Equations over finite abelian groups

Erhard Aichinger

Institute for Algebra
Johannes Kepler University Linz
Linz, Austria

AAA106, Olomouc, February 2025

Supported by the Austrian Science Fund (FWF) : P33878

Zeros of polynomials

Theorem J. Ax 1964

Let $f \in \mathbb{F}_q[x_1, \ldots, x_N]$ nonconstant, $V(f) := \{\boldsymbol{a} \in \mathbb{F}_q^N \mid f(\boldsymbol{a}) = 0\}$, $e \in \mathbb{N}_0$ with $e < \frac{N}{\deg(f)}$. Then

$$q^e \mid \#V(f).$$

Examples:

- $f = a_1x_1 + \cdots + a_Nx_N + b$. Then $\#V(f) \in \{0, q^{N-1}\}$.
- $f = x_1x_2x_3 + x_4x_5x_6$. Then $q \mid \#V(f)$ since $1 < 6/3$ because of the Theorem. Furthermore, $q^2 \nmid \#V(f)$ [D. Katz 2012].

Improved to $f_1 = \cdots = f_r = 0$ by N. Katz (1971): **Ax-Katz Theorem**.

Generalization to abelian groups

Goal: Generalize to functions $f : A \to B$ with A, B finite abelian groups.

In the example $f_1 = \cdots = f_r = 0$ with $(f_1, \ldots, f_r) \in \mathbb{F}_q[x_1, \ldots, x_N]^r$ we have

$$A = (\mathbb{F}_q, +)^N \text{ and } B = (\mathbb{F}_q, +)^r.$$

More precisely, for a prime p and finite abelian p-groups A, B, we want to find a number $\nu(A, B, \deg(f))$ with

$$p^{\nu(A,B,\deg(f))} \mid \#V(f) = \#f^{-1}(\{0\}).$$

Question: What is the right notion of *degree*?

Definition of the degree of a function

Setup: We let A, B be abelian groups, $f : A \to B$.
Definition through difference operator:

- For $a \in A$, $\Delta_a(f)(x) := f(x+a) - f(x)$.
- $\mathrm{fdeg}(f) :=$ the minimal $n \in \mathbb{N}_0$ with $\Delta_{a_1}\Delta_{a_2}\cdots\Delta_{a_{n+1}} f = 0$ for all $a_1, \ldots, a_{n+1} \in A$.
- **Intuitive:** $f : \mathbb{R} \to \mathbb{R}$ is a polynomial of degree $\leq 2 \Leftrightarrow f''' = 0$.
- **Problems:**
  - $\Delta_a(f \circ g) = \ ?$ ("Chain rule")
  - $f : \mathbb{Z}_2 \to \mathbb{Z}_3, f(0) = 1, f(1) = 2$ satisfies $\Delta_1 f = f$. Hence $\mathrm{fdeg}(f) = \infty$.

The definition of the degree

Setup: We let A, B be abelian groups, $f : A \to B$.
Definition through an abstract version of the difference operator: [Vaughan-Lee 1983]

- Group ring $\mathbb{Z}[A] := \{\sum_{a\in A} z_a\tau_a \mid (z_a)_{a\in A} \in \mathbb{Z}^{(A)}\}$.
- $\mathbb{Z}[A]$ acts on B^A by

$$\begin{aligned} (\tau_a * f)\,(x) &= f(x+a) \\ ((\textstyle\sum_{a\in A} z_a\tau_a) * f)\,(x) &= \textstyle\sum_{a\in A} z_a f(x+a) \\ ((\tau_a - 1) * f)\,(x) &= f(x+a) - f(x). \end{aligned}$$

- In this way, B^A is a $\mathbb{Z}[A]$-module.

The definition of the degree

Setup: We let A, B be abelian groups, $f : A \to B$.
Definition through an abstract version of the difference operator:
[Vaughan-Lee 1983]

- The difference operator is given by $\Delta_a = \tau_a - 1$.
- $\Delta_a * f\,(x) = ((\tau_a - 1) * f)\,(x) = f(x + a) - f(x)$.
- $I :=$ augmentation ideal of $\mathbb{Z}[A] =$ ideal generated by $\{\tau_a - 1 \mid a \in A\} = \{\sum_{a \in A} z_a \tau_a \in \mathbb{Z}[A] \mid \sum_{a \in A} z_a = 0\}$
- $\operatorname{fdeg}(f) := \min\left(\{n \in \mathbb{N}_0 \mid I^{n+1} * f = 0\} \cup \{\infty\}\right)$.

The two invariants

Let A, B be abelian groups. We define two numbers.

- The best upper bound for the degrees:

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

  Can be infinite. Finite if A, B are finite p-groups for the same p.

- The summation invariant:

$$\sigma(A,B) := \sup\{m \in \mathbb{N}_0 \cup \{-\infty\} \mid \forall f \in B^A : \deg(f) \le m \Longrightarrow \underbrace{\sum_{a\in A} f(a)}_{\int f} = 0\}.$$

We know (explanation later)

$$\delta(\mathbb{Z}_p, \mathbb{Z}_{p^b}) = b\,(p-1) \quad \text{and} \quad \sigma(\mathbb{Z}_p^N, \mathbb{Z}_{p^b}) = N(p-1) - 1 \text{ if } N \ge b$$

Application of the two invariants

Let $f : \mathbb{Z}_p^N \to \mathbb{Z}_p$. We look for $b \in \mathbb{N}_0$ such that $p^b \mid \#V(f)$. Let $\chi : \mathbb{Z}_p \to \mathbb{Z}_{p^b}$, $\chi(0) = 1$, $\chi(x) = 0$ for $x \neq 0$. Then

$$[\#V(f)]_{p^b} = \sum_{a \in A} \chi(f(a)) = \int \chi \circ f.$$

Hence $p^b \mid \#V(f)$ if $\operatorname{fdeg}(\chi \circ f) \leq \sigma(\mathbb{Z}_p^N, \mathbb{Z}_{p^b}) = N(p-1) - 1$. Now we have:

$$\operatorname{fdeg}(\chi \circ f) \leq \operatorname{fdeg}(\chi) \cdot \operatorname{fdeg}(f) \leq b(p-1) \operatorname{fdeg}(f).$$

Thus we look for b that guarantees:

$$b\,(p-1) \operatorname{fdeg}(f) \leq N(p-1) - 1,$$

which holds if $b < N/\operatorname{fdeg}(f)$.

Comparison to Ax-Katz

So far we proved:

Theorem

Let $f : \mathbb{Z}_p^N \to \mathbb{Z}_p$ nonconstant, and let $e \in \mathbb{N}_0$ with $e < N/\operatorname{fdeg}(f)$. Then $p^e \mid \#V(f)$.

- This technique proves the prime field case of Ax's Theorem.
- For polynomials over $\mathbb{F}_q$, $\operatorname{fdeg}(f) \leq \deg(f)$. We obtain some cases of O. Moreno's and C.J. Moreno's improvement of the Ax-Katz Theorem.

History

- "Polynomial maps on groups" and "Generalized polynomials" and "Solutions to Frechét's functional equation" are other names for functions of finite functional degree (see [Leibman 2002] and [Hyers, Isac, Rassias 1998]).
- $\mathrm{fdeg}(f \circ g) \leq \mathrm{fdeg}(f) \cdot \mathrm{fdeg}(g)$ was proved for abelian groups in [Leibman 2002].
- Linearity properties that are equivalent to "finite degree" were used in [Mayr 2012] to give a polynomial time algorithm for the subpower membership problem of algebras of prime power size with nilpotent Mal'cev reduct.
- Application to statements on zeros of functions in [Aichinger, Moosbauer 2021].

Recent History

- P.L. Clark, U. Schauz, J. Algebra, 2022: *Functional degrees and arithmetic applications I: the set of functional degrees:*

Theorem

For $A = \prod_{i=1}^{n} \mathbb{Z}_{p^{a_i}}$ with $a_1 \geq a_2 \geq \cdots \geq a_n$ and $B = \mathbb{Z}_{p^b}$, the maximal degree of a function from A to B is

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

This settles $\delta(A,B)$ for all finite abelian groups.

- P.L. Clark, U. Schauz, arXiv, 2023: *Functional degrees and arithmetic applications II: The Group-Theoretic Prime Ax-Katz Theorem*
- P.L. Clark, U. Schauz, arXiv, 2023: *Functional degrees and arithmetic applications III: Beyond Prime Exponent*

The summation invariant:

$$\sigma(A,B) := \sup\{m \in \mathbb{N}_0 \cup \{-\infty\} \mid \forall f \in B^A : \deg(f) \leq m \Rightarrow \int f = 0\}.$$

What is known on $\sigma(\prod_{i=1}^{n} \mathbb{Z}_{p^{a_i}}, \mathbb{Z}_{p^b})$ with $b > 0$?

1. $b = 1$: $\sigma = \left(\sum_{i=1}^{n}(p^{a_i} - 1)\right) - 1$. [Aichinger, Moosbauer 2021]
2. $a_1 = \cdots = a_n = 1$: $\sigma = n(p-1)$ if $n \geq b$ and $\sigma = -\infty$ if $n < b$. [P.L. Clark, N. Triantafillou 2024]
3. $n = 1$: $\sigma = p^{a_1 - b + 1} - 2$ if $a_1 \geq b$ and $\sigma = -\infty$ if $a_1 < b$. [P.L. Clark, N. Triantafillou 2024]

Computing inside $\mathbb{Z}_{p^b}[A]$

- $\mathbb{Z}_{p^b}[A]$ operates on B^A by $(\sum_{a\in A} f_a\tau_a) * g \ \ (x) = \sum_{a\in A} f_a g(x+a)$.
- The augmentation ideal I is generated by $\{\Delta_a \mid a \in A\}$.
- $f \in B^A$. Then $\mathrm{fdeg}(f) \leq d \iff I^{d+1} * f = 0$.
- Let $\omega := \sum_{a\in A} \tau_a$.
- Then $\omega * f = (\int f) \cdot \omega$.
- One obtains that $\sigma(A, \mathbb{Z}_{p^b})$ is the largest $d \in \mathbb{N}_0$ such that $\omega \in I^{d+1}$.

Computing inside $\mathbb{Z}[t_1, \ldots, t_k]$

Let $A := \prod_{i=1}^{k} \mathbb{Z}_{p^{a_i}}$.

- $\mathbb{Z}_{p^b}[A] \cong \mathbb{Z}[t_1, \ldots, t_k]/\langle p^b, t_1^{p^{a_1}} - 1, \ldots, t_k^{p^{a_k}} - 1\rangle$.
- Augmentation ideal $I = \langle p^b, t_1 - 1, \ldots, t_k - 1\rangle$.
- Computations: Linear Algebra over $\mathbb{Z}[t_1, \ldots, t_k]$: Use Strong Gröbner Bases (Survey article [Aichinger 2024]).
- This gives a list of new cases for σ, but the formula in general is unknown.

Some new values of σ

```
p=2 a={2, 1, 0, 0, 0} b=2 s=2
p=2 a={2, 1, 0, 0, 0} b=3 s=1
p=2 a={3, 1, 0, 0, 0} b=2 s=4
p=2 a={2, 2, 0, 0, 0} b=2 s=5
p=2 a={2, 1, 1, 0, 0} b=2 s=3
p=2 a={3, 1, 0, 0, 0} b=3 s=3
p=2 a={2, 2, 0, 0, 0} b=3 s=2
p=2 a={2, 1, 1, 0, 0} b=3 s=3
p=2 a={3, 1, 0, 0, 0} b=4 s=1
p=2 a={2, 2, 0, 0, 0} b=4 s=2
p=2 a={2, 1, 1, 0, 0} b=4 s=2
p=2 a={4, 1, 0, 0, 0} b=2 s=8
p=2 a={3, 2, 0, 0, 0} b=2 s=7
p=2 a={3, 1, 1, 0, 0} b=2 s=5
p=2 a={2, 2, 1, 0, 0} b=2 s=6
p=2 a={2, 1, 1, 1, 0} b=2 s=4
p=2 a={4, 1, 0, 0, 0} b=3 s=5
p=2 a={3, 2, 0, 0, 0} b=3 s=5
p=2 a={3, 1, 1, 0, 0} b=3 s=4
```

```
p=2 a={4, 1, 1, 1, 0} b=7 s=3
p=2 a={3, 2, 1, 1, 1} b=2 s=10
p=2 a={2, 2, 2, 1, 1} b=2 s=10
p=2 a={4, 1, 1, 1, 1} b=3 s=8
p=2 a={7, 1, 0, 0, 0} b=6 s=8
```

```
p=3 a={2, 1, 0, 0, 0} b=2 s=5
p=3 a={2, 1, 0, 0, 0} b=3 s=3
p=3 a={3, 1, 0, 0, 0} b=2 s=11
p=3 a={2, 2, 0, 0, 0} b=2 s=15
p=3 a={2, 1, 1, 0, 0} b=2 s=7
p=3 a={3, 1, 0, 0, 0} b=3 s=7
```