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 thereof from that holds over any finite commutative ring of prime characteristic. We deduce this from a group-theoretic result that gives a lower bound on the p-adic divisibility of the number of simultaneous zeros of a system of maps from a fixed "source" finite commutative group of exponent p to varying "target" finite commutative p-groups. Our proof is morally a recasting of Wilson's proof of Ax-Katz over $\mathbb{F}_p$ in terms of 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 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 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.

We denote by $\mathbb{N}$ the 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 total ordering that extends the usual one on $\mathbb{N}$ and in which $-\infty$ is the least element and ∞ is the greatest element.

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 $\mathrm{ord}_q(0) = \infty$.

We say that a (not necessarily commutative) ring R is a **domain** if for all $x, y \in R$, if $xy = 0$ then $x = 0$ or $y = 0$.

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

Theorem 1.1. *Let $n, r, d_1, \ldots, d_r \in \mathbb{Z}^+$ with $d_1 \geq \ldots \geq d_r$ and*

$$d_1 + \ldots + d_r < n. \tag{1}$$

For $1 \leq j \leq r$, let $P_j(t_1, \ldots, t_n) \in \mathbb{F}_q[t_1, \ldots, t_n]$ be a polynomial of degree d_j. Let

$$Z = \{(x_1, \ldots, x_n) \in \mathbb{F}_q^n \mid P_1(x_1, \ldots, x_n) = \ldots = P_r(x_1, \ldots, x_n) = 0\}$$

be the common zero set in $\mathbb{F}_q^n$ of the P_i's. Then:

a) *(Chevalley-Warning* [Ch35], [Wa35]*) We have $\#Z \equiv 0 \pmod{p}$.*

b) *(Ax-Katz* [Ax64], [Ka71]*) We have $\mathrm{ord}_q(\#Z) \geq \left\lceil \frac{n-(d_1+\ldots+d_r)}{d_1} \right\rceil$.*

Theorem 1.1b) in the case of one polynomial (i.e., $r = 1$) 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? When 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 that divides $\#\{(x_1, \ldots, x_n) \in R^n \mid f_1(x_1, \ldots, x_n) = \ldots = f_r(x_1, \ldots, x_n) = 0\}$ for all polynomials $f_1, \ldots, f_r \in R$ 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,[1] and there had been no known analogue of Chevalley-Warning – let alone of Ax-Katz – over any finite nonprincipal ring until the following recent result.

Theorem 1.2. *(Aichinger-Moosbauer* [AM21, Thm. 12.6]*) Let R be a finite rng[2] of order a power of a prime number p. Let $n \in \mathbb{Z}^+$, and let $f_1, \ldots, f_r$ be polynomial expressions over R in n variables. If $\sum_{i=1}^r \deg(f_i) < n$, then*

$$p \mid \#\{(x_1, \ldots, x_n) \in R^n \mid f_1(x_1, \ldots, x_n) = \ldots = f_r(x_1, \ldots, x_n) = 0\}.$$

The first main result of the present paper shows that the Ax-Katz Theorem extends verbatim to all finite commutative rings 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 $(R, +) \cong (\mathbb{Z}/p\mathbb{Z})^N$ for some $N \in \mathbb{Z}^+$. Let $f_1, \ldots, f_r$ be polynomial expressions over R in $n \geq 1$ variables, of degrees $d_1 \geq \ldots \geq d_r \geq 1$. We put*

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

Then

$$\mathrm{ord}_p(\#Z(f_1, \ldots, f_r)) \geq \left\lceil \frac{N(n - (d_1 + \ldots + d_r))}{d_1} \right\rceil. \tag{2}$$

[1] For every $n \in \mathbb{Z}^+$ there is a finite commutative ring in which every ideal can be generated by n elements and some ideal requires n generators [Cl18, Cor. 4.3].

[2] A rng is like a ring but not necessarily having a multiplicative identity. It need not be commutative.

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

$$\mathrm{ord}_p(\mathbf{z}) \geq \left\lceil \frac{N(n-(d_1+\ldots+d_r))}{d_1} \right\rceil. \tag{3}$$

The conclusion of the Ax-Katz Theorem is

$$\mathrm{ord}_{p^N}(\mathbf{z}) \geq \left\lceil \frac{n-(d_1+\ldots+d_r)}{d_1} \right\rceil.$$

Since $\mathrm{ord}_{p^N}(\mathbf{z}) = \frac{\mathrm{ord}_p(\mathbf{z})}{N}$, the p-adic congruence given by Ax-Katz is

$$\mathrm{ord}_p(\mathbf{z}) \geq N\left\lceil \frac{n-(d_1+\ldots+d_r)}{d_1} \right\rceil. \tag{4}$$

The latter placement of the ceiling functions is more favorable, so that the bound (4) is better than the bound (3). 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 $f : A \to B$; so B^A is itself a commutative group under pointwise addition. For $a \in A$, we define an endomorphism Δ_a of B^A by

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

These endomorphisms all commute. Following Aichinger-Moosbauer, we assign to each $f \in B^A$ a **functional degree** $\mathrm{fdeg}(f) \in \widetilde{\mathbb{N}}$ as follows:
• We put $\mathrm{fdeg}(f) = -\infty$ if and only if $f = 0$.[3]
• For $n \in \mathbb{N}$, we say that $\mathrm{fdeg}(f) \leq n$ if we have $\Delta_{a_1} \cdots \Delta_{a_{n+1}} f = 0$ for all $a_1, \ldots, a_{n+1} \in A$. If this holds for some $n \in \mathbb{N}$, then $\mathrm{fdeg}(f)$ is the least n for which it holds.
• If $\mathrm{fdeg}(f) \leq n$ holds for no $n \in \mathbb{N}$, then we put $\mathrm{fdeg}(f) = \infty$.

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

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

[3]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.

and we also put

$$\mathcal{F}(A,B) \coloneqq \{f \in B^a \mid \mathrm{fdeg}(f) < \infty\}.$$

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

$$([a]f)(x) \coloneqq f(x+a).$$

In view of this, we may 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 is finite (i.e., if there is $N \in \mathbb{Z}^+$ such that $Nb = 0$ for all $b \in B$, we take $\exp(B)$ to be the least such N) and 0 otherwise, and then 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 expression over R in n variables, and let $E(f) \in R^{R^n}$ be the associated function. Then* $\mathrm{fdeg}(E(f)) \le \deg(f)$.

Proof. This is [AM21, Lemma 12.5]. □

In other words, 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 $N \in \mathbb{Z}^+$, let p be a prime number, and let*

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

be finite commutative p-groups. Let $f_1,\dots,f_r : A^N \to B$ be functions. If

$$\left(\sum_{j=1}^r \mathrm{fdeg}(f_j)\right)\left(\sum_{i=1}^n (p^{b_i}-1)\right) < \left(\sum_{i=1}^m p^{a_i}-1\right)N, \tag{5}$$

then

$$p \mid \#\{\mathbf{a} \in A^N \mid f_1(\mathbf{a}) = \ldots = f_r(\mathbf{a}) = 0\}.$$

Proof. This is [AM21, Thm. 12.2]. □

Applying Theorem 1.6 with $A = B = (R,+)$, the additive group of a finite ring 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 $N, r \in \mathbb{Z}^+$, let $A = (\mathbb{Z}/p\mathbb{Z})^N$, and let $\beta_1,\dots,\beta_r \in \mathbb{Z}^+$. For $1 \le j \le r$, let $f_j \in (\mathbb{Z}/p^{\beta_j}\mathbb{Z})^A$ be functions. Let $d_1,\dots,d_r \in \mathbb{N}$ be such that* $\mathrm{fdeg}(f_j) \le d_j$ *for all $1 \le j \le r$ and* $\max(d_1,\dots,d_r) \ge 1$. *Put*

$$M \coloneqq \max_{1\le j\le r} p^{\beta_j-1}d_j.$$

Put

$$Z(f_1,\dots,f_r) \coloneqq \{x \in (\mathbb{Z}/p\mathbb{Z})^N \mid f_j(x) = 0 \text{ for all } 1 \le j \le r\}.$$

Then

$$\mathrm{ord}_p(\#Z(f_1,\dots,f_r)) \ge \left\lceil \frac{N - \sum_{j=1}^r \frac{p^{\beta_j}-1}{p-1} d_j}{M} \right\rceil.$$

This result has the following consequence:

Theorem 1.8 (Group-Theoretic Prime Ax-Katz Theorem)**.** *Let $NN, r \in \mathbb{Z}^+$, let $A = (\mathbb{Z}/p\mathbb{Z})^N$, and let $f_1,\dots,f_r \in A^{A^n}$ be functions, not all constant, with functional degrees $d_1 \ge \dots \ge d_r$. If*

$$\mathbf{z} \coloneqq \#\{x \in A^n \mid f_1(x) = \dots = f_r(x) = 0\},$$

then we have

$$\mathrm{ord}_p(\mathbf{z}) \ge \left\lceil N\big(n - \textstyle\sum_{j=1}^r d_j\big)/d_1 \right\rceil.$$

Proof. Let $\tilde{A} = A^n \cong (\mathbb{Z}/p\mathbb{Z})^{nN}$. For $1 \le i \le N$, let $\pi_i : A \to \mathbb{Z}/p\mathbb{Z}$ be the kth coordinate projection. For $1 \le j \le r$ and $1 \le k \le N$, put $f_{j,k} \coloneqq \pi_k \circ f_j \in (\mathbb{Z}/p\mathbb{Z})^{A^n} = (\mathbb{Z}/p\mathbb{Z})^{\tilde{A}}$. By [CS21, Lemma 3.8b)], for all $1 \le i \le N$, we have

$$\mathrm{fdeg}(f_{j,k}) \le d_j.$$

Since the functions f_j are not all constant, we have $d_1 \ge 1$. 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 the maps $f_{j,k} \in (\mathbb{Z}/p^{\mathbb{Z}})^{\tilde{A}}$ we get

$$\mathrm{ord}_p(\mathbf{z}) \ge \frac{Nn - N\sum_{j=1}^r d_j}{d_1}.$$ □

Remark 1.9. *In an earlier version of our work, Theorem 1.8 was our main result. Then in March of 2022, D. Grynkiewicz sent us a draft manuscript* [GGZ]*. 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 $f_1,\dots,f_r \in \mathbb{Z}[t_1,\dots,t_N]$ rather than arbitary functions between commutative p-groups. In a later draft of the same manuscript, Grynkiewicz, Geroldinger and Zhong give a weighted version of their result.*

Switching from Theorem 1.8 to Theorem 1.7 made the proof easier*: cf. Remark 2.2.*

If R is a finite rng with underlying additive group $(R,+)$ finite of exponent p, then applying Theorem 1.7 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 4.2), we will get our p-weight improvement of Theorem 1.3 that recovers the Moreno-Moreno Theorem.

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.

• §5 contains a provocative (but tentative) final thought.

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 Representaton for $f \in B^{\mathbb{Z}^N}$

2.1. **Preliminaries.** Let $N \in \mathbb{Z}^+$. In this section we give a canonical series representation for each $f \in \mathcal{F}(\mathbb{Z}^N, B)$.

For $d \in \mathbb{Z}^+$, we put $\binom{t}{d} := \frac{t(t-1)\cdots(t-d+1)}{d!} \in \mathbb{Q}[t]$. For $x \in \mathbb{N}$, we have that $\binom{x}{d}$ is the usual binomial coefficient and is thus a non-negative integer. Moreover we have $\binom{x}{d} \in \mathbb{Z}$ for all $x \in \mathbb{Z}$: see e.g. [CC, p. 19]. These **integer-valued polynomials** are discussed in §2.3. We take $\binom{x}{0} : \mathbb{Z} \to \mathbb{Z}$ to be the constant function 1 and for any negative integer n, we take $\binom{x}{n} : \mathbb{Z} \to \mathbb{Z}$ to be the zero function.

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

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

(i) *We have $f(\mathbb{Z}^N) \subset \underline{B}$.*
(ii) *For all $1 \le i \le N$, we have $(\Delta_i f)(\mathbb{Z}^N) \subset \underline{B}$, and we have $f(\underline{0}) \in \underline{B}$.*

Proof. (i) $\implies$ (ii) is immediate.
(ii) $\implies$ (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 $\underline{x} \in \mathbb{Z}^N$. □

Because $e_1, \ldots, e_N$ is a set of generators for $\mathbb{Z}^N$, it follows from [CS21, Lemmas 3.6 and 3.7] that for $f \in \mathcal{F}(\mathbb{Z}^N, B) \setminus \{0\}$ the functional degree of f is the largest $n \in \mathbb{N}$ such that there are $i_1, \ldots, i_n \in \{1, \ldots, N\}$ such that

$$\Delta_{i_1} \cdots \Delta_{i_n} f \neq 0.$$

For $\underline{n} := (n_1, \ldots, n_N) \in \mathbb{N}^N$, we put

$$\Delta^{\underline{n}} := \Delta_1^{n_1} \cdots \Delta_n^{n_N} \in \mathbb{Z}/e(B)\mathbb{Z}[\mathbb{Z}^N].$$

Let $f \in \mathcal{F}(\mathbb{Z}^N, B) \setminus \{0\}$, and fix $1 \le i \le N$. Then there is a largest $d_i \in \mathbb{N}$ such that

$$\Delta_{i_1}^{d_i} f \neq 0$$

and we call this quantity the **i-th partial functional degree** $\mathrm{fdeg}_i(f)$ of f. We also put $\mathrm{fdeg}_i(0) := -\infty$, while if for all $n \in \mathbb{N}$ we have $\Delta_i^n f \neq 0$, we put $\mathrm{fdeg}_i(f) = \infty$. It follows from [CS21, Lemma 3.12] that for all $f \in B^{\mathbb{Z}^N}$ and all $1 \le i \le N$ we have

$$\mathrm{fdeg}_i(f) \le \mathrm{fdeg}(f) \le \sum_{i=1}^{N} \mathrm{fdeg}_i(f). \tag{6}$$

Remark 2.2. *Let $A_1, \dots, A_N, B$ be commutative groups In* [AM21, §5]*, Aichinger and Moosbauer associate partial functional degrees* $\mathrm{fdeg}_1(f), \dots, \mathrm{fdeg}_N(f)$ *to a map $f \in B^{\bigoplus_{i=1}^N A_i}$ in a way that generalizes the definition we have given and such that (6) continues to hold. The proof of their more general form of (6) becomes significantly more difficult.*

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

Lemma 2.3. *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*

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

The following result is related to [AT92, Lemma 2.1] and [Sc14, Thm. 2.5].

Theorem 2.4. *Let $N \in \mathbb{Z}^+$, let B be a commutative group, let $f \in B^{\mathbb{Z}^N}$. If there is $(a_1, \dots, a_N) \in \mathbb{Z}^N$ such that for all $(b_1, \dots, b_N) \in \mathbb{Z}^N$ with $0 \le b_i \le \mathrm{fdeg}_i(f)$ for all $1 \le i \le N$ we have $f(a_1 + b_1, \dots, a_N + b_N) = 0$, then $f = 0$.*

Proof. For $1 \le i \le N$ we put $d_i \coloneqq \mathrm{fdeg}_i(f)$. If some $d_i = 0$, then $f = 0$, so we may assume that $d_i \ge 0$ for all $1 \le i \le N$. We proceed by induction on N.
Base Case: Suppose that $N = 1$, so we have $f \in B^{\mathbb{Z}}$, $\mathrm{fdeg}(f) \le d_1$ and $f(a) = f(a+1) = \dots = f(a + d_1) = 0$. Applying Lemma 2.3 with $n = d_1 + 1$, we get that $f = 0$.
Induction Step: Suppose that $N \ge 2$ and that the result holds for all $f \in \mathcal{F}(\mathbb{Z}^{N-1}, B)$. For $0 \le j \le d_N$, put

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

Then we have $\mathrm{fdeg}_i g_j \le d_i$ for all $1 \le i \le N-1$ and g_j vanishes identically on $\prod_{i=1}^{N-1} [x_i, x_i + d_i]$, so induction gives $g_j = 0$ for all $0 \le j \le d_n$. It follows that for all $(a_1, \dots, a_{N-1}) \in \mathbb{Z}^{N-1}$ the function $f(a_1, \dots, a_{N-1}, \cdot) : \mathbb{Z} \to B$ vanishes on $[a_N, a_N + d_N]$, and it has functional degree at most d_n. By the Base Case these functions are identically zero, which means that f is identically zero. □

2.2. **The Fundamental Representation.**

Theorem 2.5. *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*

$$\forall x \in \mathbb{N}^N,\ f(x) = \sum_{\underline{n} \in \mathbb{N}^N} \binom{x_1}{n_1} \cdots \binom{x_N}{n_N} a_{\underline{n}}. \tag{7}$$

Namely, for all $\underline{n} \in \mathbb{N}^N$ we have $a_{\underline{n}} = (\Delta^{\underline{n}} f)(\underline{0})$.

b) *Let $d \in \mathbb{N}$. The following are equivalent:*
   (i) *We have* $\mathrm{fdeg}(f) \le d$.
   (ii) *We have*

$$\forall x \in \mathbb{Z}^N,\ f(x) = \sum_{\substack{\underline{n} \in \mathbb{N}^N \\ |\underline{n}| \le d}} \binom{x_1}{n_1} \cdots \binom{x_N}{n_N} (\Delta^{\underline{n}} f)(\underline{0}). \tag{8}$$

Proof. a) First of all, for each $x = (x_1, \ldots, x_N) \in \mathbb{N}^N$ 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 the sum in (7) is actually finite. As seen above, 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 $\underline{m}, \underline{n} \in \mathbb{N}$ we have

$$\Delta^{\underline{m}} \left(\binom{x_1}{n_1} \cdots \binom{x_N}{n_N} \right) (\underline{0}) = \prod_{i=1}^{N} \binom{0}{n_i - m_i} = \begin{cases} 1 & \text{if } \underline{m} = \underline{n} \\ 0 & \text{otherwise} \end{cases}. \tag{9}$$

It follows that if we apply $\Delta^{\underline{n}}$ to $\sum a_{\underline{n}} \binom{x_1}{n_1} \cdots \binom{x_N}{n_N}$ and evaluate at $\underline{0}$ we get part a) except for the existence of the function $a_\bullet$. To see this, consider

$$g \coloneqq f - \sum_{\underline{n} \in \mathbb{N}^N} \binom{x_1}{n_1} \cdots \binom{x_N}{n_N} (\Delta^{\underline{n}} f)(\underline{0}) \in B^{\mathbb{Z}^N}.$$

Then we have $\Delta^{\underline{n}}(g)(\underline{0}) = 0$ for all $\underline{n} \in \mathbb{N}^N$, so it suffices to show that the only function with this property is the zero function. We show that $g(x_1, \ldots, x_N) = 0$ for all $\underline{x} = (x_1, \ldots, x_N) \in \mathbb{N}^N$ by induction on

$$|\underline{x}| \coloneqq x_1 + \ldots + x_N.$$

The base case is $g(\underline{0}) = (\Delta^{\underline{0}} g)(\underline{0}) = 0$. Now fix $d \in \mathbb{Z}^+$, suppose that for all $h \in B^{\mathbb{Z}^N}$ with $(\Delta^{\underline{n}} h)(\underline{0}) = 0$ for all $\underline{n} \in \mathbb{N}^N$ we have $h(\underline{x}) = 0$ for all $\underline{x} = (x_1, \ldots, x_N) \in \mathbb{N}^N$ with $|\underline{x}| \coloneqq x_1 + \ldots + x_N < d$, and let $\underline{x} \in \mathbb{N}^N$ with $|\underline{x}| = d$. Choose $1 \leq i \leq N$ such that $x_i \geq 1$. By our induction hypothesis we have

$$(\Delta_i^{x_i} g)(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_N) = 0,$$

and using Lemma 2.3 together with the inductive hypothesis that

$$\forall\ 0 \leq y_i < x,\ g(x_1, \ldots, x_{i-1}, y_i, x_{i+1}, \ldots, x_N) = 0,$$

we get that $g(x_1, \ldots, x_N) = 0$, completing the induction step and the proof of part a).
b) (i) $\implies$ (ii) Since $\operatorname{fdeg} f \leq d$, we have $(\Delta^{\underline{n}} f)(\underline{0}) = 0$ for all $\underline{n} \in \mathbb{N}^N$ with $|\underline{n}| > d$, so

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

If we put $P \coloneqq \sum_{\underline{n} \in \mathbb{N}^n, |\underline{n}| \leq d} \binom{x_1}{n_1} \cdots \binom{x_N}{n_N} (\Delta^{\underline{n}} f)(\underline{0})$, then $f - P$ has functional degree at most d and vanishes on $\mathbb{N}^N$, so by Theorem 2.4 we have $f = P$.
(ii) $\implies$ (i): It follows from (9) that the functional degree of

$$\sum_{\substack{\underline{n} \in \mathbb{N}^N \\ |\underline{n}| \leq d}} \binom{x_1}{n_1} \cdots \binom{x_N}{n_N} a_{\underline{n}}$$

is the largest $|\underline{n}|$ such that $a_{\underline{n}} \neq 0$, which is by assumption at most d. □

Remark 2.6. a) *For B a finitely generated commutative group, the series representation (8) was explored in* [Sc14, §2].

b) *The series expansion of Theorem 2.5 is a discrete analogue of the Taylor series expansion of a smooth function $f : \mathbb{R}^N \to \mathbb{R}$. Theorem 2.5a) 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.

b) *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 $\underline{a} \in \mathbb{Z}^N$.*

2.3. **Polynomial Functions and Integer-Valued Polynomials.** In this section we use Theorem 2.5 to make some further extensions of the Aichinger-Moosbauer functional calculus, in particular comparing 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 useful to understand that these techniques can be viewed in terms of the Aichinger-Moosbauer calculus.

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

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

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 2.7. *Let R be a nonzero commutative ring, and let $N \in \mathbb{Z}^+$. The following are equivalent:*

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

(ii) *The function*

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

lies in the image of E.

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

Proof. Case 1: Suppose R is a finite field $\mathbb{F}_q$. 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 and explicitly determined its kernel: it is $\langle t_1^q - t_1, \ldots, t_n^q - t_b \rangle$. For English language proofs of modest generalizations, see [Cl14, Cor. 2.5 and Prop. 4.4].

Case 2: Suppose that R is not a field; equivalently, there is an ideal $(0) \subsetneq I \subsetneq R$. Then for all $F \in \mathbf{P}(R^N, R)$, the function F is **congruence-preserving**: for $x = (x_1, \ldots, x_N)$, $y = (y_1, \ldots, y_N) \in R^N$ are such that $x_i \equiv y_i \pmod I$ for all $1 \leq i \leq N$, then $f(x) \equiv f(y) \pmod I$. Let $a \in I \setminus \{0\}$. Then

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

so $\delta_{0,1}$ is not congruence-preserving.
Case 3: Suppose that R is infinite. Then [CS21, Thm. 4.9a)] gives $\mathrm{fdeg}(\delta_{0,1}) = \infty$, so $\delta_{0,1}$ is not a polynomial function by Lemma 1.5. □

If R is an infinite commutative ring that is not a field, we just gave two proofs (in Cases 2 and 3) 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 a nonzero commutative ring R, by Lemma 1.5 we have

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

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

Question 2.8. *For which nonzero commutative rings R and $N \in \mathbb{Z}^+$ do we have $\mathbf{P}(R^N, R) = \mathcal{F}(R^N, R)$ – i.e., when is every $f \in R^{R^N}$ of finite functional degree a polynomial function?*

Here is an answer to Question 2.8 when R is finite.

Proposition 2.9. *For a nonzero finite commutative ring R, the following are equivalent:*

(i) *For all $N \in \mathbb{Z}^+$, we have $\mathbf{P}(R^N, R) = \mathcal{F}(R^N, R)$.*
(ii) *For some $N \in \mathbb{Z}^+$, we have $\mathbf{P}(R^N, R) = \mathcal{F}(R^N, R)$.*
(iii) *For some $r \in \mathbb{Z}^+$, prime numbers $p_1 < \ldots < p_r$ and positive integers $a_1, \ldots, a_r$, we have*

$$R \cong \prod_{i=1}^r \mathbb{F}_{p_i^{a_i}}.$$

Proof. If R is a finite commutative ring of order $p_1^{a_1} \cdots p_r^{a_r}$ (for primes $p_1 < \ldots < p_r$), 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 $p_i^{a_i}$ [Cl-CA, Thm. 8.37]. We call $\mathfrak{r}_i$ the **p_i-primary component** of R. We have a natural ring isomorphism

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

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. In this case, by [AM21, Thm. 9.1] we have

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

and so our problem reduces to the previous problem of when the evaluation map is surjecitve. By Proposition 2.7, this holds if and only if R is a finite field. So: independently

of $N \in \mathbb{Z}^+$, every function $f \in R^{R^N}$ of finite functional degree is a polynomial function if and only if for all $p \mid \#R$, the p-primary component of R is a finite field. □

When R is infinite we do not know a complete answer to Question 2.8, but we will exhibit some positive and negative results. Here is one:

Proposition 2.10. *For all $N \in \mathbb{Z}^+$, we have $\mathbf{P}(\mathbb{Q}^N, \mathbb{Q}) = \mathcal{F}(\mathbb{Q}^N, \mathbb{Q})$.*

Proof. Let $g \in \mathcal{F}(\mathbb{Q}^N, \mathbb{Q})$. By Theorem 2.5 there is a function $a_\bullet : \mathbb{N}^N \to \mathbb{Q}$ and $d \in \mathbb{N}$ such that

$$\forall x = (x_1, \ldots, x_N) \in \mathbb{Z}^N,\ g(x) = \sum_{\underline{n} \in \mathbb{N}^N,\ |\underline{n}| \leq d} a_{\underline{n}} \binom{x_1}{n_1} \cdots \binom{x_n}{n_N}.$$

Let $f \in \mathbb{Q}[t_1, \ldots, t_N]$ be the polynomial

$$f(t_1, \ldots, t_n) = \sum_{\underline{n} \in \mathbb{N}^N,\ |\underline{n}| \leq d} a_{\underline{n}} \binom{t_1}{n_1} \cdots \binom{t_n}{n_N}.$$

Then $E(f), g \in \mathcal{F}(\mathbb{Q}^N, \mathbb{Q})$ and

$$\forall x \in \mathbb{Z}^N,\ E(f)(x) = g(x).$$

By [AM21, Lemma 3.2] Theorem 2.4 applies to $(E(f) - g)|_{\mathbb{Z}^N}$, giving $(E(f) - g)|_{\mathbb{Z}^N} = 0$. This implies $E(f) = g$: in fact, we claim that if $h \in \mathcal{F}(\mathbb{Q}^N, \mathbb{Q})$, if $h|_{\mathbb{Z}^N} = 0$, then $h = 0$.

To see this, let $D \in \mathbb{Z}^+$, and define $h_D \in \mathbb{Q}^{\mathbb{Z}^N}$ by

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

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]. By hypothesis, h_D is identically zero on $D\mathbb{Z}^N$, so by Theorem 2.4 we have $(h_D)|_{\mathbb{Z}^N} = 0$. This holds for all $D \in \mathbb{Z}^+$, so $h = 0$. □

From now until the end of the section we will assume that R is an infinite commutative domain, with fraction field K. In this case the evaluation map $E : R[t_1, \ldots, t_N] \to R^{R^N}$ 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 the infinite domain R and, in fact, a little more. Namely, we define the subring of **integer-valued polynomials**

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

Proposition 2.11. *Let R be an infinite commutative domain, with fraction field K, and let $f \in \mathrm{Int}(R^N, R)$. Let $\widetilde{E(f)} \coloneqq E(f)|_{R^N} \in R^{R^N}$. Then*

$$\mathrm{fdeg}(\widetilde{E(f)}) = \deg(f).$$

Proof. Let $f \in \mathrm{Int}(R^N, R)$. We write $E(f)$ for associated function from K^N to K and $\widetilde{E(f)}$ for the associated function from R^N to K. Thus $\widetilde{E(f)}$ is obtained from $E(f)$ by restricting the domain from K^N to R^N and then resttricting the codomain from K to R. By [CS21, Cor. 3.10] domain restriction causes the functional degree to stay the same or decrease, while codomain restriction preserves the functional degree, so

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

Put $d \coloneqq \deg(f)$; we may certainly assume that $d \geq 0$. Seeking a contradiction, suppose that $\operatorname{fdeg}(\widetilde{E(f)}) < d$. Then for all $x_1, \ldots, x_d \in R^N$ we have $\Delta_{x_1} \cdots \Delta_{x_d} \widetilde{E(f)} = 0$. Thus the polynomial function$\Delta_{x_1} \cdots \Delta_{x_d} E(f)$ vanishes identically on R^N, and Theorem 2.5 implies that it must be 0. But over any field K of characteristic 0, for $d \in \mathbb{N}$, evidently

$$\mathcal{B}^d \coloneqq \left\{ \binom{t_1}{n_1} \cdots \binom{t_N}{n_N} \mid n = (n_1, \ldots, n_N) \in \mathbb{N}^N \mid |\underline{n}| \leq d \right\}$$

is a K-basis for the space of polynomials of degree at most d (equivalently, for the space of polynomial functions of functional degree at most d). Since $\deg(f) = d$, the polynomial f has at least one "binomial monomial term" $\binom{t_1}{n_1} \cdots \binom{t_n}{n_N}$ with $n_1 + \ldots + n_N = d$ and then $\Delta^{(n_1,\ldots,n_N)} E(f) \neq 0$, a contradiction. □

So for commutative domains of characteristic 0, we get a further refinement

$$\mathbf{P}(R^N, R) \subseteq \operatorname{Int}(R^N, R) \subseteq \mathcal{F}(R^N, R) \subseteq R^{R^N},$$

which yields in particular a negative answer to Question 2.8 whenever we have $\operatorname{Int}(R^N, R) \supsetneq \mathbf{P}(R^N, R)$. This certainly holds for $R = \mathbb{Z}$: e.g. $\frac{t(t-1)}{2}$ is an integer-valued polynomial that does not lie in $\mathbb{Z}[t]$. This motivates the following result:

Theorem 2.12.

a) *The set* $\mathcal{B} \coloneqq \{\binom{x_1}{n_1} \cdots \binom{x_n}{n_N} \mid \underline{n} \in \mathbb{N}^N\}$ *is a basis for the* $\mathbb{Z}$*-module* $\mathcal{F}(\mathbb{Z}^N, \mathbb{Z})$.

b) *We have* $\mathcal{F}(\mathbb{Z}^N, \mathbb{Z}) = \operatorname{Int}(\mathbb{Z}^N, \mathbb{Z})$.

Proof. a) Theorem 2.5c) implies that $\mathcal{B}$ spans $\mathcal{F}(\mathbb{Z}^N, \mathbb{Z})$ as a $\mathbb{Z}$-module. For $\underline{m} \in \mathbb{N}$, the $\mathbb{Z}$-linear map $L_{\underline{m}} : \mathbb{Z}^{\mathbb{Z}^N} \to \mathbb{Z}$ given by $f \mapsto (\Delta^{\underline{m}} f)(\underline{0})$ kills $\binom{x_1}{n_1} \cdots \binom{x_N}{n_N}$ iff $\underline{m} \neq \underline{n}$, so $\binom{x_1}{m_1} \cdots \binom{x_n}{m_N}$ cannot be a $\mathbb{Z}$-linear combination of any of the other elements of $\mathcal{B}$.
b) By Proposition 2.11 we have $\operatorname{Int}(\mathbb{Z}^N, \mathbb{Z}) \subseteq \mathcal{F}(\mathbb{Z}^N, \mathbb{Z})$. The well-known fact that for all $n \in \mathbb{N}$ we have $\binom{x}{n} \in \operatorname{Int}(\mathbb{Z}, \mathbb{Z})$ follows from Lemma 2.1 and induction. Since $\operatorname{Int}(\mathbb{Z}^N, \mathbb{Z})$ is a ring, we have $b \in \operatorname{Int}(\mathbb{Z}^N, \mathbb{Z})$ for all $b \in \mathcal{B}$. So

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

Theorem 2.12 implies that $\mathcal{B}$ is a $\mathbb{Z}$-basis for the ring $\operatorname{Int}(\mathbb{Z}^N, \mathbb{Z})$ of integer-valued polynomials, a result of Ostrowski [Os19]. See [CC, Ch. 11] for a general treatment of $\operatorname{Int}(R^N, R)$ for a commutative domain R. Cahen-Chabert also address when $\operatorname{Int}(R^N, R) = \mathbf{P}(R^N, R)$ 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 all $N \in \mathbb{Z}^+$ we have $\operatorname{Int}(R^N) \subsetneq \mathcal{F}(R^N, R)$ when $R \supsetneq \mathbb{Q}$ is a $\mathbb{Q}$-algebra.

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

$$\mathfrak{C} : R \to \operatorname{End}(R, +), \ r \mapsto r\bullet : x \mapsto rx$$

is an isomorphism (equivalently, is surjective).

Example 2.13. a) *Each of the following rings is a Cayley ring:* $\mathbb{F}_p$, $\mathbb{Z}$, $\mathbb{Q}$. *Moreover any subring of* $\mathbb{Q}$ *is a Cayley ring: such rings are precisely the localizations of* $\mathbb{Z}$ *and they are in bijection with subsets of the set* $\mathcal{P}$ *of prime numbers.*

b) *A commutative ring R is* not *a Cayley ring if it is free of rank greater than* 1 *as a module over some proper subring. From this we see that none of the following rings are Cayley rings: a field other than $\mathbb{Q}$ or $\mathbb{F}_p$; an algebra over a field F such that $F \subsetneq R$; the ring of integers $\mathbb{Z}_K$ of any number field $K \supsetneq \mathbb{Q}$; the valuation ring of a p-adic field $K \supsetneq \mathbb{Q}_p$.*

Proposition 2.14. *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 contrapositive, 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 2.11 L is therefore not given by any integer-valued polynomial. This establishes the result for $N = 1$. For any $N \in \mathbb{Z}^+$, the function $L_N : R^N \to R$ by $L_N(x_1, \ldots, x_N) = L(x_1)$ is again $\mathbb{Z}$-linear but is not the restriction to R^N of any K-linear polynomial function, so $L_N \in \mathcal{F}(R^N, R) \setminus \mathrm{Int}(R^N, R)$. □

Proposition 2.14 and Example 2.13 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.**

Corollary 2.15 (Homomorphic Functoriality II)**.** *Let B, B' be commutative groups, let $\beta : B \to B'$ be a homomorphism, and let $f \in B^{\mathbb{Z}^N}$.*

a) *For all $\underline{x} \in \mathbb{N}^N$ we have*

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

b) *If f has functional degree $d < \infty$, then for all $\underline{x} \in \mathbb{Z}^N$ we have*

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

Proof. On one hand, by Theorem 2.5a) we have

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

And, if f has functional degree $d < \infty$, then by [CS21, Lemma 3.9b)], the function $\beta_* f \in (B')^{\mathbb{Z}^N}$ has functional degree at most d, as well, so by Theorem 2.5b) we have

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

On the other hand, the map $\beta_* : B^{\mathbb{Z}^N} \to (B')^{\mathbb{Z}^N}$ is a homomorphism of $\mathbb{Z}[\mathbb{Z}^N]$-modules, so for all $\underline{n} \in \mathbb{N}^N$ we have $\Delta^{\underline{n}}(\beta_* f) = \beta \circ \Delta^{\underline{n}} f$. The result follows. □

Let A, B, B' be commutative groups and let $\beta : B \to B'$ be a surjective homomorphism. As mentioned in [CS21, §2.5], the map $B^A \ni f \mapsto \beta \circ f \in (B')^A$ gives a surjective group homomorphism

$$\beta_* : B^A \to (B')^A.$$

Suppose now that $A = \mathbb{Z}^N$ and $f \in \mathcal{F}(\mathbb{Z}^N, B')$, so f is of the form (8) for a finitely nonzero function $a_\bullet : \mathbb{N}^N \to B'$. By a **lift** of $a_\bullet$ we will mean a function $A_\bullet : \mathbb{N}^N \to B$ such that $\beta \circ A_\bullet = a_\bullet$ and such that for all $\underline{n} \in \mathbb{N}^N$ we have $A_{\underline{n}} = 0 \iff a_{\underline{n}} = 0$. Such lifts always exist. To such a lift we attach the following function $F \in B^A$:

$$\forall \underline{x} \in \mathbb{Z}^N,\ F(\underline{x}) = \sum_{\underline{n} \in \mathbb{N}^N} \binom{x_1}{n_1} \cdots \binom{x_N}{n_N} A_{\underline{n}}.$$

By Corollary 2.15 we have that $\beta_* F = f$, and by our choice of $A_\bullet$ we have

$$\mathrm{fdeg}(F) = \mathrm{fdeg}(f).$$

We will also call the associated function $F \in B^A$ a **lift** of $f \in (B')^A$. Notice that in general a given $f \in \mathcal{F}(\mathbb{Z}^N, B')$ has many different lifts.

Combining this discussion with Theorems 2.5 and 2.12 we find that for $N, m \in \mathbb{Z}^+$, every $f \in \mathcal{F}(\mathbb{Z}^N, \mathbb{Z}/m\mathbb{Z})$ is the reduction of an integer-valued polynomial of degree equal to $\mathrm{fdeg}(f)$. In particular, this applies when for some $p \in \mathcal{P}$ we have $m = p^b$ and f is $(p^{a_1}, \ldots, p^{a_N})$-periodic for some $a_1, \ldots, a_N \in \mathbb{Z}^+$, i.e., lies in the image of the natural map $B^{\bigoplus_{i=1}^N \mathbb{Z}/p^{a_i}\mathbb{Z}} \to B^{\mathbb{Z}^N}$. This situation is considered in the next subsection.

Remark 2.16. *The fact that functions $\mathbb{Z}/p^a\mathbb{Z} \to \mathbb{Z}/p^b\mathbb{Z}$ can 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 $\mathbb{Z}_K/\mathfrak{p}^a \to \mathbb{Z}_K/\mathfrak{p}^b$ 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 $\mathbb{Z}_K/\mathfrak{p}^a$ and $\mathbb{Z}_K/\mathfrak{p}^b$ are finite rings of p-power order for some $p \in \mathcal{P}$). Perhaps these works could be refined using conisderations from the present paper and from* [CS21].

2.5. **Representation of Functions Between Finite Commutative p-Groups.** If A is a finitely generated commutative group, then of course for some $N \in \mathbb{Z}^+$ we have a surjective group homomorphism $\alpha : \mathbb{Z}^N \to A$. Up to a harmless isomorphism, we may write A as $\bigoplus_{i=1}^N \mathbb{Z}/a_i\mathbb{Z}$ with $a_i \in \{0\} \cup \mathbb{Z}^{\geq 2}$ and take

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

We then have an embedding

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

and thus every $f \in \mathcal{F}(A, B)$ has the same functional degree as its pullback to $\mathbb{Z}^N$ which by Theorem 2.5b) has a canonical series representation (8).

The following notation will be helpful: for $p \in \mathcal{P}$, $N \in \mathbb{Z}^+$ and $\underline{a} = (a_1, \ldots, a_N) \in \mathbb{Z}^N$ with $a_1 \geq \ldots \geq a_N$ and $b \in \mathbb{Z}^+$, we put

$$\delta_p(\underline{a}, b) \coloneqq \delta(\bigoplus_{i=1}^N \mathbb{Z}/p^{a_i}\mathbb{Z}, \mathbb{Z}/p^b\mathbb{Z}) = \sum_{i=1}^N (p^{a_i} - 1) + (b-1)(p-1)p^{a_1 - 1}.$$

Theorem 2.17. *Let $p \in \mathcal{P}$, let $N, a_1, \ldots, a_N \in \mathbb{Z}^+$, put $A := \bigoplus_{i=1}^N \mathbb{Z}/p^{a_i}\mathbb{Z}$, and let $\alpha : \mathbb{Z}^N \to A$ be the above quotient map. Let B be a commutative group, let $f \in B^A$, and let $\tilde{f} := \alpha^* f$ be its pullback to a function from $\mathbb{Z}^N$ to B.*

a) *Let $b \in \mathbb{Z}^+$. If B has exponent p^b, or if just $p^b y = 0$ for all $y \in f(A)$, then for all $\underline{x} \in \mathbb{Z}^N$ we have*

$$\tilde{f}(\underline{x}) = \sum_{\substack{\underline{n} \in \mathbb{N}^N \\ |\underline{n}| \leq \delta_p(\underline{a}, b)}} \binom{x_1}{n_1} \cdots \binom{x_N}{a_N} (\Delta^{\underline{n}} \tilde{f})(\underline{0}).$$

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

$$(\Delta^{\underline{n}}(f))(\underline{0}) = (\Delta^{\underline{n}}(\tilde{f}))(\underline{0}) \in p^b B.$$

Proof. Let $\underline{B} := \langle f(A) \rangle$ be the subgroup generated by the image of f. Since A is finite and B is commutative, the subgroup $\underline{B}$ is finite. In the situation of part a) we have that $\underline{B}$ is a p^b-torsion group. By [CS21, Cor. 3.10b)] we may assume that $\underline{B} = B$, so that part a) follows from Theorem 2.5 and [CS21, Thm. 4.9c)].

To prove part b), let $\beta_b : B \to B/p^b B$ be the natural quotient map. We consider the expansion of the map $\beta_b \circ \tilde{f} : \mathbb{Z}^N \to B/p^b B$. By Theorem 2.5 a), combined with Corollary 2.15 a), for all $\underline{x} \in \mathbb{N}^N$,

$$(\beta_b \circ \tilde{f})(\underline{x}) = \sum_{\underline{n} \in \mathbb{N}^N} \binom{x_1}{n_1} \cdots \binom{x_N}{a_N} ((\Delta^{\underline{n}} \tilde{f})(\underline{0}) + p^b B).$$

But, since the exponent of $B/p^b B$ divides p^b, we can also apply part a), combine it with Corollary 2.15 b), and obtain, for all $\underline{x} \in \mathbb{Z}^N$,

$$(\beta_b \circ \tilde{f})(\underline{x}) = \sum_{\substack{\underline{n} \in \mathbb{N}^N \\ |\underline{n}| \leq \delta_p(\underline{a}, b)}} \binom{x_1}{n_1} \cdots \binom{x_N}{a_N} ((\Delta^{\underline{n}} \tilde{f})(\underline{0}) + p^b B).$$

Comparing coefficients, and using the uniqueness in Theorem 2.5a), we get

$$(\Delta^{\underline{n}} \tilde{f})(\underline{0}) + p^b B = 0 \in B/p^b B$$

for all $\underline{n} \in \mathbb{N}^n$ with $|\underline{n}| > \delta_p(\underline{a}, b)$. The stated result follows. □

3. The Group-Theoretic Ax-Katz Theorem

3.1. **Wilson's Lemma.** For $p \in \mathcal{P}$, we abbreviate $\{0, \ldots, p-1\}$ to $[p)$. Let $\mathbb{Z}_{(p)}$ be the rational numbers of non-negative p-adic valuation.

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

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

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

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

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

then

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

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 $i_1, \ldots, i_b \in [0, p-2]$ then

$$\sum_{\underline{x} \in [p)^b} x_1^{i_1} \cdots x_b^{i_b} = \prod_{j=1}^{b} \sum_{x_j \in [p)} x_j^{i_j} \equiv 0 \pmod{p^b}.$$

From this we deduce that if $g \in \mathbb{Z}_{(p)}[t_1, \ldots, t_b]$ has $\mathrm{fdeg}_i(g) \leq p-2$ for all $1 \leq i \leq b$ then

$$\int_{[p)^b} g = \sum_{\underline{x} \in [p)^b} g(\underline{x}) \equiv 0 \pmod{p^b}.$$

Step 2: If the result holds for a set of polynomials $f_1, \ldots, f_m$ then it holds for the $\mathbb{Z}$-submodule of $\mathbb{Z}^{\mathbb{Z}^N}$ that they generate. Because of this and Theorem 2.5 it suffices to show that the result holds for

$$f(\underline{x}) = \prod_{i=1}^{N} \binom{x_1}{n_1} \cdots \binom{x_n}{n_N}$$

for all $(n_1, \ldots, n_N) \in \mathbb{N}^N$ with $|\underline{n}| < (N-b+1)(p-1)$. Since for all $1 \leq i \leq N$ we have $\mathrm{fdeg}_i(f) = n_i$, it follows that

$$\#\{1 \leq i \leq N \mid \mathrm{fdeg}_i(f) < p-1\} \geq b,$$

for if not we would have $\deg(f) \geq (N-b+1)(p-1)$. So we may suppose without loss of generality that $\mathrm{fdeg}_i(f) < p-1$ for all $1 \leq i \leq b$. Then for all $y_{b+1}, \ldots, y_N \in \mathbb{Z}$, we have

$$f(t_1, \ldots, t_b, y_{b+1}, \ldots, y_N) \in \mathbb{Z}_{(p)}[t_1, \ldots, t_b],$$

so using Step 1 we get

$$\int_{[p)^N} f = \sum_{(x_1, \ldots, x_b) \in [p)^b} f(x_1, \ldots, x_b, y_{b+1} \ldots, y_N) \equiv 0 \pmod{p^b}. \qquad \square$$

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

$$M \coloneqq \max_{1 \leq j \leq r} p^{\beta_j - 1} d_j$$

and

$$B \coloneqq \left\lceil \frac{N - \sum_{j=1}^r \frac{p^{\beta_j}-1}{p-1} d_j}{\max_{1 \leq j \leq r} p^{\beta_j - 1} d_j} \right\rceil = \left\lceil \frac{N - \sum_{j=1}^r \frac{p^{\beta_j}-1}{p-1} d_j}{M} \right\rceil.$$

We have

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

so

$$\sum_{j=1}^{r} \frac{p^{\beta_j}-1}{p-1} d_j < N + M(1-B) \tag{10}$$

For $1 \leq j \leq r$, let

$$\chi_j : \mathbb{Z} \to \mathbb{Z}/p^B\mathbb{Z} \text{ by } \chi(x) = \begin{cases} 1 & \text{if } x \equiv 0 \pmod{p^{\beta_j}} \\ 0 & \text{otherwise} \end{cases}.$$

Let

$$\chi \coloneqq \bigotimes_{j=1}^{r} \chi_j : \mathbb{Z}^r \to \mathbb{Z}/p^B\mathbb{Z},\ (x_1, \ldots, x_r) \mapsto \prod_{j=1}^{r} \chi_j(x_j).$$

Let $\widetilde{\chi}$ be a lift of χ from $\mathbb{Z}/p^B\mathbb{Z}$ to $\mathbb{Z}$ in the sense of §2.4, and similarly for $1 \leq j \leq r$ let $\widetilde{\chi}_j$ be a lift of χ_j from $\mathbb{Z}/p^B\mathbb{Z}$ to $\mathbb{Z}$.

Let $x \in \mathbb{Z}^N$, and write $\overline{x}$ for the image of x in $(\mathbb{Z}/p\mathbb{Z})^N$, so for all $x \in \mathbb{Z}^N$, we have

$$\chi(f_1(\overline{x}), \ldots, f_r(\overline{x})) = \begin{cases} 1 & \text{if } \overline{x} \in Z(f_1, \ldots, f_r) \\ 0 & \text{otherwise} \end{cases}.$$

For $1 \leq j \leq r$, let F_j be obtained from f_j by pulling back from $(\mathbb{Z}/p\mathbb{Z})^N$ to $\mathbb{Z}^N$, and let $\tilde{F}_j$ be obtained from F_j by lifting from $\mathbb{Z}/p^{\beta_j}\mathbb{Z}$ to $\mathbb{Z}$ in the sense of §2.4. In particular, by §2.4 we have $\mathrm{fdeg}(\tilde{F}_j) = \mathrm{fdeg}(F_j) = \mathrm{fdeg}(f_j) \leq d_j$ for all $1 \leq j \leq r$. Thus the desired conclusion that $p^B \mid \#Z(f_1, \ldots, f_r)$ is equivalent to

$$\int_{[p)^N} \chi(\tilde{F}_1, \ldots, \tilde{F}_r) = 0 \in \mathbb{Z}/p^B\mathbb{Z}.$$

and thus also to

$$\mathrm{ord}_p \left(\int_{[p)^N} \widetilde{\chi}(\tilde{F}_1, \ldots, \tilde{F}_r \right) \geq B. \tag{11}$$

The function χ_j is the pullback from $\mathbb{Z}/p^{\beta_j}\mathbb{Z}$ to $\mathbb{Z}$ of the function $\delta_{0,1} \in (\mathbb{Z}/p^B\mathbb{Z})^{\mathbb{Z}/p^{\beta_j}\mathbb{Z}}$, so by [CS21, Prop. 4.4 and Thm. 4.7] and §2.4, we have

$$\mathrm{fdeg}(\widetilde{\chi}_j) = \mathrm{fdeg}(\chi_j) = \delta(\mathbb{Z}/p^{\beta_j}\mathbb{Z}, \mathbb{Z}/p^B\mathbb{Z}) = (p^{\beta_j}-1) + (B-1)p^{\beta_j-1}(p-1).$$

By Theorem 2.17, there is a function $c_j : \mathbb{N} \to \mathbb{Z}$ such that $\tilde{c}_j(n_j) = 0$ for all but finitely many n_j's, such that

$$\forall x_j \in \mathbb{Z},\ \chi_j(x_j) = \sum_{n_j \in \mathbb{N}} \binom{x_j}{n_j} c_j(n_j)$$

and such that for all $b \in \mathbb{Z}^+$ we have

$$n_j > (p-1)\left(\frac{p^{\beta_j}-1}{p-1} + (b-1)p^{\beta_j-1} \right) \implies p^b \mid c_j(n_j).$$

Our lift of χ_j to $\widetilde{\chi}_j$ consists of lifting c_j to $\tilde{c}_j : \mathbb{N} \to \mathbb{Z}$ in such a way that $c_j(n_j) = 0 \implies \tilde{c}_j(n_j) = 0$. It follows that

$$\forall 1 \leq b \leq B,\ n_j > (p-1)\left(\frac{p^{\beta_j}-1}{p-1} + (b-1)p^{\beta_j-1} \right) \implies p^b \mid \tilde{c}_j(n_j). \tag{12}$$

Now we have

$$\int_{[p)^N} \chi(\tilde{F}_1, \dots, \tilde{F}_r) = \int_{[p)^N} \chi_1(\tilde{F}_1) \cdots \chi_r(\tilde{F}_r)$$

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

Thus to prove (11) it suffices to show that

$$\forall \underline{n} \in \mathbb{N}^r,\ \mathrm{ord}_p \left(\sum_{x \in [p)^N} \binom{\tilde{F}_1(x)}{n_1} \cdots \binom{\tilde{F}_r(x)}{n_r} c_1(n_1) \cdots c_r(n_r) \right) \geq B. \tag{13}$$

To show this, fix $\underline{n} = (n_1, \dots, n_r) \in \mathbb{N}^r$. For $1 \leq j \leq r$, let α_j be the integer such that

$$(p-1) \left(\frac{p^{\beta_j} - 1}{p-1} + (\alpha_j - 1) p^{\beta_j - 1} \right) < n_j \leq (p-1) \left(\frac{p^{\beta_j} - 1}{p-1} + \alpha_j p^{\beta_j - 1} \right),$$

so (12) gives that either $\mathrm{ord}_p(\tilde{c}_j(n_j)) \geq B$ for some j – so (13) certainly holds – or

$$\forall 1 \leq j \leq r,\ \mathrm{ord}_p(\tilde{c}_j(n_j)) \geq \alpha_j.$$

Define $\ell \in \mathbb{Z}$ by

$$\ell \coloneqq B - \sum_{j=1}^{r} \alpha_j,$$

so

$$\sum_{j=1}^{r} \mathrm{ord}_p(\tilde{c}_j(n_j)) \geq \sum_{j=1}^{r} \alpha_j = B - \ell. \tag{14}$$

Then (13) certainly holds for $\underline{n}$ if $\ell \leq 0$, so we may assume that $\ell \geq 1$.

Applying [AM21, Thm. 4.3 and Lemma 6.1], the definition of M and (10) we get

$$\mathrm{fdeg} \left(\binom{\tilde{F}_r}{n_1} \cdots \binom{\tilde{F}_r}{n_r} \right) \leq \sum_{j=1}^{r} n_j d_j$$

$$\leq (p-1) \sum_{j=1}^{r} \left(\frac{p^{\beta_j} - 1}{p-1} + \alpha_j p^{\beta_j - 1} \right) d_j \leq (p-1) \left(\sum_{j=1}^{r} \frac{p^{\beta_j} - 1}{p-1} d_j + (B - \ell) M \right)$$

$$< (p-1)(N + M - \ell M) \leq (p-1)(N - \ell + 1),$$

so Lemma 3.1 yields

$$\mathrm{ord}_p \left(\int_{[p)^N} \binom{\tilde{F}_1}{n_1} \cdots \binom{\tilde{F}_r}{n_r} \right) \geq \ell. \tag{15}$$

Combining (14) and (15) we get (13), which completes the proof of Theorem 1.7.

Remark 3.2. *From Theorem 1.7 we can immediately deduce an analogous result for maps $f_1 : A \to B_1, \dots, f_r : A \to B_r$, where A is a finite commutative group of prime exponent p, $B_1, \dots, B_r$ are any nontrivial finite commutative p-groups, and $d_1, \dots, d_r \in \mathbb{N}$ are such*

that $\mathrm{fdeg}(f_j) \leq d_j$ *for all* j *and* $\max_{1\leq j\leq r} d_j \geq 1$.

Indeed, up to isomorphism we may write $A = (\mathbb{Z}/p\mathbb{Z})^N$ *and for all* $1 \leq j \leq r$,

$$B_j = \bigoplus_{j=1}^{K(j)} \mathbb{Z}/p^{\beta_{j,k}}\mathbb{Z} \text{ with } \beta_{j,1} \geq \ldots \geq \beta_{j,K(j)} \geq 1.$$

Let $Z(f_1, \ldots, f_r) = \{x \in A \mid \forall 1 \leq j \leq r,\ f_j(x) = 0\}$. *Composing each* $f_j : A \to B_j$ *with the coordinate projections* $\pi_k : B_j \to \mathbb{Z}/p^{\beta_{j,k}}\mathbb{Z} =: B_{j,k}$, *we get maps* $f_{j,k} := \pi_k \circ f_j$ *for all* $1 \leq j \leq r,\ 1 \leq k \leq K(j)$ *such that* $\max_{1\leq k\leq K(j)} \mathrm{fdeg}\, f_{j,k} = \mathrm{fdeg}(f_j) \leq d_j$. *Evidently, for* $x \in A$ *we have* $f_j(x) = 0$ *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 maps* $\{f_{j,k} : A \to B_{j,k}\}$ *we get*

$$\mathrm{ord}_p(\#Z(f_1, \ldots, f_r)) \geq \left\lceil \frac{N - \sum_{j=1}^r \sum_{k=1}^{K(j)} \frac{p^{\beta_{j,k}}-1}{p-1} d_j}{\max_{1\leq j\leq r} p^{\beta_{j,1}-1} d_j} . \right\rceil.$$

This result may be viewed as a generalization of Theorem 1.7, which we recover by taking each B_j *to be cyclic. However, in practice this result seems to* lose information *from Theorem 1.7 in that for each* j *we use only* $\max_{1\leq k\leq K(j)} \mathrm{fdeg}(\pi_k \circ f_j)$ *instead of the individual functional degrees of the maps* $\pi_k \circ f_j$. *Earlier in our work we proved Theorem 1.8 (which is essentially this result with* $\beta_{j,k} = 1$ *for all* j *and* k*) directly, and this loss of information made the proof significantly more difficult.*

4. p-WEIGHTS

For $p \in \mathcal{P}$ and $d \in \mathbb{N}$, we may uniquely write $d = \sum_{i=0}^N a_i p^i$ with each $a_i \in [p)$. Using this base p expansion, we define the **p-weight**

$$\sigma_p(d) := \sum_{i=0}^N a_i.$$

We have $\sigma_p(d) \leq d$ with equality iff $d \in [p)$. 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 ring. The **p-weight degree** of a nonzero monomial $ct_1^{d_1} \cdots t_n^{d_n}$ with $c \in R \setminus \{0\}$ is defined to be

$$\sigma_p(ct_1^{d_1} \cdots t_n^{d_n}) := \sum_{i=1}^n \sigma_p(d_i),$$

and the **p-weight** degree of a nonzero polynomial $f \in R[t_1, \ldots, t_n]$ is the maximum p-weight degree of a nonzero monomial term. We put $\sigma_p(0) := -\infty$.

A polynomial has positive degree if and only if it has positive p-weight degree.

Lemma 4.1. *Let* $A_1, \ldots, A_n$ *be commutative groups, let* R *be a rng, and for each* $1 \leq i \leq n$ *let* $f_i : A_i \to R$ *be a nonzero function. Let*

$$f : \prod_{i=1}^n A_i \to R,\ (a_1, \ldots, a_n) \mapsto f_1(a_1) \cdots f_n(a_n).$$

a) *We have* $\mathrm{fdeg}(f) \leq \sum_{i=1}^n \mathrm{fdeg}(f_i)$.
b) [AM21, Lemma 6.2] *If* R *is a domain, then we have* $\mathrm{fdeg}(f) = \sum_{i=1}^n \mathrm{fdeg}(f_i)$.

Proof. Induction reduces us to the $n = 2$ case. For $x \in A_1$ and $y \in A_2$ we have

$$(\Delta_x f)(a,b) = f(x+a,b) - f(a,b) = (\Delta_x f_1)(a) f_2(b),$$
$$(\Delta_y f)(a,b) = f(a,y+b) - f(a,b) = f_1(a)(\Delta_y f_2)(b),$$

and thus it follows that for all $x_1, \ldots, x_I, a \in A_1$ and $y_1, \ldots, y_J, b \in A_2$ we have

$$\left(\prod_{i=1}^{I} \Delta_{x_i} \prod_{j=1}^{J} \Delta_{y_j} f\right)(a,b) = \left((\prod_{i=1}^{I} \Delta_{x_i} f_1)(a)\right)\left((\prod_{j=1}^{J} \Delta_{y_j} f_2)(b)\right). \tag{16}$$

Both parts follow easily from this. For part a), for $i = 1, 2$ put $d_i = \mathrm{fdeg}(f_i)$. We may assume that $d_1, d_2 < \infty$ or there is nothing to prove. Then in (16) the right hand side is 0 unless $I \le d_1$ and $J \le d_2$, hence is certainly 0 if $I + J \ge d_1 + d_2 + 1$. For part b), taking $I = d_1$ and $J = d_2$ there are sequences $x_1, \ldots, x_{d_1}, a \in A_1$ and $y_1, \ldots, y_{d_2}, b \in A_2$ such that $\left((\prod_{i=1}^{d_1} \Delta_{x_i} f_1)(a)\right)$ and $\left((\prod_{j=1}^{d_2} \Delta_{y_j} f_2)(b)\right)$ are both nonzero, hence so is their product since R is a domain. □

Proposition 4.2. *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 we have*

$$\mathrm{fdeg}(E(f)) \le \sigma_p(f). \tag{17}$$

Proof. Since $\mathrm{fdeg}(E(f)) = -\infty$ iff $E(f) = 0$, we may assume that $E(f) \neq 0$.

By [AM21, Lemma 3.2] we have $\mathrm{fdeg}(f_1 + f_2) \le \max(\mathrm{fdeg}(f_1), \mathrm{fdeg}(f_2))$. 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

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

Using [AM21, Lemmas 6.1] and Lemma 4.1a), we get

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

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

$$E(t^n) \le \sigma_p(t^n).$$

Writing $n = \sum_{i=0}^{N} a_i p^i$ with $a_i \in [p)$ and using [AM21, Lemma 12.5], we get

$$\mathrm{fdeg}(E(t^n)) = \mathrm{fdeg}\left(\prod_{i=0}^{N} E(t^{p^i})^{a_i}\right) \le \sum_{i=0}^{N} a_i \,\mathrm{fdeg}(E^{t^{p_i}}) = \sum_{i=0}^{N} a_i = \sigma_p(n),$$

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

Combining Theorem 1.7 and Proposition 4.2 yields Theorem 1.3b). Applying Theorem 1.3b) to $R = \mathbb{F}_{p^N}$, we get the Moreno-Moreno Theorem [MM95, Thm. 1].

Theorem 4.3 (Moreno-Moreno)**.** *Let $f_1, \ldots, f_r \in \mathbb{F}_{p^N}[t_1, \ldots, t_n]$ be polynomials of positive degrees. Let*

$$Z(f_1, \ldots, f_r) \coloneqq \{(x_1, \ldots, x_n) \in \mathbb{F}_{p^N}^n \mid f_1(x_1, \ldots, x_n) = \ldots = f_r(x_1, \ldots, x_n) = 0\}.$$

Then

$$\mathrm{ord}_p(Z(f_1, \ldots, f_r)) \ge \left\lceil N \left(\frac{n - \sum_{j=1}^{r} \sigma_p(f_j)}{\max_{j=1}^{r} \sigma_p(f_j)} \right) \right\rceil.$$

Let R be a commutative ring of prime characteristic p. Must we have equality in (17)? 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. For our purposes the more interesting case is when $R = \mathbb{F}_q$, as 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 say that a nonzero monomial $c_{\underline{d}} t_1^{d_1} \cdots t_n^{d_n} \in \mathbb{F}_q[t_1, \ldots, t_n]$ is **reduced** if $d_i \leq q-1$ for all $1 \leq i \leq n$. 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 for any $f \in \mathbb{F}_q[t_1, \ldots, t_n]$ 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 $E \in \mathbb{F}_q^{\mathbb{F}_q^n}$ is $E(f)$ 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

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

depends only 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 4.4 (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 4.2 and Theorem 4.4 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

$$\mathrm{ord}_q(\mathbf{z}) \geq \left\lceil \frac{n - \sum_{j=1}^r \sigma_p(\overline{f_j})}{\max_{j=1}^r \sigma_p(\overline{f_j})} \right\rceil. \tag{18}$$

which by Theorem 4.4 is the optimal application of Theorem 1.7 to polynomials over $\mathbb{F}_q$.

Remark 4.5. *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 $q = p$.*

It would be interesting to characterize the functional degree for polynomial functions over other finite rings, especially finite commutative rings of characteristic p.

5. Final Thoughts

In this paper we have given a group-theoretic version of the Prime Ax-Katz Theorem. It would clearly be desirable to have a group-theoretic version of Ax-Katz over $\mathbb{F}_q$ rather than just over $\mathbb{F}_p$ (cf. Remark 1.4). But what form should this result take?

Again we remark that neither Ax-Katz nor Moreno-Moreno encompasses the other. That is, for a polynomial system $f_1, \ldots, f_r \in \mathbb{F}_{p^N}[t_1, \ldots, t_n]$, when $n > 1$ it is *not known* that

$$\operatorname{ord}_{p^N}(Z(f_1, \ldots, f_r)) \geq \left\lceil \frac{n - \sum_{j=1}^r \sigma_p(f_j)}{\max_{j=1}^r \sigma_p(f_j)} \right\rceil.$$

Next we remark that Moreno-Moreno is not really about $\mathbb{F}_p$: indeed, given any extension of finite fields $\mathbb{F}_q \subset \mathbb{F}_{q^N}$ and any polynomial system $f_1, \ldots, f_n \in \mathbb{F}_{q^N}[t_1, \ldots, t_n]$, the proof of Theorem 4.3 works verbatim, taking Ax-Katz over $\mathbb{F}_q$ as input, to show that

$$\operatorname{ord}_q(Z(f_1, \ldots, f_r)) \geq \left\lceil N \left(\frac{n - \sum_{j=1}^r \sigma_q(f_j)}{\max_{j=1}^r \sigma_q(f_j)} \right) \right\rceil,$$

where $\sigma_q(f)$ is the **q-weight degree** of the polynomial f, defined as for the p-weight degree but using base q expansions: this result appears for instance as [MC03, Thm. 6].

This makes us suspect that there ought to be an R-linear generalization of the Aichinger-Moosbauer calculus: that is, for a commutative ring R, two R-modules A and B and a function $f : A \to B$, there should be $\operatorname{fdeg}_R(f) \in \widetilde{\mathbb{N}}$ satisfying most of the formal properties of the usual functional degree but having $\operatorname{fdeg}_R(f) = 1$ if and only if $f - f(0)$ is an R-module homomorphism and such that if $f \in \mathbb{F}_{q^N}[t_1, \ldots, t_n]$, then

$$\operatorname{fdeg}_{\mathbb{F}_q}(E(f)) = \sigma_q(\overline{f}),$$

where $\overline{f}$ is the $\mathbb{F}_{q^n}$-reduced polynomial associated to f.

We hope to return to these ideas in a future work.

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.

[Cl18] P.L. Clark, *A note on rings of finite rank.* Comm. Algebra 46 (2018), 4223–f4232.

[CS21] P.L. Clark and U. Schauz, *Functional Degrees and Arithmetic Applications I: The Set of Functional Degrees.* To appear, J. of Algebra. `https://arxiv.org/abs/2201.02763`

[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.*

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

[K] I. Kaplansky, *Infinite abelian groups.* University of Michigan Press, Ann Arbor, 1954.

[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.

[MC03] O. Moreno and F.N. Castro, *On the covering radius of certain cyclic codes.* Applied algebra, algebraic algorithms and error-correcting codes (Toulouse, 2003), 129–138, Lecture Notes in Comput. Sci., 2643, Springer, Berlin, 2003.

[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.

[S] J.-P. Serre, *Lectures on the Mordell-Weil theorem.* Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt. With a foreword by Brown and Serre. Third edition. Aspects of Mathematics. Friedr. Vieweg & Sohn, Braunschweig, 1997.

[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.

[Za74] Y.G. Zarkhin, *Noncommutative cohomologies and Mumford groups.* Mathematical Notes of the Academy of Sciences of the USSR 15 (1974), 241–244.