AX'S LEMMA IN THE AICHINGER–MOOSBAUER CALCULUS

PETE L. CLARK AND NICHOLAS TRIANTAFILLOU

Abstract. In 1964, J. Ax gave a ten line proof of the Chevalley–Warning Theorem. The novelty was an innocuous result about summing a polynomial $f \in \mathbb{F}_q[t_1, \ldots, t_N]$ over all $x \in \mathbb{F}_q^N$. Recent work of Aichinger–Moosbauer provides a context in which we can seek to generalize Ax's Lemma to maps $f : A \to B$ between any two finite commutative groups, and indeed Aichinger–Moosbauer proved such a result when the target group B has prime exponent. In this paper we define a **summation invariant** $\sigma(A, B)$ that fits naturally into the Aichinger–Moosbauer caclulus. We give upper and lower bounds on $\sigma(A, B)$ and its exact value in many (but not all) cases. We also give Diophantine applications, including a qualitative Ax–Katz Theorem for polynomials over any finite rng. The bounds that we get turn out to be closely related to Ax's part of the Ax–Katz Theorem.

1. Introduction

1.1. **Overview and Main Results.** In this paper A and B will always denote commutative groups, and except for occasional allusions and recalled general results, A will be assumed to be finite. We denote by B^A the set of all functions $f : A \to B$. Then B^A is itself a commutative group under pointwise addition, and indeed has a natural $\mathbb{Z}[A]$-module structure (see §3).

To each $f \in B^A$, following Aichinger and Moosbauer [AM21] we assign a **functional degree** $\deg(f) \in \mathbb{N} \cup \{\pm\infty\}$. Here we use the convention of [CS22, Definition 2.3], in which $\deg(f) = -\infty$ if and only if $f = 0$.[1]

For $d \in \mathbb{N} \cup \{-\infty\}$, let

$$\mathcal{F}^d(A, B) \coloneqq \{f : A \to B \mid \deg(f) \leq d\}$$

and

$$\mathcal{F}(A, B) \coloneqq \{f : A \to B \mid \deg(f) < \infty\};$$

these are subgroups of B^A. We define a **summation map**

$$\int : B^A \to B, \ (f : A \to B) \mapsto \int f \coloneqq \sum_{x \in A} f(x)$$

and then the **summation invariant**

$$\sigma(A, B) \coloneqq \sup\{d \in \mathbb{N} \cup \{-\infty\} \mid \int f = 0 \text{ for all } f \in \mathcal{F}^d(A, B)\}.$$

In this paper we are interested in the following problem.

[1]Aichinger and Moosbauer do not allow $-\infty$ as a functional degree and instead define the 0 map to have functional degree 0. We find that the present convention deals with the trivial case in a tidier way, but there is certainly no essential difference.

Problem 1. *Compute $\sigma(A,B)$ for every finite commutative group A and commutative group B.*

We do not completely solve Problem 1, but we address it significantly enough to give a wide-ranging Diophantine application. Here are some of our main results:

• In §2 the computation of $\sigma(A,B)$ is reduced to the case in which A is a p-group and B is a finite cyclic p-group for some prime number p.

• In §3.2 we give an upper bound on $\sigma(A,B)$ (Proposition 3.8).

• In §4 we determine $\sigma(A,B)$ when A is cyclic (Theorem 4.2).

• In §5 we determine $\sigma(A,B)$ when A has exponent p (Theorem 5.1). In order to do so, we make use of a characterization of $\sigma(A,B)$ in terms of the filtration on the group ring $(\mathbb{Z}/\exp(B)\mathbb{Z})[A]$ given by powers of the augmentation ideal in order to reduce to a purely algebraic result on group rings (Theorem 5.2), which in turn requires an auxiliary result on Grassmannians that we establish in §5.3.

• In §6 we give a Diophantine application (Theorem 6.2): let R be a finite rng.[2] Let p be a prime number dividing the order of R. Let $r, d_1, \ldots, d_r$ be positive integers. Then there is a function $V : \mathbb{Z}^+ \to \mathbb{Z}^+$ such that for all $b \in \mathbb{Z}^+$, if $n \geq V(b)$, then for every system $f_1, \ldots, f_r$ of polynomial expressions with n indeterminates and coefficients in R such that for each j, f_j has degree d_j, the cardinality of the zero locus $\{x \in R^n \mid f_1(x) = \ldots = f_r(x) = 0\}$ is divisible by p^b. When R is a finite field, this is a qualitative consequence of a celebrated result of J. Ax [Ax64]. Thus our resut extends this "Ax Effect" from finite fields to all finite rngs. Even restricting to finite commutative rings, this is the first Ax–Katz type result over any ring that is neither a principal ideal ring nor has prime characteristic.

We deduce Theorem 6.2 from a purely group-theoretic result (Theorem 6.5) in a manner that stands in close analogy to Aichinger–Moosbauer's group-theoretic generalization of the Chevalley-Warning Theorem (see §1.2). In fact the Diophantine content of these results is carried by a group-theoretic result (Theorem 6.4) whose proof is essentially a classic argument of Ax translated into the Aichinger–Moosbauer functional calculus. This cleanly illustrates that the computation of the key invariant $\sigma(A,B)$ — along with another invariant $\delta^\circ(A,B)$ that was computed by the first author and U. Schauz — is where most of the content resides.

1.2. **Motivation and Context.** In this section we would like to provide some additional context, explaining how our work is motivated by and may be viewed as a continuation and synthesis of prior results of Chevalley–Warning, Ax–Katz, Wilson, Aichinger–Moosbauer and Clark–Schauz.

We begin by recalling the following celebrated results on the p-divisibility of the number of solutions to a low degree system of polynomial equations over a finite

[2]A "rng" is like a ring but need not have a multiplicative identity. It also need not be commutative.

field. For a nonzero integer n and an integer $q \geq 2$, we denote by $\mathrm{ord}_q(n)$ the largest $b \in \mathbb{N}$ such that $q^b \mid n$; we also put $\mathrm{ord}_q(0) = \infty$.

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 $f_j(t_1, \ldots, t_N) \in \mathbb{F}_q[t_1, \ldots, t_N]$ be a polynomial of degree d_j. Let

$$Z = \{(x_1, \ldots, x_N) \in \mathbb{F}_q^N \mid f_1(x_1, \ldots, x_N) = \ldots = f_r(x_1, \ldots, x_N) = 0\}$$

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

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

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

The proofs of Theorem 1.1a) given by Chevalley and by Warning are elementary but nontrivial: they require more than one page. In [Ax64], apart from proving the $r = 1$ case of Theorem 1.1b), J. Ax also gave a remarkable *ten line proof* of Theorem 1.1a). What Chevalley and Warning had missed is merely the following:

Lemma 1.2 (Ax's Lemma)**.** *Let q be a prime power, and let $a_1, \ldots, a_N \in \mathbb{N}$.*

a) *If each a_i is a positive multiple of $q-1$, then*

$$\sum_{x=(x_1,\ldots,x_N) \in \mathbb{F}_q^N} x_1^{a_1} \cdots x_N^{a_N} = (-1)^N.$$

b) *If a_i is not a positive multiple of $q-1$ for some $1 \leq i \leq N$, then*

$$\sum_{x=(x_1,\ldots,x_N) \in \mathbb{F}_q^N} x_1^{a_1} \cdots x_N^{a_N} = 0.$$

c) *If $f \in \mathbb{F}_q[t_1, \ldots, t_N]$ has degree less than $(q-1)N$, then $\sum_{x \in \mathbb{F}_q^N} f(x) = 0$.*

There is no known ten line proof of Theorem 1.1b). Ax's proof of the $r = 1$ case polynomial used Jacobi sums and Stickelberger's congruence, while N.M. Katz's proof of the general case used zeta functions and p-adic cohomology. An Ax-style proof of Theorem 1.1b) was given by Wan [Wa89], while Hou [Ho05] gave a short deduction of the full statement of Theorem 1.1b) from the $r = 1$ case, and D.J. Katz [Ka12] proved a result in coding theory that implies Theorem 1.1b).

None of the proofs of Theorem 1.1b) look anything like Ax's proof of theorem 1.1a). However, Wilson gave in [Wi06] a proof of Theorem 1.1b) *in the case of q a prime number* using a result [Wi06, Lemma 4] that is cognate to Ax's Lemma: we will state a form of his result after introducing some further terminology.

Next we discuss the recent work of Aichinger–Moosbauer [AM21] that gives a fully fledged finite difference calculus for maps between commutative groups. As mentioned above, for commutative groups A and B and any function $f : A \to B$, this calculus assigns a **functional degree** [AM21, §2], [CS22, §2.3]

$$\mathrm{fdeg}(f) \in \mathbb{N} \cup \{\pm\infty\}.$$

In the case in which A and B are both finite p-groups, every function has finite functional degree, and thus there is a largest functional degree $\delta(A, B)$. The quantity $\delta(A, B)$ was determined by Aichinger–Moosbauer in special cases and then in general by Clark–Schauz [CS22, Thm. 4.9]: see §2.1. Moreover, if R is a rng,

$f \in R[t_1, \ldots, t_N]$ is a polynomial and $E(f) : R^N \to R$ is the function obtained by evaluating f at elements of R^N, then we have [AM21, Lemma 12.5]

$$\operatorname{fdeg}(E(f)) \leq \deg(f). \tag{2}$$

The following result is Wilson's Lemma ([Wi06, lemma 4]) translated into the language of functional degrees. It appeared in a draft of [CS23a] but was later taken out because only a variant "lifted version" was used [CS23a, Lemma 3.1].

Lemma 1.3 (Wilson's Ax Lemma)**.** *Let p be a prime number, and let $1 \leq b \leq N$. Let $f : (\mathbb{Z}/p\mathbb{Z})^N \to \mathbb{Z}/p^b\mathbb{Z}$ be a function. If*

$$\operatorname{fdeg}(f) < (N - b + 1)(p - 1), \tag{3}$$

then

$$\sum_{x \in A} f(x) = 0.$$

In §7 we will deduce Lemma 1.3 from [CS23a, Lemma 3.1].

Aichinger and Moosbauer also proved an Ax-type Lemma:

Lemma 1.4. *(Aichinger–Moosbauer's Ax Lemma* [AM21, Lemma 12.1]*)*
Let A and B be finite commutative p-groups, with A nontrivial and B of exponent p. Let $f, g : A \to B$ be maps such that $\operatorname{fdeg}(f) < \operatorname{fdeg}(g)$. Then we have

$$\sum_{x \in A} f(x) = 0.$$

Proof. This is [AM21, Lemma 12.1]. It also follows from our Corollary 3.3 . □

Aichinger–Moosbauer applied Lemma 1.4 to prove the following result.

Theorem 1.5. *Let p be a prime number and let $A = \bigoplus_{i=1}^m \mathbb{Z}/p^{a_i}\mathbb{Z}$ and $B = \bigoplus_{i=1}^n \mathbb{Z}/p^{b_i}\mathbb{Z}$ be finite commutative p-groups. Let $f_1, \ldots, f_r : A^N \to B$ be functions, and suppose that*

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

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

As explained in §6.4, Theorem 1.1a) is a consequence of Theorem 1.5 and (2).

Recently [CS23a, Cor. 1.9] used Lemma 1.3 to Clark–Schauz prove the following **Group-Theoretic Prime Ax–Katz Theorem**:

Theorem 1.6. *Let $N, n, r \in \mathbb{Z}^+$, and put $A = (\mathbb{Z}/p\mathbb{Z})^n$. Let $f_1, \ldots, f_r : A^N \to A$ be nonconstant functions. If*

$$Z \coloneqq \{x \in A^N \mid f_1(x) = \ldots = f_r(x) = 0\},$$

then

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

This recovers Theorem 1.1b) over the prime field $\mathbb{F}_p$ and also the p-weight variant of Theorem 1.1b) given by Moreno-Moreno [MM95].

It is natural to ask for a version of Theorem 1.6 for any finite commutative group A (one easily reduces to the case of a p-group). We observe that both Lemma 1.3 and Lemma 1.4 address Problem 1:

Lemma 1.7. *Let p be a prime number.*

a) *(Wilson) Let $N, b \in \mathbb{Z}^+$ with $N \geq b$. Then we have*
$$\sigma((\mathbb{Z}/p\mathbb{Z})^N, \mathbb{Z}/p^b\mathbb{Z}) \geq (N - b + 1)(p - 1) - 1.$$

b) *(Aichinger–Moosbauer) Let A be a finite commutative p-group, and let B be a commutative group of exponent p. Then we have*
$$\sigma(A, B) \geq \delta(A, B) - 1.$$

This strongly suggests that a systematic study of $\sigma(A, B)$ is relevant to extending Theorem 1.6 to the situation where A has composite exponent. This leads to the "Ax Effect" and related results pursued in §6 of this paper.

1.3. **A Concurrent Work.** After this paper was first written, the first author and U. Schauz continued their work on group-theoretic generalizations of Theorem 1.1b) in [CS23b]. A version of Ax's Lemma appears there as well, but with some subtle differences. In order to explain the discrepancy, in §7, for a finite commutative group A and $B \in \mathbb{Z}^+$ we define a **lifted summation constant** $\tilde{\sigma}(A, \mathbb{Z}/B\mathbb{Z})$.

We include in this section a brief comparison of $\tilde{\sigma}(A, \mathbb{Z}/B\mathbb{Z})$ and $\sigma(A, \mathbb{Z}/B\mathbb{Z})$: it turns out that we have $\tilde{\sigma}(A, \mathbb{Z}/B\mathbb{Z}) \leq \sigma(A, \mathbb{Z}/B\mathbb{Z})$ in all cases, but in the cases of most importance to Theorem 1.1b) and its generalizations, the inequality is strict. There is a kind of "rivalry" between our approach and the approach taken in [CS23b] that seems interesting. But we leave the task of a systematic comparison and possible synthesis to a future work.

2. Introducing $\sigma(A, B)$

2.1. **Notation and Recalled Results.** We write $\mathbb{N}$ for the set of non-negative integers, $\mathbb{Z}^+$ for the set of positive integers and $\mathcal{P}$ for the set of prime numbers.

If R is a commutative ring, M is an R-module, and I is an ideal of R, then we put
$$M[I] \coloneqq \{x \in M \mid ax = 0 \ \forall a \in I\},$$
the I-torsion submodule of M.

In this paper, abstract commutative groups will always be written additively. For a commutative group A, we put $A^\bullet \coloneqq A \setminus \{0\}$. For $N \in \mathbb{Z}^+$ we put
$$A[N] \coloneqq \{a \in A \mid Na = 0\},$$
$$A[N^\infty] \coloneqq \{a \in A \mid N^k a = 0 \text{ for some } k \in \mathbb{Z}^+\},$$
and
$$A[\mathrm{tors}] = \bigcup_{N \in \mathbb{Z}^+} A[N].$$
If there is some $N \in \mathbb{Z}^+$ such that $A = A[N]$, then we say A has **finite exponent** and define the **exponent** $\exp(A)$ to be the least such N; otherwise we put

$\exp(A) := 0$.[3]

In [CS22, §4] the authors determine, for each finite commutative group, the set of functional degrees

$$\mathcal{D}(A,B) := \{\mathrm{fdeg}(f) \mid f \in B^A\}.$$

We also put

$$\delta(A,B) := \{\sup \mathrm{fdeg}(f) \mid f \in B^A\} \text{ and } \delta^\circ(A,B) := \{\sup \mathrm{fdeg}(f) \mid f \in \mathcal{F}(A,B)\}.$$

In particular, we have:

Theorem 2.1 (Clark–Schauz)**.** *Let A, B be nontrivial commutative groups, with A finite and B of finite exponent.*

a) *Suppose that for a prime number p and positive integers $a_1 \geq \ldots a_r$ and b we have $A \cong \bigoplus_{i=1}^r \mathbb{Z}/p^{a_i}\mathbb{Z}$ and $\exp(B) = p^b$. Then*

$$\delta(A,B) = \delta^\circ(A,B) = \sum_{i=1}^r (p^{a_i} - 1) + (b-1)(p-1)p^{a_1-1}.$$

b) *If there is no prime number p such that A and B are both finite p-groups, then $\delta(A,B) = \infty$.*

c) *Suppose that the distinct prime divisors of $\#A$ are $p_1 < \ldots < p_r$. For $1 \leq i \leq r$, let $A_i := A[p_i^\infty]$ and $B_i := B[p_i^\infty]$. Then*

$$\delta^\circ(A,B) = \max_{1 \leq i \leq r} \delta^\circ(A_i,B_i) = \max_{1 \leq i \leq r} \delta(A_i,B_i).$$

Remark 2.2. *While for any commutative ring R, any $n \in \mathbb{Z}^+$ and any $d \in \mathbb{N}$, we know an explicit R-module basis for the set $R[t_1,\ldots,t_n]_{\leq d}$ of polynomial functions of degree at most d – namely the set of monomials $t_1^{a_1}\cdots t_n^{a_n}$ with $a_1 + \ldots + a_n \leq d$ – for most finite commutative p-groups A and B we do not (yet) know the structure of the finite $\mathbb{Z}$-module $\mathcal{F}^d(A,B)$ nor a minimal set of generators.*

2.2. **The Summation Invariant.** If A is finite, we define a map

$$\textstyle\int : B^A \to B,\ (f : A \to B) \mapsto \int f := \sum_{x \in A} f(x).$$

It is immediate that $\int$ is a group homomorphism. Still assuming that A is finite, we define the **summation invariant**

$$\sigma(A,B) := \sup\{d \in \mathbb{N} \cup \{-\infty\} \mid \textstyle\int f = 0 \text{ for all } f \in \mathcal{F}^d(A,B)\}.$$

For $b \in B$, let $C_b : A \to B$ be the function mapping every $a \in A$ to b. Then

$$\textstyle\int C_b = (\#A)b,$$

so $\int C_b = 0$ if and only if $b \in B[\#A]$. Since the functions of functional degree 0 are precisely the functions C_b for $b \in B^\bullet$, we deduce:

Lemma 2.3. *Let A be a finite commutative group, and let B be a commutative group. Then $\sigma(A,B) \geq 0$ if and only if $\exp(B) \mid \#A$.*

In particular, we have $\sigma(A,B) = -\infty$ unless B has finite exponent.

[3]This is not a standard definition, but it is analogous to the definition of "characteristic zero."

2.3. **Reductions in the computation of $\sigma(A,B)$.** Throughout this section A and B are nontrivial commutative groups with A finite and B of finite exponent. In this context it is certainly clear that $\int f \neq 0$ for some $f \in B^A$: just take a function that is nonzero at exactly one element of A. However this kind of "delta function" (cf. [AM21, §7] and [CS22, §4.2]) need not have finite functional degree, making it non-obvious that $\sigma(A,B)$ is necessarily finite. However the next result shows that this is always the case as a consequence of an important "primary decomposition" for the summation invariant.

Proposition 2.4. *Let A and B be nontrivial commutative groups with A finite and $B = B[N]$ for some $N \in \mathbb{Z}^+$. Let $p_1 < \dots p_n$ be the distinct prime divisors of $(\#A)\cdot N$, and for $1 \leq i \leq n$, let $A_i \coloneqq A[p_i^\infty]$ and $B_i \coloneqq B[p_i^\infty]$, so*

$$A = \prod_{i=1}^n A_i \text{ and } B = \prod_{i=1}^n B_i.$$

We have

$$\sigma(A,B) = \min_{i|B_i\neq 0} \sigma(A_i,B_i) < \infty. \tag{4}$$

Proof. Let $f \in B^A$ have finite functional degree. By [CS22, Thm. 3.13], we have $f = (f_1,\dots,f_n)$ for functions $f_i \in B_i^{A_i}$. We have $\int f = 0$ if and only if $\sum_{x\in A} f_i(x) = 0$ for all $1 \leq i \leq n$. For $1 \leq i \leq r$ we have

$$\sum_{x\in A} f_i(x) = \frac{\#A}{\#A_i} \sum_{x_i \in A_i} f_i(x_i).$$

Since $\sum_{x_i\in A_i} f_i(x_i)$ is an element of the p_i-group B_i and $p_i \nmid \frac{\#A}{\#A_i}$, we deduce:

$$\int f = 0 \iff \forall 1 \leq i \leq r,\ \frac{\#A}{\#A_i} \int f_i = 0 \iff \forall 1 \leq i \leq r,\ \int f_i = 0.$$

If i is such that $B_i \neq 0$, then we have

$$\sigma(A_i,B_i) < \delta(A_i,B_i) < \infty :$$

indeed for any $b_i \in B_i \setminus \{0\}$ the delta function δ_{0,b_i} has $\int \delta_{0,b_i} = b_i \neq 0$ and – like every function between finite commutative p-groups – finite functional degree. In particular, there is $f_i \in B_i^{A_i}$ of functional degree $\sigma(A_i,B_i)+1$ such that $\int f_i \neq 0$.

Also by [CS22, Thm. 3.13] we have

$$\operatorname{fdeg}(f) = \max_i \operatorname{fdeg}(f_i) = \max_{i|B_i\neq\{0\}} \operatorname{fdeg}(f_i).$$

Thus for $d \in \mathbb{N}$, there is $f \in B^A$ of functional degree d with $\int f \neq 0$ if and only if for some i there is $f_i \in B_i^{A_i}$ of functional degree d with $\int f_i \neq 0$ if and only if

$$d > \min_{i|B_i\neq 0} \sigma(A_i,B_i),$$

and thus we have

$$\sigma(A,B) = \min_{i|B_i\neq 0} \sigma(A_i,B_i).$$

As mentioned above, for all i with $B_i \neq 0$ we have $\sigma(A_i,B_i) < \delta(A_i,B_i) < \infty$, and this shows that $\sigma(A,B) < \infty$. □

Lemma 2.5. *Let A and B be nontrivial commutative groups, with A finite and B of finite exponent.*

a) *We have* $\sigma(A,B) < \delta(A,B)$.
b) *If* $\iota : B \hookrightarrow B'$ *is an injective homomorphism, then* $\sigma(A,B) \geq \sigma(A,B')$.
c) *If* $\iota : A \hookrightarrow A'$ *is an injective homomorphism, then* $\sigma(A',B) \geq \sigma(A,B)$.

Proof. a) If A and B are not both p-groups, then

$$\sigma(A,B) < \infty = \delta(A,B).$$

If A and B are both finite p-groups, then $\delta(A,B) < \infty$, so $\sigma(A,B) = \delta(A,B)$ would imply that $\int f = 0$ for every $f \in B^A$. Taking f to be any delta function $\delta_{0,b}$ for $b \in B \setminus \{0\}$ we get $\int \delta_{0,b} \neq 0$.
b) If $f \in B^A$ has functional degree at most $\sigma(A,B')$, then $\iota \circ f \in (B')^A$ and

$$\operatorname{fdeg}(\iota \circ f) = \operatorname{fdeg}(f) \leq \sigma(A,B'),$$

so

$$\int f = \int (\iota \circ f) = 0.$$

c) Without loss of generality we may identify A with $\iota(A)$ and assume that A is a subgroup of A'. Let $f : A' \to B$ have functional degree at most $\sigma(A,B)$. For $y \in A'$, we write $[y]f : A' \to B$ for the function $x \mapsto f(y+x)$.[4]

It is easy to see that $\operatorname{fdeg}([y]f) = \operatorname{fdeg}(f)$: for instance, this follows from the fact that $\operatorname{fdeg}(f)$ depends only on the annihilator ideal of f as a $\mathbb{Z}[A]$-module [CS22, Lemma 3.7] because $[y]$ is a unit in the group ring and thus $\operatorname{ann}([y]f) = \operatorname{ann}(f)$. Or: just because for all $a \in A'$ we have

$$\Delta_a([y]f)(x) = f(a+y+x) - f(y+x) = ([y]\Delta_a f)(x)$$

we get: for all $a_0, \ldots, a_d \in A'$, $\Delta_{a_0} \cdots \Delta_{a_d} f = 0$ if and only if $\Delta_{a_0} \cdots \Delta_{a_d}([y]f) = 0$.

Now let $x_1, \ldots, x_r$ be a set of coset representatives for A in A', and for $1 \leq i \leq r$, let g_i be the restriction of $[x_i]f$ to A. By [CS22, Lemma 3.9a)], we get

$$\operatorname{fdeg}(g_i) = \operatorname{fdeg}(f|_A) \leq \operatorname{fdeg}(f) \leq \sigma(A,B),$$

and thus

$$\int f = \int_{x \in A'} f(x) = \sum_{i=1}^{r} \sum_{a \in A} f(x_i + a) = \sum_{i=1}^{r} \int g_i = 0. \qquad \square$$

Lemma 2.6. *Let* A *be a finite commutative group, and let* B *be a commutative group of finite exponent.*

a) *Let* $\{B_x\}_{x \in X}$ *be a family of nontrivial commutative groups. We have*

$$\sigma(A, \bigoplus_{x \in X} B_x) = \sigma(A, \prod_{x \in X} B_x) = \min_{x \in X} \sigma(A, B_x).$$

b) *We have* $\sigma(A,B) = \sigma(A, \mathbb{Z}/\exp(B)\mathbb{Z})$.

Proof. a) Let $f : A \to \prod_{x \in X} B_x$, so $f = (f_x)$ with $f_x : A \to B_x$. By [CS22, Lemma 2.16] we have $\operatorname{fdeg}(f) = \sup_{x \in X} \operatorname{fdeg}(f_x)$. Moreover we have $\int f = 0$ if and only if $\int f_x = 0$ for all $x \in X$, and it follows that

$$\sigma(A, \prod_{x \in X} B_x) = \min_{x \in X} \sigma(A, B_x).$$

[4]The notation comes from the interpretation of the set $B^{A'}$ of all maps $f : A' \to B$ as a module over the group ring $\mathbb{Z}[A']$: see §3.

If this minimum is $-\infty$, then there is $x \in X$ and $b_x \in B_x \setminus B_x[\#A]$. Let $b \in \bigoplus_{x\in X} B_x$ have x-coordinate b_x and all other coordinates 0; then the constant function $C_b : A \to B$ has functional degree 0 and $\int C_b \neq 0$, so

$$\sigma(A, \bigoplus_{x\in X} B_x) = -\infty = \min_{x\in X} \sigma(A, B_x).$$

Otherwise, let $x \in X$ be such that

$$\sigma(A, B_x) = \min_{x\in X} \sigma(A, B_x) \geq 0.$$

Then there is a function $f_x : A \to B_x$ of functional degree $\sigma(A, B_x) + 1$ such that $\int f_x \neq 0$. Let $f : A \to \bigoplus_{x\in X} B_x$ be the function with x-component f_x and every other component 0. Then $\mathrm{fdeg}(f) = \sigma(A, B_x) + 1$ and $\int f \neq 0$, so $\sigma(A, \bigoplus_{x\in X} B_x) \leq \sigma(A, \prod_{x\in X} B_x)$. Since $\bigoplus_{x\in X} B_x \hookrightarrow \prod_{x\in X} B_x$ is an injective homomorphism, so part b) gives

$$\sigma(A, \bigoplus_{x\in X} B_x) \geq \sigma(A, \prod_{x\in X} B_x).$$

b) Let N be the exponent of B. Then by [CS22, Thm. 2.1], we may write $B = \bigoplus_{x\in X} C_x$, where C_x is cyclic of exponent $M_x \mid N$ and $M_x = N$ for at least one x. By parts b) and c), we get

$$\sigma(A, B) = \sigma(A, \bigoplus_{x\in X} C_x) = \min_{x\in X} \sigma(A, C_x) = \sigma(A, \mathbb{Z}/N\mathbb{Z}) = \sigma(A, \mathbb{Z}/\exp(B)\mathbb{Z}). \quad \square$$

2.4. **When $\sigma(A, B) = 0$.**

Theorem 2.7. *Let A and B be nontrivial commutative groups, with A finite. The following are equivalent:*

(i) *We have $\sigma(A, B) = 0$.*
(ii) *We have $\exp(B) \mid \#A$ and moreover: the Sylow 2-subgroup $A[2^\infty]$ is nontrivial, cyclic and isomorphic to the Sylow 2-subgroup of $\mathbb{Z}/\exp(B)\mathbb{Z}$.*

Proof. Step 1: By Lemma 2.3, we have $\sigma(A, B) = -\infty$ if and only if $\exp B \nmid \#A$, so we may assume that $\exp B \mid \#A$. Let $p_1 < \ldots < p_r$ be the distinct prime numbers dividing $\exp B$, and for $1 \leq i \leq r$ put

$$A_i \coloneqq A[p_i^\infty] \text{ and } B_i \coloneqq B[p_i^\infty].$$

For all $1 \leq i \leq r$ we have $\exp B_i \mid \#A_i$, so $\sigma(A_i, B_i) \geq 0$. Proposition 2.4 thus gives

$$\sigma(A, B) = 0 \iff \sigma(A_i, B_i) = 0 \text{ for some } 1 \leq i \leq r.$$

so we are reduced to the case in which A is a finite p-group and B is a p-group of exponent dividing $\#A$. Moreover Lemma 2.6b) gives $\sigma(A, B) = \sigma(A, \mathbb{Z}/\exp(B)\mathbb{Z})$, so we are reduced to the case in which

$$A = \bigoplus_{i=1}^{r} \mathbb{Z}/p^{a_i}\mathbb{Z} \text{ and } B = \mathbb{Z}/p^b\mathbb{Z} \text{ with } a_1 \geq \ldots \geq a_r \geq 1.$$

We must show that if $p > 2$ then $\int f = 0$ for all $f : A \to B$ of functional degree 1, while for $p = 2$ there is $f : A \to B$ of functional degree 1 such that $\int f \neq 0$ if and only if A is nontrivial, cyclic and isomorphic to B.
Step 2: Let $f : A \to B$ have functional degree 1. By [CS22, Remark 4c)], there is a nonzero group homomorphism $\epsilon : A \to B$ and $b_\bullet \in B$ such that

$$\forall x \in A,\ f(x) = \epsilon(x) + b_\bullet.$$

We have

$$\int f = \int \epsilon + (\#A) \cdot b_\bullet = \int \epsilon,$$

so we may assume that f is a group homomorphism. The image $\underline{B} \coloneqq f(A)$ is therefore cyclic of order $p^{b'}$ for some $1 \leq b' \leq \min(a_1, b)$, and conversely every such b' is certainly attained by a suitable f. Every nonempty fiber of f has cardinality $\frac{\#A}{\#\underline{B}} = p^{a_1+\ldots+a_r-b'}$, so

$$\int f = p^{a_1+\ldots+a_r-b'} \sum_{y \in \underline{B}} y.$$

Since $p^{b-b'} \pmod{p^b}$ is a generator for $\underline{B}$, we have

$$\sum_{y \in \underline{B}} y = p^{b-b'} \sum_{i=0}^{p^{b'}-1} i \pmod{p^b} = \frac{p^{b-b'}(p^{b'}-1)p^{b'}}{2} \pmod{p^b}.$$

- When $p > 2$, this shows: $\sum_{y \in \underline{B}} y = 0$, so $\int f = 0$. So $\sigma(A, B) \geq 1$ in this case.
- When $p = 2$, we find that

$$\int f = 0 \iff a_1 + \ldots + a_r - b' + b - 1 \geq b \iff a_1 + \ldots + a_r \geq b' + 1.$$

As mentioned above, the largest possible value of b' is $\min(a_1, b)$, so we find that that $\sigma(A, B) = 0$ if and only if $a_1 = b$ and $r = 1$. This holds if and only if A is nontrivial, cyclic and isomorphic to B. □

Remark 2.8. *Maintain the notation of Theorem 2.7. The proof of Theorem 2.7 shows that if $f : A \to B$ is a group homomorphism, then $\int f \neq 0$ if and only if the Sylow 2-subgroup $A[2^\infty]$ of A is nontrivial cyclic and the restriction of f to $A[2^\infty]$ is an injection. Moreover, because in all cases we have*

$$a_1 + \ldots + a_r - b' + b - 1 \geq b - 1,$$

it also shows that when $\int f \neq 0$, then $\int f$ has order 2 in B. Taking f to be the identity map on a finite commutative group A, we recover Miller's group-theoretic generalization of Wilson's Theorem: see [Mi03] *and* [Cl-W, Thm. 1.4].

3. Group Rings

3.1. **Two group ring characterizations of $\sigma(A, \mathbb{Z}/N\mathbb{Z})$.** Let A, B be commutative groups with A finite. Then B^A is naturally a module over the group ring $(\mathbb{Z}/\exp(B)\mathbb{Z})[A]$. We have an augmentation homomorphism

$$\varphi : (\mathbb{Z}/\exp(B)\mathbb{Z})[A] \twoheadrightarrow \mathbb{Z}/\exp(B)\mathbb{Z}$$

that is uniquely determined by mapping, for each $a \in A$, the element $[a]$ to 1. Put

$$I \coloneqq \ker(\varphi),$$

the augmentation ideal. Since B is a $\mathbb{Z}/\exp(B)\mathbb{Z}$-module, we may endow B with the structure of a $(\mathbb{Z}/\exp(B)\mathbb{Z})[A]$-module by letting each $[a]$ act on B as 1_B: this is the natural $\mathbb{Z}/\exp(B)\mathbb{Z}$-module structure on B pulled back via the map φ.

Aichinger and Moosbauer define the functional degree of a nonzero $f \in B^A$ using the augmentation ideal: namely, we say $\mathrm{fdeg}(f) \leq n$ if and only if I^{n+1} kills f. Equivalently, for $d \in \mathbb{N}$ we have

$$\mathcal{F}^d(A, B) = B^A[I^{d+1}] = \{f \in B^A \mid \forall \theta \in I^{d+1},\ \theta f = 0\}.$$

This also means that the determination of $\delta(A,B)$ – the largest possible functional degree for $f \in B^A$ – is equivalent to the commutative algebra problem of determining whether the augmentation ideal of $(\mathbb{Z}/\exp(B)\mathbb{Z})[A]$ is nilpotent and if so computing its nilpotency index $\nu_{A,B}(I)$, i.e., the smallest power of I that is (0). If we put $\nu_{A,B}(I) = \infty$ if I is not nilpotent, then we get [CS22, Thm. 4.1]

$$\delta(A,B) = \nu_{A,B}(I) - 1.$$

Aichinger and Moosbauer showed that for nontrivial finite commutative groups A and B, the augmentation ideal I of $(\mathbb{Z}/\exp(B))\mathbb{Z}[A]$ is nilpotent if and only if A and B are both p-groups for some prime p, which was the first result determining when $\delta(A,B)$ is finite for such groups A and B (a special case of Theorem 2.1).

In the works of Aichinger–Moosbauer and Clark–Schauz, this algebraic interpretation of $\delta(A,B)$ allowed information to flow in both directions: in many cases $\nu_{A,B}(I)$ is easy to compute or was already known, and this determines $\delta(A,B)$. However for most pairs of finite commutative p-groups A and B, the nilpotency index $\nu_{A,B}(I)$ was *not* known, and thus the determination of $\delta(A,B)$ by Clark–Schauz – using prior results of a more arithmetic nature – gave the first general solution of this algebraic problem.

In this section we will give an analogous discussion for the quantity $\sigma(A,B)$. Indeed we will give two interpretations of $\sigma(A,B)$ in terms of powers of the augmentation ideal in the group ring $(\mathbb{Z}/\exp(B)\mathbb{Z})[A]$.

First: the map $\int : B^A \to B$ is in fact a $(\mathbb{Z}/\exp(B)\mathbb{Z})[A]$-module homomorphism: it is evidently a $\mathbb{Z}/\exp(B)\mathbb{Z}$-module homomorphism, so the matter of this is that for all $a \in A$ and $f \in B^A$ we have

$$\int ([a]f) = \sum_{x \in A} ([a]f)(x) = \sum_{x \in A} f(a+x) = \sum_{x \in A} f(x) = \int f.$$

It follows that

$$\int (IB^A) = 0.$$

Suppose now that $B = \mathbb{Z}/N\mathbb{Z}$ for $N \in \mathbb{N}$. (Recall that in Lemma 2.6b) we reduced the general case to this case.) Then we may identify the group ring $(\mathbb{Z}/N\mathbb{Z})[A]$ with $(\mathbb{Z}/N\mathbb{Z})^A$: the element $\sum_{a \in A} n_a[x]$ corresponds to the function $a \in A \mapsto n_a \in \mathbb{Z}/N\mathbb{Z}$. This is compatible with the $(\mathbb{Z}/N\mathbb{Z})[A]$-module structure on $(\mathbb{Z}/N\mathbb{Z})^A$. It follows that $(\mathbb{Z}/N\mathbb{Z})^A$ is a free, rank 1 $(\mathbb{Z}/N\mathbb{Z})^A$-module with basis $\delta_{0,1}$, the function that maps 0 to 1 and every other element of A to 0. Under this identification, the functional $\int : (\mathbb{Z}/N\mathbb{Z})^A \to \mathbb{Z}/N\mathbb{Z}$ is precisely the augmentation homomorphism φ. We deduce:

Theorem 3.1. *Let A be a finite commutative group, and let $N \in \mathbb{Z}^+$.*

a) *For $f \in (\mathbb{Z}/N\mathbb{Z})^A$, we have $\int f = 0$ if and only if $f \in I(\mathbb{Z}/N\mathbb{Z})^A$.*

b) *If $N \mid \#A$, then $\sigma(A, \mathbb{Z}/N\mathbb{Z})$ is the largest $k \in \mathbb{N}$ such that*

$$(\mathbb{Z}/N\mathbb{Z})^A[I^{k+1}] \subseteq I(\mathbb{Z}/N\mathbb{Z})^A.$$

Corollary 3.2. *Let $N \in \mathbb{Z}^+$, and let A be a finite commutative group. Then $[(\mathbb{Z}/N\mathbb{Z})^A : I(\mathbb{Z}/N\mathbb{Z})^A] = N$.*

Proof. We have

$$(\mathbb{Z}/N\mathbb{Z})^A / I(\mathbb{Z}/N\mathbb{Z})^A \cong (\mathbb{Z}/N\mathbb{Z})[A]/I\mathbb{Z}/N\mathbb{Z}[A] \cong \varphi((\mathbb{Z}/N\mathbb{Z})[A]) \cong \mathbb{Z}/N\mathbb{Z}. \quad \square$$

Corollary 3.3. *Let p be a prime number, let A be a finite commutative p-group, and let B be a commutative group of exponent p. We have*

$$\sigma(A, \mathbb{Z}/p\mathbb{Z}) = \delta(A, B) - 1.$$

Proof. Lemma 2.6b) gives $\delta(A, B) = \delta(A, \mathbb{Z}/p\mathbb{Z})$, so we may assume that $B = \mathbb{Z}/p\mathbb{Z}$.

Every $f \in (\mathbb{Z}/p\mathbb{Z})^A$ is annihilated by $I^{\delta(A,\mathbb{Z}/p\mathbb{Z})+1}$, so every $g \in I(\mathbb{Z}/p\mathbb{Z})^A$ is annihilated by $I^{\delta(A,\mathbb{Z}/p\mathbb{Z})}$. It follows that

$$I(\mathbb{Z}/p\mathbb{Z})^A \subseteq \mathcal{F}^{\delta(A,\mathbb{Z}/p\mathbb{Z})-1}(A, \mathbb{Z}/p\mathbb{Z}) \subsetneq \mathcal{F}(A, \mathbb{Z}/p\mathbb{Z}) = (\mathbb{Z}/p\mathbb{Z})^A.$$

By Lemma 3.2b) we have $[(\mathbb{Z}/p\mathbb{Z})^A : I(\mathbb{Z}/p\mathbb{Z})^A] = p$, so by Theorem 3.1 we have

$$\mathrm{Ker}(\int) = I(\mathbb{Z}/p\mathbb{Z})^A = \mathcal{F}^{\delta(A,\mathbb{Z}/p\mathbb{Z})-1}(A, \mathbb{Z}/p\mathbb{Z}). \qquad \square$$

Remark 3.4. *Lemma 1.7b) was stated as an inequality, following* [AM21, Lemma 12.1]. *But because $\delta(A, B)$ is finite in this case, if $\sigma(A, \mathbb{Z}/p\mathbb{Z})$ were equal to $\delta(A, B)$ that would mean that $\int f = 0$ for* every *function $f \in B^A$. This conclusion is manifestly false: take f to be nonzero at exactly one point.*

But our proof of this result is different from that of [AM21, Lemma 12.1].

Our next application is a sort of analogue of the Fundamental Theorem of Calculus in the case where A is a finite cyclic group.

Corollary 3.5. *Let $M, N \in \mathbb{Z}^+$, and let $B = B[M]$ be an M-torsion commutative group. For $f : \mathbb{Z}/N\mathbb{Z} \to B$, the following are equivalent:*

(i) *We have $\int f = 0$.*
(ii) *The function g "is a derivative": there is $g : \mathbb{Z}/N\mathbb{Z} \to B$ such that $f(x) = g(x+1) - g(x)$ for all $x \in \mathbb{Z}/N\mathbb{Z}$.*

Proof. Step 1: The group B is isomorphic to $\bigoplus_{x \in X} \mathbb{Z}/M_x\mathbb{Z}$ for $M_x \mid M$. For a finite commutative group A and a map $f : A \to \prod_{x \in X} \mathbb{Z}/M_x\mathbb{Z}$, we may write $f = (f_x : A \to \mathbb{Z}/M_x\mathbb{Z})$. Each of the properties of lying in the kernel of $\int$ and being a derivative holds for f if and only if it holds for each f_x, so to prove the result for maps $f : \mathbb{Z}/N\mathbb{Z} \to \prod_{x \in X} \mathbb{Z}/M_x\mathbb{Z}$ we reduce to the case of $B = \mathbb{Z}/M_x\mathbb{Z}$.

Suppose now that $f : \mathbb{Z}/N\mathbb{Z} \to \bigoplus_{x \in X} \mathbb{Z}/M_x\mathbb{Z}$. Then for all $a \in \mathbb{Z}/N\mathbb{Z}$ we have $f_x(a) = 0$ for all but finitely many $x \in X$; but $\mathbb{Z}/N\mathbb{Z}$ is also finite, so in fact $f_x = 0$ for all but finitely many x. Thus: if f is the derivative of some $g : \mathbb{Z}/N\mathbb{Z} \to \prod_{x \in X} \mathbb{Z}/M_x\mathbb{Z}$, then also f is the derivative of some $h : \mathbb{Z}/N\mathbb{Z} \to \bigoplus_{x \in X} \mathbb{Z}/M_x\mathbb{Z}$, since for all but finitely many $x \in X$ we may just take $g_x = 0$. So we have reduced to maps $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/M\mathbb{Z}$.

Step 2: Let $f \in (\mathbb{Z}/M\mathbb{Z})^{\mathbb{Z}/N\mathbb{Z}}$. Lemma 3.2 says that $\int f = 0$ iff $f \in I(\mathbb{Z}/N\mathbb{Z})^{\mathbb{Z}/M\mathbb{Z}}$. By [CS22, Remark 2.7b)], the ideal I is generated by $[1] - [0]$. Thus we have $f \in I(\mathbb{Z}/M\mathbb{Z})^{\mathbb{Z}/N\mathbb{Z}}$ if and only if $f = ([1] - [0])g = \Delta_1(g)$. $\square$

We now move on to our second group ring interpretation of $\sigma(A, B)$, which holds in the case $B = \mathbb{Z}/N\mathbb{Z}$. (Recall that in §2 we reduced the general computation of $\sigma(A, B)$ to this case.) Let A be a finite commutative group, and let $N \in \mathbb{Z}^+$. In the group ring $(\mathbb{Z}/N\mathbb{Z})[A]$, consider the **norm element**

$$\omega := \sum_{x \in A} [x].$$

For any $\eta \in (\mathbb{Z}/N\mathbb{Z})[A]$, we have

$$\omega\eta = \varphi(\eta)\omega,$$

where $\varphi : (\mathbb{Z}/N\mathbb{Z})[A] \to \mathbb{Z}/N\mathbb{Z}$ is the augmentation map.

Lemma 3.6. *Let $\mathfrak{r}$ be a finite commutative ring in which each ideal is principal. For $m, n \in \mathbb{Z}^+$, let $M_{m,n}(\mathfrak{r})$ be the set of $m \times n$ matrices with coefficients in $\mathfrak{r}$. For $A \in M_{m,n}(\mathfrak{r})$, let* $\operatorname{rowspace}(A)$ *be the $\mathfrak{r}$-submodule of $\mathfrak{r}^n$ generated by the rows of A. Then we have*

$$\#\operatorname{rowspace}(A) \cdot \#\operatorname{Ker}(A) = (\#\mathfrak{r})^n.$$

Proof. Of course, the map $v \in M_{1,n}(\mathfrak{r}) = \mathfrak{r}^n \mapsto Av \in M_{m,1}(\mathfrak{r}) = \mathfrak{r}^m$ is $\mathfrak{r}$-linear, so the first isomorphism theorem for $\mathfrak{r}$-modules gives us:

$$\mathfrak{r}^n / \operatorname{Ker}(A) \cong A(\mathfrak{r}^n)$$

and thus

$$(\#\mathfrak{r})^n = \#\operatorname{Ker}(A) \cdot \#A(\mathfrak{r}^n).$$

Evidently $A(\mathfrak{r}^n)$ is the column space of A, i.e., the $\mathfrak{r}$-submodule of $\mathfrak{r}^m$ generated by the columns of A. So our task is to show a version of "row rank" = "column rank" in this context, namely that

$$\#\operatorname{rowspace}(A) = \#\operatorname{columnspace}(A).$$

In turn the row space of A is the column space of the transpose A^T, so it suffices to show that

$$\#A(\mathfrak{r}^n) = \#A^T(\mathfrak{r}^m).$$

We will use that the ring $\mathfrak{r}$ is an **elementary divisor ring** [Ka49, §12]: this means there is $P \in \mathrm{GL}_m(\mathfrak{r})$ and $Q \in GL_n(\mathfrak{r})$ such that PAQ is diagonal – i.e., has $a_{ij} = 0$ unless $i = j$. Put $r \coloneqq \min(m, n)$. We do not change the size of the image of a map between finite sets by composing with bijections, so because $\mathfrak{r}$ is an elementary divisor ring we may assume that A is diagonal, say with diagonal entries $a_1, \ldots, a_r$. Then the row space is the direct sum of the cyclic $\mathfrak{r}$-modules $R_1, \ldots, R_r$ generated by the rows $(a_1, 0, \ldots, 0), \ldots, (0, \ldots, a_r, 0, \ldots, 0)$ (all other rows are zero). The cyclic $\mathfrak{r}$-module R_i is isomorphic to $\mathfrak{r}/\operatorname{ann}(R_i) \cong \mathfrak{r}/\operatorname{ann}(a_i)$, so the size of the row space is $\prod_{i=1}^r \#\mathfrak{r}/\operatorname{ann}(a_i)$. Exactly the same holds for the column space: it is the direct sum of the cyclic $\mathfrak{r}$-modules $C_1, \ldots, C_r$ generated by the columns $(a_1, 0, \ldots, 0), \ldots, (0, \ldots, a_r, 0, \ldots, 0)$ (all other columns are zero), so it also has size $\prod_{i=1}^r \#\mathfrak{r}/\operatorname{ann}(a_i)$. □

Theorem 3.7. *Let A be a finite commutative group, and let $N \in \mathbb{Z}^+$ be such that $N \mid \#A$. Let I be the augmentation ideal of the group ring $R \coloneqq (\mathbb{Z}/N\mathbb{Z})[A]$, and let $\omega = \sum_{x \in A}[x] \in (\mathbb{Z}/N\mathbb{Z})[A]$ be the norm element. Then for all $d \in \mathbb{N}$, we have*

$$\sigma(A, \mathbb{Z}/N\mathbb{Z}) = d \iff \omega \in I^{d+1} \setminus I^{d+2}.$$

Proof. Step 1: We will show that if $\omega \in I^{d+1}$, then $\sigma(A, \mathbb{Z}/N\mathbb{Z}) \geq d$.

Indeed, under our identification of $(\mathbb{Z}/N\mathbb{Z})^A$ with the group ring R, we have $\mathcal{F}^d(A, \mathbb{Z}/N\mathbb{Z}) = R[I^{d+1}]$, so if $\omega \in I^{d+1}$ then for all $f \in \mathcal{F}^d(A, \mathbb{Z}/N\mathbb{Z})$ we have

$$0 = \omega f = \varphi(f)\omega = (\textstyle\int f)\omega$$

and thus $\int f = 0$.
Step 2: Let $J_1 \supsetneq J_2$ be ideals of R. We claim that we have a proper containment of torsion submodules:

$$R[J_2] \supsetneq R[J_1].$$

For this it suffices to show that for any ideal J of R, we have

$$\#J \cdot \#R[J] = \#R, \tag{5}$$

for then as J grows in size, $R[J]$ must shrink. To see this, let $n \coloneqq \#A$, and write out the elements of A in some order: $A = \{x_1 = 0, x_2, \ldots, x_n\}$, and thereby identify $R = (\mathbb{Z}/N\mathbb{Z})[A]$ with $(\mathbb{Z}/N\mathbb{Z})^n$. Now let $m \coloneqq \#J$, and write out the elements of J in some order: $J = \{r_1, \ldots, r_m\}$, with each $j_i \in (\mathbb{Z}/N\mathbb{Z})^n$. This allows us to define the matrix

$$A_J \in M_{m,n}(\mathbb{Z}/N\mathbb{Z}),$$

whose rows are $r_1, \ldots, r_m$. Evidently the row space of A_J is J itself. We claim that the size of $\mathrm{Ker}(A_J)$ is $\#R[J]$; if so, we apply Lemma 3.6 with $\mathfrak{r} = \mathbb{Z}/N\mathbb{Z}$ to get

$$\#J \cdot \#R[J] = \#\,\mathrm{rowspace}(A_J) \cdot \#\,\mathrm{Ker}(A_J) = \#(\mathbb{Z}/N\mathbb{Z})^n = \#R.$$

To establish the claim, for $b = \sum_{i=1}^n b_i[x_i] \in R$, put

$$b^* \coloneqq \sum_{i=1}^n b_i[-x_i]$$

and then define $b_{1^*}, \ldots, b_{n^*}$ by

$$\sum_{i=1}^n b_{i^*}[x_i] = \sum_{i=1}^n b_i[-x_i].$$

Then for $a = \sum_{i=1}^n a_i[x_i] \in R$, the matrix product

$$[a_1, \ldots, a_n][b_1, \ldots, b_n]^T = \sum_{i=1}^n a_i b_i$$

is the coefficient of $[0]$ in ab^*. It follows that b lies in the kernel of A_J if and only if for all $1 \le j \le m$, the coefficient of $[0]$ in $r_j b^*$ is 0. But for all $x \in A$, we have $[-x]r_j \in J$, so $[-x]r_j = r_{x(j)}$ for some $1 \le x(j) \le m$, so the coefficient of $[0]$ in $[-x]r_j b^*$ is the coefficient of $[x]$ in $r_j b^*$. This shows that b lies in the kernel of A_J if and only if $r_j b^* = 0$ for all j. We deduce that the kernel of A_J is $R[J]^*$; since $b \mapsto b^*$ is an involution on R, we have $\#\,\mathrm{Ker}(A_J) = \#R[J]^* = \#R[J]$.
Step 3: Let $d \in \mathbb{N}$ be such that $\omega \notin I^{d+2}$. Then $J \coloneqq \langle I^{d+2}, \omega \rangle \supsetneq I^{d+2}$, so by Step 2, there is

$$f \in R[I^{d+2}] \setminus R[J] = \mathcal{F}^{d+1}(A, \mathbb{Z}/N\mathbb{Z}) \setminus R[J].$$

Since f is killed by I^{d+2} and not by J, we must have

$$(\textstyle\int f)\omega = \omega f \neq 0,$$

and thus $\int f \neq 0$. So $\sigma(A, \mathbb{Z}/N\mathbb{Z}) < d + 1$. □

3.2. **An Upper Bound on $\sigma(A, B)$.**

Proposition 3.8. *Let $N, a_1, \ldots, a_N, b \in \mathbb{Z}^+$. Then for any commutative group B,*

$$\sigma(\bigoplus_{i=1}^{N} \mathbb{Z}/a_i\mathbb{Z}, B) \leq \sum_{i=1}^{N}(a_i - 1) - 1.$$

Proof. Put $A = \bigoplus_{i=1}^{N} \mathbb{Z}/a_i\mathbb{Z}$. If B does not have finite exponent, then by Lemma 2.3 we have $\sigma(A, B) = -\infty$ and the result holds trivially. So we may assume that B has finite exponent. Then using Proposition 2.4 we reduce to the case in which A and B are both p-groups for some prime number p, so we may suppose that $A = \bigoplus_{i=1}^{N} \mathbb{Z}/p^{e_i}\mathbb{Z}$. If $\exp(B) = p^b$, then using Lemma 2.6b), Lemma 2.5b), Corollary 3.3 and Theorem 2.1a), we get

$$\sigma(A, B) = \sigma(A, \mathbb{Z}/p^b\mathbb{Z}) \leq \sigma(A, \mathbb{Z}/p\mathbb{Z})$$

$$= \delta(A, \mathbb{Z}/p\mathbb{Z}) - 1 = \sum_{i=1}^{N}(p^{e_i} - 1) - 1 = \sum_{i=1}^{N}(a_i - 1) - 1. \qquad \square$$

As the proof shows, the upper bound on $\sigma(A, B)$ given in Proposition 3.8 is an equality when A is a p-group and B has exponent p. We will see that equality also holds when A has exponent p and $\sigma(A, B) \geq 0$: this is Theorem 5.1.

Example 3.9. *Take $A = B = \mathbb{Z}/4\mathbb{Z}$. Proposition 3.8 gives $\sigma(\mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}) \leq 2$, while by Theorem 2.7 we have $\sigma(\mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}) = 0$. This is the minimal example in which strict inequality occurs in Proposition 3.8 Our next result (Theorem 4.2) implies that the inequality in Proposition is strict when $A = \mathbb{Z}/p^a\mathbb{Z}$ and $B = \mathbb{Z}/p^b\mathbb{Z}$ for any prime p and integers $2 \leq b \leq a$.*

4. Computing $\sigma(A, B)$ when A is cyclic

In this section we will compute the invariant $\sigma(A, B)$ when A is a finite cyclic group and B is a commutative group of finite exponent. By Lemma 2.5e) we have $\sigma(A, B) = \sigma(A, \mathbb{Z}/\exp(B)\mathbb{Z})$ so we may assume that B is also finite cyclic. Then §3 further reduces us to the case in which A and B are p-primary groups. Thus we are left to compute $\sigma(\mathbb{Z}/p^a\mathbb{Z}, \mathbb{Z}/p^b\mathbb{Z})$ for $a, b \in \mathbb{Z}^+$.

We need one preliminary. let $k \in \mathbb{Z}^+$, and consider the function

$$x \mapsto \binom{x}{k} \pmod{p^b} : \mathbb{Z} \to \mathbb{Z}/p^b\mathbb{Z}.$$

It is easy to see that this function descends to $\mathbb{Z}/p^a\mathbb{Z}$ for some $a \in \mathbb{Z}^+$: indeed, since $\binom{x}{k}$ is an polynomial with integer coefficients divided by $k!$, we may take $a = b + v_p(d!)$. However one can usually take a smaller value for a than this. Indeed, the minimal a for each b and k is known:

Theorem 4.1. *Let p a prime, and let $k, b \in \mathbb{Z}^+$. The least $N \in \mathbb{Z}^+$ such that*

$$\forall x \in \mathbb{Z}, \binom{x+N}{k} \pmod{p^b} = \binom{x}{k} \pmod{p^b}$$

is $p^{b+\lfloor \log_p k \rfloor}$.

Proof. This is [Fr67, Thm. 4.8].[5] □

Theorem 4.2. *Let p be a prime, and let $a, b \in \mathbb{Z}^+$.*

a) *If $a < b$, then $\sigma(\mathbb{Z}/p^a\mathbb{Z}, \mathbb{Z}/p^b\mathbb{Z}) = -\infty$.*
b) *If $a \geq b$, then $\sigma(\mathbb{Z}/p^a\mathbb{Z}, \mathbb{Z}/p^b\mathbb{Z}) = p^{a-b+1} - 2$.*

Proof. a) If $a < b$, then $\sigma(\mathbb{Z}/^a\mathbb{Z}, \mathbb{Z}/p^b\mathbb{Z}) = -\infty$ by Lemma 2.3.
b) Suppose $1 \leq b \leq a$. For any $d \in \mathbb{N}$, consider the function

$$\tilde{B}_d : \mathbb{Z} \to \mathbb{Z}/p^b\mathbb{Z},\ x \mapsto \binom{x}{d} \pmod{p^b}.$$

Theorem 4.1 implies that for all $0 \leq d \leq p^{a-b+1} - 1$, the function

$$\tilde{B}_d : \mathbb{Z} \to \mathbb{Z}/p^b\mathbb{Z},\ x \mapsto \binom{x}{d} \pmod{p^b}$$

is p^a-periodic, so it descends to a function

$$B_d : \mathbb{Z}/p^a\mathbb{Z} \to \mathbb{Z}/p^b\mathbb{Z},$$

but the function $\tilde{B}_{p^{a-b+1}}$ is not p^a-periodic. It follows that for all $0 \leq n \leq p^{a-b+1}-1$, the functions $B_0, \ldots, B_n$ form a basis for the $\mathbb{Z}/p^b\mathbb{Z}$-module $\mathcal{F}^n(\mathbb{Z}/p^a\mathbb{Z}, \mathbb{Z}/p^b\mathbb{Z})$ of functions $f : \mathbb{Z}/p^a\mathbb{Z} \to \mathbb{Z}/p^b\mathbb{Z}$ of functional degree at most n. This in turn implies that for all $0 \leq n \leq p^{a-b+1} - 1$ we have $\sigma(\mathbb{Z}/p^a\mathbb{Z}, \mathbb{Z}/p^b\mathbb{Z}) \geq n$ if and only if $\int B_d = 0$ for all $0 \leq d \leq n$. We claim that $\int B_d = 0$ for all $0 \leq d \leq p^{a-b+1} - 2$ but $\int B_{p^{a-b+1}-1} \neq 0$, which will complete the proof.

By Corollary 3.5, for $0 \leq d \leq p^{a-b+1}-1$ we have $\int B_d = 0$ if and only if $B_d = \Delta_1 g$ for some $g : \mathbb{Z}/p^a\mathbb{Z} \to \mathbb{Z}/p^b\mathbb{Z}$. Pulling back by the quotient map $q : \mathbb{Z} \to \mathbb{Z}/p^a\mathbb{Z}$ induces an injective $\mathbb{Z}/p^b\mathbb{Z}[\mathbb{Z}]$-module homomorphism N

$$q^* : (\mathbb{Z}/p^b\mathbb{Z})^{\mathbb{Z}/p^a\mathbb{Z}} \hookrightarrow (\mathbb{Z}/p^b\mathbb{Z})^{\mathbb{Z}},$$

which means that we may view functions $f : \mathbb{Z}/p^a\mathbb{Z} \to \mathbb{Z}/p^b\mathbb{Z}$ as p^a-periodic functions $F : \mathbb{Z} \to \mathbb{Z}/p^b\mathbb{Z}$, compatibly with the derivative operator $\Delta_1 = [1] - [0]$. For all $d \in \mathbb{N}$ we have

$$\Delta_1 \tilde{B}_{d+1} = \tilde{B}_d.$$

It follows that for all $0 \leq d \leq p^{a-b+1} - 2$ we have

$$\Delta_1 B_{d+1} = B_d,$$

so $\int B_d = 0$ and thus $\sigma(\mathbb{Z}/p^a\mathbb{Z}, \mathbb{Z}/p^b\mathbb{Z}) \geq p^{a-b+1} - 2$. On the other hand, since $\Delta_1 \tilde{B}_{p^{a-b+1}} = \tilde{B}_{p^{a-b+1}-1}$, every function $G : \mathbb{Z} \to \mathbb{Z}/p^b\mathbb{Z}$ with $\Delta_1 G = \tilde{B}_{p^{a-b+1}-1}$ is of the form $\tilde{B}_{p^{a-b+1}} + C$ for some $C \in \mathbb{Z}/p^b\mathbb{Z}$. Since none of these functions are p^a-periodic, the function $B_{p^{a-b+1}-1}$ is not a derivative, so $\int B_{p^{a-b+1}-1} \neq 0$. □

5. Computing $\sigma((\mathbb{Z}/p\mathbb{Z})^N, \mathbb{Z}/p^b\mathbb{Z})$

5.1. **Statement of the Result.** In this section we compute $\sigma((\mathbb{Z}/p\mathbb{Z})^N, \mathbb{Z}/p^b\mathbb{Z}))$ for all $N, b \in \mathbb{Z}^+$.

Theorem 5.1. *Let p be a prime, and let $b, N \in \mathbb{Z}^+$.*

a) *If $N < b$, then $\sigma((\mathbb{Z}/p\mathbb{Z})^N, \mathbb{Z}/p^b\mathbb{Z}) = -\infty$.*
b) *If $N \geq b$, then $\sigma((\mathbb{Z}/p\mathbb{Z})^N, \mathbb{Z}/p^b\mathbb{Z}) = N(p-1) - 1$.*

[5] Fray writes "Although this result and the corresponding one for fixed k are known, references on them are not readily available."

Part a) follows from Lemma 2.3, while the upper bound in part b) comes from Proposition 3.8. The lower bound in part b) is a consequence of the following result:

Theorem 5.2. *Let p be a prime, and let $N \in \mathbb{Z}^+$. There is $C_p(N) \in \mathbb{Z} \setminus p\mathbb{Z}$ such that in the group ring $\mathbb{Z}[(\mathbb{Z}/p\mathbb{Z})^N]$ we have*

$$C_p(N)\left(\sum_{x \in (\mathbb{Z}/p\mathbb{Z})^N} [x] - p^N\right) \in I^{N(p-1)}.$$

More precisely, we may take

$$C_p(N) \coloneqq \begin{cases} 1 & N = 1 \\ \prod_{d=2}^{N}(1 - p^{d-1}) & N \geq 2 \end{cases}.$$

Assuming Theorem 5.2, let $1 \leq b \leq N$. Under the reduction modulo p^b homomorphism $\mathbb{Z}[(\mathbb{Z}/p\mathbb{Z})^N] \to \mathbb{Z}/p^b\mathbb{Z}[(\mathbb{Z}/p\mathbb{Z})^N]$ the augmentation ideal of the first ring maps onto the augmentation ideal of the second ring; denoting the augmentation ideal of $\mathbb{Z}/p^b\mathbb{Z}[(\mathbb{Z}/p\mathbb{Z})^N]$ by I_{p^b} and once again setting

$$\omega \coloneqq \sum_{x \in (\mathbb{Z}/p\mathbb{Z})^N} [x],$$

Theorem 5.2 gives

$$C_p(N)\sigma \in I_{p^b}^{N(p-1)},$$

which implies $\omega \in I_{p^b}^{N(p-1)}$ since $C_p(N)$ is a unit in $\mathbb{Z}/p^b\mathbb{Z}[(\mathbb{Z}/p\mathbb{Z})^N]$. According to Theorem 3.7, since $\omega \in I_{p^b}^{N(p-1)}$, we have $\sigma((\mathbb{Z}/p\mathbb{Z})^N, \mathbb{Z}/p^b\mathbb{Z}) \geq N(p-1) - 1$.

We will prove Theorem 5.2 by induction on N. We treat the base case, then give a linear algebraic result, then use that result to prove the induction step.

5.2. **The Base Case.** We work in the group ring $\mathbb{Z}[\mathbb{Z}/p\mathbb{Z}]$, with augmentation ideal I. Put

$$\alpha \coloneqq \sum_{i=1}^{p-1} ([i] - [0])^{p-1} \in \mathbb{Z}[\mathbb{Z}/p\mathbb{Z}].$$

Evidently α lies in I^{p-1}. On the other hand, the multiplicative group $U(p) = (\mathbb{Z}/p\mathbb{Z})^\times$ acts on $\mathbb{Z}[\mathbb{Z}/p\mathbb{Z}]$ by ring automorphisms, such that for $u \in (\mathbb{Z}/p\mathbb{Z})^\times$, and $x \in \mathbb{Z}/p\mathbb{Z}$ we have $u[x] = [ux]$. Evidently α lies in the invariant subring $\mathbb{Z}[\mathbb{Z}/p\mathbb{Z}]^{U(p)}$, which is the ring of *almost constant* elements $\eta = \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \eta_x[x]$ such that $\eta_x = \eta_y$ for all $x, y \neq 0$. The almost constant elements are precisely the $\mathbb{Z}$-linear combinations of ω and $[0]$, so there are $m, n \in \mathbb{Z}$ such that

$$\alpha = m\omega + n[0].$$

Since $0 = \varphi(\alpha) = mp + n$ and the coefficient of $[0]$ in α is $(p-1)(-1)^{p-1}$, we find:

$$\omega - p = \omega - p[0] = (-1)^p\alpha \in I^{p-1}.$$

Thus in the notation of Theorem 5.2, we may indeed take $C_p(1) = 1$.

5.3. **A bijection of Grassmannians.** Let F be a field, and let $V_{/F}$ be an N-dimensional vector space. For $1 \leq d \leq n-1$, let $\mathbb{G}_d(V)$ be the set of d-dimensional linear subspaces of V. Recall that there is a bijection from $\mathbb{G}_d(V)$ to $\mathbb{G}_{N-d}(V)$: let $V^\vee = \mathrm{Hom}_F(V, F)$ be the dual space. Then

$$P : \mathbb{G}_d(V^\vee) \to \mathbb{G}_{N-d}(V),\ W \mapsto P(W) \coloneqq \bigcap_{\ell \in W} \mathrm{Ker}(\ell)$$

is a bijection, so if $\iota : V \to V^\vee$ is a vector space isomorphism then

$$\Phi : \mathbb{G}_d(V) \xrightarrow{\mathbb{G}_d(\iota)} \mathbb{G}_d(V^\vee) \xrightarrow{\Phi} \mathbb{G}_{N-d}(V)$$

is a bijection. An isomorphism $\iota : V \to V^\vee$ comes in particular from any nondegenerate symmetric bilinear form $\langle , \rangle$ on V: $v \mapsto \langle v, \cdot \rangle$. If $V = F^N$ one can take the standard dot product, and then the map Φ is just

$$W \in \mathbb{G}_d(V) \mapsto W^\perp \coloneqq \{v \in F^N \mid \forall w \in W,\ v \cdot w = 0\}.$$

When $F = \mathbb{R}$ this bijection has a desirable additional property: for all $W \in \mathbb{G}_d(V)$ we have $W \cap W^\perp = \{0\}$. For a symmetric bilinear form $\langle , \rangle$ on V, the associated bijection Φ has the property $W \cap \Phi(W) = \{0\}$ if and only if the bilinear form is anisotropic: for all $v \in V$, $\langle v, v \rangle = 0$ implies $v = 0$. However, depending upon F and N, an N-dimensional F-vector space may or may not admit an anisotropic symmetric bilinear form. In particular, such a form does not exist over a finite field F unless $N \leq 2$. Nevertheless we have the following result.

Proposition 5.3. *Let $N, d \in \mathbb{Z}$ with $1 \leq d < N$. For any field F, there is a bijection*

$$\Phi : \mathbb{G}_d(F^N) \to \mathbb{G}_{N-d}(F^N)$$

such that $W \cap \Phi(W) = \{0\}$ for all $W \in \mathbb{G}_d(F^N)$.

Proof. Consider the bipartite graph $\mathcal{G} = (V_1, V_2, E)$ where $V_1 = \mathbb{G}_d(F^N)$, $V_2 = \mathbb{G}_{N-d}(F^N)$ and there is an edge connecting $W \in \mathbb{G}_d(F^N)$ to $X \in \mathbb{G}_{N-d}(F^N)$ if and only $W \cap X = \{0\}$. The desired result is equivalent to the existence of a perfect matching in $\mathcal{G}$: a bijection $\Phi : V_1 \to V_2$ such that $x \sim \Phi(x)$ for all $x \in V_1$.
Case 1: $F = \mathbb{F}_q$ is finite. In this case we will apply Hall's Marriage Theorem [IAM, Thm. 9.46] to obtain a semi-perfect matching $\Phi : V_1 \to V_2$, i.e., an injection such that for all $v \in V_1$ we have that $\Phi(v)$ is adjacent to v. Since V_1 and V_2 are finite sets of the same cardinality, this gives the desired bijection.

For $W \in \mathbb{G}_d(\mathbb{F}_q^N)$, the number of $X \in \mathbb{G}_{N-d}(\mathbb{F}_q^N)$ such that $W \cap X = \{0\}$ is:[6]

$$\frac{(q^N - q^d) \cdots (q^N - q^{N-1})}{(q^{N-d} - 1) \cdots (q^{N-d} - q^{N-d-1})} = q^{d(N-d)}.$$

Replacing d with $N - d$, we get: for each $X \in \mathbb{G}_{N-d}(\mathbb{F}_q^N)$, the number of $W \in \mathbb{G}_d(\mathbb{F}_q^N)$ such that $W \cap X = \{0\}$ is also $q^{d(N-d)}$. Thus $\mathcal{G}$ is a $q^{d(N-d)}$-regular graph. For any nonempty subset $S \subseteq V_1$, the number of edges with a vertex lying in S is $q^{d(N-d)} \cdot \#S$. So if the set $N(S) = \{v \in V_2 \mid \text{ some vertex in } S \text{ is adjacent to } v\}$ had size less than $\#S$, then by the Pigeonhole Principle some vertex in $N(S)$ would be adjacent to more than $q^{d(N-d)}$ vertices in S, contradicting the regularity of the graph. Thus Hall's Marriage Theorem applies.

[6]The numerator is the number of ordered bases for such an X and the denominator is $\#\,\mathrm{GL}_{N_d}(\mathbb{F}_q)$.

Case 2: F is infinite, say of cardinality κ. In this case the set of edges containing a given vertex of $\mathcal{G}$ has cardinality κ.[7] So it suffices to show that any κ-regular bipartite graph (V_1, V_2, E) with $\#V_1 = \#V_2 = \kappa$ has a perfect matching. This can be shown by a transfinite back-and-forth argument. Let α be the least ordinal of cardinality κ. We may identify V_1 with $\alpha \times \{1\}$ and V_2 with $\alpha \times \{2\}$. We define a transfinite process with two stages for each $\beta \in \alpha$, i.e., for each ordinal $0 \leq \beta < \alpha$. At Stage β, part one, if the element $(\beta, 1)$ of V_1 has not been matched at any earlier stage, we match it with the smallest unmatched element of V_2; otherwise we do nothing. At Stage β, part two we do exactly the same with the roles of V_2 and V_1 reversed. At any stage β of the process we have used at most $2\#\beta < \kappa$ edges, so these matchings are always possible. In the end we get a perfect matching. □

Remark 5.4. *A nearly identical argument shows that for $1 \leq d < N$ and any field F, there is a bijection*

$$\Psi : \mathbb{G}_d(F^N) \to \mathbb{G}_{N-d}(F^N)$$

such that $W \cap \Phi(W) \supsetneq \{0\}$ for all $W \in \mathbb{G}_d(F^N)$. In particular, taking $d = 1$, we get that there is a bijection Ψ between lines in F^N and hyperplanes in F^N such that $\ell \in \Psi(\ell)$ for all lines ℓ. Even in $\mathbb{R}^3$ this does not seem immediately obvious.

5.4. **The Induction Step.** Let $N \geq 2$, and put $V \coloneqq (\mathbb{Z}/p\mathbb{Z})^N$. We call elements of $\mathbb{G}_1(V)$ *lines* and elements of $\mathbb{G}_{N-1}(V)$ *hyperplanes*.

Inductively, we may suppose that there is $C_p(N-1) \in \mathbb{Z} \setminus p\mathbb{Z}$ such that for any hyperplane H we have

$$C_p(N-1)(\sum_{x \in H}[x] - p^{N-1}) \in I_H^{(p-1)(N-1)} \subset I^{(p-1)(N-1)}.$$

Here I_H is the augmentation ideal of $\mathbb{Z}[H]$, which under the natural injective ring homomorphism $\mathbb{Z}[H] \hookrightarrow \mathbb{Z}[V]$ is mapped into the augmentation ideal I of $\mathbb{Z}[V]$. By Proposition 5.3 there is a bijection $\ell \mapsto H(\ell)$ from the set of lines in $(\mathbb{Z}/p\mathbb{Z})^N$ to the set of hyperplanes in $(\mathbb{Z}/p\mathbb{Z})^N$ such that we have $\ell \cap H(\ell) = \{0\}$ for all lines ℓ. Now we put

$$\alpha_\ell = C_p(N-1)\left(\sum_{x \in \ell}[x] - p\right)\left(\sum_{y \in H(\ell)}[y] - p^{N-1}\right) \in \mathbb{Z}[V]$$

and

$$\alpha \coloneqq \sum_{\ell \in \mathbb{G}_1(V)} \alpha_\ell.$$

It is clear that $\alpha \in I^{N(p-1)}$. We wish to show that

$$\alpha = C_p(N)(\sum_{x \in V}[x] - p^N)$$

[7] One can see this, for instance, as follows: for $W \in \mathbb{G}_d(F^N)$, let $v_1, \ldots, v_d$ be a basis of W, and let $w_{d+1}, \ldots, w_{N-1}$ be such that $v_1, \ldots, v_d, w_{d+1}, \ldots, w_{N-1}$ is linearly independent. Then for every $\omega \in F^N$ that is nonzero in the quotient $\overline{V} = F^N/\langle v_1, \ldots, v_d, w_{d+1}, \ldots, w_{N-1}\rangle$, we have that $X_\omega = \langle w_{d+1}, \ldots, w_{N-1}, \omega\rangle$ is an $N-d$-dimensional subspace such that $W \cap X_\omega = \{0\}$. Moreover $X_\omega = X_{\omega'}$ if and only if $q(\omega) = q(\omega')$, where $q : V \to \overline{V}$ is the quotient map. But $\overline{V}$ is a one-dimensional F-vector space, hence has cardinality κ. Since $\#\mathbb{G}_d(F^N) = \kappa$ for all $1 \leq d < N$, this is the largest possible degree. Alternately, for each $W \in \mathbb{G}_d(F^N)$, the set of $X \in \mathbb{G}_{N-d}(F^N)$ such that $W \cap X = \{0\}$ is the set of F-rational points of a nonempty Zariski-open subset of $\mathbb{G}_{N_d}$, which is a rational variety, and every such set has cardinality κ.

for some $C_p(N) \in \mathbb{Z} \setminus p\mathbb{Z}$. We claim that $\alpha = \sum_{x \in V} \alpha_x [x]$ is almost constant: i.e., for all $x, y \in V \setminus \{0\}$, we have $\alpha_x = \alpha_y$. Assuming the claim: the almost constant elements are precisely the invariants $\mathbb{Z}[V]^{\mathrm{GL}(V)}$, which consist of $\mathbb{Z}$-linear combinations of $\omega = \sum_{x \in V} [x]$ and $[0] = 1$. So there are $m, n \in \mathbb{Z}$ such that

$$\alpha = m\omega + n[0].$$

For each $\ell \in \mathbb{G}_1(V)$, the coefficient of $[0]$ in α_ℓ is $C_p(N-1)(p^{N-1}-1)(p-1)$, so the coefficient of $[0]$ in α is

$$C_p(N-1)(p^{N-1}-1)(p-1) \cdot \#\mathbb{G}_1(V) = C_p(N-1)(p^N-1)(p^{N-1}-1).$$

We have

$$0 = \varphi(\alpha) = mp^N + n,$$

so

$$\alpha = m(\omega - p^N).$$

Since also

$$m + n = \alpha_0 = C_p(N-1)(p^N-1)(p^{N-1}-1),$$

we get

$$\alpha = (1 - p^{N-1})C_p(N-1).$$

Thus, for $N \geq 2$ if we take

$$C_p(N) \coloneqq \prod_{d=2}^{N} (1 - p^{d-1}) \in \mathbb{Z} \setminus p\mathbb{Z},$$

then

$$\alpha = C_p(N)(\omega - p^N) \in I^{N(p-1)}.$$

Finally we must establish the claim that α is almost constant. For $\ell \in \mathbb{G}_1(V)$ and $x \in V$, the coefficient $\alpha_{\ell,x}$ of $[x]$ in α_x takes on only four possible values:
• When $x = 0$ it takes the value $c_1 = C_p(N-1)(p^{N-1}-1)(p-1)$.
• When x lies in $\ell \setminus \{0\}$ (hence $x \notin H(\ell)$) it takes the value $c_2 = C_p(N-1)(1-p^{N-1})$.
• When x lies in $H(\ell) \setminus \{0\}$ (hence $x \notin \ell$) it takes the value $c_3 = C_p(N-1)(1-p)$.
• When x lies in neither ℓ nor $H(\ell)$ it takes the value $c_4 = C_p(N-1)$. The point of this is that the integers c_1, c_2, c_3, c_4 do not depend on ℓ.

Now let $x \in V \setminus \{0\}$. The number of lines ℓ containing x is 1, while the number of lines ℓ such that x lies in $H(\ell)$ is the number of hyperplanes containing x, which is $\#\mathbb{G}_{N-2}(V/\langle x \rangle) = \frac{p^{N-1}-1}{p-1}$. The number of lines ℓ such that $x \notin (\ell \cup H(\ell))$ is one less than the number of hyperplanes not containing x – every hyperplane H is of the form $H(\ell)$ for a unique line ℓ, and the extra condition that $x \notin \ell$ rules out precisely the hyperplane $H(\langle x \rangle)$ – so is $\frac{p^N-1}{p-1} - \frac{p^{N-1}-1}{p-1} - 1$. So for $x \neq 0$, we have

$$\alpha_x = c_2 + \frac{p^{N-1}-1}{p-1} c_3 + \left(\frac{p^N-1}{p-1} - \frac{p^{N-1}-1}{p-1} - 1 \right) c_4,$$

establishing that α is almost constant and completing the proof.

6. The Ax Effect

6.1. **Introduction.** Consider the following result:

Theorem 6.1 (Ax Effect)**.** *Let $q = p^a$ be a prime power. If we fix $r, \dots, d_r \in \mathbb{Z}^+$, then there is a function*

$$V : \mathbb{Z}^+ \to \mathbb{Z}^+$$

such that for all $b \in \mathbb{Z}^+$, if $n \geq V(b)$, then every polynomial system $P_1, \dots, P_r \in \mathbb{F}_q[t_1, \dots, t_n]$ with $\deg(P_j) = d_r$ for all j has

$$\operatorname{ord}_p \left(\#\{x \in \mathbb{F}_q^n \mid f_1(x) = \ldots = f_r(x) = 0\} \right) \geq b.$$

The Ax Effect says that if we hold the number and degrees of the polynomials fixed and increase the number of variables, the guaranteed p-adic divisibility on the size of the solution set grows arbitrarily large. This is an immediate consequence of Theorem 1.1b). We call it the "Ax Effect" because it is also a consequence of a weaker form of Theorem 1.1b) established in J. Ax's 1964 work [Ax64, p. 260, Cor.].

In this section we will extend the Ax Effect to any finite rng.

Theorem 6.2 (Ring-Theoretic Ax Effect)**.** *Let R be a finite rng. Fix positive integers $r, d_1, \dots, d_r$. For each prime $p \mid \#R$, there is a function $V : \mathbb{Z}^+ \to \mathbb{Z}^+$ such that for all $b \in \mathbb{Z}^+$, if $n \geq V(b)$, then all polynomial expressions $f_1, \dots, f_r$ in n indeterminates over R with $\deg(f_j) = d_j)$ for all j, we have*

$$\operatorname{ord}_p \left(\#\{x \in R^n \mid f_1(x) = \ldots = f_r(x) = 0\} \right) \geq b.$$

Indeed, we may take

$$V(b) = \max \left(b, \frac{\delta^0((R,+), \mathbb{Z}/p^b\mathbb{Z}) \left(\sum_{j=1}^r \operatorname{fdeg}(f_j) \right) + 1}{p-1} \right).$$

Remark 6.3. *Certainly in Theorem 6.2 we need $p \mid \#R$: for a prime number $\ell \nmid \#R$, if we take $d_1 = \ldots = d_r = 1$, then the solution locus is a coset of a subgroup of $(R^n, +)$ so has size not divisible by ℓ. It seems likely that* for all $r, d_1, \dots, d_r \in \mathbb{Z}^+$ *and any $\ell \nmid \#R$, there is a system of r polynomials with degrees $d_1, \dots, d_r$ and solution locus of size not divisible by ℓ.*

As in the prior work of Aichinger–Moosbauer and Clark–Schauz [AM21], [CS23a], this ring-theoretic result is an immediate consequence of purely group-theoretic results that we now discuss. Here is the key:

Theorem 6.4 (Group-Theoretic Prime Ax Theorem)**.** *Let A be a finite commutative group. Let $r \in \mathbb{Z}^+$. For each $1 \leq j \leq r$, let B_j be a finite commutative group, and let $f_j : A \to B_j$ be a map of finite functional degree. Put*

$$Z = Z(f_1, \dots, f_r) \coloneqq \{x \in A \mid \forall 1 \leq j \leq r,\ f_j(x) = 0\}.$$

Let p be a prime dividing each of $\#A$, $\#B_1, \dots, \#B_r$, and let $b \in \mathbb{Z}^+$. If

$$\sum_{j=1}^r \delta^0(B_j, \mathbb{Z}/p^b\mathbb{Z}) \operatorname{fdeg}(f_j) \leq \sigma(A[p^\infty], \mathbb{Z}/p^b\mathbb{Z}), \tag{6}$$

then

$$p^b \mid \#Z(f_1, \dots, f_r).$$

Remarkably, the proof of Theorem 6.4 is a close analogue of Ax's ten line proof of Theorem 1.1a). More precisely, this proof generalizes seven of the ten lines of Ax's proof; the other three lines compute the quantities δ° and σ appearing in (6) in the cases needed to prove Theorem 1.1a).

The quantities $\delta^0(B_j, \mathbb{Z}/p^b\mathbb{Z})$ appearing in Theorem 6.4 are known in all cases: see Theorem 2.1. Although we do not know the exact value of $\sigma(A[p^\infty], \mathbb{Z}/p^b\mathbb{Z})$ in all cases, we know enough about it to deduce the following result.

Theorem 6.5 (Group-Theoretic Ax Effect)**.** *Let p be a prime, and let A and B be finite commutative groups, each of size divisible by p. For each $r, d_1, \ldots, d_r \in \mathbb{Z}^+$, there is a function $V : \mathbb{Z}^+ \to \mathbb{Z}^+$ such that for all $b \in \mathbb{Z}^+$, if $N \geq V(b)$ and*

$$f_1, \ldots, f_r : A^N \to B$$

are functions with $\operatorname{fdeg}(f_j) = d_j$ for all j, then

$$p^b \mid \{x \in A^N \mid f_1(x) = \ldots = f_r(x) = 0\}.$$

Indeed, we may take

$$V(b) = \max\left(b, \frac{\delta^0(B, \mathbb{Z}/p^b\mathbb{Z})\left(\sum_{j=1}^r \operatorname{fdeg}(f_j)\right) + 1}{p-1}\right).$$

Theorem 6.2 follows immediately from Theorem 6.5 using (2).

We prove Theorem 6.4 in §6.2 and Theorem 6.5 in §6.3. In §6.4 we make some further remarks about these bounds; in particular we will see that a special case of Theorem 6.4 is even more closely connected to Ax's work towards Theorem 1.1b) than the qualitative consequence Theorem 6.1 suggests.

6.2. **Proof of Theorem 6.4.** Note that this argument is longer than seven lines because the result has been stated in maximum generality, making it a bit notationally heavy. We hope that the underlying simplicity of the argument is not obscured.

We put $B \coloneqq \bigoplus_{j=1}^r B_j$. For a commutative group X, we put

$$X_p \coloneqq X[p^\infty].$$

Step 1: Suppose A and B are p-groups. Let $\chi : B \to \mathbb{Z}/p^b\mathbb{Z}$ map 0 to 1 and every other element to 0. Then for all $x \in A$, we have

$$\chi(f_1(x), \ldots, f_r(x)) = \begin{cases} 1 & \text{if } f_j(x) = 0 \text{ for all } j \\ 0 & \text{otherwise} \end{cases},$$

so we have $\int \chi(f_1, \ldots, f_r) = \#Z(f_1, \ldots, f_r)$ and thus

$$\#Z(f_1, \ldots, f_r) \equiv \int \chi(f_1, \ldots, f_r) \pmod{p^b}.$$

For commutative groups $\mathcal{B}_1, \ldots, \mathcal{B}_r$ and C, suppose we have a map

$$G : \bigoplus_{j=1}^r \mathcal{B}_j \to C.$$

For $1 \leq J \leq r$, the **Jth partial functional degree** $\operatorname{pfdeg}_J(G)$ [AM21, Definition 5.1] is the supremum of the functional degrees of all functions $g : \mathcal{B}_J \to C$

obtained from G by evaluating every argument but the Jth at an element $x' \in \bigoplus_{j\in\{1,\dots,r\}\setminus\{J\}} \mathcal{B}_j$. We recall [AM21, Thm. 5.3]: if also for all $1 \le j \le r$ we have $f_j : A \to \mathcal{B}_j$, then $G(f_1,\dots,f_r) : A \to C$ and

$$\operatorname{fdeg}(G(f_1,\dots,f_r)) \le \sum_{j=1}^{r} \operatorname{pfdeg}_j(G)\operatorname{fdeg}(f_j).$$

Therefore

$$\operatorname{fdeg}(G(f_1,\dots,f_r)) \le \sum_{j=1}^{r} \operatorname{pfdeg}_j(G)\operatorname{fdeg}(f_j) \le \sum_{j=1}^{r} \delta(B_j,\mathbb{Z}/p^b\mathbb{Z})\operatorname{fdeg}(f_j).$$

We now apply the above with $\mathcal{B}_j = B_j$ for all j and $G = \chi$. Since B_j is a finite p-group, every map from B_j to $\mathbb{Z}/p^b\mathbb{Z}$ has finite functional degree, and thus

$$\operatorname{fdeg}(\chi(f_1,\dots,f_r)) \le \sum_{j=1}^{r} \delta(B_j,\mathbb{Z}/p^b\mathbb{Z})\operatorname{fdeg}(f_j) = \sum_{j=1}^{r} \delta^\circ(B_j,\mathbb{Z}/p^{\mathbb{Z}})\operatorname{fdeg}(f_j) \le \sigma(A,\mathbb{Z}/p^b\mathbb{Z}).$$

It follows that $\int \chi(f_1,\dots,f_r) = 0$, completing the proof in this case.
Step 2: Since A and B are finite, we have

$$A = \bigoplus_{p\in\mathcal{P}} A_p \text{ and } B = \bigoplus_{p\in\mathcal{P}} \bigoplus_{j=1}^{r} (B_j)_p,$$

and these are all really finite direct sum decompositions. If X and Y are finite commutative groups and $f \in \mathcal{F}(X,Y)$, then for all $p \in \mathcal{P}$ we have $f(X_p) \subset Y_p$, and moreover, if we write f_p for $f|_{X_p} : X_p \to Y_p$ then $f = \bigoplus_p f_p$ and $\operatorname{fdeg}(f) = \max_p \operatorname{fdeg}(f_p)$ [AM21, Thm. 9.2]. Moreover we have for all j that

$$\delta^0(B_j,\mathbb{Z}/p^b\mathbb{Z}) = \delta((B_j)_p,\mathbb{Z}/p^b\mathbb{Z}).$$

So if $\mathcal{S}$ is the set of prime divisors of $\#A\cdot\#B$, then for all $p \in \mathcal{S}$ we have

$$Z(f_1,\dots,f_r) = \prod_{p\in\mathcal{S}} Z((f_1)_p,\dots,(f_r)_p). \tag{7}$$

Applying Step 1 to $\{(f_j)_p : A_p \to (B_j)_p\}_{j=1}^r$, we find that p^b divides the size of $Z((f_1)_p,\dots,(f_r)_p)$, which is one of the factors in the Cartesian product representation (7) for $Z(f_1,\dots,f_r)$, so $p^b \mid \#Z(f_1,\dots,f_r)$.

6.3. **Proof of the Group-Theoretic Ax Effect.** Let $p \in \mathcal{P}$, and let A and B be finite commutative groups each of size divisible by p. Fix $r, d_1,\dots,d_r, b \in \mathbb{Z}^+$. We must show that there is $V(b) \in \mathbb{Z}^+$ such that for all $N \ge V(b)$ and any $f_1,\dots,f_r : A^N \to B$ with $\operatorname{fdeg}(f_j) = d_j$ for all j, we have $p^b \mid \#Z(f_1,\dots,f_r)$.

By Theorem 6.4, we see that $p^b \mid \#Z(f_1,\dots,f_r)$ whenever

$$\delta^\circ(B,\mathbb{Z}/p^b\mathbb{Z})\left(\sum_{j=1}^{r}\operatorname{fdeg}(f_j)\right) \le \sigma(A[p^\infty]^N,\mathbb{Z}/p^b\mathbb{Z}).$$

Since $p \mid \#A$, we have an injective group homomorphism $(\mathbb{Z}/p\mathbb{Z})^N \hookrightarrow A[p^\infty]^N$, so by Lemma 2.5c) and Theorem 5.1, when $N \ge b$ we have

$$N(p-1)-1 = \sigma((\mathbb{Z}/p\mathbb{Z})^N,\mathbb{Z}/p^b\mathbb{Z}) \le \sigma(A[p^\infty]^N,\mathbb{Z}/p^b\mathbb{Z}).$$

It follows that $p^b \mid \#Z(f_1, \ldots, f_r)$ when

$$N \geq \max\left(b, \frac{\delta^0(B, \mathbb{Z}/p^b\mathbb{Z})\left(\sum_{j=1}^r \operatorname{fdeg}(f_j)\right) + 1}{p-1}\right),$$

completing the proof of Theorem 6.5.

6.4. **Remarks.** Let us take $b = 1$ in Theorem 6.4, and focus on the case of p-groups, so that we have finite commutative p-groups A, $B_1, \ldots, B_r$ and maps $\{f_j : A \to B_j\}_{j=1}^r$. To better compare with other results, we replace A by A^N for some $N \in \mathbb{Z}^+$ (this neither gains nor loses generality), so that we have maps $\{f_j : A^N \to B_j\}_{j=1}^r$. Then we get in particular that $\#Z(f_1, \ldots, f_r)$ is divisible by p if

$$\sum_{j=1}^r \delta(B_j, \mathbb{Z}/p\mathbb{Z}) \operatorname{fdeg}(f_j) \leq \delta(A^N, \mathbb{Z}/pZ) - 1 = N\delta(A, \mathbb{Z}/p\mathbb{Z}) - 1$$

i.e., if and only if

$$\sum_{j=1}^r \delta(B_j, \mathbb{Z}/p\mathbb{Z}) \operatorname{fdeg}(f_j) < N\delta(A, \mathbb{Z}/p\mathbb{Z}).$$

This result is slightly more general than Theorem 1.5:one recovers that result by taking all the groups $B_1, \ldots, B_r$ to be the same.[8] If we further take $A = B$, then we get that the number of simultaneous zeros of $f_1, \ldots, f_r : A^N \to A$ is divisible by p if $\sum_{j=1}^r \operatorname{fdeg}(f_j) < N$. This is [AM21, Thm. 12.3], which is a group-theoretic generalization of the Chevalley–Warning Theorem. But more than that, the proof given by Aichinger–Moosbauer (to which our proof reduces) is remarkably close to J. Ax's famous *ten line proof* of Chevalley–Warning.

It is interesting to see what the bound of Theorem 6.4 gives in the "classical case": let $A = (\mathbb{Z}/p\mathbb{Z})^a$ for some $a \in \mathbb{Z}^+$, let $N \in \mathbb{Z}^+$, and for maps

$$f_1, \ldots, fr : A^N \to A$$

we put

$$Z(f_1, \ldots, f_r) = \{x \in A^N \mid f_1(x) = \ldots = f_r(x) = 0\}.$$

Then Theorem 6.4 gives that for $b \in \mathbb{Z}^+$, we have $p^b \mid \#Z(f_1, \ldots, f_r)$ if

$$\sum_{j=1}^r \delta((\mathbb{Z}/p\mathbb{Z})^a, \mathbb{Z}/p^b\mathbb{Z}) \operatorname{fdeg}(f_j) \leq \sigma((\mathbb{Z}/p\mathbb{Z})^{aN}, \mathbb{Z}/p^b\mathbb{Z}).$$

We get that if $b \leq aN$, we have $p^b \mid \#Z(f_1, \ldots, f_r)$ if

$$b < a\left(\frac{N}{\sum_{j=1}^r \operatorname{fdeg}(f_j)} - 1\right) + 1$$

if and only if

$$b \leq \left\lceil a\left(\frac{N}{\sum_{j=1}^r \operatorname{fdeg}(f_j)} - 1\right)\right\rceil.$$

[8] Aichinger and Moosbauer's proof of [AM21, Thm. 12.2] would yield this more general result.

In particular, when $r = 1$ our bound is

$$\mathrm{ord}_p(\#Z(f) \geq \left\lceil a\left(\frac{N}{\mathrm{fdeg}(f)} - 1\right)\right\rceil.$$

When $r = 1$, the Ax–Katz bound was already proved by Ax: working over $\mathbb{F}_{p^a}$, it is

$$\mathrm{ord}_p(\#Z(f) \geq a\left\lceil \frac{N}{\deg(f)} - 1\right\rceil.$$

Thus when $r = a = 1$, this simple argument *does* prove Ax–Katz. When $r = 1$ and $a > 1$, our bound is overall incomparable to Ax's bound: it is weaker in that when $\deg(f) \nmid N$ because Ax's placement of the ceiling function is more favorable, but it is stronger in that the functional degree is equal to the p-weight degree of the Chevalley-reduced representative (see [CS23a, §4]).

But as mentioned above, Ax also gave a result [Ax64, p. 260, Cor.] for any system $f_1, \ldots, f_r$ of polynomials: putting $D \coloneqq \sum_{j=1}^r \deg(f_j)$, Ax showed

$$\mathrm{ord}_p(\#Z(f_1, \ldots, f_r)) \geq a\left\lceil \frac{N}{D} - 1\right\rceil.$$

Putting $\underline{D} \coloneqq \sum_{j=1}^r \mathrm{fdeg}(f_j)$, our bound is

$$\mathrm{ord}_p(\#Z(f_1, \ldots, f_r) \geq \left\lceil a\left(\frac{N}{\underline{D}} - 1\right)\right\rceil.$$

We end this section by mentioning that Theorem 6.2 is the first result of its kind: i.e., the first Ax–Katz type higher p-adic congruence for the size of the solution set of a polynomial system over an arbitrary finite rng R. The cases that had previously been addressed are precisely (i) when R is a finite field [Ax64], [Ka71], (ii) when R is a finite commutative principal ring [MR75], [Ka12], and (iii) when $(R, +)$ has exponent p [CS23a].

7. The Lifted Summation Constant

Let $N \in \mathbb{Z}^+$ and let $a_1, \ldots, a_N, b \in \mathbb{Z}^{\geq 2}$ be such that $a_N \mid a_{N-1} \mid \ldots \mid a_1$. We put

$$[\mathbf{a}] \coloneqq \prod_{i=1}^N \{0, 1, \ldots, a_i - 1\}.$$

For a commutative group B and a function $F : \mathbb{Z}^N \to B$, we put

$$\int_{[\mathbf{a}]} F \coloneqq \sum_{x \in [\mathbf{a}]} F(x).$$

We define the **lifted summation constant** $\tilde{\sigma}(\bigoplus_{i=1}^N \mathbb{Z}/a_i\mathbb{Z}, \mathbb{Z}/b\mathbb{Z})$ as the supremum of all $d \in \mathbb{N} \cup \{-\infty\}$ such that for all $F : \mathbb{Z}^N \to \mathbb{Z}$ with functional degree at most d, we have $b \mid \int_{[\mathbf{a}]} F$.

The following result is the analogue for $\tilde{\sigma}$ of Proposition 3.8.

Lemma 7.1. *We have* $\tilde{\sigma}(\bigoplus_{i=1}^N \mathbb{Z}/a_i\mathbb{Z}, \mathbb{Z}/b\mathbb{Z}) \leq \sum_{i=1}^N (a_i - 1) - 1 < \infty$.

Proof. Take $F : \mathbb{Z}^N \to \mathbb{Z}$ by $F(x) = \prod_{i=1}^N \binom{x_i}{a_i - 1}$. By [CS23a, §2.3] we have $\mathrm{fdeg}(F) = \sum_{i=1}^N a_i$. Moreover, for $x = (x_1, \ldots, x_N) \in [\mathbf{a}]$, we have

$$F(x) = \begin{cases} 1 & \text{if } x = (a_1 - 1, \ldots, a_N - 1) \\ 0 & \text{otherwise} \end{cases},$$

so $\int_{[\mathbf{a}]} F = 1$, which is not divisible by b. □

Lemma 7.2. *We have*

$$\tilde{\sigma}(\bigoplus_{i=1}^N \mathbb{Z}/a_i\mathbb{Z}, \mathbb{Z}/b\mathbb{Z}) \leq \sigma(\bigoplus_{i=1}^N \mathbb{Z}/a_i\mathbb{Z}, \mathbb{Z}/b\mathbb{Z}).$$

Proof. We suppose that $f : \bigoplus_{i=1}^N \mathbb{Z}/a_i\mathbb{Z} \to \mathbb{Z}/b\mathbb{Z}$ has functional degree at most $\tilde{\sigma}(\bigoplus_{i=1}^N \mathbb{Z}/a_i\mathbb{Z}, \mathbb{Z}/b\mathbb{Z})$. Let $q : \mathbb{Z}^N \twoheadrightarrow \bigoplus_{i=1}^N \mathbb{Z}/a_i\mathbb{Z}$ be the natural map. By [CS22, Lemma 3.9] we have

$$\mathrm{fdeg}(f \circ q) = \mathrm{fdeg}(f) \leq \tilde{\sigma}(\bigoplus_{i=1}^N \mathbb{Z}/a_i\mathbb{Z}, \mathbb{Z}/b\mathbb{Z}) < \infty,$$

so by [CS23a, §2.4] there is a function $F : \mathbb{Z}^N \to \mathbb{Z}$ such that $F \pmod{b\mathbb{Z}} = f \circ q$ and $\mathrm{fdeg}(F) = \mathrm{fdeg}(f \circ q) = \mathrm{fdeg}(f) \leq \tilde{\sigma}(\bigoplus_{i=1}^N \mathbb{Z}/a_i\mathbb{Z}, \mathbb{Z}/b\mathbb{Z})$. By definition of the lifted summation constant we have $b \mid \int_{[\mathbf{a}]} F$; since $[\mathbf{a}]$ is a set of coset representatives for $\bigoplus_{i=1}^N \mathbb{Z}/a_i\mathbb{Z}$ in $\mathbb{Z}^N$, this implies $\int f = 0$. □

Of course Lemma 7.1 follows from Proposition 3.8 and Lemma 7.2, but in the proof of Lemma 7.2 we needed to know that $\tilde{\sigma}$ is always finite, which Lemma 7.1 gives.

The analogue of Proposition 2.4 also holds for $\tilde{\sigma}$: namely if $p_1 < \ldots < p_r$ are the distinct primes divding $a_1 \cdots a_N \cdot b$ and for a finite commutative group X, X_i denotes the Sylow p_i-subgroup of X, then

$$\tilde{\sigma}(\bigoplus_{i=1}^N \mathbb{Z}/a_i\mathbb{Z}, \mathbb{Z}/b\mathbb{Z}) = \min_{1 \leq i \leq r} \tilde{\sigma}((\bigoplus_{i=1}^N \mathbb{Z}/a_i\mathbb{Z})_i, (\mathbb{Z}/b\mathbb{Z})_i).$$

We omit the proof. So as usual we are reduced to the case of commutative p-groups.

Wilson's proof of Theorem 1.1b) over the prime field $\mathbb{F}_p$ implicitly uses this lifted summation constant. Indeed, [Wi06, Lemma 4] is equivalent to the following result:

Lemma 7.3. *Let p be a prime number, and let $N, b \in \mathbb{Z}^+$ with $N \geq b$. Then*

$$\tilde{\sigma}((\mathbb{Z}/p\mathbb{Z})^N, \mathbb{Z}/p^b\mathbb{Z}) \geq (N - b + 1)(p - 1) - 1. \tag{8}$$

Proof. This is [CS23a, Lemma 3.1]. □

Combining Lemmas 7.3 and 7.2, we get Lemma 1.7a).

We end by showing some cases where $\tilde{\sigma} = \sigma$ and one important case where $\tilde{\sigma} < \sigma$.

• Suppose $a \geq b \geq 1$. From [CS23b, Prop. 2.2 and Lemma 2.3] we get

$$\tilde{\sigma}(\mathbb{Z}/p^a\mathbb{Z}, \mathbb{Z}/p^b\mathbb{Z}) = p^{a-b+1} - 2.$$

Combining with our Theorem 4.2 we deduce

$$\tilde{\sigma}(\mathbb{Z}/p^a\mathbb{Z}, \mathbb{Z}/p^b\mathbb{Z}) = \sigma(\mathbb{Z}/p^a\mathbb{Z}, \mathbb{Z}/p^b\mathbb{Z}).$$

In fact our proof of Theorem 4.2 applies verbatim to $\tilde{\sigma}$.

• It follows from [CS23b, Cor. 2.7] that

$$\tilde{\sigma}(\bigoplus_{i=1}^{N} \mathbb{Z}/p^{a_i}\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}) = \sum_{i=1}^{N} (p^{a_i} - 1) - 1.$$

By Corollary 3.3, we have

$$\sigma(\bigoplus_{i=1}^{N} \mathbb{Z}/p^{a_i}\mathbb{Z}, \mathbb{Z}/p\mathbb{Z})) = \delta(\bigoplus_{i=1}^{N} \mathbb{Z}/p^{a_i}\mathbb{Z}, \mathbb{Z}/p\mathbb{Z})) - 1 = \sum_{i=1}^{N} (p^{a_i} - 1) - 1,$$

so $\sigma = \tilde{\sigma}$ in this case as well.

• It follows from [CS23b, Cor. 2.8] that for $N \geq b \geq 1$ we have

$$\tilde{\sigma}((\mathbb{Z}/p\mathbb{Z})^N, \mathbb{Z}/p^b\mathbb{Z}) = (N - b + 1)(p - 1) - 1, \tag{9}$$

or in other words that equality holds in (8). However, by Theorem 5.1 we have

$$\sigma((\mathbb{Z}/p\mathbb{Z})^N, \mathbb{Z}/p^b\mathbb{Z}) = N(p - 1) - 1, \tag{10}$$

which shows that when $N \geq b \geq 2$ we have

$$\tilde{\sigma}((\mathbb{Z}/p\mathbb{Z})^N, \mathbb{Z}/p^b\mathbb{Z}) < \sigma((\mathbb{Z}/p\mathbb{Z})^N, \mathbb{Z}/p^b\mathbb{Z}).$$

References

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

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

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

[IAM] P.L. Clark, *Introduction to Advanced Mathematics.* `http://alpha.math.uga.edu/~pete/3200_supplemental.pdf`

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

[Cl-W] P.L. Clark, *Wilson's Theorem: an algebraic approach.* `alpha.math.uga.edu/~pete/wilson_easy.pdf`

[CS22] P.L. Clark and U. Schauz, *Functional degrees and arithmetic applications I: the set of functional degrees.* J. Algebra 608 (2022), 691–718.

[CS23a] P.L. Clark and U. Schauz, *Functional degrees and arithmetic applications II: the group-theoretic prime Ax–Katz Theorem.* `https://arxiv.org/abs/2305.01304`

[CS23b] P.L. Clark and U. Schauz, *Functional degrees and arithmetic applications III: beyond prime exponent.* Preprint.

[Fr67] R.D. Fray, *Congruence properties of ordinary and q-binomial coefficients.* Duke Math. J. 34 (1967), 467–480.

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

[HW] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers.* Sixth edition. Revised by D. R. Heath-Brown and J. H. Silverman. With a foreword by Andrew Wiles. Oxford University Press, Oxford, 2008.

[Ka49] I. Kaplansky, *Elementary divisors and modules.* Trans. Amer. Math. Soc. 66 (1949), 464–491.

[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.

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

[Mi03] G.A Miller, *A new proof of the generalized Wilson's theorem*. Ann. of Math. (2) 4 (1903), 188–190.

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

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

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

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