Chapter 2
Group Identities on Symmetric Units

2.1 Introduction

We now turn our attention from the unit group of the group ring to the set of symmetric units. Some definitions are in order. Let R be a ring. Then an involution is a function $*: R \to R$ satisfying $(r+s)^* = r^* + s^*$, $(rs)^* = s^* r^*$ and $(r^*)^* = r$ for all $r, s \in R$. Classic examples of involutions include conjugation on the complex numbers and the transpose function $(r_{ij}) \mapsto (r_{ji})$ on the ring of $n \times n$ matrices over any field.

The elements of R fixed by an involution are said to be symmetric with respect to that involution, and we write R^+ for the set of symmetric elements. From time to time, we will also consider the set of skew elements, $R^- = \{r \in R : r^* = -r\}$. If R is an F-algebra with char $F \neq 2$, and $*$ fixes F elementwise, then R is easily seen to be a direct sum (as vector spaces) of R^+ and R^-, since $r = (\frac{r+r^*}{2}) + (\frac{r-r^*}{2})$, for all $r \in R$. We write $\mathscr{U}^+(R)$ for the set of symmetric units. It seems natural to explore the extent to which the symmetric units determine the structure of the unit group.

If F is a field and G a group, then FG has a natural involution given by

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

This is the involution upon which we focus in this book. In Chapter 7, we will briefly examine other involutions, but until then, *whenever we mention $*$ on FG, we will assume that it is this involution.* It is easy to see that if char $F \neq 2$, then the symmetric elements are the F-linear combinations of $g + g^{-1}$, $g \in G$. When F has characteristic 2, we must consider the elements of order 1 or 2 as well, since we cannot take $\frac{g+g^{-1}}{2}$. Nearly all of the results for the symmetric units assume that char $F \neq 2$.

An obvious first question is this: If $\mathscr{U}^+(FG)$ satisfies a group identity, does it follow that $\mathscr{U}(FG)$ satisfies a group identity? The answer, in general, is no. Recall, for instance, that if char $F = 0$ and G is torsion, then $\mathscr{U}(FG)$ satisfies a 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_2,
© Springer-Verlag London Limited 2010

identity if and only if G is abelian (see Corollary 1.2.21). However, we have the following simple observation. Recall that a Hamiltonian 2-group has the form $Q_8 \times E$, where Q_8 is the quaternion group and E is an elementary abelian 2-group.

Lemma 2.1.1. *Let F be any field and G a Hamiltonian 2-group. Then $(FG)^+$ is the centre of FG.*

Proof. Take $\alpha = \sum_{g\in G} \alpha_g g \in FG$. Then α is central if and only if

$$\alpha = \sum_{g\in G} \alpha_g h^{-1}gh$$

for all $h \in G$; that is, if and only if $\alpha_g = \alpha_{g^h}$ for all $g,h \in G$. But it is easy to see that every element of order 1 or 2 in G is central, and if $a \in G$ does not have order 1 or 2, then the conjugates of a are a and a^{-1}. Thus, the central elements are precisely the linear combinations of the elements of order 1 or 2, and the terms $a+a^{-1}$ for all other group elements. But these are the symmetric elements of FG. □

Thus, in this case, the symmetric units commute, and therefore they satisfy a group identity. We will see that many of the results concerning the symmetric elements break down into two cases: groups containing the quaternions and groups not containing them.

Of course, if the symmetric units do not commute, then they do not form a group, since $(\alpha\beta)^* = \beta^*\alpha^* = \beta\alpha$, for all $\alpha, \beta \in (FG)^+$. (See Bovdi et al. [18] and Bovdi [17] for a discussion of the groups G such that $\mathscr{U}^+(FG)$ is a group.) But, we can still ask if $\mathscr{U}^+(FG)$ satisfies a group identity.

In this chapter, we will present the results of Giambruno et al. [39] (for torsion groups) and Sehgal and Valenti [96] (for groups with elements of infinite order). Their results provide a complete classification of the groups G such that $\mathscr{U}^+(FG)$ satisfies a group identity, whenever F is an infinite field of characteristic different from 2 (subject to the same condition on G modulo its torsion elements that was needed in the previous chapter). The problem is currently open for finite fields and fields of characteristic 2.

An interesting question along the way is this: Is there an analogue for Hartley's conjecture? We will need the notion of a $*$-polynomial identity. We can define an involution on the free algebra $F\{x_1,x_2,\ldots\}$ by letting $x_1^* = x_2$, $x_3^* = x_4$, and so forth. Renumbering, we obtain the free algebra with involution $F\{x_1,x_1^*,x_2,x_2^*,\ldots\}$. Let R be an F-algebra with involution; that is, we insist that $(\lambda r)^* = \lambda r^*$ for all $\lambda \in F$, $r \in R$. We say that R satisfies a $*$-polynomial identity if there is a nonzero polynomial $f(x_1,x_1^*,\ldots,x_n,x_n^*) \in F\{x_1,x_1^*,\ldots\}$ such that $f(r_1,r_1^*,\ldots,r_n,r_n^*) = 0$ for all $r_1,\ldots,r_n \in R$. As part of the Giambruno et al. result, we will see that if G is torsion and $\mathscr{U}^+(FG)$ satisfies a group identity, then $(FG)^+$ satisfies a polynomial identity. In particular, then, FG must satisfy a $*$-polynomial identity. (Indeed, if $f(x_1,\ldots,x_n)$ is a polynomial identity for $(FG)^+$, then $f(x_1+x_1^*,\ldots,x_n+x_n^*)$ is a $*$-polynomial identity for FG.) But more can be said, due to this classical result of Amitsur.

Proposition 2.1.2. *Let F be a field and R an F-algebra with involution (with or without an identity). If R satisfies a $*$-polynomial identity, then R satisfies a polynomial identity.*

Proof. See [48, p. 195]. $\square$

Thus, Hartley's conjecture is true for the symmetric units as well.

We can always assume that our group identity is an identity in two variables. We do have to be a little bit careful in our argument, in that we must make sure that we are only making symmetric substitutions.

Lemma 2.1.3. *Let R be a ring with involution and suppose that $\mathscr{U}^+(R)$ satisfies a group identity. Then $\mathscr{U}^+(R)$ satisfies an identity of the form $x^{i_1}y^{j_1}x^{i_2}\cdots y^{j_{m-1}}x^{i_m}=1$, where each exponent is a nonzero integer and $i_1>0$.*

Proof. Suppose that $\mathscr{U}^+(R)$ satisfies $w(x_1,\dots,x_n)=1$. Notice that if $u,v\in\mathscr{U}^+(R)$, then also $u^ivu^i\in\mathscr{U}^+(R)$ for any positive integer i. Thus, we can substitute x^iyx^i for x_i, and we obtain a group identity of the required form, replacing x with x^{-1} if necessary in order to ensure that $i_1>0$. $\square$

It is useful to know about the involutions on matrix rings as well. Fortunately, these have been extensively studied. We have already seen that the transpose function is an involution on $M_n(F)$ for any field F. If n is even, there is another important involution, called the symplectic involution. If $A_{11},A_{12},A_{21},A_{22}\in M_{n/2}(F)$, then we let

$$\begin{pmatrix}A_{11} & A_{12}\\ A_{21} & A_{22}\end{pmatrix}^s=\begin{pmatrix}A_{22}^t & -A_{12}^t\\ -A_{21}^t & A_{11}^t\end{pmatrix},$$

where t is the usual matrix transpose. In fact, by [57, Propositions 2.19 and 2.20], all of the involutions on $M_n(F)$ can be expressed in terms of these two involutions. But up to an isomorphism respecting the involution, we can simplify that result and allow for division rings as well. The following is a classical result due to Kaplansky.

Proposition 2.1.4. *Let D be a division ring of characteristic different from 2 and n a positive integer. Let $*$ be any involution on $M_n(D)$. Then, up to an automorphism θ of $M_n(D)$ satisfying $\theta(A^*)=(\theta(A))^*$ for all $A\in M_n(D)$, we have either:*

1. *there exist an involution $^-$ of D and an invertible diagonal matrix*

$$U=\begin{pmatrix}u_{11} & 0 & \cdots & 0\\ 0 & u_{22} & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \cdots & u_{nn}\end{pmatrix}$$

such that $\bar{u}_{ii}=u_{ii}$ for all i, and if $A=(a_{ij})\in M_n(D)$, then $A^*=U^{-1}BU$, where $b_{ij}=\bar{a}_{ji}$ for all i and j; or

2. *D is a field, n is even, and $*$ is the symplectic involution.*

Proof. See [6, Theorem 4.6.8 and Lemma 4.6.11]. $\square$

Note that involutions of the sort described in the first part of the preceding proposition are said to be of transpose (or orthogonal) type.

We will begin with some results concerning semiprime rings with involution, and then move on to group rings of finite groups and the general torsion case. Following that, we will discuss semiprime group rings of nontorsion groups, and then the general case.

2.2 Semiprime Rings

Throughout this section, F is an infinite field of characteristic different from 2 and R is an F-algebra having an involution $*$ such that $*$ fixes F elementwise.

Let us begin with the following lemma.

Lemma 2.2.1. *Suppose $\mathscr{U}^+(R)$ satisfies the group identity $w(x,y) = 1$, as in Lemma 2.1.3. Then there is a positive integer n, depending only upon w, such that*

1. *if $a \in R$ is square-zero, then $(aa^*)^n = 0$; and*
2. *if $b, c \in R^+$ are square-zero, then $(cbcd)^n = 0$ for all $d \in R^+$.*

Proof. Suppose $a \in R$, $a^2 = 0$. Then for any $\lambda \in F$, we have $(1+\lambda a)(1+\lambda a^*) \in \mathscr{U}^+(R)$, as its inverse is easily seen to be $(1-\lambda a^*)(1-\lambda a)$. In the same way, $(1+\lambda a^*)(1+\lambda a) \in \mathscr{U}^+(R)$. Thus,

$$w((1+\lambda a)(1+\lambda a^*), (1+\lambda a^*)(1+\lambda a)) = 1.$$

Expanding this, we obtain $\sum_{i=1}^m p_i(a,a^*)\lambda^i = 0$, where each p_i is a polynomial in a and a^*. We now apply a Vandermonde argument similar to Lemma 1.2.4. Indeed, since F is infinite, let $\lambda_1, \ldots, \lambda_{m+1}$ be distinct elements of F. We have

$$\begin{pmatrix} 1 & \lambda_1 & \lambda_1^2 & \cdots & \lambda_1^m \\ 1 & \lambda_2 & \lambda_2^2 & \cdots & \lambda_2^m \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \lambda_{m+1} & \lambda_{m+1}^2 & \cdots & \lambda_{m+1}^m \end{pmatrix} \begin{pmatrix} 0 \\ p_1(a,a^*) \\ \vdots \\ p_m(a,a^*) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

As a Vandermonde matrix is invertible, we get that $p_i(a,a^*) = 0$ for all i. However, we note that in

$$w((1+\lambda a)(1+\lambda a^*), (1+\lambda a^*)(1+\lambda a)),$$

we have at most two consecutive instances of $1+\lambda a$ or $1+\lambda a^*$ (and at most two consecutive instances of their inverses, $1-\lambda a$ and $1-\lambda a^*$). Since $(1+\lambda a)^2 = 1+2\lambda a$, and similarly for the other terms, we know that the leading coefficient is $p_m(a,a^*) = \pm 2^k (aa^*)^l a^j$, where $k \geq 0$, $l \geq 1$, and $j \in \{0,1\}$. Thus, $(aa^*)^{l+1} = 0$, and the first part is established.

For the second part, we note that for any $\lambda \in F$,

$$(1+\lambda c)(1+\lambda b)(1+\lambda c), (1+\lambda b)(1+\lambda c)(1+\lambda b) \in \mathscr{U}^+(R).$$

Substituting these symmetric units into w, we repeat the argument above and learn that $(cb)^r = 0$ for some positive integer r. But notice that cdc is symmetric and square-zero. Thus, replacing c with cdc, we get $(cdcb)^r = 0$, hence $(cbcd)^{r+1} = 0$. Taking n to be the larger of $l+1$ and $r+1$, we are done. □

The next result is Theorem 1 in [39]. The proof is very nice, but it requires some machinery that is not needed elsewhere in the book. For convenience, the proof can be found in the appendix.

Proposition 2.2.2. *Let R be semiprime. Fix a central element $z \in R$ and a positive integer k. If $a \in R$ satisfies $(ab(z-a)b^*)^k = 0$ for all $b \in R$, then a is central in R.*

As an easy consequence, we have

Lemma 2.2.3. *If R is semiprime and $a \in R^+$ satisfies $(ab)^k = 0$ for all $b \in R^+$, then a is central.*

Proof. Let $b = cac^*$ for any $c \in R$. Then b is symmetric, hence $(acac^*)^k = 0$. We now apply Proposition 2.2.2, using $z = 0$. □

We can now deduce

Lemma 2.2.4. *If R is semiprime and $\mathscr{U}^+(R)$ satisfies a group identity, then every symmetric idempotent of R is central.*

Proof. Let e be a symmetric idempotent. Take any $r \in R$. Then $(er(1-e))^2 = 0$; hence, by Lemma 2.2.1, there exists a positive integer n such that

$$0 = ((er(1-e))(er(1-e))^*)^n = (er(1-e)r^*e)^n.$$

It follows that $(er(1-e)r^*)^{n+1} = 0$. Thus, applying Proposition 2.2.2 with $z = 1$, we see that e is central. □

This gives us a nice consequence for semiprime group rings.

Lemma 2.2.5. *Let F be an infinite field of characteristic different from 2 and G a group, such that FG is semiprime and $\mathscr{U}^+(FG)$ satisfies a group identity. If g is an element of finite order in G, and char F does not divide $o(g)$, then $\langle g \rangle$ is a normal subgroup.*

Proof. Observe that $\frac{1}{o(g)}\hat{g}$ is a symmetric idempotent. Thus, by the previous lemma, it is central. Therefore, $\langle g \rangle$ is normal. □

In particular, it follows that if char $F = 0$ and G is torsion, or if char $F = p > 2$ and G is a torsion p'-group, then G is abelian or Hamiltonian. We will refine this observation later on.

We record two other results for later use. The first is similar to Lemma 1.5.7.

Lemma 2.2.6. *Suppose that $\mathscr{U}^+(R)$ satisfies a group identity. Let S be a nil F-subalgebra of R (without identity) such that S is invariant under $*$. Then S satisfies a polynomial identity.*

Proof. Assume that the group identity is of the form $w(x,y) = 1$, as in Lemma 2.1.3. We can consider the power series ring $F\{x_1,x_2\}[[z]]$, and by Lemma 1.2.25, the elements $1+x_1z$ and $1+x_2z$ generate a free subgroup of the unit group. Thus,

$$0 \neq w(1+x_1z, 1+x_2z) - 1 = \sum_{i\geq 0} f_i(x_1,x_2)z^i,$$

and some f_m is not the zero polynomial. Choosing $s_1, s_2 \in S^+$, we know that $1+\lambda s_i \in \mathscr{U}^+(R)$ for each i and all $\lambda \in F$. Thus,

$$0 = w(1+\lambda s_1, 1+\lambda s_2) - 1 = \sum_{i\geq 0} f_i(s_1,s_2)\lambda^i.$$

But, for any particular s_1 we have $(1+s_1)^{-1} = 1 - s_1 + s_1^2 - \cdots \pm s_1^k$ for some k, and similarly for s_2. That is, there exists a $j \geq m$ such that $f_i(s_1,s_2) = 0$ for all $i > j$. Thus,

$$\sum_{i=0}^{j} f_i(s_1,s_2)\lambda^i = 0.$$

Since F is infinite, choose distinct elements $\lambda_1, \ldots, \lambda_{j+1} \in F$. Then

$$\begin{pmatrix} 1 & \lambda_1 & \lambda_1^2 & \cdots & \lambda_1^j \\ 1 & \lambda_2 & \lambda_2^2 & \cdots & \lambda_2^j \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \lambda_{j+1} & \lambda_{j+1}^2 & \cdots & \lambda_{j+1}^j \end{pmatrix} \begin{pmatrix} f_0(s_1,s_2) \\ f_1(s_1,s_2) \\ \vdots \\ f_j(s_1,s_2) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Since a Vandermonde matrix is invertible, each $f_i(s_1,s_2) = 0$. In particular, S^+ satisfies $f_m(x_1,x_2)$. That is, S satisfies the $*$-polynomial identity $g_m(x_1,x_1^*,x_2,x_2^*) = f_m(x_1+x_1^*, x_2+x_2^*)$. But then Proposition 2.1.2 tells us that S satisfies a polynomial identity. □

Lemma 2.2.7. *Let R be semiprime and suppose that $\mathscr{U}^+(R)$ satisfies a group identity. Take any square-zero symmetric element a of R. Then:*

1. *if b is a symmetric nilpotent element of R, then $aba = 0$; and*
2. *if $c,d \in R$ satisfy $cd = 0$, then $cad = 0$.*

Proof. For the first part, let us suppose, to begin with, that $b^2 = 0$. Then by Lemma 2.2.1, $(abar)^n = 0$ for all $r \in R^+$. Thus, by Lemma 2.2.3, aba is central. But aba is also square-zero, and a semiprime ring cannot have a nonzero central nilpotent element, lest it generate a nonzero nilpotent ideal. Thus, $aba = 0$.

Let us consider the general case. If $aba \neq 0$, then let i be the largest positive integer such that $ab^ia \neq 0$. (If $b^j = 0$, then evidently $i < j$.) Take any $r \in R^+$. Then

$(b^i arab^i)^2 = b^i ar(ab^{2i}a)rab^i = 0$, and $b^i arab^i$ is symmetric. Thus, as we have just observed, $ab^i arab^i a = 0$. Hence, $(ab^i ar)^2 = 0$ for all $r \in R^+$, and by Lemma 2.2.3, $ab^i a$ is central. Once again, we cannot have nonzero central nilpotent elements, so $ab^i a = 0$, giving us a contradiction.

For the second part, suppose that s is a square-zero element of R. By Lemma 2.2.1, $(ss^*)^n = (s^*s)^n = 0$. But this implies that $(s+s^*)^{2n} = 0$. Indeed, when we expand $(s+s^*)^{2n}$, we get a number of terms in which s^2 or $(s^*)^2$ appear, and these vanish, along with $(ss^*)^n + (s^*s)^n = 0$. Thus, by the first part of the lemma, we have $a(s+s^*)a = 0$ or, equivalently, $asa = -as^*a$. Now, $(sas)^2 = 0$, so replacing s with sas, we obtain $a(sas + (sas)^*)a = 0$. Thus,

$$asasa = -as^*(as^*a) = (as^*a)sa = -asasa,$$

and, therefore, $asasa = 0$. Now, for any $r \in R$, we see that drc is square-zero, hence $adrcadrca = 0$ and $(cadr)^3 = 0$ for all $r \in R$. By Proposition 1.4.7, this cannot happen unless $cad = 0$. We are done. □

The semiprime case for group rings of torsion groups will be resolved quickly once we have dealt with the finite group case.

2.3 Group Rings of Finite Groups

Let us suppose that G is a finite group. We once again assume that F is an infinite field. We begin with a useful general lemma.

Lemma 2.3.1. *Let R be a ring with involution, with $\frac{1}{2} \in R$, and let I be a $*$-invariant nil ideal of R. Then $\mathscr{U}^+(R/I)$ is the image of $\mathscr{U}^+(R)$ under the natural map $R \to R/I$.*

Proof. It is evident that symmetric units map to symmetric units. Take any symmetric unit $\bar{u} \in \bar{R} = R/I$. Let $\bar{v} = (\bar{u})^{-1}$. Then $uv - 1 \in I$, say $uv = 1 + r$, with $r \in I$. But r is nilpotent, so let us say that $r^k = 0$. Then we have $uv(1 - r + r^2 - \cdots \pm r^{k-1}) = 1$, hence u has a right inverse and, by the same argument, a left inverse in R. That is, $u \in \mathscr{U}(R)$. Now, $\bar{u} = \bar{u}^*$, hence $u^* = u + s$ for some $s \in I$. Thus, $u + u^* = 2u(1+t)$ for some $t \in I$. As t is nilpotent, $2u(1+t)$ is a unit, and it is clearly symmetric. Also, $\overline{\frac{1}{2}(u+u^*)} = \bar{u}$. Thus, $\bar{u}$ is the image of a symmetric unit in R. We are done. □

First of all, suppose that char $F = p > 2$. We must show that if $\mathscr{U}^+(FG)$ satisfies a group identity, then the p-elements of G form a group. Let us begin with

Lemma 2.3.2. *Let F be an infinite field of characteristic $p > 2$ and G a finite group. If $\mathscr{U}^+(FG)$ satisfies a group identity, then for every p-element g of G, $(g-1)^2 \in J(FG)$.*

Proof. Observe that $J(FG)$ is invariant under $*$. Indeed, one of the definitions of $J(FG)$ is that it consists of all $\alpha \in FG$ such that $1 - \beta\alpha\gamma \in \mathscr{U}(FG)$ for all $\beta, \gamma \in$

FG (see [62, Lemma 4.3]). Thus, if $\alpha \in J(FG)$, then $1-\beta\alpha^*\gamma = (1-\gamma^*\alpha\beta^*)^* \in \mathscr{U}(FG)$ for all $\beta, \gamma \in FG$; hence $\alpha^* \in J(FG)$. Let $R = FG/J(FG)$. Then R has an induced involution. Furthermore, by Proposition 1.3.3, $J(FG)$ is nilpotent. Thus, by the preceding lemma, $\mathscr{U}^+(R)$ is a homomorphic image of $\mathscr{U}^+(FG)$ and therefore satisfies a group identity. We claim that if $r \in R$ is nilpotent, then $rr^* = 0$. This will complete the proof, since if $g \in G$ is a p-element, then $g-1$ is nilpotent, hence

$$(g-1)(g^{-1}-1) = (g-1)(g-1)^* \in J(FG),$$

and therefore $(g-1)^2 = -g(g-1)(g^{-1}-1) \in J(FG)$.

We know that R is semisimple, so let us write

$$R = Re_1 \oplus \cdots \oplus Re_m,$$

where each e_i is a primitive central idempotent, and $Re_i \cong M_{n_i}(D_i)$, with n_i a positive integer and D_i a division algebra.

Suppose, first of all, that e_i is symmetric. Then the projection $R \to Re_i$ induces an involution on $M_{n_i}(D_i)$. Furthermore, every symmetric unit $ae_i \in Re_i$ is the image of a symmetric unit $ae_i + (1-e_i)$ in R. (If $(ae_i)(be_i) = e_i$, then also $(ae_i + (1-e_i))(be_i + (1-e_i)) = 1$.) Thus, the symmetric units of $M_{n_i}(D_i)$ satisfy a group identity. Considering Proposition 2.1.4, we may assume that this involution is either of transpose type or symplectic. Suppose that it is of transpose type. Then the matrix unit E_{11} is easily seen to be a symmetric idempotent. By Lemma 2.2.4, E_{11} is central. Thus, $n_i = 1$ and Re_i is a division algebra. On the other hand, if the involution is symplectic, then D_i is a field and $E_{11} + E_{n_i/2+1, n_i/2+1}$ is a symmetric idempotent and, therefore, central. Clearly, $n_i = 2$ and by definition of the symplectic involution on 2×2 matrices, the symmetric elements are simply scalar multiples of the identity matrix.

Suppose, on the other hand, that e_i is not symmetric. Then e_i^* is also a primitive central idempotent, say $e_i^* = e_j$. Notice that if $ae_i \in \mathscr{U}(Re_i)$, then ae_i is the image of $ae_i + a^*e_j + (1-(e_i+e_j))$, and this is a symmetric unit. Thus, $GL_{n_i}(D_i)$ satisfies a group identity. By Proposition 1.2.2, D_i is a field, and by Lemma 1.2.6, $n_i = 1$. Thus, Re_i is a field.

In summary, each Re_i is a division algebra or a 2×2 matrix ring over a field, and in the latter case, it has an induced involution under which all of the symmetric elements are central. Now, suppose that $r \in R$ is nilpotent. Then so is each re_i. If Re_i is a division algebra, then $re_i = 0$. Otherwise, re_i is a nilpotent 2×2 matrix. Since the minimal polynomial of this matrix has degree at most 2, $(re_i)^2 = 0$. Thus, $r^2 = 0$. By Lemma 2.2.1, $(rr^*)^n = 0$, and by the same argument, if Re_i is a division algebra, then $rr^*e_i = 0$. If Re_i is a 2×2 matrix ring, then rr^*e_i is symmetric, hence central. But a central nilpotent matrix must be the zero matrix. Thus, $rr^* = 0$. □

In order to show that the p-elements form a subgroup, we need to borrow a result about group representations. For our purposes, when we speak of a representation over a field F, we will mean a homomorphism $\rho : G \to GL_n(F)$, where G is a finite group, n (the degree) is a positive integer and F is an algebraically closed field.

Recall that ρ is said to be faithful if $\ker(\rho) = 1$. As usual, we write $SL_n(F)$ for the group of $n \times n$ matrices of determinant one over a field F, and $PSL_n(F)$ for the group obtained by factoring out the centre of $SL_n(F)$.

Proposition 2.3.3. *Let F be the algebraic closure of $\mathbb{Z}_p$, the field of p elements, where p is any prime. Let G be a finite group generated by two p-elements g and h. Suppose that G has a faithful irreducible representation ρ over F such that the minimal polynomials of $\rho(g)$ and $\rho(h)$ are quadratic. Then G has a subgroup isomorphic to $SL_2(\mathbb{Z}_p)$.*

Proof. See [45, Theorem 3.8.1]. □

Now we have

Lemma 2.3.4. *Let F be an infinite field of characteristic $p > 2$ and let G be a finite group. If, for every p-element g of G, we have $(g-1)^2 \in J(FG)$, then the p-elements of G form a (normal) subgroup.*

Proof. First of all, we can assume that F is the field mentioned in Proposition 2.3.3. Indeed, by Proposition 1.3.3, we can shrink the field to $\mathbb{Z}_p$ and then expand it to its algebraic closure. Thus, we will assume that this is indeed our field.

Next, we note that our hypothesis upon G is inherited by its subgroups and homomorphic images. Indeed, if $H \leq G$, then for any p-element g of H, we have $(g-1)^2 \in J(FG) \cap FH \subseteq J(FH)$, by Proposition 1.3.3. If H is normal, then for any p-element $\bar{g}$ of $\bar{G} = G/H$, let us choose an integer k, relatively prime to p, such that g^k is a p-element. Then $(g^k-1)^2 \in J(FG)$. By Proposition 1.3.3, $J(FG)$ is nilpotent, hence the image of $J(FG)$ under $\varepsilon_H : FG \to F\bar{G}$ is a nilpotent ideal of $F\bar{G}$. But the Jacobson radical of a ring contains every nil ideal. Thus, $(\bar{g}^k-1)^2 \in \varepsilon_H(J(FG)) \subseteq J(F\bar{G})$. Of course, g^{k^l} is a p-element for each positive integer l. As $\bar{g}$ is a p-element, we can choose l in such a way that $\bar{g}^{k^l} = \bar{g}$. Thus, replacing k with k^l, we get $(\bar{g}-1)^2 \in J(F\bar{G})$.

Let G be a group of smallest order satisfying the hypothesis of the lemma but not its conclusion. It must have two p-elements whose product is not a p-element and, by minimality, G must be generated by those two elements. Furthermore, we claim that G has an irreducible representation ρ of degree greater than 1. If not, then $FG/J(FG)$ is a direct sum of copies of F, and therefore commutative. It follows that for every $g \in G'$, $g-1 \in J(FG)$. Now $J(FG)$ is nilpotent, hence g is a p-element. That is, G is commutative modulo a p-group and therefore, the p-elements of G form a subgroup.

Next, we claim that ρ is faithful. Suppose $1 \neq K = \ker(\rho)$. Surely $K \neq G$, so by minimality, the p-elements of K form a subgroup N, necessarily normal in G. If $N \neq 1$, then again by minimality of $|G|$, the p-elements of G/N form a subgroup as well. Thus, the p-elements of G form a subgroup, contradicting the choice of G. Therefore, K is a p'-group. We know that the p-elements of G/K form a normal subgroup L/K. But ρ induces a faithful irreducible representation on G/K. Since $\Delta(G/K, L/K)$ is nilpotent, by Lemma 1.1.1, it follows that

$\Delta(G/K, L/K) \subseteq J(F(G/K))$. That is, every element of L/K is in the kernel of every irreducible representation of G/K. Since this representation is faithful on G/K, $L = K$ and G has no p-elements, a contradiction. Thus, ρ is faithful on G.

Finally, if g is any p-element in G, then $(g-1)^2 \in J(FG)$, hence the minimal polynomial of $\rho(g)$ is either linear or quadratic. If it is linear, then $\rho(g)$ is a scalar multiple of the identity matrix. But g is a p-element, so this cannot happen in a field of characteristic p unless $g \in \ker(\rho)$, which is not allowed. Thus, the conditions of Proposition 2.3.3 are met, and G contains a subgroup isomorphic to $SL_2(\mathbb{Z}_p)$.

We know, therefore, that $SL_2(\mathbb{Z}_p)$ satisfies the hypothesis of the lemma, but by inspection, its p-elements do not form a subgroup. Thus, by minimality, $G = SL_2(\mathbb{Z}_p)$. Factoring out its centre, we obtain $PSL_2(\mathbb{Z}_p)$ and again, its p-elements do not form a subgroup. But this contradicts the minimality of $|G|$, and we are done. □

Thus, if G is finite and $\mathscr{U}^+(FG)$ satisfies a group identity, then the p-elements of G form a normal subgroup P. In fact, we can simply consider G/P due to the following two results (which do not depend upon F being infinite).

Lemma 2.3.5. *Suppose that R is an F-algebra with involution, where char $F = p \neq 2$. Let I be a nil ideal invariant under $*$. If $\mathscr{U}^+(R)$ satisfies the group identity $w(x_1,\dots,x_n) = 1$, then so does $\mathscr{U}^+(R/I)$. Conversely, if $p > 0$, I is nil of bounded exponent and $\mathscr{U}^+(R/I)$ satisfies a group identity, then $\mathscr{U}^+(R)$ satisfies a group identity.*

Proof. Suppose that $\mathscr{U}^+(R)$ satisfies a group identity $w(x_1,\dots,x_n) = 1$. Choose symmetric units $\bar{u}_1,\dots,\bar{u}_n \in \bar{R} = R/I$. By Lemma 2.3.1, we may assume that each $u_i \in \mathscr{U}^+(R)$. Thus, since $w(u_1,\dots,u_n) = 1$, we must have $w(\bar{u}_1,\dots,\bar{u}_n) = 1$.

Conversely, suppose that $p > 0$, I is nil of bounded exponent at most p^l and $\mathscr{U}^+(R/I)$ satisfies $w(x,y) = 1$. If $u, v \in \mathscr{U}^+(R)$, then $\bar{u}, \bar{v} \in \mathscr{U}^+(\bar{R})$, hence $w(\bar{u},\bar{v}) = 1$. That is, $w(u,v) - 1 \in I$, hence $0 = (w(u,v)-1)^{p^l} = w(u,v)^{p^l} - 1$. Thus, $\mathscr{U}^+(R/I)$ satisfies $(w(x,y))^{p^l} = 1$. □

We now have the following lemma, similar to Lemma 1.2.18.

Lemma 2.3.6. *Let F be a field of characteristic $p > 2$ and G a group such that $\mathscr{U}^+(FG)$ satisfies a group identity $w(x_1,\dots,x_n) = 1$. If N is a normal p-subgroup of G, and either N is finite or G is locally finite, then $\mathscr{U}^+(F(G/N))$ satisfies $w(x_1,\dots,x_n) = 1$.*

Proof. If N is finite, then by Lemma 1.1.1, $\Delta(G,N)$ is nilpotent. It is surely $*$-invariant as well. By the preceding lemma, $\mathscr{U}^+(F(G/N))$ satisfies $w(x_1,\dots,x_n) = 1$.

Now suppose that G is locally finite. Let $\bar{G} = G/N$. Take $\bar{\alpha}_1,\dots,\bar{\alpha}_n \in \mathscr{U}^+(F\bar{G})$. We may lift the $\bar{\alpha}_i$ up to elements $\alpha_i \in (FG)^+$, and similarly for their inverses, since $(F\bar{G})^+$ is the image of $(FG)^+$ under $FG \to F\bar{G}$. Let H be the subgroup of G generated by the supports of all of these elements. Since H is finitely generated, it is finite. Therefore, since $\mathscr{U}^+(FH)$ satisfies $w(x_1,\dots,x_n) = 1$, the finite case tells us that $\mathscr{U}^+(F(H/(H \cap N)))$ also satisfies $w(x_1,\dots,x_n) = 1$. Replacing G with H and N with $H \cap N$, we obtain our result. □

Thus, for finite groups G, $\mathscr{U}^+(FG)$ satisfies a group identity if and only if $\mathscr{U}^+(F(G/P))$ satisfies a group identity. Hence, we may assume that G has no elements with order divisible by char F. According to Lemma 2.2.5, every subgroup of G is normal, hence G is abelian or Hamiltonian. There is nothing to be said if G is abelian. In the Hamiltonian case, $G = Q_8 \times E \times O$, where E is an elementary abelian 2-group and O is abelian with every element having odd order. We would like to eliminate O. Then the finite case will be done, by Lemma 2.1.1. To this end, we have the following lemma.

Lemma 2.3.7. *Let F be an infinite field of characteristic $p > 2$. Let $G = Q_8 \times \langle c \rangle$. If $\mathscr{U}^+(FG)$ satisfies $w(x,y) = 1$, then there exists a positive integer m, depending only upon w, such that the order of c divides $2p^m$.*

Proof. Notice that the sets $\{\lambda^2 : \lambda \in \mathbb{Z}_p\}$ and $\{-1-\mu^2 : \mu \in \mathbb{Z}_p\}$ each contain $\frac{p+1}{2}$ elements. Thus, they overlap, and we may choose $\lambda, \mu \in F$ such that $\lambda^2 + \mu^2 = -1$. Write $Q_8 = \langle g, h : g^2 = h^2, h^4 = 1, gh = h^{-1}g \rangle$. Then it is easily verified that $\theta : F(Q_8 \times \langle c \rangle) \to M_2(F\langle c \rangle)$ given by

$$\theta(g) = \begin{pmatrix} \lambda & \mu \\ \mu & -\lambda \end{pmatrix}, \quad \theta(h) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \text{and} \quad \theta(c) = \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix}$$

is a homomorphism.

It is also easy to check that $\alpha = \frac{1}{4}(c + c^{-1}g^2)(\mu g - h + \lambda gh)(1 - g^2)$ and $\beta = \frac{1}{4}(c + c^{-1}g^2)(\mu g + h + \lambda gh)(1 - g^2)$ are symmetric and square-zero. Thus, by Lemma 2.2.1, there exists an n, depending only on w, such that $(\alpha\beta)^n = 0$ and so $(\theta(\alpha)\theta(\beta))^n = 0$. But

$$\theta(\alpha) = \begin{pmatrix} 0 & c^{-1} - c \\ 0 & 0 \end{pmatrix} \text{ and } \theta(\beta) = \begin{pmatrix} 0 & 0 \\ c^{-1} - c & 0 \end{pmatrix}.$$

Thus,

$$\begin{pmatrix} (c^{-1} - c)^{2n} & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

That is, $(c^{-1} - c)^{2n} = 0$. Choosing m so that $p^m \geq 2n$, we get $c^{-p^m} = c^{p^m}$, hence $c^{2p^m} = 1$, as required. □

Thus, if we have $G/P = Q_8 \times E \times O$, then as O cannot contain p-elements, we must have $O = 1$. As we mentioned above, this proves

Proposition 2.3.8. *Let F be an infinite field of characteristic $p > 2$ and G a finite group. Then $\mathscr{U}^+(FG)$ satisfies a group identity if and only if the p-elements of G form a (normal) subgroup P and G/P is abelian or a Hamiltonian 2-group.*

If char $F = 0$, we cannot use the technique of Lemma 2.3.7, since F may not contain λ and μ satisfying $\lambda^2 + \mu^2 = -1$. But we are still able to reduce to the Hamiltonian 2-groups. We will make use of the following famous result due to Tits (a corollary of Tits' alternative).

Proposition 2.3.9. *Suppose that $A, B \in GL_2(\mathbb{C})$, and that A has two eigenvalues with distinct magnitudes, as does B. Further suppose that the eigenspaces of A are distinct from those of B. Then there exists a positive integer n such that A^n and B^n generate a free group.*

Proof. See [95, Lemma 5.3]. □

We recall that for any field F of characteristic different from 2, the ring of (Hamiltonian) quaternions over F, $\mathbb{H}(F)$, is the F-vector space with basis $\{1, i, j, k\}$ made into an F-algebra through the rules $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$ and $ki = -ik = j$.

Lemma 2.3.10. *Let $G = Q_8 \times \langle c \rangle$, where $c \neq 1$ has odd order. Then $\mathscr{U}^+(\mathbb{Q}G)$ does not satisfy a group identity.*

Proof. We may assume that $o(c) = q$, an odd prime. It is easy to see that if ξ is a primitive qth root of unity, then the map $\mathbb{Q}\langle c \rangle \to \mathbb{Q}(\xi)$ given by $c \mapsto \xi$ is an epimorphism. As ξ has minimal polynomial $1 + x + \cdots + x^{q-1}$ over $\mathbb{Q}$, the kernel of this homomorphism is clearly $\mathbb{Q}\langle c \rangle(\frac{1}{q}\hat{c})$. Letting $e_1 = 1 - \frac{1}{q}\hat{c}$, we see that e_1 is a symmetric central idempotent, hence $\mathbb{Q}\langle c \rangle = \mathbb{Q}\langle c \rangle e_1 \oplus \mathbb{Q}\langle c \rangle (1 - e_1)$, and our epimorphism restricts to an isomorphism on $\mathbb{Q}\langle c \rangle e_1$.

Next, notice that the map $\mathbb{Q}Q_8 \to \mathbb{H}(\mathbb{Q})$ given by $g \mapsto i$, $h \mapsto j$ is also an epimorphism. Its kernel is easily seen to be $\mathbb{Q}Q_8(\frac{1+g^2}{2})$. Letting $e_2 = 1 - \frac{1+g^2}{2}$ we see that e_2 is a symmetric central idempotent and our epimorphism restricts to an isomorphism on $\mathbb{Q}Q_8 e_2$. Working in $\mathbb{Q}G \cong \mathbb{Q}Q_8 \otimes_{\mathbb{Q}} \mathbb{Q}\langle c \rangle$, we see that $e = e_1 e_2$ is a central symmetric idempotent and we have an epimorphism $\theta : \mathbb{Q}G \to \mathbb{H}(\mathbb{Q}(\xi))$ given by $g \mapsto i$, $h \mapsto j$, $c \mapsto \xi$, restricting to an isomorphism on $\mathbb{Q}Ge$.

Note that in $\mathbb{C}$, elements of the form $\lambda + \mu i$, with $\lambda, \mu \in \mathbb{Q}(\xi)$, are uniquely expressed in this form. Otherwise, we would get $i \in \mathbb{Q}(\xi)$. If this happened, then $\mathbb{Q}(\xi)$ would contain a primitive $4q$th root of unity. But the minimal polynomial of such a root of unity over $\mathbb{Q}$ has degree $\varphi(4q) = 2(q-1)$, where φ is the Euler function. However, $\varphi(q) = q - 1$, so this is impossible. Thus, we identify the elements of the form $\lambda + \mu i$ of $\mathbb{H}(\mathbb{Q}(\xi))$ with the subfield $\mathbb{Q}(\xi, i)$ of $\mathbb{C}$. (Equivalently, we could identify the elements $\lambda + \mu j$ with this subfield.)

Evidently, then, $(1 + \xi i)(1 - \xi^{-1} i)$ and $(1 + \xi j)(1 - \xi^{-1} j)$ are units in $\mathbb{H}(\mathbb{Q}(\xi))$. Furthermore,

$$(1 + \xi i)(1 - \xi^{-1} i) = \theta((1 + cg)(1 + (cg)^*)e)$$

and

$$(1 + \xi j)(1 - \xi^{-1} j) = \theta((1 + ch)(1 + (ch)^*)e).$$

As θ is an isomorphism on $\mathbb{Q}Ge$, $(1 + cg)(1 + (cg)^*)e$ and $(1 + ch)(1 + (ch)^*)e$ are units of $\mathbb{Q}Ge$; hence

$$(1 + cg)(1 + (cg)^*)e + (1 - e), (1 + ch)(1 + (ch)^*)e + (1 - e) \in \mathscr{U}^+(\mathbb{Q}G),$$

so $u = (1 + \xi i)(1 - \xi^{-1} i)$ and $v = (1 + \xi j)(1 - \xi^{-1} j)$ are images under θ of symmetric units in $\mathbb{Q}G$. It follows that $w(u, v) = 1$ if $w(x, y) = 1$ is a group identity for $\mathscr{U}^+(\mathbb{Q}G)$.

Now, $\mathbb{H}(\mathbb{Q}(\xi))$ may be regarded as a right $\mathbb{Q}(\xi,i)$-space with basis $\{1,j\}$. Consider the left regular representation on $\mathbb{H}(\mathbb{Q}(\xi))$; that is, the map sending r to ρ_r, where $\rho_r(s) = rs$ for all s. Surely $w(\rho_u,\rho_v) = 1$. But with respect to the basis $\{1,j\}$ we calculate the matrix of ρ_u to be

$$A = \begin{pmatrix} 2+(\xi-\xi^{-1})i & 0 \\ 0 & 2+(\xi^{-1}-\xi)i \end{pmatrix}$$

and the matrix of ρ_v to be

$$B = \begin{pmatrix} 2 & \xi^{-1}-\xi \\ \xi-\xi^{-1} & 2 \end{pmatrix}.$$

The eigenvalues of A are clearly distinct positive real numbers. A calculation reveals that the eigenvalues of B are the same as those of A. Furthermore, the eigenvectors of A are obvious and are not eigenvectors for B. Thus, the preceding proposition applies, and we get that powers of A and B generate a free group. This contradicts the hypothesis that they satisfy a group identity, and we are done. □

We can now conclude the torsion case for fields of characteristic zero.

Proposition 2.3.11. *Let F be a field of characteristic zero and G a torsion group. Then $\mathscr{U}^+(FG)$ satisfies a group identity if and only if G is abelian or a Hamiltonian 2-group.*

Proof. By Lemma 2.2.5, if $\mathscr{U}^+(FG)$ satisfies a group identity, then G is abelian or Hamiltonian. In the latter case, $G \simeq Q_8 \times E \times O$, where $E^2 = 1$ and every element of O has odd order. By the last lemma, $O = 1$. The converse follows immediately from Lemma 2.1.1. □

2.4 Group Rings of Torsion Groups

Having dealt with the characteristic zero case, we can now assume that F is infinite and char $F = p > 2$. The next step will be to show that if $\mathscr{U}^+(FG)$ satisfies a group identity, then FG satisfies a polynomial identity. This breaks down into three cases: $N(FG) = 0$, $N(FG)$ nonzero nilpotent, and $N(FG)$ not nilpotent. In the first of these cases, where FG is semiprime, we can do even better. We start with

Lemma 2.4.1. *Suppose F is an infinite field, char $F = p > 2$ and FG is semiprime. Further suppose that $\mathscr{U}^+(FG)$ satisfies a group identity. If $g \in G$ has order p, then $\langle g\rangle$ is normalized by every torsion element of G.*

Proof. Take $h \in G$ with $o(h) = p^m$, $m \geq 0$. Observe that $\hat{g}$ is symmetric and square-zero and $(h-1)(h^{-1}-1)$ is symmetric with $((h-1)(h^{-1}-1))^{p^m} = 0$. Thus, by Lemma 2.2.7, $\hat{g}(h-1)(h^{-1}-1)\hat{g} = 0$. Expanding this and discarding the $(\hat{g})^2$ terms, we get $\hat{g}h\hat{g} + \hat{g}h^{-1}\hat{g} = 0$. Writing this as a sum of group elements, we note that each element must appear at least three times in order to get a zero sum. Thus, a group element appears at least twice in either $\hat{g}h\hat{g}$ or $\hat{g}h^{-1}\hat{g}$. As the proofs for the two cases are essentially the same, assume that $g^{i_1}hg^{j_1} = g^{i_2}hg^{j_2}$. If $i_1 = i_2$, then $j_1 = j_2$, so we may assume that $i_1 \neq i_2$ and $j_1 \neq j_2$, with all exponents in the range of 0 to $p-1$. Then $h^{-1}g^{i_1-i_2}h = g^{j_2-j_1}$. As $i_1 - i_2$ is not divisible by p, by taking a suitable power we get that $h^{-1}gh \in \langle g \rangle$. Thus, $\langle g \rangle$ is normalized by the p-elements of G.

Suppose that $k \in G$ is a p'-element. By Lemma 2.2.5, $\langle k \rangle$ is normal in G. Thus, $\langle k, g \rangle$ is finite. We can now apply Proposition 2.3.8 to $\langle k, g \rangle$, and we get that its p-elements form a normal subgroup. Therefore, (g,k) is both a p-element and a p'-element, hence g and k commute. Thus, $\langle g \rangle$ is normalized by both the p-elements and the p'-elements and therefore by all elements of finite order. □

Proposition 2.4.2. *Suppose F is an infinite field, char $F \neq 2$, G is torsion and FG is semiprime. Then $\mathscr{U}^+(FG)$ satisfies a group identity if and only if G is abelian or a Hamiltonian 2-group.*

Proof. The characteristic zero case is handled in Proposition 2.3.11, so let char $F = p > 2$ and suppose that $\mathscr{U}^+(FG)$ satisfies a group identity. By the preceding lemma, if $g \in G$ has order p, then $\langle g \rangle$ is a normal subgroup. But by Proposition 1.2.9, this contradicts the semiprimeness of FG. Thus, G has no p-elements. By Lemma 2.2.5, G is abelian or Hamiltonian. In the latter case, $G = Q_8 \times E \times O$, where $E^2 = 1$ and O is an abelian group in which every element has odd, p'-order. By Lemma 2.3.7, $O = 1$, and the necessity is proved.

Lemma 2.1.1 proves the sufficiency. □

Let us now extend Hartley's conjecture.

Proposition 2.4.3. *Let F be an infinite field of characteristic $p \neq 2$ and G a torsion group. If $\mathscr{U}^+(FG)$ satisfies a group identity, then FG satisfies a polynomial identity. In particular, G is locally finite. Also, if $p > 2$, then the p-elements of G form a (normal) subgroup.*

Proof. Once we show that FG satisfies a polynomial identity, the fact that G is locally finite will follow from Proposition 1.1.4, and then the fact that the p-elements form a subgroup will come from Proposition 2.3.8. If $p = 0$, then Propositions 2.3.11 and 1.1.4 do the job. Thus, we assume that $p > 2$.

Suppose, first of all, that $N(FG)$ is a nilpotent ideal. By Proposition 1.2.22, $\phi_p(G)$ is finite, and by Proposition 2.3.8, its p-elements form a group. Thus, $\phi_p(G)$ is a finite p-group. By Lemma 2.3.6, $\mathscr{U}^+(F(G/\phi_p(G)))$ satisfies a group identity. But by Proposition 1.2.9, $F(G/\phi_p(G))$ is semiprime. Thus, by Proposition 2.4.2, $G/\phi_p(G)$ is abelian or a Hamiltonian 2-group. If it is abelian, then $[FG, FG] \subseteq \Delta(G, \phi_p(G))$. But $\Delta(G, \phi_p(G))$ is a nilpotent ideal by Lemma 1.1.1, hence FG satisfies $[x,y]^{p^l} = 0$ for some l. If, on the other hand, $G/\phi_p(G)$ is a Hamiltonian 2-group, then by Lemma 2.1.1, $(F(G/\phi_p(G)))^+$ is commutative. That is, $[(FG)^+, (FG)^+] \subseteq \Delta(G, \phi_p(G))$, hence FG satisfies the $*$-polynomial identity $[x + x^*, y + y^*]^{p^l} = 0$. By Proposition 2.1.2, FG satisfies a polynomial identity.

Now, suppose that $N(FG)$ is not nilpotent. It is surely nil, so by Lemma 2.2.6, $N(FG)$ satisfies a polynomial identity. By Lemma 1.2.16, FG satisfies a nondegenerate multilinear GPI. Thus, by Proposition 1.2.15, $(G:\phi(G))<\infty$ and $|(\phi(G))'|<\infty$. In particular, G is locally finite. Considering finite subgroups of G, we see from Proposition 2.3.8 that the p-elements of G form a normal subgroup P.

By Lemma 2.3.6, $\mathscr{U}^+(F(G/P))$ satisfies a group identity. But $F(G/P)$ is semiprime, hence by Proposition 2.4.2, G/P is abelian or a Hamiltonian 2-group. In the former case, G' is a p-group, hence $(\phi(G))'$ is a finite p-group. That is, G has a p-abelian subgroup of finite index, and by Proposition 1.1.4, FG satisfies a polynomial identity. If $G/P \simeq Q_8 \times E$, where E is an elementary abelian 2-group, then there exists a normal subgroup H of G, containing P, such that $G/H \simeq Q_8$ and $H/P \simeq E$. Since H/P is abelian, as we have just seen, FH satisfies a polynomial identity. That is, H has a p-abelian subgroup of finite index and, therefore, so does G. □

As usual, we write P for the subgroup of G consisting of p-elements. Let us first consider the case where G does not contain the quaternions. Let H be any finitely generated (hence finite) subgroup of G. Let N be the group of p-elements of H. By Proposition 2.3.8, H/N is abelian or a Hamiltonian 2-group. Now, $(|N|,|H/N|)=1$. Thus, by the Schur–Zassenhaus theorem, H is the semidirect product $N \rtimes K$, for some subgroup K. If H/N is a Hamiltonian 2-group, then K contains the quaternions, which is impossible. So H/N is abelian, and H', and hence G', is a p-group. We already know that FG satisfies a polynomial identity. In view of Theorem 1.3.1, if we can show that G' has bounded exponent, then we will know that $\mathscr{U}(FG)$ satisfies a group identity and we will be done. In order to do this, we need versions of Lemmas 1.3.5 and 1.3.6, assuming only that $\mathscr{U}^+(FG)$ satisfies a group identity (and that F is infinite).

Lemma 2.4.4. *Let F be an infinite field of characteristic $p>2$ and let $G=A\rtimes\langle g\rangle$, where A is an abelian p-subgroup and g has prime order $q\neq p$. If $\mathscr{U}^+(FG)$ satisfies a group identity, then G' has bounded exponent.*

Proof. Define $\theta: FA \to FA$ as in the proof of Lemma 1.3.5, and recall that for all $\beta \in FA$, $\theta(\beta)$ is central and $\hat{g}\beta\hat{g}=\theta(\beta)\hat{g}$. Take any $a\in A$. Let $\alpha=\hat{g}a^{-1}(1-g^{-1})$. Clearly $\alpha^2=0$; hence, by Lemma 2.2.1, there exists an n (independent of the choice of a) such that $(\alpha\alpha^*)^{p^n}=0$. But $\alpha^*=(1-g)a\hat{g}$. Thus,

$$\begin{aligned}\alpha\alpha^* &= \hat{g}a^{-1}(2-g-g^{-1})a\hat{g}\\ &= 2(\hat{g})^2-\hat{g}a^{-1}ga\hat{g}-\hat{g}a^{-1}g^{-1}a\hat{g}\\ &= 2q\hat{g}-\hat{g}(g,a)\hat{g}-\hat{g}(g^{-1},a)\hat{g}\\ &= (2q-\theta((g,a))-\theta((g^{-1},a)))\hat{g}.\end{aligned}$$

Now, $2q-\theta((g,a))-\theta((g^{-1},a))$ is central, so it follows that

$$(2q-\theta((g,a))-\theta((g^{-1},a)))^{p^n}q^{p^n-1}\hat{g}=0.$$

As $2q-\theta((g,a))-\theta((g^{-1},a))\in FA$, it follows that

$$(2q - \theta((g,a)) - \theta((g^{-1},a)))^{p^n} = 0.$$

Everything in FA commutes, hence

$$(2q)^{p^n} = \theta((g,a))^{p^n} + \theta((g^{-1},a))^{p^n}.$$

As $(2q)^{p^n}$ is a nonzero multiple of the identity element, one of the conjugates of (g,a) or (g^{-1},a) appearing in this last equation must have order dividing p^n. Thus, (g,a) or (g^{-1},a) has order dividing p^n, and by Lemma 1.3.4, G' has bounded exponent. □

Lemma 2.4.5. *Let F be an infinite field of characteristic $p > 2$ and let $G = A \rtimes \langle g \rangle$, where A is an abelian p-subgroup and g has order p. If $\mathscr{U}^+(FG)$ satisfies a group identity, then G' has bounded exponent.*

Proof. Notice that $\hat{g}$ is square-zero and symmetric and, for any $a \in A$, so is $a^{-1}\hat{g}a$. Hence, by Lemma 2.2.1, there exists r, independent of the choice of a, such that $(a^{-1}\hat{g}a\hat{g})^{p^r} = 0$. Now follow the proof of Lemma 1.3.6. □

We also need the following lemma.

Lemma 2.4.6. *Let F be any field and G a group. Let N be a torsion normal subgroup of G having no elements of order divisible by char F. Suppose either that N is finite or G is locally finite. If $\mathscr{U}^+(FG)$ satisfies the group identity $w(x_1,\ldots,x_n) = 1$, then so does $\mathscr{U}^+(F(G/N))$.*

Proof. In the proof of Lemma 1.3.9, we simply note that e is symmetric, and now apply the same proof to the symmetric units. □

Remark 2.4.7. Notice that if F is infinite and char $F \neq 2$, then by Proposition 2.4.3, if G is torsion and $\mathscr{U}^+(FG)$ satisfies a group identity, then we get for free that G is locally finite. If char $F = 0$, this implies that we can choose any normal subgroup N in the above lemma. If char $F = p > 2$, then we know that the p-elements of N form a normal subgroup, so we can factor out the p-elements and then the p'-elements. Thus, we can factor out any normal subgroup N here as well. This is obviously the case for group identities on $\mathscr{U}(FG)$ too (even if char $F = 2$).

The first part of the main result of Giambruno et al. [39] is

Theorem 2.4.8. *Let F be an infinite field of characteristic $p \neq 2$ and G a torsion group not containing Q_8. Then the following are equivalent:*

(i) $\mathscr{U}^+(FG)$ satisfies a group identity;
(ii) $\mathscr{U}(FG)$ satisfies a group identity;
(iii) a. $p = 0$ and G is abelian, or
b. $p > 2$, G has a p-abelian subgroup of finite index and G' is a p-group of bounded exponent.

Proof. It is clear that (ii) implies (i), and (iii) implies (ii) comes from Theorem 1.3.1 (or is trivial if $p=0$). Thus, we must show that (i) implies (iii). The characteristic zero case was dealt with in Proposition 2.3.11. Thus, let p be an odd prime, and assume that $\mathscr{U}^+(FG)$ satisfies a group identity. We have already seen that FG satisfies a polynomial identity (hence G has a p-abelian normal subgroup A of finite index, by Proposition 1.1.4) and G' is a p-group. Thus, we need only show that G' has bounded exponent.

By Lemma 2.3.6, $\mathscr{U}^+(F(G/A'))$ satisfies a group identity. It suffices to show that $(G/A')'$ has bounded exponent. Thus, we factor out A' and assume that A is abelian. Write $A = H \times K$, where H is a p-group and K is a p'-group. Then K is normal and by Lemma 2.4.6, $\mathscr{U}^+(F(G/K))$ satisfies a group identity. Also, $(G/K)' = G'K/K \simeq G'/(G' \cap K) = G'$, since G' is a p-group. Thus, we factor out K and assume that A is a p-group. In view of Lemmas 2.4.4 and 2.4.5, the proof of Lemma 1.3.10 shows us that G' has bounded exponent. We are done. □

If G contains the quaternions, then $\mathscr{U}(FG)$ cannot satisfy a group identity for any infinite field of characteristic different from 2 (see Theorem 1.3.2 and Corollary 1.2.21). However, the second main theorem from [39] is

Theorem 2.4.9. *Let F be an infinite field of characteristic $p \neq 2$ and G a torsion group containing Q_8. If $p=0$, then $\mathscr{U}^+(FG)$ satisfies a group identity if and only if G is a Hamiltonian 2-group. If $p>2$, then $\mathscr{U}^+(FG)$ satisfies a group identity if and only if G has a p-abelian normal subgroup A of finite index, the p-elements of G form a (normal) subgroup P of bounded exponent, and G/P is a Hamiltonian 2-group.*

Proof. The characteristic zero case was resolved in Proposition 2.3.11, so suppose $p>2$. Assume that $\mathscr{U}^+(FG)$ satisfies a group identity. By Proposition 2.4.3, FG satisfies a polynomial identity, and Proposition 1.1.4 shows the existence of A. Proposition 2.4.3 also says that P is a subgroup. As G is locally finite, Lemma 2.3.6 tells us that $\mathscr{U}^+(F(G/P))$ satisfies a group identity. But $F(G/P)$ is semiprime. Thus, by Proposition 2.4.2, G/P is abelian or a Hamiltonian 2-group. It surely cannot be abelian, since G contains Q_8.

Thus, it remains only to show that P has bounded exponent. By Theorem 2.4.8, P' has bounded exponent. Therefore, it suffices to show that P/P' has bounded exponent. We know that we can factor out P'. Thus, we assume that P is abelian. Suppose that $G/P = (HL)/P$ where $H/P \simeq Q_8$ and L/P is an elementary abelian 2-group. Take any $g \in H$. Then $\langle P, g\rangle$ does not contain Q_8. Thus, by Theorem 2.4.8, $\langle P, g\rangle'$ has bounded exponent. Similarly, $\langle P, L\rangle'$ has bounded exponent. Noting that in any group we have $(gh,k) = (g,k)^h(h,k)$, we see that since P is abelian, it follows that (P,G) has bounded exponent. Thus, we can safely quotient out (P,G) and assume that P is central. But then G has a subgroup isomorphic to $Q_8 \times P$. It follows from Lemma 2.3.7 that P has bounded exponent, and the necessity is complete.

Let us prove the sufficiency. But FG satisfies a polynomial identity and P is a normal p-subgroup of bounded exponent. Thus, by Lemma 1.3.14, $\Delta(G,P)$ is nil of bounded exponent at most p^k, for some k. Now, if $\alpha, \beta \in \mathscr{U}^+(FG)$, then by

Lemma 2.1.1, $(\alpha,\beta)-1 \in \Delta(G,P)$ and therefore, $(\alpha,\beta)^{p^k}=1$. Thus, $\mathscr{U}^+(FG)$ satisfies a group identity. □

Combining Theorems 2.4.8 and 1.3.1 with the proof of Theorem 2.4.9, we obtain the following fact. If F is an infinite field of characteristic $p \neq 2$ and G is a torsion group, and if $\mathscr{U}^+(FG)$ satisfies a group identity, then it satisfies $(x,y)^{p^k}=1$ for some $k \geq 0$ (or $(x,y)=1$ if $p=0$).

2.5 Semiprime Group Rings

Let us move on to the results of Sehgal and Valenti [96] determining when $\mathscr{U}^+(FG)$ satisfies a group identity if G has elements of infinite order. Once again, we let F be an infinite field of characteristic $p \neq 2$. This time, G will be an arbitrary group. We let T denote the set of torsion elements, P the set of p-elements, and Q the set of p'-elements in T. (For convenience, when $p=0$, we let $P=1$ and $Q=T$.)

We begin with the semiprime case. By Lemma 2.2.5, if $g \in Q$, then $\langle g \rangle$ is a normal subgroup. It follows that Q is a normal subgroup (and, indeed, every subgroup of Q is normal in G). Thus, by Proposition 2.4.2, Q is abelian or a Hamiltonian 2-group. Curiously, this will be the only time we have to worry about the quaternions; indeed, they will only appear when the characteristic is zero. Let us begin with

Lemma 2.5.1. *Let F be an infinite field of characteristic different from 2. Suppose that G has a finite subgroup H and an element g of infinite order such that $G=\langle H,g\rangle$. Further suppose that FG is semiprime. If $\mathscr{U}^+(FG)$ satisfies a group identity, and FH has no nilpotent elements, then every idempotent of FH is central in FG.*

Proof. By Proposition 1.3.3, $J(FH)$ is nilpotent. Thus, by our assumption on FH, $J(FH)=0$. Therefore, FH is a direct sum of matrix rings over division rings. But any 2×2 or larger matrix ring surely has nilpotent elements. Therefore, FH is a direct sum of division rings. As division rings only have 0 and 1 as idempotents, it follows that the idempotents of FH are the sums of the primitive central idempotents. Thus, it suffices to show that the primitive central idempotents of FH are central in FG.

Let e be a primitive central idempotent of FH. By Lemma 2.2.4, any symmetric idempotent is central in FG. Thus, assume $e^* \neq e$. Now, e^* is also a primitive central idempotent of FH. Since $e+e^*$ is a symmetric idempotent, it is central in FG. That is, $e^g+(e^*)^g=e+e^*$. As we observed above, H is normal in G. Thus, e^g and $(e^*)^g$ are also primitive central idempotents of FH, and we must have $e^g=e$ or e^*. In the former case, e is centralized by H and g and is therefore central in FG. That is, we may assume that $e^g=e^*$. Repeating the same procedure with g^{-1} in place of g, we get $e^{g^{-1}}=e^*$. Expanding these equations, we get $eg=ge^*$, $g^{-1}e=e^*g^{-1}$, $eg^{-1}=g^{-1}e^*$ and $ge=e^*g$. Let $\alpha=(g+g^{-1})e$ and $\beta=(g+g^{-1})e^*$. Now,

$$\alpha^*=e^*(g+g^{-1})=(g+g^{-1})e=\alpha$$

and similarly, $\beta^* = \beta$. Also,

$$\alpha^2 = (g+g^{-1})e(g+g^{-1})e = (g+g^{-1})^2 e^* e = 0,$$

as e and e^* are distinct primitive central idempotents. Similarly, $\beta^2 = 0$. By Lemma 2.2.1, $\alpha\beta$ is nilpotent. But $\alpha\beta = (g+g^{-1})^2(e^*)^2 = (g+g^{-1})^2 e^*$. It follows that for any n, $(\alpha\beta)^n = (g+g^{-1})^{2n}e^*$. If this is 0, then so is $g^{2n}(g+g^{-1})^{2n}e^*$. Expanding this last expression, we get e^* plus a linear combination of group elements outside of H. Thus, $(\alpha\beta)^n \neq 0$, and we have a contradiction. □

We intend to apply this lemma when H is a Hamiltonian 2-group. Happily, the group rings of Q_8 have been studied thoroughly. The following result is classical.

Proposition 2.5.2. *Let F be any field. Then FQ_8 has a nonzero nilpotent element if and only if there exist $\lambda, \mu \in F$ such that $\lambda^2 + \mu^2 = -1$.*

Proof. See [94, Proposition VI.1.13]. □

Lemma 2.5.3. *Let F be an infinite field of characteristic different from 2 and G a group generated by a finite Hamiltonian 2-group H and an element a of infinite order. If FG is semiprime and $\mathscr{U}^+(FG)$ satisfies a group identity, then char $F = 0$ and every idempotent of FH is central in FG.*

Proof. Suppose, first of all, that $\lambda^2 + \mu^2 = -1$ has no solution in F. By Proposition 2.5.2, FQ_8 has no nilpotent elements. Now, $H = Q_8 \times E$, where $E = C_2 \times \cdots \times C_2$. Thus, $FH = FQ_8 \otimes_F FC_2 \otimes_F FC_2 \otimes_F \cdots \otimes_F FC_2$. But if $C_2 = \langle c \rangle$, then

$$FC_2 = FC_2\left(\frac{1+c}{2}\right) \oplus FC_2\left(\frac{1-c}{2}\right) \cong F \oplus F.$$

Thus, FH is a direct sum of copies of FQ_8 and therefore has no nilpotent elements. It follows from Lemma 2.5.1 that every idempotent of FH is central in FG. Also, we know that $\lambda^2 + \mu^2 = -1$ has a solution in $\mathbb{Z}_p$ for every prime p. Thus, char $F = 0$.

It remains to dispense with the case where $\lambda^2 + \mu^2 = -1$ has a solution. We know that every subgroup of H is normal in G. Thus, conjugation by a induces an automorphism of Q_8 under which every subgroup is invariant. By inspection, we can see that any such automorphism must be conjugation by an element of Q_8, say k. But then ak^{-1} centralizes Q_8. Furthermore, $G = \langle H, ak^{-1} \rangle$ and since H is finite and normal, this implies that ak^{-1} has infinite order. Thus, we replace a with ak^{-1} and assume that $G = Q_8 \times \langle a \rangle$.

Writing $Q_8 = \langle g, h \rangle$, we know that there is an epimorphism $\theta : FQ_8 \to M_2(F)$ given by

$$\theta(g) = \begin{pmatrix} \lambda & \mu \\ \mu & -\lambda \end{pmatrix} \text{ and } \theta(h) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Indeed, an easy calculation reveals that the matrices $\theta(g)$, $\theta(h)$ and $\theta(gh)$, together with the identity matrix, form a basis of $M_2(F)$. In fact, the kernel of θ is $FQ_8(\frac{1+g^2}{2})$, which is clearly an ideal invariant under $*$, as g^2 is both central and symmetric, and $FQ_8(\frac{1-g^2}{2}) \cong M_2(F)$. Thus, θ induces an involution on $M_2(F)$ and furthermore, if $\theta(\gamma)$ is a symmetric unit in $M_2(F)$, then $\gamma(\frac{1-g^2}{2}) + \frac{1+g^2}{2}$ is a symmetric unit in FQ_8. This means that the symmetric units in $M_2(F)$ are images of symmetric units in FQ_8.

Observe that the traces of $\theta(g)$, $\theta(h)$ and $\theta(gh)$ are all zero. Furthermore, $(\theta(g))^* = \theta(g^*) = \theta(g^{-1}) = -\theta(g)$, and similarly for h and gh. Thus, $\theta(g)$, $\theta(h)$ and $\theta(gh)$ span a three-dimensional subspace of the set of skew elements in $M_2(F)$. Surely the identity matrix is symmetric, so $(M_2(F))^- \neq M_2(F)$. Thus, these three matrices are a basis for $(M_2(F))^-$. Similarly, they are a basis for the set of matrices of trace zero, so the matrices of trace zero are precisely the skew matrices.

We can extend θ to $\theta : FG \to M_2(F\langle a\rangle)$ via

$$\theta(a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}.$$

Thus, the symmetric units in $M_2(F\langle a\rangle)$ are images of symmetric units in FG, and the symmetric units in $M_2(F\langle a\rangle)$ satisfy a group identity.

Now, E_{12} and E_{21} are both skew, having trace zero. Furthermore,

$$A = \begin{pmatrix} a-a^{-1} & 0 \\ 0 & a-a^{-1} \end{pmatrix}$$

is central and obviously skew, by definition of θ. Therefore,

$$AE_{12} = \begin{pmatrix} 0 & a-a^{-1} \\ 0 & 0 \end{pmatrix} \text{ and } AE_{21} = \begin{pmatrix} 0 & 0 \\ a-a^{-1} & 0 \end{pmatrix}$$

are both symmetric and square-zero. But their product is

$$\begin{pmatrix} (a-a^{-1})^2 & 0 \\ 0 & 0 \end{pmatrix},$$

and this is not nilpotent. By Lemma 2.2.1, we have a contradiction. □

Suppose that FG is semiprime and $\mathscr{U}^+(FG)$ satisfies a group identity. We know that Q is abelian or a Hamiltonian 2-group. Choose any idempotent $e \in FQ$. Let $a \in G$ have infinite order and take any $b \in Q$. Since Q is locally finite, we can find a finite subgroup H of Q containing b and the support of e. We know that H is normal in G. Thus, in $\langle H, a\rangle$, every element outside of H has infinite order, so $F\langle H, a\rangle$ is semiprime. Once again, H is abelian or a Hamiltonian 2-group. In the former case, FH is a direct sum of fields, and therefore Lemma 2.5.1 applies. In the latter case, Lemma 2.5.3 applies. Either way, e commutes with a and b. That is, e commutes with Q and with every element of infinite order. When char $F = 0$, this implies that e is central in FG. If char $F = p > 2$, then to make the same statement, we must prove that $Q = T$; that is, that G has no p-elements.

Lemma 2.5.4. *Let F be an infinite field of characteristic $p > 2$. Suppose that G has an element of infinite order and FG is semiprime. If $\mathscr{U}^+(FG)$ satisfies a group identity, then G has no p-elements.*

Proof. Let $g \in P$ have order p. By Lemma 2.4.1, $\langle g \rangle$ is normalized by T. Thus, the elements of order p in G generate an elementary abelian p-subgroup H, which is obviously normal in G. Let $a \in G$ have infinite order. We claim that the set $\{g^{a^i} : i \geq 0\}$ is finite.

Suppose this is not the case. If $g^a \in \langle g \rangle$, then $g^{a^i} \in \langle g \rangle$ for all $i \geq 0$, contradicting our hypothesis. So, we may assume that $g^a \notin \langle g \rangle$. As H is an elementary abelian p-group, we have a direct product $\langle g \rangle \times \langle g^a \rangle$. Similarly, we may assume that $g^{a^2} \notin \langle g, g^a \rangle$ and $g^{a^3} \notin \langle g, g^a, g^{a^2} \rangle$, and we get a direct product $\langle g \rangle \times \langle g^a \rangle \times \langle g^{a^2} \rangle \times \langle g^{a^3} \rangle$. Noting that $\hat{g}(a+a^{-1})\hat{g}$ is square-zero and symmetric and that $(\hat{g})^{a^2}(1-g^{a^2}) = 0$, we see from Lemma 2.2.7 that

$$(\hat{g})^{a^2}\hat{g}(a+a^{-1})\hat{g}(1-g^{a^2}) = 0.$$

Now, H is normal in G and $g \in H$, but $a^2 \notin H$, hence a and a^{-1} lie in different cosets modulo H. Thus, the linear combinations of elements in Ha must sum to zero, as must those in Ha^{-1}. That is,

$$(\hat{g})^{a^2}\hat{g}a^{-1}\hat{g}(1-g^{a^2}) = 0.$$

Simplifying and multiplying on the right by a, we obtain

$$(\hat{g})^{a^2}\hat{g}(\hat{g})^a(1-g^{a^3}) = 0.$$

But we have zero equal to a product of terms lying, respectively, in $F\langle g^{a^2} \rangle$, $F\langle g \rangle$, $F\langle g^a \rangle$ and $F\langle g^{a^3} \rangle$. As the product of the groups in question is direct, one of these terms is zero, which is not the case. The claim is proved.

Let $K = \langle g, a \rangle$, and let N be the subgroup of K generated by the finite set of conjugates of g discussed above. Then N is normal in K and since $N \leq H$, N is a finite elementary abelian p-group. Thus, by Lemma 1.1.1, $\Delta(K,N)$ is nilpotent. Hence, for any group element g of order p and any element a of infinite order, we get that $(1-g)a^{-1} + a(1-g^{-1})$ is nilpotent and symmetric. By Proposition 1.2.9, $\langle g \rangle$ is not a normal subgroup of G. Thus, there exists a conjugate g' of g with $g' \notin \langle g \rangle$. As g' has order p as well, we see that $\hat{g'}$ is symmetric and square-zero. Thus, by Lemma 2.2.7,

$$\hat{g'}((1-g)a^{-1} + a(1-g^{-1}))\hat{g'} = 0.$$

Once again, a and a^{-1} do not lie in the same coset of H, so separating the terms corresponding to each coset, we see that $\hat{g'}(1-g)a^{-1}\hat{g'} = 0$. Multiplying by a, we obtain

$$\hat{g'}(1-g)(\hat{g'})^a = 0.$$

If $(g')^a \notin \langle g \rangle \times \langle g' \rangle$, then we have a direct product $\langle g \rangle \times \langle g' \rangle \times \langle (g')^a \rangle$, in which case one of the terms in the above product is zero, which is not the case. Thus, $(g')^a \in \langle g, g' \rangle$. Similarly, $g^a \in \langle g, g' \rangle$. That is, $\langle g, g' \rangle$ is a subgroup of order p^2 normalized by every element of infinite order. We saw above that it is normalized by T as well; hence, the subgroup is normal. But this contradicts Proposition 1.2.9. Thus, g does not exist, and G has no p-elements. □

In summary, we know that $T = Q$, and T is abelian or a Hamiltonian 2-group (with the latter case only occurring if the characteristic is zero). Also, every idempotent in FT is central in FG. One last condition is required.

Lemma 2.5.5. *Let F be an infinite field of characteristic different from 2 and G a group such that FG is semiprime. If FT has a nonsymmetric idempotent and $\mathscr{U}^+(FG)$ satisfies a group identity, then G/T satisfies a group identity.*

Proof. If G is torsion, there is nothing to say, so let G have an element of infinite order and suppose that e is a nonsymmetric idempotent of FT. If $\mathscr{U}^+(FG)$ satisfies $w(x,y) = 1$, then we claim that G/T satisfies this identity as well. Let H be the (finite normal) subgroup of T generated by the support of e. Since e is known to be central, it is a sum of primitive central idempotents of FH. Thus, since e is not symmetric, one of the primitive central idempotents is not symmetric. Say

$$FH = FHe_1 \oplus FHe_1^* \oplus FHe_3 \oplus \cdots \oplus FHe_n$$

is the Wedderburn decomposition of FH. Since each idempotent of FH is central, we have

$$FG = FGe_1 \oplus FGe_1^* \oplus FGe_3 \oplus \cdots \oplus FGe_n$$

as well. If $g \in G$, then $ge_1 + g^{-1}e_1^* + e_3 + \cdots + e_n$ is a symmetric unit. Thus, for any $g, h \in G$,

$$w(ge_1 + g^{-1}e_1^* + e_3 + \cdots + e_n, he_1 + h^{-1}e_1^* + e_3 + \cdots + e_n) = 1.$$

Looking only at the first component, we have $w(ge_1, he_1) = e_1$, hence $w(g,h)e_1 = e_1$. But $w(g,h)$ is a group element, and if $w(g,h)e_1 = e_1$, then $w(g,h)$ lies in H. That is, G/T satisfies $w(x,y) = 1$. □

The first part of the main result of [96] is

Theorem 2.5.6. *Let F be an infinite field of characteristic $p \neq 2$, and let G be a group containing an element of infinite order. Suppose that FG is semiprime. If $\mathscr{U}^+(FG)$ satisfies a group identity, then*

1. *if $p = 0$, then the set of torsion elements, T, is a (normal) subgroup of G, and T is abelian or a Hamiltonian 2-group;*
2. *if $p > 2$, then T is an abelian (normal) p'-subgroup of G;*
3. *every idempotent in FT is central in FG; and*
4. *if FT contains a nonsymmetric idempotent, then G/T satisfies a group identity.*

Conversely, if G/T is a u.p. group and FG satisfies the above four conditions, then $\mathscr{U}^+(FG)$ satisfies a group identity.

Proof. We have only to verify the converse. Of course we are done if the conditions of Theorem 1.4.9 are satisfied, for in this case $\mathscr{U}(FG)$ satisfies a group identity. First of all, note that in the proof of Theorem 1.4.9 it is sufficient to assume for the third condition that every idempotent of FT is central in FG. For the remaining conditions, there are only two cases to consider, namely, if $p = 0$ and T is a Hamiltonian 2-group, or if every idempotent of FT is symmetric. In fact, the former case is contained in the latter. We know that every idempotent of FT is central and, by Lemma 2.1.1, every central element in FT, where T is a Hamiltonian 2-group, is symmetric. Thus, in any case, we can assume that every idempotent of FT is symmetric. We claim that $\mathscr{U}^+(FG)$ is abelian.

Take any $\alpha \in \mathscr{U}^+(FG)$. By Remark 1.4.10, there is a finite subgroup E of T such that for any primitive idempotent e of FE, we have $\alpha e = \lambda g$ for some $\lambda \in \mathscr{U}(FEe)$ and some $g \in G$. Since e is symmetric and central, $\lambda g = (\lambda g)^* = g^{-1}\lambda^*$. Thus, $g^2 e = \lambda^{-1}(g^{-1}\lambda^* g) \in FEe$. (Remember that E is a normal subgroup, since $\frac{1}{|E|}\hat{E}$ is a central idempotent.) But $g^2 e$ would not lie in FEe if g had infinite order. Thus, $g \in T$ and, in fact, $\alpha e = \lambda g \in FTe$. That is, $\alpha \in \mathscr{U}^+(FT)$. But T is abelian or a Hamiltonian 2-group, and either way, by Lemma 2.1.1, we see that the symmetric elements commute. We are done. □

Remark 2.5.7. It follows from the proof of the sufficiency above that if we replace the fourth condition with the assumption that every idempotent in FT is symmetric, then the symmetric units of FG commute.

2.6 The General Case for Nontorsion Groups

Let us now discuss group rings that are not semiprime. We let F be an infinite field of characteristic $p > 2$ (as the characteristic zero case is done). Once again, G is a group containing an element of infinite order, T is the set of torsion elements, P is the set of p-elements and Q is the set of p'-elements in T. As in the previous chapter, we will handle the case in which $N(FG)$ is nilpotent first.

Proposition 2.6.1. *Let F be an infinite field of characteristic $p > 2$ and G a group containing an element of infinite order. Suppose that $N(FG)$ is nilpotent. Then $\mathscr{U}^+(FG)$ satisfies a group identity if and only if P is a finite (normal) subgroup of G and $\mathscr{U}^+(F(G/P))$ satisfies a group identity.*

Proof. Suppose that $\mathscr{U}^+(FG)$ satisfies a group identity. By Proposition 1.2.22, $\phi_p(G)$ is finite. Thus, by Proposition 2.3.8, the p-elements of $\phi_p(G)$ form a group, so $\phi_p(G)$ is a finite p-group. Therefore, by Lemma 2.3.6, $\mathscr{U}^+(F(G/\phi_p(G)))$ satisfies a group identity. But by Proposition 1.2.9, $F(G/\phi_p(G))$ is semiprime. It follows from Theorem 2.5.6 that $G/\phi_p(G)$ has no p-elements. Thus, $P = \phi_p(G)$, and the necessity is proved. The sufficiency follows from Lemmas 2.3.5 and 1.1.1. □

Thus, in order to deal with groups containing only finitely many p-elements, it remains to show that the p-elements form a subgroup when $N(FG)$ is not nilpotent. We begin with

Proposition 2.6.2. *Let F be an infinite field of characteristic $p > 2$ and G a group. If $N(FG)$ is not nilpotent and $\mathscr{U}^+(FG)$ satisfies a group identity, then FG satisfies a polynomial identity.*

Proof. If G is torsion, then Proposition 2.4.3 does the job, so assume that G is not torsion. By Lemma 1.4.4, $T \cap \phi(G)$ is a locally finite group. Thus, by Proposition 2.3.8, its p-elements form a subgroup; hence, $\phi_p(G)$ is a p-group. Suppose it is finite. By Proposition 1.2.9, $F(G/\phi_p(G))$ is semiprime. Thus, $FG/\Delta(G,\phi_p(G))$ has no nilpotent ideals, hence $N(FG) \subseteq \Delta(G,\phi_p(G))$. By Lemma 1.1.1, $\Delta(G,\phi_p(G))$ is nilpotent, so $N(FG)$ is nilpotent, contrary to our assumption. Thus, $\phi_p(G) = \phi(G) \cap P$ is an infinite group.

By Lemma 2.2.6, $N(FG)$ satisfies a polynomial identity. As $N(FG)$ is not nilpotent, Lemma 1.2.16 tells us that FG satisfies a nondegenerate multilinear GPI. Thus, by Proposition 1.2.15, $(G : \phi(G)) < \infty$ and $|(\phi(G))'| < \infty$. Hence, by Proposition 1.1.4, it suffices to show that $F\phi(G)$ satisfies a polynomial identity. By Proposition 2.6.1, $N(F\phi(G))$ is not nilpotent. Thus, replacing G with $\phi(G)$, we assume that G is an FC-group. Then we know that G' is finite, so we can factor out $G' \cap P$ and assume that G' is a finite p'-group. Now, $(G,P) \leq G' \cap P = 1$. Thus, P is central. The last part of the proof of Proposition 1.5.9 finishes the argument. □

As promised, we now have this proposition.

Proposition 2.6.3. *Let F be an infinite field of characteristic $p > 2$ and let G be a group. If $\mathscr{U}^+(FG)$ satisfies a group identity, then P is a (normal) subgroup of G and $\Delta(P)$ is locally nilpotent.*

Proof. If we can show that P is a subgroup, then we are done, since it is locally finite by Proposition 2.4.3, and therefore $\Delta(P)$ is locally nilpotent, by Lemma 1.1.1. If G is torsion, then Proposition 2.4.3 gives us the result. So, assume that G is nontorsion. If $N(FG)$ is nilpotent, then Proposition 2.6.1 does the job. Thus, we assume that $N(FG)$ is not nilpotent. By Proposition 2.6.2, FG satisfies a polynomial identity. Take any $g_1,\ldots,g_n \in P$ and let H be the subgroup they generate. Then FH is a finitely generated algebra satisfying a polynomial identity. By Proposition 1.5.12, $J(FH)$ is nilpotent. Now the Jacobson radical contains every nil ideal, so $N(FH)$ is nilpotent. By Propositions 2.4.3 and 2.6.1, H is a p-group. Thus, P is a group, and we are done. □

As we have seen, if P is finite, there is nothing more to do. The second part of the main result of [96] is

Theorem 2.6.4. *Let F be an infinite field of characteristic $p > 2$ and G a nontorsion group. Suppose that G contains finitely many p-elements. If $\mathscr{U}^+(FG)$ satisfies a group identity, then*

1. *the p-elements of G form a (finite normal) subgroup P of G;*
2. *the torsion elements of G/P form an abelian group, T/P;*
3. *every idempotent of $F(T/P)$ is central in $F(G/P)$; and*
4. *if $F(T/P)$ has a nonsymmetric idempotent, then G/T satisfies a group identity.*

Conversely, if G satisfies the four conditions above, and G/T is a u.p. group, then $\mathscr{U}^+(FG)$ satisfies a group identity.

What happens if P is infinite? In fact, if P has bounded exponent, then we are done as well. By Proposition 2.6.1, $N(FG)$ is not nilpotent. Hence, by Proposition 2.6.2, FG satisfies a polynomial identity (and therefore has a p-abelian normal subgroup of finite index, by Proposition 1.1.4). Thus, by Lemma 1.3.14, $\Delta(G,P)$ is nil of bounded exponent. By Lemma 2.3.5, $\mathscr{U}^+(FG)$ satisfies a group identity if and only if $\mathscr{U}^+(F(G/P))$ satisfies a group identity. As $F(G/P)$ is semiprime, Theorem 2.5.6 gives us the third part of the result.

Theorem 2.6.5. *Let F be an infinite field of characteristic $p > 2$ and G a nontorsion group. Suppose that G contains infinitely many p-elements and that the p-elements have bounded exponent. If $\mathscr{U}^+(FG)$ satisfies a group identity, then*

1. *the p-elements of G form a (normal) subgroup P of bounded exponent;*
2. *the torsion elements of G/P form an abelian group, T/P;*
3. *every idempotent of $F(T/P)$ is central in $F(G/P)$;*
4. *if $F(T/P)$ has a nonsymmetric idempotent, then G/T satisfies a group identity; and*
5. *G has a p-abelian normal subgroup of finite index.*

Conversely, if G satisfies the five conditions above, and G/T is a u.p. group, then $\mathscr{U}^+(FG)$ satisfies a group identity.

Now we can consider groups in which P has unbounded exponent. We need to borrow the following general result about $*$-polynomial identities on prime algebras. The proof can be found in Theorems 2.4.13 and 3.1.62 of [91]. If $f(x_1,x_1^*,\ldots,x_n,x_n^*)$ is a $*$-polynomial in $F\{x_1,x_1^*,\ldots,x_n,x_n^*\}$, then we can construct a polynomial $g(x_1,\ldots,x_{2n}) \in F\{x_1,\ldots,x_{2n}\}$ by replacing each x_i^* with x_{n+i}. If f is a $*$-polynomial identity for an F-algebra R, then we say that f is special if g is a polynomial identity for R. (For example, let $R = M_2(F)$ under the transpose involution. Then R satisfies $[x_1-x_1^*,x_2-x_2^*]$, but surely not $[x_1-x_3,x_2-x_4]$. Thus, $[x_1-x_1^*,x_2-x_2^*]$ is not special for $M_2(F)$.)

Proposition 2.6.6. *Let F be an infinite field and R a prime F-algebra having an involution $*$ fixing F elementwise. Suppose that R satisfies a polynomial identity. Then either*

1. *R satisfies precisely the same $*$-polynomial identities as $M_n(F')$, under either the transpose or symplectic involution, for some positive integer n and some extension field F' of F; or*
2. *every $*$-polynomial identity of R is special.*

Let us now refine Lemma 2.2.6.

Lemma 2.6.7. *Let F be an infinite field of characteristic different from 2 and let R be an F-algebra with an involution $*$ that fixes F elementwise. If I is a $*$-invariant nil ideal of R, let S be the F-subalgebra of R generated by 1 and I. Suppose that $\mathscr{U}^+(R)$ satisfies a group identity. Then S satisfies $*$-polynomial identities $f(x_1,x_1^*,\ldots,x_4,x_4^*)$ and $g(x_1,x_1^*,\ldots,x_4,x_4^*)$ such that*

1. *f is not a $*$-polynomial identity for $M_n(F)$ under the transpose involution, for any $n \geq 2$;*
2. *f is not a $*$-polynomial identity for $M_{2n}(F)$ under the symplectic involution for any $n \geq 2$; and*
3. *the sum of the monomials of g that do not involve any x_i^* is not a polynomial identity for $M_n(F)$ for any $n \geq 2$.*

Proof. Let $w(x,y)=1$ be a group identity for $\mathscr{U}^+(R)$, as in Lemma 2.1.3, and let $F\{x_1,x_1^*,x_2,x_2^*\}[[z]]$ be the ring of formal power series over the free algebra with involution. We write

$$w((1+x_1z)(1+x_1^*z),(1+x_2z)(1+x_2^*z))-1=\sum_{i\geq 0} f_i(x_1,x_1^*,x_2,x_2^*)z^i.$$

Now, if $a_1,a_2\in I$, then for any $\lambda\in F$, we have $(1+\lambda a_j)(1+\lambda a_j^*)\in\mathscr{U}^+(R)$, for $j=1,2$. Thus,

$$0=w((1+\lambda a_1)(1+\lambda a_1^*),(1+\lambda a_2)(1+\lambda a_2^*))-1=\sum_{i\geq 0} f_i(a_1,a_1^*,a_2,a_2^*)\lambda^i.$$

Fixing $a_1,a_2\in I$, and noting that if $a_1^k=0$, then $(1+\lambda a_1)^{-1}=1-\lambda a_1+\lambda^2a_1^2-\cdots\pm\lambda^{k-1}a_1^{k-1}$, and similarly for the other terms, we see that there exists a positive integer j such that $f_i(a_1,a_1^*,a_2,a_2^*)=0$ for all $i>j$. Thus,

$$\sum_{i=0}^{j} f_i(a_1,a_1^*,a_2,a_2^*)\lambda^i=0.$$

As there are infinitely many choices for λ, a Vandermonde determinant argument (as in Lemma 1.2.4) tells us that each $f_i(a_1,a_1^*,a_2,a_2^*)=0$, $0\leq i\leq j$ (and obviously for all $i>j$). That is, I satisfies each f_i.

By definition of S, we have $[S,S]\subseteq I$. Thus, letting

$$g_i(x_1,x_1^*,\ldots,x_4,x_4^*)=f_i([x_1,x_3],[x_1,x_3]^*,[x_2,x_4],[x_2,x_4]^*)$$

for each i, we see that S satisfies each g_i. We will demonstrate that at least one g_i is not the zero polynomial by showing that it is not satisfied by a matrix ring.

Take any matrix ring $M_n(F)$, $n\geq 2$, with any involution. Suppose A is a square-zero matrix. Then noting that $(1+Az)^s=1+sAz$ for all integers s and similarly for $1+A^*z$, we have

$$\sum_{i\geq 0} f_i(A,A^*,A^*,A)z^i = w((1+Az)(1+A^*z),(1+A^*z)(1+Az))-1.$$

In this product we have no more than two consecutive identical terms, and no term is adjacent to its inverse. Replacing $(1+Az)^s$ with $1+sAz$, $s\in\{\pm1,\pm2\}$, we see that the highest term appearing is

$$\pm 2^u A^v (A^*A)^c (A^*)^d z^m = f_m(A,A^*,A^*,A)z^m,$$

with $u,c\geq 0$, $v,d\in\{0,1\}$.

Suppose first of all that $*$ is the transpose involution. Then let $A=E_{12}$. Notice that

$$f_m(E_{12},E_{21},E_{21},E_{12}) = \pm 2^u E_{12}^v (E_{21}E_{12})^c E_{21}^d = \pm 2^u E_{12}^v E_{22}^c E_{21}^d \neq 0.$$

If $M_n(F)$ satisfies g_m, then

$$0 = g_m(E_{11},E_{11},E_{22},E_{22},E_{12},E_{21},E_{21},E_{12}) = f_m(E_{12},E_{21},E_{21},E_{12}),$$

and we have a contradiction.

Next, suppose that $n=2h$, $h\geq 2$, and $*$ is the symplectic involution. Let $A=E_{12}+E_{h+1,h+2}$. Notice that

$$\begin{aligned} &f_m(E_{12}+E_{h+1,h+2},E_{h+2,h+1}+E_{21},E_{h+2,h+1}+E_{21},E_{12}+E_{h+1,h+2}) \\ &\quad = \pm 2^u (E_{12}+E_{h+1,h+2})^v (E_{22}+E_{h+2,h+2})^c (E_{h+2,h+1}+E_{21})^d. \end{aligned}$$

As $E_{22}+E_{h+2,h+2}$ is an idempotent, this is not zero. If $M_n(F)$ satisfies g_m, then

$$\begin{aligned} 0 &= g_m(E_{11}+E_{h+1,h+1},E_{h+1,h+1}+E_{11},E_{h+2,h+2}+E_{22},E_{22}+E_{h+2,h+2}, \\ &\qquad E_{12}+E_{h+1,h+2},E_{h+2,h+1}+E_{21},E_{h+2,h+1}+E_{21},E_{12}+E_{h+1,h+2}) \\ &= f_m(E_{12}+E_{h+1,h+2},E_{h+2,h+1}+E_{21},E_{h+2,h+1}+E_{21},E_{12}+E_{h+1,h+2}), \end{aligned}$$

and again, we have a contradiction.

Finally, we claim that there exists an i such that if we let $\tilde{f}_i(x_1,x_2)$ be the sum of the monomials in f_i containing no x_r^* terms, then $\tilde{f}_i(E_{12},E_{21})\neq 0$ in $M_n(F)$, $n\geq 2$. If $A,B\in M_n(F)$ are square-zero, then calculating

$$\sum_{i\geq 0} f_i(A,A^*,B,B^*)z^i = w((1+Az)(1+A^*z),(1+Bz)(1+B^*z))-1,$$

we see that we do not get identical consecutive terms in the product, nor will a term appear next to its inverse. Replacing $(1+Az)^{-1}$ with $1-Az$, and so forth, and dropping all of the monomials involving A^* and B^*, the highest remaining term will be something of the form $\tilde{f}_s(A,B)=\pm A^v(BA)^cB^d$, with $c\geq 0$ and $v,d\in\{0,1\}$. Letting $A=E_{12}$, $B=E_{21}$, we see that this is not zero, establishing the claim. Defining g_s as above, we see that $\tilde{g}_s(x_1,x_2,x_3,x_4)=\tilde{f}_s([x_1,x_3],[x_2,x_4])$. Evidently S satisfies g_s, but

$$\tilde{g}_s(E_{12},E_{21},E_{22},E_{11}) = \tilde{f}_s(E_{12},E_{21}) \neq 0.$$

We are done. □

But we can be more specific. Note that every primitive ring is prime. Indeed, let R be primitive, and let I_1 and I_2 be nonzero ideals of R. If M is a faithful irreducible left R-module, then I_2M is a submodule of M. Since M is faithful, $I_2M \neq 0$, and since M is irreducible, this implies that $I_2M = M$. Similarly, $0 \neq M = I_1M = I_1I_2M$. Thus, $I_1I_2 \neq 0$, and R is prime.

Lemma 2.6.8. *Let F, R, I and S be as in the preceding lemma, with char $F = p > 2$. If $\mathscr{U}^+(R)$ satisfies a group identity, then there exists a positive integer k such that S satisfies the $*$-polynomial identities $[x_1+x_1^*,x_2]^{p^k} = 0$ and $([x_1+x_1^*,x_2]x_3)^{p^k} = 0$.*

Proof. Take f and g as in the preceding lemma. Let $F\{x_1,x_1^*,x_2,x_2^*,x_3,x_3^*\}$ be the free algebra with involution and let K be the ideal of this algebra generated by $f(a_1,a_1^*,\dots,a_4,a_4^*)$ and $g(a_1,a_1^*,\dots,a_4,a_4^*)$, together with their images under $*$, for all $a_i \in F\{x_1,x_1^*,x_2,x_2^*,x_3,x_3^*\}$. Let $W = R/K$. Then W has the induced involution and satisfies the $*$-polynomials f and g. Therefore, by Proposition 2.1.2, it satisfies a polynomial identity.

Let B be a primitive ideal of W; that is, let W/B be a primitive ring. Suppose that B is invariant under $*$. Then W/B has the induced involution and satisfies f. As we noted above, a primitive ring is prime. Thus, we examine the two possibilities allowed by Proposition 2.6.6. If $n \geq 2$, then f is not satisfied by $M_n(F')$ under the transpose involution nor by $M_{2n}(F')$ under the symplectic involution. Thus, if the first case of Proposition 2.6.6 occurs, then $n = 1$, hence we have a field or $M_2(F')$ under the symplectic involution. In the latter case, we note that the symmetric elements are simply scalar multiples of the identity matrix. Thus, W/B satisfies $[x_1+x_1^*,x_2] = 0$. The alternative is that W/B satisfies the polynomial $h(x_1,\dots,x_8)$ obtained by replacing x_i^* with x_{4+i} in f, $1 \leq i \leq 4$. But by Proposition 1.5.11, W/B satisfies the same polynomial identities as some $M_n(F')$. If $n \geq 2$, then we know that $M_n(F)$ under the transpose involution does not satisfy f, so take $A_1,\dots,A_4 \in M_n(F')$ with $f(A_1,A_1^*,\dots,A_4,A_4^*) \neq 0$. Then, substituting $x_i = A_i$ and $x_{4+i} = A_i^*$, $1 \leq i \leq 4$, we see that $M_n(F')$ does not satisfy h. It follows that $n = 1$ and W/B is commutative. Thus, in any case, W/B satisfies $[x_1+x_1^*,x_2] = 0$.

Suppose, on the other hand, that $B^* \not\subseteq B$. Then $(B+B^*)/B$ is a nonzero ideal of W/B. But W/B is primitive and satisfies a polynomial identity. Thus, by Proposition 1.5.11, W/B is simple, so $W = B+B^*$. We can see that a typical element is $(b+b^*)+B = b^*+B$, $b \in B$. But $(b^*)^* \equiv 0 \pmod{B}$ for all $b \in B$. Thus, for any $b_1,\dots,b_4 \in B^*$, we have

$$0 = g(b_1,b_1^*,\dots,b_4,b_4^*) \equiv g(b_1,0,\dots,b_4,0) \pmod{B}.$$

That is, letting $\tilde{g}$ be the sum of the monomials in g not involving any x_i^*, we have $\tilde{g}(b_1,b_2,b_3,b_4) \equiv 0 \pmod{B}$. Putting this another way, W/B satisfies $\tilde{g}$. By Proposition 1.5.11, W/B satisfies the same polynomial identities as some $M_n(F')$. But Lemma 2.6.7 tells us that $n = 1$. Thus, W/B is commutative. In all cases, then,

$[w_1 + w_1^*, w_2] \in B$ (and, therefore, $[w_1 + w_1^*, w_2]w_3 \in B$) for all $w_i \in W$ and all primitive ideals B of W.

The intersection of the primitive ideals is $J(W)$. Since W is a finitely generated F-algebra, Proposition 1.5.12 tells us that $J(W)$ is nilpotent. Thus, W satisfies the required $*$-polynomial identities. But W is the relatively free algebra with involution of the variety determined by f and g. Therefore, for any $s_1, s_2, s_3 \in S$, we see that $[s_1 + s_1^*, s_2]^{p^k} = 0$ and $([s_1 + s_1^*, s_2]s_3)^{p^k} = 0$, as required. □

Lemma 2.6.9. *Let F be an infinite field of characteristic $p > 2$ and G a nontorsion group with P infinite. Suppose that $\mathcal{U}^+(FG)$ satisfies a group identity and G has an abelian normal subgroup A of finite index. Then $\Delta(G, A \cap P)$ is nil and satisfies the $*$-polynomial identities $[x_1 + x_1^*, x_2]^{p^k} = 0$ and $([x_1 + x_1^*, x_2]x_3)^{p^k} = 0$ for some positive integer k.*

Proof. By Proposition 2.6.1, $N(FG)$ is not nilpotent, since P is infinite. Furthermore, Proposition 2.6.3 tells us that $\Delta(P)$ is locally nilpotent. The first part of the proof of Lemma 1.5.14 shows us that $\Delta(G, A \cap P)$ is locally nilpotent, hence nil. Thus, by the previous lemma, $\Delta(G, A \cap P)$ satisfies the required $*$-polynomial identities. □

We must show that G' has to be a p-group of bounded exponent. For now, we have

Lemma 2.6.10. *Let F be an infinite field of characteristic $p > 2$ and G a nontorsion group with P infinite. Suppose that $\mathcal{U}^+(FG)$ satisfies a group identity and G has an abelian normal subgroup A of finite index. Then $(G, A \cap P)$ is an abelian p-group of bounded exponent.*

Proof. Since A and P are normal subgroups, $(G, A \cap P)$ is clearly an abelian p-group. Thus, we need only check that it has bounded exponent. By the previous lemma, $\Delta(G, A \cap P)$ satisfies $[x_1 + x_1^*, x_2]^{p^k} = 0$. Choose any $a \in A \cap P$ and any $g \in G$. If we can bound the order of (a, g), then we will be done, as $(G, A \cap P)$ is abelian. We have

$$\begin{aligned} 0 &= [(a-1)g + ((a-1)g)^*, (a-1)g]^{p^k} \\ &= (a + a^{-1} - a^g - (a^{-1})^g)^{p^k} \\ &= a^{p^k} + a^{-p^k} - (a^{p^k})^g - (a^{-p^k})^g, \end{aligned}$$

since A is abelian. Thus, $a^{p^k} + a^{-p^k} = (a^{p^k})^g + (a^{-p^k})^g$. That is, $a^{p^k} = (a^{p^k})^g$ or $(a^{-p^k})^g$. In the former case, $(a, g)^{p^k} = a^{-p^k}(a^{p^k})^g = 1$, as desired. Let us consider the latter case.

If $b = a^{p^k}$, then we have $b^{-1}g = gb$, hence $bg^2 = g^2b$. Thus,

$$\begin{aligned}
&[(b-1)g+((b-1)g)^*, g(b-1)]\\
&\quad = (b-1)g^2(b-1)+g^{-1}(b^{-1}-1)g(b-1)-g(b-1)^2g-g(b-1)g^{-1}(b^{-1}-1)\\
&\quad = (b-1)^2g^2+(b-1)^2-(b^{-1}-1)^2g^2-(b^{-1}-1)^2\\
&\quad = ((b-1)^2-(b^{-1}-1)^2)(g^2+1)\\
&\quad = b^{-2}(b+1)(b-1)^3(g^2+1).
\end{aligned}$$

Of course, $b \in A \cap P$. Therefore, $[(b-1)g+((b-1)g)^*, g(b-1)]^{p^k} = 0$, and hence

$$b^{-2p^k}(b^{p^k}+1)(b^{p^k}-1)^3(g^{2p^k}+1) = 0.$$

Of course b^{-2p^k} is a unit. Also, b^{p^k} is a p-element. If its order is p^r, $r \geq 0$, then $(b^{p^k}+1)^{p^r} = 2$. Thus, $b^{p^k}+1$ is also a unit. It follows that $(b^{p^k}-1)^3(g^{2p^k}+1) = 0$ and multiplying on the left by $(b^{p^k}-1)^{p-3}$, we get

$$(b^{p^{k+1}}-1)(g^{2p^k}+1) = 0.$$

That is,

$$b^{p^{k+1}} + b^{p^{k+1}}g^{2p^k} = g^{2p^k}+1$$

and hence

$$a^{p^{2k+1}} + a^{p^{2k+1}}g^{2p^k} = g^{2p^k}+1.$$

If $a^{p^{2k+1}} = 1$, then also $(a,g)^{p^{2k+1}} = a^{-p^{2k+1}}(a^g)^{p^{2k+1}} = 1$, as desired. Otherwise, $a^{p^{2k+1}}g^{2p^k} = 1$ and, therefore, $a^{p^{2k+1}} = g^{2p^k}$. That is, $a^{2p^{2k+1}} = 1$. Since $a \in P$, we have $a^{p^{2k+1}} = 1$ and the same conclusion follows. In any case, $(a,g)^{p^{2k+1}} = 1$, and we are done. □

We close the chapter with the final part of the result of Sehgal and Valenti [96].

Theorem 2.6.11. *Let F be an infinite field of characteristic $p > 2$ and G a nontorsion group. Suppose that the p-elements of G are of unbounded exponent. Then the following are equivalent:*

(i) $\mathscr{U}^+(FG)$ satisfies a group identity;
(ii) $\mathscr{U}(FG)$ satisfies a group identity;
(iii) G has a p-abelian normal subgroup A of finite index, and G' is a p-group of bounded exponent.

Proof. Clearly (ii) implies (i), and we see from Theorem 1.5.16 that (iii) implies (ii). Thus, let us assume that $\mathscr{U}^+(FG)$ satisfies a group identity and show that G has a p-abelian normal subgroup A of finite index and that G' is a p-group of bounded exponent. By Proposition 2.6.1, $N(FG)$ is not nilpotent. Therefore, by Proposition 2.6.2, FG satisfies a polynomial identity, and the existence of A follows from Proposition 1.1.4. Now, A' is a finite p-group, so by Lemma 2.3.6, $\mathscr{U}^+(F(G/A'))$ satisfies a group identity. Furthermore, the p-elements of G/A' have unbounded exponent, and if $(G/A')'$ is a p-group of bounded exponent, then so is G'. Thus, we factor out A' and assume that A is abelian. Then, by Lemma 2.6.9, $\Delta(G,A\cap P)$ is nil. It follows from Lemma 2.3.5 that $\mathcal{U}^+(F(G/(A\cap P)))$ satisfies a group identity. Also, by Lemma 2.6.10, $(G,A\cap P)$ is a p-group of bounded exponent. Thus, we factor out $(G,A\cap P)$ and assume that $A\cap P$ is central (and of unbounded exponent, since $(P:A\cap P)\leq(G:A)<\infty$). In fact, since P has a central subgroup of finite p-power index, Proposition 1.3.7 says that P' is a finite p-group. Thus, let us factor out P' and assume that P is abelian.

Take any $g,h\in G$ and $a\in A\cap P$. Since a is central, we have

$$(a-a^{-1})(g-g^{-1})\in(\Delta(G,A\cap P))^+.$$

Also,

$$(a-a^{-1})h^{-1},(a-a^{-1})^{p-2}gh\in\Delta(G,A\cap P).$$

Thus, by Lemma 2.6.9,

$$([(a-a^{-1})(g-g^{-1}),(a-a^{-1})h^{-1}](a-a^{-1})^{p-2}gh)^{p^k}=0.$$

Again, a is central, so we have

$$(a-a^{-1})^{p^{k+1}}([g-g^{-1},h^{-1}]gh)^{p^k}=0.$$

Multiplying through by $a^{p^{k+1}}$, we get

$$(a^{2p^{k+1}}-1)([g-g^{-1},h^{-1}]gh)^{p^k}=0.$$

Recall that $A\cap P$ has unbounded exponent. Thus, we have infinitely many different $a^{2p^{k+1}}$; hence, by Lemma 1.5.8, $([g-g^{-1},h^{-1}]gh)^{p^k}=0$. Equivalently,

$$(gh^{-1}gh-(g,h)-h^{-1}g^2h+1)^{p^k}=0.$$

Since this holds for any $g\in G$, it also holds for ag. Thus,

$$(a^2gh^{-1}gh-(g,h)-a^2h^{-1}g^2h+1)^{p^k}=0.$$

By Lemma 1.3.16,

$$a^{2p^k}(gh^{-1}gh)^{p^k}-(g,h)^{p^k}-a^{2p^k}(h^{-1}g^2h)^{p^k}+1\in[FG,FG].$$

But elements of $[FG,FG]$ must have trace zero, so either $(g,h)^{p^k}$ or $a^{2p^k}(h^{-1}g^2h)^{p^k}$ is the identity. However, $A\cap P$ has unbounded exponent, so we can choose a in such a way that $a^{2p^k}\neq(h^{-1}g^2h)^{-p^k}$. Thus, $(g,h)^{p^k}=1$ for all $g,h\in G$. But $G'\leq P$, and P is abelian. Thus, G' is a p-group of bounded exponent, and the proof is complete. □

Springer

http://www.springer.com/978-1-84996-503-3

Group Identities on Units and Symmetric Units of Group Rings
Lee, G.T.
2010, XII, 196 p., Hardcover
ISBN: 978-1-84996-503-3