

Polynomial identities

Christian Kassel

Institut de Recherche Mathématique Avancée
CNRS - Université de Strasbourg
Strasbourg, France

Colloquium
Department of Mathematics
University of Southern California
Los Angeles, USA
30 September 2009

Overview

- We give a short introduction to the **classical theory of polynomial identities**...
- ... followed by a description of some **recent developments** involving group gradings
- Our main objects of study are **matrix algebras**

The classical theory of polynomial identities

Definition of polynomial identities

- We fix a field k of **characteristic zero** (e.g., $k = \mathbb{C}$)

All algebras we shall consider are **associative unital k -algebras**

- **Definition.** Let A be an algebra. A **polynomial identity (PI)** for A is a non-zero polynomial $f(X_1, \dots, X_n)$ in a finite number of non-commuting variables X_1, \dots, X_n with coefficients in k such that

$$f(a_1, \dots, a_n) = 0$$

for all $a_1, \dots, a_n \in A$.

- We shall only consider **homogeneous** PIs

(Recall that a polynomial is **homogeneous** if it is a linear combination of monomials all having the same degree in each variable)

There is **no loss of generality** in considering only homogeneous PIs since each homogeneous summand of a PI is a PI

PI-algebras

- An algebra for which there is a PI is called a **PI-algebra**
- Any **commutative algebra** A is a PI-algebra since

$$f(X, Y) = [X, Y] \stackrel{\text{def}}{=} XY - YX$$

is a PI for A .

- As we shall see, all **finite-dimensional algebras** are PI-algebras

In particular, all matrix algebras are PI-algebras

- **Not all algebras are PI-algebras:**

E.g., **free algebras** $k\langle X_1, \dots, X_n \rangle$ with $n \geq 2$ are not PI-algebras

A polynomial identity for 2×2 -matrices

- **A degree 5 polynomial identity:** The polynomial

$$\begin{aligned} f(X, Y, Z) &= [[X, Y]^2, Z] \\ &= XYXYZ - XY^2XZ - YX^2YZ + YXYXZ \\ &\quad - ZXYXY + ZXY^2X + ZYX^2Y - ZYXYX \end{aligned}$$

is a PI for the algebra $M_2(k)$ of 2×2 -matrices with entries in k .

Consequently, $M_2(k)$ is a **PI-algebra**

- *Proof.* By **Cayley-Hamilton** any 2×2 -matrix M satisfies the identity

$$M^2 = \operatorname{tr}(M) M - \det(M) I$$

If $M = [X, Y]$, then $\operatorname{tr}(M) = 0$. Hence its **square**

$$M^2 = -\det(M) I$$

is a **scalar matrix**, which then commutes with any matrix Z . □

A polynomial identity for 2×2 -matrices

- **A degree 5 polynomial identity:** The polynomial

$$\begin{aligned}f(X, Y, Z) &= [[X, Y]^2, Z] \\&= XYXYZ - XY^2XZ - YX^2YZ + YXYXZ \\&\quad - ZXYXY + ZXY^2X + ZYX^2Y - ZYXYX\end{aligned}$$

is a PI for the algebra $M_2(k)$ of 2×2 -matrices with entries in k .

Consequently, $M_2(k)$ is a **PI-algebra**

- *Proof.* By **Cayley-Hamilton** any 2×2 -matrix M satisfies the identity

$$M^2 = \operatorname{tr}(M) M - \det(M) I$$

If $M = [X, Y]$, then $\operatorname{tr}(M) = 0$. Hence its **square**

$$M^2 = -\det(M) I$$

is a **scalar matrix**, which then commutes with any matrix Z . □

Subalgebras of PI-algebras are PI-algebras

Any **subalgebra** of a **PI-algebra** is clearly a **PI-algebra**

Let us draw two simple interesting consequences:

- ▶ **Quaternions form a PI-algebra:** This follows from the well-known fact that the algebra \mathbb{H} of quaternions is a subalgebra of $M_2(\mathbb{C})$
- ▶ **Non-linearity of free algebras:** Since $M_2(K)$ is a PI-algebra for any field extension K of k and a non-commutative free algebra is not a PI-algebra, one **cannot embed** $k\langle X_1, \dots, X_n \rangle$ (with $n \geq 2$) as a subalgebra into a matrix algebra of the form $M_2(K)$

Remark. By contrast, any **free group** F_n can be embedded as a subgroup into $SL_2(\mathbb{Z})$, hence into the **general linear group** $GL_2(\mathbb{Q})$

Subalgebras of PI-algebras are PI-algebras

Any **subalgebra** of a **PI-algebra** is clearly a **PI-algebra**

Let us draw two simple interesting consequences:

- ▶ **Quaternions form a PI-algebra:** This follows from the well-known fact that the algebra \mathbb{H} of quaternions is a subalgebra of $M_2(\mathbb{C})$
- ▶ **Non-linearity of free algebras:** Since $M_2(K)$ is a PI-algebra for any field extension K of k and a non-commutative free algebra is not a PI-algebra, one **cannot embed** $k\langle X_1, \dots, X_n \rangle$ (with $n \geq 2$) as a subalgebra into a matrix algebra of the form $M_2(K)$

Remark. By contrast, any **free group** F_n can be embedded as a subgroup into $SL_2(\mathbb{Z})$, hence into the **general linear group** $GL_2(\mathbb{Q})$

The matrix algebra $M_3(k)$ is a PI-algebra

We construct a PI for the algebra $M_3(k)$ of 3×3 -matrices as follows:

By Cayley-Hamilton any matrix $X \in M_3(k)$ satisfies a relation of the form

$$X^3 = \lambda_2 X^2 + \lambda_1 X + \lambda_0 I$$

where $\lambda_0, \lambda_1, \lambda_2$ are scalars (depending on X). Taking the commutator with another matrix Y , we obtain

$$[X^3, Y] = \lambda_2 [X^2, Y] + \lambda_1 [X, Y]$$

Now we take the commutator with $[X, Y]$, thus obtaining

$$[[X^3, Y], [X, Y]] = \lambda_2 [[X^2, Y], [X, Y]]$$

Finally, taking the commutator with $[[X^2, Y], [X, Y]]$, we obtain for $M_3(k)$ the **degree 11 polynomial identity**

$$[[[X^3, Y], [X, Y]], [[X^2, Y], [X, Y]]]$$

All matrix algebras are PI-algebras

- Proceeding in a similar fashion, we obtain a polynomial identity for any algebra for which there is an integer $n \geq 1$ such that any element $a \in A$ satisfies an identity of the form

$$a^n + \lambda_{n-1}a^{n-1} + \cdots + \lambda_1a + \lambda_0 = 0$$

where $\lambda_0, \lambda_1, \dots, \lambda_{n-1}$ are scalars (depending on a)

- In this way we obtain for the algebra $M_n(k)$ of $n \times n$ -matrices a **polynomial identity of degree $2^{n+1} - 2^{n-1} - 1$**
- Are there polynomial identities for $M_n(k)$ of (much) **smaller degree**?

For an **answer**, see the next slides

Standard polynomials

- ▶ The **standard polynomial** S_d of degree d is given by

$$S_d(X_1, \dots, X_d) = \sum_{\sigma \in \text{Sym}_d} \varepsilon(\sigma) X_{\sigma(1)} X_{\sigma(2)} \cdots X_{\sigma(d)}$$

Clearly, $S_d(a_1, \dots, a_d) = 0$ if $a_i = a_j$ for some $i \neq j$

Proposition. *If $\dim(A) < d$, then $S_d(X_1, \dots, X_d)$ is a PI for A*

- ▶ *Proof.* Let $(e_i)_i$ be a basis of A . Then for any $a_1, \dots, a_d \in A$ the element $S_d(a_1, \dots, a_d)$ is a linear combination of elements of the form $S_d(e_{i_1}, \dots, e_{i_d})$. Each of the latter must be zero since for dimension reasons there must be a repetition in each sequence e_{i_1}, \dots, e_{i_d} . \square
- ▶ Consequently, any **finite-dimensional algebra** is a **PI-algebra**
 - It follows from the above proposition that there is a PI of degree $n^2 + 1$ for the **matrix algebra** $M_n(k)$
 - We can still do **better**...

Standard polynomials

- ▶ The **standard polynomial** S_d of degree d is given by

$$S_d(X_1, \dots, X_d) = \sum_{\sigma \in \text{Sym}_d} \varepsilon(\sigma) X_{\sigma(1)} X_{\sigma(2)} \cdots X_{\sigma(d)}$$

Clearly, $S_d(a_1, \dots, a_d) = 0$ if $a_i = a_j$ for some $i \neq j$

Proposition. *If $\dim(A) < d$, then $S_d(X_1, \dots, X_d)$ is a PI for A*

- ▶ *Proof.* Let $(e_i)_i$ be a basis of A . Then for any $a_1, \dots, a_d \in A$ the element $S_d(a_1, \dots, a_d)$ is a linear combination of elements of the form $S_d(e_{i_1}, \dots, e_{i_d})$. Each of the latter must be zero since for dimension reasons there must be a repetition in each sequence e_{i_1}, \dots, e_{i_d} . \square

- ▶ Consequently, any **finite-dimensional algebra** is a **PI-algebra**

- It follows from the above proposition that there is a PI of degree $n^2 + 1$ for the **matrix algebra** $M_n(k)$
- We can still do **better**...

Standard polynomials

- ▶ The **standard polynomial** S_d of degree d is given by

$$S_d(X_1, \dots, X_d) = \sum_{\sigma \in \text{Sym}_d} \varepsilon(\sigma) X_{\sigma(1)} X_{\sigma(2)} \cdots X_{\sigma(d)}$$

Clearly, $S_d(a_1, \dots, a_d) = 0$ if $a_i = a_j$ for some $i \neq j$

Proposition. *If $\dim(A) < d$, then $S_d(X_1, \dots, X_d)$ is a PI for A*

- ▶ *Proof.* Let $(e_i)_i$ be a basis of A . Then for any $a_1, \dots, a_d \in A$ the element $S_d(a_1, \dots, a_d)$ is a linear combination of elements of the form $S_d(e_{i_1}, \dots, e_{i_d})$. Each of the latter must be zero since for dimension reasons there must be a repetition in each sequence e_{i_1}, \dots, e_{i_d} . \square
- ▶ Consequently, any **finite-dimensional algebra** is a **PI-algebra**
 - It follows from the above proposition that there is a PI of degree $n^2 + 1$ for the **matrix algebra** $M_n(k)$
 - We can still do **better**...

The Amitsur-Levitzki theorem

- The following deep result is due to Amitsur and Levitzki (1950)

Theorem. The *standard polynomial* $S_{2n}(X_1, \dots, X_{2n})$ of degree $2n$ is a polynomial identity for the matrix algebra $M_n(k)$

- The degree $2n$ is **optimal** because there are no PIs of degree $< 2n$ for $M_n(k)$
- The proof of the theorem is difficult, but the latter assertion is easy to prove

So let us give a proof. . . (see next slide)

Multilinear polynomials

- A homogeneous polynomial is called **multilinear** if it is a linear combination of monomials all of degree one in each variable
- A **multilinear polynomial** of degree d is of the form

$$\sum_{\sigma \in \text{Sym}_d} \lambda_{\sigma} X_{\sigma(1)} X_{\sigma(2)} \cdots X_{\sigma(d)} \quad (1)$$

where λ_{σ} are scalars

- By a standard **multilinearization** procedure, one shows that if an algebra has a homogeneous PI of some degree, then it has a multilinear PI of the same degree

There are no PIs of degree $< 2n$ for $M_n(k)$

- Indeed, suppose that $M_n(k)$ has a PI of degree $d \leq 2n - 1$, then it would have a **multilinear PI** of the form (1)
- To prove that **this is impossible**, it suffices to exhibit d matrices M_1, M_2, \dots, M_d such that the product $M_1 M_2 \cdots M_d$ is non-zero and the product

$$M_{\sigma(1)} M_{\sigma(2)} \cdots M_{\sigma(d)}$$

of any other permutation σ of these matrices is zero

- Consider the **elementary** matrices $E_{i,j}$ with $1 \leq i, j \leq n$; they form a basis of $M_n(k)$ and they multiply as

$$E_{i,j} E_{m,n} = \delta_{j,m} E_{i,n}$$

The product of the $2n - 1$ matrices

$$E_{1,1}, E_{1,2}, E_{2,2}, E_{2,3}, E_{3,3}, \dots, E_{n-1,n}, E_{n,n}$$

is non-zero whereas the product of any other permutation of this sequence of matrices is zero. This shows that **$M_n(k)$ has no PI of degree $2n - 1$**

- The same proof can be made to work for **any degree $d < 2n - 1$**

T-ideals

- Let A be a PI-algebra. The **set $\text{Id}(A)$ of polynomial identities** for A (together with 0) forms a **two-sided ideal** of the free algebra $k\langle X_1, X_2, \dots \rangle$
- A **T-ideal** is a two-sided ideal of $k\langle X_1, X_2, \dots \rangle$ that is preserved under all substitution of variables, equivalently, under all algebra endomorphisms of $k\langle X_1, X_2, \dots \rangle$

The ideal $\text{Id}(A)$ of polynomial identities is a **T-ideal**

- **Problem.** **Determine the ideal $\text{Id}(A)$** for a given PI-algebra A

This is a **difficult** problem, solved only for a handful of algebras:

- (a) If A is **commutative**, then $\text{Id}(A)$ is generated by the **degree 2** standard polynomial $S_2 = [X_1, X_2]$
- (b) If $A = M_2(k)$, then $\text{Id}(A)$ is generated by the **degree 4** standard polynomial S_4 and the **degree 5** polynomial $[[X, Y]^2, Z]$

The Specht problem

- **The problem.** Is $\text{Id}(A)$ generated by a **finite number** of polynomial identities as a T-ideal?
- In 1987 **Kemer** gave a **positive answer** to the Specht problem for any PI-algebra (whether it is finitely generated or not)

The proof of Kemer's theorem is difficult and does not yield a bound on the number of generators or their degrees

- We now turn to a class of algebras **with extra structure**...

Graded polynomial identities

Graded algebras

Fix a finite group G

- An algebra A is **G -graded** if it has a decomposition into a family of vector subspaces indexed by the elements of the group

$$A = \bigoplus_{g \in G} A_g$$

and compatible with the product on A in the sense that for all $g, h \in G$,

$$A_g \cdot A_h \subset A_{gh}$$

The subspace A_g is called the **homogeneous component** of degree g

The component A_e corresponding to the unit e of G is a **subalgebra** of A

- $\mathbb{Z}/2$ -graded algebras are also called **superalgebras**; they come up in physics

Weyl algebras and **Clifford algebras** are superalgebras

Elementary gradings of matrices

- Fix a group G
- Let us describe a special type of G -grading of $M_n(k)$ called an **elementary grading** (a description of all gradings of $M_n(k)$ will be given in the Appendix)
- An **elementary grading** of $M_n(k)$ is obtained for each sequence g_1, \dots, g_n of length n of elements of G : we grade $M_n(k)$ by specifying that each **elementary matrix** $E_{i,j}$ belongs to the homogeneous component of degree $g_i^{-1}g_j$
- **Example of an elementary $G = \mathbb{Z}/2$ -grading.** We have $M_3(k) = A_0 \oplus A_1$ where A_0 is the 5-dimensional vector space consisting of the matrices

$$\begin{pmatrix} * & 0 & * \\ 0 & * & 0 \\ * & 0 & * \end{pmatrix}$$

and A_1 is the 4-dimensional vector space consisting of the matrices

$$\begin{pmatrix} 0 & * & 0 \\ * & 0 & * \\ 0 & * & 0 \end{pmatrix}$$

(This grading corresponds to the triple $(0, 1, 0) \in (\mathbb{Z}/2)^3$)

Graded polynomial identities

- To define polynomial identities for **ordinary algebras**, we used an arbitrary finite number of non-commuting variables

To define identities for **G-graded algebras**, we need a numerable set of non-commuting variables for each element of G

Let $\{X_1(g), X_2(g), \dots\}$ be the set of variables corresponding to the element $g \in G$

- **Definition.** Let A be a G -graded algebra. A **graded polynomial identity** (G -PI) for A is a non-zero polynomial in the variables $X_i(g)$ that vanishes in A whenever we replace each variable $X_i(g)$ by an element of the homogeneous component A_g of degree g

Examples of graded polynomial identities

- It is **easier to find G-PIs** than ordinary PIs, as show the following stupid examples:

(a) If A is a G -graded algebra and f is an **ordinary PI for the subalgebra** A_e (where e is the unit of G), then f is a G -PI for A (Replace each variable X_i by the variable $X_i(e)$)

(b) Suppose that A is **trivially graded**, i.e., $A_g = 0$ for each $g \neq e$. Then $X(g)$ is a G -PI for each $g \neq e$

- Non-trivial examples of graded polynomial identities.** Consider the **elementary $\mathbb{Z}/2$ -grading** of $M_2(k)$ corresponding to the couple $(0, 1) \in (\mathbb{Z}/2)^2$. We have $M_2(k) = A_0 \oplus A_1$, where

$$A_0 = \left\{ \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \right\} \quad \text{and} \quad A_1 = \left\{ \begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix} \right\}$$

Check that $X_1(0)X_1(1) - X_1(1)X_1(0)$ and

$$X_1(0)(X_1(1)X_2(1) + X_2(1)X_1(1)) - (X_1(1)X_2(1) + X_2(1)X_1(1))X_1(0)$$

are **G-PIs** for $M_2(k)$

The Specht problem in the graded case

- ▶ Let f be an algebra endomorphism of the free algebra on the variables $X_i(g)$ where $g \in G$ and $i = 1, 2, \dots$

We say that f is **admissible** if each $f(X_i(g))$ is a linear combination of monomials $X_{i_1}(g_1)X_{i_2}(g_2) \cdots X_{i_r}(g_r)$ such that $g_1g_2 \cdots g_r = g$

- A two-sided ideal of the free algebra on the variables $X_i(g)$ is a **G-T-ideal** if it is preserved under all admissible algebra endomorphisms
- The set $\text{Id}_G(A)$ of G-PIs for A (together with 0) is a G-T-ideal

- ▶ In 2008 Aljadeff and Kanel-Belov proved the following

Theorem. *If A is a PI-algebra, then $\text{Id}_G(A)$ is generated by a **finite number** of graded polynomial identities as a G-T-ideal*

- This provides an example of a (hard) result for ordinary polynomial identities that **extends to graded polynomial identities**

The Specht problem in the graded case

- ▶ Let f be an algebra endomorphism of the free algebra on the variables $X_i(g)$ where $g \in G$ and $i = 1, 2, \dots$

We say that f is **admissible** if each $f(X_i(g))$ is a linear combination of monomials $X_{i_1}(g_1)X_{i_2}(g_2) \cdots X_{i_r}(g_r)$ such that $g_1g_2 \cdots g_r = g$

- A two-sided ideal of the free algebra on the variables $X_i(g)$ is a **G-T-ideal** if it is preserved under all admissible algebra endomorphisms
 - The set $\text{Id}_G(A)$ of G-PIs for A (together with 0) is a G-T-ideal
- ▶ In 2008 **Aljadeff and Kanel-Belov** proved the following

Theorem. *If A is a PI-algebra, then $\text{Id}_G(A)$ is generated by a **finite number** of graded polynomial identities as a G-T-ideal*

- This provides an example of a (hard) result for ordinary polynomial identities that **extends to graded polynomial identities**

A result about nilpotency

We now give an example of a result on ordinary polynomial identities that **does not extend** to graded polynomial identities

Proposition. *If f^r is a PI for $M_n(\mathbb{C})$ for some $r \geq 2$, then f is a PI*

This means that if any evaluation of f is a **nilpotent** matrix, then this matrix is zero

Proof. It is based on the existence of a division ring D inside $M_n(\mathbb{C})$ such that there is an algebra isomorphism

$$M_n(\mathbb{C}) \cong D \otimes_K \mathbb{C}$$

where K is the center of D (for instance, $M_2(\mathbb{C}) \cong \mathbb{H} \otimes_{\mathbb{R}} \mathbb{C}$)

Now if $f(X_1, \dots, X_d)^r \in \text{Id}(M_n(\mathbb{C}))$, then $f(a_1, \dots, a_d)^r = 0$ for all $a_1, \dots, a_d \in M_n(\mathbb{C})$, hence for all $a_1, \dots, a_d \in D$. Since a division ring has no non-zero nilpotent elements, $f(a_1, \dots, a_d) = 0$ for all $a_1, \dots, a_d \in D$. This shows that $f(X_1, \dots, X_d)$ is a PI for D , hence for $M_n(\mathbb{C})$. \square

In this proof we have used the fact that if an algebra A is obtained from an algebra B by an **extension of scalars**, then they have the same polynomial identities:

$$\text{Id}(A) = \text{Id}(B)$$

A different behavior in the graded case

By contrast with what happens in the ungraded case, there are examples of gradings on matrix algebras and of graded polynomials f such that f' is a G -PI for some $r \geq 2$, but not f

Example. Let $G = \mathbb{Z}/6 \rtimes \text{Sym}_3$, where the symmetric group Sym_3 acts on $\mathbb{Z}/6$ by the sign of permutations; this is a group of order 36 with the following presentation:

$$G = \langle s, t, z \mid s^3 = t^2 = z^6 = 1, ts = s^{-1}t, sz = zs, tz = z^{-1}t \rangle$$

There is a G -graded algebra structure on $M_6(\mathbb{C})$ (its homogeneous components are all one-dimensional) for which the following holds:

Aljadeff, Haile & Natapov: The polynomial

$$f = X(s) X(t)^2 X(z^2)^3 - \omega X(t) X(z^2) X(t) X(z^2)^2 X(s)$$

is not a G -PI for $M_6(\mathbb{C})$, but f^3 is a G -PI for $M_6(\mathbb{C})$
(here $\omega = e^{2\pi i/3}$ is a primitive third root of unity)

When Hopf algebras come in...

Towards more general polynomial identities

- It is possible to extend the theory of polynomial identities to a bigger class of algebras, namely to **comodule algebras** over Hopf algebras

Graded algebras are instances of comodule algebras

- Let H be a **Hopf algebra**; this is essentially an algebra together with an algebra map $\Delta : H \rightarrow H \otimes H$, called the **coproduct**, satisfying certain properties (coassociativity, counitality) dual to the properties satisfied by the product in an associative unital algebra

Hopf algebras are essential tools in the theory of **quantum groups**

- An H -**comodule algebra** is an algebra A together with an algebra map $\delta : A \rightarrow A \otimes H$, called the **coaction**, satisfying certain standard properties

Comodule algebras

- A G -graded algebra is the same as an H -comodule algebra, where $H = kG$ is the group algebra with coproduct given by

$$\Delta(g) = g \otimes g \quad (g \in G)$$

- There is an important class of comodule algebras called Hopf Galois extensions

Classical Galois extensions of fields are instances of Hopf Galois extensions with H being the dual Hopf algebra of the algebra of the Galois group

Hopf Galois extensions can be viewed as analogues of principal fiber bundles in “non-commutative geometry”; now the rôle of the structural group is played by a Hopf algebra. There are numerous instances of such “quantum principal fiber bundles” in quantum group theory

Polynomial identities for comodule algebras

- To define a theory of **polynomial identities for comodule algebras** over a given Hopf algebra H , we fix a basis $(h_i)_i$ of H , and for each basis element h_i we pick a numerable set $\{X_1(h_i), X_2(h_i), \dots\}$ of non-commuting variables
- Let T_H be the **free non-commutative algebra** generated by these variables. There is a structure of H -comodule algebra on T_H induced by the coproduct of H

Definition. Let A be an H -comodule algebra. An **H -polynomial identity** for A is an element $f \in T_H$ such that $\mu(f) = 0$ for every algebra map $\mu : T_H \rightarrow A$ preserving the coactions, i.e., such that the following square commutes:

$$\begin{array}{ccc} T_H & \xrightarrow{\mu} & A \\ \delta \downarrow & & \delta \downarrow \\ T_H \otimes H & \xrightarrow{\mu \otimes \text{id}_H} & A \otimes H \end{array}$$

- An **ordinary polynomial identity** is an H -polynomial identity for the one-dimensional Hopf algebra $H = k$
- A **graded polynomial identity** is an H -polynomial identity for a group algebra $H = kG$

A universal algebra

- Given an H -comodule algebra A , let $\text{Id}_H(A)$ be the **two-sided ideal** of T_H consisting of all H -polynomial identities for A
- The **Specht problem** for $\text{Id}_H(A)$ is **open** for a general Hopf algebra
- The quotient-algebra $U_H(A) = T_H / \text{Id}_H(A)$ is the **universal algebra** in which all H -polynomial identities for A vanish
- The algebra $U_H(A)$ turns out to be useful:

After a suitable **localization of the (big) center** of $U_H(A)$ we obtain an algebra **parametrizing** an important class of Hopf Galois extensions

See details in **joint work with Eli Aljadeff** (Adv. Math., 2008)

APPENDIX

Gradings on matrix algebras

Fine grading and twisted group algebras

Let $A = \bigoplus_{g \in G} A_g$ be a G -graded algebra for a finite group G

- Such a grading is called **fine** if for all $g, h \in G$,

$$\dim(A_g) = 1 \quad \text{and} \quad A_g \cdot A_h = A_{gh}$$

Then necessarily $\dim(A) = |G|$

- Pick a non-zero element u_g in each A_g . Then

$$u_g u_h = \alpha(g, h) u_{gh} \tag{2}$$

for some non-zero scalar $\alpha(g, h)$. Because of the associativity of the product, the scalars $\alpha(g, h)$ satisfy the **cocycle condition**:

$$\alpha(g, h) \alpha(gh, k) = \alpha(g, hk) \alpha(h, k) \quad (g, h, k \in G) \tag{3}$$

- Conversely, given a **cocycle** on G , i.e., a map $\alpha : G \times G \rightarrow k - \{0\}$ satisfying (3), we can define an **associative algebra** whose underlying vector space has a basis $(u_g)_g$ indexed by the elements of G and whose product is given by (2)

Such an algebra is called a **twisted group algebra** and is denoted by $k^\alpha G$

Groups of central type and non-degenerate cocycles

- Let $k^\alpha G$ be a twisted group algebra for some cocycle α

If there is an algebra isomorphism

$$k^\alpha G \cong M_n(k)$$

for some $n \geq 1$, then we say that G is of **central type** and α is **non-degenerate**

- If α is **non-degenerate**, then $|G| = n^2$ and $M_n(k)$ has a **fine G -grading**
- (Howlett, Isaacs, 1982) Any group of central type is **solvable**
- It is easy to check that an **abelian group** G is of central type if and only if

$$G \cong H \times H$$

for some abelian group H

- The group $\mathbb{Z}/6 \rtimes \text{Sym}_3$ considered above is of central type

Gradings on $M_n(\mathbb{C})$

Let G be a finite group

- Suppose we are given the following **data**:
 - (a) a subgroup H of G **of central type**
 - (b) a **non-degenerate** cocycle α on H
 - (c) a sequence g_1, \dots, g_d of elements of G

Then we can **define a G -grading** on $A = \mathbb{C}^\alpha H \otimes M_d(\mathbb{C})$ by setting

$$A_g = \text{Span}\{u_h \otimes E_{i,j} \mid g^{-1}hg_j = g\}$$

- **Bahturin and Zaicev** (2002) proved that each G -grading of $M_n(\mathbb{C})$ is of this form

References on classical polynomial identities

E. Formanek, *The polynomial identities and invariants of $n \times n$ matrices*, Regional Conference Series in Mathematics, 78, Amer. Math. Soc., Providence, RI, 1991.

A. R. Kemer, *Ideals of Identities of Associative Algebras*, Translations of Monographs, 87 Amer. Math. Soc., 1991.

C. Procesi, *Rings with polynomial identities*, Marcel Dekker, Inc., New York, 1973.

L. Rowen, *Polynomial identities in ring theory*, Academic Press, New York, 1980.

References on recent developments

E. Aljadeff, D. Haile, M. Natapov, *Graded identities of matrix algebras and the universal graded algebra*, arXiv:0710.5568, Trans. Amer. Math. Soc. in press.

E. Aljadeff, A. Kanel-Belov, *Representability and Specht problem for G -graded algebras*, arXiv:0903.0362.

E. Aljadeff, C. Kassel, *Polynomial identities and noncommutative versal torsors*, Adv. Math. 218 (2008), 1453–1495.

Yu. A. Bahturin, S. K. Sehgal, M. V. Zaicev, *Group gradings on associative algebras*, J. Algebra 241 (2001), 677–698.

Yu. A. Bahturin, M. V. Zaicev, *Group gradings on matrix algebras*, Can. Math. Bull. 45 (2002), 499–508.

R. Howlett, I. Isaacs, *On groups of central type*, Math. Z. 179 (1982) 555–569.

THANK YOU FOR YOUR ATTENTION