ISRAEL JOURNAL OF MATHEMATICS 104 (1998), 145–155

GROUP-GRADED ALGEBRAS WITH POLYNOMIAL IDENTITY

BY

YURI BAHTURIN

Department of Algebra, Faculty of Mathematics and Mechanics
Moscow State University, 119899 Moscow, Russia
e-mail: bahturin@mech.math.msu.su

AND

ANTONIO GIAMBRUNO

Dipartimento di Matematica ed Applicazioni, Università di Palermo
Via Archirafi, 34, 90123 Palermo, Italy
e-mail: giambruno@ipamat.math.unipa.it

AND

DAVID M. RILEY

Department of Mathematics, The University of Alabama
Tuscaloosa, AL 35487-0350, USA
e-mail: driley@gp.as.ua.edu

ABSTRACT

Let G be a finite group and let $R = \sum_{g\in G} R_g$ be any associative algebra over a field such that the subspaces R_g satisfy $R_gR_h \subseteq R_{gh}$. We prove that if R_1 satisfies a PI of degree d, then R satisfies a PI of degree bounded by an explicit function of d and the order of G. This result implies the following: if H is a finite-dimensional semisimple commutative Hopf-algebra and R is any H-module algebra with R^H satisfying a PI of degree d, then R satisfies a PI of degree bounded by an explicit function of d and the dimension of H.

Received May 20, 1996

1. Introduction

In this paper we consider associative algebras over an arbitrary field F which have the form

$$R = \sum_{g \in G} R_g,$$

where G is a finite multiplicative group and

$$R_g R_h \subseteq R_{gh} \quad \text{for all } g, h \in G.$$

Bergen and Cohen showed in [1] that any G-graded algebra R is a PI-algebra as soon as its identity component R_1 is a PI-algebra. This is not true if G is infinite because any free associative algebra with unity is graded by the infinite cyclic group with identity component the base field. The proof in [1] uses a PI-structure theorem on the centralisers of separable algebras proved by Montgomery in [4]. This approach does not produce a bound on the degree of the polynomial identity satisfied by R except in the case when R is graded-semiprime. Our primary aim is to provide a new, quantitative proof of this result which bounds the minimal degree of the polynomial identity satisfied by R in terms of $|G|$ and the minimal degree of an identity satisfied by R_1, only. Namely, we prove the following:

THEOREM: *Let F be an arbitrary field and let G any finite group of order s. Suppose that R is a G-graded associative F-algebra such that R_1 satisfies a polynomial identity of degree d. Then R satisfies a polynomial identity of degree n, where n is any integer satisfying the inequality*

$$\frac{s^n (sd-1)^{2n}}{(sd-1)!} < n!.$$

It follows that R satisfies a polynomial identity of degree n as soon as

$$es(sd-1)^2 \leq n,$$

where e is the base of the natural logarithm.

Our Theorem also leads to the following quantitative version of [1; Theorem 7, part (4)]. We adopt their notation.

COROLLARY: *Let H be an s-dimensional semisimple commutative Hopf-algebra over F and let R be an H-module algebra. Suppose that $s < \infty$ and that*

$$R^H = \{a \in R |\, h \cdot a = \epsilon(h) a, \quad \text{for all } h \in H\}$$

satisfies a polynomial identity of degree d. Then R satisfies a polynomial identity of degree n, where n is any integer satisfying the inequality

$$\frac{s^n(sd-1)^{2n}}{(sd-1)!} < n!.$$

Proof: We may assume that the polynomial identity satisfied by R^H is multilinear. Let K be a field extension of F that splits H. Then according to [1; Theorem 5], $\overline{R} = R\bigotimes_F K$ is directly G-graded by $G = G(\overline{H})$. Moreover, its identity component $\overline{R}_1$ satisfies $\overline{R}_1 = \overline{R}^{\overline{H}} = \overline{R^H}$. Since $\overline{R^H}$ satisfies the same multilinear identities as R^H and $|G| = \dim_K \overline{H} = s$, the result follows from the Theorem. ∎

A similar result for algebras graded by finite semigroups is mentioned in the concluding section.

Finally, let us point out that our combinatorial technique was inspired by the work of Latyshev [3] and Regev [5].

2. Free graded algebras

Let $F\langle Z\rangle$ be the free associative algebra over F generated by a countably infinite set Z, and let G be a finite group of order s. We represent Z in the form

$$Z = \bigcup_{g\in G} Z_g,$$

where $Z_g = \{z_1^{(g)}, z_2^{(g)}, \ldots\}$ are disjoint sets. We often abbreviate $Z_1 = Y$ and $z_i^{(1)} = y_i$ for each $i \geq 1$. The indeterminates from Z_g are said to be of homogeneous degree g. The **homogeneous degree** of a monomial $z_{i_1}^{(g_1)} \cdots z_{i_t}^{(g_t)}$ in $F\langle Z\rangle$ is defined to be $g_1 g_2 \cdots g_t$, as opposed to its **total degree**, which is defined to be t. Denote by $\mathcal{F}_g$ the subspace of the algebra $F\langle Z\rangle$ generated by all the monomials having homogeneous degree g. Notice that $\mathcal{F}_g\mathcal{F}_h \subseteq \mathcal{F}_{gh}$ for every g, h in G. Consequently, $F\langle Z\rangle = \bigoplus_{g\in G}\mathcal{F}_g$ is a direct G-grading, and $F\langle Z\rangle$ is the **free** G**-graded algebra** generated by the sets Z_g, $g \in G$.

3. Graded identities

Let us fix an enumeration of G: $1 = g_1, g_2, \ldots, g_s$. R is said to satisfy the graded identity

$$f = f(z_1^{(g_1)}, \ldots, z_{t_1}^{(g_1)}, z_1^{(g_2)}, \ldots, z_{t_2}^{(g_2)}, \ldots, z_1^{(g_s)}, \ldots, z_{t_s}^{(g_s)}) \equiv 0,$$

where f is a nonzero element of $F\langle Z\rangle$, if for arbitrary $r_i^{(g_i)},\ldots,r_{t_i}^{(g_i)}\in R_{g_i}$ the equality

$$f(r_1^{(g_1)},\ldots,r_{t_1}^{(g_1)},r_1^{(g_2)},\ldots,r_{t_2}^{(g_2)},\ldots,r_1^{(g_s)},\ldots,r_{t_s}^{(g_s)})=0$$

is satisfied in R. We denote by $T_G(R)$ the set of all polynomials $f\in F\langle Z\rangle$ such that the graded identity $f\equiv 0$ is satisfied by R. In other words, $T_G(R)$ is the ideal of G-graded identities of R.

If for each $i\geq 1$ we set $x_i=\sum_{g\in G}z_i^{(g)}$, then the set $T(R)$ of polynomials in the x_i's vanishing in R coincides with the T-ideal of polynomial identities of R. It is clear that $T(R)\subseteq T_G(R)$.

For each $n\geq 1$, define a subspace of $F\langle Z\rangle$ by

$$V_n=\mathrm{Span}_F\{x_{\sigma(1)}\cdots x_{\sigma(n)}\mid \sigma\in\mathcal{S}_n\}.$$

Then V_n is the space of multilinear polynomials of degree n in the variables x_i, $1\leq i\leq n$. Let G^n denote the direct product of n copies of G. For each $a=(a_1,\ldots,a_n)$ in G^n define

$$V_n^a=\mathrm{Span}_F\{z_{\sigma(1)}\cdots z_{\sigma(n)}\mid \sigma\in\mathcal{S}_n, z_i=z_i^{(a_i)}\text{ for each } i\}.$$

Notice that V_n^a is the space of multilinear polynomials of degree n in the variables $z_1^{(a_1)},\ldots,z_n^{(a_n)}$. Assign

$$V_n^G=\bigoplus_{a\in G^n}V_n^a.$$

From the definitions above, it follows that $V_n\subseteq V_n^G$ and

$$V_n\cap T_G(R)=V_n\cap T(R).$$

Observe as well that

$$\dim_F V_n=n!\quad\text{and}\quad \dim_F V_n^G=|G|^n n!.$$

The integers

$$c_n(R)=\dim_F\frac{V_n}{V_n\cap T(R)}\quad\text{and}\quad c_n^G(R)=\dim_F\frac{V_n^G}{V_n^G\cap T_G(R)}$$

are called the nth codimension and the nth G-graded codimension of R.

LEMMA 3.1: *For every n, $c_n(R) \leq c_n^G(R)$.*

Proof: We have

$$\frac{V_n}{V_n \cap T(R)} = \frac{V_n}{V_n \cap [V_n^G \cap T_G(R)]} \cong \frac{V_n + [V_n^G \cap T_G(R)]}{V_n^G \cap T_G(R)},$$

the latter being a subspace of

$$\frac{V_n^G}{V_n^G \cap T_G(R)}. \quad \blacksquare$$

Notice that R satisfies an (ordinary) multilinear polynomial identity of degree n precisely when $c_n(R) < n!$. Therefore, by the lemma, in order to prove that R satisfies an identity, it suffices to show that $c_n^G(R) < n!$ for some n.

4. The width of a monomial

For a monomial w in $F\langle Z\rangle$, we say w has **width** m if w contains a product of m consecutive submonomials of homogeneous degree 1, and m is maximal. We wish to demonstrate next that if a monomial has large total degree then it must also have large width.

Let us begin with a general lemma about finite groups.

LEMMA 4.1: *Any fixed word $w = a_1 a_2 \cdots a_{|G|d}$ in a finite group G contains a product of d consecutive subwords each with trivial evaluation.*

Proof: Set $t = |G|d$. Then the number of initial subwords $w_1 := a_1, w_2 := a_1a_2, \ldots, w_t := a_1a_2\cdots a_t$ of w is t. Therefore there exists g in G which is the evaluation of at least d-many of these initial subwords. If $g = 1$ then there exists $i_1 < \cdots < i_d$ such that evalutating in G we have

$$1 = w_{i_1} = w_{i_2} = \cdots = w_{i_d}.$$

Therefore in this case the required product of subwords of w is

$$w_{i_1}(a_{i_1+1}\cdots a_{i_2})\cdots(a_{i_{d-1}+1}\cdots a_{i_d}).$$

So, we may assume that $g \neq 1$ and g is the evaluation of at least $d+1$ initial subwords. So, there exists $i_1 < \cdots < i_{d+1}$ such that evaluating in G we have

$$g = w_{i_1} = w_{i_2} = \cdots = w_{i_{d+1}}.$$

Now for each j, $1 \leq j \leq d$, write $w_{i_{j+1}} = w_{i_j} g_j$ where g_j is the appropriate subword of w. It follows that the evaluation of each g_j in G is 1 and

$$w_{i_{d+1}} = w_{i_1} g_1 g_2 \cdots g_d.$$

Thus $g_1 g_2 \cdots g_d$ is the required product of subwords of w. ∎

We now apply this result to the free G-graded algebra.

COROLLARY 4.2: *Every monomial w in $F\langle Z\rangle$ of total degree $|G|d$ has width at least d.*

Proof: Again put $t = |G|d$, and write $w = v_1 v_2 \cdots v_t$, where the v_i's lie in Z. Let a_i be the homogeneous degree of each v_i. Now applying Lemma 4.1 to the fixed word $a_1 a_2 \cdots a_t$ in G yields the desired result. ∎

Let us remark that this bound on the width of w is tight. We now deduce the key result from this section. Recall that we have set $Y = Z_1$ and $y_i = z_i^{(1)}$ for all $i \geq 1$.

PROPOSITION 4.3: *Suppose that*

$$y_1 y_2 \cdots y_d + \sum_{\substack{\sigma \in S_d \\ \sigma \neq 1}} \alpha_\sigma y_{\sigma(1)} \cdots y_{\sigma(d)} \in T_G(R),$$

where the α_σ are scalars. Then for every monomial $w = v_1 v_2 \cdots v_t$ in $F\langle Z\rangle$ with total degree $t \geq |G|d$ we have

$$v_1 v_2 \cdots v_t \in \mathrm{Span}_F\{v_{\tau(1)} \cdots v_{\tau(t)} \mid \tau \in S_t, \tau \neq 1\} + T_G(R).$$

Proof: By the previous corollary, $w = w' u_1 \cdots u_d w''$, where the u_i are elements of $\mathcal{F}_1$. Thus,

$$\begin{aligned} v_1 v_2 \cdots v_t &\equiv w' u_1 \cdots u_d w'' \\ &\equiv - \sum_{\substack{\sigma \in S_d \\ \sigma \neq 1}} \alpha_\sigma w' u_{\sigma(1)} \ldots u_{\sigma(d)} w'' \pmod{T_G(R)}. \end{aligned}$$ ∎

5. Good permutations

Let $1 \leq t \leq n$ be integers and let $\sigma \in S_n$. Following [5], we call the permutation σ t-**bad** if there exists a sequence $1 \leq i_1 < \cdots < i_t \leq n$ such that $\sigma(i_1) > \cdots > \sigma(i_t)$. Otherwise, σ is t-**good**.

For each $\sigma \in \mathcal{S}_n$ and $a = (a_1, \ldots, a_n)$ in G^n, set $w_\sigma^a = z_{\sigma(1)} \cdots z_{\sigma(n)}$, where $z_i = z_i^{(a_i)}$. The monomial w_σ^a is called t-good if σ is t-good. Notice that there are $|G|^n$-many t-good monomials in V_n^G corresponding to the same t-good permutation in $\mathcal{S}_n$.

Proposition 5.1: *Suppose that R_1 satisfies a polynomial identity of degree d, and fix integers t and n where $n \geq t \geq |G|d$. For each $a = (a_1, \ldots, a_n)$ in G^n, V_n^a is spanned, modulo $V_n^G \cap T_G(R)$, by the set*

$$\{w_\sigma^a | \, \sigma \in \mathcal{S}_n \text{ is } t\text{-good}\}.$$

Proof: We may assume that R_1 satisfies a multilinear polynomial identity of degree d. Fix a in G^n and set $w = w_1^a = z_1 z_2 \cdots z_n$, where $z_i = z_i^{(a_i)}$ for each i. The natural basis

$$\mathcal{M}_w = \{w_\sigma^a | \, \sigma \in \mathcal{S}_n\}$$

of V_n^a is well-ordered by the left lexicographic order on the subscripts of the z_i's. We shall show that whenever σ is t-bad, then, modulo $V_n^G \cap T_G(R)$, w_σ^a is a linear combination of smaller monomials in $\mathcal{M}_w$.

By assumption, there exist $1 \leq i_1 < \cdots < i_t \leq n$ such that $\sigma(i_1) > \cdots > \sigma(i_t)$. Factorise w_σ accordingly:

$$w_\sigma = w_0 (z_{\sigma(i_1)} \cdots)(z_{\sigma(i_2)} \cdots) \cdots (z_{\sigma(i_t)} \cdots).$$

Write $w_j = z_{\sigma(i_j)} \cdots z_{\sigma(i_{j+1}-1)}$ for each j, $1 \leq j \leq t-1$, and $w_t = z_{\sigma(i_t)} \cdots z_{\sigma(i_n)}$. Now, by Proposition 4.3, we have

$$w_1 w_2 \cdots w_t \equiv \sum_{\substack{\tau \in \mathcal{S}_t \\ \tau \neq 1}} \alpha_\tau w_{\tau(1)} \cdots w_{\tau(t)} \pmod{V_t^G \cap T_G(R)},$$

for some scalars α_τ. It follows that

$$w_\sigma \equiv \sum_{\substack{\tau \in \mathcal{S}_t \\ \tau \neq 1}} \alpha_\tau w_0 (z_{\sigma(i_{\tau(1)})} \cdots) \cdots (z_{\sigma(i_{\tau(t)})} \cdots) \pmod{V_n^G \cap T_G(R)}.$$

Because all the monomials on the right are smaller in the lexicographic ordering, the result now follows. ∎

According to [5; Theorem 1.8], if $n \geq t$ then the number of t-good permutations in $\mathcal{S}_n$ is at most

$$\frac{(t-1)^{2n}}{(t-1)!}.$$

We have, therefore, the following immediate corollary to Proposition 5.1.

COROLLARY 5.2: *For $n \geq t \geq |G|d$,*

$$c_n^G(R) \leq \frac{|G|^n(t-1)^{2n}}{(t-1)!}.$$

We are now ready to deduce our main result.

THEOREM 5.3: *Suppose that R_1 satisfies a polynomial identity of degree d. Then R satisfies a polynomial identity of degree n, where n is any integer satisfying the inequality*

$$\frac{|G|^n(|G|d-1)^{2n}}{(|G|d-1)!} < n!.$$

In particular, if n is the least integer such that

$$e|G|(|G|d-1)^2 \leq n$$

then R satisfies a polynomial identity of degree n.

Proof: For n large enough,

$$c_n(R) \leq c_n^G(R) \leq \frac{|G|^n(|G|d-1)^{2n}}{(|G|d-1)!} < n!.$$

Therefore R satisfies a multilinear polynomial identity of degree n. It remains to estimate the minimal integer n satisfying this inequality. Consider Euler's gamma function

$$\Gamma(x) = \int_0^\infty t^{x-1}e^{-t}\,dt.$$

The following inequality is well-known:

$$\left(\frac{x}{e}\right)^x < \frac{\Gamma(x+1)}{\sqrt{2\pi x}} < \Gamma(x+1)$$

for all $x \geq 1$ (see page 105 of [2], for example). Substituting n for x where n is the least integer greater than or equal to $e|G|(|G|d-1)^2$ yields

$$(|G|(|G|d-1)^2)^n < \left(\frac{n}{e}\right)^n < \Gamma(n+1) = n!$$

as required. ∎

6. Some applications

The combinatorial nature of our result enables us to apply it in the situations where the other approaches were not successful. Here we give just two simple examples. It is well-known that the homomorphic images of matrix rings or group rings need not be such rings themselves. Nevertheless, our approach gives positive results even in this situation. We start with a corollary for matrix rings.

Example 6.1: Fix an integer $s \geq 2$, and consider the full matrix ring $M_s(R)$ over an algebra R. If R satisfies a polynomial identity of degree d, then $M_s(R)$ satisfies a polynomial identity of any degree at least $es(sd-1)^2$. The same conclusion holds for a homomorphic image of $M_s(R)$ provided that the image of the set of diagonal matrices satisfies an identity of degree d.

To see why, observe that $M_s(R)$ is directly $\mathbf{Z}/s\mathbf{Z}$-graded with zero component the set of diagonal matrices and generating component (formally) spanned by the set

$$\{e_{i,i+1} \,|\, 1 \leq i \leq s-1\} \cup \{e_{s,1}\}.$$

Because the set of diagonal matrices has the same T-ideal as R, the result now follows from our Theorem. Notice, though, that a better bound can be deduced from Theorem 4.4 of [5].

Now suppose that S is any homomorphic image of $M_s(R)$ and that the image of the set of diagonal matrices satisfies a polynomial identity of degree d. Then since S inherits the $\mathbf{Z}/s\mathbf{Z}$-grading (which may no longer be direct), S must satisfy a PI of degree as above.

Example 6.2: Suppose that H is a normal subgroup of finite index s in a group G. Let S be any homomorphic image of the group ring FG. (For example, $S = FG$.) If the corresponding image of FH satisfies a PI of degree d, then S satisfies a PI of any degree at least $es(sd-1)^2$.

This follows as above since FG has a natural G/H-grading with identity component FH.

7. Gradings by semigroups

One might wonder if a result similar to our Theorem might hold if R is graded instead by a finite semigroup S. The role played by the identity element in the group case is now played by the collection of idempotents in S. Indeed, for each idempotent e in S the component R_e of R is a subalgebra of R; therefore, it is necessary to assume that each R_e satisfies a PI.

THEOREM 7.1: *Suppose that R is an associative F-algebra graded by a finite semigroup S. If for each idempotent e in S, R_e satisfies a polynomial identity of degree at most d, then R satisfies a polynomial identity of degree n, where n is an integer bounded by a function depending only on d and the order of S.*

Proof: The only significant modification required for the proof is a semigroup analogue of Lemma 4.1. Namely, one needs to verify that a long enough word in S contains a product of d-many consecutive subwords whose evaluation is the same idempotent e in S. Let us briefly outline such an argument.

Let $|S| = m > 1$ and for $d > 1$ set $t = m(d-1)+1$. Define integers $r_1, \ldots, r_{t-1}$ by $r_{t-1} = 1$ and $r_i = mr_{i+1} + 1$ for $i < t-1$. Suppose that we are given a word $w = w_1$ in S of length at least $mr_1 + 1$. We can find subwords a_1, c_1 and $b_1^{(1)}, \ldots, b_1^{(r_1)}$ of w_1 such that $w_1 = a_1 b_1^{(1)} \cdots b_1^{(r_1)} c_1$ and

$$a_1 = a_1 b_1^{(1)} = \cdots = a_1 b_1^{(1)} \cdots b_1^{(r_1)}$$

in S. Then $a_1 b_1^{(i)} = a_1$ in S for all $i \leq r_1$. Now consider the subword $w_2 = b_1^{(1)} \cdots b_1^{(r_1)}$ of w_1. Treat w_2 as a new word of length r_1 in S, and repeat the argument above to find a_2 with similar properties. In this manner, we can find subwords $a_1, a_2, \ldots, a_t$ of w such that $w' = a_1 a_2 \cdots a_t$ is a subword of w and $a_i a_j = a_i$ in S whenever $i < j$. Then there exist $i_1 < \cdots < i_d$ such that $a_{i_1} = \cdots = a_{i_d} = a$ for some a in S. Thus w' contains a product of d consecutive subwords whose evaluation is a. Since a is an idempotent, the claim follows. ∎

ACKNOWLEDGEMENT: The first author received support from RFFR 93-11-01543 and ISF M22000; the second author was supported in part by the CNR and MURST of Italy; and the third author received support from the CNR and the RGC at the University of Alabama.

References

[1] J. Bergen and M. Cohen, *Actions of commutative Hopf algebras*, The Bulletin of the London Mathematical Society **18** (1986), 159–164.

[2] O. J. Farrell and B. Ross, *Solved Problems: Gamma and Beta Functions, Legendre Polynomials, Bessel Functions*, Dover Publications, New York, 1971.

[3] V. H. Latyshev, *On the theorem of Regev about identities in the tensor product of P.I. algebras*, (Russian), Uspekhi Matematicheskikh Nauk **27** (1972), 213–214.

[4] S. Montgomery, *Centralizers of separable subalgebras*, The Michigan Mathematical Journal **22** (1975), 15–24.

[5] A. Regev, *The representations of S_n and explicit identities for P.I. algebras*, Journal of Algebra **51** (1978), 25–40.

[6] A. E. Zalesskii and M. B. Smirnov, *On identities of graded algebras*, (Russian), Algebra i analiz (Sankt Peterburg) **5** (1993), 116–120.