GROUP RINGS, FRÉCHET'S FUNCTIONAL EQUATION, AND COUNTING ZEROS

Erhard Aichinger
Institute for Algebra
Austrian Science Fund FWF P33878

JOHANNES KEPLER
UNIVERSITY LINZ

Theorem (Counting Zeros: Chevalley, Warning, Ax, Katz)

Let $f_1, \ldots, f_r \in \mathbb{F}_q[x_1, \ldots, x_n]$, and let $v := \#\{\boldsymbol{a} \in \mathbb{F}_q^n \mid f_1(\boldsymbol{a}) = \cdots = f_r(\boldsymbol{a}) = 0\}$. Then

1. $v = 0$ or $v \geq q^{n - \sum_{i=1}^r \deg(f_i)}$.
   Warning's Second Theorem (1935); improvements by Heath-Brown (2001) and Moreno and Moreno (1995)
2. $$q^{\left\lceil \frac{n - \sum_{i=1}^r \deg(f_i)}{\max_{i \in [r]} \deg(f_i)} \right\rceil} \text{ divides } v.$$
   Ax (1964) and Katz (1971); improvements by Moreno and Moreno (1995)

Such results were used in [Kawałek and Krzaczkowski, 2020] to provide a linear time Monte-Carlo algorithm to solve equations over nilpotent groups.

Goal of this presentation

- We try to formulate Ax-Katz-type Theorems for mappings on abelian groups.
- We obtain results that are weaker than the Ax-Katz-Moreno-Moreno Theorems, but some new results on the way.
- The proofs use only a modest amount of number theory.
- The technique looks promising.

Functional Degree

A, B ... abelian groups, $f : A \to B$
($A = F^n$ and $B = F^r$ in Warning's Theorem).

Definition

- For $a \in A$, $\Delta_a(f)\,(x) := f(x+a) - f(x)$.
- 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 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

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

- 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]

- $((\tau_a - 1) * f)(x) := f(x+a) - f(x)$.
- $I :=$ augmentation ideal of $\mathbb{Z}[A] =$ ideal generated by $\{\tau_a - 1 \mid a \in A\} = \{\sum_{a \in A} z_a \tau_a \in \mathbb{Z}[A] \mid \sum_{a \in A} z_a = 0\}$

Definition of the functional degree

FDEG$(f) := \min(\{n \in \mathbb{N}_0 \mid (\mathrm{Aug}(\mathbb{Z}[A]))^{n+1} * f = 0\} \cup \{\infty\})$.

Maximal degree

For two abelian groups A, B, we define

$$\delta(A, B) := \sup\left(\{\textsf{FDEG}(f) \mid f \in B^A\}\right).$$

Theorem (EA, Moosbauer 2020)

- $\delta(A, B) < \infty \iff |A| = 1$ or $|B| = 1$ or $\exists p \in \mathbb{P} :$ A is a finite p-group and B is a p-group of finite exponent.
- If B is of finite exponent n, then
  $$\delta(A, B) = \underbrace{\min\{m \in \mathbb{N} \mid (\mathrm{Aug}(\mathbb{Z}_n[A]))^m = 0\}}_{\text{nilpotency index of } \mathrm{Aug}(\mathbb{Z}_n[A])} - 1.$$

General results on $\delta(A, B)$

$$\delta(A,B) := \sup\left(\{\textsf{FDEG}(f) \mid f \in B^A\}\right).$$

Lemma (EA and Moosbauer 2020)

Let A, B be abelian groups.

- $\delta(A, \mathbb{Z}_{p^\beta}) \leq \beta\, \delta(A, \mathbb{Z}_p)$.
- $\delta(A_1 \times A_2, B) \leq \delta(A_1, B) + \delta(A_2, B)$.

Theorem (Leibman 2002)

$\textsf{FDEG}(f \circ g) \leq \textsf{FDEG}(f) \cdot \textsf{FDEG}(g)$.

Self-contained proof in [EA and Moosbauer, 2020].

Known results on $\delta(A, B)$

$$\delta(A,B) := \sup\left(\{\text{FDEG}(f) \mid f \in B^A\}\right) = (\text{nilpotency index of } \operatorname{Aug}(\mathbb{Z}_{\exp(B)}[A])) - 1$$

$\delta(A,B)$	$B = \mathbb{Z}_p$	$B = \mathbb{Z}_{p^\beta}$

Known results on $\delta(A, B)$

$$\delta(A,B) := \sup\left(\{\text{FDEG}(f) \mid f \in B^A\}\right) = (\text{nilpotency index of } \operatorname{Aug}(\mathbb{Z}_{\exp(B)}[A])) - 1$$

$\delta(A,B)$	$B = \mathbb{Z}_p$	$B = \mathbb{Z}_{p^\beta}$
A is not a p-group	∞	∞

Known results on $\delta(A, B)$

$$\delta(A,B) := \sup\left(\{\textsf{FDEG}(f) \mid f \in B^A\}\right) = (\text{nilpotency index of } \operatorname{Aug}(\mathbb{Z}_{\exp(B)}[A])) - 1$$

$\delta(A, B)$	$B = \mathbb{Z}_p$	$B = \mathbb{Z}_{p^\beta}$
A is not a p-group	∞	∞
$A = \mathbb{Z}_{p^\alpha}$	$p^\alpha - 1$ Karpilovsky 1987	

Known results on $\delta(A, B)$

$$\delta(A,B) := \sup\left(\{\text{FDEG}(f) \mid f \in B^A\}\right) = (\text{nilpotency index of } \operatorname{Aug}(\mathbb{Z}_{\exp(B)}[A])) - 1$$

$\delta(A,B)$	$B = \mathbb{Z}_p$	$B = \mathbb{Z}_{p^\beta}$
A is not a p-group	∞	∞
$A = \mathbb{Z}_{p^\alpha}$	$p^\alpha - 1$ Karpilovsky 1987	$\beta p^\alpha - (\beta-1)p^{\alpha-1} - 1$ R. Wilson 2006

Known results on $\delta(A, B)$

$$\delta(A,B) := \sup(\{\mathrm{FDEG}(f) \mid f \in B^A\}) = (\text{nilpotency index of } \mathrm{Aug}(\mathbb{Z}_{\exp(B)}[A])) - 1$$

$\delta(A,B)$	$B = \mathbb{Z}_p$	$B = \mathbb{Z}_{p^\beta}$
A is not a p-group	∞	∞
$A = \mathbb{Z}_{p^\alpha}$	$p^\alpha - 1$ Karpilovsky 1987	$\beta p^\alpha - (\beta - 1)p^{\alpha-1} - 1$ R. Wilson 2006
$A = (\mathbb{Z}_p)^n$	$n(p-1)$ Karpilovski 1987	

Known results on $\delta(A, B)$

$$\delta(A,B) := \sup\left(\{\textsf{FDEG}(f) \mid f \in B^A\}\right) = (\text{nilpotency index of } \operatorname{Aug}(\mathbb{Z}_{\exp(B)}[A])) - 1$$

$\delta(A, B)$	$B = \mathbb{Z}_p$	$B = \mathbb{Z}_{p^\beta}$
A is not a p-group	∞	∞
$A = \mathbb{Z}_{p^\alpha}$	$p^\alpha - 1$ Karpilovsky 1987	$\beta p^\alpha - (\beta - 1)p^{\alpha-1} - 1$ R. Wilson 2006
$A = (\mathbb{Z}_p)^n$	$n(p-1)$ Karpilovski 1987	$\leq \beta n(p-1)$

Known results on $\delta(A, B)$

$$\delta(A,B) := \sup\left(\{\text{FDEG}(f) \mid f \in B^A\}\right) = (\text{nilpotency index of } \operatorname{Aug}(\mathbb{Z}_{\exp(B)}[A])) - 1$$

$\delta(A,B)$	$B = \mathbb{Z}_p$	$B = \mathbb{Z}_{p^\beta}$
A is not a p-group	∞	∞
$A = \mathbb{Z}_{p^\alpha}$	$p^\alpha - 1$ Karpilovsky 1987	$\beta p^\alpha - (\beta-1)p^{\alpha-1} - 1$ R. Wilson 2006
$A = (\mathbb{Z}_p)^n$	$n(p-1)$ Karpilovski 1987	$\leq \beta n(p-1)$ $(\beta + n - 1)(p-1)$

Known results on $\delta(A, B)$

$$\delta(A,B) := \sup\left(\{\textsf{FDEG}(f) \mid f \in B^A\}\right) = (\text{nilpotency index of } \operatorname{Aug}(\mathbb{Z}_{\exp(B)}[A])) - 1$$

$\delta(A,B)$	$B = \mathbb{Z}_p$	$B = \mathbb{Z}_{p^\beta}$
A is not a p-group	∞	∞
$A = \mathbb{Z}_{p^\alpha}$	$p^\alpha - 1$ Karpilovsky 1987	$\beta p^\alpha - (\beta - 1)p^{\alpha-1} - 1$ R. Wilson 2006
$A = (\mathbb{Z}_p)^n$	$n(p-1)$ Karpilovski 1987	$\leq \beta n(p-1)$ $(\beta + n - 1)(p-1)$
$A = \prod_{i=1}^n \mathbb{Z}_{p^{\alpha_i}}$	$\sum_{i=1}^n (p^{\alpha_i} - 1)$ Karpilovsky 1987	

Known results on $\delta(A, B)$

$$\delta(A,B) := \sup\left(\{\text{FDEG}(f) \mid f \in B^A\}\right) = (\text{nilpotency index of } \operatorname{Aug}(\mathbb{Z}_{\exp(B)}[A])) - 1$$

$\delta(A, B)$	$B = \mathbb{Z}_p$	$B = \mathbb{Z}_{p^\beta}$
A is not a p-group	∞	∞
$A = \mathbb{Z}_{p^\alpha}$	$p^\alpha - 1$ Karpilovsky 1987	$\beta p^\alpha - (\beta - 1)p^{\alpha-1} - 1$ R. Wilson 2006
$A = (\mathbb{Z}_p)^n$	$n(p-1)$ Karpilovski 1987	$\leq \beta n(p-1)$ $(\beta + n - 1)(p-1)$
$A = \prod_{i=1}^n \mathbb{Z}_{p^{\alpha_i}}$	$\sum_{i=1}^n (p^{\alpha_i} - 1)$ Karpilovsky 1987	$< \infty$ OPEN

Theorem (EA, 2021)

Let $\beta, n \in \mathbb{N}$, p a prime, and let C_p be the cyclic group of order p multiplicatively written.

- $\delta(\mathbb{Z}_p^n, \mathbb{Z}_{p^\beta}) = (\beta + n - 1)(p - 1)$.
- The nilpotency index of the augmentation ideal of $\mathbb{Z}_{p^\beta}[C_p^n]$ is $(\beta + n - 1)(p - 1) + 1$.
- Let
$$\begin{aligned} A &= \langle x_j - 1 \mid j \in [n] \rangle, \\ N &= \langle x_j^p - 1 \mid j \in [n] \rangle. \end{aligned}$$
be ideals of $\mathbb{Z}[x_1, \ldots, x_n]$, and $\mu := (\beta + n - 1)(p - 1)$. Then $A^\mu \not\subseteq N + \langle p^\beta \rangle$ and $A^{\mu+1} \subseteq N + \langle p^\beta \rangle$.

Proof of $A^{\mu+1} \subseteq N + \langle p^\beta \rangle$.

- $s(x) := \sum_{i=0}^{p-1} x^i$.
- $\exists h \in \mathbb{Z}[x]$: $(x-1)^p = x^p - 1 + ph(x) = s(x)(x-1) + ph(x)$.
- $\exists g \in \mathbb{Z}[x]$: $(x-1)^{p-1} = s(x) + pg(x)$.
- $(x-1)^{n(p-1)} \equiv (-p)^{n-1} s(x) + p^n g(x)^n \pmod{x^p - 1}$. (Induction, 14 lines)
- For all $r, t \in \mathbb{N}_0$: $1 \leq r \leq n$ and $t \geq r - 1 \Rightarrow$
  $\langle x_1 - 1, \ldots, x_r - 1 \rangle^{t(p-1)+1} \subseteq \langle x_j^p - 1 \mid j \in [n] \rangle + (p^{t-r+1})$.
  (Induction on r, 1 page)
- For $r := n$ and $t := \beta + n - 1$, we have $A^{(\beta+n-1)(p-1)+1} \subseteq N + (p^\beta)$.

Sums that are 0

Theorem (EA 2021)

Let $n, \beta \in \mathbb{N}$ with $\beta \leq n$, let B be an abelian group of exponent p^β, and let $f : \mathbb{Z}_p^n \to B$. If $\textsc{Fdeg}(f) < n(p-1)$, then

$$\sum_{a \in \mathbb{Z}_p^n} f(a) = 0.$$

An application

Theorem

Let $\alpha, \gamma \in \mathbb{N}$, let $A = \mathbb{Z}_p^\alpha$, $B = \mathbb{Z}_p^\gamma$, let $f_1, \ldots, f_r : A \to B$, let $d \in \mathbb{N}$ be such that $\max_{i \in [r]}(\text{FDEG}(f_i)) \leq d$, let $V(f_1, \ldots, f_r) := \{a \in A \mid f_1(a) = \cdots = f_r(a) = 0\}$, and let

$$\beta := \lceil \left(\frac{\alpha}{d} - r\gamma \right) \rceil.$$

Then $p^\beta \mid \#V(f_1, \ldots, f_s)$.

Proof:

- $f := (f_1, \ldots, f_r) : A \to B^r$.
- FDEG$(f) = \max_{i \in [r]}$ FDEG$(f_i) \le d$.
- $\chi : B^r \to \mathbb{Z}_{p^\beta}$ defined by $\chi(0) = 1$ and $\chi(b) = 0$ for $b \in B^r \setminus \{0\}$.
- FDEG$(\chi) \le (\beta + r\gamma - 1)(p - 1)$.
- By [Leibman, 2002], FDEG$(\chi \circ f) \le$ FDEG$(\chi) \cdot$ FDEG(f).
- FDEG$(\chi \circ f) \le (\beta + r\gamma - 1)(p-1)d = (\lceil(\frac{\alpha}{d} - r\gamma)\rceil + r\gamma - 1)(p-1)d < (\frac{\alpha}{d} - r\gamma + 1 + r\gamma - 1)(p-1)d = \frac{\alpha}{d}(p-1)d = \alpha(p-1)$.
- $\sum_{a \in A} \chi(f(a)) = 0$.

Comparison to the Ax-Katz Theorem:

We compare this for the case that $A = \mathbb{F}_q^n$, $B = \mathbb{F}_q$, f_i's are polynomials:

- There is Moreno and Moreno's bound (1995), which in some cases improves the Ax-Katz Theorem. We obtain their bound in the case that all f_i are of equal p-weight degree.
- We obtain the prime field case of Ax's Theorem (1964).