FUNCTIONAL DEGREES AND ARITHMETIC APPLICATIONS II: THE GROUP-THEORETIC PRIME AX-KATZ THEOREM

PETE L. CLARK AND UWE SCHAUZ

Abstract. We give a version of Ax-Katz's p-adic congruences and Moreno-Moreno's p-weight refinement that holds over any finite commutative ring of prime characteristic. We deduce this from a purely group-theoretic result that gives a lower bound on the p-adic divisibility of the number of simultaneous zeros of a system of maps $f_j : A \to B_j$ from a fixed "source" finite commutative group A of exponent p to varying "target" finite commutative p-groups B_j. Our proof combines Wilson's proof of Ax-Katz over $\mathbb{F}_p$ with the functional calculus of Aichinger-Moosbauer.

1. Introduction

This is the second in a sequence of papers in which we attempt a synthesis and further development of work of Wilson [Wi06] and of Aichinger and Moosbauer [AM21]. Whereas in the first paper [CS21] we applied arithmetic results of Weisman [We77] and Wilson [Wi06] to answer a purely algebraic problem posed by Aichinger-Moosbauer, in this paper the process is reversed: we use the algebraic work of [CS21] along with Aichinger-Moosbauer's functional calculus to deduce arithmetic results. In particular we give a purely group-theoretic result that implies the theorem of Ax-Katz in the case of systems of polynomial equations over a prime finite field $\mathbb{F}_p$ and the theorem of Moreno-Moreno on systems of polynomial equations over a finite field $\mathbb{F}_q$.

1.1. **Notation and Terminology.** We denote by $\mathcal{P}$ the set of (positive) prime numbers, write $\mathbb{N}$ for the set of non-negative integers, and put $\mathbb{Z}^+ \coloneqq \mathbb{N} \setminus \{0\}$. We endow the set

$$\widetilde{\mathbb{N}} \coloneqq \mathbb{N} \cup \{-\infty, \infty\}$$

with the most evident total ordering, in which $-\infty$ is the least element and ∞ is the greatest element. The symbol $-\infty$ is also used as the degree of the zero polynomial, which explains our restriction to nonzero polynomials or functions in some theorems.

Throughout, $q = p^N$ denotes a positive integer power of a prime number p and $\mathbb{F}_q$ shall denote "the" (unique up to isomorphism) finite field of order q. For $n \in \mathbb{Z} \setminus \{0\}$, we denote by $\mathrm{ord}_q(n)$ the largest power of q that divides n; we also put $\mathrm{ord}_q(0) = \infty$.

In this paper, rings are not necessarily commutative. We say that a ring R is a **domain** if for all $x, y \in R$, $xy = 0$ implies $x = 0$ or $y = 0$. A **rng** is like a ring but not necessarily having a multiplicative identity. If $R, R_1, \ldots, R_r$ are sets, such that each of the sets $R_1, \ldots, R_r$ contains a distinguished element denoted 0, and if $f_1 : R^n \to R_1$, $\ldots$, $f_r : R^n \to R_r$ are functions (possibly given as polynomials), we also define

$$Z(f_1, \ldots, f_r) = Z_{R^n}(f_1, \ldots, f_r) \coloneqq \big\{x \in R^n \mid f_1(x) = 0, \ldots, f_r(x) = 0\big\}.$$

1.2. **Chevalley-Warning and Ax-Katz.** We begin by recalling the following results of Chevalley-Warning and Ax-Katz.

Theorem 1.1. *Let $p \in \mathcal{P}$ and $q := p^N$. Let $f_1, \ldots, f_r \in \mathbb{F}_q[t_1, \ldots, t_n]$ be nonzero polynomials. If $Z := Z_{\mathbb{F}_q^n}(f_1, \ldots, f_r)$ and $\sum_{j=1}^r \deg(f_j) < n$, then*

a) $\operatorname{ord}_p(\#Z) \geq 1$ (Chevalley-Warning Theorem [Ch35], [Wa35]),

b) $\operatorname{ord}_q(\#Z) \geq \left\lceil \frac{n - \sum_{j=1}^r \deg(f_j)}{\max_{j=1}^r \deg(f_j)} \right\rceil$ (Ax-Katz Theorem [Ax64], [Ka71]).

Theorem 1.1b) in the case of one polynomial was proved in 1964 by J. Ax [Ax64], while the general case was proved in 1971 by N.M. Katz [Ka71]. Also in [Ax64], Ax gave a strikingly simple ten line proof of Theorem 1.1a). There is certainly no known ten line proof of Theorem 1.1b): Ax's proof for one polynomial used methods of algebraic number theory – Jacobi sums and Stickelberger's congruence – while Katz's proof of the general case used some sophisticated arithmetic geometry – zeta functions and p-adic cohomology. An Ax-style proof of Theorem 1.11.1b) was given by D. Wan [Wa89], while Hou [Ho05] gave a short deduction of Theorem 1.11.1b) from the $r = 1$ case. Also D.J. Katz [Ka12] proved a result in coding theory that implies Theorem 1.1b).

What if we replace $\mathbb{F}_q$ by a finite ring R? If R is finite commutative and *principal* (i.e., every ideal of R is principal), then for each prime number p the largest power of p dividing $\#Z_{R^n}(f_1, \ldots, f_r)$ for all polynomials $f_1, \ldots, f_r \in R[t_1, \ldots, t_n]$ of given positive degrees was determined: for $r = 1$ by Marshall-Ramage [MR75] and in general by D.J. Katz [Ka09].

A finite commutative ring is Artinian, hence is a finite product of finite local Artinian rings, each of which must have prime power order. In this way we immediately reduce to the case of finite rings of prime power order. Most such rings are however *not* principal, and there had been no known analogue of Chevalley-Warning – let alone of Ax-Katz – over any finite non-principal ring until the following recent result.

Theorem 1.2. (Aichinger-Moosbauer [AM21, Thm. 12.6]) *Let R be a finite rng of order a power of a prime number p, and let $f_1, \ldots, f_r \in R[t_1, \ldots, t_n]$ be nonzero polynomials. If $Z := Z_{R^n}(f_1, \ldots, f_r)$ and $\sum_{i=1}^r \deg(f_i) < n$, then*

$$\operatorname{ord}_p(\#Z) \geq 1.$$

Our first main result gives a version of Ax-Katz for all finite rngs of exponent p.

Theorem 1.3 (Ring-Theoretic Prime Ax-Katz Theorem)**.** *Let R be a finite rng with underlying additive group $(R, +)$ of prime exponent p, so $(R, +) \cong \big((\mathbb{Z}/p\mathbb{Z})^N, +\big)$ for some $N \in \mathbb{Z}^+$. Let $f_1, \ldots, f_r \in R[t_1, \ldots, t_n]$ be nonzero polynomials. If $Z := Z_{R^n}(f_1, \ldots, f_r)$, then*

$$\operatorname{ord}_p(\#Z) \geq \left\lceil \frac{N\big(n - \sum_{j=1}^r \deg(f_j)\big)}{\max_{j=1}^r \deg(f_j)} \right\rceil.$$

Remark 1.4. *If we take R to be the finite field $\mathbb{F}_{p^N}$ of order p^N, the conclusion of Theorem 1.3 is that*

$$\operatorname{ord}_p(\#Z) \geq \left\lceil \frac{N\big(n - \sum_{j=1}^r \deg(f_j)\big)}{\max_{j=1}^r \deg(f_j)} \right\rceil, \tag{1}$$

while the Ax-Katz Theorem yields the p-adic congruence

$$\text{ord}_p(\#Z) \geq N \,\text{ord}_{p^N}(\#Z) \geq N\left\lceil \frac{n - \sum_{j=1}^r \deg(f_j)}{\max_{j=1}^r \deg(f_j)} \right\rceil. \tag{2}$$

The latter placement of the ceiling functions is more favorable, as the lower bound in (2) is better than the lower bound in (1) if $N > 1$. This is why we speak of Theorem 1.3 as a generalization of the "Prime Ax-Katz Theorem" and not of the Ax-Katz Theorem.

Moreno-Moreno [MM95] used the Prime Ax-Katz Theorem as input to give a different p-adic congruence for polynomial systems over any finite field $\mathbb{F}_q$ that takes into account the p-weight degrees of the polynomials. When $q > p$ the Moreno-Moreno p-adic congruences neither imply nor are implied by the Ax-Katz p-adic congruences: cf. [MM95, Thm. 0-1]. In §4 we will give a p-weight version of Theorem 1.3 that generalizes the Moreno-Moreno p-adic congruences from $\mathbb{F}_q$ to any finite commutative ring of prime exponent.

Theorems 1.2 and 1.3 follow from deeper group-theoretic results, as we now explain.

1.3. **The Aichinger-Moosbauer Functional Calculus.** In their recent work [AM21], Aichinger-Moosbauer developed a fully fledged calculus of finite differences for functions $f : A \to B$, where A and B are commutative groups. When A and B are $\mathbb{R}$-vector spaces, this subject has a long pedigree, going back at least to work of Fréchet [Fr09]. More recent works addressing the same topic include Leibman [Lei02] – who works with not necessarily commutative groups – and Laczkovich [La04] – who surveys and works to synthesize some of the prior literature. Neverthless, though the idea of such a calculus was not new, Aichinger-Moosbauer's work is strikingly elegant, systematic and useful.

We denote by B^A the set of all functions $f : A \to B$. It is a commutative group under pointwise addition. For each $a \in A$, we define a **difference operator** $\Delta_a \in \text{End}(B^A)$ by

$$\Delta_a f : x \longmapsto f(x+a) - f(x).$$

These endomorphisms all commute. Following Aichinger-Moosbauer, we assign to each $f \in B^A$ a **functional degree** $\text{fdeg}(f) \in \widetilde{\mathbb{N}}$ as follows:

- We put $\text{fdeg}(f) = -\infty$ if and only if $f = 0$.[1]
- For $n \in \mathbb{N}$, we say that $\text{fdeg}(f) \leq n$ if $\Delta_{a_1} \cdots \Delta_{a_{n+1}} f = 0$ for all $a_1, \ldots, a_{n+1} \in A$. If this holds for some $n \in \mathbb{N}$, then $\text{fdeg}(f)$ is the least n for which it holds.
- If $\text{fdeg}(f) \leq n$ holds for no $n \in \mathbb{N}$, then we put $\text{fdeg}(f) = \infty$.

In other words, if we set $\sup(\emptyset) := -\infty$, then

$$\text{fdeg}(f) = \sup\left\{n \in \mathbb{N} \mid \exists a_1, \ldots, a_n \in A,\, \Delta_{a_1} \cdots \Delta_{a_n} f \neq 0\right\}. \tag{3}$$

For commutative groups A and B and $d \in \mathbb{N}$, we put

$$\mathcal{F}^d(A,B) := \{f \in B^A \mid \text{fdeg}(f) \leq d\},$$

and we also put

$$\mathcal{F}(A,B) := \{f \in B^A \mid \text{fdeg}(f) < \infty\}.$$

[1] Aichinger-Moosbauer in [AM21] assign the functional degree 0 to the zero function. Here we follow the convention of [CS21]. It certainly makes no mathematical difference.

As introduced in [AM21, §2] and also discussed in [CS21, §3], if $\mathbb{Z}[A]$ is the integral group ring of A, then the commutative group B^A has a canonical $\mathbb{Z}[A]$-module structure determined by the product

$$[a]f : x \longmapsto [a]f(x) \coloneqq f(x+a)$$

of scalars of the form $[a] \in \mathbb{Z}[A]$ and vectors $f \in B^A$. In view of this, we may equally well view Δ_a as the element $[a] - [0]$ of $\mathbb{Z}[A]$, since this element acts on B^A in the previously defined way. We write $e(B)$ for the exponent $\exp(B)$ if this number is finite and set $e(B) := 0$ otherwise. This means $e(B) \neq 0$ if and only if there exists an $N \in \mathbb{Z}^+$ such that $Nb = 0$ for all $b \in B$, and then $e(B) = \exp(B)$ is the least such N. With that definition, B^A is canonically a $\mathbb{Z}/e(B)\mathbb{Z}$-module, so we may also view Δ_a as living in the group ring $(\mathbb{Z}/e(B)\mathbb{Z})[A]$.

The functional degree gives a notion of "polynomial function of degree d" even when there is no ring in sight. Moreover the notion of functional degree is partially compatible with the degree of an actual polynomial function, in the following sense:

Lemma 1.5. *Let R be a rng, let f be a polynomial over R in n variables, and let $E(f) \in R^{R^n}$ be the associated function. Then* $\operatorname{fdeg}(E(f)) \leq \deg(f)$.

Proof. This is [AM21, Lemma 12.5]. □

Lemma 1.5 shows that any discrepancy between the functional degree and the degree of a polynomial map will only make Chevalley-Warning / Ax-Katz type results stated in terms of the functional degree *stronger* than their classical analogues.

Here is the group-theoretic result of Aichinger-Moosbauer that underlies Theorem 1.2.

Theorem 1.6 (Group-Theoretic Chevalley-Warning Theorem)**.**
Let $N, m, \alpha_1, \dots, \alpha_m, n, \beta_1, \dots, \beta_n, r \in \mathbb{Z}^+$, let $p \in \mathcal{P}$, and let

$$A \coloneqq \bigoplus_{i=1}^{m} \mathbb{Z}/p^{\alpha_i}\mathbb{Z},\ B \coloneqq \bigoplus_{i=1}^{n} \mathbb{Z}/p^{\beta_i}\mathbb{Z}$$

be finite commutative p-groups. Let $f_1, \dots, f_r : A^N \to B$ be nonzero functions. If $Z := Z_{A^N}(f_1, \dots, f_r)$ and

$$\left(\sum_{j=1}^{r} \operatorname{fdeg}(f_j)\right)\left(\sum_{i=1}^{n}(p^{\beta_i}-1)\right) < \left(\sum_{i=1}^{m} p^{\alpha_i} - 1\right)N,$$

then

$$\operatorname{ord}_p(\#Z) \geq 1.$$

Proof. This is [AM21, Thm. 12.2]. □

Applying Theorem 1.6 with $A = B = (R, +)$, the additive group of a finite rng of order a power of p and using Lemma 1.5, we deduce Theorem 1.2.

Here is the main result of this paper.

Theorem 1.7. *Let $N, r, \beta_1, \dots, \beta_r \in \mathbb{Z}^+$, let $p \in \mathcal{P}$, and put $A := (\mathbb{Z}/p\mathbb{Z})^N$. For each $1 \le j \le r$, let $f_j \in (\mathbb{Z}/p^{\beta_j}\mathbb{Z})^A$ be a nonzero function. If $Z := Z_A(f_1, \dots, f_r)$, then*

$$\operatorname{ord}_p(\#Z) \ge \left\lceil \frac{N - \sum_{j=1}^r \frac{p^{\beta_j}-1}{p-1} \operatorname{fdeg}(f_j)}{\max_{j=1}^r p^{\beta_j - 1} \operatorname{fdeg}(f_j)} \right\rceil.$$

Remark 1.8. *The codomains of the maps f_j in Theorem 1.7 can easily be generalized from cyclic p-groups $\mathbb{Z}/p^{\beta_j}\mathbb{Z}$ to arbitrary finite commutative p-groups B_j. If, for each $1 \le j \le r$,*

$$B_j \;=\; \bigoplus_{k=1}^{K(j)} \mathbb{Z}/p^{\beta_{j,k}}\mathbb{Z} \quad \text{with } \beta_{j,1} \ge \cdots \ge \beta_{j,K(j)} \ge 1\,,$$

then each of the given maps $f_j : A \to B_j$ can be composed with the coordinate projection $\pi_k : B_j \to \mathbb{Z}/p^{\beta_{j,k}}\mathbb{Z} =: B_{j,k}$, for $1 \le k \le K(j)$. This yields functions $f_{j,k} := \pi_k \circ f_j$ with

$$\max_{1 \le k \le K(j)} \big(\operatorname{fdeg}(f_{j,k})\big) \;=\; \operatorname{fdeg}(f_j)\,.$$

Evidently, $f_j(x) = 0$ for all j if and only if $f_{j,k}(x) = 0$ for all j and k. So, applying Theorem 1.7 to the family of all maps $f_{j,k} : A \to B_{j,k}$ that are nonzero, we get

$$\operatorname{ord}_p(\#Z(f_1, \dots, f_r)) \;\ge\; \left\lceil \frac{N - \sum_{j=1}^r \operatorname{fdeg}(f_j) \sum_{k=1}^{K(j)} \frac{p^{\beta_{j,k}}-1}{p-1}}{\max_{j=1}^r p^{\beta_{j,1}-1} \operatorname{fdeg}(f_j)} \right\rceil.$$

This result may be viewed as a generalization of Theorem 1.7, which we recover by taking each B_j to be cyclic. In practice, however, this result loses information from Theorem 1.7 in that for each j we use only $\max_{1 \le k \le K(j)} \big(\operatorname{fdeg}(\pi_k \circ f_j)\big)$ instead of the individual functional degrees of the maps $\pi_k \circ f_j$.

We also have the following corollary, which generalizes Theorem 1.3:

Corollary 1.9 (Group-Theoretic Prime Ax-Katz Theorem)**.** *Let $N, n, r \in \mathbb{Z}^+$, and put $A := (\mathbb{Z}/p\mathbb{Z})^N$. Let $f_1, \dots, f_r \in A^{A^n}$ be nonzero functions. If $Z := Z_{A^n}(f_1, \dots, f_r)$, then*

$$\operatorname{ord}_p(\#Z) \;\ge\; \left\lceil \frac{N\big(n - \sum_{j=1}^r \operatorname{fdeg}(f_j)\big)}{\max_{j=1}^r \operatorname{fdeg}(f_j)} \right\rceil.$$

Proof. Let $\tilde{A} := A^n \cong (\mathbb{Z}/p\mathbb{Z})^{nN}$. For $1 \le k \le N$, let $\pi_k : A \to \mathbb{Z}/p\mathbb{Z}$ be the kth coordinate projection. For $1 \le j \le r$ and $1 \le k \le N$, put

$$f_{j,k} := \pi_k \circ f_j \in (\mathbb{Z}/p\mathbb{Z})^{A^n} = (\mathbb{Z}/p\mathbb{Z})^{\tilde{A}}, \quad \text{with} \quad \operatorname{fdeg}(f_{j,k}) \le \operatorname{fdeg}(f_j)$$

according to [CS21, Lemma 3.8b)]. For $x \in A^n$, we have $f_j(x) = 0$ for all j if and only if $f_{j,i}(x) = 0$ for all j and i. So, applying Theorem 1.7 to to the family of all maps $f_{j,k} \in (\mathbb{Z}/p^{\mathbb{Z}})^{\tilde{A}}$ that are nonzero, we get

$$\operatorname{ord}_p(\#Z) \;\ge\; \cdots \;\ge\; \left\lceil \frac{Nn - \sum_{j=1}^r \sum_{k=1}^N \operatorname{fdeg}(f_j)}{\max_{j=1}^r \operatorname{fdeg}(f_j)} \right\rceil \;=\; \left\lceil \frac{N\big(n - \sum_{j=1}^r \operatorname{fdeg}(f_j)\big)}{\max_{j=1}^r \operatorname{fdeg}(f_j)} \right\rceil. \qquad \square$$

If R is a finite rng with underlying additive group $(R, +)$ finite of exponent p, then applying Corollary 1.9 with $A = (R, +)$ and using Lemma 1.5, we deduce Theorem 1.3. Combining it instead with a p-weight analogue of Lemma 1.5 (Proposition 4.3), we will get our p-weight improvement of Theorem 1.3 that recovers the Moreno-Moreno Theorem.

Remark 1.10. *In an earlier version of our work, Corollary 1.9 was our main result, but switching to Theorem 1.7 made the proof* easier*: cf. Remark 1.8. The idea to this improvement arose from a draft manuscript* [GGZ] *that D. Grynkiewicz sent us in March of 2022. These results are also contained in the arxiv preprint* [Gr22]*. The statement of our Theorem 1.7 is directly inspired by* [GGZ, Thm. 1.3.22]*, which is closely related to Theorem 1.7 but involves sums over residue systems modulo p and reductions modulo powers of p of polynomials $f_1, \ldots, f_r \in \mathbb{Z}[t_1, \ldots, t_N]$ rather than arbitrary functions between commutative p-groups. Moreover, in a later draft of the same manuscript, Grynkiewicz, Geroldinger and Zhong give a weighted version of their result.*

1.4. **Structure of the Paper.**

• In §2 we give a canonical series representation for a map $f : A \to B$ between commutative groups of finite functional degree when A is finitely generated. Moreover, for commutative domains of characteristic 0, we explore the connection between functions of finite functional degree and integer-valued polynomials.

• In §3 we carry over a lemma of Wilson to our setting and then prove Theorem 1.7.

• In §4 we discuss p-weights and prove a p-weight improvement of Theorem 1.3.

• In §5 we discuss work of the present authors [CS23] and of Clark-Triantafillou [CT23] that continues and complements the present work.

1.5. **Acknowledgments.** Thanks to E. Aichinger for his interest in our present work, which led to the communication of the results of Geroldinger-Grynkiewicz-Zhong. Thanks to D. Grynkiewicz for showing us two early versions of [GGZ]. Thanks to A.C. Cojocaru, N. Jones and N. Triantafillou for stimulating conversations.

2. The Fundamental Representation for $f \in B^{\mathbb{Z}^N}$

2.1. **Preliminaries.** Let $N \in \mathbb{Z}^+$, and let B be a commutative group. In this section we give a canonical series representation for functions $f \in \mathcal{F}(\mathbb{Z}^N, B)$ in terms of **binomial polynomials**:

$$\binom{t}{d} := \frac{t(t-1)\cdots(t-d+1)}{d!} \in \mathbb{Q}[t] \quad \text{if} \quad d \in \mathbb{Z}^+.$$

Obviously, $\binom{x}{d}$ is an integer if $x \in \mathbb{N}$, as it is the usual binomial coefficient. But, $\binom{x}{d}$ is always an integer, also for negative $x \in \mathbb{Z}$: see e.g. [CC, p. 19]. The binomial polynomials $\binom{t}{d} \in \mathbb{Q}[t]$ are **integer-valued polynomials** as they give rise to functions $\binom{x}{d}$ from $\mathbb{Z}$ to $\mathbb{Z}$. We also take $\binom{x}{0} : \mathbb{Z} \to \mathbb{Z}$ to be the constant function 1. And, we define $\binom{x}{d} : \mathbb{Z} \to \mathbb{Z}$ to be the zero function for negative $d \in \mathbb{Z}$. We discuss this kind of functions in §2.3.

For $1 \le i \le n$, let e_i be the ith standard basis vector of $\mathbb{Z}^N$. We write Δ_i for the difference operator Δ_{e_i} of $B^{\mathbb{Z}^N}$.

Lemma 2.1. *Let $\underline{B}$ be a subgroup of the commutative group B, and let $f \in B^{\mathbb{Z}^N}$. Then the following properties are equivalent:*

(i) $f(\mathbb{Z}^N) \subseteq \underline{B}$.
(ii) $\Delta_i f(\mathbb{Z}^N) \subseteq \underline{B}$ *for all* $1 \le i \le N$, *and* $f(\underline{0}) \in \underline{B}$.

Proof. (i) $\Rightarrow$ (ii) is immediate.

(ii) $\Rightarrow$ (i): For any $\underline{x} \in \mathbb{Z}^N$ and any $1 \le i \le N$, we have

$$\Delta_i f(\underline{x}) \ = \ f(\underline{x} + e_i) - f(\underline{x}) \ \in \ \underline{B},$$

which shows that $f(\underline{x}+e_i) \in \underline{B} \iff f(\underline{x}) \in \underline{B}$. Since $f(\underline{0}) \in B$, an immediate inductive argument now shows that $f(\underline{x}) \in \underline{B}$ for all $\underline{x} \in \mathbb{Z}^N$. □

For $\underline{n} \coloneqq (n_1, \dots, n_N) \in \mathbb{N}^N$, we put

$$\Delta^{\underline{n}} \coloneqq \Delta_1^{n_1} \cdots \Delta_N^{n_N}.$$

Because $e_1, \dots, e_N$ is a set of generators for $\mathbb{Z}^N$, the following characterization of the functional degree follows from or [AM21, Lemmas 2.2], or from [CS21, Lemma 3.11]:

Proposition 2.2. *Let $f \in B^{\mathbb{Z}^N}$ and define $\sup(\emptyset) := -\infty$. Then*

$$\operatorname{fdeg}(f) \,=\, \sup\big\{|\underline{n}| \mid \underline{n} \in \mathbb{N}^N,\, \Delta^{\underline{n}} f \neq 0\big\}.$$

If we compare this expression with the following definition of the **j-th partial functional degree** for functions f in $B^{\mathbb{Z}^N}$, which is given by

$$\operatorname{fdeg}_j(f) \,:=\, \sup\big\{n \in \mathbb{N} \mid \Delta_j^n f \neq 0\big\}, \tag{4}$$

it is easy to see that, for each $1 \leq j \leq N$,

$$\operatorname{fdeg}_j(f) \,\leq\, \operatorname{fdeg}(f) \,\leq\, \sum_{i=1}^{N} \operatorname{fdeg}_i(f).$$

All this can easily be generalized to domains that are a direct product of arbitrary commutative groups $A_1, \dots, A_N$, as in [AM21, §5]. Regarding this product as an internal direct product, we define the j-th partial functional degree of a function $f \in B^{\bigoplus_{i=1}^N A_i}$ by

$$\operatorname{fdeg}_j(f) \,:=\, \sup\big\{n \in \mathbb{N} \mid \exists\, a_1, \dots, a_n \in A_j,\, \Delta_{a_n} \cdots \Delta_{a_1} f \neq 0\big\}.$$

It follows from [AM21, Lemmas 2.2] or [CS21, Lemma 3.11] that

$$\operatorname{fdeg}(f) \,=\, \sup\big\{n \in \mathbb{N} \mid \exists\, a_1, \dots, a_n \in A_1 \cup \cdots \cup A_n,\, \Delta_{a_n} \cdots \Delta_{a_1} f \neq 0\big\} \tag{5}$$

From this we easily get [AM21, Theorem 5.2], for which we present a shortened proof:

Theorem 2.3. *Let $A_1, \dots, A_N, B$ be commutative groups, and let $f \in B^{\bigoplus_{i=1}^N A_i}$. Then, for each $1 \leq j \leq N$,*

$$\operatorname{fdeg}_j(f) \,\leq\, \operatorname{fdeg}(f) \,\leq\, \sum_{i=1}^{N} \operatorname{fdeg}_i(f).$$

Proof. We may assume $f \neq 0$, as the inequality holds otherwise. Comparing (3) and (4), we see that $\operatorname{fdeg}_j(f) \leq \operatorname{fdeg}(f)$. To prove $\operatorname{fdeg}(f) \leq \sum_{i=1}^N \operatorname{fdeg}_i(f) =: n \geq 0$, let $a_1, \dots, a_{n+1} \in A_1 \cup \cdots \cup A_n$. By (5), it suffices to show that $\Delta_{a_{n+1}} \cdots \Delta_{a_1} f = 0$. As $n+1 > \sum_{i=1}^N \operatorname{fdeg}_i(f)$, there exists a $1 \leq j \leq N$ such that more than $n_j := \operatorname{fdeg}_j(f)$ of the elements $a_1, \dots, a_{n+1}$ lie inside A_j. Without loss of generality, assume $a_1, \dots, a_{n_j+1} \in A_j$. Then $\Delta_{a_{n_j+1}} \cdots \Delta_{a_1} f = 0$, by (4), and $\Delta_{a_{n+1}} \cdots \Delta_{a_1} f = 0$ follows. □

For the convenience of the reader, we also restate [CS21, Lemma 2.2].

Lemma 2.4. *Let A and B be commutative groups. Let $a \in A$, $n \in \mathbb{N}$ and let Δ_a^n be the n-fold product $\Delta_a \cdots \Delta_a \in \operatorname{End} B^A$. For all $f \in B^A$ and all $x \in A$, we have*

$$\Delta_a^n f(x) \,=\, \sum_{i=0}^{n} (-1)^i \tbinom{n}{i} f(x + (n-i)a) \,=\, \sum_{j=0}^{n} (-1)^{n-j} \tbinom{n}{j} f(x + ja).$$

We recall an old result for comparison and future use:

Lemma 2.5. *Let R be a commutative domain, let $f \in R[t_1, \ldots, t_n]$, and let X_i be a nonempty subset of R with $\#X_i > \deg_i(f)$, for each $1 \leq i \leq n$. If $f(x) = 0$ for all $x \in X := \prod_{i=1}^n X_i$, then $f = 0$.*

Proof. We can immediately reduce to the case in which $\#X_i = \deg_i(f) + 1$ for all i. Then the case $R = \mathbb{Z}$ is [AT92, Lemma 2.1], and their proof works verbatim over any commutative domain. More general results appear in [Sc08, §2]; see also [Cl14, Thm. 12]. □

The following result is related to Lemma 2.5 and also to [Sc14, Thm. 2.5].

Lemma 2.6. *Let $N \in \mathbb{Z}^+$, let B be a commutative group and let $f \in B^{\mathbb{Z}^N}$. For each $1 \leq i \leq N$, let $a_i \in \mathbb{Z}$, $d_i \in \mathbb{N}$ with $d_i \geq \mathrm{fdeg}_i(f)$, and put*

$$[a_i, a_i + d_i] := \{a_i, a_i + 1, \ldots, a_i + d_i\}.$$

If $f(\underline{x}) = 0$ for all $\underline{x} \in \prod_{i=1}^N [a_i, a_i + d_i]$, then $f = 0$.

Proof. We proceed by induction on N.

Base Case: Suppose that $N = 1$, i.e. $f \in B^{\mathbb{Z}}$, $\mathrm{fdeg}(f) \leq d_1$ and $f(a) = f(a+1) = \cdots = f(a + d_1) = 0$. Applying Lemma 2.4 with $d_1 + 1$ in the place of that lemma's n, with 1 in the place of that lemma's a, and with $a - 1$, resp. a, in the place of that lemma's x, we can deduce $f(a-1) = 0$, rsp. $f(a + d_1 + 1) = 0$. Repeating this argument we get $\cdots = f(a-2) = f(a-1) = 0$ and $0 = f(a + d_1 + 1) = f(a + d_1 + 2) = \cdots$, i.e. $f = 0$.

Induction Step: Suppose that $N \geq 2$ and that the result holds for all $f \in \mathcal{F}(\mathbb{Z}^{N-1}, B)$. For $0 \leq j \leq d_N$, put

$$g_j \coloneqq f(\,\cdot, \ldots, \cdot, a_N + j) : \mathbb{Z}^{N-1} \to B.$$

Then we have $\mathrm{fdeg}_i\, g_j \leq d_i$ for all $1 \leq i \leq N-1$ and g_j vanishes identically on $\prod_{i=1}^{N-1} [a_i, a_i + d_i]$, so induction gives $g_j = 0$ for all $0 \leq j \leq d_N$. It follows that for each fixed $(x_1, \ldots, x_{N-1}) \in \mathbb{Z}^{N-1}$ the function $f(x_1, \ldots, x_{N-1}, \cdot) : \mathbb{Z} \to B$ vanishes on $[a_N, a_N + d_N]$, and it has functional degree at most d_N. So, by the base case, these functions are identically zero, which means that f is identically zero. □

Lemma 2.7. *Let B be a commutative group, and let $f : \mathbb{N}^N \longrightarrow B$ be a function. If $\Delta^{\underline{n}} f(\underline{0}) = 0$ for all $\underline{n} \in \mathbb{N}^N$, then f is the zero function.*

Proof. Given a function $f : \mathbb{N}^N \to B$ with $\Delta^{\underline{n}} f(\underline{0}) = 0$ for all $\underline{n} \in \mathbb{N}^N$, we prove the formally stronger conclusion $\Delta^{\underline{m}} f(\underline{x}) = 0$ for all $\underline{x}, \underline{m} \in \mathbb{N}^N$. We do this by induction on $|\underline{x}| \coloneqq x_1 + \cdots + x_N$.

Base Case: If $|\underline{x}| = 0$ then $\underline{x} = \underline{0}$ and $\Delta^{\underline{m}} f(\underline{x}) = \Delta^{\underline{m}} f(\underline{0}) = 0$ for all $\underline{m} \in \mathbb{N}^N$, by the assumption on f.

Induction Step: Let $\underline{0} \neq \underline{x} \in \mathbb{N}^N$ and assume that the statement holds for all $\underline{z} \in \mathbb{N}^N$ with $|\underline{z}| < |\underline{x}|$, and for all $\underline{m} \in \mathbb{N}^N$. As $\underline{x} \neq \underline{0}$, there is an index i such that $x_i \geq 1$. Hence, by the induction hypothesis, for each $\underline{m} \in \mathbb{N}^N$,

$$\Delta^{\underline{m}} f(\underline{x} - e_i) = 0 \quad \text{and} \quad \Delta^{\underline{m} + e_i} f(\underline{x} - e_i) = 0,$$

so that

$$\begin{aligned}\Delta^{\underline{m}} f(\underline{x}) &= \Delta^{\underline{m}} f(\underline{x}) - \Delta^{\underline{m}} f(\underline{x} - e_i) \\ &= \Delta_i(\Delta^{\underline{m}} f)(\underline{x} - e_i) \\ &= \Delta^{\underline{m}+e_i} f(\underline{x} - e_i) \\ &= 0,\end{aligned}$$

completing the induction step and the proof. □

2.2. **The Fundamental Representation.** We can now prove the following result, on which much of the rest of this work is based.

Theorem 2.8. *Let B be a commutative group, and let $f \in B^{\mathbb{Z}^N}$.*

a) *There is a unique function $a_\bullet : \mathbb{N}^N \to B$ such that*

$$f(\underline{x}) = \sum_{\underline{n} \in \mathbb{N}^N} \binom{x_1}{n_1} \cdots \binom{x_N}{n_N} a_{\underline{n}} \quad \text{for all } \underline{x} \in \mathbb{N}^N.$$

The function values of $a_\bullet$ are given by the formula $a_{\underline{n}} = \Delta^{\underline{n}} f(\underline{0})$.

b) *If $d := \operatorname{fdeg}(f) < \infty$, then*

$$f(\underline{x}) = \sum_{\substack{\underline{n} \in \mathbb{N}^N \\ |\underline{n}| \leq d}} \binom{x_1}{n_1} \cdots \binom{x_N}{n_N} \Delta^{\underline{n}} f(\underline{0}) \quad \text{for all } \underline{x} \in \mathbb{Z}^N.$$

Proof. a) To prove the uniqueness, assume there is an $a_\bullet$ with $f(\underline{x}) := \sum \binom{x_1}{n_1} \cdots \binom{x_N}{n_N} a_{\underline{n}}$ for all $\underline{x} \in \mathbb{N}^N$. For each $\underline{x} = (x_1, \ldots, x_N) \in \mathbb{N}^N$ we have $\binom{x_1}{n_1} \cdots \binom{x_N}{n_N} = 0$ unless $n_i \leq x_i$ for all $1 \leq i \leq N$, so for each fixed $\underline{x}$ we have a finite sum. For all $n \in \mathbb{Z}^+$, we have $\binom{x+1}{n} - \binom{x}{n} = \binom{x}{n-1}$. From this it follows that, for all $\underline{m}, \underline{n} \in \mathbb{N}$,

$$\Delta^{\underline{m}} \left(\binom{x_1}{n_1} \cdots \binom{x_N}{n_N} \right) (\underline{0}) = \prod_{i=1}^{N} \binom{0}{n_i - m_i} = \begin{cases} 1 & \text{if } \underline{m} = \underline{n}, \\ 0 & \text{otherwise.} \end{cases}$$

With that, if we apply $\Delta^{\underline{m}}$ to $f(\underline{x}) = \sum \binom{x_1}{n_1} \cdots \binom{x_N}{n_N} a_{\underline{n}}$ and evaluate at $\underline{0}$, we see that $a_{\underline{m}} = \Delta^{\underline{m}} f(\underline{0})$. So, the function $a_\bullet : \underline{n} \mapsto \Delta^{\underline{n}} f(\underline{0})$ is the only possible choice.

To show that this choice indeed yields the function f, define $\hat{f} : \mathbb{N}^N \to B$ by

$$\hat{f}(\underline{x}) := \sum_{\underline{n} \in \mathbb{N}^N} \binom{x_1}{n_1} \cdots \binom{x_N}{n_N} \Delta^{\underline{n}} f(\underline{0}).$$

By what we have already proven about the uniqueness of coefficients, for each $\underline{n} \in \mathbb{N}^N$, the coefficient $\Delta^{\underline{n}} f(\underline{0})$ must be equal to $\Delta^{\underline{n}} \hat{f}(\underline{0})$, i.e. $\Delta^{\underline{n}}(f - \hat{f})(\underline{0}) = 0$. With that, Lemma 2.7 yields $f - \hat{f} = 0$, i.e. $f = \hat{f}$, as desired.

b) We have $\Delta^{\underline{n}} f(\underline{0}) = 0$ for all $\underline{n} \in \mathbb{N}^N$ with $|\underline{n}| > d$, so

$$f(\underline{x}) = \sum_{\substack{\underline{n} \in \mathbb{N}^N \\ |\underline{n}| \leq d}} \binom{x_1}{n_1} \cdots \binom{x_N}{n_N} \Delta^{\underline{n}} f(\underline{0}) \quad \text{for all } \underline{x} \in \mathbb{N}^N.$$

The right hand side of this equation, however, defines a function $P : \mathbb{Z}^N \to B$. And, $f - P$ has functional degree at most d and vanishes on $\mathbb{N}^N$. So, by Lemma 2.6, $f = P$. □

A finite linear combination $\sum_{|\underline{n}|\le d}\binom{x_1}{n_1}\cdots\binom{x_N}{n_N}a_{\underline{n}}$ of multivariate binomial polynomials $\binom{x_1}{n_1}\cdots\binom{x_N}{n_N}$ with coefficients $a_{\underline{n}}$ in the group B, as in Theorem 2.8b), was called a **polyfract** in [Sc14]. Due to the uniqueness of the coefficients $a_{\underline{n}}$ in Theorem 2.8a), we do not have to distinguish between a polyfract $\sum_{|\underline{n}|\le d}\binom{x_1}{n_1}\cdots\binom{x_N}{n_N}a_{\underline{n}}$, where the x_i may be seen as symbolic variables, and the corresponding polyfractal function

$$f : \mathbb{Z}^N \longrightarrow B\,,\ x \longmapsto \sum_{\substack{\underline{n}\in\mathbb{N}^N\\ |\underline{n}|\le d}} \binom{x_1}{n_1}\cdots\binom{x_N}{n_N}a_{\underline{n}}\,.$$

It is also clear that the functional degree of such a map is given by

$$\operatorname{fdeg}(f) \;=\; \sup\big\{|\underline{n}| \le d \mid \underline{n}\in\mathbb{N}^N,\, a_{\underline{n}}\neq 0\big\}\,, \tag{6}$$

where $\sup(\emptyset) := -\infty$. This follows from the fact that

$$\Delta_i^{m_i}\binom{x_i}{n_i} \;=\; \binom{x_i}{n_i-m_i}$$

and the observation that $x_i \mapsto \binom{x_i}{n_i-m_i}$ is not the zero map whenever $m_i \le n_i$. So if we combine Theorem 2.8b) with formula (6), we obtain the following corollary, which allows us to calculate the functional degree in a more localized fashion – at least if the functional degree is known to be finite.

Corollary 2.9. *Let B be a commutative group, and let $f \in B^{\mathbb{Z}^N}$. If $\operatorname{fdeg}(f) < \infty$ then*

$$\operatorname{fdeg}(f) \;=\; \operatorname{fdeg}_{\underline{0}}(f) \;:=\; \sup\big\{|\underline{n}| \mid \underline{n}\in\mathbb{N}^N,\, \Delta^{\underline{n}}f(\underline{0})\neq 0\big\}\,.$$

In this corollary, the point $\underline{0}$ can be replaced by any other point $\underline{a}\in\mathbb{Z}^N$, since $\operatorname{fdeg}([\underline{a}]f) = \operatorname{fdeg}(f)$. If $\operatorname{fdeg}(f)=\infty$, however, we may have $\operatorname{fdeg}_{\underline{0}}(f)<\infty$. This is because $\operatorname{fdeg}_{\underline{0}}(f)$ depends only on the function values $f(\underline{x})$ at points $\underline{x}\in\mathbb{N}^N$, whereas the requirement $\operatorname{fdeg}(f)<\infty$ allows only one unique extension from $\mathbb{N}^N$ to $\mathbb{Z}^N$ – the extension given by the formula in Theorem 2.8b).

We also see that in the case $B=\mathbb{Q}$, the series representation in Theorem 2.8b) provides a polynomial $\hat{f}\in\mathbb{Q}[t_1,\dots,t_N]$ that describes f:

Corollary 2.10. *If $f\in\mathbb{Q}^{\mathbb{Z}^N}$ has finite functional degree, then there exists a polynomial $\hat{f}\in\mathbb{Q}[t_1,\dots,t_N]$ with $\deg(\hat{f})=\operatorname{fdeg}(f)$ and $\hat{f}(\underline{x})=f(\underline{x})$ for all $\underline{x}\in\mathbb{Z}^N$.*

Remark 2.11.

a) *For B a finitely generated commutative group, the series representation in Theorem 2.8b) was explored in* [Sc14, §2].

b) *The series expansion of Theorem 2.8 is a discrete analogue of the Taylor series expansion of a smooth function $f:\mathbb{R}^N\to\mathbb{R}$. Theorem 2.8a) implies a* uniqueness *property: for any two functions $a_\bullet, b_\bullet : \mathbb{N}^N\to B$ that each map all but finitely many elements of the domain to 0, define associated functions*

$$f_{a_\bullet} : \mathbb{Z}^N\to B,\ \underline{x}\mapsto \sum_{\underline{n}\in\mathbb{N}^N}\binom{x_1}{n_1}\cdots\binom{x_N}{n_N}a_{\underline{n}}$$

and

$$f_{b_\bullet} : \mathbb{Z}^N\to B,\ \underline{x}\mapsto \sum_{\underline{n}\in\mathbb{N}^N}\binom{x_1}{n_1}\cdots\binom{x_N}{n_N}b_{\underline{n}}.$$

Then $f_{a_\bullet} = f_{b_\bullet}$ if and only if $a_\bullet = b_\bullet$. This is a discrete analogue of the fact that in a power series expansion centered at 0, the coefficients are determined by the partial derivatives at 0.

c) *Just as it is immediate to also consider Taylor series expansions centered at a nonzero point $a \in \mathbb{R}^N$, there are also representations of $f \in \mathcal{F}(\mathbb{Z}^N, B)$ based on the values $\Delta^{\underline{n}} f(\underline{a})$ for any fixed $\underline{a} \in \mathbb{Z}^N$.*

Next we recall some notation and a result from [CS21, §3.2]. If $\varepsilon : A \to A$ and $\mu : B \to B'$ are homomorphisms of commutative groups, then we have group homomorphisms

$$\varepsilon^* : B^A \longrightarrow B^{A'}, \;\; f \longmapsto \varepsilon^* f \coloneqq f \circ \varepsilon$$

and

$$\mu_* : B^A \longrightarrow (B')^A, \;\; f \longmapsto \mu_* f \coloneqq \mu \circ f.$$

It is easy to see that ε^* is injective if and only if ε is surjective and that μ_* is surjective if and only if μ is surjective.

The following result is [CS21, Lemma 3.9].

Lemma 2.12 (Homomorphic Functoriality I)**.** *Let $\varepsilon : A' \to A$ and $\mu : B \to B'$ be homomorphisms of commutative groups, and let $f \in B^A$. Then:*

a) $\operatorname{fdeg} \varepsilon^* f \leq \operatorname{fdeg} f$*, with equality if ε is surjective;*
b) $\operatorname{fdeg} \mu_* f \leq \operatorname{fdeg} f$*, with equality if μ is injective.*

The following conceptually similar result is a consequence of Theorem 2.8.

Corollary 2.13 (Homomorphic Functoriality II)**.** *Let B, B' be commutative groups, let $\mu : B \to B'$ be a homomorphism, and let $f \in B^{\mathbb{Z}^N}$.*

a)
$$\mu_* f(\underline{x}) \;=\; \sum_{\underline{n} \in \mathbb{N}^N} \binom{x_1}{n_1} \cdots \binom{x_N}{n_N} \mu(\Delta^{\underline{n}} f(\underline{0})) \quad \textit{for all } \underline{x} \in \mathbb{N}^N.$$

b) *If $d \coloneqq \operatorname{fdeg}(\mu_* f) < \infty$, then*
$$\mu_* f(\underline{x}) \;=\; \sum_{\substack{\underline{n} \in \mathbb{N}^N \\ |\underline{n}| \leq d}} \binom{x_1}{n_1} \cdots \binom{x_N}{n_N} \mu(\Delta^{\underline{n}} f(\underline{0})) \quad \textit{for all } \underline{x} \in \mathbb{Z}^N.$$

Proof. The map $\mu_* : B^{\mathbb{Z}^N} \to (B')^{\mathbb{Z}^N}$ is a homomorphism of $\mathbb{Z}[\mathbb{Z}^N]$-modules. Therefore, for all $\underline{n} \in \mathbb{N}^N$,

$$\Delta^{\underline{n}} \mu_* f \;=\; \Delta^{\underline{n}}(\mu_* f) \;=\; \mu_*(\Delta^{\underline{n}} f) \;=\; \mu_* \Delta^{\underline{n}} f\,. \tag{7}$$

From this and Theorem 2.8a) it follows that, for all $\underline{x} \in \mathbb{N}^N$,

$$\mu_* f(\underline{x}) \;=\; \sum_{\underline{n} \in \mathbb{N}^N} \binom{x_1}{n_1} \cdots \binom{x_N}{n_N} \Delta^{\underline{n}} \mu_* f(\underline{0}) \;=\; \sum_{\underline{n} \in \mathbb{N}^N} \binom{x_1}{n_1} \cdots \binom{x_N}{n_N} \mu(\Delta^{\underline{n}} f(\underline{0}))\,,$$

establishing part a). Applying Theorem 2.8b) to $\mu_* f$ and using (7) again, we get that, for all $\underline{x} \in \mathbb{Z}^N$,

$$\mu_* f(\underline{x}) \;=\; \sum_{\substack{\underline{n} \in \mathbb{N}^N \\ |\underline{n}| \leq d}} \binom{x_1}{n_1} \cdots \binom{x_N}{n_N} \Delta^{\underline{n}} \mu_* f(\underline{0}) \;=\; \sum_{\substack{\underline{n} \in \mathbb{N}^N \\ |\underline{n}| \leq d}} \binom{x_1}{n_1} \cdots \binom{x_N}{n_N} \mu(\Delta^{\underline{n}} f(\underline{0}))\,.$$

□

2.3. **Polynomial Functions and Integer-Valued Polynomials.** In this section we use Theorem 2.8 to compare integer-valued polynomials to functions of finite functional degree. The results of this section are *not* used elsewhere in this paper. However, integer-valued polynomials and their reductions occur in Wilson's proof of Ax-Katz over $\mathbb{F}_p$ [Wi06, Lemma 4], and the technique of representing functions between residue rings of $\mathbb{Z}$ via integer-valued polynomials also occurs in a work of Varga [Va14] generalizing Warning's Second Theorem. It seems potentially useful to know that these techniques can be viewed in terms of the Aichinger-Moosbauer calculus.

Let R be a non-trivial commutative ring, let $N \in \mathbb{Z}^+$, and consider the **evaluation map**

$$E : R[t_1, \ldots, t_n] \longrightarrow R^{R^N}, \ f \longmapsto (x \mapsto f(x)).$$

This is an R-algebra homomorphism; its image is, by definition, the ring of **polynomial functions** on R^N, which we denote by $\mathbf{P}(R^N, R)$. The map E is never an isomorphism, though the manner of the failure depends upon R. If R is finite then $R[t_1, \ldots, t_n]$ is infinite while R^{R^N} is finite, so E has an infinite kernel. If R is infinite, then E is not surjective [Cl14, Thm. 4.3]. More precisely:

Proposition 2.14. *Let R be a non-trivial commutative ring, and let $N \in \mathbb{Z}^+$. Then the following properties are equivalent:*

(i) *The evaluation map $E : R[t_1, \ldots, t_N] \longrightarrow R^{R^N}$ is surjective.*

(ii) *The function*

$$\delta_{0,1} \in R^{R^N}, \ x \longmapsto \begin{cases} 1 & \text{if } x = 0 \\ 0 & \text{if } x \neq 0 \end{cases}$$

lies in the image of E.

(iii) *The ring R is a finite field.*

Proof. To show that (iii) implies (i), which then entails (ii), assume that $R = \mathbb{F}_q$ is a finite field. In this case the study of E was the essence of Chevalley's proof of Theorem 1.1a) in [Ch35]. He showed that E is surjective, with kernel $\langle t_1^q - t_1, \ldots, t_N^q - t_N \rangle$. For English language proofs of modest generalizations, see [Cl14, Cor. 2.5 and Prop. 4.4].

To show that ¬(iii) implies ¬(ii), which then entails ¬(i), we distinguish two cases.
Case 1, R is not a field: In this case, there exists a proper ideal I in R, and then every function F in the image $\mathbf{P}(R^N, R)$ of E is **congruence-preserving** module I: if $x = (x_1, \ldots, x_N)$, $y = (y_1, \ldots, y_N) \in R^N$ are such that $x_i \equiv y_i \pmod I$ for all $1 \leq i \leq N$, then $f(x) \equiv f(y) \pmod I$. But, if $a \in I \setminus \{0\}$, then $a \equiv 0 \pmod I$ while

$$\delta_{0,1}(0, \ldots, 0) = 1 \not\equiv 0 = \delta_{0,1}(a, \ldots, a) \pmod I.$$

So $\delta_{0,1}$ is not congruence-preserving and does not lie in the image of E.
Case 2, R is not finite: In this case, [CS21, Thm. 4.9a)] gives $\mathrm{fdeg}(\delta_{0,1}) = \infty$. So by Lemma 1.5, $\delta_{0,1}$ is not a polynomial function, and does not lie in the image of E. □

If R is an infinite commutative ring that is not a field, we just gave two proofs (in Cases 1 and 2) that $\delta_{0,1} \in R^{R^N} \setminus \mathbf{P}(R^N, R)$. The second proof showed more: that $\delta_{0,1}$ has infinite functional degree. In general, for non-trivial commutative rings R, Lemma 1.5 says that

$$\mathbf{P}(R^N, R) \subseteq \mathcal{F}(R^N, R) \subseteq R^{R^N}. \tag{8}$$

This leads to a more interesting version of the question of when E is surjective.

Question 2.15. *For which non-trivial commutative rings R and numbers $N \in \mathbb{Z}^+$ do we have $\mathbf{P}(R^N, R) = \mathcal{F}(R^N, R)$ – i.e., when is every function $f \in R^{R^N}$ of finite functional degree a polynomial function?*

Here is an answer to Question 2.15 when R is finite.

Proposition 2.16. *For non-trivial finite commutative rings R, the following properties are equivalent:*

(i) $\mathbf{P}(R^N, R) = \mathcal{F}(R^N, R)$ *for all* $N \in \mathbb{Z}^+$.
(ii) $\mathbf{P}(R^N, R) = \mathcal{F}(R^N, R)$ *for some* $N \in \mathbb{Z}^+$.
(iii) $R \cong \prod_{i=1}^r \mathbb{F}_{p_i^{\alpha_i}}$ *for some* $r, \alpha_1, \ldots, \alpha_r \in \mathbb{Z}^+$ *and prime numbers* $p_1 < \cdots < p_r$.

Proof. If R is a finite commutative ring of order $p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ (for primes $p_1 < \cdots < p_r$), then we have a unique internal direct product decomposition $R = \prod_{i=1}^r \mathfrak{r}_i$, with $\mathfrak{r}_i$ a ring of order $p_i^{\alpha_i}$ [Cl-CA, Thm. 8.37] – the **p_i-primary component** of R. We have a natural ring isomorphism

$$R[t_1, \ldots, t_n] = \prod_{i=1}^r \mathfrak{r}_i[t_1, \ldots, t_n]$$

and also, by [AM21, Thm. 9.4] or [CS21, Thm. 3.13], a natural decomposition

$$\mathcal{F}(R^N, R) = \prod_{i=1}^r \mathcal{F}(\mathfrak{r}_i^N, \mathfrak{r}_i).$$

Using these decompositions we get that

$$\mathbf{P}(R^N, R) = \mathcal{F}(R^N, R) \iff \forall 1 \leq i \leq N,\ \mathbf{P}(\mathfrak{r}_i^N, \mathfrak{r}_i) = \mathcal{F}(\mathfrak{r}_i^N, \mathfrak{r}_i).$$

So we reduce to the case in which R has prime power order and, by [AM21, Thm. 9.1],

$$R^{R^N} = \mathcal{F}(R^N, R).$$

Hence, our problem reduces to the previous problem of when the evaluation map is surjective. By Proposition 2.14, this holds if and only if R is a finite field. So, independent of $N \in \mathbb{Z}^+$: $\mathbf{P}(R^N, R) = \mathcal{F}(R^N, R)$ if and only if, for all $1 \leq i \leq r$, $\mathfrak{r}_i$ is a finite field $\mathbb{F}_{p_i^{\alpha_i}}$, i.e. $R \cong \prod_{i=1}^r \mathbb{F}_{p_i^{\alpha_i}}$. □

When R is infinite we do not know a complete answer to Question 2.15, but we will exhibit some positive and negative results.

Lemma 2.17. *Let $h \in \mathcal{F}(\mathbb{Q}^N, \mathbb{Q})$. If $h|_{\mathbb{Z}^N} = 0$ then $h = 0$.*

Proof. Let $D \in \mathbb{Z}^+$, and define $h_D \in \mathbb{Q}^{\mathbb{Z}^N}$ by

$$h_D(\underline{x}) := h\left(\frac{x_1}{D}, \ldots, \frac{x_N}{D}\right).$$

The function h_D is obtained by precomposing h with a group endomorphism of $(\mathbb{Q}^N, +)$, so $h_D \in \mathcal{F}(\mathbb{Q}^N, \mathbb{Q})$ by [AM21, Thm. 4.3]. Hence, by Corollary 2.10, there exists a polynomial $\hat{h}_D(\underline{t}) \in \mathbb{Q}[t_1, \ldots, t_N]$ with $\hat{h}_D(\underline{x}) = h_D(\underline{x})$ for all $\underline{x} = (x_1, \ldots, x_N) \in \mathbb{Z}^N$. Applying Lemma 2.5 to $\hat{h}_D$ with $X = (D\mathbb{Z})^N$ gives $\hat{h}_D = 0$. Thus for all $D \in \mathbb{Z}^+$ we have $h|_{(D^{-1}\mathbb{Z})^N} = 0$, so $h = 0$. □

Proposition 2.18. *For all $N \in \mathbb{Z}^+$, we have $\mathbf{P}(\mathbb{Q}^N, \mathbb{Q}) = \mathcal{F}(\mathbb{Q}^N, \mathbb{Q})$.*

Proof. That $\mathbf{P}(\mathbb{Q}^N, \mathbb{Q}) \subseteq \mathcal{F}(\mathbb{Q}^N, \mathbb{Q})$ is clear. To show that $\mathcal{F}(\mathbb{Q}^N, \mathbb{Q}) \subseteq \mathbf{P}(\mathbb{Q}^N, \mathbb{Q})$ let $g \in \mathcal{F}(\mathbb{Q}^N, \mathbb{Q})$, say with $\mathrm{fdeg}(g) \leq d \in \mathbb{N}$. By Corollary 2.10, there exists a polynomial $\hat{g} \in \mathbb{Q}[t_1, \ldots, t_N]$ with $\deg(\hat{g}) \leq d$ such that $\hat{g}(\underline{x}) = g(\underline{x})$, for all $\underline{x} = (x_1, \ldots, x_N) \in \mathbb{Z}^N$. So $h := E(\hat{g}) - g$ is zero on $\mathbb{Z}^N$ and $\mathrm{fdeg}(h) \leq d$ by [AM21, Lemma 3.2]. By Lemma 2.17 it follows that $h = 0$, which implies $E(\hat{g}) = g$, i.e. $g \in \mathbf{P}(\mathbb{Q}^N, \mathbb{Q})$. □

From now until the end of §2.3 we will assume that R is a commutative domain of characteristic 0, with fraction field K. In this case the evaluation map $E : R[t_1, \ldots, t_N] \longrightarrow R^{R^N}$ is injective [Cl14, Prop. 4.5] and thus induces an isomorphism $R[t_1, \ldots, t_N] \xrightarrow{\sim} \mathbf{P}(R^N, R)$. It is a result of Aichinger-Moosbauer [AM21, Lemma 10.4] that for all $f \in K[t_1, \ldots, t_n]$ we have $\mathrm{fdeg}(E(f)) = \deg(f)$. We will show that the same conclusion holds over R and, in fact, a little more. Namely, we consider the subring of **integer-valued polynomials**

$$\mathrm{Int}(R^N, R) := \left\{ f \in K[t_1, \ldots, t_N] \mid E(f)(R^N) \subseteq R \right\} \subseteq K[t_1, \ldots, t_N].$$

Proposition 2.19. *Let R be a commutative domain. If $f \in \mathrm{Int}(R^N, R)$ and $E_R(f) := \big(x \mapsto f(x)\big) \in R^{R^N}$, then*

$$\mathrm{fdeg}(E_R(f)) \leq \deg(f), \tag{9}$$

with equality if R has characteristic 0.

Proof. Let $f \in \mathrm{Int}(R^N, R)$. By Lemma 2.12, domain restriction and codomain restriction does not increase the functional degree, so Lemma 1.5 yields

$$\mathrm{fdeg}(E_R(f)) \leq \mathrm{fdeg}(E(f)) \leq \deg(f).$$

Now, assume that R has characteristic 0 and that $d := \deg(f) \geq 0$. To complete the proof, it suffices to show that $\mathrm{fdeg}(E_R(f)) \geq d$. As $\deg(f) = d$, a monomial $t_1^{n_1} t_2^{n_2} \cdots t_N^{n_N}$ with $n_1 + n_2 + \cdots + n_N = d$ occurs in the standard expansion of f. If the operators Δ_i are applied to polynomials in the same way as they are applied to functions, then $\deg(\Delta_1^{n_1} \cdots \Delta_N^{n_N} f) = \deg(f) - (n_1 + \cdots + n_N) = 0$, because each application of a Δ_i reduces the degree by exactly 1, as the quotient field of R has characteristic 0. This shows that the function $\Delta_1^{n_1} \cdots \Delta_N^{n_N} E_R(f) = E_R(\Delta_1^{n_1} \cdots \Delta_N^{n_N} f)$ is constant but not zero, so that $\mathrm{fdeg}(E_R(f)) \geq d$, indeed. □

If R is a commutative domain of characteristic $p > 0$, strict inequality can occur in (9). To get an equality one needs to use the p-weight degree and, when R is finite, reduced polynomials: see §4.3.

For a commutative domains R, Proposition 2.19 gives a refinement of (8):

$$\mathbf{P}(R^N, R) \subseteq \mathrm{Int}(R^N, R) \subseteq \mathcal{F}(R^N, R) \subseteq R^{R^N}. \tag{10}$$

This yields a negative answer to Question 2.15 whenever $\mathrm{Int}(R^N, R) \supsetneq \mathbf{P}(R^N, R)$, which certainly holds for $R = \mathbb{Z}$ as e.g. $t(t-1)/2$ is an integer-valued polynomial that does not lie in $\mathbb{Z}[t]$. This leads us to the following result:

Theorem 2.20.

a) $\mathcal{B} := \left\{ \binom{x_1}{n_1} \cdots \binom{x_n}{n_N} \mid \underline{n} \in \mathbb{N}^N \right\}$ *is a basis of the $\mathbb{Z}$-module $\mathcal{F}(\mathbb{Z}^N, \mathbb{Z})$.*

b) $\mathcal{F}(\mathbb{Z}^N, \mathbb{Z}) = \mathrm{Int}(\mathbb{Z}^N, \mathbb{Z})$.

Proof. Part b) of Theorem 2.8 implies that $\mathcal{B}$ spans $\mathcal{F}(\mathbb{Z}^N, \mathbb{Z})$ as a $\mathbb{Z}$-module, and part a) of that theorem states the uniqueness property that characterizes a basis.

By Proposition 2.19, we also have $\mathrm{Int}(\mathbb{Z}^N, \mathbb{Z}) \subseteq \mathcal{F}(\mathbb{Z}^N, \mathbb{Z})$, and it remains to show that $\mathcal{F}(\mathbb{Z}^N, \mathbb{Z}) \subseteq \mathrm{Int}(\mathbb{Z}^N, \mathbb{Z})$. The well-known fact that for all $n \in \mathbb{N}$ we have $\binom{x}{n} \in \mathrm{Int}(\mathbb{Z}, \mathbb{Z})$ follows from Lemma 2.1 and induction. Since $\mathrm{Int}(\mathbb{Z}^N, \mathbb{Z})$ is a ring, we have $b \in \mathrm{Int}(\mathbb{Z}^N, \mathbb{Z})$ for all $b \in \mathcal{B}$. So,

$$\mathcal{F}(\mathbb{Z}^N, \mathbb{Z}) = \langle \mathcal{B} \rangle_{\mathbb{Z}} \subseteq \mathrm{Int}(\mathbb{Z}^N, \mathbb{Z}). \qquad \square$$

Theorem 2.20 implies that $\mathcal{B}$ is a $\mathbb{Z}$-basis of the ring $\mathrm{Int}(\mathbb{Z}^N, \mathbb{Z})$ of integer-valued polynomials, a result of Ostrowski [Os19]. See [CC, Ch. 11] for a general treatment of $\mathrm{Int}(R^N, R)$ for commutative domains R. Cahen-Chabert also address when $\mathrm{Int}(R^N, R) = \mathbf{P}(R^N, R)$ in [CC, §I.3], showing in particular that equality holds when every residue field of R is infinite [CC, Cor. I.3.7], so e.g. when R is a $\mathbb{Q}$-algebra. Our next result implies that, for each $N \in \mathbb{Z}^+$, $\mathrm{Int}(R^N, R) \subsetneq \mathcal{F}(R^N, R)$ whenever $R \supsetneq \mathbb{Q}$ is a $\mathbb{Q}$-algebra.

Let us say that a ring R is a **Cayley ring** if the Cayley homomorphism

$$\mathfrak{C} : R \longrightarrow \mathrm{End}(R, +), \ r \longmapsto r\bullet : x \mapsto rx$$

is an isomorphism (equivalently, is surjective).

Example 2.21.

a) *The following rings are Cayley ring:*
   1. *prime fields, i.e. $\mathbb{Q}$ and the finite fields $\mathbb{F}_p$ with $p \in \mathcal{P}$;*
   2. *subrings of $\mathbb{Q}$, i.e. localizations of $\mathbb{Z}$, including $\mathbb{Z}$ and $\mathbb{Q}$.*

b) *A commutative ring is* not *Cayley if it is free of rank greater than* 1 *as a module over some proper subring. Thus, none of the following rings are Cayley rings:*
   1. *non-prime fields, i.e. fields other than $\mathbb{Q}$ and $\mathbb{F}_p$, for all $p \in \mathcal{P}$;*
   2. *algebras R over any field F such that $F \subsetneq R$;*
   3. *rings of integers $\mathbb{Z}_K$ of number fields $K \supsetneq \mathbb{Q}$;*
   4. *valuation rings of p-adic fields $K \supsetneq \mathbb{Q}_p$, for any $p \in \mathcal{P}$.*

Proposition 2.22. *Let R be a commutative domain of characteristic* 0*. If for some $N \in \mathbb{Z}^+$ we have $\mathrm{Int}(R^N, R) = \mathcal{F}(R^N, R)$, then R is a Cayley ring.*

Proof. Proceeding by contraposition, suppose that R is not a Cayley ring: this means precisely that there is a $\mathbb{Z}$-linear map $L : (R, +) \to (R, +)$ that is not of the form $E(f)$ for a linear polynomial $f \in R[t]$. If K is the fraction field of R, then moreover L is not of the form $E(f)$ for a linear polynomial $f \in K[t]$: if $f = ax + b$ with $a, b \in K$, then evaluating at 0 gives $b = 0$ and evaluating at 1 gives $a = L(1) \in R$. Since $\mathrm{fdeg}(L) = 1$, by Proposition 2.19. L is therefore not given by any integer-valued polynomial. This establishes the result for $N = 1$. For each $N \in \mathbb{Z}^+$, the function $L_N : R^N \to R$ with $L_N(x_1, \ldots, x_N) = L(x_1)$ is again $\mathbb{Z}$-linear, but it is not the restriction to R^N of any K-linear polynomial function. So $L_N \in \mathcal{F}(R^N, R) \setminus \mathrm{Int}(R^N, R)$. $\square$

Proposition 2.22 and Example 2.21 give lots of examples in which $\mathrm{Int}(R^N, R) \subsetneq \mathcal{F}(R^N, R)$: e.g. any field $K \supsetneq \mathbb{Q}$. On the other hand, using similar arguments to the ones we have made, one can show that $\mathrm{Int}(R^N, R) = \mathcal{F}(R^N, R)$ for any subring R of $\mathbb{Q}$.

2.4. **Lifting.** Suppose that $\mu : B \to B'$ is a surjective homomorphism of commutative groups and $f \in \mathcal{F}(\mathbb{Z}^N, B')$. By Theorem 2.8b), there is a unique function $a_\bullet : \mathbb{N}^N \to B'$ that is nonzero in at most finitely many points, we say **finitely nonzero**, such that

$$f(\underline{x}) = \sum_{\underline{n} \in \mathbb{N}^N} \binom{x_1}{n_1} \cdots \binom{x_N}{n_N} a_{\underline{n}} \quad \text{for all } \underline{x} \in \mathbb{Z}^N.$$

By a **lift** of $a_\bullet$ to B (through μ) we will mean a finitely nonzero function $\tilde{a}_\bullet : \mathbb{N}^N \to B$ such that $\mu \circ \tilde{a}_\bullet = a_\bullet$. A **proper lift** is a lift $\tilde{a}_\bullet$ that moreover satisfies, for all $\underline{n} \in \mathbb{N}^N$,

$$\tilde{a}_{\underline{n}} = 0 \iff a_{\underline{n}} = 0\,.$$

Proper lifts always exist, and they are unique if and only if $\mu : B \to B'$ is an isomorphism or $a_\bullet$ is identically 0. To a proper lift $\tilde{a}_\bullet$ we attach the function $\tilde{f} \in B^{\mathbb{Z}^N}$ defined by

$$\tilde{f}(\underline{x}) := \sum_{\underline{n} \in \mathbb{N}^N} \binom{x_1}{n_1} \cdots \binom{x_N}{n_N} \tilde{a}_{\underline{n}}\,.$$

We see that $\operatorname{fdeg}(\tilde{f}) = \sup\{|\underline{n}| \mid \tilde{a}_{\underline{n}} \neq 0\} = \sup\{|\underline{n}| \mid a_{\underline{n}} \neq 0\} = \operatorname{fdeg}(f)$. Combined with Corollary 2.13, we have

$$\mu \circ \tilde{f} = f \quad \text{and} \quad \operatorname{fdeg}(\tilde{f}) = \operatorname{fdeg}(f)\,.$$

We also call $\tilde{f}$ a **proper lift** of f, and may conversely say that f is the **reduction** of $\tilde{f}$.

Moreover, the concept of a proper lift can be strengthened if B and B' are direct products (or direct sums) of families $(B_j)_{j \in J}$ and $(B'_j)_{j \in J}$, respectively, and if μ is the Cartesian product (or direct product) of homomorphisms $\mu_j : B_j \to B'_j$. In that situation, if $\tilde{\pi}_j : B \to B_j$ and $\pi_j : B' \to B'_j$ denote the corresponding projections, we have $\pi_j \circ \mu = \mu_j \circ \tilde{\pi}_j$ for each $j \in J$. We then say $\tilde{a}_\bullet : \mathbb{N}^N \to B$ is **coordinate-wise proper** if each $\tilde{\pi}_j \circ \tilde{a}_\bullet : \mathbb{N}^N \to B_j$ is a proper lift of $\pi_j \circ a_\bullet : \mathbb{N}^N \to B'_j$. Accordingly, we speak of a coordinate-wise proper lift $\tilde{f} \in B^{\mathbb{Z}^N}$ of $f \in \mathcal{F}(\mathbb{Z}^N, B')$ if each $\tilde{\pi}_j \circ \tilde{f}$ is a proper lift of $\pi_j \circ f$. This kind of proper lifts always exist, as well, as one can construct the coordinate-wise lifts $\tilde{\pi}_j \circ \tilde{a}_\bullet$ first, and then combine them into one lift $\tilde{a}_\bullet$.

Combining this discussion with Theorems 2.8 and 2.20, we find that for each $N, m \in \mathbb{Z}^+$, every $f \in \mathcal{F}(\mathbb{Z}^N, \mathbb{Z}/m\mathbb{Z})$ is the reduction of an integer-valued polynomial of degree $\operatorname{fdeg}(f)$. In particular, this applies when for some $p \in \mathcal{P}$ we have $m = p^\beta$ and f is $(p^{\alpha_1}, \ldots, p^{\alpha_N})$-periodic for some $\alpha_1, \ldots, \alpha_N \in \mathbb{Z}^+$, i.e., if f lies in the image of the natural map $(\mathbb{Z}/p^\beta\mathbb{Z})^{\bigoplus_{i=1}^N \mathbb{Z}/p^{\alpha_i}\mathbb{Z}} \to (\mathbb{Z}/p^\beta\mathbb{Z})^{\mathbb{Z}^N}$, a situation that we are about to examine in more detail.

Remark 2.23. *The fact that functions $\mathbb{Z}/p^\alpha\mathbb{Z} \to \mathbb{Z}/p^\beta\mathbb{Z}$ can (after pullback via $\varepsilon : \mathbb{Z} \to \mathbb{Z}/p^\alpha\mathbb{Z}$) be represented by reductions of integer-valued polynomials is applied in work of Varga* [Va14]. *In* [CW18] *this work was generalized to maps of the form $\mathbb{Z}_K/\mathfrak{p}^\alpha \to \mathbb{Z}_K/\mathfrak{p}^\beta$ where K is a number field, $\mathbb{Z}_K$ is its ring of integers, and $\mathfrak{p}$ is a nonzero prime ideal of $\mathbb{Z}_K$ (so that $\mathbb{Z}_K/\mathfrak{p}^\alpha$ and $\mathbb{Z}_K/\mathfrak{p}^\beta$ are finite rings of p-power order for some $p \in \mathcal{P}$). Perhaps these works could be refined using considerations from the present paper and* [CS21].

2.5. **Representation of Functions Between Finite Commutative p-Groups.** If A is a finitely generated commutative group, then for some $N \in \mathbb{Z}^+$ we have a surjective group homomorphism $\varepsilon : \mathbb{Z}^N \to A$. Indeed, up to a harmless isomorphism, we may write A as $\bigoplus_{i=1}^N \mathbb{Z}/a_i\mathbb{Z}$ with parameters $1 \neq a_i \in \mathbb{N}$ and then take

$$\varepsilon : \mathbb{Z}^N \to \bigoplus_{i=1}^N \mathbb{Z}/a_i\mathbb{Z}\,, \quad (x_1, \ldots, x_N) \mapsto (x_1 + a_1\mathbb{Z}, \ldots, x_N + a_N\mathbb{Z})\,.$$

As recalled in Lemma 2.12, the pullback map ε^* restricts to an injective group homomorphism

$$\varepsilon^* : \mathcal{F}(A, B) \hookrightarrow \mathcal{F}(\mathbb{Z}^N, B)\,.$$

and thus every $f \in \mathcal{F}(A, B)$ has the same functional degree as its pullback to $\mathbb{Z}^N$, which by Theorem 2.8b) has a canonical series representation.

For commutative groups A and B, we recall the quantity

$$\delta(A, B) := \sup\{\mathrm{fdeg}(f) \mid f \in B^A\},$$

introduced in [AM21] and further studied in [CS21]. It depends only on the isomorphism type of A and B, and moreover, as shown in [CS21, Cor. 4.3],

$$\delta(A, B) = \delta(A, \mathbb{Z}/e(B)\mathbb{Z}).$$

When both A and B are nontrivial and finite, [CS21, Thm. 4.9] says that $\delta(A, B) < \infty$ if and only if A and B are p-groups for the same $p \in \mathcal{P}$. Moreover, by [CS21, Thm. 4.9c)], if $p \in \mathcal{P}$ and $N, \beta, \alpha_1, \ldots, \alpha_N \in \mathbb{Z}^+$, then

$$\delta\big(\bigoplus_{i=1}^N \mathbb{Z}/p^{\alpha_i}\mathbb{Z}, \mathbb{Z}/p^\beta\mathbb{Z}\big) = \delta_p\big(\underline{\alpha}, \beta\big)\,,$$

where

$$\delta_p\big(\underline{\alpha}, \beta\big) := \sum_{i=1}^N (p^{\alpha_i} - 1) + (\beta - 1)(p - 1)p^{\max\{\alpha_1, \ldots, \alpha_N\} - 1}.$$

Theorem 2.24. *Let $p \in \mathcal{P}$, let $N, \alpha_1, \ldots, \alpha_N \in \mathbb{Z}^+$, and put $A := \bigoplus_{i=1}^N \mathbb{Z}/p^{\alpha_i}\mathbb{Z}$. Let B be a commutative group, and let $F : \mathbb{Z}^N \to B$ be the pullback of a function $f : A \to B$.*

a) *If $\beta \in \mathbb{Z}^+$ is such that $p^\beta f(a) = 0$ for all $a \in A$, then*

$$F(\underline{x}) = \sum_{\substack{\underline{n} \in \mathbb{N}^N \\ |\underline{n}| \leq \delta_p(\underline{\alpha}, \beta)}} \binom{x_1}{n_1} \cdots \binom{x_N}{n_N} \Delta^{\underline{n}} F(\underline{0}) \quad \text{for all } \underline{x} \in \mathbb{Z}^N.$$

b) *For all $h \in \mathbb{Z}^+$ and all $\underline{n} \in \mathbb{N}^n$ with $|\underline{n}| > \delta_p(\underline{\alpha}, h)$,*

$$\Delta^{\underline{n}} F(\underline{x}) \in p^h B \quad \text{for all } \underline{x} \in \mathbb{Z}^N.$$

c) *Let $\mu_h : B \to B/p^hB$ be the quotient map. The conclusion of part b) continues to hold for every function $F : \mathbb{Z}^N \to B$ such that $\mu_h \circ F : \mathbb{Z}^N \to B/p^hB$ is the pullback of a function $g : A \to B/p^hB$.*

Proof. a) Let $\underline{B} := \langle f(A) \rangle$ be the subgroup generated by the image of f. Because $f(a) \in B[p^\beta]$ for all $a \in A$, we have that $\underline{B} = \underline{B}[p^\beta]$. We may view f as a function with codomain $\underline{B}$, which by [CS21, Cor. 3.10b)] does not change its functional degree, so we may assume that $B = \underline{B}$. So by [CS21, Thm. 4.9c)], we get

$$\operatorname{fdeg}(F) \,=\, \operatorname{fdeg}(f) \,\leq\, \delta_p(\underline{\alpha}, \beta),$$

and the result follows from Theorem 2.8.

b) Let $\mu_h : B \to B/p^hB$ be the quotient map. The map $\mu_h \circ f : A \to B/p^hB$ has functional degree at most $\delta_p(\underline{\alpha}, h)$, hence so does its pullback to $\mathbb{Z}^N$, which is $\mu_h \circ F$. For all $\underline{n} \in \mathbb{N}^N$ with $|\underline{n}| > \delta_p(\underline{\alpha}, h)$ this means $\mu_h \circ \Delta^{\underline{n}} F = \Delta^{\underline{n}}(\mu_h \circ F) = 0$, which implies that, for all $\underline{x} \in \mathbb{Z}^N$, $\mu_h(\Delta^{\underline{n}} F(\underline{x})) = \mu_h \circ \Delta^{\underline{n}} F(\underline{x}) = 0$, i.e. $\Delta^{\underline{n}} F(\underline{x}) \in p^h B$.

c) The proof of the previous part used only that $\mu_h \circ F$ is pulled back from A. □

We deduce following results, the latter being a vector-valued analogue of the former.

Corollary 2.25. *Let $p \in \mathcal{P}$, and let $N, \beta, \alpha_1, \ldots, \alpha_N \in \mathbb{Z}^+$. Let $f : \bigoplus_{i=1}^N \mathbb{Z}/p^{\alpha_i}\mathbb{Z} \to \mathbb{Z}/p^\beta\mathbb{Z}$ be any function, let $F : \mathbb{Z}^N \to \mathbb{Z}/p^\beta\mathbb{Z}$ be the pullback of f, and let $\tilde{F} : \mathbb{Z}^N \to \mathbb{Z}$ be a proper lift of F. Then:*

a)
$$\tilde{F}(\underline{x}) \;=\; \sum_{\substack{\underline{n} \in \mathbb{N}^N \\ |\underline{n}| \leq \delta_p(\underline{\alpha}, \beta)}} \binom{x_1}{n_1} \cdots \binom{x_N}{n_N} \Delta^{\underline{n}} \tilde{F}(\underline{0}) \quad \textit{for all } \underline{x} \in \mathbb{Z}^N.$$

b) *For all $h \in \mathbb{Z}^+$ and all $\underline{n} \in \mathbb{N}^n$ with $|\underline{n}| > \delta_p(\underline{\alpha}, h)$,*
$$p^h \;\big|\; \Delta^{\underline{n}} \tilde{F}(\underline{0})\,.$$

Proof. a) Since $\operatorname{fdeg}(\tilde{F}) = \operatorname{fdeg}(F) = \operatorname{fdeg}(f) \leq \delta_p(\underline{\alpha}, \beta)$, this follows from Theorem 2.8b).

b) Assuming $\underline{n} > \delta_p(\underline{\alpha}, h)$, we prove that p^h divides $\Delta^{\underline{n}} \tilde{F}(\underline{0})$. If $h \geq \beta$ then

$$\operatorname{fdeg}(\tilde{F}) \,=\, \operatorname{fdeg}(F) \,=\, \operatorname{fdeg}(f) \,\leq\, \delta_p(\underline{\alpha}, \beta) \,\leq\, \delta_p(\underline{\alpha}, h) \,<\, |\underline{n}|\,,$$

so that $\Delta^{\underline{n}} \tilde{F}(\underline{0}) = 0$, which is divisible by p^h. Hence, we may assume $1 \leq h < \beta$. We show that, in this case, Theorem 2.24c) applies to $\tilde{F}$ and $\mathbb{Z}$ in the place of F and B, which then yields $\Delta^{\underline{n}} \tilde{F}(\underline{0}) \in p^h\mathbb{Z}$, i.e. $p^h \mid \Delta^{\underline{n}} \tilde{F}(\underline{0})$, as desired. With the canonic surjections $\mu_\beta : \mathbb{Z} \to \mathbb{Z}/p^\beta\mathbb{Z}$ and $\mu_h^\beta : \mathbb{Z}/p^\beta\mathbb{Z} \to \mathbb{Z}/p^h\mathbb{Z}$, it suffices to recognize $\mu_h \circ \tilde{F}$ as the pullback of $g := \mu_h^\beta \circ f$. Since F is the pullback of f, however, we obtain $\mu_h^\beta \circ F$ as the pullback of $\mu_h^\beta \circ f$. But, $\mu_h^\beta \circ F = \mu_h \circ \tilde{F}$, because $\mu_h = \mu_h^\beta \circ \mu_\beta$ and $\mu_\beta \circ \tilde{F} = F$, as $\tilde{F}$ is a lift of F. So, indeed, $\mu_h \circ \tilde{F}$ is the pullback of the function g. □

Corollary 2.26. *Let $p \in \mathcal{P}$, let $N, \beta, \alpha_1, \ldots, \alpha_N \in \mathbb{Z}^+$. For each j in a nonempty index set J, let $\beta_j \in \{1, \ldots, \beta\}$. Let $f : \bigoplus_{i=1}^N \mathbb{Z}/p^{\alpha_i}\mathbb{Z} \to \prod_{j \in J} \mathbb{Z}/p^{\beta_j}\mathbb{Z}$ be any function, let $F : \mathbb{Z}^N \to \prod_{j \in J} \mathbb{Z}/p^{\beta_j}\mathbb{Z}$ be the pullback of f, and let $\tilde{F} : \mathbb{Z}^N \to \prod_{j \in J} \mathbb{Z} = \mathbb{Z}^J$ be a proper lift of F. Then:*

a)
$$\tilde{F}(\underline{x}) \;=\; \sum_{\substack{\underline{n} \in \mathbb{N}^N \\ |\underline{n}| \leq \delta_p(\underline{\alpha}, \beta)}} \binom{x_1}{n_1} \cdots \binom{x_N}{n_N} \Delta^{\underline{n}} \tilde{F}(\underline{0}) \quad \textit{for all } \underline{x} \in \mathbb{Z}^N.$$

b) *If $\tilde{F}$ is coordinate-wise proper then, for all $h \in \mathbb{Z}^+$ and all $\underline{n}$ with $|\underline{n}| > \delta_p(\underline{\alpha}, h)$, p^h divides each coordinate of $\Delta^{\underline{n}} \tilde{F}(\underline{0}) \in \mathbb{Z}^J$.*

Proof. a) The exponent of $\prod_{j\in J}\mathbb{Z}/p^{\beta_j}\mathbb{Z}$ divides p^β, so that

$$\mathrm{fdeg}(\tilde{F}) \,=\, \mathrm{fdeg}(F) \,=\, \mathrm{fdeg}(f) \,\leq\, \delta_p(\underline{\alpha},\beta)\,,$$

and Theorem 2.8b) applies to give the result.

b) Fix $j\in J$ and assume $\tilde{F}$ as in the hypothesis. Then $\tilde{\pi}_j\circ\tilde{F}$ is a proper lift of $\pi_j\circ F$, where $\pi_j:\prod_{i\in J}\mathbb{Z}/p^{\beta_i}\mathbb{Z}\to\mathbb{Z}/p^{\beta_j}\mathbb{Z}$ and $\tilde{\pi}_j:\mathbb{Z}^J\to\mathbb{Z}$ are the coordinate projections. So, the functions $\tilde{F}_j := \tilde{\pi}_j\circ\tilde{F}$, $F_j := \pi_j\circ F$, and $f_j := \pi_j\circ f$ meet the requirements of Corollary 2.25b), which yields

$$p^h \;\mid\; \Delta^{\underline{n}}\tilde{F}_j(\underline{0}) \,=\, \Delta^{\underline{n}}(\tilde{\pi}_j\circ\tilde{F})(\underline{0}) \,=\, (\tilde{\pi}_j\circ\Delta^{\underline{n}}\tilde{F})(\underline{0}) \,=\, \tilde{\pi}_j(\Delta^{\underline{n}}\tilde{F}(\underline{0}))\,. \qquad \square$$

3. The Group-Theoretic Ax-Katz Theorem

3.1. **Wilson's Lemma.** Let $N\in\mathbb{Z}^+$. For $s,t_1,\ldots,t_N\in\mathbb{N}$, we put

$$[s) \,:=\, \{0,1,\ldots,s-1\} \quad \text{ and } \quad [s^{\underline{t}}) \,:=\, \prod_{i=1}^{N}[s^{t_i}).$$

With $\mathbb{Z}_{(p)}$ we denote the set of rational numbers of non-negative p-adic valuation. For each $x\in\mathbb{R}$, we set

$$\overline{x} \,:=\, \max(x,0).$$

Now, let A and B be commutative groups, and let $S\subseteq A$ be a finite subset. Following [KP12], for each $f\in B^A$, we define

$$\int_S f \,:=\, \sum_{x\in S} f(x)\in B.$$

The following result is an equivalent (but simpler) reformulation of [Wi06, Lemma 4].

Lemma 3.1. *Let $p\in\mathcal{P}$ and let $N,\beta\in\mathbb{Z}^+$. If $f\in\mathbb{Z}^{\mathbb{Z}^N}$ is such that*

$$\mathrm{fdeg}(f) \,<\, (p-1)(N-\beta+1)\,,$$

then

$$\int_{[p)^N} f \,\equiv\, 0 \pmod{p^\beta}.$$

Proof. Step 1: If $0\leq i\leq p-2$ then $\sum_{x\in\mathbb{Z}/p\mathbb{Z}} x^i = 0$: indeed, upon choosing a generator ζ of the cyclic group $(\mathbb{Z}/p\mathbb{Z})^\times$, we get

$$\sum_{x\in\mathbb{Z}/p\mathbb{Z}} x^i \,=\, \sum_{j=0}^{p-2}(\zeta^i)^j \,=\, \frac{(\zeta^i)^{p-1}-1}{\zeta^i-1} \,=\, 0\,.$$

It follows that if $i_1,\ldots,i_\beta\in[p-1)$ then

$$\sum_{(x_1,\ldots,x_\beta)\in[p)^\beta} x_1^{i_1}\cdots x_\beta^{i_\beta} \,=\, \prod_{j=1}^{\beta}\sum_{x_j\in[p)} x_j^{i_j} \,\equiv\, 0 \pmod{p^\beta}.$$

We deduce that if $g\in\mathbb{Z}_{(p)}[x_1,\ldots,x_\beta]$ has $\deg_j(g)\leq p-2$ for all $1\leq j\leq\beta$, then

$$\int_{[p)^\beta} g \,=\, \sum_{(x_1,\ldots,x_\beta)\in[p)^\beta} g(x_1,\ldots,x_\beta) \,\equiv\, 0 \pmod{p^\beta}.$$

Step 2: If the result holds for a set of functions $f_1, \dots, f_m$ then it holds for the $\mathbb{Z}$-submodule of $\mathbb{Z}^{\mathbb{Z}^N}$ that they generate. Because of this and Theorem 2.8, it suffices to show that the result holds for the polynomial

$$f \coloneqq \binom{x_1}{n_1} \cdots \binom{x_N}{n_N} \in \mathbb{Q}[x_1, \dots, x_N],$$

where $(n_1, \dots, n_N) \in \mathbb{N}^N$ is arbitrary with $|\underline{n}| < (p-1)(N-\beta+1)$. Under that requirement we have

$$\#\big\{1 \le j \le N \mid n_j < p-1\big\} \ge \beta,$$

for if not, we would get $|\underline{n}| = \sum_{j=1}^N n_j \ge (p-1)(N-\beta+1)$. So, we may assume, without loss of generality, that $n_j < p-1$ for all $1 \le j \le \beta$. Then, for every fixed $\underline{y} = (y_{\beta+1}, \dots, y_N) \in \mathbb{Z}^{N-\beta}$,

$$g_{\underline{y}}(x_1, \dots, x_\beta) \coloneqq f(x_1, \dots, x_\beta, y_{\beta+1}, \dots, y_N) \in \mathbb{Z}_{(p)}[x_1, \dots, x_\beta],$$

and $\deg_j(g_{\underline{y}}) = n_j \le p-2$ for all $1 \le j \le \beta$. So, using Step 1, we get

$$\int_{[p)^N} f \;=\; \sum_{\underline{y} \in [p)^{N-\beta}} \; \sum_{(x_1, \dots, x_\beta) \in [p)^\beta} g_{\underline{y}}(x_1, \dots, x_\beta) \;\equiv\; 0 \pmod{p^\beta}. \qquad \square$$

3.2. **The Proof of Theorem 1.7.**

Proof of Theorem 1.7. Without lose of generality, we may assume that, for $1 \le j \le r$,

$$d_j \coloneqq \operatorname{fdeg}(f_j) > 0.$$

We set

$$\mathcal{M} \coloneqq \max_{1 \le j \le r} p^{\beta_j - 1} d_j \in \mathbb{Z}^+$$

and put

$$\beta \coloneqq \left\lceil \frac{N - \sum_{j=1}^r \frac{p^{\beta_j}-1}{p-1} d_j}{\max\limits_{1 \le j \le r} p^{\beta_j - 1} d_j} \right\rceil = \left\lceil \frac{N - \sum_{j=1}^r \frac{p^{\beta_j}-1}{p-1} d_j}{\mathcal{M}} \right\rceil.$$

We have

$$\beta < \frac{N - \sum_{j=1}^r \frac{p^{\beta_j}-1}{p-1} d_j}{\mathcal{M}} + 1$$

and thus

$$\sum_{j=1}^r \frac{p^{\beta_j}-1}{p-1} d_j < N - \mathcal{M}(\beta - 1). \tag{11}$$

For $1 \le j \le r$, we define $\chi_j : \mathbb{Z} \to \mathbb{Z}/p^\beta\mathbb{Z}$ by

$$\chi_j(x) \coloneqq \begin{cases} 1 & \text{if } x \equiv 0 \pmod{p^{\beta_j}}, \\ 0 & \text{otherwise.} \end{cases}$$

Since χ_j is pulled back from $\mathbb{Z}/p^{\beta_j}\mathbb{Z}$, it has finite functional degree; let $\widetilde{\chi}_j$ be a proper lift of χ_j from $\mathbb{Z}/p^\beta\mathbb{Z}$ to $\mathbb{Z}$. Let $\chi : \mathbb{Z}^r \to \mathbb{Z}/p^\beta\mathbb{Z}$ be the tensor product $\bigotimes_{j=1}^r \chi_j$ of the χ_j, and let $\widetilde{\chi} : \mathbb{Z}^r \to \mathbb{Z}$ be the tensor product $\bigotimes_{j=1}^r \widetilde{\chi}_j$ of the $\widetilde{\chi}_j$: for all $(x_1, \dots, x_r) \in \mathbb{Z}^r$,

$$\chi(x_1, \dots, x_r) \coloneqq \prod_{j=1}^r \chi_j(x_j) = \prod_{j=1}^r \widetilde{\chi}_j(x_j) + p^\beta\mathbb{Z} = \widetilde{\chi}(x_1, \dots, x_r) + p^\beta\mathbb{Z}.$$

For $1 \le j \le r$, let $F_j : \mathbb{Z}^N \to \mathbb{Z}/p^{\beta_j}\mathbb{Z}$ be the pullback of f_j and let $\tilde{F}_j$ be a proper lift of F_j from $\mathbb{Z}/p^{\beta_j}\mathbb{Z}$ to $\mathbb{Z}$. Then, with the bijection $[p)^N \to (\mathbb{Z}/p\mathbb{Z})^N$ given by $\underline{x} \mapsto [\underline{x}] := (x_j + p\mathbb{Z})_{j=1}^N$, we have for all $\underline{x} \in [p)^N$,

$$\chi(\tilde{F}_1(\underline{x}), \dots, \tilde{F}_r(\underline{x})) \;=\; \begin{cases} 1 & \text{if } [\underline{x}] \in Z(f_1, \dots, f_r), \\ 0 & \text{otherwise.} \end{cases}$$

Thus, the desired conclusion that p^β divides $\#Z(f_1, \dots, f_r)$ is equivalent to

$$\int_{[p)^N} \chi(\tilde{F}_1, \dots, \tilde{F}_r) \;=\; 0 \;\in\; \mathbb{Z}/p^\beta\mathbb{Z}\,,$$

and thus also to

$$\operatorname{ord}_p\!\left(\int_{[p)^N} \widetilde{\chi}(\tilde{F}_1, \dots, \tilde{F}_r)\right) \;\ge\; \beta\,. \tag{12}$$

By Corollary 2.25, there is a function $c_j : \mathbb{N} \to \mathbb{Z}$ with $c_j(n) = 0$ for all but finitely many $n \in \mathbb{N}$, such that, for all $x \in \mathbb{Z}$,

$$\tilde{\chi}_j(x) \;=\; \sum_{n \in \mathbb{N}} \binom{x_j}{n} c_j(n)\,,$$

and, for each $h \in \mathbb{Z}^+$,

$$n_j > p^{\beta_j} - 1 + (h-1)(p-1)p^{\beta_j - 1} \implies p^h \,\big|\, c_j(n_j)\,. \tag{13}$$

Therefore, for all $\underline{x} \in \mathbb{Z}^N$,

$$\begin{aligned} \tilde{\chi}(\tilde{F}_1(\underline{x}), \dots, \tilde{F}_r(\underline{x})) &= \tilde{\chi}_1(\tilde{F}_1(\underline{x})) \cdots \tilde{\chi}_r(\tilde{F}_r(\underline{x})) \\ &= \sum_{\underline{n} \in \mathbb{N}^r} \binom{\tilde{F}_1(\underline{x})}{n_1} \cdots \binom{\tilde{F}_r(\underline{x})}{n_r} c_1(n_1) \cdots c_r(n_r)\,. \end{aligned}$$

Hence,

$$\begin{aligned} \int_{[p)^N} \tilde{\chi}(\tilde{F}_1, \dots, \tilde{F}_r) &= \int_{[p)^N} \sum_{\underline{n} \in \mathbb{N}^r} \binom{\tilde{F}_1}{n_1} \cdots \binom{\tilde{F}_r}{n_r} c_1(n_1) \cdots c_r(n_r) \\ &= \sum_{\underline{n} \in \mathbb{N}^r} c_1(n_1) \cdots c_r(n_r) \int_{[p)^N} \binom{\tilde{F}_1}{n_1} \cdots \binom{\tilde{F}_r}{n_r}\,. \end{aligned}$$

Thus to prove (12), it suffices to show that, for each $\underline{n} = (n_1, \dots, n_r) \in \mathbb{N}^r$,

$$\operatorname{ord}_p\big(c_1(n_1) \cdots c_r(n_r)\big) \;+\; \operatorname{ord}_p\!\left(\int_{[p)^N} \binom{\tilde{F}_1}{n_1} \cdots \binom{\tilde{F}_r}{n_r}\right) \;\ge\; \beta. \tag{14}$$

Now, for each $1 \le j \le r$, let h_j be the unique integer with

$$p^{\beta_j} - 1 + (h_j - 1)(p-1)p^{\beta_j - 1} \;<\; n_j \;\le\; p^{\beta_j} - 1 + h_j(p-1)p^{\beta_j - 1}. \tag{15}$$

Then (13) gives $\operatorname{ord}_p(c_j(n_j)) \ge h_j$. So, on one hand,

$$\operatorname{ord}_p\big(c_1(n_1) \cdots c_r(n_r)\big) \;=\; \sum_{j=1}^r \operatorname{ord}_p(c_j(n_j)) \;\ge\; \sum_{j=1}^r h_j \;=:\; \alpha\,, \tag{16}$$

and then (14) certainly holds if $\alpha \geq \beta$. On the other hand, if $\alpha < \beta$ then $\beta - 1 - \alpha \geq 0$. Hence, as $\operatorname{fdeg}(\tilde{F}_j) = \operatorname{fdeg}(F_j) = \operatorname{fdeg}(f_j) \leq d_j$, using [AM21, Thm. 4.3 & Lem. 6.1], (15), the definition of $\mathcal{M}$, (11) and that $\mathcal{M} \geq 1$, we get

$$\begin{aligned}
\operatorname{fdeg}\left(\binom{\tilde{F}_1}{n_1}\cdots\binom{\tilde{F}_r}{n_r}\right) &\leq \sum_{j=1}^{r} n_j d_j \\
&\leq (p-1)\sum_{j=1}^{r}\Big(\frac{p^{\beta_j}-1}{p-1} + h_j p^{\beta_j - 1}\Big) d_j \\
&\leq (p-1)\Big(\sum_{j=1}^{r}\frac{p^{\beta_j}-1}{p-1} d_j + \mathcal{M}\alpha\Big) \\
&< (p-1)\big(N - \mathcal{M}(\beta - 1 - \alpha)\big) \\
&\leq (p-1)\big(N - (\beta - \alpha) + 1\big).
\end{aligned}$$

Hence, Lemma 3.1 implies

$$\operatorname{ord}_p\left(\int_{[p)^N}\binom{\tilde{F}_1}{n_1}\cdots\binom{\tilde{F}_r}{n_r}\right) \geq \beta - \alpha\,. \tag{17}$$

Combining (16) and (17) we get (14), which completes the proof of Theorem 1.7. □

4. p-WEIGHTS

4.1. **p-weight degrees.** Let $p \in \mathcal{P}$. Each $d \in \mathbb{N}$ can be written in the form $d = \sum_{i=0}^{N} a_i p^i$ with uniquely determined coefficients $a_i \in [p)$. Using this base p expansion, we define the **p-weight** of d as

$$\sigma_p(d) = \sigma_{p,\mathbb{N}}(d) \coloneqq \sum_{i=0}^{N} a_i.$$

We have $\sigma_p(d) \leq d$ with equality if and only if $d \in [p)$. For fixed p and large d, we have $\sigma_p(d) = O(\log d)$, so the p-weight of d can be much smaller than d itself.

Let R be a commutative rng. The **p-weight degree** of a nonzero monomial term $c\,t_1^{d_1}\cdots t_n^{d_n}$ with $c \in R \setminus \{0\}$ is defined to be

$$\sigma_p(c\,t_1^{d_1}\cdots t_n^{d_n}) \coloneqq \sum_{i=1}^{n}\sigma_p(d_i),$$

and the p-weight degree of a nonzero polynomial $f \in R[t_1,\dots,t_n]$ is the maximum p-weight degree of its nonzero monomial terms. We also set $\sigma_p(0) \coloneqq -\infty$. A polynomial has positive degree if and only if it has positive p-weight degree.

We will also need the product $\bigotimes_{i=1}^{n} f_i$ of functions $f_1 : A_1 \to R$, …, $f_n : A_n \to R$ on commutative groups $A_1,\dots,A_n$, where R is again a rng, which is defined by

$$\bigotimes_{i=1}^{n} f_i : \prod_{i=1}^{n} A_i \to R\,, \quad (x_1,\dots,x_n) \mapsto f_1(x_1)\cdots f_n(x_n)\,.$$

In this setting, we have the following lemmas.

Lemma 4.1. *For each $1 \le j \le n$, let $a_{j,1}, \dots, a_{j,K(j)} \in A_j \subseteq \prod_{i=1}^n A_i$, and let $(a_1, \dots, a_K)$ be a permutation of all $K := K(1) + \cdots + K(n)$ given elements $a_{j,k}$. Then*

$$\Delta_{a_1} \cdots \Delta_{a_K} \big(f_1 \otimes \cdots \otimes f_n\big) \;=\; \big(\Delta_{a_{1,1}} \cdots \Delta_{a_{1,K(1)}} f_1\big) \otimes \cdots \otimes \big(\Delta_{a_{n,1}} \cdots \Delta_{a_{n,K(n)}} f_n\big)\,.$$

Proof. If $a = (a, 0) \in A_1 = A_1 \times \{0\} \subseteq A_1 \times A_2$ and $(x_1, x_2) \in A_1 \times A_2$ then

$$\begin{aligned} \big(\Delta_a(f_1 \otimes f_2)\big)(x_1, x_2) \;&=\; f_1(x_1 + a) f_2(x_2) - f_1(x_1) f_2(x_2) \\ &=\; (f_1(x_1 + a) - f_1(x_1)) f_2(x_2) \\ &=\; \big((\Delta_a f_1) \otimes f_2\big)(x_1, x_2)\,. \end{aligned}$$

Hence, $\Delta_a(f_1 \otimes f_2) = (\Delta_a f_1) \otimes f_2$. More generally, if $a \in A_j$ then

$$\Delta_a(f_1 \otimes \cdots \otimes f_n) \;=\; f_1 \otimes \cdots \otimes f_{j-1} \otimes (\Delta_a f_j) \otimes f_{j+1} \otimes \cdots \otimes f_n\,.$$

From this, and the commutativity of the operators $\Delta_{a_{j,k}}$, the stated equation follows. □

Lemma 4.2. *We have*

$$\operatorname{fdeg}_j\big(\bigotimes_{i=1}^n f_i\big) \;\le\; \operatorname{fdeg}(f_j) \quad \textit{for all } 1 \le j \le n\,.$$

In particular,

$$\operatorname{fdeg}\big(\bigotimes_{i=1}^n f_i\big) \;\le\; \sum_{i=1}^n \operatorname{fdeg}(f_i)\,.$$

Equality holds in both inequalities, as shown in [AM21, Lemma 6.2]*, if R is a domain and the functions $f_1, \dots, f_n$ are all nonzero.*

Proof. Assume $1 \le j \le n$. Lemma 4.1 shows that $\Delta_{a_{j,1}} \cdots \Delta_{a_{j,K(j)}} \big(f_1 \otimes \cdots \otimes f_n\big) = 0$ whenever $K(j) > \operatorname{fdeg}(f_j)$, because

$$\Delta_{a_{j,1}} 1 \cdots \Delta_{a_{j,K(j)}} \big(f_1 \otimes \cdots \otimes f_n\big) \;=\; f_1 \otimes \cdots \otimes f_{j-1} \otimes \cdots \otimes \big(\Delta_{a_{j,1}} \cdots \Delta_{a_{j,K(j)}} f_j\big) \otimes f_{j+1} \otimes \cdots \otimes f_n$$

and $\Delta_{a_{j,1}} \cdots \Delta_{a_{j,K(j)}} f_j = 0$ if $K(j) > \operatorname{fdeg}(f_j)$. This means $\operatorname{fdeg}_j\big(\bigotimes_{i=1}^n f_i\big) \le \operatorname{fdeg}(f_j)$. If we combine these inequalities with Theorem 2.3, we get

$$\operatorname{fdeg}\big(\bigotimes_{i=1}^n f_i\big) \;\le\; \sum_{i=1}^n \operatorname{fdeg}_i\big(\bigotimes_{j=1}^n f_j\big) \;\le\; \sum_{i=1}^n \operatorname{fdeg}(f_i)\,.$$

It remains to show that

$$\operatorname{fdeg}\big(\bigotimes_{i=1}^n f_i\big) \;\ge\; \sum_{i=1}^n \operatorname{fdeg}(f_i)$$

whenever R is a domain and $K(j) := \operatorname{fdeg}(f_j) \ge 0$, for all $1 \le j \le n$. To prove this, we choose for each $1 \le j \le n$ elements $a_{j,1}, \dots, a_{j,K(j)} \in A_j$ such that

$$\Delta_{a_{j,1}} \cdots \Delta_{a_{j\,K(j)}} f_j \neq 0\,.$$

Then, by Lemma 4.1, and because R is a domain,

$$\Delta_{a_{1,1}} \cdots \Delta_{a_{n,K(n)}} \big(f_1 \otimes \cdots \otimes f_n\big) \;=\; \big(\Delta_{a_{1,1}} \cdots \Delta_{a_{1,K(1)}} f_1\big) \otimes \cdots \otimes \big(\Delta_{a_{n,1}} \cdots \Delta_{a_{n,K(n)}} f_n\big) \;\neq\; 0\,,$$

which means that $\operatorname{fdeg}\big(\bigotimes_{i=1}^n f_i\big) \ge K(1) + \cdots + K(n) = \sum_{i=1}^n \operatorname{fdeg}(f_i)$, indeed. □

The next result is the first half of [AM21, Theorem 10.3] in a more general setting.

Proposition 4.3. *Let $p \in \mathcal{P}$, and let R be a commutative ring of characteristic p. Let $f \in R[t_1, \ldots, t_n]$ be a polynomial, with associated function $E(f) \in R^{R^n}$. Then*

$$\operatorname{fdeg}(E(f)) \leq \sigma_p(f). \tag{18}$$

Proof. Since $\operatorname{fdeg}(E(f)) = -\infty$ if $E(f) = 0$, we may assume that $E(f) \neq 0$. By [AM21, Lemma 3.2] we have $\operatorname{fdeg}(f_1+f_2) \leq \max\big(\operatorname{fdeg}(f_1), \operatorname{fdeg}(f_2)\big)$. Since $\sigma_p(f)$ is the maximum of the p-weight degrees of the nonzero monomial terms of f, we reduce to the case of a monomial term

$$f = c\, t_1^{d_1} \cdots t_n^{d_n}, \ \ c \in R \setminus \{0\}.$$

Using [AM21, Lemmas 6.1] and Lemma 4.2, we get

$$\operatorname{fdeg}(c\, t_1^{d_1} \cdots t_n^{d_n}) \leq \operatorname{fdeg}(c) + \sum_{i=1}^n \operatorname{fdeg}(E(t_i^{d_i})) = \sum_{i=1}^n \operatorname{fdeg}(E(t_i^{d_i})).$$

We have reduced to the univariate monomial case and must show: for all $d \in \mathbb{Z}^+$ we have

$$\operatorname{fdeg}(E(t^d)) \leq \sigma_p(d).$$

Writing $d = \sum_{i=0}^N a_i p^i$ with $a_i \in [p)$ and using [AM21, Lemma 6.1], we get

$$\operatorname{fdeg}(E(t^d)) = \operatorname{fdeg}\left(\prod_{i=0}^N (E(t^{p^i}))^{a_i}\right) \leq \sum_{i=0}^N a_i \operatorname{fdeg}(E(t^{p_i})) = \sum_{i=0}^N a_i = \sigma_p(d),$$

since each $E(t^{p^i})$ is a nonzero group homomorphism and thus has functional degree 1. □

4.2. **A Generalized Moreno-Moreno Theorem.** Combining Corollary 1.9 and Proposition 4.3 we get:

Theorem 4.4. *Let R be a finite commutative ring of prime characteristic p and order p^N. Let $f_1, \ldots, f_r \in R[t_1, \ldots, t_n]$ be nonzero polynomials. If $Z := Z_{R^n}(f_1, \ldots, f_r)$, then*

$$\operatorname{ord}_p(\#Z) \geq \left\lceil \frac{N\big(n - \sum_{j=1}^r \sigma_p(f_j)\big)}{\max_{j=1}^r \sigma_p(f_j)} \right\rceil.$$

Proof. The result trivially holds if all functions $E(f_j)$ are zero. If some but not all functions $E(f_j)$ are zero, it is enough to prove the theorem for the set of functions f_j with $E(f_j) \neq 0$, as that yields a lower bound at least as good as the stated one. So we may assume that Corollary 1.9 applies. The resulting inequality

$$\operatorname{ord}_p(\#Z) \geq \left\lceil \frac{N\big(n - \sum_{j=1}^r \operatorname{fdeg}(E(f_j))\big)}{\max_{j=1}^r \operatorname{fdeg}(E(f_j))} \right\rceil$$

remains true if every functional degree $\operatorname{fdeg}(E(f_j))$ is replaced by an upper bound for $\operatorname{fdeg}(E(f_j))$, such as the one given in Proposition 4.3. □

If in Theorem 4.4 we take R to be the finite field $\mathbb{F}_{p^N}$, we recover the Moreno-Moreno Theorem [MM95, Thm. 1].

Theorem 4.5 (Moreno-Moreno)**.** *Let $p \in \mathbb{P}$ and $q := p^N$. Let $f_1, \ldots, f_r \in \mathbb{F}_q[t_1, \ldots, t_n]$ be nonzero polynomials. If $Z := Z_{\mathbb{F}_q}(f_1, \ldots, f_r)$, then*

$$\operatorname{ord}_p(\#Z) \geq \left\lceil \frac{N\big(n - \sum_{j=1}^r \sigma_p(f_j)\big)}{\max_{j=1}^r \sigma_p(f_j)} \right\rceil.$$

4.3. **Functional degrees of polynomial functions in positive characteristic.** Let R be a commutative ring of prime characteristic p. Must we have equality in (18)? When R is a field, this is answered by [AM21, Thm. 10.3]. In this result Aichinger-Moosbauer show that $\mathrm{fdeg}(E(f)) = \sigma_p(f)$ whenever R is an infinite field of characteristic p. Later in this section we will show that this result continues to hold whenever R is an infinite *domain* of characteristic p.

The case of $R = \mathbb{F}_q$ is more closely related to the main results in this paper: a strict inequality $\mathrm{fdeg}(E(f)) < \sigma_p(f)$ would yield a further improvement of the Ax-Katz Theorem. It turns out that strict inequality can occur, however in a way that leads only to improvements of the Ax-Katz Theorem that had already been well understood.

To explain, we call a nonzero monomial term $c_{\underline{d}}\, t_1^{d_1} \cdots t_n^{d_n} \in \mathbb{F}_q[t_1, \ldots, t_n]$ **reduced** if $d_j \leq q-1$ for all $1 \leq j \leq n$. (Note the strong dependence on the ground field.) A polynomial is **reduced** if each of its nonzero monomial terms are reduced.

Just using the fact that $x^q = x$ for all $x \in \mathbb{F}_q$, it is easy to see that to every $f \in \mathbb{F}_q[t_1, \ldots, t_n]$ there is a reduced polynomial $\overline{f} \in \mathbb{F}_q[t_1, \ldots, t_n]$ that induces the same function $\mathbb{F}_q^n \to \mathbb{F}_q$ as f. Already in [Ch35], Chevalley showed that every function in $\mathbb{F}_q^{\mathbb{F}_q^n}$ is equal to $E(f)$ for a unique reduced polynomial f. (For an English language proof and some modest generalizations, see [Cl14, §2.3 and §3.1].) In particular, the polynomial $\overline{f}$ alluded to above is the unique reduced polynomial inducing the same function as f.

Now for any $f_1, \ldots, f_r \in \mathbb{F}_q[t_1, \ldots, t_n]$, since the solution set

$$Z(f_1, \ldots, f_r) \coloneqq \{x \in \mathbb{F}_q^n \mid f_1(x) = \cdots = f_r(x) = 0\}$$

depends only on the associated functions $E(f_1), \ldots, E(f_r)$, we always have

$$Z(f_1, \ldots, f_r) = Z(\overline{f_1}, \ldots, \overline{f_r}).$$

One gets easy strengthenings of many results of Chevalley-Warning type – in particular the theorems of Chevalley-Warning and Ax-Katz – by replacing $f_1, \ldots, f_r$ by $\overline{f_1}, \ldots, \overline{f_r}$, since in this process none of the degrees can increase.

The following result is part of [AM21, Thm. 10.3].

Theorem 4.6 (Aichinger-Moosbauer)**.** *Let $f \in \mathbb{F}_q[t_1, \ldots, t_n]$ be a nonzero polynomial, and let $E(f) \in \mathbb{F}_q^{\mathbb{F}_q^n}$ be the associated polynomial function. Then*

$$\mathrm{fdeg}(E(f)) = \sigma_p(\overline{f}).$$

Proposition 4.3 and Theorem 4.6 imply that

$$\sigma_p(\overline{f}) = \mathrm{fdeg}(E(f)) \leq \sigma_p(f)\,;$$

that is, passing to the reduced polynomial also cannot increase the p-weight degree. So, in the setting of the Moreno-Moreno Theorem, one can improve the conclusion to

$$\mathrm{ord}_p(\#Z_{\mathbb{F}_q^n}(f_1, \ldots, f_r)) \geq \left\lceil \frac{N\big(n - \sum_{j=1}^r \sigma_p(\overline{f_j})\big)}{\max_{j=1}^r \sigma_p(\overline{f_j})} \right\rceil$$

which by Theorem 4.6 is the optimal application of Corollary 1.9 to polynomials over $\mathbb{F}_q$.

Remark 4.7. *For a reduced polynomial $f \in \mathbb{F}_p[t_1, \ldots, t_n]$, we have $\deg(f) = \sigma_p(f)$, so Moreno-Moreno gives no essential improvement upon Ax-Katz when $q = p$.*

Now we prepare for our generalization of [AM21, Thm. 10.3] with the following result.

Lemma 4.8. *Let A be an infinite commutative codomain that is a finitely generated $\mathbb{F}_p$-algebra. Let $x_1, \ldots, x_m \in A \setminus \{0\}$, and let $M \in \mathbb{Z}^+$. Then there is a maximal ideal $\mathfrak{m}$ of A such that:*

(i) *$x_1, \ldots, x_m \notin \mathfrak{m}$, and*
(ii) *$A/\mathfrak{m}$ is a finite field of size greater than M.*

Proof. Replacing $x_1, \ldots, x_m$ with $x := x_1 \cdots x_m$, we reduce to the case of $m = 1$. Zariski's Lemma [Cl-CA, Thm. 11.1] implies that for every maximal ideal $\mathfrak{m}$ of A, the field $A/\mathfrak{m}$ is a finite-dimensional $\mathbb{F}_p$-vector space, hence a finite field. The same argument shows that A is not itself a field; also A is a Noetherian ring [Cl-CA, Cor. 8.39]. Moreover, since A is a finitely generated algebra over the field $\mathbb{F}_p$ it is a Jacobson domain [Cl-CA, Prop. 11.3b)], so $\bigcap_{\mathfrak{m} \in \operatorname{MaxSpec} A} \mathfrak{m} = (0)$. In particular A has infinitely many maximal ideals, since a finite intersection of nonzero ideals in a domain is nonzero. It follows that the set $\mathcal{U}(x)$ of maximal ideals $\mathfrak{m}$ of A such that $x \notin \mathfrak{m}$ is nonempty. We claim that $\mathcal{U}(x)$ is moreover infinite: if on the contrary we had $\mathcal{U}(x) = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_n\}$, then for $1 \le i \le n$ choose $y_i \in \mathfrak{m}_i \setminus \{0\}$, and we see that $xy_1 \cdots y_n$ is a nonzero element of A that lies in every maximal ideal of A: contradiction. Finally, by [Cl-CA, Thm. 22.23], in any Noetherian ring S, for all $M \in \mathbb{Z}^+$ there are only finitely man ideals I of M such that S/I is finite of size at most M. So in any infinite family of maximal ideals of A, the size of the residue ring approaches infinity. □

Theorem 4.9. *Let R be an infinite commutative domain of characteristic p. Let $f \in R[t_1, \ldots, t_n]$ and let $E(f) \in \mathbf{P}(R^n, R)$ be the associated polynomial function. Then*

$$\operatorname{fdeg}(E(f)) = \sigma_p(f).$$

Proof. By Proposition 4.3 it suffices to show that $\operatorname{fdeg}(E(f)) \ge \sigma_p(f)$. Let K be the fraction field of R.
Case 1, $K/\mathbb{F}_p$ is an algebraic field extension: This case is already covered by [AM21, Thm. 10.3], as necessarily $R = K$: indeed, for every nonzero element $x \in R$ there is a positive integer n_x such that $x^{n_x} = 1$, so $x^{-1} = x^{n_x - 1} \in R$.
Case 2, $K/\mathbb{F}_p$ is transcendental: In this case R must contain elements that are transcendental over $\mathbb{F}_p$: let t be such an element, and let A be the $\mathbb{F}_p$-subalgebra of R generated by t and the coefficients of f. Let $a \in \mathbb{Z}^+$. By Lemma 4.8, there is a maximal ideal $\mathfrak{m}$ of A that does not contain any of the coefficients of f and such that $\mathbb{F} := A/\mathfrak{m}$ is a finite field $\mathbb{F}$ of order at least p^a. Let $\underline{f}$ be the image of f in $\mathbb{F}[t_1, \ldots, t_n]$. By Lemma 2.12 we have

$$\operatorname{fdeg}(E(f)) \ge \operatorname{fdeg}(E(f)|_{A^n}) \ge \operatorname{fdeg}(E(\underline{f})).$$

By our choice of $\mathfrak{m}$, the monomials appearing in $\underline{f}$ with nonzero coefficient are the same as those appearing in f with nonzero coefficient, so $\sigma_p(\underline{f}) = \sigma_p(f)$. Choosing a larger than $\max_{1 \le i \le n} \deg_i(f)$ makes $\underline{f}$ $\mathbb{F}$-reduced, so by Theorem 4.6 we have

$$\operatorname{fdeg}(E(f)) \ge \operatorname{fdeg}(E(\underline{f})) = \sigma_p(\underline{f}) = \sigma_p(f).$$ □

5. Further Work

It is natural to ask for a generalization of Theorem 1.7 in which instead of $(\mathbb{Z}/p\mathbb{Z})^N$, we may take A to be any finite commutative p-group. Such a result will be given in the forthcoming work [CS23]. The proof follows the same basic strategy: the p-adic divisibility comes from a combination of Corollary 2.25 and a generalization of Lemma 3.1 to sums of the form $\int_{\prod_{i=1}^N [p^{\alpha_i})} f$.

Here is a quick overview of this work: to solve the number-theoretic problem of determining $\mathrm{ord}_p(\int_{\prod_{i=1}^N [p^{\alpha_i})} f)$ for

$$f(\underline{x}) = \binom{x_1}{n_1} \cdots \binom{x_N}{n_N}$$

in terms of $n_1, \ldots, n_N$ is not very difficult, but to solve the discrete optimization problem of, for each fixed $\underline{\alpha} = (\alpha_1, \ldots, \alpha_N)$, minimizing this quantity over all $\underline{n} = (n_1, \ldots, n_N) \in \mathbb{N}^N$ with fixed $d \coloneqq |\underline{n}|$ takes more work. Then we must minimize the total p-adic divisibility obtained from this and from Corollary 2.25. The answer obtained is intricate in the general case, suggesting that these complications may be inherent to the problem.

The $\beta = 1$ case of Lemma 3.1 gives a result of Ax [Ax64]; let's call it *Ax's Lemma*. Ax's Lemma comprises most of the ten line proof of Chevalley-Warning referred to in the introduction. It suggests a further problem in the Aichinger-Moosberger calculus.

Question 5.1. *Let A and B be finite commutative p-groups. What is the largest $d \in \tilde{\mathbb{N}}$ such that for all $f \in B^A$ with $\mathrm{fdeg}(f) \leq d$, we have*

$$\int_A f \coloneqq \sum_{x \in A} f(x) = 0\,?$$

Let us call this largest possible d the **summation invariant** $\sigma(A, B)$. In this notation, Ax's Lemma amounts to:

$$\forall p \in \mathcal{P},\ \forall N \in \mathbb{Z}^+,\ \sigma\big((\mathbb{Z}/p\mathbb{Z})^N, \mathbb{Z}/p\mathbb{Z}\big) = N(p-1) - 1.$$

In the paper [CT23] the following generalization of Ax's Lemma will be shown:

$$\forall p \in \mathcal{P},\ \forall N \in \mathbb{Z}^+,\ \forall 1 \leq \beta \leq N,\ \sigma((\mathbb{Z}/p\mathbb{Z})^N, \mathbb{Z}/p^\beta\mathbb{Z}) = N(p-1) - 1. \tag{19}$$

In [CT23] we use (19) to derive a qualitative generalization of Ax-Katz over any finite rng R of size divisible by p: if we fix the number and degrees of polynomials $f_1, \ldots, f_r$, then $\mathrm{ord}_p(\#Z_{R^N}(f_1, \ldots, f_r))$ approaches infinity with the number N of variables.

Such results also follow from the main theorem of [CS23] – but the argument is different. Unlike the proofs presented here and in [CS23], the arguments of [CT23] do not use the fundamental representation (Theorem 2.8): they work entirely in finite characteristic.

Notice that (19) is a finite characteristic variant of Lemma 3.1, but when $\beta > 1$ the conclusion of (19) is stronger than the conclusion of Lemma 3.1. At first this seems strange: if in Lemma 3.1 we weakened $\mathrm{fdeg}(f) < (p-1)(N-\beta+1)$ to $\mathrm{fdeg}(f) < N(p-1)$ then in general it is false that $\mathrm{ord}_p(\int_{[p)^N} f) \geq \beta$. However, to compare the two results we must take $f : (\mathbb{Z}/p\mathbb{Z})^N \to \mathbb{Z}/p^\beta\mathbb{Z}$ and pull it back to $F : \mathbb{Z}^N \to \mathbb{Z}/p^\beta\mathbb{Z}$, so the bound of (19) applies only to functions $F : \mathbb{Z}^N \to \mathbb{Z}/p^\beta\mathbb{Z}$ that are p-periodic, whereas Lemma 3.1 applies to all functions $F : \mathbb{Z}^N \to \mathbb{Z}/p^\beta\mathbb{Z}$. Thus in the application of Lemma 3.1 to results

on maps between finite commutative groups, we are losing critical information, namely periodicity properties of the functions coming from the fact that they were pulled back from finite characteristic. This explains why our present approach also includes Theorem 2.24, which uses the periodicity properties to deduce further p-adic divisibilities coming from the coefficients of the fundamental representation.

The two-pronged approach taken here and in [CS23] seems to be quantitatively superior to the approach via $\sigma(A, B)$ alone taken in [CT23], but it would be interesting to clarify the relationship between them.

References

[AM21] E. Aichinger and J. Moosbauer, *Chevalley-Warning type results on abelian groups*. J. Algebra 569 (2021), 30–66.

[AT92] N. Alon and M. Tarsi *Colorings and orientations of graphs*. Combinatorica 12 (1992), 125–134.

[Ax64] J. Ax, *Zeroes of polynomials over finite fields*. Amer. J. Math. 86 (1964), 255–261.

[CC] P.-J. Cahen and J.-L. Chabert, *Integer-valued polynomials*. Mathematical Surveys and Monographs, 48. American Mathematical Society, Providence, RI, 1997.

[Ch35] C. Chevalley, *Démonstration d'une hypothèse de M. Artin*. Abh. Math. Sem. Univ. Hamburg 11 (1935), 73–75.

[Cl-CA] P.L. Clark, *Commutative Algebra*. `http://alpha.math.uga.edu/~pete/integral.pdf`

[Cl14] P.L. Clark, *The Combinatorial Nullstellensätze revisited*. Electron. J. Combin. 21 (2014), no. 4, Paper 4.15, 17 pp.

[CS21] P.L. Clark and U. Schauz, *Functional Degrees and Arithmetic Applications I: The Set of Functional Degrees*. J. Algebra 608 (2022), 691–718.

[CS23] P.L. Clark and U. Schauz, *Functional Degrees and Arithmetic Applications III: The Main Theorem*. In preparation.

[CT23] P.L. Clark and N. Triantafillou, *The generalized group-theoretic Ax Lemma*. In preparation.

[CW18] P.L. Clark and L.D. Watson, *Varga's theorem in number fields*. Integers 18 (2018), Paper No. A74, 11 pp.

[Fr09] M. Fréchet, *Une définition fonctionnelle des polynomes*. Nouv. Ann. Math.: J. Cand. Éc. Polytech. Norm. 9 (1909), 145–162.

[GGZ] A. Geroldinger, D.J. Grynkiewicz and Q. Zhong, *Combinatorial Factorization Theory*. Preprint.

[Gr22] D.J. Grynkiewicz, *A Generalization of the Chevalley-Warning and Ax-Katz Theorems with a View Towards Combinatorial Number Theory*. `https://arxiv.org/abs/2208.12895`

[Ho05] X.-D. Hou, *A note on the proof of a theorem of Katz*. Finite Fields Appl. 11 (2005), 316–319.

[Ka71] N.M. Katz, *On a theorem of Ax*. Amer. J. Math. 93 (1971), 485–499.

[Ka09] D.J. Katz, *Point count divisibility for algebraic sets over $\mathbb{Z}/p^\ell\mathbb{Z}$ and other finite principal rings*. Proc. Amer. Math. Soc. 137 (2009), 4065–4075.

[Ka12] D.J. Katz, *On theorems of Delsarte-McEliece and Chevalley-Warning-Ax-Katz*. Des. Codes Cryptogr. 65 (2012), 291–324.

[KP12] R.N. Karasev and F.V. Petrov, *Partitions of nonzero elements of a finite field into pairs*. Israel J. Math. 192 (2012), 143–156.

[La04] M. Laczkovich, *Polynomial mappings on abelian groups*. Aequationes Math. 68 (2004), 177–199.

[Lei02] A. Leibman, *Polynomial mappings of groups*. Israel J. Math. 129 (2002), 29–60.

[MM95] O. Moreno and C.J. Moreno, *Improvements of the Chevalley-Warning and the Ax-Katz theorems*. Amer. J. Math. 117 (1995), 241–244.

[MR75] M. Marshall and G. Ramage, *Zeros of polynomials over finite principal ideal rings*. Proc. Amer. Math. Soc. 49 (1975), 35–38.

[Os19] A. Ostrowski, *Über ganzwertie Polynome in algebraischen Zahlkörpen*. J. reine angew. Math. 149 (1919), 117-124.

[Sc08] U. Schauz, *Algebraically solvable problems: describing polynomials as equivalent to explicit solutions*. Electron. J. Combin. 15 (2008), no. 1, Research Paper 10, 35 pp.

[Sc14] U. Schauz, *Classification of polynomial mappings between commutative groups.* J. Number Theory 139 (2014), 1–28.

[Va14] L. Varga, *Combinatorial Nullstellensatz modulo prime powers and the parity argument.* Combinatorial Nullstellensatz modulo prime powers and the parity argument. Electron. J. Combin. 21 (2014), no. 4, Paper 4.44, 17 pp.

[Wa35] E. Warning, *Bemerkung zur vorstehenden Arbeit von Herrn Chevalley.* Abh. Math. Sem. Hamburg 11 (1935), 76–83.

[Wa89] D.Q. Wan, *An elementary proof of a theorem of Katz.* Amer. J. Math. 111 (1989), 1–8.

[We77] C.S. Weisman, *Some congruences for binomial coefficients.* Michigan Math. J. 24 (1977), 141–151.

[Wi06] R.M. Wilson, *A lemma on polynomials modulo p^m and applications to coding theory.* Discrete Math. 306 (2006), 3154–3165.