Identities in prime rings

Jose **Brox**

Centre for Mathematics
University of Coimbra

INSTITUTE OF MATHEMATICS AND INFORMATICS
BULGARIAN ACADEMY OF SCIENCES

19/02/21

Structure of the talk

- **First part**: I will introduce prime rings and show how some identities are usually simplified with a method which requires some ingenuity
- **Second part**: I will explain a new method for simplifying identities, based on polynomials, which is systematic

Prime rings: generalizing domains

- Commutative case: R **integral domain** if, for $a, b \in R$,

$$ab = 0 \text{ implies } a = 0 \text{ or } b = 0$$

E.g.: $\mathbb{Z}$, $\mathbb{Q}$, any field F, $F[X_1, \ldots, X_n]$

- Noncommutative case: R **prime** if, for I, J ideals of R,

$$IJ = 0 \text{ implies } I = 0 \text{ or } J = 0$$

E.g.: $\mathbb{M}_n(F)$, any simple ring, $F\langle X_1, \ldots, X_n\rangle$

- The **center** of a prime unital ring is an integral domain

Prime rings: generalizing domains

- Prime rings R are a good generalization of integral domains D
- D has a **field of fractions**

$$Q_D := D(D^*)^{-1} \;(e.g. Q_{\mathbb{Z}} = \mathbb{Q})$$

  R has a (Martindale) **ring of quotients $Q(R)$** with a "similar" construction
- The center of $Q(R)$ is **a field** $\mathcal{C}$, the **extended centroid**
- $\mathrm{char}(D) = \mathrm{char}(Q_D)$, $\mathrm{char}(R) = \mathrm{char}(\mathcal{C})$

Prime ring tools: extended centroid

- Informally we see the elements of $\mathcal{C}$ as **scalars** for R
- Formally we consider $\hat{R} := \mathcal{C}R + \mathcal{C}$ inside $Q(R)$
- We have $\lambda x = x\lambda$ for all $\lambda \in \mathcal{C}, x \in R$
- R is not in general an algebra over $\mathcal{C}$, but $\hat{R}$ is
- $\hat{R}$ is a prime ring with extended centroid $\mathcal{C}$
- We consider $R = \hat{R}$ **without loss of generality**
- Hence we have $Z(R) = \mathcal{C}$, a **field**

Prime ring tools: multiplication algebra

- For $a \in R$, define the **multiplication maps** L_a, R_a

$$L_a(x) := ax, R_a(x) := xa, \ x \in R$$

- $L_a, R_a \in \mathrm{End}_{\mathcal{C}}(R)$ are linear endomorphisms of R
- The **multiplication algebra** $\boldsymbol{M(R)}$ is the unital algebra inside $\mathrm{End}_{\mathcal{C}}(R)$ generated by L_a, R_a for all $a \in R$

$$\boxed{M(R) := \langle L_a, R_a \mid a \in R \rangle \leq \mathrm{End}_{\mathcal{C}}(R)}$$

- $M(R) \cong R \otimes_{\mathcal{C}} R^{op}$ as $\mathcal{C}$-algebras via

$$\boxed{L_a R_b \mapsto a \otimes b}$$

Prime rings: identities

- Commutative case: R **integral domain** if, for $a, b \in R$,

$$ab = 0 \text{ implies } a = 0 \text{ or } b = 0$$

- **Characterization by elements:** R is prime iff

$$aRb = 0 \text{ implies } a = 0 \text{ or } b = 0$$

Proof: $aRb = 0$ implies $\mathrm{Id}(a)\mathrm{Id}(b) = 0$
$IJ = 0$ implies $aRb = 0$ for all $a \in I, b \in J$

- **As an identity:**

$$\boxed{axb = 0 \text{ for all } x \in R \text{ implies } a = 0 \text{ or } b = 0}$$

Prime rings: identities with more variables

- If R is prime then

$$aRbRc = 0 \text{ implies } a = 0 \text{ or } b = 0 \text{ or } c = 0$$

Proof:

  - Either $bRc = 0$, implying $b = 0$ or $c = 0$,
  - or is $d \in R$ with $bdc \neq 0$; then $aR(bdc) = 0$ implies $a = 0$

- **As an identity:**

$$\boxed{a_0 \boldsymbol{x_1} a_1 \boldsymbol{x_2} a_2 \cdots \boldsymbol{x_n} a_n = 0 \text{ for all } x_i \in R \text{ implies some } a_i = 0}$$

Prime rings: identities with more monomials

- What about an identity with two terms, like

$$axb + cxd = 0 \text{ for all } x \in R?$$

Answer: If $b \neq 0$ then $a = \lambda c$ for some $\lambda \in \mathcal{C}$

- More in general:

Lemma (Martindale 1969)

Let R be a prime ring and $a_1, b_1, \ldots, a_n, b_n \in R$. If $b_1 \neq 0$ and

$$a_1xb_1 + a_2xb_2 + \cdots + a_nxb_n = 0 \text{ for all } x \in R$$

then $a_1 \in \mathcal{C}a_2 + \mathcal{C}a_3 + \cdots + \mathcal{C}a_n$

Identities that interest us

- The identities that interest us today are of the form
$$\boxed{\sum_{i,j=0}^{n} \lambda_{ij} a^i x a^j = 0}$$
with fixed $a \in R$, $\lambda_{ij} \in \mathcal{C}$ and arbitrary $x \in R$
- Suppose $\lambda_{ij} \neq 0$. By Martindale's lemma, either $a^j = 0$ or $a^i \in \sum_k \mathcal{C} a^k$. Hence ***a* is algebraic!**
- **Martindale's lemma** can help in **finding the possible minimal polynomials** for a

Motivation: Herstein's theory

- Herstein's theory is the study of **nonassociative structures and objects** arising from associative rings
- In R define the product $[x, y] := xy - yx$
  $(R, +, [\cdot, \cdot])$ is a **Lie ring** $\boldsymbol{R^-}$
  $Z(R)$ and $[R, R]$ are Lie ideals of R^-
- In R define the product $x \circ y := xy + yx$
  $(R, +, \circ)$ is a **Jordan ring** $\boldsymbol{R^+}$

Theorem (Herstein 1955)

If R is a simple ring then R^+ is a simple Jordan ring and $R^-/([R, R] \cap Z(R))$ is a simple Lie ring $(\mathrm{char}(R) \neq 2)$

Motivation: Herstein's theory

- Herstein's theory is important in the **classification of Lie and Jordan algebras**
- A Lie algebra over a field is a Lie subalgebra of some R^- (**universal enveloping algebra**)
- The celebrated **Zelmanov's theorem classifies the strongly prime Jordan algebras**, and they are all subalgebras of some R^+, except for a family of specific finite dimension

Example: adnilpotent elements

- Define $\mathrm{ad}_a(x) := [a, x]$. Then $\mathrm{ad}_a^2(x) = [a, [a, x]]$
- An element a is **adnilpotent of index at most** n if

$$\mathrm{ad}_a^n(R) = 0$$

- $\mathrm{ad}_a^1(R) = [a, R] = 0$ iff $ax = xa$ for all $x \in R$ ($a \in Z(R)$)
- $\mathrm{ad}_a^2(R) = [a, [a, R]] = 0$ iff

$$a^2x - 2axa + xa^2 = 0 \text{ for all } x \in R$$

If R is prime, Martindale's lemma guarantees a is algebraic over $\mathcal{C}$

Example: using Martindale's lemma

- $\mathrm{ad}_a^2(x) = [a, [a, x]] = a^2x - 2axa + xa^2 = 0$,

$$\boldsymbol{a^2} x \mathbf{1} - \boldsymbol{a} x 2a + \mathbf{1} x a^2 = 0$$

- Martindale: since $1 \neq 0$ there are $\lambda, \mu \in \mathcal{C}$ such that

$$a^2 = \lambda a + \mu$$

- We want to determine the possible values for λ, μ
- We substitute and use Martindale's lemma repeatedly

Example: using Martindale's lemma

- $a^2x - 2axa + xa^2 = 0, a^2 = \lambda a + \mu$

$$(\boldsymbol{\lambda a} + \boldsymbol{\mu})x - 2axa + x(\boldsymbol{\lambda a} + \boldsymbol{\mu}) =$$
$$ax(\lambda - 2a) + x(2\mu + \lambda a) = 0$$

- Martindale: different possibilities from different terms
- Martindale 1: $\lambda - 2a = 0$ or $a = \alpha \in \mathcal{C}$
- If $\lambda = 2a$:
  - If $\mathrm{char}(\mathcal{C}) = 2$ then $\lambda = 0$, $a^2 = \mu \in \mathcal{C}$
  - If $\mathrm{char}(\mathcal{C}) \neq 2$ then $a = \lambda/2 \in \mathcal{C}$

$$\boxed{a \in \mathcal{C}, \text{ or } a^2 \in \mathcal{C} \text{ and } \mathrm{char}(\mathcal{C}) = 2}$$

Structure of adnilpotent elements

$$\boxed{\mathrm{ad}_a^2(R) = 0 \Rightarrow a \in \mathcal{C} \text{ or } a^2 \in \mathcal{C} \text{ and } \mathrm{char}(\mathcal{C}) = 2}$$

- **Minimal polynomials:** $X - \lambda, X^2 - \lambda$ $(\mathrm{char}(\mathcal{C}) = 2)$
- As n increases, the application of Martindale's lemma to $\mathrm{ad}_a^n(R) = 0$ gets more cumbersome (more possibilities)

Theorem (Martindale,Miers 1983)

Let R be a prime ring with $\mathrm{char}(R) > n$ and let $a \in R$ be adnilpotent of order exactly n. Then the minimal polynomial of a over $\mathcal{C}$ is

$$(X - \lambda)^{\lfloor (n+1)/2 \rfloor}$$

for some $\lambda \in \mathcal{C}$

A new strategy

- The identities that interest us today are of the form

$$\boxed{\sum_{i,j=0}^{n} \lambda_{ij} a^i x a^j = 0}$$

- **Goal:** Given such an identity, **find all the possible minimal polynomials** for a, not by Martindale's lemma, but **in a systematic way**
- **Method:** Transform to a **problem of polynomials** in 2 variables, **through the multiplication algebra**. Apply elementary algebraic geometry

Prime ring tools: multiplication algebra

- For $a \in R$, define the **multiplication maps** L_a, R_a

$$L_a(x) := ax, R_a(x) := xa, \ x \in R$$

- $L_a, R_a \in \mathrm{End}_{\mathcal{C}}(R)$ are linear endomorphisms of R
- The **multiplication algebra** $\boldsymbol{M(R)}$ is the unital algebra inside $\mathrm{End}_{\mathcal{C}}(R)$ generated by L_a, R_a for all $a \in R$

$$\boxed{M(R) := \langle L_a, R_a \mid a \in R \rangle \leq \mathrm{End}_{\mathcal{C}}(R)}$$

- $M(R) \cong R \otimes_{\mathcal{C}} R^{op}$ as $\mathcal{C}$-algebras via

$$\boxed{L_a R_b \mapsto a \otimes b}$$

From the identity to a polynomial

- We see the left side of identity as an element of the multiplication algebra applied to x
- $ax = L_a(x)$, $xa = R_a(x)$
- $a^2x = L_{a^2}(x) = L_a^2(x)$, $xa^2 = R_a^2(x)$
- $axa = L_aR_a(x)$, $a^2xa = L_a^2R_a(x)$, etc.

$$\boxed{\sum_{i,j=0}^{n} \lambda_{ij} a^i x a^j = \left(\sum_{i,j=0}^{n} \lambda_{ij} L_a^i R_a^j \right)(x)}$$

From the identity to a polynomial

$$\sum_{i,j=0}^{n} \lambda_{ij} a^i x a^j = \left(\sum_{i,j=0}^{n} \lambda_{ij} L_a^i R_a^j \right) (x)$$

- $\sum_{i,j=0}^{n} \lambda_{ij} L_a^i R_a^j = f(L_a, R_a)$ with

$$f(X,Y) := \sum_{i,j=0}^{n} \lambda_{ij} X^i Y^j \in \mathcal{C}[X,Y]$$

From the identity to a polynomial

$$f(X,Y) := \sum_{i,j=0}^{n} \lambda_{ij} X^i Y^j \in \mathcal{C}[X,Y]$$

- **E.g.:** $a^2x - axa + 2xa^2 \Rightarrow$ $f(X,Y) = X^2 - XY + 2Y^2$
- The following claims are **equivalent**:
  1. $\sum_{i,j=0}^{n} \lambda_{ij} a^i x a^j = 0$ for all $x \in R$
  2. $f(L_a, R_a)(R) = 0$
  3. $f(L_a, R_a) = 0$ in $M(R)$

From the multiplication algebra to a polynomial ring

- Call $M(a)$ to the **subalgebra** of $M(R)$ generated by $\mathcal{C}$ and L_a, R_a **for a fixed** $\boldsymbol{a} \in R$
- The following claims are **equivalent**:
  1. $\sum_{i,j=0}^{n} \lambda_{ij} a^i x a^j = 0$ for all $x \in R$
  2. $f(L_a, R_a)(R) = 0$
  3. $f(L_a, R_a) = 0$ in $M(R)$
  4. $f(L_a, R_a) = 0$ in $M(a)$
- We have $M(R) \cong R \otimes_{\mathcal{C}} R^{op}$ as $\mathcal{C}$-algebras, $L_a R_b \mapsto a \otimes b$
  We have $M(a) \cong \mathcal{C}[a] \otimes_{\mathcal{C}} \mathcal{C}[a]^{op}$, same isomorphism

From the multiplication algebra to a polynomial ring

Theorem: If $a \in R$ is algebraic with minimal polynomial p then $M(a) \cong \mathcal{C}[X, Y]/\langle p(X), p(Y)\rangle$

Proof.

- a algebraic implies $\mathcal{C}[a] \cong \mathcal{C}[X]/\langle p(X)\rangle$
- $M(a) \cong \mathcal{C}[a] \otimes_{\mathcal{C}} \mathcal{C}[a]^{op} = \mathcal{C}[a] \otimes_{\mathcal{C}} \mathcal{C}[a]$
- $M(a) \cong \mathcal{C}[X]/\langle p(X)\rangle \otimes_{\mathcal{C}} \mathcal{C}[Y]/\langle p(Y)\rangle \cong \mathcal{C}[X, Y]/\langle p(X), p(Y)\rangle$ □

Corollary: If a is algebraic with minimal polynomial p then a satisfies $f(L_a, R_a) = 0$ iff $f(X, Y) \in \langle p(X), p(Y)\rangle$

Elementary algebraic geometry

- We want to solve an **inverse ideal membership problem**: Given $f \in \mathcal{C}[X, Y]$, which are the $p \in \mathcal{C}[X]$ such that $f \in \langle p(X), p(Y) \rangle$?

$$\boxed{f = f_1 p(X) + f_2 p(Y) \text{ with } f_1, f_2 \in \mathcal{C}[X, Y]}$$

- If $q | p$ and $f \in \langle p(X), p(Y) \rangle$ then $f \in \langle q(X), q(Y) \rangle$, so only the maximal p have to be determined
- $\{p(X), p(Y)\}$ is a **Gröbner basis** for $\langle p(X), p(Y) \rangle$. So $f \in \langle p(X), p(Y) \rangle$ iff the **division** of f by $\{p(X), p(Y)\}$ gives **0 remainder**

Root structure

$$\boxed{f = f_1 p(X) + f_2 p(Y) \text{ with } f_1, f_2 \in \mathcal{C}[X,Y]}$$

- If the roots of p are $\lambda_i \in \overline{\mathcal{C}}$ then $f(\lambda_i, \lambda_j) = 0$ for all i, j
- Since $p(X) | f(X,X)$, **the roots of p are among the roots of $f(X,X)$**
- We lack the **multiplicities**: different p could be possible by changing multiplicities
- To find the multiplicities, we **generalize an idea from univariate theory:** λ is a root of f of multiplicity k iff $f^{(i)}(\lambda) = 0$ only for $0 \leq i \leq k$ $(\mathrm{char}(\mathcal{C}) = 0)$

Hasse derivatives

- We need the Taylor expansion of a polynomial in two variables around $(a,b) \in \mathcal{C}^2$:

$$f(X,Y) = \sum_{0 \leq i+j \leq \deg f} \frac{\partial_{X^i}\partial_{Y^j} f(a,b)}{i!j!}(X-a)^i(Y-b)^j$$

- But if $\mathrm{char}(\mathcal{C}) > 0$ **we cannot divide** by an arbitrary $i!$
- We use **Hasse derivatives** $D_{X^iY^j}$ instead of the usual ones

$$\boxed{D_{X^i}X^n = \binom{n}{i}X^{n-i},\ D_{X^i}Y^n = 0,\ D_{X^iY^j} = D_{X^i} \circ D_{Y^j}}$$

- The **Taylor expansion** of f around $(a,b) \in \mathcal{C}^2$ is

$$f(X,Y) = \sum_{0 \leq i+j \leq \deg f} D_{X^iY^j} f(a,b)(X-a)^i(Y-b)^j$$

Root structure

Main Theorem

If $p := \prod_{i=1}^{m}(X - \lambda_i)^{e_i}$ then $f \in \langle p(X), p(Y)\rangle$ iff

$$D_{X^r Y^s} f(\lambda_i, \lambda_j) = 0$$

for all λ_i, λ_j and all $0 \leq r < e_i, 0 \leq s < e_j$.

- Each ordered pair of roots must annihilate all $D_{X^r Y^s} f(X, Y)$ for r, s up to the corresponding multiplicities of said roots
- *The* **proof** *uses the Taylor expansion, the fact that* $\{p(X), p(Y)\}$ *is a Gröbner basis, and a result similar to the Chinese remainder theorem available in this particular case*

Determining the minimal polynomials

- The **possible roots** of p are the roots of $f(X,X)$
- $S := \{\lambda_1, \cdots, \lambda_n\}$ are roots of p iff f annihilates at the **finite rectangular grid** $S \times S$
- We compute the **multiplicities** of the roots **through the zeros of the derivatives**

	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
X	f	$\cdot$	$\cdot$	$\cdot$
X^2	f, D_X, D_Y, D_{XY}	$\cdot$	$\cdot$	$\cdot$
$X(X-1)$	f	f	f	f
$X^2(X-1)$	f, D_X, D_Y, D_{XY}	f, D_X	f, D_Y	f
$X^2(X-1)^2$	f, D_X, D_Y, D_{XY}	f, D_X, D_Y, D_{XY}	f, D_X, D_Y, D_{XY}	f, D_X, D_Y, D_{XY}

Row: maximal minimal polynomial. **Column:** point. **Entry:** derivatives annihilated.

Adnilpotent elements

$$\boxed{\mathrm{ad}_a^n(R) = 0 \Rightarrow f(X,Y) = (X-Y)^n}$$

- $f(X,X) = 0$, so any $\lambda \in \mathcal{C}$ can be a root. But if λ_1, λ_2 are roots, then $f(\lambda_1, \lambda_2) = (\lambda_1 - \lambda_2)^n = 0$ forces $\lambda_1 = \lambda_2$
- The minimal polynomials are of the form $(X - \lambda)^k$

$$\boxed{f_{ij}(X,Y) := D_{X^iY^j}(X-Y)^n = (-1)^j \binom{n}{i}\binom{n-i}{j}(X-Y)^{n-i-j}}$$

- If $n-i-j > 0$ or $n-i-j < 0$ then $f_{ij}(\lambda,\lambda) = 0$
- If $i + j = n$ then $f_{ij}(\lambda,\lambda) = (-1)^j \binom{n}{i}$
- Some of those binomial coefficients can be zero, depending on $\mathrm{char}(\mathcal{C})$

Adnilpotent elements

Theorem

Let R be a prime ring and $a \in R$ be an adnilpotent element of index at most n. Put $t := \lfloor (n+1)/2 \rfloor$ and let $m := k+1$ where $k \in \mathbb{N}$ is the maximum such that $\mathrm{char}(R)$ divides

$$\gcd\left(\binom{n}{t}, \binom{n}{t+1}, \ldots, \binom{n}{t+k}\right),$$

or $k = -1$ if the gcd *is empty. Then there exists $\lambda \in \overline{\mathcal{C}}$ such that the maximal possible minimal polynomial of a is*

$$(X-\lambda)^{t+m}$$

Identities in prime rings
Jose Brox
Prime rings
Identities
Herstein's theory
Polynomializing
Algebraic geometry
Examples
Generalizations

Example: 2D plot

In this example $\mathcal{C} = \mathbb{R}$.

- Consider the identity (fixed a, for all $x \in R$)

$$a^5x - a^4x + a^3x - a^2x + 2a^3xa - 2a^2xa - axa^3 + axa^4 + xa^5 - xa^6 = 0$$

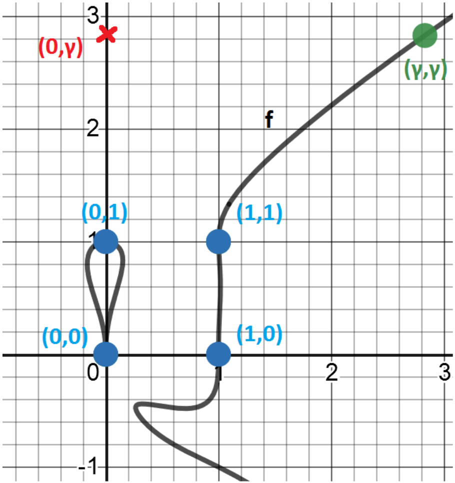
- The associated polynomial f in two variables is

$$X^5 - X^4 + X^3 - X^2 + 2X^3Y - 2X^2Y - XY^3 + XY^4 + Y^5 - Y^6 = f(X, Y)$$

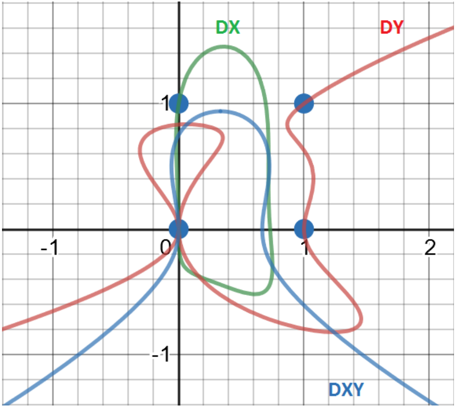
- The possible roots for p arise from $f(X, X) = 0$:

$$-X^6 + 3X^5 - X^3 - X^2 = 0 = X^2(X-1)(X-\alpha)(X-\beta)(X-\gamma)$$

  with α, β complex conjugates and $\gamma \approx 2.83$
- We check numerically that
  $0 \notin \{f(0,\alpha), f(0,\beta), f(1,\alpha), f(1,\beta), f(\gamma,\alpha), f(\gamma,\beta), f(\alpha,\beta)\}$
- **The rest we can check graphically with a real 2D plot**



Since $f = 0$ goes through the grid $\{(0,0),(0,1),(1,0),(1,1)\}$, $X(X-1)$ is a possible minimal polynomial



- D_X, D_Y, D_{XY} go through $(0,0)$
- D_X goes through $(0,1)$ but not through $(1,0)$
- D_Y goes through $(1,0)$ but not through $(0,1)$
- $X^2(X-1)$ is a possible minimal polynomial, $X^2(X-1)^2$ is not

Example: 2D plot

- In summary, the possible minimal polynomials are

$$X, X-1, X-\alpha, X-\beta, X-\gamma, X^2, X(X-1), X^2(X-1)$$

- Then a can only satisfy

$$a^5x-a^4x+a^3x-a^2x+2a^3xa-2a^2xa-axa^3+axa^4+xa^5-xa^6=0$$

if $a\in\{0,1,\alpha,\beta,\gamma\}$, $a^2=0$, $a^2=a$ or $a^3=a^2$
($a\in\{\alpha,\beta\}$ is actually not possible, since $\mathcal{C}=\mathbb{R}$)

- Without redundancies: either $a=\gamma$ or $a^3=a^2$

Generalization: semiprime rings

Possible generalizations of the results

- Can we use a similar method in semiprime rings?
- **Semiprime rings**: the noncommutative analogue of **reduced rings**
- We still have $M(R) \cong R \otimes_{\mathcal{C}} R^{op}$
- But now $\mathcal{C}$ **is not a field**
- A semiprime ring is a **subdirect product of prime rings**

Generalization: several elements

- Can we use a similar method for identities of the form

$$\sum_{i=0}^{n} a_i x b_i = 0,$$

with some nontrivial relations between the elements a_i, b_i?

- We have to use now (Bokut,Chen,Chen 2010)

$$\mathcal{C}\langle X, Y\rangle / I \otimes_{\mathcal{C}} \mathcal{C}\langle Z, W\rangle / J \cong \mathcal{C}\langle X, Y, Z, W\rangle / \langle I, J, K\rangle,$$

with K the ideal of $[X, Z], [X, W], [Y, Z], [Y, W]$

- **Martindale's lemma** is now an **elementary consequence**

Generalization: several variables

- Can we use a similar method for identities of the form

$$\sum_{i=0}^{n} a_i \boldsymbol{x} b_i \boldsymbol{y} c_i + d_i \boldsymbol{y} e_i \boldsymbol{x} f_i = 0?$$

- We can solve **iteratively**: first x is supposed constant
- Tecnically we would work with $\boldsymbol{M}(\boldsymbol{M}(\boldsymbol{R}))$
- If R is prime then $M(R)$ is prime with extended centroid $\mathcal{C}$ (Cabrera,Mohammed 1999)

The Bittersweet End

Thank you for your attention!

Identities: so easy to think about, so hard to verbalize!