University of Alberta

Symmetric Elements in Group Rings and Related Problems

by

Gregory Thomas Lee ©

A thesis submitted to the Faculty of Graduate Studies and Research in partial fulfillment of the requirements for the degree of Doctor of Philosophy

in

Mathematics

Department of Mathematical Sciences

Edmonton, Alberta

Spring 2000

0-612-59994-9

University of Alberta

Library Release Form

Name of Author: Gregory Thomas Lee

Title of Thesis: Symmetric Elements in Group Rings and Related Problems

Degree: Doctor of Philosophy

Year this Degree Granted: 2000

Gregory T. Lee

Gregory Thomas Lee
311 Tunis St.
Ingersoll, Ontario
N5C 1W9
CANADA

Date: April 14, 2000

University of Alberta

Faculty of Graduate Studies and Research

The undersigned certify that they have read, and recommend to the Faculty of Graduate Studies and Research for acceptance, a thesis entitled **Symmetric Elements in Group Rings and Related Problems** submitted by **Gregory Thomas Lee** in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Mathematics.

S K Sehgal
Dr. S. K. Sehgal (Supervisor)

Dr. H. H. Brungs

Gerald Cliff
Dr. G. H. Cliff

Dr. P. Jelen

M. Shirvani
Dr. M. Shirvani

H. H-B
Dr. D. S. Passman
(University of Wisconsin–Madison)

Date: April 11, 2000

ABSTRACT

Let F be a field and G a group. The group ring, FG, admits a natural involution, $*$, which maps each group element to its inverse. Most of this thesis is devoted to the study of the set of symmetric elements, $(FG)^+$. This is the set of elements of FG which are fixed by $*$.

We first consider the Lie structure of FG. When the characteristic of F is different from 2, we classify the groups G such that $(FG)^+$ is Lie nilpotent, or Lie n-Engel. In particular, if G does not contain the quaternion group, Q_8, we show that if $(FG)^+$ is Lie nilpotent, then so is FG, and similarly, if $(FG)^+$ is Lie n-Engel, then FG is Lie m-Engel, for some m. We provide similar results for the characteristic 2 case, and for the set of skew elements, $(FG)^- = \{\alpha \in FG : \alpha^* = -\alpha\}$, when G contains no 2-elements.

Next, we examine the set of symmetric units of FG, where G is a torsion group. Let us say that the symmetric units are nilpotent if they satisfy the group identity $(x_1, \dots, x_n) = 1$, for some $n \geq 2$, where $(x_1, x_2) = x_1^{-1}x_2^{-1}x_1x_2$, and $(x_1, \dots, x_{n+1}) = ((x_1, \dots, x_n), x_{n+1})$. We determine the conditions under

which the set of symmetric units is nilpotent, provided char $F \neq 2$. In particular, if G does not contain Q_8, we show that the symmetric units are nilpotent if and only if the entire unit group is nilpotent.

Finally, we look at the integral group ring, $\mathbb{Z}A$, of a finite abelian group A. It is known that if $n \leq 5$, and U is a torsion matrix with identity augmentation in $GL_n(\mathbb{Z}A)$, then U is conjugate in $GL_n(\mathbb{Q}A)$ to a diagonal matrix with group elements on the diagonal. It is also known that this will not hold in general when $n \geq 6$. We provide a condition on the Sylow subgroups of A which will cause this property to hold. In addition, we provide some generalizations to infinite abelian groups.

ACKNOWLEDGEMENTS

I would like to thank my supervisor, Dr. Sudarshan Sehgal, for all of his help. He has patiently guided me through two degrees, not to mention introducing me to the subject of group rings in the first place. I cannot thank him enough.

My work has been funded by scholarships from the Killam Trusts, the Natural Sciences and Engineering Research Council of Canada, the Province of Alberta, and the University of Alberta, and I would like to thank them all for their generous support.

Finally, thanks to my family and friends for their encouragement over the years.

Chapter 3 of this thesis, with the exception of §3.7, is a combination of the papers [Lee1] and [Lee2]. The results on Lie nilpotent symmetric elements in [Lee1] were first published in the Proceedings of the American Mathematical Society in Volume 127, Number 11, published by the American Mathematical Society. The results on Lie n-Engel symmetric elements from [Lee2] are reprinted from Communications in Algebra, Volume 28, Number 2 (2000), p. 867–881, by courtesy of Marcel Dekker Inc. The results in Chapter 5 are contained in [LeS], which will appear in Publicacions Matemàtiques. They are included with the permission of the Department of Mathematics of the Universitat Autònoma de Barcelona.

This thesis was typeset using $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX.

TABLE OF CONTENTS

Chapter 1

INTRODUCTION

Let G be a group, and R a ring with identity. The group ring, RG, is an important object of study in modern algebra. Our purpose in this thesis is to contribute some theorems concerning the structure of the group ring and its unit group, with a particular emphasis placed upon the symmetric elements.

If F is a field, then the symmetric elements of FG are those which are fixed by the natural involution, $*$, which maps each group element to its inverse. Most of our results will explore the extent to which the symmetric elements determine the structure of FG.

Chapter 2 contains necessary background material. We discuss some basic properties of groups, and some conditions on rings, and present the classical theorems which classified the group rings that satisfy the ring-theoretic conditions. We also give some basic facts about involutions and polynomial identities.

In Chapter 3, we examine some Lie properties of FG. As with any ring, we can define the Lie product via $[a, b] = ab - ba$. The group rings which are Lie nilpotent or Lie n-Engel were determined in the 1970's. However, a more recent paper by Giambruno and Sehgal showed that if G contains no 2-elements, and char $F \neq 2$, then the set of symmetric elements is Lie nilpotent if and only if FG is Lie nilpotent.

We extend this result to groups not containing an isomorphic copy of the quaternion group, Q_8. If G does contain Q_8, then FG will not be Lie nilpotent, but we show that the set of symmetric elements will be Lie nilpotent precisely when $G \simeq Q_8 \times E \times P$, where E is an elementary abelian 2-group, and P is a finite p-group, if char $F = p > 2$. We also present a similar result concerning group rings whose symmetric elements are Lie n-Engel. An element $\alpha \in FG$ is said to be skew if $\alpha^* = -\alpha$. We provide the conditions under which the skew elements are Lie n-Engel, assuming that the group contains no 2-elements, even when the characteristic is 2.

Chapter 4 looks at the unit group of a group ring, with an emphasis on the symmetric units. Let F be a field, and G a torsion group. The group rings whose unit groups satisfy a group identity have been classified in a series of papers by Giambruno-Jespers-Valenti, Giambruno-Sehgal-Valenti, Passman, Liu, and Liu-Passman. Recently, Giambruno-Sehgal-Valenti have established the conditions under which the set of symmetric units will satisfy a group identity.

Our interest lies in a particular group identity: that is, nilpotency. The groups G such that the unit group of FG is nilpotent were classified in the 1970's. Our contribution in this chapter is to classify the torsion groups G such that the symmetric units of FG are nilpotent. What we mean by this is that the symmetric units satisfy the group identity $(x_1, \dots, x_n) = 1$, for some $n \geq 2$. (Here, $(x_1, x_2) = x_1^{-1}x_2^{-1}x_1x_2$, and $(x_1, \dots, x_{n+1}) = ((x_1, \dots, x_n), x_{n+1})$.) Indeed, it turns out that if G does not contain the quaternions, then the symmetric units are nilpotent if and only if the entire unit group is nilpotent. If G does contain the quaternions, we discover that the symmetric units are nilpotent precisely when $G \simeq Q_8 \times E \times P$, where $E^2 = 1$ and P is a finite p-group. That is, precisely when the set of symmetric elements is Lie nilpotent.

Our final chapter explores an entirely different sort of problem. Here, we are examining the integral group ring, $\mathbb{Z}A$, where A is an abelian group. A famous conjecture due to Zassenhaus states that if G is a finite group, and u is a torsion unit in $\mathbb{Z}G$ of augmentation one, then u is conjugate in the rational group algebra to an element of G. This problem has been extended to matrices in the following manner. Let A be a finite abelian group, and suppose U is a torsion matrix in $GL_n(\mathbb{Z}A)$ with identity augmentation. Is U necessarily conjugate in $GL_n(\mathbb{Q}A)$ to a diagonal matrix with group elements on the diagonal?

A recent paper by Marciniak-Sehgal has given an affirmative answer for $n \leq 5$, and all A. However, Cliff-Weiss have given a counterexample for $n = 6$, and have further shown that we will obtain a positive answer for all n precisely when A has at most one non-cyclic Sylow subgroup. We examine the groups with two or more non-cyclic Sylow subgroups, and establish a condition under which we can obtain an affirmative answer to the question. We then proceed to generalize these results to arbitrary abelian groups, using the notion of stable conjugacy.

Chapter 2

PRELIMINARIES AND ASSUMED RESULTS

2.1. Group rings

The purpose of this chapter is to state some basic definitions and gather together some useful properties of groups and rings which we will need later. As the results in this chapter will tend to be of the well-known variety, we will, for the most part, simply supply references.

Let G be a group and R a ring with identity. The group ring, RG, is the set of all formal sums

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

with $\alpha_g \in R$ for all $g \in G$, and all but finitely many α_g equal to zero. Then RG is a ring with addition defined via

$$\sum_{g\in G}\alpha_g g+\sum_{g\in G}\beta_g g=\sum_{g\in G}(\alpha_g+\beta_g)g$$

and multiplication defined via

$$(\sum_{g\in G}\alpha_g g)(\sum_{h\in G}\beta_h h)=\sum_{g\in G}(\sum_{h\in G}\alpha_h\beta_{h^{-1}g})g.$$

Expressing this last formula another way,

$$(\sum_{g\in G}\alpha_g g)(\sum_{h\in G}\beta_h h)=\sum_{g\in G}\sum_{h\in G}\alpha_g\beta_h gh.$$

We identify R with the set of elements $\{r \cdot 1_G : r \in R\}$ and G with the set $\{1_R \cdot g : g \in G\}$.

Our main interests in this thesis will be the group ring, FG, where F is a field, and the integral group ring, $\mathbb{Z}G$. When F is a field, FG may also be referred to as a group algebra.

The augmentation map on RG is the function $\epsilon : RG \to R$ given by

$$\epsilon(\sum_{g \in G} \alpha_g g) = \sum_{g \in G} \alpha_g.$$

It is easily seen to be a ring homomorphism, and we write $\Delta_R(G)$ for its kernel, the augmentation ideal. We have

Lemma 2.1.1. *The augmentation ideal $\Delta_R(G)$ consists of the terms*

$$r_1(g_1 - 1) + \cdots + r_k(g_k - 1)$$

with each $r_i \in R$, each $g_i \in G$, and k a positive integer.

Proof. Clearly, if $g \in G$, then $g - 1 \in \Delta_R(G)$, and since $\Delta_R(G)$ is an ideal, it contains all of the sums of the form indicated. On the other hand, suppose $\alpha = \sum_{g \in G} \alpha_g g \in \Delta_R(G)$. Then

$$\begin{aligned} \alpha &= \sum_{g \in G} \alpha_g(g - 1) + \sum_{g \in G} \alpha_g \\ &= \sum_{g \in G} \alpha_g(g - 1) \end{aligned}$$

since $\sum_{g \in G} \alpha_g = \epsilon(\alpha) = 0$. □

Let N be a normal subgroup of G. Then the natural homomorphism $G \to G/N$ mapping g to gN induces a homomorphism $\epsilon_N : RG \to R(G/N)$. We let $\Delta_R(G, N)$ denote the kernel of ϵ_N. Notice that $\Delta_R(G) = \Delta_R(G, G)$. In a similar manner to the last lemma, we have

Lemma 2.1.2. *The ideal $\Delta_R(G,N)$ consists of the elements of the form*

$$r_1 g_1(n_1 - 1) + \cdots + r_k g_k(n_k - 1)$$

with each $r_i \in R$, $g_i \in G$, $n_i \in N$, and k a positive integer.

In particular, suppose that $N = \langle z \rangle$ is a finite normal cyclic subgroup of G. Then $\Delta_R(G,N)$ is the ideal of RG generated by the elements $z^i - 1$, for positive integers i. But $z^i - 1 = (z-1)(z^{i-1} + \cdots + z + 1)$, hence $\Delta_R(G,N) = RG(z-1)$.

2.2. Group theory

Let us recall some facts from group theory.

Let G be any group. We use round brackets to denote commutators in G; that is, $(g,h) = g^{-1}h^{-1}gh$ for any $g,h \in G$. Recursively, we define

$$(g_0, g_1, \cdots, g_{n+1}) = ((g_0, \cdots, g_n), g_{n+1}).$$

If A and B are subsets of G, then we write (A,B) for the subgroup generated by (a,b), for all $a \in A$, $b \in B$, and we let

$$(A_0, \cdots, A_{n+1}) = ((A_0, \cdots, A_n), A_{n+1}).$$

Of course, we write G' for the commutator subgroup, (G,G).

The lower central series of G is defined as follows. We let $\gamma_1(G) = G$, and for each positive integer n, $\gamma_{n+1}(G) = (\gamma_n(G), G)$. Thus

$$G = \gamma_1(G) \supseteq \gamma_2(G) \supseteq \gamma_3(G) \supseteq \cdots$$

and, in fact, it it easy to see that each $\gamma_n(G)$ is normal in G.

Let $\zeta(G)$ denote the centre of G. We also have the upper central series of G, which is defined by letting $\zeta_0(G) = 1$, and for each $n \geq 0$, letting $\zeta_{n+1}(G)$ be the unique subgroup of G, containing $\zeta_n(G)$, such that

$$\zeta_{n+1}(G)/\zeta_n(G) = \zeta(G/\zeta_n(G)).$$

Thus,

$$1 = \zeta_0(G) \subseteq \zeta_1(G) \subseteq \zeta_2(G) \subseteq \cdots$$

and again, each $\zeta_n(G)$ is normal in G. We recall the following basic fact.

Lemma 2.2.1. *Let G be a group and n a positive integer. Then the following are equivalent:*

(1) $\zeta_n(G) = G$;

(2) $\gamma_{n+1}(G) = 1$; *and,*

(3) $(g_0, g_1, \ldots, g_n) = 1$ *for all* $g_0, \ldots, g_n \in G$.

Proof. The equivalence of (1) and (2) is seen in [Rob, 5.1.9]. Clearly, (2) implies (3), since $(g_0, \ldots, g_n) \in \gamma_{n+1}(G)$ for all $g_i \in G$. Assume that (3) holds, and let us prove (1) by induction on n. If $n = 1$, then $(g_0, g_1) = 1$ for all $g_0, g_1 \in G$, hence G is abelian, as required. If $(g_0, \ldots, g_{n+1}) = 1$, then $(g_0, \ldots, g_n)$ is central, for all $g_i \in G$. Let $\bar{G} = G/\zeta(G)$. Then letting $\bar{g} = g\zeta(G) \in \bar{G}$ for any $g \in G$, we have $(\bar{g}_0, \ldots, \bar{g}_n) = \bar{1}$. Thus, by our inductive hypothesis, $\zeta_n(G/\zeta(G)) = G/\zeta(G)$. But by definition of the upper central series,

$$\zeta_n(G/\zeta(G)) = \zeta_{n+1}(G)/\zeta(G),$$

hence $G = \zeta_{n+1}(G)$, as required. □

If, for any positive integer n, G satisfies one (hence all) of the properties in Lemma 2.2.1, then G is said to be nilpotent. If n is the least integer for which this is true, then G is nilpotent of class n. (The trivial group is said to be nilpotent of class zero.)

We need a few facts about nilpotent groups. Recall that for any prime p, $g \in G$ is said to be a p-element if the order of g, $o(g)$, is a power of p, and a p'-element if $o(g)$ is finite, but not divisible by p. A p-group (resp. p'-group) is a group consisting entirely of p-elements (resp. p'-elements).

Lemma 2.2.2. *Let G be a nilpotent group. Then G has the following properties.*

(1) *Every subgroup and homomorphic image of G is nilpotent.*

(2) *The elements of finite order form a normal subgroup, T, in G. T is the restricted direct product $\prod H_p$, where H_p is the subgroup consisting of all of the p-elements in G, and the product extends over all primes p.*

(3) *If N is a nontrivial normal subgroup of G, then $N \cap \zeta(G) \neq 1$.*

(4) *If G contains a p-element, then it contains one in its centre.*

(5) *If a and b are elements with relatively prime, finite orders in G, then $ab = ba$.*

Proof. Parts (1), (2), and (3) are 5.1.4, 5.2.7, and 5.2.1 in [Rob], respectively. (4) is an immediate consequence of (2) and (3). Let us prove (5). Since $a, b \in T$, we may assume that $G = T = \prod H_p$. Let A (resp. B) be the product of those H_p for which p divides the order of a (resp. b). Then the product AB is direct, and therefore $a \in A$, $b \in B$ implies that $ab = ba$. □

We may extend the upper central series to the ordinals, and obtain

$$1 = \zeta_0(G) \subseteq \zeta_1(G) \subseteq \cdots \subseteq \zeta_\alpha(G) \subseteq \zeta_{\alpha+1}(G) \subseteq \cdots,$$

the transfinitely extended upper central series. Here,

$$\zeta_{\alpha+1}(G)/\zeta_\alpha(G) = \zeta(G/\zeta_\alpha(G))$$

and if α is a limit ordinal, then

$$\zeta_\alpha(G) = \bigcup_{\beta<\alpha} \zeta_\beta(G).$$

This series must eventually stop. That is, there exists an α such that $\zeta_\alpha(G) = \zeta_{\alpha+1}(G)$ and therefore, $\zeta_\beta(G) = \zeta_\alpha(G)$ for all $\beta > \alpha$. If $\zeta_\alpha(G) = \zeta_{\alpha+1}(G)$, then $\zeta_\alpha(G)$ is called the hypercentre of G. We say that G is hypercentral if G is its own hypercentre. Evidently, every nilpotent group is hypercentral. However, a countably infinite direct product of nilpotent groups of increasingly large nilpotency classes would be hypercentral, but not nilpotent.

Recall that for any class of groups, $\mathcal{C}$, a group G is said to be locally $\mathcal{C}$ if, for every finite subset S of G, S is contained in a subgroup of G which is in $\mathcal{C}$. Thus, a group is locally nilpotent if every finitely generated subgroup of G is nilpotent. We have

Proposition 2.2.3. *If G is hypercentral, then G is locally nilpotent.*

Proof. See [Rob, 12.2.4]. □

Next, the derived series of G is defined by taking $G^{(0)} = G$, and for each positive integer n, $G^{(n+1)} = (G^{(n)})'$. A group, G, is said to be solvable if $G^{(n)} = 1$ for some n. Clearly, every nilpotent group is solvable. We also have the following result.

Theorem 2.2.4 (Schur). *Let G be a solvable group. Suppose, for a fixed prime p and positive integer n, we have $g^{p^n} \in \zeta(G)$ for every $g \in G$. Then there exists a positive integer m such that $h^{p^m} = 1$ for every $h \in G'$.*

Proof. See [Seh1, Corollary I.4.3]. □

Recall that a group is said to have bounded exponent if there exists a positive integer n such that $g^n = 1$ for all $g \in G$. The least such n is called the exponent of G. We write $G^n = 1$. Thus, we could also state Theorem 2.2.4 by saying that if G is solvable, and $G^{p^n} \subseteq \zeta(G)$, then $(G')^{p^m} = 1$.

Of course, every finite abelian group is a direct product of cyclic groups. In fact, this extends to abelian groups of bounded exponent.

Theorem 2.2.5 (Prüfer-Baer). *Let G be an abelian group of bounded exponent. Then G is a direct product of cyclic groups.*

Proof. See [Rob, 4.3.5]. □

It is well-known that every finite p-group is nilpotent. The finiteness assumption cannot be dropped, but it can be weakened to an assertion that G' is finite. To see this, we first need the following lemma, which is also going to be useful to us.

Lemma 2.2.6. *Let G be a group, and let A be an abelian normal subgroup of G. The conjugation action of G on A forms a group of automorphisms, H, of A. Suppose that A has exponent p^n, for some prime p, and H is a finite p-group. Then there exists a positive integer r such that*

$$(A, \underbrace{G, G, \ldots, G}_{r \text{ times}}) = 1.$$

Proof. See [Sehl, Lemma V.4.1]. □

Theorem 2.2.7. *Let G be a p-group such that G' is finite. Then G is nilpotent.*

Proof. Our proof is by induction on $|G'|$. If G' is trivial, then G is abelian, and there is nothing to do. Otherwise, G' is a nontrivial nilpotent group, and we choose a positive integer i such that the i-th term of the lower central series of G', $\gamma_i(G') \neq 1$, but $\gamma_{i+1}(G') = 1$. Let $A = \gamma_i(G')$. Then A is central in G', and therefore abelian, and it is easily seen to be normal in G. Furthermore, each element of G acts by conjugation as a p-element on A (since G is a p-group). Since A is finite (being contained in G'), there are only finitely many automorphisms of A. Thus, by the last lemma,

$$(A, \underbrace{G, G, \ldots, G}_{r \text{ times}}) = 1$$

for some r. But G/A is a p-group, and $(G/A)' = G'A/A = G'/A$, hence $|(G/A)'| < |G'|$. By our inductive assumption, G/A is nilpotent, hence there exists a positive integer $t \geq 2$ such that

$$(\underbrace{G, \ldots, G}_{t \text{ times}}) \subseteq A.$$

Therefore,

$$(\underbrace{G, \ldots, G}_{r+t \text{ times}}) = 1$$

and G is nilpotent. □

Now, let G be any group. We say that g is an FC-element of G if it has only finitely many conjugates. (Clearly, any central element is an FC-element.) If g and h are FC-elements, then a conjugate of gh is of the form $k^{-1}ghk = (k^{-1}gk)(k^{-1}hk)$, hence gh has only finitely many conjugates. Also, $k^{-1}g^{-1}k = (k^{-1}gk)^{-1}$, hence g^{-1} is an FC-element, and therefore, the FC-elements form a (normal) subgroup of G, which is denoted by $\phi(G)$. G is said to be an FC-group if $G = \phi(G)$. Recall that G is said to be torsion if every element of G has finite order. The following theorem combines 5.2.18 and 14.5.8 of [Rob].

Theorem 2.2.8. *Let G be a torsion group. If G is either nilpotent or an FC-group, then G is locally finite.*

We will also require the following fundamental result about finite groups.

Theorem 2.2.9 (Schur-Zassenhaus). *Suppose N is a normal subgroup of G, where G is a finite group. If $|N|$ and $|G/N|$ are relatively prime, then G contains a subgroup H of order $|G/N|$.*

Proof. See [Rob, 9.1.2]. $\square$

In the notation of the Schur-Zassenhaus Theorem, since H and N have relatively prime orders, $H \cap N = 1$, hence $|HN| = |H| \cdot |N| = |G|$, and therefore G is the semidirect product $G = N \rtimes H$.

Finally, we recall that a group G is called a Dedekind group if every subgroup of G is normal. Certainly every abelian group is Dedekind. A Dedekind group which is not abelian is said to be Hamiltonian. These groups are described in the following result, which is [Rob, 5.3.7].

Theorem 2.2.10 (Dedekind-Baer). *The group G is Hamiltonian if and only if $G \simeq Q_8 \times E \times O$, where Q_8 is the quaternion group of order 8, E is an abelian group of exponent at most 2, and O is an abelian group, where every element of O has finite, odd order.*

We will always write Q_8 for the group

$$\langle g, h | g^4 = 1, h^2 = g^2, h^{-1}gh = g^{-1} \rangle.$$

In this section, we will gather some definitions of properties of rings, and some results concerning when these properties will hold for group rings.

Let R be a ring, and I an ideal of R. We say that I is nilpotent if there exists a natural number n such that $I^n = (0)$. That is, if and only if $\alpha_1\alpha_2\cdots\alpha_n = 0$ for all $\alpha_1, \ldots, \alpha_n \in I$. An ideal I is said to be nil if, for each $\alpha \in I$, there exists a positive integer m such that $\alpha^m = 0$. We say that the nil ideal I is nil of bounded exponent if the number m may be chosen independently of α.

The ring, R, is said to be semiprime if it has no nonzero nilpotent ideals. The semiprime group algebras have been classified. Indeed, we have

Theorem 2.3.1 (Passman). *Let F be a field and G a group. If char $F = 0$, then FG is semiprime. If char $F = p > 0$, then the following are equivalent:*

(1) *FG is semiprime;*

(2) *G has no finite normal subgroup N such that p divides $|N|$; and,*

(3) *the FC-subgroup, $\phi(G)$, contains no p-elements.*

Proof. See Theorems 4.2.12 and 4.2.13 in [Pas1]. □

We would also like to know some conditions under which the augmentation ideal will be nil or nilpotent.

Lemma 2.3.2. *Let F be a field of characteristic $p > 0$, and let G be a p-group. Then*

(1) *if G is finite, then $\Delta_F(G)$ is nilpotent, and*

(2) *if G is abelian and has bounded exponent, then $\Delta_F(G)$ is nil of bounded exponent.*

Proof. (1) Our proof is by induction on $|G|$. If $|G| = 1$, then $\Delta_F(G) = (0)$, and there is nothing to do. Otherwise, we let G be nontrivial, and assume that the result holds for smaller p-groups. We take $z \in \zeta(G)$ such that $o(z) = p$. Then letting $\bar{G} = G/\langle z \rangle$, our inductive hypothesis tells us that $\Delta_F(\bar{G})$ is nilpotent. Let us say $(\Delta_F(\bar{G}))^n = (\bar{0})$. We claim that $(\Delta_F(G))^{pn} = (0)$. Take any $\alpha_1, \dots, \alpha_{pn} \in \Delta_F(G)$. Then the augmentation of each $\bar{\alpha}_i \in F\bar{G}$ is zero, hence $\bar{\alpha}_1, \dots, \bar{\alpha}_{pn} \in \Delta_F(\bar{G})$. Thus, $\bar{\alpha}_1 \cdots \bar{\alpha}_n = \bar{0}$, which means that $\alpha_1 \cdots \alpha_n$ is in $\Delta_F(G, \langle z \rangle)$, the kernel of $FG \to F\bar{G}$. But $\Delta_F(G, \langle z \rangle) = (z-1)FG$. Therefore, $\alpha_1 \cdots \alpha_{pn} \in ((z-1)FG)^p = (z-1)^p FG$, since $z-1$ is central in FG. But $(z-1)^p = z^p - 1 = 0$, hence $(\Delta_F(G))^{pn} = (0)$, as required.

(2) Take $\alpha = \sum_{g \in G} \alpha_g g \in \Delta_F(G)$. Suppose G has exponent p^m. Then, since FG is commutative,

$$\alpha^{p^m} = \sum_{g \in G} \alpha_g^{p^m} g^{p^m} = \sum_{g \in G} \alpha_g^{p^m} = (\sum_{g \in G} \alpha_g)^{p^m} = 0^{p^m} = 0,$$

hence $\Delta_F(G)$ is nil of bounded exponent. $\square$

Let R be a ring. We say that R is prime if, for any nonzero ideals I and J, IJ is nonzero. It will be useful to know when FG is prime. We have

Theorem 2.3.3 (Connell). *Let G be a group and F a field. Then the following are equivalent:*

(1) *FG is prime;*

(2) *G has no nontrivial finite normal subgroups; and,*

(3) *$\phi(G)$ is a torsion-free abelian group.*

Proof. See [Pas1, Theorem 4.2.10]. $\square$

Now, let R be a ring with identity, and let M be a unitary left R-module. We say that M is semisimple if, for every submodule N_1, there exists a submodule

N_2 of M such that M is the direct sum $N_1 \oplus N_2$. R is said to be a semisimple ring if ${}_RR$ is a semisimple module. For any ring S, we let $M_n(S)$ denote the ring of $n \times n$ matrices with entries in S, where n is a positive integer. We record the following celebrated result, which is [Lam, Theorem 3.5].

Theorem 2.3.4 (Wedderburn-Artin). *Let R be a ring with identity. If R is semisimple, then*

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

for some natural numbers $n_1, \ldots, n_k$ and division rings $D_1, \ldots, D_k$.

This relates to group rings through the following theorem.

Theorem 2.3.5 (Maschke). *Let F be a field, and G a finite group. If char F does not divide $|G|$, then FG is semisimple.*

Proof. See [Lam, Theorem 6.1]. $\square$

Suppose R is a semisimple ring. Let us say $R = M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k)$, as in the Wedderburn-Artin Theorem. Recall that $f \in R$ is said to be an idempotent if $f^2 = f$. If f is a central idempotent in R, then $f = (f_1, \ldots, f_k)$, where each f_i is a central idempotent in $M_{n_i}(D_i)$. But then each f_i is a central scalar matrix, $\lambda_i I_{n_i} \in M_{n_i}(D_i)$, where I_{n_i} is the identity matrix, and $\lambda_i^2 = \lambda_i$. But D_i is a division ring, hence $\lambda_i = 0$ or 1. Let e_i be the identity element of $M_{n_i}(D_i)$. Then the central idempotents of R are precisely the sums of the subsets of $\{e_1, \ldots, e_k\}$. A central idempotent is called a primitive central idempotent if it is not zero, and cannot be expressed as the sum of two central idempotents of R, unless one of these is zero. Hence, we see that the primitive central idempotents of R are precisely the identity elements of the $M_{n_i}(D_i)$.

Furthermore, for each i, it is clear that $Re_i = M_{n_i}(D_i)$. These matrix rings are easily seen to be simple rings (i.e. nonzero, and containing no ideals other than (0) or $M_{n_i}(D_i)$). We call them the simple Wedderburn components of R.

Finally, let R be any ring. We use square brackets to denote the Lie product (also called the Lie bracket or Lie commutator) on R. That is,

$$[x, y] = xy - yx.$$

We also write

$$[x_1, \dots, x_n, x_{n+1}] = [[x_1, \dots, x_n], x_{n+1}]$$

for each integer $n \geq 2$. We will frequently use the following basic fact.

Lemma 2.3.6. *Let R be a ring with identity such that R has prime characteristic p. Then for any $x, y \in R$, and any integer $m \geq 0$,*

$$[x, \underbrace{y, y, \dots, y}_{p^m \text{ times}}] = [x, y^{p^m}].$$

Proof. If $m = 0$, there is nothing to do. Otherwise, let $\rho_y : R \to R$ be given by $\rho_y(\alpha) = \alpha y$, for all $\alpha \in R$, and define $\lambda_y : R \to R$ via $\lambda_y(\alpha) = y\alpha$, for all $\alpha \in R$. Then $[x, y] = \rho_y(x) - \lambda_y(x)$, and

$$[x, \underbrace{y, \dots, y}_{p^m \text{ times}}] = (\rho_y - \lambda_y)^{p^m}(x).$$

But the actions of λ_y and ρ_y are easily seen to commute. Thus, since λ_y and ρ_y are in the ring of $\mathbb{Z}$-linear functions from R to R, and this ring has characteristic p,

$$(\rho_y - \lambda_y)^{p^m}(x) = (\rho_y)^{p^m}(x) - (\lambda_y)^{p^m}(x) = xy^{p^m} - y^{p^m}x$$

and we are done. $\square$

Let R be a ring. An involution on R is a function $*: R \to R$ satisfying

$$(r+s)^* = r^* + s^*,$$
$$(rs)^* = s^* r^*, \text{ and}$$
$$(r^*)^* = r$$

for all $r, s \in R$. An element r of R is said to be symmetric (with respect to $*$) if $r^* = r$, and we write R^+ for the set of symmetric elements. On the other hand, r is said to be skew if $r^* = -r$. We write R^- for the set of skew elements. The following lemma is easy.

Lemma 2.4.1. *Let R be a ring with involution. Take any $r_1, r_2 \in R^+$, and any $s_1, s_2 \in R^-$. Then*

(1) $[r_1, r_2] \in R^-$;
(2) $[r_1, s_1] \in R^+$; *and,*
(3) $[s_1, s_2] \in R^-$.

Proof. (1) We have

$$[r_1, r_2]^* = (r_1r_2 - r_2r_1)^* = r_2^*r_1^* - r_1^*r_2^* = r_2r_1 - r_1r_2 = -[r_1, r_2].$$

The other parts are similar. □

Let F be a field and G a group. Then FG has a natural involution given by

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

We will always assume that this is our involution on FG. Clearly, an element of FG is symmetric if and only if the coefficient of g agrees with the coefficient of

g^{-1}, for all $g \in G$. Thus, the symmetric elements are the F-linear combinations of $g+g^{-1}$, for $g \in G$, and the elements of order 1 or 2. If char $F \neq 2$, and $g^2 = 1$, then $g = \frac{g+g^{-1}}{2}$, hence we need only consider the F-linear combinations of the elements $g+g^{-1}$. Similarly, when char $F \neq 2$, the skew elements are the F-linear combinations of $g - g^{-1}$, for $g \in G$. If char $F = 2$, then $(FG)^+ = (FG)^-$. The sets $(FG)^+$ and $(FG)^-$ will be of great interest to us.

Let F be a field. Then a ring R (not necessarily with identity) is said to be an F-algebra if $(R, +)$ is a unitary left F-module, and $f(rs) = (fr)s = r(fs)$ for all $r, s \in R$, and all $f \in F$. (For instance, FG is an F-algebra, for any group G.) We let $F\{x_1, x_2, \dots\}$ denote the free algebra on the countably infinite set $\{x_1, x_2, \dots\}$. That is, the elements of $F\{x_1, x_2, \dots\}$ are polynomials in the noncommuting indeterminates $x_1, x_2, \dots$. Let Λ be a subset of the F-algebra R. Then we say that Λ satisfies a polynomial identity if there exists some nonzero polynomial $f(x_1, \dots, x_n) \in F\{x_1, x_2, \dots\}$ such that $f(\lambda_1, \dots, \lambda_n) = 0$ for all $\lambda_i \in \Lambda$. For example, R is commutative if it satisfies the polynomial identity $x_1x_2 - x_2x_1$, and we say that R is Lie nilpotent if it satisfies the identity

$$[x_1, x_2, \dots, x_n]$$

for some integer $n \geq 2$. (Of course, we can also consider these last two properties for rings which are not F-algebras.)

We record the following facts, the proofs of which are immediate.

Lemma 2.4.2. *Let R be an F-algebra.*

(1) *If Λ is a subset of R which satisfies the polynomial identity f, then any subset of Λ satisfies f.*

(2) *If R satisfies the polynomial identity f, and I is any ideal of R, then R/I satisfies f.*

We will be interested in knowing when FG, $(FG)^+$ and $(FG)^-$ satisfy various polynomial identities. The earliest results in this direction were the following.

Theorem 2.4.3 (Passman). *Let F be a field and G a group. If FG satisfies a polynomial identity, then $(G : \phi(G)) < \infty$ and $|(\phi(G))'| < \infty$.*

Proof. See [Pas1, Theorem 5.2.14]. $\square$

In fact, there is a necessary and sufficient condition. Recall that, for any prime p, a group G is said to be p-abelian if G' is a finite p-group. We also take 0-abelian to mean abelian.

Theorem 2.4.4 (Isaacs-Passman, Passman). *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 contains a p-abelian subgroup of finite index.*

Proof. See Corollaries 5.3.8 and 5.3.10 in [Pas1]. $\square$

We also have this straightforward observation.

Lemma 2.4.5. *Let F be a field and G a group. Suppose $(FG)^+$ satisfies a polynomial identity f. Then*

(1) *if H is a subgroup of G, then $(FH)^+$ satisfies f, and*

(2) *if N is a normal subgroup of G, and char $F \neq 2$, then $(F(G/N))^+$ satisfies f.*

Proof. (1) is clear, since $FH \subseteq FG$. (2) The natural homomorphism $\theta : FG \to F(G/N)$ maps symmetric elements to symmetric elements. Indeed, if $\alpha = \sum_{g\in G} \alpha_g g$, then

$$\theta(\alpha^*) = \theta(\sum_{g\in G} \alpha_g g^{-1}) = \sum_{g\in G} \alpha_g g^{-1} N = (\sum_{g\in G} \alpha_g g N)^* = (\theta(\alpha))^*.$$

However, since char $F \neq 2$, the symmetric elements of $F(G/N)$ are of the form $\sum_{g\in G} \alpha_g(gN + g^{-1}N)$, with $\alpha_g \in F$. But

$$\theta(\sum_{g\in G} \alpha_g(g + g^{-1})) = \sum_{g\in G} \alpha_g(gN + g^{-1}N),$$

and since $\sum_{g\in G} \alpha_g(g + g^{-1}) \in (FG)^+$, we observe the following. Namely, if $s_1, \ldots, s_n \in (F(G/N))^+$, then $s_i = \theta(r_i)$ for some $r_i \in (FG)^+$, and therefore

$$f(s_1, \ldots, s_n) = f(\theta(r_1), \ldots, \theta(r_n)) = \theta(f(r_1, \ldots, r_n)) = \theta(0) = 0,$$

since $(FG)^+$ satisfies f. $\square$

Finally, we may define an involution on the free algebra $F\{x_1, y_1, x_2, y_2, \ldots\}$ (again with a countable infinitude of noncommuting indeterminates) by setting $x_i^* = y_i$, $y_i^* = x_i$, and extending this to an involution. We write

$$F\{x_1, x_1^*, x_2, x_2^*, \ldots\}$$

for the free algebra with involution. An element of this algebra is, of course, a polynomial in the x_i and the x_i^*, which do not commute. Suppose further that R is an F-algebra with involution. Then R is said to satisfy a $*$-polynomial identity if there exists $0 \neq f(x_1, x_1^*, x_2, x_2^*, \ldots, x_n, x_n^*) \in F\{x_1, x_1^*, \ldots\}$ such that $f(r_1, r_1^*, \ldots, r_n, r_n^*) = 0$ for all $r_1, \ldots, r_n \in R$. Then we will need the following important result.

Theorem 2.4.6 (Amitsur). *Let R be an F-algebra, and suppose that R satisfies a $*$-polynomial identity. Then R satisfies a polynomial identity.*

Proof. See [Her, p. 196]. $\square$

Chapter 3

LIE PROPERTIES OF GROUP RINGS

3.1. Background to the problem

In this chapter, we will consider two Lie properties of a ring, and establish the conditions under which the sets of symmetric or skew elements of a group ring will have these properties.

First, we recall that for any ring R, and any subset, Λ, of R, we say that Λ is Lie nilpotent if there exists an integer $n \geq 2$ such that

$$[\lambda_1, \lambda_2, \dots, \lambda_n] = 0$$

for all $\lambda_1, \dots, \lambda_n \in \Lambda$. The least such n is called the index of nilpotency of Λ. The conditions under which the group ring, FG, is Lie nilpotent were determined in the early 1970's. We record this well-known result.

Theorem 3.1.1 (Passi-Passman-Sehgal). *Let F be a field of characteristic $p \geq 0$, and let G be a group. Then FG is Lie nilpotent if and only if G is nilpotent and p-abelian.*

A version of this chapter has been published. G. T. Lee, *Group rings whose symmetric elements are Lie nilpotent*, 1999. Proceedings of the American Mathematical Society. 127: 3153–3159 and G. T. Lee, *The Lie n-Engel property in group rings*, 2000. Communications in Algebra. 28: 867–881.

Proof. See [Seh1, Theorem V.4.4]. □

For any positive integer n, we say that the subset Λ of R is Lie n-Engel provided

$$[\lambda, \underbrace{\mu, \mu, \ldots, \mu}_{n \text{ times}}] = 0$$

for all λ and μ in Λ. Clearly, if Λ is Lie nilpotent, then it is Lie n-Engel for a suitable n. However, Lie nilpotency is a stronger condition, as we see in the following result from the late 1970's.

Theorem 3.1.2 (Sehgal). *Let F be a field and G a group. Then FG is Lie n-Engel (for some n) if and only if either*

(1) *char $F = p > 0$, G is nilpotent, and G contains a normal subgroup A such that G/A and A' are both finite p-groups, or*

(2) *char $F = 0$ and G is abelian.*

Proof. See [Seh1, Theorem V.6.1]. □

In the early 1990's, a new question arose. Namely, is it sufficient to assume that $(FG)^+$ or $(FG)^-$ is Lie nilpotent in order to establish that FG is Lie nilpotent? This result was shown.

Theorem 3.1.3 (Giambruno-Sehgal). *Let F be a field of characteristic different from 2. Let G be a group containing no elements of order 2. Then the following are equivalent:*

(1) *$(FG)^+$ is Lie nilpotent;*

(2) *$(FG)^-$ is Lie nilpotent; and,*

(3) *FG is Lie nilpotent.*

Proof. This is the main result of [GS]. $\square$

This theorem cannot hold if we simply dispense with the restriction on 2-elements. To see this, we simply use

Lemma 3.1.4. *Let F be a field, and let $G = Q_8 \times E$, where E has exponent 1 or 2. Then every symmetric element in FG is central in FG.*

Proof. The symmetric elements are F-linear combinations of elements of order 2 in G, and elements of the form $x + x^{-1}$, for $x \in G$. It is easy to see that elements of order 1 or 2 in G are central, so it suffices to show that $x + x^{-1}$ is central, for all $x \in G$. But then $x = yc$, with $y \in Q_8$, $c \in E$. Then $yc + (yc)^{-1} = yc + y^{-1}c = (y + y^{-1})c$, since $c^2 = 1$ and c is central. Thus, it remains only to show that $y + y^{-1}$ is central, for all $y \in Q_8$. But this is easily verified. $\square$

In particular, then, $(FQ_8)^+$ is commutative, but if char $F \neq 2$, then FQ_8 is not even Lie n-Engel, by Theorem 3.1.2. The quaternion group, however, is the key to our work. We will show that if G does not contain an isomorphic copy of Q_8, and $(FG)^+$ is Lie nilpotent, then FG is Lie nilpotent. We will then classify the groups, G, containing Q_8, for which $(FQ_8)^+$ is Lie nilpotent.

In fact, most of the proofs in [Lee1], which concerned Lie nilpotency, only required $(FG)^+$ to be Lie n-Engel. Therefore, we will establish the conditions under which $(FG)^+$ is Lie n-Engel first, and then make the necessary modifications for Lie nilpotency.

The following interesting result was proved in [GS].

Proposition 3.1.5. *Let F be a field and G a group. If $\zeta^2(G) = \{z^2 : z \in \zeta(G)\}$ is infinite, and either $(FG)^+$ or $(FG)^-$ satisfies $[x_1, \ldots, x_n] = 0$ for some $n \geq 2$, then FG also satisfies $[x_1, \ldots, x_n] = 0$.*

This result does not hold for the Lie n-Engel property. However, we can obtain a weaker result. We need a bit of terminology.

Let R be an F-algebra with involution. Suppose that R satisfies the $*$-polynomial identity $f(x_1, x_1^*, \ldots, x_r, x_r^*)$. We write f as a sum of terms of the form $\alpha x_{i_1}^{\epsilon_1} \cdots x_{i_k}^{\epsilon_k}$, with $\alpha \in F$, each $i_j \in \{1, \ldots, r\}$, each $\epsilon_i \in \{1, *\}$, and $k \geq 0$ (where $k = 0$ gives a constant term). Each $\alpha x_{i_1}^{\epsilon_1} \cdots x_{i_k}^{\epsilon_k}$ is called a monomial. We say that a monomial is $*$-linear in x_i if precisely one of $\{x_i, x_i^*\}$ appears in the monomial. The $*$-polynomial f is said to be $*$-linear in x_i provided each monomial of f is $*$-linear in x_i. Also, f is said to be $*$-multilinear if it is $*$-linear in each of the variables that occurs in f. We need the following straightforward lemma.

Lemma 3.1.6. *Suppose $\alpha \in FG$, for any field F and group G. If, for infinitely many different $x \in G$, we have $(x-1)\alpha = 0$, then $\alpha = 0$.*

Proof. Suppose $\alpha \neq 0$. Then $\alpha = \alpha_1 g_1 + \cdots + \alpha_k g_k$, for some nonzero $\alpha_1, \ldots, \alpha_k \in F$, and pairwise distinct group elements $g_1, \ldots, g_k$. Now, $(x-1)\alpha = 0$ if and only if $(x-1)\alpha g_1^{-1} = 0$, hence we may as well assume that $g_1 = 1$. Then, for any $x \in G$, $(x-1)\alpha = 0$ implies

$$\alpha_1 x + \alpha_2 x g_2 + \cdots + \alpha_k x g_k = \alpha_1 + \alpha_2 g_2 + \cdots + \alpha_k g_k.$$

Thus, x must be one of the group elements on the right side of this expression, hence $x \in \{1, g_2, \ldots, g_k\}$. But there are only finitely many such x, and we have a contradiction. □

Now, we make an observation about $*$-polynomial identities.

Lemma 3.1.7. *Let F be a field and G a group, with $\zeta^2(G)$ infinite. Suppose FG satisfies a $*$-polynomial identity, $f(x_1, x_1^*, \ldots, x_n, x_n^*)$, which is $*$-linear in some*

x_i. Then FG satisfies g, where g is the sum of all monomials of f containing x_i (and not x_i^*).

Proof. We let $h = f - g$. Then x_i^* occurs exactly once in each monomial of h, and x_i does not occur at all. Without loss of generality, let us assume $i = 1$. Choose any $z \in \zeta(G)$. Then for any $\alpha_1, \dots, \alpha_n \in FG$,

$$\begin{aligned}
0 &= f(z\alpha_1, (z\alpha_1)^*, \alpha_2, \alpha_2^*, \dots, \alpha_n, \alpha_n^*) \\
&= g(z\alpha_1, (z\alpha_1)^*, \dots, \alpha_n, \alpha_n^*) + h(z\alpha_1, (z\alpha_1)^*, \dots, \alpha_n, \alpha_n^*) \\
&= g(z\alpha_1, z^{-1}\alpha_1^*, \alpha_2, \alpha_2^*, \dots, \alpha_n, \alpha_n^*) + h(z\alpha_1, z^{-1}\alpha_1^*, \dots, \alpha_n, \alpha_n^*) \\
&= zg(\alpha_1, \alpha_1^*, \dots, \alpha_n, \alpha_n^*) + z^{-1}h(\alpha_1, \alpha_1^*, \dots, \alpha_n, \alpha_n^*).
\end{aligned}$$

Here, we have made use of the fact that z is central, and x_1 occurs exactly once in each monomial of g, but not at all in h, and x_1^* occurs exactly once in each monomial of h, but not at all in g.

Also,

$$\begin{aligned}
0 &= z^{-1}f(\alpha_1, \alpha_1^*, \dots, \alpha_n, \alpha_n^*) \\
&= z^{-1}g(\alpha_1, \alpha_1^*, \dots, \alpha_n, \alpha_n^*) + z^{-1}h(\alpha_1, \alpha_1^*, \dots, \alpha_n, \alpha_n^*).
\end{aligned}$$

Subtracting, we obtain

$$(z - z^{-1})g(\alpha_1, \alpha_1^*, \dots, \alpha_n, \alpha_n^*) = 0$$

and therefore

$$(z^2 - 1)g(\alpha_1, \alpha_1^*, \dots, \alpha_n, \alpha_n^*) = 0$$

for all $\alpha_1, \dots, \alpha_n \in FG$, and all $z \in \zeta(G)$. Since $\zeta^2(G)$ is infinite, Lemma 3.1.6 tells us that $g(\alpha_1, \alpha_1^*, \dots, \alpha_n, \alpha_n^*) = 0$ for all $\alpha_1, \dots, \alpha_n \in FG$, as required. □

Note that we do not say that g is a $*$-polynomial identity for FG, since g could be the zero polynomial.

In particular, if $(FG)^+$ is Lie n-Engel, then FG satisfies the $*$-polynomial identity

$$[x_1 + x_1^*, \underbrace{x_2 + x_2^*, x_2 + x_2^*, \ldots, x_2 + x_2^*}_{n \text{ times}}].$$

Clearly, this is $*$-linear in x_1, but not x_2 (unless $n = 1$). Similarly, if $(FG)^-$ is Lie n-Engel, then FG satisfies

$$[x_1 - x_1^*, \underbrace{x_2 - x_2^*, \ldots, x_2 - x_2^*}_{n \text{ times}}].$$

From the last lemma, we immediately deduce

Proposition 3.1.8. *Let F be a field and G a group with $|\zeta^2(G)| = \infty$. If $(FG)^+$ (resp. $(FG)^-$) is Lie n-Engel, then FG satisfies the $*$-polynomial identity*

$$[x_1, \underbrace{x_2 + x_2^*, \ldots, x_2 + x_2^*}_{n \text{ times}}]$$

(resp.

$$[x_1, \underbrace{x_2 - x_2^*, \ldots, x_2 - x_2^*}_{n \text{ times}}]).$$

We now have

Proposition 3.1.9. *Let F be a field and G a group, with $\zeta^2(G)$ infinite. If FG satisfies a $*$-multilinear $*$-polynomial identity f, then FG satisfies g, where g is the sum of all monomials of f containing no $*$'s.*

Proof. We apply Lemma 3.1.7 to each variable in turn. □

Finally, we have the

Proof of Proposition 3.1.5. If $(FG)^+$ is Lie nilpotent, then FG satisfies the $*$-polynomial identity

$$[x_1 + x_1^*, \ldots, x_n + x_n^*].$$

This is $*$-multilinear. Hence, by Proposition 3.1.9, FG satisfies $[x_1, \ldots, x_n]$, as required.

If $(FG)^-$ is Lie nilpotent, the proof is similar. □

Since the $*$-polynomial identity we obtain when $(FG)^+$ or $(FG)^-$ is Lie n-Engel is not $*$-multilinear, we cannot conclude that FG is Lie n-Engel, even if $\zeta^2(G)$ is infinite. Indeed, this will turn out to be false, in general.

3.2. Some lemmata

We will prove a few basic properties of group rings, FG, whose symmetric elements are Lie n-Engel. Let us begin with

Lemma 3.2.1. *Let F be a field of characteristic different from 2, and let G be any group. If $(FG)^+$ is Lie n-Engel, then every element of order 2 in G is central.*

Proof. Let us assume that the characteristic of F is $p > 2$. Let y be any element of order 2 in G, and take any $x \in G$. We wish to show that $xy = yx$. Suppose, first of all, that $o(x) = 2$. Then x and y are symmetric elements of FG, and choosing m such that $p^m \geq n$, we have

$$0 = [x, \underbrace{y, \ldots, y}_{p^m \text{ times}}] = [x, y^{p^m}]$$

by Lemma 2.3.6. Since p is odd, $y^{p^m} = y$, and x commutes with y.

Now, let x have arbitrary order. Then

$$0 = [x + x^{-1}, \underbrace{y, \ldots, y}_{p^m \text{ times}}] = [x + x^{-1}, y^{p^m}]$$

for some m. Once again, this gives us $[x+x^{-1},y]=0$. Therefore,

$$xy + x^{-1}y - yx - yx^{-1} = 0,$$

and since these are just group elements, $xy = x^{-1}y$, yx, or yx^{-1}. If $xy = x^{-1}y$, then $x^2 = 1$, and the first case completes the proof. If $xy = yx$, there is nothing to do. If $xy = yx^{-1}$, then $(xy)^2 = xyxy^{-1} = 1$ and by the first case, y and xy commute. Therefore, $yxy = xy^2$, and $yx = xy$, as required.

Finally, suppose the characteristic of F is zero. In this case, F contains a copy of the integers, $\mathbb{Z}$, and $\mathbb{Z}G \subseteq FG$ in a natural way. Thus, $(\mathbb{Z}G)^+$ is Lie n-Engel. Now, every symmetric element of $(\mathbb{Z}/3\mathbb{Z})G$ is easily seen to be the image of a symmetric element of $\mathbb{Z}G$ under the standard homomorphism $\mathbb{Z}G \to (\mathbb{Z}/3\mathbb{Z})G$. Thus, $((\mathbb{Z}/3\mathbb{Z})G)^+$ is Lie n-Engel, and it follows from the characteristic 3 case that every element of order 2 in G is central. $\square$

We will frequently encounter situtations in which $[a+a^{-1}, b+b^{-1}] = 0$ for some $a, b \in G$. Expanding this expression, we are left with seven possibilities for ab. However, we can reduce this number to four. Indeed, we have

Lemma 3.2.2. *Let F be a field with char $F \neq 2$, and let G be a group such that $(FG)^+$ is Lie n-Engel. If, for some $a, b \in G$, we have $[a+a^{-1}, b+b^{-1}] = 0$, then ab is equal to one of the following: ba, $b^{-1}a$, ba^{-1} or $b^{-1}a^{-1}$.*

Proof. In the expression

$$\begin{aligned} 0 &= [a+a^{-1}, b+b^{-1}] \\ &= ab + ab^{-1} + a^{-1}b + a^{-1}b^{-1} - ba - ba^{-1} - b^{-1}a - b^{-1}a^{-1} \end{aligned}$$

the term ab must be cancelled in some manner. But these are just group elements, so ab can either agree with one of the subtracted terms, or it can agree with at least two of the added terms (since the characteristic is not 2). If it agrees with a subtracted term, then we are done. If ab agrees with two of $\{a^{-1}b, ab^{-1}, a^{-1}b^{-1}\}$, then it agrees with at least one of $\{a^{-1}b, ab^{-1}\}$. Then either $ab = a^{-1}b$ (in which case $a^2 = 1$) or $ab = ab^{-1}$ (in which case $b^2 = 1$), or possibly both. By Lemma 3.2.1, either a or b is central, hence $ab = ba$. $\square$

We will also need the following lemma, which allows us to conclude that the group contains the quaternions, under certain conditions.

Lemma 3.2.3. *Let $G = \langle a, b\rangle$, with $b^{-1}ab = a^{-1}$, and let F be a field with char $F \neq 2$. If $(FG)^+$ is Lie n-Engel, then either $a^2 = 1$ (and G is abelian) or $o(a) = 4$, $o(b) = 4t$, for some odd number t, and $\langle a, b^t\rangle \simeq Q_8$.*

Proof. If $a^2 = 1$, then $b^{-1}ab = a$, and there is nothing to do, so let us assume $a^2 \neq 1$. We begin by noting that for any integer i, $b^{-1}a^ib = a^{-i}$, hence $a^i \in \zeta(G)$ if and only if $a^{2i} = 1$. Also, $b^{-2}ab^2 = b^{-1}a^{-1}b = a$, hence $b^2 \in \zeta(G)$, but $b \notin \zeta(G)$. Assume the characteristic of F is $p > 2$. Suppose b has finite order. Since $b^2 \in \zeta(G)$, but $b \notin \zeta(G)$, b has order $2k$ for some positive integer k. If k is odd, then by Lemma 3.2.1, b^k is central, and since b^2 is central, b is central. This is impossible. Therefore, 4 divides $o(b)$. Let us write $o(b) = 2^rt$, where t is odd and $r \geq 2$. In the next argument, if $o(b) = \infty$, then we will simply let $t = 1$. Then choosing m such that $(FG)^+$ is Lie p^m-Engel, we obtain

$$0 = [ab^t + b^{-t}a^{-1}, \underbrace{b^t + b^{-t}, \dots, b^t + b^{-t}}_{p^m \text{ times}}] = [ab^t + b^{-t}a^{-1}, b^{p^mt} + b^{-p^mt}].$$

Lemma 3.2.2 gives us four possibilities for $ab^tb^{p^mt} = ab^{t(1+p^m)}$. These are:

(1) $ab^{t(1+p^m)} = b^{tp^m}ab^t$. Then $ab^{tp^m} = b^{tp^m}a$. Thus, $b^{tp^m} \in \zeta(G)$. Since tp^m is odd, the fact that $b^{tp^m} \in \zeta(G)$ and $b^2 \in \zeta(G)$ implies that $b \in \zeta(G)$. But this is false.

(2) $ab^{t(1+p^m)} = b^{t(p^m-1)}a^{-1}$. Since $b^{t(p^m-1)}$ is central (because $p^m - 1$ is even), we obtain $ab^{t(1+p^m)} = a^{-1}b^{t(p^m-1)}$. Hence $a^2 = b^{-2t}$.

(3) $ab^{t(1+p^m)} = b^{-tp^m}ab^t$. Because

$$b^{-tp^m}ab^t = b^{-tp^m}ab^{tp^m}b^{t(1-p^m)} = a^{-1}b^{t(1-p^m)},$$

we get $ab^{t(1+p^m)} = a^{-1}b^{t(1-p^m)}$. Hence $a^2 = b^{-2tp^m}$.

(4) $ab^{t(1+p^m)} = b^{-t(p^m+1)}a^{-1}$. Here, $ab^{t(1+p^m)}$ has order 2, and by Lemma 3.2.1, it is central. Since $1+p^m$ is even, $b^{t(1+p^m)} \in \zeta(G)$, and therefore a is central. But this is a contradiction.

Therefore, $a^2 = b^{-2t}$ or b^{-2tp^m}. Either way, a^2 is a power of b^2, and is therefore central. Thus, $a^4 = 1$. Since $a^2 \neq 1$, $o(a) = 4$. Thus, $b^{4tp^m} = a^{-4}$ or a^{-4p^m}, both of which are 1. This contradicts the $o(b) = \infty$ case. Furthemore, since tp^m is odd, and $o(b) = 2^rt$ for some $r \geq 2$, $o(b) = 4t$. Thus, $o(a) = o(b^t) = 4$, $a^2 = b^{-2st}$ for some odd number s (so $a^2 = b^{2t}$), and $b^{-t}ab^t = a^{-1}$. Therefore, $\langle a, b^t \rangle \simeq Q_8$.

If char $F = 0$, then $(\mathbb{Z}G)^+ \subseteq (FG)^+$, and therefore $(\mathbb{Z}G)^+$ is Lie n-Engel. Hence $((\mathbb{Z}/3\mathbb{Z})G)^+$ is Lie n-Engel, and the result now follows from the characteristic 3 case. $\square$

3.3. The case without quaternions

Having established Lemma 3.2.3, we can deal with the groups which do not contain a copy of Q_8 in much the same manner as the groups without elements of order 2 were handled in [GS].

Lemma 3.3.1. *Let $G = \langle a, b \rangle$, and suppose $[a + a^{-1}, b + b^{-1}] = 0$. If $Q_8 \not\subseteq G$, and char $F \neq 2$, then $(FG)^+$ is Lie n-Engel if and only if G is abelian.*

Proof. Suppose $[a, b] \neq 0$. By Lemma 3.2.2, $[a+a^{-1}, b+b^{-1}] = 0$ yields $ab = ba$, ba^{-1}, $b^{-1}a$ or $b^{-1}a^{-1}$. If $ab = ba$, we have a contradiction. If $ab = ba^{-1}$, then $b^{-1}ab = a^{-1}$, and Lemma 3.2.3 tells us that G contains a copy of Q_8, which is a contradiction. Similarly, if $ab = b^{-1}a$, then $a^{-1}b^{-1}a = b$, and again, we get a contradiction from Lemma 3.2.3. In the final case, $ab = b^{-1}a^{-1}$, hence $(ab)^2 = 1$, and therefore $ab \in \zeta(G)$. Thus, $a^2b = aba$, and therefore $ab = ba$. This is a contradiction.

The converse is obvious. □

Lemma 3.3.2. *Let F be a field and G a group not containing Q_8. Suppose $(FG)^+$ is Lie n-Engel. Then*

(1) *if char $F = p > 2$, then $G^{p^m} \subseteq \zeta(G)$, for some m; and,*

(2) *if char $F = 0$, then G is abelian.*

Proof. Let us prove (1). Choose m such that $p^m \geq n$. Then for any $a, b \in G$,

$$0 = [a + a^{-1}, \underbrace{b + b^{-1}, \dots, b + b^{-1}}_{p^m \text{ times}}] = [a + a^{-1}, b^{p^m} + b^{-p^m}].$$

By Lemma 3.3.1, $ab^{p^m} = b^{p^m}a$. Therefore $b^{p^m} \in \zeta(G)$.

To obtain (2), we note that for all odd primes q, since $(\mathbb{Z}G)^+$ is Lie n-Engel, $((\mathbb{Z}/q\mathbb{Z})G)^+$ is Lie n-Engel, hence $G^{q^m} \subseteq \zeta(G)$ for some m. Since this holds for different primes q, G is abelian. □

We can now classify the groups G for which $Q_8 \not\subseteq G$, and $(FG)^+$ is Lie n-Engel. We have

Theorem 3.3.3. *Suppose $Q_8 \not\subseteq G$ and char $F = p \neq 2$. Then the following are equivalent:*

(1) *$(FG)^+$ is Lie n-Engel, for some n;*

(2) *FG is Lie m-Engel, for some m; and,*

(3) *either*

   (i) $p = 0$ and G is abelian, or

(ii) $p > 2$, G is nilpotent, and there exists a normal subgroup A of G such that G/A and A' are both finite p-groups.

Proof. Obviously, (2) implies (1). Also, by Theorem 3.1.2, (2) and (3) are equivalent. Therefore, we need only show that (1) implies (3). Assume that $(FG)^+$ is Lie n-Engel. If F has characteristic zero, then by Lemma 3.3.2, G is abelian, as required. Let us assume, therefore, that char $F = p > 2$. We know that

$$[x_1 + x_1^*, \underbrace{x_2 + x_2^*, \ldots, x_2 + x_2^*}_{n \text{ times}}]$$

is a $*$-polynomial identity for FG. By Theorem 2.4.6, FG satisfies a polynomial identity. Therefore, by Theorem 2.4.3, $(G : \phi(G)) < \infty$ and $|(\phi(G))'| < \infty$. By Lemma 3.3.2, $G^{p^m} \subseteq \zeta(G)$, for some m. Since $\zeta(G) \subseteq \phi(G)$, $G/\phi(G)$ is a p-group (which we know to be finite).

To show that G is nilpotent, it will suffice to show that $H = G/\zeta(G)$ is nilpotent. Let $N = \phi(G)/\zeta(G)$. Then $H^{p^m} = 1$, and $H/N \simeq G/\phi(G)$, hence H/N is a finite p-group. Also, since $(\phi(G))'$ is finite, $N' = (\phi(G))'\zeta(G)/\zeta(G)$ is finite.

Now, H/N' acts upon N/N' by conjugation. Since H/N' is a p-group, H/N' acts as a p-group of automorphisms. Take any $h, k \in H$. If $hN = kN$, then for any $g \in N$, $(hk^{-1}, g^{-1}) \in N'$, hence $kh^{-1}ghk^{-1}g^{-1} \in N'$, and therefore $h^{-1}gh = k^{-1}gk \pmod{N'}$. Since there are only finitely many cosets of N in H, we see that H/N' acts as a finite group of automorphisms of N/N'. Since $N^{p^m} = 1$, Lemma 2.2.6 tells us that

$$(N/N', \underbrace{H/N', \ldots, H/N'}_{r \text{ times}}) = 1$$

for some r. That is,

$$(N, \underbrace{H, \ldots, H}_{r \text{ times}}) \subseteq N'.$$

Since N'/N'' is finite and H is a p-group, H/N'' acts as a finite p-group of automorphisms of N'/N''. Again, by Lemma 2.2.6,

$$(N', \underbrace{H, \ldots, H}_{s \text{ times}}) \subseteq N''$$

for some positive integer s. Therefore,

$$(N, \underbrace{H, \ldots, H}_{r+s \text{ times}}) \subseteq N''.$$

Repeating this argument, we will eventually conclude that

$$(N, \underbrace{H, \ldots, H}_{t \text{ times}}) = 1$$

for some t (since N' is nilpotent, being a finite p-group). But H/N is also nilpotent, so

$$(\underbrace{H, \ldots, H}_{u \text{ times}}) \subseteq N$$

for some $u \geq 2$, and we conclude that

$$(\underbrace{H, \ldots, H}_{t+u \text{ times}}) = 1.$$

Thus, H is nilpotent.

Now, since G is nilpotent, and $G/\zeta(G)$ is a p-group of bounded exponent by Lemma 3.3.2, it follows from Theorem 2.2.4 that G' is a p-group. In particular, then, $(\phi(G))'$ is a p-group, and we already know that it is finite. Since we have already established that $G/\phi(G)$ is a finite p-group, the theorem is proved. □

3.4. The case with quaternions

We will now proceed to classify the groups G, containing Q_8, for which $(FG)^+$ is Lie n-Engel. Recall that the quaternion group is generated by two elements, g and h, each of order 4, and we will write $Q_8 = \langle g, h \rangle$. We begin with

Lemma 3.4.1. *Let F be a field with characteristic $p > 2$. Let C be a cyclic group, and suppose that $(F(Q_8 \times C))^+$ is Lie p^m-Engel, for some $m \geq 0$. Then C has order p^v or $2p^v$ for some $0 \leq v \leq m$.*

Proof. Let us write $Q_8 = \langle g, h \rangle$, and $C = \langle c \rangle$. Then we obtain

$$\begin{aligned} 0 &= [gc + (gc)^{-1}, \underbrace{hc + (hc)^{-1}, \dots, hc + (hc)^{-1}}_{p^m \text{ times}}] \\ &= [gc + g^{-1}c^{-1}, h^{p^m}c^{p^m} + h^{-p^m}c^{-p^m}], \end{aligned}$$

since g and h commute with c. By Lemma 3.2.2, we have four cases to consider.

(1) $gh^{p^m}c^{p^m+1} = h^{p^m}gc^{p^m+1}$. Then $gh^{p^m} = h^{p^m}g$. But p^m is odd, hence h^{p^m} is not central in Q_8, which is a contradiction.

(2) $gh^{p^m}c^{p^m+1} = h^{p^m}g^{-1}c^{p^m-1}$. Thus $c^2 = h^{-p^m}g^{-1}h^{p^m}g^{-1} \in Q_8 \cap C = 1$. Therefore $c^2 = 1$, hence $c^{2p^m} = 1$.

(3) $gh^{p^m}c^{p^m+1} = h^{-p^m}gc^{1-p^m}$. Then $c^{2p^m} = h^{-p^m}g^{-1}h^{-p^m}g \in Q_8 \cap C = 1$, and $c^{2p^m} = 1$.

(4) $gh^{p^m}c^{p^m+1} = h^{-p^m}g^{-1}c^{-p^m-1}$. Then $(gh^{p^m})^2 = c^{-2(p^m+1)} \in Q_8 \cap C = 1$, and therefore $(gh^{p^m})^2 = 1$. By Lemma 3.2.1, gh^{p^m} is central in G. But p^m is odd, and neither gh nor gh^{-1} is central in Q_8.

We are done. □

Next, we show that if an element does not have order $4p^k$ for some k, then it must centralize the quaternions.

Lemma 3.4.2. *Suppose $Q_8 = \langle g, h \rangle \subseteq G$, char $F = p > 2$, and $(FG)^+$ is Lie n-Engel. If $b \in G$ and b does not centralize $\langle g, h \rangle$, then $o(b) = 4p^m$ for some $m \geq 0$, and each of $\langle b^{p^m}, g \rangle$ and $\langle b^{p^m}, h \rangle$ is either abelian or isomorphic to Q_8.*

Proof. Choosing k such that $(FG)^+$ is Lie p^k-Engel, we obtain

$$0 = [b + b^{-1}, \underbrace{g + g^{-1}, \dots, g + g^{-1}}_{p^k \text{ times}}] = [b + b^{-1}, g^{p^k} + g^{-p^k}] = [b + b^{-1}, g + g^{-1}],$$

since g has order 4. Once again, Lemma 3.2.2 reduces the problem to four cases.

(1) $bg = gb$.

(2) $bg = gb^{-1}$. Then $g^{-1}bg = b^{-1}$. Since $o(g) = 4$, Lemma 3.2.3 tells us that either $b^2 = 1$ and b is central, or $o(b) = 4$ and $\langle b, g\rangle \simeq Q_8$. This is the assertion, for g, with $m = 0$.

(3) $bg = g^{-1}b$. Then $b^{-1}gb = g^{-1}$. Since $o(g) = 4$, Lemma 3.2.3 tells us that $o(b) = 4t$ where t is odd, and $\langle g, b^t\rangle \simeq Q_8$. Furthermore, $b^{-2}gb^2 = g$, hence b^2 commutes with g, and obviously b^2 commutes with b^t as well. Hence, in particular, b^4 centralizes $\langle g, b^t\rangle$. Since b^4 has order t, which is odd, and $|\langle g, b^t\rangle| = 8$, we have $\langle b^4\rangle \cap \langle g, b^t\rangle = 1$. Thus, $\langle b, g\rangle = \langle g, b^t\rangle \times \langle b^4\rangle \simeq Q_8 \times C_t$, where C_t is the cyclic group of order t. By Lemma 3.4.1, $t = p^m$ for some m, since t is odd, and the result is proved for g.

(4) $bg = g^{-1}b^{-1}$. Then $(bg)^2 = 1$ and bg is central. Hence $b^2g = bgb$, and $bg = gb$.

Thus, either $bg = gb$ or $o(b) = 4p^m$ for some $m \geq 0$ and $\langle b^{p^m}, g\rangle$ is either abelian or Q_8. The same can be said if we replace g with h, and the proof is complete. □

The next two results narrow the possibilities down to $H \times P$, where H is a Hamiltonian 2-group and P is a p-group.

Lemma 3.4.3. *Suppose $(FG)^+$ is Lie n-Engel, where char $F = p > 2$. If $Q_8 \subseteq G$, then the 2-elements of G form a normal subgroup which is a Hamiltonian 2-group.*

Proof. Take any 2-elements $x, y \in G$. Let us say that $o(x) = 2^r$ and $o(y) = 2^t$ for some $r, t \geq 0$. Choose k such that $p^k > n$. Then since p^k is odd, it is a unit modulo 2^t. Thus, we may choose $s > 0$ such that $p^{ks} \equiv 1 \pmod{2^t}$. Let $m = ks$.

Then

$$0 = [x + x^{-1}, y^{p^m} + y^{-p^m}] = [x + x^{-1}, y + y^{-1}]$$

by our choice of m. By Lemma 3.2.2, we have four cases.

(1) $xy = yx$.

(2) $xy = yx^{-1}$. Here, $y^{-1}xy = x^{-1}$ and by Lemma 3.2.3, either x and y commute or $\langle x, y\rangle \simeq Q_8$.

(3) $xy = y^{-1}x$. Then $x^{-1}yx = y^{-1}$, and either x and y commute or $\langle x, y\rangle \simeq Q_8$.

(4) $xy = y^{-1}x^{-1}$. In this case, xy has order 2 and is therefore central. We get $yxy = xy^2$, hence $yx = xy$.

Thus, either x and y commute or the group they generate is isomorphic to Q_8. We conclude that $y^{-1}xy = x^{\pm 1}$. Thus, $\langle x\rangle$ is normal in $\langle x, y\rangle$, and by symmetry, so is $\langle y\rangle$. Therefore, $\langle x, y\rangle = \langle x\rangle\langle y\rangle$, hence $\langle x, y\rangle$ is a 2-group. That is, the 2-elements form a subgroup H whose every cyclic subgroup is normal in H. Since H is not abelian, it is Hamiltonian. Clearly H is normal in G. □

Lemma 3.4.4. *Suppose F has characteristic $p > 2$, $(FG)^+$ is Lie n-Engel, and $Q_8 = \langle g, h\rangle \subseteq G$. Then $G \simeq Q_8 \times E \times P$, where $E^2 = 1$ and P is a p-group of bounded exponent.*

Proof. Suppose there exists an element x of G whose order is either infinity or an odd prime different from p. By Lemma 3.4.2, x centralizes $\langle g, h\rangle$ and by comparing orders, we see that $\langle x\rangle \cap \langle g, h\rangle = 1$. Thus $\langle g, h, x\rangle = \langle g, h\rangle \times \langle x\rangle \simeq Q_8 \times \langle x\rangle \subseteq G$. By Lemma 3.4.1, we have a contradiction. Thus, G is torsion, and its elements have order $2^r p^t$, for some $r, t \geq 0$. By Lemma 3.4.3, the 2-elements of G form a normal subgroup, H. If we can show that the p-elements form a normal subgroup, P, then we will certainly have $G = H \times P$. By Lemma 3.4.3, H is a Hamiltonian 2-group, hence by Theorem 2.2.10, $H \simeq Q_8 \times E$, with

$E^2 = 1$. Thus all that remains is to show that the p-elements form a subgroup P of bounded exponent. (Normality of P will follow immediately.)

We know that every element has order $2^r p^t$ and since the Sylow 2-subgroup is $Q_8 \times E$, $r = 0$, 1 or 2. Let x and y be p-elements of G, and suppose $\langle x, y\rangle$ contains a 2-element, z. By Lemma 3.4.2, x and y centralize $\langle g, h\rangle$, hence z centralizes $\langle g, h\rangle$. But it is easy to verify that no element of order 4 in $Q_8 \times E$ centralizes $\langle g, h\rangle$. Thus, $o(z) = 1$ or 2. In particular, Q_8 does not lie in $\langle x, y\rangle$. But $(F\langle x, y\rangle)^+$ is Lie n-Engel, hence by Theorem 3.3.3, $F\langle x, y\rangle$ is Lie n-Engel and, in particular, $\langle x, y\rangle$ is nilpotent. Therefore, since x and y are p-elements, $\langle x, y\rangle$ is a p-group.

Thus, we know that $G \simeq Q_8 \times E \times P$, where $E^2 = 1$ and P is a p-group. If x is an element of P, then $Q_8 \times \langle x\rangle \subseteq G$. Therefore, by Lemma 3.4.1, if $(FG)^+$ is Lie p^m-Engel, then $o(x)$ divides p^m. Thus, P has bounded exponent. □

We will also need to borrow the next lemma.

Lemma 3.4.5 (Passman). *Let G be a torsion group, and F a field of characteristic $p > 0$. Let A be an abelian normal subgroup of finite index in G. Suppose I is an ideal of FA, satisfying $g^{-1}\alpha g \in I$ for all $\alpha \in I$, and all $g \in G$. If I is nil of bounded exponent, then $I(FG)$ is an ideal of FG which is nil of bounded exponent.*

Proof. See [Pas2, Lemma 3.2]. (Although the fields in that paper were assumed to be infinite, that fact was not used in the proof of Lemma 3.2.) □

We now present the main result of this section, which completes the classification of the groups G for which $(FG)^+$ is Lie n-Engel.

Theorem 3.4.6. *Let F be a field of characteristic different from 2, and let G be a group containing Q_8. Then $(FG)^+$ is Lie n-Engel for some n if and only if either*

(1) *char $F = p > 2$ and $G \simeq Q_8 \times E \times P$, where $E^2 = 1$ and P is a nilpotent p-group of bounded exponent containing a normal subgroup A of finite index such that A' is also finite; or,*

(2) *char $F = 0$ and $G \simeq Q_8 \times E$, where $E^2 = 1$.*

Proof. Let us suppose that the characteristic of F is $p > 2$. Assume $(FG)^+$ is Lie n-Engel. By Lemma 3.4.4, $G \simeq Q_8 \times E \times P$ where $E^2 = 1$ and P is a p-group of bounded exponent. But $(FP)^+$ is Lie n-Engel as well, and since $Q_8 \not\subseteq P$, we deduce from Theorem 3.3.3 that P is nilpotent and contains a normal subgroup A of finite index, such that A' is finite.

Conversely, suppose $G \simeq Q_8 \times E \times P$, where $E^2 = 1$ and P is a nilpotent p-group of bounded exponent, and that P has a normal subgroup A such that $(P : A)$ and $|A'|$ are both finite. We claim that $(FG)^+$ is Lie n-Engel, for some n. Our proof is by induction on $|A'|$.

The first step is to establish that $(FG)^+$ is Lie n-Engel when $|A'| = 1$. Thus, we are assuming that A is abelian. Since the characteristic of our field is not 2, each symmetric element is an F-linear combination of terms of the form $y + y^{-1}$, where $y \in G$. That is, it must be a sum of terms of the form $\lambda(xc + x^{-1}c^{-1})$, where $\lambda \in F$, $x \in Q_8 \times E$, and $c \in P$. But

$$\lambda(xc + x^{-1}c^{-1}) = \lambda(x + x^{-1}) + \lambda x(c - 1) + \lambda x^{-1}(c^{-1} - 1).$$

We observe that $\lambda(x+x^{-1})$ is a symmetric element in $F(Q_8 \times E)$. But by Lemma 3.1.4, every element of $(F(Q_8 \times E))^+$ is central in $F(Q_8 \times E)$, hence in FG. In addition, the terms $\lambda x(c-1)$ and $\lambda x^{-1}(c^{-1} - 1)$ are in $\Delta_F(G, P)$. Thus, an arbitrary symmetric element of FG must be of the form $\mu = \rho + \sigma$, where ρ is central in FG and $\sigma \in \Delta_F(G, P)$. It follows that for any positive integer r,

$\mu^{p^r} = \rho^{p^r} + \sigma^{p^r}$. If we can show that for a fixed r, independent of the choice of μ, we have $\sigma^{p^r} = 0$, then $\mu^{p^r} = \rho^{p^r}$ will be central in FG. In particular, for any $\nu \in (FG)^+$, we will have

$$0 = [\nu, \mu^{p^r}] = [\nu, \underbrace{\mu, \ldots, \mu}_{p^r \text{ times}}].$$

That is, $(FG)^+$ will be Lie p^r-Engel, as required.

Now, we need to show that $\Delta_F(G,P)$ is a nil ideal of bounded exponent. We first note that P/A is a finite p-group. Thus, by Lemma 2.3.2, it follows that $\Delta_F(P/A)$ is a nilpotent ideal. Let us say that $(\Delta_F(P/A))^{p^m} = (0)$. Take any $\alpha_1, \ldots, \alpha_{p^m} \in \Delta_F(P)$. Then looking at the elements $\bar{\alpha}_1, \ldots, \bar{\alpha}_{p^m} \in F\bar{P} = F(P/A)$, we see that each has augmentation zero. That is, each $\bar{\alpha}_i \in \Delta_F(P/A)$, hence $\bar{\alpha}_1 \cdots \bar{\alpha}_{p^m} = \bar{0}$. Thus, $\alpha_1 \cdots \alpha_{p^m} \in \Delta_F(P, A)$ and therefore, $(\Delta_F(P))^{p^m} \subseteq \Delta_F(P, A)$. We recall that $\Delta_F(G, P) = FG\Delta_F(P)$. Hence,

$$(\Delta_F(G, P))^{p^m} = (FG\Delta_F(P))^{p^m} \subseteq FG\Delta_F(P, A).$$

But $\Delta_F(P, A) = FP\Delta_F(A)$, so

$$\begin{aligned} FG\Delta_F(P, A) &= (FG)(FP)\Delta_F(A) = FG\Delta_F(A) \\ &= (FG)(F(E \times A))\Delta_F(A) = FG\Delta_F(E \times A, A). \end{aligned}$$

Thus, it remains only to show that $FG\Delta_F(E \times A, A)$ is nil of bounded exponent. But $E \times A$ is an abelian normal subgroup of G. Also,

$$(G : E \times A) = 8(P : A) < \infty.$$

In addition, an element of $\Delta_F(E \times A, A)$ is an F-linear combination of terms of the form $h(a-1)$, with $h \in E \times A$, and $a \in A$. If $g \in G$, then

$$g^{-1}(h(a-1))g = (g^{-1}hg)(g^{-1}ag - 1) \in \Delta_F(E \times A, A),$$

because A and $E \times A$ are normal in G. Thus, by Lemma 3.4.5, if we can show that $\Delta_F(E \times A, A)$ is a nil ideal of bounded exponent in $F(E \times A)$, then we will know that $FG\Delta_F(E \times A, A)$ is nil of bounded exponent, as required. However, $\Delta_F(E \times A, A) = F(E \times A)\Delta_F(A)$, and since $F(E \times A)$ is commutative, it will suffice to show that $\Delta_F(A)$ is nil of bounded exponent. But A is an abelian p-group of bounded exponent, hence by Lemma 2.3.2, $\Delta_F(A)$ is nil of bounded exponent. The case in which $|A'| = 1$ is complete.

Now, suppose $|A'| > 1$, and that for all groups G satisfying (1), with smaller $|A'|$, $(FG)^+$ is Lie n-Engel, for some n. Choose any $\alpha, \beta \in (FG)^+$. Also, since P is nilpotent and A' is a nontrivial normal subgroup, we may choose an element $z \in \zeta(P) \cap A'$ such that $o(z) = p$. Let us work in $F\bar{G}$, where $\bar{G} = Q_8 \times E \times (P/\langle z \rangle)$. Certainly $P/\langle z \rangle$ is a nilpotent p-group of bounded exponent. Furthermore, it contains a normal subgroup $A/\langle z \rangle$ with $(P/\langle z \rangle : A/\langle z \rangle) = (P : A) < \infty$ and

$$|(A/\langle z \rangle)'| = |A'\langle z \rangle/\langle z \rangle| = |A'/\langle z \rangle| < |A'|.$$

Thus, by our inductive assumption, $(F\bar{G})^+$ is Lie n-Engel, for some n. Choose j such that $p^j > n$. Then we have

$$\bar{0} = [\bar{\alpha}, \underbrace{\bar{\beta}, \dots, \bar{\beta}}_{p^j \text{ times}}] = [\bar{\alpha}, \bar{\beta}^{p^j}].$$

That is, $[\alpha, \beta^{p^j}]$ is in $\Delta_F(G, \langle z \rangle)$. But $\Delta_F(G, \langle z \rangle) = \Delta_F(G, \langle z^2 \rangle)$, since $o(z)$ is odd, hence $\Delta_F(G, \langle z \rangle) = (z^2 - 1)FG = (z - z^{-1})FG$. Thus, $[\alpha, \beta^{p^j}] = (z - z^{-1})\omega$, with $\omega \in FG$. But $\alpha, \beta^{p^j} \in (FG)^+$, so $[\alpha, \beta^{p^j}] \in (FG)^-$. Hence, $((z - z^{-1})\omega)^* = -(z - z^{-1})\omega$. But $z - z^{-1}$ is both skew and central, and therefore $((z - z^{-1})\omega)^* = -(z - z^{-1})\omega^*$. Thus, $(z - z^{-1})\omega = (z - z^{-1})\omega^*$ and, in fact, $(z - z^{-1})\omega = (z - z^{-1})\eta_1$, where $\eta_1 = \frac{\omega + \omega^*}{2}$ is symmetric.

Next,

$$[\alpha, \underbrace{\beta, \dots, \beta}_{2p^j \text{ times}}] = [(z - z^{-1})\eta_1, \underbrace{\beta, \dots, \beta}_{p^j \text{ times}}] = (z - z^{-1})[\eta_1, \underbrace{\beta, \dots, \beta}_{p^j \text{ times}}],$$

since $z - z^{-1}$ is central in FG. But by the same argument,

$$[\eta_1, \underbrace{\beta, \dots, \beta}_{p^j \text{ times}}] = (z - z^{-1})\eta_2$$

for some $\eta_2 \in (FG)^+$. That is,

$$[\alpha, \underbrace{\beta, \dots, \beta}_{2p^j \text{ times}}] = (z - z^{-1})^2 \eta_2,$$

for some $\eta_2 \in (FG)^+$. Iterating this procedure, we obtain

$$[\alpha, \underbrace{\beta, \dots, \beta}_{p^{j+1} \text{ times}}] = (z - z^{-1})^p \eta_p$$

for some $\eta_p \in (FG)^+$. But $(z - z^{-1})^p = 0$, and we conclude that $(FG)^+$ is Lie p^{j+1}-Engel. We are done.

If char $F = 0$, and $(FG)^+$ is Lie n-Engel, then $(\mathbb{Z}G)^+$ is Lie n-Engel. Therefore, for any odd prime q, $((\mathbb{Z}/q\mathbb{Z})G)^+$ is Lie n-Engel. Then by Lemma 3.4.4, $G \simeq Q_8 \times E \times P$, where $E^2 = 1$, and P is a q-group, for each odd prime q. Thus, $G \simeq Q_8 \times E$. In this case, $(FG)^+$ is commutative by Lemma 3.1.4, hence $(FG)^+$ is Lie n-Engel. □

3.5. Skew elements

The result of Giambruno and Sehgal (Theorem 3.1.3) showed that if $(FG)^-$ is Lie nilpotent, and G contains no elements of order 2, then FG is Lie nilpotent. We cannot extend this to groups not containing the quaternions. For example, let G be a dihedral group, say

$$G = \langle \sigma, \tau | \sigma^r = \tau^2 = (\sigma\tau)^2 = 1 \rangle,$$

where $r \geq 3$. If char $F \neq 2$, then the elements of order 1 and 2 do not appear in the support of any skew elements of FG. (That is, these elements must have coefficient zero.) But for any i, $(\sigma^i\tau)^2 = 1$, hence $(FG)^- = (F\langle\sigma\rangle)^-$, which is commutative. However, G is not even nilpotent unless it is a 2-group. Thus, by

Theorem 3.1.2, FG is not even Lie n-Engel, let alone Lie nilpotent. However, we will show that if G contains no 2-elements (excluding the identity, of course), and $(FG)^-$ is Lie n-Engel, then FG is Lie m-Engel, for some m. We begin with

Lemma 3.5.1. *Let $G = \langle a, b\rangle$ be a group satisfying $a \neq 1$ and $b^{-1}ab = a^{-1}$. If G has no 2-elements, and char $F \neq 2$, then $(FG)^-$ is not Lie n-Engel, for any n.*

Proof. Since $a^2 \neq 1$, we see that b is not central, but b^2 is. Hence, since there are no 2-elements, b has infinite order. Also, if a^i is central for some integer i, then $a^{-i} = b^{-1}a^ib = a^i$, which means that $a^{2i} = 1$. Since there are no 2-elements, $a^i = 1$. In particular, a^2 is not central.

Suppose char $F = p > 2$, and $(FG)^-$ is Lie p^m-Engel, for some $m \geq 0$. Now, $b^2 \in \zeta(G)$, and b^2 has infinite order. Thus, $(\zeta(G))^2$ is infinite. By Proposition 3.1.8, FG satisfies

$$0 = [x, \underbrace{y - y^*, \dots, y - y^*}_{p^m \text{ times}}] = [x, (y - y^*)^{p^m}].$$

Thus,

$$0 = [ab, b^{p^m} - b^{-p^m}].$$

Expanding this expression, we obtain

$$ab^{1+p^m} - ab^{1-p^m} - b^{p^m}ab + b^{-p^m}ab = 0.$$

Since these are all group elements, we have three cases to consider.

(1) $ab^{1+p^m} = ab^{1-p^m}$. Then $b^{2p^m} = 1$, hence b is torsion, which is impossible.

(2) $ab^{1+p^m} = b^{p^m}ab$. Since $1 + p^m$ is even, b^{1+p^m} is central. Thus, $b^{1+p^m}a = b^{p^m}ab$, and therefore, $ba = ab$. But a is not central, and we have a contradiction.

(3) $ab^{1+p^m} = b^{-p^m}ab$. In this case, $ab^{p^m} = b^{-p^m}a$. Since p^m is odd, we have

$$ab^{p^m} = b^{p^m}(b^{-p^m}ab^{p^m}) = b^{p^m}a^{-1}.$$

Thus, $a^2 = b^{2p^m}$, which is central. Contradiction.

Therefore, $(FG)^-$ is not Lie n-Engel, for any n.

Now, if F has characteristic zero, and $(FG)^-$ is Lie n-Engel, then so is $(\mathbb{Z}G)^-$, and therefore, $((\mathbb{Z}/3\mathbb{Z})G)^-$ is Lie n-Engel. But we just saw that this is impossible. □

Lemma 3.5.2. *Suppose $G = \langle a, b\rangle$, and $[a - a^{-1}, b - b^{-1}] = 0$. Suppose further that G has no 2-elements and F is a field of characteristic different from 2. If $(FG)^-$ is Lie n-Engel, then G is abelian.*

Proof. Suppose G is not abelian. Expanding the equality $[a - a^{-1}, b - b^{-1}] = 0$, we find that ab must be equal to at least one of the other group elements, namely

$$ab = a^{-1}b,\ ab^{-1},\ a^{-1}b^{-1},\ ba,\ ba^{-1},\ b^{-1}a, \text{ or } b^{-1}a^{-1}.$$

But G is not abelian, hence $ab \neq ba$. Also, a, b, and ab are all different from 1 (lest a and b commute). Since there are no 2-elements, a^2, b^2, and $(ab)^2$ are all different from 1 as well. Thus, $ab \neq a^{-1}b$, ab^{-1}, or $b^{-1}a^{-1}$. If $ab = ba^{-1}$, then $b^{-1}ab = a^{-1}$ and by Lemma 3.5.1, $\langle a, b\rangle$ is abelian, which is not the case. Similarly, if $ab = b^{-1}a$, then $aba^{-1} = b^{-1}$ and Lemma 3.5.1 gives a contradiction. We conclude that $ab = a^{-1}b^{-1}$. That is, $a^2 = b^{-2}$. Certainly then, $a^2 \in \zeta(G)$, but $a \notin \zeta(G)$, and since there are no 2-elements, a has infinite order. Also,

$$0 = [a - a^{-1}, b - b^{-1}] = [(1 - a^{-2})a, (1 - b^{-2})b] = (1 - a^{-2})(1 - b^{-2})[a, b]$$

since a^{-2} and b^{-2} are central. Thus, for any positive integer k,

$$(1-a^{-2k})(1-b^{-2})[a,b] = (1+a^{-2}+a^{-4}+\cdots+a^{-2(k-1)})(1-a^{-2})(1-b^{-2})[a,b] = 0.$$

Since the set $\{a^{-2k} : k \geq 1\}$ is infinite, Lemma 3.1.6 implies that $(1-b^{-2})[a,b] = 0$. By the same argument, $[a,b] = 0$. We have a contradiction. $\square$

We may now proceed as we did with the symmetric elements.

Lemma 3.5.3. *Let G be a group with no 2-elements. Suppose that char $F \neq 2$, and $(FG)^-$ is Lie n-Engel. Then*

(1) *if char $F = p > 2$, then $G^{p^m} \subseteq \zeta(G)$, for some $m \geq 0$;*

(2) *if char $F = 0$, then G is abelian.*

Proof. Suppose char $F = p > 2$, and $(FG)^-$ is Lie p^m-Engel. Take any $a, b \in G$. Then

$$0 = [a - a^{-1}, \underbrace{b - b^{-1}, \ldots, b - b^{-1}}_{p^m \text{ times}}] = [a - a^{-1}, b^{p^m} - b^{-p^m}].$$

By Lemma 3.5.2, $\langle a, b^{p^m} \rangle$ is abelian. That is, b^{p^m} is central, as required.

If char $F = 0$, then $(\mathbb{Z}G)^-$ is Lie n-Engel, and so, for any odd prime q, $((\mathbb{Z}/q\mathbb{Z})G)^-$ is Lie n-Engel. It follows from the first case that $G/\zeta(G)$ is a q-group, for each such q. Thus, $G = \zeta(G)$. $\square$

This allows us to prove our main result about skew elements. We present

Theorem 3.5.4. *Let G be a group with no 2-elements and let F be a field with characteristic $p \neq 2$. Then the following are equivalent:*

(1) *$(FG)^-$ is Lie n-Engel, for some n;*

(2) *FG is Lie m-Engel, for some m; and,*

(3) *either*

  (i) $p = 0$ and G is abelian, or

  (ii) $p > 2$, G is nilpotent, and there exists a normal subgroup A of G such that G/A and A' are both finite p-groups.

Proof. It is obvious that (2) implies (1), and by Theorem 3.1.2, (2) and (3) are equivalent. Thus, we assume that $(FG)^-$ is Lie n-Engel and prove (3). If char $F = 0$, then Lemma 3.5.3 does the job. Otherwise, since $(FG)^-$ is Lie n-Engel, FG satisfies the $*$-polynomial identity

$$[x - x^*, \underbrace{y - y^*, \ldots, y - y^*}_{n \text{ times}}].$$

Now, proceed as in the proof of Theorem 3.3.3. □

3.6. Lie nilpotent symmetric elements

Let us now turn our attention to the problem of classifying the groups, G, such that $(FG)^+$ is Lie nilpotent. If G contains no 2-elements, then this has been handled in [GS]. First, let us broaden this result to groups which do not contain a copy of the quaternions.

Theorem 3.6.1. *Let F be a field of characteristic $p \neq 2$, and let G be a group which does not contain Q_8. Then the following are equivalent:*

(1) *$(FG)^+$ is Lie nilpotent;*

(2) *FG is Lie nilpotent; and,*

(3) *G is nilpotent and p-abelian.*

Proof. Clearly, (2) implies (1), and by Theorem 3.1.1, (2) and (3) are equivalent. Thus, we have only to verify that (1) implies (3).

Since $(FG)^+$ is Lie nilpotent, it is Lie n-Engel, for a suitable n. If char $F = 0$, then by Lemma 3.3.2, G is abelian, as required. Suppose, therefore, that char $F = p > 2$. By Theorem 3.3.3, G is nilpotent. In addition, $G/\zeta(G)$ is a p-group of bounded exponent, by Lemma 3.3.2. Thus, by Theorem 2.2.4, G' is a p-group. It remains only to show that G' is finite. Suppose G contains an element x of infinite order. By Lemma 3.3.2, $x^{p^m} \in \zeta(G)$, for some m. Thus, $(\zeta(G))^2$ is infinite. By Proposition 3.1.5, FG is Lie nilpotent, hence G' is finite, as required. Thus, we may assume that G is a torsion nilpotent group. Then, by Lemma 2.2.2, G is the restricted direct product $\prod_q P_q$, where each P_q is the unique Sylow q-subgroup of G, and the product extends over all primes q. Thus, $G' = \prod_q P_q'$. Since G' is a p-group, $G' = P_p'$. Thus, we need only show that P_p' is finite. Since $(FP_p)^+$ is Lie nilpotent, we may as well assume that G is a nilpotent p-group.

Our proof is by induction on the nilpotency class of G. If G is abelian, there is nothing to do. Otherwise, $G/\zeta(G)$ has smaller nilpotency class, and by our inductive assumption, $(G/\zeta(G))'$ is finite. If $\zeta(G)$ is infinite, then since G is a p-group, $(\zeta(G))^2 = \zeta(G)$, hence $|(\zeta(G))^2| = \infty$. By Proposition 3.1.5, FG is Lie nilpotent, hence G' is finite. Finally, if $|\zeta(G)| < \infty$, then since $(G/\zeta(G))' = G'\zeta(G)/\zeta(G)$ is finite, we see that $|G'\zeta(G)| < \infty$, hence $|G'| < \infty$. We are done. □

Of course, once we reduced the problem to the p-groups, we could have resolved the situation with an appeal to Theorem 3.1.3, but we included the proof here for the sake of completeness.

Now, let us consider the groups which contain the quaternions. We have

Lemma 3.6.2. *Let F be a field of characteristic $p \neq 2$, and G a group containing Q_8 such that $(FG)^+$ is Lie nilpotent. Then*

(1) *if $p > 2$, then $G \simeq Q_8 \times E \times P$, where $E^2 = 1$ and P is a finite p-group, and*

(2) *if $p = 0$, then $G \simeq Q_8 \times E$, where $E^2 = 1$.*

Proof. Since $(FG)^+$ is Lie nilpotent, it is Lie n-Engel. Part (2) follows from Theorem 3.4.6. To prove (1), we use Theorem 3.4.6 to get $G \simeq Q_8 \times E \times P$, where

$E^2 = 1$ and P is a p-group. Now, $(FP)^+$ is Lie nilpotent, and $Q_8 \not\subseteq P$. Hence, by Theorem 3.6.1, P' is finite. If P is infinite, then P/P' is an infinite abelian p-group. Thus, $(\zeta(Q_8 \times E \times (P/P')))^2$ is infinite. Since $(F(Q_8 \times E \times (P/P')))^+$ is Lie nilpotent, by Lemma 2.4.5, we see from Proposition 3.1.5 that $F(Q_8 \times E \times (P/P'))$ is Lie nilpotent. But, since $(Q_8 \times E \times (P/P'))'$ is not a p-group, this contradicts Theorem 3.1.1. We are done. $\square$

In fact, the converse of the last lemma is true as well. In [Lee1], we showed this via a greatly simplified version of the lifting argument used in the proof of Theorem 3.4.6. However, we will reap the benefits later if we prove a slightly stronger result now.

Let R be a ring, and Λ any subset of R. We define a sequence of (associative) ideals of R as follows. Let $\Lambda_{(0)} = R$, and for each $i \geq 0$, let $\Lambda_{(i+1)}$ be the ideal generated by all of the Lie products $[\alpha, \beta]$, with $\alpha \in \Lambda_{(i)}$, $\beta \in \Lambda$. We might say that Λ is strongly Lie nilpotent if $\Lambda_{(n)} = (0)$ for some n.

Lemma 3.6.3. *Let R be a ring, and Λ any subset of R. Suppose μ is central in R, and $\Lambda_{(i)} \subseteq \mu R$, for some i. Then, for any $j \geq 0$, $\Lambda_{(i+j)} \subseteq \mu\Lambda_{(j)}$.*

Proof. Our proof is by induction on j. If $j = 0$, there is nothing to do. Otherwise, we assume that $\Lambda_{(i+j)} \subseteq \mu\Lambda_{(j)}$, and prove that $\Lambda_{(i+j+1)} \subseteq \mu\Lambda_{(j+1)}$. But $\Lambda_{(i+j+1)}$ is generated by the Lie products $[\alpha, \beta]$, where $\alpha \in \Lambda_{(i+j)}$, $\beta \in \Lambda$. However, $\Lambda_{(i+j)} \subseteq \mu\Lambda_{(j)}$, hence $\alpha = \mu\gamma$, for some $\gamma \in \Lambda_{(j)}$. Thus,

$$[\alpha, \beta] = [\mu\gamma, \beta] = \mu[\gamma, \beta] \in \mu\Lambda_{(j+1)},$$

as μ is central. Since $\Lambda_{(j+1)}$ is an ideal, we are done. $\square$

Lemma 3.6.4. *Let F be a field of characteristic $p > 2$, and let $G = Q_8 \times E \times P$, where $E^2 = 1$ and $|P| = p^m$. Then $((FG)^+)_{(p^m)} = (0)$.*

Proof. Our proof is by induction on m. If $m = 0$, then $G = Q_8 \times E$. By Lemma 3.1.4, $(F(Q_8 \times E))^+$ is central in $F(Q_8 \times E)$, hence $((F(Q_8 \times E))^+)_{(1)} = (0)$, as required. Suppose $|P| = p^{m+1}$, and the result holds for smaller P. Since P is a finite p-group, we may choose $z \in \zeta(P)$ such that $o(z) = p$. Let $\bar{G} = Q_8 \times E \times (P/\langle z\rangle)$. By our inductive assumption, $((F\bar{G})^+)_{(p^m)} = (\bar{0})$. That is,

$$((FG)^+)_{(p^m)} \subseteq \Delta_F(G, \langle z\rangle) = (z-1)FG.$$

Therefore, by Lemma 3.6.3,

$$((FG)^+)_{(2p^m)} \subseteq (z-1)((FG)^+)_{(p^m)} \subseteq (z-1)^2 FG.$$

Iterating this argument, we see that

$$((FG)^+)_{(p^{m+1})} \subseteq (z-1)^p FG = (0),$$

as required. □

Thus, if char $F = p > 2$, and $G = Q_8 \times E \times P$, where $E^2 = 1$ and $|P| = p^m$, then for any $\alpha_0, \alpha_1, \ldots, \alpha_{p^m} \in (FG)^+$, we have

$$[\alpha_0, \alpha_1, \ldots, \alpha_{p^m}] \in ((FG)^+)_{(p^m)} = (0)$$

and therefore $(FG)^+$ is Lie nilpotent. (Indeed, it is strongly Lie nilpotent.) If char $F = 0$, and G is a Hamiltonian 2-group, then $(FG)^+$ is commutative, by Lemma 3.1.4. Combining this information with Lemma 3.6.2, we have proved our second main result on groups G for which $(FG)^+$ is Lie nilpotent, namely

Theorem 3.6.5. *Let F be a field of characteristic $p \neq 2$, and let G be a group containing the quaternions. Then $(FG)^+$ is Lie nilpotent if and only if either*

(1) *$p > 2$ and $G \simeq Q_8 \times E \times P$, where $E^2 = 1$ and P is a finite p-group, or*

(2) *$p = 0$ and $G \simeq Q_8 \times E$, where $E^2 = 1$.*

3.7. The characteristic 2 case

When the characteristic of F is 2, there is no distinction between $(FG)^+$ and $(FG)^-$. The papers on the subject of symmetric elements have all avoided characteristic 2, but with a small modification to our earlier proofs, we can handle the groups containing no 2-elements. Our result is

Theorem 3.7.1. *Let F be a field of characteristic 2, and G a group containing no 2-elements. Then the following are equivalent:*

(1) *$(FG)^+$ is Lie n-Engel, for some n;*

(2) *FG is Lie m-Engel, for some m;*

(3) *$(FG)^+$ is Lie nilpotent;*

(4) *FG is Lie nilpotent; and,*

(5) *G is abelian.*

Since the implications (5) $\Rightarrow$ (4) $\Rightarrow$ (3) $\Rightarrow$ (1) and (5) $\Rightarrow$ (2) $\Rightarrow$ (1) are transparent, it will suffice to show that (1) $\Rightarrow$ (5). We start with

Lemma 3.7.2. *Let F be a field of characteristic 2. Let $G = \langle a, b \rangle$ be a group satisfying $a \neq 1$ and $b^{-1}ab = a^{-1}$. If G has no 2-elements, then $(FG)^+$ is not Lie n-Engel.*

Proof. Since $a^2 \neq 1$, and $b^{-1}ab = a^{-1}$, we have $b^2 \in \zeta(G)$, but $b \notin \zeta(G)$. As there are no 2-elements, b has infinite order. Also, if a^i is central, then

$a^{-i} = b^{-1}a^ib = a^i$, hence $a^{2i} = 1$. But G contains no 2-elements, and therefore, $a^i = 1$.

Now, suppose there exists an $m \geq 0$ such that $(FG)^+$ is Lie 2^m-Engel. Since $b^2 \in \zeta(G)$, and $o(b) = \infty$, $(\zeta(G))^2$ is infinite. By Proposition 3.1.8, FG satisfies

$$0 = [x, \underbrace{y + y^*, \ldots, y + y^*}_{2^m \text{ times}}] = [x, (y + y^*)^{2^m}].$$

Thus,

$$0 = [b, (ab^2)^{2^m} + (ab^2)^{-2^m}] = [b, a^{2^m}b^{2^{m+1}} + a^{-2^m}b^{-2^{m+1}}].$$

Therefore,

$$ba^{2^m}b^{2^{m+1}} + ba^{-2^m}b^{-2^{m+1}} + a^{2^m}b^{2^{m+1}+1} + a^{-2^m}b^{1-2^{m+1}} = 0.$$

We must cancel the first term with another group element. There are three cases.

(1) $ba^{2^m}b^{2^{m+1}} = ba^{-2^m}b^{-2^{m+1}}$. Then $a^{2^m}b^{2^{m+1}} = a^{-2^m}b^{-2^{m+1}}$, and we obtain $a^{2^{m+1}} = b^{-2^{m+2}} \in \zeta(G)$. Therefore, $a^{2^{m+1}} = 1$, and since there are no 2-elements, $a = 1$. Contradiction.

(2) $ba^{2^m}b^{2^{m+1}} = a^{2^m}b^{2^{m+1}+1}$. Then $ba^{2^m} = a^{2^m}b$, hence $a^{2^m} \in \zeta(G)$. In this case, $a^{2^m} = 1$ and therefore, $a = 1$. Again, a contradiction.

(3) $ba^{2^m}b^{2^{m+1}} = a^{-2^m}b^{1-2^{m+1}}$. However, $ba^{2^m} = a^{-2^m}b$, and therefore, $a^{-2^m}b^{1+2^{m+1}} = a^{-2^m}b^{1-2^{m+1}}$. Thus, $b^{2^{m+2}} = 1$, and b is torsion. This is also a contradiction.

Therefore, $(FG)^+$ is not Lie n-Engel. □

Having proved Lemma 3.7.2, the proofs of Lemma 3.5.2 and Lemma 3.5.3 follow verbatim for the characteristic 2 case. Thus, we have

Lemma 3.7.3. *Let G be a group with no 2-elements, and F a field of characteristic 2. If $(FG)^+$ is Lie n-Engel, then there exists an m such that $G^{2^m} \subseteq \zeta(G)$.*

Finally, we have the

Proof of Theorem 3.7.1. Suppose $(FG)^+$ is Lie n-Engel. In view of Lemma 3.7.3, we use the proof of Theorem 3.3.3 to establish that G is nilpotent. By Lemma 3.7.3 and Theorem 2.2.4, G' is a 2-group. But G has no 2-elements, and we conclude that G is abelian. □

Chapter 4

SYMMETRIC UNITS IN GROUP RINGS

4.1. Background to the problem

We now turn our attention to the unit group of FG and, in particular, the symmetric units. In any ring, R, with identity, by a unit of R we mean an element with a two-sided multiplicative inverse. We write $\mathcal{U}(R)$ for the group of units of R. If R has an involution, $*$, then we let $\mathcal{U}^+(R)$ denote the set of symmetric units. That is,

$$\mathcal{U}^+(R) = \{\alpha \in \mathcal{U}(R) : \alpha^* = \alpha\}.$$

We wish to know how the symmetric units influence the structure of the unit group of the group ring.

Let us begin with some results about $\mathcal{U}(FG)$. First of all, let H be any group. We say that H satisfies a group identity if there exists a nontrivial reduced word $w(x_1, \ldots, x_n)$ in the free group with generators $x_1, \ldots, x_n$ (for some $n \geq 1$) such that

$$w(h_1, \ldots, h_n) = 1$$

for all $h_1, \ldots, h_n \in H$. We see, for instance, that

(1) an abelian group would satisfy the identity $x_1^{-1}x_2^{-1}x_1x_2$;

A version of this chapter has been submitted for publication. G. T. Lee, *Nilpotent symmetric units in group rings*, submitted to Communications in Algebra.

(2) a group of bounded exponent would satisfy x_1^k for some $k \geq 1$; and,

(3) a nilpotent group would satisfy the identity

$$(x_1, x_2, \ldots, x_n)$$

for some $n \geq 2$.

On the other hand, a nonabelian free group does not satisfy any group identity.

Let G be a torsion group and F a field. We might wonder when $\mathcal{U}(FG)$ satisfies a group identity. The following result was conjectured by Hartley. It was established for infinite fields when char $F = 0$ or char $F = p > 0$ and G is a p'-group by Giambruno-Jespers-Valenti [GJV]. It was then extended to arbitrary torsion groups by Giambruno-Sehgal-Valenti [GSV1]. The finite field case was handled by Liu (in [Liu]).

Theorem 4.1.1. *Let G be a torsion group and F a field. If $\mathcal{U}(FG)$ satisfies a group identity, then FG satisfies a polynomial identity.*

Proof. See [Liu, Theorem 1.1]. □

In fact, Passman [Pas2] and Liu-Passman [LP] have found a necessary and sufficient condition for $\mathcal{U}(FG)$ to satisfy a group identity. (For the characteristic zero case, this had already been done in [GSV1].) These results may be summed up as follows.

Theorem 4.1.2. *Let G be a torsion group and F a field of characteristic $p \geq 0$. If $p = 0$, then $\mathcal{U}(FG)$ satisfies a group identity if and only if G is abelian. If $p > 0$, then $\mathcal{U}(FG)$ satisfies a group identity if and only if G has a p-abelian normal subgroup of finite index, and either*

(1) *G' is a p-group of bounded exponent, or*

(2) *G has bounded exponent and F is finite.*

Proof. For the characteristic zero case, see [GSV1, Lemma 2.3]. The positive characteristic case may be found in Theorems 1.1 and 1.2 of [LP]. $\square$

We are interested in one particular group identity, and that is nilpotency. The conditions under which $\mathcal{U}(FG)$ is nilpotent were determined long before the more general results on group identities were proved. The finite groups were handled by Bateman-Coleman, and the general case was dealt with by Khripta and Fisher-Parmenter-Sehgal. Their results are summarized in the next two theorems.

Theorem 4.1.3. *Let F be a field of characteristic $p > 0$, and let G be a group containing a central element of order p. Then $\mathcal{U}(FG)$ is nilpotent if and only if G is nilpotent and G' is a finite p-group.*

Proof. See [Sehl, Theorem VI.3.1]. $\square$

Now, if $\mathcal{U}(FG)$ is nilpotent, then since $\mathcal{U}(FG)$ contains G, G is nilpotent. Thus, if G contains an element of order p, it must contain such an element in its centre. Also, by Lemma 2.2.2, the torsion elements of G form a subgroup, $T(G)$. Thus, the remaining case is covered by

Theorem 4.1.4. *Let F be a field of characteristic $p \geq 0$, and let G be a group containing no p-elements (if $p > 0$). Then $\mathcal{U}(FG)$ is nilpotent if and only if G is nilpotent and either*

(1) *$T(G)$ is central in G, or*
(2) *$|F| = p$, a Mersenne prime, $T(G)$ is an abelian group of exponent $p^2 - 1$, and for all $x \in G$, and all $t \in T(G)$, $x^{-1}tx = t$ or t^p.*

Proof. See [Sehl, Theorem VI.3.6]. $\square$

We recall that a Mersenne prime is a prime of the form $2^k - 1$ for some positive integer k.

Now, if S is a subset of a group, we say that S satisfies the group identity $w(x_1, \ldots, x_n)$ if

$$w(s_1, \ldots, s_n) = 1$$

for all $s_1, \ldots, s_n \in S$. Our interest, naturally, lies in the set $\mathcal{U}^+(FG)$. The first results about $\mathcal{U}^+(FG)$ were the following, which form the main result of [GSV2].

Theorem 4.1.5 (Giambruno-Sehgal-Valenti). *Let F be an infinite field of characteristic different from 2, and G a torsion group not containing Q_8. Then $\mathcal{U}^+(FG)$ satisfies a group identity if and only if $\mathcal{U}(FG)$ satisfies a group identity.*

Theorem 4.1.6 (Giambruno-Sehgal-Valenti). *Let F be an infinite field, and G a torsion group containing Q_8. If char $F = 0$, then $\mathcal{U}^+(FG)$ satisfies a group identity if and only if G is a Hamiltonian 2-group. If char $F = p > 2$, then $\mathcal{U}^+(FG)$ satisfies a group identity if and only if G contains a p-abelian subgroup of finite index, and the p-elements of G form a normal subgroup P of G, of bounded exponent, such that G/P is a Hamiltonian 2-group.*

Our contribution in this chapter will be to classify the torsion groups, G, for which $\mathcal{U}^+(FG)$ is nilpotent, when char $F \neq 2$. Since $\mathcal{U}^+(FG)$ is not, in general, a group, we had better explain what this means.

Definition 4.1.7. *Let H be a group, and S a subset of H. Then we say that S is nilpotent provided S satisfies the group identity*

$$(x_1, x_2, \ldots, x_n)$$

for some $n \geq 2$.

We shall see later that it is easy to verify that this definition is equivalent to saying that the subgroup of H generated by S is nilpotent.

The results in [GSV2] were for infinite fields. Clearly, this restriction was necessary, since if $|F| < \infty$, and $|G| < \infty$, then $\mathcal{U}(FG)$ is a finite group, hence it certainly satisfies a group identity, and therefore $\mathcal{U}^+(FG)$ satisfies a group identity, irrespective of the structure of G. However, under the stronger hypothesis that $\mathcal{U}^+(FG)$ is nilpotent, we will be able to accommodate finite fields. Thus, we will not be able to use the results from [GSV2] directly, although we can do so if char $F = 0$. Let us dispense with that case now.

Proposition 4.1.8. *Let F be a field of characteristic zero, and G a torsion group. Then $\mathcal{U}^+(FG)$ is nilpotent if and only if G is abelian or a Hamiltonian 2-group.*

Proof. Since $|F| = \infty$ and $\mathcal{U}^+(FG)$ satisfies a group identity, Theorems 4.1.2, 4.1.5 and 4.1.6 tell us that G is abelian or a Hamiltonian 2-group. Conversely, if G is abelian or a Hamiltonian 2-group, then by Lemma 3.1.4, $(FG)^+$ is commutative, hence $\mathcal{U}^+(FG)$ is commutative, and we are done. $\square$

Thus, we need only consider fields of odd characteristic p. Our plan of attack is the following. We want to deal with finite groups first, and then generalize our results to locally finite groups. One problem we shall have to overcome will be the groups which have no finite normal subgroups at all; that is, the groups G for which FG is a prime ring. Therefore, we will tackle that problem immediately. After we have handled the locally finite groups, we will show that if $\mathcal{U}^+(FG)$ is nilpotent, then G is hypercentral, which will complete our work in this chapter.

In this section, we will eliminate the prime group rings from consideration. Our result is

Proposition 4.2.1. *Let F be a field of characteristic different from 2, and G a torsion group, such that FG is a prime ring. If $\mathcal{U}^+(FG)$ satisfies a group identity, then G is the trivial group.*

In order to prove this, we are going to need some generalizations of polynomial identities. Our discussion here will be slightly informal, and we refer the reader to [Row] for the more formal definitions.

Let R be an F-algebra with identity. Then a generalized polynomial identity (GPI) for R is a function

$$f(x_1, \dots, x_n) = \sum_{i=1}^{m} h_i(x_1, \dots, x_n),$$

where each h_i is an expression of the form

$$\alpha_0 x_{j_1} \alpha_1 x_{j_2} \cdots \alpha_{k-1} x_{j_k} \alpha_k,$$

where the x_i are noncommuting indeterminates, with each $\alpha_t \in R$, each $j_t \in \{1, \dots, n\}$, and such that

$$f(r_1, \dots, r_n) = 0$$

for all $r_1, \dots, r_n \in R$. The terms h_i are called the monomials of f. The GPI f is said to be multilinear if, for each indeterminate x_i appearing in f, x_i appears exactly once in each monomial of f. Thus, the multilinear GPI's are precisely the functions of the form

$$f(x_1, \dots, x_n) = \sum_{\sigma \in S_n} f^{\sigma}(x_1, \dots, x_n),$$

where S_n is the symmetric group on n letters, and

$$f^\sigma(x_1,\dots,x_n)=\sum_{j=1}^{a_\sigma}\alpha_{0,\sigma,j}x_{\sigma(1)}\alpha_{1,\sigma,j}x_{\sigma(2)}\cdots\alpha_{n-1,\sigma,j}x_{\sigma(n)}\alpha_{n,\sigma,j},$$

with each $\alpha_{i,\sigma,j}\in R$, each a_σ and n a positive integer, such that

$$f(r_1,\dots,r_n)=0$$

for all $r_1,\dots,r_n\in R$. This GPI is said to be nondegenerate (or proper) if, for some $\sigma\in S_n$, $f^\sigma(x_1,\dots,x_n)$ is not itself a GPI for R. Otherwise, f is said to be degenerate.

This is useful to us because of

Theorem 4.2.2 (Passman). *Let F be a field and G a group. Then FG satisfies a nondegenerate multilinear GPI if and only if $(G:\phi(G))<\infty$ and $(\phi(G))'$ is finite.*

Proof. See [Pas1, Theorem 5.3.15]. $\square$

Now, suppose R has an involution, $*$. Then a $*$-generalized polynomial identity ($*$-GPI) for R is a function

$$f(x_1,x_1^*,\dots,x_n,x_n^*)=\sum_{i=1}^{m}h_i(x_1,x_1^*,\dots,x_n,x_n^*),$$

where each h_i is an expression of the form

$$\alpha_0x_{j_1}^{\epsilon_1}\alpha_1x_{j_2}^{\epsilon_2}\cdots\alpha_{k-1}x_{j_k}^{\epsilon_k}\alpha_k,$$

with each $\alpha_t\in R$, each $j_t\in\{1,\dots,n\}$, each $\epsilon_t\in\{1,*\}$, and such that

$$f(r_1,r_1^*,\dots,r_n,r_n^*)=0$$

for all $r_1,\dots,r_n\in R$. We say that f is multilinear if, for each indeterminate x_i such that either x_i or x_i^* appears in f, we have exactly one of $\{x_i,x_i^*\}$ appearing in each monomial of f. (Thus, for instance, $x_1x_2 + x_1^*x_2$ is multilinear, but $x_1x_1^*$ is not.) In general, then, the multilinear $*$-GPI's are the functions of the form

$$f(x_1, x_1^*, \ldots, x_n, x_n^*) = \sum_{\sigma \in S_n} \sum_{\epsilon_1 \in \{1,*\}} \cdots \sum_{\epsilon_n \in \{1,*\}} f^{(\sigma,\epsilon_1,\ldots,\epsilon_n)}(x_1, x_1^*, \ldots, x_n, x_n^*)$$

such that if we let $\tau = (\sigma, \epsilon_1, \ldots, \epsilon_n)$, then

$$f^\tau(x_1, x_1^*, \ldots, x_n, x_n^*) = \sum_{j=1}^{a_\tau} \alpha_{0,\tau,j} x_{\sigma(1)}^{\epsilon_1} \alpha_{1,\tau,j} x_{\sigma(2)}^{\epsilon_2} \cdots x_{\sigma(n)}^{\epsilon_n} \alpha_{n,\tau,j}$$

with each $\alpha_{i,\tau,j} \in R$, each a_τ and n a positive integer, and such that

$$f(r_1, r_1^*, \ldots, r_n, r_n^*) = 0$$

for all $r_1, \ldots, r_n \in R$.

Suppose f is the above multilinear $*$-GPI. For each $\sigma \in S_n$, and each

$$\epsilon_1, \ldots, \epsilon_n \in \{1, *\},$$

let

$$g^{(\sigma,\epsilon_1,\ldots,\epsilon_n)}(x_1, \ldots, x_{2n})$$

be the expression obtained by replacing x_i^* with x_{n+i}, for $1 \le i \le n$, in

$$f^{(\sigma,\epsilon_1,\ldots,\epsilon_n)}(x_1, x_1^*, \ldots, x_n, x_n^*).$$

Then we say that f is nondegenerate if, for some $\sigma, \epsilon_1, \ldots, \epsilon_n$, we find that $g^{(\sigma,\epsilon_1,\ldots,\epsilon_n)}$ is not a GPI for R. (Otherwise, f is degenerate.)

Amitsur's result, that if R satisfies a $*$-polynomial identity, then it satisfies a polynomial identity, does not generalize to $*$-GPI's. However, for prime rings, everything works out.

Theorem 4.2.3 (Rowen). *Let R be an F-algebra with identity, such that R satisfies a nondegenerate multilinear $*$-GPI. If R is a prime ring, then R satisfies a nondegenerate multilinear GPI.*

Proof. See [Row, Theorem 9]. □

Therefore, we have

Corollary 4.2.4. *Let F be a field and G a torsion group such that FG is prime. If FG satisfies a nondegenerate, multilinear $*$-GPI, then G is the trivial group.*

Proof. Combining the last two theorems, we see that $(G : \phi(G)) < \infty$. Since FG is prime, Theorem 2.3.3 tells us that $\phi(G)$ is torsion-free. But G is torsion, hence $\phi(G) = 1$. Thus G is finite, hence $G = \phi(G) = 1$, as required. □

In [Row], Rowen describes a standard multilinearization process; that is, a means of obtaining a multilinear GPI from any GPI, or a multilinear $*$-GPI from any $*$-GPI. As we are interested in the form of the resulting multilinear identity, and not just its existence, we will discuss the multilinearization process. Since GPI's are a special case of $*$-GPI's, we will only discuss $*$-GPI's.

Suppose we have a $*$-GPI, $f(x_1, x_1^*, \ldots, x_n, x_n^*)$, for R. First, we want to obtain a $*$-GPI such that if either x_i or x_i^* occurs in it, then at least one of $\{x_i, x_i^*\}$ occurs in each monomial, for every i. Suppose, without loss of generality, that either x_1 or x_1^* occurs in f, but there exists a monomial h of f in which neither of these occurs. Let

$$f'(x_2, x_2^*, \ldots, x_n, x_n^*) = f(0, 0, x_2, x_2^*, \ldots, x_n, x_n^*).$$

Certainly, f' is a $*$-GPI for R, and the monomial h remains in f'. Furthermore, there are fewer indeterminates in f' than in f, so this process must stop, lest we run out of variables. Thus, we may assume that our GPI is $f(x_1, x_1^*, \ldots, x_n, x_n^*)$, and for each i, $1 \leq i \leq n$, either x_i or x_i^* (or both) will occur in each monomial of f.

In any monomial of f, the degree of the i-th indeterminate will be the sum of the degrees of x_i and x_i^*. The degree of the monomial is the sum of the degrees of all of the indeterminates, and the degree of f is the maximum of the degrees of all of the monomials. Let t be the degree of f, less n. If $t = 0$, then it is easy to see that f is multilinear (since all n indeterminates occur in each monomial). Otherwise, choose an i such that for some monomial, h, of f, h is not linear in the i-th indeterminate. That is, either x_i or x_i^* occurs twice, or both of them occur. Without loss of generality, let us say $i = 1$. Then, let

$$\begin{aligned} f''(x_1, x_1^*, \ldots, x_n, x_n^*, x_{n+1}, x_{n+1}^*) = {} & f(x_1 + x_{n+1}, x_1^* + x_{n+1}^*, x_2, x_2^*, \ldots, x_n, x_n^*) \\ & - f(x_1, x_1^*, x_2, x_2^*, \ldots, x_n, x_n^*) \\ & - f(x_{n+1}, x_{n+1}^*, x_2, x_2^*, \ldots, x_n, x_n^*). \end{aligned}$$

Clearly f'' is a $*$-GPI for R, and f'' has degree less than or equal to the degree of f. Also, we see that for each j, $1 \leq j \leq n+1$, at least one of $\{x_j, x_j^*\}$ occurs in every monomial of f''. Thus, the value t is smaller for f'' and, by induction, we may use this process to obtain a multilinear $*$-GPI for R.

As we mentioned earlier, we want to know how this process applies to particular $*$-GPI's. Suppose $f(x_1, x_1^*)$ is a $*$-GPI for R of degree n. Then

$$f''(x_1, x_1^*, x_2, x_2^*) = f(x_1 + x_2, x_1^* + x_2^*) - f(x_1, x_1^*) - f(x_2, x_2^*).$$

For each monomial of f of degree m, $f(x_1 + x_2, x_1^* + x_2^*)$ gives us 2^m monomials, obtained by replacing each $x_1^{\epsilon_i}$ with either $x_1^{\epsilon_i}$ or $x_2^{\epsilon_i}$, in every possible way, where ϵ_i is a fixed element of $\{1, *\}$. Subtracting $f(x_1, x_1^*)$ and $f(x_2, x_2^*)$, we remove those monomials containing only $x_1^{\epsilon_i}$, or only $x_2^{\epsilon_i}$. Thus, the degree of the first indeterminate of each monomial is reduced by at least one from the original f. We are going to perform this step $n-1$ times. Thus, we may ignore any monomials of degree less than n, as well as any monomials for which the degree of the first indeterminate drops by more than 1 at any given step. Therefore, we shall assume that $f(x_1, x_1^*)$ only consisted of monomials of degree n. Thus, in f'', each such monomial was replaced by n monomials, in each of which exactly one x_1 (or x_1^*) was replaced by x_2 (or x_2^*, respectively), plus some irrelevant terms. Performing this step again, each of the monomials of f'' will be replaced with $n-1$ monomials obtained by replacing exactly one x_1 (or x_1^*) with x_3 (or x_3^*, respectively). Iterating this, we obtain

Lemma 4.2.5. *Let $f(x_1, x_1^*)$ be a $*$-GPI of degree n for R. Suppose $h_1, \ldots, h_k$ are the monomials of f of degree n. Then R satisfies the multilinear $*$-GPI which is the sum of the $(n!)k$ monomials we get by replacing each h_i with the $n!$ monomials obtained by substituting each permutation of $\{x_1, \ldots, x_n\}$ for the various occurrences of x_1, leaving any and all $*$'s in place.*

For instance, if

$$f(x_1, x_1^*) = x_1 x_1^* x_1 - x_1^2,$$

then the only monomial of degree 3 is $x_1 x_1^* x_1$, and we obtain the multilinear $*$-GPI

$$\sum_{\sigma \in S_3} x_{\sigma(1)} x_{\sigma(2)}^* x_{\sigma(3)}.$$

Of course, it remains to be seen whether any of the multilinear $*$-GPI's so produced will turn out to be nondegenerate.

We will use these $*$-GPI's repeatedly, beginning with

Lemma 4.2.6. *Let F be a field and G a torsion group such that FG is prime. Suppose we have $\alpha \in F$, $a \in FG$, and a positive integer n such that*

$$(ar(\alpha - a)r^*)^n = 0$$

for all $r \in FG$. Then $a = 0$ or α.

Proof. We see that FG satisfies the $*$-GPI

$$(ax_1(\alpha - a)x_1^*)^n.$$

Multilinearizing this expression, Lemma 4.2.5 tells us that FG satisfies the multilinear $*$-GPI

$$\sum_{\sigma \in S_{2n}} ax_{\sigma(1)}(\alpha - a)x^*_{\sigma(2)} \cdots ax_{\sigma(2n-1)}(\alpha - a)x^*_{\sigma(2n)}.$$

If this is nondegenerate, then by Corollary 4.2.4, $G = 1$, in which case the result is trivial. Thus, we may assume that this $*$-GPI is degenerate. Letting $x_{2n+1} = x_1^*, \ldots, x_{4n} = x_{2n}^*$, we see that the term in which precisely the indeterminates

$$x_1, x_{2n+2}, x_3, x_{2n+4}, \ldots, x_{2n-1}, x_{4n}$$

occur, in that order, must vanish on FG. That is,

$$ax_1(\alpha - a)x_{2n+2} \cdots ax_{2n-1}(\alpha - a)x_{4n} = 0$$

for all $x_i \in FG$. But then, for any $x_0 \in FG$, we have

$$x_0ax_1(\alpha - a)x_{2n+2} \cdots ax_{2n-1}(\alpha - a)x_{4n} = 0.$$

However, letting I_1 be the ideal generated by a, and I_2 the ideal generated by $\alpha - a$, we note that an arbitrary element of $(I_1I_2)^n$ is a sum of terms of this form. Thus, $(I_1I_2)^n = (0)$. Since FG is prime, $I_1 = (0)$ or $I_2 = (0)$. That is, $a = 0$ or $\alpha - a = 0$. $\square$

As an immediate consequence, we have

Lemma 4.2.7. *If G is torsion, FG is prime, $a \in (FG)^+$, and for some $n \geq 1$, we have $(as)^n = 0$ for all $s \in (FG)^+$, then $a = 0$.*

Proof. If $r \in FG$, then $rar^* \in (FG)^+$, and therefore $(arar^*)^n = 0$. Apply Lemma 4.2.6 with $\alpha = 0$. □

Now, let us see what a group identity can do for us. First, let us restrict the form of the group identity.

Lemma 4.2.8. *Let R be an F-algebra with involution, and suppose that $\mathcal{U}^+(R)$ satisfies a group identity. Then $\mathcal{U}^+(R)$ satisfies a group identity of the form*

$$x^{i_1}y^{j_1}\cdots x^{i_k}y^{j_k}$$

with $k \geq 1$, and each exponent different from zero.

Proof. Suppose $\mathcal{U}^+(R)$ satisfies $w(x_1, \ldots, x_n)$. For any $\alpha, \beta \in \mathcal{U}^+(R)$, and any positive integer i, $\beta^i\alpha\beta^i \in \mathcal{U}^+(R)$. Thus, substituting x^iyx^i for x_i in w, we get a group identity, v, in two variables. Clearly, none of the y's will be cancelled, since w is reduced, hence v is nontrivial. Also,

$$v(x, y) = x^{i_1}y^{j_1}\cdots x^{i_k}y^{j_k}x^{i_{k+1}},$$

where $k \geq 1$, and all of the exponents are nonzero. Then conjugating by $x^{-i_{k+1}}$, $\mathcal{U}^+(R)$ satisfies

$$x^{i_1+i_{k+1}}y^{j_1}x^{i_2}y^{j_2}\cdots x^{i_k}y^{j_k}.$$

If $i_1 + i_{k+1} \neq 0$, then we are done. Otherwise, $\mathcal{U}^+(R)$ satisfies

$$y^{j_1}x^{i_2}y^{j_2}\cdots x^{i_k}y^{j_k},$$

hence it also satisfies

$$y^{j_1+j_k}x^{i_2}y^{j_2}\cdots x^{i_k}.$$

Interchanging x and y, $\mathcal{U}^+(R)$ satisfies

$$x^{j_1+j_k}y^{i_2}x^{j_2}\cdots x^{j_{k-1}}y^{i_k}$$

which is of the correct form unless $j_1 + j_k = 0$. This process must eventually stop, since the identity v is nontrivial, and we are left with an identity which is either of the proper form, or of the form x^t for some $t \neq 0$. (Substituting x^{-1} for x if necessary, we may assume $t > 0$.) In the latter case, substituting xyx for x, we see that $\mathcal{U}^+(R)$ satisfies $x(yx^2)^{t-1}yx$, hence it also satisfies $x^2(yx^2)^{t-1}y$, and we are done. $\square$

We can now place a restriction upon the square-zero elements of FG.

Lemma 4.2.9. *Suppose G is torsion, char $F \neq 2$, FG is prime and $\mathcal{U}^+(FG)$ satisfies a group identity. Then there exists a positive integer n such that for all $a \in FG$ with $a^2 = 0$, we have $(a^*a)^n = 0$.*

Proof. By Lemma 4.2.8, we may assume that $\mathcal{U}^+(FG)$ satisfies the group identity $w(x,y) = x^{i_1}y^{j_1}\cdots x^{i_k}y^{j_k}$, where $k \geq 1$ and all of the exponents are nonzero. Replacing x with x^{-1} or y with y^{-1} if necessary, we may also assume that $i_1 > 0$ and $j_k < 0$.

Take $a \in FG$ such that $a^2 = 0$. Then $(1+a)(1+a^*), (1+a^*)(1+a) \in \mathcal{U}^+(FG)$, hence

$$\begin{aligned} 1 &= w((1+a)(1+a^*), (1+a^*)(1+a)) \\ &= ((1+a)(1+a^*))^{i_1}\cdots((1+a^*)(1+a))^{j_k}. \end{aligned}$$

Expanding this expression, and noting that $(1+a)^{-1} = 1-a$ and $(1+a^*)^{-1} = 1-a^*$, we obtain a product of terms of the form $1 \pm a$ and $1 \pm a^*$, with no more than 2 consecutive $1 \pm a$ terms and no more than 2 consecutive $1 \pm a^*$ terms.

Also, $1 + a$ and $1 - a$ are never consecutive, and neither are $1 + a^*$ and $1 - a^*$. That is, we have an expression of the form

$$1 = (1 + a)(1 + \lambda_1 a^*)(1 + \lambda_2 a)(1 + \lambda_3 a^*) \cdots (1 + \lambda_m a)(1 - a^*)$$

where each $\lambda_i \in \{\pm 1, \pm 2\}$, and the first and last terms are correct, since $i_1 > 0$, $j_k < 0$.

Now, expanding this expression, and discarding all terms containing a^2 or $(a^*)^2$, we get a sum of terms of the form $\pm 2^b (a^*)^{\mu_1} (aa^*)^q a^{\mu_2}$, where $q \geq 0$, $b \geq 0$, and each $\mu_i \in \{0, 1\}$. Multiplying on the left by a^*, the terms in which $\mu_1 = 1$ yield $(a^*)^2$ on the left, and we discard these terms. Then, multiplying on the right by a, the terms in which $\mu_2 = 1$ give a^2 on the right, and we discard these terms as well. Thus, we are left with a polynomial in a^*a. Furthermore, in the expression $(1 + a)(1 + \lambda_1 a^*) \cdots (1 - a^*)$, the only term of highest degree is $-\lambda_1 \cdots \lambda_m aa^* \cdots aa^*$. Since each λ_i is ± 1 or ± 2, and the characteristic is not 2, this is not the zero monomial, and since $\mu_1 = \mu_2 = 0$ for this monomial, we did not discard it when we multiplied by a^* on the left and a on the right, so this polynomial is not trivial.

Thus, there exists a nonzero polynomial $f(x) = \sum_{i=1}^{d} \rho_i x^i$, $d > 0$, $\rho_i \in F$, $\rho_d = 1$, such that $f(a^*a) = 0$ for all $a \in FG$ such that $a^2 = 0$. (Since the case $a = 0$ must be considered, there is no constant term.) In particular, if $y \in FG$, then $(aya)^2 = 0$, and therefore

$$0 = f(a^*y^*a^*aya) = \sum_{i=1}^{d} \rho_i (a^*y^*a^*aya)^i.$$

Multilinearizing this expression, Lemma 4.2.5 reveals that FG satisfies the multilinear $*$-GPI

$$\sum_{\sigma \in S_{2d}} a^* y^*_{\sigma(1)} a^* a y_{\sigma(2)} a \cdots a^* y^*_{\sigma(2d-1)} a^* a y_{\sigma(2d)} a.$$

If this is nondegenerate, then by Corollary 4.2.4, $G = 1$, and there is nothing to do. Let us assume, therefore, that the expression is degenerate for all $a \in FG$

with $a^2 = 0$. Substituting $y_{2d+1} = y_1^*, \dots, y_{4d} = y_{2d}^*$, we know that FG must satisfy the term in which the indeterminates

$$y_{2d+1}, y_2, y_{2d+3}, y_4, \cdots, y_{4d-1}, y_{2d}$$

occur, in that order. That is,

$$a^* y_{2d+1} a^* a y_2 a a^* y_{2d+3} a^* \cdots a y_{2d} a = 0$$

for all $y_i \in FG$. Letting $y_{2d+1} = y_{2d+3} = \cdots = a$, and $y_2 = y_4 = \cdots = a^*$, we get $(a^* a)^{3d} = 0$, as required. □

Lemma 4.2.10. *Suppose G is torsion, char $F \neq 2$, FG is prime and $\mathcal{U}^+(FG)$ satisfies a group identity. Then there exists a positive integer n such that if $s, t \in (FG)^+$ and $s^2 = t^2 = 0$, then $(stsd)^n = 0$ for all $d \in (FG)^+$.*

Proof. By Lemma 4.2.8, we may assume that $\mathcal{U}^+(FG)$ satisfies the group identity $w(x, y) = x^{i_1} y^{j_1} \cdots x^{i_k} y^{j_k}$, where $k \geq 1$ and all of the exponents are nonzero. Take any $s, t \in (FG)^+$, such that $s^2 = t^2 = 0$. Then $(1 + s)(1 + t)(1 + s)$ and $(1 + t)(1 + s)(1 + t)$ are symmetric units. Indeed, $((1 + s)(1 + t)(1 + s))^{-1} = (1-s)(1-t)(1-s)$. Then we obtain $1 = w((1+t)(1+s)(1+t), (1+s)(1+t)(1+s))$, which is a product of terms of the form $1 \pm s$ and $1 \pm t$, with no more than two consecutive identical terms. Also, $1 + s$ and $1 - s$ do not occur together, nor do $1 + t$ and $1 - t$. Just as we did in the proof of Lemma 4.2.9, we obtain a nontrivial polynomial $f(x) = \sum_{i=1}^{c} \rho_i x^i$, where $\rho_i \in F$ for all i, and $\rho_c = 1$, such that $f(st) = 0$ if $s, t \in (FG)^+$, $s^2 = t^2 = 0$. This polynomial depends only upon the group identity.

In particular, if $y \in FG$, then $s(y + y^*)s, t(y + y^*)t \in (FG)^+$, and

$$(s(y + y^*)s)^2 = (t(y + y^*)t)^2 = 0.$$

Thus,

$$0 = f(s(y+y^*)st(y+y^*)t) = \sum_{i=1}^{c} \rho_i (s(y+y^*)st(y+y^*)t)^i.$$

Multilinearizing this expression, we discover that FG satisfies the multilinear $*$-GPI

$$\sum_{\sigma \in S_{2c}} \sum_{\epsilon_i \in \{1,*\}} s y_{\sigma(1)}^{\epsilon_1} s t y_{\sigma(2)}^{\epsilon_2} t \cdots t y_{\sigma(2c)}^{\epsilon_{2c}} t$$

If this is nondegenerate, then by Corollary 4.2.4, $G = 1$, and the result holds. Thus, we may assume that this $*$-GPI is degenerate for all $s, t \in (FG)^+$ satisfying $s^2 = t^2 = 0$. Substituting $y_{2c+1} = y_1^*, \ldots, y_{4c} = y_{2c}^*$, we know that the term in which the indeterminates $y_1, y_2, \ldots, y_{2c}$ occur, in that order, must vanish on FG. That is, FG satisfies $sy_1sty_2tsy_3s \cdots ty_{2c}t$. Let $y_1 = y_3 = \cdots = y_{2c-1} = t$, and $y_2 = y_4 = \cdots = y_{2c} = s$. Then we obtain $(st)^{3c} = 0$.

Finally, take any $d \in (FG)^+$. Then $(sds)^2 = 0$, and $sds \in (FG)^+$, hence by the result we have just seen, $(tsds)^{3c} = 0$. Therefore, $(stsd)^{3c+1} = 0$, as required. □

Now, let us restrict the nilpotent elements of $(FG)^+$. (Here, of course, we mean an element t such that $t^k = 0$, for some k.)

Lemma 4.2.11. *Suppose char $F \neq 2$, G is torsion, FG is prime and $\mathcal{U}^+(FG)$ satisfies a group identity. Let $s \in (FG)^+$ satisfy $s^2 = 0$, and let t be a nilpotent element of $(FG)^+$. Then $sts = 0$.*

Proof. Let m be the smallest positive integer such that $t^m = 0$. Our proof is by induction on m. If $m = 1$, there is nothing to do. If $m = 2$, then $t^2 = 0$, hence by Lemma 4.2.10, $(stsd)^n = 0$ for all $d \in (FG)^+$. Therefore, by Lemma 4.2.7, $sts = 0$, as required. Now, suppose $m > 2$. Then $2(m-1) > m$, hence $(t^2)^{m-1} = 0$. Thus, by our inductive hypothesis, $st^2s = 0$. For any $d \in (FG)^+$, $tsdst \in (FG)^+$, and $(tsdst)^2 = tsd(st^2s)dst = 0$. By the $m = 2$ case, $stsdsts = 0$.

Thus, $(stsd)^2 = 0$ for all $d \in (FG)^+$, and by Lemma 4.2.7, $sts = 0$. We are done. $\square$

Next, we show that the symmetric idempotents of FG must be trivial.

Lemma 4.2.12. *Suppose G is torsion and char $F \neq 2$. If FG is prime and $\mathcal{U}^+(FG)$ satisfies a group identity, then the only symmetric idempotents of FG are 0 and 1.*

Proof. Let $f \in (FG)^+$ be an idempotent. Then since $(f-1)f = 0$, for any $r \in FG$, we have $(fr(f-1))^2 = 0$. Of course, $((fr(f-1))^*)^2 = 0$, and therefore Lemma 4.2.9 implies that there exists an n such that $(fr(f-1)(fr(f-1))^*)^n = 0$. That is,

$$0 = (fr(f-1)^2 r^* f)^n = (fr(1-f)r^* f)^n,$$

since f is a symmetric idempotent. Again, since $f^2 = f$, it follows that

$$(fr(1-f)r^*)^{n+1} = 0$$

for all $r \in FG$. By Lemma 4.2.6, $f = 0$ or 1. $\square$

This allows us to eliminate the prime case entirely. We close the section with the

Proof of Proposition 4.2.1. If char $F = 0$, then by Theorems 4.1.2, 4.1.5 and 4.1.6, G is abelian or a Hamiltonian 2-group. Any such torsion group certainly has a nontrivial finite normal subgroup, unless G=1, hence by Theorem 2.3.3, FG is not prime unless $G = 1$. Thus, we may assume char $F = p > 2$. Suppose G has a p'-element, x. Letting $\hat{x} = \sum_{i=1}^{o(x)} x$, we see that $\frac{1}{o(x)}\hat{x}$ is a symmetric idempotent of FG. Thus, by Lemma 4.2.12, $x = 1$, and therefore G is a p-group.

If $G \neq 1$, take $g \in G$ such that $o(g) = p$. Also, take any $h \in G$, say $o(h) = p^t$. Then $(\hat{g})^2 = 0$, and $(h+h^{-1}-2)^{p^t} = 0$. Clearly, $\hat{g}$ and $h+h^{-1}-2$ are symmetric. Thus, by Lemma 4.2.11,

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

and expanding this, we obtain

$$\hat{g}h\hat{g} + \hat{g}h^{-1}\hat{g} = 0,$$

since $(\hat{g})^2 = 0$. Write this as a sum of group elements. If the elements appearing in $\hat{g}h\hat{g}$ are pairwise distinct, and so are the elements appearing in $\hat{g}h^{-1}\hat{g}$, then each group element appears at most twice. But char $F > 2$, so we do not get zero, and this is a contradiction. Suppose, then, that two elements appearing in $\hat{g}h\hat{g}$ agree. Let us say

$$g^a h g^b = g^c h g^d,$$

where a, b, c, d are integers, with $0 \leq a, b, c, d < p$, and either $a \neq c$ or $b \neq d$. Then

$$(g^c h)^{-1} g^a h = g^d (g^b)^{-1},$$

hence

$$h^{-1} g^{a-c} h = g^{d-b}.$$

If $a = c$, then $g^{d-b} = 1$, hence $b = d$ as well, and we have a contradiction. Thus, $a - c \neq 0$. Since $-p < a - c < p$ and $a - c \neq 0$, and since g has prime order p, we have $\langle g^{a-c} \rangle = \langle g \rangle$. Thus, $g = (g^{a-c})^m$ for some m, and therefore, h normalizes $\langle g \rangle$. If two elements appearing in $\hat{g}h^{-1}\hat{g}$ agree, then h^{-1} normalizes $\langle g \rangle$, hence h normalizes $\langle g \rangle$. But h was arbitrary, and therefore, G has a nontrivial finite normal subgroup, $\langle g \rangle$. This contradicts Theorem 2.3.3, since FG is prime. $\square$

Our goal here is to classify the finite groups G such that $\mathcal{U}^+(FG)$ is nilpotent. We will, in fact, prove a slightly stronger result, namely

Proposition 4.3.1. *Let G be a locally finite group, and F a field of characteristic $p > 2$. Suppose $\mathcal{U}^+(FG)$ is nilpotent. Then $G \simeq P \times A$, where P is a p-group, and A is a p'-group, such that A is abelian or a Hamiltonian 2-group.*

In fact, for finite groups G of the form $P \times A$ described in the proposition, we will see in §4.5 that $\mathcal{U}^+(FG)$ is nilpotent. We mentioned earlier that if a subset of a group is nilpotent, then the subgroup generated by that subset is a nilpotent group. Let us prove this fact now.

Lemma 4.3.2. *Let H be a group and X a subset of H which generates H. If, for some $n \geq 2$, $(x_1, x_2, \ldots, x_n) = 1$ for all $x_1, \ldots, x_n \in X$, then $(h_1, h_2, \ldots, h_n) = 1$ for all $h_1, \ldots, h_n \in H$.*

Proof. Our proof is by induction on n. If $n = 2$, then the $x_i \in X$ commute and since they generate H, H is abelian. Suppose our result holds for n, and that $(x_1, \ldots, x_{n+1}) = 1$ for all $x_i \in X$. Then for every $x_1, \ldots, x_n \in X$, $(x_1, \ldots, x_n)$ commutes with every $x_{n+1} \in X$, hence with $\langle X \rangle = H$. Thus, $(x_1, \ldots, x_n) \in \zeta(H)$. Let $\bar{H} = H/\zeta(H)$. Then $(\bar{x}_1, \ldots, \bar{x}_n) = \bar{1}$, for all $\bar{x}_i \in \bar{X}$. But $\langle \bar{X} \rangle = \bar{H}$, and our inductive assumption guarantees that $(\bar{h}_1, \ldots, \bar{h}_n) = \bar{1}$ for all $\bar{h}_i \in \bar{H}$. That is, $(h_1, \ldots, h_n) \in \zeta(H)$, hence $(h_1, \ldots, h_n, h_{n+1}) = 1$ for all $h_i \in H$. □

We also need the following result. If S is a subset of a ring R, then its (left) annihilator is the set

$$\mathcal{A}(S) = \{r \in R : rs = 0 \text{ for all } s \in S\}.$$

If H is any finite subgroup of G, then we write $\hat{H} = \sum_{h \in H} h \in FG$.

Lemma 4.3.3. *Let N be a normal subgroup of G, and F a field. If $|N| = \infty$, then the annihilator of $\Delta_F(G, N)$ is $\{0\}$. If $|N| < \infty$, then the annihilator of $\Delta_F(G, N)$ is $(FG)\hat{N}$, and the annihilator of $\hat{N}$ is $\Delta_F(G, N)$.*

Proof. See [Seh1, Proposition III.4.18]. □

In [Pas2, Lemma 2.1], it was shown that if $\mathcal{U}(FG)$ satisfies a group identity w, then for any normal subgroup N of G, $\mathcal{U}(F(G/N))$ satisfies w as well. In [GSV2, Remark 4], it was observed that a similar proof works for $\mathcal{U}^+(FG)$. But these proofs depended upon knowing some properties of G which were deduced from the fact that $\mathcal{U}(FG)$ or $\mathcal{U}^+(FG)$ satisfies a group identity. In particular, in [GSV2], they implicitly used the infinitude of field elements. We will eventually see that if $\mathcal{U}^+(FG)$ satisfies $(x_1, \ldots, x_n)$ for some $n \geq 2$, then so does $\mathcal{U}^+(F(G/N))$ (for torsion groups G and fields F of characteristic different from 2). For now, we have

Lemma 4.3.4. *Let G be a group, and F a field of characteristic $p > 2$ such that $\mathcal{U}^+(FG)$ satisfies the group identity $(x_1, \ldots, x_n)$, for a fixed $n \geq 2$. Let N be a finite normal subgroup of G. If N is a p-group or a p'-group, then $\mathcal{U}^+(F(G/N))$ satisfies $(x_1, \ldots, x_n)$ as well.*

Proof. Suppose N is a p-group. Let $\epsilon_N : FG \to F(G/N)$ be the natural homomorphism. Of course, $\epsilon_N((FG)^+) = (F(G/N))^+$, hence for any $\beta \in \mathcal{U}^+(F(G/N))$, we may choose $\alpha \in (FG)^+$ such that $\epsilon_N(\alpha) = \beta$. Now, β is a unit, hence there exists $\nu \in F(G/N)$ such that $\beta\nu = 1$. Choosing $\mu \in FG$ such that $\epsilon_N(\mu) = \nu$, we have $\epsilon_N(\alpha\mu - 1) = 0$, hence $\alpha\mu - 1 \in \Delta_F(G, N)$. By Lemma 2.3.2, $\Delta_F(N)$ is a nilpotent ideal. Let us say that $(\Delta_F(N))^{p^t} = (0)$. Then

$$(\Delta_F(G, N))^{p^t} = (FG\Delta_F(N))^{p^t} = (0).$$

Thus, we have

$$0 = (\alpha\mu - 1)^{p^t} = (\alpha\mu)^{p^t} - 1,$$

and therefore, $(\alpha\mu)^{p^t} = 1$. Similarly, $(\mu\alpha)^{p^t} = 1$, hence $\alpha \in \mathcal{U}(FG)$. Thus, for any $\beta_1, \dots, \beta_n \in \mathcal{U}^+(F(G/N))$, there exist $\alpha_1, \dots, \alpha_n \in \mathcal{U}^+(FG)$ such that $\epsilon_N(\alpha_i) = \beta_i$, for all i. That is,

$$(\beta_1, \dots, \beta_n) = \epsilon_N((\alpha_1, \dots, \alpha_n)) = 1,$$

as required.

Now, suppose N is a p'-group. Let $\eta = \frac{\hat{N}}{|N|}$. Clearly, η is a symmetric central idempotent of FG. Let us define a function $\theta : F(G/N) \to FG$ as follows. Letting $F\bar{G} = F(G/N)$, we define $\theta(\bar{\alpha}) = \alpha\eta + 1 - \eta$, for all $\alpha \in FG$. First, let us see that this is well-defined. If $\bar{\alpha} = \bar{\beta}$, then $\alpha - \beta \in \Delta_F(G, N)$, hence by Lemma 4.3.3, $(\alpha - \beta)\eta = 0$. Thus, $\theta(\bar{\alpha}) = \theta(\bar{\beta})$. We also note that $\theta((F(G/N))^+) \subseteq (FG)^+$. Indeed, if $\bar{\alpha} \in (F\bar{G})^+$, then we may assume $\alpha \in (FG)^+$, and therefore $\theta(\bar{\alpha}) = \alpha\eta + 1 - \eta \in (FG)^+$. Next, we claim that $\theta(\mathcal{U}(F(G/N))) \subseteq \mathcal{U}(FG)$. If $\bar{\alpha}\bar{\beta} = \bar{1} = \bar{\beta}\bar{\alpha}$, then $\alpha\beta - 1 \in \Delta_F(G, N)$ hence, by Lemma 4.3.3, $(\alpha\beta - 1)\eta = 0$. Thus

$$\theta(\bar{\alpha})\theta(\bar{\beta}) = (\alpha\eta + 1 - \eta)(\beta\eta + 1 - \eta) = \alpha\beta\eta + 1 - \eta = \eta + 1 - \eta = 1 = \theta(\bar{\beta})\theta(\bar{\alpha}),$$

hence $\theta(\bar{\alpha})$ is a unit. Also, θ is a group homomorphism on $\mathcal{U}(F(G/N))$. Indeed, if $\bar{\alpha}, \bar{\beta} \in \mathcal{U}(F(G/N))$, then

$$\theta(\bar{\alpha}\bar{\beta}) = \alpha\beta\eta + 1 - \eta = (\alpha\eta + 1 - \eta)(\beta\eta + 1 - \eta) = \theta(\bar{\alpha})\theta(\bar{\beta}).$$

Now, we observe that θ is injective on $\mathcal{U}(F(G/N))$. Indeed, if $\theta(\bar{\alpha}) = 1$, then $\alpha\eta + 1 - \eta = 1$, hence $(\alpha - 1)\eta = 0$. By Lemma 4.3.3, $\alpha - 1 \in \Delta_F(G, N)$, hence $\bar{\alpha} = \bar{1}$, as required. Thus, θ is a monomorphism mapping $\mathcal{U}(F(G/N))$ isomorphically onto a subgroup of $\mathcal{U}(FG)$. Since θ maps symmetric elements to symmetric elements, if $\bar{\alpha}_1, \dots, \bar{\alpha}_n \in \mathcal{U}^+(F(G/N))$, then

$$1 = (\theta(\bar{\alpha}_1), \dots, \theta(\bar{\alpha}_n)) = \theta(\bar{\alpha}_1, \dots, \bar{\alpha}_n),$$

hence $(\bar{\alpha}_1, \dots, \bar{\alpha}_n) = \bar{1}$, since θ is injective. We are done. $\square$

Now, we need some results about matrices. If R is a ring with identity and n is a positive integer, then $M_n(R)$ denotes the ring of $n \times n$ matrices over R, and $GL_n(R)$ denotes the group of invertible $n \times n$ matrices over R. The next result will be useful later as well.

Lemma 4.3.5. *Let R be a commutative ring with identity. If $a, b, c, d, \alpha \in R$, and $ad - bc = 1$, then*

$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix}\right) = \begin{pmatrix} w_1 & b^2\alpha \\ w_2 & w_3 \end{pmatrix}$$

for some $w_1, w_2, w_3 \in R$. It follows that for any positive integer n,

$$\left(\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}, \underbrace{\begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix}, \dots, \begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix}}_{n \text{ times}}\right) = \begin{pmatrix} v_1 & \alpha^{2^{n+1}-1} \\ v_2 & v_3 \end{pmatrix}$$

for some $v_1, v_2, v_3 \in R$.

Proof. The first part is an easy computation, and the second part follows from the first by induction. $\square$

In particular, if $\alpha = 1$, then we are never going to get the identity matrix in the right side of the expression above, and therefore the subgroup of $GL_2(R)$ generated by

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

will not be nilpotent.

Let n be a positive integer, and suppose that $*$ is an involution on $M_n(F)$, for any field, F. If α is central in $M_n(F)$, and $\beta \in M_n(F)$, then

$$\alpha^*\beta = (\beta^*\alpha)^* = (\alpha\beta^*)^* = \beta\alpha^*,$$

hence α^* is central. Thus, $*$ leaves the centre, which we identify with F, invariant. We say that $*$ is an involution of the first kind if $a^* = a$ for all $a \in F$. Otherwise, $*$ induces a nontrivial involution of F, and we say that $*$ is an involution of the second kind. We will let T denote the transpose involution, given by $(a_{ij})^T = (a_{ji})$. If $n = 2m$, then $M_n(F)$ also has the canonical symplectic involution given by

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}^* = \begin{pmatrix} D^T & -B^T \\ -C^T & A^T \end{pmatrix}$$

for all $A, B, C, D \in M_m(F)$. In fact, the involutions of $M_n(F)$ have been studied, and we will need the following results.

Lemma 4.3.6. *Let $*$ be an involution of the first kind on $M_n(F)$, where n is a positive integer, and char $F \neq 2$. Then there exists a matrix $U \in GL_n(F)$ such that $U^T = \pm U$, and for all $X \in M_n(F)$, $X^* = U^{-1}X^TU$.*

Proof. See [KMRT, Proposition 2.19]. □

Lemma 4.3.7. *Let $*$ be an involution of the second kind on $M_n(F)$, where char $F \neq 2$ and n is a positive integer. Let λ be the restriction of $*$ to the centre, F. Then we can define an involution $\circ$ on $M_n(F)$ via $(a_{ij})^\circ = (\lambda(a_{ij}))^T$. Also, there exists a matrix $U \in GL_n(F)$ such that $U^\circ = U$, and $X^* = U^{-1}X^\circ U$ for all $X \in M_n(F)$.*

Proof. See [KMRT, Proposition 2.20]. □

We want to look at semisimple group rings, FG. We will have

$$FG \cong \bigoplus_i M_{n_i}(F_i)$$

and we will be interested in the symmetric elements of $M_{n_i}(F_i)$. We have

Lemma 4.3.8. *Let F be a field of characteristic $p > 2$. Let n be a positive integer, and $*$ an involution on $M_n(F)$. If $n = 1$ or $n = 2$ and $*$ is the canonical symplectic involution, then the symmetric elements (with respect to $*$) commute. Otherwise, the subgroup of $GL_n(F)$ generated by the symmetric units is not nilpotent.*

Proof. The case $n = 1$ requires no comment, so we will assume $n \geq 2$. If $n = 2$ and $*$ is the canonical symplectic involution, then the symmetric elements are simply

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, \quad a \in F,$$

which commute.

Let H be the subgroup of $GL_n(F)$ generated by the symmetric units, and suppose $*$ is of the first kind. By Lemma 4.3.6, there exists a matrix $U \in GL_n(F)$ such that $U^T = \pm U$ and $Y^* = U^{-1}Y^TU$ for all $Y \in M_n(F)$. First, let us assume that $U^T = U$. If $X \in GL_n(F)$ satisfies $X^T = X$, then $(XU)^* = U^{-1}U^TX^TU = XU$. Since the identity matrix I_n satisfies $I_n^T = I_n$, we get $U^* = U$ as well. Thus, H contains XU and U, and therefore H contains $(XU)U^{-1} = X$, for all $X \in GL_n(F)$ satisfying $X^T = X$. Such matrices would include

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus I_{n-2}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \oplus I_{n-2}, \text{ and } \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \oplus I_{n-2},$$

where I_{n-2} may be omitted if $n = 2$. Thus, H contains

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \oplus I_{n-2} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \oplus I_{n-2}$$

and

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \oplus I_{n-2} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \oplus I_{n-2}.$$

But we observed earlier that the group generated by

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

is not nilpotent.

Now, suppose $U^T = -U$. If $n = 2$, then

$$U = \begin{pmatrix} 0 & a \\ -a & 0 \end{pmatrix}$$

for some $a \in F^{\times}$. In this case, it is easy to verify that $*$ is the canonical symplectic involution, and we have already dealt with this case. Since

$$\det(U) = \det(U^T) = \det(-U) = (-1)^n \det(U),$$

and U is invertible, n must be even, say $n = 2m$, $m \geq 2$. Suppose $X \in GL_n(F)$ satisfies $X^T = -X$. Then

$$(XU)^* = U^{-1}U^TX^TU = U^{-1}(-U)(-X)U = XU.$$

If $Z \in GL_n(F)$ and $Z^T = -Z$, then $(Z^{-1})^T = -Z^{-1}$, so $(Z^{-1}U)^* = Z^{-1}U$. Thus, H contains XU and $Z^{-1}U$, and therefore it contains $XU(Z^{-1}U)^{-1} = XZ$. For any $A \in GL_m(F)$, let

$$X = \begin{pmatrix} 0 & -A \\ A^T & 0 \end{pmatrix}, \; Z = \begin{pmatrix} 0 & I_m \\ -I_m & 0 \end{pmatrix}.$$

Then H contains

$$XZ = \begin{pmatrix} A & 0 \\ 0 & A^T \end{pmatrix},$$

for all $A \in GL_m(F)$. If H is nilpotent, then clearly $GL_m(F)$ is nilpotent, so $GL_2(F)$ is nilpotent, which we have seen to be false.

Finally, suppose $*$ is an involution of the second kind. Let λ be the restriction of $*$ to the centre, F. We define an involution $\circ$ on $M_n(F)$ via $(a_{ij})^\circ = (\lambda(a_{ij}))^T$. By Lemma 4.3.7, there is a matrix $U \in GL_n(F)$ satisfying $U^\circ = U$, and such that $Y^* = U^{-1}Y^\circ U$ for all $Y \in M_n(F)$. Take any $X \in GL_n(F)$ such that $X^\circ = X$. Then $(XU)^* = U^{-1}(XU)^\circ U = XU$. Clearly, $I_n^\circ = I_n$, hence $U^* = U$. Thus, H contains XU and U, and therefore $(XU)U^{-1} = X$, for all $X \in GL_n(F)$ such that $X^\circ = X$. But an automorphism λ of F must fix its prime subfield, $\mathbb{F}_p$, elementwise. Thus, $\circ$ acts as T on $M_n(\mathbb{F}_p)$, so H contains the units of $M_n(\mathbb{F}_p)$ which are symmetric with respect to T. We have already seen that in this case, H is not nilpotent. We are done. $\square$

We are now ready to deal with the semisimple case.

Lemma 4.3.9. *Let F be a field of characteristic $p > 2$ and let G be a finite p'-group. If $\mathcal{U}^+(FG)$ is nilpotent, then G is abelian or a Hamiltonian 2-group.*

Proof. Let $\mathbb{F}_p$ be the prime subfield of F. If $\mathcal{U}^+(FG)$ is nilpotent, then surely $\mathcal{U}^+(\mathbb{F}_pG)$ is nilpotent, so we will assume that F has order p. Now, by Maschke's Theorem, FG is semisimple, and we will let $e_1, \ldots, e_k$ be the primitive central idempotents of FG. Thus, $FGe_i \cong M_{n_i}(D_i)$ for all i, where $D_i = F_i$ is a finite division ring, hence, by Wedderburn's Little Theorem, a field. Let $\pi_i : FG \to M_{n_i}(F_i)$ be the projection.

Clearly, if e_i is a primitive central idempotent, then so is e_i^*. Suppose that $e_1 \neq e_1^* = e_2$. Let $\alpha \in FG$ be such that $\alpha e_1 \in GL_{n_1}(F_1)$, say $(\alpha e_1)(\gamma e_1) = e_1 = (\gamma e_1)(\alpha e_1)$. Then

$$(\alpha^* e_1^*)(\gamma^* e_1^*) = (e_1\gamma e_1\alpha)^* = (\gamma\alpha e_1)^* = e_1^* = (\gamma^* e_1^*)(\alpha^* e_1^*),$$

hence $\alpha^* e_1^* \in GL_{n_2}(F_2)$. Let $\beta = \alpha e_1 + \alpha^* e_1^* + \sum_{i=3}^{k} e_i$. Clearly, $\beta^* = \beta$, and for each i, $\pi_i(\beta)$ is one of αe_1, $\alpha^* e_1^*$, or some e_i. That is, the projection of β onto each Wedderburn component is a unit, hence $\beta \in \mathcal{U}^+(FG)$. But $\pi_1(\beta) = \alpha e_1$, hence $\pi_1(\mathcal{U}^+(FG)) = GL_{n_1}(F_1)$. But we saw above that $GL_{n_1}(F_1)$ is not nilpotent unless $n_1 = 1$. Thus, if $n_i > 1$, then $e_i^* = e_i$.

In this case, FGe_i is invariant under $*$. Let αe_i be a symmetric unit in FGe_i. Then letting $\beta = \alpha e_i + \sum_{j\neq i} e_j$, we see that $\beta \in \mathcal{U}^+(FG)$, and $\pi_i(\beta) = \alpha e_i$. Thus, the symmetric units of $FGe_i = M_{n_i}(F_i)$ are all in the homomorphic image of the symmetric units of FG. Since $\mathcal{U}^+(FG)$ is nilpotent, the set of symmetric units in each $M_{n_i}(F_i)$ generates a nilpotent group. By Lemma 4.3.8, this can only occur when the symmetric elements in $M_{n_i}(F_i)$ commute. Now, if $\rho \in (FG)^+$, then ρe_i is symmetric in $M_{n_i}(F_i)$. Thus, the projections of the elements of $(FG)^+$ into each Wedderburn component commute. We are excluding the $n_i = 1$ case, but here, all projections commute. Hence, $(FG)^+$ is commutative. In particular, it is Lie nilpotent, and so by Theorems 3.6.1 and 3.6.5, since G is a p'-group, G is abelian or a Hamiltonian 2-group. □

Now, let us look more generally at finite groups. First, we shall examine the 2-elements.

Lemma 4.3.10. *Let F be a field of characteristic greater than 2, and G a finite group. If $\mathcal{U}^+(FG)$ is nilpotent, then the 2-elements of G form a normal subgroup which is either abelian or Hamiltonian.*

Proof. If the 2-elements form a subgroup H, then it is certainly normal. In this case, $\mathcal{U}^+(FH)$ is nilpotent, and therefore Lemma 4.3.9 tells us that H is abelian or Hamiltonian. Let us show that the 2-elements do indeed form a subgroup.

If G has odd order there is nothing to do. Otherwise, let N_1 be the subgroup of G generated by the elements of order 2. The elements of order 2 are symmetric units, and therefore form a nilpotent subset of G. By Lemma 4.3.2, N_1 is a nilpotent group, and since it is generated by 2-elements, it is a 2-group. It is certainly normal as well. Now, let us work in G/N_1. Since $\mathcal{U}^+(F(G/N_1))$ is nilpotent by Lemma 4.3.4, our previous argument gives us a normal subgroup N_2/N_1 of G/N_1 such that N_2/N_1 is a 2-group containing all of the elements of order 2 in G/N_1. That is, N_2 is a 2-group containing every element of G whose order divides 4. Proceeding in this fashion, we will eventually obtain all of the 2-elements, since G is finite. □

If $x \in G$, we write $C_G(x)$ for the centralizer of x in G. Similarly, $C_G(S)$ is the centralizer of the subset S. The next few results give us some facts about the p-elements and p'-elements of G.

Lemma 4.3.11. *Let F be a field of characteristic $p > 2$, and G a torsion group. Suppose $\mathcal{U}^+(FG)$ is nilpotent. Let x be a p-element of G. If y is a p'-element of G whose order is either 2 or odd, then x and y commute.*

Proof. By Lemma 4.3.2, the subgroup $\langle \mathcal{U}^+(FG)\rangle$ of $\mathcal{U}(FG)$ is nilpotent. Now, if $x \in G$, $o(x) = p^m$, then $(x + x^{-1})^{p^m} = 2$, hence $\frac{x+x^{-1}}{2}$ is a p-element of $\langle \mathcal{U}^+(FG)\rangle$. Suppose y has order 2. Then $y \in \mathcal{U}^+(FG)$ and, indeed, $\frac{x+x^{-1}}{2}$ and y are elements with relatively prime orders in the nilpotent group $\langle \mathcal{U}^+(FG)\rangle$, which means they commute. Thus,

$$0 = [x + x^{-1}, y] = xy + x^{-1}y - yx - yx^{-1}.$$

Now, the term xy must cancel with something, and since char $F > 2$, either $xy = yx$ (as desired), or $xy = yx^{-1}$. But in the latter case, $\langle x, y\rangle$ is the dihedral group of order $2p^m$. However, the 2-elements of this group do not form a subgroup, contradicting Lemma 4.3.10. This case is complete.

On the other hand, if y is an odd p'-element of G, then choosing $k > 0$ such that $p^k \equiv 1 \pmod{o(y)}$, we have $y^{p^k} = y$, and therefore $(y + y^{-1})^{p^k} = y + y^{-1}$. However,

$$(1 + y^2)(1 - y^2 + y^4 - \cdots + y^{2(o(y)-1)}) = 1 + y^{2o(y)} = 2,$$

since $o(y)$ is odd, and therefore $y + y^{-1} = y^{-1}(1 + y^2)$ is in $\mathcal{U}^+(FG)$. Thus, $(y + y^{-1})^{p^k-1} = 1$, and $y + y^{-1}$ is a p'-element of $\langle \mathcal{U}^+(FG)\rangle$. Therefore, $\frac{x+x^{-1}}{2}$ and $y + y^{-1}$ commute. That is, $[x + x^{-1}, y + y^{-1}] = 0$. Hence,

$$xy + xy^{-1} + x^{-1}y + x^{-1}y^{-1} - yx - yx^{-1} - y^{-1}x - y^{-1}x^{-1} = 0.$$

We claim that $xy = yx$. Indeed, xy must be cancelled in this expression. It can agree with a subtracted term, or at least two added terms (since the characteristic is not 2). If $xy = x^{-1}y$, then $x^2 = 1$. Since x is a p-element, $x = 1$ and therefore $xy = yx$. Similarly if $xy = xy^{-1}$. Thus, we may assume that xy agrees with a subtracted term. If $xy = yx^{-1}$, then $y^{-1}xy = x^{-1}$. Therefore, $y^{-2}xy^2 = x$. Thus, $y^2 \in C_G(x)$, hence $y \in C_G(x)$, since y has odd order. Similarly if $xy = y^{-1}x$. If $xy = y^{-1}x^{-1}$, then $(xy)^2 = 1$, and by the first part of this proof, x and xy commute. Thus $x^2y = xyx$, and $xy = yx$, as required. □

Lemma 4.3.12. *Let G be a finite group, and F a field of characteristic $p > 2$. If $\mathcal{U}^+(FG)$ is nilpotent then the p'-elements of G form a normal subgroup which is either abelian or a Hamiltonian 2-group.*

Proof. Once we prove that the p'-elements form a subgroup, the rest will follow from Lemma 4.3.9. If G is a p'-group, there is nothing to do. Otherwise, let P be the set of p-elements of G, and $K = C_G(P)$. Clearly, the p-elements of K are central in K, hence they form a central p-subgroup P_1. Then K/P_1 is a p'-group, and by the Schur-Zassenhaus Theorem (Theorem 2.2.9), there exists a p'-subgroup L of K such that we have a semidirect product $K = P_1 \rtimes L$. But P_1 is central, hence $K = P_1 \times L$, and L is the set of all p'-elements in K. However, by Lemma 4.3.11, every odd p'-element of G centralizes P, and hence lies in K. Thus, we have a p'-subgroup L of G which contains all of the odd p'-elements. By Lemma 4.3.10, the 2-elements of G form a normal subgroup M. Thus, LM is a p'-subgroup of G containing all of the 2-elements and all of the odd p'-elements. If x is a p'-element of F, then x is the product of a 2-element and an odd p'-element, hence LM is the subgroup we are seeking. □

Lemma 4.3.13. *Let F be a field of characteristic $p > 2$, and G a finite group. If $\mathcal{U}^+(FG)$ is nilpotent, then the p-elements of G form a normal subgroup.*

Proof. By Lemma 4.3.10, the 2-elements of G form a normal subgroup H. Our proof is by induction on $|H|$. If $|H| = 1$, then applying Lemma 4.3.12, we see that the p'-elements form a normal subgroup K. Thus, by Schur-Zassenhaus, there exists a p-subgroup P such that $G = K \rtimes P$. But by Lemma 4.3.11, the p-elements commute with the odd p'-elements. Thus, $G = K \times P$, and P is the set of all p-elements, which completes this case.

Now, suppose $|H| > 1$, and our result holds for smaller H. By Lemma 4.3.12, the p'-elements form a subgroup which is either abelian or a Hamiltonian 2-group. In either an abelian group or a Hamiltonian 2-group, the elements of order 2 are central. That is, the elements of order 2 in G commute with all p'-elements. Furthermore, by Lemma 4.3.11, the elements of order 2 commute with all of the p-elements. Thus, letting $N = \{g \in G : g^2 = 1\}$, we know that N is a central subgroup. Furthermore, by Lemma 4.3.4, $\mathcal{U}^+(F(G/N))$ is nilpotent, and the Sylow 2-subgroup of G/N is smaller than that of G. By our inductive assumption, the p-elements of G/N form a normal subgroup N_1/N. That is, $N_1 = \{g \in G : g^{2p^m} = 1 \text{ for some } m\}$ is a subgroup of G. Once again, the elements of order 2 in N_1 form a central subgroup K_1, and N_1/K_1 is a p-group. By yet another application of Schur-Zassenhaus, $N_1 = K_1 \rtimes P_1$, and since K_1 is central in N_1, $N_1 = K_1 \times P_1$, where P_1 is the group of all p-elements in N_1. By definition of N_1, the p-elements of G all lie in N_1, hence the p-elements of G form a subgroup, as required. $\square$

We can now give the

Proof of Proposition 4.3.1. To see that the p-elements of G form a group, we need only consider the finitely generated case. Since G is locally finite, we may assume that G is finite and, by Lemma 4.3.13, the p-elements do indeed form a subgroup. Similarly for the p'-elements, using Lemma 4.3.12. Clearly these subgroups are normal in G and intersect trivially, hence $G = P \times A$, where P is a p-group and A is a p'-group. Suppose $x, y \in A$, and $xy \neq yx$. Then for any $z \in A$, $\langle x, y, z\rangle$ is a Hamiltonian 2-group, by Lemma 4.3.12. Thus, either A

is abelian, or A is a 2-group, and $y^{-1}xy = x^{\pm 1}$ for all $x, y \in A$. That is, A is abelian or a Hamiltonian 2-group. □

4.4. Group rings of locally finite groups

In this section, we will strengthen Proposition 4.3.1, and obtain our final results for locally finite groups. In the next section, we will show that if $\mathcal{U}^+(FG)$ is nilpotent, then G must be locally finite. First, let us suppose that $Q_8 \not\subseteq G$. Our result is

Proposition 4.4.1. *Let G be a locally finite group not containing Q_8. Let F be a field of characteristic $p > 2$. Then $\mathcal{U}^+(FG)$ is nilpotent if and only if G is nilpotent and p-abelian.*

By Proposition 4.3.1, we may assume that $G \simeq P \times A$, where P is a p-group and A is abelian. If we can show that P is nilpotent and p-abelian, then G will enjoy these properties as well. Thus, we may assume that G is a p-group. Let us strengthen Lemma 4.3.4.

Lemma 4.4.2. *Let G be a torsion group, and F a field of characteristic $p > 2$ such that $\mathcal{U}^+(FG)$ satisfies the group identity $(x_1, \ldots, x_n)$, for a fixed $n \geq 2$. Let N be a finite normal subgroup of G. Then $\mathcal{U}^+(F(G/N))$ satisfies $(x_1, \ldots, x_n)$.*

Proof. Since $\mathcal{U}^+(FN)$ satisfies $(x_1, \ldots, x_n)$, Lemma 4.3.13 reveals that the p-elements of N form a normal subgroup, P. Clearly, P is normal in G as well. By Lemma 4.3.4, $\mathcal{U}^+(F(G/P))$ satisfies $(x_1, \ldots, x_n)$, and so does $\mathcal{U}^+(F(N/P))$. Since N/P is a p'-group, Lemma 4.3.4 also tells us that $\mathcal{U}^+(F((G/P)/(N/P)))$ satisfies $(x_1, \ldots, x_n)$. But $(G/P)/(N/P) \simeq G/N$, and we are done. □

Lemma 4.4.3. *Let G be a locally finite group and char $F = p > 2$. Suppose $\mathcal{U}^+(FG)$ satisfies $(x_1, \dots, x_n)$, for a fixed $n \geq 2$. Let N be any normal subgroup of G. Then $\mathcal{U}^+(F(G/N))$ satisfies $(x_1, \dots, x_n)$.*

Proof. Let $F\bar{G} = F(G/N)$. Choose any $\bar{\alpha}_1, \dots, \bar{\alpha}_n \in \mathcal{U}^+(F\bar{G})$. Let $\bar{\beta}_i = \bar{\alpha}_i^{-1}$, for each i. Then $\alpha_i\beta_i - 1$ and $\beta_i\alpha_i - 1$ lie in $\Delta_F(G, N)$. Thus, each

$$\alpha_i\beta_i - 1 = \sum_{j=1}^{k} \lambda_j g_j(n_j - 1)$$

for some $\lambda_j \in F$, $g_j \in G$, and $n_j \in N$, and

$$\beta_i\alpha_i - 1 = \sum_{j=1}^{l} \lambda'_j g'_j(n'_j - 1)$$

for some $\lambda'_j \in F$, $g'_j \in G$, and $n'_j \in N$. Let H be the subgroup of G generated by the support of each α_i and each β_i, together with all of the g_j, n_j, g'_j, and n'_j. Then H is finitely generated, hence finite. Also, each $\alpha_i, \beta_i \in FH$, and each $\alpha_i\beta_i - 1$ and each $\beta_i\alpha_i - 1$ lies in $\Delta_F(H, H \cap N)$. That is, $\bar{\beta}_i = \bar{\alpha}_i^{-1}$ in $F\bar{H} = F(H/(H \cap N))$. Now, $H \cap N$ is a finite normal subgroup of H. Thus, since $\mathcal{U}^+(FH)$ satisfies $(x_1, \dots, x_n)$, Lemma 4.4.2 shows us that $\mathcal{U}^+(F\bar{H})$ satisfies $(x_1, \dots, x_n)$. Therefore, $(\bar{\alpha}_1, \dots, \bar{\alpha}_n) = \bar{1}$. But $\bar{\alpha}_1, \dots, \bar{\alpha}_n$ were arbitrarily chosen in $\mathcal{U}^+(F(G/N))$, hence $\mathcal{U}^+(F(G/N))$ satisfies $(x_1, \dots, x_n)$. $\square$

Let us get back to the task of proving Proposition 4.4.1. Suppose $G = H \times K$. If $\alpha = \sum_{h \in H} \alpha_h h \in FH$, and $\beta = \sum_{k \in K} \beta_k k \in FK$, then $\alpha\beta = \sum_{h \in H} \sum_{k \in K} \alpha_h \beta_k hk$. These group elements hk are pairwise distinct, hence $\alpha\beta = 0$ if and only if $\alpha = 0$ or $\beta = 0$. The next lemma is borrowed from [Seh1, Section VI.3].

Lemma 4.4.4. *Suppose char $F = p > 0$, and let G be a group containing an infinite central subgroup A such that A is a p-group of bounded exponent. Then* *for any $0 \neq \delta \in FG$, and any positive integer t, there exist central elements $\mu_1, \dots, \mu_t \in (FG)^+$ such that each $\mu_i^2 = 0$, but $\mu_1 \cdots \mu_t \delta \neq 0$.*

Proof. By Theorem 2.2.5, A is a direct product of cyclic groups. Since shrinking A does not harm our conclusion, let us say that $A = \prod_{i=1}^{\infty} A_i$, where each A_i is a nontrivial p-group. Write $\delta = \sum_{i=1}^{k} g_i \alpha_i$, where each $0 \neq \alpha_i \in FA$, and the g_i lie in distinct cosets of A in G. Each α_i has finite support, so there exists an m such that the support of all of the α_i's is contained in $\prod_{i=1}^{m} A_i$. For each i, $1 \leq i \leq t$, let $\mu_i = \hat{A}_{m+i}$. Clearly, $\mu_i \in (FG)^+$, $\mu_i^2 = 0$, and μ_i is central in FG, since A_i is central in G, for all i. But, as we saw above, $\mu_1 \cdots \mu_t \alpha_i \neq 0$, for all i, and then

$$\mu_1 \cdots \mu_t \delta = \sum_{i=1}^{k} g_i(\mu_1 \cdots \mu_t \alpha_i).$$

But the elements of G appearing in the support of $g_i \mu_1 \cdots \mu_t \alpha_i$ are surely in $g_i A$, for each i, hence $\mu_1 \cdots \mu_t \delta \neq 0$. □

Lemma 4.4.5. *Let F be a field of characteristic $p > 0$, and suppose G contains an infinite central subgroup A, such that A is a p-group of bounded exponent. If $\mathcal{U}^+(FG)$ is nilpotent, then $(FG)^+$ is Lie nilpotent.*

Proof. Take any positive integer $t \geq 2$, and any $\alpha_1, \dots, \alpha_t \in (FG)^+$. If

$$[\alpha_1, \dots, \alpha_t] \neq 0,$$

then let $\delta = [\alpha_1, \dots, \alpha_t]$, and choose $\mu_1, \dots, \mu_t$ as in Lemma 4.4.4 such that each $\mu_i^2 = 0$ but $\mu_1 \mu_2 \cdots \mu_t [\alpha_1, \dots, \alpha_t] \neq 0$. Now, for each i, $1 + \mu_i \alpha_i$ is a unit with inverse $1 - \mu_i \alpha_i$, and so it is clearly in $\mathcal{U}^+(FG)$. Thus,

$$(1 + \mu_1 \alpha_1, 1 + \mu_2 \alpha_2) = 1 + \mu_1 \mu_2 [\alpha_1, \alpha_2]$$

and then, by induction, we can see that

$$(1 + \mu_1 \alpha_1, \dots, 1 + \mu_t \alpha_t) = 1 + \mu_1 \cdots \mu_t [\alpha_1, \dots, \alpha_t].$$

We are assuming that $\mu_1 \cdots \mu_t[\alpha_1, \ldots, \alpha_t] \neq 0$, hence $(1+\mu_1\alpha_1, \ldots, 1+\mu_t\alpha_t) \neq 1$. But $\mathcal{U}^+(FG)$ is nilpotent, so there exists a t such that

$$(1+\mu_1\alpha_1, \ldots, 1+\mu_t\alpha_t) = 1$$

and therefore, $[\alpha_1, \ldots, \alpha_t] = 0$ for all $\alpha_1, \ldots, \alpha_t \in (FG)^+$, as required. □

Let us now consider some special cases.

Lemma 4.4.6. *Suppose char $F = p > 2$, G is a nilpotent p-group, and G' has bounded exponent. If $\mathcal{U}^+(FG)$ is nilpotent, then G' is actually finite.*

Proof. Assume G' is infinite. Then we may choose an r such that $\gamma_r(G)$, the r-th term of the lower central series, is infinite, but $\gamma_{r+1}(G)$ is finite. (This r must exist, since G is nilpotent.) By Lemma 4.3.4, $\mathcal{U}^+(F(G/\gamma_{r+1}(G)))$ is nilpotent, and if we can show that $(G/\gamma_{r+1}(G))'$ is finite, then we will know that $G'/\gamma_{r+1}(G)$ is finite, and since $\gamma_{r+1}(G)$ is finite, we will have a contradiction. But $G/\gamma_{r+1}(G)$ has an infinite central subgroup $\gamma_r(G)/\gamma_{r+1}(G)$ contained in $(G/\gamma_{r+1}(G))' = G'/\gamma_{r+1}(G)$. Since G' has bounded exponent, by Lemma 4.4.5 we see that $(F(G/\gamma_{r+1}(G)))^+$ is Lie nilpotent. Since G is a p-group, Theorem 3.6.1 tells us that $(G/\gamma_{r+1}(G))'$ is finite, and we are done. □

We will eventually reduce the problem to a p-group G of bounded exponent. If we can show that FG satisfies a polynomial identity, then we will be done, because of

Lemma 4.4.7. *Let F be a field of characteristic $p > 2$. Suppose G is a p-group of bounded exponent, with $(G : \phi(G)) < \infty$ and $|(\phi(G))'| < \infty$. If $\mathcal{U}^+(FG)$ is nilpotent, then G is nilpotent and p-abelian.*

Proof. We will follow quite closely part of the proof of Theorem 3.3.3, and therefore omit some of the details. We have $G^{p^m} = 1$ for some m. Also, since

$(G:\phi(G))<\infty$ and $|(\phi(G))'|<\infty$, $G/(\phi(G))'$ acts as a finite p-group of automorphisms of $\phi(G)/(\phi(G))'$, which is an abelian p-group of bounded exponent. From Lemma 2.2.6, we get

$$(\phi(G)/(\phi(G))', G/(\phi(G))', \dots, G/(\phi(G))') = 1.$$

Thus, $(\phi(G), G, \dots, G) \subseteq (\phi(G))'$. Since $(\phi(G))'/(\phi(G))''$ is finite, $G/(\phi(G))''$ acts as a finite p-group of automorphisms of $(\phi(G))'/(\phi(G))''$. By Lemma 2.2.6,

$$((\phi(G))'/(\phi(G))'', G/(\phi(G))'', \dots, G/(\phi(G))'') = 1,$$

hence

$$((\phi(G))', G, \dots, G) \subseteq (\phi(G))''.$$

Thus, $(\phi(G), G, \dots, G) \subseteq (\phi(G))''$. Since $(\phi(G))'$ is a finite p-group, it is nilpotent, and repeating this argument, we must obtain $(\phi(G), G, \dots, G) = 1$. But $G/\phi(G)$ is nilpotent as well, hence $(G, \dots, G) \subseteq \phi(G)$, and therefore $(G, \dots, G) = 1$, and G is nilpotent. Since G has bounded exponent, so does G', and Lemma 4.4.6 reveals that G is p-abelian as well. □

We also need this computational lemma.

Lemma 4.4.8. *Let R be a ring with identity. Let η be a central element of R satisfying $\eta^2 = 0$. If $\alpha \in R$, and $\beta \in \mathcal{U}(R)$, then $1+\eta\alpha \in \mathcal{U}(R)$, and for all $n \geq 1$,*

$$(1+\eta\alpha, \underbrace{\beta, \dots, \beta}_{n \text{ times}}) = 1 + \eta\left(\sum_{i=0}^{n}(-1)^i \binom{n}{i} \beta^{-(n-i)}\alpha\beta^{n-i}\right).$$

Proof. Clearly, $1+\eta\alpha$ is a unit with inverse $1-\eta\alpha$. We check the formula by induction. When $n=1$, we have

$$(1+\eta\alpha, \beta) = (1-\eta\alpha)\beta^{-1}(1+\eta\alpha)\beta = 1+\eta(\beta^{-1}\alpha\beta - \alpha)$$

as required. Assuming the formula works for n, to check the $n+1$ case, we simply apply the $n = 1$ case, and we find that the coefficient of α will be $(-1)^n$, the coefficient of $\beta^{-(n+1)}\alpha\beta^{n+1}$ will be 1, and if $0 < i < n+1$, the coefficient of $\beta^{-(n+1-i)}\alpha\beta^{n+1-i}$ will be $(-1)^i(\binom{n}{i} + \binom{n}{i-1}) = (-1)^i\binom{n+1}{i}$, as required. $\square$

Let us now present the

Proof of Proposition 4.4.1. Suppose $\mathcal{U}^+(FG)$ is nilpotent. By Proposition 4.3.1, $G \simeq P \times A$, where P is a p-group and A is abelian. Thus, it will suffice to show that P is nilpotent and P' is finite. That is, we will assume that G is a locally finite p-group. If FG is prime, then Proposition 4.2.1 shows us that $G = 1$. Therefore, by Theorem 2.3.3, we may assume that G has a nontrivial finite normal subgroup N. If we can show that $(G/N)'$ is finite, then since $(G/N)' = G'N/N$, and N is finite, we will know that $|G'N| < \infty$, and therefore G' is finite. By Theorem 2.2.7, G will be nilpotent as well, and we will be done.

Let $\eta = \hat{N}$. Then η is central in FG, and $\eta^2 = 0$. We know that there exists an m such that $(\alpha_1, \ldots, \alpha_{p^m+1}) = 1$ for all $\alpha_1, \ldots, \alpha_{p^m+1} \in \mathcal{U}^+(FG)$. Take any $\alpha \in (FG)^+$, $\beta \in \mathcal{U}^+(FG)$. Clearly, $1 + \eta\alpha$ is a symmetric unit. Thus,

$$(1 + \eta\alpha, \underbrace{\beta, \ldots, \beta}_{p^m \text{ times}}) = 1.$$

But Lemma 4.4.8 gives a formula for the left side of this expression. Indeed, since p divides $\binom{p^m}{i}$ whenever $0 < i < p^m$, we obtain $1 + \eta(\beta^{-p^m}\alpha\beta^{p^m} - \alpha) = 1$. Therefore, $\beta^{-p^m}\alpha\beta^{p^m} - \alpha$ annihilates $\eta = \hat{N}$. By Lemma 4.3.3, the annihilator of η is $\Delta_F(G, N)$. Hence, working in $F\bar{G} = F(G/N)$, we obtain $[\bar{\alpha}, \bar{\beta}^{p^m}] = \bar{0}$.

Now, G is a locally finite p-group, and therefore an element of FG is a unit if and only if it does not have augmentation zero. (Indeed, suppose $\rho \in FG$, and $e = \epsilon(\rho)$, where $\epsilon : FG \to F$ is the augmentation map. We may assume that G is generated by the support of ρ, and is therefore finite. Then by Lemma 2.3.2, there exists a positive integer t such that $(\rho - e)^{p^t} = 0$. But then $\rho^{p^t} = e^{p^t}$, which is a unit of F, provided $e \neq 0$.) Thus, for any $\gamma \in (FG)^+$, either $\gamma \in \mathcal{U}^+(FG)$ or $1+\gamma \in \mathcal{U}^+(FG)$. In the latter case, if $\alpha \in (FG)^+$, then

$$\bar{0} = [\bar{\alpha}, (\overline{1+\gamma})^{p^m}] = [\bar{\alpha}, \bar{1} + \bar{\gamma}^{p^m}].$$

Therefore, in either case, $[\bar{\alpha}, \bar{\gamma}^{p^m}] = \bar{0}$. Since every element of $(F\bar{G})^+$ is an image under $FG \to F(G/N)$ of an element of $(FG)^+$, we see that $(F\bar{G})^+$ satisfies the polynomial identity $[\lambda, \mu^{p^m}] = 0$. Substituting $\lambda + \lambda^*$ for λ, and $\mu + \mu^*$ for μ, we see that $F\bar{G}$ satisfies a $*$-polynomial identity. Therefore, by Theorem 2.4.6, $F\bar{G}$ satisfies a polynomial identity.

Next, if $\bar{x}, \bar{y} \in \bar{G}$, then

$$\bar{0} = [\bar{x} + \bar{x}^{-1}, (\bar{y} + \bar{y}^{-1})^{p^m}] = [\bar{x} + \bar{x}^{-1}, \bar{y}^{p^m} + \bar{y}^{-p^m}].$$

Expanding this expression, $\bar{x}\bar{y}^{p^m}$ must agree either with a subtracted term or at least two added terms. We claim that, in fact, $\bar{x}\bar{y}^{p^m} = \bar{y}^{p^m}\bar{x}$. If $\bar{x}\bar{y}^{p^m} = \bar{x}^{-1}\bar{y}^{p^m}$, then $\bar{x}^2 = \bar{1}$, hence $\bar{x} = \bar{1}$, since G is a p-group. Thus, $\bar{x}$ commutes with $\bar{y}^{p^m}$. Similarly if $\bar{x}\bar{y}^{p^m} = \bar{x}\bar{y}^{-p^m}$. Thus, we may assume that $\bar{x}\bar{y}^{p^m}$ agrees with a subtracted term. If $\bar{x}\bar{y}^{p^m} = \bar{y}^{p^m}\bar{x}^{-1}$, then $\bar{y}^{-p^m}\bar{x}\bar{y}^{p^m} = \bar{x}^{-1}$, hence $\bar{y}^{2p^m} \in C_{\bar{G}}(\bar{x})$. Since G is a p-group, $\bar{y}^{p^m}$ commutes with $\bar{x}$. Similarly if $\bar{x}\bar{y}^{p^m} = \bar{y}^{-p^m}\bar{x}$. If $\bar{x}\bar{y}^{p^m} = \bar{y}^{-p^m}\bar{x}^{-1}$, then $(\bar{x}\bar{y}^{p^m})^2 = \bar{1}$, hence $\bar{x}\bar{y}^{p^m} = \bar{1}$, and therefore $\bar{x}$ and $\bar{y}^{p^m}$ commute. The final case is $\bar{x}\bar{y}^{p^m} = \bar{y}^{p^m}\bar{x}$, and the claim is proved. Since $\bar{x}$ and $\bar{y}$ were arbitrary, $(\bar{G})^{p^m} \subseteq \zeta(\bar{G})$. That is, $\bar{G}/\zeta(\bar{G})$ is a p-group of bounded exponent. Furthermore, since $\mathcal{U}^+(FG)$ is nilpotent, Lemma 4.4.3 tells us that $\mathcal{U}^+(F\bar{G})$ is nilpotent, and therefore $\mathcal{U}^+(F(\bar{G}/\zeta(\bar{G})))$ is nilpotent. Since $F\bar{G}$ satisfies a polynomial identity, so does $F(\bar{G}/\zeta(\bar{G}))$, and therefore, by Theorem 2.4.3, $(\bar{G}/\zeta(\bar{G}) : \phi(\bar{G}/\zeta(\bar{G}))) < \infty$ and $|(\phi(\bar{G}/\zeta(\bar{G})))'| < \infty$. By Lemma 4.4.7, $\bar{G}/\zeta(\bar{G})$ is nilpotent, hence $\bar{G}$ is nilpotent, and furthermore, by Theorem 2.2.4, $(\bar{G})'$ is a p-group of bounded exponent. By Lemma 4.4.6, it follows that $(\bar{G})'$ is finite, which is what we were trying to prove.

Conversely, if G is nilpotent and p-abelian, then by Theorem 4.1.3, if G contains a central element of order p, we know that $\mathcal{U}(FG)$ is nilpotent, hence

$\mathcal{U}^+(FG)$ is nilpotent. If G contains no central element of order p, then G contains no p-element at all, since it is nilpotent, and since G' is a p-group, G is abelian. Surely, $\mathcal{U}^+(FG)$ is nilpotent in this case. $\square$

Now, let us consider the case in which $Q_8 \subseteq G$. In view of Proposition 4.3.1, we may assume that $G \simeq Q_8 \times E \times P$, where $E^2 = 1$ and P is a p-group. We will show that P must be finite. First, we shall consider the group $G = Q_8 \times \langle x \rangle$, with x a p-element. We will borrow the following construction from [GSV2, Lemma 6]. Write

$$Q_8 = \langle g, h | g^4 = 1, g^2 = h^2, h^{-1}gh = g^{-1} \rangle.$$

Let F be the field of p elements, where p is a prime greater than 2. Clearly, $|\{f^2 : f \in F\}| = |\{-1 - f^2 : f \in F\}| = \frac{p+1}{2}$, hence there exist c and d in F such that $c^2 + d^2 = -1$. Then we define $\theta : FG \to M_2(F\langle x \rangle)$ via

$$\theta(g) = \begin{pmatrix} c & d \\ d & -c \end{pmatrix}, \ \theta(h) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \text{ and } \theta(x) = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}.$$

This is easily seen to be a ring homomorphism. Let

$$\alpha = (x + x^{-1}g^2)(dg - h + cgh)(1 - g^2)$$

and

$$\beta = (x + x^{-1}g^2)(dg + h + cgh)(1 - g^2).$$

The key properties of α and β are that $\alpha, \beta \in (FG)^+$, $\alpha^2 = \beta^2 = 0$, and

$$\theta(\alpha) = \begin{pmatrix} 0 & 4(x^{-1} - x) \\ 0 & 0 \end{pmatrix}, \ \theta(\beta) = \begin{pmatrix} 0 & 0 \\ 4(x^{-1} - x) & 0 \end{pmatrix}.$$

(These facts can be easily verified.) We will use these definitions in the proof of the next lemma.

Lemma 4.4.9. *Let F be a field of characteristic $p > 2$, and $G = Q_8 \times \langle x \rangle$, where x is a p-element. If, for a particular $n \geq 2$, $\mathcal{U}^+(FG)$ satisfies $(u_1, \ldots, u_n) = 1$, then $o(x) \leq 2^{n+1} - 2$.*

Proof. Since $\mathcal{U}^+(FG)$ satisfies $(u_1, \ldots, u_n)$, so does $\mathcal{U}^+(\mathbb{F}_p G)$, hence we may assume that $F = \mathbb{F}_p$. In the above notation, $1 + \frac{\alpha}{4}$ is a symmetric unit with inverse $1 - \frac{\alpha}{4}$. Similarly, $1 + \frac{\beta}{4}$ is a symmetric unit, and

$$\theta(1 + \frac{\alpha}{4}) = \begin{pmatrix} 1 & x^{-1} - x \\ 0 & 1 \end{pmatrix} \text{ and } \theta(1 + \frac{\beta}{4}) = \begin{pmatrix} 1 & 0 \\ x^{-1} - x & 1 \end{pmatrix}.$$

Since the symmetric units satisfy $(u_1, \ldots, u_n) = 1$, their homomorphic images must satisfy this identity as well, hence

$$\begin{aligned} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} &= \left(\begin{pmatrix} 1 & x^{-1} - x \\ 0 & 1 \end{pmatrix}, \underbrace{\begin{pmatrix} 1 & 0 \\ x^{-1} - x & 1 \end{pmatrix}, \ldots, \begin{pmatrix} 1 & 0 \\ x^{-1} - x & 1 \end{pmatrix}}_{n-1 \text{ times}} \right) \\ &= \begin{pmatrix} w_1 & (x^{-1} - x)^{2^n - 1} \\ w_2 & w_3 \end{pmatrix} \end{aligned}$$

for some $w_1, w_2, w_3 \in F\langle x \rangle$, by Lemma 4.3.5.

Thus, $(x^{-1} - x)^{2^n - 1} = 0$, and therefore $0 = x^{2^n - 1}(x^{-1} - x)^{2^n - 1} = (1 - x^2)^{2^n - 1}$. Expanding this out, we see that the coefficient of $x^{2(2^n - 1)}$ is -1, and therefore this must cancel with one of the lower terms. That is, $x^{2^{n+1} - 2} = x^j$ for some $0 \leq j < 2^{n+1} - 2$, and we see that $o(x) \leq 2^{n+1} - 2$, as required. □

Lemma 4.4.10. *Suppose char $F = p > 2$, and $G = Q_8 \times P$, where P is a locally finite p-group. If $\mathcal{U}^+(FG)$ is nilpotent, then P is finite.*

Proof. Take $x \in P$. If $\mathcal{U}^+(FG)$ satisfies $(u_1, \ldots, u_n) = 1$, then $\mathcal{U}^+(F(Q_8 \times \langle x \rangle))$ satisfies $(u_1, \ldots, u_n) = 1$, and then Lemma 4.4.9 puts a bound on the order of x. Thus, P has bounded exponent. Furthermore, $\mathcal{U}^+(FP)$ is nilpotent, and so by Proposition 4.4.1, P' is finite. Suppose P is infinite. Then P/P' is an infinite abelian p-group of bounded exponent, which is central in $Q_8 \times (P/P')$. Also, $\mathcal{U}^+(F(G/P')) = \mathcal{U}^+(F(Q_8 \times (P/P')))$ is nilpotent, by Lemma 4.4.3. Thus, by Lemma 4.4.5, $(F(Q_8 \times (P/P')))^+$ is Lie nilpotent. But this contradicts Theorem 3.6.5. $\square$

This gives us our second main result for this section, namely

Proposition 4.4.11. *Let F be a field of characteristic $p > 2$. Suppose G is locally finite and $\mathcal{U}^+(FG)$ is nilpotent. If $Q_8 \subseteq G$, then $G \simeq Q_8 \times E \times P$, where $E^2 = 1$ and P is a finite p-group.*

Proof. By Proposition 4.3.1, $G \simeq A \times P$, where A is a Hamiltonian 2-group and P is a p-group. By Theorem 2.2.10, $A \simeq Q_8 \times E$, where $E^2 = 1$. Thus, $G \simeq Q_8 \times E \times P$, and therefore $\mathcal{U}^+(F(Q_8 \times P))$ is nilpotent. By Lemma 4.4.10, P is finite, and we are done. $\square$

If $G = Q_8 \times E \times P$, where $E^2 = 1$ and P is a finite p-group, then $\mathcal{U}^+(FG)$ is nilpotent, but we will postpone the proof of this until the end of the chapter.

4.5. The general case

We will now demonstrate that if $\mathcal{U}^+(FG)$ is nilpotent, then G is locally finite. This, combined with our results from the last section, will give us our main theorems for this chapter.

To begin with, let H be a group. We say that H satisfies a semigroup identity if there exist two distinct words of the form $x_{i_1} \cdots x_{i_n}$ and $x_{j_1} \cdots x_{j_m}$ in the free group with generators $x_1, \ldots, x_t$ such that

$$h_{i_1} \cdots h_{i_n} = h_{j_1} \cdots h_{j_m}$$

for all $h_r \in H$. Thus, if H satisfies a semigroup identity, then it satisfies a group identity. In [Okn, Theorem 7.2], it is shown that the nilpotency of H is equivalent to H satisfying one of a series of semigroup identities. As a consequence, we have

Lemma 4.5.1. *Let H be a nilpotent group. Then H satisfies a semigroup identity of the form*

$$x_{i_1} \cdots x_{i_n} = x_{j_1} \cdots x_{j_n}$$

for some $n \geq 1$.

This allows us to prove

Lemma 4.5.2. *Let F be any field and G any group. Suppose $\mathcal{U}^+(FG)$ is nilpotent. If S is a nil ideal of FG with $S^* = S$, then S satisfies a polynomial identity.*

Proof. By Lemma 4.3.2, $\langle \mathcal{U}^+(FG) \rangle$ is nilpotent. Therefore, by Lemma 4.5.1, $\langle \mathcal{U}^+(FG) \rangle$ satisfies a nontrivial semigroup identity of the form

$$x_{i_1} x_{i_2} \cdots x_{i_n} = x_{j_1} \cdots x_{j_n},$$

where $n \geq 1$. Take any $s_i \in S^+$. Then each $1 + s_i$ is a unit with inverse $1 - s_i + s_i^2 - \cdots$, since $s_i^k = 0$, for some k. Thus,

$$(1 + s_{i_1}) \cdots (1 + s_{i_n}) = (1 + s_{j_1}) \cdots (1 + s_{j_n}).$$

Expanding this expression, we obtain a polynomial in the s_i, where the only terms of highest degree are $s_{i_1} \cdots s_{i_n}$ and $s_{j_1} \cdots s_{j_n}$. Since the semigroup identity is nontrivial, these are not the same monomial, so S^+ satisfies a nontrivial polynomial identity. Of course, S is an F-algebra. Thus, by Theorem 2.4.6, S satisfies a polynomial identity. $\square$

We wish to show that if $\mathcal{U}^+(FG)$ is nilpotent and G has trivial centre, then $G = 1$. Let us handle the semiprime case first. We recall from Theorem 2.3.1

that FG is semiprime if and only if G has no finite normal subgroup H such that p divides $|H|$, where char $F = p > 0$. Or, equivalently, if and only if $\phi_p(G)$ is trivial. Here, $\phi_p(G)$ is the subgroup of $\phi(G)$ generated by its p-elements.

Lemma 4.5.3. *If char $F = p > 2$, G is torsion, FG is semiprime, $\mathcal{U}^+(FG)$ is nilpotent, and $\zeta(G) = 1$, then $G = 1$.*

Proof. If FG is prime, then Proposition 4.2.1 completes the proof, hence we may assume that G has a nontrivial finite normal subgroup N. Since FG is semiprime, N is a p'-group. Thus, N contains an element $h \neq 1$ such that either h has order 2, or h has odd, p'-order. Take any $g \in G$. Since N is normal, $\langle N, g\rangle = N\langle g\rangle$ is finite. But $\mathcal{U}^+(F\langle N, g\rangle)$ is nilpotent, and by Propositions 4.4.1 and 4.4.11, $\langle N, g\rangle$ is nilpotent and either $\langle N, g\rangle'$ is a p-group, or $\langle N, g\rangle \simeq Q_8 \times E \times P$, where $E^2 = 1$ and P is a p-group. Thus, $\langle N, g\rangle$ is a finite nilpotent group, and therefore it is the direct product of its Sylow subgroups. If $\langle N, g\rangle'$ is a p-group, then all of the Sylow subgroups except possibly the Sylow p-subgroup are abelian, hence any element of p'-order is central in $\langle N, g\rangle$. If $\langle N, g\rangle \simeq Q_8 \times E \times P$, then we see immediately that any element of order 2 is central, and there are no elements of odd, p'-order. That is, h is central in $\langle N, g\rangle$, hence h and g commute. But g was arbitrary, hence $h \in \zeta(G)$. This contradicts the assumption that G is centreless. $\square$

In any ring R, we let $N(R)$ denote the sum of all of the nilpotent ideals of R. We claim that $N(R)$ is a nil ideal. In fact, the sum of any collection of nil ideals is nil. Indeed, if r is in the sum of a collection of nil ideals, then it is in the sum of a finite collection of these ideals, hence we have only to prove it for finite sums of ideals. Thus, by induction, it suffices to show that the sum of two nil ideals is nil. Let I_1 and I_2 be nil ideals of R. Take $a \in I_1$ and $b \in I_2$. Suppose that $a^k = 0$. Then in R/I_2, $a + b + I_2 = a + I_2$, hence $(a + b + I_2)^k = a^k + I_2 = I_2$, and therefore $(a+b)^k \in I_2$. Thus, since I_2 is nil, $a+b$ is a nilpotent element, and we are done. However, $N(R)$ need not be nilpotent. Indeed, if char $F = p > 0$, and G is a group, then by a result of Passman [Pas1, Theorem 8.1.12], $N(FG)$ is nilpotent if and only if $\phi_p(G)$ is finite. We need this in order to prove

Lemma 4.5.4. *If char $F = p > 2$, G is torsion, $\mathcal{U}^+(FG)$ is nilpotent and $\zeta(G) = 1$, then $G = 1$.*

Proof. Let $N = N(FG)$. Suppose, first, that N is a nilpotent ideal. We observed above that in this case, $\phi_p(G)$ is finite. Let $\bar{G} = G/\phi_p(G)$. We claim that $F\bar{G}$ is semiprime. Suppose $g \in G$ is such that $\bar{g} \in \phi(\bar{G})$. Then there exist $g_1, \ldots, g_n \in G$ such that $\bar{y}^{-1}\bar{g}\bar{y} \in \{\bar{g}_1, \ldots, \bar{g}_n\}$, for all $y \in G$. That is,

$$y^{-1}gy \in \phi_p(G)g_1 \cup \phi_p(G)g_2 \cup \cdots \cup \phi_p(G)g_n,$$

which is a finite set. Thus, $g \in \phi(G)$. Clearly, then, $\phi(\bar{G}) = \phi(G)/\phi_p(G)$, which is a p'-group, hence $F\bar{G}$ is semiprime. We claim that $\zeta(\bar{G}) = \bar{1}$. Indeed, suppose $z \in G$ is such that $\bar{z} \in \zeta(\bar{G})$. Then $\bar{z} \in \phi(\bar{G})$, hence $z \in \phi(G)$. By Theorem 2.2.8, a torsion FC-group is locally finite. Since $\mathcal{U}^+(F(\phi(G)))$ is nilpotent, Propositions 4.4.1 and 4.4.11 show us that $\phi(G)$ is nilpotent. Thus, $\phi_p(G)$ is a p-group (since it is generated by p-elements), and we may write $z = z_1z_2$, where $z_1 \in \phi_p(G)$ and z_2 is a p'-element. But then $\bar{z} = \bar{z}_2$, so we will assume, without loss of generality, that z is a p'-element of G. Furthermore, since $z \in \phi(G)$, we have $y^{-1}zy \in \phi(G)$, for all $y \in G$. Then, since $\bar{z}^{-1}\bar{y}^{-1}\bar{z}\bar{y} = \bar{1}$, we have $z^{-1}y^{-1}zy \in \phi_p(G)$. But this element is the product of two p'-elements, z^{-1} and $y^{-1}zy$, in a nilpotent group, and so it is necessarily p'. Thus, $z^{-1}y^{-1}zy = 1$ for all $y \in G$, and $z \in \zeta(G)$, hence $z = 1$ and, in particular, $\bar{z} = \bar{1}$. That is, $G/\phi_p(G)$ is centreless and $F(G/\phi_p(G))$ is semiprime. Since $\mathcal{U}^+(F(G/\phi_p(G)))$ is nilpotent by Lemma 4.3.4, Lemma 4.5.3 tells us that $G/\phi_p(G)$ is trivial. Thus, G is a finite p-group, which can only be centreless if it is trivial.

Now, suppose N is not nilpotent. As we observed above, N is still a nil ideal. Clearly, if I is a nilpotent ideal of FG, then so is I^*, and therefore $N^* = N$. By Lemma 4.5.2, N satisfies a polynomial identity. We can apply the multilinearization process of §4.2 to this polynomial identity, and thereby obtain a (nontrivial) multilinear polynomial identity for N. Renumbering the variables and multiplying by a scalar if necessary, we may assume that N satisfies

$$\sum_{\sigma \in S_t} \alpha_\sigma x_{\sigma(1)} \cdots x_{\sigma(t)},$$

where each $\alpha_\sigma \in F$, $\alpha_1 = 1$, and $t \geq 1$. Since N is not nilpotent, we may choose $a_1, \ldots, a_t \in N$ such that $a_1 a_2 \cdots a_t \neq 0$. For any $y_1, \ldots, y_t \in FG$, we see that $a_i y_i \in N$ for all i, hence

$$\sum_{\sigma \in S_t} \alpha_\sigma a_{\sigma(1)} y_{\sigma(1)} \cdots a_{\sigma(t)} y_{\sigma(t)}$$

is a multilinear GPI for FG. If it is degenerate, then FG vanishes on the $\sigma = 1$ term, namely $a_1 y_1 \cdots a_t y_t$. But taking $y_1 = \cdots = y_t = 1$, we see that this is not the case. Therefore, FG satisfies a nondegenerate GPI, and by Theorem 4.2.2, $(G : \phi(G)) < \infty$ and $|(\phi(G))'| < \infty$. Clearly, then, G is locally finite, and it follows from Propositions 4.4.1 and 4.4.11 that G is nilpotent. But a centreless nilpotent group is trivial. □

In order to show that G is locally finite, we will show that any finitely generated subgroup of G must be hypercentral. We have

Lemma 4.5.5. *Let F be a field of characteristic greater than 2, and let G be any group. Suppose $\mathcal{U}^+(FG)$ satisfies the group identity $(u_1, \ldots, u_n)$, for some $n \geq 2$. Further suppose that there is an ascending series of normal subgroups of G,*

$$N_0 \subseteq N_1 \subseteq \cdots \subseteq N_\alpha \subseteq N_{\alpha+1} \subseteq \cdots$$

indexed by the ordinals, such that for some ordinal β, $N_\beta = \bigcup_{\alpha<\beta} N_\alpha$. If, for all $\alpha < \beta$, $\mathcal{U}^+(F(G/N_\alpha))$ satisfies $(u_1, \ldots, u_n)$, then $\mathcal{U}^+(F(G/N_\beta))$ satisfies $(u_1, \ldots, u_n)$.

Proof. For any normal subgroup N of G, we will let $\epsilon_N : FG \to F(G/N)$ denote the natural map. Suppose that $\mathcal{U}^+(F(G/N_\beta))$ does not satisfy $(u_1, \ldots, u_n)$. Take $\eta_1, \ldots, \eta_n \in \mathcal{U}^+(F(G/N_\beta))$ such that $(\eta_1, \ldots, \eta_n) \neq 1$. Since $\epsilon_N((FG)^+) = (F(G/N))^+$ for any normal subgroup N, let us choose $\gamma_i \in (FG)^+$ such that $\epsilon_{N_\beta}(\gamma_i) = \eta_i$. Suppose we can show that for some $\alpha < \beta$, the $\epsilon_{N_\alpha}(\gamma_i)$ are units, for all i. Then since they are clearly symmetric,

$$(\epsilon_{N_\alpha}(\gamma_1), \ldots, \epsilon_{N_\alpha}(\gamma_n)) = 1,$$

by assumption. In this case,

$$(\epsilon_{N_\beta}(\gamma_1), \ldots, \epsilon_{N_\beta}(\gamma_n)) = 1,$$

which is a contradiction.

Therefore, it remains to show that there exists an $\alpha < \beta$ such that $\epsilon_{N_\alpha}(\gamma_i)$ is a unit, for each i. But each η_i is a unit, so there exist $\rho_1, \ldots, \rho_n \in \mathcal{U}(F(G/N_\beta))$ such that each $\rho_i = \eta_i^{-1}$. Take $\theta_1, \ldots, \theta_n \in FG$ such that $\epsilon_{N_\beta}(\theta_i) = \rho_i$. Thus, $\epsilon_{N_\beta}(\gamma_i\theta_i) = \eta_i\rho_i = 1$, and $\epsilon_{N_\beta}(\theta_i\gamma_i) = \rho_i\eta_i = 1$, for all i. That is, $\gamma_i\theta_i - 1$ and $\theta_i\gamma_i - 1$ are in $\Delta_F(G, N_\beta)$. Thus,

$$\gamma_i\theta_i - 1 = \sum_j \mu_{ij}(n_{ij} - 1)$$

and

$$\theta_i\gamma_i - 1 = \sum_j \mu'_{ij}(n'_{ij} - 1)$$

with each $\mu_{ij}, \mu'_{ij} \in FG$, and each $n_{ij}, n'_{ij} \in N_\beta$. Since there are only finitely many n_{ij} and n'_{ij}, and N_β is the union of the N_α, with $\alpha < \beta$, there exists an $\alpha < \beta$ such that $n_{ij}, n'_{ij} \in N_\alpha$ for all i and j. Thus, each $\gamma_i\theta_i - 1, \theta_i\gamma_i - 1 \in$

$\Delta_F(G, N_\alpha)$, so $\epsilon_{N_\alpha}(\gamma_i)\epsilon_{N_\alpha}(\theta_i) = 1$ and $\epsilon_{N_\alpha}(\theta_i)\epsilon_{N_\alpha}(\gamma_i) = 1$, for all i, which is what we wanted. □

Recall that we let $\zeta_\alpha(G)$ denote the α-th term of the transfinitely extended upper central series of G.

Lemma 4.5.6. *Suppose char $F = p > 2$ and G is a countable torsion group. Further suppose that $\mathcal{U}^+(FG)$ satisfies the identity $(u_1, \ldots, u_n)$, for some $n \geq 2$. Then for any α, $\mathcal{U}^+(F(G/\zeta_\alpha(G)))$ satisfies $(u_1, \ldots, u_n)$.*

Proof. Our proof is by transfinite induction. If α is a limit ordinal, then Lemma 4.5.5 does the job. Otherwise, we will assume that $\mathcal{U}^+(F(G/\zeta_\alpha(G)))$ satisfies the identity $(u_1, \ldots, u_n)$ and prove that $\mathcal{U}^+(F(G/\zeta_{\alpha+1}(G)))$ satisfies $(u_1, \ldots, u_n)$. Now,

$$G/\zeta_{\alpha+1}(G) \simeq (G/\zeta_\alpha(G))/(\zeta_{\alpha+1}(G)/\zeta_\alpha(G)) = (G/\zeta_\alpha(G))/\zeta(G/\zeta_\alpha(G)).$$

Thus, it remains to check that if $\mathcal{U}^+(FG)$ satisfies $(u_1, \ldots, u_n)$ for some countable group G, then $\mathcal{U}^+(F(G/\zeta(G)))$ satisfies $(u_1, \ldots, u_n)$. Of course, $\zeta(G)$ is countable. If it is finite, then Lemma 4.4.2 finishes the proof. Otherwise, let $\zeta(G) = \{g_1, g_2, \ldots\}$. We will define a series of central subgroups of G as follows. Let $N_0 = 1$, and for each $k \geq 1$, $N_k = \langle N_{k-1}, g_k \rangle$. Since each N_k is a finitely generated torsion abelian group, it is finite, and then by Lemma 4.4.2, each $\mathcal{U}^+(F(G/N_k))$ satisfies $(u_1, \ldots, u_n)$. Also, $N_0 \subseteq N_1 \subseteq \cdots$ and $\zeta(G) = \bigcup_{k=0}^{\infty} N_k$. Therefore, by Lemma 4.5.5, $\mathcal{U}^+(F(G/\zeta(G)))$ satisfies $(u_1, \ldots, u_n)$. □

This gives us what we have been looking for, namely

Lemma 4.5.7. *Let F be a field of characteristic $p > 2$ and let G be a torsion group. If $\mathcal{U}^+(FG)$ is nilpotent, then G is locally finite.*

Proof. Suppose this is not true. Take a finitely generated subgroup H of G which is not finite. Then H is countable, and $\mathcal{U}^+(FH)$ is nilpotent. Let K be the hypercentre of H. By Lemma 4.5.6, $\mathcal{U}^+(F(H/K))$ is nilpotent. But H/K is centreless, so Lemma 4.5.4 implies that $H = K$. That is, H is hypercentral. By Proposition 2.2.3, H is locally nilpotent, hence locally finite, and since H is finitely generated, it is finite. We have a contradiction. $\square$

Incidentally, we now have

Proposition 4.5.8. *Suppose G is a torsion group, and F is a field of characteristic different from 2. If $\mathcal{U}^+(FG)$ satisfies $(x_1, \ldots, x_n)$ for a fixed $n \geq 2$, then for any normal subgroup N of G, $\mathcal{U}^+(F(G/N))$ satisfies $(x_1, \ldots, x_n)$.*

Proof. Suppose char $F = 0$. Then by Proposition 4.1.8, G is abelian or a Hamiltonian 2-group. Thus, by Lemma 3.1.4, $(FG)^+$ is commutative, hence $\mathcal{U}^+(FG)$ satisfies (x_1, x_2), and therefore $(x_1, \ldots, x_n)$. If char $F > 2$, then combining Lemmata 4.5.7 and 4.4.3, we get our result. $\square$

Time to finish up. Our first main result for the chapter is

Theorem 4.5.9. *Let F be a field of characteristic $p \neq 2$, and G a torsion group not containing Q_8. Then the following are equivalent:*

(1) *$\mathcal{U}^+(FG)$ is nilpotent;*

(2) *$\mathcal{U}(FG)$ is nilpotent; and,*

(3) *G is nilpotent and p-abelian.*

Proof. Suppose $\mathcal{U}^+(FG)$ is nilpotent. If char $F = 0$, then by Proposition 4.1.8, G is abelian, giving (3). If char $F > 2$, then combining Lemma 4.5.7 with Proposition 4.4.1, we get (3). Thus, (1) implies (3). Clearly, (2) implies (1). Assume (3). Thus G is nilpotent and p-abelian. If char $F = 0$, there is nothing to do, so assume $p > 2$. If G contains a p-element, then by Theorem 4.1.3, $\mathcal{U}(FG)$ is nilpotent. If G contains no p-elements, then it is abelian, hence (3) implies (2), and we are done. □

Finally, let us complete the case in which $Q_8 \subseteq G$. We recall that for a ring, R, and a subset, Λ, of R, we define a sequence of associative ideals of R as follows. We let $\Lambda_{(0)} = R$, and for each $i \geq 0$, $\Lambda_{(i+1)}$ is the ideal generated by all of the Lie commutators $[\alpha, \beta]$, where $\alpha \in \Lambda_{(i)}$, $\beta \in \Lambda$. Our second main result is

Theorem 4.5.10. *Let F be a field of characteristic $p \neq 2$, and G a torsion group containing Q_8. Then $\mathcal{U}^+(FG)$ is nilpotent if and only if either*

(1) *$p > 2$ and $G \simeq Q_8 \times E \times P$, where $E^2 = 1$ and P is a finite p-group, or*

(2) *$p = 0$ and $G \simeq Q_8 \times E$, where $E^2 = 1$.*

Proof. If char $F = 0$, then Proposition 4.1.8 tells us what we need to know. Suppose $p > 2$. If $\mathcal{U}^+(FG)$ is nilpotent, then by Lemma 4.5.7 and Proposition 4.4.11, we see that $G \simeq Q_8 \times E \times P$, where $E^2 = 1$ and P is a finite p-group. Now, let us consider the converse.

Suppose $G = Q_8 \times E \times P$, where $E^2 = 1$ and P is a group of order p^m, for some $m \geq 0$. We claim that for each positive integer n, and any $\alpha, \beta_1, \dots, \beta_n \in \mathcal{U}^+(FG)$, we have

$$(\alpha, \beta_1, \dots, \beta_n) - 1 \in ((FG)^+)_{(n)}.$$

This will complete the proof, since $((FG)^+)_{(p^m)} = (0)$, by Lemma 3.6.4. Our proof is by induction on n. If $n = 1$, then

$$(\alpha, \beta_1) - 1 = \alpha^{-1}\beta_1^{-1}\alpha\beta_1 - 1 = \alpha^{-1}\beta_1^{-1}[\alpha, \beta_1] \in ((FG)^+)_{(1)}.$$

Then, assuming that $(\alpha, \beta_1, \ldots, \beta_n) - 1 \in ((FG)^+)_{(n)}$, we obtain

$$\begin{aligned}(\alpha, \beta_1, \ldots, \beta_n, \beta_{n+1}) - 1 &= (\alpha, \beta_1, \ldots, \beta_n)^{-1}\beta_{n+1}^{-1}(\alpha, \beta_1, \ldots, \beta_n)\beta_{n+1} - 1 \\ &= (\alpha, \beta_1, \ldots, \beta_n)^{-1}\beta_{n+1}^{-1}[(\alpha, \beta_1, \ldots, \beta_n), \beta_{n+1}] \\ &= (\alpha, \beta_1, \ldots, \beta_n)^{-1}\beta_{n+1}^{-1}[(\alpha, \beta_1, \ldots, \beta_n) - 1, \beta_{n+1}]\end{aligned}$$

which is in $((FG)^+)_{(n+1)}$, as required. $\square$

Comparing Theorems 4.5.9 and 4.5.10 with Theorems 3.6.1 and 3.6.5, we obtain the following interesting consequence.

Corollary 4.5.11. *Let F be a field of characteristic different from 2, and G a torsion group. Then $\mathcal{U}^+(FG)$ is nilpotent if and only if $(FG)^+$ is Lie nilpotent.*

We might also ask when $\mathcal{U}^+(FG)$ will be nilpotent if G is not torsion. But Theorem 4.5.9 will not hold in this case. Indeed, let G be an orderable group which is not nilpotent. By [Pas1, Corollary 13.2.8], any nonabelian free group will suffice. Of course, $\mathcal{U}(FG)$ contains G, hence $\mathcal{U}(FG)$ is not nilpotent. However, it is well-known (and easy to verify) that

$$\mathcal{U}(FG) = \{fg : f \in \mathcal{U}(F), g \in G\}.$$

Since G is torsion-free, it has no elements of order 2. Thus, $\mathcal{U}^+(FG) = \mathcal{U}(F)$, which is commutative, hence $\mathcal{U}^+(FG)$ is certainly nilpotent.

Chapter 5

TORSION MATRICES OVER GROUP RINGS

5.1. Background to the problem

Let us now switch gears and consider the integral group ring, $\mathbb{Z}G$. In the 1960's, Zassenhaus made a series of conjectures about the units of $\mathbb{Z}G$. The first of these, commonly known as (ZC1), is the following.

Conjecture 5.1.1 (Zassenhaus). *Let G be a finite group. If $u \in \mathcal{U}(\mathbb{Z}G)$, $u^m = 1$ for some positive integer m, and $\epsilon(u) = 1$, then there exists a unit α in the rational group algebra, $\mathbb{Q}G$, such that $\alpha^{-1}u\alpha \in G$.*

Here, we recall that $\epsilon : \mathbb{Z}G \to \mathbb{Z}$ is the augmentation map. A good deal of work has been done on this conjecture. It has been established for finite nilpotent groups (see [Seh2, Theorem 40.4]), and for various other classes of groups, but the problem remains open for finite groups in general.

In proving certain cases of this conjecture, it has been possible to translate the problem into a question about matrices, which is actually a generalization of the problem, and is interesting in its own right. (See, for instance, [MRSW].)

A version of this chapter has been accepted for publication. G. T. Lee, S. K. Sehgal, *Torsion matrices over commutative integral group rings*, Publicacions Matemàtiques (to appear).

Let us discuss this problem. We recall that for a ring, R, with identity, and a positive integer n, we let $GL_n(R)$ denote the group of invertible $n \times n$ matrices over R. Given any matrix $U = (u_{ij}) \in GL_n(\mathbb{Z}G)$, we define

$$\epsilon^* : GL_n(\mathbb{Z}G) \to GL_n(\mathbb{Z})$$

via

$$\epsilon^*(U) = (\epsilon(u_{ij})).$$

This is easily seen to be a group homomorphism. We let $SGL_n(\mathbb{Z}G)$ be the kernel of ϵ^*. That is, $SGL_n(\mathbb{Z}G)$ is the group of invertible $n \times n$ matrices over $\mathbb{Z}G$ with identity augmentation. We present

Problem 5.1.2. *Let G be a finite group and n a positive integer. Is is true that for every torsion matrix $U \in SGL_n(\mathbb{Z}G)$, U is conjugate in $GL_n(\mathbb{Q}G)$ to a diagonal matrix with group elements on the diagonal?*

Our interest lies in $\mathbb{Z}A$, where A is abelian. For abelian groups, this question has recently been linked to another interesting problem. We let Tr denote the usual trace of a matrix. Also, if $\alpha = \sum_{g \in A} \alpha_g g \in \mathbb{Z}A$, then we write $\alpha \geq 0$ if and only if $\alpha_g \geq 0$ for all $g \in A$.

Theorem 5.1.3 (Marciniak-Sehgal). *Let A be a finite abelian group, and n a positive integer. Let $U \in SGL_n(\mathbb{Z}A)$ be a torsion matrix. Then U is conjugate in $GL_n(\mathbb{Q}A)$ to a matrix $diag(g_1, \dots, g_n)$, with each $g_i \in A$, if and only if $Tr(U) \geq 0$.*

Proof. See [MS3, Proposition]. □

Theorem 5.1.3 allows us to translate the problem back from the matrix ring to the group ring. Let us consider Problem 5.1.2 for finite abelian groups A.

When $n = 1$, this amounts to asking if the only torsion units of $\mathbb{Z}A$ are $\pm A$. But a positive answer to this question is a classical theorem of Higman (see [Seh2, Corollary 1.6]). When $n = 2$, Luthar and Passi obtained an affirmative answer for all finite abelian groups, A, if $\mathbb{Q}A$ is replaced with $\mathbb{C}A$, the complex group algebra. (See [LuP, Theorem 3.1].) Recently, however, the following result was obtained.

Theorem 5.1.4 (Marciniak-Sehgal). *Let A be a finite abelian group, and $n \leq 5$. Then every torsion matrix $U \in SGL_n(\mathbb{Z}A)$ is conjugate in $GL_n(\mathbb{Q}A)$ to a diagonal matrix with group elements on the diagonal.*

Proof. This is the main result of [MS3]. □

In fact, it is also known that this last result cannot be extended beyond $n = 5$, because of the following counterexample.

Example 5.1.5 (Cliff-Weiss). Let $A = C_6 \times C_6$, the direct product of two cyclic groups of order 6. Then there exists a torsion matrix $U \in SGL_6(\mathbb{Z}A)$ such that U is not conjugate in $GL_6(\mathbb{Q}A)$ to any matrix of the form $\operatorname{diag}(g_1, \ldots, g_6)$, with each $g_i \in A$. (See [ClW].)

Cliff and Weiss actually constructed the counterexample explicitly. Of course, this gives us a counterexample for $n > 6$ as well. Indeed, let U be the matrix from Example 5.1.5. By Theorem 5.1.3, $\mathrm{Tr}(U) \not\geq 0$. Let us say that the coefficient of g_0 in $\mathrm{Tr}(U)$ is negative. Now,

$$\epsilon(\mathrm{Tr}(U)) = \mathrm{Tr}(\epsilon^*(U)) = \mathrm{Tr}(I_6) = 6 > 0,$$

hence there exists some $g_1 \in A$ such that the coefficient of g_1 in $\mathrm{Tr}(U)$ is positive. Let

$$V = U \oplus g_1 I_{n-6} \in GL_n(\mathbb{Z}A).$$

Clearly, $V \in SGL_n(\mathbb{Z}A)$, and $V^6 = I_n$, since $U^6 = I_6$ and A has exponent 6. But $\mathrm{Tr}(V) = \mathrm{Tr}(U) + (n-6)g_1$, hence the coefficient of g_0 in $\mathrm{Tr}(V)$ is negative and therefore, by Theorem 5.1.3, we obtain a negative answer to Problem 5.1.2 for the group $C_6 \times C_6$ and all $n \geq 6$.

Thus, we will obtain an affirmative answer for all finite abelian groups A if and only if $n \leq 5$. The next question would be, for which finite abelian groups A do we obtain a positive answer for all n? The answer is found in

Theorem 5.1.6 (Cliff-Weiss). *Let G be a finite nilpotent group. Then the following are equivalent:*

(1) *for every positive integer n, and every torsion matrix $U \in SGL_n(\mathbb{Z}G)$, U is conjugate in $GL_n(\mathbb{Q}G)$ to a diagonal matrix with group elements on the diagonal, and*

(2) *G has at most one non-cyclic Sylow subgroup.*

Proof. See [ClW, Theorem 6.3]. □

Our question, then, is this. Suppose A has two or more non-cyclic Sylow subgroups. Can we obtain an affirmative answer to Problem 5.1.2 for particular values of $n \geq 6$? The following result has been known for some time.

Theorem 5.1.7 (Marciniak-Ritter-Sehgal-Weiss). *Let A be a finite abelian group, and n a positive integer, such that $n < p$ for every prime p dividing $|A|$. Then for every torsion matrix $U \in SGL_n(\mathbb{Z}A)$, U is conjugate in $GL_n(\mathbb{Q}A)$ to a matrix $diag(g_1, \dots, g_n)$, with each $g_i \in A$.*

Proof. See [MRSW, Theorem 4.6]. □

However, in view of Theorem 5.1.6, it seems reasonable to believe that we could obtain an affirmative answer just by restricting the Sylow subgroups which are not cyclic. Our main result for finite groups is the following.

Theorem 5.1.8. *Let A be a finite abelian group and $n \geq 6$. Suppose that either*

(1) *A has at most one non-cyclic Sylow subgroup, or*

(2) *if q_1 and q_2 are the two smallest (distinct) primes such that the Sylow q_1- and q_2-subgroups of A are non-cyclic, then $q_1 + q_2 > \frac{n^2+n-8}{4}$.*

Then for any torsion matrix $U \in SGL_n(\mathbb{Z}A)$, U is conjugate in $GL_n(\mathbb{Q}A)$ to a diagonal matrix with group elements on the diagonal.

The next section will be devoted to the proof of this result, and the final section will examine some generalizations to infinite groups.

5.2. Finite groups

Let us prove Theorem 5.1.8. We will follow the same plan of attack as in [MS3]. Fix a number $n \geq 6$, and suppose the theorem fails for n. Choose an abelian group A, of minimal order, which provides us with a counterexample U. That is, $U \in SGL_n(\mathbb{Z}A)$, U is torsion, and U is not conjugate in $GL_n(\mathbb{Q}A)$ to any diagonal matrix with group elements on the diagonal. By Theorem 5.1.3, $\mathrm{Tr}(U) \not\geq 0$. Thus, there exists $h \in A$ such that the coefficient of h in $\mathrm{Tr}(U)$ is negative. Now, $h^{-1}U \in SGL_n(\mathbb{Z}A)$, $h^{-1}U$ is torsion, and $\mathrm{Tr}(h^{-1}U) = h^{-1}\mathrm{Tr}(U)$. Thus, the coefficient of 1 in $\mathrm{Tr}(h^{-1}U)$ is negative. Replacing U with $h^{-1}U$, we will assume that the coefficient of 1 in $\mathrm{Tr}(U)$ is negative.

Now, let $\alpha = \mathrm{Tr}(U)$, and let S_+ be the set of elements of A with positive coefficients in α, and S_- the set with negative coefficients. Then we may write

$$\alpha = \alpha_+ - \alpha_-$$

where S_+ is the support of α_+, S_- is the support of α_-, and $\alpha_+ \geq 0$, $\alpha_- \geq 0$. Notice also that S_+ and S_- are disjoint, and $1 \in S_-$. Let us explicitly write

$$\alpha_+ = \sum_{g \in S_+} \alpha_g g, \ \alpha_- = \sum_{g \in S_-} \alpha_g g.$$

We will need to use the following result from [LuP]. Let G be a finite group, and let $C_1, \dots, C_r$ be the conjugacy classes of G. Write $h_i = |C_i|$. Take any matrix V with entries in $\mathbb{C}G$. We may write $V = \sum_{g \in G} V_g g$, where each V_g has complex entries. Also, for each i, let $\nu_i(V) = \sum_{g \in C_i} \mathrm{Tr}(V_g)$. The lemma we require is

Lemma 5.2.1 (Luthar-Passi). *If V is a torsion matrix in $GL_n(\mathbb{C}G)$, then*

$$\sum_{i=1}^{r} \frac{|\nu_i(V)|^2}{h_i} \leq n^2,$$

with equality holding if and only if V is a central matrix. If $V \in GL_n(\mathbb{Z}G)$, then equality holds if and only if $V = \pm g I_n$, for some $g \in G$.

Proof. See [LuP, Corollary 2.3]. □

For our purposes, this gives

Lemma 5.2.2. *(a) $\sum_{g \in S_+} \alpha_g - \sum_{g \in S_-} \alpha_g = n$, and (b) $\sum_{g \in A} \alpha_g^2 < n^2$.*

Proof. To get (a), we note that

$$\sum_{g \in S_+} \alpha_g - \sum_{g \in S_-} \alpha_g = \epsilon(\mathrm{Tr}(U)) = \mathrm{Tr}(\epsilon^*(U)) = \mathrm{Tr}(I_n) = n.$$

Now, let us prove (b). Since A is abelian, its conjugacy classes have only 1 element. Thus, each $\nu_i(U)$ (in the notation of Lemma 5.2.1) is simply $\mathrm{Tr}(U_g)$, where $U = \sum_{g \in A} U_g g$, and

$$\sum_{g \in A} \mathrm{Tr}(U_g) g = \mathrm{Tr}(U) = \sum_{g \in A} \pm \alpha_g g.$$

Therefore, by Lemma 5.2.1,

$$\sum_{g \in A} \alpha_g^2 \leq n^2$$

with equality if and only if $U = \pm gI_n$ for some $g \in A$. But $U \in SGL_n(\mathbb{Z}A)$, hence $U \neq -gI_n$, and if $U = gI_n$, then U is not a counterexample to Theorem 5.1.8, contrary to our assumption. Thus, the inequality is strict, as required. $\square$

Let us restrict the size of S_+. We have

Lemma 5.2.3. $|S_+| \leq \frac{n^2+n}{2} - 1$.

Proof. Suppose this is not the case. Then $\epsilon(\alpha_+) \geq |S_+| \geq \frac{n^2+n}{2}$ (since the coefficients of α_+ are positive). By Lemma 5.2.2,

$$\epsilon(\alpha_-) = \epsilon(\alpha_+) - n \geq \frac{n^2 - n}{2}.$$

Thus, by Lemma 5.2.2, since the cofficients of α_+ and α_- are positive integers, we have

$$n^2 > \sum_{g \in A} \alpha_g^2 \geq \sum_{g \in S_+} \alpha_g + \sum_{g \in S_-} \alpha_g \geq \frac{n^2 + n}{2} + \frac{n^2 - n}{2} = n^2$$

which is a contradiction. $\square$

For each prime p, let $\mathcal{E}_p$ be the set of all subgroups of order p in A. Let $\mathcal{E} = \bigcup_p \mathcal{E}_p$. We define σ to be $|\mathcal{E}|$, the number of subgroups of A of prime order. If A has at most one non-cyclic Sylow subgroup, then by Theorem 5.1.6, we obtain an affirmative answer to Problem 5.1.2 for A, for all positive integers n, hence A is not a counterexample to Theorem 5.1.8, contrary to our assumption. Thus, A has at least two non-cyclic Sylow subgroups, and q_1 and q_2 are the two smallest primes such that the Sylow q_1- and q_2-subgroups of A are non-cyclic. Clearly, then, A contains a copy of the group $C_{q_1} \times C_{q_1} \times C_{q_2} \times C_{q_2}$. It is easy to verify that $C_{q_1} \times C_{q_1}$ contains $q_1 + 1$ subgroups of prime order, and similarly for $C_{q_2} \times C_{q_2}$, so $\sigma \geq q_1 + q_2 + 2$. By the restriction placed upon q_1 and q_2 in Theorem 5.1.8, this implies that $\sigma > \frac{n^2+n}{4}$. For any $x \in S_-$ and any $H \in \mathcal{E}$, we let $T_{x,H} = Hx \cap S_+$.

Let us prove

Lemma 5.2.4. *No $T_{x,H}$ is empty.*

Proof. We have the usual projection $\pi : \mathbb{Z}A \to \mathbb{Z}(A/H)$. Applying π to each element in any matrix, we obtain a group homomorphism

$$\pi^* : GL_n(\mathbb{Z}A) \to GL_n(\mathbb{Z}(A/H)).$$

Since U is torsion, $\pi^*(U)$ is torsion, and it is easy to verify that $\pi^*(U)$ has identity augmentation. That is, $\pi^*(U) \in SGL_n(\mathbb{Z}(A/H))$. Now, let p be any prime, and P the Sylow p-subgroup of A. Then it is clear that PH/H is the Sylow p-subgroup of A/H. Thus, if the Sylow p-subgroup of A is cyclic, then the Sylow p-subgroup of A/H is cyclic. It follows that A/H is a group of the type discussed in Theorem 5.1.8. Since A is a group of minimal order which provides a counterexample, $\pi(\alpha) = \mathrm{Tr}(\pi^*(U)) \geq 0$. Now, the coefficients of α_- are positive, hence they do not cancel each other out when we apply π. Thus, since $x \in S_-$, $\pi(x)$ is in the support of $\pi(\alpha_-)$. But $\pi(\alpha) = \pi(\alpha_+) - \pi(\alpha_-)$, and $\pi(\alpha) \geq 0$, hence $\pi(x)$ must also appear in the support of $\pi(\alpha_+)$. That is, there exists some group element y such that

$$y \in S_+ \cap \pi^{-1}(\pi(x)) = S_+ \cap Hx = T_{x,H},$$

and $T_{x,H}$ is nonempty. □

We will now examine the intersections between the various sets $T_{x,H}$.

Lemma 5.2.5. *The sets $T_{x,H}$ have the following properties.*

(1) *For any $H \in \mathcal{E}$ and $x, y \in S_-$, the sets $T_{x,H}$ and $T_{y,H}$ are either disjoint or identical. In fact, they coincide if and only if $xy^{-1} \in H$.*

(2) *Assume $H, K \in \mathcal{E}$, with $H \neq K$. For any $x, y \in S_-$, if $T_{x,H} \cap T_{y,K}$ is nonempty, then $xy^{-1} \in HK \backslash (H \cup K)$ and $|T_{x,H} \cap T_{y,K}| = 1$.*

Proof. (1) It is a basic property of cosets that Hx and Hy are either disjoint or coincide, and the latter occurs if and only if $xy^{-1} \in H$. Since $T_{x,H} = Hx \cap S_+$, there is nothing more to do.

(2) Suppose $T_{x,H} \cap T_{y,K}$ is not the empty set. Then let us say $g \in Hx \cap Ky \cap S_+$. Thus, $g \in HKx \cap HKy$, hence $xy^{-1} \in HK$, by the same basic property of cosets. Suppose $xy^{-1} \in H \cup K$. Without loss of generality, we will say that $xy^{-1} \in K$. Since $g \in Hx$, $gx^{-1} \in H$. But $gx^{-1} = (gy^{-1})(yx^{-1})$. Since $g \in Ky$, $gy^{-1} \in K$, and $yx^{-1} = (xy^{-1})^{-1} \in K$, hence $gx^{-1} \in H \cap K$. But H and K are distinct subgroups of prime order, and therefore $H \cap K = 1$. Thus, $gx^{-1} = 1$, and therefore $g = x \in S_-$. But $g \in S_+$, and S_+ and S_- are disjoint. This is a contradiction, proving the first part of (2). Now, suppose $g_1, g_2 \in T_{x,H} \cap T_{y,K}$. Then g_1x^{-1} and g_2x^{-1} lie in H, hence $g_1g_2^{-1} \in H$, and similarly, $g_1g_2^{-1} \in K$, hence $g_1 = g_2$. That is, $T_{x,H} \cap T_{y,K}$ contains only one element. □

Take any $x \in S_-$, and let $T_x = \bigcup_{H \in \mathcal{E}} T_{x,H}$. If H and K are distinct elements of $\mathcal{E}$, then since $xx^{-1} = 1 \in H \cup K$, we see from Lemma 5.2.5 that $T_{x,H}$ and $T_{x,K}$ are disjoint. Thus, T_x is a subset of S_+ which is a union of σ pairwise disjoint, and nonempty (by Lemma 5.2.4) sets. Therefore $|T_x| \geq \sigma > \frac{n^2+n}{4}$. Let us consider the intersections of the various sets T_x.

Lemma 5.2.6. *Let x and y be distinct elements of S_-. If $T_x \cap T_y$ is nonempty, then either*

(i) xy^{-1} has order pq for distinct primes p and q, and then $|T_x \cap T_y| \leq 2$; or,

(ii) xy^{-1} is a p-element for some prime p, and $T_x \cap T_y \subseteq \bigcup_{H,K \in \mathcal{E}_p} T_{x,H} \cap T_{y,K}$.

Proof. We know that the sets $\bigcup_{H \in \mathcal{E}} T_{x,H}$ and $\bigcup_{K \in \mathcal{E}} T_{y,K}$ interesect, hence there exist $H, K \in \mathcal{E}$ such that $T_{x,H}$ and $T_{y,K}$ intersect. Let us say $H \in \mathcal{E}_p$, $K \in \mathcal{E}_q$, for (not necessarily distinct) primes p and q. First, suppose $p = q$. Lemma 5.2.5 gives us two possibilities, but in either of them, $xy^{-1} \in HK$. Therefore, xy^{-1} is a p-element.

Now, suppose that $p \neq q$. Then, of course, $H \neq K$, hence by part (2) of Lemma 5.2.5, $xy^{-1} \in HK \backslash (H \cup K)$. But the elements of HK, excluding H and K, all have order pq. Thus, the two possiblities for the order of xy^{-1} are established. Continuing with the $p \neq q$ case, we have $\langle xy^{-1} \rangle = HK$, since $o(xy^{-1}) = pq$. Thus, H (resp. K) is the unique Sylow p-subgroup (resp. Sylow q-subgroup) of $\langle xy^{-1} \rangle$. In particular, then, if H_1 and K_1 are any other pair of elements of $\mathcal{E}$, then they are not the Sylow subgroups of $\langle xy^{-1} \rangle$, hence $T_{x,H_1} \cap T_{y,K_1}$ is empty. (If H_1 and K_1 have the same order, then we have already seen that if $T_{x,H_1} \cap T_{y,K_1}$ is nonempty, then xy^{-1} is a p-element, which is a contradiction.) Thus,

$$|T_x \cap T_y| = |(T_{x,H} \cap T_{y,K}) \cup (T_{x,K} \cap T_{y,H})| \leq 2,$$

by Lemma 5.2.5.

Let us complete the $p = q$ case. If $T_{x,H_1} \cap T_{y,K_1}$ is nonempty, for some $H_1 \in \mathcal{E}_{p_1}$, $K_1 \in \mathcal{E}_{p_2}$, where $p_1 \neq p_2$, then we saw earlier that xy^{-1} has order $p_1 p_2$, which is false. If $H_2, K_2 \in \mathcal{E}_{q_1}$, and $T_{x,H_2} \cap T_{y,K_2}$ is not the empty set, then since $xy^{-1} \in H_2 K_2$ by Lemma 5.2.5, xy^{-1} is a q_1-element. Since xy^{-1} is a p-element, $p = q_1$. Therefore, $T_{x,H}$ can meet $T_{y,K}$ only if $H, K \in \mathcal{E}_p$, and therefore

$$T_x \cap T_y \subseteq \bigcup_{H,K \in \mathcal{E}_p} (T_{x,H} \cap T_{y,K})$$

as required. $\square$

Next, let us put a lower bound on $\epsilon(\alpha_+)$.

Lemma 5.2.7. $\epsilon(\alpha_+) \geq \sigma \cdot \max\{\alpha_g : g \in S_-\}$.

Proof. Take any $g \in S_-$. We will show that $\epsilon(\alpha_+) \geq \sigma \alpha_g$. Take any subgroup $H \in \mathcal{E}$, and let $\pi : \mathbb{Z}A \to \mathbb{Z}(A/H)$ denote the natural projection. Also, let $\bar{g} = \pi(g)$. Then the coefficient of $\bar{g}$ in $\pi(\alpha_-)$ is β, where

$$\beta = \sum_{h \in S_- \cap \pi^{-1}(\bar{g})} \alpha_h.$$

But all of these α_h values are positive, and $g \in S_- \cap \pi^{-1}(\bar{g})$, hence $\beta \geq \alpha_g$. Similarly, the coefficient of $\bar{g}$ in $\pi(\alpha_+)$ is γ, where

$$\gamma = \sum_{h \in S_+ \cap \pi^{-1}(\bar{g})} \alpha_h = \sum_{h \in T_{g,H}} \alpha_h = \epsilon\Big(\sum_{h \in T_{g,H}} \alpha_h h\Big).$$

Now, we may apply π to each element of a matrix, obtaining a homomorphism π^*, and we get $\pi(\alpha) = \mathrm{Tr}(\pi^*(U))$. Here, $\pi^*(U)$ is a torsion matrix in $SGL_n(\mathbb{Z}(A/H))$. As we saw in the proof of Lemma 5.2.4, A/H satisfies the conditions of Theorem 5.1.8 hence, by the minimality of A, $\pi(\alpha) \geq 0$. That is, $\pi(\alpha_+) - \pi(\alpha_-) \geq 0$ and therefore, the coefficient of $\bar{g}$ in $\pi(\alpha_+) - \pi(\alpha_-)$ is greater than or equal to zero. Thus, $\gamma \geq \beta$. Therefore,

$$\epsilon\Big(\sum_{h \in T_{g,H}} \alpha_h h\Big) \geq \beta \geq \alpha_g.$$

Recalling that α_+ has positive coefficients, we have

$$\epsilon(\alpha_+) \geq \epsilon\Big(\sum_{h \in T_g} \alpha_h h\Big)$$

and since we have already seen that the union $\bigcup_{H \in \mathcal{E}} T_{g,H}$ is disjoint, we get

$$\epsilon(\alpha_+) \geq \sum_{H \in \mathcal{E}} \epsilon\Big(\sum_{h \in T_{g,H}} \alpha_h h\Big) \geq |\mathcal{E}|\alpha_g = \sigma\alpha_g,$$

as required. □

In fact, α_- must have a very simple form.

Lemma 5.2.8. $\alpha_- = \sum_{g \in S_-} g$. *In particular,* $\epsilon(\alpha_-) = |S_-|$.

Proof. Suppose that not all coefficients of α_- are 1. Then by Lemma 5.2.7, $\epsilon(\alpha_+) \geq 2\sigma > \frac{n^2+n}{2}$. By Lemma 5.2.2,

$$\epsilon(\alpha_-) = \epsilon(\alpha_+) - n > \frac{n^2 - n}{2}.$$

As in the proof of Lemma 5.2.3, we obtain a contradiction. □

Next, we need to know that S_- contains at least five elements. We have

Lemma 5.2.9. $|S_-| > \frac{n^2-3n}{4}$.

Proof. By Lemma 5.2.7, $\epsilon(\alpha_+) \geq \sigma > \frac{n^2+n}{4}$. Thus, $|S_-| = \epsilon(\alpha_-) = \epsilon(\alpha_+) - n > \frac{n^2-3n}{4}$. □

Clearly, since $n \geq 6$, this means $|S_-| > 4$. For any distinct $x, y \in S_-$, we say that T_x and T_y have a large intersection if xy^{-1} is a p-element. Otherwise, the intersection is said to be small. (By Lemma 5.2.6, the intersection can contain at most two elements in this case.)

Lemma 5.2.10. *There exist distinct elements x and y in S_- such that T_x and T_y have small intersection.*

Proof. Suppose all of the intersections $T_x \cap T_y$ are large. Then xy^{-1} is a p-element for some prime p. It is straightforward to verify that it must be the same prime p for all pairs x and y. Since $1 \in S_-$, S_- is contained in P, the Sylow p-subgroup of A. Suppose $g \in T_x \cap T_y$, for some distinct $x, y \in S_-$. Then by Lemma 5.2.6, $g \in T_{x,H} \cap T_{y,K}$ for some $H, K \in \mathcal{E}_p$. Thus, $g \in Hx$, so $gx^{-1} \in H \subseteq P$, and $x \in S_- \subseteq P$, hence $g \in P$. Thus, $T_x \cap T_y \subseteq P$, for all $x \neq y$ in S_-.

Now, fix any $x \in S_-$, and choose a prime q, different from p, which divides $|A|$. (This is possible, since $|A|$ is divisible by at least two primes, by assumption.) Take $H \in \mathcal{E}_q$. By Lemma 5.2.4, $T_{x,H}$ is not empty, say $g \in T_{x,H}$. If $g \in P$, then since $x \in S_- \subseteq P$, $gx^{-1} \in P$. Also, $g \in Hx$, hence $gx^{-1} \in P \cap H = 1$. Therefore, $g = x$. But $g \in S_+$, and $x \in S_-$, which gives us a contradiction. Therefore $g \in T_x \backslash P$.

We know that for any $x \neq y \in S_-$, $T_x \cap T_y \subseteq P$, hence

$$\bigcup_{y \in S_- \backslash \{x\}} (T_x \cap T_y) \subseteq P,$$

and therefore,

$$g \in T_x \backslash P \subseteq T_x \backslash (\bigcup_{y \in S_- \backslash \{x\}} (T_x \cap T_y)).$$

That is, each T_x contains an element which is not in any other T_y. Now, for any $x_i \in S_-$, $T_{x_i} \subseteq S_+$, and therefore, writing $S_- = \{x_1, x_2, \dots, x_{|S_-|}\}$, we have

$$T_{x_1} \cup T_{x_2} \cup \cdots \cup T_{x_{|S_-|}} \subseteq S_+.$$

But we recall that any T_{x_i} contains at least σ elements, and each new set in the union adds at least one new element. Therefore, $|S_+| \geq \sigma + |S_-| - 1$. But then

$$n = \epsilon(\alpha_+) - |S_-| \geq |S_+| - |S_-| \geq \sigma + |S_-| - 1 - |S_-| = \sigma - 1 > \frac{n^2+n}{4} - 1 > n$$

for $n \geq 6$. This is a contradiction. $\square$

Lemma 5.2.11. $|S_+| \geq 2\sigma - 1$.

Proof. We know that each $|T_u| \geq \sigma$. If any two such sets are disjoint, then $|S_+| \geq 2\sigma$, and we are done. Thus, we will assume that no two T_u's are disjoint. Suppose that for some pairwise distinct $x, y, z \in S_-$, T_x and T_y have small intersection, and T_y and T_z have small intersection. We have two cases. First, if T_x and T_z have small intersection, then

$$|T_x \cup T_y \cup T_z| = |T_x| + |T_y \backslash (T_x \cap T_y)| + |T_z \backslash ((T_x \cup T_y) \cap T_z)| \geq \sigma + (\sigma - 2) + (\sigma - 4)$$

since each set has order at least σ, and any pair has at most two elements in common. But then $|S_+| \geq 3\sigma - 6 > 2\sigma - 1$, since $\sigma > \frac{n^2+n}{4} > 10$. Second, if T_x and T_z have large intersection, then by Lemma 5.2.6, there exists a prime p such that $T_x \cap T_z \subseteq \bigcup_{H,K \in \mathcal{E}_p} T_{x,H} \cap T_{z,K} \subseteq \bigcup_{H \in \mathcal{E}_p} T_{x,H}$. Choose one of $\{q_1, q_2\}$ which is not p (without loss of generality, say q_1). Then $T_x \backslash (T_x \cap T_z) \supseteq \bigcup_{H \in \mathcal{E}_{q_1}} T_{x,H}$, since the $T_{x,H}$ are disjoint, for a fixed x, by Lemma 5.2.5. Again, we have

$$|T_x \cup T_y \cup T_z| = |T_y| + |T_z \backslash (T_z \cap T_y)| + |T_x \backslash (T_x \cap (T_y \cup T_z))|.$$

Now, $|T_y| \geq \sigma$, and since T_z and T_y have small intersection, $|T_z \backslash (T_z \cap T_y)| \geq \sigma - 2$. Also, $|T_x \backslash (T_x \cap T_z)| \geq |\bigcup_{H \in \mathcal{E}_{q_1}} T_{x,H}| \geq q_1 + 1$, since the $T_{x,H}$ are nonempty, disjoint, and there are at least $q_1 + 1$ of them by choice of q_1. Now, $|T_x \cap T_y| \leq 2$, hence $|T_x \backslash (T_x \cap (T_y \cup T_z))| \geq q_1 + 1 - 2 = q_1 - 1$. Thus,

$$|T_x \cup T_y \cup T_z| \geq \sigma + \sigma - 2 + q_1 - 1 \geq 2\sigma - 1,$$

since q_1, being a prime, is at least 2. This is what we wanted to know, and therefore

($*$) We may assume that, for any distinct $a, b, c \in S_-$, either T_a and T_b have large intersection, or T_b and T_c have large intersection.

We know from Lemma 5.2.10 that there exist distinct x and z in S_- such that T_x and T_z have small intersection. Since they cannot be disjoint, Lemma 5.2.6 tells us that xz^{-1} has order pq for distinct primes p and q. We know from Lemma 5.2.9 that $|S_-| \geq 5$, so let us say that v, w, x, y and z are distinct elements of S_-. By ($*$), T_x and T_y cannot have small intersection hence, by Lemma 5.2.6, xy^{-1} is an r-element for some prime r. If $p \neq r \neq q$, then $yz^{-1} = (xy^{-1})^{-1}xz^{-1}$ has order divisible by three primes, contradicting Lemma 5.2.6. Thus, xy^{-1} is a p-element or a q-element. Without loss of generality, it is a p-element. Then yz^{-1}, being the product of an element of order pq and a p-element, must have order q or pq (given the choices afforded by Lemma 5.2.6). In the latter case, T_y and T_z have small intersection, which is disallowed by ($*$), hence yz^{-1} is a q-element. Again by ($*$), T_x and T_w have large intersection, hence xw^{-1} is an r-element for some prime r. If $p \neq r \neq q$, then $zw^{-1} = (xz^{-1})^{-1}xw^{-1}$ has order divisible by p, q, and r, which is impossible. Thus, xw^{-1} is a p-element or a q-element. Suppose xw^{-1} is a p-element. Then since xy^{-1} is a p-element, so is $wy^{-1} = (xw^{-1})^{-1}xy^{-1}$. Now, $zw^{-1} = (xz^{-1})^{-1}xw^{-1}$. Since xz^{-1} has order pq and xw^{-1} is a p-element, zw^{-1} must have order q or pq. Once again, ($*$) disallows the latter, hence zw^{-1} is a q-element. But $wy^{-1} = (zw^{-1})^{-1}(yz^{-1})^{-1}$, and both zw^{-1} and yz^{-1} are q-elements. Therefore, wy^{-1} is both a p-element and a q-element, which is impossible. It follows that xw^{-1} must be a q-element. Thus, $wy^{-1} = (xw^{-1})^{-1}xy^{-1}$, being the product of a q-element and a p-element, has order pq.

Once again, T_x and T_v must have small intersection. Thus, xv^{-1} is an r-element for some prime r, and once again, $r = p$ or q. Suppose xv^{-1} is a p-element. Then $yv^{-1} = (xy^{-1})^{-1}xv^{-1}$, being a product of two p-elements, is a p-element. However, $zv^{-1} = (xz^{-1})^{-1}xv^{-1}$. Since xz^{-1} has order pq, and xv^{-1} is a p-element, we again see that zv^{-1} is a q-element. But yz^{-1} is also a q-element, hence $yv^{-1} = yz^{-1}zv^{-1}$ is both a p-element and a q-element, giving us a contradiction. Therefore, xv^{-1} is a q-element. But then $yv^{-1} = (xy^{-1})^{-1}xv^{-1}$ is the product of a p-element and a q-element, hence it has order pq. That is, T_y and T_v have small intersection, but T_w and T_y also have small intersection, and this contradicts $(*)$. The proof is complete. □

And now, the proof of Theorem 5.1.8 is basically done.

Proof of Theorem 5.1.8. By Lemma 5.2.11, $|S_+| \geq 2\sigma - 1$. But we know that $\sigma > \frac{n^2+n}{4}$, hence $|S_+| > \frac{n^2+n}{2} - 1$. This contradicts Lemma 5.2.3. □

Of course, the restriction placed upon the group becomes much harsher as n increases, but for small values of n, it is fairly mild. For instance, if $n = 6$, we are assuming that $q_1 + q_2 \geq 9$. In this case, the theorem reduces to

Corollary 5.2.12. *Let A be a finite abelian group. Suppose that at most one of the Sylow p-subgroups, $p \leq 5$, is non-cyclic. Then for any torsion matrix $U \in SGL_6(\mathbb{Z}A)$, U is conjugate in $GL_6(\mathbb{Q}A)$ to a diagonal matrix with group elements on the diagonal.*

We close this thesis by applying our results from the last section to obtain some theorems about $\mathbb{Z}A$, where A is an infinite abelian group. First, let us consider group traces. Let K be a field and R a K-algebra with identity. Let $[R, R]$ denote the K-subspace of R spanned by the Lie products $[a, b]$, with $a, b \in R$. Then for any positive integer n, we define the Bass rank map

$$r : M_n(R) \to R/[R, R]$$

via $r(B) = \mathrm{Tr}(B) + [R, R]$. This map is clearly K-linear, and $r(BC) = r(CB)$ for all $B, C \in M_n(R)$. Suppose $R = KG$, for some group G. Then we say that a matrix $B \in M_n(R)$ has a group trace if there exists a diagonal matrix $D = \mathrm{diag}(g_1, \ldots, g_n)$, with each $g_i \in G$, such that $r(B^k) = r(D^k)$ for all positive integers k. When G is abelian, this amounts to saying that $\mathrm{Tr}(B^k) = \sum_{i=1}^{n} g_i^k$ for all $k \geq 1$, for some fixed group elements $g_1, \ldots, g_n$. (See [BMS] and [ChP] for a more extensive discussion of the group trace property.) Clearly, if A is abelian and $B \in SGL_n(\mathbb{Z}A)$ is conjugate to a diagonal matrix $D = \mathrm{diag}(g_1, \ldots, g_n)$, then $\mathrm{Tr}(B^k) = \mathrm{Tr}(D^k)$ for all positive integers k, and therefore B has a group trace. In fact, more can be said. Making use of Theorem 5.1.7, the following result was proved.

Theorem 5.3.1 (Chadha-Passi). *Let A be an abelian group. Let n be a positive integer such that $n < p$ for every prime p such that A has a p-element. Then every torsion matrix $U \in SGL_n(\mathbb{Z}A)$ has a group trace.*

Proof. See [ChP, Theorem 3.3]. □

We would like to use our Theorem 5.1.8 to obtain another condition under which U will have a group trace. We will need to borrow two results. First,

Lemma 5.3.2 (Chadha-Passi). *Let A be a finitely generated abelian group. Let U be a torsion matrix in $GL_n(\mathbb{C}A)$, for some positive integer n. Then no element of infinite order in A appears in the support of $Tr(U^k)$, for any positive integer k.*

Proof. See [ChP, pp. 629–630]. □

The next lemma is [BMS, Proposition 15], simplified for abelian groups.

Lemma 5.3.3 (Bovdi-Marciniak-Sehgal). *Let G and H be abelian groups, and let $\beta : G \to H$ be a group homomorphism. Take any matrix $V \in M_n(\mathbb{Q}G)$, where n is a positive integer. Suppose that β is injective on the set*

$$\bigcup_{k=1}^{\infty} supp(Tr(V^k)).$$

Let $\beta^*(V)$ be the matrix obtained by applying β to each group element appearing in V. If $\beta^*(V)$ has a group trace, then V has a group trace.

We can now prove

Theorem 5.3.4. *Let A be an abelian group and n a positive integer. Suppose either that $n \leq 5$ or we have*

(1) *every finite subgroup of A has at most one non-cyclic Sylow subgroup; or,*

(2) *if q_1 and q_2 are the two smallest (distinct) primes such that the Sylow q_1- and q_2-subgroups of some finite subgroup of A are non-cyclic, then $q_1 + q_2 > \frac{n^2+n-8}{4}$.*

Then every torsion matrix $U \in SGL_n(\mathbb{Z}A)$ has a group trace.

Proof. Since the condition on A is certainly inherited by subgroups, there is no harm in assuming that A is generated by the group elements appearing in the support of one or more entries of U. In particular, we may assume that A is finitely generated. In this case, Lemma 5.3.2 says that the elements of infinite order in A do not appear in the support of $\mathrm{Tr}(U^r)$ for any $r \geq 1$. Let us write $A = T \times F$, where T is finite and F is a free abelian group. Then the support of $\mathrm{Tr}(U^r)$ is contained in T for all $r \geq 1$. Thus, letting $\beta : A \to T$ be the obvious projection, we note that β is injective on T, hence we see from Lemma 5.3.3 that if $\beta^*(U) \in SGL_n(\mathbb{Z}T)$ has a group trace, then U has a group trace. In effect, we have reduced the problem to the case in which A is finite. But by Theorem 5.1.4 (if $n \leq 5$) or Theorem 5.1.8 (if $n \geq 6$), U is conjugate to a diagonal matrix $\mathrm{diag}(g_1, \dots, g_n)$ in this case. It follows immediately that U has a group trace. □

Since we are dealing with abelian groups, the restriction on the Sylow subgroups of finite subgroups of A could be replaced with a restriction on the Sylow subgroups of A. However, requiring such subgroups to be cyclic is too strong a condition. For example, let p be a prime, and define a group with countably many generators $x_1, x_2, \dots$ such that $x_1^p = 1$ and $x_{i+1}^p = x_i$, for all $i \geq 1$. This is easily seen to be an infinite abelian p-group. However, every finite subgroup (indeed, every proper subgroup) of this group is cyclic. We call this group the quasicyclic p-group, and denote it by $\mathbb{Z}_{p^\infty}$. If p and q are distinct primes, then $\mathbb{Z}_{p^\infty} \times \mathbb{Z}_{q^\infty}$ does not have cyclic Sylow subgroups, but it would still satisfy part (1) of Theorem 5.3.4, no matter what p and q are.

When dealing with infinite groups, it would be rather optimistic to expect our matrix U to be conjugate to a diagonal matrix, particularly since even (ZC1) fails for infinite nilpotent groups (see [MS2]). Instead, let us introduce the following notion. Let K be a subfield of the complex numbers and G a group. For any positive integer n, we say that two matrices $A, B \in GL_n(KG)$ are stably conjugate if there exist roots of unity $\xi_1, \dots, \xi_k \in K$ such that

$$A \oplus \mathrm{diag}(\xi_1, \dots, \xi_k) \quad \text{and} \quad B \oplus \mathrm{diag}(\xi_1, \dots, \xi_k)$$

are conjugate in $GL_{n+k}(KG)$.

The Bass rank map r, described above, induces a rank function $r : K_0(R) \to R/[R, R]$. For details about this map, see [MS1, p. 572]. We mention it only in order to connect the following two results.

Theorem 5.3.5 (Marciniak-Sehgal). *Let G be a finitely generated nilpotent group, and let K be a characteristic zero splitting field for T, the (necessarily finite) subgroup of G consisting of its torsion elements. Then the rank map r is injective on $K_0(KG)$.*

Proof. See [MS1, Theorem 4.1]. □

Here, we recall that a field K of characteristic zero is said to be a splitting field for the finite group G if the simple Wedderburn components of KG are all matrix rings over K. We also recall the result of Brauer [CuR, Corollary 15.18] which states that if G has exponent n, and ξ is a primitive n-th root of unity in $\mathbb{C}$, then $\mathbb{Q}(\xi)$ is a splitting field for G.

Theorem 5.3.6 (Bovdi-Marciniak-Sehgal). *Let $K = \mathbb{Q}(\xi)$, where ξ is a primitive d-th root of unity. Let G be a group such that the rank map is injective on $K_0(KG)$. If $U \in GL_n(KG)$ satisfies $U^d = I_n$, then the following are equivalent:*

(1) *U is stably conjugate to a diagonal matrix with group elements on the diagonal, and*
(2) *U has a group trace.*

Proof. See [BMS, Proposition 14]. □

Combining these results, we obtain our final theorem. Letting $\overline{\mathbb{Q}}$ denote the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$, we have

Theorem 5.3.7. *Let A be an abelian group and n a positive integer. Suppose either that $n \leq 5$ or else (1) or (2) of Theorem 5.3.4 holds. Then every torsion matrix $U \in SGL_n(\mathbb{Z}A)$, regarded as a matrix in $GL_n(\overline{\mathbb{Q}}A)$, is stably conjugate to a diagonal matrix with group elements on the diagonal.*

Proof. Once again, we are free to assume that A is finitely generated. Let us write $A = T \times F$, where T is finite and F is a free abelian group. By Theorem 5.3.5, if K is a splitting field for T in $\mathbb{C}$, then the Bass rank map is injective on $K_0(KA)$. By Brauer's Theorem, this only requires K to contain a primitive e-th root of unity, where e is the exponent of T. Let $m = de$, where d is the multiplicative order of U. Then, let us take $K = \mathbb{Q}(\xi)$, where ξ is a primitive m-th root of unity. By Theorem 5.3.6, U is stably conjugate over KA to a diagonal matrix with group elements on the diagonal if and only if U has a group trace. But by Theorem 5.3.4, U does indeed have a group trace. Enlarging the field to $\overline{\mathbb{Q}}$ does not harm our conclusion. Therefore, we are done. $\square$

Remark. The definition of stable conjugacy in [BMS] is slightly different from the one we have used. In that paper, the scalars ξ_i were not assumed to be roots of unity. However, examining the relevant proofs (to wit, the proofs of Propositions 13 and 14), we can see that only roots of unity were used. In addition, in view of Theorem 5.3.1, it will also suffice to assume in Theorem 5.3.7 that $n < p$ for every prime p such that A has a p-element.

BIBLIOGRAPHY

[BMS] A. Bovdi, Z. Marciniak, and S. K. Sehgal, *Torsion units in infinite group rings*, J. Number Theory **47** (1994), 284–299.

[ChP] G. K. Chadha and I. B. S. Passi, *Bass conjecture and the group trace property*, Comm. Algebra **26** (1998), 627–639.

[ClW] G. Cliff and A. Weiss, *Finite groups of matrices over group rings*, Trans. Amer. Math. Soc. **352** (2000), 457–475.

[CuR] C. W. Curtis and I. Reiner, *Methods of representation theory, Vol. I*, Wiley-Interscience, New York, 1981.

[GJV] A. Giambruno, E. Jespers, and A. Valenti, *Group identities on units of rings*, Arch. Math. (Basel) **63** (1994), 291–296.

[GS] A. Giambruno and S. K. Sehgal, *Lie nilpotence of group rings*, Comm. Algebra **21** (1993), 4253–4261.

[GSV1] A. Giambruno, S. Sehgal, and A. Valenti, *Group algebras whose units satisfy a group identity*, Proc. Amer. Math. Soc. **125** (1997), 629–634.

[GSV2] A. Giambruno, S. K. Sehgal, and A. Valenti, *Symmetric units and group identities*, Manuscripta Math. **96** (1998), 443–461.

[Hal] M. Hall, *The theory of groups*, Macmillan, New York, 1959.

[Her] I. N. Herstein, *Rings with involution*, University of Chicago Press, Chicago, 1976.

[Hun] T. W. Hungerford, *Algebra*, Springer-Verlag, New York, 1974.

[KMRT] M.-A. Knus, A. Merkurjev, M. Rost, and J.-P. Tignol, *The book of involutions*, American Mathematical Society, Providence, Rhode Island, 1998.

[Lam] T. Y. Lam, *A first course in noncommutative rings*, Springer-Verlag, New York, 1991.

[Lee1] G. T. Lee, *Group rings whose symmetric elements are Lie nilpotent*, Proc. Amer. Math. Soc. **127** (1999), 3153–3159.

[Lee2] G. T. Lee, *The Lie n-Engel property in group rings*, Comm. Algebra **28** (2000), 867–881.

[Lee3] G. T. Lee, *Nilpotent symmetric units in group rings*, preprint.

[LeS] G. T. Lee and S. K. Sehgal, *Torsion matrices over commutative integral group rings*, Publ. Mat., to appear.

[Liu] C.-H. Liu, *Group algebras with units satisfying a group identity*, Proc. Amer. Math. Soc. **127** (1999), 327–336.

[LP] C.-H. Liu and D. S. Passman, *Group algebras with units satisfying a group identity II*, Proc. Amer. Math. Soc. **127** (1999), 337–341.

[LuP] I. S. Luthar and I. B. S. Passi, *Torsion units in matrix group rings*, Comm. Algebra **20** (1992), 1223–1228.

[MRSW] Z. Marciniak, J. Ritter, S. K. Sehgal, and A. Weiss, *Torsion units in integral group rings of some metabelian groups, II*, J. Number Theory **25** (1987), 340–352.

[MS1] Z. S. Marciniak and S. K. Sehgal, *Finite matrix groups over nilpotent group rings*, J. Algebra **181** (1996), 565–583.

[MS2] Z. S. Marciniak and S. K. Sehgal, *Zassenhaus conjecture and infinite nilpotent groups*, J. Algebra **184** (1996), 207–212.

[MS3] Z. S. Marciniak and S. K. Sehgal, *Torsion matrices over abelian group rings*, J. Group Theory **3** (2000), 67–75.

[Okn] J. Okniński, *Semigroup algebras*, Marcel Dekker, New York, 1991.

[Pas1] D. S. Passman, *The algebraic structure of group rings*, Wiley, New York, 1977.

[Pas2] D. S. Passman, *Group algebras whose units satisfy a group identity. II*, Proc. Amer. Math. Soc. **125** (1997), 657–662.

[Rob] D. J. S. Robinson, *A course in the theory of groups. Second edition*, Springer-Verlag, New York, 1996.

[Row] L. H. Rowen, *Generalized polynomial identities*, J. Algebra **34** (1975), 458–480.

[Seh1] S. K. Sehgal, *Topics in group rings*, Marcel Dekker, New York, 1978.

[Seh2] S. K. Sehgal, *Units in integral group rings*, Longman, New York, 1993.