]$ such that

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

This family $\left(x_n\right)_{n\in N}$ obviously satisfies $\left(x_n\right)_{n\in N} \in \left(\mathbb{Q}\left[\Xi\right]\right)^N$ (since it satisfies $\left(x_n\right)_{n\in N} \in \left(\mathbb{Z}\left[\Xi\right]\right)^N \subseteq \left(\mathbb{Q}\left[\Xi\right]\right)^N$) and

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

Hence, this family $\left(x_n\right)_{n\in N}$ must be equal to the family $\left(\widetilde{x}_n\right)_{n\in N}$ (because, according to Theorem 22 **(a)**, the only 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

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

is the family $\left(\widetilde{x}_n\right)_{n\in\mathbb{N}}$). Since this family $\left(x_n\right)_{n\in N}$ satisfies $\left(x_n\right)_{n\in N} \in \left(\mathbb{Z}\left[\Xi\right]\right)^N$, this yields that $\left(\widetilde{x}_n\right)_{n\in N} \in \left(\mathbb{Z}\left[\Xi\right]\right)^N$. This proves Assertion 2.

Thus, both assertions 1 and 2 are proven, and consequently the proof of Theorem 22 **(c)** is complete.

Now we come to the main application of Theorem 13:

Theorem 25. Let $F : \mathbb{P} \times \mathbb{N} \to \mathbb{N}$ be a pseudo-monotonous map. Let N be a nest. Let $m \in \mathbb{N}$. Let Ξ denote the family $\left(X_{k,n}\right)_{(k,n)\in\{1,2,...,m\}\times N}$ of symbols. This family is clearly the union $\bigcup\limits_{k\in\{1,2,...,m\}} X_{k,N}$ of the families $X_{k,N}$ defined by $X_{k,N} = \left(X_{k,n}\right)_{n\in N}$ for each $k \in \{1, 2, ..., m\}$. For each $k \in \{1, 2, ..., m\}$, the family $X_{k,N} = \left(X_{k,n}\right)_{n\in N}$ consists of $|N|$ symbols; their union Ξ is a family consisting of $m \cdot |N|$ symbols. (Consequently, $\mathbb{Z}\left[\Xi\right] = \mathbb{Z}\left[\left(X_{k,n}\right)_{(k,n)\in\{1,2,...,m\}\times N}\right]$ 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 $f \in \mathbb{Z}\left[\alpha_1, \alpha_2, ..., \alpha_m\right]$ be a polynomial in m variables.

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

$$\left(w_{F,n}\left(\left(x_k\right)_{k\in N}\right) = f\left(w_{F,n}\left(X_{1,N}\right), w_{F,n}\left(X_{2,N}\right), ..., w_{F,n}\left(X_{m,N}\right)\right) \qquad \text{for every } n \in N\right). \tag{44}$$

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

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

(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 $n \in N$.

Proof of Theorem 25. Define a family $(b_n)_{n\in N} \in (\mathbb{Q}[\Xi])^N$ of polynomials in the indeterminates Ξ by

$$b_n = f\left(w_{F,n}(X_{1,N}), w_{F,n}(X_{2,N}), ..., w_{F,n}(X_{m,N})\right) \qquad \text{for every } n \in N. \tag{45}$$

Then, Theorem 22 **(a)** yields that there exists *one and only one* family $(x_n)_{n\in N} \in (\mathbb{Q}[\Xi])^N$ of elements of $\mathbb{Q}[\Xi]$ such that

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

Since the assertion $\left(b_n = w_{F,n}\left((x_k)_{k\in N}\right) \text{ for every } n \in N\right)$ is equivalent to (44)[37], this rewrites as follows: There exists *one and only one* family $(x_n)_{n\in N} \in (\mathbb{Q}[\Xi])^N$ of elements of $\mathbb{Q}[\Xi]$ such that

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

Thus, Theorem 25 **(a)** is proven.

Next, we are going to prove Theorem 25 **(b)**.

First, notice that every $k \in \{1,2,...,m\}$ satisfies

$$w_{F,n}(X_{k,N}) \in \mathbb{Z}\left[\Xi_{\mathbb{N}_{|n}}\right] \qquad \text{for every } n \in N \tag{46}$$

(because $w_{F,n}(X_{k,N}) = w_{F,n}\left((X_{k,m})_{m\in N}\right) = \sum\limits_{d|n} \widetilde{F}(d)\, X_{k,d}^{n/d} = \sum\limits_{d\in\mathbb{N}_{|n}} \widetilde{F}(d)\, X_{k,d}^{n/d} \in \mathbb{Z}\left[\Xi_{\mathbb{N}_{|n}}\right]$, since $X_{k,d} \in \mathbb{Z}\left[\Xi_{\mathbb{N}_{|n}}\right]$ for every $d \in \mathbb{N}_{|n}$). Hence,

$$w_{F,d}(X_{k,N}) \in \mathbb{Z}\left[\Xi_{\mathbb{N}_{|n}}\right] \qquad \text{for every } n \in N \text{ and every } d \in \mathbb{N}_{|n} \tag{47}$$

(because (46), applied to d instead of n, yields $w_{F,d}(X_{k,N}) \in \mathbb{Z}\left[\Xi_{\mathbb{N}_{|d}}\right] \subseteq \mathbb{Z}\left[\Xi_{\mathbb{N}_{|n}}\right]$, because $\Xi_{\mathbb{N}_{|d}} \subseteq \Xi_{\mathbb{N}_{|n}}$, because $\mathbb{N}_{|d} \subseteq \mathbb{N}_{|n}$, since $d \in \mathbb{N}_{|n}$).

Further, notice that every $n \in N$ satisfies

$$\mathbb{Q}\left[\Xi_{\mathbb{N}_{|n}}\right] \cap \mathbb{Z}[\Xi] = \mathbb{Z}\left[\Xi_{\mathbb{N}_{|n}}\right]. \tag{48}$$

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

$$\begin{aligned}
&\left(b_n = w_{F,n}\left((x_k)_{k\in N}\right) \text{ for every } n \in N\right)\\
\Longleftrightarrow\ &\left(f\left(w_{F,n}(X_{1,N}), w_{F,n}(X_{2,N}), ..., w_{F,n}(X_{m,N})\right) = w_{F,n}\left((x_k)_{k\in N}\right) \text{ for every } n \in N\right) \qquad \text{(because of (45))}\\
\Longleftrightarrow\ &\left((44) \text{ holds}\right).
\end{aligned}$$

In fact, this follows from a general rule: If U and V are two sets of symbols such that $U \subseteq V$, then $\mathbb{Q}[U] \cap \mathbb{Z}[V] = \mathbb{Z}[U]$. [38]

Now, the family $(\widetilde{x}_n)_{n\in N}$ defined in Theorem 22 **(a)** is the same as the family $(f_n)_{n\in N}$ defined in Theorem 25 **(a)** [39].

Theorem 22 **(b)** yields that the family $(\widetilde{x}_n)_{n\in N} \in (\mathbb{Q}[\Xi])^N$ defined in Theorem 22 **(a)** satisfies $\widetilde{x}_n \in \mathbb{Q}\left[b_{\mathbb{N}_{|n}}\right]$ for every $n \in N$. Since the family $(\widetilde{x}_n)_{n\in N}$ defined in Theorem 22 **(a)** is the same as the family $(f_n)_{n\in N}$ defined in Theorem 25 **(a)**, this yields that the family $(f_n)_{n\in N}$ defined in Theorem 25 **(a)** satisfies $f_n \in \mathbb{Q}\left[b_{\mathbb{N}_{|n}}\right]$ for every $n \in N$. Hence, $f_n \in \mathbb{Q}\left[\Xi_{\mathbb{N}_{|n}}\right]$ (where $\mathbb{Q}\left[\Xi_{\mathbb{N}_{|n}}\right]$ means the sub-$\mathbb{Q}$-algebra of $\mathbb{Q}[\Xi]$ generated by the polynomials $X_{k,d}$ for $k \in \{1,2,...,m\}$ and $d \in \mathbb{N}_{|n}$), because $\mathbb{Q}\left[b_{\mathbb{N}_{|n}}\right] \subseteq \mathbb{Q}\left[\Xi_{\mathbb{N}_{|n}}\right]$ (since $\mathbb{Q}\left[b_{\mathbb{N}_{|n}}\right]$ is the sub-$\mathbb{Q}$-algebra of $\mathbb{Q}[\Xi]$ generated by the polynomials b_d for all $d \in \mathbb{N}_{|n}$, and every of these polynomials b_d lies in $\mathbb{Q}\left[\Xi_{\mathbb{N}_{|n}}\right]$ because the definition of b_d states

$$b_d = f\left(w_{F,d}(X_{1,N}), w_{F,d}(X_{2,N}), ..., w_{F,d}(X_{m,N})\right) \in \mathbb{Z}\left[\Xi_{\mathbb{N}_{|n}}\right] \qquad (\text{by (47), since } f \in \mathbb{Z}[\alpha_1,\alpha_2,...,\alpha_m])$$
$$\subseteq \mathbb{Q}\left[\Xi_{\mathbb{N}_{|n}}\right]$$

).

Now we are going to prove that $f_n \in \mathbb{Z}[\Xi]$. In fact, for every $k \in \{1,2,...,m\}$, let $X_{k,N}^p$ denote the family of the p-th powers of all elements of the family $X_{k,N}$ (considered as elements of $\mathbb{Z}[X_{k,N}]$). In other words, we let $X_{k,N}^p = \left(X_{k,n}^p\right)_{n\in N}$. Clearly, $\Xi = \bigcup\limits_{k\in\{1,2,...,m\}} X_{k,N}$ yields $\Xi^p = \bigcup\limits_{k\in\{1,2,...,m\}} X_{k,N}^p$.

But for any divisor d of n, the assertions $d \nmid (n/p)$ and $p^{v_p(n)} \mid d$ are equivalent[40]. Hence, every divisor d of n which satisfies $d \nmid (n/p)$ must satisfy $\widetilde{F}(d) \equiv 0 \operatorname{mod} p^{F(p,v_p(n))}\mathbb{Z}[\Xi]$ [41].

[38] *Proof.* In order to verify this, we need to show that any polynomial $P \in \mathbb{Q}[V]$ satisfies ($P \in \mathbb{Q}[U]$ and $P \in \mathbb{Z}[V]$) if and only if it satisfies $P \in \mathbb{Z}[U]$.

In fact, any polynomial $P \in \mathbb{Q}[V]$ has the form $P = \sum\limits_{\alpha \in V_{\text{fin}}^{\mathbb{N}}} \lambda_\alpha \prod\limits_{v\in V} v^{\alpha(v)}$, where $\lambda_\alpha \in \mathbb{Q}$ for every $\alpha \in V_{\text{fin}}^{\mathbb{N}}$.

- This polynomial P satisfies $P \in \mathbb{Q}[U]$ if and only if $\lambda_\alpha = 0$ for every $\alpha \in V_{\text{fin}}^{\mathbb{N}} \setminus U_{\text{fin}}^{\mathbb{N}}$.
- This polynomial P satisfies $P \in \mathbb{Z}[V]$ if and only if $\lambda_\alpha \in \mathbb{Z}$ for every $\alpha \in V_{\text{fin}}^{\mathbb{N}}$.
- This polynomial P satisfies $P \in \mathbb{Z}[U]$ if and only if $\lambda_\alpha \in \mathbb{Z}$ for every $\alpha \in U_{\text{fin}}^{\mathbb{N}}$ and $\lambda_\alpha = 0$ for every $\alpha \in V_{\text{fin}}^{\mathbb{N}} \setminus U_{\text{fin}}^{\mathbb{N}}$.

Hence, this polynomial P satisfies ($P \in \mathbb{Q}[U]$ and $P \in \mathbb{Z}[V]$) if and only if it satisfies $P \in \mathbb{Z}[U]$, qed.

[39] In fact, the family $(\widetilde{x}_n)_{n\in N}$ defined in Theorem 22 **(a)** is the only family $(x_n)_{n\in N} \in (\mathbb{Q}[\Xi])^N$ satisfying $\left(b_n = w_{F,n}\left((x_k)_{k\in N}\right)\right.$ for every $\left.n \in N\right)$, while the family $(f_n)_{n\in N}$ defined in Theorem 25 **(a)** is the only family $(x_n)_{n\in N} \in (\mathbb{Q}[\Xi])^N$ satisfying (44). Since $\left(b_n = w_{F,n}\left((x_k)_{k\in N}\right)\right.$ for every $\left.n \in N\right)$ is equivalent to (44), this yields that the family $(\widetilde{x}_n)_{n\in N}$ defined in Theorem 22 **(a)** is the same as the family $(f_n)_{n\in N}$ defined in Theorem 25 **(a)**.

[40] We have already proven this during our proof of Theorem 4.

[41] In fact, let d be a divisor of n satisfying $d \nmid (n/p)$. Then, $p^{v_p(n)} \mid d$ (since the assertions $d \nmid (n/p)$

Obviously,

$$\begin{aligned} w_{F,n/p}\left(X_{k,N}^{p}\right) &= w_{F,n/p}\left(\left(X_{k,n}^{p}\right)_{n\in N}\right) \\ &= \sum_{d\mid(n/p)} \widetilde{F}(d)\ \underbrace{\left(X_{k,d}^{p}\right)^{(n/p)/d}}_{=X_{k,d}^{p\cdot(n/p)/d}=X_{k,d}^{n/d}} \qquad \left(\text{since } w_{F,n/p} = \sum_{d\mid(n/p)} \widetilde{F}(d)\, X_{d}^{(n/p)/d}\right) \\ &= \sum_{d\mid(n/p)} \widetilde{F}(d)\, X_{k,d}^{n/d} \end{aligned}$$

and

$$\begin{aligned} w_{F,n}\left(X_{k,N}\right) &= w_{F,n}\left(\left(X_{k,n}\right)_{n\in N}\right) = \sum_{d\mid n} \widetilde{F}(d)\, X_{k,d}^{n/d} \qquad \left(\text{since } w_{F,n} = \sum_{d\mid n} \widetilde{F}(d)\, X_{d}^{n/d}\right) \\ &= \underbrace{\sum_{\substack{d\mid n;\\ d\mid(n/p)}}}_{=\sum_{d\mid(n/p)}} \widetilde{F}(d)\, X_{k,d}^{n/d} + \sum_{\substack{d\mid n;\\ d\nmid(n/p)}} \underbrace{\widetilde{F}(d)}_{\substack{\equiv 0 \operatorname{mod} p^{F(p,v_p(n))}\mathbb{Z}[\Xi] \\ \text{(since } d \text{ is a divisor of } n \\ \text{which satisfies } d\nmid(n/p))}} X_{k,d}^{n/d} \\ &\equiv \sum_{d\mid(n/p)} \widetilde{F}(d)\, X_{k,d}^{n/d} + \underbrace{\sum_{\substack{d\mid n;\\ d\nmid(n/p)}} 0X_{k,d}^{n/d}}_{=0} = \sum_{d\mid(n/p)} \widetilde{F}(d)\, X_{k,d}^{n/d} \operatorname{mod} p^{F(p,v_p(n))}\mathbb{Z}[\Xi], \end{aligned}$$

so that

$$w_{F,n/p}\left(X_{k,N}^{p}\right) \equiv w_{F,n}\left(X_{k,N}\right) \operatorname{mod} p^{F(p,v_p(n))}\mathbb{Z}[\Xi]. \tag{49}$$

On the other hand, $(b_n)_{n\in N} \in (\mathbb{Z}[\Xi])^N$. Hence, Theorem 22 **(c)** yields that the family $(\widetilde{x}_n)_{n\in N} \in (\mathbb{Q}[\Xi])^N$ defined in Theorem 22 **(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 (42). Since the family $(\widetilde{x}_n)_{n\in N}$ defined in Theorem 22 **(a)** is the same as the family $(f_n)_{n\in N}$ defined in Theorem 25 **(a)**, this rewrites as follows: The family $(f_n)_{n\in N}$ defined in Theorem 25 **(a)** satisfies $(f_n)_{n\in N} \in (\mathbb{Z}[\Xi])^N$ if and only if every $n \in N$ and every $p \in \operatorname{PF} n$ satisfies (42). But since every $n \in N$ and every $p \in \operatorname{PF} n$ satisfies (42) (because the definition of $b_{n/p}$ yields

$$b_{n/p} = f\left(w_{F,n/p}\left(X_{1,N}\right), w_{F,n/p}\left(X_{2,N}\right), ..., w_{F,n/p}\left(X_{m,N}\right)\right)$$

and $p^{v_p(n)} \mid d$ are equivalent), so that $v_p(d) \geq v_p(n)$. Together with $v_p(d) \leq v_p(n)$ (which is because $d \mid n$ yields $\dfrac{n}{d} \in \mathbb{Z}$, thus $v_p\left(\dfrac{n}{d}\right) \geq 0$ and now $v_p(n) = v_p\left(d\dfrac{n}{d}\right) = v_p(d) + \underbrace{v_p\left(\dfrac{n}{d}\right)}_{\geq 0} \geq v_p(d)$), this becomes $v_p(d) = v_p(n)$. Hence, the equality $v_p\left(\widetilde{F}(d)\right) = F(p, v_p(d))$ (which follows from (3), applied to d instead of n) rewrites as $v_p\left(\widetilde{F}(d)\right) = F(p, v_p(n))$, so that $p^{F(p,v_p(n))} \mid \widetilde{F}(d)$, and thus $\widetilde{F}(d) \equiv 0 \operatorname{mod} p^{F(p,v_p(n))}\mathbb{Z}[\Xi]$.

and thus

$$\begin{aligned} b_{n/p}\left(\Xi^p\right) &= f\left(w_{F,n/p}\left(X_{1,N}^p\right), w_{F,n/p}\left(X_{2,N}^p\right), ..., w_{F,n/p}\left(X_{m,N}^p\right)\right) \\ &\equiv f\left(w_{F,n}\left(X_{1,N}\right), w_{F,n}\left(X_{2,N}\right), ..., w_{F,n}\left(X_{m,N}\right)\right) \qquad \text{(because of (49))} \\ &= b_n \operatorname{mod} p^{F(p,v_p(n))}\mathbb{Z}\left[\Xi\right] \end{aligned}$$

(by the definition of b_n)), this yields that the family $(f_n)_{n\in N}$ defined in Theorem 25 **(a)** satisfies $(f_n)_{n\in N} \in (\mathbb{Z}[\Xi])^N$. Hence, $f_n \in \mathbb{Z}[\Xi]$ for every $n \in N$. Combining this with $f_n \in \mathbb{Q}\left[\Xi_{\mathbb{N}_{|n}}\right]$ (which also holds for every $n \in N$), we obtain

$$f_n \in \mathbb{Q}\left[\Xi_{\mathbb{N}_{|n}}\right] \cap \mathbb{Z}[\Xi] = \mathbb{Z}\left[\Xi_{\mathbb{N}_{|n}}\right]$$

(by (48)). This proves Theorem 25 **(b)**.

[...]

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

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#5d: Analoga of integrality criteria for radical Witt polynomials.*
http://www.cip.ifi.lmu.de/~grinberg/algebra/witt5d.pdf