SEMIGROUP IDENTITIES ON UNITS OF INTEGRAL GROUP RINGS

by MICHAEL A. DOKUCHAEV and JAIRO Z. GONÇALVES†

(Received 16 August 1994)

Abstract. Let $U(RG)$ be the group of units of a group ring RG over a commutative ring R with 1. We say that a group is an SIT-group if it is an extension of a group which satisfies a semigroup identity by a torsion group. It is a consequence of the main result that if G is torsion and $R = \mathbb{Z}$, then $U(RG)$ is an SIT-group if and only if G is either abelian or a Hamiltonian 2-group. If R is a local ring of characteristic 0 only the first alternative can occur.

1. Introduction. Let R be a commutative ring with 1, G be a group and $U(RG)$ be the group of units of the group ring RG. It has been intensively investigated that if $U(RG)$ satisfies some group theoretical condition, then G is somewhat restricted and a nontrivial ring theoretical property of RG holds. See [**1**], [**2**], [**3**], [**9**] for example. In this direction there is the following conjecture, which we attribute to Brian Hartley.

CONJECTURE. *Let K be a field and let G be a torsion group. If $U(KG)$ satisfies a group identity, then KG satisfies a polynomial identity.*

In an earlier work [**3**] addressed to this question, it was shown that the conjecture is true if K is an infinite field and $U(KG)$ satisfies a semigroup identity. Let $\langle a, b\rangle$ be the free semigroup (group) freely generated by a and b, and let $w_1(a,b)$, $w_2(a,b)$ be two distinct words in $\{a,b\}$. We say that a group G satisfies the *semigroup* (*group*) *identity* $w_1(a,b) = w_2(a,b)$, if it holds true for every substitution of the variables by elements of G. Certainly, if a group G satisfies a semigroup identity, then it satisfies a group identity. But the converse is not true, as can be seen in [**8**]. We say that a group H is an SIT-group if H is an extension of a group satisfying a semigroup identity by a torsion group.

The main question considered in this paper is: *when is the group of units $U(\mathbb{Z}G)$ of an integral group ring $\mathbb{Z}G$ an* SIT-*group*? We prove the following:

THEOREM. *If the torsion elements $t(G)$ of a group G form a subgroup and $U(\mathbb{Z}G)$ is an* SIT-*group, then any torsion subgroup of G is normal in G and $t(G)$ is either abelian or a Hamiltonian* 2-*group.*

An immediate consequence is:

COROLLARY. *If G is torsion then $U(\mathbb{Z}G)$ is an* SIT-*group if, and only if, G is either abelian or a Hamiltonian* 2-*group.*

In view of Passman's Theorem ([**7**, Theorem 5.37]) we can also conclude that if G is torsion and $U(\mathbb{Z}G)$ satisfies a semigroup identity, then $\mathbb{Z}G$ satisfies a polynomial identity.

Let us note that a free (noncyclic) group is never an SIT-group. We shall use this

† The first author was supported by NSERC-Canada and the second by CNPq-Brazil.

observation together with the Hartley and Pickel Theorem [**4**], throughout the paper. In fact, our result can be considered as an attempt to extend this theorem to torsion groups.

We end up our work answering our main question for local rings of characteristic 0.

2. Preliminary results. Rosenblatt [**8**] describes a class of group identities that is very convenient to handle. Let $\mathbf{i}=(i_1,\ldots,i_s)$, $\mathbf{j}=(j_1,\ldots,j_s)$ be $\{0,1\}$-valued sequences. Let $F=\langle X,Y\rangle$ be the free group generated by X and Y. An R-equation is an expression of the form

$$X_1^{i_1}X_2^{i_2}\ldots X_s^{i_s}=X_1^{j_1}X_2^{j_2}\ldots X_s^{j_s}, \tag{2.1}$$

where $X_k=Y^{-k}XY^k$, and $\sum_{r=1}^{s} i_r=\sum_{r=1}^{s} j_r$.

Certainly, an R-equation is a nontrivial group equation if i and j are distinct sequences. Furthermore, we observe that after some obvious cancellations, it reduces to a nontrivial semigroup equation.

The result below, which is implicit in [**8**], and proved in [**3**], will be necessary in the sequel.

Lemma 2.2. *If a group satisfies a nontrivial semigroup identity, then it satisfies a non-trivial R-equation.*

Let G be a group and let x and g be elements of G, with $|\langle g\rangle|=n\geq 5$, $n\neq 6$ and $x\notin N_G\langle g\rangle$. Here $N_G\langle g\rangle$ denotes the normalizer of $\langle g\rangle$ in G. Moreover, let φ be the Euler phi function, and let $1<i<n$, $(i,n)=1$, $m=\varphi(n)$,

$$i^m=1+kn,\qquad v=1+(g-1)x\hat{g},\qquad \hat{g}=\sum_{j=0}^{n-1}g^j,\qquad A=1+g+\ldots+g^{i-1}.$$

Then $u=A^m-k\hat{g}$ and v are units of infinite order in $U(\mathbb{Z}G)$ (see [**10**, pages 2 and 32]). For a positive integer τ we have

$$u^\tau=A^{\tau m}-k\alpha_\tau\hat{g},\qquad 1=\varepsilon(u^\tau)=i^{\tau m}-k\alpha_\tau n,$$

where $\alpha_\tau=\dfrac{i^{m\tau}-1}{i^m-1}$ and ε is the augmentation function on $\mathbb{Z}G$. If l is a positive integer we set $u_l^\tau=v^{-l}u^\tau v^l$. For a $\{0,1\}$-sequence $\mathbf{i}=(i_1,\ldots,i_s)$ we define a new sequence $\mathbf{i}^*=(i_1,\ldots,i_{s-1})$, and a polynomial $p_i(X)\in\mathbb{Z}[X]$ by

$$p_i(X)=i_1+2i_2X^{i_1}+3i_3X^{i_1+i_2}+\ldots+si_sX^{i_1+\cdots+i_{s-1}}.$$

Lemma 2.3. *With the notation above we have*
(i) $p_i(A^{\tau m})=p_{i^*}(A^{\tau m})+si_sA^{\tau m(i_1+\cdots+i_{s-1})}$
(ii) $u_1^{\tau i_1}\ldots u_s^{\tau i_s}=u^{\tau(i_1+\cdots+i_s)}+p_i(A^{\tau m})(A^{\tau m}-1)(g-1)x\hat{g}$.

Proof. We obtain (i) easily from

$$p_i(X)=p_{i^*}(X)+si_sX^{i_1+\cdots+i_{s-1}}.$$

We shall prove (ii) by induction on the length of $\mathbf{i}$. Since $\hat{g}u^{\tau} = \hat{g}\varepsilon(u^{\tau}) = \hat{g}$, we have

$$\begin{aligned} v^{-l}u^{\tau}v^{l} &= [1 - l(g-1)x\hat{g}]u^{\tau}[1 + l(g-1)x\hat{g}] \\ &= [u^{\tau} - l(g-1)x\hat{g}[1 + l(g-1)x\hat{g}] = u^{\tau} + l(A^{\tau m} - 1)(g-1)x\hat{g}. \end{aligned}$$

Hence

$$u_1^{\tau i_1} = u^{\tau i_1} + i_1(A^{\tau m} - 1)(g-1)x\hat{g},$$

and the Lemma is proved for a $\{0, 1\}$-sequence (i_1) of length 1.

Now we prove the induction step. Note that

$$\begin{aligned} u^{\tau(i_1+\ldots+i_{s-1})}(g-1) &= (A^{\tau m} - k\alpha_{\tau}\hat{g})^{i_1+\cdots+i_{s-1}}(g-1) \\ &= A^{\tau m(i_1+\ldots+i_{s-1})}(g-1). \end{aligned}$$

Therefore

$$\begin{aligned} u_1^{\tau i_1}\ldots u_{s-1}^{\tau i_{s-1}}u_s^{\tau i_s} &= [u^{\tau(i_1+\ldots+i_{s-1})} + p_{i^*}(A^{\tau m})(A^{\tau m} - 1)(g-1)x\hat{g}] \\ &\quad \times [u^{\tau} + s(A^{\tau m} - 1)(g-1)x\hat{g}]^{i_s} \\ &= u^{\tau(i_1+\ldots+i_{s-1}+i_s)} + i_s s(A^{\tau m} - 1)u^{\tau(i_1+\ldots+i_{s-1})}(g-1)x\hat{g} \\ &\quad + p_{i^*}(A^{\tau m})(A^{\tau m} - 1)(g-1)x\hat{g}u^{\tau i_s} \\ &= u^{\tau(i_1+\ldots+i_{s-1}+i_s)} + [p_{i^*}(A^{\tau m}) + i_s \,.\, sA^{\tau m(i_1+\ldots+i_{s-1})}] \\ &\quad \times (A^{\tau m} - 1)(g-1)x\hat{g}. \end{aligned}$$

Now, using (i) we get (ii). The lemma is proved. □

For a subgroup H of $\langle g\rangle$ we denote by $\Delta_{\mathbb{Z}\langle g\rangle}(H)$ the kernel of the natural ring homomorphism

$$\mathbb{Z}\langle g\rangle \to \mathbb{Z}(\langle g\rangle/H).$$

The next lemma generalizes a well known argument about normalizers.

Lemma 2.4. *Let $|\langle g\rangle| = n$, $u \in \mathbb{Z}\langle g\rangle$, $x \notin N_G\langle g\rangle$, and let H be the largest subgroup of $\langle g\rangle$ such that $x \in N_G(H)$. Then $ux\hat{g} = 0$ implies $u \in \Delta_{\mathbb{Z}\langle g\rangle}(H)$. In particular, if $H = \{1\}$ then $u = 0$.*

Proof. Let k be the smallest nonnegative integer such that $H = \langle g^k\rangle$, and let

$$u = a_0 + a_1 g + \ldots + a_{k-1}g^{k-1},$$

where $a_i \in \mathbb{Z}H$. Then we have

$$(a_0 + a_1 g + \ldots + a_{k-1}g^{k-1})x\hat{g} = 0. \tag{2.5}$$

We want to show that for every i, $i = 0, \ldots, k-1$ we have

$$a_i \,.\, \hat{g} = 0. \tag{2.6}$$

Assume that $a_{i'}\hat{g} \neq 0$ for some $i' \in \{0, 1, \ldots, k-1\}$. Note that $a_{i'}^x \in \mathbb{Z}H$, where $a_{i'}^x = x^{-1}a_{i'}x$. If $a_{i'}^x\hat{g} = 0$ then $a_{i'}^x \in \Delta_{\mathbb{Z}\langle g\rangle}(H)$ and $a_{i'} \in \Delta_{\mathbb{Z}\langle g\rangle}(H)$, because $(1 - g^k)^x \in \Delta_{\mathbb{Z}\langle g\rangle}(H)$. Therefore $a_{i'}\hat{g} = 0$, contrary to hypothesis. Consequently $a_{i'}^x\hat{g} \neq 0$ and $a_{i'}x\hat{g} \neq 0$. Hence, if t is a positive integer such that $g^{kt} \in \operatorname{supp} a_{i'}$, it follows from (2.5) that

$$g^{kt}g^{i'}x = g^{kt'}g^{i''}xg^{s} \tag{2.7}$$

for some $i'' \in \{0, 1, \ldots, k-1\}$, $i'' \neq i'$, some integer t' and $s \in \{0, 1, \ldots, n-1\}$. By (2.7), it is easy to see that $xg^s x^{-1} \in \langle g \rangle$, and so $s \equiv 0 (\mathrm{mod}\ k)$. From (2.7), in view of $x \in N_G(H)$, we obtain $g^{kt}g^{i'}x = g^{k\bar{t}}g^{i''}x$, for some integer $\bar{t}$, where

$$g^{k\bar{t}} = g^{kt}(g^s)^{x^{-1}}.$$

Consequently, $g^{kt}g^{i'} = g^{k\bar{t}}g^{i''}$, which implies $i' = i''$, a contradiction.

Now, from (2.6) we conclude that $a_i \in \Delta_{\mathbb{Z}\langle g \rangle}(H)$, and $u \in \Delta_{\mathbb{Z}\langle g \rangle}(H)$, as required. □

LEMMA 2.8. *Suppose that the set of torsion elements $t(G)$ of a group G forms a subgroup, which is either Abelian or a Hamiltonian 2-group. If $U(\mathbb{Z}G)$ is an* SIT-*group, then any subgroup of $t(G)$ is normal in G.*

Proof. Let $g \in t(G)$ and $x \in G$. Let us denote by H' the first commutator subgroup of $H = \langle g, x \rangle$ and $[g, x] = g^{-1}x^{-1}gx$. By the assumption $\langle g, g^x \rangle = \langle g, [g, x] \rangle$ is finite, and therefore $[g, x] \in t(G)$. Hence $H' = \langle [g, x]^h \mid h \in H \rangle$ is torsion and, consequently, H' is either Abelian or a Hamiltonian 2-group. In both cases H is solvable. Since $U(\mathbb{Z}G)$ does not contain a free noncyclic subgroup, by Hartley and Pickel's Theorem [**4**], we conclude that $x \in N_G\langle g \rangle$. Since x is arbitrary $\langle g \rangle$ is normal in G. The lemma is proved. □

3. The proof of the theorem. In view of Lemma 2.8 we can assume that G is a torsion group. Let $g \in G$, $|\langle g \rangle| = p^e = n \geq 5$, p a prime and $x \in G$, $x \notin N_G\langle g \rangle$. Let $N \lhd U(\mathbb{Z}G)$ be such that $U(\mathbb{Z}G)/N$ is torsion and N satisfies a semigroup identity. Define elements u and v as in Lemma 2.3. Then u^τ, $v^l \in N$ for some positive integers τ and l, and, by Lemma 2.2, N satisfies an R-equation (2.1). For a positive integer $\tau' \equiv 0 (\mathrm{mod}\ \tau)$ put $X = u^{\tau'}$ and $Y = v^l$ in (2.1). Then, by Lemma 2.3, we get

$$[p_j(A^{\tau' m}) - p_i(A^{\tau' m})](A^{\tau' m} - 1)(g-1)x\hat{g} = 0. \tag{3.1}$$

Suppose that x does not normalize any nonidentity subgroup of $\langle g \rangle$. Then, by Lemma 2.4, we obtain that

$$[p_j(A^{\tau' m}) - p_i(A^{\tau' m})](A^{\tau' m} - 1)(g-1) = 0. \tag{3.2}$$

Since $(i_1, \ldots, i_s)$ and $(j_1, \ldots, j_s)$ are distinct $\{0, 1\}$-sequences, then $p_j(X) - p_i(X)$ is not identically zero. Let $n' \mid n$, $n' \geq 5$, and ξ be a primitive complex n'-th root of unity. Applying the map $g \mapsto \xi$ we see that $B = (1 + \xi + \xi^3 + \ldots + \xi^{i-1})^m$ is the image of A^m. By [6, Theorem 3.3.3(i)], B is a unit of infinite order in $\mathbb{Z}[\xi]$. Hence B^τ also has infinite order, and by (3.2) B^τ, $B^{2\tau}$, $B^{3\tau}, \ldots$ are distinct zeros of $p_j(X) - p_i(X)$, a contradiction. Therefore x normalizes a nonidentity subgroup of $\langle g \rangle$.

Let $\langle g^{p^j} \rangle$ be the largest subgroup of $\langle g \rangle$ which is normalized by x. It follows from (3.1) and Lemma 2.4 that

$$[p_j(A^{\tau' m}) - p_i(A^{\tau' m})](A^{\tau' m} - 1)(g-1) = (g^{p^j} - 1)\gamma, \qquad \gamma \in \mathbb{Z}\langle g \rangle.$$

If $p^j \geq 5$, then for a complex p^j-th root of unity ξ we have

$$[p_j(B^{\tau'}) - p_i(B^{\tau'})](\xi - 1),$$

where B is obtained from A^m by applying the map $g \mapsto \xi$. Again, B^τ, $B^{2\tau}$, $B^{3\tau}, \ldots$ are distinct roots of $p_j(X) - p_i(X)$, which is impossible. Hence $p^j < 5$. In particular, if $p > 3$, then $\langle g\rangle \lhd G$. Since $U(\mathbb{Z}\langle x,g\rangle)$ does not contain a free noncyclic subgroup, it follows from Hartley and Pickely [**4**] that $\langle x,g\rangle$ is abelian. Consequently, we have shown that

$$|\langle g\rangle| = p^e,\ p>3, \qquad \Rightarrow g\in z(G), \tag{3.3}$$

where $z(G)$ denotes the center of G.

If $p^j=3$, then $\langle g^3,x\rangle$ is finite and, by [**4**] again, we get that $x\in C_G\langle g^3\rangle$, where $C_G\langle g^3\rangle$ denotes the centralizer of g^3 in G. Thus

$$|\langle g\rangle| = 3^e \Rightarrow g^3\in z(G). \tag{3.4}$$

Let now $p=2$ and $p^j\in\{2,4\}$. We claim that

$$g^4\in z(G). \tag{3.5}$$

Indeed, if $p^j=2$, then, by [**4**], $\langle g^2,x\rangle$ is either abelian or a Hamiltonian 2-group. In both cases $[g^4,x]=1$. If $p^j=4$ and $[g^4,x]\neq 1$, then $\langle g^4,x\rangle$ is the quaternion group of order 8. It is easy to see that

$$x^2=[g^4,x]\Rightarrow [g^2,x]^{g^2}=x^2[g^2,x]^{-1},$$

and

$$1=[x^2,g^2]\Rightarrow [g^2,x]^x=[g^2,x]^{-1}.$$

Therefore $\langle g^2,x\rangle' = \langle x^2,[g^2,x]\rangle$ is abelian, and applying [**4**] for $U(\mathbb{Z}\langle g^2,x\rangle)$ we conclude that $\langle g^2,x\rangle$ is the quaternion group of order 8. This is impossible, since $g^8\neq 1$, and we have proved (3.5).

It follows from (3.3), (3.4) and (3.5) that $\exp G/z(G)$ divides 12. By [**5**, Theorem IX.4], G is locally finite. Again by [**4**], G is either abelian or a Hamiltonian 2-group. The theorem is proved. □

4. Semigroup identities on units of group rings over local rings. Our main result allows us to answer for $\mathbb{Z}_{(p)}$ the same question raised for $\mathbb{Z}$ in the introduction. Here $\mathbb{Z}_{(p)}$ denotes the localization of $\mathbb{Z}$ at the prime ideal (p).

Let $\mathbb{H}$ be the usual rational quaternion algebra, i.e.,

$$\mathbb{H}=\{\alpha+\beta i+\gamma j+\delta k \mid i^2=j^2=-1,\quad ij=-ji=k,\quad \alpha,\beta,\gamma,\delta\in\mathbb{Q}\}.$$

We define

$$\mathbb{H}_{(p)}=\{\alpha+\beta i+\gamma j+\delta k\in\mathbb{H}\mid \alpha,\beta,\gamma,\delta\in\mathbb{Z}_{(p)}\}.$$

We need

LEMMA 4.1. *$U(\mathbb{H}_{(p)})$ contains a free noncyclic group.*

Proof. Let us denote by $zU(\mathbb{H}_{(p)})$ the center of $U(\mathbb{H}_{(p)})$. In view of [**2**, Lemma 2.3], it is enough to show that $U(\mathbb{H}_{(p)})/zU(\mathbb{H}_{(p)})$ contains no nontrivial abelian normal subgroups. To do this we mimic the proof of [**2**, Lemma 2.5]. By Tits Alternative [**10**], $U(\mathbb{H}_{(p)})$ contains a free noncyclic group.

LEMMA 4.2. *Let $K_8=\langle a,b\mid a^4=1,\ a^2=b^2,\ b^{-1}ab=a^{-1}\rangle$ be the quaternion group of order 8. Then $U(\mathbb{Z}_{(p)}K_8)$ contains a free noncyclic group.*

Proof. We consider two cases:

(i) $p \neq 2$. Then

$$\mathbb{Z}_{(p)}K_8 \cong \mathbb{H}_{(p)} \oplus \bigoplus_{i=1}^{4} \mathbb{Z}_{(p)},$$

and the proof follows directly from Lemma 4.1.

(ii) $p = 2$. We have that

$$\mathbb{Q}K_8 \cong \mathbb{H} \oplus \bigoplus_{i=1}^{4} \mathbb{Q},$$

where for the central idempotent $e = \frac{1}{2}(1 - a^2) \in \mathbb{Q}K_8$ we have $\mathbb{Q}K_8 e \cong \mathbb{H}$. Hence $\mathbb{Z}_{(2)}K_8 \cong \mathbb{H}_{(2)}$, and applying the same reasoning as in [**2**, Lemma 2.1], we obtain that

$$[U(\mathbb{Z}_{(2)}K_8 e) : (U(\mathbb{Z}_{(2)}K_8))e] < \infty.$$

By Lemma 4.1 the result follows. □

From Lemma 4.2 and from our main theorem we immediately obtain

THEOREM 4.3. *Let R be a local ring of characteristic* 0. *Suppose that the set of torsion elements $t(G)$ of a group G forms a subgroup, and suppose that $U(RG)$ forms a* SIT-*group. Then $t(G)$ is abelian, and any subgroup of $t(G)$ is normal in G.*

ACKNOWLEDGMENTS. Both authors wish to thank the Department of Mathematics of the University of Alberta, and Professor S. K. Sehgal, for their warm hospitality and attention while this work was carried out.

REFERENCES

1. A. A. Bovdi, *The multiplicative group of an integral group ring* (Russian) (Uzhgorod, 1987).

2. J. Z. Gonçalves, Integral group rings whose group of units is solvable: an elementary proof, *Bol. Soc. Brasil. Mat.* **16**, 2 (1985), 1–9.

3. J. Z. Gonçalves and A. Mandel, Semigroup identities on units of group algebras, *Archiv. Mater. (Basel)* **57** (1991), 539–545.

4. B. Hartley and P. F. Pickel, Free subgroups in the unit groups of integral group rings, *Canad. J. Math.* **32** (1980), 1342–1352.

5. B. Huppert and N. Blackburn, *Finite groups* II (Springer-Verlag, Berlin-Heidelberg, 1982).

6. G. Karpilovsky, *Unit groups of classical rings* (Oxford University Press, 1988).

7. D. S. Passman, *The algebraic structure of group rings* (Wiley-Interscience, New York, 1977).

8. J. M. Rosenblatt, Invariant measures and growth conditions. *Trans. A.M.S.* **193** (1974), 33–52.

9. S. K. Sehgal, *Topics in group rings* (Marcel Dekker, New York, 1978).

10. S. K. Sehgal, *Units in integral group rings* (Wiley, New York, 1993).

11. J. Tits, Free subgroups in linear groups, *J. Algebra* **20** (1972), 250–270.

INSTITUTO DE MATEMÁTICA E ESTATISTICA
UNIVERSIDADE DE SÃO PAULO
CP 66281-AG CID. DE SÃO PAULO
CEP 05389-970 SÃO PAULO-BRAZIL
dokucha@ime.usp.br
jzg@ime.usp.br