Proceedings of the Edinburgh Mathematical Society (2004) **47**, 557–560 ©
DOI:10.1017/S0013091503000804 Printed in the United Kingdom

A 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, Republic of China* (phlee@math.ntu.edu.tw)

(Received 22 September 2003)

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

Keywords: division ring; group of units; group identity; polynomial identity

2000 *Mathematics 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 non-trivial 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 significant progress in the past decade [**5**, **6**, **9**–**12**].

The group identities are special cases of rational identities that 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 centre $Z(D)$ infinite and $U(D)$ satisfying a group identity is commutative (see [**1**] and [**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 (see [**7**] and [**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 the ring of polynomials by $D[x]$ and the ring of Laurent series by $D((x))$ in a central indeterminate x over a division ring D. It is well known that $D((x))$ is a division ring and that $D[x] \subseteq D((x))$. Hence every non-zero 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 [**13**, Remark 8.2.10]

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

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 about $D[x]$ that plays an important role below. Since $D[x]$ is a PLID, for any non-zero $r_1, r_2 \in D[x]$, there exist non-zero $s_1, s_2 \in D[x]$ such that $s_2 r_1 = s_1 r_2$ [**13**, Proposition 8.2.3]. If both r_1 and r_2 are linear, we can also choose s_1 and s_2 to be linear.

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 that $s_2 r_1 = s_1 r_2$ to the reader. □

Corollary 2. *Let D be a division ring, $r_i = 1 + a_i x \in D[x]$ and $r = r_1^{\gamma_1} r_2^{\gamma_2} \cdots r_m^{\gamma_m}$, where γ_i are non-zero 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**, Propositions 2.3.26 and 2.3.27].

Lemma 3. *Let D be a division ring with centre F and let $f(x)$ be 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 centre F. Suppose that the group $U(D)$ of units satisfies a non-trivial group identity $w(z_1, \dots, z_m) = z_1^{\gamma_1} \cdots z_m^{\gamma_m}$, where the γ_i are non-zero integers and the z_i 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 $z_1 = \cdots = z_m = y \in U(D)$ 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 non-trivial 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 $\alpha = \beta$, that F is finite and that D does not satisfy any non-trivial PI.

Let $S = F\{y_1, \dots, y_m\}$ be the free algebra in indeterminates $y_1, \dots, y_m$ over F, where $y_i = y_j$ if $z_i = z_j$ in $w(z_1, \dots, z_m)$ 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 $i = 1, \dots, m$.

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

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

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

Replacing each $(1+y_kx)^{-1}$ in $w(1+y_1x, \dots, 1+y_mx)$ by the above expression, we obtain

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

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

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

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

If $w(1 + u_1x, \dots, 1 + u_mx) = 1$ for all $u_1, \dots, u_m \in D$, then $f_i(u_1, \dots, u_m) = 0$ for all $i = 1, 2, \dots$. Thus D satisfies some non-trivial PI $f_i(y_1, \dots, y_m)$, contradicting our assumption. Hence, $w(1+u_1x, \dots, 1+u_mx) \neq 1$ for some $u_1, \dots, u_m \in D$. By Corollary 2, $w(1 + u_1x, \dots, 1 + u_mx)$ 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 $i = 1, \dots, m$, we have $g_2(c)^{-1}g_1(c) = w(1 + u_1c, \dots, 1+u_mc) = 1$ since $w(z_1, \dots, z_m)$ is a group identity for $U(D)$. Note that $m \leqslant 2\alpha$ 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 $i = 1, \dots, m$ 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. Alg.* **3** (1966), 304–359.
2. K. I. Beidar, W. S. Martindale III and A. V. Mikhalev, *Rings with generalized identities* (Marcel Dekker, New York, 1996).

3. G. M. Bergman, Rational relations and rational identities in division rings, I, *J. Alg.* **43** (1976), 252–266.
4. G. M. Bergman, Rational relations and rational identities in division rings, II, *J. Alg.* **43** (1976), 267–297.
5. A. Giambruno, E. Jespers and A. Valenti, Group identities on units of rings, *Arch. Math.* **63** (1994), 291–296.
6. A. Giambruno, S. K. Sehgal and A. Valenti, Group algebras whose units satisfy a group identity, *Proc. Am. Math. Soc.* **125** (1997), 629–634.
7. L. K. Hua, On the multiplicative groups of a field, *Acad. Sinica Sci. Record* **3** (1950), 1–6.
8. T. Y. Lam, *A first course in noncommutative rings* (Springer, 1991).
9. C.-H. Liu, Group algebras with units satisfying a group identity, *Proc. Am. Math. Soc.* **127** (1999), 327–336.
10. C.-H. Liu, Some properties on rings with units satisfying a group identity, *J. Alg.* **232** (2000), 226–235.
11. C.-H. Liu and D. S. Passman, Group algebras with units satisfying a group identity, II, *Proc. Am. Math. Soc.* **127** (1999), 337–341.
12. D. S. Passman, Group algebras whose units satisfy a group identity, II, *Proc. Am. Math. Soc.* **125** (1997), 657–662.
13. L. H. Rowen, *Polynomial identities in ring theory* (Academic, 1980).
14. A. I. Valitskas, Rational identities of radical algebras, *Izv. VUZ Mat.* **11** (1985), 63–72 (in Russian; English translation in *Soviet Math. (Iz. VUZ)* **29** (1985), 88–99).