ISRAEL JOURNAL OF MATHEMATICS, Vol. 36, No. 2, 1980

# GENERALIZED RATIONAL IDENTITIES AND RINGS WITH INVOLUTION

BY

PAUL C. DESMARAIS AND WALLACE S. MARTINDALE, 3RD

ABSTRACT

The main goal of this paper is to present the following generalization of a theorem of Desmarais: Let $D$ be a fixed division ring and let $E \supseteq D$ be a division ring with involution $*$ and with infinite center $C$ such that $(E:C)=\infty$. If $S$ is the set of all $2m$-tuples of the form $(a_1, a_2, \cdots, a_m, a_1^*, a_2^*, \cdots, a_m^*)$, $a_i \in E$, then any generalized rational identity (over $D$) vanishing on $S$ (where defined) must in fact vanish on $E^{2m}$ (where defined). The result follows as a corollary to Bergman's generalization of Amitsur's basic result on rational identities, and for completeness we present Cohn's account of Bergman's result.

In his dissertation [5] the first author, using the notions and methods of Amitsur's fundamental paper on rational identities [2], proved the following result:

THEOREM (Desmarais). *If $E$ is a division ring with involution such that its center $C$ is infinite and $(E:C)=\infty$, then any rational identity satisfied by the symmetric elements of $E$ must be satisfied by $E$ itself.*

The proof was rather lengthy and it has become clear that in fact a substantial generalization of Desmarais's theorem follows quickly from two results — one on generalized rational identities due to Bergman and the other on generalized polynomial identities with involution due independently to Skinner and Rowen.

Therefore this paper is primarily an expository one. For completeness we present as a central theorem a slightly expanded version of a basic result of Bergman [3], following the account given by Cohn in [4] (section 7.2, specifically lemma 7.2.5 and theorem 7.2.6).

The key points of Bergman's paper are (1) his way of defining generalized rational identities and (2) a key remark relating generalized rational identities in a very explicit way to generalized polynomial identities.

Received January 30, 1979 and in revised form October 25, 1979

We begin by stating two results on generalized polynomial identities in the special context of division rings. Let $Y = \{y_1, y_2, \cdots, y_m\}$, let $A$ be an algebra over a field $F$, let $A_F\langle Y\rangle$ be the free product of $A$ over $F$ with the free noncommutative algebra $F[Y]$, and let $A^m$ denote the set of all $m$-tuples over $A$. If $S$ is a subset of $A^m$ we say that $f \in A_F\langle Y\rangle$ is a generalized polynomial identity, GPI, for $S$ over $F$ if $f$ vanishes on $S$.

THEOREM (Amitsur [1]), *If $E$ is a division ring with center $C$ and $0 \neq f \in E_C\langle Y\rangle$ is a GPI for $E^m$ over $C$ then $(E : C) < \infty$.*

THEOREM (Skinner–Rowen). *Let $Y = \{y_1, y_2, \cdots, y_m, w_1, w_2, \cdots, w_m\}$ and let $E$ be a division ring with involution $*$ and with center $C$. Let $S = \{p \in E^{2m} \mid p = (a_1, a_2, \cdots, a_m, a_1^*, a_2^*, \cdots, a_m^*),\ a_i \in E\}$. If $0 \neq f \in E_C\langle Y\rangle$ is a GPI for $S$ over $C$ then $(E : C) < \infty$.*

This latter result is a special case of a theorem first proved (unpublished) by Skinner in his dissertation ([9], theorem 4.1) for primitive rings. In published form it is a corollary to a more general result of Rowen ([8], theorem 6) for prime rings. Rowen's result generalized a theorem of the author's ([7], theorem 4.7), also for prime rings but where just the symmetric elements were assumed to satisfy a GPI.

Throughout the remainder of this paper $D$ will be a fixed division ring. We set $X = \{x_1, x_2, \cdots, x_m\}$ and, following Bergman, denote by $R(X, D)$ the set of all formal *rational expressions* in the disjoint union $X \cup D$ involving the binary operations $+$, $-$, $\cdot$ and the unary operation of forming inverses. We emphasize that no associativity is assumed, e.g., $(x_1^{-1} + x_2) + x_1 \neq x_1^{-1} + (x_2 + x_1)$, and that the formal inverse of any expression may be formed, e.g. $(x_1 - x_1)^{-1} \in R(X, D)$. The phrase *polynomial expression* will be used when just $+$, $-$, $\cdot$ are involved.

Every element $f \in R(X, D)$ may be built up from $X \cup D$ as follows. Start with a polynomial expression $g_1$ in the elements of $X \cup D$. Then let $g_2$ be a polynomial expression in $g_1^{-1}$ and the elements of $X \cup D$. Inductively let $g_i$ be a polynomial expression in $g_1^{-1}, g_2^{-1}, \cdots, g_{i-1}^{-1}$ and the elements of $X \cup D$. An arbitrary element $f$ is then a polynomial in $g_1^{-1}, g_2^{-1}, \cdots, g_n^{-1}$ and the elements of $X \cup D$. We shall say $f$ involves the $n$ inverses $g_1^{-1}, g_2^{-1}, \cdots, g_n^{-1}$. We illustrate this with an example (Hua's identity). Let

$$f = [x^{-1} + (a^{-1} - x)^{-1}]^{-1} - [x - x(ax)] \qquad \text{where } x \in X \text{ and } a \in D.$$

Here we may take $g_1 = x$, $g_2 = a$, $g_3 = g_2^{-1} - x$, $g_4 = g_1^{-1} + g_3^{-1}$, $f = g_4^{-1} - [x - x(ax)]$.

Next let $E$ be any division ring containing $D$ and, as earlier, let $E^m$ denote the set of $m$-tuples over $E$. If $f$ is a rational expression involving the inverses $g_1^{-1}, g_2^{-1}, \cdots, g_n^{-1}$ and $p \in E^m$, we say that $f(p)$ exists in $E$ if and only if each $g_i(p)$ exists and is nonzero. This definition is meaningful since $g_1$ is always defined and the $g_i$'s are defined inductively. Notationally one would write

$$f(p) = f(p, g_1(p)^{-1}, g_2(p, g_1(p)^{-1})^{-1}, \cdots).$$

We set $\operatorname{dom} f = \{p \in E^m \mid f(p) \text{ is defined}\}$ and $Z(f) = \{p \in \operatorname{dom} f \mid f(p) = 0\}$. For $S$ a subset of $E^m$ we say that $f$ is nondegenerate on $S$ if $S \cap \operatorname{dom} f$ is nonempty. If $q = (a_1, a_2, \cdots, a_m) \in S$ then we let $D_q$ denote the subdivision ring of $E$ generated by $D$ and the $a_i$'s. $S$ is called a *flat subset* of $E^m$ if and only if for any two elements $p, q$ in $S$, there exist infinitely many $c \in C$, the center of $E$, such that $(1-c)p + cq \in S$ (Bergman originally called such a subset "webbed"). We close this paragraph with the key definition: if $E \supseteq D$ and $S$ is a subset of $E^m$, an element $f \in R(X, D)$ is a generalized rational identity, GRI, on $S$ if $f(p) = 0$ for all $p \in S \cap \operatorname{dom} f$. We allow the possibility that $f$ might be degenerate. $I(S)$ will denote the set of all GRI's on $S$.

The polynomial ring $E[T]$, where $t$ is a commutative indeterminate over the division ring $E$ (with center $C$), is well known to be a (right) Ore domain and as such has a division ring of right quotients $\bar{E} = E(t)$ with infinite center $C(t)$. For each $c \in C$ we set

$$E_c(t) = \{\phi(t) \in E(t) \mid \phi(c) \text{ is defined}\}.$$

$E_c(t)$ is well known to be a (local) ring for which the substitution $t \to c$ yields a homomorphism of $E_c(t)$ into $E$. One may also form the division ring of formal Laurent series $E\{t\}$ which contains as a subring the set of formal power series $E\{t\}^+$. It is clear that $E(t)$ is a subdivision ring of $E\{t\}$ and that $E_0(t)$ is contained in $E\{t\}^+$. Next form $E(u)$, which has an endomorphism $\phi$ which is the identity on $E$ but which maps $u$ to $u^2$. Then form the skew Laurent series ring $\tilde{E} = E(u)\{v\}$ with respect to $\phi$, i.e., the law $vu = u^2v$ and its consequences must be obeyed. It is well known that since $\phi$ is of infinite order the center of $\tilde{E}$ is $C$ and $(\tilde{E} : C) = \infty$.

The proof of the following key result is a simplification, due to Bergman [3], of the proof of lemma 14 in Amitsur [2]. The theorem relates GRI's to GPI's.

Main Theorem. *Let $E$ be a division ring containing $D$ and let $S$ be a flat subset of $E^m$. If $f$ is a GRI on $S$ but not a GRI on $E^m$ then there exists $q \in S$ and $h \in D_q\langle Y\rangle$ (free product over the prime field) such that $h$ vanishes on $S$ but not on $E^m$.*

PROOF. Let $f$ involve the inverses $g_1^{-1}, g_2^{-1}, \cdots, g_n^{-1}$ and let $p \in E^m$ for which $f(p)$ is defined and $f(p) \neq 0$ but $f$ is a GRI on $S$. Suppose $f$ is degenerate on $S$. Among all elements of $S$ pick $q \in S$ such that $g_1(q), g_2(q), \cdots, g_j(q)$ are defined, with $j$ maximal, $1 \leqq j \leqq n$. We claim that $g = g_1 g_2 \cdots g_j$ is a nondegenerate GRI on $S$. Indeed, $g(q)$ exists, and suppose $g(s)$ exists and is nonzero for some $s \in S$, thus forcing $g_j(s) \neq 0$. If $j = n$ then $s \in \operatorname{dom} f$, a contradiction, while if $j < n$, then $g_{j+1}(s)$ exists, contradicting the maximality of $j$. Furthermore, $g(p)$ exists and is nonzero since $p \in \operatorname{dom} f$. Therefore we may assume without loss of generality that $f$ is a nondegenerate GRI on $S$ such that $f(p) \neq 0$. We then choose $q \in S \cap \operatorname{dom} f$.

As a consequence of theorem 15 in Amitsur [2] $\tilde{E}_C\langle Y\rangle$ is imbeddable in a division ring $H$ and $H\{t\}^+$ is in turn contained in the division ring $K = H\{t\}$. For $y = (y_1, y_2, \cdots, y_m) \in H^m \subseteq K^m$ we next aim to show that $f$ is defined at the point $(1-t)q + ty \in \tilde{E}_C\langle Y\rangle\{t\}^m \subseteq K^m$. Clearly $g_1[(1-t)q + ty] \in H_0(t)$ is of the form $\phi_1(t) = \Sigma_{i=0}^{l} \psi_i(y)t^i$, where each $\psi_i(y) \in [D_q, Y]$, the subring of $\tilde{E}_C\langle Y\rangle$ generated by $D_q$ and $Y$. Since $\phi_1(0) = \psi_0(y) = g_1(q) \neq 0$, $\phi_1(t)^{-1} \in H_0(t)$ and is also of the form $\Sigma_{i=0}^{\infty} \sigma_i(y)t^i$ with $\sigma_0(y) = g_1(q)^{-1}$ and each $\sigma_i(y) \in [D_q, Y]$. Hence

$$g_2[(1-t)q + ty, g_1[(1-t)q + ty]^{-1}] \in H_0(t)$$

is of the form $\phi_2(t) = \Sigma_{i=0}^{\infty} \lambda_i(y)t^i$, $\lambda_i(y) \in [D_q, Y]$, $\phi_2(0) = \lambda_0(y) = g_2(q) \neq 0$. Continuing in this fashion one finally obtains that $f[(1-t)q + ty]$ lies in $H_0(t)$ but at the same time can be written as $\Sigma_{i=0}^{\infty} h_i(y)t^i$, $h_i(y) \in [D_q, Y]$.

For any $r \in E^m$ consider the homomorphism $\tau_r : \tilde{E}_C\langle Y\rangle\{t\}^+ \to \tilde{E}_C\{t\}^+$ which is the identity on $\tilde{E}$ and sends $y_i \to r_i$ and $t \to t$. Since $\tau_r$ preserves sums, products, and inverses we have

$$f[(1-t)q + tr] = \tau_r(f[(1-t)q + ty]) = \tau_r\left(\sum_{i=0}^{\infty} h_i(y)t^i\right) = \sum_{i=0}^{\infty} h_i(r)t^i$$

where $h_i(y) \in [D_q, Y]$.

Now let $r \in S$ and set $\phi(t) = f[(1-t)q + tr]$. Since $S$ is flat there exist infinitely many $c \in C$ such that $(1-c)q + cr \in S$, $\phi(c)$ is defined and $f[(1-c)q + cr] = 0$. However $\phi(t)$ can have only a finite number of roots from $C$ and so it follows that for $r \in S$, $f[(1-t)q + tr] = 0$, whence each $h_i(r) = 0$. But $\chi(t) = f[(1-t)q + tp] \neq 0$ since $\chi(1) = f(p) \neq 0$. Accordingly some $h_j(0) \neq 0$, and if $h$ is a pre-image of $h_j$ under the "inclusion" map $D_q\langle Y\rangle \to \tilde{E}_C\langle Y\rangle$ then $h \in D_q\langle Y\rangle$ vanishes on $S$ but not on $E^m$. This completes the proof.

THEOREM (Bergman). *Let $D$ be a fixed division ring with center $K$ and let $D \subseteq E_i$, $i = 1,2$ be any two division rings whose respective centers $C_i$ are such that $K \subseteq C_i$, $C_i$ is infinite and $(E_i : C_i) = \infty$. Then $I(E_1^m) = I(E_2^m)$.*

PROOF. We first establish the theorem for the special case where $E_1 \subseteq E_2$ and $C_1 \subseteq C_2$. Set $S = E_1^m$, easily seen to be a flat subset of $E_2^m$ since $C_1 \subseteq C_2$ and $C_1$ is infinite. Suppose $f$ is a GRI on $S$ but not on $E_2^m$. We may apply the Main Theorem to obtain $h \in D_q\langle Y\rangle$ for some $q \in S$ such that $h$ vanishes on $S$ but not on $E_2^m$. We note that $D_q \subseteq E_1$, that the inclusion map $\sigma : D_q\langle Y\rangle \to E_{1_{C_1}}\langle Y\rangle$ is a homomorphism, and likewise the inclusion map $\tau : E_{1_{C_1}}\langle Y\rangle \to E_{2_{C_2}}\langle Y\rangle$ is also a homomorphism since $C_1 \subseteq C_2$.

What we have shown is that $\sigma(h)$ is a GPI for $E_1^m$ over $C_1$ whereas $\tau\sigma(h)$ is not a GPI for $E_2^m$ over $C_2$. But this is a contradiction to the aforementioned Amitsur's theorem since $\sigma(h)$ vanishing on $E_1$ would imply $(E_1 : C_1) < \infty$.

We return now the general case. Form $\hat{D} = \bar{\bar{D}}$ and note that its center is $K(t)$, infinite field, with $(\hat{D} : K(t)) = \infty$. Now let $E \supseteq D$ satisfy the hypothesis of the theorem and note that $\hat{E}$ contains both $\hat{D}$ and $E$. Furthermore the center $C(t)$ of $\hat{E}$ contains both $C$ and $K(t)$ since by assumption $K \subseteq C$. But then by the argument of the preceding paragraph $I(\hat{D}^m) = I(\hat{E}^m) = I(E^m)$ and the proof is complete.

We now turn our attention to the main purpose of this note, that of proving a generalization of Desmarais's theorem.

THEOREM. *Let $D$ be a fixed division ring and let $E \supseteq D$ be a divison ring with involution $*$ and with infinite center $C$ and such that $(E : C) = \infty$. Let $X = \{x_1, x_2, \cdots, x_m, z_1, z_2, \cdots, z_m\}$ and set*

$$S = \{p \in E^{2m} \mid p = (a_1, a_2, \cdots, a_m, a_1^*, a_2^*, \cdots, a_m^*),\ a_i \in E\}.$$

*Then $I(S) = I(E^{2m})$.*

PROOF. Suppose $f$ is a GRI on $S$ which is not a GRI on $E^{2m}$. The set $C_S = \{c \in C \mid c^* = c\}$ is still infinite and for each $c \in C_S$, $p, q \in S$ we have $(1-c)p + cq \in S$, i.e. $S$ is flat. We set $Y = \{y_1, y_2, \cdots, y_m, w_1, w_2, \cdots, w_m\}$. The conditions of the Main Theorem are satisfied and so there exists a polynomial $h \in D_q\langle Y\rangle$ such that $h$ vanishes on $S$ but not on $E^{2m}$. Let $\sigma$ be the inclusion map of $D_q\langle Y\rangle$ into $E_C\langle Y\rangle$. By Skinner's theorem $\sigma(h) = 0$ since $(E : C) = \infty$, a contradiction.

To obtain Desmarais's original theorem (as stated at the beginning of this paper) take $D = K = C$ the center of a division ring $E$ with involution $*$, $C$

infinite and $(E:C)=\infty$. Consider

$$X=\{x_1,x_2,\cdots,x_m\},\qquad S=\{(a_1,a_2,\cdots,a_m)\mid a_i^*=a_i,\ a_1\in E\}$$

and let $f$ be a rational identity on $S$. Then take $Z=\{x_1,x_2,\cdots,x_m,z_1,z_2,\cdots,z_m\}$, form

$$T=\{(a_1,a_2,\cdots,a_m,a_1^*,a_2^*,\cdots,a_m^*)\mid a_i\in E\}$$

and set $g=f(x_1+z_1,x_2+z_2,\cdots,x_m+z_m)$. Then $g$ is a rational identity on $T$. An application of the preceding theorem says that $g$ is a rational identity on $E^{2m}$, and in particular $f$ is a rational identity on $E^m$.

We close with the observation that the framework in which the Main Theorem is stated allows one to study other possibilities for the set $S$. For instance various results of Kharchenko [6] involving (generalized) identities with automorphisms or derivations should now be extendable to the context of rational identities.

## REFERENCES

1. S. A. Amitsur, *Generalized polynomial identities and pivotal monomials*, Trans. Amer. Math. Soc. **114** (1965), 210–226.

2. S. A. Amitsur, *Rational identites and applications to algebra and geometry*, J. Algebra **3** (1966), 304–359.

3. G. M. Bergman, *Skew fields of noncommutative rational functions, after Amitsur*, Sem. Schützenberger — Lentin — Nivat 1969/70 No. 16 (Paris 1970).

4. P. M. Cohn, *Skew Field Constructions*, Cambridge Univ. Press, 1977.

5. P. C. Desmarais, *Rings with involution, generalized pivotal monomials and rational identities*, Ph.D. thesis, Univ. of Mass., 1974.

6. V. K. Kharchenko, *Generalized identities with automorphisms*, Algebra i Logika **14** (1975), 215–237.

7. W. S. Martindale, 3rd, *Prime rings with involution and generalized polynomial identities*, J. Algebra **22** (1972), 502–516.

8. L. H. Rowen, *Structure of rings with involution applied to generalized polynomial identities*, Canad. J. Math. **27** (1975), 573–584.

9. J. B. Skinner, *Generalized polynomial identities*, Ph.D. thesis, Univ. of Mass., 1970.

AMERICAN INTERNATIONAL COLLEGE
SPRINGFIELD, MA 01109 USA

UNIVERSITY OF MASSACHUSETTS
AMHERST, MA 01003 USA