Witt vectors. Part 1
Michiel Hazewinkel
Sidenotes by Darij Grinberg

Witt#5: Around the integrality criterion 9.93
[version 1.1 (21 April 2013), not completed, not proofread]

In [1], section 9.93, Hazewinkel states that *"The (integrality aspects of the) theory of Witt vectors can be developed solely on the basis of this lemma 9.93."*. The purpose of this note is to point out how this is done (at least, by proving Theorem 9.73, even slightly generalized), to prove and extend Lemma 9.93 in [1] and to show some more of its applications.

First, let us introduce some notation:

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

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

Definition 3. Let Ξ be a family of symbols. We consider the polynomial ring $\mathbb{Q}[\Xi]$ (this is the polynomial ring over $\mathbb{Q}$ in the indeterminates Ξ; in other words, we use the symbols from Ξ as variables for the polynomials) and its subring $\mathbb{Z}[\Xi]$ (this is the polynomial ring over $\mathbb{Z}$ in the indeterminates Ξ). [1]. For any $n \in \mathbb{N}$, let Ξ^n mean the family of the n-th powers of all elements of our family Ξ (considered as elements of $\mathbb{Z}[\Xi]$) [2]. (Therefore, whenever $P \in \mathbb{Q}[\Xi]$ is a polynomial, then $P(\Xi^n)$ is the polynomial obtained from P after replacing every indeterminate by its n-th power.[3])

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

Definition 4. If m and n are two integers, then we write $m \perp n$ if and only if m is coprime to n. If m is an integer and S is a set, then we write $m \perp S$ if and only if ($m \perp n$ for every $n \in S$).

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

Here are some examples of nests: For instance, $\mathbb{N}_+$ itself is a nest. For every prime p, the set $\{1, p, p^2, p^3, ...\}$ is a nest; we denote this nest by $p^{\mathbb{N}}$. For

[1]For instance, Ξ can be $(X_0, X_1, X_2, ...)$, in which case $\mathbb{Z}[\Xi]$ means $\mathbb{Z}[X_0, X_1, X_2, ...]$. Or, Ξ can be $(X_0, X_1, X_2, ...; Y_0, Y_1, Y_2, ...; Z_0, Z_1, Z_2, ...)$, in which case $\mathbb{Z}[\Xi]$ means $\mathbb{Z}[X_0, X_1, X_2, ...; Y_0, Y_1, Y_2, ...; Z_0, Z_1, Z_2, ...]$.

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

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

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 [4].

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

If A is a commutative ring with unity, if N is a set, if $(x_d)_{d \in N} \in A^N$ is a family of elements of A indexed by elements of N, and if $P \in \mathbb{Z}[X_N]$, then we denote by $P\left((x_d)_{d \in N}\right)$ the element of A that we obtain if we substitute x_d for X_d for every $d \in N$ into the polynomial P. (For instance, if $N = \{1, 2, 5\}$ and $P = X_1^2 + X_2 X_5 - X_5$, and if $x_1 = 13$, $x_2 = 37$ and $x_5 = 666$, then $P\left((x_d)_{d \in N}\right) = 13^2 + 37 \cdot 666 - 666$.)

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

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

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

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

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

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

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

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

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

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

Definition 8. Let $n \in \mathbb{Z} \setminus \{0\}$. Let $p \in \mathbb{P}$. We denote by $v_p(n)$ the largest nonnegative integer m satisfying $p^m \mid n$. Clearly, $p^{v_p(n)} \mid n$ and $v_p(n) \geq 0$. Besides, $v_p(n) = 0$ if and only if $p \nmid n$.
We also set $v_p(0) = \infty$; this way, our definition of $v_p(n)$ extends to all $n \in \mathbb{Z}$ (and not only to $n \in \mathbb{Z} \setminus \{0\}$).

Definition 9. Let $n \in \mathbb{N}_+$. We denote by $\operatorname{PF} n$ the set of all prime divisors of n. By the unique factorization theorem, the set $\operatorname{PF} n$ is finite and satisfies $n = \prod\limits_{p \in \operatorname{PF} n} p^{v_p(n)}$.

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

This Theorem 1 is part of the (well-known) Chinese Remainder Theorem for modules, which is proven in every book on commutative algebra; however, let us also give a quick proof of Theorem 1 here, in order for this note to be self-contained.

Proof of Theorem 1. We are going to prove Theorem 1 by induction over N. First, the induction base: The case of $N = 0$ is obvious (in this case, the assertion of Theorem 1 has to be interpreted as $M = M$, which is obviously true), and the case of $N = 1$ is obvious as well (in this case, the assertion of Theorem 1 simply states that $I_1 \cdot M = I_1 M$, which is true). For the induction step, let us fix some $m \in \mathbb{N}_+$ such that $m > 1$, and let us assume that Theorem 1 is proven for $N = m - 1$. We want to prove that Theorem 1 holds for $N = m$ as well. In other words, we want to prove that $I_1 I_2 ... I_m \cdot M = I_1 M \cap I_2 M \cap ... \cap I_m M$ for any m ideals I_1, I_2, ..., I_m of A which satisfy

$$(I_i + I_j = A \text{ for any two elements } i \text{ and } j \text{ of } \{1, 2, ..., m\} \text{ satisfying } i < j). \tag{1}$$

So let I_1, I_2, ..., I_m be m such ideals. For every $i \in \{1, 2, ..., m-1\}$, we have $I_i + I_m = A$ (due to (1) (applied to $j = m$), since $i < m$); thus, there exist $a_i \in I_i$ and $b_i \in I_m$ such that $a_i + b_i = 1$, and thus $1 = a_i + b_i \equiv a_i \operatorname{mod} I_m$ (since $b_i \in I_m$). Therefore,

$$1 = \prod_{i=1}^{m-1} \underbrace{1}_{\equiv a_i \operatorname{mod} I_m} \equiv \prod_{i=1}^{m-1} a_i \operatorname{mod} I_m,$$

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

so that $1 \in \prod_{i=1}^{m-1} a_i + I_m$. But $\prod_{i=1}^{m-1} a_i \in I_1 I_2 ... I_{m-1}$ (since $a_i \in I_i$ for every $i \in \{1, 2, ..., m-1\}$). Hence, $1 \in \prod_{i=1}^{m-1} a_i + I_m$ yields $1 \in I_1 I_2 ... I_{m-1} + I_m$. Thus, $I_1 I_2 ... I_{m-1} + I_m = A$.

But since Theorem 1 is proven for $N = m-1$, we must have $J_1 J_2 ... J_{m-1} \cdot M = J_1 M \cap J_2 M \cap ... \cap J_{m-1} M$ for any $m-1$ ideals J_1, J_2, ..., J_{m-1} of A which satisfy

$$(J_i + J_j = A \text{ for any two elements } i \text{ and } j \text{ of } \{1, 2, ..., m-1\} \text{ satisfying } i < j). \quad (2)$$

In particular, applying this to the ideals $J_1 = I_1$, $J_2 = I_2$, ..., $J_{m-1} = I_{m-1}$ (which satisfy (2) because of (1)), we obtain $I_1 I_2 ... I_{m-1} \cdot M = I_1 M \cap I_2 M \cap ... \cap I_{m-1} M$. Thus,

$$I_1 M \cap I_2 M \cap ... \cap I_m M = \underbrace{I_1 M \cap I_2 M \cap ... \cap I_{m-1} M}_{= I_1 I_2 ... I_{m-1} \cdot M} \cap I_m M = I_1 I_2 ... I_{m-1} M \cap I_m M$$

$$= \underbrace{A}_{= I_1 I_2 ... I_{m-1} + I_m} \cdot (I_1 I_2 ... I_{m-1} M \cap I_m M)$$

$$= (I_1 I_2 ... I_{m-1} + I_m) \cdot (I_1 I_2 ... I_{m-1} M \cap I_m M) \subseteq I_1 I_2 ... I_{m-1} \cdot I_m \cdot M$$

$$\left(\begin{array}{c} \text{since } (U+V) \cdot (UM \cap VM) \subseteq UV \cdot M \text{ for any two ideals } U \text{ and } V \text{ of } A \text{, because} \\ (U+V) \cdot (UM \cap VM) = U \cdot \underbrace{(UM \cap VM)}_{\subseteq VM} + V \cdot \underbrace{(UM \cap VM)}_{\subseteq UM} \subseteq UVM + VUM \\ = UVM + UVM \subseteq UVM \end{array} \right)$$

$$= I_1 I_2 ... I_m \cdot M.$$

But clearly, $I_1 I_2 ... I_m \cdot M \subseteq I_1 M \cap I_2 M \cap ... \cap I_m M$ (since $I_1 I_2 ... I_m \cdot M \subseteq I_i \cdot M$ for every $i \in \{1, 2, ..., m\}$). Thus, $I_1 I_2 ... I_m \cdot M = I_1 M \cap I_2 M \cap ... \cap I_m M$. This completes the induction step, and thus Theorem 1 is verified.

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

Corollary 2. Let A be an Abelian group (written additively). Let $n \in \mathbb{N}_+$. Then, $nA = \bigcap_{p \in \operatorname{PF} n} \left(p^{v_p(n)} A \right)$.

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, $\prod_{i=1}^{N} p_i^{v_{p_i}(n)} = \prod_{p \in \operatorname{PF} n} p^{v_p(n)} = n$.

Define an ideal I_i of $\mathbb{Z}$ by $I_i = p_i^{v_{p_i}(n)} \mathbb{Z}$ 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 $p_i^{v_{p_i}(n)}$ and $p_j^{v_{p_j}(n)}$ are coprime[7], and thus, by Bezout's theorem, there exist integers α and β such that $1 = p_i^{v_{p_i}(n)} \alpha + p_j^{v_{p_j}(n)} \beta$ in $\mathbb{Z}$, and therefore $1 = \underbrace{p_i^{v_{p_i}(n)} \alpha}_{\in p_i^{v_{p_i}(n)} \mathbb{Z} = I_i} + \underbrace{p_j^{v_{p_j}(n)} \beta}_{\in p_j^{v_{p_j}(n)} \mathbb{Z} = I_j} \in I_i + I_j$

[7]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)

in $\mathbb{Z}$, and thus $I_i + I_j = \mathbb{Z}$). Hence, Theorem 1 (applied to $\mathbb{Z}$ and A instead of A and M, respectively) yields $I_1 I_2 ... I_N \cdot A = I_1 A \cap I_2 A \cap ... \cap I_N A$. Since

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

and

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

(since $\operatorname{PF} n = \{p_1, p_2, ..., p_N\}$), this becomes $nA = \bigcap_{p \in \operatorname{PF} n} \left(p^{v_p(n)} A\right)$. 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[8]. Let $k \in \mathbb{N}$ and $\ell \in \mathbb{N}$ be such that $k > 0$. Let $a \in A$ and $b \in A$. If $a \equiv b \bmod p^k A$, then $a^{p^\ell} \equiv b^{p^\ell} \bmod p^{k+\ell} A$.

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

Now we can start with the main theorem - an extension of Lemma 9.93 in [1]:

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

$$\left(\varphi_p(a) \equiv a^p \bmod pA \text{ holds for every } a \in A \text{ and } p \in \mathbb{P} \cap N\right). \qquad (3)$$

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

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

$$\varphi_p\left(b_{n/p}\right) \equiv b_n \bmod p^{v_p(n)} A. \qquad (4)$$

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

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

This Theorem 4 is stronger than Lemma 9.93 in [1]. In fact, if we set $N = \mathbb{N}_+$ in Theorem 4, and require the ring A to have characteristic zero, then we obtain Lemma 9.93 in [1] (in a slightly different formulation, however - for example, our Assertion $\mathcal{C}$ is the congruence (9.94) in [1] with n replaced by n/p). None of the requirements $N = \mathbb{N}_+$ and "A has characteristic zero" is necessary for Theorem 4 to hold; however, requiring

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

A to have characteristic zero would make the family $(x_n)_{n\in N}$ unique in Assertion $\mathcal{D}$ (we will detail this later in Theorem 9).

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

$$\left(b_n = w_n\left((x_k)_{k\in N}\right) \text{ for every } n \in N\right). \tag{5}$$

We want to prove that Assertion $\mathcal{C}$ holds, i. e., that every $n \in N$ and every $p \in \operatorname{PF} n$ satisfies (4). 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 [9]). Thus, applying (5) to n/p instead of n yields $b_{n/p} = w_{n/p}\left((x_k)_{k\in N}\right)$. But $w_{n/p}\left((x_k)_{k\in N}\right) = \sum\limits_{d\mid (n/p)} dx_d^{(n/p)/d}$ and $w_n\left((x_k)_{k\in N}\right) = \sum\limits_{d\mid n} dx_d^{n/d}$. Now, (5) yields

$$b_n = w_n\left((x_k)_{k\in N}\right) = \sum_{d\mid n} dx_d^{n/d} = \sum_{\substack{d\mid n;\\ d\mid (n/p)}} dx_d^{n/d} + \sum_{\substack{d\mid n;\\ d\nmid (n/p)}} dx_d^{n/d}. \tag{6}$$

But for any divisor d of n, the assertions $d \nmid (n/p)$ and $p^{v_p(n)} \mid d$ are equivalent[10]. Thus,

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

Thus, (6) becomes

$$b_n = \sum_{\substack{d\mid n;\\ d\mid (n/p)}} dx_d^{n/d} + \underbrace{\sum_{\substack{d\mid n;\\ d\nmid (n/p)}} dx_d^{n/d}}_{\equiv 0 \bmod p^{v_p(n)}A} \equiv \sum_{\substack{d\mid n;\\ d\mid (n/p)}} dx_d^{n/d} + 0 = \sum_{\substack{d\mid n;\\ d\mid (n/p)}} dx_d^{n/d} = \sum_{d\mid (n/p)} dx_d^{n/d} \bmod p^{v_p(n)}A. \tag{7}$$

On the other hand,

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

$$\varphi_p\left(b_{n/p}\right) = \varphi_p\left(\sum_{d\mid (n/p)} dx_d^{(n/p)/d}\right) = \sum_{d\mid (n/p)} d\left(\varphi_p\left(x_d\right)\right)^{(n/p)/d} \tag{8}$$

---

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

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

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

(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 $\dfrac{n}{d} \in \mathbb{Z}$ and thus $v_p\left(\dfrac{n}{d}\right) \geq 0$. Let $\alpha = v_p((n/p)/d)$ and $\beta = v_p(d)$. Then, $\alpha + \beta = v_p((n/p)/d) + v_p(d) = v_p(n/p) = v_p(n) - \underbrace{v_p(p)}_{=1} = v_p(n) - 1$. 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, $\beta = v_p(d)$ yields $p^\beta \mid d$, so that there exists some $\kappa \in \mathbb{N}$ such that $d = \kappa p^\beta$. Applying Lemma 3 to the values $k = 1$, $\ell = \alpha$, $a = \varphi_p(x_d)$ and $b = x_d^p$ (which satisfy $a \equiv b \bmod p^k A$ because of (3), applied to $a = x_d$) yields $(\varphi_p(x_d))^{p^\alpha} \equiv (x_d^p)^{p^\alpha} \bmod p^{1+\alpha} A$. Using the equation $(n/p)/d = p^\alpha \nu$, we get

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

Multiplying this congruence with p^β, we obtain

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

In other words,

$$p^\beta (\varphi_p(x_d))^{(n/p)/d} \equiv p^\beta x_d^{n/d} \bmod p^{v_p(n)} A$$

(since $1 + \underbrace{\alpha + \beta}_{=v_p(n)-1} = v_p(n)$). Now, multiplying this congruence with κ, we get

$$\kappa p^\beta (\varphi_p(x_d))^{(n/p)/d} \equiv \kappa p^\beta x_d^{n/d} \bmod p^{v_p(n)} A,$$

which rewrites as

$$d (\varphi_p(x_d))^{(n/p)/d} \equiv d x_d^{n/d} \bmod p^{v_p(n)} A$$

(since $\kappa p^\beta = d$). Hence, (8) becomes

$$\varphi_p(b_{n/p}) = \sum_{d \mid (n/p)} \underbrace{d (\varphi_p(x_d))^{(n/p)/d}}_{\equiv d x_d^{n/d} \bmod p^{v_p(n)} A} \equiv \sum_{d \mid (n/p)} d x_d^{n/d} \equiv b_n \bmod p^{v_p(n)} A$$

(by (7)). This proves (4), 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 (4).

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

$$b_m = \sum_{d \mid m} d x_d^{m/d} \tag{9}$$

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 (9) holds for every $m \in N \cap \{1, 2, ..., n-1\}$. Now, we must construct an element $x_n \in A$ such that (9) 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 [11] and in $\{1, 2, ..., n-1\}$ [12], 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 [13]). Besides, $n/p \in \{1, 2, ..., n-1\}$. Hence, $n/p \in N \cap \{1, 2, ..., n-1\}$. Since (by our assumption) the equation (9) holds for every $m \in N \cap \{1, 2, ..., n-1\}$, we can thus conclude that (9) holds for $m = n/p$. In other words, $b_{n/p} = \sum\limits_{d \mid (n/p)} d x_d^{(n/p)/d}$. From this equation, we can conclude (by the same reasoning as in the proof of the implication $\mathcal{D} \Longrightarrow \mathcal{C}$) that

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

Comparing this with (4), we obtain

$$\sum_{d \mid (n/p)} d x_d^{n/d} \equiv b_n \operatorname{mod} p^{v_p(n)} A. \tag{10}$$

Now, for any divisor d of n, the assertions $d \nmid (n/p)$ and $p^{v_p(n)} \mid d$ are equivalent[14]. Thus,

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

Hence,

$$\begin{aligned}
\sum_{\substack{d \mid n;\\ d \neq n}} d x_d^{n/d} &= \underbrace{\sum_{\substack{d \mid n;\\ d \nmid (n/p);\\ d \neq n}} d x_d^{n/d}}_{\equiv 0 \operatorname{mod} p^{v_p(n)} A} + \sum_{\substack{d \mid n;\\ d \mid (n/p);\\ d \neq n}} d x_d^{n/d} \equiv \sum_{\substack{d \mid n;\\ d \mid (n/p);\\ d \neq n}} d x_d^{n/d} = \sum_{\substack{d \mid n;\\ d \mid (n/p)}} d x_d^{n/d} \\
&\qquad \left(\begin{array}{c}\text{since for any divisor } d \text{ of } n \text{, the assertions } (d \mid (n/p) \text{ and } d \neq n) \text{ and } d \mid (n/p) \\ \text{are equivalent, because if } d \mid (n/p)\text{, then } d \neq n \text{ (since } n \nmid (n/p)\text{)}\end{array}\right) \\
&= \sum_{d \mid (n/p)} d x_d^{n/d} \equiv b_n \operatorname{mod} p^{v_p(n)} A \qquad (\text{by (10)}).
\end{aligned}$$

In other words,

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

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

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

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

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

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

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

Hence, there exists an element x_n of A that satisfies $b_n - \sum\limits_{\substack{d \mid n; \\ d \neq n}} d x_d^{n/d} = n x_n$. Fix such an x_n. We now claim that this element x_n satisfies (9) for $m = n$. In fact,

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

(since $b_n - \sum\limits_{\substack{d \mid n; \\ d \neq n}} d x_d^{n/d} = n x_n$). Hence, (9) 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 (9) for every $m \in N$. Therefore, this family satisfies

$$\begin{aligned} b_n &= \sum_{d \mid n} d x_d^{n/d} \qquad \text{(by (9), applied to } m = n) \\ &= w_n \left((x_k)_{k \in N} \right) \end{aligned}$$

for every $n \in N$. So we have proven that there exists a family $(x_n)_{n \in N} \in A^N$ which satisfies $b_n = w_n \left((x_k)_{k \in N} \right)$ for every $n \in N$. In other words, we have proven Assertion $\mathcal{D}$. Thus, the implication $\mathcal{C} \Longrightarrow \mathcal{D}$ 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[15]:

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

$$(\varphi_1 = \operatorname{id}) \qquad \text{and} \tag{11}$$

$$(\varphi_n \circ \varphi_m = \varphi_{nm} \text{ for every } n \in N \text{ and every } m \in N \text{ satisfying } nm \in N). \tag{12}$$

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

$$\varphi_p \left(b_{n/p} \right) \equiv b_n \bmod p^{v_p(n)} A. \tag{13}$$

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

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

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

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

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

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

$$\sum_{d \mid n} \phi(d) \varphi_d(b_{n/d}) \in nA.$$

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

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

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

$$\mu(n) = \begin{cases} (-1)^{|\operatorname{PF} n|}, & \text{if } (v_p(n) \leq 1 \text{ for every } p \in \operatorname{PF} n) \\ 0, & \text{otherwise} \end{cases}. \tag{14}$$

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

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

$$\sum_{d \mid n} \phi(d) = n; \tag{16}$$

$$\sum_{d \mid n} \mu(d) = [n = 1]; \tag{17}$$

$$\sum_{d \mid n} \mu(d) \frac{n}{d} = \phi(n); \tag{18}$$

$$\sum_{d \mid n} d\mu(d) \phi\left(\frac{n}{d}\right) = \mu(n). \tag{19}$$

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

Proof of Theorem 6. First, let us prove the identity (15). In fact, for every $n \in \mathbb{N}_+$, the assertions $(v_p(n) \leq 1$ for every $p \in \operatorname{PF} n)$ and $n = \prod_{p \in \operatorname{PF} n} p$ are equivalent[16]; hence, (15) follows directly from (14). This proves (15).

[16] In fact, if $n = \prod_{p \in \operatorname{PF} n} p$, then $(v_p(n) \leq 1$ for every $p \in \operatorname{PF} n)$ (because n equals the product $\prod_{p \in \operatorname{PF} n} p$, and every prime occurs only once in this product), and conversely, if $(v_p(n) \leq 1$ for every $p \in \operatorname{PF} n)$, then $n = \prod_{p \in \operatorname{PF} n} p$ (because every $p \in \operatorname{PF} n$ satisfies $v_p(n) \leq 1$ and $v_p(n) \geq 1$ (since $p \in \operatorname{PF} n$ yields $p \mid n$), so that $v_p(n) = 1$, and consequently, $n = \prod_{p \in \operatorname{PF} n} \underbrace{p^{v_p(n)}}_{=p^1=p} = \prod_{p \in \operatorname{PF} n} p$).

Next, let us show (16). Let $n \in \mathbb{N}_+$. Then, for every $m \in \{1, 2, ..., n\}$, the number $\gcd(m, n)$ is a divisor of n. Hence, for every $m \in \{1, 2, ..., n\}$, there exists one and only one divisor d of n such that $\gcd(m, n) = d$. Thus,

$$\{1, 2, ..., n\} = \bigcup_{d \mid n} \{m \in \{1, 2, ..., n\} \mid \gcd(m, n) = d\}.$$

Since the sets $\{m \in \{1, 2, ..., n\} \mid \gcd(m, n) = d\}$ for varying d are pairwise disjoint (because $\gcd(m, n)$ cannot equal two distinct numbers for one and the same m), this yields that

$$|\{1, 2, ..., n\}| = \sum_{d \mid n} |\{m \in \{1, 2, ..., n\} \mid \gcd(m, n) = d\}|. \tag{20}$$

For every divisor d of n, the map

$$\left\{m \in \left\{1, 2, ..., \frac{n}{d}\right\} \mid m \perp \frac{n}{d}\right\} \to \{m \in \{1, 2, ..., n\} \mid \gcd(m, n) = d\},$$
$$x \mapsto dx$$

is a bijection (because this map is well-defined[17], injective[18] and surjective[19]), so that

$$\left|\left\{m \in \left\{1, 2, ..., \frac{n}{d}\right\} \mid m \perp \frac{n}{d}\right\}\right| = |\{m \in \{1, 2, ..., n\} \mid \gcd(m, n) = d\}|.$$

Since

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

(by the definition of ϕ), this becomes

$$\phi\left(\frac{n}{d}\right) = |\{m \in \{1, 2, ..., n\} \mid \gcd(m, n) = d\}|. \tag{21}$$

[17] *Proof.* Let d be a divisor of n. For every $x \in \left\{m \in \left\{1, 2, ..., \frac{n}{d}\right\} \mid m \perp \frac{n}{d}\right\}$, we have $x \in \left\{1, 2, ..., \frac{n}{d}\right\}$ and $x \perp \frac{n}{d}$, so that $dx \in \{1, 2, ..., n\}$ (since $x \in \left\{1, 2, ..., \frac{n}{d}\right\}$) and $\gcd(dx, n) = \gcd\left(dx, d\frac{n}{d}\right) = d \underbrace{\gcd\left(x, \frac{n}{d}\right)}_{\substack{=1 \text{ (since} \\ x \perp \frac{n}{d})}} = d$, and therefore $dx \in \{m \in \{1, 2, ..., n\} \mid \gcd(m, n) = d\}$.

[18] since $d \neq 0$

[19] *Proof.* Let d be a divisor of n. Let $y \in \{m \in \{1, 2, ..., n\} \mid \gcd(m, n) = d\}$. Then, $y \in \{1, 2, ..., n\}$ and $\gcd(y, n) = d$. Hence, $\frac{y}{d} \in \mathbb{Z}$ (since $d = \gcd(y, n) \mid y$), so that $\frac{y}{d} \in \left\{1, 2, ..., \frac{n}{d}\right\}$ (since $y \in \{1, 2, ..., n\}$) and $\frac{y}{d} \perp \frac{n}{d}$ (since $d \gcd\left(\frac{y}{d}, \frac{n}{d}\right) = \gcd\left(d\frac{y}{d}, d\frac{n}{d}\right) = \gcd(y, n) = d$ yields $\gcd\left(\frac{y}{d}, \frac{n}{d}\right) = 1$). Thus, $\frac{y}{d} \in \left\{m \in \left\{1, 2, ..., \frac{n}{d}\right\} \mid m \perp \frac{n}{d}\right\}$. Of course, $y = d\frac{y}{d}$. Therefore, there exists some $x \in \left\{m \in \left\{1, 2, ..., \frac{n}{d}\right\} \mid m \perp \frac{n}{d}\right\}$ such that $y = dx$ (namely, $x = \frac{y}{d}$). In other words, y lies in the image of our map.

Now,

$$\sum_{d|n}\phi(d)=\sum_{d\in\mathbb{N}_{|n}}\phi(d)=\sum_{d\in\mathbb{N}_{|n}}\phi\left(\frac{n}{d}\right)\qquad\left(\begin{array}{c}\text{here we substituted }\dfrac{n}{d}\text{ for }d\text{ in the sum, since the map}\\ \mathbb{N}_{|n}\to\mathbb{N}_{|n},\ d\mapsto\dfrac{n}{d}\text{ is a bijection}\end{array}\right)$$
$$=\sum_{d|n}\phi\left(\frac{n}{d}\right)=\sum_{d|n}\left|\{m\in\{1,2,...,n\}\mid\gcd(m,n)=d\}\right|\qquad(\text{by (21)})$$
$$=\left|\{1,2,...,n\}\right|\qquad(\text{by (20)})$$
$$=n.$$

Thus, (16) is proven.

Let us now prove the remaining three identities. Let us denote by $\mathcal{P}(U)$ the power set of any set U. We notice that for every finite set S of primes, we have

$$\mu\left(\prod_{p\in S}p\right)=(-1)^{|S|}\tag{22}$$

[20].

Recall also that every finite set U and every $k\in\mathbb{N}$ satisfy

$$\left|\{S\in\mathcal{P}(U)\ \mid |S|=k\}\right|=\binom{|U|}{k}.\tag{23}$$

(This is a classical fact in elementary combinatorics, saying that the number of k-element subsets of the finite set U is $\binom{|U|}{k}$.) Thus, it is easy to see that every finite set U satisfies

$$\sum_{S\in\mathcal{P}(U)}(-1)^{|S|}=[|U|=0]\tag{24}$$

---

[20] *Proof.* Let S be a finite set of primes. Set $N=\prod_{p\in S}p$. Then, $\operatorname{PF}N=\operatorname{PF}\left(\prod_{p\in S}p\right)=S$. We have $N=\prod_{p\in S}p=\prod_{p\in\operatorname{PF}N}p$ (since $S=\operatorname{PF}N$). Now, (15) yields

$$\mu(N)=\begin{cases}(-1)^{|\operatorname{PF}N|}, & \text{if }N=\prod_{p\in\operatorname{PF}N}p\\ 0, & \text{otherwise}\end{cases}=(-1)^{|\operatorname{PF}N|}\qquad\left(\text{since }N=\prod_{p\in\operatorname{PF}N}p\right)$$
$$=(-1)^{|S|}\qquad(\text{since }\operatorname{PF}N=S).$$

This rewrites as $\mu\left(\prod_{p\in S}p\right)=(-1)^{|S|}$ (since $N=\prod_{p\in S}p$).

[21].

The map

$$L : \mathcal{P}(\operatorname{PF} n) \to \left\{d \in \mathbb{N}_{|n} \ \mid\ \mu(d) \neq 0\right\} \qquad \text{defined by} \qquad \left(L(S) = \prod_{p \in S} p \text{ for every } S \in \mathcal{P}(\operatorname{PF} n)\right)$$

is well-defined[22], surjective (since every element e of $\left\{d \in \mathbb{N}_{|n} \ \mid\ \mu(d) \neq 0\right\}$ satisfies $e = L(S)$ for some $S \in \mathcal{P}(\operatorname{PF} n)$, namely for $S = \operatorname{PF} e$ [23]) and injective[24]. Hence, L is a bijection. Besides, every $S \in \mathcal{P}(\operatorname{PF} n)$ satisfies $\mu(L(S)) = (-1)^{|S|}$ (since (22)

---

[21] *Proof of (24):* Let U be a finite set. Then,

$$\begin{aligned}
\sum_{S \in \mathcal{P}(U)} (-1)^{|S|} &= \sum_{k \in \mathbb{N}} \underbrace{\sum_{\substack{S \in \mathcal{P}(U);\\ |S| = k}} (-1)^k}_{= |\{S \in \mathcal{P}(U) \ \mid |S| = k\}| \cdot (-1)^k} = \sum_{k \in \mathbb{N}} \underbrace{|\{S \in \mathcal{P}(U) \ \mid |S| = k\}|}_{\substack{= \binom{|U|}{k} \\ \text{(by (23))}}} \cdot (-1)^k \\
&= \sum_{k \in \mathbb{N}} \binom{|U|}{k} (-1)^k = (1 + (-1))^{|U|} \qquad \text{(by the binomial formula)} \\
&= 0^{|U|} = \begin{cases} 1, & \text{if } |U| = 0; \\ 0, & \text{otherwise} \end{cases} = [|U| = 0].
\end{aligned}$$

This proves (24).

[22] *Proof.* Let $S \in \mathcal{P}(\operatorname{PF} n)$. Then, S is a subset of $\operatorname{PF} n$. Hence, each element p of S is a prime divisor of n. Therefore, the product $\prod_{p \in S} p$ of these elements also divides n. In other words, $\prod_{p \in S} p \in \mathbb{N}_{|n}$. Hence, the formula (22) yields $\mu\left(\prod_{p \in S} p\right) = (-1)^{|S|} \neq 0$.

Thus, $\prod_{p \in S} p \in \left\{d \in \mathbb{N}_{|n} \ \mid\ \mu(d) \neq 0\right\}$ (since $\prod_{p \in S} p \in \mathbb{N}_{|n}$).

Now, forget that we fixed S. We have thus shown that $\prod_{p \in S} p \in \left\{d \in \mathbb{N}_{|n} \ \mid\ \mu(d) \neq 0\right\}$ for each $S \in \mathcal{P}(\operatorname{PF} n)$. Hence, the map L is well-defined.

[23] *Proof.* Let $e \in \left\{d \in \mathbb{N}_{|n} \ \mid\ \mu(d) \neq 0\right\}$. We must prove that $e = L(S)$ for $S = \operatorname{PF} e$. In other words, we must prove that $e = L(\operatorname{PF} e)$.

From $e \in \left\{d \in \mathbb{N}_{|n} \ \mid\ \mu(d) \neq 0\right\}$, we obtain that $\mu(e) \neq 0$. Hence, $e = \prod_{p \in \operatorname{PF} e} p$ (because otherwise, (15) would yield $\mu(e) = \begin{cases} (-1)^{|\operatorname{PF} e|}, & \text{if } e = \prod_{p \in \operatorname{PF} e} p \\ 0, & \text{otherwise} \end{cases} = 0$, which would contradict $\mu(e) \neq 0$). On the other hand, from $e \in \left\{d \in \mathbb{N}_{|n} \ \mid\ \mu(d) \neq 0\right\}$, we obtain $e \in \mathbb{N}_{|n}$, so that $e \mid n$ and thus $\operatorname{PF} e \subseteq \operatorname{PF} n$. In other words, $\operatorname{PF} e \in \mathcal{P}(\operatorname{PF} n)$. Hence, $L(\operatorname{PF} e)$ is well-defined. The definition of $L(\operatorname{PF} e)$ shows that $L(\operatorname{PF} e) = \prod_{p \in \operatorname{PF} e} p$.

Thus, $e = \prod_{p \in \operatorname{PF} e} p = L(\operatorname{PF} e)$.

[24] since for every $S \in \mathcal{P}(\operatorname{PF} n)$, we have $S = \operatorname{PF}\left(\prod_{p \in S} p\right) = \operatorname{PF}(L(S))$, and thus S can be uniquely reconstructed from $L(S)$

yields $\mu\left(L\left(S\right)\right)=\mu\left(\prod_{p\in S}p\right)=\left(-1\right)^{\left|S\right|}$, because S is a finite set of primes). Now,

$$\sum_{d\mid n}\mu\left(d\right)=\sum_{d\in\mathbb{N}_{|n}}\mu\left(d\right)=\sum_{\substack{d\in\mathbb{N}_{|n};\\ \mu\left(d\right)\neq 0}}\mu\left(d\right)$$

$$\left(\begin{array}{c}\text{here, we have removed from the sum all addends with }\mu\left(d\right)=0,\\ \text{but these addends are all zero and thus don't change the sum}\end{array}\right)$$

$$=\sum_{S\in\mathcal{P}\left(\operatorname{PF}n\right)}\underbrace{\mu\left(L\left(S\right)\right)}_{=\left(-1\right)^{\left|S\right|}}\qquad\left(\text{since }L:\mathcal{P}\left(\operatorname{PF}n\right)\to\left\{d\in\mathbb{N}_{|n}\ \mid\ \mu\left(d\right)\neq 0\right\}\text{ is a bijection}\right)$$

$$=\sum_{S\in\mathcal{P}\left(\operatorname{PF}n\right)}\left(-1\right)^{\left|S\right|}=\left[\left|\operatorname{PF}n\right|=0\right]\qquad\left(\text{by (24), applied to }U=\operatorname{PF}n\right)$$

$$=\left[n=1\right]$$

[25]. This proves (17).

It remains to prove the remaining two identities (18) and (19). First, let us show (18):

For any $p\in\operatorname{PF}n$, let us denote by U_p the subset $\left\{m\in\left\{1,2,...,n\right\}\mid\left(p\mid m\right)\right\}$ of the set $\left\{1,2,...,n\right\}$. We have

$$\left\{m\in\left\{1,2,...,n\right\}\mid m\perp n\right\}=\left\{1,2,...,n\right\}\setminus\bigcup_{p\in\operatorname{PF}n}\left\{m\in\left\{1,2,...,n\right\}\mid\left(p\mid m\right)\right\}$$

(since an element $m\in\left\{1,2,...,n\right\}$ satisfies $m\perp n$ if and only if there is no $p\in\operatorname{PF}n$ such that $p\mid m$). In other words,

$$\left\{m\in\left\{1,2,...,n\right\}\mid m\perp n\right\}=\left\{1,2,...,n\right\}\setminus\bigcup_{p\in\operatorname{PF}n}U_p\qquad(25)$$

(since $\left\{m\in\left\{1,2,...,n\right\}\mid\left(p\mid m\right)\right\}=U_p$ for every $p\in\operatorname{PF}n$). But by the principle of inclusion and exclusion[26] (applied to the family $\left(U_p\right)_{p\in\operatorname{PF}n}$ of subsets of the set $\left\{1,2,...,n\right\}$), we have

$$\left|\left\{1,2,...,n\right\}\setminus\bigcup_{p\in\operatorname{PF}n}U_p\right|=\sum_{S\subseteq\operatorname{PF}n}\left(-1\right)^{\left|S\right|}\left|\bigcap_{p\in S}U_p\right|,$$

[25]because for an integer $n\in\mathbb{N}_+$, the assertion $\left|\operatorname{PF}n\right|=0$ is equivalent to $n=1$, since we have the following chain of equivalences:

$$\left(\left|\operatorname{PF}n\right|=0\right)\Longleftrightarrow\left(\operatorname{PF}n=\varnothing\right)\Longleftrightarrow\left(n\text{ has no prime divisors}\right)\Longleftrightarrow\left(n=1\right)$$

[26]The *principle of inclusion and exclusion* states that if X and U are finite sets, and $\left(U_x\right)_{x\in X}\in\left(\mathcal{P}\left(U\right)\right)^X$ is a family of subsets of U, then $\left|U\setminus\bigcup_{x\in X}U_x\right|=\sum_{S\subseteq X}\left(-1\right)^{\left|S\right|}\left|\bigcap_{x\in S}U_x\right|$, where $\bigcap_{x\in\varnothing}U_x$ denotes the whole set U. We are applying this principle to the sets $X=\operatorname{PF}n$ and $U=\left\{1,2,...,n\right\}$ and the family $\left(U_x\right)_{x\in X}=\left(U_p\right)_{p\in X}\in\left(\mathcal{P}\left(U\right)\right)^X$ here.

where $\bigcap_{p\in\varnothing} U_p$ denotes the whole set $\{1,2,...,n\}$. Now, the definition of ϕ yields

$$\begin{aligned}\phi(n) &= |\{m\in\{1,2,...,n\} \mid m\perp n\}| = \left|\{1,2,...,n\}\setminus \bigcup_{p\in\operatorname{PF}n} U_p\right| \qquad \text{(by (25))}\\ &= \sum_{S\subseteq \operatorname{PF}n} (-1)^{|S|}\left|\bigcap_{p\in S} U_p\right|. \qquad (26)\end{aligned}$$

But for every $S\subseteq \operatorname{PF}n$, we have

$$\begin{aligned}\bigcap_{p\in S} U_p &= \bigcap_{p\in S}\{m\in\{1,2,...,n\} \mid (p\mid m)\} = \left\{m\in\{1,2,...,n\} \mid \underbrace{(\text{every } p\in S \text{ satisfies } p\mid m)}_{\substack{\text{this assertion is equivalent to}\\ \prod_{p\in S} p\mid m,\text{ since } p \text{ is prime for every } p\in S}}\right\}\\ &= \left\{m\in\{1,2,...,n\} \mid \left(\prod_{p\in S} p\mid m\right)\right\}\end{aligned}$$

and thus

$$\left|\bigcap_{p\in S} U_p\right| = \left|\left\{m\in\{1,2,...,n\} \mid \left(\prod_{p\in S} p\mid m\right)\right\}\right| = \frac{n}{\prod_{p\in S} p}$$

[27]. Hence, (26) becomes

$$\begin{aligned}\phi(n) &= \sum_{S\subseteq\operatorname{PF}n}(-1)^{|S|}\left|\bigcap_{p\in S}U_p\right| = \underbrace{\sum_{S\subseteq\operatorname{PF}n}}_{=\sum_{S\in\mathcal{P}(\operatorname{PF}n)}}\underbrace{(-1)^{|S|}}_{=\mu(L(S))}\underbrace{\frac{n}{\prod_{p\in S}p}}_{\substack{=\frac{n}{L(S)},\\ \text{since } L(S)=\prod_{p\in S}p}} = \sum_{S\in\mathcal{P}(\operatorname{PF}n)}\mu(L(S))\frac{n}{L(S)}\\ &= \sum_{\substack{d\in\mathbb{N}_{|n};\\ \mu(d)\neq 0}}\mu(d)\frac{n}{d} \qquad \left(\begin{array}{c}\text{here, we have substituted } d \text{ for } L(S) \text{ in the sum,}\\ \text{since } L:\mathcal{P}(\operatorname{PF}n)\to\left\{d\in\mathbb{N}_{|n}\ \mid\ \mu(d)\neq 0\right\} \text{ is a bijection}\end{array}\right)\\ &= \sum_{d\in\mathbb{N}_{|n}}\mu(d)\frac{n}{d} \qquad \left(\begin{array}{c}\text{here, we have added to the sum some addends with } \mu(d)=0,\\ \text{but these addends are all zero and thus don't change the sum}\end{array}\right)\\ &= \sum_{d\mid n}\mu(d)\frac{n}{d}.\end{aligned}$$

Thus, (18) is proven.

[27] This is because $\prod_{p\in S} p$ is a divisor of n (since each $p\in S$ is a prime divisor of n, and thus their product $\prod_{p\in S} p$ is also a divisor of n), and each divisor d of n satisfies $|\{m\in\{1,2,...,n\} \mid (d\mid m)\}| = \frac{n}{d}$ (since there are exactly $\frac{n}{d}$ elements of the set $\{1,2,...,n\}$ divisible by d, namely d, $2d$, $3d$, ..., $\frac{n}{d}d$).

Now, we are going to prove the identity (19) by strong induction over n. So let $m \in \mathbb{N}$ be an integer, and assume that the identity (19) holds for every $n \in \mathbb{N}_+$ satisfying $n < m$. Then, we have to prove that (19) also holds for $n = m$.

In fact, we have

$$\sum_{d|e} d\mu(d)\phi\left(\frac{e}{d}\right) = \mu(e) \tag{27}$$

for every divisor e of m satisfying $e \neq m$ [28].

Now,

$$\sum_{e|m} \underbrace{\sum_{d|e}}_{=\sum_{\substack{d|m;\\ d|e}}} d\mu(d)\phi\left(\frac{e}{d}\right) = \underbrace{\sum_{e|m}\sum_{\substack{d|m;\\ d|e}}}_{=\sum_{d|m}\sum_{\substack{e|m;\\ d|e}}} d\mu(d)\phi\left(\frac{e}{d}\right) = \sum_{d|m} d\mu(d)\sum_{\substack{e|m;\\ d|e}} \phi\left(\frac{e}{d}\right).$$

Since every divisor d of m satisfies

$$\sum_{\substack{e|m;\\ d|e}} \phi\left(\frac{e}{d}\right) = \sum_{\substack{e\in\mathbb{N}_{|m};\\ d|e}} \phi\left(\frac{e}{d}\right) = \sum_{f\in\mathbb{N}_{|(m/d)}} \phi(f)$$

$$\left(\begin{array}{c}\text{here, we substituted } f \text{ for } \dfrac{e}{d} \text{ in the sum, since the map}\\ \left\{e\in\mathbb{N}_{|m} \mid (d \mid e)\right\} \to \mathbb{N}_{|(m/d)},\ e\mapsto \dfrac{e}{d} \text{ is a bijection}\\ \text{(because } d \mid m\text{)}\end{array}\right)$$

$$= \sum_{f|(m/d)} \phi(f) = m/d \qquad \left(\text{by (16), with } n \text{ and } d \text{ replaced by } m/d \text{ and } f\right),$$

this becomes

$$\begin{aligned}
&\sum_{e|m}\sum_{d|e} d\mu(d)\phi\left(\frac{e}{d}\right)\\
&= \sum_{d|m} d\mu(d)\underbrace{\sum_{\substack{e|m;\\ d|e}} \phi\left(\frac{e}{d}\right)}_{=m/d} = \sum_{d|m} \underbrace{d\cdot(m/d)}_{=m}\mu(d) = m \underbrace{\sum_{d|m}\mu(d)}_{\substack{=[m=1]\\ \text{(by (17) (applied to } m \text{ instead of } n))}}\\
&= m[m=1] = m\begin{cases}1, & \text{if } m=1;\\ 0, & \text{if } m\neq 1\end{cases} = \begin{cases}m, & \text{if } m=1;\\ 0, & \text{if } m\neq 1\end{cases} = \begin{cases}1, & \text{if } m=1;\\ 0, & \text{if } m\neq 1\end{cases} = [m=1]\\
&= \sum_{d|m}\mu(d) \qquad \text{(by (17) (applied to } m \text{ instead of } n))\\
&= \sum_{\substack{d|m;\\ d\neq m}}\mu(d) + \underbrace{\sum_{\substack{d|m;\\ d=m}}\mu(d)}_{=\mu(m)} = \sum_{\substack{d|m;\\ d\neq m}}\mu(d) + \mu(m).
\end{aligned}$$

[28] *Proof of (27):* Let e be a divisor of m satisfying $e \neq m$. Thus, $e < m$. Also, clearly, $e \in \mathbb{N}_+$.

But we have assumed that the identity (19) holds for every $n \in \mathbb{N}_+$ satisfying $n < m$. Applying this to $n = e$, we conclude that (19) holds for $n = e$ (sinc $e \in \mathbb{N}_+$ and $e < m$). In other words, we have $\sum_{d|e} d\mu(d)\phi\left(\frac{e}{d}\right) = \mu(e)$. This proves (27).

Thus,

$$\sum_{\substack{d|m;\\ d\neq m}} \mu(d) + \mu(m) = \sum_{e|m} \sum_{d|e} d\mu(d)\,\phi\left(\frac{e}{d}\right)$$

$$= \underbrace{\sum_{\substack{e|m;\\ e\neq m}} \sum_{d|e} d\mu(d)\,\phi\left(\frac{e}{d}\right)}_{\substack{=\mu(e)\\ \text{(by (27))}}} + \underbrace{\sum_{\substack{e|m;\\ e=m}} \sum_{d|e} d\mu(d)\,\phi\left(\frac{e}{d}\right)}_{=\sum_{d|m} d\mu(d)\phi\left(\frac{m}{d}\right)}$$

$$= \sum_{\substack{e|m;\\ e\neq m}} \mu(e) + \sum_{d|m} d\mu(d)\,\phi\left(\frac{m}{d}\right) = \sum_{\substack{d|m;\\ d\neq m}} \mu(d) + \sum_{d|m} d\mu(d)\,\phi\left(\frac{m}{d}\right)$$

(here, we substituted d for e in the first sum). Therefore,

$$\mu(m) = \sum_{d|m} d\mu(d)\,\phi\left(\frac{m}{d}\right).$$

In other words, (19) holds for $n = m$. This completes our induction, and thus (19) is proven.

Hence, the proof of Theorem 6 is now complete.

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

$$\left(b_n = \sum_{d|n} d\varphi_{n/d}(y_d) \text{ for every } n \in N\right). \tag{28}$$

We want to prove that Assertion $\mathcal{C}$ holds, i. e., that every $n \in N$ and every $p \in \operatorname{PF} n$ satisfies (13). 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 [29]). Thus, applying (28) to n/p instead of n yields $b_{n/p} = \sum_{d|(n/p)} d\varphi_{(n/p)/d}(y_d)$. Now, (28) yields

$$b_n = \sum_{d|n} d\varphi_{n/d}(y_d) = \sum_{\substack{d|n;\\ d|(n/p)}} d\varphi_{n/d}(y_d) + \sum_{\substack{d|n;\\ d\nmid(n/p)}} d\varphi_{n/d}(y_d). \tag{29}$$

But for any divisor d of n, the assertions $d \nmid (n/p)$ and $p^{v_p(n)} \mid d$ are equivalent[30]. Thus,

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

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

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

Thus, (29) becomes

$$\begin{aligned} b_n &= \sum_{\substack{d\mid n;\\ d\mid (n/p)}} d\varphi_{n/d}(y_d) + \underbrace{\sum_{\substack{d\mid n;\\ d\nmid (n/p)}} d\varphi_{n/d}(y_d)}_{\equiv 0 \bmod p^{v_p(n)}A} \equiv \sum_{\substack{d\mid n;\\ d\mid (n/p)}} d\varphi_{n/d}(y_d) + 0 = \sum_{\substack{d\mid n;\\ d\mid (n/p)}} d\varphi_{n/d}(y_d) \\ &= \sum_{d\mid (n/p)} d\varphi_{n/d}(y_d) \bmod p^{v_p(n)}A. \qquad (30) \end{aligned}$$

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

$$\begin{aligned} \varphi_p(b_{n/p}) &= \varphi_p\left(\sum_{d\mid (n/p)} d\varphi_{(n/p)/d}(y_d)\right) \\ &= \sum_{d\mid (n/p)} d\underbrace{\varphi_p\left(\varphi_{(n/p)/d}(y_d)\right)}_{=\left(\varphi_p\circ\varphi_{(n/p)/d}\right)(y_d)} \qquad \text{(since } \varphi_p \text{ is a group endomorphism)} \\ &= \sum_{d\mid (n/p)} d \underbrace{\left(\varphi_p\circ\varphi_{(n/p)/d}\right)}_{=\varphi_{p\cdot(n/p)/d} \text{ (due to (12))}} (y_d) \\ &= \sum_{d\mid (n/p)} d\underbrace{\varphi_{p\cdot(n/p)/d}}_{=\varphi_{n/d}}(y_d) = \sum_{d\mid (n/p)} d\varphi_{n/d}(y_d) \equiv b_n \bmod p^{v_p(n)}A \end{aligned}$$

(by (30)). In other words, (13) 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 (13).

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

$$b_m = \sum_{d\mid m} d\varphi_{m/d}(y_d) \qquad (31)$$

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 (31) holds for every $m \in N \cap \{1,2,...,n-1\}$. Now, we must construct an element $y_n \in A$ such that (31) 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 [31] and in $\{1,2,...,n-1\}$ [32], 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 [33]). Besides, $n/p \in \{1,2,...,n-1\}$.

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

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

[33] 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 (31) holds for every $m \in N \cap \{1, 2, ..., n-1\}$, we can thus conclude that (31) holds for $m = n/p$. In other words, $b_{n/p} = \sum\limits_{d|(m/p)} d\varphi_{(m/p)/d}(y_d)$. From this equation, we can conclude (by the same reasoning as in the proof of the implication $\mathcal{E} \Longrightarrow \mathcal{C}$) that

$$\varphi_p(b_{n/p}) = \sum_{d|(n/p)} d\varphi_{n/d}(y_d).$$

Comparing this with (13), we obtain

$$\sum_{d|(n/p)} d\varphi_{n/d}(y_d) \equiv b_n \operatorname{mod} p^{v_p(n)} A. \tag{32}$$

Now, for any divisor d of n, the assertions $d \nmid (n/p)$ and $p^{v_p(n)} \mid d$ are equivalent[34]. Thus,

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

Hence,

$$\begin{aligned}
&\sum_{\substack{d|n;\\ d\neq n}} d\varphi_{n/d}(y_d)\\
&= \underbrace{\sum_{\substack{d|n;\\ d\nmid(n/p);\\ d\neq n}} d\varphi_{n/d}(y_d)}_{\equiv 0 \operatorname{mod} p^{v_p(n)} A} + \sum_{\substack{d|n;\\ d|(n/p);\\ d\neq n}} d\varphi_{n/d}(y_d) \equiv \sum_{\substack{d|n;\\ d|(n/p);\\ d\neq n}} d\varphi_{n/d}(y_d) = \sum_{\substack{d|n;\\ d|(n/p)}} d\varphi_{n/d}(y_d)\\
&\qquad \left(\begin{array}{c}\text{since for any divisor } d \text{ of } n \text{, the assertions } (d \mid (n/p) \text{ and } d \neq n) \text{ and } d \mid (n/p)\\ \text{are equivalent, because if } (d \mid (n/p)) \text{, then } d \neq n \text{ (since } n \nmid (n/p)\text{)}\end{array}\right)\\
&= \sum_{d|(n/p)} d\varphi_{n/d}(y_d) \equiv b_n \operatorname{mod} p^{v_p(n)} A \qquad \text{(by (32))}.
\end{aligned}$$

In other words,

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

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

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

Hence, there exists an element y_n of A that satisfies $b_n - \sum\limits_{\substack{d|n;\\ d\neq n}} d\varphi_{n/d}(y_d) = ny_n$. Fix

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

such a y_n. We now claim that this element y_n satisfies (31) for $m = n$. In fact,

$$\sum_{d\mid n} d\varphi_{n/d}(y_d) = \sum_{\substack{d\mid n;\\ d\neq n}} d\varphi_{n/d}(y_d) + \underbrace{\sum_{\substack{d\mid n;\\ d=n}} d\varphi_{n/d}(y_d)}_{\substack{=n\varphi_{n/n}(y_n)=n\varphi_1(y_n)=ny_n,\\ \text{due to (11)}}} = \sum_{\substack{d\mid n;\\ d\neq n}} d\varphi_{n/d}(y_d) + ny_n = b_n$$

(since $b_n - \sum_{\substack{d\mid n;\\ d\neq n}} d\varphi_{n/d}(y_d) = ny_n$). Hence, (31) 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 (31) for every $m \in N$. Therefore, this family satisfies $b_n = \sum_{d\mid n} d\varphi_{n/d}(y_d)$ for every $n \in N$ (by (31), applied to $m = n$). So we have proven that there exists a family $(y_n)_{n\in N} \in A^N$ which satisfies $b_n = \sum_{d\mid n} d\varphi_{n/d}(y_d)$ 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 (28) holds. Then, every $n \in N$

satisfies

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

$$=\sum_{e\mid n}\mu(e)\underbrace{\varphi_e\left(\sum_{d\mid(n/e)}d\varphi_{(n/e)/d}(y_d)\right)}_{\substack{=\sum_{d\mid(n/e)}d\varphi_e\left(\varphi_{(n/e)/d}(y_d)\right)\\ \text{(since } \varphi_e \text{ is a group endomorphism)}}} \qquad \left(\begin{array}{c}\text{since } b_{n/e}=\sum_{d\mid(n/e)}d\varphi_{(n/e)/d}(y_d)\\ \text{by (28) (applied to } n/e \text{ instead of } n)\end{array}\right)$$

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

$$=\underbrace{\sum_{e\mid n}\sum_{\substack{d\mid n;\\ d\mid(n/e)}}}_{=\sum_{d\mid n}\sum_{e\mid n;\ d\mid(n/e)}}\mu(e)d\left(\underbrace{\varphi_e\circ\varphi_{(n/e)/d}}_{\substack{=\varphi_{e\cdot(n/e)/d}\\ \text{(by (12))}}}\right)(y_d)=\sum_{d\mid n}\sum_{\substack{e\mid n;\\ d\mid(n/e)}}\mu(e)d\underbrace{\varphi_{e\cdot(n/e)/d}}_{=\varphi_{n/d}}(y_d)$$

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

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

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

$$\left(\text{since (17) (with } n \text{ and } d \text{ replaced by } n/d \text{ and } e) \text{ yields } \sum_{e\mid(n/d)}\mu(e)=[n/d=1]=[n=d]\right)$$

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

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

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

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

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

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

$$n y_n = \sum_{d \mid n} \mu(d) \varphi_d \left(b_{n/d}\right). \tag{33}$$

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

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

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

$$\left(\text{since } e y_e = \sum_{d \mid e} \mu(d) \varphi_d \left(b_{e/d}\right) \text{ by (33) (applied to } e \text{ instead of } n\text{)}\right)$$

$$= \sum_{e \mid n} \underbrace{\sum_{d \mid e}}_{=\sum_{\substack{d \mid n; \\ d \mid e}}} \mu(d) \underbrace{\varphi_{n/e}\left(\varphi_d\left(b_{e/d}\right)\right)}_{=\left(\varphi_{n/e} \circ \varphi_d\right)\left(b_{e/d}\right)} = \underbrace{\sum_{e \mid n} \sum_{\substack{d \mid n; \\ d \mid e}}}_{=\sum_{d \mid n} \sum_{\substack{e \mid n; \\ d \mid e}}} \mu(d) \left(\underbrace{\varphi_{n/e} \circ \varphi_d}_{\substack{=\varphi_{(n/e) \cdot d} \\ \text{(by (12))}}}\right)\left(b_{e/d}\right) = \sum_{d \mid n} \sum_{\substack{e \mid n; \\ d \mid e}} \mu(d) \varphi_{(n/e) \cdot d}\left(b_{e/d}\right)$$

$$= \sum_{d \mid n} \mu(d) \sum_{\substack{e \mid n; \\ d \mid e}} \varphi_{(n/e) \cdot d}\left(b_{e/d}\right). \tag{34}$$

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, (34) becomes

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

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

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

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

$$\left(\text{since (17) (applied to } n/h \text{ instead of } n\text{) yields } \sum_{d\mid(n/h)}\mu(d) = [n/h=1] = [n=h]\right)$$

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

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

$$= \underbrace{\sum_{\substack{h\mid n;\\ h\neq n}}0\varphi_{n/h}(b_h)}_{=0} + \underbrace{[n=n]}_{=1}\underbrace{\varphi_{n/n}}_{\substack{=\varphi_1=\mathrm{id}\\ (\text{by } (11))}}(b_n) = 0 + 1\,\mathrm{id}(b_n) = \mathrm{id}(b_n) = b_n.$$

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

$$\sum_{d\mid n}\phi(d)\varphi_d(b_{n/d}) = \sum_{d\mid n}\sum_{e\mid(n/d)}\phi(e)\,d\varphi_{n/d}(y_d)$$

(this equation is proven in exactly the same way as we have shown the equation $\sum_{d\mid n}\mu(d)\varphi_d(b_{n/d}) = \sum_{d\mid n}\sum_{e\mid(n/d)}\mu(e)\,d\varphi_{n/d}(y_d)$ 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 (16), with n and d replaced by n/d and e), this becomes

$$\sum_{d\mid n} \phi(d)\, \varphi_d(b_{n/d}) = \sum_{d\mid n} \underbrace{\sum_{e\mid(n/d)} \phi(e)}_{=n/d} d\varphi_{n/d}(y_d) = \sum_{d\mid n} \underbrace{(n/d)\, d}_{=n} \varphi_{n/d}(y_d) = n \sum_{d\mid n} \varphi_{n/d}(y_d) \in nA.$$

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

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

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

$$nz_n = \sum_{d\mid n} \phi(d)\, \varphi_d(b_{n/d}). \tag{35}$$

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

$$y_n = \sum_{h\mid n} \mu(h)\, \varphi_h(z_{n/h}).$$

Thus,

$$\begin{aligned}
ny_n &= n\sum_{h\mid n}\mu\left(h\right)\varphi_h\left(z_{n/h}\right) = \sum_{h\mid n}\underbrace{n}_{=h\cdot n/h}\mu\left(h\right)\varphi_h\left(z_{n/h}\right)\\
&= \sum_{h\mid n}h\mu\left(h\right)\underbrace{\left(n/h\right)\varphi_h\left(z_{n/h}\right)}_{\substack{=\varphi_h\left(\left(n/h\right)z_{n/h}\right)\\ \text{(since}\\ n/h\in\mathbb{Z}\text{ and since }\varphi_h\text{ is}\\ \text{a group endomorphism)}}} = \sum_{h\mid n}h\mu\left(h\right)\varphi_h\left(\left(n/h\right)z_{n/h}\right)\\
&= \sum_{h\mid n}h\mu\left(h\right)\underbrace{\varphi_h\left(\sum_{d\mid\left(n/h\right)}\phi\left(d\right)\varphi_d\left(b_{\left(n/h\right)/d}\right)\right)}_{\substack{=\sum_{d\mid\left(n/h\right)}\phi(d)\varphi_h\left(\varphi_d\left(b_{\left(n/h\right)/d}\right)\right)\\ \text{(since }\varphi_h\text{ is a group endomorphism)}}}\\
&\qquad\left(\begin{array}{c}\text{since the equation (35), applied to }n/h\text{ instead of }n,\\ \text{yields }\left(n/h\right)z_{n/h}=\sum_{d\mid\left(n/h\right)}\phi\left(d\right)\varphi_d\left(b_{\left(n/h\right)/d}\right)\end{array}\right)\\
&= \sum_{h\mid n}h\mu\left(h\right)\sum_{d\mid\left(n/h\right)}\phi\left(d\right)\underbrace{\varphi_h\left(\varphi_d\left(b_{\left(n/h\right)/d}\right)\right)}_{=\left(\varphi_h\circ\varphi_d\right)\left(b_{\left(n/h\right)/d}\right)}\\
&= \sum_{h\mid n}h\mu\left(h\right)\underbrace{\sum_{d\mid\left(n/h\right)}}_{=\sum_{d\in\mathbb{N}_{\mid\left(n/h\right)}}}\phi\left(\underbrace{d}_{=\frac{hd}{h}}\right)\left(\underbrace{\varphi_h\circ\varphi_d}_{\substack{=\varphi_{hd}\\ \text{(by (12))}}}\right)\left(\underbrace{b_{\left(n/h\right)/d}}_{=b_{n/\left(hd\right)}}\right)\\
&= \sum_{h\mid n}h\mu\left(h\right)\sum_{d\in\mathbb{N}_{\mid\left(n/h\right)}}\phi\left(\frac{hd}{h}\right)\varphi_{hd}\left(b_{n/\left(hd\right)}\right).
\end{aligned}$$

Since every divisor h of n satisfies

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

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

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

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

$$\begin{aligned}
ny_n &= \sum_{h \mid n} h\mu\left(h\right) \underbrace{\sum_{d \in \mathbb{N}_{\mid (n/h)}} \phi\left(\frac{hd}{h}\right) \varphi_{hd}\left(b_{n/(hd)}\right)}_{= \sum_{\substack{e \in \mathbb{N}_{\mid n}; \\ h \mid e}} \phi\left(\frac{e}{h}\right) \varphi_e\left(b_{n/e}\right)} = \sum_{h \mid n} h\mu\left(h\right) \underbrace{\sum_{\substack{e \in \mathbb{N}_{\mid n}; \\ h \mid e}}}_{= \sum_{\substack{e \mid n; \\ h \mid e}}} \phi\left(\frac{e}{h}\right) \varphi_e\left(b_{n/e}\right) \\
&= \underbrace{\sum_{h \mid n} \sum_{\substack{e \mid n; \\ h \mid e}}}_{= \sum_{e \mid n} \sum_{\substack{h \mid n; \\ h \mid e}}} h\mu\left(h\right) \phi\left(\frac{e}{h}\right) \varphi_e\left(b_{n/e}\right) = \sum_{e \mid n} \underbrace{\sum_{\substack{h \mid n; \\ h \mid e}}}_{= \sum_{h \mid e}} h\mu\left(h\right) \phi\left(\frac{e}{h}\right) \varphi_e\left(b_{n/e}\right) \\
&= \sum_{e \mid n} \underbrace{\sum_{h \mid e} h\mu\left(h\right) \phi\left(\frac{e}{h}\right)}_{\substack{= \mu(e) \text{ (by (19), with} \\ d \text{ and } n \text{ replaced by } h \text{ and } e)}} \varphi_e\left(b_{n/e}\right) = \sum_{e \mid n} \mu\left(e\right) \varphi_e\left(b_{n/e}\right) \\
&= \sum_{d \mid n} \mu\left(d\right) \varphi_d\left(b_{n/d}\right) \qquad \text{(here we substituted } d \text{ for } e \text{ in the sum)}.
\end{aligned}$$

In other words, we have proven (33). 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

$$\sum_{d\mid n} \phi(d)\, \varphi_d\left(b_{n/d}\right) = \sum_{d\in\mathbb{N}_{|n}} \phi(d)\, \varphi_d\left(b_{n/d}\right) = \sum_{d\in\mathbb{N}_{|n}} \phi(n/d)\, \varphi_{n/d}\left(\underbrace{b_{n/(n/d)}}_{=b_d}\right)$$

$$\left(\begin{array}{c}\text{here we substituted } \dfrac{n}{d} \text{ for } d \text{ in the sum, since the map} \\ \mathbb{N}_{|n} \to \mathbb{N}_{|n},\ d \mapsto \dfrac{n}{d} \text{ is a bijection}\end{array}\right)$$

$$= \sum_{d\in\mathbb{N}_{|n}} \phi\left(\frac{n}{d}\right) \varphi_{n/d}\left(b_d\right) = \sum_{d\mid n} \phi\left(\frac{n}{d}\right) \varphi_{n/d}\left(b_d\right)$$

$$= \sum_{d\mid n} \underbrace{\left|\left\{m \in \{1,2,...,n\} \mid \gcd(m,n) = d\right\}\right| \varphi_{n/d}\left(b_d\right)}_{=\sum\limits_{\substack{m\in\{1,2,...,n\};\\ \gcd(m,n)=d}} \varphi_{n/d}(b_d)} \qquad \text{(because of (21))}$$

$$= \sum_{d\mid n} \sum_{\substack{m\in\{1,2,...,n\};\\ \gcd(m,n)=d}} \underbrace{\varphi_{n/d}\left(b_d\right)}_{\substack{=\varphi_{n/\gcd(m,n)}\left(b_{\gcd(m,n)}\right)\\ \text{(since } d=\gcd(m,n))}} = \sum_{d\mid n} \sum_{\substack{m\in\{1,2,...,n\};\\ \gcd(m,n)=d}} \varphi_{n/\gcd(m,n)}\left(b_{\gcd(m,n)}\right)$$

$$= \sum_{\substack{m\in\{1,2,...,n\};\\ \gcd(m,n)\mid n}} \varphi_{n/\gcd(m,n)}\left(b_{\gcd(m,n)}\right) = \sum_{m\in\{1,2,...,n\}} \varphi_{n/\gcd(m,n)}\left(b_{\gcd(m,n)}\right)$$

$$\left(\text{since every } m \in \{1,2,...,n\} \text{ satisfies } \gcd(m,n) \mid n\right)$$

$$= \sum_{m=1}^{n} \varphi_{n/\gcd(m,n)}\left(b_{\gcd(m,n)}\right) = \sum_{i=1}^{n} \varphi_{n/\gcd(i,n)}\left(b_{\gcd(i,n)}\right) \qquad (\text{here we substituted } i \text{ for } m \text{ in the sum}).$$

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

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

Now, here comes the extension of Theorem 5:

> **Theorem 7.** Let N be a nest. Let A be a torsionfree Abelian group (written additively). For every $n \in N$, let $\varphi_n : A \to A$ be an endomorphism of the group A such that (11) and (12) 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

$$\left(b_n = \sum_{d\mid n} d\varphi_{n/d}\left(y_d\right) \text{ for every } n \in N \right). \tag{36}$$

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 (36).

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

$$\left(b_n = \sum_{d\mid n} d\varphi_{n/d}\left(y_d\right) \text{ for every } n \in N \right) \qquad \text{and} \tag{37}$$

$$\left(b_n = \sum_{d\mid n} d\varphi_{n/d}\left(y'_d\right) \text{ for every } n \in N \right), \tag{38}$$

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 $\sum\limits_{\substack{d\mid n;\\ d\neq n}} d\varphi_{n/d}\left(y_d\right) = \sum\limits_{\substack{d\mid n;\\ d\neq n}} d\varphi_{n/d}\left(y'_d\right)$ (because $y_d = y'_d$ holds for every divisor d of n satisfying $d \neq n$ [35]). But (37) yields

$$b_n = \sum_{d\mid n} d\varphi_{n/d}\left(y_d\right) = \sum_{\substack{d\mid n;\\ d\neq n}} d\varphi_{n/d}\left(y_d\right) + \underbrace{\sum_{\substack{d\mid n;\\ d=n}} d\varphi_{n/d}\left(y_d\right)}_{\substack{=n\varphi_{n/n}(y_n)\\ =n\varphi_1(y_n)=ny_n\\ \text{(due to (11))}}} = \sum_{\substack{d\mid n;\\ d\neq n}} d\varphi_{n/d}\left(y_d\right) + ny_n$$

and similarly (38) leads to

$$b_n = \sum_{\substack{d\mid n;\\ d\neq n}} d\varphi_{n/d}\left(y'_d\right) + ny'_n.$$

[35] *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 $d < n$).

Thus, $\sum\limits_{\substack{d|n;\\ d\neq n}} d\varphi_{n/d}(y_d) + ny_n = b_n = \sum\limits_{\substack{d|n;\\ d\neq n}} d\varphi_{n/d}(y'_d) + ny'_n$. Subtracting the equality $\sum\limits_{\substack{d|n;\\ d\neq n}} d\varphi_{n/d}(y_d) = \sum\limits_{\substack{d|n;\\ d\neq n}} d\varphi_{n/d}(y'_d)$ from this equality, we obtain $ny_n = ny'_n$, so that $n(y_n - y'_n) = \underbrace{ny_n}_{=ny'_n} - ny'_n = 0$ 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 (36). 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 (36). In other words, Assertion $\mathcal{E}'$ holds. Hence, we have proven the implication $\mathcal{E} \Longrightarrow \mathcal{E}'$. Together with $\mathcal{E}' \Longrightarrow \mathcal{E}$, this yields $\mathcal{E} \Longleftrightarrow \mathcal{E}'$. Combining this with $\mathcal{C} \Longleftrightarrow \mathcal{E} \Longleftrightarrow \mathcal{F} \Longleftrightarrow \mathcal{G} \Longleftrightarrow \mathcal{H}$, we see that all six assertions $\mathcal{C}$, $\mathcal{E}$, $\mathcal{E}'$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ are equivalent. This proves Theorem 7.

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

Theorem 9. Let N be a nest. Let A be a torsionfree commutative ring with unity. For every $p \in \mathbb{P} \cap N$, let $\varphi_p : A \to A$ be an endomorphism of the ring A such that (3) 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

$$\left(b_n = w_n\left((x_k)_{k\in N}\right) \text{ for every } n \in N\right). \tag{39}$$

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

Lemma 10. Let N be a nest. Let A be a torsionfree commutative ring with unity. Let $(b_n)_{n\in N} \in A^N$ be a family of elements of A. Then, there exists *at most one* family $(x_n)_{n\in N} \in A^N$ of elements of A satisfying (39).

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

$$\left(b_n = w_n\left((x_k)_{k\in N}\right) \text{ for every } n \in N\right) \qquad \text{and} \tag{40}$$

$$\left(b_n = w_n\left((x'_k)_{k\in N}\right) \text{ for every } n \in N\right), \tag{41}$$

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 $\sum\limits_{\substack{d|n;\\ d\neq n}} dx_d^{n/d} = \sum\limits_{\substack{d|n;\\ d\neq n}} d\left(x'_d\right)^{n/d}$ (because $x_d = x'_d$ holds for every divisor d of n satisfying $d \neq n$ [36]). But (40) yields

$$b_n = w_n\left((x_k)_{k\in N}\right) = \sum_{d|n} dx_d^{n/d} = \sum_{\substack{d|n;\\ d\neq n}} dx_d^{n/d} + \underbrace{\sum_{\substack{d|n;\\ d=n}} dx_d^{n/d}}_{\substack{=nx_n^{n/n}\\ =nx_n^1=nx_n}} = \sum_{\substack{d|n;\\ d\neq n}} dx_d^{n/d} + nx_n$$

and similarly (41) leads to

$$b_n = \sum_{\substack{d|n;\\ d\neq n}} d\left(x'_d\right)^{n/d} + nx'_n.$$

Thus, $\sum\limits_{\substack{d|n;\\ d\neq n}} dx_d^{n/d} + nx_n = d_n = \sum\limits_{\substack{d|n;\\ d\neq n}} d\left(x'_d\right)^{n/d} + nx'_n$. Subtracting the equality $\sum\limits_{\substack{d|n;\\ d\neq n}} dx_d^{n/d} = \sum\limits_{\substack{d|n;\\ d\neq n}} d\left(x'_d\right)^{n/d}$ from this equality, we obtain $nx_n = nx'_n$, so that $n\left(x_n - x'_n\right) = \underbrace{nx_n}_{=nx'_n} - nx'_n = 0$ 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 (39). 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 (39). In other words, Assertion $\mathcal{D}'$ holds. Hence, we have proven the implication $\mathcal{D} \Longrightarrow \mathcal{D}'$. Together with $\mathcal{D}' \Longrightarrow \mathcal{D}$, this yields $\mathcal{D} \Longleftrightarrow \mathcal{D}'$. Combining this with $\mathcal{C} \Longleftrightarrow \mathcal{D}$, we see that all three assertions $\mathcal{C}$, $\mathcal{D}$ and $\mathcal{D}'$ are equivalent. This proves Theorem 9.

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

> **Theorem 11.** Let N be a nest. Let A be a commutative ring with unity. For every $n \in N$, let $\varphi_n : A \to A$ be an endomorphism of the ring A such that the conditions (3), (11) and (12) are satisfied.

[36] *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 $d < n$).

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[37], and thus Theorem 11 is proven.

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

Theorem 12. Let N be a nest. Let A be a torsionfree commutative ring with unity. For every $n \in N$, let $\varphi_n : A \to A$ be an endomorphism of the ring A such that the conditions (3), (11) and (12) 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[38], 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 $\mathbb{Z}$:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Before we prove this result, we need a lemma:

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

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

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

For every $n \in N$, define a map $\varphi_n : \mathbb{Z}[\Xi] \to \mathbb{Z}[\Xi]$ by $\varphi_n(P) = P(\Xi^n)$ for every polynomial $P \in \mathbb{Z}[\Xi]$. It is clear that φ_n is an endomorphism of the ring $\mathbb{Z}[\Xi]$ [39]. The

[39] 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

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

condition (3) is satisfied, since $\varphi_p(a) = a(\Xi^p) \equiv a^p \mod p\mathbb{Z}[\Xi]$ (by Lemma 14) holds for every $a \in A$. The condition (11) is satisfied as well (since $\varphi_1(P) = P(\Xi^1) = P(\Xi) = P$ for every $P \in \mathbb{Z}[\Xi]$), and the condition (12) is also satisfied (since $\varphi_n \circ \varphi_m = \varphi_{nm}$ for every $n \in N$ and every $m \in N$ satisfying $nm \in N$ [40]). Hence, the three conditions (3), (11) and (12) 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 $\mathcal{C} \Longleftrightarrow \mathcal{C}_\Xi$ (since $A = \mathbb{Z}[\Xi]$ and $\varphi_p(b_{n/p}) = b_{n/p}(\Xi^p)$);
- we have $\mathcal{D} \Longleftrightarrow \mathcal{D}_\Xi$ (since $A = \mathbb{Z}[\Xi]$);
- we have $\mathcal{D}' \Longleftrightarrow \mathcal{D}'_\Xi$ (since $A = \mathbb{Z}[\Xi]$);
- we have $\mathcal{E} \Longleftrightarrow \mathcal{E}_\Xi$ (since $A = \mathbb{Z}[\Xi]$ and $\varphi_{n/d}(y_d) = y_d\left(\Xi^{n/d}\right)$);
- we have $\mathcal{E}' \Longleftrightarrow \mathcal{E}'_\Xi$ (since $A = \mathbb{Z}[\Xi]$ and $\varphi_{n/d}(y_d) = y_d\left(\Xi^{n/d}\right)$);
- we have $\mathcal{F} \Longleftrightarrow \mathcal{F}_\Xi$ (since $A = \mathbb{Z}[\Xi]$ and $\varphi_d(b_{n/d}) = b_{n/d}\left(\Xi^d\right)$);
- we have $\mathcal{G} \Longleftrightarrow \mathcal{G}_\Xi$ (since $A = \mathbb{Z}[\Xi]$ and $\varphi_d(b_{n/d}) = b_{n/d}\left(\Xi^d\right)$);
- we have $\mathcal{H} \Longleftrightarrow \mathcal{H}_\Xi$ (since $A = \mathbb{Z}[\Xi]$ and $\varphi_{n/\gcd(i,n)}\left(b_{\gcd(i,n)}\right) = b_{\gcd(i,n)}\left(\Xi^{n/\gcd(i,n)}\right)$).

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:

[40] *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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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 $n \in \mathbb{N}$ [41]. 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 $\mathcal{C}_\Xi \Longleftrightarrow \mathcal{C}_\varnothing$ (since $\mathbb{Z}[\Xi] = \mathbb{Z}$ and $b_{n/p}(\Xi^p) = b_{n/p}$);
- we have $\mathcal{D}_\Xi \Longleftrightarrow \mathcal{D}_\varnothing$ (since $\mathbb{Z}[\Xi] = \mathbb{Z}$);
- we have $\mathcal{D}'_\Xi \Longleftrightarrow \mathcal{D}'_\varnothing$ (since $\mathbb{Z}[\Xi] = \mathbb{Z}$);
- we have $\mathcal{E}_\Xi \Longleftrightarrow \mathcal{E}_\varnothing$ (since $\mathbb{Z}[\Xi] = \mathbb{Z}$ and $y_d\left(\Xi^{n/d}\right) = y_d$);
- we have $\mathcal{E}'_\Xi \Longleftrightarrow \mathcal{E}'_\varnothing$ (since $\mathbb{Z}[\Xi] = \mathbb{Z}$ and $y_d\left(\Xi^{n/d}\right) = y_d$);
- we have $\mathcal{F}_\Xi \Longleftrightarrow \mathcal{F}_\varnothing$ (since $\mathbb{Z}[\Xi] = \mathbb{Z}$ and $b_{n/d}\left(\Xi^d\right) = b_{n/d}$);
- we have $\mathcal{G}_\Xi \Longleftrightarrow \mathcal{G}_\varnothing$ (since $\mathbb{Z}[\Xi] = \mathbb{Z}$ and $b_{n/d}\left(\Xi^d\right) = b_{n/d}$);
- we have $\mathcal{H}_\Xi \Longleftrightarrow \mathcal{H}_\varnothing$ (since $\mathbb{Z}[\Xi] = \mathbb{Z}$ and $b_{\gcd(i,n)}\left(\Xi^{n/\gcd(i,n)}\right) = b_{\gcd(i,n)}$).

Hence, the equivalence of the assertions $\mathcal{C}_\Xi$, $\mathcal{D}_\Xi$, $\mathcal{D}'_\Xi$, $\mathcal{E}_\Xi$, $\mathcal{E}'_\Xi$, $\mathcal{F}_\Xi$, $\mathcal{G}_\Xi$ 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 $q \in \mathbb{Z}$ 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
$$\left(q^n = w_n\left((x_k)_{k\in\mathbb{N}_+}\right) \text{ for every } n \in \mathbb{N}_+\right).$$

(b) There exists *one and only one* family $(y_n)_{n\in\mathbb{N}_+} \in \mathbb{Z}^{\mathbb{N}_+}$ of integers such that
$$\left(q^n = \sum_{d\mid n} dy_d \text{ for every } n \in \mathbb{N}_+\right).$$

(c) Every $n \in \mathbb{N}_+$ satisfies
$$\sum_{d\mid n} \mu(d)\, q^{n/d} \in n\mathbb{Z}.$$

(d) Every $n \in \mathbb{N}_+$ satisfies
$$\sum_{d\mid n} \phi(d)\, q^{n/d} \in n\mathbb{Z}.$$

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

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

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

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

$$q^{n/p} \equiv q^n \operatorname{mod} p^{v_p(n)}\mathbb{Z}. \tag{42}$$

[42].

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

$$\begin{aligned} b_{n/p} &= q^{n/p} \equiv q^n && \text{(by (42))} \\ &= b_n \operatorname{mod} p^{v_p(n)}\mathbb{Z} \end{aligned}$$

), 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 $(b_n)_{n\in N} \in \mathbb{Z}^N$,

- 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.

The different parts of Theorem 16 - particularly, parts **(b)**, **(c)**, **(d)** and **(e)** (of course, **(e)** is just a simple restatement of **(d)**) appear fairly often in literature about number theory and combinatorics. For instance, Theorem 16 **(d)** appears as (4.64) in the book [4], which gives a number-theoretical proof for every $q \in \mathbb{Z}$ and a combinatorial proof for the case $q \geq 0$. The latter proof shows that, if $q \geq 0$, then $\frac{1}{n}\sum_{d\mid n} \phi(d)\, q^{n/d}$

[42] 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 $q^u \equiv (q^u)^p = q^{up} \operatorname{mod} p\mathbb{Z}$, and thus $(q^u)^{p^\ell} \equiv (q^{up})^{p^\ell} \operatorname{mod} p^{1+\ell}\mathbb{Z}$ (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, $(q^u)^{p^\ell} \equiv (q^{up})^{p^\ell} \operatorname{mod} p^{1+\ell}\mathbb{Z}$ becomes $q^{n/p} \equiv q^n \operatorname{mod} p^{v_p(n)}\mathbb{Z}$ (since $q^{n/p} = (q^u)^{p^\ell}$, $q^n = (q^{up})^{p^\ell}$ and $1 + \ell = v_p(n)$). Thus, (42) is proven.

is the number of all colored necklaces consisting of n beads, where there are q colors that one can use (of course, one is not forced to use them all!) and one considers two necklaces equal if they differ from each other only in a cyclic rotation (not an axial reflection!). Of course, the number of such necklaces must be an integer, and thus $\sum\limits_{d\mid n} \phi(d) q^{n/d} \in n\mathbb{Z}$, proving Theorem 16 **(d)** in the case $q \geq 0$. One can also derive Theorem 16 **(c)** in the case $q \geq 0$ from a similar observation: Count necklaces again (identifying any two necklaces which differ from each other only in a cyclic rotation), but this time count only the *aperiodic* necklaces (these are the necklaces whose coloring is not invariant under any cyclic rotation, except of the trivial rotation). This time, there are $\dfrac{1}{n} \sum\limits_{d\mid n} \mu(d) q^{n/d}$ of them, and this leads to Theorem 16 **(c)**. However, in the case $q < 0$, these proofs of Theorems 16 **(d)** and **(c)** make no sense, and I don't know whether there exist combinatorial proofs for them in this case.

Note also that applying Theorem 16 **(c)** to a prime number n yields Fermat's Little Theorem (in fact, if n is prime, then the only divisors of n are 1 and n, and thus $\sum\limits_{d\mid n} \mu(d) q^{n/d} = \underbrace{\mu(1)}_{=1} \underbrace{q^{n/1}}_{=q^n} + \underbrace{\mu(n)}_{=-1} \underbrace{q^{n/n}}_{=q^1=q} = q^n - q$, so that Theorem 16 **(c)** becomes $q^n - q \in n\mathbb{Z}$, which is Fermat's Little Theorem).

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 $q \in \mathbb{Z}$ 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

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

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

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

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

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

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

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

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

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

The proof is similar, but verifying Assertion $\mathcal{C}_\varnothing$ turns out harder than in Theorem 16. To simplify this step as far as possible, we will have to apply an analogue of Lemma 4 **(b)** from [3] for power series instead of polynomials:

Lemma 18. Let Ξ be a family of symbols. Let $a \in \mathbb{Z}[\Xi]$ be a polynomial. Let p be a prime.

(a) For every $\ell \in \mathbb{N}$, we have $(a(\Xi^p))^{p^\ell} \equiv a^{p^{\ell+1}} \bmod p^{\ell+1}\mathbb{Z}[\Xi]$.

(b) For every $m \in \mathbb{N}_+$ satisfying $p \mid m$, we have $(a(\Xi^p))^{m/p} \equiv a^m \bmod p^{v_p(m)}\mathbb{Z}[\Xi]$.

(c) Let $\mathbb{Z}[[\Xi]]$ denote the ring of all power series over $\mathbb{Z}$ in the indeterminates Ξ. If a is a polynomial with constant term 1, then for every $m \in \mathbb{Z}\backslash\{0\}$ satisfying $p \mid m$, we have $(a(\Xi^p))^{m/p} \equiv a^m \bmod p^{v_p(m)}\mathbb{Z}[[\Xi]]$. (Note that it makes sense to speak of $(a(\Xi^p))^{m/p}$ and a^m even for negative m since we have supposed that a is a polynomial with constant term 1 and therefore invertible in $\mathbb{Z}[[\Xi]]$).

Proof of Lemma 18. **(a)** Lemma 18 **(a)** is Lemma 4 **(b)** in [3], and we refer to [3] for its proof.

(b) We have $m/p \in \mathbb{N}_+$ (since $p \mid m$). Let $\ell = v_p(m/p)$. Then, $v_p(m) = v_p((m/p) \cdot p) = \underbrace{v_p(m/p)}_{=\ell} + \underbrace{v_p(p)}_{=1} = \ell + 1$. Thus, $p^{v_p(m)} = p^{\ell+1}$, so that $p^{v_p(m)} \mid m$ becomes $p^{\ell+1} \mid m$. Thus, there exists $s \in \mathbb{N}_+$ such that $m = sp^{\ell+1}$. Hence, $m/p = sp^{\ell+1}/p = sp^\ell$. Thus,

$$\begin{aligned}(a(\Xi^p))^{m/p} &= (a(\Xi^p))^{sp^\ell} = \left((a(\Xi^p))^{p^\ell}\right)^s \equiv \left(a^{p^{\ell+1}}\right)^s \qquad \text{(by Lemma 18 **(a)**)} \\ &= a^{sp^{\ell+1}} = a^m \bmod p^{\ell+1}\mathbb{Z}[\Xi] \qquad \left(\text{since } sp^{\ell+1} = m\right).\end{aligned}$$

In other words, $(a(\Xi^p))^{m/p} \equiv a^m \bmod p^{v_p(m)}\mathbb{Z}[\Xi]$ (since $v_p(m) = \ell + 1$). This proves Lemma 18 **(b)**.

(c) Since a is a polynomial with constant term 1, there exists a multiplicative inverse a^{-1} of a in the ring $\mathbb{Z}[[\Xi]]$. Clearly, $a^{-1}(\Xi^p)$ is the multiplicative inverse of $a(\Xi^p)$ in the ring $\mathbb{Z}[[\Xi]]$ (because $a^{-1}(\Xi^p) \cdot a(\Xi^p) = \underbrace{(a^{-1} \cdot a)}_{=1}(\Xi^p) = 1(\Xi^p) = 1$). Hence, both power series $(a(\Xi^p))^{m/p}$ and a^m are well-defined elements of $\mathbb{Z}[[\Xi]]$ (since m/p and m are integers).

Since $m \in \mathbb{Z} \setminus \{0\}$, we have either $m > 0$ or $m < 0$. In the case $m > 0$, we have $m \in \mathbb{N}_+$, so that Lemma 18 **(b)** yields $\left(a\left(\Xi^p\right)\right)^{m/p} \equiv a^m \operatorname{mod} p^{v_p(m)}\mathbb{Z}\left[\Xi\right]$, and thus $\left(a\left(\Xi^p\right)\right)^{m/p} \equiv a^m \operatorname{mod} p^{v_p(m)}\mathbb{Z}\left[\left[\Xi\right]\right]$ (since $p^{v_p(m)}\mathbb{Z}\left[\Xi\right] \subseteq p^{v_p(m)}\mathbb{Z}\left[\left[\Xi\right]\right]$), and therefore Lemma 18 **(c)** is proven in the case $m > 0$. In the case $m < 0$, we have $-m \in \mathbb{N}_+$, so that Lemma 18 **(b)** (applied to $-m$ instead of m) yields $\left(a\left(\Xi^p\right)\right)^{-m/p} \equiv a^{-m} \operatorname{mod} p^{v_p(-m)}\mathbb{Z}\left[\Xi\right]$, and thus $\left(a\left(\Xi^p\right)\right)^{-m/p} \equiv a^{-m} \operatorname{mod} p^{v_p(-m)}\mathbb{Z}\left[\left[\Xi\right]\right]$ (since $p^{v_p(-m)}\mathbb{Z}\left[\Xi\right] \subseteq p^{v_p(-m)}\mathbb{Z}\left[\left[\Xi\right]\right]$), which becomes $\left(a\left(\Xi^p\right)\right)^{-m/p} \equiv a^{-m} \operatorname{mod} p^{v_p(m)}\mathbb{Z}\left[\left[\Xi\right]\right]$ (since $v_p(-m) = v_p(m)$), and multiplying this congruence by $a^m \left(a\left(\Xi^p\right)\right)^{m/p}$ yields
$a^m \equiv \left(a\left(\Xi^p\right)\right)^{m/p} \operatorname{mod} p^{v_p(m)}\mathbb{Z}\left[\left[\Xi\right]\right]$, which rewrites as $\left(a\left(\Xi^p\right)\right)^{m/p} \equiv a^m \operatorname{mod} p^{v_p(m)}\mathbb{Z}\left[\left[\Xi\right]\right]$, and therefore Lemma 18 **(c)** is proven in the case $m < 0$. Hence, Lemma 18 **(c)** is proven in each of the cases $m > 0$ and $m < 0$. Consequently, Lemma 18 **(c)** must always hold, and our proof of Lemma 18 is complete.

A consequence from Lemma 18 is the following congruence between binomial coefficients:

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,

$$\binom{qn/p}{rn/p} \equiv \binom{qn}{rn} \operatorname{mod} p^{v_p(n)}\mathbb{Z}. \tag{43}$$

Proof of Lemma 19. Since $p \in \operatorname{PF} n$, we know that p is a prime and satisfies $p \mid n$.

If $rn \notin \mathbb{N}$, then Lemma 19 is easily seen to be true.[43] Hence, in the case when $rn \notin \mathbb{N}$, we have proven Lemma 19. Therefore, we can WLOG assume that $rn \in \mathbb{N}$ for the rest of the proof. Assume this.

Since $rn \in \mathbb{N}$, we have $rn \geq 0$. Combined with $n > 0$, this yields $r \geq 0$.

Let $m = qn$. Then, $p \mid m$ (since $p \mid n$). As an easy consequence from Lemma 18, we have $\left(1 + X^p\right)^{m/p} \equiv \left(1 + X\right)^m \operatorname{mod} p^{v_p(m)}\mathbb{Z}\left[\left[X\right]\right]$. [44] Hence, for every $\lambda \in \mathbb{N}$, we

[43] *Proof.* Assume that $rn \notin \mathbb{N}$. Then, $rn/p \notin \mathbb{N}$ (because otherwise, we would have $rn/p \in \mathbb{N}$, hence $rn = \underbrace{p}_{\in \mathbb{N}} \cdot \underbrace{rn/p}_{\in \mathbb{N}} \in \mathbb{N} \cdot \mathbb{N} \subseteq \mathbb{N}$, contradicting $rn \notin \mathbb{N}$). By the definition of $\binom{qn/p}{rn/p}$, we have

$$\binom{qn/p}{rn/p} = \begin{cases} \frac{1}{(rn/p)!} \prod_{k=0}^{rn/p-1} (qn/p - k), & \text{if } rn/p \in \mathbb{N}; \\ 0, & \text{if } rn/p \notin \mathbb{N} \end{cases} = 0 \qquad (\text{since } rn/p \notin \mathbb{N}).$$

By the definition of $\binom{qn}{rn}$, we have

$$\binom{qn}{rn} = \begin{cases} \frac{1}{(rn)!} \prod_{k=0}^{rn-1} (qn - k), & \text{if } rn \in \mathbb{N}; \\ 0, & \text{if } rn \notin \mathbb{N} \end{cases} = 0 \qquad (\text{since } rn \notin \mathbb{N}).$$

Since $\binom{qn/p}{rn/p} = 0$ and $\binom{qn}{rn} = 0$, both sides of the equality (43) are 0. Thus, the equality (43) holds. In other words, Lemma 19 is true, qed.

[44] *Proof.* Applying Lemma 18 **(c)** to the family $\Xi = (X)$ and the polynomial $a = 1 + X \in \mathbb{Z}\left[\Xi\right]$ (which has constant term 1), we obtain $\left(a\left(\Xi^p\right)\right)^{m/p} \equiv a^m \operatorname{mod} p^{v_p(m)}\mathbb{Z}\left[\left[\Xi\right]\right]$. Since $a = 1 + X$ and therefore $a\left(\Xi^p\right) = 1 + X^p$ (because $a\left(\Xi^p\right)$ is the result of replacing every indeterminate in the polynomial a by its p-th power), this becomes $\left(1 + X^p\right)^{m/p} \equiv \left(1 + X\right)^m \operatorname{mod} p^{v_p(m)}\mathbb{Z}\left[\left[X\right]\right]$, qed.

have

$$\left(\text{the coefficient of the power series } \left(1+X^p\right)^{m/p} \text{ before } X^\lambda\right)$$
$$\equiv \left(\text{the coefficient of the power series } (1+X)^m \text{ before } X^\lambda\right) \operatorname{mod} p^{v_p(m)}\mathbb{Z}. \qquad (44)$$

But the binomial formula yields

$$\left(1+X^p\right)^{m/p} = \sum_{\kappa\in\mathbb{N}} \underbrace{\binom{m/p}{\kappa}}_{=\binom{m/p}{p\kappa/p}} \underbrace{\left(X^p\right)^\kappa}_{=X^{p\kappa}} = \sum_{\kappa\in\mathbb{N}} \binom{m/p}{p\kappa/p} X^{p\kappa} = \sum_{\lambda\in p\mathbb{N}} \binom{m/p}{\lambda/p} X^\lambda$$

(here we substituted λ for $p\kappa$, since the map $\mathbb{N}\to p\mathbb{N}$, $\kappa\mapsto p\kappa$ is a bijection)

$$= \sum_{\lambda\in\mathbb{N}} \binom{m/p}{\lambda/p} X^\lambda - \sum_{\lambda\in\mathbb{N}\setminus p\mathbb{N}} \underbrace{\binom{m/p}{\lambda/p}}_{\substack{=0,\text{ since}\\ \lambda/p\notin\mathbb{N},\\ \text{since }\lambda\notin p\mathbb{N}}} X^\lambda$$
$$= \sum_{\lambda\in\mathbb{N}} \binom{m/p}{\lambda/p} X^\lambda - \underbrace{\sum_{\lambda\in\mathbb{N}\setminus p\mathbb{N}} 0X^\lambda}_{=0} = \sum_{\lambda\in\mathbb{N}} \binom{m/p}{\lambda/p} X^\lambda,$$

and thus every $\lambda\in\mathbb{N}$ satisfies

$$\left(\text{the coefficient of the power series } \left(1+X^p\right)^{m/p} \text{ before } X^\lambda\right) = \binom{m/p}{\lambda/p}. \qquad (45)$$

Besides, the binomial formula yields

$$(1+X)^m = \sum_{\lambda\in\mathbb{N}} \binom{m}{\lambda} X^\lambda.$$

Hence, every $\lambda\in\mathbb{N}$ satisfies

$$\left(\text{the coefficient of the power series } (1+X)^m \text{ before } X^\lambda\right) = \binom{m}{\lambda}. \qquad (46)$$

Thus, every $\lambda\in\mathbb{N}$ satisfies

$$\binom{m/p}{\lambda/p} = \left(\text{the coefficient of the power series } \left(1+X^p\right)^{m/p} \text{ before } X^\lambda\right) \qquad (\text{by } (45))$$
$$\equiv \left(\text{the coefficient of the power series } (1+X)^m \text{ before } X^\lambda\right) \qquad (\text{by } (44))$$
$$= \binom{m}{\lambda} \operatorname{mod} p^{v_p(m)}\mathbb{Z} \qquad (\text{by } (46)).$$

Since $m = qn$, this becomes

$$\binom{qn/p}{\lambda/p} \equiv \binom{qn}{\lambda} \operatorname{mod} p^{v_p(qn)}\mathbb{Z}.$$

Hence,
$$\binom{qn/p}{\lambda/p} \equiv \binom{qn}{\lambda} \operatorname{mod} p^{v_p(n)}\mathbb{Z}$$
(since $v_p(qn) = \underbrace{v_p(q)}_{\geq 0} + v_p(n) \geq v_p(n)$ yields $p^{v_p(n)} \mid p^{v_p(qn)}$ and thus $p^{v_p(qn)}\mathbb{Z} \subseteq p^{v_p(n)}\mathbb{Z}$). Applying this to $\lambda = rn$, we obtain (43), and thus Lemma 19 is proven.

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
$$\begin{aligned} b_{n/p} &= \binom{qn/p}{rn/p} \equiv \binom{qn}{rn} \qquad \text{(by (43))} \\ &= b_n \operatorname{mod} p^{v_p(n)}\mathbb{Z} \end{aligned}$$
), 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 $(b_n)_{n\in N} \in \mathbb{Z}^N$,

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

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

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

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

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

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

$$\left(\binom{qn-1}{rn-1} = \sum_{d|n} dy_d \text{ for every } n \in \mathbb{N}_+\right).$$

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

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

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

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

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

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

(f) If $r \neq 0$, then every $n \in \mathbb{N}_+$ satisfies

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

(g) If $r \neq 0$, then every $n \in \mathbb{N}_+$ satisfies

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

(h) If $r \neq 0$, then every $n \in \mathbb{N}_+$ satisfies

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

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

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

$$\binom{qn/p-1}{rn/p-1} \equiv \binom{qn-1}{rn-1} \operatorname{mod} p^{v_p(n)}\mathbb{Z}. \tag{47}$$

Proof of Lemma 21. Since $p \in \operatorname{PF} n$, we know that p is a prime and satisfies $p \mid n$.

If $r \leq 0$, then $\binom{qn/p-1}{rn/p-1} = 0$ (since $r \leq 0$ yields $rn/p \leq 0$ and thus $rn/p-1 < 0$) and $\binom{qn-1}{rn-1} = 0$ (since $r \leq 0$ yields $rn \leq 0$ and thus $rn-1 < 0$), and thus (47) becomes trivial. Hence, in the case $r \leq 0$ we have proven Lemma 21. Therefore, we can WLOG assume that $r > 0$ for the rest of the proof. Assume this.

If $rn \notin \mathbb{N}$, then $\binom{qn/p-1}{rn/p-1} = 0$ (since $rn \notin \mathbb{N}$ yields $rn/p \notin \mathbb{N}$ and thus $rn/p-1 \notin \mathbb{N}$) and $\binom{qn-1}{rn-1} = 0$ (since $rn \notin \mathbb{N}$ yields $rn-1 \notin \mathbb{N}$), and thus (47) becomes trivial. Hence, in the case $rn \notin \mathbb{N}$ we have proven Lemma 21. Therefore, we can WLOG assume that $rn \in \mathbb{N}$ for the rest of the proof. Assume this.

It is also easy to prove Lemma 21 in the case when $q = 0$ [45]. Hence, for the rest of this proof, we can WLOG assume that $q \neq 0$. Assume this. Then, $v_p(q)$ is a well-defined nonnegative integer (not ∞).

---

[45] *Proof.* Assume that $q = 0$. Recall that

$$\binom{-1}{\tau} = (-1)^\tau \qquad \text{for every } \tau \in \mathbb{N}. \tag{48}$$

But since $rn \in \mathbb{N}$ and

$$v_p(rn) = v_p\left(\underbrace{r}_{=\frac{\alpha}{\beta}}\right) + v_p(n) = \underbrace{v_p\left(\frac{\alpha}{\beta}\right)}_{\substack{=v_p(\alpha)-v_p(\beta)\geq 0 \\ (\text{since } v_p(\alpha)\geq v_p(\beta))}} + v_p(n) \geq v_p(n) \geq 1$$

(since $p \mid n$), we have $p \mid rn$. Thus, $p \in \operatorname{PF}(rn)$ (since p is a prime) and $rn/p \in \mathbb{Z}$. On the other hand, $rn/p > 0$ (since $r > 0$ and $n > 0$). Combined with $rn/p \in \mathbb{Z}$, this yields $rn/p \in \mathbb{N}_+$. Hence, $rn/p - 1 \in \mathbb{N}$.

On the other hand, $rn > 0$ (since $r > 0$ and $n > 0$). Combining this with $rn \in \mathbb{N}$, this yields $rn \in \mathbb{N}_+$. Thus, $rn - 1 \in \mathbb{N}$.

Now, applying (42) to -1 and rn instead of q and n, we obtain $(-1)^{rn/p} \equiv (-1)^{rn} \operatorname{mod} p^{v_p(rn)}\mathbb{Z}$. Since $p^{v_p(rn)}\mathbb{Z} \subseteq p^{v_p(n)}\mathbb{Z}$ (because $v_p(rn) \geq v_p(n)$), this yields $(-1)^{rn/p} \equiv (-1)^{rn} \operatorname{mod} p^{v_p(n)}\mathbb{Z}$.

But since $q = 0$, we have

$$\begin{aligned}\binom{qn/p-1}{rn/p-1} &= \binom{0n/p-1}{rn/p-1} = \binom{-1}{rn/p-1} = (-1)^{rn/p-1} \\ &\qquad (\text{by (48), applied to } \tau = rn/p-1 \text{ (since } rn/p-1 \in \mathbb{N})) \\ &= -(-1)^{rn/p} \equiv -(-1)^{rn} \operatorname{mod} p^{v_p(n)}\mathbb{Z} \qquad \left(\text{since } (-1)^{rn/p} \equiv (-1)^{rn} \operatorname{mod} p^{v_p(n)}\mathbb{Z}\right).\end{aligned}$$

In the proof of Lemma 19, we have shown that

$$\binom{qn/p}{\lambda/p} \equiv \binom{qn}{\lambda} \operatorname{mod} p^{v_p(qn)}\mathbb{Z} \qquad \text{for every } \lambda \in \mathbb{N}.$$

In other words, $p^{v_p(qn)} \mid \binom{qn/p}{\lambda/p} - \binom{qn}{\lambda}$, so that

$$v_p\left(\binom{qn/p}{\lambda/p} - \binom{qn}{\lambda}\right) \geq v_p(qn). \tag{49}$$

But any $a \in \mathbb{Q}$ and $b \in \mathbb{Q} \setminus \{0\}$ satisfy

$$\binom{a}{b} = \frac{a}{b}\binom{a-1}{b-1} \tag{50}$$

Also, since $q = 0$, we have

$$\begin{aligned}\binom{qn-1}{rn-1} &= \binom{0n-1}{rn-1} = \binom{-1}{rn-1} = (-1)^{rn-1} \\ &\qquad \text{(by (48), applied to } \tau = rn-1 \text{ (since } rn-1 \in \mathbb{N}\text{))} \\ &= -(-1)^{rn} \equiv \binom{qn/p-1}{rn/p-1} \operatorname{mod} p^{v_p(n)}\mathbb{Z}.\end{aligned}$$

Thus, Lemma 21 is proven in the case when $q = 0$.

[46]. Thus,

$$v_p\left(\underbrace{\binom{qn/p}{\lambda/p}}_{\substack{=\frac{qn/p}{\lambda/p}\binom{qn/p-1}{\lambda/p-1}\\ \text{(by (50), applied to}\\ a=qn/p \text{ and } b=\lambda/p)}} - \underbrace{\binom{qn}{\lambda}}_{\substack{=\frac{qn}{\lambda}\binom{qn-1}{\lambda-1}\\ \text{(by (50), applied to}\\ a=qn \text{ and } b=\lambda)}}\right) = v_p\left(\underbrace{\frac{qn/p}{\lambda/p}}_{=\frac{qn}{\lambda}}\binom{qn/p-1}{\lambda/p-1} - \frac{qn}{\lambda}\binom{qn-1}{\lambda-1}\right)$$
$$= v_p\left(\frac{qn}{\lambda}\binom{qn/p-1}{\lambda/p-1} - \frac{qn}{\lambda}\binom{qn-1}{\lambda-1}\right) = v_p\left(\frac{qn}{\lambda}\left(\binom{qn/p-1}{\lambda/p-1} - \binom{qn-1}{\lambda-1}\right)\right)$$
$$= \underbrace{v_p\left(\frac{qn}{\lambda}\right)}_{=v_p(qn)-v_p(\lambda)} + v_p\left(\binom{qn/p-1}{\lambda/p-1} - \binom{qn-1}{\lambda-1}\right) = v_p(qn) - v_p(\lambda) + v_p\left(\binom{qn/p-1}{\lambda/p-1} - \binom{qn-1}{\lambda-1}\right).$$

Hence, (49) becomes

$$v_p(qn) - v_p(\lambda) + v_p\left(\binom{qn/p-1}{\lambda/p-1} - \binom{qn-1}{\lambda-1}\right) \geq v_p(qn).$$

This simplifies to

$$v_p\left(\binom{qn/p-1}{\lambda/p-1} - \binom{qn-1}{\lambda-1}\right) \geq v_p(\lambda).$$

---

[46] *Proof.* Since $b \in \mathbb{Q} \setminus \{0\} = (\mathbb{Q} \setminus \mathbb{N}) \cup (\mathbb{N} \setminus \{0\})$, we must have either $b \in \mathbb{Q} \setminus \mathbb{N}$ or $b \in \mathbb{N} \setminus \{0\}$.

If $b \in \mathbb{Q}\setminus\mathbb{N}$, then $b \notin \mathbb{N}$ and thus $\binom{a}{b} = \frac{a}{b}\binom{a-1}{b-1}$, because $\binom{a}{b} = 0$ (since $b \notin \mathbb{N}$) and $\binom{a-1}{b-1} = 0$ (since $b \notin \mathbb{N}$ yields $b-1 \notin \mathbb{N}$).

If $b \in \mathbb{N} \setminus \{0\}$, then $b-1 \in \mathbb{N}$ and thus

$$\binom{a}{b} = \frac{\prod_{k=0}^{b-1}(a-k)}{b!} = \frac{a\prod_{k=1}^{b-1}(a-k)}{b\cdot(b-1)!} \qquad \left(\text{since } \prod_{k=0}^{b-1}(a-k) = a\prod_{k=1}^{b-1}(a-k) \text{ and } b! = b\cdot(b-1)!\right)$$
$$= \frac{a}{b}\cdot\frac{\prod_{k=1}^{b-1}(a-k)}{(b-1)!} = \frac{a}{b}\cdot\frac{\prod_{k=0}^{(b-1)-1}(a-(k+1))}{(b-1)!} \qquad \text{(here we substituted } k \text{ for } k-1 \text{ in the product)}$$
$$= \frac{a}{b}\cdot\underbrace{\frac{\prod_{k=0}^{(b-1)-1}((a-1)-k)}{(b-1)!}}_{=\binom{a-1}{b-1} \text{ (since } b-1\in\mathbb{N})} = \frac{a}{b}\binom{a-1}{b-1}.$$

Hence, in each of the two cases $b \in \mathbb{Q} \setminus \mathbb{N}$ and $b \in \mathbb{N} \setminus \{0\}$, we have $\binom{a}{b} = \frac{a}{b}\binom{a-1}{b-1}$. Since these two cases cover all possibilities, we have thus proven that $\binom{a}{b} = \frac{a}{b}\binom{a-1}{b-1}$ for any $a \in \mathbb{Q}$ and any $b \in \mathbb{Q} \setminus \{0\}$.

In other words, $p^{v_p(\lambda)} \mid \dbinom{qn/p-1}{\lambda/p-1} - \dbinom{qn-1}{\lambda-1}$, so that

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

Applying this to $\lambda = rn$, we obtain

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

This yields (47) (since $r = \dfrac{\alpha}{\beta}$ yields $v_p(rn) = v_p\left(\dfrac{\alpha}{\beta} n\right) = \underbrace{v_p\left(\dfrac{\alpha}{\beta}\right)}_{\substack{=v_p(\alpha)-v_p(\beta)\geq 0 \\ (\text{since } v_p(\alpha)\geq v_p(\beta))}} + v_p(n) \geq v_p(n)$, so that $p^{v_p(rn)}\mathbb{Z} \subseteq p^{v_p(n)}\mathbb{Z}$). Thus, Lemma 21 is proven.

Proof of Theorem 20. We know that r is an integer. Thus, there exist two integers α and β with $v_p(\alpha) \geq v_p(\beta)$ and $r = \dfrac{\alpha}{\beta}$ (namely, $\alpha = r$ and $\beta = 1$ (since $\dfrac{r}{1} = 1$ and $v_p(r) \geq 0 = v_p(1)$)). Hence, (47) yields that every $n \in \mathbb{N}_+$ and every $p \in \operatorname{PF} n$ satisfy

$$\binom{qn/p-1}{rn/p-1} \equiv \binom{qn-1}{rn-1} \operatorname{mod} p^{v_p(n)}\mathbb{Z}. \tag{51}$$

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

$$\begin{aligned} b_{n/p} &= \binom{qn/p-1}{rn/p-1} \equiv \binom{qn-1}{rn-1} \qquad\qquad (\text{by } (51)) \\ &= b_n \operatorname{mod} p^{v_p(n)}\mathbb{Z} \end{aligned}$$

), 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 $(b_n)_{n\in N} \in \mathbb{Z}^N$,

- assertion $\mathcal{D}'_\varnothing$ is equivalent to Theorem 20 **(a)** (since $N = \mathbb{N}_+$ and $b_n = \dbinom{qn-1}{rn-1}$);
- assertion $\mathcal{E}'_\varnothing$ is equivalent to Theorem 20 **(b)** (since $N = \mathbb{N}_+$ and $b_n = \dbinom{qn-1}{rn-1}$);
- assertion $\mathcal{F}_\varnothing$ is equivalent to Theorem 20 **(c)** (since $N = \mathbb{N}_+$ and $b_{n/d} = \dbinom{qn/d-1}{rn/d-1}$);
- 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 $(b_n)_{n\in N} \in \mathbb{Z}^N$).

Now it remains to prove Theorem 20 **(f)**, Theorem 20 **(g)** and Theorem 20 **(h)**. To this end, let us assume that $r \neq 0$.

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

$$\sum_{d\mid n}\mu(d)\underbrace{\binom{qn/d}{rn/d}}_{\substack{=\frac{qn/d}{rn/d}\binom{qn/d-1}{rn/d-1}\\ \text{(by (50), applied to}\\ a=qn/d\text{ and }b=rn/d)}} = \sum_{d\mid n}\mu(d)\underbrace{\frac{qn/d}{rn/d}}_{=\frac{q}{r}}\binom{qn/d-1}{rn/d-1} = \frac{q}{r}\underbrace{\sum_{d\mid n}\mu(d)\binom{qn/d-1}{rn/d-1}}_{\substack{\in n\mathbb{Z}\\ \text{(by Theorem 20 (c))}}} \in \frac{q}{r}n\mathbb{Z}.$$

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

$$\sum_{d\mid n}\phi(d)\underbrace{\binom{qn/d}{rn/d}}_{\substack{=\frac{qn/d}{rn/d}\binom{qn/d-1}{rn/d-1}\\ \text{(by (50), applied to}\\ a=qn/d\text{ and }b=rn/d)}} = \sum_{d\mid n}\phi(d)\underbrace{\frac{qn/d}{rn/d}}_{=\frac{q}{r}}\binom{qn/d-1}{rn/d-1} = \frac{q}{r}\underbrace{\sum_{d\mid n}\phi(d)\binom{qn/d-1}{rn/d-1}}_{\substack{\in n\mathbb{Z}\\ \text{(by Theorem 20 (d))}}} \in \frac{q}{r}n\mathbb{Z}.$$

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

$$\begin{aligned}\sum_{i=1}^{n}\underbrace{\binom{q\gcd(i,n)}{r\gcd(i,n)}}_{\substack{=\frac{q\gcd(i,n)}{r\gcd(i,n)}\binom{q\gcd(i,n)-1}{r\gcd(i,n)-1}\\ \text{(by (50), applied to}\\ a=q\gcd(i,n)\text{ and }b=r\gcd(i,n))}} &= \sum_{i=1}^{n}\underbrace{\frac{q\gcd(i,n)}{r\gcd(i,n)}}_{=\frac{q}{r}}\binom{q\gcd(i,n)-1}{r\gcd(i,n)-1}\\ &= \frac{q}{r}\underbrace{\sum_{i=1}^{n}\binom{q\gcd(i,n)-1}{r\gcd(i,n)-1}}_{\substack{\in n\mathbb{Z}\\ \text{(by Theorem 20 (e))}}} \in \frac{q}{r}n\mathbb{Z}.\end{aligned}$$

Thus, altogether we have now proven Theorem 20 completely.

Note that Theorem 20 **(h)** is a generalization of the problem proposed in [5] (in fact, the problem proposed in [5] follows from Theorem 20 **(h)** for $r = 1$).

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

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

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

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

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

(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

$$b_{n/p}(\Xi^p) \equiv b_n \operatorname{mod} p^{v_p(n)}\mathbb{Z}[\Xi]. \tag{52}$$

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[47]:

Lemma 23. 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

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

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

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

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

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

[47]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

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

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

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

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

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

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

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

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

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

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 $p^{v_p(n)}\mathbb{Q}[\Xi] = \mathbb{Q}[\Xi]$ for every $n \in N$ and every $p \in \operatorname{PF} n$, and $n\mathbb{Q}[\Xi] = \mathbb{Q}[\Xi]$ 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 $b_{n/p}(\Xi^p) \equiv b_n \bmod p^{v_p(n)}\mathbb{Q}[\Xi]$, because $p^{v_p(n)}\mathbb{Q}[\Xi] = \mathbb{Q}[\Xi]$). Thus, it also satisfies the Assertion

$\mathcal{D}'^{\mathbb{Q}}_{\Xi}$ of Lemma 23 (since Lemma 23 yields that the assertions $\mathcal{C}^{\mathbb{Q}}_{\Xi}$ and $\mathcal{D}'^{\mathbb{Q}}_{\Xi}$ 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

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

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

$$\widetilde{x}_n \in \mathbb{Q}\left[b_{\mathbb{N}_{|n}}\right] \text{ is already proven for every } n \in N \text{ satisfying } n < m. \tag{53}$$

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 $b_n = w_n\left((\widetilde{x}_k)_{k\in N}\right)$ for every $n \in N$. In particular, for $n = m$, this yields

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

so that $\widetilde{x}_m = \dfrac{1}{m}\left(b_m - \sum\limits_{\substack{d|m;\\ d\neq m}} d\widetilde{x}_d^{m/d}\right)$. Now, every divisor d of m satisfying $d \neq m$ must satisfy $d\widetilde{x}_d^{m/d} \in \mathbb{Q}\left[b_{\mathbb{N}_{|m}}\right]$ (in fact, $d \mid m$ and $d \neq m$ yield $d < m$, and thus (53) (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 $d\widetilde{x}_d^{m/d} \in \mathbb{Q}\left[b_{\mathbb{N}_{|m}}\right]$), and clearly $b_m \in \mathbb{Q}\left[b_{\mathbb{N}_{|m}}\right]$. Hence, $\widetilde{x}_m = \dfrac{1}{m}\left(\underbrace{b_m}_{\in\mathbb{Q}\left[b_{\mathbb{N}_{|m}}\right]} - \sum\limits_{\substack{d|m;\\ d\neq m}} \underbrace{d\widetilde{x}_d^{m/d}}_{\in\mathbb{Q}\left[b_{\mathbb{N}_{|m}}\right]}\right) \in \mathbb{Q}\left[b_{\mathbb{N}_{|m}}\right]$. 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 (52).

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 (52).

Assertion 2: If every $n \in N$ and every $p \in \operatorname{PF} n$ satisfies (52), 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 $\left(b_n = w_n\left((\widetilde{x}_k)_{k\in N}\right) \text{ for every } n \in N\right)$ (according to Theorem 22 **(a)**). Thus, there exists a family $(x_n)_{n\in N} \in (\mathbb{Z}[\Xi])^N$ satisfying $\left(b_n = w_n\left((x_k)_{k\in N}\right) \text{ for every } n \in N\right)$ (namely, the family $(x_n)_{n\in N} = (\widetilde{x}_n)_{n\in N}$). 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 (52). Thus, Assertion 1 is proven.

Proof of Assertion 2: Assume that every $n \in N$ and every $p \in \operatorname{PF} n$ satisfies (52). 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 $(x_n)_{n\in N} \in (\mathbb{Z}[\Xi])^N$ of elements of $\mathbb{Z}[\Xi]$ such that

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

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

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

Hence, this family $(x_n)_{n\in N}$ must be equal to the family $(\widetilde{x}_n)_{n\in N}$ (because, according to Theorem 22 **(a)**, the only family $(x_n)_{n\in N} \in (\mathbb{Q}[\Xi])^N$ of elements of $\mathbb{Q}[\Xi]$ such that

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

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

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

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

$$\left(w_n\left((x_k)_{k\in N}\right) = f\left(w_n(X_{1,N}), w_n(X_{2,N}), ..., w_n(X_{m,N})\right) \qquad \text{for every } n \in N\right). \tag{54}$$

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

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

(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

$$b_n = f\left(w_n\left(X_{1,N}\right), w_n\left(X_{2,N}\right), ..., w_n\left(X_{m,N}\right)\right) \qquad \text{for every } n \in N. \tag{55}$$

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

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

Since the assertion $\left(b_n = w_n\left((x_k)_{k\in N}\right) \text{ for every } n \in N\right)$ is equivalent to (54)[48], 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

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

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

$$w_n\left(X_{k,N}\right) \in \mathbb{Z}\left[\Xi_{\mathbb{N}_{|n}}\right] \qquad \text{for every } n \in N \tag{56}$$

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

$$w_d\left(X_{k,N}\right) \in \mathbb{Z}\left[\Xi_{\mathbb{N}_{|n}}\right] \qquad \text{for every } n \in N \text{ and every } d \in \mathbb{N}_{|n} \tag{57}$$

(because (56), applied to d instead of n, yields $w_d\left(X_{k,N}\right) \in \mathbb{Z}\left[\Xi_{\mathbb{N}_{|d}}\right] \subseteq \mathbb{Z}\left[\Xi_{\mathbb{N}_{|n}}\right]$, 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

$$\mathbb{Q}\left[\Xi_{\mathbb{N}_{|n}}\right] \cap \mathbb{Z}[\Xi] = \mathbb{Z}\left[\Xi_{\mathbb{N}_{|n}}\right]. \tag{58}$$

In fact, this follows from a general rule: If U and V are two sets of symbols such that $U \subseteq V$, then $\mathbb{Q}[U] \cap \mathbb{Z}[V] = \mathbb{Z}[U]$. [49]

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

$$\begin{aligned}
&\left(b_n = w_n\left((x_k)_{k\in N}\right) \text{ for every } n \in N\right)\\
\iff &\left(f\left(w_n\left(X_{1,N}\right), w_n\left(X_{2,N}\right), ..., w_n\left(X_{m,N}\right)\right) = w_n\left((x_k)_{k\in N}\right) \text{ for every } n \in N\right) \qquad \text{(because of (55))}\\
\iff &\left((54) \text{ holds}\right).
\end{aligned}$$

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

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)** [50].

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

$$b_d = f\left(w_d\left(X_{1,N}\right), w_d\left(X_{2,N}\right), ..., w_d\left(X_{m,N}\right)\right) \in \mathbb{Z}\left[\Xi_{\mathbb{N}_{|n}}\right] \qquad \left(\text{by (57), since } f \in \mathbb{Z}[\alpha_1, \alpha_2, ..., \alpha_m]\right)$$
$$\subseteq \mathbb{Q}\left[\Xi_{\mathbb{N}_{|n}}\right]$$

).

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 $\Xi^p = \bigcup\limits_{k\in\{1,2,...,m\}} X_{k,N}^p$.

Obviously,

$$w_{n/p}\left(X_{k,N}^p\right) = w_{n/p}\left(\left(X_{k,n}^p\right)_{n\in N}\right) = \sum_{d|(n/p)} d \underbrace{\left(X_{k,d}^p\right)^{(n/p)/d}}_{=X_{k,d}^{p\cdot(n/p)/d}=X_{k,d}^{n/d}} \qquad \left(\text{since } w_{n/p} = \sum_{d|(n/p)} dX_d^{(n/p)/d}\right)$$
$$= \sum_{d|(n/p)} dX_{k,d}^{n/d}$$

$\alpha \in V_{\text{fin}}^{\mathbb{N}}$.

- 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.

[50] 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 $\left(b_n = w_n\left((x_k)_{k\in N}\right) \text{ for every } n \in N\right)$, 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 (54). Since $\left(b_n = w_n\left((x_k)_{k\in N}\right) \text{ for every } n \in N\right)$ is equivalent to (54), 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)**.

and

$$w_n\left(X_{k,N}\right) = w_n\left(\left(X_{k,n}\right)_{n\in N}\right) = \sum_{d\mid n} dX_{k,d}^{n/d} \qquad \left(\text{since } w_n = \sum_{d\mid n} dX_d^{n/d}\right)$$

$$= \sum_{\substack{d\mid n;\\ d\mid(n/p)}} dX_{k,d}^{n/d} + \sum_{\substack{d\mid n;\\ d\nmid(n/p)}} dX_{k,d}^{n/d} = \underbrace{\sum_{\substack{d\mid n;\\ d\mid(n/p)}}}_{=\sum_{d\mid(n/p)}} dX_{k,d}^{n/d} + \sum_{\substack{d\mid n;\\ p^{v_p(n)}\mid d}} \underbrace{d}_{\substack{\equiv 0 \operatorname{mod} p^{v_p(n)}\mathbb{Z}[\Xi],\\ \text{since } p^{v_p(n)}\mid d}} X_{k,d}^{n/d}$$

$$\left(\begin{array}{c}\text{since for any divisor } d \text{ of } n\text{, the assertions } d\nmid(n/p) \text{ and } p^{v_p(n)}\mid d \text{ are equivalent,}\\ \text{as we saw during the proof of Theorem 4}\end{array}\right)$$

$$\equiv \sum_{d\mid(n/p)} dX_{k,d}^{n/d} + \sum_{\substack{d\mid n;\\ p^{v_p(n)}\mid d}} 0X_{k,d}^{n/d} = \sum_{d\mid(n/p)} dX_{k,d}^{n/d} \operatorname{mod} p^{v_p(n)}\mathbb{Z}\left[\Xi\right],$$

so that

$$w_{n/p}\left(X_{k,N}^p\right) \equiv w_n\left(X_{k,N}\right) \operatorname{mod} p^{v_p(n)}\mathbb{Z}\left[\Xi\right]. \tag{59}$$

On the other hand, $\left(b_n\right)_{n\in N} \in \left(\mathbb{Z}\left[\Xi\right]\right)^N$. Hence, Theorem 22 **(c)** yields that the family $\left(\widetilde{x}_n\right)_{n\in N} \in \left(\mathbb{Q}\left[\Xi\right]\right)^N$ defined in Theorem 22 **(a)** satisfies $\left(\widetilde{x}_n\right)_{n\in N} \in \left(\mathbb{Z}\left[\Xi\right]\right)^N$ if and only if every $n \in N$ and every $p \in \operatorname{PF} n$ satisfies (52). Since the family $\left(\widetilde{x}_n\right)_{n\in N}$ defined in Theorem 22 **(a)** is the same as the family $\left(f_n\right)_{n\in N}$ defined in Theorem 25 **(a)**, this rewrites as follows: The family $\left(f_n\right)_{n\in N}$ defined in Theorem 25 **(a)** satisfies $\left(f_n\right)_{n\in N} \in \left(\mathbb{Z}\left[\Xi\right]\right)^N$ if and only if every $n \in N$ and every $p \in \operatorname{PF} n$ satisfies (52). But since every $n \in N$ and every $p \in \operatorname{PF} n$ satisfies (52) (because the definition of $b_{n/p}$ yields

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

and thus

$$b_{n/p}\left(\Xi^p\right) = f\left(w_{n/p}\left(X_{1,N}^p\right), w_{n/p}\left(X_{2,N}^p\right), ..., w_{n/p}\left(X_{m,N}^p\right)\right) \equiv f\left(w_n\left(X_{1,N}\right), w_n\left(X_{2,N}\right), ..., w_n\left(X_{m,N}\right)\right)$$
$$\text{(because of (59))}$$
$$= b_n \operatorname{mod} p^{v_p(n)}\mathbb{Z}\left[\Xi\right]$$

(by the definition of b_n)), this yields that the family $\left(f_n\right)_{n\in N}$ defined in Theorem 25 **(a)** satisfies $\left(f_n\right)_{n\in N} \in \left(\mathbb{Z}\left[\Xi\right]\right)^N$. Hence, $f_n \in \mathbb{Z}\left[\Xi\right]$ 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

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

(by (58)). This proves Theorem 25 **(b)**.

Theorem 25 is a very powerful result. Applied to $N = \mathbb{N}_+$ and $m = 3$, it yields Theorem 9.73 in [1][51]. Applied to $N = \{1, p, p^2, p^3, ...\}$ (where p is a prime) and $m = 3$,

[51] Keep in mind that the notations in our Theorem 25 are slightly different from the notations in Theorem 9.73 in [1]:

Theorem 25 yields Theorem 5.2 in [1][52]. Besides, the $m = 3$ and $N = \{1, p, p^2, p^3, ...\}$ particular case of our Theorem 25 is equivalent to Theorem 5 in [3][53]. We can also apply Theorem 25 to various other nests N and to $m > 3$ (though in the applications known to me, only the $m \leq 3$ case is ever used, and this is the reason why in [1] our theorem is only formulated for $m = 3$).

Let us also remark that Theorem 22, applied to $N = \{1, p, p^2, p^3, ...\}$ (where p is a prime), is only a little bit weaker than Theorem 3 in [3][54] (weaker because our Theorem 22 **(c)** requires the assumption $(b_n)_{n \in N} \in (\mathbb{Z}[\Xi])^N$, while Theorem 3 **(c)** in [3] doesn't require the corresponding assumption; however, the difference is irrelevant).

[...]

[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`

- our polynomial f is called φ in [1];
- our indeterminates $X_{1,1}$, $X_{1,2}$, $X_{1,3}$, ..., $X_{2,1}$, $X_{2,2}$, $X_{2,3}$, ..., $X_{3,1}$, $X_{3,2}$, $X_{3,3}$, ... are called X_1, X_2, X_3, ..., Y_1, Y_2, Y_3, ..., Z_1, Z_2, Z_3, ... in [1];
- finally, our polynomials f_1, f_2, f_3, ... are called φ_1, φ_2, φ_3, ... in [1].

[52] Keep in mind that the notations in our Theorem 25 are distinctly different from the notations in Theorem 5.2 in [1]:

- our polynomial f is called φ in [1];
- our indeterminates $X_{1,1}$, $X_{1,p}$, X_{1,p^2}, ..., $X_{2,1}$, $X_{2,p}$, X_{2,p^2}, ..., $X_{3,1}$, $X_{3,p}$, X_{3,p^2}, ... are called X_0, X_1, X_2, ..., Y_0, Y_1, Y_2, ..., Z_0, Z_1, Z_2, ... in [1];
- our polynomials f_1, f_p, f_{p^2}, ... are called φ_0, φ_1, φ_2, ... in [1];
- finally, the polynomials denoted by w_1, w_2, w_3, ... in Sections 5-8 of [1] are actually the polynomials denoted by w_p, w_{p^2}, w_{p^3}, ... in our notations (and this only if we rename the variables X_0, X_1, X_2, ... into X_1, X_p, X_{p^2}, ... etc.), and *not* the polynomials denoted by w_1, w_2, w_3, ... in our notations!

[53] Keep in mind that the notations in our Theorem 25 are distinctly different from the notations in [3]:

- our indeterminates $X_{1,1}$, $X_{1,p}$, X_{1,p^2}, ..., $X_{2,1}$, $X_{2,p}$, X_{2,p^2}, ..., $X_{3,1}$, $X_{3,p}$, X_{3,p^2}, ... are called X_0, X_1, X_2, ..., Y_0, Y_1, Y_2, ..., Z_0, Z_1, Z_2, ... in [3];
- the polynomials denoted by w_1, w_2, w_3, ... in [3] are actually the polynomials denoted by w_p, w_{p^2}, w_{p^3}, ... in our notations (and this only if we rename the variables X_0, X_1, X_2, ... into X_1, X_p, X_{p^2}, ... etc.), and *not* the polynomials denoted by w_1, w_2, w_3, ... in our notations!

[54] Keep in mind that the notations in our Theorem 22 are distinctly different from the notations in [3]:

- our polynomials b_1, b_p, b_{p^2}, ... are referred to as p_0, p_1, p_2, ... in [3];
- our polynomials x_1, x_p, x_{p^2}, ... are referred to as f_0, f_1, f_2, ... in [3];
- the polynomials denoted by w_1, w_2, w_3, ... in [3] are actually the polynomials denoted by w_p, w_{p^2}, w_{p^3}, ... in our notations (and this only if we rename the variables X_0, X_1, X_2, ... into X_1, X_p, X_{p^2}, ... etc.), and *not* the polynomials denoted by w_1, w_2, w_3, ... in our notations!

[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] Ronald L. Graham, Donald E. Knuth, Oren Patashnik, *Concrete Mathematics*, 2nd Edition, 1994.

[5] *Sum of binomial coefficients [with gcd] (MathLinks topic #91364)*,
http://www.mathlinks.ro/Forum/viewtopic.php?t=91364