Units in Group Rings

By:
Daniel Cox

Faculty Advisor:
Dr. Gregory T. Lee

A project submitted to the Department of Mathematical Sciences in conformity with the requirements for Math 4301 (Honours Seminar)

Lakehead University
Thunder Bay, Ontario

For Helen, who has always encouraged my love for numbers.

Abstract

In this paper, we review the classical ways in which units are constructed within a group ring. We investigate some results explored by Sehgal and Polcino Milies that deal with group rings which contain either strictly trivial units, or units which themselves form nilpotent groups. We also look at some conditions which were discussed in books by Sehgal and Lee which result in the unit group being solvable, as well.

0 Introduction

"*Pure mathematics is, in its way, the poetry of logical ideas.*"

Albert Einstein

What might be the first formal description of a group ring (though not yet named as such) came from Sir William Rowan Hamilton in 1843, when he devised the first non-commutative algebra: the *quaternions* ([1]). Similar structures, such as *biquaternions* and *octonions*, followed soon after. The contributions of A. Cayley, T. Molien, G. Frobenius, H. Maschke, and E. Noether, among others, established the importance of group rings as an algebraic structure ([1]). Group rings have since found applications in many different branches of algebra, and there are naturally many open problems which are areas of active research.

This paper will focus on the study of units in group rings, and properties of the groups formed by these units. However, we must first review some concepts from group and ring theory, and define the group ring and some of its properties before we may establish some results in this subject.

1 Preliminaries

Let us recall some definitions from group and ring theory. The results in this section follow from largely from [1] and [2].

Definition 1.1. *Let G be a group, and g a nontrivial element of G. If g has finite order, we say g is a torsion element. If every element of G is a torsion element, then we say G is a torsion group. In the case that G is abelian, these elements form a subgroup, called the torsion subgroup and denoted T_G. If the identity is the only such element in G, then G is called torsion free. Moreover, if G is an abelian group, then the factor group G/T_G is necessarily torsion free.*

Definition 1.2. *An abelian group is said to be free abelian if it is a direct product of infinite cyclic groups.*

Theorem 1.3. *Let G be a finitely generated, torsion free, abelian group. Then G is free abelian.*

Definition 1.4. *If G is any group, the exponent of G is the least positive integer n such that, for all $g \in G$, $g^n = 1$ holds. If no such integer exists, we say G has infinite exponent.*

Theorem 1.5 (**Prüfer**). *If A is an abelian group of bounded exponent, then A is isomorphic to a direct product of cyclic groups.*

Definition 1.6. *Let G be a group and $<$ a relation on G such that, for all $x, y, z \in G$, $<$ has the following properties:*

(i) If $x < y$ and $y < z$, then $x < z$.

(ii) If $x \neq y$, then either $x < y$, or $y < x$, but not both.

(iii) If $x < y$, then $zx < zy$ and $xz < yz$.

A group G with such a relation is said to be ordered.

Note that it follows from the above relation that $y^{-1} < x^{-1}$ whenever $x < y$. As an example, the real numbers under addition are an ordered group and, therefore, the integers under addition must also form an ordered group. As it happens, the latter is a specific example of the following result:

Lemma 1.7. *If X is an infinite cyclic group, then X is ordered.*

Proof. Suppose $X = \langle x \rangle$. Then the relation $<$ given by $x^a < x^b$ if and only if $a < b$ satisfies the properties of 1.6. This follows readily from the ordering on $\mathbb{Z}$ and the fact that, for infinite cyclic groups, two elements are equal if and only if their powers (when expressed in terms of the generating element) are equal. Thus infinite cyclic groups are ordered. □

Definition 1.8. *If H is a subgroup of a group G, then the complete set of representatives of left (right) cosets is called a left (right) transversal of H in G.*

Definition 1.9. *Let G be a group and H a subgroup of G. We say that H is characteristic in G if, for any automorphism σ of G, we have that $\sigma(H) = H$.*

Proposition 1.10. *Let G be a group and H a characteristic subgroup in G. Then $H \trianglelefteq G$.*

Proof. Let G and H be as above. Consider the mapping $\phi_g : G \to G$ given by $\phi_g(a) = gag^{-1}$ for arbitrary $a, g \in G$. As this is merely conjugation by g, ϕ_g is an automorphism on G. Since H is characteristic in G, it follows that $\phi_g(H) = gHg^{-1} = H$. As g was arbitrary, it follows that $H \trianglelefteq G$. □

Definition 1.11. *A group G is solvable if there is a chain of subgroups such that*

$$\{1_G\} = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_n = G$$

and G_{i+1}/G_i is abelian for $i = 0, 1, \ldots, n-1$. A chain of such subgroups is called an abelian subnormal series of G.

Let us briefly turn our attention to some properties of solvable groups.

Lemma 1.12. *Subgroups and factor groups of solvable groups are solvable.*

Lemma 1.13. *Let $H \trianglelefteq G$. If both H and G/H are solvable, then G is solvable.*

Let us now introduce the definition of a nilpotent group:

Definition 1.14. *A group G is called nilpotent if it contains a series of subgroups such that*

$$\{1_G\} = G_0 \leq G_1 \leq \ldots \leq G_n = G$$

and such that each subgroup G_{i-1} is normal in G and each factor group G_{i+1}/G_i is contained in the centre of G/G_i for $i = 0, 1, \ldots, n-1$. A chain of such subgroups is called a central series of G.

Lemma 1.15. *Subgroups and factor groups of nilpotent groups are nilpotent.*

Remark 1.16. From the definition, if G is abelian, then it is nilpotent with the central series $\{1_G\} \trianglelefteq G$. We may also observe that, since $G_i \trianglelefteq G$ implies that $G_i \trianglelefteq G_{i+1}$ for $i = 0, 1, \ldots, n-1$, it follows from the definition that nilpotent groups are solvable. However, since the fact that a subgroup is abelian does not necessarily mean that it is a subgroup of a group's centre, and since normality of subgroups is not a transitive property, it does not follow that solvable groups are nilpotent. Thus, we have the following implications:

$$\text{Abelian} \Rightarrow \text{Nilpotent} \Rightarrow \text{Solvable}.$$

Definition 1.17. *Let G be a group, let g, $h \in G$, and let A and B be nonempty subsets of G. Then:*

1. *The element $g^{-1}h^{-1}gh$ is called the commutator of g and h, and is denoted $[g, h]$.*
2. *The group generated by the commutators of elements from A and from B is denoted $[A, B] = \langle\ [a, b] \mid a \in A, b \in B\ \rangle$.*
3. *The subgroup of G generated by the commutators of its elements, called the commutator or derived subgroup of G, is denoted by $G' = \langle\ [g, h] \mid g, h \in G\ \rangle$.*

Proposition 1.18. *Let G be a group, let g, $h \in G$, and let $H \leq G$. Then:*

1. *$gh = hg[g, h]$; $gh = hg$ if and only if $[g, h] = 1_G$.*
2. *$[G, H] = [H, G]$*
3. *$H \trianglelefteq G$ if and only if $[H, G] \leq H$.*
4. *$H \trianglelefteq G$ and G/H is abelian if and only if $G' \leq H$. In particular, G/G' is the largest abelian quotient of G.*

Proof. 1. This follows from the definition of $[g, h]$.

2. Since $[G, H]$ is a subgroup of G, then for every $[g, h] \in [G, H]$, $[g, h]^{-1} \in [G, H]$. However, $[g, h]^{-1} = (g^{-1}h^{-1}gh)^{-1} = h^{-1}g^{-1}hg = [h, g] \in [H, G]$. So $[G, H] \leq [H, G]$ and by similar argument we have that $[H, G] \leq [G, H]$. Thus, by double inclusion, they must be equal.

3. Suppose $H \trianglelefteq G$. Then $g^{-1}hg \in H$ for all $h \in H$ and $g \in G$. Moreover, $h^{-1} \in H$ and, by closure of H, we have that $h^{-1}g^{-1}hg = [h, g] \in H$ for all $h \in H$ and $g \in G$. So $[H, G] \leq H$. Now suppose $[H, G] \leq H$. Then, for all $h \in H$ and $g \in G$, we have that $h^{-1}g^{-1}hg \in H$, and hence $h^{-1}g^{-1}hgH = H$. In particular, it follows that $g^{-1}hg = hH = H$, so that $g^{-1}hg \in H$ for all $h \in H$ and $g \in G$. Thus $H \trianglelefteq G$, as desired.

4. Suppose $H \trianglelefteq G$ and G/H is abelian. Then, for all $g, k \in G$ we have that $(gH)(kH) = (kH)(gH)$. In particular

$$\begin{aligned} 1H &= (gH)^{-1}(kH)^{-1}(gH)(kH) \\ &= g^{-1}k^{-1}gkH \\ &= [g, k]H. \end{aligned}$$

Thus we have that $[g, k] \in H$ for all $g, k \in G$, and $G' \leq H$.

Now suppose $G' \leq H$. Consider the commutator subgroup $[H, G]$. An arbitrary element is of the form $\prod_{i \in I}[h_i, g_i]$, where $h_i \in H$, $g_i \in G$ for each $i \in I$, I being

some index set. Of course $h_i, g_i \in G$ for every $i \in I$. Hence $[h_i, g_i] \in G'$ for every $i \in I$ and, by closure, every product of the $[h_i, g_i]$'s must be in G' also. Thus $[H, G] \leq G' \leq H$, which, by (2), means that $H \trianglelefteq G$. To see that G/H is abelian, note that, for arbitrary gH and kH in G/H, $[g, k] \in G' \leq H$ and thus

$$\begin{aligned}(gH)(kH) &= (gk)H \\ &= (kg[g,k])H \\ &= (kg)H = (kH)(gH).\end{aligned}$$

□

Definition 1.19. *A group G is said to be p-abelian if its commutator subgroup G' is a finite p-group. By convention, a group that is abelian is called 0-abelian.*

Let us make use of the concept of commutators and commutator subgroups to give an alternate definition of solvable group. We can repeatedly form derived subgroups as follows:

$$G^{(0)} = G;\ G^{(n)} = [G^{(n-1)}, G^{(n-1)}],\ n \geq 1.$$

Definition 1.20. *The descending series of subgroups*

$$G^{(0)} \geq G^{(1)} \geq \ldots \geq G^{(n)} \geq \ldots$$

is called the derived series of the group G. If the series terminates, then the smallest integer n such that $G^{(n)} = \{1_G\}$ is called the derived length of G.

Theorem 1.21. *A group G is solvable if and only if its derived series terminates.*

Proof. Suppose G has a finite derived series given by

$$G^{(0)} \geq G^{(1)} \geq \ldots \geq G^{(n)} = \{1_G\}$$

By 1.18.4, this is an abelian subnormal series for G. Hence G is solvable.

Now suppose that G is solvable. Let us consider an abelian subnormal series of G given by

$$G = G_0 \geq G_1 \geq \ldots \geq G_n = \{1_G\}$$

Clearly $G^{(0)} \leq G_0$, so let us suppose that $G^{(i)} \leq G_i$ holds for every i, $1 \leq i \leq m$. Proceeding inductively, let us consider $G^{(m+1)}$. We have that $G^{(m+1)} \leq G^{(m)} \leq G_m$ by our induction hypothesis. Then $G^{(m+1)} = [G^{(m)}, G^{(m)}] \leq [G_m, G_m]$, and, by 1.18.4, we have that $[G_m, G_m] \leq G_{m+1}$, thus completing the induction step. It follows that $G^{(n)} = \{1_G\}$, hence G is solvable. □

Now let us inductively define two new series of subgroups:

$$\gamma_1(G) = G,\ \gamma_2(G) = G',\ \text{and } \gamma_i(G) = [\gamma_{i-1}(G), G].$$

$$Z_0(G) = \{1_G\},\ Z_1(G) = Z(G),\ \text{and } Z_i(G)$$

is the unique subgroup of G such that $Z_i(G)/Z_{i-1}(G) = Z(G/Z_{i-1}(G))$. The group $Z_i(G)$ is called the i^{th} centre of G.

Definition 1.22. *The sequences of subgroups*

$$\{1_G\} = Z_0(G) \subset Z_1(G) \subset \ldots \subset Z_n(G) \subset \ldots$$

and

$$G = \gamma_1(G) \supset \gamma_2(G) \supset \ldots \supset \gamma_n(G) \supset \ldots$$

are called the upper central series and the lower central series of G, respectively.

Lemma 1.23. *Let*

$$\{1_G\} = A_0 \subset A_1 \subset \ldots \subset A_n \subset \ldots$$

be an ascending central series of a group G. Then $A_n \subset Z_n(G)$ for all $n \geq 0$.

Proof. Let us proceed by induction. When $n = 1$, the result holds trivially. Therefore, let us assume the result holds for some $n \geq 1$ and consider A_{n+1}. Since $A_{n+1}/A_n \subset Z(G/A_n)$, it follows that, for $a \in A_{n+1}$ and $g \in G$, $a^{-1}g^{-1}ag \in A_n \subset Z_n(G)$. So $(aZ_n(G))(gZ_n(G)) = (gZ_n(G))(aZ_n(G))$. By the way that $Z_{n+1}(G)$ is defined, we must have that $a \in Z_{n+1}(G)$. Hence $A_{n+1} \subset Z_{n+1}(G)$, completing the induction step. □

Lemma 1.24. *Let*

$$G = A_0 \supset A_1 \supset \ldots \supset A_n \supset \ldots$$

be a descending central series of a group G. Then $\gamma_n(G) \subset A_{n-1}$ for all $n \geq 0$.

Proof. The case where $n = 1$ is trivial. Proceeding inductively, let us assume that $\gamma_n(G) \subset A_{n-1}$ for some $n \geq 1$. Since A_{n-1}/A_n lies in the centre of G/A_n, we have that $[A_{n-1}, G] \subset A_n$. Hence $\gamma_{n+1}(G) = [\gamma_n(G), G] \subset [A_{n-1}, G] \subset A_n$, which completes the induction step. □

From these lemmata we have that, if G is a nilpotent group, then all central series of G have the same length. We call this number the nilpotency class of G. As we saw above, all abelian groups are nilpotent, and we can now say that the nontrivial abelian groups are exactly those of nilpotency class 1.

The notion of nilpotency class highlights an important idea underlying the study of commutators, solvable groups, and nilpotent groups. In a sense, the series of subgroups which we have given in the definitions of solvability and nilpotence can be thought of as a way of sectioning up our group in a such a way that we can create these groupings of commutative and central elements, respectively. The more we have to section up our group, the farther we are from having an abelian group. Thus, we can almost think of the nilpotency class of a group as a measure of its "abelianness," or "nonabelianess," if one prefers. Hence these structures help us to create a kind of spectrum of abelianness, as illustrated in 1.16.

Let us now explore some results regarding nilpotent groups which will be useful to us in future. The next three lemmata come from [3].

Lemma 1.25. *If G is a nilpotent group, then the elements of order p, where p is a prime, form a subgroup.*

Lemma 1.26. *If G is a nilpotent group and H a normal subgroup of G, then H intersects the centre of G nontrivially.*

Proof. Let G and H be as described. Since G is nilpotent, there is some n such that $G = Z_n(G)$, the n-th centre of G. Thus there exists a least natural number j such that $H \cap Z_j(G) \neq \{1_G\}$, but $H \cap Z_{j-1}(G) = \{1_G\}$. Since H is normal in G, it follows from 1.18.3 that $[H, G] \leq H$. Thus $[H \cap Z_j(G), G] \leq H$. Moreover, from the way the upper central series is defined, we have that $[Z_j(G), G] \leq Z_{j-1}(G)$; hence $[H \cap Z_j(G), G] \leq Z_{j-1}(G)$. We have shown that $[H \cap Z_j(G), G] \subseteq H \cap Z_{j-1}(G) = \{1_G\}$. It must be that $H \cap Z_j(G) \subseteq H \cap Z(G)$. □

Lemma 1.27. *If G is a nilpotent group with an element of order p, where p is a prime, then G has an element of order p in its centre.*

Proof. Let G be a nilpotent group with an element of prime order p, say g. By 1.25, the elements of order p form a subgroup, which we will denote P. We claim that P is normal. To see this, let h be an arbitrary element of G. Observe that

$$(h^{-1}gh)^p = h^{-1}g^p h = h^{-1}h = 1_G.$$

So the order of $h^{-1}gh$ divides p, a prime. Since $h^{-1}gh$ is not the identity, its order is not 1, so it must be p. Hence $h^{-1}gh \in P$, and it follows that P is normal. Applying the previous lemma, $P \cap Z(G)$ is nontrivial. In other words, G contains an element of order p in its centre. □

Lemma 1.28. *Let G be a group with the upper central series*

$$\{1_G\} = Z_0(G) \subset Z_1(G) \subset \cdots \subset Z_n(G) \subset \cdots .$$

If the centre of G is torsion free, then each factor $Z_{i+1}(G)/Z_i(G)$ is torsion free.

Corollary 1.29. *If G is a torsion free nilpotent group, then its upper central factors are also torsion free. Moreover, if G is finitely generated, then G admits a central sequence*

$$\{1_G\} = G_0 \subset \cdots \subset G_n = G,$$

all of whose factors are infinite cyclic.

Theorem 1.30 (**Schur**)**.**

1. *If G is a group such that its center is of finite index n, then G' is finite and $(G')^n = 1$.*
2. *If G is a solvable group satisfying $G^{p^m} \subseteq Z(G)$ for a fixed prime power p^m, then $(G')^{p^M} = 1$ for a fixed M.*

Proof. See [4], $I.4.2$ and $I.4.3$. □

We will now look at a type of group construction called the free group. We first introduce some new terminology. Let us consider a set of symbols $\Lambda = \{a_i\}_{i\in I}$; we call this set an alphabet, and each of the a_i are letters in this alphabet. Define the set $\Lambda^{-1} = \{a_i^{-1}\}_{i\in I}$. This set will be of importance shortly.

We define a word in this alphabet to be any finite string of letters of the form

$$w = a_{i_1}^{\epsilon_{i_1}} \cdots a_{i_n}^{\epsilon_{i_n}},$$

where n is any positive integer, $a_{i_j} \in \Lambda$, and $\epsilon_{i_j} = \pm 1$, $1 \leq j \leq n$. The integer n will be called the length of the word w. We use the convention that a word of length 0 is called the empty word and is denoted by 1. Powers apply in the usual way and, if u and v are two words, then uv is obtained via juxtaposition of the letters in each word.

Definition 1.31. *Let u and v be words in some alphabet $\Lambda = \{a_i\}_{i\in I}$. We say that u is equivalent to v and write $u \sim v$ if there exists a sequence of words:*

$$u = u_1, u_2, \ldots, u_n = v, \quad n \geq 1,$$

such that either $u_{i+1} = w_1 a_j^{\epsilon_j} a_j^{-\epsilon_j} w_2$ and $u_i = w_1 w_2$, or vice versa, with $\epsilon_j = \pm 1$ and w_1 and w_2, words in Λ.

The relation $\sim$ above is an equivalence relation. We let $\bar{w}$ denote the equivalence class of w under this relation.

Definition 1.32. *A word w is called reduced if it contains no two consecutive symbols of the form $a_i^{\epsilon_i} a_i^{-\epsilon_i}$, where $\epsilon_i = \pm 1$.*

Proposition 1.33. *Let W denote the set of all words in a given alphabet Λ. Then each equivalence class $\bar{w}$, $w \in W$, contains precisely one reduced word. Consequently, if $u, v \in W$ are reduced words, then $u \sim v$ if and only if $\bar{u} = \bar{v}$.*

Theorem 1.34. *Let W be the set of all words in an alphabet Λ, and let $F = \{\bar{w} \mid w \in W\}$. If we define an operation $\diamond$ in F by*

$$\bar{u} \diamond \bar{v} = \bar{uv}, \quad \forall u, v \in W,$$

then $(F, \diamond)$ is a group.

Definition 1.35. *The group F constructed above is called the free group on Λ. If the set Λ is finite with n elements, then we say that F is a free group on n generators.*

While there are many deep results concerning free groups, we omit them here, since we have included the construction of the free group mainly so that we may introduce the following concept:

Definition 1.36. *Let $\langle a_1, a_2, \ldots \rangle$ be the free group on a countable infinitude of generators. If G is any group, then we say that G satisfies a group identity if there exists a nontrivial reduced word $w(a_1, \ldots, a_n) \in \langle a_1, a_2, \ldots \rangle$ such that $w(g_1, \ldots, g_n) = 1$ for all $g_i \in G$.*

We have already encountered a simple example of a group identity. We may say that G is abelian if it satisfies the group identity $[g_1, g_2] = 1$ for all $g_1, g_2 \in G$, or nilpotent if it satisfies $[g_1, \ldots, g_n] = 1$ for some $n \geq 2$. We also say G is n-Engel if it satisfies

$$[g_1, \underbrace{g_2, \ldots, g_2}_{n \text{ times}}] = 1.$$

We will refer to these concepts a little later. Let us now leave the realm of group theory to discuss some concepts from ring theory, some of which will be needed in future.

Definition 1.37. *Let R be a ring and I a nonempty subset of R. Then I is called a left (right) ideal of R if the following hold:*

1. *I is a subring of R*
2. *I is closed under left (right) multiplication (i.e. $rI \subseteq I$, or $Ir \subseteq I$) for all $r \in R$.*

We refer to I simply as an ideal (or two-sided ideal) if it is both a left and a right ideal. Furthermore, I is called a proper ideal if it is neither R nor $\{0\}$.

Definition 1.38. *Let x and y be arbitrary elements of a ring R. Then the element $xy - yx$ is called the Lie commutator of x and y. To avoid any confusion with the other type of commutator defined earlier, we use the notation (x, y) to mean the Lie commutator. We also use (R, R) to denote the additive subgroup of R generated by all the Lie commutators of R.*

Note the above definition can be extended in the following manner:

$$(x, y, z) = ((x, y), z)$$

so that

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

For the ring R, we will use the following notation: $\lambda_1(R) = R$, and, for any natural number $k > 1$, $\lambda_k(R) = (\lambda_{k-1}(R), R)$.

Definition 1.39. *If there exists an $m \in \mathbb{N}$ such that, for a given ring R, $\lambda_{m+1}(R) = 0$ holds, then R is called a Lie nilpotent ring.*

Note that, if R is a Lie nilpotent ring, then it satisfies

$$(x_1, \ldots, x_n) = 0$$

for all $x_i \in R$. Furthermore, we say that R is Lie n-Engel if it satisfies

$$(x_1, \underbrace{x_2, \ldots, x_2}_{n \text{ times}}) = 0$$

for some positive integer n.

Definition 1.40. *We define inductively the Lie power as follows: $R^{(1)} = R$, and for any natural number k, with $k > 1$, $R^{(k)}$ is the ideal of R generated by $(R^{(k-1)}, R)$.*

Definition 1.41. *If there exists an $m \in \mathbb{N}$ such that $R^{(m+1)} = 0$ holds, then R is called a strongly Lie nilpotent ring.*

Before we present the next lemma, let us recall that a ring element r is called idempotent if $r^2 = r$ and nilpotent if $r^k = 0$ for some positive integer k.

Lemma 1.42. *Let R be a ring without nilpotent elements. Then every idempotent element r belonging to R is central.*

Proof. Let $r \in R$ be an idempotent element. Observe that, for any $s \in R$,

$$(rs - rsr)^2 = rsrs - rsrsr - rsrs + rsrsr = 0.$$

Since R contains no nilpotent elements, we must have that $rs = rsr$. Similarly, $(sr - rsr)^2 = 0$, so that $sr = rsr$. In other words, $sr = rs$. Since r and s were arbitrary, we have shown that every idempotent element is in fact central. □

Definition 1.43. *Let R be a ring. We define the left R-module (or left module over R) as a set M with the following operations:*

1. *There is a binary operation $+$ on M under which M is an abelian group.*
2. *An action of R on M which is denoted by rm and, for all $r, s \in R$ and $m, n \in M$, satisfies:*
   - *(a) $(r + s)m = rm + sm$,*
   - *(b) $(rs)m = r(sm)$,*
   - *(c) $r(m + n) = rm + rn$.*

   Additionally, if R has unity, then
   - *(d) $1m = m$.*

We can define right R-modules in a similar way by moving the ring elements from the left side to the right side in definitions 2(a) to 2(c). Moreover, we see that, if R is commutative and M is a left R-module, then M can be made into a right R-module by additionally defining $mr = rm$, where $r \in R$ and $m \in M$. It is also worth noting that R can be a left (right) module over itself. Then we see that the submodules are precisely the left (right) ideals of R.

Definition 1.44. *Let R be a ring and M be some R-module. An R-submodule of M is a subgroup N of M which is itself a module under the action of ring elements.*

Note that, for any R-module M, both $\{0\}$ and M are trivial R-submodules of M. If M is a nonzero R-module such that its only submodules are the trivial submodules, then we call M a simple module.

Let us now recall that the direct sum of two groups H and K is the set $H \oplus K = \{(h, k) \mid h \in H, k \in K\}$ together with the componentwise operations of the groups H and K (that is, if $(h_1, k_1), (h_2, k_2) \in H \oplus K$, then $(h_1, k_1)(h_2, k_2) = (h_1h_2, k_1k_2)$). There is a similar structure with modules:

Definition 1.45. *Let A and B be modules of a ring R. We define the direct sum of A and B by $A \oplus B = \{a \oplus b \mid a \in A, b \in B\}$. The operations on $A \oplus B$ are given by*

1. $(a_1 \oplus b_1) + (a_2 \oplus b_2) = (a_1 + a_2) \oplus (b_1 + b_2)$*; and*
2. $r(a \oplus b) = ra \oplus rb$*, where $r \in R$.*

Definition 1.46. *A submodule N of an R-module M is called a direct summand if there exists another module N' such that $M = N \oplus N'$. A module which contains no nontrivial direct summand is called indecomposable.*

Definition 1.47. *An R-module M is called semisimple if every submodule of M is a direct summand.*

Proposition 1.48. *Let N be a nontrivial submodule of a semisimple module M. The N is semisimple and it contains a simple submodule.*

Theorem 1.49. *Let M be an R-module. Then the following conditions are equivalent:*

1. *M is semisimple;*
2. *M is a direct sum of simple submodules; and,*
3. *M is a sum (not necessarily direct) of simple submodules.*

Definition 1.50. *A ring R is called semisimple if R, when considered as a left module over itself, is semisimple.*

Considering R as a left R-module whose submodules are the left ideals of R, the above definition can also be stated as R is semisimple if every left ideal is a direct summand. Also note that any field K is semisimple since its only ideals are trivial, and hence are trivially direct summands.

Theorem 1.51. *Let R be a ring. Then the following conditions are equivalent:*

(i) Every R-module is semisimple

(ii) R is a semisimple ring

(iii) R is a direct sum of a finite number of minimal left ideals

Theorem 1.52 (**Wedderburn-Artin**)**.** *A ring R is semisimple if and only if it is the direct sum of matrix algebras over division rings. We write*

$$R \simeq M_{n_1}(D_1) \oplus \ldots \oplus M_{n_s}(D_s).$$

In particular, if R is commutative, then R must be a finite direct sum of fields.

2 Group Rings

Here, we explore some results which follow from [1].

Definition 2.1. *Let G be a group and R a ring. Then the group ring RG is defined as RG=$\{\ r_1g_1 + r_2g_2 + \ldots + r_ng_n : r_i \in R, g_i \in G, i = 1, 2, \ldots, n\ \}$. That is, RG can be thought of as the set of all finite formal sums of elements in G with coefficients in R. If R is commutative then RG is called a group algebra.*

Depending on the application, we will use either $\alpha = \sum_{g\in G} r_g \cdot g$ or $\alpha = \sum_{g\in G} r(g) \cdot g$ to represent elements of RG. For either notation, it is to be understood that only finitely many of the coefficients from R are nonzero, even though G may be infinite. Thus, if we are given elements $\alpha = \sum_{g\in G} r_g \cdot g$ and $\beta = \sum_{g\in G} s_g \cdot g$ in RG, then $\alpha = \beta$ if and only if $r_g = s_g$ for all $g \in G$. We call the support of the element α the set $supp(\alpha) = \{\ g \mid r_g \neq 0\ \}$.

Addition in RG is defined in an intuitive manner:

$$(\sum_{g\in G} r_g \cdot g) + (\sum_{g\in G} s_g \cdot g) = \sum_{g\in G} (r_g + s_g) \cdot g.$$

For $\alpha = \sum_{g\in G} r_g \cdot g$ and $\beta = \sum_{h\in G} s_h \cdot h$, we define the product $\alpha\beta$ as follows:

$$\alpha\beta = \sum_{g\in G} \sum_{h\in G} r_g s_h \cdot gh.$$

This definition of the product, together with the closure of R and G, allow us to rewrite the above as:

$$\alpha\beta = \sum_{\bar{g}\in G} v_{\bar{g}} \cdot \bar{g}$$

where

$$v_{\bar{g}} = \sum_{gh=\bar{g}} r_g s_h.$$

From these definitions, we see that RG is closed under addition, and the taking of products. The operation of addition in RG is based on the operation of addition in R, so those properties of R under addition also hold in RG. Furthermore, the way in which products are defined means that the left and right distributive properties will follow from R, as will associativity. Hence RG is a ring. If we further define the product of elements of R by elements of RG as

$$s\,(\sum_{g\in G} r_g \cdot g) = \sum_{g\in G} (sr_g) \cdot g$$

then we see that RG is also a left (right) R-module.

Proposition 2.2. *If R is a ring with unity, then the group ring RG is a ring with unity.*

Proof. Let R be a ring with unity element 1_R. Then $1_R r = r 1_R = r$ for every $r \in R$. Furthermore, it follows that the element $1_R \cdot 1_G$ exists in RG. Let $\sum_{g\in G} r_g \cdot g$ be an arbitrary element in RG. Observe that:

$$\begin{aligned}(1_R \cdot 1_G) \cdot (\sum_{g\in G} r_g \cdot g) &= \sum_{g\in G} 1_R r_g \cdot 1_G g \\ &= \sum_{g\in G} r_g \cdot g \\ &= \sum_{g\in G} r_g 1_R \cdot g 1_G = (\sum_{g\in G} r_g \cdot g) \cdot (1_R \cdot 1_G).\end{aligned}$$

Hence, the element $1_R \cdot 1_G$ is unity in RG. □

Definition 2.3. *The homomorphism $\phi : RG \to R$ given by*

$$\phi(\sum_{g\in G} r_g \cdot g) = \sum_{g\in G} r_g$$

is called the augmentation mapping of RG. Its kernel, denoted by $\triangle(G)$, is called the augmentation ideal of RG.

The above definition, together with the first isomorphism theorem for rings, implies that

$$RG/\triangle(G) \simeq R$$

Proposition 2.4. *Let R be a commutative ring. The map $^* : RG \to RG$ given by*

$$(\sum_{g\in G} r_g \cdot g)^* = \sum_{g\in G} r_g \cdot g^{-1}$$

satisfies the following properties:

(i) $(\alpha + \beta)^* = \alpha^* + \beta^*$

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

(iii) $\alpha^{**} = \alpha$

Lemma 2.5. *If the augmentation ideal $\triangle(G)$ is a direct summand of RG as an RG-module, then G is finite and $|G|$ is invertible in R.*

Theorem 2.6 (**Maschke's Theorem**)**.** *Let G be a group. Then the group ring RG is semisimple if and only if the following conditions hold:*

(i) R is a semisimple ring;

(ii) G is finite; and,

(iii) $|G|$ is invertible in R.

Recall that a field K is always semisimple, and that $|G|$ is invertible in K if and only if $|G| \neq 0$ in K. This holds if and only if $char(K) \nmid |G|$. Thus we have the following:

Corollary 2.7. *Let G be a finite group and K, a field. Then the group algebra KG is semisimple if and only if char(K)* $\nmid |G|$.

3 Units of Group Rings

First, we examine some general facts which follow from [1] so that we may then move on to some results from [4].

For any ring R we let $U(R)$ denote the group of units of the ring R. Thus, we use $U(RG)$ to mean the group of units of the group ring RG. Since the augmentation mapping ϕ is a ring homomorphism, it follows that, if $u \in U(RG)$, then $\phi(u) \in U(R)$.

Let us use the notation $U_1(RG)$ to mean the subgroup of units of augmentation 1 in $U(RG)$. That is:

$$U_1(RG) = \{u \in U(RG) \mid \phi(u) = 1\}.$$

It follows that, if u is a unit of the group ring $\mathbb{Z}G$, then $\phi(u) = \pm 1$, and hence

$$U(\mathbb{Z}G) = \pm U_1(\mathbb{Z}G).$$

Thus, for an arbitrary ring R, we have that

$$U(RG) = U(R) \times U_1(RG).$$

This is a classical way in which we might construct units in a group ring. We will now give some other examples of some types of units, and how they can be constructed.

Definition 3.1 (**Trivial units**). *An element of the form rg, where $r \in U(R)$ and $g \in G$, has an inverse $r^{-1}g^{-1}$. The elements of this form are called the trivial units of RG.*

Example 3.2. *In the integral group ring $\mathbb{Z}G$, the elements $\pm g$, where $g \in G$, are trivial units.*

Example 3.3. *If K is a field and G a group, then elements of the form kg, where $g \in G$, $k \in K$, and $k \neq 0$, are the trivial units of KG.*

Definition 3.4 (**Unipotent units**). *Let η be a square zero element (i.e. $\eta^2 = 0$) of a ring R. Then $(1-\eta)(1+\eta) = 1 - \eta^2 = 1$. Thus, the elements $1+\eta$ and $1-\eta$ are units in R. By the same token, if η is some nilpotent element (that is, $\eta^k = 0$ for some $k \in \mathbb{Z}^+$), then it follows that:*

$$(1-\eta)(1+\eta+\eta^2+\ldots+\eta^{k-1}) = 1-\eta^k = 1;$$
$$(1+\eta)(1-\eta+\eta^2-\ldots\pm\eta^{k-1}) = 1\pm\eta^k = 1.$$

Again, the elements $1+\eta$ and $1-\eta$ are units in R. We call these elements the unipotent units of R.

With this last definition in mind, let K be a field of characteristic $p > 0$ and consider the group algebra KG. If g is an element of G of order p^n, then $(1-g)^{p^n} = 0$. Letting $\lambda = 1 - g$, we have that $1 - \lambda = g$ is a trivial unit. However, if $char(K) \neq 2$, then $1 + \lambda = 2 - g$ is a nontrivial unit. Also note that $g(1 - g)$ is also nilpotent, thus $1 + g - g^2$ will be a nontrivial unit, so long as $g^2 \neq 1$.

Let R be a ring that contains zero divisors, say x and y, so that $xy = 0$. Then, for any other $r \in R$, we have that $\eta = yrx$ is a square zero element, which, by the previous definition, means $1 + \eta$ is a unit.

Definition 3.5 (**Bicyclic units**). *Let us consider when $R = \mathbb{Z}G$. Suppose $a \in G$ is an element of finite order $n \geq 2$. Then $(a - 1)(1 + a + a^2 + \ldots + a^{n-1}) = 0$, so that $a - 1$ is a zero divisor. Letting $\hat{a} = 1 + a + \ldots + a^{n-1}$ and taking any other $g \in G$, we may construct a unit μ of the form*

$$\mu_{a,g} = 1 + (a - 1)g\hat{a}.$$

Such a unit is called a bicyclic unit. We denote by B_2 the subgroup of $U(\mathbb{Z}G)$ generated by all the bicyclic units of $\mathbb{Z}G$.

Similar to $\hat{a}$ in the previous definition, we also use the notation $\hat{H}$ to mean the sum over all elements of a (sub)group H. That is,

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

Proposition 3.6. *Let g and h be elements of a group G, with g being an element of finite order n. Then, the bicyclic unit $\mu_{g,h}$ is trivial if and only if h normalizes $\langle g \rangle$. In this case, $\mu_{g,h} = 1$.*

Proof. ($\Rightarrow$) Suppose that $h^{-1}gh = g^j$ for some positive integer j. Then $gh = hg^j$ and, since $g^j\hat{g} = \hat{g}$, it follows that $gh\hat{g} = h\hat{g}$. Directly from the definition, we get that

$$\begin{aligned} \mu_{g,h} &= 1 + (g - 1)h\hat{g} \\ &= 1 + gh\hat{g} - h\hat{g} \\ &= 1 + h\hat{g} - h\hat{g} = 1. \end{aligned}$$

($\Leftarrow$) Conversely, let us assume that $\mu_{g,h}$ is trivial. Since $\mu_{g,h}$ is of augmentation 1, there exists some $x \in G$ such that $1 + (1 - g)h\hat{g} = x$, and thus

$$1 + h(1 + g + \ldots + g^{n-1}) = x + gh(1 + g + \ldots + g^{n-1}).$$

If $x = 1$, then we must have that $h = ghg^i$ for some integer i. Hence $h^{-1}gh = g^{-i}$. So let us assume that $x \neq 1$. Then $h \notin \langle g \rangle$ (or else we would have $x = 1$). Since 1 appears on the left-hand side of the above equation, it follows that $1 = ghg^k$ for some integer k. Thus $h = g^{-(k+1)}$, so that $h^{-1}gh = g^{k+1}gg^{-(k+1)} = g$, and thus $gh = hg$. But that would mean $x + gh\hat{g} = x + hg\hat{g} = x + h\hat{g} = 1 + h\hat{g}$ and hence $x = 1$, which is a contradiction. □

Proposition 3.7. *Let G be a finite group. Then the group B_2 is trivial if and only if every subgroup of G is normal.*

Proof. ($\Rightarrow$) Suppose G is finite and B_2 is trivial. Let H be an arbitrary subgroup of G, with h some arbitrary element in H. By closure of H, all powers of h appear in H. If g is some arbitrary element of G, then by the previous theorem we have that $g^{-1}hg = h^j \in H$. Since h and g were arbitrary, it follows that $g^{-1}Hg = H$. In other words, H is normal in G.

($\Leftarrow$) Conversely, suppose every subgroup of G is normal. Then for any $a, b \in G$, we have that a normalizes $\langle b \rangle$. Hence $\mu_{b,a}$ is trivial, by the previous theorem. Since this holds for any $a, b \in G$, it follows that B_2 must be trivial. □

Recall that a nonabelian group G in which every subgroup is normal is called Hamiltonian. Thus the above result implies that G must be either abelian or Hamiltonian if the group of bicyclic units in $\mathbb{Z}G$ is trivial. The next result will show that if there exists a nontrivial bicyclic unit, then B_2 is a group of infinite order.

Proposition 3.8. *Every nontrivial bicyclic unit $\mu_{g,h}$ of $\mathbb{Z}G$ has infinite order.*

Proof. We claim that $(\mu_{g,h})^s = 1 + s(g-1)h\hat{g}$. We proceed inductively on s. Clearly, if $s = 1$, the result holds, so assume that the above holds for s and consider $(\mu_{g,h})^{s+1}$. We have that

$$\begin{aligned}(\mu_{g,h})^{s+1} &= (\mu_{g,h})^s(\mu_{g,h}) \\ &= (1 + s(g-1)h\hat{g})(1 + (g-1)h\hat{g}) \\ &= 1 + (g-1)h\hat{g} + s(g-1)h\hat{g} + (s-1)(g-1)h\hat{g}(g-1)h\hat{g} \\ &= 1 + (s+1)(g-1)h\hat{g},\end{aligned}$$

since $\hat{g}(g-1) = 0$. Thus $(\mu_{g,h})^s = 1$ if and only if $(g-1)h\hat{g} = 0$, which happens if and only if $\mu_{g,h} = 1$. □

We now make an aside to recall that, for a given $n \in \mathbb{Z}^+$, Euler's totient function (which we will denote Φ) tells us the number of positive integers which are both less than or equal to and relatively prime to n. This function has the property that, if a and n are relatively prime, then $a^{\Phi(n)} \equiv 1 \pmod{n}$, in itself a neat result. We use this to construct a new unit:

Definition 3.9 (**Bass cyclic units**)**.** *Let g be an element of order n in a group G. A Bass cyclic unit is an element of the group ring $\mathbb{Z}G$ of the form:*

$$\mu_a = (1 + g + \ldots + g^{a-1})^{\Phi(n)} + \frac{1 - a^{\Phi(n)}}{n}\hat{g},$$

where a is an integer such that $2 \leq a \leq n-2$ and a and n are relatively prime.

Proposition 3.10. *The bass cyclic unit μ_a of $\mathbb{Z}G$ is of infinite order.*

Definition 3.11 (**Alternating units**). *Let $g \in G$ be an element of odd order n and let c be an integer such that c and $2n$ are relatively prime. Then the element*

$$\mu = 1 - g + g^2 - \ldots + g^{c-1}$$

is called an alternating unit of $\mathbb{Z}\langle g \rangle$.

Lemma 3.12. *Let $\gamma = \sum_{g \in G} \gamma(g) \cdot g$ be a unit of finite order in the integral group ring $\mathbb{Z}G$ of a finite group G and assume that $\gamma(1) \neq 0$. Then $\gamma = \gamma(1) = \pm 1$.*

Corollary 3.13. *Suppose that $\gamma = \sum_{g \in G} \gamma(g) \cdot g$ is a central unit in the integral group ring $\mathbb{Z}G$ of a finite group G, which is of finite order. Then γ is of the form $\gamma = \pm g$, with $g \in Z(G)$.*

Theorem 3.14. *Let A be a finite abelian group. Then, the group of torsion units of the integral group ring $\mathbb{Z}A$ is $\pm A$.*

Theorem 3.15 (**Passman-Bass**). *Let $\gamma = \sum_{g \in G} \gamma(g) \cdot g$ be an element of $\mathbb{Z}G$ which satisfies $\gamma^n = 1$ for some $n \in \mathbb{Z}^+$. If $\gamma(1) \neq 0$, then $\gamma = \pm 1$.*

Corollary 3.16. *Suppose $\gamma \in \mathbb{Z}G$ has that property that it commutes with γ^* (recall * is the mapping defined in proposition 2.4). If γ is a unit of finite order, then $\gamma = \pm g$ for some $g \in G$.*

Corollary 3.17. *All central units of finite order in $\mathbb{Z}G$ are trivial.*

Corollary 3.18. *If A is any abelian group, then all torsion units of $\mathbb{Z}A$ are trivial.*

Theorem 3.19 (**Higman**). *Let G be a torsion group. Then all units of $\mathbb{Z}G$ are trivial if and only if G is either an abelian group of exponent 1, 2, 3, 4, or 6, or is a Hamiltonian 2-group.*

Theorem 3.20. *Let X be an infinite cyclic group and let R be a ring without zero divisors. Then the units of RX are trivial.*

Proof. Suppose R and X are as described, and let u be some unit in RX. Multiplying u by some suitable power of x, we obtain another unit of the form

$$\bar{u} = \sum_{i=0}^{n} r_i \cdot x^i, \text{where } n \geq 0, r_0 \neq 0, \text{and } r_n \neq 0.$$

Since $\bar{u}$ is a unit, it has some inverse of the form

$$v = \sum_{k=j}^{m} s_k \cdot x^k, \text{where } j \leq m, s_j \neq 0, \text{and } s_m \neq 0.$$

Since R has no zero divisors, the product $\bar{u}v$ must contain the terms $r_n s_m \cdot x^{n+m}$ and $r_0 s_j \cdot x^j$. But $\bar{u}v = 1$, so we must have that $n + m = j = 0$, and therefore $n = m = 0$. It follows that $\bar{u}$ is trivial, and so too must be u. □

As an immediate consequence of the previous result, we get the following:

Corollary 3.21. *If X is an infinite cyclic group, then $U(\mathbb{Z}X) = \pm X$.*

Theorem 3.20 is actually a specific example of a more general result. Recall from 1.6 that an ordered group G is one with a transitive relation $<$ such that, for distinct elements $g, h \in G$, either $g < h$ or $h < g$, but not both. In 1.7, we saw that infinite cyclic groups are in fact ordered. Thus, we can further extend the previous theorem as follows:

Theorem 3.22. *Let G be an ordered group and R a ring without zero divisors. Then RG contains no nontrivial zero divisors and no nontrivial units.*

Proof. Let R and G be as described and let γ and ρ be elements in RG such that $\gamma\rho = 0$ or 1. Since G is an ordered group, we may express γ in the form

$$\gamma = \sum_{i=0}^{n} r_i \cdot g_i, \text{ with } g_0 < g_1 < \ldots < g_n, \ r_0 \neq 0, \text{ and } r_n \neq 0.$$

Similarly, for ρ, we can write

$$\rho = \sum_{j=0}^{m} s_j \cdot h_j, \text{ with } h_0 < h_1 < \ldots < h_m, \ s_0 \neq 0, \text{ and } s_m \neq 0.$$

It follows from the ordering of G that

$$g_0h_0 < g_0h_1 < \ldots < g_0h_m < \ldots < g_nh_m.$$

If R has no nontrivial zero divisors, then the product $\gamma\rho$ must contain the terms $r_0s_0 \cdot g_0h_0$ and $r_ns_m \cdot g_nh_m$. Moreover, these terms must be distinct since, if $g_0h_0 = g_nh_m$ and $g_0 < g_n$, then we would have that $h_m < h_0$, which is a contradiction.

Since the product has only one term, either 0 or 1, both $r_0s_0 \cdot g_0h_0$ and $r_ns_m \cdot g_nh_m$ cannot survive in the product. We must have that $n = m = 0$.

Thus, if $\gamma\rho = 0$, it must be that $r_0s_0 = 0$. But this is a contradiction, since R contains no nontrivial zero divisors. In other words, RG contains no nontrivial zero divisors.

We have also shown that, if $\gamma\rho = \rho\gamma = 1$ and $n = m = 0$, then γ and ρ are of the form of trivial units. □

Theorem 3.23. *Let A be a torsion free abelian group, and let K be a field. Then the units of KA are trivial.*

Theorem 3.24. *Let G be a group that has a subnormal chain of the form*

$$\{1_G\} = G_0 \triangleleft G_1 \triangleleft \ldots \triangleleft G_n = G,$$

where each G_i/G_{i-1} is infinite cyclic, and let K be a field. Then the units of KG are trivial.

Corollary 3.25. *Let G be a torsion-free nilpotent group and let K be a field. Then the units of KG are trivial.*

Proof. Let $u \in KG$ be a unit. Replacing G with the group generated by the supports of u and u^{-1}, we may assume, without loss of generality, that G is finitely generated. Applying 1.29, it follows that finitely generated torsion free nilpotent groups admit a subnormal series like that of the previous theorem. It follows that the units of KG must be trivial. □

We now arrive at a conjecture which is very well known among those in the field:

Conjecture 3.26 (**Unit conjecture**). *Let G be a torsion-free group and let K be a field. Then the units of KG are trivial.*

There are specific cases where this has been shown to hold, however the general case has remained unproven since it was originally stated by Kaplansky over 40 years ago ([1]). We have included it here, if only due to its notoriety within the subject.

Let us now turn our attention to the question of when the unit group of a group ring forms a nilpotent group. In particular, we look at the result of Khripta, which establishes necessary and sufficient conditions for group algebras with groups containing p-elements over fields of prime characteristic $p > 0$. We also state some results from [4], one of which establishes necessary and sufficient conditions for nilpotence of the unit group of $\mathbb{Z}G$. However, we first require a few results from [5].

Lemma 3.27. *Let K be a field of characteristic $p > 0$ and G a group such that $U(KG)$ satisfies $w(x_1, \ldots, x_n) = 1$. If N is a finite normal p-subgroup of G, then $U(K(G/N))$ satisfies $w(x_1, \ldots, x_n) = 1$.*

Lemma 3.28. *Let K be a field of characteristic $p > 0$, and let G be a nilpotent group such that $|G'| = p^k$. Then $(KG)^{(2p^k)} = 0$.*

Theorem 3.29 (**Passi-Passman-Sehgal**). *The group algebra KG of the group G over a field K of characteristic $p \geq 0$ is Lie nilpotent if and only if G is nilpotent and p-abelian.*

For the next lemma, we recall the notation $x^y = y^{-1}xy$.

Lemma 3.30. *Let R be a ring of prime characteristic p, and suppose ν is a central, square zero element in R. Then for arbitrary $a \in R$ and $u \in U(R)$, we have*

$$[1 + \nu a, \underbrace{u, \ldots, u}_{p^n \ terms}] = 1 + \nu(a^{u^{p^n}} - a)$$

for any $n \geq 2$.

Proof. Let us assume that ν, a, and u are as given. Observe that:

$$\begin{aligned}[1+\nu a, u] &= (1+\nu a)^{-1}u^{-1}(1+\nu a)u \\ &= (1-\nu a)u^{-1}(1+\nu a)u \\ &= 1+\nu(a^u - a),\end{aligned}$$

and therefore

$$[1+\nu a, u, u] = 1+\nu(a^{u^2} - 2a^u + a).$$

Proceeding inductively, we get

$$[1+\nu a, \underbrace{u, \ldots, u}_{k \text{ terms}}] = 1+\nu\left(a^{u^k} - \binom{k}{1}a^{u^{k-1}} + \binom{k}{2}a^{u^{k-2}} - \ldots + (-1)^k a\right).$$

Selecting $k = p^n$ and noting that p divides $\binom{p^n}{i}$ whenever $0 < i < p^n$, we may conclude that

$$1 = [1+\nu a, \underbrace{u, \ldots, u}_{p^n \text{ terms}}] = 1+\nu(a^z - a), \text{ where } z = u^{p^n}.$$

□

Supposing we have some central element g of order p in G, we can use $\nu = \hat{g}$ in the previous lemma, since $\nu^2 = 0$.

Lemma 3.31. *Let G be a group with an element g of order p in $Z(G)$. If K is a field of characteristic p, and $U(KG)$ is p^n-Engel, then $G^{p^n} \subseteq Z(G)$.*

Proof. Let g be as given and let us construct the element $\nu = \hat{g}$; as we mentioned above, ν is square zero. Thus, by 3.30, for any $x, y \in G$, it follows that

$$1 = [1+\nu x, \underbrace{y, \ldots, y}_{p^n \text{ terms}}] = 1+\nu(x^z - x), \text{ where } z = y^{p^n}.$$

From this, it follows that $\nu(x^z - x) = 0$, and therefore $\nu x^z = \nu x$. Hence there exists a j such that $x^z = xg^j$. Conjugating again by z and using the fact that g is central, it follows that $x^{z^2} = z^{-1}xg^j z = z^{-1}xzg^j = xg^j g^j = xg^{2j}$. Then $x^{z^p} = xg^{jp} = x$, since g has order p. In other words, $x^{z^p} = x^{y^{p^{n+1}}}$ is a central element. Since both x and y were arbitrary, and our choice of n independent of x and y, we have the result we desired. □

Lemma 3.32. *If R is a ring with central, square zero elements $\nu_1, \ldots, \nu_n$, then for any $r_1, \ldots, r_n \in R$, we have*

$$[1+\nu_1 r_1, \ldots, 1+\nu_n r_n] = 1+\nu_1 \cdots \nu_n(r_1, \ldots, r_n).$$

Proof. We proceed by induction. Observe that, when $n = 2$, we have

$$\begin{aligned}[1 + \nu_1 r_1, 1 + \nu_2 r_2] &= (1 - \nu_1 r_1)(1 - \nu_2 r_2)(1 + \nu_1 r_1)(1 + \nu_2 r_2) \\ &= (1 - \nu_2 r_2 - \nu_1 r_1 + \nu_1 \nu_2 r_1 r_2)(1 + \nu_2 r_2 + \nu_1 r_1 + \nu_1 \nu_2 r_1 r_2) \\ &= 1 + \nu_1 \nu_2 r_1 r_2 - \nu_1 \nu_2 r_2 r_1 = 1 + \nu_1 \nu_2 (r_1, r_2).\end{aligned}$$

Thus our base case holds. Assuming our hypothesis holds for some $n \geq 2$, observe that

$$\begin{aligned}[1 + \nu_1 r_1, \ldots, 1 + \nu_n r_n, 1 + \nu_{n+1} r_{n+1}] &= [[1 + \nu_1 r_1, \ldots, 1 + \nu_n r_n], 1 + \nu_{n+1} r_{n+1}] \\ &= [1 + \nu_1 \cdots \nu_n (r_1, \ldots, r_n), 1 + \nu_{n+1} r_{n+1}] \\ &= 1 + \nu_1 \cdots \nu_{n+1}((r_1, \ldots, r_n), r_{n+1}) \\ &= 1 + \nu_1 \cdots \nu_{n+1}(r_1, \ldots, r_{n+1}).\end{aligned}$$

This completes the induction step. □

Lemma 3.33. *Let R be a ring. Then for any positive integer n, $\gamma_n(U(R)) \subseteq 1 + R^{(n)}$. In particular, if R is strongly Lie nilpotent, then $U(R)$ is nilpotent.*

Theorem 3.34 (**Khripta**)**.** *Let G be a group having an element g of order p. If K is a field of characteristic p, then $U(KG)$ is nilpotent if and only if G is nilpotent and p-abelian.*

Proof. ($\Rightarrow$) Suppose that $U(KG)$ is nilpotent. Treating G as a subgroup of $U(KG)$, it follows that G is nilpotent. Moreover, since G has an element of order p, it follows from 1.27 that G has an element of order p in its centre. By 3.31 and 1.30, G' must be a p-group of bounded exponent. We assume towards a contradiction that G' is infinite.

Since G is nilpotent, it follows that the lower central series eventually terminates. Therefore, we can find a largest natural number n such that $\gamma_n(G)$ is infinite, but $\gamma_{n+1}(G)$ is finite. Then $\gamma_{n+1}(G)$ is a finite p-group. Observe that

$$G'/\gamma_{n+1}(G) = G'/(\gamma_{n+1}(G) \cap G') \simeq (G'\gamma_{n+1}(G))/\gamma_{n+1}(G).$$

Thus, it suffices to show that $G'/\gamma_{n+1}(G)$ is finite. But by 3.27, it follows that $U(K(G/\gamma_{n+1}(G)))$ is nilpotent. Moreover, by definition, $\gamma_{n+1}(G) = [\gamma_n(G), G]$. Thus, we may factor out $\gamma_{n+1}(G)$ and assume that $\gamma_n(G)$ is an infinite central p-group of bounded exponent. Applying 1.5, we may assume G contains a central subgroup of the form $A = \prod_{i=1}^{\infty} A_i$, where each A_i is a nontrivial cyclic p-group.

Let X be a transversal of A in G. We suppose that $U(KG)$ satisfies $[x_1, \ldots, x_m] = 1$, and take any $\alpha_1, \ldots, \alpha_m \in KG$. Since these elements all have finite support, we may choose a natural number k so that $(\alpha_1, \ldots, \alpha_m) = \sum_j \beta_j h_j$, where each $\beta_j \in K(A_1 \times \cdots \times A_k)$ and $h_j \in X$. For each i, $1 \leq i \leq m$, we let $\eta_i = \hat{A}_{k+i}$. As each

η_i is central and square zero, it follows that $1 + \eta_i\alpha_i \in U(KG)$ for all i. Thus, the group identity on $U(KG)$, together with 3.32, gives us the following:

$$\begin{aligned} 1 &= [1 + \eta_1\alpha_1, \ldots, 1 + \eta_m\alpha_m] \\ &= 1 + \eta_1 \cdots \eta_m(\alpha_1, \ldots, \alpha_m) \\ &= 1 + \eta_1 \cdots \eta_m \sum_j \beta_j h_j. \end{aligned}$$

Since each of the h_j's lie in distinct (i.e. disjoint) cosets of A, we must have that $\eta_1 \cdots \eta_m\beta_j = 0$ for all j. Furthermore, the product of the A_i's is direct. As no $\eta_i = 0$, we must have that $\beta_j = 0$ for all j. In other words, $(\alpha_1, \ldots, \alpha_m) = \sum 0 = 0$. The α_i's being arbitrary, it follows that KG is Lie nilpotent. But then, by 3.29, we have that G' is a finite p-group.

($\Leftarrow$) Conversely, assume that G is nilpotent with G' a finite p-group. By 3.28, we must have that $(KG)^{(2p^k)} = 0$ for some positive integer k. But then, by 3.33, $\gamma_{2p^k}(U(KG)) \subseteq 1 + (KG)^{2p^k} = 1$, so $U(KG)$ is nilpotent, as desired. □

Before we discuss another major result regarding nilpotent unit groups, we must first look at a few preliminary results from [4].

Lemma 3.35. *Suppose that $U(\mathbb{Z}G)$ is nilpotent. Then, for $t, t_1, t_2 \in T_G, g \in G$, we have the following implications:*

(i) $g^{-1}tg \neq t \Rightarrow g^{-1}tg = t^{-1}$

(ii) $|t|$ *is odd* $\Rightarrow gt = tg$

(iii) $|t_1| > 1$ *and odd,* $|t_2|$ *is even* $\Rightarrow T_G$ *is central in* G.

Lemma 3.36. *If G is a nilpotent group, then $\mathbb{Q}G$ has no nilpotent elements if and only if the torsion subgroup of G is a normal subgroup and one of the following conditions is met:*

(1) T_G is abelian and for $g \in G$, we have locally on T_G that

$$x^{-1}tx = t^{i(x)} \text{ for all } t \in T.$$

That is, for a finite subgroup B of T_G, we have that $x^{-1}bx = b^i$ for all $b \in B$, where i depends on both B and x.

(2) $T_G = A \times E \times K_8$ where A is an abelian group in which every element has odd order, E is an elementary abelian 2-group, and K_8 is the quaternion group such that modulo every n, with an element of order n in A, the multiplicative order of 2 is odd. Moreover, K_8 is normal in G, conjugation by any $g \in G$ induces an inner automorphism on K_8, and conjugation by $g \in G$ acts as described in (1) on $A \times E$.

Theorem 3.37. *$U(\mathbb{Z}G)$ is nilpotent if and only if G is nilpotent and T_G satisfies one of the following:*

(i) T_G is central in G,

(ii) T_G is an abelian 2-group and for $g \in G, t \in T_G$, we have that

$$g^{-1}tg = t^{\epsilon(g)},\ \epsilon(g) = \pm 1$$

(iii) $T_G = E \times K_8$ where $E^2 = 1$ and K_8 is the quaternion group of order 8. Moreover, E is central in G and conjugation by any $g \in G$ induces one of the four inner automorphisms on K_8.

For good measure, we state the following result regarding group algebras.

Theorem 3.38. *Let KG be a group algebra over a field K of characteristic $p \geq 0$. If $p > 0$, let G have no element of order p. Then $U(KG)$ is nilpotent if and only if G is nilpotent and one of the following holds:*

(i) T_G is a central subgroup

(ii) $|K| = 2^\beta - 1 = p$, a Mersenne prime; T_G is an abelian group of exponent (p^2-1), and for $g \in G, t \in T_G$, we have that

$$g^{-1}tg = t \text{ or } t^p.$$

4 Conclusion

" The study of mathematics, like the Nile, begins in minuteness but ends in magnificence."

Charles Caleb Colton

There are a number of useful results in [4] concerning solvable unit groups which warrant further exploration. For example, there is the following result due to Zassenhaus:

Lemma 4.1. *Let $G = K_8 \times \langle x \rangle$, where $\langle x \rangle$ is a cyclic group of prime order $p > 2$. Then $U(\mathbb{Z}G)$ is not solvable.*

Another similar result to that of 3.37 above is the following:

Theorem 4.2. *Suppose that $U(\mathbb{Z}G)$ is solvable. Then*

(1) The torsion elements of G form a group which is either abelian or a Hamiltonian 2-group, with every subgroup normal in G.

Conversely, if G is a solvable group satisfying (1) and G/T_G is nilpotent, then $U(\mathbb{Z}G)$ is solvable.

Corollary 4.3. *If G is finite then $U(\mathbb{Z}G)$ is solvable if and only if G is abelian or a Hamiltonian 2-group.*

Regarding the group ring $\mathbb{Q}G$, [4] also discusses the following results:

Theorem 4.4. *Suppose that $U(\mathbb{Q}G)$ is solvable. Then*

(2) The torsion elements of G form an abelian subgroup T_G with every subgroup normal in G.

Conversely, if G is a solvable group satisfying (1) and (2) above, then $U(\mathbb{Q}G)$ is solvable.

Corollary 4.5. *If G is finite, then $U(\mathbb{Q}G)$ is solvable if and only if G is abelian.*

There is the following result due to Bateman:

Theorem 4.6. *If K is a field of positive characteristic $p \neq 2, 3$ and G is a finite group, then $U(\mathbb{Q}G)$ is solvable if and only if G' is a p-group.*

Lee, in [5], also offers an extensive examination of necessary and sufficient conditions of the solvability of $U(KG)$.

Lemma 4.7. *Let K be a field of characteristic $p \geq 2$ and G a group. Let N be a finite normal p-subgroup of G. Then $U(KG)$ is solvable if and only if $U(K(G/N))$ is solvable.*

Theorem 4.8. *Let K be a field of characteristic $p \geq 0$, with $|K| > 3$. Let G be a finite group. The $U(KG)$ is solvable if and only if G is p-abelian.*

Theorem 4.9. *Let K be a field of characteristic $p \geq 0$ and G a torsion group. Suppose that $|K| > 3$. The $U(KG)$ is solvable if and only if either*

1. *$p \neq 2$ and G is p-abelian; or*
2. *$p = 2$, G has a 2-abelian subgroup of index at most 2, and G' is a 2-group of bounded exponent.*

Corollary 4.10. *Let K be a field such that char $K \neq 2, 3$ and let G be a torsion group. Then $U(KG)$ is solvable if and only if KG is Lie solvable.*

For those instances when G is a nontorsion group, Lee gives the following results:

Theorem 4.11. *Let K be a field of characteristic $p > 0$ and G a nontorsion group containing finitely many p-elements. Then $U(KG)$ is solvable if and only if the p-elements of G form a subgroup P and $U(K(G/P))$ is solvable.*

Theorem 4.12. *Let K be a field of characteristic $p > 2$ and G a nontorsion group containing infinitely many p-elements. Then $U(KG)$ is solvable if and only if G is p-abelian.*

Theorem 4.13. *Let K be a field of characteristic 2 and G a nontorsion group containing infinitely many 2-elements. Then $U(KG)$ is solvable if and only if*

1. *G has a 2-abelian subgroup A of index at most 2;*
2. *the 2-elements of G form a subgroup P;*
3. *the torsion elements of G/P form an abelian group, T/P; and*
4. *every idempotent of $K(G/P)$ is central.*

Theorem 4.14. *Let K be a field of characteristic 2 and G a nontorsion group whose 2-elements have unbounded exponent. Then $U(KG)$ is solvable if and only if G has a 2-abelian subgroup A of index at most 2, and G' is a 2-group of bounded exponent.*

In future research, these results and their proofs might be explored in depth.

References

[1] C. Polcino Milies and S. K. Sehgal, 2002: *An Introduction to Group Rings*. Kluwer Academic Publishers, 371 pp.

[2] D. S. Dummit and R. M. Foote, 2004: *Abstract Algebra*. John Wiley and Sons, Inc, 932 pp.

[3] D. J. S. Robinson, 1996: *A Course in the Theory of Groups*. Springer-Verlag New York Inc, 499 pp.

[4] S. K. Sehgal, 1978: *Topics in Group Rings*. Marcel Dekker Inc, 251 pp.

[5] G. T. Lee, 2010: *Group Identities on Units and Symmetric Units of Group Rings*. Springer, 194 pp.