

G -IDENTITIES ON ASSOCIATIVE ALGEBRAS

Y. BAHTURIN, A. GIAMBRUNO, AND M. ZAICEV

(Communicated by Ken Goodearl)

ABSTRACT. Let R be an algebra over a field and G a finite group of automorphisms and anti-automorphisms of R . We prove that if R satisfies an essential G -polynomial identity of degree d , then the G -codimensions of R are exponentially bounded and R satisfies a polynomial identity whose degree is bounded by an explicit function of d . As a consequence we show that if R is an algebra with involution $*$ satisfying a $*$ -polynomial identity of degree d , then the $*$ -codimensions of R are exponentially bounded; this gives a new proof of a theorem of Amitsur stating that in this case R must satisfy a polynomial identity and we can now give an upper bound on the degree of this identity.

§1. INTRODUCTION

Let R be an algebra over a field F and G a finite group of automorphisms and anti-automorphisms of R . G -polynomials and G -polynomial identities are defined in a natural way (see [M] and [GR]). Two kinds of problems are usually considered:

- (1) Suppose that the ring of invariants R^G satisfies a polynomial identity or more generally that R satisfies a G -polynomial identity of degree d ; under what circumstances must R also satisfy a polynomial identity?
- (2) In the case of hypotheses giving a positive solution to the above problem, can one find an upper bound for the degree of a polynomial identity of R (as a function of d)?

It is well known (see [M]) that problem 1 has a negative answer in general. In case G is a group of automorphisms and R has no $|G|$ -torsion, Kharchenko [K] proved that a polynomial identity (PI) in R^G forces the existence of a polynomial identity in R . Let $*$ denote an involution (an anti-automorphism of order 2) on R ; when $G = \{1, *\}$, Amitsur in two subsequent papers ([A1] and [A2]) gave a positive answer to problem 1 with no further hypotheses on R .

We should remark that, if G is arbitrary, by combining the results of Amitsur and Kharchenko it is easy to prove that R^G PI forces R PI in case of no $|G|$ -torsion.

What about problem 2? Very little is known for general algebras. Both Amitsur and Kharchenko gave bounds on the degree of a polynomial identity satisfied by R provided R is a semiprime algebra. While passing from semiprime algebras to arbitrary ones (by using the famous Amitsur's trick) it was proved that R must satisfy an identity of the form $S_{|G|d}(x_1, \dots, x_{|G|d})^m$ where $S_{|G|d}(x_1, \dots, x_{|G|d})$ is the

Received by the editors December 18, 1996 and, in revised form, May 13, 1997.

1991 *Mathematics Subject Classification*. Primary 16R50; Secondary 16W20.

Y. Bahturin and M. Zaicev acknowledge support by the Russian Foundation of Fundamental Research, grant 96-01-00146. A. Giambruno was supported by MURST and CNR of Italy.

standard polynomial of degree $|G|d$. Thus no information on m was available and, so, no dependence between d and the degree of an identity on R was established.

In this paper we will approach problem 1 (and 2) by translating it into a problem concerning the (G -)codimensions of the algebra R . The sequence of codimensions was introduced by Regev in [Re1] as a basic tool for proving the tensor product theorem and it was applied in [Re2] for finding explicit identities of a PI-algebra. A basic theorem proved by Regev states that an algebra R satisfies a PI if and only if the codimensions of R are exponentially bounded. The sequence of G -codimension was introduced and studied in [GR].

For an algebra R let $c_n(R)$ and $c_n(R|G)$ denote the n -th codimension and the n -th G -codimension respectively of R . In this paper we introduce the notion of an essential G -polynomial and we prove that if R satisfies an essential G -identity of degree d , then $c_n(R|G)$ and, so, $c_n(R)$ is bounded by the exponential function $|G|^n(f(d, |G|) - 1)^{2n}$ where $f(d, |G|)$ is explicitly computed. It also follows that $f(d, |G|)$ is an upper bound for the degree of a polynomial identity satisfied by R .

As a consequence we give a positive solution to a question raised in [GR], namely we prove that if R is an algebra with involution $*$ satisfying a $*$ -polynomial identity of degree d , the $*$ -codimensions $c_n(R|*)$ of R are exponentially bounded by a function of d . This gives a new proof of Amitsur's theorems and we can now give an upper bound on the degree of a PI satisfied by R .

In order to bound the codimensions, we use and extend a result of Latyshev; our main tools are the properties of m -indecomposable words introduced and studied by Razmyslov (see [R]) and we are now able to find an estimate on their number (namely Lemma 2).

One final remark is in order. As a consequence of this estimate the results of [BZ] are improved in that there is now an explicit formula that gives an upper bound for the degree of the identity satisfied by a Lie (super)algebra L graded by a finite group G of order t if the trivial component of L satisfies a non-trivial identity of degree d and this bound depends on t and d entirely.

§2. G -POLYNOMIALS AND G -IDENTITIES

Throughout $\text{Aut}^*(R)$ will be the group of automorphisms and anti-automorphisms of the F -algebra R and $G \leq \text{Aut}^*(R)$ a finite group. If $\text{Aut}(R)$ is the group of automorphisms of R , then $G \cap \text{Aut}(R)$ is a subgroup of G of index ≤ 2 .

Let X be a set, G a finite group and H a subgroup of G of index two. If we interpret H as automorphisms and $G \setminus H$ as anti-automorphisms, we can construct $F\langle X|G \rangle$, the free algebra on X with G -action. $F\langle X|G \rangle$ is freely generated by the set $\{x^g = g(x) \mid x \in X, g \in G\}$ on which G acts in a natural way: $(x^{g_1})^{g_2} = x^{(g_2g_1)}$. Extend this action to $F\langle X|G \rangle$: if v and w are monomials, $g \in G$, then $(vw)^g = v^g w^g$ if $g \in H$ and $(vw)^g = w^g v^g$ if $g \in G \setminus H$. By linearity now G acts on $F\langle X|G \rangle$ with H as automorphisms and $G \setminus H$ as anti-automorphisms. Given any algebra R as above, by interpreting $G \leq \text{Aut}^*(R)$ and $H = G \cap \text{Aut}(R)$, any set theoretic map $\phi : X \mapsto R$ extends uniquely to a homomorphism $\bar{\phi} : F\langle X|G \rangle \mapsto R$ such that $\bar{\phi}(x^g) = \phi(x)^g$. For fixed R , let $\bar{\Phi}$ be the set of all such homomorphisms and set

$$I = \bigcap_{\bar{\phi} \in \bar{\Phi}} \text{Ker} \bar{\phi}.$$

An element $f \in F\langle X|G \rangle$ will be called a G -polynomial. If $f \in I$, then f will be called a G -identity for R .

Let $G^n = G \times \cdots \times G$ and $g = (g_1, \dots, g_n) \in G^n$. Denote by

$$P_{n,g} = \text{Span}_F \{ x_{\sigma(1)}^{g_{\sigma(1)}} \cdots x_{\sigma(n)}^{g_{\sigma(n)}} \mid \sigma \in S_n \}$$

the space of multilinear polynomials in $F\langle X|G \rangle$ in the variables $x_1^{g_1}, \dots, x_n^{g_n}$. In particular, for $1 = (1, \dots, 1)$ we have $P_{n,1} = P_n$. Also let $Q_n = \sum_{g \in G^n} P_{n,g}$ be the space of multilinear G -polynomials in x_1, \dots, x_n .

A G -identity $f \in Q_n$ will be called an *essential* one if it is of the form

$$f = x_1^1 \cdots x_n^1 + \sum_{\substack{1 \neq \sigma \in S_n \\ g \in G^n}} \alpha_{\sigma,g} x_{\sigma(1)}^{g_1} \cdots x_{\sigma(n)}^{g_n}.$$

If we let $J \subset F\langle X \rangle \subset F\langle X|G \rangle$ be the T-ideal of identities of R , then $c_n(R) = \dim \frac{P_n+J}{J}$ and $c_n(R|G) = \dim \frac{Q_n+I}{I}$ are called the n -th codimension of R and the n th G -codimension of R , respectively. The relation between these two dimensions is given in the following ([GR, Lemma 4.4])

Lemma 1. $c_n(R) \leq c_n(R|G)$.

§3. DECOMPOSABLE MONOMIALS

Introduce a partial ordering on the variables x_i^g by requiring that $x_i^g < x_j^h$ if $i < j$ for $g, h \in G$; extend this ordering lexicographically to all monomials (words) in Q_n by comparing them from left to right.

Following [R] we introduce the following:

Definition. A monomial $w \in P_{n,g}$ is said to be m -decomposable if it can be represented in the form $w = aw_m w_{m-1} \cdots w_1 b$ where w_i ($i = 1, \dots, m$) are nonempty monomials such that

- the left variable in the monomial w_i is greater than any other variable in this monomial ($i = 1, \dots, m$);
- the first variable in the monomial w_{i+1} is greater than the first variable in the monomial w_i ($i = 1, \dots, m-1$).

In case w has no m -decompositions then it is said to be m -indecomposable.

In this section we want to find a bound on the number $a_m(n)$ of m -indecomposable multilinear monomials in x_1, \dots, x_n . It is well known that $a_m(n)$ satisfies the following recurrent relation (see [R, Section 2.1])

$$(1) \quad a_m(n) = \sum_{i=0}^{n-1} \frac{(n-1)!}{i!(n-1-i)!} a_m(i) a_{m-1}(n-1-i),$$

where $a_m(0) = 1$. Moreover if we set

$$b_m(n) = \frac{a_m(n)}{n!},$$

asymptotically the value $b_m(n)$ is less than $(\frac{1}{c})^n$ for any fixed c . We will need an explicit estimate for n , depending only on c and m .

Let $t = m + \lceil \log_2 c \rceil$ and $N = 2^{2^{t+1}}$. We denote by $p_j, j \geq 3$ an integer for which

$$\underbrace{\log_N \cdots \log_N}_{j-2} p_j = p_2$$

and set $p_2 = 2^{t^2}$. We remark that with such a choice of p_2 the inequality

$$(2) \quad n!p_2 > 2^{tn}$$

is satisfied for all natural n . We set $f(m, c) = \log_2 p_m$.

Lemma 2. *Let $n \geq f(m, c)$. Then $b_m(n) < (\frac{1}{c})^n$.*

Proof. From (1) above it follows that $b_k(n)$ satisfies the following recurrent relation

$$(3) \quad b_k(n) = \frac{1}{n} \sum_{i=0}^{n-1} b_k(i)b_{k-1}(n-1-i),$$

where $b_k(0) = 1$. It is easy to observe, that $b_2(n) = \frac{1}{n!}$. In what follows we assume that $k \geq 2$.

First, we show that if the following conditions are satisfied

$$(4) \quad b_k(j) < p\varepsilon^j, \quad j = 0, 1, \dots$$

$$(5) \quad b_{k+1}(j) < q(2\varepsilon)^j, \quad j = 0, 1, \dots, n-1,$$

where $\varepsilon < \frac{1}{2}$, then

$$(6) \quad b_{k+1}(n) < \frac{2pq}{n}(2\varepsilon)^{n-1}.$$

In fact, it follows from (3) that

$$b_{k+1}(n) < \frac{1}{n} \sum_{i=0}^{n-1} q(2\varepsilon)^i p\varepsilon^{n-1-i} = \frac{pq}{n}(2\varepsilon)^{n-1} \sum_{i=0}^{n-1} \left(\frac{1}{2}\right)^i < \frac{2pq}{n}(2\varepsilon)^{n-1}.$$

We assume now, that (4) holds, $n_0 > \frac{p}{\varepsilon}$ and $q \geq \left(\frac{1}{2\varepsilon}\right)^{n_0} > \left(\frac{1}{2\varepsilon}\right)^{\frac{p}{\varepsilon}}$. Then the inequality (5) is satisfied for all $j \leq n_0$, since $b_k(n) \leq 1$ for all k and n . But then, by (6), $b_{k+1}(j) < q(2\varepsilon)^j$ also for $j = n_0 + 1$, since $\frac{2p}{n_0} \leq 2\varepsilon$. It follows that with such a choice of q the inequality (5) holds for all j . So, we have shown that if

$$b_k(j) < q_k \varepsilon_k^j$$

for all j , then

$$b_{k+1}(j) < q_{k+1} \varepsilon_{k+1}^j$$

also for all j with $\varepsilon_{k+1} = 2\varepsilon_k$ and

$$(7) \quad q_{k+1} \geq \left(\frac{1}{\varepsilon_{k+1}}\right)^{\frac{q_k}{\varepsilon_k}}.$$

We set $\varepsilon_2 = 2^{-t}$. From (2) it follows that $b_2(j) < p_2 \varepsilon_2^j$ for all j . Then $\varepsilon_{k+1} = 2^{-r}$ and $r \leq t$. Hence

$$\left(\frac{1}{\varepsilon_{k+1}}\right)^{\frac{q_k}{\varepsilon_k}} = (2^r 2^{r+1})^{q_k} \leq N^{q_k}.$$

Thus the inequality (7) is satisfied by all numbers of the form $q_2 = p_2, \dots, q_k = p_k, q_{k+1} = N^{p_k} = p_{k+1}$. Hence, for $k = m$ we have

$$b_m(n) < p_m \varepsilon_m^n \quad \text{and} \quad \varepsilon_m = 2^{m-2} \varepsilon_2 = 2^{m-t-2}.$$

By the choice of the number t the following inequality holds:

$$t \geq m + \log_2 c - 1 = m + \log_2 2c - 2.$$

Hence $\varepsilon_m \leq \frac{1}{2c}$. But then

$$(8) \quad b_m(n) < p_m \left(\frac{1}{2c} \right)^n.$$

By the hypothesis, $n \geq \log_2 p_m$. Hence $p_m \left(\frac{1}{2} \right)^n \leq 1$ and from (8) we obtain the required estimate. Lemma 2 has been proven. \square

§4. MAIN RESULT

In this section we shall prove the result on G -identities mentioned in the introduction and then we shall deduce Amitsur's theorem [A1] on rings with involution with the desired bound on the degree of a PI for R .

Theorem 1. *Let R be an algebra over a field F and G a finite subgroup of $\text{Aut}^*(R)$. Suppose that R satisfies some multilinear essential G -identity of degree d . Then for n sufficiently large we have $c_n(R|G) \leq |G|^n (f(d, |G|) - 1)^{2n}$ and R satisfies a non-trivial polynomial identity, whose degree is bounded by the function $f(d, |G|)$. In case $G \leq \text{Aut}(R)$, then $c_n(R|G) \leq |G|^n (d - 1)^{2n}$ and R satisfies a non-trivial polynomial identity, whose degree is bounded by $3|G|(d - 1)^2$.*

The proof of this theorem will be deduced after a sequence of reductions. Suppose throughout that G is a finite subgroup of $\text{Aut}^*(R)$ and R satisfies an essential G -identity f of degree d .

Notice that in order to prove that R satisfies an ordinary identity whose degree is bounded by a function $k = k(d, |G|)$ it is enough to find an integer n for which the following inequality is satisfied:

$$(9) \quad \dim \frac{P_n + I}{I} < n!$$

and to show that $n \leq k(d, |G|)$. Note that $P_n \subset Q_n$ therefore it is enough to show that

$$(10) \quad c_n(R|G) = \dim \frac{Q_n + I}{I} < n!.$$

Let us denote by $V^{(d)}$ the linear span of d -indecomposable monomials.

Lemma 3. *If R satisfies a multilinear essential G -identity of degree d , then for any n we have $Q_n \subset I + V^{(d)}$.*

Proof. Suppose by contradiction that the Lemma is false. Then there exists a counterexample $B = x_{i_1}^{s_1} \cdots x_{i_n}^{s_n}$ which is minimal in the left lexicographic order defined in the previous section.

By the hypotheses R satisfies an identity of degree d , hence

$$(11) \quad x_1^1 \cdots x_d^1 \equiv \sum_{\substack{1 \neq \sigma \in S_d \\ g \in G^d}} \alpha_{\sigma, g} x_{\sigma(1)}^{g_1} \cdots x_{\sigma(d)}^{g_d} \pmod{I},$$

for some $\alpha_{\sigma, g} \in F$.

Since the ideal of G -identities of R is invariant under all endomorphisms of $F\langle X|G \rangle$ commuting with the G -action (i.e., $\theta(a^g) = \theta(a)^g$), (11) implies that

$$(12) \quad t_1 \cdots t_d \equiv \sum_{\substack{1 \neq \sigma \in S_d \\ g \in G^d}} \alpha_{\sigma, g} t_{\sigma(1)}^{g_1} \cdots t_{\sigma(d)}^{g_d} \pmod{I}$$

for any $t_1, \dots, t_n \in F\langle X|G \rangle$.

Since $B \notin V^{(d)}$, there exist indices j_1, \dots, j_d which determine a d -decomposition on B . We will write $y_1 = x_{i_1}^{s_1}, \dots, y_n = x_{i_n}^{s_n}$ for convenience.

We denote by a_0 the product $y_1 \cdots y_{j_1-1}$, if $j_1 > 1$. If $j_1 = 1$, then we simply assume that a_0 is the empty word. Similarly, we set $a_{d+1} = y_{j_{d+1}} \cdots y_n$ if $j_d < n$ and set a_{d+1} the empty word as soon as $j_d = n$. For all $k = 1, \dots, d-1$ we set

$$a_k = y_{j_k} y_{j_k+1} \cdots x_{j_{k+1}-1}$$

and $a_d = y_{j_d}$. Then $B = a_0 a_1 \cdots a_d a_{d+1}$. But it follows from (12) that, modulo I , we can express B as a linear combination of products of the form $B_{\sigma, g} = a_0 a_{\sigma(1)}^{g_1} \cdots a_{\sigma(d)}^{g_d} a_{d+1}$ where $\sigma \in S_d$ and $\sigma \neq 1$. Since B is a minimal counterexample and all $B_{\sigma, g}$ are less than B , we obtain (modulo I) an expression of B as a linear combination of d -indecomposable monomials, a contradiction. \square

To complete the proof of Theorem 1, notice that (modulo I) Q_n is a sum of $|G|^n$ subspaces $P_{n, g}$ and every $P_{n, g}$ contains no more than $a_d(n)$ linearly independent monomials. By Lemma 2 it follows that the inequalities (9) and (10) hold for $n \geq f(d, |G|)$ and, so, R satisfies a PI of degree $f(d, |G|)$. But then by [GR, Lemma 4.7], $c_n(R|G) \leq |G|^n c_n(R) \leq |G|^n (f(d, |G|) - 1)^{2n}$.

In case $G \leq \text{Aut}(R)$ one can give an estimate of the degree of an identity on R which is better than the one given by the function $f(d, |G|)$ above. To accomplish this, one should observe that the space Q_n can be spanned (modulo I) by the d -good monomials in the sense of [Re2]. In this case since by [Re2, Theorem 1.8] the number of d -good monomials is $\leq \frac{(d-1)^{2n}}{(d-1)!}$ it follows that $c_n(R|G) \leq |G|^n (d-1)^{2n}$ and, as in [BGR] R satisfies a PI of degree $\leq e|G|(d-1)^2$ where e is the basis of the natural logarithms.

We can now improve Amitsur's theorem. In case $G = \{1, *\}$ where $*$ is an involution, G -polynomials and G -identities are called $*$ -polynomials and $*$ -identities respectively. Also, $c_n(R|G) = c_n(R|*)$ is called the n -th $*$ -codimension of R .

Corollary 1. *Let R be an algebra with involution $*$ over a field F satisfying a non-trivial $*$ -identity of degree d . Then for n sufficiently large we have $c_n(R|*) \leq 2^n (f(2d, 2) - 1)^{2n}$ and R satisfies a non-trivial polynomial identity whose degree is bounded by the function $f(2d, 2)$.*

Proof. By applying the usual linearization process to the $*$ -identity of R , we get that R satisfies a $*$ -identity of the form

$$\sum_{s \in G^d} \alpha_s x_1^{s_1} \cdots x_d^{s_d} + \sum_{\substack{1 \neq \sigma \in S_d \\ q \in G^d}} \beta_{\sigma, q} x_{\sigma(1)}^{q_1} \cdots x_{\sigma(d)}^{q_d}$$

where $s = (s_1, \dots, s_d), q = (q_1, \dots, q_d) \in G^d$ and $G = \{1, *\}$. Also, without loss of generality we may assume that $\alpha_1 \neq 0$ for $1 = (1, \dots, 1)$. Replacing x_i by $x_{2i-1} x_{2i}$

for all $i = 1, \dots, d$, we obtain a $*$ -identity of the form

$$x_1 \cdots x_{2d} + \sum_{\substack{1 \neq \sigma \in S_{2d} \\ q \in G^{2d}}} \gamma_{\sigma, q} x_{\sigma(1)}^{q_1} \cdots x_{\sigma(2d)}^{q_{2d}}.$$

Since this is an essential G -identity on R , Theorem 1 gives the desired conclusion. \square

REFERENCES

- [A1] S. A. Amitsur, *Rings with involution*, Israel J. Math. **6** (1968), 99 – 106. MR **39**:256
- [A2] S. A. Amitsur, *Identities in rings with involution*, Israel J. Math. **7** (1969), 63 – 68. MR **39**:4216
- [BGR] Y. Bahturin, A. Giambruno and D. Riley, *Group-graded algebras with polynomial identity*, Israel J. Math. **104** (1998), 145–156.
- [BZ] Y. Bahturin and M. Zaicev, *Identities of graded algebras*, J. Algebra, to appear.
- [GR] A. Giambruno and A. Regev, *Wreath products and P.I. algebras*, J. Pure Applied Algebra **35** (1985), 133 –149. MR **86e**:16027
- [K] V. K. Kharchenko, *Galois extensions and quotient rings*, Algebra i Logika **13** (1974), 460 – 484 (Russian); English transl. (1975), 264 – 281. MR **53**:498
- [L] V. N. Latyshev, *On the theorem of Regev about identities in the tensor product of P.I. algebras*, Uspekhi Mat. Nauk. **27** (1972), 213 – 214 (Russian). MR **52**:13924
- [M] S. Montgomery, *Fixed rings of finite automorphism groups of associative rings*, LNM n. 818 Springer-Verlag, Berlin, 1980. MR **81j**:16041
- [R] Yu. P. Razmyslov, *Identities of Algebras and Their Representations*, Transl. Math. Monogr., vol. 138, Amer. Math. Soc., Providence RI, 1994 xiii+318pp. MR **95i**:16022
- [Re1] A. Regev, *Existence of identities in $A \otimes B$* , Israel J. Math. **11** (1972), 131 – 152. MR **47**:3442
- [Re2] A. Regev, *The representations of S_n and explicit identities for P.I. algebras*, J. Algebra **51** (1978), 25 – 40. MR **57**:9745

(Y. Bahturin and M. Zaicev) DEPARTMENT OF ALGEBRA, FACULTY OF MATHEMATICS AND MECHANICS, MOSCOW STATE UNIVERSITY, MOSCOW, 119899 RUSSIA

E-mail address: bahturin@mech.math.msu.su

E-mail address: zaicev@nw.math.msu.su

(A. Giambruno) DIPARTIMENTO DI MATEMATICA E APPLICAZIONI, UNIVERSITÀ DI PALERMO, VIA ARCHIRAFI 34, 90123 PALERMO, ITALY

E-mail address: a.giambruno@unipa.it