Group Identities on Units and Symmetric Units of Group Rings

Algebra and Applications

Volume 12

Algebra and Applications aims to publish well written and carefully refereed monographs with up-to-date information about progress in all fields of algebra, its classical impact on commutative and noncommutative algebraic and differential geometry, K-theory and algebraic topology, as well as applications in related domains, such as number theory, homotopy and (co)homology theory, physics and discrete mathematics.

Particular emphasis will be put on state-of-the-art topics such as rings of differential operators, Lie algebras and super-algebras, group rings and algebras, C^*-algebras, Kac-Moody theory, arithmetic algebraic geometry, Hopf algebras and quantum groups, as well as their applications. In addition, Algebra and Applications will also publish monographs dedicated to computational aspects of these topics as well as algebraic and geometric methods in computer science.

Gregory T. Lee

Group Identities on Units and Symmetric Units of Group Rings

Springer

Gregory T. Lee
Department of Mathematical Sciences
Lakehead University
Thunder Bay, Ontario P7B 5E1
Canada

ISBN 978-1-84996-503-3 e-ISBN 978-1-84996-504-0
DOI 10.1007/978-1-84996-504-0
Springer London Dordrecht Heidelberg New York

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Control Number: 2010932810

AMS Codes: 16S34, 16U60, 20C07, 16W10, 16R50

Cover design: SPi Publisher Services

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

For Michelle

Preface

The unit group $\mathscr{U}(FG)$ of the group ring FG is an important object of study. It is interesting to explore the conditions under which this group satisfies various identities. Early results of this type appear in Sehgal's classic book [94]. My purpose here is to pick up where that book leaves off and present the fascinating results that have appeared, for the most part, since the mid nineties.

A group G (or a subset S of G) is said to satisfy a group identity if there is a nontrivial reduced word $w(x_1,\ldots,x_n)$ in the free group $\langle x_1,x_2,\ldots\rangle$ such that $w(g_1,\ldots,g_n)=1$ for all $g_i \in G$ (or in S, as the case may be). A series of papers by Giambruno et al. [31, 38, 40], Liu [75], Liu and Passman [76] and Passman [84] presented the conditions under which $\mathscr{U}(FG)$ satisfies a group identity.

But we can also consider the involution $*$ on FG given by

$$\left(\sum_{g\in G}\alpha_g g\right)^* = \sum_{g\in G}\alpha_g g^{-1}.$$

Denote by $\mathscr{U}^+(FG)$ the set of symmetric units; that is, $\mathscr{U}^+(FG)=\{\alpha\in\mathscr{U}(FG): \alpha^*=\alpha\}$. There have been quite a few papers since the late nineties devoted to discovering the extent to which the symmetric units determine the group structure of $\mathscr{U}(FG)$. In particular, Giambruno et al. [39] and Sehgal and Valenti [96] determined when $\mathscr{U}^+(FG)$ satisfies a group identity. Furthermore, a series of papers by Lee [67], Lee et al. [69] and Lee and Spinelli [73, 74] examined the conditions under which $\mathscr{U}^+(FG)$ satisfies specific group identities. The quaternion group Q_8 tends to provide a counterexample to every question asked, since it is easily verified that the symmetric elements of FQ_8 are central. It is, however, an engrossing problem to classify the counterexamples.

In an effort to maintain consistency, I always assume that our group ring is over a field, even though some of the results have been extended to suitable domains or other rings. Also, the involution on FG will always be the classical one described above, although I break this rule in Chapter 7 in order to mention a few recent results allowing more general involutions.

I assume that the reader has had an introductory graduate course on groups and rings, and so use standard results freely. Some prior exposure to the concept of a group ring (in particular, to the famous books of Passman [82] and Sehgal [94]) would be an asset, but it is not essential. To be sure, I am not attempting anything so ambitious as these books, where essentially, all of the major results concerning the ring structure of FG and the group structure of $\mathscr{U}(FG)$ were discussed. Given the explosion of work on group rings in recent years, such an attempt now would be all but impossible. (It would most definitely be impossible for this author!) Instead, this book is largely a continuation of the chapters *Lie Properties in KG* and *Units in Group Rings II* in [94]. I freely borrow theorems from [82] and [94], but the purloined results are all stated in full for the reader's convenience. Also, it will be clear to the reader that results labeled "Theorem" in this book are the main theorems on group identities and Lie identities of group rings. A number of major classical results are, therefore, presented as propositions.

This book contains seven chapters and an appendix. Here is a brief summary of their contents.

In Chapter 1, we discuss the conditions under which $\mathscr{U}(FG)$ satisfies a group identity. The first step is to establish Hartley's conjecture; namely, if $\mathscr{U}(FG)$ satisfies a group identity, and G is torsion, then FG satisfies a polynomial identity. After that, necessary and sufficient conditions are found, for both torsion and nontorsion groups G. When G is nontorsion, a suitable restriction must be imposed upon G modulo its torsion part for the sufficiency. A well-known conjecture due to Kaplansky states that if G is torsion-free, then the only units of FG are the trivial units, namely λg, with $0 \neq \lambda \in F$ and $g \in G$. It is certainly true if G is a u.p. (unique product) group, and we impose this as our restriction upon G modulo its torsion part.

Chapter 2 covers the same territory for the symmetric units. We find that if F is infinite and G is torsion, then FG satisfies a polynomial identity whenever $\mathscr{U}^+(FG)$ satisfies a group identity. Necessary and sufficient conditions are then presented for $\mathscr{U}^+(FG)$ to satisfy a group identity, for both torsion and nontorsion groups G.

Chapter 3 contains proofs of theorems concerning Lie identities satisfied by the set of symmetric elements, $(FG)^+$. (The corresponding results for all of FG are classical.) These results are essential to our later discussion, as there is an intimate connection between the Lie properties of FG (resp., $(FG)^+$), and corresponding group identities of $\mathscr{U}(FG)$ (resp., $\mathscr{U}^+(FG)$).

In Chapters 4, 5 and 6, we consider particular group identities. Chapter 4 contains classical results establishing when $\mathscr{U}(FG)$ is nilpotent and recent results for $\mathscr{U}^+(FG)$. Similarly, Chapters 5 and 6 contain results pertaining to the bounded Engel and solvability properties respectively, for both $\mathscr{U}(FG)$ and $\mathscr{U}^+(FG)$.

In Chapter 7, some related results are mentioned. In particular, we discuss some identities related to those mentioned earlier, and some recent results concerning involutions other than the classical one on FG.

The appendix contains some results concerning the central closure of a prime ring. These are needed in order to prove Proposition 2.2.2.

I would like to thank Ernesto Spinelli and the anonymous reviewers for their helpful suggestions. I also thank Lynn Brandon and Lauren Stoney at Springer for their help with the publication process. Portions of this book were written while I was visiting the University of Alberta and the Università del Salento, and I thank their respective mathematics departments for their warm hospitality. Also, I want to thank my wife and family for their ongoing support. Finally, I thank my teacher, Professor Sudarshan Sehgal, who introduced me to this beautiful subject years ago, and who has been a tremendous source of help to me ever since.

Thunder Bay, Ontario
February 2010 Gregory T. Lee

Contents

Chapter 1
Group Identities on Units of Group Rings

1.1 Introduction

Let G be a group and R a ring. (Unless otherwise indicated, we shall assume throughout the book that every ring has an identity.) The group ring RG is the set of all formal sums

$$\sum_{g\in G} r_g g$$

with each $r_g \in R$ and all but finitely many $r_g = 0$. It forms a ring under the operations

$$\left(\sum_{g\in G} r_g g\right) + \left(\sum_{g\in G} s_g g\right) = \sum_{g\in G} (r_g + s_g)\, g$$

and

$$\left(\sum_{g\in G} r_g g\right)\left(\sum_{g\in G} s_g g\right) = \sum_{g\in G}\left(\sum_{h\in G} r_h s_{h^{-1}g}\right) g.$$

We ignore the zero terms in an element and just write $r_1 g_1 + \cdots + r_n g_n$. In particular, we identify the elements of G with the group ring elements $1g$ and the elements of R with the group ring elements $r1$.

If N is a normal subgroup of G, then the natural homomorphism $G \to G/N$ induces a ring homomorphism $\varepsilon_N : RG \to R(G/N)$. We write $\Delta(G,N)$ for the kernel of this homomorphism. It is easily seen to be the ideal consisting of the finite sums of terms of the form $rg(n-1)$, with $r \in R$, $g \in G$, and $n \in N$. In particular, if $N = G$, then $\varepsilon = \varepsilon_G$ is called the augmentation map, and we write $\Delta(G) = \Delta(G,G)$. The ideal $\Delta(G)$ is called the augmentation ideal. This is the set of sums of terms of the form $r(g-1)$, with $r \in R$ and $g \in G$. Let us mention a well-known result.

Lemma 1.1.1. *Let G be a group and R a commutative ring of characteristic p^m, for some prime p. If N is a finite normal subgroup of G, then $\Delta(G,N)$ is a nilpotent ideal if and only if N is a p-group.*

G.T. Lee, *Group Identities on Units and Symmetric Units of Group Rings*, Algebra and Applications 12, DOI 10.1007/978-1-84996-504-0_1,

Proof. Suppose N is a finite p-group. If $\alpha_1,\dots,\alpha_l \in \Delta(G,N)$, then we can see that $\alpha_1\cdots\alpha_l$ is a sum of terms of the form

$$rg_1(n_1-1)g_2(n_2-1)\cdots g_l(n_l-1),$$

with each $g_i \in G$, $n_i \in N$ and $r \in R$. As N is normal, this can be rewritten as

$$rg(n_1'-1)(n_2'-1)\cdots(n_l'-1),$$

with $g \in G$ and each $n_i' \in N$.

That is, it suffices to show that $\Delta(N)$ is nilpotent. Our proof is by induction on the order of N. The result is trivial if $|N| = 1$. Otherwise, we know that N has an element z of order p in its centre. Then by induction, there exists a k such that $(\Delta(N/\langle z\rangle))^k = 0$. That is, $(\Delta(N))^k \subseteq \Delta(N,\langle z\rangle)$. But it is easy to see that $\Delta(N,\langle z\rangle) = (z-1)RN$, and as z is central in RN and has order p, we have $(z-1)^p \in pR\langle z\rangle$; hence $(\Delta(N))^{kpm} \subseteq (z-1)^{pm}RN = 0$, as required.

Conversely, if N is not a p-group, then let $h \in N$ be a p'-element. Then $h-1 \in \Delta(G,N)$; but if $(h-1)^n = 0$, then $(h-1)^{p^j} = 0$ for some suitably large j. However, $(h-1)^{p^j} \equiv h^{p^j} - 1 \pmod{pRN}$, and $h^{p^j} - 1 \notin pRN$, giving us a contradiction. □

We will largely be interested in the group ring FG over a field F, and in particular the unit group, $\mathscr{U}(FG)$. This is the set of all elements $u \in FG$ for which there exists $v \in FG$ such that $uv = vu = 1$. Aside from the trivial units λg, with $0 \neq \lambda \in F$ and $g \in G$, constructing units can be a difficult problem. Of course, in any ring R, if $r \in R$ satisfies $r^n = 0$, for some positive integer n, then

$$(1+r)(1-r+r^2-\cdots\pm r^{n-1}) = 1.$$

Thus, $1+r \in \mathscr{U}(R)$.

We can apply this to group rings in the following way. If H is a finite subgroup of G, let

$$\hat{H} = \sum_{h\in H} h.$$

In particular, if g is a torsion element of G, let

$$\hat{g} = \widehat{\langle g\rangle} = \sum_{i=0}^{o(g)-1} g^i.$$

Now, suppose that N is a finite normal subgroup of G, with $|N|$ divisible by char F. Then clearly $(\hat{N})^2 = |N|\hat{N} = 0$, and $\hat{N}$ is central. Thus, for any $\alpha \in FG$,

$$(1+\alpha\hat{N})(1-\alpha\hat{N}) = 1.$$

Let $\langle x_1,x_2,\dots\rangle$ be the free group on a countable infinitude of generators. If G is any group, then we say that G satisfies a group identity if there exists a nontrivial reduced word $w(x_1,\dots,x_n) \in \langle x_1,x_2,\dots\rangle$ such that $w(g_1,\dots,g_n) = 1$ for all $g_i \in G$.

To give some examples of group identities, define

$$(x_1,x_2) = x_1^{-1}x_2^{-1}x_1x_2$$

and recursively,

$$(x_1,\dots,x_{n+1}) = ((x_1,\dots,x_n),x_{n+1}).$$

Then G is abelian if it satisfies

$$(x_1,x_2) = 1$$

or nilpotent if it satisfies

$$(x_1,x_2,\dots,x_n) = 1$$

for some $n \geq 2$. We also say that it is n-Engel if it satisfies

$$(x_1,\underbrace{x_2,x_2,\dots,x_2}_{n \text{ times}}) = 1$$

and bounded Engel if it is n-Engel for some n.

The following reduction will be useful.

Lemma 1.1.2. *If a group G satisfies a group identity, then it also satisfies a group identity of the form*

$$x^{a_1}y^{b_1}x^{a_2}y^{b_2}\cdots x^{a_n}y^{b_n} = 1,$$

where each a_i and b_i is nonzero, $a_1 < 0$ and $b_n > 0$.

Proof. Suppose that G satisfies $w(x_1,\dots,x_n) = 1$. Substitute x^iyx^{-i} for each x_i, and notice that $(x^iyx^{-i})^j = x^iy^jx^{-i}$ for any integer j. Reducing, we obtain a nontrivial group identity

$$x^{c_1}y^{d_1}\cdots x^{c_k}$$

for G, with each c_i and d_i nonzero. Thus, conjugating by x^{-c^k}, we see that G also satisfies

$$x^{c_1+c_k}y^{d_1}\cdots y^{d_{k-1}}.$$

If $c_1 + c_k \neq 0$, then we are essentially done (replacing x with x^{-1} and y with y^{-1} if necessary, in order to make the first exponent negative and the last positive). Otherwise, we have the group identity

$$y^{d_1}x^{c_2}\cdots y^{d_{k-1}}.$$

Interchange x and y and repeat. Eventually we either obtain an identity of the correct form, or else we end up with the identity $x^m = 1$ for some positive integer m. But in the latter case, replacing x with $x^{-1}y$ does the job. □

The earliest results about units in group rings satisfying a group identity concerned specific identities, such as nilpotency and solvability; we will discuss these in later chapters. We begin with the most general situation. Brian Hartley made the following famous conjecture.

Conjecture 1.1.3. Let G be a torsion group and F a field. If $\mathscr{U}(FG)$ satisfies a group identity, then FG satisfies a polynomial identity.

By this we mean that if we let $F\{x_1, x_2, \ldots\}$ denote the free algebra on noncommuting indeterminates $x_1, x_2, \ldots$, then there exists a nonzero polynomial $f(x_1, \ldots, x_n)$ in $F\{x_1, x_2, \ldots\}$ such that $f(\alpha_1, \ldots, \alpha_n) = 0$ for all $\alpha_i \in FG$. For example, a commutative ring would satisfy $x_1x_2 - x_2x_1 = 0$. The conditions under which FG satisfies a polynomial identity were determined in classical results due to Isaacs and Passman. Recall that for any prime p, a group G is said to be p-abelian if its commutator subgroup G' is a finite p-group and that 0-abelian means abelian.

Proposition 1.1.4. *Let F be a field of characteristic $p \geq 0$ and G a group. Then FG satisfies a polynomial identity if and only if G has a p-abelian subgroup of finite index.*

Proof. See [82, Corollaries 5.3.8 and 5.3.10]. □

Assume first that the field is infinite.Gonçalves and Mandel [43] verified Hartley's conjecture in the special case that the group identity is actually a semigroup identity (that is, an identity of the form $x_{i_1}x_{i_2}\cdots x_{i_k} = x_{j_1}x_{j_2}\cdots x_{j_l}$). Giambruno et al. handled the characteristic 0 case as well as the characteristic $p > 0$ case where G has no p-elements in [31]. The general case was proved by Giambruno et al. in [38]. Passman then found necessary and sufficient conditions for $\mathscr{U}(FG)$ to satisfy a group identity in [84].

When F is finite, the result is different. Liu verified Hartley's conjecture for finite fields in [75], and Liu and Passman found necessary and sufficient conditions in [76].

In the next section, we present the proof of the conjecture, and the proof of the necessary and sufficient conditions is given in the following section. The remainder of the chapter is devoted to the result of Giambruno et al. [40] classifying the groups with elements of infinite order such that $\mathscr{U}(FG)$ satisfies a group identity.

1.2 Proof of Hartley's Conjecture

Throughout, we let F be a field of characteristic $p \geq 0$. Let us discuss a few facts about group identities on $\mathscr{U}(R)$, where R is an F-algebra. It will be useful, in particular, to consider the case where $R = M_n(F)$, the ring of $n \times n$ matrices over F. For instance, if G is a finite group, and p does not divide $|G|$, then by Maschke's theorem (see [62, Theorem 6.1]), FG is semisimple. It is, of course, Artinian as well, since it is finite-dimensional. Thus, we can apply the Wedderburn–Artin theorem, namely

Proposition 1.2.1. *Let R be a semisimple Artinian ring. Then*

$$R \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k),$$

where each n_i is a positive integer and each D_i is a division ring.

Proof. See [62, Theorem 3.5]. □

But we will be able to concern ourselves only with the case where the division algebra is a field, due to the following result, which is Lemma 2.0 in Gonçalves [42].

Proposition 1.2.2. *Let D be a noncommutative division algebra such that D is finite-dimensional over its centre. Then $\mathscr{U}(D)$ contains a nonabelian free group.*

As a nonabelian free group cannot possibly satisfy a group identity, we can dispense with this case.

Let us fix a group identity of the form $w(x,y) = 1$ described in Lemma 1.1.2. We begin with

Lemma 1.2.3. *There exists a nonzero polynomial $f(x)$ such that for every F-algebra R whose unit group satisfies $w(x,y) = 1$, we have $f(ab) = 0$ for every a and b in R such that $a^2 = b^2 = 0$. This polynomial has coefficients in the prime subfield of F and depends only upon w and the characteristic of F.*

Proof. Substituting $x = x_2x_1^{-1}$ and $y = x_1^{-1}x_2$ in w, we obtain a new group identity for $\mathscr{U}(R)$, of the form

$$1 = v(x_1,x_2) = x_1^{m_1}x_2^{n_1}\cdots x_1^{m_k}x_2^{n_k},$$

with each $m_i, n_i \in \{\pm 1, \pm 2\}$ and $m_1 = n_k = 1$.

Suppose that char $F \neq 2$. Define a polynomial

$$g(x_1,x_2) = (1+m_1x_1)(1+n_1x_2)\cdots(1+m_kx_1)(1+n_kx_2) - 1.$$

Notice that $g(x_1,x_2) = g_1(x_1,x_2) + g_2(x_1,x_2) + g_3(x_1,x_2)$, where g_1 is the sum of all of the monomials in g in which either x_1^2 or x_2^2 appears, g_2 is the sum of the other monomials starting with x_1 and ending with x_2, and g_3 is the sum of the remaining terms. Now, g_2 is a linear combination of terms of the form $(x_1x_2)^i$ for various i (otherwise, an x_1^2 or x_2^2 must appear), and, indeed, the unique term of highest degree in g is $m_1n_1\cdots m_kn_k(x_1x_2)^k$, a monomial in g_2. As the characteristic is not 2, this is not a zero term.

Now, $x_2g_2(x_1,x_2)x_1$ is a polynomial in x_2x_1, so let us take $f(x)$ such that $f(x_2x_1) = x_2g_2(x_1,x_2)x_1$. Notice that $g_1(a,b) = 0$, since a^2 or b^2 will appear, and both are zero. Also, $bg_3(a,b)a = 0$, since each monomial in g_3 starts with x_2 or ends with x_1, hence we will have b^2 at the beginning or a^2 at the end.

Thus, $f(ba) = bg_2(a,b)a = bg(a,b)a$, so it suffices to show that $bg(a,b)a = 0$. But notice that for any integer n, $(1+a)^n = 1+na$, and similarly for b, so in particular, $1+a$ and $1+b$ are units, and

$$\begin{aligned} 1 &= v(1+a,1+b) \\ &= (1+a)^{m_1}(1+b)^{n_1}\cdots(1+a)^{m_k}(1+b)^{n_k} \\ &= (1+m_1a)(1+n_1b)\cdots(1+m_ka)(1+n_kb) \\ &= g(a,b)+1, \end{aligned}$$

hence $g(a,b) = 0$, as required.

Suppose now that char $F = 2$. Replacing x_1 with x_1x_2 and x_2 with x_1x_3 in $v(x_1,x_2)$ and reducing, we may instead assume that our group identity is of the form

$$v(x_1,x_2,x_3) = x_{i_1}^{l_1} \cdots x_{i_r}^{l_r},$$

with $1 \leq i_j \leq 3$ for all j, $i_j \neq i_{j+1}$, and each $l_j \in \{\pm 1\}$. Also, $i_1 = 1$ and $i_r = 3$. Define a polynomial

$$g(x_1,x_2) = (1+y_1)\cdots(1+y_r) - 1,$$

where

$$y_j = \begin{cases} x_1x_2x_1, & \text{if } i_j = 1, \\ x_2x_1x_2x_1x_2, & \text{if } i_j = 2, \\ (x_1+x_2x_1)x_2(x_1+x_1x_2), & \text{if } i_j = 3. \end{cases}$$

Now write $g = g_1 + g_2 + g_3$ as in the preceding case. Calculating $y_1 \cdots y_r$, and noting that $y_1 = x_1x_2x_1$ and $y_r = (x_1+x_2x_1)x_2(x_1+x_1x_2)$, we see that g_2 has a unique term $(x_1x_2)^s$ of highest degree. In particular, g_2 is not the zero polynomial and again, $x_2g_2(x_1,x_2)x_1$ is a polynomial in x_2x_1, say $f(x)$. Furthermore, aba, $babab$ and $(a+ba)b(a+ab)$ are all square-zero. (The first two of these are obvious. For the third, notice that

$$(a+ab)(a+ba) = a^2 + 2aba + ab^2a = 0,$$

since $a^2 = b^2 = 0$ and char $F = 2$.) Thus,

$$(1+aba)^2 = (1+babab)^2 = (1+(a+ba)b(a+ab))^2 = 1.$$

Therefore,

$$v(1+aba, 1+babab, 1+(a+ba)b(a+ab)) = 1.$$

It follows that

$$0 = b(v(1+aba, 1+babab, 1+(a+ba)b(a+ab)) - 1)a = bg(a,b)a$$

and, as in the previous case, we see that this implies that

$$0 = bg_2(a,b)a = f(ba).$$

We are done. □

It will be helpful later to express the next lemma in slightly greater generality than is presently necessary; that is, in terms of domains, rather than fields.

Lemma 1.2.4. *Let D be an integral domain, and let $f(x) \in D[x]$ be a polynomial of degree $n \geq 1$. Let R be a D-algebra, and suppose that D has no zero divisors in R. If $r \in R$, and there exist distinct $\lambda_i \in D$, $1 \leq i \leq n+1$, such that $f(\lambda_i r) = 0$ for all i, then $r^n = 0$.*

Proof. Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$. Then we get

$$\begin{pmatrix} 1 & \lambda_1 & \lambda_1^2 & \cdots & \lambda_1^n \\ 1 & \lambda_2 & \lambda_2^2 & \cdots & \lambda_2^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \lambda_{n+1} & \lambda_{n+1}^2 & \cdots & \lambda_{n+1}^n \end{pmatrix} \begin{pmatrix} a_0 \\ a_1r \\ \vdots \\ a_nr^n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

But a Vandermonde matrix has nonzero determinant, so it is invertible in the field of fractions of D. In particular, as D has no zero divisors in R, we may work in $D^{-1}R$, hence $a_nr^n = 0$. Since $0 \neq a_n \in D$, $r^n = 0$. □

Lemma 1.2.5. *There exists a positive integer n, determined by $w(x,y)$ and char F, so that every F-algebra R such that $\mathscr{U}(R)$ satisfies $w(x,y) = 1$ has the following property. Namely, if $a,b \in R$, $a^2 = b^2 = 0$, but $(ab)^n \neq 0$, then $|F| \leq n$ and ab is not nilpotent.*

Proof. Consider the polynomial $f(x)$ from Lemma 1.2.3, and let n be its degree. If $\lambda \in F$, then $(\lambda a)^2 = 0$, so $f(\lambda ab) = 0$. By Lemma 1.2.4, if F has more than n elements, then $(ab)^n = 0$, a contradiction.

Also, if $(ab)^m = 0$ for some m, then notice that the minimal polynomial for ab divides f and x^m, so it must be x^k for some $k \leq n$; again, we have a contradiction. □

Now we can give some restrictions on matrix rings whose unit groups satisfy $w(x,y) = 1$. As usual, we write $GL_n(F)$ for the unit group of $M_n(F)$, and E_{ij} for the matrix having a 1 in the i,j position and zeroes elsewhere.

Lemma 1.2.6. *There exists an integer m, determined by the group identity $w(x,y) = 1$ and char F, so that if $GL_k(F)$ (with $k \geq 2$) satisfies $w(x,y) = 1$, then $k \leq m$ and $|F| \leq m$.*

Proof. Notice that $E_{12}^2 = E_{21}^2 = 0$, but $E_{12}E_{21} = E_{11}$, which is not nilpotent. Thus, by Lemma 1.2.5, $|F| \leq n$, where n is as in the statement of that lemma.

Choose an extension field F' of F of smallest possible degree so that $|F'| > n$. Then regarding F' as an F-module, we note that F' acts on itself via multiplication, and so may be regarded as a unital subring of $\mathrm{End}_F F'$. But, of course, choosing a basis for F' over F, we then identify $\mathrm{End}_F F'$ with $M_r(F)$, where $|F|^r = |F'|$. That is, $M_2(F')$ is a unital subring of $M_{2r}(F)$. We already know that $GL_2(F')$ cannot satisfy $w(x,y) = 1$, hence $GL_{2r}(F)$ cannot. Letting m be the larger of n and $2r$, we have our result, subject to putting a bound on r, independent of the choice of F. But finite fields have extensions of every degree, so any $r \geq \log_p(n+1) \geq \log_{|F|}(n+1)$ will work, where $\mathrm{char}\, F = p$. □

The polynomial identity situation for matrix rings is well understood. For any positive integer r, the standard polynomial identity of degree r is

$$s_r(x_1,\ldots,x_r) = \sum_{\sigma \in S_r} a_\sigma x_{\sigma(1)}x_{\sigma(2)}\cdots x_{\sigma(r)},$$

where the sum ranges over the symmetric group S_r, and a_σ is 1 if σ is even and -1 if σ is odd. The following is a classical result due to Amitsur and Levitzki.

Proposition 1.2.7. *For any positive integer k, $M_k(F)$ satisfies $s_{2k}(x_1,\dots,x_{2k}) = 0$.*

Proof. See [82, Theorem 5.1.9]. □

We can now complete the proof for locally finite p'-groups. (By a p'-group we mean a group with no elements of order p.) If $\alpha \in FG$, then the support of α, $\mathrm{supp}(\alpha)$, is the set of all $g \in G$ with nonzero coefficients in α.

Proposition 1.2.8. *Let F be a field of characteristic $p \geq 0$ and G a locally finite group. If $p > 0$, suppose that G has no p-elements. If $\mathscr{U}(FG)$ satisfies a group identity, then FG satisfies a polynomial identity.*

Proof. Let us say that $\mathscr{U}(FG)$ satisfies $w(x,y) = 1$, and let m be the integer from Lemma 1.2.6. Choose any $\alpha_i \in FG$, $1 \leq i \leq 2m$, and let H be the (necessarily finite) subgroup of G generated by the supports of the α_i. Then $FH = \bigoplus_i M_{n_i}(D_i)$, where each D_i is an F-division algebra. Since $\mathscr{U}(FH)$ satisfies $w(x,y) = 1$, so does $GL_{n_i}(D_i)$. By Proposition 1.2.2, each D_i is therefore a field, and by Lemma 1.2.6, $n_i \leq m$. Thus, by Proposition 1.2.7, $M_{n_i}(D_i)$ satisfies $s_{2m}(x_1,\dots,x_{2m}) = 0$, and therefore so does FH. That is,

$$s_{2m}(\alpha_1,\dots,\alpha_{2m}) = 0.$$

But the α_i were arbitrary elements of FG, and we are done. □

Let us extend the result to semiprime group rings. Recall that a ring is said to be semiprime if it has no nonzero nilpotent ideals. The semiprime group rings were classified in a classical result due to Passman. Note that for any group G, we write $\phi(G)$ for the FC-centre; that is, the subgroup of G consisting of elements with only finitely many conjugates. We say that G is an FC-group if $G = \phi(G)$. For any prime p, we write $\phi_p(G)$ for the subgroup generated by the p-elements in $\phi(G)$.

Proposition 1.2.9. *Let G be any group. If F is a field of characteristic zero, then FG is semiprime. If $\mathrm{char}\, F = p \geq 2$, then the following are equivalent:*

(i) FG is semiprime,
(ii) G does not have a finite normal subgroup with order divisible by p, and
(iii) $\phi_p(G) = 1$.

Proof. See [82, Theorems 4.2.12 and 4.2.13]. □

We need a couple of lemmas to begin the semiprime case.

Lemma 1.2.10. *Suppose R is a ring and whenever $a,b,c \in R$ satisfy $a^2 = bc = 0$, we have $bac = 0$. Then every idempotent in R is central.*

Proof. Let e be an idempotent, and take any $r \in R$. Then let $a = er(1-e)$, $b = e$ and $c = 1-e$. Since $(1-e)e = 0$, we have $a^2 = bc = 0$, hence

$$0 = bac = e^2r(1-e)^2 = er(1-e).$$

Therefore, $er = ere$. Interchanging b and c, and using $a = (1-e)re$, we get $re = ere$, hence $re = er$, and e is central. □

Lemma 1.2.11. *Suppose R is a semiprime ring, and whenever $a^2 = bc = 0$, for $a,b,c \in R$, we have $bac = 0$. Then for any $b,c,d \in R$ with d nilpotent and $bc = 0$, we have $bdc = 0$.*

Proof. We suppose that this is true for all d such that $d^n = 0$, and prove that it is true for all d such that $d^{n+1} = 0$. Notice that

$$(1-d)(1+d+d^2+\cdots+d^n) = 1,$$

hence

$$0 = bc = (b(1-d))((1+d+d^2+\cdots+d^n)c).$$

Also, for any $r \in R$, $(crb)^2 = 0$, and therefore, by hypothesis,

$$b(1-d)(crb)(1+d+d^2+\cdots+d^n)c = 0.$$

Now, if $i \geq 2$, then $(d^i)^n = 0$, hence by induction, $bd^ic = 0$. It follows that

$$b(1-d)crb(1+d)c = 0,$$

and as $bc = 0$, we can reduce this to $bdcrbdc = 0$. Thus, for any $r_1, r_2 \in R$, $r_1bdcrbdcr_2 = 0$, and it follows that if I is the ideal generated by bdc, then $I^2 = 0$. Thus, since R is semiprime, $I = 0$, and therefore $bdc = 0$. □

Let us see what happens when FG is a semiprime group ring satisfying the above conditions. The following lemma will be needed for groups with elements of infinite order as well. If char $F = p > 0$, then we write P for the set of p-elements of G and Q for the set of p'-elements (of finite order). When $p = 0$, we let $P = 1$, and $Q = T$, the set of torsion elements.

Lemma 1.2.12. *Let G be a group, and let F be a field of characteristic $p \geq 0$ such that FG is semiprime. Let us suppose that for all $\alpha,\beta,\gamma \in FG$ with $\alpha^2 = \beta\gamma = 0$ we have $\beta\alpha\gamma = 0$. If $\mathscr{U}(FG)$ satisfies a group identity, then P and Q are (normal) subgroups of G, and Q is abelian. Furthermore, every subgroup of P is normal in T and every subgroup of Q is normal in G.*

Proof. Suppose $p > 0$, and take $g,h \in P$. Then $(g-1)^{p^t} = 0$ for some $t \geq 0$. Also, $(1-h)\hat{h} = 0$. Thus, by Lemma 1.2.11, $(1-h)(g-1)\hat{h} = 0$. But as $(1-h)\hat{h} = 0$, this means that $(1-h)g\hat{h} = 0$, so $g\hat{h} = hg\hat{h}$. Since $g \in \operatorname{supp}(g\hat{h})$, we have $g = hgh^i$ for some i. That is, $g^{-1}hg \in \langle h\rangle$, hence $\langle h\rangle$ is normal in $\langle P\rangle$, and similarly, so is $\langle g\rangle$. Thus, gh lies in $\langle g\rangle\langle h\rangle$, which is a subgroup of order dividing $o(g)o(h)$ and therefore a p-group. That is, the p-elements form a (normal) subgroup of G.

Take $g \in P$ and $h \in Q$. Then we still obtain $g = hgh^i$, hence $hg^{-1}h^{-1}g = h^{i+1}$. Now, $g \in P$, and P is a normal subgroup; hence the commutator $hg^{-1}h^{-1}g$ is in P, but h^{i+1} is a p'-element. It follows that h commutes with g. That is, $\langle g\rangle$ is normal

in P and is centralized by every p'-element, so $\langle g\rangle$ is normalized by the torsion elements.

Now, let F have any characteristic and, take any $g \in Q$. Since char F does not divide $o(g)$, we have an idempotent $\frac{1}{o(g)}\hat{g}$. By Lemma 1.2.10, this idempotent is central. That is, $\langle g\rangle$ is normal in G, so every subgroup of Q is normal in G.

In particular, Q is locally finite, so consider any finite subgroup H of Q. Then FH is semisimple, and therefore a direct sum of matrix rings over division rings. As E_{11} is a noncentral idempotent in any 2×2 or larger matrix ring, FH is a direct sum of division rings. But in view of Proposition 1.2.2, each division ring must be a field. Thus H, and therefore Q, is abelian. □

Suppose that the conditions of the above lemma apply, and G is torsion. If $1 \neq g \in P$, then $\langle g\rangle$ is a finite normal p-subgroup, contradicting Proposition 1.2.9. We have the following.

Lemma 1.2.13. *Let F be a field and G a torsion group, such that FG is semiprime. If $\mathscr{U}(FG)$ satisfies a group identity, and if $\beta\alpha\gamma = 0$ for every $\alpha,\beta,\gamma \in FG$ with $\alpha^2 = \beta\gamma = 0$, then G is abelian.*

Thus, we are left with the situation where there exist $\alpha,\beta,\gamma \in FG$ with $\alpha^2 = \beta\gamma = 0$, but $\beta\alpha\gamma \neq 0$. Some additional terminology is required.

First, suppose that $0 \neq f(x_1,\ldots,x_n)$ is a polynomial identity for an F-algebra R (or, indeed, for any left or right ideal I in R). There is a standard linearization process, as follows. First, if any x_i does not appear in every monomial in f, then we substitute 0 for x_i and obtain a new polynomial identity in fewer variables. We repeat this until every variable appears in every monomial, and call this new polynomial identity f'.

Now, suppose that one of the variables, let us say x_1, appears two or more times in some monomial of $f'(x_1,\ldots,x_n)$. Then notice that I also satisfies

$$f''(x_1,\ldots,x_{n+1}) = f'(x_1+x_{n+1},x_2,\ldots,x_n) - f'(x_1,x_2,\ldots,x_n) - f'(x_{n+1},x_2,\ldots,x_n).$$

Now, f'' is a polynomial of degree no greater than that of f', and in which every x_i appears in every monomial. Iterating this procedure, we eventually obtain a polynomial identity for I in which every variable appears exactly once in each monomial. We call such a polynomial multilinear. Thus, we have

Lemma 1.2.14. *Let F be a field and R an F-algebra. Let I be a right ideal in R. If I satisfies a polynomial identity of degree r, then I satisfies a multilinear polynomial identity of degree at most r.*

Let us discuss the notion of a generalized polynomial identity, or GPI. A GPI $f(x_1,\ldots,x_n)$ for an F-algebra R is a sum of terms of the form

$$r_0 x_{i_1} r_1 x_{i_2} \cdots r_k x_{i_{k+1}} r_{k+1},$$

where $r_i \in R$ and k is an integer, such that $f(a_1,\ldots,a_n) = 0$ for all $a_i \in R$. That is, elements of the ring are permitted to appear in the GPI, not just coefficients from