Witt vectors. Part 1

Michiel Hazewinkel
Sidenotes by Darij Grinberg

Witt#5f: Ghost-Witt integrality for binomial rings

[version 1.1 (13 September 2014), not proofread]

§1. Definitions and basic results from [5]

The purpose of this note is applying results from [5] to the particular case of binomial rings, and extend them (in this particular case) by additional equivalent assertions.

We start by introducing notation that will be used. The following definitions 1, 2, 3, 4, 5, 6, 7, 8, 9 and 10 are copied from [5].

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 $n \in S$).

---

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

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

Here are some examples of nests: For instance, $\mathbb{N}_+$ itself is a nest. For every prime p, the set $\{1, p, p^2, p^3, ...\}$ is a nest; we denote this nest by $p^{\mathbb{N}}$. For any integer m, the set $\{n \in \mathbb{N}_+ \mid n \perp m\}$ is a nest; we denote this nest by $\mathbb{N}_{\perp m}$. For any positive integer m, the set $\{n \in \mathbb{N}_+ \mid n \leq m\}$ is a nest; we denote this nest by $\mathbb{N}_{\leq m}$. For any integer m, the set $\{n \in \mathbb{N}_+ \mid (n \mid m)\}$ is a nest; we denote this nest by $\mathbb{N}_{|m}$. Another example of a nest is the set $\{1, 2, 3, 5, 6, 10\}$.

Clearly, every nest N contains the element 1 [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

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

[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.

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,

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

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

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

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

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

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

Let us state a couple of theorems whose proofs we will mostly skip:

Theorem 1. 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

$$\left(\varphi_p(a) \equiv a^p \bmod pA \text{ holds for every } a \in A \text{ and } p \in \mathbb{P}\cap N\right). \quad (1)$$

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

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

$$\varphi_p\left(b_{n/p}\right) \equiv b_n \bmod p^{v_p(n)} A. \quad (2)$$

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

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

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

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

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

Proof of Theorem 1. According to Theorem 4 of [5], the assertions $\mathcal{C}$ and $\mathcal{D}$ are equivalent.

On the other hand, if $(x_n)_{n \in N} \in A^N$ is a family of elements of A, then every $n \in N$ satisfies $w_n\left((x_k)_{k \in N}\right) = \sum_{d \mid n} d x_d^{n/d}$. Therefore, the assertions $\mathcal{D}$ and $\mathcal{D}^{\text{expl}}$ are equivalent. Combining this with the fact that the assertions $\mathcal{C}$ and $\mathcal{D}$ are equivalent, we conclude that the three assertions $\mathcal{C}$, $\mathcal{D}$ and $\mathcal{D}^{\text{expl}}$ are equivalent. This proves Theorem 1.

Theorem 2. 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 (1) holds.

Let $(b_n)_{n \in N} \in A^N$ be a family of elements of A. Then, the five assertions $\mathcal{C}$, $\mathcal{D}$, $\mathcal{D}'$, $\mathcal{D}^{\text{expl}}$ and $\mathcal{D}^{\text{expl}\prime}$ are equivalent, where the assertions $\mathcal{C}$, $\mathcal{D}$ and $\mathcal{D}^{\text{expl}}$ are the ones stated in Theorem 1, and the assertions $\mathcal{D}'$ and $\mathcal{D}^{\text{expl}\prime}$ are the following ones:

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

$$\left(b_n = w_n\left((x_k)_{k \in N}\right) \text{ for every } n \in N \right). \tag{3}$$

Assertion $\mathcal{D}^{\text{expl}\prime}$: There exists *one and only one* family $(x_n)_{n \in N} \in A^N$ of elements of A such that

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

Proof of Theorem 2. Whenever $(x_n)_{n \in N} \in A^N$ is a family of elements of A, every $n \in N$ satisfies $w_n\left((x_k)_{k \in N}\right) = \sum_{d \mid n} d x_d^{n/d}$. Hence, the assertions $\mathcal{D}'$ and $\mathcal{D}^{\text{expl}\prime}$ are equivalent.

But according to Theorem 9 of [5], the assertions $\mathcal{C}$, $\mathcal{D}$ and $\mathcal{D}'$ are equivalent. Combined with the fact that the assertions $\mathcal{D}'$ and $\mathcal{D}^{\text{expl}\prime}$ are equivalent, this yields that the four assertions $\mathcal{C}$, $\mathcal{D}$, $\mathcal{D}'$ and $\mathcal{D}^{\text{expl}\prime}$ are equivalent. Combined with the fact that the assertions $\mathcal{C}$, $\mathcal{D}$ and $\mathcal{D}^{\text{expl}}$ are equivalent (this is due to Theorem 1), this yields that the five assertions $\mathcal{C}$, $\mathcal{D}$, $\mathcal{D}'$, $\mathcal{D}^{\text{expl}}$ and $\mathcal{D}^{\text{expl}\prime}$ are equivalent. This proves Theorem 2.

Theorem 3. 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. Assume that

$$(\varphi_1 = \mathrm{id}) \qquad \text{and} \tag{4}$$

$$(\varphi_n \circ \varphi_m = \varphi_{nm} \text{ for every } n \in N \text{ and every } m \in N \text{ satisfying } nm \in N). \tag{5}$$

Also, assume that (1) holds.

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

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

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

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

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

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

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

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

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

Proof of Theorem 3. According to Theorem 5 of [5], the five assertions $\mathcal{C}$, $\mathcal{E}$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ are equivalent. Combined with the fact that the three assertions $\mathcal{C}$, $\mathcal{D}$ and $\mathcal{D}^{\mathrm{expl}}$ are equivalent (this is due to Theorem 1), this yields that the assertions $\mathcal{C}$, $\mathcal{D}$, $\mathcal{D}^{\mathrm{expl}}$, $\mathcal{E}$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ are equivalent. This proves Theorem 3.

Theorem 4. 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 (1), (4) and (5) are satisfied.

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

- the assertions $\mathcal{C}$, $\mathcal{D}$ and $\mathcal{D}^{\mathrm{expl}}$ are the ones stated in Theorem 1,

- the assertions $\mathcal{D}'$ and $\mathcal{D}^{\mathrm{expl}\prime}$ are the ones stated in Theorem 2,
- the assertions $\mathcal{E}$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ are the ones stated in Theorem 3, 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

$$\left(b_n = \sum_{d\mid n} d\varphi_{n/d}\left(y_d\right) \text{ for every } n \in N \right). \tag{6}$$

Proof of Theorem 4. Theorem 7 of [5] yields that the six assertions $\mathcal{C}$, $\mathcal{E}$, $\mathcal{E}'$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ are equivalent. Combined with the fact that the five assertions $\mathcal{C}$, $\mathcal{D}$, $\mathcal{D}'$, $\mathcal{D}^{\mathrm{expl}}$ and $\mathcal{D}^{\mathrm{expl}\prime}$ are equivalent (this follows from Theorem 2), this yields that the assertions $\mathcal{C}$, $\mathcal{D}$, $\mathcal{D}'$, $\mathcal{D}^{\mathrm{expl}}$, $\mathcal{D}^{\mathrm{expl}\prime}$, $\mathcal{E}$, $\mathcal{E}'$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ are equivalent. Theorem 4 is thus proven.

§2. Binomial rings

So far we have done nothing but rewriting some results of [5]. We will now introduce the so-called binomial rings, and study the simplifications that occur in Theorem 4 when it is applied to such rings. The notion of binomial rings is a classical one (see [3] and [4], among other sources).

First, let us define binomial coefficients.

Definition 11. Let B be a $\mathbb{Q}$-algebra with unity. For any $u \in B$ and any $r \in \mathbb{Q}$, we define an element $\binom{u}{r} \in B$ by

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

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

It is clear that Definition 11 generalizes the standard definition of binomial coefficients $\binom{u}{r}$ with $u \in \mathbb{N}$ and $r \in \mathbb{N}$. As a consequence, we will refer to the elements $\binom{u}{r}$ defined in Definition 11 as "binomial coefficients". We will be mainly concerned with rings which are not $\mathbb{Q}$-algebras but in which the binomial coefficients $\binom{u}{r}$ can still be defined.

Definition 12. Let A be a commutative ring with unity. We denote by $\mathbb{N}_{+A}$ the subset $\{n \cdot 1_A \mid n \in \mathbb{N}_+\}$ of A. This subset $\mathbb{N}_{+A}$ is multiplicatively closed, so a localization $(\mathbb{N}_{+A})^{-1} A$ of the ring A is defined. If A is torsionfree, then the canonical ring homomorphism $A \to (\mathbb{N}_{+A})^{-1} A$ is injective (because if A is torsionfree, then each element of $\mathbb{N}_{+A}$ is a non-zerodivisor in A). Hence, whenever A is torsionfree, we will regard A as a subring of its localization $(\mathbb{N}_{+A})^{-1} A$. It should be noticed that $(\mathbb{N}_{+A})^{-1} A$ is a $\mathbb{Q}$-algebra, since each element of $\mathbb{N}_{+A}$ has been made invertible in $(\mathbb{N}_{+A})^{-1} A$. Hence, whenever A is a torsionfree commutative ring with unity, an element $\binom{u}{r} \in (\mathbb{N}_{+A})^{-1} A$ is well-defined for every $u \in A$ and $r \in \mathbb{Q}$ (because every $u \in A$ lies in $(\mathbb{N}_{+A})^{-1} A$). Of course, this element $\binom{u}{r}$ does not always lie in A (for example, if $A = \mathbb{Z}[X]$, $r = 2$ and $u = X$, then $\binom{u}{r} = \binom{X}{2} = \frac{1}{2}(X^2 - X) \in \left(\mathbb{N}_{+\mathbb{Z}[X]}\right)^{-1} (\mathbb{Z}[X])$ does not lie in $\mathbb{Z}[X]$).

Definition 13. Let A be a commutative ring with unity. We say that A is a *binomial ring* if A is torsionfree and satisfies the following property: For any $u \in A$ and any $r \in \mathbb{N}$, the element $\binom{u}{r} \in (\mathbb{N}_{+A})^{-1} A$ lies in A.

The most important example of a binomial ring is:

Proposition 5. The ring $\mathbb{Z}$ is a binomial ring.

The proof of this hinges upon the following easy fact:

Proposition 6. Let A be a $\mathbb{Q}$-algebra. Let $u \in A$. Let $r \in \mathbb{Z}$. Then,

$$\binom{u}{r} = (-1)^r \binom{r-u-1}{r}.$$

Proposition 6 is known as the *upper negation formula*.

Proof of Proposition 6. If $r \notin \mathbb{N}$, then the equality $\binom{u}{r} = (-1)^r \binom{r-u-1}{r}$ is obvious by virtue of both binomial coefficients $\binom{u}{r}$ and $\binom{r-u-1}{r}$ being zero. Hence, for the rest of this proof, we can WLOG assume that $r \in \mathbb{N}$. Assume

this. Since $r \in \mathbb{N}$, the definition of $\binom{r-u-1}{r}$ yields

$$\begin{aligned}
\binom{r-u-1}{r} &= \frac{1}{r!}\prod_{k=0}^{r-1}\underbrace{((r-u-1)-k)}_{\substack{=-(u-((r-1)-k)) \\ =(-1)(u-((r-1)-k))}} = \frac{1}{r!}\underbrace{\prod_{k=0}^{r-1}\left((-1)\left(u-((r-1)-k)\right)\right)}_{=\left(\prod_{k=0}^{r-1}(-1)\right)\left(\prod_{k=0}^{r-1}(u-((r-1)-k))\right)} \\
&= \frac{1}{r!}\underbrace{\left(\prod_{k=0}^{r-1}(-1)\right)}_{=(-1)^r}\underbrace{\left(\prod_{k=0}^{r-1}\left(u-((r-1)-k)\right)\right)}_{\substack{=\prod_{k=0}^{r-1}(u-k) \\ \text{(here, we substituted } k \text{ for } (r-1)-k \\ \text{in the product)}}} \\
&= \frac{1}{r!}(-1)^r\prod_{k=0}^{r-1}(u-k) = (-1)^r\frac{1}{r!}\prod_{k=0}^{r-1}(u-k)\,.
\end{aligned}$$

Multiplying this identity with $(-1)^r$, we obtain

$$(-1)^r\binom{r-u-1}{r} = \frac{1}{r!}\prod_{k=0}^{r-1}(u-k)\,.$$

On the other hand, since $r \in \mathbb{N}$, the definition of $\binom{u}{r}$ yields

$$\binom{u}{r} = \frac{1}{r!}\prod_{k=0}^{r-1}(u-k)\,.$$

Compared to $(-1)^r\binom{r-u-1}{r} = \frac{1}{r!}\prod_{k=0}^{r-1}(u-k)$, this proves $\binom{u}{r} = (-1)^r\binom{r-u-1}{r}$. Proposition 6 is proven.

Proof of Proposition 5. Clearly, the ring $\mathbb{Z}$ is torsionfree. Hence, in order to prove that $\mathbb{Z}$ is binomial, we only need to show that for any $u \in \mathbb{Z}$ and any $r \in \mathbb{N}$, the element $\binom{u}{r} \in \left(\mathbb{N}_{+\mathbb{Z}}\right)^{-1}\mathbb{Z}$ lies in $\mathbb{Z}$.

So let $r \in \mathbb{N}$. We need to prove that $\binom{u}{r} \in \mathbb{Z}$ for every $u \in \mathbb{Z}$.

For every $u \in \mathbb{N}$, the definition of $\binom{u}{r}$ yields $\binom{u}{r} = \frac{1}{r!}\prod_{k=0}^{r-1}(u-k)$ (since $r \in \mathbb{N}$). Hence, for every $u \in \mathbb{N}$, the number $\binom{u}{r}$ is the binomial coefficient "u choose r" known from enumerative combinatorics. Thus, by a known fact from enumerative combinatorics, every $u \in \mathbb{N}$ satisfies

$$\binom{u}{r} = (\text{the number of all } r\text{-element subsets of the set } \{1,2,...,u\}) \in \mathbb{Z} \quad (7)$$

(because the cardinality of any finite set is $\in \mathbb{Z}$). Thus, $\binom{u}{r} \in \mathbb{Z}$ is proven for every $u \in \mathbb{N}$.

Now it remains to prove $\binom{u}{r} \in \mathbb{Z}$ for every $u \in \mathbb{Z}$ satisfying $u \notin \mathbb{N}$. So let $u \in \mathbb{Z}$ satisfy $u \notin \mathbb{N}$. Since $u \notin \mathbb{N}$, we know that u is a negative integer, so that $-u$ is a positive integer. Thus, $r - u - 1 \in \mathbb{N}$ (since $r \in \mathbb{N}$). Hence, (7) (applied to $r - u - 1$ instead of u) yields $\binom{r-u-1}{r} \in \mathbb{Z}$. But Proposition 6 (applied to $A = \mathbb{Q}$) yields

$$\binom{u}{r} = (-1)^r \underbrace{\binom{r-u-1}{r}}_{\in \mathbb{Z}} \in (-1)^r \mathbb{Z} \subseteq \mathbb{Z}.$$

We have thus proven that $\binom{u}{r} \in \mathbb{Z}$ for every $u \in \mathbb{Z}$. As explained above, this concludes the proof that $\mathbb{Z}$ is binomial. Thus, Proposition 5 is proven.

For a less trivial example of a binomial ring, we can take the ring of all integer-valued polynomials:

Proposition 7. Let X be a symbol. The subring $\{A \in \mathbb{Q}[X] \mid A(n) \in \mathbb{Z} \text{ for every } n \in \mathbb{Z}\}$ of $\mathbb{Q}[X]$ is a binomial ring.

The proof of this proposition is easy and left to the reader. It is a known fact that the subring $\{A \in \mathbb{Q}[X] \mid A(n) \in \mathbb{Z} \text{ for every } n \in \mathbb{Z}\}$ of $\mathbb{Q}[X]$ is the free $\mathbb{Z}$-module with basis $\left(\binom{X}{0}, \binom{X}{1}, \binom{X}{2}, ...\right)$; this, however, is not needed in the proof.

Of course, every commutative $\mathbb{Q}$-algebra with unity itself is a binomial ring (because if A is a commutative $\mathbb{Q}$-algebra with unity, then $\left(\mathbb{N}_{+A}\right)^{-1} A = A$).

A crucial property of binomial rings is that they satisfy a generalization of Fermat's little theorem:

Theorem 8. Let A be a binomial ring. Let $p \in \mathbb{P}$. Let $a \in A$. Then, $a^p \equiv a \bmod pA$.

Theorem 8 is one of the fundamental properties of binomial rings. It appears in [4, Proposition 1.1], and also follows from the implication (1) $\Longrightarrow$ (4) in Theorem 4.1 in Jesse Elliott's paper [3]. We will reproduce the proof from [3] (in more details). The main ingredient of the proof of this theorem is the following fact about finite fields:

Proposition 9. Let $p \in \mathbb{P}$.

(a) Consider the polynomial ring $(\mathbb{Z}/(p\mathbb{Z}))[X]$ in one indeterminate X over $\mathbb{Z}/(p\mathbb{Z})$. Then, $\prod_{k=0}^{p-1} (X - k) = X^p - X$ in $(\mathbb{Z}/(p\mathbb{Z}))[X]$.

(b) Consider the polynomial ring $\mathbb{Z}[X]$ in one indeterminate X over $\mathbb{Z}$. Then, there exists some $Q \in \mathbb{Z}[X]$ such that $\prod_{k=0}^{p-1} (X - k) = X^p - X + pQ$ in $\mathbb{Z}[X]$.

Proof of Proposition 9. **(a)** Since $p \in \mathbb{P}$, it is clear that $\mathbb{Z} \diagup (p\mathbb{Z})$ is a field.

Define a polynomial $R \in (\mathbb{Z} \diagup (p\mathbb{Z}))[X]$ by

$$R = \prod_{k=0}^{p-1} (X - k) - (X^p - X).$$

This polynomial R has degree $\deg R \leq p-1$. (In fact, both polynomials $\prod_{k=0}^{p-1} (X-k)$ and $X^p - X$ have degree p and leading term X^p; hence, their leading terms cancel upon subtraction, and their difference R is a polynomial of degree $\leq p-1$.)

Let π be the canonical projection $\mathbb{Z} \to \mathbb{Z} \diagup (p\mathbb{Z})$. Clearly, π is a ring homomorphism, and we have $\operatorname{Ker} \pi = p\mathbb{Z}$.

We recall the following known fact:

Fact Pf9.1: Let F be a field, and let $P \in F[X]$ be a polynomial. If the polynomial P has more than $\deg P$ roots in F, then $P = 0$.

Now, let $\lambda \in \mathbb{Z} \diagup (p\mathbb{Z})$. Then, there exists some $\ell \in \{0, 1, ..., p-1\}$ such that λ is the residue class of ℓ modulo p. Consider this ℓ. Then, by the definition of π, we have $\pi(\ell) =$ (the residue class of ℓ modulo p) $= \lambda$. Hence, $\lambda - \pi(\ell) = 0$.

But since $\ell \in \{0, 1, ..., p-1\}$, it is clear that $\lambda - \pi(\ell)$ is a factor in the product $\prod_{k=0}^{p-1} (\lambda - \pi(k))$. Hence, at least one factor in the product $\prod_{k=0}^{p-1} (\lambda - \pi(k))$ is 0 (since $\lambda - \pi(\ell) = 0$). This yields that the whole product $\prod_{k=0}^{p-1} (\lambda - \pi(k))$ is 0 (because if one factor in a product is 0, then the whole product must be 0). We have thus shown that $\prod_{k=0}^{p-1} (\lambda - \pi(k)) = 0$.

Also, $\ell^p \equiv \ell \bmod p$ by Fermat's Little Theorem. Thus, $p \mid \ell^p - \ell$, so that $\ell^p - \ell \in p\mathbb{Z} = \operatorname{Ker} \pi$, hence $\pi(\ell^p - \ell) = 0$. Since

$$\begin{aligned} \pi(\ell^p - \ell) &= \left(\underbrace{\pi(\ell)}_{=\lambda} \right)^p - \underbrace{\pi(\ell)}_{=\lambda} \qquad \text{(since } \pi \text{ is a ring homomorphism)} \\ &= \lambda^p - \lambda, \end{aligned}$$

this rewrites as $\lambda^p - \lambda = 0$.

Now, since

$$R = \prod_{k=0}^{p-1} \left(X - \underbrace{k}_{=\pi(k)} \right) - (X^p - X) = \prod_{k=0}^{p-1} (X - \pi(k)) - (X^p - X),$$

we have

$$R(\lambda) = \underbrace{\prod_{k=0}^{p-1} (\lambda - \pi(k))}_{=0} - \underbrace{(\lambda^p - \lambda)}_{=0} = 0,$$

so that

$$\lambda \in \{x \in \mathbb{Z}/(p\mathbb{Z}) \mid R(x) = 0\} = (\text{the set of roots of the polynomial } R \text{ in } \mathbb{Z}/(p\mathbb{Z}))\,.$$

Now forget that we fixed λ. We thus have shown that every $\lambda \in \mathbb{Z}/(p\mathbb{Z})$ satisfies

$$\lambda \in (\text{the set of roots of the polynomial } R \text{ in } \mathbb{Z}/(p\mathbb{Z}))\,.$$

That is, every $\lambda \in \mathbb{Z}/(p\mathbb{Z})$ is a root of the polynomial R in $\mathbb{Z}/(p\mathbb{Z})$. Hence, there exist at least p roots of the polynomial R in $\mathbb{Z}/(p\mathbb{Z})$ (since there exist p elements of $\mathbb{Z}/(p\mathbb{Z})$). Since $p > p-1 \geq \deg R$, this yields that the polynomial R has more than $\deg R$ roots in $\mathbb{Z}/(p\mathbb{Z})$. Therefore, applying Fact Pf9.1 to $F = \mathbb{Z}/(p\mathbb{Z})$ and $P = R$, we obtain $R = 0$. Hence, $0 = R = \prod_{k=0}^{p-1}(X-k) - (X^p - X)$, so that $\prod_{k=0}^{p-1}(X-k) = X^p - X$ in $(\mathbb{Z}/(p\mathbb{Z}))[X]$. This proves Proposition 9 **(a)**.

(b) Let π be the canonical projection $\mathbb{Z} \to \mathbb{Z}/(p\mathbb{Z})$. Clearly, $\operatorname{Ker}\pi = p\mathbb{Z}$.

Consider the polynomial ring $\mathbb{Z}[X]$ in one indeterminate X over $\mathbb{Z}$, and the polynomial ring $(\mathbb{Z}/(p\mathbb{Z}))[X]$ in one indeterminate X over $\mathbb{Z}/(p\mathbb{Z})$. The canonical projection $\pi : \mathbb{Z} \to \mathbb{Z}/(p\mathbb{Z})$ induces a ring homomorphism $\pi[X] : \mathbb{Z}[X] \to (\mathbb{Z}/(p\mathbb{Z}))[X]$. We have $\operatorname{Ker}(\pi[X]) = p \cdot \mathbb{Z}[X]$.

By the definition of $\pi[X]$, we have $(\pi[X])(X) = X$.

Since $\pi[X]$ is a ring homomorphism, the polynomial $\prod_{k=0}^{p-1}(X-k) - (X^p - X) \in \mathbb{Z}[X]$ satisfies

$$\begin{aligned}
&(\pi[X])\left(\prod_{k=0}^{p-1}(X-k) - (X^p - X)\right) \\
&= \prod_{k=0}^{p-1}\left(\underbrace{(\pi[X])(X)}_{=X} - k\right) - \left(\left(\underbrace{(\pi[X])(X)}_{=X}\right)^p - \underbrace{(\pi[X])(X)}_{=X}\right) \\
&= \prod_{k=0}^{p-1}(X-k) - (X^p - X) = 0
\end{aligned}$$

(since Proposition 9 **(a)** yields $\prod_{k=0}^{p-1}(X-k) = X^p - X$ in $(\mathbb{Z}/(p\mathbb{Z}))[X]$). Hence, the polynomial $\prod_{k=0}^{p-1}(X-k) - (X^p - X) \in \mathbb{Z}[X]$ satisfies

$$\prod_{k=0}^{p-1}(X-k) - (X^p - X) \in \operatorname{Ker}(\pi[X]) = p \cdot \mathbb{Z}[X]\,.$$

In other words, there exists some $Q \in \mathbb{Z}[X]$ such that $\prod_{k=0}^{p-1}(X-k) - (X^p - X) = pQ$. In other words, there exists some $Q \in \mathbb{Z}[X]$ such that $\prod_{k=0}^{p-1}(X-k) = X^p - X + pQ$. This proves Proposition 9 **(b)**.

Proof of Theorem 8. We know that A is a binomial ring. Hence, by the definition of a binomial ring, for any $u \in A$ and any $r \in \mathbb{N}$, the element $\binom{u}{r} \in \left(\mathbb{N}_{+A}\right)^{-1} A$ lies in A. Applied to $u = a$ and $r = p$, this yields that the element $\binom{a}{p} \in \left(\mathbb{N}_{+A}\right)^{-1} A$ lies in A. By the definition of $\binom{a}{p}$, we have

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

(since $p \in \mathbb{N}$), so that

$$\frac{1}{p!} \prod_{k=0}^{p-1} (a-k) = \binom{a}{p} \in A.$$

Multiplying this with $p!$, we obtain

$$\prod_{k=0}^{p-1} (a-k) \in \underbrace{p!}_{=p(p-1)!} A = p \underbrace{(p-1)!A}_{\subseteq A} \subseteq pA.$$

Now, consider the polynomial ring $\mathbb{Z}[X]$ in one indeterminate X over $\mathbb{Z}$. Due to Proposition 9 **(b)**, there exists some $Q \in \mathbb{Z}[X]$ such that $\prod\limits_{k=0}^{p-1} (X-k) = X^p - X + pQ$ in $\mathbb{Z}[X]$. Consider this Q. Evaluating the polynomial identity $\prod\limits_{k=0}^{p-1} (X-k) = X^p - X + pQ$ at $X = q$, we obtain

$$\prod_{k=0}^{p-1} (a-k) = a^p - a + pQ(a),$$

so that

$$a^p - a = \underbrace{\prod_{k=0}^{p-1} (a-k)}_{\in pA} - p \underbrace{Q(a)}_{\in A} \in pA - pA \subseteq pA.$$

Hence, $a^p \equiv a \bmod pA$. This proves Theorem 8.

We will soon prove more properties of binomial rings. Let us first recall a known fact:

Proposition 10. Let A be a commutative ring with unity. Let $p \in \mathbb{P}$. Let $a \in A$ and $b \in A$. Then, $(a+b)^p \equiv a^p + b^p \bmod pA$.

Proof of Proposition 10. It is known that $p \mid \binom{p}{k}$ for every $k \in \{1, 2, ..., p-1\}$ (since p is prime). Thus, for every $k \in \{1, 2, ..., p-1\}$, there exists some $s \in \mathbb{Z}$ such that $\binom{p}{k} = ps$. Denote this s by s_k. Then, $s_k \in \mathbb{Z}$ satisfies $\binom{p}{k} = ps_k$ for every $k \in \{1, 2, ..., p-1\}$.

By the binomial formula,

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} = \underbrace{\binom{p}{0}}_{=1} \underbrace{a^0}_{=1} \underbrace{b^{p-0}}_{=b^p} + \sum_{k=1}^{p-1} \underbrace{\binom{p}{k}}_{\substack{=ps_k \\ \text{(since } k\in\{1,2,\ldots,p-1\}\text{)}}} a^k b^{p-k} + \underbrace{\binom{p}{p}}_{=1} a^p \underbrace{b^{p-p}}_{=b^0=1}$$

$$= b^p + \sum_{k=1}^{p-1} \underbrace{ps_k a^k b^{p-k}}_{\substack{\equiv 0 \bmod pA \\ \text{(since } ps_k a^k b^{p-k} \in pA\text{)}}} + a^p$$

$$\equiv b^p + \sum_{k=1}^{p-1} 0 + a^p = b^p + a^p = a^p + b^p \bmod pA.$$

This proves Proposition 10.

Lemma 11. Let A be a commutative ring with unity, and $p \in \mathbb{Z}$ be an integer[7]. 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 $a^{p^\ell} \equiv b^{p^\ell} \bmod p^{k+\ell} A$.

Lemma 11 is exactly Lemma 3 in [9], and thus will not be proven here. Now here is an important property of power series over binomial rings:

Theorem 12. Let Ξ be a family of symbols. Let A be a binomial ring. Let $u \in A$. Let $A\left[\left[\Xi\right]\right]$ denote the ring of power series in the indeterminates Ξ over A (just as $A\left[\Xi\right]$ denotes the ring of polynomials in the indeterminates Ξ over A). Let $P \in A\left[\left[\Xi\right]\right]$ be a power series with constant term 1. Then, the canonical embedding $A \to \left(\mathbb{N}_{+A}\right)^{-1} A$ induces a canonical embedding $A\left[\left[\Xi\right]\right] \to \left(\left(\mathbb{N}_{+A}\right)^{-1} A\right)\left[\left[\Xi\right]\right]$, which we will regard as an inclusion. Clearly, $P \in A\left[\left[\Xi\right]\right] \subseteq \left(\left(\mathbb{N}_{+A}\right)^{-1} A\right)\left[\left[\Xi\right]\right]$ and $u \in A \subseteq \left(\mathbb{N}_{+A}\right)^{-1} A$. Since $\left(\mathbb{N}_{+A}\right)^{-1} A$ is a $\mathbb{Q}$-algebra, a power series $P^u \in \left(\left(\mathbb{N}_{+A}\right)^{-1} A\right)\left[\left[\Xi\right]\right]$ is thus defined. This power series P^u lies in $A\left[\left[\Xi\right]\right]$.

Proof of Theorem 12. It is well-known that whenever B is a commutative $\mathbb{Q}$-algebra, v is an element of B, and $Q \in B\left[\left[\Xi\right]\right]$ is a power series with constant term 1, then a power series $Q^v \in B\left[\left[\Xi\right]\right]$ is defined. Applied to $B = \left(\left(\mathbb{N}_{+A}\right)^{-1} A\right)\left[\left[\Xi\right]\right]$, $v = u$ and $Q = P$, this yields that a power series $P^u \in \left(\left(\mathbb{N}_{+A}\right)^{-1} A\right)\left[\left[\Xi\right]\right]$ is defined. It remains to prove that this power series P^u lies in $A\left[\left[\Xi\right]\right]$.

Let C be the power series $P - 1 \in A\left[\left[\Xi\right]\right]$. Since the power series P has constant term 1, the power series $P - 1$ has constant term 0. In other words, the power series C has constant term 0 (since $C = P - 1$). Applying the binomial formula, we thus get

$$(1+C)^u = \sum_{r\in\mathbb{N}} \binom{u}{r} C^r, \tag{8}$$

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

where the sum on the right hand side converges because the power series C has constant term 0. But we know that $\dbinom{u}{r} \in A$ for every $u \in A$ and $r \in \mathbb{N}$ (since A is a binomial ring). Thus, every $r \in \mathbb{N}$ satisfies

$$\underbrace{\binom{u}{r}}_{\in A \subseteq A[[\Xi]]} \underbrace{C^r}_{\in A[[\Xi]]} \in A[[\Xi]] \cdot A[[\Xi]] \subseteq A[[\Xi]].$$

Hence, the equality (8) shows that $(1+C)^u$ is a convergent sum of power series in $A[[\Xi]]$. Hence, $(1+C)^u$ itself lies in $A[[\Xi]]$. Since $1+C = P$ (because $C = P-1$), we have thus shown that P^u lies in $A[[\Xi]]$. This proves Theorem 12.

Lemma 13. Let Ξ be a family of symbols. Let A be a binomial ring. Let $n \in \mathbb{Z}$. Let $u \in A$. Let $A[[\Xi]]$ denote the ring of power series in the indeterminates Ξ over A.

Let P and Q be two power series in $A[[\Xi]]$ with constant term 1. Assume that $P \equiv Q \bmod nA[[\Xi]]$. Then, $P^u \equiv Q^u \bmod nA[[\Xi]]$.

Proof of Lemma 13. The ideal $nA[[\Xi]]$ is closed with respect to the (Ξ)-adic topology on $A[[\Xi]]$. Hence, every sequence of elements of $nA[[\Xi]]$ which converges in $A[[\Xi]]$ has its limit lying in $nA[[\Xi]]$. Thus, every convergent infinite sum whose addends lie in $nA[[\Xi]]$ must itself lie in $nA[[\Xi]]$.

Now, let C be the power series $P - 1 \in A[[\Xi]]$. Since the power series P has constant term 1, the power series $P-1$ has constant term 0. In other words, the power series C has constant term 0 (since $C = P - 1$). Applying the binomial formula, we thus get

$$(1+C)^u = \sum_{r \in \mathbb{N}} \binom{u}{r} C^r, \tag{9}$$

where the sum on the right hand side converges because the power series C has constant term 0.

Also, let D be the power series $Q - 1 \in A[[\Xi]]$. Since the power series Q has constant term 1, the power series $Q-1$ has constant term 0. In other words, the power series D has constant term 0 (since $D = Q - 1$). Applying the binomial formula, we thus get

$$(1+D)^u = \sum_{r \in \mathbb{N}} \binom{u}{r} D^r, \tag{10}$$

where the sum on the right hand side converges because the power series D has constant term 0.

Subtracting (10) from (9), we obtain

$$(1+C)^u - (1+D)^u = \sum_{r \in \mathbb{N}} \binom{u}{r} C^r - \sum_{r \in \mathbb{N}} \binom{u}{r} D^r = \sum_{r \in \mathbb{N}} \binom{u}{r} \left(C^r - D^r\right). \tag{11}$$

Thus, the infinite sum $\sum_{r \in \mathbb{N}} \dbinom{u}{r} \left(C^r - D^r\right)$ converges.

Since $C = \underbrace{P}_{\equiv Q \bmod nA[[\Xi]]} - 1 \equiv Q - 1 = D \bmod nA[[\Xi]]$, we have $C^r \equiv D^r \bmod nA[[\Xi]]$ for every $r \in \mathbb{N}$. Thus, $C^r - D^r \in nA[[\Xi]]$ for every $r \in \mathbb{N}$. But we know that $\binom{u}{r} \in A$ for every $u \in A$ and $r \in \mathbb{N}$ (since A is a binomial ring). Thus,

$$\underbrace{\binom{u}{r}}_{\in A} \underbrace{\left(C^r - D^r\right)}_{\in nA[[\Xi]]} \in A \cdot nA[[\Xi]] = n \cdot \underbrace{A \cdot A[[\Xi]]}_{\subseteq A[[\Xi]]} \subseteq nA[[\Xi]]$$

for every $r \in \mathbb{N}$. Hence, $\sum_{r \in \mathbb{N}} \binom{u}{r} \left(C^r - D^r\right) \in nA[[\Xi]]$ (since every convergent infinite sum whose addends lie in $nA[[\Xi]]$ must itself lie in $nA[[\Xi]]$). Due to (11), this rewrites as $(1+C)^u - (1+D)^u \in nA[[\Xi]]$. Since $1 + C = P$ (because $C = P - 1$) and $1 + D = Q$ (because $D = Q - 1$), this rewrites as $P^u - Q^u \in nA[[\Xi]]$. In other words, $P^u \equiv Q^u \bmod nA[[\Xi]]$. Lemma 13 is thus proven.

Lemma 14. Let X be a symbol. Let A be a binomial ring. Let $p \in \mathbb{P}$. Let $A[[X]]$ denote the ring of power series in the indeterminate X over A.

(a) The power series $1 + X$ and $1 + X^p$ have constant term 1. Thus, the power series $(1+X)^u$ and $(1+X^p)^u$ are well-defined and lie in $A[[X]]$ for every $u \in A$.

(b) We have $(1+X^p)^{qn/p} \equiv (1+X)^{qn} \bmod p^{v_p(n)} A[[X]]$ for every $n \in p\mathbb{N}_+$ and $q \in A$.

Proof of Lemma 14. It is clear that the power series $1 + X$ and $1 + X^p$ have constant term 1 (since $p > 0$).

(a) Let $u \in A$. Applying Theorem 12 to $P = 1 + X$ and $\Xi = (X)$, we conclude that the power series $(1+X)^u$ is well-defined and lies in $A[[X]]$. Applying Theorem 12 to $P = 1 + X^p$ and $\Xi = (X)$, we conclude that the power series $(1+X^p)^u$ is well-defined and lies in $A[[X]]$. This proves Lemma 14 **(a)**.

(b) Let $n \in p\mathbb{N}_+$ and $q \in A$. We need to prove that $(1+X^p)^{qn/p} \equiv (1+X)^{qn} \bmod p^{v_p(n)} A[[X]]$.

We defined $v_p(n)$ as the largest nonnegative integer m satisfying $p^m \mid n$. Thus, $p^{v_p(n)} \mid n$. Hence, there exists a $z \in \mathbb{Z}$ such that $n = z p^{v_p(n)}$. Consider this z. Since $z p^{v_p(n)} = n \in p\mathbb{N}_+ \subseteq \mathbb{N}_+$, we have $z \in \mathbb{N}_+$.

Since $n \in p\mathbb{N}_+$, we have $n/p \in \mathbb{N}_+$, so that $v_p(n/p) \geq 0$. Thus, $v_p(n/p)$ is a nonnegative integer. Denote this nonnegative integer $v_p(n/p)$ by ℓ. Then, $\ell = v_p(n/p) \geq 0$.

Applying Proposition 10 to $A[[X]]$, 1 and X instead of A, a and b, we obtain $(1+X)^p \equiv 1^p + X^p \bmod pA[[X]]$. Since $1^p = 1$ and $p = p^1$, this rewrites as $(1+X)^p \equiv 1 + X^p \bmod p^1 A[[X]]$. Hence, Lemma 11 (applied to $A[[X]]$, 1, $(1+X)^p$ and $1 + X^p$ instead of A, k, a and b) yields that

$$((1+X)^p)^{p^\ell} \equiv (1+X^p)^{p^\ell} \bmod p^{1+\ell} A[[X]].$$

Since $((1+X)^p)^{p^\ell} = (1+X)^{pp^\ell} = (1+X)^{p^{1+\ell}}$ (because $pp^\ell = p^1 p^\ell = p^{1+\ell}$), this rewrites as

$$(1+X)^{p^{1+\ell}} \equiv (1+X^p)^{p^\ell} \bmod p^{1+\ell} A\left[[X]\right]. \tag{12}$$

Let Ξ be the one-element family (X) of indeterminates. Then, $A\left[[\Xi]\right] = A\left[[X]\right]$. Hence, (12) rewrites as

$$(1+X)^{p^{1+\ell}} \equiv (1+X^p)^{p^\ell} \bmod p^{1+\ell} A\left[[\Xi]\right].$$

Hence, Lemma 13 (applied to qz, $p^{1+\ell}$, $(1+X)^{p^{1+\ell}}$ and $(1+X^p)^{p^\ell}$ instead of u, n, P and Q) yields

$$\left((1+X)^{p^{1+\ell}}\right)^{qz} \equiv \left((1+X^p)^{p^\ell}\right)^{qz} \bmod p^{1+\ell} A\left[[\Xi]\right].$$

Since $\left((1+X)^{p^{1+\ell}}\right)^{qz} = (1+X)^{p^{1+\ell} qz}$ and $\left((1+X^p)^{p^\ell}\right)^{qz} = (1+X^p)^{p^\ell qz}$, this rewrites as

$$(1+X)^{p^{1+\ell} qz} \equiv (1+X^p)^{p^\ell qz} \bmod p^{1+\ell} A\left[[\Xi]\right]. \tag{13}$$

But

$$\underbrace{1}_{=v_p(p)} + \underbrace{\ell}_{=v_p(n/p)} = v_p(p) + v_p(n/p) = v_p\left(\underbrace{p \cdot (n/p)}_{=n}\right) = v_p(n),$$

so that

$$p^{1+\ell} qz = p^{v_p(n)} qz = q \underbrace{z p^{v_p(n)}}_{=n} = qn \tag{14}$$

and thus

$$\underbrace{p^\ell}_{=\frac{1}{p} p^{\ell+1}} qz = \frac{1}{p} \underbrace{p^{\ell+1} qz}_{=qn} = qn/p. \tag{15}$$

Due to (14) and (15), the congruence (13) rewrites as

$$(1+X)^{qn} \equiv (1+X^p)^{qn/p} \bmod p^{1+\ell} A\left[[\Xi]\right].$$

Due to $1+\ell = v_p(n)$ and $A\left[[\Xi]\right] = A\left[[X]\right]$, this rewrites as $(1+X)^{qn} \equiv (1+X^p)^{qn/p} \bmod p^{v_p(n)} A\left[[X]\right]$. This proves Lemma 14 **(b)**.

Using Lemma 14, we can now show a congruence property of binomial coefficients with "numerator" in a binomial ring:

Lemma 15. Let A be a binomial ring. Let $n \in \mathbb{N}_+$ and let $p \in \operatorname{PF} n$. Let $q \in A$ and $r \in \mathbb{Q}$. Then,

$$\binom{qn/p}{rn/p} \equiv \binom{qn}{rn} \bmod p^{v_p(n)} A. \tag{16}$$

This Lemma 15 is a generalization of Lemma 19 from [5]. In fact, since $\mathbb{Z}$ is a binomial ring, we can apply Lemma 15 to $A = \mathbb{Z}$, and obtain precisely Lemma 19 from [5].

It should be said that Lemma 15 is nothing like a novel result. Indeed, it is well-known in the case when $A = \mathbb{Z}$, and in the general case it follows from the known fact that, loosely speaking, any divisibility of a polynomial by an integer which holds everywhere in $\mathbb{Z}$ must hold everywhere in any binomial ring. This known fact is, e. g., a consequence of the implication (1) $\Longrightarrow$ (2) of Theorem 4.1 in Elliott's paper [3] (to which I also refer the reader for a precise statement).

Also, in most cases, the exponent $v_p(n)$ in (16) can be replaced by larger numbers. Details can be found by searching the internet for "Jacobsthal's congruence". Again, the case $A = \mathbb{Z}$ is "the worst case" in the sense that divisibilities that hold in this case must hold always in binomial rings. We will, however, never need these stronger results.

Proof of Lemma 15. Since $p \in \operatorname{PF} n$, we know that p is a prime and satisfies $p \mid n$. Thus, $p \in \mathbb{P}$ (since p is a prime). Also, $n \in p\mathbb{N}_+$ (since $n \in \mathbb{N}_+$ and $p \mid n$), so that $n/p \in \mathbb{N}_+$.

If $rn \notin \mathbb{N}$, then Lemma 15 is easily seen to be true.[8] 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 $r \geq 0$.

Set $m = qn$. Lemma 14 yields $(1 + X^p)^{qn/p} \equiv (1 + X)^{qn} \bmod p^{v_p(n)} A\left[[X]\right]$. Since $qn = m$, this rewrites as $(1 + X^p)^{m/p} \equiv (1 + X)^m \bmod p^{v_p(n)} A\left[[X]\right]$. Hence, for every $\lambda \in \mathbb{N}$, we have

$$\begin{aligned}&\Big(\text{the coefficient of the power series } (1 + X^p)^{m/p} \text{ before } X^\lambda\Big) \\ &\equiv \big(\text{the coefficient of the power series } (1 + X)^m \text{ before } X^\lambda\big) \bmod p^{v_p(n)} A. \end{aligned} \tag{17}$$

But it is easy to see that

$$\sum_{\lambda \in \mathbb{N}} \binom{m/p}{\lambda/p} X^\lambda = \sum_{\lambda \in p\mathbb{N}} \binom{m/p}{\lambda/p} X^\lambda \tag{18}$$

[8] *Proof.* Assume that $rn \notin \mathbb{N}$. Then, $rn/p \notin \mathbb{N}$ as well (since $p \in \mathbb{N}_+$). Hence, both sides of (16) vanish. Thus, (16) holds, i. e., Lemma 15 is true, qed.

[9]. However, the binomial formula yields

$$\begin{aligned}
&(1+X^p)^{m/p} \\
&= \sum_{\mu\in\mathbb{N}} \underbrace{\binom{m/p}{\mu}}_{=\binom{m/p}{p\mu/p}} \underbrace{(X^p)^\mu}_{=X^{p\mu}} = \sum_{\mu\in\mathbb{N}} \binom{m/p}{p\mu/p} X^{p\mu} = \sum_{\lambda\in p\mathbb{N}} \binom{m/p}{\lambda/p} X^\lambda \\
&\qquad \text{(here we substituted } \lambda \text{ for } p\mu\text{, since the map } \mathbb{N}\to p\mathbb{N},\ \mu\mapsto p\mu \text{ is a bijection)} \\
&= \sum_{\lambda\in\mathbb{N}} \binom{m/p}{\lambda/p} X^\lambda \qquad \text{(by (18))}\,,
\end{aligned}$$

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

$$\Big(\text{the coefficient of the power series } (1+X^p)^{m/p} \text{ before } X^\lambda\Big) = \binom{m/p}{\lambda/p}. \quad (19)$$

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

$$\big(\text{the coefficient of the power series } (1+X)^m \text{ before } X^\lambda\big) = \binom{m}{\lambda}. \qquad (20)$$

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

$$\begin{aligned}
\binom{m/p}{\lambda/p} &= \Big(\text{the coefficient of the power series } (1+X^p)^{m/p} \text{ before } X^\lambda\Big) \qquad \text{(by (19))} \\
&\equiv \big(\text{the coefficient of the power series } (1+X)^m \text{ before } X^\lambda\big) \qquad \text{(by (17))} \\
&= \binom{m}{\lambda} \bmod p^{v_p(n)}A \qquad \text{(by (20))}\,.
\end{aligned}$$

---

[9] *Proof of (18):* Every $\lambda\in\mathbb{N}\setminus(p\mathbb{N})$ satisfies $\lambda\notin p\mathbb{N}$. Hence, every $\lambda\in\mathbb{N}\setminus(p\mathbb{N})$ satisfies $\lambda/p\notin\mathbb{N}$. Thus, every $\lambda\in\mathbb{N}\setminus(p\mathbb{N})$ satisfies

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

(since $\lambda/p\notin\mathbb{N}$). Thus, $\sum\limits_{\lambda\in\mathbb{N}\setminus(p\mathbb{N})} \underbrace{\binom{m/p}{\lambda/p}}_{\substack{=0\\ (\text{since } \lambda\in\mathbb{N}\setminus(p\mathbb{N}))}} X^\lambda = \sum\limits_{\lambda\in\mathbb{N}\setminus(p\mathbb{N})} 0X^\lambda = 0.$

Now, $p\mathbb{N}\subseteq\mathbb{N}$, so that the sum $\sum\limits_{\lambda\in\mathbb{N}}\binom{m/p}{\lambda/p}X^\lambda$ decomposes as

$$\sum_{\lambda\in\mathbb{N}}\binom{m/p}{\lambda/p}X^\lambda = \sum_{\lambda\in p\mathbb{N}}\binom{m/p}{\lambda/p}X^\lambda + \underbrace{\sum_{\lambda\in\mathbb{N}\setminus p\mathbb{N}}\binom{m/p}{\lambda/p}X^\lambda}_{=0} = \sum_{\lambda\in p\mathbb{N}}\binom{m/p}{\lambda/p}X^\lambda.$$

This proves (18).

Since $m = qn$, this becomes

$$\binom{qn/p}{\lambda/p} \equiv \binom{qn}{\lambda} \bmod p^{v_p(n)} A.$$

Applying this to $\lambda = rn$, we obtain (16), and thus Lemma 15 is proven.

Here comes a result similar to, but somewhat more interesting than, Lemma 15:

Lemma 16. Let A be a binomial ring. Let $n \in \mathbb{N}_+$ and let $p \in \operatorname{PF} n$. Let $q \in A$ and $r \in \mathbb{Q}$. Assume that there exist two integers α and β with $v_p(\alpha) \geq v_p(\beta)$ and $r = \dfrac{\alpha}{\beta}$. Then,

$$\binom{qn/p-1}{rn/p-1} \equiv \binom{qn-1}{rn-1} \bmod p^{v_p(n)} A. \tag{21}$$

This Lemma 16 is a generalization of Lemma 21 from [5]. In fact, since $\mathbb{Z}$ is a binomial ring, we can apply Lemma 16 to $A = \mathbb{Z}$, and obtain precisely Lemma 21 from [5].

It seems impossible to prove Lemma 16 by generalizing the proof of Lemma 21 in [5]. However, the we can prove Lemma 16 in a different way. It requires two lemmas. The first one is a very basic one about binomial coefficients in binomial rings:

Lemma 17. Let A be a binomial ring. Let $u \in A$. Let $r \in \mathbb{Q}$. Then,

$$\binom{u}{r} = \binom{u-1}{r-1} + \binom{u-1}{r}.$$

When applied to $A = \mathbb{Z}$, Lemma 17 yields the standard recursion of the binomial coefficients.

Proof of Lemma 17. If $r \notin \mathbb{N}$, then Lemma 17 is easily proven[10]. Hence, for the rest of this proof, we can WLOG assume that $r \in \mathbb{N}$. Assume this.

If $r = 0$, then Lemma 17 is also obvious[11]. Hence, for the rest of this proof, we can WLOG assume that $r \neq 0$. Assume this.

Since $r \in \mathbb{N}$ and $r \neq 0$, we have $r \in \mathbb{N}_+$ and thus $r - 1 \in \mathbb{N}$.

[10] *Proof.* Assume that $r \notin \mathbb{N}$. Then, $r - 1 \notin \mathbb{N}$ as well. This causes the binomial coefficient $\binom{u-1}{r-1}$ to vanish, while $r \notin \mathbb{N}$ shows that the binomial coefficients $\binom{u}{r}$ and $\binom{u-1}{r}$ vanish as well. Hence, the equation that needs to be proven ($\binom{u}{r} = \binom{u-1}{r-1} + \binom{u-1}{r}$) reduces to $0 = 0 + 0$, which is tautological. Thus, Lemma 17 is proven if $r \notin \mathbb{N}$.

[11] *Proof.* Assume that $r = 0$. Then, $r - 1 = -1 \notin \mathbb{N}$, so that the binomial coefficient $\binom{u-1}{r-1}$ vanishes. On the other hand, $\binom{u}{0}$ and $\binom{u-1}{0}$ both equal 1, since we have $\binom{x}{0} = 1$ for every

By the definition of $\binom{u}{r}$, we have

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

$$= \frac{1}{r!}\underbrace{(u-0)}_{=u}\prod_{k=1}^{r-1}(u-k) = \frac{1}{r!}u\prod_{k=1}^{r-1}(u-k) = \frac{1}{r!}u\prod_{k=0}^{r-2}\underbrace{(u-(k+1))}_{=(u-1)-k}$$

(here, we substituted $k+1$ for k in the product)

$$= \frac{1}{r!}u\prod_{k=0}^{r-2}((u-1)-k). \tag{22}$$

By the definition of $\binom{u-1}{r}$, we have

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

$$= \frac{1}{r!}\underbrace{\prod_{k=0}^{r-1}((u-1)-k)}_{=((u-1)-(r-1))\prod\limits_{k=0}^{r-2}((u-1)-k)} \qquad \text{(since } r \in \mathbb{N}\text{)}$$

$$= \frac{1}{r!}\underbrace{((u-1)-(r-1))}_{=u-r}\prod_{k=0}^{r-2}((u-1)-k)$$

$$= \frac{1}{r!}(u-r)\prod_{k=0}^{r-2}((u-1)-k).$$

$x \in A$ (this follows readily from the definition of $\binom{x}{0}$). Now, since $r = 0$, we have

$$\binom{u}{r} - \binom{u-1}{r} = \underbrace{\binom{u}{0}}_{=1} - \underbrace{\binom{u-1}{0}}_{=1} = 1 - 1 = 0.$$

Compared with $\binom{u-1}{r-1} = 0$, this yields $\binom{u-1}{r-1} = \binom{u}{r} - \binom{u-r}{r}$. Thus, $\binom{u}{r} = \binom{u-1}{r-1} + \binom{u-1}{r}$. Hence, Lemma 17 is proven in the case when $r = 0$.

Subtracting this equation from (22), we obtain

$$\begin{aligned}
\binom{u}{r} - \binom{u-1}{r} &= \frac{1}{r!} u \prod_{k=0}^{r-2} ((u-1)-k) - \frac{1}{r!} (u-r) \prod_{k=0}^{r-2} ((u-1)-k) \\
&= \frac{1}{r!} \underbrace{(u-(u-r))}_{=r} \prod_{k=0}^{r-2} ((u-1)-k) = \underbrace{\frac{1}{r!} r}_{\substack{= \frac{1}{(r-1)!} \\ \text{(since } r! = r \cdot (r-1)!\text{)}}} \underbrace{\prod_{k=0}^{r-2}}_{= \prod_{k=0}^{(r-1)-1}} ((u-1)-k) \\
&= \frac{1}{(r-1)!} \prod_{k=0}^{r-2} ((u-1)-k) \,. \qquad (23)
\end{aligned}$$

On the other hand, the definition of $\binom{u-1}{r-1}$ yields

$$\begin{aligned}
\binom{u-1}{r-1} &= \begin{cases} \dfrac{1}{(r-1)!} \displaystyle\prod_{k=0}^{(r-1)-1} ((u-1)-k) \,, & \text{if } r-1 \in \mathbb{N}; \\ 0, & \text{if } r-1 \notin \mathbb{N} \end{cases} \\
&= \frac{1}{(r-1)!} \prod_{k=0}^{(r-1)-1} ((u-1)-k) \qquad (\text{since } r-1 \in \mathbb{N}) \\
&= \binom{u}{r} - \binom{u-1}{r} \qquad (\text{by (23)}) \,,
\end{aligned}$$

so that $\binom{u}{r} = \binom{u-1}{r-1} + \binom{u-1}{r}$. Thus, Lemma 17 is proven.

We are not yet completely ready to prove Lemma 16; we still need the following fact (which we will also use independently):

Lemma 18. Let A be a binomial ring. Let $n \in \mathbb{N}_+$ and let $p \in \operatorname{PF} n$. Let $q \in A$. Then,

$$q^n \equiv q^{n/p} \bmod p^{v_p(n)} A.$$

Proof of Lemma 18. Since $p \in \operatorname{PF} n$, we know that p is a prime and satisfies $p \mid n$. Thus, $p \in \mathbb{P}$ (since p is a prime). Also, $n \in p\mathbb{N}_+$ (since $n \in \mathbb{N}_+$ and $p \mid n$), so that $n/p \in \mathbb{N}_+$.

We defined $v_p(n)$ as the largest nonnegative integer m satisfying $p^m \mid n$. Thus, $p^{v_p(n)} \mid n$. Hence, there exists a $z \in \mathbb{Z}$ such that $n = z p^{v_p(n)}$. Consider this z. Since $z p^{v_p(n)} = n \in p\mathbb{N}_+ \subseteq \mathbb{N}_+$, we have $z \in \mathbb{N}_+$.

We have $n/p \in \mathbb{N}_+$, so that $v_p(n/p) \geq 0$. Thus, $v_p(n/p)$ is a nonnegative integer. Denote this nonnegative integer $v_p(n/p)$ by ℓ. Then, $\ell = v_p(n/p) \geq 0$.

Now, $v_p(p) + v_p(n/p) = v_p\left(\underbrace{p \cdot (n/p)}_{=n}\right) = v_p(n)$. Since $v_p(p) = 1$ and $v_p(n/p) = \ell$, this rewrites as $1 + \ell = v_p(n)$. Thus, $p^{1+\ell} = p^{v_p(n)}$, so that

$$p^{1+\ell} z = p^{v_p(n)} z = z p^{v_p(n)} = n. \qquad (24)$$

Also, $\underbrace{p}_{=p^1} p^\ell = p^1 p^\ell = p^{1+\ell}$, so that $pp^\ell z = p^{1+\ell} z = n$ (by (24)) and thus

$$p^\ell z = n/p. \tag{25}$$

Theorem 8 (applied to $a = q$) yields $q^p \equiv q \bmod pA$. In other words, $q^p \equiv q \bmod p^1 A$ (since $p = p^1$). Lemma 11 (applied to $k = 1$, $a = q^p$ and $b = q$) thus yields $(q^p)^{p^\ell} \equiv q^{p^\ell} \bmod p^{1+\ell} A$. Since $(q^p)^{p^\ell} = q^{pp^\ell} = q^{p^{1+\ell}}$ (because $pp^\ell = p^1 p^\ell = p^{1+\ell}$), this rewrites as $q^{p^{1+\ell}} \equiv q^{p^\ell} \bmod p^{1+\ell} A$. Since $1 + \ell = v_p(n)$, this rewrites as $q^{p^{v_p(n)}} \equiv q^{p^\ell} \bmod p^{v_p(n)} A$. Taking the z-th power of this congruence, we obtain

$$\left(q^{p^{v_p(n)}}\right)^z \equiv \left(q^{p^\ell}\right)^z \bmod p^{v_p(n)} A.$$

But since

$$\left(q^{p^{v_p(n)}}\right)^z = q^{p^{v_p(n)} z} = q^n \qquad \left(\text{since } p^{v_p(n)} z = z p^{v_p(n)} = n\right)$$

and

$$\left(q^{p^\ell}\right)^z = q^{p^\ell z} = q^{n/p} \qquad \left(\text{since } p^\ell z = n/p \text{ (by (25))}\right),$$

this rewrites as $q^n \equiv q^{n/p} \bmod p^{v_p(n)} A$. This proves Lemma 18.

Proof of Lemma 16. Since $p \in \operatorname{PF} n$, we know that p is a prime and satisfies $p \mid n$. Thus, $p \in \mathbb{P}$ (since p is a prime). Also, $n \in p\mathbb{N}_+$ (since $n \in \mathbb{N}_+$ and $p \mid n$), so that $n/p \in \mathbb{N}_+$.

Lemma 16 is readily seen to hold if $rn \notin \mathbb{N}_+$. [12] 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 $rn > 0$. Combined with $n > 0$, this yields $r > 0$.

It is easy to see that there exist two **coprime** integers α' and β' such that $\beta' \perp p$ and $r = \dfrac{\alpha'}{\beta'}$ [13]. Consider these α' and β'.

---

[12] *Proof.* Assume that $rn \notin \mathbb{N}_+$. Then, $rn/p \notin \mathbb{N}_+$. Hence, neither $rn - 1$ nor $rn/p - 1$ lies in $\mathbb{N}$. Consequently, both sides of (21) vanish, so that (21) is trivially satisfied. Thus, Lemma 16 is proven if $rn \notin \mathbb{N}_+$.

[13] *Proof.* By assumption, there exist two integers α and β with $v_p(\alpha) \geq v_p(\beta)$ and $r = \dfrac{\alpha}{\beta}$. Consider these α and β. Since $\dfrac{\alpha}{\beta} = r > 0$, both α and β are nonzero. Thus, $v_p(\alpha)$ and $v_p(\beta)$ are well-defined nonnegative integers (not ∞). Now, let $h = \gcd(\alpha, \beta)$. Then, $h = \gcd(\alpha, \beta) \mid \alpha$, so that $\dfrac{\alpha}{h} \in \mathbb{Z}$. Also, $h = \gcd(\alpha, \beta) \mid \beta$, so that $\dfrac{\beta}{h} \in \mathbb{Z}$. Since $\alpha \neq 0$ and $\beta \neq 0$, we have $\gcd(\alpha, \beta) \neq 0$, so that $h = \gcd(\alpha, \beta) \neq 0$. Thus, $v_p(h)$ is a well-defined nonnegative integer (not ∞).

Since

$$\gcd\left(\frac{\alpha}{h}, \frac{\beta}{h}\right) = \frac{\gcd(\alpha, \beta)}{h} = \frac{h}{h} \qquad (\text{since } \gcd(\alpha, \beta) = h)$$
$$= 1,$$

the integers $\dfrac{\alpha}{h}$ and $\dfrac{\beta}{h}$ are coprime. That is, $\dfrac{\alpha}{h} \perp \dfrac{\beta}{h}$.

Since $\alpha = \dfrac{\alpha}{h} \cdot h$, we have $v_p(\alpha) = v_p\left(\dfrac{\alpha}{h} \cdot h\right) = v_p\left(\dfrac{\alpha}{h}\right) + v_p(h)$. Since $\beta = \dfrac{\beta}{h} \cdot h$, we have

Recall that $rn \in \mathbb{N}_+ \subseteq \mathbb{Z}$. Since $r = \dfrac{\alpha'}{\beta'}$, this rewrites as $\dfrac{\alpha'}{\beta'} n \in \mathbb{Z}$. In other words, $\dfrac{\alpha' n}{\beta'} \in \mathbb{Z}$. In other words, $\beta' \mid \alpha' n$. But $\beta' \perp \alpha'$ (since α' and β' are coprime).

It is known that if x, y and z are three integers such that $x \perp y$ and $x \mid yz$, then $x \mid z$. Applying this to $x = \beta'$, $y = \alpha'$ and $z = n$, we obtain $\beta' \mid n$. Hence, $\dfrac{n}{\beta'}$ is an integer. Denote this integer by g. Then, $|g|$ is a nonnegative integer. Moreover, $g = \dfrac{n}{\beta'} \neq 0$ (since $n \neq 0$), so that $|g| > 0$. Thus, $|g|$ is a positive integer. In other words, $|g| \in \mathbb{N}_+$.

We have

$$|\alpha'| \cdot |g| = \left| \alpha' \underbrace{g}_{= \frac{n}{\beta'}} \right| = \left| \underbrace{\alpha' \cdot \frac{n}{\beta'}}_{= \frac{\alpha'}{\beta'} \cdot n} \right| = \left| \underbrace{\frac{\alpha'}{\beta'}}_{=r} \cdot n \right| = |rn| = rn \qquad \text{(since } rn > 0\text{)} \quad (26)$$

$v_p(\beta) = v_p\left(\dfrac{\beta}{h} \cdot h\right) = v_p\left(\dfrac{\beta}{h}\right) + v_p(h)$. Now,

$$v_p\left(\frac{\alpha}{h}\right) + v_p(h) = v_p(\alpha) \geq v_p(\beta) = v_p\left(\frac{\beta}{h}\right) + v_p(h).$$

Subtracting the nonnegative integer $v_p(h)$ from this inequality, we obtain $v_p\left(\dfrac{\alpha}{h}\right) \geq v_p\left(\dfrac{\beta}{h}\right)$.

Now, assume (for the sake of contradiction) that we don't have $\dfrac{\beta}{h} \perp p$. Then, $p \mid \dfrac{\beta}{h}$ (since p is a prime), so that $v_p\left(\dfrac{\beta}{h}\right) \geq 1$. Consequently, $v_p\left(\dfrac{\alpha}{h}\right) \geq v_p\left(\dfrac{\beta}{h}\right) \geq 1$, and thus $p \mid \dfrac{\alpha}{h}$. Now, p is a common divisor of $\dfrac{\alpha}{h}$ and $\dfrac{\beta}{h}$ (since $p \mid \dfrac{\alpha}{h}$ and $p \mid \dfrac{\beta}{h}$). Since p is a prime, this yields that $\dfrac{\alpha}{h}$ and $\dfrac{\beta}{h}$ have a common prime divisor. But this is clearly absurd (since $\dfrac{\alpha}{h}$ and $\dfrac{\beta}{h}$ are coprime). This contradiction shows that our assumption (that we don't have $\dfrac{\beta}{h} \perp p$) was wrong. Hence, we have $\dfrac{\beta}{h} \perp p$.

Finally, $\dfrac{\left(\dfrac{\alpha}{h}\right)}{\left(\dfrac{\beta}{h}\right)} = \dfrac{\alpha}{\beta} = r$, so that $r = \dfrac{\left(\dfrac{\alpha}{h}\right)}{\left(\dfrac{\beta}{h}\right)}$.

Altogether, we know that $\dfrac{\alpha}{h}$ and $\dfrac{\beta}{h}$ are two coprime integers such that $\dfrac{\beta}{h} \perp p$ and $r = \dfrac{\left(\dfrac{\alpha}{h}\right)}{\left(\dfrac{\beta}{h}\right)}$. Hence, there exist two integers α' and β' such that $\beta' \perp p$ and $r = \dfrac{\alpha'}{\beta'}$ (namely, $\alpha' = \dfrac{\alpha}{h}$ and $\beta' = \dfrac{\beta}{h}$), qed.

and

$$|\beta'|\,q\cdot|g| = \underbrace{|\beta'|\cdot|g|}_{=|\beta'\cdot g|}\,q = \left|\beta'\cdot\underbrace{g}_{=\frac{n}{\beta'}}\right| q = \left|\underbrace{\beta'\cdot\frac{n}{\beta'}}_{=n}\right| q = \underbrace{|n|}_{\substack{=n\\(\text{since } n>0)}}\ q = nq = qn. \quad (27)$$

Since $|\alpha'| \in \mathbb{Z}$ (because $\alpha' \in \mathbb{Z}$), we can view $|\alpha'|$ as an element of A. Also, since $|\beta'| \in \mathbb{Z}$ (because $\beta' \in \mathbb{Z}$), the element $|\beta'|\,q$ of A is well-defined. Hence, $|\alpha'| - |\beta'|\,q$ is an element of A.

It is known that if x, y and z are three integers such that $x \perp y$, $x \mid z$ and $y \mid z$, then $xy \mid z$. Applying this to $x = \beta'$, $y = p$ and $z = n$, we obtain $\beta' p \mid n$. Thus, $\dfrac{n}{\beta' p} \in \mathbb{Z}$. Hence, g is divisible by p (since g is an integer and satisfies $g \diagup p = \dfrac{n}{\beta'} \diagup p = \dfrac{n}{\beta' p} \in \mathbb{Z}$). That is, $p \mid g$. Combined with $g \mid |g|$ (because $|g|$ equals either g or $-g$), this yields $p \mid g \mid |g|$. Since p is a prime, this means that p is a prime divisor of $|g|$. In other words, $p \in \operatorname{PF}(|g|)$.

Now, we can apply Lemma 15 to $|\alpha'| - |\beta'|\,q$, $|\alpha'|$ and $|g|$ instead of q, r and n (because $|g| \in \mathbb{N}_+$ and $p \in \operatorname{PF}(|g|)$). As a result, we obtain

$$\binom{(|\alpha'| - |\beta'|\,q)\cdot|g| \diagup p}{|\alpha'|\cdot|g| \diagup p} \equiv \binom{(|\alpha'| - |\beta'|\,q)\cdot|g|}{|\alpha'|\cdot|g|} \bmod p^{v_p(|g|)}A.$$

Since

$$(|\alpha'| - |\beta'|\,q)\cdot|g| = \underbrace{|\alpha'|\cdot|g|}_{\substack{=rn\\(\text{by (26)})}} - \underbrace{|\beta'|\,q\cdot|g|}_{\substack{=qn\\(\text{by (27)})}} = rn - qn$$

and $|\alpha'|\cdot|g| = rn$ (by (26)), this congruence rewrites as

$$\binom{(rn-qn) \diagup p}{rn \diagup p} \equiv \binom{rn-qn}{rn} \bmod p^{v_p(|g|)}A. \quad (28)$$

Since $\beta' \perp p$, we have $p \nmid \beta'$ (because p is prime), so that $v_p(\beta') = 0$. But $g = \dfrac{n}{\beta'}$, so that $n = g\beta'$ and thus

$$v_p(n) = v_p(g\beta') = v_p(g) + \underbrace{v_p(\beta')}_{=0} = v_p(g).$$

Since $v_p(g) = v_p(|g|)$ [14], this rewrites as

$$v_p(n) = v_p(|g|). \quad (29)$$

[14] *Proof.* If $g \geq 0$, then $g = |g|$, so that $v_p(g) = v_p(|g|)$. Hence, for the rest of the proof of $v_p(g) = v_p(|g|)$, we can WLOG assume that we don't have $g \geq 0$. Assume this. Then, $g < 0$, so that $|g| = -g = (-1)\,g$. Hence, $v_p(|g|) = v_p((-1)\,g) = \underbrace{v_p(-1)}_{\substack{=0\\(\text{since } p\nmid -1)}} + v_p(g) = v_p(g)$, qed.

Hence, (28) rewrites as

$$\binom{(rn-qn)\,/\,p}{rn/p} \equiv \binom{rn-qn}{rn} \bmod p^{v_p(n)} A. \tag{30}$$

On the other hand, recall that $rn \in \mathbb{N}_+$, so that $rn-1 \in \mathbb{N}$. Thus, $(-1)^{rn-1}$ is well-defined. Moreover, $p \mid |g| \mid |\alpha'| \cdot |g| = rn$, so that rn/p is an integer. Thus, $(-1)^{rn/p-1}$ is well-defined. Now, it is easy to see that

$$(-1)^{rn/p} \equiv (-1)^{rn} \bmod p^{v_p(n)} A. \tag{31}$$

[15]

We have $rn \in \mathbb{N}_+ \subseteq \mathbb{Z}$. Thus, Proposition 6 (applied to $qn-1$ and rn instead of u and r) yields

$$\begin{aligned}\binom{qn-1}{rn} &= (-1)^{rn} \binom{rn-(qn-1)-1}{rn} = (-1)^{rn} \binom{rn-qn}{rn} \\ &\qquad \left(\text{since } rn-(qn-1)-1 = rn-qn\right).\end{aligned} \tag{32}$$

On the other hand, $rn/p \in \mathbb{Z}$ (since $p \mid rn$). Hence, Proposition 6 (applied to

[15] *Proof of (31):* Recall that $|g| \in \mathbb{N}_+$ and $p \in \operatorname{PF}(|g|)$. Thus, applying Lemma 18 to $|g|$ and -1 instead of n and q, we obtain

$$(-1)^{|g|} \equiv (-1)^{|g|/p} \bmod p^{v_p(|g|)} A.$$

Since $v_p(|g|) = v_p(n)$ (according to (29)), this rewrites as

$$(-1)^{|g|} \equiv (-1)^{|g|/p} \bmod p^{v_p(n)} A.$$

Taking the $|\alpha'|$-th power of this congruence, we obtain

$$\left((-1)^{|g|}\right)^{|\alpha'|} \equiv \left((-1)^{|g|/p}\right)^{|\alpha'|} \bmod p^{v_p(n)} A.$$

Since

$$\begin{aligned}\left((-1)^{|g|}\right)^{|\alpha'|} &= (-1)^{|g|\cdot|\alpha'|} = (-1)^{rn} \\ &\qquad \left(\text{because } |g|\cdot|\alpha'| = |\alpha'|\cdot|g| = rn \text{ (by (26))}\right)\end{aligned}$$

and

$$\begin{aligned}\left((-1)^{|g|/p}\right)^{|\alpha'|} &= (-1)^{(|g|/p)\cdot|\alpha'|} = (-1)^{rn/p} \\ &\qquad \left(\text{since } (|g|/p)\cdot|\alpha'| = \frac{1}{p}\underbrace{|\alpha'|\cdot|g|}_{\substack{=rn \\ \text{(by (26))}}} = \frac{1}{p} rn = rn/p\right),\end{aligned}$$

this rewrites as

$$(-1)^{rn} \equiv (-1)^{rn/p} \bmod p^{v_p(n)} A.$$

This proves (31).

$qn/p-1$ and rn/p instead of u and r) yields

$$\begin{aligned}
\binom{qn/p-1}{rn/p} &= (-1)^{rn/p}\binom{rn/p-(qn/p-1)-1}{rn/p} \\
&= \underbrace{(-1)^{rn/p}}_{\equiv(-1)^{rn} \bmod p^{v_p(n)}A} \underbrace{\binom{(rn-qn)/p}{rn/p}}_{\substack{\equiv\binom{rn-qn}{rn} \bmod p^{v_p(n)}A \\ \text{(by (30))}}} \\
&\qquad \left(\text{since } rn/p-(qn/p-1)-1 = rn/p-qn/p = (rn-qn)/p\right) \\
&\equiv (-1)^{rn}\binom{rn-qn}{rn} = \binom{qn-1}{rn} \bmod p^{v_p(n)}A \qquad \left(\text{due to (32)}\right). \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (33)
\end{aligned}$$

Finally, Lemma 17 (applied to qn/p and rn/p instead of u and r) yields

$$\binom{qn/p}{rn/p} = \binom{qn/p-1}{rn/p-1} + \binom{qn/p-1}{rn/p},$$

so that

$$\begin{aligned}
\binom{qn/p-1}{rn/p-1} &= \underbrace{\binom{qn/p}{rn/p}}_{\substack{\equiv\binom{qn}{rn} \bmod p^{v_p(n)}A \\ \text{(by (16))}}} - \underbrace{\binom{qn/p-1}{rn/p}}_{\substack{\equiv\binom{qn-1}{rn} \bmod p^{v_p(n)}A \\ \text{(by (33))}}} \\
&\equiv \binom{qn}{rn} - \binom{qn-1}{rn} \bmod p^{v_p(n)}A. \qquad (34)
\end{aligned}$$

But Lemma 17 (applied to qn and rn instead of u and r) yields

$$\binom{qn}{rn} = \binom{qn-1}{rn-1} + \binom{qn-1}{rn},$$

so that

$$\binom{qn-1}{rn-1} = \binom{qn}{rn} - \binom{qn-1}{rn} \equiv \binom{qn/p-1}{rn/p-1} \bmod p^{v_p(n)}A$$

(by (34)). This proves (21). Thus, Lemma 16 is proven.

Here is an obvious corollary of Lemma 16:

Corollary 19. Let A be a binomial ring. Let $n \in \mathbb{N}_+$ and let $p \in \operatorname{PF} n$. Let $q \in A$ and $r \in \mathbb{Z}$. Then,

$$\binom{qn/p-1}{rn/p-1} \equiv \binom{qn-1}{rn-1} \bmod p^{v_p(n)}A.$$

Proof of Corollary 19. There exist two integers α and β with $v_p(\alpha) \geq v_p(\beta)$ and $r = \dfrac{\alpha}{\beta}$ [16]. Thus, Lemma 16 yields $\dbinom{qn/p-1}{rn/p-1} \equiv \dbinom{qn-1}{rn-1} \bmod p^{v_p(n)} A$. This proves Corollary 19.

Here is a further property of binomial coefficients, which we won't need until much later:

Proposition 20. Let A be a binomial ring. Let $a \in A$ and $b \in \mathbb{Q} \backslash \{0\}$. Then,

$$\binom{a}{b} = \frac{a}{b}\binom{a-1}{b-1}.$$

Proof of Proposition 20. In the case when $b \notin \mathbb{N}$, the equality $\dbinom{a}{b} = \dfrac{a}{b}\dbinom{a-1}{b-1}$ holds (by virtue of both of its sides being 0), so that Proposition 20 is true in this case. Hence, for the rest of this proof, we can WLOG assume that $b \in \mathbb{N}$. Assume this.

Combining $b \in \mathbb{N}$ with $b \in \mathbb{Q} \setminus \{0\}$, we obtain $b \in \mathbb{N} \setminus \{0\} = \mathbb{N}_+$, so that $b - 1 \in \mathbb{N}$. Hence, the definition of $\dbinom{a-1}{b-1}$ yields

$$\binom{a-1}{b-1} = \frac{1}{(b-1)!} \prod_{k=0}^{(b-1)-1} ((a-1)-k). \tag{35}$$

[16] *Proof.* Since $r \in \mathbb{Z}$, we know that r is an integer. Thus, $v_p(r) \geq 0 = v_p(1)$. Also, $r = \dfrac{r}{1}$. Hence, there exist two integers α and β with $v_p(\alpha) \geq v_p(\beta)$ and $r = \dfrac{\alpha}{\beta}$ (namely, $\alpha = r$ and $\beta = 1$), qed.

But the definition of $\binom{a}{b}$ yields

$$\begin{aligned}
\binom{a}{b} &= \frac{1}{b!}\prod_{k=0}^{b-1}(a-k) \qquad \text{(since } b \in \mathbb{N}\text{)} \\
&= \frac{1}{b\cdot(b-1)!}\underbrace{(a-0)}_{=a}\prod_{k=1}^{b-1}(a-k) \\
&\qquad \left(\text{since } \prod_{k=0}^{b-1}(a-k) = (a-0)\prod_{k=1}^{b-1}(a-k) \text{ and } b! = b\cdot(b-1)!\right) \\
&= \frac{1}{b\cdot(b-1)!}a\prod_{k=1}^{b-1}(a-k) = \frac{a}{b}\cdot\frac{1}{(b-1)!}\prod_{k=1}^{b-1}(a-k) \\
&= \frac{a}{b}\cdot\frac{1}{(b-1)!}\prod_{k=0}^{(b-1)-1}\underbrace{(a-(k+1))}_{=(a-1)-k} \qquad \text{(here we substituted } k \text{ for } k-1 \text{ in the product)} \\
&= \frac{a}{b}\cdot\underbrace{\frac{1}{(b-1)!}\prod_{k=0}^{(b-1)-1}((a-1)-k)}_{=\binom{a-1}{b-1} \text{ (by (35))}} = \frac{a}{b}\binom{a-1}{b-1}.
\end{aligned}$$

This proves Proposition 20.

§3. The ghost-Witt equivalence theorem for binomial rings

We will now state our main theorem:

Theorem 30. Let N be a nest. Let A be a binomial ring. Let $(b_n)_{n\in N} \in A^N$ be a family of elements of A. Then, the following assertions $\mathcal{C}_{\text{bin}}$, $\mathcal{D}_{\text{bin}}$, $\mathcal{D}'_{\text{bin}}$, $\mathcal{D}^{\text{expl}}_{\text{bin}}$, $\mathcal{D}^{\text{expl}\prime}_{\text{bin}}$, $\mathcal{E}_{\text{bin}}$, $\mathcal{E}'_{\text{bin}}$, $\mathcal{F}_{\text{bin}}$, $\mathcal{G}_{\text{bin}}$, $\mathcal{H}_{\text{bin}}$, $\mathcal{I}_{\text{bin}}$ and $\mathcal{I}'_{\text{bin}}$ are equivalent:

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

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

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

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

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

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

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

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

Assertion $\mathcal{D}_{\text{bin}}^{\text{expl}\prime}$*:* There exists *one and only one* family $(x_n)_{n\in N} \in A^N$ of elements of A such that

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

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

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

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

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

Assertion $\mathcal{F}_{\text{bin}}$*:* Every $n \in N$ satisfies

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

Assertion $\mathcal{G}_{\text{bin}}$*:* Every $n \in N$ satisfies

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

Assertion $\mathcal{H}_{\text{bin}}$*:* Every $n \in N$ satisfies

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

Assertion $\mathcal{I}_{\text{bin}}$*:* There exists a family $(q_n)_{n\in N} \in A^N$ of elements of A such that

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

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

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

As the reader will readily notice, most parts of Theorem 30 are particular cases of corresponding parts of Theorem 4. We will explain this in detail when we come to the proof of Theorem 30. However, Assertions $\mathcal{I}_{\text{bin}}$ and $\mathcal{I}'_{\text{bin}}$ don't seem to be extendable to the general case of Theorem 4, so we will have to prove them from scratch.

Most of Theorem 30 is not new and goes back to Dwork, Dress, Siebeneicher, Hazewinkel and many others (e. g., see the equivalence $\mathcal{D}^{\text{expl}}_{\text{bin}} \iff \mathcal{F}_{\text{bin}} \iff \mathcal{G}_{\text{bin}} \iff \mathcal{H}_{\text{bin}}$ in the case $A = \mathbb{Z}$ and $N = \mathbb{N}_+$ appear in [2, Corollary on page 10]), although they rarely worked in the setting of binomial rings. Some of the underlying ideas go back to Schur and even earlier. Only Assertions $\mathcal{I}_{\text{bin}}$ and $\mathcal{I}'_{\text{bin}}$ seem to never have been studied before.

Before we start proving Theorem 30, let us quote a lemma (which is a consequence of the Chinese Remainder Theorem for modules):

Lemma 31. Let A be an Abelian group (written additively). Let $n \in \mathbb{N}_+$. Then, $nA = \bigcap\limits_{p \in \operatorname{PF} n} \left(p^{v_p(n)} A\right)$.

Lemma 31 is Corollary 2 in [5]; thus we are not going to prove it here.

Let us also isolate as a lemma a very simple arithmetical argument which will be used several times:

Lemma 32. Let $n \in \mathbb{N}_+$. Let $p \in \operatorname{PF} n$. For any divisor d of n, the assertions $d \nmid (n/p)$ and $p^{v_p(n)} \mid d$ are equivalent (that is, $d \nmid (n/p)$ holds if and only if $p^{v_p(n)} \mid d$ holds).

Proof of Lemma 32. Let d be a divisor of n. Then, $n/d \in \mathbb{Z}$. Thus, we can define an integer $e \in \mathbb{Z}$ by $e = n/d$. Consider this e. Then, $e = n/d$, so that $de = n$.

Since e is an integer, we have $v_p(e) \geq 0$.

We will prove the following assertions:

Assertion Pf32.1: If $d \nmid (n/p)$, then $p^{v_p(n)} \mid d$.

Assertion Pf32.2: If $p^{v_p(n)} \mid d$, then $d \nmid (n/p)$.

Proof of Assertion Pf32.1: Assume that $d \nmid (n/p)$.

We have defined $v_p(d)$ to be the largest nonnegative integer m satisfying $p^m \mid d$. Thus, $p^{v_p(d)} \mid d$.

Since $e = n/d$, we have $\dfrac{e}{p} = \dfrac{n/d}{p} = \dfrac{n}{pd} = \dfrac{n/p}{d} \notin \mathbb{Z}$ (since $d \nmid (n/p)$), so that $p \nmid e$. Thus, $v_p(e) = 0$. But $v_p(d) + v_p(e) = v_p\left(\underbrace{de}_{=n}\right) = v_p(n)$, so that $v_p(n) = v_p(d) + \underbrace{v_p(e)}_{=0} = v_p(d)$. Hence, $p^{v_p(n)} = p^{v_p(d)} \mid d$. This proves Assertion Pf32.1.

Proof of Assertion Pf32.2: Assume that $p^{v_p(n)} \mid d$.

We have defined $v_p(d)$ to be the largest nonnegative integer m satisfying $p^m \mid d$. Thus, $v_p(d) =$ (the largest nonnegative integer m satisfying $p^m \mid d$). But since $p^{v_p(n)} \mid d$, we have

$$v_p(n) \leq (\text{the largest nonnegative integer } m \text{ satisfying } p^m \mid d) = v_p(d),$$

so that

$$v_p(d) \geq v_p\left(\underbrace{n}_{=de}\right) = v_p(de) = v_p(d) + v_p(e).$$

Subtracting $v_p(d)$ from this inequality yields $0 \geq v_p(e)$ (because $v_p(d)$ is a non-negative integer, not ∞). Combined with $v_p(e) \geq 0$, this results in $v_p(e) = 0$. Thus, $p \nmid e$. In other words, $\dfrac{e}{p} \notin \mathbb{Z}$. Since $e = n/d$, this rewrites as $\dfrac{n/d}{p} \notin \mathbb{Z}$. Hence, $\dfrac{n/p}{d} = \dfrac{n}{pd} = \dfrac{n/d}{p} \notin \mathbb{Z}$, so that $d \nmid (n/p)$. This proves Assertion Pf32.2.

Now, the assertions $d \nmid (n/p)$ and $p^{v_p(n)} \mid d$ are equivalent. This is because the former of these assertions implies the latter (according to Assertion Pf32.1), and because the latter of these assertions implies the former (according to Assertion Pf32.2). Thus, Lemma 32 is proven.

Proof of Theorem 30. By the definition of a "binomial ring", every binomial ring is torsionfree. Since A is a binomial ring, this yields that A is torsionfree.

For every $n \in N$, define a map $\varphi_n : A \to A$ by $\varphi_n = \mathrm{id}$. Clearly, φ_n is an endomorphism of the ring A for every $a \in A$. Moreover, every $a \in A$ and $p \in \mathbb{P} \cap N$ satisfy $\varphi_p(a) \equiv a^p \bmod pA$ [17]. In other words, the condition (1) is satisfied. Moreover, the condition (4) is satisfied (since $\varphi_1 = \mathrm{id}$ by the definition of φ_1), and the condition (5) is also satisfied (since $\varphi_n \circ \varphi_m = \varphi_{nm}$ for every $n \in N$ and every $m \in N$ satisfying $nm \in N$ [18]). Hence, the three conditions (1), (4) and (5) are satisfied. Therefore, Theorem 4 yields that the assertions $\mathcal{C}$, $\mathcal{D}$, $\mathcal{D}'$, $\mathcal{D}^{\mathrm{expl}}$, $\mathcal{D}^{\mathrm{expl}\prime}$, $\mathcal{E}$, $\mathcal{E}'$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ are equivalent, where:

- the assertions $\mathcal{C}$, $\mathcal{D}$ and $\mathcal{D}^{\mathrm{expl}}$ are the ones stated in Theorem 1,
- the assertions $\mathcal{D}'$ and $\mathcal{D}^{\mathrm{expl}\prime}$ are the ones stated in Theorem 2,
- the assertions $\mathcal{E}$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ are the ones stated in Theorem 3, and
- the assertion $\mathcal{E}'$ is the one stated in Theorem 4.

Now, comparing the assertions $\mathcal{C}$, $\mathcal{D}$, $\mathcal{D}'$, $\mathcal{D}^{\mathrm{expl}}$, $\mathcal{D}^{\mathrm{expl}\prime}$, $\mathcal{E}$, $\mathcal{E}'$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ with the respective assertions $\mathcal{C}_{\mathrm{bin}}$, $\mathcal{D}_{\mathrm{bin}}$, $\mathcal{D}'_{\mathrm{bin}}$, $\mathcal{D}^{\mathrm{expl}}_{\mathrm{bin}}$, $\mathcal{D}^{\mathrm{expl}\prime}_{\mathrm{bin}}$, $\mathcal{E}_{\mathrm{bin}}$, $\mathcal{E}'_{\mathrm{bin}}$, $\mathcal{F}_{\mathrm{bin}}$, $\mathcal{G}_{\mathrm{bin}}$ and $\mathcal{H}_{\mathrm{bin}}$, we notice that:

- we have $\mathcal{C} \Longleftrightarrow \mathcal{C}_{\mathrm{bin}}$ (since $\underbrace{\varphi_p}_{\substack{=\mathrm{id} \\ \text{(by the definition} \\ \text{of } \varphi_p)}}(b_{n/p}) = \mathrm{id}(b_{n/p}) = b_{n/p}$);
- we have $\mathcal{D} \Longleftrightarrow \mathcal{D}_{\mathrm{bin}}$ (because Assertions $\mathcal{D}$ and $\mathcal{D}_{\mathrm{bin}}$ are identical);
- we have $\mathcal{D}' \Longleftrightarrow \mathcal{D}'_{\mathrm{bin}}$ (because Assertions $\mathcal{D}'$ and $\mathcal{D}'_{\mathrm{bin}}$ are identical);

[17] *Proof.* Let $a \in A$ and $p \in \mathbb{P} \cap N$. By the definition of φ_p, we have $\varphi_p = \mathrm{id}$, so that $\varphi_p(a) = \mathrm{id}(a) = a \equiv a^p \bmod pA$ (since Theorem 8 yields $a^p \equiv a \bmod pA$), qed.

[18] *Proof.* Let $n \in N$ and $m \in N$ be such that $nm \in N$. By the definition of φ_n, we have $\varphi_n = \mathrm{id}$. By the definition of φ_m, we have $\varphi_m = \mathrm{id}$. By the definition of φ_{nm}, we have $\varphi_{nm} = \mathrm{id}$. Since $\varphi_n = \mathrm{id}$ and $\varphi_m = \mathrm{id}$, we have $\varphi_n \circ \varphi_m = \mathrm{id} \circ \mathrm{id} = \mathrm{id} = \varphi_{nm}$, qed.

- we have $\mathcal{D}^{\mathrm{expl}} \Longleftrightarrow \mathcal{D}_{\mathrm{bin}}^{\mathrm{expl}}$ (because Assertions $\mathcal{D}^{\mathrm{expl}}$ and $\mathcal{D}_{\mathrm{bin}}^{\mathrm{expl}}$ are identical);
- we have $\mathcal{D}^{\mathrm{expl}\prime} \Longleftrightarrow \mathcal{D}_{\mathrm{bin}}^{\mathrm{expl}\prime}$ (because Assertions $\mathcal{D}^{\mathrm{expl}\prime}$ and $\mathcal{D}_{\mathrm{bin}}^{\mathrm{expl}\prime}$ are identical);
- we have $\mathcal{E} \Longleftrightarrow \mathcal{E}_{\mathrm{bin}}$ (since $\underbrace{\varphi_{n/d}}_{\substack{=\mathrm{id} \\ \text{(by the definition} \\ \text{of } \varphi_{n/d}\text{)}}} (y_d) = \mathrm{id}\,(y_d) = y_d$);
- we have $\mathcal{E}' \Longleftrightarrow \mathcal{E}'_{\mathrm{bin}}$ (since $\underbrace{\varphi_{n/d}}_{\substack{=\mathrm{id} \\ \text{(by the definition} \\ \text{of } \varphi_{n/d}\text{)}}} (y_d) = \mathrm{id}\,(y_d) = y_d$);
- we have $\mathcal{F} \Longleftrightarrow \mathcal{F}_{\mathrm{bin}}$ (since $\underbrace{\varphi_d}_{\substack{=\mathrm{id} \\ \text{(by the definition} \\ \text{of } \varphi_d\text{)}}} (b_{n/d}) = \mathrm{id}\,(b_{n/d}) = b_{n/d}$);
- we have $\mathcal{G} \Longleftrightarrow \mathcal{G}_{\mathrm{bin}}$ (since $\underbrace{\varphi_d}_{\substack{=\mathrm{id} \\ \text{(by the definition} \\ \text{of } \varphi_d\text{)}}} (b_{n/d}) = \mathrm{id}\,(b_{n/d}) = b_{n/d}$);
- we have $\mathcal{H} \Longleftrightarrow \mathcal{H}_{\mathrm{bin}}$ (since $\underbrace{\varphi_{n/\gcd(i,n)}}_{\substack{=\mathrm{id} \\ \text{(by the definition} \\ \text{of } \varphi_{n/\gcd(i,n)}\text{)}}} \left(b_{\gcd(i,n)}\right) = \mathrm{id}\left(b_{\gcd(i,n)}\right) = b_{\gcd(i,n)}$).

Hence, the (already proven) equivalence of the assertions $\mathcal{C}$, $\mathcal{D}$, $\mathcal{D}'$, $\mathcal{D}^{\mathrm{expl}}$, $\mathcal{D}^{\mathrm{expl}\prime}$, $\mathcal{E}$, $\mathcal{E}'$, $\mathcal{F}$, $\mathcal{G}$ and $\mathcal{H}$ yields the equivalence of the assertions $\mathcal{C}_{\mathrm{bin}}$, $\mathcal{D}_{\mathrm{bin}}$, $\mathcal{D}'_{\mathrm{bin}}$, $\mathcal{D}_{\mathrm{bin}}^{\mathrm{expl}}$, $\mathcal{D}_{\mathrm{bin}}^{\mathrm{expl}\prime}$, $\mathcal{E}_{\mathrm{bin}}$, $\mathcal{E}'_{\mathrm{bin}}$, $\mathcal{F}_{\mathrm{bin}}$, $\mathcal{G}_{\mathrm{bin}}$ and $\mathcal{H}_{\mathrm{bin}}$.

Now let us prove the equivalence of these assertions with the remaining two assertions $\mathcal{I}_{\mathrm{bin}}$ and $\mathcal{I}'_{\mathrm{bin}}$. We will do this by proving the implications $\mathcal{C}_{\mathrm{bin}} \Longrightarrow \mathcal{I}_{\mathrm{bin}}$, $\mathcal{I}_{\mathrm{bin}} \Longrightarrow \mathcal{C}_{\mathrm{bin}}$, $\mathcal{I}_{\mathrm{bin}} \Longrightarrow \mathcal{I}'_{\mathrm{bin}}$ and $\mathcal{I}'_{\mathrm{bin}} \Longrightarrow \mathcal{I}_{\mathrm{bin}}$.

Proof of the implication $\mathcal{I}_{\mathrm{bin}} \Longrightarrow \mathcal{C}_{\mathrm{bin}}$: Assume that Assertion $\mathcal{I}_{\mathrm{bin}}$ holds. In other words, there exists a family $(q_n)_{n \in N} \in A^N$ of elements of A such that

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

Consider this family $(q_n)_{n \in N}$. We are going to prove that Assertion $\mathcal{C}_{\mathrm{bin}}$ holds as well.

Let $n \in N$ and $p \in \mathrm{PF}\, n$. We are going to show that $b_{n/p} \equiv b_n \bmod p^{v_p(n)} A$.

Since $n \in N$, every divisor of n lies in N (because N is a nest). Since $p \in \mathrm{PF}\, n$, we know that p is a prime divisor of n. Thus, p is a prime and satisfies $p \mid n$. Since $p \mid n$ and $n \in \mathbb{N}_+$, we have $n/p \in \mathbb{N}_+$, and thus n/p is a divisor of n. Therefore, $n/p \in N$ (since every divisor of n lies in N). Hence, we can apply

(36) to n/p instead of n. Thus we obtain

$$b_{n/p} = \sum_{d \mid (n/p)} d \binom{q_d \left(n/p\right)/d}{\left(n/p\right)/d} = \sum_{d \mid (n/p)} d \binom{q_d \left(n/d\right)/p}{\left(n/d\right)/p} \tag{37}$$

$$\left(\text{since } \left(n/p\right)/d = \left(n/d\right)/p \text{ for every divisor } d \text{ of } n/p\right).$$

On the other hand, applying (36) directly, we obtain

$$\begin{aligned} b_n &= \sum_{d \mid n} d \binom{q_d n/d}{n/d} \\ &= \underbrace{\sum_{\substack{d \mid n; \\ d \mid (n/p)}}}_{\substack{= \sum\limits_{d \mid (n/p)} \\ \text{(since the divisors } d \text{ of } n \\ \text{satisfying } d \mid (n/p) \text{ are exactly} \\ \text{the divisors of } n/p)}} d \binom{q_d n/d}{n/d} + \underbrace{\sum_{\substack{d \mid n; \\ d \nmid (n/p)}}}_{\substack{= \sum\limits_{\substack{d \mid n; \\ p^{v_p(n)} \mid d}} \\ \text{(because for every divisor } d \text{ of } n, \\ \text{the assertions } d \nmid (n/p) \text{ and } p^{v_p(n)} \mid d \\ \text{are equivalent (by Lemma 32))}}} d \binom{q_d n/d}{n/d} \\ &= \sum_{d \mid (n/p)} d \binom{q_d n/d}{n/d} + \sum_{\substack{d \mid n; \\ p^{v_p(n)} \mid d}} \underbrace{d}_{\substack{\equiv 0 \bmod p^{v_p(n)} A \\ \text{(since } p^{v_p(n)} \mid d\text{)}}} \binom{q_d n/d}{n/d} \\ &\equiv \sum_{d \mid (n/p)} d \binom{q_d n/d}{n/d} + \underbrace{\sum_{\substack{d \mid n; \\ p^{v_p(n)} \mid d}} 0 \binom{q_d n/d}{n/d}}_{=0} = \sum_{d \mid (n/p)} d \binom{q_d n/d}{n/d} \bmod p^{v_p(n)} A. \end{aligned} \tag{38}$$

But every divisor d of n/p satisfies $n/d \in \mathbb{N}_+$ and $p \in \mathrm{PF}\left(n/d\right)$ [19]. Hence, every $s \in A$ and every divisor d of n/p satisfy

$$\binom{s\left(n/d\right)/p}{1\left(n/d\right)/p} \equiv \binom{sn/d}{1n/d} \bmod p^{v_p(n/d)} A$$

(by Lemma 15, applied to n/d, s and 1 instead of n, q and r). This rewrites as

$$\binom{s\left(n/d\right)/p}{\left(n/d\right)/p} \equiv \binom{sn/d}{n/d} \bmod p^{v_p(n/d)} A \tag{39}$$

(since $1\left(n/d\right)/p = \left(n/d\right)/p$ and $1n/d = n/d$). From this, it is easy to conclude that every $s \in A$ and every divisor d of n/p satisfy

$$d \binom{s\left(n/d\right)/p}{\left(n/d\right)/p} \equiv d \binom{sn/d}{n/d} \bmod p^{v_p(n)} A \tag{40}$$

---

[19] *Proof.* Let d be a divisor of n/p. Then, $\dfrac{n/p}{d} \in \mathbb{N}_+$ (since $n/p \in \mathbb{N}_+$ and since d is a divisor of n/p), so that $\dfrac{n/d}{p} = \dfrac{n}{pd} = \dfrac{n/p}{d} \in \mathbb{N}_+$. Thus, $n/d = \underbrace{p}_{\in \mathbb{N}_+} \underbrace{\dfrac{n/d}{p}}_{\in \mathbb{N}_+} \in \mathbb{N}_+ \mathbb{N}_+ \subseteq \mathbb{N}_+$.

Moreover, since $\dfrac{n/d}{p} \in \mathbb{N}_+$, we know that $p \mid \left(n/d\right)$, so that p is a prime divisor of n/d (since p is a prime). In other words, $p \in \mathrm{PF}\left(n/d\right)$, qed.

[20]. Thus,

$$\sum_{d\mid(n/p)} \underbrace{d\binom{q_d\,(n/d)/p}{(n/d)/p}}_{\equiv d\binom{q_d n/d}{n/d} \bmod p^{v_p(n)}A \atop \text{(by (40), applied to } s=q_d)} \equiv \sum_{d\mid(n/p)} d\binom{q_d n/d}{n/d} \bmod p^{v_p(n)}A. \tag{42}$$

Now, (37) becomes

$$\begin{aligned} b_{n/p} &= \sum_{d\mid(n/p)} d\binom{q_d\,(n/d)/p}{(n/d)/p} \equiv \sum_{d\mid(n/p)} d\binom{q_d n/d}{n/d} \qquad \text{(by (42))} \\ &\equiv b_n \bmod p^{v_p(n)}A \qquad \text{(by (38))}\,. \end{aligned}$$

Now forget that we fixed n and p. We thus have shown that every $n \in N$ and every $p \in \operatorname{PF} n$ satisfies

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

In other words, Assertion $\mathcal{C}_{\text{bin}}$ holds. We have thus proven Assertion $\mathcal{C}_{\text{bin}}$ under the assumption of Assertion $\mathcal{I}_{\text{bin}}$. In other words, the implication $\mathcal{I}_{\text{bin}} \Longrightarrow \mathcal{C}_{\text{bin}}$ is proven.

---

[20] *Proof of (40):* Let $s \in A$. Let d be a divisor of n/p. Then, (39) yields

$$\binom{s\,(n/d)/p}{(n/d)/p} \equiv \binom{sn/d}{n/d} \bmod p^{v_p(n/d)}A.$$

In other words,

$$\binom{s\,(n/d)/p}{(n/d)/p} - \binom{sn/d}{n/d} \in p^{v_p(n/d)}A. \tag{41}$$

On the other hand, we defined $v_p(d)$ as the largest nonnegative integer m satisfying $p^m \mid d$. Thus, $p^{v_p(d)} \mid d$. Thus, there exists an $e \in \mathbb{Z}$ such that $d = p^{v_p(d)}e$. Consider this e.

Now,

$$\begin{aligned} &d\binom{s\,(n/d)/p}{(n/d)/p} - d\binom{sn/d}{n/d} \\ &= \underbrace{d}_{=p^{v_p(d)}e}\left(\binom{s\,(n/d)/p}{(n/d)/p} - \binom{sn/d}{n/d}\right) \\ &= p^{v_p(d)}e\underbrace{\left(\binom{s\,(n/d)/p}{(n/d)/p} - \binom{sn/d}{n/d}\right)}_{\in p^{v_p(n/d)}A} \in p^{v_p(d)}ep^{v_p(n/d)}A = \underbrace{p^{v_p(d)}p^{v_p(n/d)}}_{=p^{v_p(d)+v_p(n/d)}}\underbrace{eA}_{\subseteq A} \\ &\subseteq p^{v_p(d)+v_p(n/d)}A. \end{aligned}$$

Since

$$v_p(d) + v_p(n/d) = v_p\left(\underbrace{d\cdot(n/d)}_{=n}\right) = v_p(n)\,,$$

this simplifies to $d\binom{s\,(n/d)/p}{(n/d)/p} - d\binom{sn/d}{n/d} \in p^{v_p(n)}A$. In other words, $d\binom{s\,(n/d)/p}{(n/d)/p} \equiv d\binom{sn/d}{n/d} \bmod p^{v_p(n)}A$. This proves (40).

Proof of the implication $\mathcal{C}_{\text{bin}} \Longrightarrow \mathcal{I}_{\text{bin}}$: Assume that Assertion $\mathcal{C}_{\text{bin}}$ holds. In other words, every $n \in N$ and every $p \in \operatorname{PF} n$ satisfies

$$b_{n/p} \equiv b_n \bmod p^{v_p(n)} A. \tag{43}$$

We will now show that Assertion $\mathcal{I}_{\text{bin}}$ holds.

Indeed, we are going to construct a family $(r_n)_{n \in N} \in A^N$ of elements of A such that every $m \in N$ satisfies

$$b_m = \sum_{d \mid m} d \binom{r_d m/d}{m/d}. \tag{44}$$

Indeed, we will construct this family $(r_n)_{n \in N}$ recursively. Here is the recursion step: Let $n \in N$ be arbitrary. Assume that we have already constructed an element r_m of A for every $m \in N \cap \{1, 2, ..., n-1\}$ in such a way that (44) is satisfied for every $m \in N \cap \{1, 2, ..., n-1\}$. We now need to construct an element r_n of A such that (44) is satisfied for every $m \in N \cap \{1, 2, ..., n\}$. Once such an r_n is constructed, our recursive step will be complete, and the family will be defined.

According to our assumption, we have already constructed an element r_m of A for every $m \in N \cap \{1, 2, ..., n-1\}$. As a consequence, we have already constructed an element $r_d \in A$ for every divisor d of n satisfying $d \neq n$ (because every such d lies in $N \cap \{1, 2, ..., n-1\}$).

Let $p \in \operatorname{PF} n$. Then, p is a prime divisor of n. In other words, p is a prime and satisfies $p \mid n$. Hence, $n/p \in \mathbb{N}_+$ (since $n \in \mathbb{N}_+$), so that n/p is a divisor of n. But since N is a nest, every divisor of n lies in N (because $n \in N$). Thus, n/p lies in N (since n/p is a divisor of n). Combined with $n/p \in \{1, 2, ..., n-1\}$ (this is clear because $n/p \in \mathbb{N}_+$ and $n/\underbrace{p}_{>1} < n/1 = n$), this yields $n/p \in N \cap \{1, 2, ..., n-1\}$. Hence, we can apply (44) to $m = n/p$ (since we know that (44) is satisfied for every $m \in N \cap \{1, 2, ..., n-1\}$). As a result of this, we obtain

$$b_{n/p} = \sum_{d \mid (n/p)} d \binom{r_d \left(n/p\right)/d}{\left(n/p\right)/d} = \sum_{d \mid (n/p)} d \binom{r_d \left(n/d\right)/p}{\left(n/d\right)/p} \tag{45}$$
$$\left(\text{since } \left(n/p\right)/d = \left(n/d\right)/p \text{ for every divisor } d \text{ of } n/p\right).$$

Recall that every $s \in A$ and every divisor d of n/p satisfy

$$d \binom{s \left(n/d\right)/p}{\left(n/d\right)/p} \equiv d \binom{sn/d}{n/d} \bmod p^{v_p(n)} A. \tag{46}$$

(This is proven exactly in the same way as we have proven (42) during the proof of the implication $\mathcal{I}_{\text{bin}} \Longrightarrow \mathcal{C}_{\text{bin}}$.)

But recall that we have already constructed an element $r_d \in A$ for every divisor d of n satisfying $d \neq n$. Thus, the sum $\sum\limits_{\substack{d \mid n; \\ d \neq n}} d \binom{r_d n/d}{n/d}$ makes sense. This

sum satisfies

$$\sum_{\substack{d\mid n;\\ d\neq n}} d\binom{r_d n/d}{n/d}$$

$$= \sum_{\substack{d\mid n;\\ d\neq n;\\ \underbrace{d\mid (n/p)}_{=\sum\limits_{d\mid (n/p)}}}} d\binom{r_d n/d}{n/d} + \sum_{\substack{d\mid n;\\ d\neq n\\ \underbrace{d\nmid (n/p)}_{=\sum\limits_{\substack{d\mid n;\\ d\neq n;\\ p^{v_p(n)}\mid d}}}}} d\binom{r_d n/d}{n/d}$$

(since the divisors d of n satisfying $d\neq n$ and $d\mid (n/p)$ are exactly the divisors of n/p)

(because for every divisor d of n, the assertions $d\nmid (n/p)$ and $p^{v_p(n)}\mid d$ are equivalent (by Lemma 32))

$$= \sum_{d\mid (n/p)} \underbrace{d\binom{r_d n/d}{n/d}}_{\equiv d\binom{r_d\,(n/d)/p}{(n/d)/p} \bmod p^{v_p(n)}A} + \sum_{\substack{d\mid n;\\ d\neq n;\\ p^{v_p(n)}\mid d}} \underbrace{d}_{\equiv 0 \bmod p^{v_p(n)}A} \binom{r_d n/d}{n/d}$$

(since $p^{v_p(n)}\mid d$)

(because (46) (applied to $s=r_d$) yields $d\binom{r_d\,(n/d)/p}{(n/d)/p} \equiv d\binom{r_d n/d}{n/d} \bmod p^{v_p(n)}A$)

$$\equiv \sum_{d\mid (n/p)} d\binom{r_d\,(n/d)/p}{(n/d)/p} + \underbrace{\sum_{\substack{d\mid n;\\ d\neq n;\\ p^{v_p(n)}\mid d}} 0\binom{r_d n/d}{n/d}}_{=0}$$

$$= \sum_{d\mid (n/p)} d\binom{r_d\,(n/d)/p}{(n/d)/p} = b_{n/p} \bmod p^{v_p(n)}A \qquad \text{(by (45))}.$$

Now forget that we fixed p. We have thus shown that every $p \in \operatorname{PF} n$ satisfies

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

In other words,

$$b_n - \sum_{\substack{d\mid n;\\ d\neq n}} d\binom{r_d n/d}{n/d} \in \bigcap_{p\in \operatorname{PF} n} \left(p^{v_p(n)}A\right) = nA \qquad \text{(by Lemma 31)}.$$

Hence, there exists some element ζ of A such that

$$b_n - \sum_{\substack{d\mid n;\\ d\neq n}} d\binom{r_d n/d}{n/d} = n\zeta. \tag{47}$$

Fix such a ζ. Now define an element r_n of A by $r_n = \zeta$.

We are now going to show that (44) is satisfied for every $m \in N \cap \{1,2,...,n\}$. Indeed, this is known to hold for every $m \in N \cap \{1,2,...,n-1\}$ (by the induction hypothesis), so we only need to check it for every $m \in (N \cap \{1,2,...,n\}) \setminus (N \cap \{1,2,...,n-1\})$. But the only such m is n. So we only need to prove that (44) is satisfied for $m = n$. Let us do this now: Since every $x \in A$ satisfies $\binom{x}{1} = x$ (this follows readily from the definition of binomial coefficients), we have $\binom{r_n}{1} = r_n$. Since n is a divisor of n, we have

$$\begin{aligned}
\sum_{d|n} d\binom{r_d n/d}{n/d} &= n \underbrace{\binom{r_n n/n}{n/n}}_{\substack{=\binom{r_n \cdot 1}{1} \\ \text{(since } n/n=1\text{)}}} + \sum_{\substack{d|n; \\ d \neq n}} d\binom{r_d n/d}{n/d} \\
&= n \underbrace{\binom{r_n \cdot 1}{1}}_{=\binom{r_n}{1}=r_n=\zeta} + \sum_{\substack{d|n; \\ d \neq n}} d\binom{r_d n/d}{n/d} \\
&= n\zeta + \sum_{\substack{d|n; \\ d \neq n}} d\binom{r_d n/d}{n/d} = b_n \qquad \text{(owing to (47))}.
\end{aligned}$$

In other words, (44) is satisfied for $m = n$.

We have thus shown that (44) is satisfied for every $m \in N \cap \{1,2,...,n\}$. Thus, we have constructed an element r_n of A such that (44) is satisfied for every $m \in N \cap \{1,2,...,n\}$. This completes the recursion step of the recursive definition of the family $(r_n)_{n \in N}$. Due to its construction, this family $(r_n)_{n \in N}$ satisfies (44) for every $m \in N$. Hence, for every $n \in N$, we have

$$b_n = \sum_{d|n} d\binom{r_d n/d}{n/d} \qquad \text{(by (44), applied to } m = n\text{)}.$$

Hence, there exists a family $(q_n)_{n \in N} \in A^N$ of elements of A such that

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

(namely, the family $(r_n)_{n \in N}$). In other words, Assertion $\mathcal{I}_{\text{bin}}$ is satisfied. We have thus proven Assertion $\mathcal{I}_{\text{bin}}$ under the assumption of Assertion $\mathcal{C}_{\text{bin}}$. In other words, the implication $\mathcal{C}_{\text{bin}} \Longrightarrow \mathcal{I}_{\text{bin}}$ is proven.

Proof of the implication $\mathcal{I}_{\text{bin}} \Longrightarrow \mathcal{I}'_{\text{bin}}$: Assume that Assertion $\mathcal{I}_{\text{bin}}$ holds. In other words, there exists a family $(q_n)_{n \in N} \in A^N$ of elements of A such that

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

Let $(Q_n)_{n\in N}$ be such a family. Thus, $(Q_n)_{n\in N} \in A^N$ is a family of elements of A such that

$$\left(b_n = \sum_{d\mid n} d \binom{Q_d n/d}{n/d} \text{ for every } n \in N \right). \tag{48}$$

We are now going to prove that Assertion $\mathcal{I}'_{\text{bin}}$ holds.

Let $(q_n)_{n\in N} \in A^N$ be any family of elements of A such that

$$\left(b_n = \sum_{d\mid n} d \binom{q_d n/d}{n/d} \text{ for every } n \in N \right). \tag{49}$$

We are going to show that this family $(q_n)_{n\in N}$ equals $(Q_n)_{n\in N}$. Indeed, let us show that

$$q_n = Q_n \qquad \text{for every } n \in N. \tag{50}$$

Proof of (50): We are going to prove (50) by strong induction over n.

Induction step:[21] Let $m \in N$. Assume that (50) holds for every $n \in N$ satisfying $n < m$. We will now show that (50) holds for $n = m$.

Applying (49) to $n = m$, we obtain

$$\begin{aligned} b_m &= \sum_{d\mid m} d \binom{q_d m/d}{m/d} \\ &= m \underbrace{\binom{q_m m/m}{m/m}}_{\substack{=\binom{q_m}{1} \\ \text{(since } q_m m/m = q_m \text{ and } m/m = 1\text{)}}} + \sum_{\substack{d\mid m; \\ d\neq m}} d \binom{q_d m/d}{m/d} \\ &\qquad \text{(since } m \text{ is a divisor of } m\text{)} \\ &= m \underbrace{\binom{q_m}{1}}_{=q_m} + \sum_{\substack{d\mid m; \\ d\neq m}} d \binom{q_d m/d}{m/d} \\ &\qquad \text{(since every } x\in A \text{ satisfies } \binom{x}{1} = x\text{)} \\ &= m q_m + \sum_{\substack{d\mid m; \\ d\neq m}} d \binom{q_d m/d}{m/d}, \end{aligned}$$

so that

$$m q_m = b_m - \sum_{\substack{d\mid m; \\ d\neq m}} d \binom{q_d m/d}{m/d}. \tag{51}$$

The same argument, using (48) in lieu of (49), reveals that

$$m Q_m = b_m - \sum_{\substack{d\mid m; \\ d\neq m}} d \binom{Q_d m/d}{m/d}. \tag{52}$$

[21] A strong induction needs no induction base.

But we have assumed that (50) holds for every $n \in N$ satisfying $n < m$. Thus, in particular, for any divisor d of m satisfying $d \neq m$, we have $q_d = Q_d$ (because $d \in N$ and $d < m$). Hence, the right hand side of (51) equals the right hand side of (52). As a consequence, the left hand sides of these two equalities must also be equal. That is, we have $mq_m = mQ_m$. In other words, $m\left(q_m - Q_m\right) = 0$.

Now, A is a binomial ring. By the definition of a binomial ring, this yields that A is torsionfree. Thus, we have $q_m - Q_m = 0$ (since m is a positive integer, and since $m\left(q_m - Q_m\right) = 0$). In other words, $q_m = Q_m$. In other words, (50) holds for $n = m$. This completes the induction step. Thus, the induction proof of (50) is complete.

Now we know that (50) holds. In other words, the family $\left(q_n\right)_{n \in N}$ equals $\left(Q_n\right)_{n \in N}$.

Now forget that we fixed $\left(q_n\right)_{n \in N}$. We thus have shown that whenever $\left(q_n\right)_{n \in N} \in A^N$ is any family of elements of A such that

$$\left(b_n = \sum_{d \mid n} d \binom{q_d n / d}{n / d} \text{ for every } n \in N \right),$$

this family $\left(q_n\right)_{n \in N}$ must equal $\left(Q_n\right)_{n \in N}$. Hence, there exists **at most one** family $\left(q_n\right)_{n \in N} \in A^N$ of elements of A such that

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

(because every such family must equal $\left(Q_n\right)_{n \in N}$). Combined with the fact that there exists **at least one** such family (because Assertion $\mathcal{I}_{\text{bin}}$ holds), this yields that there exists **one and only one** such family. In other words, Assertion $\mathcal{I}'_{\text{bin}}$ holds. We have thus proven Assertion $\mathcal{I}'_{\text{bin}}$ under the assumption of Assertion $\mathcal{I}_{\text{bin}}$. In other words, the implication $\mathcal{I}_{\text{bin}} \Longrightarrow \mathcal{I}'_{\text{bin}}$ is proven.

Proof of the implication $\mathcal{I}'_{\text{bin}} \Longrightarrow \mathcal{I}_{\text{bin}}$: The implication $\mathcal{I}'_{\text{bin}} \Longrightarrow \mathcal{I}_{\text{bin}}$ obviously holds, because if there exists one and only one family with a certain property, then there clearly exists at least one family with this property.

Now we have proven the implications $\mathcal{I}_{\text{bin}} \Longrightarrow \mathcal{I}'_{\text{bin}}$ and $\mathcal{I}'_{\text{bin}} \Longrightarrow \mathcal{I}_{\text{bin}}$. Combining these two implications, we obtain the equivalence $\mathcal{I}'_{\text{bin}} \Longleftrightarrow \mathcal{I}_{\text{bin}}$.

We also have proven the implications $\mathcal{C}_{\text{bin}} \Longrightarrow \mathcal{I}_{\text{bin}}$ and $\mathcal{I}_{\text{bin}} \Longrightarrow \mathcal{C}_{\text{bin}}$. Combining these two implications, we obtain the equivalence $\mathcal{C}_{\text{bin}} \Longleftrightarrow \mathcal{I}_{\text{bin}}$.

Combining the equivalences $\mathcal{C}_{\text{bin}} \Longleftrightarrow \mathcal{I}_{\text{bin}}$ and $\mathcal{I}'_{\text{bin}} \Longleftrightarrow \mathcal{I}_{\text{bin}}$, we obtain the equivalence $\mathcal{C}_{\text{bin}} \Longleftrightarrow \mathcal{I}_{\text{bin}} \Longleftrightarrow \mathcal{I}'_{\text{bin}}$.

Now recall that the assertions $\mathcal{C}_{\text{bin}}$, $\mathcal{D}_{\text{bin}}$, $\mathcal{D}'_{\text{bin}}$, $\mathcal{D}^{\text{expl}}_{\text{bin}}$, $\mathcal{D}^{\text{expl}\prime}_{\text{bin}}$, $\mathcal{E}_{\text{bin}}$, $\mathcal{E}'_{\text{bin}}$, $\mathcal{F}_{\text{bin}}$, $\mathcal{G}_{\text{bin}}$ and $\mathcal{H}_{\text{bin}}$ are equivalent. Combining this with the equivalence $\mathcal{C}_{\text{bin}} \Longleftrightarrow \mathcal{I}_{\text{bin}} \Longleftrightarrow \mathcal{I}'_{\text{bin}}$, we conclude that the assertions $\mathcal{C}_{\text{bin}}$, $\mathcal{D}_{\text{bin}}$, $\mathcal{D}'_{\text{bin}}$, $\mathcal{D}^{\text{expl}}_{\text{bin}}$, $\mathcal{D}^{\text{expl}\prime}_{\text{bin}}$, $\mathcal{E}_{\text{bin}}$, $\mathcal{E}'_{\text{bin}}$, $\mathcal{F}_{\text{bin}}$, $\mathcal{G}_{\text{bin}}$, $\mathcal{H}_{\text{bin}}$, $\mathcal{I}_{\text{bin}}$ and $\mathcal{I}'_{\text{bin}}$ are equivalent. Theorem 30 is thus proven.

§4. Applications in binomial rings

We can obtain several concrete divisibilities by applying Theorem 30 to particular families $(b_n)_{n \in N}$. Here is probably the simplest one:

Theorem 41. Let A be a binomial ring. Let $q \in A$. Then:

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

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

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

$$\sum_{d \mid n} \mu(d)\, q^{n/d} \in nA.$$

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

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

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

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

(f) There exists *one and only one* family $(q_n)_{n \in N} \in A^N$ of elements of A such that

$$\left(q^n = \sum_{d \mid n} d \binom{q_d n/d}{n/d} \text{ for every } n \in \mathbb{N}_+ \right).$$

This Theorem 41 generalizes Theorem 16 from [5]. Indeed, Theorem 16 from [5] can be proven by applying Theorem 41 (more precisely, parts **(a)**, **(b)**, **(c)**, **(d)** and **(e)** of Theorem 41) to $A = \mathbb{Z}$ (since $\mathbb{Z}$ is a binomial ring).

Proof of Theorem 41. Let N be the nest $\mathbb{N}_+$. Define a family $(b_n)_{n \in N} \in A^N$ by $(b_n = q^n \text{ for every } n \in N)$. According to Theorem 30, the assertions $\mathcal{C}_{\text{bin}}$, $\mathcal{D}_{\text{bin}}$, $\mathcal{D}'_{\text{bin}}$, $\mathcal{D}^{\text{expl}}_{\text{bin}}$, $\mathcal{D}^{\text{expl}\prime}_{\text{bin}}$, $\mathcal{E}_{\text{bin}}$, $\mathcal{E}'_{\text{bin}}$, $\mathcal{F}_{\text{bin}}$, $\mathcal{G}_{\text{bin}}$, $\mathcal{H}_{\text{bin}}$, $\mathcal{I}_{\text{bin}}$ and $\mathcal{I}'_{\text{bin}}$ are equivalent (these assertions were stated in Theorem 30). Since the assertion $\mathcal{C}_{\text{bin}}$ is true for our family $(b_n)_{n \in N} \in A^N$ (because every $n \in N$ and every $p \in \operatorname{PF} n$ satisfies

$$\begin{aligned} b_{n/p} &= q^{n/p} && \text{(by the definition of } b_{n/p}) \\ &\equiv q^n && \left(\text{since Lemma 18 yields } q^n \equiv q^{n/p} \bmod p^{v_p(n)} A\right) \\ &= b_n \bmod p^{v_p(n)} A \end{aligned}$$

), this yields that the assertions $\mathcal{D}_{\text{bin}}$, $\mathcal{D}'_{\text{bin}}$, $\mathcal{D}^{\text{expl}}_{\text{bin}}$, $\mathcal{D}^{\text{expl}\prime}_{\text{bin}}$, $\mathcal{E}_{\text{bin}}$, $\mathcal{E}'_{\text{bin}}$, $\mathcal{F}_{\text{bin}}$, $\mathcal{G}_{\text{bin}}$, $\mathcal{H}_{\text{bin}}$, $\mathcal{I}_{\text{bin}}$ and $\mathcal{I}'_{\text{bin}}$ must also be true for our family $(b_n)_{n\in N} \in A^N$. But for the family $(b_n)_{n\in N} \in A^N$,

- assertion $\mathcal{D}'_{\text{bin}}$ is equivalent to Theorem 41 **(a)** (since $N = \mathbb{N}_+$ and $b_n = q^n$);
- assertion $\mathcal{E}'_{\text{bin}}$ is equivalent to Theorem 41 **(b)** (since $N = \mathbb{N}_+$ and $b_n = q^n$);
- assertion $\mathcal{F}_{\text{bin}}$ is equivalent to Theorem 41 **(c)** (since $N = \mathbb{N}_+$ and $b_{n/d} = q^{n/d}$);
- assertion $\mathcal{G}_{\text{bin}}$ is equivalent to Theorem 41 **(d)** (since $N = \mathbb{N}_+$ and $b_{n/d} = q^{n/d}$);
- assertion $\mathcal{H}_{\text{bin}}$ is equivalent to Theorem 41 **(e)** (since $N = \mathbb{N}_+$ and $b_{\gcd(i,n)} = q^{\gcd(i,n)}$);
- assertion $\mathcal{I}'_{\text{bin}}$ is equivalent to Theorem 41 **(f)** (since $N = \mathbb{N}_+$ and $b_n = q^n$).

Hence, Theorem 41 **(a)**, Theorem 41 **(b)**, Theorem 41 **(c)**, Theorem 41 **(d)**, Theorem 41 **(e)** and Theorem 41 **(f)** must be true (since the assertions $\mathcal{D}'_{\text{bin}}$, $\mathcal{E}'_{\text{bin}}$, $\mathcal{F}_{\text{bin}}$, $\mathcal{G}_{\text{bin}}$, $\mathcal{H}_{\text{bin}}$ and $\mathcal{I}'_{\text{bin}}$ are true for the family $(b_n)_{n\in N} \in A^N$). This proves Theorem 41.

Here is a more interesting corollary:

Theorem 42. Let A be a binomial ring. Let $q \in A$ and $r \in \mathbb{Q}$. Then:

(a) There exists *one and only one* family $(x_n)_{n\in\mathbb{N}_+} \in A^{\mathbb{N}_+}$ of elements of A 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 $(y_n)_{n\in\mathbb{N}_+} \in A^{\mathbb{N}_+}$ of elements of A 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

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

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

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

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

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

(f) There exists *one and only one* family $(q_n)_{n \in N} \in A^N$ of elements of A such that

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

This Theorem 42 generalizes Theorem 17 from [5]. Indeed, Theorem 17 from [5] can be proven by applying Theorem 42 (more precisely, parts **(a)**, **(b)**, **(c)**, **(d)** and **(e)** of Theorem 42) to $A = \mathbb{Z}$ (since $\mathbb{Z}$ is a binomial ring).

Proof of Theorem 42. Let N be the nest $\mathbb{N}_+$. Define a family $(b_n)_{n \in N} \in A^N$ by $\left(b_n = \binom{qn}{rn} \text{ for every } n \in N \right)$. According to Theorem 30, the assertions $\mathcal{C}_{\text{bin}}$, $\mathcal{D}_{\text{bin}}$, $\mathcal{D}'_{\text{bin}}$, $\mathcal{D}^{\text{expl}}_{\text{bin}}$, $\mathcal{D}^{\text{expl}\prime}_{\text{bin}}$, $\mathcal{E}_{\text{bin}}$, $\mathcal{E}'_{\text{bin}}$, $\mathcal{F}_{\text{bin}}$, $\mathcal{G}_{\text{bin}}$, $\mathcal{H}_{\text{bin}}$, $\mathcal{I}_{\text{bin}}$ and $\mathcal{I}'_{\text{bin}}$ are equivalent (these assertions were stated in Theorem 30). Since the assertion $\mathcal{C}_{\text{bin}}$ is true for our family $(b_n)_{n \in N} \in A^N$ (because every $n \in N$ and every $p \in \operatorname{PF} n$ satisfies

$$\begin{aligned} b_{n/p} &= \binom{q(n/p)}{r(n/p)} && \text{(by the definition of } b_{n/p}) \\ &= \binom{qn/p}{rn/p} \equiv \binom{qn}{rn} && \text{(by Lemma 15)} \\ &= b_n \bmod p^{v_p(n)} A \end{aligned}$$

), this yields that the assertions $\mathcal{D}_{\text{bin}}$, $\mathcal{D}'_{\text{bin}}$, $\mathcal{D}^{\text{expl}}_{\text{bin}}$, $\mathcal{D}^{\text{expl}\prime}_{\text{bin}}$, $\mathcal{E}_{\text{bin}}$, $\mathcal{E}'_{\text{bin}}$, $\mathcal{F}_{\text{bin}}$, $\mathcal{G}_{\text{bin}}$, $\mathcal{H}_{\text{bin}}$, $\mathcal{I}_{\text{bin}}$ and $\mathcal{I}'_{\text{bin}}$ must also be true for our family $(b_n)_{n \in N} \in A^N$. But for the family $(b_n)_{n \in N} \in A^N$,

- assertion $\mathcal{D}'_{\text{bin}}$ is equivalent to Theorem 42 **(a)** (since $N = \mathbb{N}_+$ and $b_n = \binom{qn}{rn}$);
- assertion $\mathcal{E}'_{\text{bin}}$ is equivalent to Theorem 42 **(b)** (since $N = \mathbb{N}_+$ and $b_n = \binom{qn}{rn}$);
- assertion $\mathcal{F}_{\text{bin}}$ is equivalent to Theorem 42 **(c)** (since $N = \mathbb{N}_+$ and $b_{n/d} = \binom{q(n/d)}{r(n/d)} = \binom{qn/d}{rn/d}$);
- assertion $\mathcal{G}_{\text{bin}}$ is equivalent to Theorem 42 **(d)** (since $N = \mathbb{N}_+$ and $b_{n/d} = \binom{q(n/d)}{r(n/d)} = \binom{qn/d}{rn/d}$);

- assertion $\mathcal{H}_{\text{bin}}$ is equivalent to Theorem 42 **(e)** (since $N = \mathbb{N}_+$ and $b_{\gcd(i,n)} = \binom{q \gcd(i,n)}{r \gcd(i,n)}$);
- assertion $\mathcal{I}'_{\text{bin}}$ is equivalent to Theorem 42 **(f)** (since $N = \mathbb{N}_+$ and $b_n = \binom{q(n/d)}{r(n/d)} = \binom{qn/d}{rn/d}$).

Hence, Theorem 42 **(a)**, Theorem 42 **(b)**, Theorem 42 **(c)**, Theorem 42 **(d)**, Theorem 42 **(e)** and Theorem 42 **(f)** must be true (since the assertions $\mathcal{D}'_{\text{bin}}$, $\mathcal{E}'_{\text{bin}}$, $\mathcal{F}_{\text{bin}}$, $\mathcal{G}_{\text{bin}}$, $\mathcal{H}_{\text{bin}}$ and $\mathcal{I}'_{\text{bin}}$ are true for the family $(b_n)_{n \in N} \in A^N$). This proves Theorem 42.

Furthermore, we have:

Theorem 43. Let A be a binomial ring. Let $q \in A$ and $r \in \mathbb{Z}$. Then:

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

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

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

$$\sum_{d \mid n} \mu(d) \binom{qn/d - 1}{rn/d - 1} \in nA.$$

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

$$\sum_{d \mid n} \phi(d) \binom{qn/d - 1}{rn/d - 1} \in nA.$$

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

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

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

$$\sum_{d \mid n} \mu(d) \binom{qn/d}{rn/d} \in \frac{q}{r} nA.$$

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

$$\sum_{d \mid n} \phi(d) \binom{qn/d}{rn/d} \in \frac{q}{r} nA.$$

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

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

(i) There exists *one and only one* family $(q_n)_{n \in N} \in A^N$ of elements of A such that

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

This Theorem 43 generalizes Theorem 20 from [5]. Indeed, Theorem 20 from [5] can be proven by applying Theorem 43 (more precisely, parts **(a)**, **(b)**, **(c)**, **(d)**, **(e)**, **(f)**, **(g)** and **(h)** of Theorem 43) to $A = \mathbb{Z}$ (since $\mathbb{Z}$ is a binomial ring).

Proof of Theorem 43. Let N be the nest $\mathbb{N}_+$. Define a family $(b_n)_{n \in N} \in A^N$ by $\left(b_n = \binom{qn-1}{rn-1} \text{ for every } n \in N \right)$. According to Theorem 30, the assertions $\mathcal{C}_{\text{bin}}$, $\mathcal{D}_{\text{bin}}$, $\mathcal{D}'_{\text{bin}}$, $\mathcal{D}^{\text{expl}}_{\text{bin}}$, $\mathcal{D}^{\text{expl}\prime}_{\text{bin}}$, $\mathcal{E}_{\text{bin}}$, $\mathcal{E}'_{\text{bin}}$, $\mathcal{F}_{\text{bin}}$, $\mathcal{G}_{\text{bin}}$, $\mathcal{H}_{\text{bin}}$, $\mathcal{I}_{\text{bin}}$ and $\mathcal{I}'_{\text{bin}}$ are equivalent (these assertions were stated in Theorem 30). Since the assertion $\mathcal{C}_{\text{bin}}$ is true for our family $(b_n)_{n \in N} \in A^N$ (because every $n \in N$ and every $p \in \operatorname{PF} n$ satisfies

$$\begin{aligned} b_{n/p} &= \binom{q(n/p)-1}{r(n/p)-1} && \text{(by the definition of } b_{n/p}) \\ &= \binom{qn/p-1}{rn/p-1} \equiv \binom{qn-1}{rn-1} && \text{(by Corollary 19)} \\ &= b_n \bmod p^{v_p(n)} A \end{aligned}$$

), this yields that the assertions $\mathcal{D}_{\text{bin}}$, $\mathcal{D}'_{\text{bin}}$, $\mathcal{D}^{\text{expl}}_{\text{bin}}$, $\mathcal{D}^{\text{expl}\prime}_{\text{bin}}$, $\mathcal{E}_{\text{bin}}$, $\mathcal{E}'_{\text{bin}}$, $\mathcal{F}_{\text{bin}}$, $\mathcal{G}_{\text{bin}}$, $\mathcal{H}_{\text{bin}}$, $\mathcal{I}_{\text{bin}}$ and $\mathcal{I}'_{\text{bin}}$ must also be true for our family $(b_n)_{n \in N} \in A^N$. But for the family $(b_n)_{n \in N} \in A^N$,

- assertion $\mathcal{D}'_{\text{bin}}$ is equivalent to Theorem 43 **(a)** (since $N = \mathbb{N}_+$ and $b_n = \binom{qn-1}{rn-1}$);
- assertion $\mathcal{E}'_{\text{bin}}$ is equivalent to Theorem 43 **(b)** (since $N = \mathbb{N}_+$ and $b_n = \binom{qn-1}{rn-1}$);
- assertion $\mathcal{F}_{\text{bin}}$ is equivalent to Theorem 43 **(c)** (since $N = \mathbb{N}_+$ and $b_{n/d} = \binom{q(n/d)-1}{r(n/d)-1} = \binom{qn/d-1}{rn/d-1}$);

- assertion $\mathcal{G}_{\text{bin}}$ is equivalent to Theorem 43 **(d)** (since $N = \mathbb{N}_+$ and $b_{n/d} = \binom{q\,(n/d)-1}{r\,(n/d)-1} = \binom{qn/d-1}{rn/d-1}$);
- assertion $\mathcal{H}_{\text{bin}}$ is equivalent to Theorem 43 **(e)** (since $N = \mathbb{N}_+$ and $b_{\gcd(i,n)} = \binom{q\gcd(i,n)-1}{r\gcd(i,n)-1}$);
- assertion $\mathcal{I}'_{\text{bin}}$ is equivalent to Theorem 43 **(i)** (since $N = \mathbb{N}_+$ and $b_n = \binom{q\,(n/d)-1}{r\,(n/d)-1} = \binom{qn/d-1}{rn/d-1}$).

Hence, Theorem 43 **(a)**, Theorem 43 **(b)**, Theorem 43 **(c)**, Theorem 43 **(d)**, Theorem 43 **(e)** and Theorem 43 **(i)** must be true (since the assertions $\mathcal{D}'_{\text{bin}}$, $\mathcal{E}'_{\text{bin}}$, $\mathcal{F}_{\text{bin}}$, $\mathcal{G}_{\text{bin}}$, $\mathcal{H}_{\text{bin}}$ and $\mathcal{I}'_{\text{bin}}$ are true for the family $(b_n)_{n\in N} \in A^N$).

In order to complete the proof of Theorem 43, it now remains to verify parts **(f)**, **(g)** and **(h)** of Theorem 43.

Assume that $r \neq 0$. Thus, every $m \in \mathbb{N}_+$ satisfies $rm \neq 0$.

Theorem 43 **(f)** follows from Theorem 43 **(c)**, since

$$\sum_{d|n} \mu(d) \underbrace{\binom{qn/d}{rn/d}}_{=\frac{qn/d}{rn/d}\binom{qn/d-1}{rn/d-1}} = \sum_{d|n} \mu(d) \underbrace{\frac{qn/d}{rn/d}}_{=\frac{q}{r}} \binom{qn/d-1}{rn/d-1} = \frac{q}{r} \underbrace{\sum_{d|n} \mu(d) \binom{qn/d-1}{rn/d-1}}_{\in nA \text{ (by Theorem 43 (c))}}$$

(by Proposition 20, applied to $a=qn/d$ and $b=rn/d$)

$$\in \frac{q}{r} nA.$$

Theorem 43 **(g)** follows from Theorem 43 **(d)**, because

$$\sum_{d|n} \phi(d) \underbrace{\binom{qn/d}{rn/d}}_{=\frac{qn/d}{rn/d}\binom{qn/d-1}{rn/d-1}} = \sum_{d|n} \phi(d) \underbrace{\frac{qn/d}{rn/d}}_{=\frac{q}{r}} \binom{qn/d-1}{rn/d-1} = \frac{q}{r} \underbrace{\sum_{d|n} \phi(d) \binom{qn/d-1}{rn/d-1}}_{\in nA \text{ (by Theorem 43 (d))}}$$

(by Proposition 20, applied to $a=qn/d$ and $b=rn/d$)

$$\in \frac{q}{r} nA.$$

Theorem 43 **(h)** follows from Theorem 43 **(e)**, since

$$\sum_{i=1}^{n} \underbrace{\binom{q\gcd(i,n)}{r\gcd(i,n)}}_{\substack{=\frac{q\gcd(i,n)}{r\gcd(i,n)}\binom{q\gcd(i,n)-1}{r\gcd(i,n)-1} \\ \text{(by Proposition 20, applied to} \\ a=q\gcd(i,n) \text{ and } b=r\gcd(i,n))}} = \sum_{i=1}^{n} \underbrace{\frac{q\gcd(i,n)}{r\gcd(i,n)}}_{=\frac{q}{r}} \binom{q\gcd(i,n)-1}{r\gcd(i,n)-1}$$

$$= \frac{q}{r} \underbrace{\sum_{i=1}^{n} \binom{q\gcd(i,n)-1}{r\gcd(i,n)-1}}_{\substack{\in nA \\ \text{(by Theorem 43 (e))}}} \in \frac{q}{r} nA.$$

Now, all parts of Theorem 43 are proven. The proof of Theorem 43 is thus complete.

§5. The integer case

Since $\mathbb{Z}$ is a binomial ring, we can apply Theorem 30 to $A = \mathbb{Z}$ and obtain a result about families of integers. This alone is not very interesting. What is interesting is that we can add a further equivalent assertion to this result:

Theorem 60. Let N be a nest. Let $(b_n)_{n\in N} \in \mathbb{Z}^N$ be a family of integers. Then, the following assertions $\mathcal{C}_\varnothing$, $\mathcal{D}_\varnothing$, $\mathcal{D}'_\varnothing$, $\mathcal{D}^{\text{expl}}_\varnothing$, $\mathcal{D}^{\text{expl}\prime}_\varnothing$, $\mathcal{E}_\varnothing$, $\mathcal{E}'_\varnothing$, $\mathcal{F}_\varnothing$, $\mathcal{G}_\varnothing$, $\mathcal{H}_\varnothing$, $\mathcal{I}_\varnothing$, $\mathcal{I}'_\varnothing$, $\mathcal{K}_\varnothing$ and $\mathcal{K}^{\text{inv}}_\varnothing$ are equivalent:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Assertion $\mathcal{K}_\varnothing$: There exist two sets U and V and two maps $f : U \to U$ and $g : V \to V$ such that every $n \in N$ satisfies

$$|\mathrm{Fix}\,(f^n)| < \infty, \qquad |\mathrm{Fix}\,(g^n)| < \infty \qquad \text{and} \qquad |\mathrm{Fix}\,(f^n)| - |\mathrm{Fix}\,(g^n)| = b_n.$$

Here, whenever S is a set and $h : S \to S$ is a map, we denote by $\mathrm{Fix}\,(h)$ the set of fixed points of the map h.

Assertion $\mathcal{K}_\varnothing^{\mathrm{inv}}$: There exist two sets U and V and two *invertible* maps $f : U \to U$ and $g : V \to V$ such that every $n \in N$ satisfies

$$|\mathrm{Fix}\,(f^n)| < \infty, \qquad |\mathrm{Fix}\,(g^n)| < \infty \qquad \text{and} \qquad |\mathrm{Fix}\,(f^n)| - |\mathrm{Fix}\,(g^n)| = b_n.$$

Here, whenever S is a set and $h : S \to S$ is a map, we denote by $\mathrm{Fix}\,(h)$ the set of fixed points of the map h.

Assertions $\mathcal{K}_\varnothing$ and $\mathcal{K}_\varnothing^{\mathrm{inv}}$ appear to be of a totally different nature than the assertions preceding them, although in the proof we will see that they are actually very close to Assertion $\mathcal{E}_\varnothing$. Note that the equivalence $\mathcal{D}_\varnothing \iff \mathcal{F}_\varnothing \iff \mathcal{G}_\varnothing \iff \mathcal{H}_\varnothing$ (at least in the case when $N = \mathbb{N}_+$) appears as the Corollary on page 10 of the paper [2] by Dress and Siebeneicher; they also more or less state the equivalence $\mathcal{F}_\varnothing \iff \mathcal{G}_\varnothing \iff \mathcal{H}_\varnothing \iff \mathcal{K}_\varnothing^{\mathrm{inv}}$ (again, only in the case when $N = \mathbb{N}_+$) on page 3 (in the sentence encompassing formulas (1.5) and (1.6)).

"Almost" all of Theorem 60 follows from Theorem 30 just by setting $A = \mathbb{Z}$; the only thing that needs to be proven is the equivalence of Assertions $\mathcal{K}_\varnothing$ and $\mathcal{K}_\varnothing^{\mathrm{inv}}$ to the other assertions. While the proof of this is rather easy, it will be long because of lots of notations which we will need to introduce. Before we start with this proof, let us make a definition which has already been made in Theorem 60:

Definition 60. Whenever S is a set and $h : S \to S$ is a map, we denote by $\mathrm{Fix}\,(h)$ the set of fixed points of the map h.

We start with the following lemma, which will aid us in proving the implication $\mathcal{E}_\varnothing \iff \mathcal{K}_\varnothing^{\mathrm{inv}}$:

Lemma 61. Let N be a nest. Let $(s_n)_{n \in N} \in \mathbb{N}^N$ be a family of **nonnegative** integers. Then, there exists a set P and an *invertible* map $j : P \to P$ such that every $n \in N$ satisfies

$$|\mathrm{Fix}\,(j^n)| = \sum_{d \mid n} d s_d.$$

In order to prove this lemma, let us define the notion of a "disjoint union" of sets which are not necessarily a-priori disjoint:

Definition 61. Let I be a set. For every $i \in I$, let U_i be a set. Then, we define $\bigsqcup\limits_{i \in I} U_i$ (where i is a symbol used for indexing) to be the set $\bigcup\limits_{i \in I} \{i\} \times U_i$ (which is a subset of $I \times \left(\bigcup\limits_{i \in I} U_i \right)$). This set $\bigsqcup\limits_{i \in I} U_i$ is called

the *disjoint union* of the sets U_i over all $i \in I$. (Notice that each $i \in I$ satisfies $\{i\} \times U_i \cong U_i$ as sets, and the sets $\{i\} \times U_i$ for distinct $i \in I$ are pairwise disjoint. Hence, $\bigsqcup_{i \in I} U_i = \bigcup_{i \in I} \{i\} \times U_i$ is a union of pairwise disjoint sets which are isomorphic to the respective sets U_i. This should not be confused with the union $\bigcup_{i \in I} U_i$, which can be much smaller than $\bigsqcup_{i \in I} U_i$ when the sets U_i are not pairwise disjoint.)

Definition 62. Let I be a set. For every $i \in I$, let U_i and V_i be two sets and $f_i : U_i \to V_i$ a map. Then, we define $\bigsqcup_{i \in I} f_i$ (where i is a symbol used for indexing) to be the map $F : \bigsqcup_{i \in I} U_i \to \bigsqcup_{i \in I} V_i$ which satisfies

$$(F(i, \alpha) = (i, f_i(\alpha)) \qquad \text{for every } i \in I \text{ and every } \alpha \in U_i).$$

This map $\bigsqcup_{i \in I} f_i$ is called the *disjoint union* of the maps f_i over all $i \in I$.

The disjoint union of maps has the following properties:

Proposition 62. Let I be a set. For every $i \in I$, let U_i, V_i and W_i be three sets and $f_i : U_i \to V_i$ and $g_i : V_i \to W_i$ be two maps. Then,

$$\left(\bigsqcup_{i \in I} g_i \right) \circ \left(\bigsqcup_{i \in I} f_i \right) = \bigsqcup_{i \in I} (g_i \circ f_i)$$

as maps from $\bigsqcup_{i \in I} U_i$ to $\bigsqcup_{i \in I} W_i$.

Proposition 63. Let I be a set. For every $i \in I$, let U_i be a set. Then, the map $\bigsqcup_{i \in I} \mathrm{id}_{U_i} : \bigsqcup_{i \in I} U_i \to \bigsqcup_{i \in I} U_i$ is the identity map.

Proposition 64. Let I be a set. For every $i \in I$, let U_i and V_i be two sets and $f_i : U_i \to V_i$ an invertible map. Then, the map $\bigsqcup_{i \in I} f_i : \bigsqcup_{i \in I} U_i \to \bigsqcup_{i \in I} V_i$ is also invertible and satisfies

$$\left(\bigsqcup_{i \in I} f_i \right)^{-1} = \bigsqcup_{i \in I} \left(f_i^{-1} \right).$$

Propositions 62, 63 and 64 belong to the very fundaments of mathematics and will not be proven here.

Proof of Lemma 61 (sketched). Let J be the set $\bigsqcup_{n \in N} \{1, 2, ..., s_n\}$. Then, $J = \bigcup_{n \in N} \{n\} \times \{1, 2, ..., s_n\}$ (by the definition of $\bigsqcup_{n \in N} \{1, 2, ..., s_n\}$), so that $J \subseteq N \times \mathbb{N}_+$.

Define a map $r : N \times \mathbb{N}_+ \to N$ by

$$(r(n, i) = n \qquad \text{for every } (n, i) \in N \times \mathbb{N}_+).$$

Since $J \subseteq N \times \mathbb{N}_+$, it is clear that $r(j)$ is defined for every $j \in J$.

Let us notice that every $d \in N$ satisfies

$$\{j \in J \mid r(j) = d\} = \{d\} \times \{1, 2, ..., s_d\} \tag{53}$$

and therefore

$$|\{j \in J \mid r(j) = d\}| = |\{d\} \times \{1, 2, ..., s_d\}| = \underbrace{|\{d\}|}_{=1} \cdot \underbrace{|\{1, 2, ..., s_d\}|}_{=s_d} = s_d. \tag{54}$$

Let us now introduce some notations:

- For every positive integer d, we denote by Z_d the ring $\mathbb{Z} \diagup (d\mathbb{Z})$. This is a finite commutative ring with size

$$|Z_d| = d. \tag{55}$$

- For every $i \in \mathbb{N}$ and every positive integer d, let $\overline{i}_d$ denote the residue class of i modulo d. This residue class is an element of $\mathbb{Z} \diagup (d\mathbb{Z}) = Z_d$. Note that the map $\mathbb{Z} \to \mathbb{Z} \diagup (d\mathbb{Z})$ which sends every integer w to $\overline{w}_d$ is a ring homomorphism. Thus, $\overline{0}_d = 0$, $\overline{1}_d = 1$, and any two integers u and v satisfy $\overline{u}_d + \overline{v}_d = \overline{u+v}_d$ and $\overline{u}_d \cdot \overline{v}_d = \overline{uv}_d$.

- For every positive integer d and every integer u, define a map $P_{d,u} : Z_d \to Z_d$ by

$$(P_{d,u}(x) = x + \overline{u}_d \qquad \text{for every } x \in Z_d).$$

It is easy to see that

$$P_{d,0} = \mathrm{id}_{Z_d} \qquad \text{for every positive integer } d. \tag{56}$$

Moreover,

$$P_{d,u} \circ P_{d,v} = P_{d,u+v} \qquad \text{for every positive integer } d \text{ and any } u \in \mathbb{Z} \text{ and } v \in \mathbb{Z}. \tag{57}$$

Finally,

$$P_{d,u}^{\ell} = P_{d,\ell u} \qquad \text{for every positive integer } d, \text{ any } u \in \mathbb{Z} \text{ and any } \ell \in \mathbb{N}. \tag{58}$$

Also, for every positive integer d and every $u \in \mathbb{Z}$,

$$\text{the map } P_{d,u} : Z_d \to Z_d \text{ is invertible.} \tag{59}$$

Now, let Q be the set $\bigsqcup_{j \in J} Z_{r(j)}$. Then, $Q = \bigsqcup_{j \in J} Z_{r(j)} = \bigcup_{j \in J} \{j\} \times Z_{r(j)}$ (by the definition of $\bigsqcup_{j \in J} Z_{r(j)}$).

Now, let α be the map $\bigsqcup_{j \in J} P_{r(j),1} : \bigsqcup_{j \in J} Z_{r(j)} \to \bigsqcup_{j \in J} Z_{r(j)}$. This map is well-defined since for every $j \in J$, the map $P_{r(j),1} : Z_{r(j)} \to Z_{r(j)}$ is well-defined.

We know that the map α is a map from $\bigsqcup_{j \in J} Z_{r(j)}$ to $\bigsqcup_{j \in J} Z_{r(j)}$. Since $\bigsqcup_{j \in J} Z_{r(j)} = Q$, this rewrites as follows: The map α is a map from Q to Q.

We know that $P_{r(j),1} : Z_{r(j)} \to Z_{r(j)}$ is an invertible map for every $j \in J$ (due to (59), applied to $r(j)$ and 1 instead of d and u). Thus, Proposition 64 (applied to J, j, $Z_{r(j)}$, $Z_{r(j)}$ and $P_{r(j),1}$ instead of I, i, U_i, V_i and f_i) yields that the map $\bigsqcup_{j \in J} P_{r(j),1} : \bigsqcup_{j \in J} Z_{r(j)} \to \bigsqcup_{j \in J} Z_{r(j)}$ is also invertible and satisfies $\left(\bigsqcup_{j \in J} P_{r(j),1} \right)^{-1} = \bigsqcup_{j \in J} \left(P_{r(j),1}^{-1} \right)$.

So we know that the map $\bigsqcup_{j \in J} P_{r(j),1} : \bigsqcup_{j \in J} Z_{r(j)} \to \bigsqcup_{j \in J} Z_{r(j)}$ is invertible. Since this map $\bigsqcup_{j \in J} P_{r(j),1}$ has been called α, this rewrites as follows: The map α is invertible.

Also, every $n \in \mathbb{N}$ satisfies

$$\alpha^n = \bigsqcup_{j \in J} P_{r(j),n}. \tag{60}$$

(Indeed, this is easy to see by induction over n, using the fact that $\alpha = \bigsqcup_{j \in J} P_{r(j),1}$ as well as (57) and (56).)

Now fix an $n \in N$. It is easy to see that

$$\operatorname{Fix}(\alpha^n) = \bigcup_{\substack{j \in J; \\ r(j) | n}} \{j\} \times Z_{r(j)}$$

(since (60) shows that an element of $\{j\} \times Z_{r(j)}$ is fixed under α^n if and only if $r(j) \mid n$). Hence,

$$\begin{aligned}
|\operatorname{Fix}(\alpha^n)| &= \left| \bigcup_{\substack{j \in J; \\ r(j) | n}} \{j\} \times Z_{r(j)} \right| = \sum_{\substack{j \in J; \\ r(j) | n}} \underbrace{\left| \{j\} \times Z_{r(j)} \right|}_{= |\{j\}| \cdot \left| Z_{r(j)} \right|} \\
&\qquad \left(\text{since the sets } \{j\} \times Z_{r(j)} \text{ are clearly pairwise disjoint for distinct } j \right) \\
&= \sum_{\substack{j \in J; \\ r(j) | n}} \underbrace{|\{j\}|}_{=1} \cdot \underbrace{\left| Z_{r(j)} \right|}_{\substack{= r(j) \\ \text{(by (55), applied to} \\ r(j) \text{ instead of } d)}} = \sum_{\substack{j \in J; \\ r(j) | n}} r(j) \\
&= \sum_{\substack{d \in N; \\ d | n}} \sum_{\substack{j \in J; \\ r(j) = d}} \underbrace{r(j)}_{\substack{= d \\ (\text{since } r(j) = d)}} \\
&\qquad \text{(since every } j \in J \text{ such that } r(j) = d \text{ satisfies } r(j) \in N \text{ and } r(j) \mid n) \\
&= \sum_{\substack{d \in N; \\ d | n}} d \cdot \underbrace{(\text{the number of all } j \in J \text{ satisfying } r(j) = d)}_{\substack{= |\{j \in J \mid r(j) = d\}| = s_d \\ \text{(by (54))}}} \\
&= \sum_{\substack{d \in N; \\ d | n}} d s_d = \sum_{\substack{d | n; \\ d \in N}} d s_d = \sum_{d | n} d s_d
\end{aligned}$$

(since every divisor d of n satisfies $d \in N$ anyway).

Now forget that we fixed n. We thus have shown that every $n \in N$ satisfies $\left|\operatorname{Fix}\left(\alpha^n\right)\right| = \sum_{d \mid n} d s_d$. Moreover, we know that $\alpha : Q \to Q$ is invertible.

Hence, there exists a set P and an *invertible* map $j : P \to P$ such that every $n \in N$ satisfies

$$\left|\operatorname{Fix}\left(j^n\right)\right| = \sum_{d \mid n} d s_d$$

(namely, we can take $P = Q$ and $j = \alpha$). Lemma 61 is thus proven.

Lemma 61 almost completely takes care of the implication $\mathcal{E}_\varnothing \Longrightarrow \mathcal{K}_\varnothing^{\mathrm{inv}}$ (we will show this argument in details later). Let us now state a fact to which the implication $\mathcal{K}_\varnothing \Longrightarrow \mathcal{E}_\varnothing$ boils down to:

Proposition 65. Let N be a nest. Let P be a set, and $j : P \to P$ be a map. Assume that every $n \in N$ satisfies $\left|\operatorname{Fix}\left(j^n\right)\right| < \infty$. Then, there exists a family $\left(s_n\right)_{n \in N} \in \mathbb{N}^N$ of **nonnegative** integers such that every $n \in N$ satisfies

$$\left|\operatorname{Fix}\left(j^n\right)\right| = \sum_{d \mid n} d s_d.$$

Before we start proving this, let us state a simple lemma:

Lemma 66. Let P be a set. Let $j : P \to P$ be a map. Let n and m be nonnegative integers such that $m \mid n$. Then, $\operatorname{Fix}\left(j^m\right) \subseteq \operatorname{Fix}\left(j^n\right)$.

The proof of this is a well-known induction argument and left to the reader. We record another lemma:

Lemma 67. Let X be a finite set. Let $j : X \to X$ be a map. Let $n \in \mathbb{N}_+$. Assume that

$$\text{every } x \in X \text{ satisfies } j^n(x) = x. \tag{61}$$

Assume also that

$$\text{every } x \in X \text{ and } k \in \{1, 2, ..., n-1\} \text{ satisfy } j^k(x) \neq x. \tag{62}$$

Then, $|X|$ is a nonnegative integer divisible by n.

Again, this is a well-known fact. Here is a very brief sketch of its proof:

Proof of Lemma 67 (sketched). Clearly, $|X|$ is a nonnegative integer (since X is finite). Let Z_n be the cyclic group with n elements, and ζ a generator of Z_n. Then, the group Z_n can be presented by its generator ζ with the only relation being $\zeta^n = 1$. But from (61), we know that $j^n = \mathrm{id}_X$. Hence, we can define a group action of the group Z_n on the set X by letting $\zeta \cdot x = j(x)$ for every $x \in X$. This action is free (due to (62)). Hence, every orbit under this action has size $|Z_n| = n$. But the set X is the disjoint union of all orbits under the action. Hence, $|X|$ is the sum of the sizes of these orbits. Since the size of each orbit is n, this yields that $|X|$ is the sum of several n's. Thus, $|X|$ is divisible by n. This proves Lemma 67.

Finally, one more classical lemma:

Lemma 68. Let X be a set. Let $j : X \to X$ be a map. Let $x \in X$. Assume that the set $\{m \in \mathbb{N}_+ \mid j^m(x) = x\}$ is nonempty. Then, there exists an $f \in \mathbb{N}_+$ such that

$$\{m \in \mathbb{N}_+ \mid j^m(x) = x\} = f \cdot \mathbb{N}_+.$$

Lemma 68 is a well-known fact (even if not usually written in this form). It is (more or less) the reason why every element of a finite group has a well-defined order. The proof proceeds by letting f be the smallest element of $\{m \in \mathbb{N}_+ \mid j^m(x) = x\}$ (indeed, such an element exists because $\{m \in \mathbb{N}_+ \mid j^m(x) = x\}$ is a nonempty subset of $\mathbb{N}_+$), and showing that $\{m \in \mathbb{N}_+ \mid j^m(x) = x\} = f \cdot \mathbb{N}_+$ (this uses division with remainder). We will not give any more details on this proof.

Proof of Proposition 65. For every $n \in N$, define a subset $\mathfrak{F}_n$ of $\operatorname{Fix}(j^n)$ by

$$\mathfrak{F}_n = (\operatorname{Fix}(j^n)) \setminus \bigcup_{\substack{e \in N; \\ e < n}} (\operatorname{Fix}(j^e)). \tag{63}$$

Since $\mathfrak{F}_n$ is a subset of $\operatorname{Fix}(j^n)$, we have

$$|\mathfrak{F}_n| \leq |\operatorname{Fix}(j^n)| < \infty \qquad \text{for every } n \in N.$$

That is, $\mathfrak{F}_n$ is a finite set for every $n \in N$.

Now, we are going to show the following assertions:

Assertion 1: Every $n \in N$ satisfies

$$\operatorname{Fix}(j^n) = \bigcup_{\substack{d \in N; \\ d \mid n}} \mathfrak{F}_d.$$

Assertion 2: The sets $\mathfrak{F}_d$ for distinct $d \in N$ are pairwise disjoint.

Assertion 3: For every $n \in N$, we have

$$|\operatorname{Fix}(j^n)| = \sum_{\substack{d \in N; \\ d \mid n}} |\mathfrak{F}_d|.$$

Assertion 4: For every $n \in N$, the number $|\mathfrak{F}_n|$ is a nonnegative integer divisible by n.

Proof of Assertion 1: Let $n \in N$. Since N is a nest, this yields that every divisor of n lies in N (because every divisor of an element of a nest must lie in that nest).

Let $x \in \operatorname{Fix}(j^n)$ be arbitrary. We are going to show that $x \in \bigcup_{\substack{d \in N; \\ d \mid n}} \mathfrak{F}_d$.

Indeed, we know that $x \in \operatorname{Fix}(j^n)$. That is, x is a fixed point of the map j^n. Thus $j^n(x) = x$.

Now, $n \in N \subseteq \mathbb{N}_+$ and $j^n(x) = x$. Hence, there exists an $m \in \mathbb{N}_+$ such that $j^m(x) = x$ (namely, $m = n$). In other words, the set $\{m \in \mathbb{N}_+ \mid j^m(x) = x\}$ is nonempty. Hence, Lemma 68 (applied to P instead of X) yields that there exists an $f \in \mathbb{N}_+$ such that

$$\{m \in \mathbb{N}_+ \mid j^m(x) = x\} = f \cdot \mathbb{N}_+. \tag{64}$$

Consider this f.

Since $n \in \mathbb{N}_+$ and $j^n(x) = x$, we have $n \in \{m \in \mathbb{N}_+ \mid j^m(x) = x\} = f \cdot \mathbb{N}_+$ (by (64)). Thus, $f \mid n$. Since $f \in \mathbb{N}_+$, this yields that f is a divisor of n. Since every divisor of n lies in N, this yields that f lies in N. Thus, $f \in N$. On the other hand,

$$f = f \cdot \underbrace{1}_{\in \mathbb{N}_+} \in f \cdot \mathbb{N}_+ = \{m \in \mathbb{N}_+ \mid j^m(x) = x\} \qquad \text{(by (64))},$$

so that $f \in \mathbb{N}_+$ and $j^f(x) = x$. We can rewrite $j^f(x) = x$ as $x \in \operatorname{Fix}\left(j^f\right)$.

On the other hand, it is easy to see (using (64)) that

$$x \notin \bigcup_{\substack{e \in N; \\ e < f}} \left(\operatorname{Fix}\left(j^e\right)\right)$$

[22]. Combining this with $x \in \operatorname{Fix}\left(j^f\right)$, we obtain

$$x \in \left(\operatorname{Fix}\left(j^f\right)\right) \setminus \bigcup_{\substack{e \in N; \\ e < f}} \left(\operatorname{Fix}\left(j^e\right)\right) = \mathfrak{F}_f$$

(since $\mathfrak{F}_f = \left(\operatorname{Fix}\left(j^f\right)\right) \setminus \bigcup_{\substack{e \in N; \\ e < f}} \left(\operatorname{Fix}\left(j^e\right)\right)$ by the definition of $\mathfrak{F}_f$). Thus, $x \in \mathfrak{F}_f \subseteq \bigcup_{\substack{d \in N; \\ d \mid n}} \mathfrak{F}_d$ (since f is an element of N satisfying $f \mid n$).

Now, forget that we have fixed x. We thus have shown that every $x \in \operatorname{Fix}\left(j^n\right)$ satisfies $x \in \bigcup_{\substack{d \in N; \\ d \mid n}} \mathfrak{F}_d$. In other words,

$$\operatorname{Fix}\left(j^n\right) \subseteq \bigcup_{\substack{d \in N; \\ d \mid n}} \mathfrak{F}_d. \tag{65}$$

Now, let y be any element of $\bigcup_{\substack{d \in N; \\ d \mid n}} \mathfrak{F}_d$. We are going to prove that $y \in \operatorname{Fix}\left(j^n\right)$.

Since $y \in \bigcup_{\substack{d \in N; \\ d \mid n}} \mathfrak{F}_d$, there exists a $g \in N$ satisfying $g \mid n$ satisfying $y \in \mathfrak{F}_g$. Consider this g. Since $g \in N \subseteq \mathbb{N}_+$, we know that g is a nonnegative integer. Now,

$$y \in \mathfrak{F}_g = \left(\operatorname{Fix}\left(j^g\right)\right) \setminus \bigcup_{\substack{e \in N; \\ e < g}} \left(\operatorname{Fix}\left(j^e\right)\right) \qquad \text{(by the definition of } \mathfrak{F}_g\text{)}$$

$$\subseteq \operatorname{Fix}\left(j^g\right) \subseteq \operatorname{Fix}\left(j^n\right) \qquad \text{(by Lemma 66, applied to } g \text{ instead of } m \text{ (since } g \mid n\text{))}.$$

[22] *Proof:* Assume (for the sake of contradiction) that $x \in \bigcup_{\substack{e \in N; \\ e < f}} \left(\operatorname{Fix}\left(j^e\right)\right)$. Then, there exists an element $e \in N$ satisfying $e < f$ such that $x \in \operatorname{Fix}\left(j^e\right)$. Consider this e.

We have $x \in \operatorname{Fix}\left(j^e\right)$. This means that $j^e(x) = x$. Also, $e \in N \subseteq \mathbb{N}_+$. Since $e \in \mathbb{N}_+$ and $j^e(x) = x$, we have $e \in \{m \in \mathbb{N}_+ \mid j^m(x) = x\} = f \cdot \mathbb{N}_+$ (by (64)). Since every element of $f \cdot \mathbb{N}_+$ is $\geq f$, this shows that $e \geq f$. But this contradicts $e < f$. This contradiction shows that our assumption (that $x \in \bigcup_{\substack{e \in N; \\ e < f}} \left(\operatorname{Fix}\left(j^e\right)\right)$) was wrong. Hence, we have $x \notin \bigcup_{\substack{e \in N; \\ e < f}} \left(\operatorname{Fix}\left(j^e\right)\right)$, qed.

Now, forget that we fixed y. We thus have proven that every $y \in \bigcup\limits_{\substack{d \in N; \\ d \mid n}} \mathfrak{F}_d$ satisfies $y \in \operatorname{Fix}\left(j^n\right)$. In other words,

$$\bigcup_{\substack{d \in N; \\ d \mid n}} \mathfrak{F}_d \subseteq \operatorname{Fix}\left(j^n\right).$$

Combined with (65), this yields $\operatorname{Fix}\left(j^n\right) = \bigcup\limits_{\substack{d \in N; \\ d \mid n}} \mathfrak{F}_d$. This proves Assertion 1.

Proof of Assertion 2: Let d_1 and d_2 be two distinct elements of N. We are going to prove that the sets $\mathfrak{F}_{d_1}$ and $\mathfrak{F}_{d_2}$ are disjoint.

Indeed, since d_1 and d_2 are distinct, we have either $d_1 < d_2$ or $d_2 < d_1$. Since the situation is symmetric with respect to d_1 and d_2, we can WLOG assume that $d_1 < d_2$. So assume this.

Let $x \in \mathfrak{F}_{d_1} \cap \mathfrak{F}_{d_2}$.

By the definition of $\mathfrak{F}_{d_1}$, we have

$$\mathfrak{F}_{d_1} = \left(\operatorname{Fix}\left(j^{d_1}\right)\right) \setminus \bigcup_{\substack{e \in N; \\ e < d_1}} \left(\operatorname{Fix}\left(j^e\right)\right) \subseteq \operatorname{Fix}\left(j^{d_1}\right).$$

Now, $x \in \mathfrak{F}_{d_1} \cap \mathfrak{F}_{d_2} \subseteq \mathfrak{F}_{d_1} \subseteq \operatorname{Fix}\left(j^{d_1}\right) \subseteq \bigcup\limits_{\substack{e \in N; \\ e < d_2}} \left(\operatorname{Fix}\left(j^e\right)\right)$ (since $d_1 \in N$ and $d_1 < d_2$).

But by the definition of $\mathfrak{F}_{d_2}$, we have

$$\mathfrak{F}_{d_2} = \left(\operatorname{Fix}\left(j^{d_2}\right)\right) \setminus \bigcup_{\substack{e \in N; \\ e < d_2}} \left(\operatorname{Fix}\left(j^e\right)\right).$$

Thus, $x \in \mathfrak{F}_{d_1} \cap \mathfrak{F}_{d_2} \subseteq \mathfrak{F}_{d_2} = \left(\operatorname{Fix}\left(j^{d_2}\right)\right) \setminus \bigcup\limits_{\substack{e \in N; \\ e < d_2}} \left(\operatorname{Fix}\left(j^e\right)\right)$. Consequently, $x \notin \bigcup\limits_{\substack{e \in N; \\ e < d_2}} \left(\operatorname{Fix}\left(j^e\right)\right)$. This contradicts the fact that $x \in \bigcup\limits_{\substack{e \in N; \\ e < d_2}} \left(\operatorname{Fix}\left(j^e\right)\right)$.

Now forget that we fixed x. We thus have found a contradiction for every $x \in \mathfrak{F}_{d_1} \cap \mathfrak{F}_{d_2}$. In other words, there exists no $x \in \mathfrak{F}_{d_1} \cap \mathfrak{F}_{d_2}$. In other words, $\mathfrak{F}_{d_1} \cap \mathfrak{F}_{d_2} = \varnothing$. We thus have shown that the sets $\mathfrak{F}_{d_1}$ and $\mathfrak{F}_{d_2}$ are disjoint.

Now forget that we fixed d_1 and d_2. We thus have proven that for any two distinct elements d_1 and d_2 of N, the sets $\mathfrak{F}_{d_1}$ and $\mathfrak{F}_{d_2}$ are disjoint. In other words: The sets $\mathfrak{F}_d$ for distinct $d \in N$ are pairwise disjoint. This proves Assertion 2.

Proof of Assertion 3: Let $n \in N$. Assertion 2 says that the sets $\mathfrak{F}_d$ for distinct $d \in N$ are pairwise disjoint. In particular, this yields that the sets $\mathfrak{F}_d$ for distinct $d \in N$ satisfying $d \mid n$ are pairwise disjoint. Hence, the union $\bigcup\limits_{\substack{d \in N; \\ d \mid n}} \mathfrak{F}_d$ is a union of pairwise disjoint sets, so that we have $\left| \bigcup\limits_{\substack{d \in N; \\ d \mid n}} \mathfrak{F}_d \right| = \sum\limits_{\substack{d \in N; \\ d \mid n}} \left|\mathfrak{F}_d\right|$. But Assertion 1

yields $\operatorname{Fix}(j^n) = \bigcup\limits_{\substack{d \in N; \\ d \mid n}} \mathfrak{F}_d$, and thus

$$|\operatorname{Fix}(j^n)| = \left| \bigcup_{\substack{d \in N; \\ d \mid n}} \mathfrak{F}_d \right| = \sum_{\substack{d \in N; \\ d \mid n}} |\mathfrak{F}_d| .$$

This proves Assertion 3.

Proof of Assertion 4: Let $n \in N$. Since N is a nest, this yields that every divisor of n lies in N (because every divisor of an element of a nest must lie in that nest).

Clearly, $n \in N \subseteq \mathbb{N}_+$. It is now easy to see that

$$\text{every } x \in \mathfrak{F}_n \text{ satisfies } j^n(x) = x. \tag{66}$$

[23]

Furthermore,

$$\text{every } x \in \mathfrak{F}_n \text{ and } k \in \{1, 2, ..., n-1\} \text{ satisfy } j^k(x) \neq x. \tag{67}$$

[24]

---

[23] *Proof of (66):* Let $x \in \mathfrak{F}_n$. Then,

$$x \in \mathfrak{F}_n = (\operatorname{Fix}(j^n)) \setminus \bigcup_{\substack{e \in N; \\ e < n}} (\operatorname{Fix}(j^e)) \subseteq \operatorname{Fix}(j^n) .$$

Hence, x is a fixed point of the map j^n. In other words, $j^n(x) = x$. This proves (66).

[24] *Proof of (67):* Let $x \in \mathfrak{F}_n$ and $k \in \{1, 2, ..., n-1\}$. Assume (for the sake of contradiction) that $j^k(x) = x$.

So we have $k \in \{1, 2, ..., n-1\} \subseteq \mathbb{N}_+$ and $j^k(x) = x$. Hence, there exists an $m \in \mathbb{N}_+$ such that $j^m(x) = x$ (namely, $m = k$). In other words, the set $\{m \in \mathbb{N}_+ \mid j^m(x) = x\}$ is nonempty. Thus, Lemma 68 yields that there exists an $f \in \mathbb{N}_+$ such that

$$\{m \in \mathbb{N}_+ \mid j^m(x) = x\} = f \cdot \mathbb{N}_+. \tag{68}$$

Consider this f.

Since $n \in \mathbb{N}_+$ and $j^n(x) = x$ (by (66)), we have $n \in \{m \in \mathbb{N}_+ \mid j^m(x) = x\} = f \cdot \mathbb{N}_+$ (by (68)). Thus, $f \mid n$. Since $f \in \mathbb{N}_+$, this shows that f is a divisor of n. Since every divisor of n lies in N, this shows that $f \in N$.

On the other hand, since $k \in \mathbb{N}_+$ and $j^k(x) = x$, we have $k \in \{m \in \mathbb{N}_+ \mid j^m(x) = x\} = f \cdot \mathbb{N}_+$ (by (68)). Thus, $f \mid k$. Since $k \in \mathbb{N}_+$, this yields that $f \leq k$. But $k < n$ (since $k \in \{1, 2, ..., n-1\}$). Thus, $f \leq k < n$.

Now,

$$f = f \cdot \underbrace{1}_{\in \mathbb{N}_+} \in f \cdot \mathbb{N}_+ = \{m \in \mathbb{N}_+ \mid j^m(x) = x\} \qquad \text{(by (68))},$$

so that $f \in \mathbb{N}_+$ and $j^f(x) = x$. In other words, x is a fixed point of the map j^f, so that

$$x \in \operatorname{Fix}\left(j^f\right) \subseteq \bigcup_{\substack{e \in N; \\ e < n}} (\operatorname{Fix}(j^e)) \tag{69}$$

(since $f \in N$ and $f < n$).

Now we know that (66) and (67) hold, and that $\mathfrak{F}_n$ is a finite set. Thus we can almost apply Lemma 67 to $\mathfrak{F}_n$ instead of X; the only thing that prevents us from doing so is the fact that j is a map $P \to P$ rather than a map $\mathfrak{F}_n \to \mathfrak{F}_n$. But we can easily see that $j(\mathfrak{F}_n) \subseteq \mathfrak{F}_n$ (mainly using (66)), which means that j **restricts to** a map $\mathfrak{F}_n \to \mathfrak{F}_n$. Applying Lemma 67 to $\mathfrak{F}_n$ and this restriction instead of X and j, we conclude that $|\mathfrak{F}_n|$ is a nonnegative integer divisible by n. This proves Assertion 4.

We have now proven all four assertions 1, 2, 3 and 4. It is now very easy to conclude the proof of Proposition 65: We know that $\left(\dfrac{|\mathfrak{F}_n|}{n}\right)_{n \in N}$ is a family of nonnegative integers (since, for every $n \in N$, Assertion 4 yields that $|\mathfrak{F}_n|$ is a nonnegative integer divisible by n, so that $\dfrac{|\mathfrak{F}_n|}{n}$ is a nonnegative integer). That is, $\left(\dfrac{|\mathfrak{F}_n|}{n}\right)_{n \in N} \in \mathbb{N}^N$. Moreover, for every $n \in N$, we have

$$\begin{aligned} |\mathrm{Fix}\,(j^n)| &= \sum_{\substack{d \in N; \\ d \mid n}} \underbrace{|\mathfrak{F}_d|}_{= d \cdot \frac{|\mathfrak{F}_d|}{d}} \qquad \text{(by Assertion 3)} \\ &= \sum_{\substack{d \in N; \\ d \mid n}} d \cdot \frac{|\mathfrak{F}_d|}{d}. \end{aligned}$$

Hence, there exists a family $(s_n)_{n \in N} \in \mathbb{N}^N$ of **nonnegative** integers such that every $n \in N$ satisfies

$$|\mathrm{Fix}\,(j^n)| = \sum_{d \mid n} d s_d$$

(namely, $\left(\dfrac{|\mathfrak{F}_n|}{n}\right)_{n \in N}$ is such a family). Proposition 65 is thus proven.

Proof of Theorem 60. Set $A = \mathbb{Z}$. Thus, elements of A are the same thing as integers. From Proposition 5, we know that $\mathbb{Z}$ is a binomial ring. In other words, A is a binomial ring (since $A = Z$).

By Theorem 30, the assertions $\mathcal{C}_{\mathrm{bin}}$, $\mathcal{D}_{\mathrm{bin}}$, $\mathcal{D}'_{\mathrm{bin}}$, $\mathcal{D}^{\mathrm{expl}}_{\mathrm{bin}}$, $\mathcal{D}^{\mathrm{expl}\prime}_{\mathrm{bin}}$, $\mathcal{E}_{\mathrm{bin}}$, $\mathcal{E}'_{\mathrm{bin}}$, $\mathcal{F}_{\mathrm{bin}}$, $\mathcal{G}_{\mathrm{bin}}$, $\mathcal{H}_{\mathrm{bin}}$, $\mathcal{I}_{\mathrm{bin}}$ and $\mathcal{I}'_{\mathrm{bin}}$ listed in Theorem 30 are equivalent.

Now, comparing the assertions $\mathcal{C}_{\mathrm{bin}}$, $\mathcal{D}_{\mathrm{bin}}$, $\mathcal{D}'_{\mathrm{bin}}$, $\mathcal{D}^{\mathrm{expl}}_{\mathrm{bin}}$, $\mathcal{D}^{\mathrm{expl}\prime}_{\mathrm{bin}}$, $\mathcal{E}_{\mathrm{bin}}$, $\mathcal{E}'_{\mathrm{bin}}$, $\mathcal{F}_{\mathrm{bin}}$, $\mathcal{G}_{\mathrm{bin}}$, $\mathcal{H}_{\mathrm{bin}}$, $\mathcal{I}_{\mathrm{bin}}$ and $\mathcal{I}'_{\mathrm{bin}}$ with the respective assertions $\mathcal{C}_{\varnothing}$, $\mathcal{D}_{\varnothing}$, $\mathcal{D}'_{\varnothing}$, $\mathcal{D}^{\mathrm{expl}}_{\varnothing}$, $\mathcal{D}^{\mathrm{expl}\prime}_{\varnothing}$, $\mathcal{E}_{\varnothing}$, $\mathcal{E}'_{\varnothing}$, $\mathcal{F}_{\varnothing}$, $\mathcal{G}_{\varnothing}$, $\mathcal{H}_{\varnothing}$, $\mathcal{I}_{\varnothing}$ and $\mathcal{I}'_{\varnothing}$, we notice that:

- we have $\mathcal{C}_{\mathrm{bin}} \Longleftrightarrow \mathcal{C}_{\varnothing}$ (since $A = \mathbb{Z}$);

But

$$x \in \mathfrak{F}_n = (\mathrm{Fix}\,(j^n)) \setminus \bigcup_{\substack{e \in N; \\ e < n}} (\mathrm{Fix}\,(j^e))$$

(by the definition of $\mathfrak{F}_n$). Hence, $x \notin \bigcup\limits_{\substack{e \in N; \\ e < n}} (\mathrm{Fix}\,(j^e))$. This contradicts (69). This contradiction shows that our assumption (that $j^k(x) = x$) was wrong. Thus, $j^k(x) \neq x$. This proves (67).

- we have $\mathcal{D}_{\text{bin}} \Longleftrightarrow \mathcal{D}_{\varnothing}$ (because $A = \mathbb{Z}$ and because elements of A are the same thing as integers);
- we have $\mathcal{D}'_{\text{bin}} \Longleftrightarrow \mathcal{D}'_{\varnothing}$ (because $A = \mathbb{Z}$ and because elements of A are the same thing as integers);
- we have $\mathcal{D}^{\text{expl}}_{\text{bin}} \Longleftrightarrow \mathcal{D}^{\text{expl}}_{\varnothing}$ (because $A = \mathbb{Z}$ and because elements of A are the same thing as integers);
- we have $\mathcal{D}^{\text{expl}\prime}_{\text{bin}} \Longleftrightarrow \mathcal{D}^{\text{expl}\prime}_{\varnothing}$ (because $A = \mathbb{Z}$ and because elements of A are the same thing as integers);
- we have $\mathcal{E}_{\text{bin}} \Longleftrightarrow \mathcal{E}_{\varnothing}$ (because $A = \mathbb{Z}$ and because elements of A are the same thing as integers);
- we have $\mathcal{E}'_{\text{bin}} \Longleftrightarrow \mathcal{E}'_{\varnothing}$ (because $A = \mathbb{Z}$ and because elements of A are the same thing as integers);
- we have $\mathcal{F}_{\text{bin}} \Longleftrightarrow \mathcal{F}_{\varnothing}$ (since $A = \mathbb{Z}$);
- we have $\mathcal{G}_{\text{bin}} \Longleftrightarrow \mathcal{G}_{\varnothing}$ (since $A = \mathbb{Z}$);
- we have $\mathcal{H}_{\text{bin}} \Longleftrightarrow \mathcal{H}_{\varnothing}$ (since $A = \mathbb{Z}$);
- we have $\mathcal{I}_{\text{bin}} \Longleftrightarrow \mathcal{I}_{\varnothing}$ (because $A = \mathbb{Z}$ and because elements of A are the same thing as integers);
- we have $\mathcal{I}'_{\text{bin}} \Longleftrightarrow \mathcal{I}'_{\varnothing}$ (because $A = \mathbb{Z}$ and because elements of A are the same thing as integers).

Hence, the (already proven) equivalence of the assertions $\mathcal{C}_{\text{bin}}$, $\mathcal{D}_{\text{bin}}$, $\mathcal{D}'_{\text{bin}}$, $\mathcal{D}^{\text{expl}}_{\text{bin}}$, $\mathcal{D}^{\text{expl}\prime}_{\text{bin}}$, $\mathcal{E}_{\text{bin}}$, $\mathcal{E}'_{\text{bin}}$, $\mathcal{F}_{\text{bin}}$, $\mathcal{G}_{\text{bin}}$, $\mathcal{H}_{\text{bin}}$, $\mathcal{I}_{\text{bin}}$ and $\mathcal{I}'_{\text{bin}}$ yields the equivalence of the assertions $\mathcal{C}_{\varnothing}$, $\mathcal{D}_{\varnothing}$, $\mathcal{D}'_{\varnothing}$, $\mathcal{D}^{\text{expl}}_{\varnothing}$, $\mathcal{D}^{\text{expl}\prime}_{\varnothing}$, $\mathcal{E}_{\varnothing}$, $\mathcal{E}'_{\varnothing}$, $\mathcal{F}_{\varnothing}$, $\mathcal{G}_{\varnothing}$, $\mathcal{H}_{\varnothing}$, $\mathcal{I}_{\varnothing}$ and $\mathcal{I}'_{\varnothing}$.

Now let us prove the equivalence of these assertions with the remaining two assertions $\mathcal{K}_{\varnothing}$ and $\mathcal{K}^{\text{inv}}_{\varnothing}$. We will do this by proving the implications $\mathcal{E}_{\varnothing} \Longrightarrow \mathcal{K}^{\text{inv}}_{\varnothing}$, $\mathcal{K}^{\text{inv}}_{\varnothing} \Longrightarrow \mathcal{K}_{\varnothing}$ and $\mathcal{K}_{\varnothing} \Longrightarrow \mathcal{E}_{\varnothing}$.

Proof of the implication $\mathcal{E}_{\varnothing} \Longrightarrow \mathcal{K}^{\text{inv}}_{\varnothing}$: Assume that Assertion $\mathcal{E}_{\varnothing}$ holds. In other words, there exists a family $(y_n)_{n \in N} \in \mathbb{Z}^N$ of integers such that

$$\left(b_n = \sum_{d \mid n} d y_d \text{ for every } n \in N \right). \tag{70}$$

Consider such a family $(y_n)_{n \in N}$. For every $n \in N$, define an integer y'_n by $y'_n = \max\{0, y_n\}$. For every $n \in N$, define an integer y''_n by $y''_n = \max\{0, -y_n\}$.

It is completely straightforward to see that

$$y'_n - y''_n = y_n \qquad \text{for every } n \in N \tag{71}$$

(since every $a \in \mathbb{Z}$ satisfies $\max\{0, a\} - \max\{0, -a\} = a$).

For every $n \in N$, the integer y'_n is nonnegative (since $y'_n = \max\{0, y_n\} \geq 0$). Thus, $(y'_n)_{n \in N}$ is a family of nonnegative integers. That is, $(y'_n)_{n \in N} \in \mathbb{N}^N$. Hence,

Lemma 61 (applied to $(s_n)_{n\in N} = (y'_n)_{n\in N}$) yields that there exists a set P' and an *invertible* map $j' : P' \to P'$ such that every $n \in N$ satisfies

$$|\mathrm{Fix}\,(j'^n)| = \sum_{d|n} dy'_d.$$

Consider this P' and this j'.

For every $n \in N$, the integer y''_n is nonnegative (since $y''_n = \max\{0, -y_n\} \geq 0$). Thus, $(y''_n)_{n\in N}$ is a family of nonnegative integers. That is, $(y''_n)_{n\in N} \in \mathbb{N}^N$. Hence, Lemma 61 (applied to $(s_n)_{n\in N} = (y''_n)_{n\in N}$) yields that there exists a set P'' and an *invertible* map $j'' : P'' \to P''$ such that every $n \in N$ satisfies

$$|\mathrm{Fix}\,(j''^n)| = \sum_{d|n} dy''_d.$$

Consider this P'' and this j''.

Now, every $n \in N$ satisfies

$$|\mathrm{Fix}\,(j'^n)| = \sum_{d|n} dy'_d < \infty,$$

$$|\mathrm{Fix}\,(j''^n)| = \sum_{d|n} dy''_d < \infty$$

and

$$\begin{aligned}
\underbrace{|\mathrm{Fix}\,(j'^n)|}_{=\sum_{d|n} dy'_d} - \underbrace{|\mathrm{Fix}\,(j''^n)|}_{=\sum_{d|n} dy''_d} &= \sum_{d|n} dy'_d - \sum_{d|n} dy''_d \\
&= \sum_{d|n} d \underbrace{(y'_d - y''_d)}_{=y_d} \\
&\qquad \text{(by (71), applied to } d \text{ instead of } n) \\
&= \sum_{d|n} dy_d = b_n \qquad \text{(by (70))}.
\end{aligned}$$

Hence, there exist two sets U and V and two *invertible* maps $f : U \to U$ and $g : V \to V$ such that every $n \in N$ satisfies

$$|\mathrm{Fix}\,(f^n)| < \infty, \qquad |\mathrm{Fix}\,(g^n)| < \infty \qquad \text{and} \qquad |\mathrm{Fix}\,(f^n)| - |\mathrm{Fix}\,(g^n)| = b_n$$

(namely, we can take $U = P'$, $V = P''$, $f = j'$ and $g = j''$). In other words, Assertion $\mathcal{K}^{\mathrm{inv}}_{\varnothing}$ holds. We have thus proven Assertion $\mathcal{K}^{\mathrm{inv}}_{\varnothing}$ under the assumption of Assertion $\mathcal{E}_{\varnothing}$. In other words, the implication $\mathcal{E}_{\varnothing} \Longrightarrow \mathcal{K}^{\mathrm{inv}}_{\varnothing}$ is proven.

Proof of the implication $\mathcal{K}^{\mathrm{inv}}_{\varnothing} \Longrightarrow \mathcal{K}_{\varnothing}$: The implication $\mathcal{K}^{\mathrm{inv}}_{\varnothing} \Longrightarrow \mathcal{K}_{\varnothing}$ is obviously valid (because the statement of Assertion $\mathcal{K}_{\varnothing}$ is clearly contained in the statement of Assertion $\mathcal{K}^{\mathrm{inv}}_{\varnothing}$).

Proof of the implication $\mathcal{K}_{\varnothing} \Longrightarrow \mathcal{E}_{\varnothing}$: Assume that Assertion $\mathcal{K}_{\varnothing}$ holds. In other words, there exist two sets U and V and two maps $f : U \to U$ and $g : V \to V$ such that every $n \in N$ satisfies

$$|\mathrm{Fix}\,(f^n)| < \infty, \qquad |\mathrm{Fix}\,(g^n)| < \infty \qquad \text{and} \qquad |\mathrm{Fix}\,(f^n)| - |\mathrm{Fix}\,(g^n)| = b_n.$$

Consider these two sets U and V and these two maps f and g.

We know that every $n \in N$ satisfies $|\mathrm{Fix}\,(f^n)| < \infty$. Hence, Proposition 65 (applied to U and f instead of P and j) yields that there exists a family $(s_n)_{n\in N} \in \mathbb{N}^N$ of **nonnegative** integers such that every $n \in N$ satisfies

$$|\mathrm{Fix}\,(f^n)| = \sum_{d|n} d s_d.$$

Denote this family $(s_n)_{n\in N}$ by $(\alpha_n)_{n\in N}$. Thus, $(\alpha_n)_{n\in N}$ is a family of **nonnegative** integers such that every $n \in N$ satisfies

$$|\mathrm{Fix}\,(f^n)| = \sum_{d|n} d\alpha_d. \tag{72}$$

We know that every $n \in N$ satisfies $|\mathrm{Fix}\,(g^n)| < \infty$. Hence, Proposition 65 (applied to V and g instead of P and j) yields that there exists a family $(s_n)_{n\in N} \in \mathbb{N}^N$ of **nonnegative** integers such that every $n \in N$ satisfies

$$|\mathrm{Fix}\,(g^n)| = \sum_{d|n} d s_d.$$

Denote this family $(s_n)_{n\in N}$ by $(\beta_n)_{n\in N}$. Thus, $(\beta_n)_{n\in N}$ is a family of **nonnegative** integers such that every $n \in N$ satisfies

$$|\mathrm{Fix}\,(g^n)| = \sum_{d|n} d\beta_d. \tag{73}$$

For every $n \in N$, it is clear that $\alpha_n - \beta_n$ is an integer (since α_n and β_n are nonnegative integers). Thus, $(\alpha_n - \beta_n)_{n\in N}$ is a family of integers, i. e., we have $(\alpha_n - \beta_n)_{n\in N} \in \mathbb{Z}^N$.

Also, recall that every $n \in N$ satisfies $|\mathrm{Fix}\,(f^n)| - |\mathrm{Fix}\,(g^n)| = b_n$. Thus, every $n \in N$ satisfies

$$b_n = \underbrace{|\mathrm{Fix}\,(f^n)|}_{\substack{=\sum_{d|n} d\alpha_d \\ \text{(by (72))}}} - \underbrace{|\mathrm{Fix}\,(g^n)|}_{\substack{=\sum_{d|n} d\beta_d \\ \text{(by (73))}}} = \sum_{d|n} d\alpha_d - \sum_{d|n} d\beta_d = \sum_{d|n} d\left(\alpha_d - \beta_d\right).$$

Hence, there exists a family $(y_n)_{n\in N} \in \mathbb{Z}^N$ of integers such that

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

(namely, the family $(\alpha_n - \beta_n)_{n\in N}$). In other words, Assertion $\mathcal{E}_\varnothing$ holds. We have thus proven Assertion $\mathcal{E}_\varnothing$ under the assumption of Assertion $\mathcal{K}_\varnothing$. In other words, the implication $\mathcal{K}_\varnothing \Longrightarrow \mathcal{E}_\varnothing$ is proven.

Now we have proven the implications $\mathcal{E}_\varnothing \Longrightarrow \mathcal{K}_\varnothing^{\mathrm{inv}}$, $\mathcal{K}_\varnothing^{\mathrm{inv}} \Longrightarrow \mathcal{K}_\varnothing$ and $\mathcal{K}_\varnothing \Longrightarrow \mathcal{E}_\varnothing$. Combining these three implications, we obtain the equivalence $\mathcal{E}_\varnothing \Longleftrightarrow \mathcal{K}_\varnothing^{\mathrm{inv}} \Longleftrightarrow \mathcal{K}_\varnothing$.

Now recall that the assertions $\mathcal{C}_\varnothing$, $\mathcal{D}_\varnothing$, $\mathcal{D}'_\varnothing$, $\mathcal{D}^{\text{expl}}_\varnothing$, $\mathcal{D}^{\text{expl}\prime}_\varnothing$, $\mathcal{E}_\varnothing$, $\mathcal{E}'_\varnothing$, $\mathcal{F}_\varnothing$, $\mathcal{G}_\varnothing$, $\mathcal{H}_\varnothing$, $\mathcal{I}_\varnothing$ and $\mathcal{I}'_\varnothing$ are equivalent. Combining this with the equivalence $\mathcal{E}_\varnothing \iff \mathcal{K}^{\text{inv}}_\varnothing \iff \mathcal{K}_\varnothing$, we conclude that the assertions $\mathcal{C}_\varnothing$, $\mathcal{D}_\varnothing$, $\mathcal{D}'_\varnothing$, $\mathcal{D}^{\text{expl}}_\varnothing$, $\mathcal{D}^{\text{expl}\prime}_\varnothing$, $\mathcal{E}_\varnothing$, $\mathcal{E}'_\varnothing$, $\mathcal{F}_\varnothing$, $\mathcal{G}_\varnothing$, $\mathcal{H}_\varnothing$, $\mathcal{I}_\varnothing$, $\mathcal{I}'_\varnothing$, $\mathcal{K}_\varnothing$ and $\mathcal{K}^{\text{inv}}_\varnothing$ are equivalent. Theorem 60 is thus proven.

We will not dwell on particular cases and applications of Theorem 60, since most of them have been already discussed in [5]. While our Theorem 60 is stronger than Theorem 15 of [5], it seems that Theorem 15 of [5] is enough for most of the interesting applications[25], so we wouldn't gain much from applying Theorem 60.

What we will do, however, is formulate and prove a "finite" version of Theorem 60:

Theorem 70. Let N be a **finite** nest. Let $(b_n)_{n\in N} \in \mathbb{Z}^N$ be a family of integers. Then, the assertions $\mathcal{C}_\varnothing$, $\mathcal{D}_\varnothing$, $\mathcal{D}'_\varnothing$, $\mathcal{D}^{\text{expl}}_\varnothing$, $\mathcal{D}^{\text{expl}\prime}_\varnothing$, $\mathcal{E}_\varnothing$, $\mathcal{E}'_\varnothing$, $\mathcal{F}_\varnothing$, $\mathcal{G}_\varnothing$, $\mathcal{H}_\varnothing$, $\mathcal{I}_\varnothing$, $\mathcal{I}'_\varnothing$, $\mathcal{K}_\varnothing$, $\mathcal{K}^{\text{inv}}_\varnothing$, $\mathcal{K}^{\text{fin}}_\varnothing$ and $\mathcal{K}^{\text{fin inv}}_\varnothing$ are equivalent, where the assertions $\mathcal{C}_\varnothing$, $\mathcal{D}_\varnothing$, $\mathcal{D}'_\varnothing$, $\mathcal{D}^{\text{expl}}_\varnothing$, $\mathcal{D}^{\text{expl}\prime}_\varnothing$, $\mathcal{E}_\varnothing$, $\mathcal{E}'_\varnothing$, $\mathcal{F}_\varnothing$, $\mathcal{G}_\varnothing$, $\mathcal{H}_\varnothing$, $\mathcal{I}_\varnothing$, $\mathcal{I}'_\varnothing$, $\mathcal{K}_\varnothing$ and $\mathcal{K}^{\text{inv}}_\varnothing$ are the ones stated in Theorem 60, and the assertions $\mathcal{K}^{\text{fin}}_\varnothing$ and $\mathcal{K}^{\text{fin inv}}_\varnothing$ are the following ones:

Assertion $\mathcal{K}^{\text{fin}}_\varnothing$: There exist two **finite** sets U and V and two maps $f : U \to U$ and $g : V \to V$ such that every $n \in N$ satisfies

$$|\operatorname{Fix}(f^n)| - |\operatorname{Fix}(g^n)| = b_n.$$

Here, whenever S is a set and $h : S \to S$ is a map, we denote by $\operatorname{Fix}(h)$ the set of fixed points of the map h.

Assertion $\mathcal{K}^{\text{fin inv}}_\varnothing$: There exist two **finite** sets U and V and two *invertible* maps $f : U \to U$ and $g : V \to V$ such that every $n \in N$ satisfies

$$|\operatorname{Fix}(f^n)| - |\operatorname{Fix}(g^n)| = b_n.$$

Here, whenever S is a set and $h : S \to S$ is a map, we denote by $\operatorname{Fix}(h)$ the set of fixed points of the map h.

The proof of this relies on the following "finite" version of Lemma 61:

Lemma 71. Let N be a **finite** nest. Let $(s_n)_{n\in N} \in \mathbb{N}^N$ be a family of **nonnegative** integers. Then, there exists a **finite** set P and an *invertible* map $j : P \to P$ such that every $n \in N$ satisfies

$$|\operatorname{Fix}(j^n)| = \sum_{d|n} d s_d.$$

The proof of Lemma 71 proceeds exactly as the proof of Lemma 61, except that one also has to notice that Q is finite. The trivial details are left to the reader.

The proof of Theorem 70, too, proceeds exactly as the proof of Theorem 60, with obvious changes to account for finiteness conditions.

[25] In particular, applying Assertion $\mathcal{K}^{\text{inv}}_\varnothing$ to families like $(b_n)_{n\in\mathbb{N}_+} = (q^n)_{n\in\mathbb{N}_+}$ and $(b_n)_{n\in\mathbb{N}_+} = \left(\binom{qn}{rn}\right)_{n\in\mathbb{N}_+}$ gives results which could be derived in a better way combinatorially.

References

[1] Michiel Hazewinkel, *Witt vectors. Part 1*, revised version: 20 April 2008.

[2] Andreas Dress, Christian Siebeneicher, *The Burnside ring of the infinite cyclic group and its relations to the necklace algebra, λ-rings and the universal ring of Witt vectors*, Advances in Mathematics **78** (1989), pp. 1-41.
https://doi.org/10.1016/0001-8708(89)90027-3

[3] Jesse Elliott, *Binomial rings, integer-valued polynomials, and λ-rings*, Journal of Pure and Applied Algebra **207** (2006), pp. 165-185.
http://www.sciencedirect.com/science/article/pii/S0022404905002161

[4] Clarence Wilkerson, *Lambda-rings, binomial domains, and vector bundles over* CP (∞), Communications in Algebra **10(3)** (1982), pp. 311-328.

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

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

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

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

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