arXiv:2305.01304v1 [math.GR] 2 May 2023

函数次数与算术应用 II：群论素数 Ax-Katz 定理

PETE L. CLARK 和 UWE SCHAUZ

Abstract. 我们给出了 Ax-Katz 的 p-进同余式以及 Moreno-Moreno 的p-权重细化版本，该版本适用于特征为素数的任意有限交换环。我们从一个纯粹的群论结果推导出这一结论，该结果给出了映射系f_j 统同时零点个数的 p-进可除性的下界： $A \to B_j$ 这些映射从一个固定的“源”有限交换群 A （指数为 p ）映到多个变化的“目标”有限交换 p群 B_j。我们的证明结合了 Wilson 对 Ax-Katz 定理在 $\mathbb{F}_p$ 上的证明与 Aichinger-Moosbauer 的函数演算。

1. Introduction

这是这一系列论文中的第二篇，我们尝试综合并进一步发展 Wilson [Wi06] 以及 Aichinger 和 Moosbauer [AM21]的研究成果。在第一篇论文 [CS21] 中，我们运用 Weisman [We77] 和 Wilson [Wi06]的算术结果，解决了 Aichinger-Moosbauer 提出的一个纯代数问题；而本文则反其道而行：我们结合 [CS21] 中的代数研究与 Aichinger-Moosbauer 的函数演算，推导出算术结果。特别是，我们给出一个纯群论结果，它蕴含了 Ax-Katz 定理在素数有限域上多项式方程组情形下的结论 $\mathbb{F}_p$ ，以及 Moreno-Moreno 关于有限域上多项式方程组的定理 $\mathbb{F}_q$。

1.1. 符号与术语。我们用 $\mathcal{P}$ 表示（正）素数集合，用 $\mathbb{N}$ 表示非负整数集合，并令 $\mathbb{Z}^+ := \mathbb{N} \setminus \{0\}$。我们赋予该集合

$$\widetilde{\mathbb{N}} := \mathbb{N} \cup \{-\infty, \infty\}$$

按照最自然的全序，其中 $-\infty$ 是最小元素， ∞ 是最大元素。符号 $-\infty$ 也用作零多项式的次数，这解释了为什么我们在某些定理中将对象限定为非零多项式或函数。

全文中， $q = p^N$ 表示素数 p 的正整数次幂，而 $\mathbb{F}_q$ 表示阶为 q的“那个”（在同构意义下唯一的）有限域。对于 $n \in \mathbb{Z} \setminus \{0\}$，我们用 $\mathrm{ord}_q(n)$表示整除 n的 q 的最高次幂；此外，规定 $\mathrm{ord}_q(0) = \infty$。

本文中的环不一定是交换的。我们称环 R 为整域，当对所有 x、 $y \in R$、 $xy = 0$ 均可推出 $x = 0$ 或 $y = 0$时成立。非结合环类似于环，但不一定具有乘法单位元。如果 R、 R_1、……、 R_r 是集合，且每个集合 R_1、……、 R_r 都包含一个记作 0 的特定元素，并且如果 $f_1 : R^n \to R_1$、……、$f_r : R^n \to R_r$ 是函数（可能由多项式给出），我们还定义

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

1.2. Chevalley-Warning 与 Ax-Katz。我们首先回顾 Chevalley-Warning 与 Ax-Katz 的以下结果。

定理 1.1。设 $p \in \mathcal{P}$和 $q := p^N$。设 $f_1, \ldots, f_r \in \mathbb{F}_q[t_1, \ldots, t_n]$ 为非零多项式。若 $Z := Z_{\mathbb{F}_q^n}(f_1, \ldots, f_r)$ 且 $\sum_{j=1}^r \deg(f_j) < n$，则
a) $\operatorname{ord}_p(\#Z) \geq 1$ (Chevalley-Warning 定理 [Ch35], [Wa35]), b) $\operatorname{ord}_q(\#Z) \geq \left\lceil \frac{n - \sum_{j=1}^r \deg(f_j)}{\max_{j=1}^r \deg(f_j)} \right\rceil$ (Ax-Katz 定理 [Ax64], [Ka71]).

单个多项式情形下的定理 1.1b) 于 1964 年由 J. Ax [Ax64], 证明，而一般情形则于 1971 年由 N.M. Katz [Ka71]证明。此外，在 [Ax64], 中，Ax 给出了一个极其简洁的十行证明，证明定理 1.1a)。目前当然还没有已知的定理 1.1b) 的十行证明：Ax 对单个多项式的证明使用了代数数论的方法——Jacobi 和与 Stickelberger 同余——而 Katz 对一般情形的证明则运用了复杂的算术几何方法——ζ 函数和 p-进上同调。D. Wan [Wa89], 给出了一个 Ax 风格的定理 1.11.1b) 证明，而 Hou [Ho05]则从 $r = 1$ 情形简洁地推导出了定理 1.11.1b)。此外，D.J. Katz [Ka12]证明了编码理论中的一个结果，该结果蕴含定理 1.1b)。

如果我们将 $\mathbb{F}_q$ 替换为有限环 R，情况会怎样？如果 R 是有限交换环且为主环（即 R 的每个理想都是主理想），那么对于每个素数 p， p整除 $\#Z_{R^n}(f_1, \ldots, f_r)$ 的最大幂，对于给定正次数的所有多项式 $f_1, \ldots, f_r \in R[t_1, \ldots, t_n]$，其结果已被确定：当 $r = 1$ 时由 Marshall-Ramage [MR75] 确定，一般情形则由 D.J. Katz [Ka09]确定。

有限交换环是阿廷环，因此是有限局部阿廷环的有限直积，而每个有限局部阿廷环都必定具有素数幂阶。这样一来，我们立即将问题归约为有限环具有素数幂阶的情形。然而，这类环大多不是主环，直到最近出现以下结果之前，在任何有限非主环上都没有已知的 Chevalley-Warning 类比结果，更不用说 Ax-Katz 了。

定理 1.2。（Aichinger-Moosbauer [AM21，定理 12.6]）设 R 是一个阶为素数 p的幂的有限 rng，且 $f_1, \ldots, f_r \in R[t_1, \ldots, t_n]$ 是非零多项式。若 $Z := Z_{R^n}(f_1, \ldots, f_r)$ 且 $\sum_{i=1}^r \deg(f_i) < n$，则

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

我们的第一个主要结果给出了适用于所有指数为 p的有限 rng 的 Ax-Katz 版本。

定理 1.3（环论素数 Ax-Katz 定理）。设 R 是一个有限 rng，其底层加法群为 $(R, +)$，且指数为素数 p，因此 $(R, +) \cong \left((\mathbb{Z}/p\mathbb{Z})^N, +\right)$，其中$N \in \mathbb{Z}^+$。设 $f_1, \ldots, f_r \in R[t_1, \ldots, t_n]$ 是非零多项式。若 $Z := Z_{R^n}(f_1, \ldots, f_r)$，则

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

注 1.4. 若取 R 为阶为 p^N 的有限域 $\mathbb{F}_{p^N}$，则定理 1.3 的结论是

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

而 Ax-Katz 定理给出了 p-进同余

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

后者对上取整函数的安排更有利，因为当 $N > 1$ 时，(2) 中的下界优于 (1) 中的下界。这就是为什么我们将定理 1.3 称为“素数 Ax-Katz 定理”的推广，而不是 Ax-Katz 定理的推广。

Moreno-Moreno [MM95] 将素数 Ax-Katz 定理作为输入，给出了适用于任意有限域 $\mathbb{F}_q$ 上多项式组的另一种 p- 进同余式，并考虑了这些多项式的 p- 权次数。当 $q > p$ Moreno-Moreno p-进同余式与 Ax-Katz p-进同余式互不蕴含：参见 [MM95，定理 0-1]。在 §4 中，我们将给出定理 1.3 的一个 p-权版本，将 Moreno-Moreno$p$-进同余式从 $\mathbb{F}_q$ 推广到任意素数指数的有限交换环。

定理 1.2 和 1.3 源自更深层的群论结果，下面我们将对此作出说明。

1.3. Aichinger-Moosbauer 泛函演算。Aichinger-Moosbauer 在近期的工作 [AM21], 中，为函数$f:\ A \to B$构建了一套完备的有限差分演算，其中 A 和 B 是交换群。当 A 和 B 是 $\mathbb{R}$- 向量空间时，这一领域历史悠久，至少可以追溯到 Fr´echet [Fr09] 的工作。针对同一主题的较近期研究包括 Leibman [Lei02] ——他研究的不一定是交换群——以及 Laczkovich [La04] ——他综述并致力于综合此前的一些文献。尽管这种演算的思想并非新鲜事物，Aichinger-Moosbauer 的工作却极为优雅、系统且实用。

我们用 B^A 表示所有函数 $f:\ A \to B$的集合。它在以下运算下构成一个交换群 po按点相加。对于每个 $a \in A$，我们定义差分算子 $\Delta_a \in$End(B^A)，如下所示:

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

这些自同态彼此都可交换。按照 Aichinger-Moosbauer 的做法，我们为每个$f \in B^A$ 赋予一个函数次数 fdeg(f) $\in \widetilde{\mathbb{N}}$，定义如下:

- 当且仅当 $f = 0$.[1] 时，我们令 fdeg(f) $= -\infty$。
- 对于 $n \in \mathbb{N}$，若对所有 $a_1, \ldots, a_{n+1} \in A$，都有 $\Delta_{a_1} \cdots \Delta_{a_{n+1}} f = 0$，则称 fdeg($f$) $\leq n$。若某个 $n \in \mathbb{N}$ 满足此条件，则 fdeg(f) 是满足该条件的最小 n。
- 若不存在任何 $n \in \mathbb{N}$ 使 fdeg(f) $\leq n$成立，则令 fdeg(f) $= \infty$。

换言之，若我们设 sup($\emptyset$) $:= -\infty$，则

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

对于交换群 A、B 和 $d \in \mathbb{N}$，我们定义

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

并且我们还令

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

[1] Aichinger-Moosbauer 在 [AM21] 中将零函数的函数次数定义为 0。这里我们遵循 [CS21] 的约定。这当然不会造成任何数学上的区别。

如 [AM21, §2] 中所引入、并在 [CS21, §3]，中讨论的，若 $\mathbb{Z}[A]$ 是 A 的整群环，则交换群 B^A 具有由以下乘积确定的典范 $\mathbb{Z}[A]$-模结构

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

形如 $[a] \in \mathbb{Z}[A]$ 的标量与向量 $f \in B^A$。鉴于此，我们也可以将 Δ_a 视为 $\mathbb{Z}[A]$ 的元素 $[a]-[0]$，因为该元素以先前定义的方式作用于 B^A。若指数 $\exp(B)$ 有限，我们记其为 $e(B)$，否则令 $e(B) := 0$。这意味着，当且仅当存在某个 $N \in \mathbb{Z}^+$，使得对所有 $b \in B$ 都有 $Nb = 0$ 时，$e(B) \neq 0$；此时，$e(B) = \exp(B)$ 是满足条件的最小 N。根据此定义，B^A 是一个典范的 $\mathbb{Z}/e(B)\mathbb{Z}$-模，因此我们也可以将 Δ_a 视为群环 $(\mathbb{Z}/e(B)\mathbb{Z})[A]$ 中的元素。

函数次数给出了“次数为 d 的多项式函数”这一概念，即使不存在环也适用。此外，函数次数的概念与实际多项式函数的次数在一定程度上相容，具体如下：

引理 1.5. 设 R 是一个非结合环，设 f 是一个在 R 上、以 n 个变量为自变量的多项式，且让 $E(f) \in R^{R^n}$ 为关联函数。那么 $\operatorname{fdeg}(E(f)) \leq \deg(f)$.

证明。这是 [AM21，第 12 条引理5]。 □

引理 1.5 表明，函数次数与多项式映射的次数之间的任何差异，只会使以函数次数表述的 Chevalley-Warning / Ax-Katz 型结果比其经典对应结果更强。

以下是 Aichinger-Moosbauer 提出的群论结果，它是定理 1.2 的理论基础。 .

定理 1.6（群论 Chevalley-Warning 定理）。设 N、m、α_1、...
...、α_m、n、β_1、.....、β_n、$r \in \mathbb{Z}^+$，设 $p \in \mathcal{P}$，并设

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

为有限交换 p群。设 $f_1, \ldots, f_r\colon\ A^N \to B$ 为非零函数。若 $Z \coloneqq Z_{A^N}(f_1, \ldots, f_r)$并且

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

then

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

证明。这是 [AM21，定理 12.2]。 □

将定理 1.6 应用于 $A = B = (R, +)$（有限非结合环的加法群，其阶为 p 的幂），并使用引理 1.5，我们推出定理 1.2。

以下是本文的主要结果。

定理 1.7. 设 N、r、β_1、…、$\beta_r \in \mathbb{Z}^+$，令 $p \in \mathcal{P}$，并置 $A := (\mathbb{Z}/p\mathbb{Z})^N$。对于每个 $1 \le j \le r$，令 $f_j \in (\mathbb{Z}/p^{\beta_j}\mathbb{Z})^A$ 为一个非零函数。若 $Z := Z_A(f_1, \dots, f_r)$，则

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

注 1.8。定理 1.7 中映射 f_j 的陪域，可以很容易地从循环 p 群 $\mathbb{Z}/p^{\beta_j}\mathbb{Z}$ 推广到任意有限交换 p 群 B_j。如果对每个 $1 \le j \le r$，

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

那么，每个给定映射 $f_j \colon A \to B_j$ 都可以与坐标投影 $\pi_k \colon B_j \to \mathbb{Z}/p^{\beta_{j,k}}\mathbb{Z} =: B_{j,k}$（其中 $1 \le k \le K(j)$）复合。由此得到函数 $f_{j,k} := \pi_k \circ f_j$，满足

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

显然，对于所有 j，$f_j(x) = 0$ 当且仅当对于所有 j 和 k，$f_{j,k}(x) = 0$。因此，将定理 1.7 应用于所有非零映射 $f_{j,k} \colon A \to B_{j,k}$ 所构成的族，可得

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

这个结果可视为定理 1.7 的推广；令每个 B_j 都是循环群，即可恢复定理 1.7。然而在实际应用中，这个结果会损失定理 1.7 中的信息，因为对于每个 j，我们只使用 $\max_{1 \le k \le K(j)} \big(\operatorname{fdeg}(\pi_k \circ f_j)\big)$，而不是各个映射 $\pi_k \circ f_j$ 的函数次数。

我们还有以下推论，它推广了定理 1.3：

推论 1.9（群论素数 Ax-Katz 定理）。设 $N, n, r \in \mathbb{Z}^+$，并令 $A := (\mathbb{Z}/p\mathbb{Z})^N$。设 $f_1, \dots, f_r \in A^{A^n}$ 为非零函数。若 $Z := Z_{A^n}(f_1, \dots, f_r)$，则

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

证明。令 $\tilde{A} := A^n \cong (\mathbb{Z}/p\mathbb{Z})^{nN}$。对于 $1 \le k \le N$，令 $\pi_k \colon A \to \mathbb{Z}/p\mathbb{Z}$ 为第 k 个坐标投影。对于 $1 \le j \le r$ 和 $1 \le k \le N$，令

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

根据 [CS21, 引理 3.8b)]。对于 $x \in A^n$，对所有 j，$f_j(x) = 0$ 成立，当且仅当对所有 j 和 i，$f_{j,i}(x) = 0$ 成立。因此，将定理 1.7 应用于所有非零映射 $f_{j,k} \in (\mathbb{Z}/p^{\mathbb{Z}})^A$ 构成的族，得到

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

若 R 是一个有限 rng，其底层加法群 $(R, +)$ 为指数 p 的有限群，那么将推论 1.9 应用于 $A = (R, +)$ 并利用引理 1.5，即可推出定理 1.3。若改为结合引理 1.5 的 p 权类比结果（命题 4.3），则可得到定理 1.3 的 p 权改进，该改进可还原 Moreno-Moreno 定理。

备注 1.10。在我们较早的一个版本中，推论 1.9 是主要结果，但改用定理 1.7 后，证明变得更简单：参见备注 1.8。这一改进的想法源自 D. Grynkiewicz 于 2022年3月发给我们的手稿草稿 [GGZ] 。这些结果也见于 arXiv 预印本 [Gr22]。我们的定理 1.7 的表述直接受到 [GGZ, Thm. 1.3.22]，的启发；该结果与定理 1.7 密切相关，但涉及模 p 的剩余系上的求和，以及多项式 $f_1, \dots, f_r \in \mathbb{Z}[t_1, \dots, t_N]$ 模 p 的幂次约化，而非交换 p 群之间的任意函数。此外，在同一手稿较晚的草稿中，Grynkiewicz、Geroldinger 和 Zhong 给出了其结果的加权版本。

1.4. 论文结构。

- 在 §2 中，我们为有限生成时的交换群之间的映射 $f\colon A \to B$ 给出一种典范级数表示，其中这些交换群具有有限函数次数。此外，对于特征 0 的交换整环，我们探讨有限函数次数的函数与整值多项式之间的联系。

- 在 §3 中，我们将 Wilson 的一个引理推广到我们的情形，并证明定理 1.7。
- 在 §4 中，我们讨论 p-权重，并证明定理 1.3 的一个 p-权重改进。
- 在 §5 中，我们讨论本文作者 [CS23] 以及 Clark-Triantafillou [CT23]的工作；这些工作延续并补充了本文的研究。

1.5. 致谢。感谢 E. Aichinger 对我们当前工作的关注，这促成了 Geroldinger-Grynkiewicz-Zhong 结果的交流。感谢 D. Grynkiewicz 向我们展示了 [GGZ] 的两个早期版本。感谢 A.C. Cojocaru、N. Jones 和 N. Triantafillou 与我们进行了富有启发性的讨论。

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

2.1. 预备知识。设 $N \in \mathbb{Z}^+$，并设 B 为一个交换群。在本节中，我们将给出函数 $f \in \mathcal{F}(\mathbb{Z}^N, B)$ 关于二项式多项式的典范级数表示：

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

显然，当 $x \in \mathbb{N}$ 时，$\binom{x}{d}$ 是一个整数，因为它是通常的二项式系数。但是，$\binom{x}{d}$ 总是整数，即使 $x \in \mathbb{Z}$ 为负数：例如参见 [CC，第 19] 页。二项式多项式 $\binom{t}{d} \in \mathbb{Q}[t]$ 是整值多项式，因为它们定义了从 $\mathbb{Z}$ 到 $\mathbb{Z}$ 的函数 $\binom{x}{d}$。我们还取 $\binom{x}{0}\colon \mathbb{Z} \to \mathbb{Z}$ 为常值函数 1。并且，我们定义 $\binom{x}{d}\colon$ 当 $d \in \mathbb{Z}$ 为负数时，$\mathbb{Z} \to \mathbb{Z}$ 为零函数。我们在 §2.3 中讨论这类函数。

对于 $1 \le i \le n$，令 e_i 为 $\mathbb{Z}^N$ 的第 i 个标准基向量。我们用 Δ_i 表示 $B^{\mathbb{Z}^N}$ 的差分算子 Δ_{e_i}。

引理 2.1. 设 $\underline{B}$ 是交换群 B 的一个子群，且 $f \in B^{\mathbb{Z}^N}$。那么以下性质等价：

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

证明. (i) $\Rightarrow$ (ii) 是显然的。
(ii) $\Rightarrow$ (i)：对于任意 $\underline{x} \in \mathbb{Z}^N$ 和任意 $1 \le i \le N$，我们有

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

这表明 $f(\underline{x}+e_i) \in \underline{B} \iff f(\underline{x}) \in \underline{B}$。由于 $f(\underline{0}) \in B$，立即可由归纳论证得出，对于所有 $\underline{x} \in \mathbb{Z}^N$，$f(\underline{x}) \in \underline{B}$。□

对于 $\underline{n} := (n_1, \dots, n_N) \in \mathbb{N}^N$，我们定义

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

由于 $e_1, .., e_N$ 是 $\mathbb{Z}^N$ 的生成元集，因此函数次数的以下刻画可由 AM21 的引理 2.2], 推出，或由 [AM21, Lemmas 2.2], or from [CS21, Lemma 3.11] 推出：

命题 2.2。令 $f \in B^{\mathbb{Z}^N}$，并定义 $\sup(\emptyset) := -\infty$。则

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

若将此表达式与下述 j 阶偏函数次数的定义进行比较，其中函数 f 属于 $B^{\mathbb{Z}^N}$，其定义为

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

容易看出，对于每个 $1 \le j \le N$,

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

这一切都可以轻易推广到由任意交换群 $A_1, \dots, A_N$ 的直积构成的整环，如 [AM21, §5] 所示。将这个直积视为内直积，我们定义函数 $f \in B^{\bigoplus_{i=1}^N A_i}$ 的第 j 个偏函数次数为

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

由 [AM21, 引理 2.2] 或 [CS21, 引理 3.11] 可得

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

由此可轻易得到 [AM21, 定理 5.2], , 下面给出一个简短的证明：

定理 2.3. 设 $A_1, \dots, A_N, B$ 为交换群，且 $f \in B^{\bigoplus_{i=1}^N A_i}$。那么，对每个 $1 \le j \le N$,

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

证明. 不妨设 $f \neq 0$，因为否则该不等式显然成立。比较 (3) 和 (4)，可知 $\operatorname{fdeg}_j(f) \le \operatorname{fdeg}(f)$。为证明 $\operatorname{fdeg}(f) \le \sum_{i=1}^N \operatorname{fdeg}_i(f) =: n \ge 0$，令 $a_1, \dots, a_{n+1} \in A_1 \cup \cdots \cup A_n$。由 (5)，只需证明 $\Delta_{a_{n+1}} \cdots \Delta_{a_1} f = 0$。由于 $n+1 > \sum_{i=1}^N \operatorname{fdeg}_i(f)$，存在一个 $1 \le j \le N$，使得超过 $n_j := \operatorname{fdeg}_j(f)$ 个元素 $a_1, \dots, a_{n+1}$ 落在 A_j 内。不失一般性，设 $a_1, \dots, a_{n_j+1} \in A_j$。于是由 (4) 得 $\Delta_{a_{n_j+1}} \cdots \Delta_{a_1} f = 0$，从而得到 $\Delta_{a_{n+1}} \cdots \Delta_{a_1} f = 0$。□

为方便读者，我们也重述 [CS21, 引理 2.2]。

引理 2.4. 设 A 和 B 是交换群。设 $a \in A$，$n \in \mathbb{N}$，并设 Δ_a^n 为 n 重积 $\Delta_a \cdots \Delta_a \in \operatorname{End} B^A$。对于所有 $f \in B^A$ 和所有 $x \in A$，我们有

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

我们回顾一个旧结果，以供比较和后续使用：

引理 2.5. 设 R 是一个交换整环，设 $f \in R[t_1, \ldots, t_n]$，并设 X_i 是 R 的一个非空子集，对于每个 $1 \leq i \leq n$，都有 $\#X_i > \deg_i(f)$。如果对于所有 $x \in X := \prod_{i=1}^n X_i$，$f(x) = 0$，那么 $f = 0$。

证明。我们可以立即归结为 $\#X_i = \deg_i(f) + 1$ 对所有 i都成立的情形。此时，情形 $R = \mathbb{Z}$ 是 [AT92，引理 2.1]，，他们的证明可原封不动地推广到任意交换整环上。更一般的结果见 [Sc08，第 2] 节；另见 [Cl14，定理 12]。□

以下结果与引理 2.5 以及 [Sc14，定理 2.5] 有关。

引理 2.6。设 $N \in \mathbb{Z}^+$，设 B 为交换群，并设 $f \in B^{\mathbb{Z}^N}$。对每个 $1 \leq i \leq N$，设 $a_i \in \mathbb{Z}$，$d_i \in \mathbb{N}$ 满足 $d_i \geq \operatorname{fdeg}_i(f)$，并令

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

若对所有 $\underline{x} \in \prod_{i=1}^N [a_i, a_i + d_i]$，$f(\underline{x}) = 0$ 均成立，则 $f = 0$。

证明。我们对 N 使用归纳法。

基例：假设 $N = 1$，即 $f \in B^{\mathbb{Z}}$，$\operatorname{fdeg}(f) \leq d_1$ 且 $f(a) = f(a+1) = \cdots = f(a + d_1) = 0$。将 $d_1 + 1$ 代入引理 2.4 中的 n，将 1 代入该引理中的 a，并将 $a - 1$（分别为 a）代入该引理中的 x，应用引理 2.4 可推出 $f(a - 1) = 0$（分别为 $f(a + d_1 + 1) = 0$）。重复此论证，我们得到 $\cdots = f(a - 2) = f(a - 1) = 0$ 且 $0 = f(a + d_1 + 1) = f(a + d_1 + 2) = \cdots$，即 $f = 0$。

归纳步骤：假设 $N \geq 2$，且对所有 $f \in \mathcal{F}(\mathbb{Z}^{N-1}, B)$ 结论均成立。对于 $0 \leq j \leq d_N$，令

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

于是，对所有 $1 \leq i \leq N - 1$，都有 $\operatorname{fdeg}_i g_j \leq d_i$，且 g_j 在 $\prod_{i=1}^{N-1} [a_i, a_i + d_i]$ 上恒为零，因此由归纳法可得，对所有 $0 \leq j \leq d_N$，$g_j = 0$ 成立。由此，对于每个固定的 $(x_1, \ldots, x_{N-1}) \in \mathbb{Z}^{N-1}$，函数 $f(x_1, \ldots, x_{N-1}, \cdot) : \mathbb{Z} \to B$ 在 $[a_N, a_N + d_N]$ 上为零，且其函数次数至多为 d_N。因此，根据基例，这些函数恒为零，这意味着 f 恒为零。□

引理 2.7. 设 B 为一个交换群，并设 $f : \mathbb{N}^N \longrightarrow B$ 为一个函数。若对所有 $\underline{n} \in \mathbb{N}^N$，$\Delta^{\underline{n}} f(\underline{0}) = 0$，则 f 是零函数。

证明。给定一个函数 $f : \mathbb{N}^N \to B$，满足 $\Delta^{\underline{n}} f(\underline{0}) = 0$ 对所有 $\underline{n} \in \mathbb{N}^N$ 成立，我们证明一个形式上更强的结论：$\Delta^{\underline{m}} f(\underline{x}) = 0$ 对所有 $\underline{x}, \underline{m} \in \mathbb{N}^N$ 成立。我们对 $|\underline{x}| := x_1 + \cdots + x_N$ 使用归纳法。

基例：若 $|\underline{x}| = 0$，则根据关于 f 的假设，$\underline{x} = \underline{0}$ 且 $\Delta^{\underline{m}} f(\underline{x}) = \Delta^{\underline{m}} f(\underline{0}) = 0$ 对所有 $\underline{m} \in \mathbb{N}^N$ 成立。

归纳步骤：设 $\underline{0} \neq \underline{x} \in \mathbb{N}^N$，并假设该命题对所有满足 $|\underline{z}| < |\underline{x}|$ 的 $\underline{z} \in \mathbb{N}^N$ 以及所有 $\underline{m} \in \mathbb{N}^N$ 均成立。由于 $\underline{x} \neq \underline{0}$，存在一个指标 i 使得 $x_i \geq 1$。因此，根据归纳假设，对每个 $\underline{m} \in \mathbb{N}^N$，

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

使得

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

从而完成归纳步骤并得出证明。 □

2.2. 基本表示。现在我们可以证明以下结果，本工作的其余大部分内容都以此为基础。

定理 2.8. 设 B 是一个交换群，并且设 $f \in B^{\mathbb{Z}^N}$。

a) 存在唯一的函数 $a_\bullet \colon \mathbb{N}^N \to B$，使得

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

$a_\bullet$ 的函数值由公式 $a_{\underline{n}} = \Delta^{\underline{n}} f(\underline{0})$ 给出。

b) 如果 $d := \operatorname{fdeg}(f) < \infty$，那么

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

证明。a) 为证明唯一性，假设存在一个 $a_\bullet$，满足 $f(\underline{x}) := \sum \binom{x_1}{n_1} \cdots \binom{x_N}{n_N} a_{\underline{n}}$ 对所有 $\underline{x} \in \mathbb{N}^N$ 均成立。对于每个 $\underline{x} = (x_1, \ldots, x_N) \in \mathbb{N}^N$，我们有 $\binom{x_1}{n_1} \cdots \binom{x_N}{n_N} = 0$，除非对所有 $1 \le i \le N$ 都有 $n_i \le x_i$；因此，对每个固定的 $\underline{x}$，我们都有一个有限和。对于所有 $n \in \mathbb{Z}^+$，都有 $\binom{x+1}{n} - \binom{x}{n} = \binom{x}{n-1}$。由此可得，对于所有 $\underline{m}$，$\underline{n} \in \mathbb{N}$，

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

由此，若将 $\Delta^{\underline{m}}$ 应用于 $f(\underline{x}) = \sum \binom{x_1}{n_1} \cdots \binom{x_N}{n_N} a_{\underline{n}}$ 并在 0 处求值，我们便可得出 $a_{\underline{m}} = \Delta^{\underline{m}} f(\underline{0})$。因此，函数 $a_\bullet \colon \underline{n} \mapsto \Delta^{\underline{n}} f(\underline{0})$ 是唯一可能的选择。

为证明这一选择确实得到函数 f，定义 $\hat{f} \colon \mathbb{N}^N \to B$ 如下：

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

根据我们已经证明的系数的唯一性，对于每个 $\underline{n} \in \mathbb{N}^N$，系数 $\Delta^{\underline{n}} f(\underline{0})$ 必须等于 $\Delta^{\underline{n}} f(\underline{0})$，即 $\Delta^{\underline{n}}(f - \hat{f})(\underline{0}) = 0$。由此，引理 2.7 得出 $f - \hat{f} = 0$，即 $f = \hat{f}$，正如所需。

b) 对于所有满足 $|\underline{n}| \ge d$ 的 $\underline{n} \in \mathbb{N}^N$，我们有 $\Delta^{\underline{n}} f(\underline{0}) = 0$，因此

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

然而，该等式的右边定义了一个函数 $P \colon \mathbb{Z}^N \to B$。并且，$f - P$ 的函数次数至多为 d，且在 $\mathbb{N}^N$ 上消失。因此，由引理 2.6，$f = P$。□

由多元二项式多项式$\binom{x_1}{n_1}\cdots\binom{x_N}{n_N}$构成的有限线性组合 $\sum_{|\underline{n}|\le d}\binom{x_1}{n_1}\cdots\binom{x_N}{n_N}a_{\underline{n}}$，其系数 $a_{\underline{n}}$属于群 B，如定理 2.8b) 中所述，在 [Sc14] 中称为多项式分形。由于定理 2.8a) 中系数 $a_{\underline{n}}$ 的唯一性，我们无需区分多项式分形 $\sum_{|\underline{n}|\le d}\binom{x_1}{n_1}\cdots\binom{x_N}{n_N}a_{\underline{n}}$（其中 x_i可视为符号变量）与相应的多项式分形函数

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

显然，这类映射的函数次数由下式给出

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

其中 $\sup(\emptyset):=-\infty$。这是由以下事实得出的：

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

并且注意到，只要 $m_i\le n_i$，$x_i\mapsto\binom{x_i}{n_i-m_i}$ 就不是零映射。因此，结合定理 2.8b) 与公式（6），我们得到以下推论，它使我们能够以更局部的方式计算函数次数——至少在已知函数次数有限时如此。

推论 2.9。设 B 是一个交换群，并设 $f\in B^{\mathbb{Z}^N}$。若 $\operatorname{fdeg}(f)<\infty$，则

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

在此推论中，点 0 可以替换为任意其他点 $\underline{a}\in\mathbb{Z}^N$，因为 $\operatorname{fdeg}([\underline{a}]f)=\operatorname{fdeg}(f)$。然而，若 $\operatorname{fdeg}(f)=\infty$，则我们可能有 $\operatorname{fdeg}_{\underline{0}}(f)<\infty$。这是因为 $\operatorname{fdeg}_{\underline{0}}(f)$ 仅取决于点 $\underline{x}\in\mathbb{N}^N$ 处的函数值 $f(\underline{x})$，而条件 $\operatorname{fdeg}(f)<\infty$ 只允许从 $\mathbb{N}^N$ 到 $\mathbb{Z}^N$ 存在唯一延拓 —— 即定理 2.8b) 中公式所给出的延拓。

我们还看到，在 $B=\mathbb{Q}$ 的情况下，定理 2.8b) 中的级数表示给出了一个多项式 $\hat{}f\in\mathbb{Q}[t_1,\dots,t_N]$，它描述了 f：

推论 2.10. 如果 $f\in\mathbb{Q}^{\mathbb{Z}^N}$ 具有有限函数次数，那么存在一个多项式 $\hat{}f\in\mathbb{Q}[t_1,\dots,t_N]$，使得 $\deg(\hat{}f)=\operatorname{fdeg}(f)$，并且对所有 $\underline{x}\in\mathbb{Z}^N$，$\hat{}f(\underline{x})=f(\underline{x})$。

注 2.11。

a) 对于 B 有限生成交换群，定理 2.8b) 中的级数表示已在 [Sc14, §2] 中探讨。b) 定理 2.8 的级数展开是光滑函数 $f\colon\mathbb{R}^N\to\mathbb{R}$ 的泰勒级数展开的离散类比。定理 2.8a) 蕴含一个唯一性性质：对于任意两个函数 $a_\bullet,b_\bullet\colon\mathbb{N}^N\to B$，若它们都仅将整环中有限多个元素映射为 0，则定义关联函数

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

and

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

那么 $f_{a_\bullet} = f_{b_\bullet}$ 当且仅当 $a_\bullet = b_\bullet$。这与如下事实互为离散类比：以 0 为中心的幂级数展开中，系数由 0 处的偏导数确定。

c) 正如同样可以直接考虑以非零点 $a \in \mathbb{R}^N$ 为中心的泰勒级数展开一样， $f \in \mathcal{F}(\mathbb{Z}^N, B)$ 也有基于任意固定 $\underline{a} \in \mathbb{Z}^N$ 处的值 $\Delta^{\underline{n}} f(\underline{a})$ 的表示。

接下来我们回顾 [CS21, §3.2] 中的一些记号和一个结果。若 $\varepsilon\colon A \to A$ 和 $\mu\colon B \to B'$ 是交换群的同态，则我们有群同态。

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

and

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

容易看出， ε^* 是单射当且仅当 ε 是满射，并且 μ_* 是满射当且仅当 μ 是满射。

以下结果见 [CS21，引理 3.9]。

引理 2.12（同态函子性 I）。设 $\varepsilon\colon A' \to A$ 和 $\mu\colon B \to B'$ 是交换群之间的同态，并设 $f \in B^A$。则：

a) $\mathrm{fdeg}\ \varepsilon^* f \le \mathrm{fdeg}\ f$，若 ε 是满射，则等号成立；

b) $\mathrm{fdeg}\ \mu_* f \le \mathrm{fdeg}\ f$，若 μ 是单射，则等号成立。

以下这个概念上相似的结果是定理 2.8 的推论。

推论 2.13（同态函子性 II）。设 B、B' 为交换群，设$\mu\colon B \to B'$ 为一个同态，并设 $f \in B^{\mathbb{Z}^N}$。

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

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

证明。映射 $\mu_*\colon B^{\mathbb{Z}^N} \to (B')^{\mathbb{Z}^N}$ 是一个 $\mathbb{Z}[\mathbb{Z}^N]$-模同态。因此，对所有 $\underline{n} \in \mathbb{N}^N$，

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

由此以及定理 2.8a)，可得对所有 $\underline{x} \in \mathbb{N}^N$，

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

从而证明 a)。再次应用定理 2.8b) 于 $\mu_* f$，并再次使用 (7)，可得对所有 $\underline{x} \in \mathbb{Z}^N$，

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

□

2.3. 多项式函数与整值多项式。本节中，我们使用定理 2.8 比较整值多项式与有限函数次数的函数。本节的结果在本文其他部分并未用到。然而，在 Wilson 对 $\mathbb{F}_p$[上 Ax-Katz 定理的证明中，会用到整值多项式及其约化（Wi06，引理 4], ）；此外，Varga 的一项工作 [Va14] （推广了 Warn- ing 第二定理）也采用了通过整值多项式表示剩余环 $\mathbb{Z}$ 之间函数的技巧。了解这些技巧可以从 Aichinger-Moosbauer 演算的角度来理解，或许会有所帮助。

设 R 是一个非平凡交换环，设 $N \in \mathbb{Z}^+$，并考虑求值映射

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

这是一个 R-代数同态；按定义，其像是 R^N 上的多项式函数环，记作 P(R^N, R)。映射 E 永远不是同构，不过其失败的方式取决于 R。若 R 是有限的，则 $R[t_1, \ldots, t_n]$ 是无限的，而 R^{R^N} 是有限的，因此 E 有无限核。若 R 是无限的，则 E 不是满射 [Cl14，定理 4.3]。更确切地说：

命题 2.14。设 R 是一个非平凡交换环，且设 $N \in \mathbb{Z}^+$。则以下性质等价：

(i) 求值映射 E：$R[t_1, \ldots, t_N] \longrightarrow R^{R^N}$ 是满射。(ii) 函数

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

位于 E的像中。

(iii) 环 R 是一个有限域。

证明。为证明 (iii) 蕴含 (i)，进而得到 (ii)，假设 $R = \mathbb{F}_q$ 是一个有限域。在这种情况下，对 E 的研究构成了 Chevalley 在 [Ch35] 中证明定理 1.1a) 的核心内容。他证明了 E 是满射，其核为 $\langle t_1^q - t_1, \ldots, t_N^q - t_N \rangle$。关于适度推广的英文证明，参见 [Cl14, 推论 2.5 和命题 4.4]。

为证明 ¬(iii) 蕴含 ¬(ii)，进而推出 ¬(i)，我们区分两种情况。

情形 1， R 不是一个域：在这种情况下， R中存在一个真理想 I ，因此， E 的像 P(R^N, R) 中的每个函数 F 都是模同余保持的 I：如果x =($x_1, \ldots, x_N$)、 y =($y_1, \ldots, y_N$) $\in R^N$满足对所有 $1 \leq i \leq N$, 都有 $x_i \equiv y_i$(模 I)，那么 f(x) $\equiv$ f(y) (模 I)。但是，如果 $a \in I \setminus \{0\}$，那么 $a \equiv 0$(模 I)，而

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

因此 $\delta_{0,\ 1}$ 不是保同余的，也不属于 E 的像。

情形 2， R 不是有限的：在此情形下， [CS21, 定理 4.9a)]给出 fdeg($\delta_{0,\ 1}$) $= \infty$。因此根据引理 1.5， $\delta_{0,\ 1}$ 不是多项式函数，也不属于 E的像。□

如果 R 是一个既非域的无限交换环，我们刚才给出了两个证明（分别对应情形 1 和情形 2），证明 $\delta_{0,1} \in R^{R^N} \setminus$ P(R^N, R)。第二个证明还表明了更多：$\delta_{0,1}$ 具有无限函数次数。一般来说，对于非平凡交换环 R，引理 1.5 指出，

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

这引出了一个更有趣的问题版本： E 何时是满射?

问题 2.15. 对于哪些非平凡交换环 R 和数 $N \in \mathbb{Z}^+$，我们有 $\mathrm{P}(R^N, R) = \mathcal{F}(R^N, R)$——也就是说，何时每个具有有限函数次数的函数 $f \in R^{R^N}$ 都是多项式函数?

下面给出当 R 为有限环时，问题 2.15 的一个答案。

命题 2.16. 对于非平凡有限交换环 R，以下性质等价:

(i) 对所有 $N \in \mathbb{Z}^+$，$\mathrm{P}(R^N, R) = \mathcal{F}(R^N, R)$。 (ii) 对某个 $N \in \mathbb{Z}^+$，$\mathrm{P}(R^N, R) = \mathcal{F}(R^N, R)$。 (iii) 对某些 $r, \alpha_1, \ldots, \alpha_r \in \mathbb{Z}^+$ 和素数 $p_1 < \cdots < p_r$，$R \cong \prod_{i=1}^r \mathbb{F}_{p_i^{\alpha_i}}$。

证明。若 R 是阶为 $p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ 的有限交换环（其中 $p_1 < \cdots < p_r$ 为素数），则存在唯一的内直积分解 $R = \prod_{i=1}^r \mathfrak{r}_i$，其中 $\mathfrak{r}_i$ 是阶为 $p_i^{\alpha_i}$ [的环；参见 Cl-CA 定理 8.37]——这是 R 的 p_i-主分量。我们有一个自然的环同构

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

并且，根据 [AM21 定理 9.4] 或 [CS21 定理 3.13]，有一个自然分解

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

利用这些分解，我们得到

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

因此，我们将问题化归为 R 具有素数幂阶的情形；根据 [AM21 定理 9.1],

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

因此，我们的问题化归为前面关于求值映射何时为满射的问题。根据命题 2.14，这当且仅当 R 是有限域时成立。所以，不论 $N \in \mathbb{Z}^+$如何：$\mathrm{P}(R^N, R) = \mathcal{F}(R^N, R)$ 当且仅当，对于所有 $1 \le i \le r$，$\mathfrak{r}_i$ 都是有限域 $\mathbb{F}_{p_i^{\alpha_i}}$，即 $R \cong \prod_{i=1}^r \mathbb{F}_{p_i^{\alpha_i}}$。 □

当 R 为无限时，我们尚不知道问题 2.15 的完整答案，但将展示一些正面和负面的结果。

引理 2.17。设 $h \in \mathcal{F}(\mathbb{Q}^N, \mathbb{Q})$。若 $h|_{\mathbb{Z}^N} = 0$，则 $h = 0$。

证明。令 $D \in \mathbb{Z}^+$，并定义 $h_D \in \mathbb{Q}^{\mathbb{Z}^N}$ 为

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

函数 h_D 是通过将 h 与 $(\mathbb{Q}^N, +)$ 的群自同态进行复合前置得到的，因此根据 [AM21, 定理 4.3], $h_D \in \mathcal{F}(\mathbb{Q}^N, \mathbb{Q})$。因此，由推论 2.10，存在一个多项式 $\hat{h}_D(\underline{t}) \in \mathbb{Q}[t_1, \ldots, t_N]$，使得对所有 $\underline{x} = (x_1, \ldots, x_N) \in \mathbb{Z}^N$，都有 $\hat{h}_D(\underline{x}) = h_D(\underline{x})$。将引理 2.5 应用于 $\hat{h}_D$，其中 $X = (D\mathbb{Z})^N$，可得 $\hat{h}_D = 0$。因此，对所有 $D \in \mathbb{Z}^+$，我们有 $h|_{(D^{-1}\mathbb{Z})^N} = 0$，所以 $h = 0$。 □

命题 2.18. 对所有 $N \in \mathbb{Z}^+$，我们有 $\mathrm{P}(\mathbb{Q}^N, \mathbb{Q}) = \mathcal{F}(\mathbb{Q}^N, \mathbb{Q})$。

证明。显然，$\mathrm{P}(\mathbb{Q}^N) \subseteq \mathcal{F}(\mathbb{Q}^N, \mathbb{Q})$。为证明 $\mathcal{F}(\mathbb{Q}^N, \mathbb{Q}) \subseteq \mathrm{P}(\mathbb{Q}^N, \mathbb{Q})$，令$g \in \mathcal{F}(\mathbb{Q}^N, \mathbb{Q})$，其 $\mathrm{fdeg}(g) \leq d \in \mathbb{N}$。根据推论 2.10，存在一个多项式 $\hat{}g \in \mathbb{Q}[t_1, \ldots, t_N]$，其 $\deg(\hat{}g) \leq d$，使得对所有 $\underline{x} = (x_1, \ldots, x_N) \in \mathbb{Z}^N$，均有 $\hat{}g(\underline{x}) = g(\underline{x})$。因此，$h := E(\hat{}g) - g$ 在 $\mathbb{Z}^N$ 上为零，并且根据 [AM21，引理 3.2]，$\mathrm{fdeg}(h) \leq d$。由引理 2.17可知 $h = 0$，这意味着 $E(\hat{}g) = g$，即 $g \in \mathrm{P}(\mathbb{Q}^N, \mathbb{Q})$。□

从现在起，直到 §2.3 结束，我们假设 R 是特征为 0 的交换整环，其分式域为 K。在这种情况下，求值映射 $E\colon R[t_1, \ldots, t_N] \longrightarrow R^{R^N}$是单射 [Cl14, 命题 4.5]，因而诱导出一个同构 $R[t_1, \ldots, t_N] \xrightarrow{\sim} \mathrm{P}(R^N, R)$。Aichinger-Moosbauer [AM21, 引理 10.4] 给出了这样一个结果：对于所有 $f \in K[t_1, \ldots, t_n]$，都有 $\mathrm{fdeg}(E(f)) = \deg(f)$。我们将证明，同样的结论对 R 也成立，事实上还能得到更多。具体而言，我们考虑整值多项式的子环

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

命题 2.19. 设 R 是一个交换整环。若 $f \in \mathrm{Int}(R^N, R)$ 且 $E_R(f) := \big(x \mapsto f(x)\big) \in R^{R^N}$，则

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

且当 R 的特征为 0 时取等号。

证明。令 $f \in \mathrm{Int}(R^N, R)$。由引理 2.12，定义域限制和陪域限制不会增加函数次数，因此由引理 1.5 可得

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

现在，假设 R 的特征为 0，且 $d := \deg(f) \geq 0$。为完成证明，只需证明 $\mathrm{fdeg}(E_R(f)) \geq d$。由于 $\deg(f) = d$，标准展开中会出现一个满足 $n_1 + n_2 + \cdots + n_N = d$ 的单项式 $t_1^{n_1} t_2^{n_2} \cdots t_N^{n_N}$。若算子$\Delta_i$ 作用于多项式的方式与作用于函数的方式相同，则 $\deg(\Delta_1^{n_1} \cdots \Delta_N^{n_N} f) = \deg(f) - (n_1 + \cdots + n_N) = 0$，因为每次应用一个 Δ_i 都会使次数恰好降低 1，这是因为 R 的商域具有特征 0。这表明函数 $\Delta_1^{n_1} \cdots \Delta_N^{n_N} E_R(f) = E_R(\Delta_1^{n_1} \cdots \Delta_N^{n_N} f)$ 是一个非零常数，因此确实有 $\mathrm{fdeg}(E_R(f)) \geq d$。□

如果 R 是特征为 $p > 0$ 的交换整环，则（9）中可能出现严格不等式。要得到等式，需要使用 p-权次数；当 R 为有限集时，还需要使用约化多项式：参见 §4.3。

对于交换整环 R，命题 2.19 给出了（8）的一个细化：

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

只要 $\mathrm{Int}(R^N, R) \supsetneq \mathrm{P}(R^N, R)$，这就为问题 2.15 给出了否定的答案；对于 $R = \mathbb{Z}$，该条件显然成立，例如 $t(t-1)/2$ 是一个不属于 $\mathbb{Z}[t]$ 的整值多项式。这引出了如下结果：

定理 2.20。
a) $\mathcal{B} := \left\{ \binom{x_1}{n_1} \cdots \binom{x_n}{n_N} \mid \underline{n} \in \mathbb{N}^N \right\}$是 $\mathbb{Z}$-模 $\mathcal{F}(\mathbb{Z}^N, \mathbb{Z})$ 的一组基。 b) $\mathcal{F}(\mathbb{Z}^N, \mathbb{Z}) = \mathrm{Int}(\mathbb{Z}^N, \mathbb{Z})$。

证明。定理 2.8 的 b) 部分表明， $\mathcal{B}$ 张成 $\mathcal{F}(\mathbb{Z}^N,\mathbb{Z})$ 作为一个 $\mathbb{Z}$-模；该定理的 a) 部分则指出了刻画一组基的唯一性性质。
根据命题 2.19，我们还有 $\mathrm{Int}(\mathbb{Z}^N,\mathbb{Z}) \subseteq \mathcal{F}(\mathbb{Z}^N,\mathbb{Z})$，因此只需证明 $\mathcal{F}(\mathbb{Z}^N,\mathbb{Z}) \subseteq \mathrm{Int}(\mathbb{Z}^N,\mathbb{Z})$。众所周知，对于所有 $n \in \mathbb{N}$，都有 $\binom{x}{n} \in \mathrm{Int}(\mathbb{Z},\mathbb{Z})$，这一事实可由引理 2.1 和归纳法得出。由于 $\mathrm{Int}(\mathbb{Z}^N,\mathbb{Z})$ 是一个环，因此对于所有 $b \in \mathcal{B}$，我们都有 $b \in \mathrm{Int}(\mathbb{Z}^N,\mathbb{Z})$。所以，

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

定理 2.20 表明， $\mathcal{B}$ 是整值多项式环 $\mathrm{Int}(\mathbb{Z}^N,\mathbb{Z})$ 的一个 $\mathbb{Z}$-基，这是 Ostrowski [Os19] 的结果。关于交换整环 R 上的 $\mathrm{Int}(R^N,R)$ 的一般论述，参见 [CC，第 11] 章。Cahen-Chabert 也在 [CC，第 I.3]，节讨论了何时 $\mathrm{Int}(R^N,R) = \mathrm{P}(R^N,R)$，并特别指出，当 R 的每个剩余域都是无限域时，等式成立 [CC，推论 I.3.7]，，例如，当 R 是一个 $\mathbb{Q}$-代数时即如此。我们的下一个结果表明，对于每个 $N \in \mathbb{Z}^+$，只要 $R \supsetneq \mathbb{Q}$ 是一个 $\mathbb{Q}$-代数，就有 $\mathrm{Int}(R^N,R) \subsetneq \mathcal{F}(R^N,R)$。

称环 R 为 Cayley 环，当且仅当 Cayley 同态

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

是同构（等价地说，是满射）。

例 2.21。

a) 以下环是 Cayley 环：1. 素域，即 $\mathbb{Q}$，以及满足 $p \in \mathcal{P}$的有限域 $\mathbb{F}_p$；2. $\mathbb{Q}$的子环，即 $\mathbb{Z}$的局部化，包括 $\mathbb{Z}$ 和 $\mathbb{Q}$。

b) 如果交换环作为某个真子环上的模是秩大于 1 的自由模，则它不是 Cayley 环。因此，以下环都不是 Cayley 环：

1. 非素域，即除 $\mathbb{Q}$ 和 $\mathbb{F}_p$之外的域，对所有 $p \in \mathcal{P}$均如此；2. 在满足 $F \subsetneq R$的任意域 F 上的代数 R；3. 数域 $K \supsetneq \mathbb{Q}$的整数环 $\mathbb{Z}_K$；4. 对任意 $p \in \mathcal{P}$，p- 进域 $K \supsetneq \mathbb{Q}_p$ 的赋值环。

命题 2.22. 设 R 是特征 0 的交换整环。若对某个 $N \in \mathbb{Z}^+$，有 $\mathrm{Int}(R^N,R) = \mathcal{F}(R^N,R)$，则 R 是 Cayley 环。

证明. 反设 R 不是 Cayley 环：这恰好意味着存在一个 $\mathbb{Z}$-线性映射 $L : (R,+) \to (R,+)$，它不能写成线性多项式 $f \in R[t]$ 的 $E(f)$ 形式。若 K 是 R 的分式域，则 L 也不能写成线性多项式 $f \in K[t]$ 的 $E(f)$ 形式：若 $f = ax + b$ 且 $a,b \in K$，则在 0 处求值得到 $b = 0$，在 1 处求值得到 $a = L(1) \in R$。由于 $\mathrm{fdeg}(L) = 1$，根据命题 2.19，L 因此不能由任何整值多项式给出。这就证明了关于 $N = 1$ 的结论。对每个 $N \in \mathbb{Z}^+$，函数 $L_N : R^N \to R$，其中 $L_N(x_1,\ldots,x_N) = L(x_1)$，也是 $\mathbb{Z}$-线性的，但它不是任何 K- 线性多项式函数在 R^N 上的限制。因此，$L_N \in \mathcal{F}(R^N,R) \setminus \mathrm{Int}(R^N,R)$。$\square$

命题 2.22 和例 2.21 给出了许多满足 $\mathrm{Int}(R^N,R) \subsetneq \mathcal{F}(R^N,R)$ 的例子：例如任意域 $K \supsetneq \mathbb{Q}$。另一方面，运用与我们之前所用类似的论证，可以证明对于 $\mathbb{Q}$ 的任意子环 R，$\mathrm{Int}(R^N,R) = \mathcal{F}(R^N,R)$。

2.4. 提升。设 $\mu\colon B \to B'$ 是交换群的一个满同态，且 $f \in \mathcal{F}(\mathbb{Z}^N, B')$。根据定理 2.8b)，存在唯一函数 $a_\bullet\colon \mathbb{N}^N \to B'$，它至多在有限多个点上非零；我们称之为有限非零函数，使得

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

我们将 $a_\bullet$ 到 B （经由 μ）的一个提升定义为一个有限非零函数 $\tilde{a}_\bullet\colon \mathbb{N}^N \to B$，使得 $\mu \circ \tilde{a}_\bullet = a_\bullet$。真提升是指满足以下条件的提升 $\tilde{a}_\bullet$：对所有 $\underline{n} \in \mathbb{N}^N$，

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

真提升总是存在，并且当且仅当 $\mu\colon B \to B'$ 是同构，或 $a_\bullet$ 恒等于 0 时，真提升唯一。对于真提升 $\tilde{a}_\bullet$，我们定义函数 $\tilde{f} \in B^{\mathbb{Z}^N}$ 如下：

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

~我们看到 $\mathrm{fdeg}(f) = \sup\{|\underline{n}| \mid \tilde{a}_{\underline{n}} \neq 0\} = \sup\{|\underline{n}| \mid a_{\underline{n}} \neq 0\} = \mathrm{fdeg}(f)$。结合推论 2.13，可得

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

W ~我们也称 $\tilde{f}$ 为 f 的真提升，反过来也可以说 f 是 $\tilde{f}$ 的约化。

此外，如果 B 和 B' 分别是族 $(B_j)_{j\in J}$ 和 $(B'_j)_{j\in J}$ 的直积（或直和），且 μ 是同态 $\mu_j\colon B_j \to B'_j$ 的笛卡尔积（或直积），则可以进一步强化真提升的概念。在这种情形下，若 $\tilde{\pi}_j\colon B \to B_j$ 和 $\pi_j\colon B' \to B'_j$ 表示相应的投影，则对每个 $j \in J$，我们都有 $\pi_j \circ \mu = \mu_j \circ \tilde{\pi}_j$。此时，如果每个 $\tilde{\pi}_j \circ \tilde{a}_\bullet\colon \mathbb{N}^N \to B_j$ 都是 $\pi_j \circ a_\bullet\colon \mathbb{N}^N \to B'_j$ 的真提升，我们就称 $\tilde{a}_\bullet\colon \mathbb{N}^N \to B$ 是逐坐标真提升。相应地，如果每个 $\tilde{\pi}_j \circ \tilde{f}$ 都是 $\pi_j \circ f$ 的真提升，我们就称 $\tilde{f} \in B^{\mathbb{Z}^N}$ 是 $f \in \mathcal{F}(\mathbb{Z}^N, B')$ 的逐坐标真提升。这类真提升也总是存在，因为可以先构造逐坐标提升 $\tilde{\pi}_j \circ \tilde{a}_\bullet$，再将它们合并为一个提升 $\tilde{a}_\bullet$。

将上述讨论与定理 2.8 和 2.20 结合起来，我们发现，对于每个 $N, m \in \mathbb{Z}^+$，每个 $f \in \mathcal{F}(\mathbb{Z}^N, \mathbb{Z}/m\mathbb{Z})$ 都是一个次数为 $\mathrm{fdeg}(f)$ 的整值多项式的约化。特别地，当存在某个 $p \in \mathcal{P}$ 使得 $m = p^\beta$，且 f 对于某些 $\alpha_1, \ldots, \alpha_N \in \mathbb{Z}^+$ 是 $(p^{\alpha_1}, \ldots, p^{\alpha_N})$-周期的时，这一结论也适用；也就是说，如果 f 属于自然映射 $(\mathbb{Z}/p^\beta\mathbb{Z})^{\oplus_{i=1}^N \mathbb{Z}/p^{\alpha_i}\mathbb{Z}} \to (\mathbb{Z}/p^\beta\mathbb{Z})^{\mathbb{Z}^N}$ 的像。这种情形正是我们接下来要深入考察的。

注 2.23. 函数 $\mathbb{Z}/p^\alpha\mathbb{Z} \to \mathbb{Z}/p^\beta\mathbb{Z}$ 可以（经由 $\varepsilon\colon \mathbb{Z} \to \mathbb{Z}/p^\alpha\mathbb{Z}$ 拉回后）表示为整值多项式的约化，这一事实已应用于 Varga 的工作 [Va14]。在 [CW18] 中，这项工作被推广到如下形式的映射 $\mathbb{Z}_K/\mathfrak{p}^\alpha \to \mathbb{Z}_K/\mathfrak{p}^\beta$，其中 K 是数域，$\mathbb{Z}_K$ 是其整数环，而 $\mathfrak{p}$ 是 $\mathbb{Z}_K$ 的非零素理想（因此 $\mathbb{Z}_K/\mathfrak{p}^\alpha$ 和 $\mathbb{Z}_K/\mathfrak{p}^\beta$ 是某个 $p \in \mathcal{P}$ 的有限环，其阶为 p 的幂）。或许可以借助本文以及 [CS21] 中的思路，对这些工作作进一步改进。

2.5. 有限交换 p-群之间的函数表示。若 A 是有限生成交换群，则对某个 $N \in \mathbb{Z}^+$，存在满群同态 $\varepsilon\colon \mathbb{Z}^N \to A$。事实上，除去一个无关紧要的同构，我们可以将 A 写成 $\bigoplus_{i=1}^N \mathbb{Z}/a_i\mathbb{Z}$，其中参数为 $1 \neq a_i \in \mathbb{N}$，然后取

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

正如引理 2.12 中所回顾的，拉回映射 ε^* 限制为一个单射群同态

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

因此，每个 $f \in \mathcal{F}(A, B)$ 的函数次数都与其拉回到 $\mathbb{Z}^N$ 后的函数次数相同；根据定理 2.8b)，后者具有典范级数表示。

对于交换群 A 和 B，我们回顾如下量

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

该量由 [AM21] 引入，并在 [CS21] 中得到进一步研究。它仅取决于 A 和 B 的同构类型；此外，正如 [CS21，推论 4.3]，所示

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

当 A 和 B 都是非平凡有限群时，[CS21，定理 4.9] 表明，$\delta(A, B) < \infty$ 当且仅当 A 和 B 是同一个 $p \in \mathcal{P}$ 对应的 p-群。此外，根据 [CS21，定理 4.9c)]，若 $p \in \mathcal{P}$ 和 $N, \beta, \alpha_1, \ldots, \alpha_N \in \mathbb{Z}^+$，则

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

其中

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

定理 2.24。设 $p \in \mathcal{P}$，令 $N, \alpha_1, \ldots, \alpha_N \in \mathbb{Z}^+$，并令 $A := \bigoplus_{i=1}^N \mathbb{Z}/p^{\alpha_i}\mathbb{Z}$。设 B为交换群，并设 $F\colon \mathbb{Z}^N \to B$ 为函数 $f\colon A \to B$的拉回。

a) 若 $\beta \in \mathbb{Z}^+$ 满足对所有 $a \in A$，$p^\beta f(a) = 0$，则

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

b) 对所有 $h \in \mathbb{Z}^+$ 及所有满足 $|\underline{n}| > \delta_p(\underline{\alpha}, h)$ 的 $\underline{n} \in \mathbb{N}^n$，

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

c) 设 $\mu_h\colon B \to B/p^hB$ 为商映射。对于每个满足 $\mu_h \circ F\colon \mathbb{Z}^N \to B/p^hB$ 是某个函数 $g\colon A \to B/p^hB$的拉回的函数 $F\colon \mathbb{Z}^N \to B$，b) 部分的结论仍然成立。

证明。a) 设 $\underline{B} := \langle f(A)\rangle$ 为由 f 的像生成的子群。由于对所有 $a \in A$，都有 $f(a) \in B[p^\beta]$，因此我们有 $\underline{B} = \underline{B}[p^\beta]$。我们可以将 f 视为一个以 $\underline{B}$ 为陪域的函数；根据 [CS21, Cor. 3.10b)]，这不会改变它的函数次数，因此我们可以假设 $B = \underline{B}$。于是，根据 [CS21, Thm. 4.9c)],，我们得到

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

结果由定理 2.8 得出。

b) 令 $\mu_h : \ B \to B/p^hB$ 为商映射。映射 $\mu_h \circ f : \ A \to B/p^hB$ 的函数次数至多为 $\delta_p(\underline{\alpha}, h)$，因此其到 $\mathbb{Z}^N$ 的拉回的函数次数也至多为 $\delta_p(\underline{\alpha}, h)$，即 $\mu_h \circ F$。对于所有满足 $|\underline{n}| > \delta_p(\underline{\alpha}, h)$ 的 $\underline{n} \in \mathbb{N}^N$，这意味着 $\mu_h \circ \Delta^{\underline{n}} F = \Delta^{\underline{n}}(\mu_h \circ F) \ = 0$，从而对于所有 $\underline{x} \in \mathbb{Z}^N$，$\mu_h(\Delta^{\underline{n}} F(\underline{x})) \ = \mu_h \circ \Delta^{\underline{n}} F(\underline{x}) \ = 0$，即 $\Delta^{\underline{n}} F(\underline{x}) \ \in p^h B$。

c) 上一部分的证明只用到了 $\mu_h \circ F$ 是从 A 拉回得到的这一点。 □

我们推出以下结果，后一个结果是前一个结果的向量值类比。

推论 2.25. 设 $p \in \mathcal{P}$，并设 $N, \beta, \alpha_1, \ldots, \alpha_N \in \mathbb{Z}^+$。设 $f\colon \bigoplus_{i=1}^N \mathbb{Z}/p^{\alpha_i}\mathbb{Z} \to \mathbb{Z}/p^\beta\mathbb{Z}$ 是任意函数，设 $F\colon \mathbb{Z}^N \to \mathbb{Z}/p^\beta\mathbb{Z}$ 是 f 的拉回，并设 $\tilde{F}\colon \mathbb{Z}^N \to \mathbb{Z}$ 是 F 的真提升。则：

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

b) 对所有 $h \in \mathbb{Z}^+$ 以及所有满足 $|\underline{n}| > \delta_p(\underline{\alpha}, h)$ 的 $\underline{n} \in \mathbb{N}^n$，

$$p^h \ \big| \ \Delta^{\underline{n}} \tilde{F}(\underline{0}) \, .$$

˜证明。a) 由于 $\mathrm{fdeg}(F) \ = \mathrm{fdeg}(F) \ = \mathrm{fdeg}(f) \ \leq \delta_p(\underline{\alpha}, \beta)$，这由定理 2.8b) 得出。

b) 假设 $\underline{n} > \delta_p(\underline{\alpha}, h)$，我们证明 p^h 整除 $\Delta^{\underline{n}} \tilde{F}(0)$。若 $h \geq \beta$，则

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

于是 $\Delta^{\underline{n}} \tilde{F}(0) \ = 0$，它可被 p^h 整除。因此，我们可以假设 $1 \leq h < \beta$。我们证明˜在此情形下，定理 2.24c) 适用于 F 和 $\mathbb{Z}$，分别代替 F 和 B；由此得到 $\Delta^{\underline{n}} \tilde{F}(0) \ \in p^h\mathbb{Z}$，即 $p^h \mid \Delta^{\underline{n}} \tilde{F}(0)$，正如所需。利用典范满射 $\mu_\beta\colon \mathbb{Z} \to \mathbb{Z}/p^\beta\mathbb{Z}$ 和 $\mu_h^\beta\colon \mathbb{Z}/p^\beta\mathbb{Z} \to \mathbb{Z}/p^h\mathbb{Z}$，只需确认 $\mu_h \circ \tilde{F}$ 是 $g := \mu_h^\beta \circ f$ 的拉回。然而，由于 F 是 f 的拉回，我们得到 $\mu_h^\beta \circ F$ 是 $\mu_h^\beta \circ f$ 的拉回。但是，$\mu_h^\beta \circ F = \mu_h \circ \tilde{F}$，因为 $\mu_h = \mu_h^\beta \circ \mu_\beta$ 和 $\mu_\beta \circ \tilde{F} = F$，而 $\tilde{F}$ 是 F 的提升。˜因此，$\mu_h \circ F$ 确实是函数 g 的拉回。□

推论 2.26。设 $p \in \mathcal{P}$，设 $N, \beta, \alpha_1, .., \alpha_N \in \mathbb{Z}^+$。对于非空指标集 J 中的每个 j，设 $\beta_j \in \{1, \ldots, \beta\}$。设 $f\colon \bigoplus_{i=1}^N \mathbb{Z}/p^{\alpha_i}\mathbb{Z} \to \prod_{j \in J} \mathbb{Z}/p^{\beta_j}\mathbb{Z}$ 是任意函数，设 $F\colon \mathbb{Z}^N \to \prod_{j \in J} \mathbb{Z}/p^{\beta_j}\mathbb{Z}$ 是 f 的拉回，并设 $\tilde{F}\colon \mathbb{Z}^N \to \prod_{j \in J} \mathbb{Z} = \mathbb{Z}^J$ 是 F 的真提升。则：

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

˜b) 如果 F 是逐坐标真提升的，那么，对于所有 $h \in \mathbb{Z}^+$ 以及所有满足 $|\underline{n}| > \delta_p(\underline{\alpha}, h)$ 的 $\underline{n}$，p^h 整除 $\Delta^{\underline{n}} \tilde{F}(0)$ 的每个坐标。

证明。a) $\prod_{j\in J}\mathbb{Z}/p^{\beta_j}\mathbb{Z}$ 的指数整除 p^β，因此

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

并且定理 2.8b) 可用于得出该结果。

b) 固定 $j\in J$，并假设 F 满足假设条件。则 $\tilde{\pi}_j\circ F$ 是 $\pi_j\circ F$ 的真提升，其中 $\pi_j\colon\ \prod_{i\in J}\mathbb{Z}/p^{\beta_i}\mathbb{Z}\to\mathbb{Z}/p^{\beta_j}\mathbb{Z}$ 和 $\tilde{\pi}_j\colon\ \mathbb{Z}^J\to\mathbb{Z}$ 是坐标投影。因此，函数 $F_j\colon=\tilde{\pi}_j\circ F$、$f_j\colon=\pi_j\circ f$ 满足推论 2.25b) 的要求，由此得到

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

3. The Group-Theoretic Ax-Katz Theorem

3.1. Wilson 引理。设 $N\in\mathbb{Z}^+$。对于 s、t_1、.....、$t_N\in\mathbb{N}$，我们定义

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

我们用 $\mathbb{Z}_{(p)}$ 表示非负 p-进赋值的有理数集合。对于每个 $x\in\mathbb{R}$，我们定义

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

现在，设 A 和 B 是交换群，且 $S\subseteq A$ 是一个有限子集。对每个 $f\in B^A$，按照[KP12], ，我们定义

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

以下结果是 [Wi06, 引理 4]的一个等价（但更简单）的改写。

引理 3.1. 设 $p\in\mathcal{P}$ 且设 $N,\beta\in\mathbb{Z}^+$。若 $f\in\mathbb{Z}^{\mathbb{Z}^N}$ 满足

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

then

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

证明. 第一步：若 $0\le i\le p-2$，则 $\sum_{x\in\mathbb{Z}/p\mathbb{Z}}x^i=0$：事实上，取循环群 $(\mathbb{Z}/p\mathbb{Z})^\times$的一个生成元$\zeta$，可得

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

因此，如果 $i_1,\dots,i_\beta\in[p-1)$，那么

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

我们推得，若对所有 $1\le j\le\beta$，$g\in\mathbb{Z}_{(p)}[x_1,\dots,x_\beta]$ 的 $\deg_j(g)\le p-2$，则

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

步骤 2：若该结论对一组函数 $f_1, \dots, f_m$ 成立，那么对它们生成的 $\mathbb{Z}^{\mathbb{Z}^N}$ 的 $\mathbb{Z}$-子模也成立。由此以及定理 2.8，只需证明该结论对多项式成立

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

其中 $(n_1, \dots, n_N) \in \mathbb{N}^N$ 任意，且满足 $|\underline{n}| < (p-1)(N-\beta+1)$。在此条件下，我们有

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

否则，我们将得到 $|\underline{n}| = \sum_{j=1}^N n_j \ge (p-1)(N-\beta+1)$。因此，不失一般性，我们可以假设，对于所有 $1 \le j \le \beta$，都有 $n_j < p-1$。于是，对于每个固定的 $\underline{y} = (y_{\beta+1}, \dots, y_N) \in \mathbb{Z}^{N-\beta}$，

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

并且对于所有 $1 \le j \le \beta$，$\deg_j(g_{\underline{y}}) = n_j \le p-2$。因此，利用步骤 1，我们得到

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

3.2. 定理 1.7 的证明。

定理 1.7 的证明。不失一般性，我们可以假设，对于 $1 \le j \le r$，

$$d_j := \mathrm{fdeg}(f_j) > 0.$$

令

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

并令

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

我们有

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

因此

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

对于 $1 \le j \le r$，我们定义 $\chi_j : \mathbb{Z} \to \mathbb{Z}/p^\beta\mathbb{Z}$ 为

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

由于 χ_j 是从 $\mathbb{Z}/p^{\beta_j}\mathbb{Z}$ 拉回的，因此它具有有限函数次数；设 $\widetilde{\chi}_j$ 是将 χ_j 从 $\mathbb{Z}/p^\beta\mathbb{Z}$ 提升到 $\mathbb{Z}$ 的真提升。设 $\chi : \mathbb{Z}^r \to \mathbb{Z}/p^\beta\mathbb{Z}$ 为 $\bigotimes_{j=1}^r \chi_j$ 的 χ_j 的张量积，并设 $\widetilde{\chi} : \mathbb{Z}^r \to \mathbb{Z}$ 为 $\bigotimes_{j=1}^r \widetilde{\chi}_j$ 的 $\widetilde{\chi}_j$ 的张量积：对于所有 $(x_1, \dots, x_r) \in \mathbb{Z}^r$，

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

对于 $1 \le j \le r$，设 $F_j\colon \mathbb{Z}^N \to \mathbb{Z}/p^{\beta_j}\mathbb{Z}$ 为 f_j 的拉回，并设 $\tilde{F}_j$ 是将 F_j 从 $\mathbb{Z}/p^{\beta_j}\mathbb{Z}$ 提升到 $\mathbb{Z}$ 的真提升。那么，对于由 $\underline{x} \mapsto [\underline{x}] := (x_j + p\mathbb{Z})_{j=1}^N$ 给出的双射 $[p)^N \to (\mathbb{Z}/p\mathbb{Z})^N$，对所有 $\underline{x} \in [p)^N$，我们有

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

因此，所需结论“p^β 整除 $\#Z(f_1, \dots, f_r)$”等价于

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

因此也等价于

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

根据推论 2.25，存在一个函数 $c_j\colon \mathbb{N} \to \mathbb{Z}$，使得对于除有限多个$n \in \mathbb{N}$之外的所有$n \in \mathbb{N}$，都有 $c_j(n) = 0$；并且对于所有 $x \in \mathbb{Z}$，

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

并且对于每个 $h \in \mathbb{Z}^+$，

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

因此，对于所有 $\underline{x} \in \mathbb{Z}^N$，

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

因此，

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

因此，要证明 (12)，只需证明对于每个 $\underline{n} = (n_1, \dots, n_r) \in \mathbb{N}^r$，

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

现在，对于每个 $1 \le j \le r$，令 h_j 为满足以下条件的唯一整数

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

于是，由（13）可得 $\operatorname{ord}_p(c_j(n_j)) \ge h_j$。因此，一方面，

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

并且如果 $\alpha \geq \beta$，那么（14）显然成立。另一方面，如果 $\alpha < \beta$，那么 $\beta - 1 - \alpha \geq 0$。˜因此，由于 $\mathsf{fdeg}(F_j) = \mathsf{fdeg}(F_j) = \mathsf{fdeg}(f_j) \leq d_j$，利用 [AM21，定理 4.3 和引理 6.1]，（15）、 $\mathcal{M}$ 的定义、（11）以及 $\mathcal{M} \geq 1$，可得

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

因此，引理 3.1 推出

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

结合 (16) 和 (17)，得到 (14)，这就完成了定理 1.7 的证明。 □

4. p-WEIGHTS

4.1. p-权次数。设 $p \in \mathcal{P}$。每个 $d \in \mathbb{N}$ 都可以写成 $d = \sum_{i=0}^{N} a_i p^i$的形式，其中系数 $a_i \in [p$ 唯一确定。利用这个基 p 展开，我们定义 d 的 p-权为

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

我们有 $\sigma_p(d) \leq d$，且等号成立当且仅当 $d \in [p)$。对于固定的 p 和较大的 d，有 $\sigma_p(d) = O(\log d)$，因此 d 的 p-权可能远小于其本身 d。

设 R 是一个交换环（不要求有幺元）。非零单项式项 $c\,t_1^{d_1}\cdots t_n^{d_n}$ 的 p-权次数（其中 $c \in R \setminus \{0\}$）定义为

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

非零多项式 $f \in R[t_1, \ldots, t_n]$ 的 p-权次数是其非零单项式项的最大 p-权次数。我们还规定 $\sigma_p(0) := -\infty$。多项式的次数为正，当且仅当其 p-权次数为正。

我们还需要定义函数 $f_1\colon A_1 \to R, \ldots, f_n\colon A_n \to R$在交换群 $A_1, \ldots, A_n$ 上的乘积 $\bigotimes_{i=1}^{n} f_i$，其中 R 仍然是一个非结合环，其定义如下：

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

在此情形下，我们有以下引理。

引理 4.1。对于每个 $1 \le j \le n$，令 $a_{j,\,1}$，…，$a_{j,\,K(j)} \in A_j \subseteq \prod_{i=1}^n A_i$，并令 $(a_1,\,\ldots,\,a_K)$ 为所有 $K := K(1) + \cdots + K(n)$ 给定元素 $a_{j,\,k}$ 的一个置换。则

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

证明。如果 $a=(a,0) \in A_1 = A_1\times\{0\}\subseteq A_1\times A_2$ 且 $(x_1,x_2)\in A_1\times A_2$，则

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

因此，$\Delta_a(f_1\otimes f_2) = (\Delta_a f_1)\otimes f_2$。更一般地，如果 $a\in A_j$，则

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

由此以及算子 $\Delta_{a_{j,\,k}}$ 的交换性，可得所述等式。 □

引理 4.2。我们有

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

特别是，

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

当 R 是整环且函数 f_1、……、f_n 均非零时，两个不等式中的等号均成立，见 [AM21，引理 6.2]，。

证明。假设 $1\le j\le n$。引理 4.1 表明，只要 $K(j) > \mathrm{fdeg}(f_j)$，就有 $\Delta_{a_{j,1}}\cdots\Delta_{a_{j,\,K(j)}}\big(f_1\otimes\cdots\otimes f_n\big) = 0$，因为

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

且 $\Delta_{a_{j,1}}\cdots\Delta_{a_{j,K(j)}}f_j = 0$，若 $K(j) > \mathrm{fdeg}(f_j)$。这意味着 $\mathrm{fdeg}_j\big(\bigotimes_{i=1}^n f_i\big) \le \mathrm{fdeg}(f_j)$。将这些不等式与定理 2.3 结合，可得

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

剩下要证明的是

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

只要 R 是一个整环，且 $K(j) := \mathrm{fdeg}(f_j) \ge 0$，对所有 $1\le j\le n$均成立。为证明这一点，我们对每个 $1\le j\le n$ 选取元素 $a_{j,\,1}$，…，$a_{j,\,K(j)}\in A_j$，使得

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

于是，由引理 4.1，且由于 R 是一个整环，$\Delta_{a_{1,\,1}}\cdots\Delta_{a_{n,\,K(n)}}\big(f_1\otimes\cdots\otimes f_n\big) = \big(\Delta_{a_{1,\,1}}\cdots\Delta_{a_{1,\,K(1)}}f_1\big)\otimes\cdots\otimes\big(\Delta_{a_{n,\,1}}\cdots\Delta_{a_{n,\,K(n)}}f_n\big) \neq 0$，这确实意味着 $\mathrm{fdeg}\big(\bigotimes_{i=1}^n f_i\big) \ge K(1)+\cdots+K(n) = \sum_{i=1}^n \mathrm{fdeg}(f_i)$。□

下一个结果是在更一般的情形下对 [AM21, Theorem 10.3] 的前半部分。

命题 4.3. 设 $p \in \mathcal{P}$，并设 R 是特征为 p 的交换环。设 $f \in R[t_1, \dots, t_n]$ 是一个多项式，其关联函数为 $E(f) \in R^{R^n}$。那么

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

证明。由于 $\operatorname{fdeg}(E(f)) = -\infty$ if $E(f) = 0$，我们可以假设 $E(f) \neq 0$。根据 [AM21, 引理 3.2]，有 $\operatorname{fdeg}(f_1+f_2) \leq \max(\operatorname{fdeg}(f_1), \operatorname{fdeg}(f_2))$。由于 $\sigma_p(f)$ 是 f 的非零单项式项的 p-权次数的最大值，因此只需考虑单项式项的情形

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

利用 [AM21, 引理 6.1] 和引理 4.2，我们得到

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

我们已将问题化归为一元单项式情形，接下来必须证明：对所有 $d \in \mathbb{Z}^+$，都有

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

将 $d = \sum_{i=0}^N a_i p^i$ 写成 $a_i \in [p)$ 的形式，并利用 [AM21, 引理 6.1],，得到

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

si由于每个 $E(t^{p^i})$ 都是非零群同态，因此其函数次数为 1。 □

4.2. 广义 Moreno-Moreno 定理。结合推论 1.9 和命题 4.3，我们得到：

定理 4.4. 设 R 是一个特征为素数 p 、阶为 p^N 的有限交换环。设 $f_1, \dots, f_r \in R[t_1, \dots, t_n]$ 为非零多项式。若 $Z := Z_{R^n}(f_1, \dots, f_r)$，则

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

证明。如果所有函数 $E(f_j)$ 均为零，则结果显然成立。如果部分但非全部函数 $E(f_j)$ 为零，只需对函数集合 $f_j$with $E(f_j) \neq 0$ 证明该定理，因为这样得到的下界至少与所述下界一样好。因此，我们可以假设推论 1.9 适用。由此得到的不等式

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

如果将每个函数次数 $\operatorname{fdeg}(E(f_j))$ 替换为 $\operatorname{fdeg}(E(f_j))$ 的一个上界（例如命题4.3中给出的上界），结论仍然成立。□

如果在定理 4.4 中取 R 为有限域 $\mathbb{F}_{p^N}$，我们便得到 Moreno-Moreno 定理 [MM95，定理 1]。

定理 4.5（Moreno-Moreno）。设 $p \in \mathbb{P}$ 和 $q := p^N$。设 $f_1, \dots, f_r \in \mathbb{F}_q[t_1, \dots, t_n]$ 为非零多项式。若 $Z := Z_{\mathbb{F}_q}(f_1, \dots, f_r)$，则

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

4.3. 正特征下多项式函数的函数次数。设 R 为特征为 p 的交换环。式 (18) 中是否必然取等号？当 R 是域时，AM21 的定理 10.3] 给出了答案。在这一结果中，Aichinger-Moosbauer 证明，当 R 是特征为 p 的无限域时，$\mathrm{fdeg}(E(f)) = \sigma_p(f)$。本节稍后将证明，只要 R 是特征为 p 的无限整环，这一结果仍然成立。

$R = \mathbb{F}_q$ 的情形与本文的主要结果关系更为密切：严格不等式 $\mathrm{fdeg}(E(f)) < \sigma_p(f)$ 将进一步改进 Ax-Katz 定理。然而，事实证明严格不等式确实可能成立，但其带来的改进仅限于此前已经得到充分理解的 Ax-Katz 定理的改进。

为此，如果对于所有 $1 \le j \le n$都有$d_j \le q-1$，我们称非零单项式项 $c_{\underline{d}} t_1^{d_1} \cdots t_n^{d_n} \in \mathbb{F}_q[t_1, \ldots, t_n]$ 是约化的。（请注意，这强烈依赖于基域。）如果一个多项式的每个非零单项式项都是约化的，则称该多项式是约化多项式。

仅利用对于所有 $x \in \mathbb{F}_q$都有 $x^q = x$ 这一事实，很容易看出，对于每个 $f \in \mathbb{F}_q[t_1, \ldots, t_n]$，都存在一个约化多项式 $\overline{f} \in \mathbb{F}_q[t_1, \ldots, t_n]$，它与 f 诱导出相同的函数 $\mathbb{F}_q^n \to \mathbb{F}_q$。早在 [年，Chevalley 就证明了，$\mathbb{F}_q^{\mathbb{F}_q^n}$ 中的每个函数都等于 $E(f)$，其中 f 是唯一的约化多项式。（关于英文证明以及一些适度的推广，参见 [Cl14、§2.3 和 §3.1]。）特别地，上文提到的多项式 $\overline{f}$ 正是与 f 诱导出相同函数的唯一约化多项式。

现在，对于任意的 $f_1, \ldots, f_r \in \mathbb{F}_q[t_1, \ldots, t_n]$，由于解集

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

只取决于关联函数 $E(f_1) \ldots, E(f_r)$，因此我们总有

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

将 $f_1, \ldots, f_r$ 替换为 $\overline{f_1}, \ldots, \overline{f_r}$，即可轻易得到许多 Chevalley-Warning 型结果的加强版本——尤其是 Chevalley-Warning 和 Ax-Katz 定理——因为在这一过程中，各多项式的次数都不会增加。

以下结果是 [AM21，定理 10.3] 的一部分。

定理 4.6（Aichinger-Moosbauer）。设 $f \in \mathbb{F}_q[t_1, \ldots, t_n]$ 为一个非零多项式，且 $E(f) \in \mathbb{F}_q^{\mathbb{F}_q^n}$ 为其关联多项式函数。则

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

命题 4.3 和定理 4.6 表明

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

tha也就是说，转为约化多项式也不会提高 p-权次数。因此，in 在 Moreno-Moreno 定理的情形下，可以将结论改进为

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

根据定理 4.6，这是推论 1.9 对 $\mathbb{F}_q$ 上多项式的最优应用。

注 4.7. 对于约化多项式 $f \in \mathbb{F}_p[t_1, \ldots, t_n]$，我们有 $\deg(f) = \sigma_p(f)$，因此当 $q = p$ 时，Moreno-Moreno 并未对 Ax-Katz 作出实质性改进。

现在，我们准备借助以下结果推广 [AM21，定理 10.3] .

引理 4.8. 设 A 是一个无限交换余域，且为有限生成的 $\mathbb{F}_p$-代数。设 $x_1, \ldots, x_m \in A \setminus \{0\}$，并设 $M \in \mathbb{Z}^+$。那么存在一个A 的极大理想 $\mathfrak{m}$，使得：

(i) $x_1, .., x_m \notin \mathfrak{m}$，且 (ii) $A/\mathfrak{m}$ 是一个大小大于 M的有限域。

证明. 用 $x := x_1 \cdots x_m$ 替换 $x_1, \ldots, x_m$后，我们归结为 $m = 1$的情形。Zariski 引理 [Cl-CA，定理 11.1] 表明，对于 A的每个极大理想 $\mathfrak{m}$，域 $A/\mathfrak{m}$ 是有限维的 $\mathbb{F}_p$-向量空间，因而是有限域。相同的论证表明A 本身不是域；此外， A 是一个诺特环 [Cl-CA，推论 8.39]。而且，由于 A是域 $\mathbb{F}_p$ 上的有限生成代数，它是一个 Jacobson 整环 [Cl-CA，命题 11.3b)], ，因此$\bigcap_{\mathfrak{m} \in \operatorname{MaxSpec} A} \mathfrak{m} = (0)$。特别地， A 有无限多个极大理想，因为整环中有限多个非零理想的交仍是非零的。由此可知，满足条件 $x \notin \mathfrak{m}$ 的 A 的极大理想集合 $\mathcal{U}(x)$ 非空。我们进一步断言， $\mathcal{U}(x)$ 是无限集：否则，若有 $\mathcal{U}(x) = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_n\}$，则对 $1 \leq i \leq n$，取 $y_i \in \mathfrak{m}_i \setminus \{0\}$，可见 $xy_1 \cdots y_n$是 A中的非零元素，且属于 A的每个极大理想：矛盾。最后，根据 [Cl-CA，定理 22.23], ，在任意诺特环 S中，对所有 $M \in \mathbb{Z}^+$，满足 S/I 为大小至多为 M的有限环的 M 的理想 I 只有有限多个。因此，在 A的任意无限极大理想族中，剩余环的大小趋于无穷。□

定理 4.9. 设 R 是一个特征为 p 的无限交换整环。设 $f \in R[t_1, \ldots, t_n]$，并令 $E(f) \in \mathrm{P}(R^n, R)$ 为相应的多项式函数。那么

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

证明。由命题 4.3，只需证明 $\operatorname{fdeg}(E(f)) \geq \sigma_p(f)$。令 K 为 R 的分式域。

情形 1， $K/\mathbb{F}_p$ 是代数域扩张：此情形已由 [AM21, Thm. 10.3], 涵盖，因为必有 $R = K$：事实上，对每个非零元素 $x \in R$，都存在正整数 n_x 使得 $x^{n_x} = 1$，因此 $x^{-1} = x^{n_x - 1} \in R$。

情况 2， $K/\mathbb{F}_p$ 是超越的：在这种情况下， R 必须包含相对于 $\mathbb{F}_p$ 超越的元素：令 t 为这样的一个元素，并令 A 为由 t 和 f 的系数生成的 R 的 $\mathbb{F}_p$-子代数。令 $a \in \mathbb{Z}^+$。根据引理 4.8，A 存在一个极大理想 $\mathfrak{m}$，它不包含 f 的任何系数，并且 $\mathbb{F} := A/\mathfrak{m}$ 是一个阶至少为 p^a 的有限域 $\mathbb{F}$。令 $\underline{f}$ 为 f 在 $\mathbb{F}[t_1, \ldots, t_n]$中的像。根据引理 2.12，我们有

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

根据我们对 $\mathfrak{m}$ 的选择，$\underline{f}$ 中非零系数单项式与 f 中非零系数单项式相同，因此 $\sigma_p(\underline{f}) = \sigma_p(f)$。选取大于 $\max_{1 \leq i \leq n} \deg_i(f)$ 的 a，使 $\underline{f}$ $\mathbb{F}$ 成为约化的。于是由定理 4.6 可得

$$\operatorname{fdeg}(E(f)) \geq \operatorname{fdeg}(E(\underline{f})) = \sigma_p(\underline{f}) = \sigma_p(f). \qquad \square$$

5. Further Work

很自然会想到将定理 1.7 推广：不再取 $(\mathbb{Z}/p\mathbb{Z})^N$，而是令 A 为任意有限交换 p-群。这样的结果将在即将发表的工作 [CS23] 中给出。证明遵循相同的基本策略： p-进可整除性来自推论 2.25 与引理 3.1 向形如 $\int_{\prod_{i=1}^N [p^{\alpha_i})} f$ 的和的推广相结合。

以下简要概述本研究的内容：为解决关于确定 $\mathrm{ord}_p(\int_{\prod_{i=1}^N [p^{\alpha_i})} f)$ 的数论问题，针对的是

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

用 $n_1, \ldots, n_N$ 表示并不太困难，但要解决离散优化问题，即对每个固定的 $\underline{\alpha} = (\alpha_1, \ldots, \alpha_N)$，在所有满足固定 $d := |\underline{n}|$ 条件的 $\underline{n} = (n_1, \ldots, n_N) \in \mathbb{N}^N$ 中将该量最小化，则需要更多工作。然后，我们必须将由此得到的结果与推论 2.25 得到的结果结合，最小化总的 p-进整除性。一般情形下得到的答案十分复杂，这表明这些复杂性可能是问题本身固有的。

引理 3.1 的 $\beta = 1$ 情形给出了 Ax [Ax64] 的一个结果；我们称之为 Ax 引理。Ax 引理包含了引言中提到的 Chevalley-Warning 定理的十行证明的大部分内容。这在 Aichinger-Moosberger 演算中提出了一个进一步的问题。

˜问题 5.1。设 A 和 B 是有限交换 p-群。对所有满足 $\mathrm{fdeg}(f) \le d$ 的 $f \in B^A$，使得 .....成立的最大 $d \in \mathbb{N}$ 是什么?

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

我们将这个最大可能的 d 称为求和不变量 $\sigma(A, B)$。用这种记法，Ax 引理可表述为:

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

在论文 [CT23] 中，将证明 Ax 引理的以下推广:

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

在 [CT23] 中，我们利用 (19) 得出 Ax-Katz 定理的一个定性推广，该推广适用于任何大小可被 p 整除的有限非结合环 R：若固定多项式 $f_1, \ldots, f_r$ 的数量和次数，则当变量数 N 增加时，$\mathrm{ord}_p(\#Z_{R^N}(f_1, \ldots, f_r))$ 趋于无穷。

这类结果也可由 [CS23] 的主定理推出——但论证方式不同。与此处以及 [CS23]，中给出的证明不同， [CT23] 中的论证并未使用基本表示（定理 2.8）：它们完全在有限特征下进行。

注意，(19) 是引理 3.1 的有限特征变体，但当 $\beta > 1$ 时，(19) 的结论强于引理 3.1 的结论。起初这似乎很奇怪：如果在引理 3.1 中将 $\mathrm{fdeg}(f) < (p-1)(N-\beta+1)$ 弱化为 $\mathrm{fdeg}(f) < N(p-1)$，那么一般而言 $\mathrm{ord}_p(\int_{[p)^N} f) \ge \beta$ 并不成立。然而，为了比较这两个结果，我们必须取 $f\colon (\mathbb{Z}/p\mathbb{Z})^N \to \mathbb{Z}/p^\beta\mathbb{Z}$ 并将其拉回到 $F\colon \mathbb{Z}^N \to \mathbb{Z}/p^\beta\mathbb{Z}$，因此 (19) 的界只适用于满足 p-周期性的函数 $F\colon \mathbb{Z}^N \to \mathbb{Z}/p^\beta\mathbb{Z}$，而引理 3.1 适用于所有函数 $F\colon \mathbb{Z}^N \to \mathbb{Z}/p^\beta\mathbb{Z}$。因此，在将引理 3.1 应用于关于有限交换群之间映射的结果时

我们丢失了关键信息，即这些函数源自有限特征并由此被拉回所具有的周期性。这解释了为什么我们目前的方法还包括定理 2.24：该定理利用周期性来根据基本表示的系数推导出更多的 p-进整除性。

本文及 [CS23] 中采用的双管齐下的方法，在定量上似乎优于 [CT23]，中单独采用 $\sigma(A, B)$ 的方法，不过厘清两者之间的关系会很有意思。

References

[AM21] E. Aichinger 和 J. Moosbauer, *Chevalley-Warning type results on abelian groups.*《代数杂志》569（2021），30–66。[AT92] N. Alon 和 M. Tarsi *Colorings and orientations of graphs*。《组合数学》12（1992），125–134。[Ax64] J. Ax, *Zeroes of polynomials over finite fields*。《美国数学杂志》86（1964），255–261。[CC] P.-J. Cahen 和 J.-L. Chabert, *Integer-valued polynomials.*《数学调查与专著》第48卷。美国数学学会，普罗维登斯，罗得岛州，1997年。[Ch35] C. Chevalley, *Démonstration d'une hypothèse de M. Artin.*《汉堡大学数学研讨班论文集》11（1935），73–75。

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

[14] *The Combinatorial Nullstellensätze revisited* 21

Clark, . Cl P.L. Clark, .《电子组合学杂志》（2014），第4期，论文4.15，共17页。[CS21] P.L. Clark 和 U. Schauz, *Functional Degrees* 608 2022 691 718 。《代数杂志》（），–。[CS23] P.L. Clark 和 U. Schauz, *Functional Degrees and Arithmetic Applications III: The Main Theorem* 。准备中。[CT23] P.L. Clark 和 N. Triantafillou, *The generalized group-theoretic Ax Lemma*。准备中。[CW18] P.L. Clark 和 L.D. Watson, *Varga's theorem in number fields.*《整数》18（2018），论文编号A74，共11页。[Fr09] M. Fr´echet, *Une définition fonctionnelle des polynomes*。《新数学年刊：综合理工学院考生杂志》9（1909），145–162。[GGZ] A. Geroldinger、D.J. Grynkiewicz 和 Q. Zhong, *Combinatorial Factorization Theory*。预印本。[Gr22] D.J. Grynkiewicz, *A Generalization of the Chevalley-Warning and Ax-Katz Theorems with a View Towards Combinatorial Number Theory.* `https://arxiv.org/abs/2208.12895` [Ho05] X.-D. Hou, *A note on the proof of a theorem of Katz*。《有限域应用》11（2005），316–319。[Ka71] N.M. Katz, *On a theorem of Ax*。《美国数学杂志》93（1971），485–499。[Ka09] D.J. Katz, *Point count divisibility for algebraic sets over $\mathbb{Z}/p\mathbb{Z}$ and other finite principal rings* 137 2009 4065 4075 。《美国数学会会刊》（），–。[Ka12] D.J. Katz, *On theorems of Delsarte-McEliece and Chevalley-Warning-Ax-Katz.*《设计、编码与密码学》65（2012），291–324。[KP12] R.N. Karasev 和 F.V. Petrov, *Partitions of nonzero elements of a finite field into pairs*。《以色列数学杂志》192（2012），143–156。[La04] M. Laczkovich, *Polynomial mappings on abelian groups.*《方程数学》68（2004），177–199。[Lei02] A. Leibman, *Polynomial mappings of groups*。《以色列数学杂志》129（2002），29–60。[MM95] O. Moreno 和 C.J. Moreno, *Improvements of the Chevalley-Warning and the Ax-Katz theorems* 117 1995 241 244 。《美国数学杂志》（），–。[MR75] M. Marshall 和 G. Ramage, *Zeros of polynomials over finite principal ideal rings*。《美国数学会会刊》49（1975），35–38。[Os19] A. Ostrowski, *Über ganzwertie Polynome in algebraischen Zahlkörpen*。《纯粹与应用数学杂志》149（1919），117-124。[Sc08] U. Schauz, *Algebraically solvable problems: describing polynomials as equivalent to explicit solutions.* 15 2008 1, 10, 35 《电子组合学杂志》（），研究论文，共 页。

[Sc14] U. Schauz, *Classification of polynomial mappings between commutative groups.*《数论杂志》139（2014），1–28。[Va14] L. Varga, *Combinatorial Nullstellensatz modulo prime powers and the parity argument*。模素数幂的组合零点定理与奇偶性论证。《电子组合学杂志》21（2014），第4期，论文4.44，共17页。[Wa35] E. Warning, *Bemerkung zur vorstehenden Arbeit von Herrn Chevalley*。《汉堡大学数学研讨班论文集》11（1935），76–83。[Wa89] D.Q. Wan, *An elementary proof of a theorem of Katz*。《美国数学杂志》111（1989），1–8。[We77] C.S. Weisman, *Some congruences for binomial coefficients.*《密歇根数学杂志》24（1977），141–151。[Wi06] R.M. Wilson, *A lemma on polynomials modulo p^m and applications to coding theory.*《离散数学》306（2006），3154–3165。