Pré-Publicações do Departamento de Matemática
Universidade de Coimbra
Preprint Number 21–30

IDENTITIES IN PRIME RINGS

JOSE BROX

ABSTRACT: Given a ring, a generalized polynomial identity (GPI) is a polynomial identity in which the coefficients can be taken from the ring. Prime rings are a class of rings very well suited to manage problems related to identities, as for example those coming from Herstein's theory, which is the study of nonassociative objects and structures arising from associative rings. In such study, a particular kind of GPI, that in one variable depending only on the powers of a single element of the ring, often appears. The standard tool for simplifying this kind of GPI, Martindale's lemma, is powerful but not systematic. I present a new method, based on translating the problem to the polynomial setting, which makes the simplification systematic and deals with all field characteristics at once. The proofs will appear elsewhere.

KEYWORDS: prime rings, generalized polynomial identities, minimal polynomial, plane curves.
MATH. SUBJECT CLASSIFICATION (2000): 16R50, 16N60, 16Z05, 68W30, 14Q05.

1. GPIs in one variable in prime rings

Prime rings are the noncommutative counterparts of integral domains. A commutative unital ring R is an integral domain if

$$ab = 0 \text{ implies } a = 0 \text{ or } b = 0, \text{ for } a, b \in R.$$

In the noncommutative setting, elements are replaced by ideals. So, a ring R is *prime* if

$$IJ = 0 \text{ implies } I = 0 \text{ or } J = 0, \text{ for } I, J \text{ ideals of } R.$$

There is also a characterization of primeness by elements. A ring R is prime if and only if

$$axb = 0 \text{ for all } x \in R \text{ implies } a = 0 \text{ or } b = 0, \text{ for } a, b \in R. \quad (1)$$

We can say that prime rings are those in which, as in (1), an identity with one term (axb) in one variable (x) cornered by two fixed expressions (a, b) can be simplified to one of those expressions ($a = 0$ or $b = 0$). What other

Received August 30, 2021.
This work was partially supported by the Centre for Mathematics of the University of Coimbra - UIDB/00324/2020, funded by the Portuguese Government through FCT/MCTES, and by FCT grant SFRH/BPD/118665/2016.

simplifications of similar identities follow from primeness? It is straightforward to show, using the characterization by elements, the following simplification of an identity with one term and two variables: if R is prime then

$$axbyc = 0 \text{ for all } x, y \in R \text{ implies } a = 0 \text{ or } b = 0 \text{ or } c = 0, \text{ for } a, b, c \in R.$$

In general an identity of this kind, formed by a linear combination of some expressions of variables cornered by some fixed elements of the ring, is called a *generalized polynomial identity (GPI)*. It is also true, but not that straightforward to show, that primeness allows to simplify any GPI in one variable. Now we need to introduce some technical concepts. Just as an integral domain can be embedded in its field of quotients, a prime ring R has a similar overring, called the Martindale ring of quotients $Q(R)$. Although $Q(R)$ is not a division ring, its center $\mathcal{C} := \mathcal{C}(R) := Z(Q(R))$ is a field, called the *extended centroid* of R. And although R is not a $\mathcal{C}$-algebra in general, we can work in $\mathcal{C}R+\mathcal{C}$ inside $Q(R)$ and informally consider the elements of $\mathcal{C}$ as scalars for R (see [2, Section 2] for more details). In this paper we will consider GPIs with coefficients in the extended centroid. As stated above, primeness allows to simplify any GPI in one variable (and degree 1 in the variable) [2, Theorem 2.3.4]:

Lemma 1.1 (**Martindale's**). *Let R be a prime ring, $a_1, b_1, \ldots, a_n, b_n \in R$ and $\lambda_1, \ldots, \lambda_n \in \mathcal{C}$. If $\lambda_1, b_1 \neq 0$ then*

$$\lambda_1 a_1 x b_1 + \cdots + \lambda_n a_n x b_n = 0 \textit{ for all } x \in R \textit{ implies } a_1 \in \mathcal{C}a_2 + \cdots + \mathcal{C}a_n. \quad (2)$$

The conclusion of Martindale's lemma is that a_1 is a linear combination of the left elements of the other terms of the GPI.

2. Operator-algebraic elements

We are interested in a special kind of GPI in one variable, in which only powers of a fixed element $a \in R$ appear as coefficients from the ring, with $\lambda_{ij} \in \mathcal{C}$:

$$\lambda_{10}ax+\lambda_{01}xa+\lambda_{20}a^2x+\lambda_{11}axa+\lambda_{02}xa^2+\lambda_{30}a^3x+\lambda_{21}a^2xa+\cdots = 0 \text{ for all } x \in R.$$

This kind of GPI appears often in Herstein's theory, the study of the nonassociative structures and objects arising from associative rings (see e.g. [3–5, 7]). We write it more concisely as

$$\sum_{i,j=0}^{n} \lambda_{ij} a^i x a^j = 0 \text{ for all } x \in R, \quad (3)$$

with the implicit assumption that $i + j > 0$. If we apply Martindale's lemma to (3), by looking at a fixed term of the form $\lambda_{ij} a^i x a^j$ with $\lambda_{ij} \neq 0$ we find that either $a^j = 0$ (implying a nilpotent, in particular algebraic), or a^i is a linear combination of the other left powers of a appearing in the GPI, implying that a is algebraic. So Martindale's lemma implies in any case that a is an algebraic element, and thus it must have a minimal polynomial. But given a GPI of this form there can be several different minimal polynomials giving rise to it. The problem we want to solve is: which are the minimal polynomials giving rise to a fixed GPI of the form (3)? We solve the problem by translating it to a polynomial problem in two variables, which we then solve by elementary algebraic geometry.

3. A polynomial problem

Given a GPI of the form (3), we can associate to it a polynomial in two variables in $\mathcal{C}[X, Y]$ by translating it term by term, translating the left power of a as a power of X and the right power of a as a power of Y. For example, the identity $a^2 x - 2axa + 3axa^3 = 0$ generates the polynomial $X^2 - 2XY + 3XY^3$. More in general we get

$$\sum_{i,j=0}^{n} \lambda_{ij} a^i x a^j \mapsto f(X, Y) := \sum_{i,j=0}^{n} \lambda_{ij} X^i Y^j.$$

It can be shown (the proofs will appear elsewhere) that the problem of finding the minimal polynomials is equivalent to this one: which are the polynomials in one variable $p \in \mathcal{C}[X]$ such that the fixed polynomial in two variables $f \in \mathcal{C}[X, Y]$ belongs to the ideal generated by $p(X)$ and $p(Y)$?

This problem can be solved through the Taylor expansion of the polynomial f. If $\mathrm{char}(\mathcal{C}) = 0$ then the coefficients of the expansion are given by evaluations of the partial derivatives of f divided by factorials of some integers. To solve this problem for any field $\mathcal{C}$ of arbitrary characteristic we need to compute the coefficients of the expansion without making any divisions. These coefficients are given by the Hasse-Schmidt partial derivatives, which are linear maps but not derivations in general, and that we succinctly present here for two variables:

$$D_{X^i}(X^m Y^n) := \binom{m}{i} X^{m-i} Y^n, D_{Y^i}(X^m Y^n) := \binom{n}{i} X^m Y^{n-i}, D_{X^i Y^j} := D_{X^i} \circ D_{Y^j}.$$

Now a version of the combinatorial nullstellensatz ([1]) accounting for multiplicities [6] solves our polynomial problem:

Theorem 3.1. *Let $p \in \mathcal{C}[X]$ have root structure $p(X) = \prod_{i=1}^{n}(X - \lambda_i)^{e_i}$ over the algebraic closure of $\mathcal{C}$. Then $f \in \mathcal{C}[X,Y]$ belongs to the ideal of $\mathcal{C}[X,Y]$ generated by $\{p(X), p(Y)\}$ if and only if for each pair of roots (λ_i, λ_j) we have*

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

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

From this theorem we can readily extract an algorithm for determining the minimal polynomials of a given GPI of the form (3) in a prime ring. The conditions on the partial derivatives imply that we can even determine them geometrically, by plotting the two-dimensional curve generated by the zeros of the polynomial in two variables and determining its behaviour over rectangular grids of potential roots.

Example 3.2. Let us determine the possible minimal polynomials making a satisfy the GPI

$$a^3xa - 2axa^2 = 0$$

in a prime ring. We consider its associated polynomial in two variables

$$f(X,Y) = X^3Y - 2XY^2.$$

By Theorem 3.1, the potential roots of the minimal polynomials must be roots of

$$f(X,X) = X^4 - 2X^3 = X^3(X-2),$$

so the potential roots are 0 (with multiplicity at most 3) and 2. We may have 0 as the unique root (with some maximal multiplicity e), 2 as the unique root, or both 2 and 0 (with some maximal multiplicity perhaps smaller than e). To determine them we compute the Hasse-Schmidt derivatives of f:

$$D_X f = 3X^2Y - 2Y^2, D_Y f = X^3 - 4XY$$

$$D_{X^2} f = \binom{3}{2} XY = 3XY, D_{XY} f = 3X^2 - 4Y, D_{Y^2} f = -\binom{2}{2} 2X = -2X$$

$$D_{X^3} f = \binom{3}{3} Y = Y, D_{X^2Y} f = 3X, D_{XY^2} f = -2, D_{Y^3} f = 0$$

$$D_{X^3Y} f = 1, D_{X^4} f = D_{X^2Y^2} f = D_{XY^3} f = 0.$$

(1) Since $D_X f, D_Y f, D_{XY} f$ have $(0,0)$ as zero, 0 can be found as the unique root of a minimal polynomial with multiplicity 2. To be found with multiplicity 3 we would need also $D_{X^2} f, D_{X^2Y} f, D_{X^2Y^2} f, D_{XY^2} f, D_{Y^2} f$ to have $(0,0)$ as zero; this happens if and only if $\mathrm{char}(\mathcal{C}) = 2$, since $D_{XY^2} f = -2$. We cannot have 0 with multiplicity 4 because $D_{X^3Y} f = 1 \neq 0$ in all characteristics.

(2) Since $D_X f(2,2) = 2^4$, $D_Y f(2,2) = -2^3$, $D_{XY} f(2,2) = 2^2$, for 2 to be found as the unique root of a minimal polynomial with multiplicity 2 it is necessary and sufficient that $\mathrm{char}(\mathcal{C}) = 2$, in which case we have $2 = 0$ and we are in the previous case.

(3) To find 0 and 2 together as roots of the same minimal polynomial, it is necessary that $D_X f(0,2) = -2^3 = 0$, so again we would have $\mathrm{char}(\mathcal{C}) = 2$ and hence only one root.

In conclusion, the maximal possible minimal polynomials for a are X^2, X^3 if $\mathrm{char}(\mathcal{C}) = 2$, and $X - 2$; so $a^3xa - 2axa^2 = 0$ for all $x \in R$ prime if and only if either $a^2 = 0$; $a^2 \neq 0, a^3 = 0$ and $2 = 0$; or $a = 2$.

References

[1] Noga Alon. Combinatorial nullstellensatz. *Combin. Probab. Comput.*, 8(1-2):7—-29, 1999.

[2] K. I. Beidar, W. S. Martindale, III, and A. V. Mikhalev. *Rings with generalized identities*, volume 196 of *Monographs and Textbooks in Pure and Applied Mathematics*. Marcel Dekker Inc., New York, 1996.

[3] Jose Brox, Esther García, and Miguel Gómez Lozano. Jordan algebras at jordan elements of semiprime rings with involution. *J. Algebra*, 468:155–181, 2016.

[4] Jose Brox, Esther García, Miguel Gómez Lozano, Rubén Muñoz Alcázar, and Guillermo Vera de Salas. A description of ad-nilpotent elements in semiprime rings with involution. *Bull. Malaysian Math. Sci. Soc.*, published online, 2021.

[5] I. N. Herstein. *Rings with involution*. Chicago Lectures in Mathematics. The University of Chicago Press, 1976.

[6] Géza Kós and Lajos Rónyai. Alon's nullstellensatz for multisets. *Combinatorica*, 32(5):589–605, 2012.

[7] W.S. Martindale and C.R. Miers. Herstein's lie theory revisited. *J. Algebra*, 98(1):14–37, 1986.

Jose Brox

University of Coimbra, CMUC, Department of Mathematics, 3001-501 Coimbra, Portugal

E-mail address: josebrox@mat.uc.pt