行政院國家科學委員會專題研究計畫　期中進度報告

體中子集之代數性(2/3)

計畫類別： 個別型計畫
計畫編號： NSC92-2115-M-002-017-
執行期間： 92 年 08 月 01 日至 93 年 07 月 31 日
執行單位： 國立臺灣大學數學系暨研究所

計畫主持人： 李白飛

報告類型： 精簡報告
報告附件： 出席國際會議研究心得報告及發表論文
處理方式： 本計畫可公開查詢

中　華　民　國 93 年 5 月 25 日

Proceedings of the Edinburgh Mathematical Society

Submitted Paper
Paper 9 April 2004

NOTE ON GROUP IDENTITIES IN DIVISION RINGS

M. A. CHEBOTAR[1] AND P.-H. LEE[2]

[1] *Department of Mechanics and Mathematics, Tula State University*
Tula, Russia (mchebotar@tula.net)
[2] *Department of Mathematics, National Taiwan University*
Taipei, Taiwan (phlee@math.ntu.edu.tw)

(Received)

Abstract Let D be a division ring whose group of units satisfies a nontrivial group identity w. Let α be the sum of positive degrees of indeterminates occurring in w. If the center of D contains more than 3α elements, then D is commutative.

Keywords: division ring, group of units, group identity, polynomial identity.
AMS 2000 Subject classification: Primary 16R50, Secondary 16K20.

Given a unital ring R, the set $U(R)$ of its units (invertible elements) forms a group, called the group of units of R. The group $U(R)$ is said to satisfy a group identity if there exists a nontrivial word $w(x_1, \dots, x_n)$ in the free group generated by $x_1, \dots, x_n, \dots$ such that $w(u_1, \dots, u_n) = 1$ for all $u_1, \dots, u_n \in U(R)$. The study of certain rings R (especially group algebras) with $U(R)$ satisfying group identities has experienced a significant progress in the past decade [5, 6, 9, 10, 11, 12].

The group identities are special cases of rational identities which were thoroughly investigated by Amitsur [1], Bergman [3, 4] and Valitskas [14]. As an application of his theory of rational identities, Amitsur proved that a division ring D with center $Z(D)$ infinite and $U(D)$ satisfying a group identity is commutative [1] [13, Theorem 8.4.2]. This extends a classical result due to Hua who showed that a division ring D with $Z(D)$ infinite and $U(D)$ solvable is commutative [7] [13, Corollary 8.4.3]. In this note we study division rings D with $Z(D)$ not necessarily infinite and $U(D)$ satisfying a group identity. We show that D is commutative so long as $Z(D)$ contains sufficiently many elements.

In what follows, we denote $D[x]$ the ring of polynomials and $D((x))$ the ring of Laurent series in a central indeterminate x over a division ring D. It is well-known that $D((x))$ is a division ring and $D[x] \subseteq D((x))$. Hence every nonzero polynomial is invertible in $D((x))$. In particular, for any $a \in D$, $1 + ax$ is invertible in $D((x))$ and, more explicitly, its inverse is given by

$$1 + \sum_{i=1}^{\infty} (-a)^i x^i$$

[13, Remark 8.2.10]. As a matter of fact, $D[x]$ is a principal left ideal domain (PLID) [13, Proposition 8.2.2], so it has a division ring $D(x)$ of fractions. Moreover, we have $D[x] \subseteq D(x) \subseteq D((x))$.

We begin with an elementary fact in $D[x]$ which plays an important role in the sequel. Since $D[x]$ is a PLID, for any nonzero $r_1, r_2 \in D[x]$, there exist nonzero $s_1, s_2 \in D[x]$ such that $s_2 r_1 = s_1 r_2$ [13, Proposition 8.2.3]. In case both r_1 and r_2 are linear, so can we choose s_1 and s_2.

Lemma 1. *Let D be a division ring. For any $r_1 = 1 + ax$, $r_2 = 1 + bx \in D[x]$, there exist $s_1, s_2 \in D[x]$ of degrees at most 1 such that $r_1 r_2^{-1} = s_2^{-1} s_1$ (in $D(x)$).*

Proof. If $a = b$, take $s_1 = s_2$ to be any element in $D[x]$ of degree at most 1. So we may assume that $a \neq b$. Let $s_1 = 1 + (b-a)a(b-a)^{-1}x$ and $s_2 = 1 + (b-a)b(b-a)^{-1}x$. We leave the verification to the reader that $s_2 r_1 = s_1 r_2$.

□

Corollary 2. *Let D be a division ring, $r_i = 1 + a_i x \in D[x]$ and $r = r_1^{\gamma_1} r_2^{\gamma_2} \dots r_m^{\gamma_m}$, where γ_i are nonzero integers. Let $I = \{i \mid i = 1, \dots, m,\ \gamma_i > 0\}$, $J = \{i \mid i = 1, \dots, m,\ \gamma_i < 0\}$, $\alpha = \sum_{i \in I} \gamma_i$ and $\beta = -\sum_{i \in J} \gamma_i$. Then $r = s_2^{-1} s_1$ (in $D(x)$), where s_1 is a polynomial of degree at most α and s_2 is a polynomial of degree at most β.*

We will also need another auxiliary result which follows from a Vandermonde argument [13, Proposition 2.3.26 and Proposition 2.3.27].

Lemma 3. *Let D be a division ring with center F and $f(x)$ a polynomial in $D[x]$ of degree n. Suppose that $f(c) = 0$ for all $c \in F$. Then F contains at most n elements.*

With all these on hand and using some ideas of [13, Theorem 8.2.11], we are now ready to prove our main result of this note.

Theorem 4. *Let D be a division ring with center F. Suppose that the group $U(D)$ of units satisfies a nontrivial group identity $w(z_1, \dots, z_m) = z_1^{\gamma_1} \dots z_m^{\gamma_m}$, where the γ_i's are nonzero integers and the z_i's are not necessarily distinct. Let $I = \{i \mid i = 1, \dots, m,\ \gamma_i > 0\}$, $J = \{i \mid i = 1, \dots, m,\ \gamma_i < 0\}$, $\alpha = \sum_{i \in I} \gamma_i$ and $\beta = -\sum_{i \in J} \gamma_i$. If F contains more than $3 \min\{\alpha, \beta\}$ elements, then D is commutative.*

Proof. If $\alpha - \beta = \gamma \neq 0$, we get $y^\gamma = 1$ for all $y \in U(D)$ by setting $z_1 = \dots = z_m = y \in U(D)$ in $w(z_1, \dots, z_m) = 1$. Then it follows from Jacobson's Theorem [8, Theorem 12.10] that D is commutative. Hence we may assume that $\alpha = \beta$.

By Amitsur's theorem cited earlier [13, Theorem 8.4.2], we are done if F is infinite. So it suffices to consider the case where F is finite. If F is finite and D satisfies a nontrivial polynomial identity (PI), then by a theorem due to Kaplansky [2, Theorem 6.1.10], D is finite-dimensional over F and so D is finite. Thus D is commutative by Wedderburn's Theorem [8, Theorem 13.1].

Therefore we shall assume in what follows that $\alpha = \beta$, F is finite and D does not satisfy any nontrivial PI.

Let $S = F\{y_1, \ldots, y_m\}$ be the free algebra in indeterminates $y_1, \ldots, y_m$ over F, where $y_i = y_j$ if $z_i = z_j$ in $w(z_1, \ldots, z_m)$ and y_i does not commute with y_j if $z_i \neq z_j$; and let $T = S((x))$ be the ring of Laurent series in a central indeterminate x over S. Note that we are assuming that x commutes with each y_i for all $i = 1, \ldots, m$.

Let H be any noncommutative division ring with center $F(x)$, the rational function field over F. Since $w(z_1, \ldots, z_m)$ is a nontrivial word, there exist nonzero $u_1, \ldots, u_m \in H$ such that $w(u_1, \ldots, u_m) \neq 1$ in view of Amitsur's theorem. Or equivalently, $w(1 + v_1, \ldots, 1 + v_m) \neq 1$ for some $v_1, \ldots, v_m \in H$ with $v_i \neq -1$ for all $i = 1, \ldots, m$. Hence, $w(1 + y_1, \ldots, 1 + y_m)$ does not coincide with 1 identically. As a consequence, we see that the rational expression $w(1 + y_1x, \ldots, 1 + y_mx)$ does not coincide with 1 identically.

Note that each $1 + y_kx$ is invertible in $S((x))$ and its inverse is given by

$$1 + \sum_{i=1}^{\infty} (-y_k)^i x^i,$$

so we have

$$w(1 + y_1x, \ldots, 1 + y_mx) = 1 + \sum_{i=1}^{\infty} f_i(y_1, \ldots, y_m)x^i,$$

where each $f_i(y_1, \ldots, y_m)$ is a polynomial in the noncommuting indeterminates $y_1, \ldots, y_m$ over F. Since $w(1 + y_1x, \ldots, 1 + y_mx)$ does not coincide with 1 identically, we conclude that some of the polynomials $f_i(y_1, \ldots, y_m)$ must be nonzero.

For $u_1, \ldots, u_m \in D$ we have $w(1 + u_1x, \ldots, 1 + u_mx) \in D(x) \subseteq D((x))$ and

$$w(1 + u_1x, \ldots, 1 + u_mx) = 1 + \sum_{i=1}^{\infty} f_i(u_1, \ldots, u_m)x^i.$$

If $w(1 + u_1x, \ldots, 1 + u_mx) = 1$ for all $u_1, \ldots, u_m \in D$, then $f_i(u_1, \ldots, u_m) = 0$ for all $i = 1, 2, \ldots$. Thus D satisfies some nontrivial PI $f_i(y_1, \ldots, y_m)$, contradicting our assumption. Hence, $w(1+u_1x, \ldots, 1+u_mx) \neq 1$ for some $u_1, \ldots, u_m \in D$. By Corollary 2, $w(1 + u_1x, \ldots, 1 + u_mx)$ can be written as $g_2(x)^{-1}g_1(x)$, where $g_1(x)$ and $g_2(x)$ are polynomials in $D[x]$ of degrees at most α.

For any $c \in F$ with $1 + u_ic \neq 0$ for all $i = 1, \ldots, m$, we have $g_2(c)^{-1}g_1(c) = w(1 + u_1c, \ldots, 1+u_mc) = 1$ since $w(z_1, \ldots, z_m)$ is a group identity for $U(D)$. Note that $m \leq 2\alpha$ and since F has more than 3α elements, by Lemma 3 there exists $c \in F$ such that $1 + u_ic \neq 0$ for all $i = 1, \ldots, m$ and $g_1(c) - g_2(c) \neq 0$, contrary to $g_2(c)^{-1}g_1(c) = 1$. Thus the theorem is now proved. □

References

1. S.A. Amitsur, Rational identities and applications to algebra and geometry, *J. Algebra*, **3** (1966), 304–359.
2. K.I. Beidar, W.S. Martindale 3rd and A.V. Mikhalev, *Rings with Generalized Identities*, Marcel Dekker, Inc., New York–Basel–Hong Kong, 1996.

3. G.M. Bergman, Rational relations and rational identities in division rings I, *J. Algebra*, **43** (1976), 252–266.
4. G.M. Bergman, Rational relations and rational identities in division rings II, *J. Algebra*, **43** (1976), 267–297.
5. A. Giambruno, E. Jespers and A. Valenti, Group identities on units of rings, *Arch. Math.(Basel)*, **63** (1994), 291–296.
6. A. Giambruno, S. K. Sehgal and A. Valenti, Group algebras whose units satisfy a group identity, *Proc. Amer. Math. Soc.*, **125** (1997), 629–634.
7. L.K. Hua, On the multiplicative groups of a field, *Acad. Sinica, Science Record*, **3** (1950), 1–6.
8. T.Y. Lam, *A First Course in Noncommutative Rings*, Springer-Verlag, New York, 1991.
9. C.-H. Liu, Group algebras with units satisfying a group identity, *Proc. Amer. Math. Soc.*, **127** (1999), 327–336.
10. C.-H. Liu, Some properties on rings with units satisfying a group identity, *J. Algebra*, **232** (2000), 226–235.
11. C.-H. Liu and D.S. Passman, Group algebras with units satisfying a group identity II, *Proc. Amer. Math. Soc.*, **127** (1999), 337–341.
12. D.S. Passman, Group algebras whose units satisfies a group identity II, *Proc. Amer. Math. Soc.*, **125** (1997), 657–662.
13. L.H. Rowen, *Polynomial Identities in Ring Theory*, Academic Press, Inc., New York, 1980.
14. A.I. Valitskas, Rational identities of radical algebras, *Izv. Vyssh. Uchebn. Zaved. Math.*, **11** (1985), 63–72. (Russian; English transl. in *Soviet Math.* (*Iz. VUZ*) **29** (1985)).