NORMAL COMPLEMENTS AND THE NUMBER TWO

HEATHER McINTOSH

Your file Votre référence
ISBN: 978-0-494-33435-5
Our file Notre référence
ISBN: 978-0-494-33435-5

Normal Complements and The Number Two

by

©Heather McIntosh

A Thesis Submitted to the School of Graduate Studies in partial fulfillment of the requirement for the degree of Master of Science

Department of Mathematics and Statistics
Memorial University of Newfoundland

May, 2007

St. John's, Newfoundland, Canada

Contents

Acknowledgements

First of all, I would like to sincerely thank my supervisor Dr. Edgar Goodaire. Every adventure needs direction and a starting point. Thanks for your guidance, your direction and above all, thanks for your patience.

Thank you to Atlantic Association for Research in the Mathematical Sciences (AARMS) for letting me take two graduate courses through their summer school at Dalhousie University. I would also like to thank Dr. M. Parmenter, Dr. Peter Booth, and Dr. Yiqiang Zhou, for the many of hours spent in their office during my masters courses, and also Dr. Peter Booth for being my teacher sponsor when I took the Graduate Program in Teaching. I am thankful for getting the opportunity to teach during my program. Another thank-you goes to the Department of Mathematics and Statistics, Dr. Goodaire and Dr. Parmenter for their financial support.

No matter how strong a bridge it will fall if it does not have a strong support structure. Thanks to all of my friends and family for being my support structure. I would also like to thank the Memorial University Cross Country running team for all their moral support. I am grateful that I was able to run with the team during my program. A special thanks goes to my Mom, Dad and my Grandma Chapman for having faith when I did not.

Thanks goes to Dr. Jennifer Hyndman for inspiring and encouraging me to do a masters degree in Algebra. Also to Mr. Abra, my grade 12 math teacher, for inspiring me to pursue mathematics.

Abstract

As a means to solving the isomorphism problem many mathematicians have studied the unit group of a group ring. The group G is contained in the group of units. Thus it is beneficial to find out how the group G sits in the unit group. One question that can be asked is: When does G have a normal complement in the unit group of a group ring? In this thesis we will investigate that question by looking at the unit groups of group rings of the form F_2G where G is a group of small order. We will also look at results from two papers by Robert Sandling ([**San84b, San89**]). In these papers Sandling shows that for modular group algebras of central-elementary-by-abelian p-groups G has a normal complement in the unit group.

CHAPTER 1

Introduction

1.1. History

A group ring RG is an R-algebra where every element can be expressed as a linear combination of elements in G with coefficients from R and G is linearly independent over R. Multiplication in RG is based on the multiplication in G and R, extended by using the distributive laws. The isomorphism problem is a famous group ring problem. It asks what conditions must be present for $RH \cong RG$ to imply that $H \cong G$ [**MS02, Des56**]. The isomorphism problem does not always have a positive result, for example, $\mathbf{C}[C_2 \times C_2] \cong \mathbf{C} \oplus \mathbf{C} \oplus \mathbf{C} \oplus \mathbf{C} \cong \mathbf{C}C_4$, but $C_2 \times C_2 \ncong C_4$[**MS02**]. A list of positive results for the modular case can be found in [**Chr04**] and [**HS06**]. W. E. Deskins [**Des56**], D. S. Passman [**Pas65**], Inder Bir S. Passi and Sudarshan K. Sehgal [**PS72**], Robert Sandling [**San84a, San96**], Wursthorn [**Wur93**], Mohamed A. M. Salim [**SS96**], Blecher, Kimmerie, Roggenkamp [**Chr04**] have all been major contributors. The group G is contained in the unit group of the group ring, so information for the isomorphism problem can often be found by looking at the unit group $U(RG)$. It is useful to know how G sits in the $U(RG)$ or if G has a normal complement in $U(RG)$. Now G has a normal complement in $U(RG)$ if there exists $W \subseteq U(RG)$ such that:

(1) $U(RG) = GW$
(2) $G \cap W = \{1\}$
(3) W is a normal subgroup of $U(RG)$.

In this setting we will write $U(RG) = W \rtimes G$. Recall that a group is torsion free if all elements have infinite order.

THEOREM 1.1.1. [**Seh93**, pp. 157-158]*In the case of integral group rings of finite groups, if a torsion free normal complement exists the isomorphism problem has a positive solution.*

PROOF. Let $\theta\colon ZG \to ZH$ be an isomorphism and note that G and H have the same order as bases of the same Z-module. Assume $U(ZH) = N \rtimes H$. Units map to units and $G \subset U(ZG)$ so for every $g \in G$, $\theta(g) = nh$ for some $n \in N$ and some $h \in H$. Then we can define $\beta\colon G \to U(ZH)/N \cong H$ by $\beta(g) = N\theta(g)$. First we want to show that this is a homomorphism. Choose $g_1, g_2 \in G$, then $\beta(g_1g_2) = N\theta(g_1g_2) = N\theta(g_1)\theta(g_2) = N\theta(g_1)N\theta(g_2) = \beta(g_1)\beta(g_2)$. Thus β is a homomorphism. Then, $\ker(\beta) = \{g \in G \mid N\theta(g) = 1\} = \{g \in G \mid \theta(g) \in N\} = \{1\}$, since N is torsion free, θ is an isomorphism and the elements of G have finite order. Thus β is an injective function and, since $|G| = |H|$, an isomorphism. $\square$

Some mathematicians who used this method to solve the isomorphism problem are: D. S. Passman and P. F. Smith [**PS81**], G. H. Cliff, S. K. Sehgal, A. R. Weiss [**CSW81**]. These results and other positive results on integral group rings can be found in [**Mil82, Seh90**]. In the modular case it has been shown that G has a normal complement in $U(FG)$ if G is a finite abelian p-group [**Joh78**], if G is a cyclic group [**Joh78**], or if G is a central-elementary-by-abelian group [**San89**].

1.2. Preliminary Results

In this section we will go over some definitions and preliminary results. Let G be a group. Then the commutator subgroup G' of the group is the subgroup generated by the set $\{(g_1, g_2) \mid g_1, g_2 \in G\}$, where $(g_1, g_2) = g_1^{-1}g_2^{-1}g_1g_2$.

DEFINITION 1.2.1. *Let* $\varepsilon\colon RG \to R$ *be the homomorphism defined by* $\varepsilon(\sum_{g\in G}\alpha_g g) = \sum_{g\in G}\alpha_g$. *The kernel of this map is called the* augmentation ideal *of* RG *and is denoted by* Δ.

REMARK 1.2.2. To prove that ε is a homomorphism, pick $\alpha = \sum_{g\in G}\alpha_g g$ and $\gamma = \sum_{g\in G}\gamma_g g \in RG$. Then $\varepsilon(\alpha+\gamma) = \varepsilon(\sum_{g\in G}\alpha_g g + \sum_{g\in G}\gamma_g g) = \varepsilon(\sum_{g\in G}(\alpha_g+\gamma_g)g) = \sum_{g\in G}(\alpha_g+\gamma_g) = \sum_{g\in G}\alpha_g + \sum_{g\in G}\gamma_g = \varepsilon(\sum_{g\in G}\alpha_g g) + \varepsilon(\sum_{g\in G}\gamma_g g)$. Also, $\varepsilon(\alpha\gamma)$ $= \varepsilon(\sum_{g\in G}\alpha_g g\sum_{h\in G}\gamma_h h) = \varepsilon(\sum_{g,h\in G}\alpha_g\gamma_h gh) = \sum_{g,h\in G}\alpha_g\gamma_h = \sum_{g\in G}\alpha_g\sum_{h\in G}\gamma_h = \varepsilon(\alpha)\varepsilon(\gamma)$. So the map is operation preserving. Thus ε is a ring homomorphism.

EXAMPLE 1.2.3. Let $C_3 = \{1, a, a^2\}$ and $R = F_2$, the field of two elements. The kernel of ε is the set $\{\sum_{g\in C_3}\alpha_g g \in F_2C_3 \mid \varepsilon(\sum_{g\in C_3}\alpha_g g) = 0_{F_2}\} = \{\alpha_0 + \alpha_1 a + \alpha_2 a^2 \mid \alpha_0+\alpha_1+\alpha_2 = 0\}$. Now $\alpha_i = 1$ or 0, so in order for $\alpha_0+\alpha_1+\alpha_2 = 0$ either,

$$\alpha_0 = \alpha_1 = \alpha_2 = 0$$

$$\text{or } \alpha_0 = \alpha_1 = 1 \text{ and } \alpha_2 = 0$$

$$\text{or } \alpha_0 = \alpha_2 = 1 \text{ and } \alpha_1 = 0$$

$$\text{or } \alpha_1 = \alpha_2 = 1 \text{ and } \alpha_0 = 0$$

Thus $\ker\varepsilon = \{0, 1+a, 1+a^2, a+a^2\} = \Delta$.

EXAMPLE 1.2.4. Let $C_2\times C_2 = \{1, a, b, ab\}$ and $R = F_2$. Then, $\ker\varepsilon = \{\sum_{g\in C_2\times C_2}\alpha_g g \in F_2(C_2\times C_2) \mid \varepsilon(\sum_{g\in C_2\times C_2}\alpha_g g) = 0\} = \{\alpha_0+\alpha_1 a+\alpha_2 b+\alpha_3 ab \mid \alpha_0+\alpha_1+\alpha_2+\alpha_3 = 0\}$. Thus, $\alpha_i = 1$ or 0, so $\alpha_0+\alpha_1+\alpha_2+\alpha_3 = 0$ in precisely the following eight cases:

(1) $\alpha_0 = \alpha_1 = \alpha_2 = \alpha_3 = 0$

(2) $\alpha_0 = \alpha_1 = \alpha_2 = \alpha_3 = 1$

(3) $\alpha_0 = \alpha_1 = 1, \alpha_2 = \alpha_3 = 0$

(4) $\alpha_0 = \alpha_2 = 1, \alpha_1 = \alpha_3 = 0$

(5) $\alpha_0 = \alpha_3 = 1, \alpha_1 = \alpha_2 = 0$

(6) $\alpha_1 = \alpha_2 = 1, \alpha_0 = \alpha_3 = 0$

(7) $\alpha_1 = \alpha_3 = 1, \alpha_0 = \alpha_2 = 0$

(8) $\alpha_2 = \alpha_3 = 1, \alpha_0 = \alpha_1 = 0$

Thus $\ker \varepsilon = \{0, 1+a+b+ab, 1+a, 1+b, 1+ab, a+b, a+ab, b+ab\}$.

DEFINITION 1.2.5. *Let N be a normal subgroup of a group G. Consider the homomorphism $\mu \colon RG \to R[G/N]$ defined by $\mu(\sum_{g\in G} \alpha_g g) = \sum_{g\in G} \alpha_g Ng = \sum_{g\in G} \alpha_g \overline{g}$. The kernel of this map is called the augmentation ideal $\Delta(G, N)$.*

REMARK 1.2.6. When $N = G$ the above map becomes $\mu \colon RG \to R[G/G] \cong R$ and is defined by $\mu(\sum_{g\in G} \alpha_g g) = \sum_{g\in G} \alpha_g Gg = \sum_{g\in G} \alpha_g G$. Then, $\ker \mu = \{\sum_{g\in G} \alpha_g g \mid \sum_{g\in G} \alpha_g G = 0\} = \{\sum_{g\in G} \alpha_g g \mid \sum_{g\in G} \alpha_g = 0\} = \ker \varepsilon = \Delta$. Thus, $\Delta = \Delta(G, G)$.

EXAMPLE 1.2.7. Write $C_2 \times C_2 = \{1, a, b, ab\}$. Then $H = \{1, a\}$ is a normal subgroup. Consider the map $\mu \colon F_2(C_2 \times C_2) \to F_2[(C_2 \times C_2)/H]$ defined by $\mu(\sum_{g\in C_2\times C_2} \alpha_g g) = \sum_{g\in C_2\times C_2} \alpha_g Hg$. Now $\ker(\mu) = \{\sum_{g\in C_2\times C_2} \alpha_g g \in F_2(C_2 \times C_2) \mid \sum_{g\in (C_2\times C_2)} \alpha_g Hg = 0\} = \{\alpha_0 + \alpha_1 a + \alpha_2 b + \alpha_3 ab \mid \alpha_0 H + \alpha_1 Ha + \alpha_2 Hb + \alpha_3 Hab = 0\} = \{\alpha_0 + \alpha_1 a + \alpha_2 b + \alpha_3 ab \mid (\alpha_0 + \alpha_1)H + (\alpha_2 + \alpha_3)Hb = 0\}$. The equation, $(\alpha_0 + \alpha_1)H + (\alpha_2 + \alpha_3)Hb = 0$ can be satisfied in four ways:

(1) $\alpha_0 = \alpha_1 = \alpha_2 = \alpha_3 = 0$

(2) $\alpha_0 = \alpha_1 = 1$ and $\alpha_2 = \alpha_3 = 0$

(3) $\alpha_0 = \alpha_1 = 0$ and $\alpha_2 = \alpha_3 = 1$

(4) $\alpha_0 = \alpha_1 = \alpha_2 = \alpha_3 = 1$.

So $\ker \mu = \{1+a+b+ab, 1+a, b+ab, 0\} = \Delta(C_2 \times C_2, H)$.

From group theory we know that we can express a group G as a union of disjoint cosets of N, where N is a normal subgroup of G. Thus $G = \bigcup_{x \in \Im} Nx$, where $Nx \cap Ny = \emptyset$ for all $x, y \in \Im \subseteq G$.

LEMMA 1.2.8. [**GJM96**, page 150] *Let N be a normal subgroup of a group G. Then $\Delta(G, N) = \sum_{n \in N}(n-1)RG$.*

PROOF. Choose $\alpha = \sum_{g \in G} \alpha_g g \in \Delta(G, N)$, where $\alpha_g \in R$. Let $G = \bigcup_{x \in \Im \subseteq G} Nx$ where $Nx \cap Ny = \emptyset$ for all $x, y \in \Im \subseteq G$. Each element $g \in G$ can be written as $g = nx$, where $x \in \Im$ and $n \in N$. Consequently, $\alpha = \sum_{g \in G} \alpha_g g = \sum_{x \in \Im} \sum_{n \in N} \alpha_{nx} nx$. Denote by $g \mapsto \overline{g}$ the natural map $G \to G/N$ and extend to a group homomorphism $RG \to R[G/N]$. Then $\overline{\alpha} = \sum_{x \in \Im} \sum_{n \in N} \alpha_{nx} Nnx = \sum_{x \in \Im} \sum_{n \in N} \alpha_{nx} Nx = \sum_{x \in \Im} \{\sum_{g \in G, Ng = Nx} \alpha_g\} Nx = \sum_{x \in \Im} \{\sum_{g \in G, \overline{g} = \overline{x}} \alpha_g\} \overline{x} = 0$. Now $\overline{x} \in G/N$ are linearly independent in $R[G/N]$, so for each $x \in \Im$, $\sum_{g \in G, \overline{g} = \overline{x}} \alpha_g = 0$. Thus $\sum_{g \in G, \overline{x} = \overline{g}} \alpha_g g = \sum_{g \in G, \overline{x} = \overline{g}} \alpha_g g - 0 = \sum_{g \in G, \overline{x} = \overline{g}} \alpha_g g - \sum_{g \in G, \overline{g} = \overline{x}} \alpha_g x = \sum_{g \in G, \overline{x} = \overline{g}} \alpha_g (gx^{-1})x - \sum_{g \in G, \overline{g} = \overline{x}} \alpha_g x = \sum_{g \in G, \overline{x} = \overline{g}} \alpha_g ((gx^{-1}) - 1)x$. Consequently, $\alpha = \sum_{x \in \Im} \sum_{g \in G, \overline{x} = \overline{g}} \alpha_g (gx^{-1} - 1)x = \sum_{x \in \Im} \sum_{g \in G, \overline{x} = \overline{g}} ((gx^{-1}) - 1)\alpha_g x$. Now $\overline{x} = \overline{g}$ so $gx^{-1} \in N$ and $\alpha \in \sum_{n \in N}(n-1)RG$. Thus $\Delta(G, N) \subseteq \sum(n-1)RG$. The other inclusion is clear. $\square$

EXAMPLE 1.2.9. Again let $H = \{1, a\}$ be the (normal) subgroup of $C_2 \times C_2 = \{1, a, b, ab\}$. By the above $\Delta(C_2 \times C_2, H) = \sum_{h \in H} F_2(C_2 \times C_2)(a+1)$. Choose $\alpha = \alpha_0 + \alpha_1 a + \alpha_2 b + \alpha_3 ab \in F_2(C_2 \times C_2)$. Then, $(1+a)(\alpha_0 + \alpha_1 a + \alpha_2 b + \alpha_3 ab) = (\alpha_0 + \alpha_1) + a(\alpha_0 + \alpha_1) + b(\alpha_2 + \alpha_3) + ab(\alpha_2 + \alpha_3)$. In F_2, $\alpha_0 + \alpha_1 = 1$ or 0 and the same can be said for $\alpha_2 + \alpha_3$. Thus the following four cases arise:

(1) $\alpha_0 + \alpha_1 = 1$ and $\alpha_2 + \alpha_3 = 1$

(2) $\alpha_0 + \alpha_1 = 1$ and $\alpha_2 + \alpha_3 = 0$

(3) $\alpha_0 + \alpha_1 = 0$ and $\alpha_2 + \alpha_3 = 1$

(4) $\alpha_0 + \alpha_1 = 0$ and $\alpha_2 + \alpha_3 = 0$

Then there are four different possibilities for α, namely $1 + a + b + ab$,$1 + a$, $b + ab$, 0. Thus $\Delta(C_2 \times C_2, H) = \{0, 1 + a, b + ab, 1 + a + b + ab\}$, which corresponds to the $\Delta(C_2 \times C_2, H)$ found in Example 1.2.7.

COROLLARY 1.2.10. *Let G be a group and R be a ring. Then $\Delta = \sum_{g \in G} R(g - 1)$.*

PROOF. From Lemma 1.2.8 we know that $\Delta = \Delta(G, G) = \sum_{g \in G} RG(g - 1)$. So any element in Δ is of the form $\sum_{g \in G} \sum_{h \in G} \alpha_h h(g - 1) \in \sum_{g \in G} R(g - 1)$. Thus $\Delta = \sum_{g \in G} R(g - 1)$. $\square$

Consider the group ring F_2C_3. According to Corollary 1.2.10, $\Delta = \sum_{g \in C_3} F_2(g + 1)$. Hence Δ is spanned over F_2 by the set $\{g + 1 \mid g \in C_3\} = \{0, a + 1, a^2 + 1\}$. Then $\Delta = \{0, a+1, a^2+1, a+a^2\}$ which corresponds with the Δ that was found in Example 1.2.3.

Consider again the group ring $F_2(C_2 \times C_2)$. According to Corollary 1.2.10, $\Delta = \sum_{g \in C_2 \times C_2} F_2(g + 1)$. Hence Δ is spanned over F_2 by the set: $\{1 + a, 1 + b, 1 + ab, 0\}$. Thus $\Delta = \{0, 1+a, 1+b, 1+ab, a+b, a+ab, b+ab, 1+a+b+ab\}$ which corresponds to the Δ that we found previously, in Example 1.2.4.

THEOREM 1.2.11. [**MS02**, page 135] *Let N be a normal subgroup of a group G. Let $S = \{x_1, \ldots, x_d\}$, be a set of generators of N. Then $\Delta(G, N) = \sum_{x_i \in S} RG(x_i - 1)$.*

PROOF. By Lemma 1.2.8, $\Delta(G, N) = \sum_{g \in N}(n - 1)RG$. Thus $\{n - 1 \mid n \in N\}$ spans $\Delta(G, N)$. As a result it is adequate to show that any element of the form $n - 1$, with $n \in N$, is in the set $\sum_{x_i \in S} RG(x_i - 1)$. Choose $n \in N$. Then $n = x_1^{t_1} x_2^{t_2} \cdots x_r^{t_r}$, where $x_i \in S$ are not necessarily distinct and $t_i = \pm 1$. The proof will proceed by induction on r using the identities

$$x^{-1} - 1 = x^{-1}(1 - x) \tag{1.1}$$

and

$$xy - 1 = x(y - 1) + (x - 1). \tag{1.2}$$

When $r = 1$, $n - 1 = x_1^{t_1} - 1$. If $t_1 = 1$, this has the right form. If $t_1 = -1$, then by identity (1.1) $x_1^{-1} - 1 = x_1^{-1}(x_1 - 1)$ is also in $\sum_{x_i \in S} RG(x_i - 1)$. Assume that the induction hypothesis is true for $1 \leq k \leq r$ and let $n - 1 = x_1^{t_1} x_2^{t_2} \cdots x_r^{t_r} x_{r+1}^{t_{r+1}} - 1$. Using (1.2),

$$\begin{aligned}(x_1^{t_1} x_2^{t_2} \cdots x_r^{t_r} x_{r+1}^{t_{r+1}}) - 1 &= ((x_1^{t_1} x_2^{t_2} \cdots x_r^{t_r}) x_{r+1}^{t_{r+1}}) - 1 \\ &= x_1^{t_1} x_2^{t_2} \cdots x_r^{t_r} (x_{r+1}^{t_{r+1}} - 1) + ((x_1^{t_1} x_2^{t_2} \cdots x_r^{t_r}) - 1).\end{aligned}$$

Now $x_1^{t_1} x_2^{t_2} \cdots x_r^{t_r} \in RG$, so by the base case $x_1^{t_1} x_2^{t_2} \cdots x_r^{t_r} (x_{r+1}^{t_{r+1}-1} - 1) \in \sum_{x_i \in S} RG(x_i - 1)$. Also by induction hypothesis $(x_1^{t_1} x_2^{t_2} \cdots x_r^{t_r}) - 1 \in \sum_{x_i \in S} RG(x_i - 1)$. Consequently $(x_1^{t_1} x_2^{t_2} \cdots x_r^{t_r} x_{r+1}^{t_{r+1}}) - 1 \in \sum_{x_i \in S} RG(x_i - 1)$. By the principle of mathematical induction $\Delta(G, H) = \sum_{x_i \in S} RG(x_i - 1)$. □

DEFINITION 1.2.12. *An element x of a ring R is nilpotent if there exists an integer $n \geq 1$ such that $x^n = 0$. A ring is nil if all its elements are nilpotent and nilpotent if, for some integer $n \geq 1$, the product of any n elements is 0.*

THEOREM 1.2.13. *Let G be a finite p-group and R be a ring of characteristic p. Then $\Delta = \Delta(G)$ is nilpotent.*

PROOF. Let $|G| = p$. Then $G = \langle a \rangle$, and Δ is generated by $1-a$. Choose $\alpha_i \in \Delta$. Then $\alpha_i = \gamma_i(1-a)$, where $\gamma_i \in RG$. So $\alpha_1\alpha_2\cdots\alpha_p = \gamma_1\gamma_2\cdots\gamma_p(1-a)^p = 0$. Assume the result is true for all groups with order less than $|G| = n$. Choose $1 \neq z \in Z(G)$ the centre of G (we can do this since p-groups have a non-trivial centre). Without loss of generality let $|z| = p$. Then $|G/\langle z \rangle| < |G|$, so by the induction hypothesis there exists an integer t such that $\Delta(G/\langle z \rangle)^{p^t} = 0$. So $\Delta^{p^t} \subseteq \Delta(G, \langle z \rangle) = (1-z)RG$. Then $\Delta^{p^{t+1}} \subseteq (1-z)^p RG = 0$. So the result is true and by the principle of mathematical induction Δ is nilpotent for any finite p-group G. □

EXAMPLE 1.2.14. Again let $G = C_2 \times C_2$ and look at the group ring F_2G. Here the field is of characteristic 2 and G is a 2-group. Recall that Δ is spanned over F_2G by $1+a$ and $1+b$. Moreover, $(1+a)^2 = (1+b)^2 = 0$. It follows readily that $\Delta^3 = 0$, in agreement with Theorem 1.2.13.

On the other hand consider the group-ring F_2C_3. Here the field is of characteristic 2 and C_3 is a 3-group, so the previous theorem does not necessarily apply. Recall that $\Delta = \{0, 1+a, 1+a^2, a+a^2\}$. Here

- $(1+a)^4 = 1+a$
- $(1+a^2)^4 = 1+a^2$
- $(a+a^2)^2 = a+a^2$.

None of the elements is nilpotent so, of course, Δ is not nilpotent.

LEMMA 1.2.15. *Let $\alpha \in RG$, where G is a group and R is any ring of coefficients. If α is a nilpotent element then $1+\alpha$ is a unit.*

PROOF. Now α is nilpotent so there exists n such that $\alpha^n = 0$. So $(1+\alpha)(1-\alpha+\alpha^2-\cdots+(-1)^{n-1}\alpha^{n-1}) = 1-\alpha+\alpha^2-\cdots+(-1)^{n-2}\alpha^{n-2}+(-1)^{n-1}\alpha^{n-1}+\alpha-$

$\alpha^2 + \cdots + (-1)^{n-1}\alpha^{n-1} + (-1)^n\alpha^n = 1 = (1 - \alpha + \alpha^2 - \cdots + (-1)^{n-1}\alpha^{n-1})(1 + \alpha)$.
Hence $1 - \alpha + \alpha^2 - \cdots + (-1)^{n-1}\alpha^{n-1}$ is the inverse of $1 + \alpha$ in RG. □

COROLLARY 1.2.16. *Let G be a finite p-group and F be a field of characteristic p. If $\alpha \in \Delta$ then $1 + \alpha$ is a unit.*

PROOF. This follows directly from Theorem 1.2.13 and Lemma 1.2.15. □

CHAPTER 2

Normal Complements

In this chapter we will look at results from two of Robert Sandling's papers, ([**San84b, San89**]). In these papers he proves that in the modular case there is a normal complement for certain p-groups G in their unit groups. In fact he actually gives an explicit form for such normal complements. Here we will prove some of Sandling's results in the case where $p = 2$. We will be using the following notation and definitions:

- G denotes a finite 2-group,
- F_2 denotes the field with 2 elements and F_2G denotes the modular group algebra,
- $V = V(F_2G)$ is the group of units.

We use throughout that $V = 1 + \Delta$. To see why, choose $v \in V$. There exists $u \in V(F_2G)$ such that $uv = 1$. Now $\varepsilon(uv) = \varepsilon(1) = 1$ since homomorphisms map identities to identities. Thus $\varepsilon(u)\varepsilon(v) = 1$ and since we are in characteristic 2 this implies that $\varepsilon(v) = \varepsilon(u) = 1$. So $v = 1 + (1 + v) \in 1 + \Delta$. So $V \subseteq 1 + \Delta$ and the other inclusion was Corollary 1.2.16. Note too that in F_2G one half the elements have augmentation 1 and the other half have augmentation 0. So $|V(F_2G)| = \frac{1}{2}|F_2G|$.

EXAMPLE 2.0.1. Let $G = C_2 \times C_2 = \langle a, b\rangle = \{a, b, ab, 1\}$. Then $|G| = 4 = 2^2$,$|F_2G| = 2^4$ and $|V(F_2G)| = 2^3$. As we found before $\Delta = \sum_{g\in G} F_2(g + 1)$, hence Δ is spanned over F_2 by the set $\{1 + a, 1 + b, 1 + ab, 0\}$. Thus $\Delta = \{0, 1 + a, 1 + b, 1 + ab, a + b, a +$

$ab, b+ab, 1+a+b+ab\}$. Then as noted earlier $V = 1+\Delta$, so $V = \{1, a, b, ab, 1+a+b, 1+a+ab, 1+b+ab, a+b+ab\}$.

LEMMA 2.0.2. *Let I be a left ideal of Δ. Then $1+I$ is a subgroup of $(V, \cdot)$.*

PROOF. Pick $1+\alpha,\ 1+\beta \in 1+I,\ \alpha,\ \beta \in I$. Then $\alpha+\beta+\alpha\beta \in I$, so $(1+\alpha)(1+\beta) = 1+\alpha+\beta+\alpha\beta \in 1+I$. Also $\beta \in I \subseteq \Delta$, so by Lemma 1.2.13, there exists an integer t such that $\beta^t = 0$. Thus as shown in the proof of Lemma 1.2.16, $(1+\beta)^{-1} = 1+\beta+\cdots+\beta^{t-1} \in 1+I$. □

LEMMA 2.0.3. *Let α and β be elements of Δ. Let I be a left ideal of Δ. Then α and β are in the same coset of $(I,+)$ if and only if $1+\alpha$ and $1+\beta$ are in the same left coset of the subgroup $(1+I, \cdot)$ of V.*

PROOF. We have α, β in the same coset of $(I,+)$

$$\begin{aligned}&\text{if and only if } \alpha \equiv \beta \mod I\\ &\text{if and only if } \alpha-\beta \in I\\ &\text{if and only if there exists } \gamma \in I \text{ such that } \alpha = \beta+\gamma\end{aligned}$$

and this occurs if and only if $1+\alpha = 1+\beta+\gamma$. Since β is in Δ, Lemma 2.0.2 says $(1+\beta)^{-1}$ exists. Consequently, $1+\alpha = 1+\beta+\gamma = (1+\beta)(1+(1+\beta)^{-1}\gamma)$. Now $1+(1+\beta)^{-1}\gamma \in 1+I$, so $1+\alpha \equiv 1+\beta$ in $(1+I, \cdot)$.

Conversely, $1+\alpha$ and $1+\beta$ are in the same left coset of $(1+I, \cdot)$ if and only if $1+\alpha \equiv 1+\beta \mod 1+I$, which happens if and only if there exists $\gamma \in I$ such that $1+\alpha = (1+\beta)(1+\gamma) = (1+\beta)+(1+\beta)\gamma$, and this occurs if and only if $(1+\alpha)-(1+\beta) = (1+\beta)\gamma$, that is, $\alpha-\beta = (1+\beta)\gamma$. Since I is a left ideal of Δ, $(1+\beta)\gamma \in I$, giving the result. □

2.1. A basis for $V(F_2G)$ when G is abelian

In this section we adapt the results from **[San84b]** to find a basis of $V(F_2G)$ when $G = \langle x_1 \rangle \times \cdots \times \langle x_d \rangle$ is an abelian 2-group. Since $V(F_2G)$ is an abelian 2-group, by the fundamental theorem of abelian groups it is isomorphic to a product of cyclic groups in one and only one way. A set $L = \{g_1, g_2, \ldots, g_t\}$ is a *basis* for $(V(F_2G), \cdot)$ over F_2 if $V(F_2G) \cong \langle g_1 \rangle \times \langle g_2 \rangle \times \cdots \times \langle g_t \rangle$.

Let $\delta = (\delta_1, \ldots, \delta_d)$ be a d-tuple of non-negative integers, not all zero. Let $P(\delta) = \prod (x_j + 1)^{\delta_j}$ where $0 \leq \delta_j < |x_j|$, the order of x_j. Let

$$D(G) = \{\delta \mid 0 \leq \delta_j < |x_j| \text{ and } 2 \nmid \delta_j \text{ for some } j\}.$$

By $1 + P(D)$ we mean $\{1 + P(\delta) \mid \delta \in D(G)\}$.

EXAMPLE 2.1.1. Let $G = C_2 \times C_2 = \langle a \rangle \times \langle b \rangle = \{1, a, b, ab\}$. The elements of $D(G)$ and $1 + P(D)$ are shown in the table.

$\delta \in D(G)$	$1 + P(\delta)$
$(1, 0)$	$1 + (a + 1) = a$
$(0, 1)$	$1 + (1 + b) = b$
$(1, 1)$	$1 + (1 + a)(1 + b) = a + b + ab$

EXAMPLE 2.1.2. Let $G = C_4 = \{1, a, a^2, a^3\}$. Then $D(G) = \{(1), (3)\}$, so $P(D) = \{(1 + a)^1, (1 + a)^3\}$ and $1 + P(D) = \{a, a + a^2 + a^3\}$.

EXAMPLE 2.1.3. Let $G = C_2 \times C_4 = \langle a \rangle \times \langle b \rangle = \{1, a, b, b^2, b^3, ab, ab^2, ab^3\}$. The elements of $D(G)$ and $1 + P(D)$ are shown in the table.

$\delta \in D(G)$	$1 + P(\delta)$
$(1,0)$	a
$(0,1)$	b
$(0,3)$	$b + b^2 + b^3$
$(1,1)$	$a + b + ab$
$(1,2)$	$a + b^2 + ab^2$
$(1,3)$	$b + b^2 + b^3 + a(1 + b + b^2 + b^3)$

THEOREM 2.1.4. **[San89]** *Let m_i denote the number of cyclic factors in $V(F_2G)$ that have order 2^i. Then $m_i = |G^{2^{i-1}}| - 2|G^{2^i}| + |G^{2^{i+1}}|$, the dimension of V is $|G| - |G^2|$ and the order of $1 + P(D)$ is $|G| - |G^2|$.*

EXAMPLE 2.1.5. Let $G = C_2 \times C_2 = \langle a \rangle \times \langle b \rangle = \{a, b, ab, 1\}$. Notice $G^{2^i} = 1$ for all $i \geq 1$. Then $m_1 = |G| - 2|G^2| + |G^4| = 4-2+1 = 3$ and $m_i = |G^{2^{i-1}}| - 2|G^{2^i}| + |G^{2^{i+1}}| = 1 - 2 + 1 = 0$ for all $i \geq 2$. Thus V has precisely 3 cyclic factors of order 2; i.e., $V \cong C_2 \times C_2 \times C_2$.

EXAMPLE 2.1.6. Let $G = C_2 \times C_4 = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}$ with $|a| = 4$, $|b| = 2$. Now $G^2 = \{1, a^2\}$ and $G^{2^i} = 1$ for all $i \geq 2$. Then $m_1 = |G| - 2|G^2| + |G^4| = 8-4+1 = 5$, $m_2 = |G^2| - 2|G^4| + |G^8| = 2 - 2 + 1 = 1$ and $m_i = |G^{2^{i-1}}| - 2|G^{2^i}| + |G^{2^{i+1}}| = 1 - 2 + 1 = 0$ for all $i \geq 3$. Thus V has 5 cyclic factors of order 2 and 1 cyclic factor of order 4; i.e., $V \cong C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_4$.

THEOREM 2.1.7. *Let G be an abelian 2-group and F_2 the field of order 2. Then for $n \geq 0$, $1 + \Delta^{n+1}$ is a subgroup of $V = (1 + \Delta, \cdot)$.*

This follows immediately from Lemma 2.0.2.

THEOREM 2.1.8. *Let $G = \langle x_1 \rangle \times \langle x_2 \rangle \times \cdots \times \langle x_d \rangle$ be an abelian finite 2-group and let F_2 be the field of order 2. For $n \geq 1$, let B_n be a subset of Δ^n whose cosets generate Δ^n/Δ^{n+1}. Let B be the union of the B_n. Then $V(F_2G)$ is generated by $1 + B$.*

PROOF. Consider $f\colon (\Delta^n/\Delta^{n+1}, +) \to (1 + \Delta^n/1 + \Delta^{n+1}, \cdot)$ defined by $f(\alpha + \Delta^{n+1}) = (1+\alpha)(1+\Delta^{n+1})$ with $\alpha \in \Delta^n$. First we show that f is well defined, that is, if $\alpha + \Delta^{n+1} = \beta + \Delta^{n+1}$, then $(1+\alpha)(1+\Delta^{n+1}) = (1+\beta)(1+\Delta^{n+1})$. Thus we want to show that $\alpha - \beta \in \Delta^{n+1}$ implies $(1+\alpha)^{-1}(1+\beta) \in 1 + \Delta^{n+1}$; that is, if α, β are in the same coset of Δ^{n+1}, which is a left ideal of Δ, then $1+\alpha$ and $1+\beta$ are in the same coset of the subgroup $1 + \Delta^{n+1}$ of $(V, \cdot)$. This is Lemma 2.0.3.

To show that f is one-to-one, we show that if $(1+\alpha)(1+\Delta^{n+1}) = (1+\beta)(1+\Delta^{n+1})$, then $\alpha + \Delta^{n+1} = \beta + \Delta^{n+1}$; that is, that $(1+\alpha)^{-1}(1+\beta) \in 1 + \Delta^{n+1}$ implies that $\alpha - \beta \in \Delta^{n+1}$. This is equivalent to showing that if $1+\alpha$ and $1+\beta$ are in the same coset of the subgroup $1 + \Delta^{n+1}$ of $(V, \cdot)$, then α and β are in the same coset of the left ideal Δ^{n+1} of Δ. This is Lemma 2.0.3. Clearly f is onto because $(1+\beta)(1+\Delta^{n+1}) \in 1+\Delta^n/1+\Delta^{n+1}$ with $\beta \in \Delta^n$ and $f(\beta+\Delta^{n+1}) = (1+\beta)(1+\Delta^{n+1})$. Now we want to show that f is operation preserving. Taking, $\alpha + \Delta^{n+1}, \beta + \Delta^{n+1} \in \Delta^n/\Delta^{n+1}$, we have

$$f((\alpha + \Delta^{n+1}) + (\beta + \Delta^{n+1})) = f((\alpha + \beta) + \Delta^{n+1}) = (1 + (\alpha + \beta))(1 + \Delta^{n+1}).$$

We claim that $(1 + (\alpha+\beta))(1+\Delta^{n+1}) = (1 + (\alpha + \beta + \alpha\beta))(1 + \Delta^{n+1})$. To see why, notice that $\alpha + \beta \in \Delta^n \subset \Delta$, since $\alpha, \beta \in \Delta^n$. By Theorem 1.2.13 every element in Δ is nilpotent. So there exists an integer t such that $(\alpha+\beta)^t = 0$. Then $(1 + (\alpha+\beta))(1 + (\alpha+\beta) + (\alpha+\beta)^2 + \cdots + (\alpha+\beta)^{t-1}) = 1$. So $(1+\alpha+\beta)^{-1} =$

$(1+(\alpha+\beta)+(\alpha+\beta)^2+\cdots+(\alpha+\beta)^{t-1}) = 1+\alpha+\beta+X$, where $X \in \Delta^{n+1}$. Then

$$\begin{aligned}(1+\alpha+\beta)^{-1}(1+\alpha+\beta+\alpha\beta) &= 1+(1+\alpha+\beta)^{-1}\underbrace{\alpha\beta}_{\in\Delta^{n+1}} \\ &= 1+(1+\alpha+\beta+X)\alpha\beta \\ &= 1+\underbrace{\alpha\beta+\alpha^2\beta+\beta\alpha\beta+X\alpha\beta}_{\in\Delta^{n+1}}\end{aligned}$$

As a result,

$$\begin{aligned}f((\alpha+\Delta^{n+1})+(\beta+\Delta^{n+1})) &= (1+(\alpha+\beta))(1+\Delta^{n+1}) \\ &= (1+(\alpha+\beta+\alpha\beta))(1+\Delta^{n+1}) \\ &= ((1+\alpha)(1+\beta))(1+\Delta^{n+1}) \\ &= (1+\alpha)(1+\Delta^{n+1})(1+\beta)(1+\Delta^{n+1}) \\ &= f(\alpha+\Delta^{n+1})f(\beta+\Delta^{n+1})\end{aligned}$$

as desired. All this shows that f is an isomorphism, so, indeed, $(1+B_n)(1+\Delta^{n+1})$ generates $1+\Delta^n/1+\Delta^{n+1}$. Now we know from Theorem 1.2.13 that Δ is nilpotent, so there exists a positive integer n such that $\Delta^n = 0$.

As shown above $(1+B_{n-1})(1+\Delta^n)$ generates $1+\Delta^{n-1}/1+\Delta^n$, so $1+B_{n-1}$ generates $1+\Delta^{n-1}/1+\Delta^n = 1+\Delta^{n-1}$. Choose $y = x(1+\Delta^{n-1}) \in 1+\Delta^{n-2}/1+\Delta^{n-1}$. Now $y^{-1}x \in 1+\Delta^{n-1}$ can be expressed as $(1+b_1)^{t_1}(1+b_2)^{t_2}\cdots(1+b_d)^{t_d}$, the b_i's $\in B$ not necessarily distinct and $t_i \in \{0,1\}$. As shown above $(1+B_{n-2})(1+\Delta^{n-1})$ generates $1+\Delta^{n-2}/1+\Delta^{n-1}$, so, $y = ((1+x_1)^{t_1}(1+x_2)^{t_2}\cdots(1+x_s)^{t_s})(1+\Delta^{n-1})$ is the product of elements in $(1+B_{n-2})(1+\Delta^{n-1})$, the x_i's $\in B_{n-2}$ not necessarily distinct. Therefore,

$$\begin{aligned}x &= y(1+b_1)^{t_1}(1+b_2)^{t_2}\cdots(1+b_d)^{t_d}\\ &= ((1+x_1)^{t_1}(1+x_2)^{t_2}\cdots(1+x_s)^{t_s})(1+\Delta^{n-1})(1+b_1)^{t_1}(1+b_2)^{t_2}\cdots(1+b_d)^{t_d}\end{aligned}$$

is in $\langle 1+B\rangle$ because $1+\Delta^{n-1}$ is generated by $1+B$. This process can be continued to show that $1+B$ generates $1+\Delta$. □

Recall that $D(G)$ is the set of those $\delta = (\delta_1, \delta_2, \ldots, \delta_d)$ where for all j, $0 \leq \delta_j < |x_j|$ and 2 does not divide δ_j for some j.

COROLLARY 2.1.9. *V is generated by $1 + P(D)$.*

PROOF. Let $G = \langle x_1\rangle \times \langle x_2\rangle \times \ldots \times \langle x_d\rangle$ and $S = \{x_1, \ldots, x_d\}$. We know from Theorem 1.2.11 that $\Delta = \{\sum \alpha_g(x_i+1) \mid x_i \in S, \alpha_g \in F_2G\}$. So the elements in Δ are linear combinations of elements of the form $h(x_i - 1)$ where $h \in G$. Now

$$\begin{aligned}h(x_i+1) &= h(x_i+1) + (x_i+1) + (x_i+1)\\ &= (h+1)(x_i+1) + (x_i+1)\\ &\equiv x_i + 1 \pmod{\Delta^2},\end{aligned}$$

so $(\Delta/\Delta^2, +)$ is generated over F_2 by $B_1 = \{(x_i+1) \mid x_i \in S\}$. Next, the elements in Δ^2 are linear combinations of elements of the form $h_i(x_i+1)h_j(x_j+1)$, where $h_i, h_j \in G$, $x_i, x_j \in S$ and the coefficients are in F_2. Then,

$$\begin{aligned}h_i(x_i+1)h_j(x_j+1) &= h_ih_j(x_i+1)(x_j+1) && \text{since } G \text{ is abelian}\\ &= h(x_i+1)(x_j+1) && \text{with } h \in G\\ &= (h+1)(x_i+1)(x_j+1) + (x_i+1)(x_j+1)\\ &\equiv (x_i+1)(x_j+1) \pmod{\Delta^3},\end{aligned}$$

so $(\Delta^2/\Delta^3, +)$ is generated over F_2 by $B_2 = \{(x_i+1)(x_j+1) \mid x_i, x_j \in S\}$. In general, elements in Δ^k are linear combinations of elements of the form $h_1(x_1+1)h_2(x_2+1)\cdots h_k(x_k+1)$, $h_i \in G$ and $x_i \in S$, with coefficients in F_2. Hence, $(\Delta^k/\Delta^{k+1}, +)$ is generated over F_2 by $B_k = \{(x_1+1)(x_2+1)\cdots(x_k+1) \mid x_i \in S, 1 \leq i \leq k\}$.

Let B be the union of all B_k's. This is actually the set of all $P(\delta)$'s, where $P(\delta)$ is a product $\prod_{j=1}^{d}(x_j-1)^{\delta_j}$. By Proposition 2.1.8, $1+B = \{1+P(\delta)\}$ generates V. Now we want to show that we may assume $0 \leq \delta_j < |x_j|$. Choose a positive integer $d \geq |x_j|$, then $d = n|x_j| + b$ where $0 \leq b < |x_j|$. Then,

$$(x_j-1)^d = (x_j+1)^{n|x_j|+b} = (x_j+1)^{n|x_j|}(x_j+1)^b = (x_j^{n|x_j|} + 1^{n|x_j|})(x_j+1)^b = 0.$$

Thus, for all $d \geq |x_j|$, $(x_j+1)^d = 0$. So $\{1+P(\delta)\}$ generates V with $0 \leq \delta_j < |x_j|$. Finally we want to show that we may assume that $2 \not| \, \delta_i$ for some i. So assume there is an element in the set $1+P(\delta)$, $0 \leq \delta_i < |x_i|$ where $t \mid \delta_i$ for all i and t is a power of 2. Therefore it is of the form $1+P(t\delta)$ where $\delta \in D$. Now,

$$1+P(t\delta) = \prod(x_i-1)^{t\delta_i} = \prod((x_i+1)^{\delta_i})^t = (1+P(\delta))^t$$

Thus $1+P(D)$ generates $V(F_2G)$. □

EXAMPLE 2.1.10. Let $G = C_4 = \{1, a, a^2, a^3\}$. Then $V = 1+\Delta$ and $V = \{1, a, a^2, a^3, 1+a+a^2, 1+a+a^3, 1+a^2+a^3, a+a^2+a^3\} \cong \langle a\rangle \times \langle 1+a+a^2\rangle \cong C_4 \times C_2$. Since $1+P(D) = \{a, a+a^2+a^3\}$, it is clear that $1+P(D)$ is a basis for V.

THEOREM 2.1.11. *Let $G = \langle x_1\rangle \times \langle x_2\rangle \times \cdots \times \langle x_d\rangle$ be an abelian 2-group and F_2 the field of order 2. Then $1+P(D)$ is a basis for $V(F_2G)$.*

PROOF. By Corollary 2.1.9, $1+P(D)$ generates $V(F_2G)$. By the fundamental theorem of abelian groups $V(F_2G)$ can be expressed as a product of cyclic groups in one and only one way. Therefore, $1+P(D)$ is a basis for $V(F_2G)$ if it has the same number of elements of each order as the invariants of $V(F_2G)$. The proof will proceed by induction on the exponent of G. Recall that the exponent of G is the smallest positive integer m such that $g^m = 1$ for all $g \in G$.

Assume $\exp(G) = 2^1$. Now $|G| = 2^d$. Notice the set $1 + P(D)$ has d elements of the form $1 + x_j$, $\binom{d}{2}$ elements of the form $(1 + x_j)(1 + x_i)$, $\binom{d}{3}$ elements of the form $(1 + x_i)(1 + x_j)(1 + x_k) \cdots$, $\binom{d}{d}$ elements of the form $(1 + x_2)(1 + x_3) \cdots (1 + x_d)$. Thus $|1 + P(D)| = 2^d - 1 = |G| - 1$. Now $1 + P(\delta) \neq 1$ for all δ, and the order of $1 + P(\delta)$ is 2. In fact, $(1 + P(\delta))^2 = 1 + \Pi_{j=1}^{d}(x_j^2 + 1)^{\delta_j} = 1$. Thus $1 + P(D)$ has $|G| - 1$ elements of order 2 and no elements of order 2^i, for all $i > 1$. On the other hand by Remark 2.1.4 $m_1(V) = |G^{2^{1-1}}| - 2|G^{2^1}| + |G^{2^{1+1}}| = |G| - 2 + 1 = |G| - 1$. Thus, $1 + P(D)$ has the same number of elements of each order as the invariants of $V(F_2G)$.

Let G have exponent 2^k and assume that for any H with exponent equal to 2^ℓ where $1 \leq \ell < k$ exactly $m_i(V(H))$ of the elements of $1 + P(D(H))$ are of order 2^i for all i. We want to show that exactly $m_i(V(G))$ of the elements of $1 + P(D(G))$ are of order 2^i, for all i. Now for all $\delta \in D(G)$, $(1 + P(\delta))^2 = 1 + \Pi_{j=1}^{d}(x_j^2 + 1)^{\delta_j}$. As a result,

$$\begin{aligned} 1 + \Pi_{j=1}^{d}(x_j^2 + 1)^{\delta_j} \neq 1 \quad & \text{if and only if} \quad \Pi_{j=1}^{d}(x_j^2 + 1)^{\delta_j} \neq 0 \\ & \text{if and only if} \quad (x_j^2 + 1)^{\delta_j} \neq 0 \text{ for all } j,\ 1 \leq j \leq d \\ & \text{if and only if} \quad 2\delta_j < |x_j| \quad \text{if and only if} \quad \delta_j < \frac{|x_j|}{2}. \end{aligned}$$

If $(1+P(\delta))^2 = 1$ then $|1+P(\delta)| \leq 2$. The only element of order 1 is the identity. The elements of order 2 along with the identity form a subgroup of exponent 2. Then by the base case, $1 + P(D)$ has the same number of elements of order 2 as the invariants of $V(F_2G)$. If the order of an element is > 2 then $(1 + P(\delta))^2 \neq 1$. Thus it is an element of $1 + P(D(G^2))$ where $\exp G^2 < \exp G$. Then by the induction hypothesis for all $i \geq 2$ exactly $m_i(V(G^2))$ of the elements of $1 + P(D(G^2))$ are of order 2^i. The number of elements of order 2^i in $1 + P(D)$ is equal to the number of elements of order $2^{i-1} \in 1 + P(D(G^2))$ which equals $m_{i-1}(V(G^2)) = |(G^2)^{2^{i-1-1}}| - 2|(G^2)^{2^{i-1}}| + |(G^2)^{2^{i+1-1}}| = |G^{2^{i-1}}| - 2|G^{2^i}| + |G^{2^{i+1}}| = m_i(V(G))$. □

EXAMPLE 2.1.12. Let $G = C_2 \times C_2 = \langle a, b \rangle = \{a, b, ab, 1\}$. As shown previously $V = 1+\Delta$, so $V = \{1, a, b, ab, 1+a+b, 1+a+ab, 1+b+ab, a+b+ab\} \cong C_2 \times C_2 \times C_2$, with basis $1 + P(D) = \{a, b, a+b+ab\}$, as shown in Table 1.

TABLE 1. The unit group of $F_2[C_2 \times C_2]$ is $\langle a \rangle \times \langle b \rangle \times \langle a+b+ab \rangle$

Elements of $V(F_2G)$	In terms of $1 + P(D)$
1	$=a^0b^0(a+b+ab)^0$
a	$= a^1 = a$
b	$= b^1 = b$
ab	$= a^1b^1(a+b+ab)^0$
$1+a+b$	$= a^1b^1(a+b+ab)^1$
$1+a+ab$	$= b^1(a+b+ab)^1$
$1+b+ab$	$= a^1(a+b+ab)^1$
$a+b+ab$	$=(a+b+ab)^1$

EXAMPLE 2.1.13. Let $C_2 \times C_4 = \{1, a, b, b^2, ab, ab^2, ab^3\}$. Then $V(F_2(C_2 \times C_4)) \cong C_2 \times C_2 \times C_2 \times C_2 \times C_2 \times C_4$, with generators, respectively, $a, b, b+b^2+b^3, a+b+ab, a+b^2+ab^2, b+b^2+b^3+a(1+b+b^2+b^3)$, the elements of $1 + P(D)$.

REMARK 2.1.14. From Theorem 2.1.11, $1 + P(D(G))$ is a basis for $V(F_2G)$. Notice that when $\sum \delta_j = 1$, $1 + P(\delta) = 1 + \prod(x_j + 1)^{\delta_j} = 1 + (x_j + 1) = x_j \in G$. It follows that G is actually a direct factor of $V(G)$, as noted in the examples we have presented. As we shall see in Section 3.3, this happens for many abelian groups.

2.2. Normal Complements with G' of order 2

In this section, we adapt some results of Sandling [**San89**] to show that G has a normal complement in the unit group of F_2G for a certain class of groups G. Specifically, we assume that G has a unique nonidentity commutator, always denoted s. Note that since s^{-1} is also a commutator, $s^{-1} = s$, so $s^2 = 1$ and $|G'| = 2$. Originally, the hope was to extend the results here to the case of a (not necessarily associative) loop, that is, a system $(L, \cdot)$ where $(a, b) \mapsto a \cdot b$ is a binary operation on L, both cancelation laws hold, and there exists an identity element. For years after Paige showed that a commutative power-associative loop algebra must be associative (in most characteristics) [**Pai55**], the possibility of the existence of nonassociative loop algebras satisfying "interesting" identities was considered unlikely. In the 1980s, however, Goodaire found some nonassociative loops, now called RA loops, whose loop rings in any characteristic are alternative, that is, they satisfy the laws $x(xy) = x^2y$ and $(yx)x = yx^2$ [**Goo83**]. RA loops have many properties. Of relevance here is that they contain a group G of index 2 for which $G' = \{1, s\}$ has order 2. In characteristic 2, even more loops have alternative loop rings. While these RA2 loops have yet to be characterized, those with a unique nonidentity commutator/associator are known to be RA2 [**CG90**]. Eventually, Goodaire and Robinson showed that any Bol loop L with $L' = \{1, s\}$ has a loop ring which, in characteristic 2, satisfies the right alternative law, but not the left [**GR95**]. These remarks explain our focus on characteristic 2 in this thesis and on groups G with a unique nonidentity commutator.

Properties of s.

- $(1+s)(1+s) = 0$ because $(1+s)(1+s) = 1+s+s+s^2 = 1+s+s+1 = 0$
- $\alpha s = s\alpha$ for all $\alpha \in F_2G$.

  To see why, note that it is enough to prove this when $\alpha = g \in G$. In this case we have $gs = sg$ or $gs = s(sg)$. If $gs = s(sg) = s^2g = g$, then $s = 1$ which is a contradiction. Thus $gs = sg$.
- For $\alpha, \beta \in F_2G$, $\alpha\beta + \beta\alpha = (1+s)\gamma$ for some $\gamma \in F_2G$.

  To see this, note that

$$\alpha\beta + \beta\alpha = \sum_{g,h\in G} \alpha_g\beta_h gh + \sum_{g,h\in G} \beta_h\alpha_g hg = \sum_{g,h\in G} \alpha_g\beta_h(gh+hg).$$

  If $gh = hg$ then $gh + hg = 0$. So

$$\begin{aligned}
\sum_{g,h\in G} \alpha_g\beta_h(gh+hg) &= \sum_{gh\neq hg} \alpha_g\beta_h(gh+hg) \\
&= \sum_{gh\neq hg} \alpha_g\beta_h(gh+sgh) \\
&= \sum_{gh\neq hg} \alpha_g\beta_h(1+s)gh \\
&= (1+s)\sum_{gh\neq hg} \alpha_g\beta_h gh = (1+s)\gamma, \text{ with } \gamma \in F_2G.
\end{aligned}$$

Let $J = J(G)$ denote the ideal $(1+s)\Delta$.

Lemma 2.2.1. *The ideal Δ^2/J is central in F_2G/J, so $1 + \Delta^2/(1+J)$ is central in $V/(1+J)$.*

PROOF. Choose $\delta_1, \delta_2 \in \Delta$ and $\alpha \in F_2G$. As shown above, there exists $\gamma_1, \gamma_2 \in F_2G$ such that $\delta_1\alpha + \alpha\delta_1 = (1+s)\gamma_1$ and $\delta_2\alpha + \alpha\delta_2 = (1+s)\gamma_2$. Thus,

$$\begin{aligned}\delta_1\delta_2\alpha &= \delta_1(\alpha\delta_2 + (1+s)\gamma_2)\\ &= \delta_1\alpha\delta_2 + (1+s)\delta_1\gamma_2\\ &= (\alpha\delta_1 + (1+s)\gamma_1)\delta_2 + (1+s)\delta_1\gamma_2\\ &= \alpha\delta_1\delta_2 + (1+s)\gamma_1\delta_2 + (1+s)\delta_1\gamma_2 \equiv \alpha\delta_1\delta_2 \mod J.\end{aligned}$$

The second half of the statement follows from the first and Lemma 2.0.3. □

Let $W = W(G)$ be the subgroup of $V(G)$ generated by $1 + J$ and by the preimages of all $1 + P(\delta)$, $\delta \in D(G/G')$ and $\sum \delta_j > 1$.

EXAMPLE 2.2.2. Let $G = D_4 = \langle a, b \mid a^4 = 1, b^2 = 1, ba = a^{-1}b\rangle$. Then $G' = \{1, a^2 = s\}$ and $\overline{G} = G/G' = \langle \overline{a}, \overline{b}\rangle$, where $|\overline{a}| = |\overline{b}| = 2$. Now Δ is spanned over F_2G by the set $\{a+1, b+1\}$, so $1 + J = 1 + (1+s)\Delta$ is generated by the set $\{1 + (1+s)(a+1) = a + s + sa, 1 + (1+s)(b+1) = b + s + sb\}$. Now if $\delta \in D(\overline{G})$ then $\delta = (\delta_1, \delta_2)$ is a pair with $0 \le \delta_i < 2$ for each i and not both $\delta_1 = 0$ and $\delta_2 = 0$. The only $1 + P(\delta)$ with $\delta \in D(\overline{G})$ where $\sum \delta_i > 1$ is $1 + (\overline{a}+1)(\overline{b}+1) = \overline{a} + \overline{b} + \overline{a}\overline{b}$. So $W(G)$ is generated by the set $\{a + s + sa, b + s + sb, a + b + ab\}$.

COROLLARY 2.2.3. *W is a normal subgroup of V.*

PROOF. Let $w \in W$, $v \in V$. Since $W \subseteq 1 + \Delta^2$ and $1 + \Delta^2/1 + J$ is central in $V/1 + J$ by Lemma 2.2.1, we have $w^{-1}v^{-1}wv \equiv 1 \mod 1 + J \implies w^{-1}v^{-1}wv \in 1 + J \subseteq W$. Now $w \in W$ and W is a subgroup, so $(w)(w^{-1}v^{-1}wv) = v^{-1}wv \in W$, as desired. □

COROLLARY 2.2.4. *If α and β are in Δ and $n \ge 1$ is a positive integer $(\alpha\beta)^n \equiv \alpha^n\beta^n$ modulo J.*

PROOF. The proof will proceed by induction on n. If $n=1$ then, $(\alpha\beta)^1=\alpha\beta=\alpha^1\beta^1$. Assume $n\geq 1$ and $\alpha^n\beta^n=(\alpha\beta)^n \pmod J$. Then,

$$\begin{aligned}(\alpha\beta)^{n+1} &= (\alpha\beta)^n\alpha\beta=\underbrace{\alpha^n\beta^n}_{\in\Delta^2}\alpha\beta && \text{by the induction hypothesis}\\ &\equiv \alpha(\alpha^n\beta^n)\beta \mod J && \text{by Lemma 2.2.1}\\ &= \alpha^{n+1}\beta^{n+1},\end{aligned}$$

so, by the principle of mathematical induction, $\alpha^{n+1}\beta^{n+1}\equiv(\alpha\beta)^{n+1} \mod J$ for all $n>0$. □

LEMMA 2.2.5. *Let $G=\langle x_1\rangle\times\langle x_2\rangle\times\cdots\times\langle x_d\rangle$. Let $\delta=(\delta_1,...,\delta_d)$ be a d-tuple of non-negative integers, not all zero. Suppose that, for all j, $\delta_j<|x_j|$. If $\delta_j\neq 0$, let s_j be the highest power of 2 less than or equal to δ_j. Then the order of the element $1+P(\delta)=1+\prod(x_j+1)^{\delta_j}$ is the minimum of the numbers $\frac{|x_j|}{s_j}$, taken over those j for which $\delta_j\neq 0$.*

PROOF. The proof will proceed by induction on the exponent of G, where $\exp G=2^n$. If $n=1$, then $\exp G=2$. So all nonidentity elements of G are of order 2 and G is elementary abelian. Then $(1+P(\delta))^2=(1+\prod(x_j+1)^{\delta_j})^2=1+\prod(x_j^2+1)^{\delta_j}=1$ (in characteristic 2). Thus $|1+P(\delta)|=2$. On the other hand, $\delta_j<2$ for all j. Thus $s_j=2^0$ and $|x_j|/s_j=2/1=2$ is the minimum of the numbers $|x_j|/s_j$. So the hypothesis is true when $n=1$. Assume $n>1$ and $\exp G=2^n$ and the results are true for groups of smaller exponent. Now for all j, $\frac{|x_j|}{s_j}$ is a power of 2 since both $|x_j|$ and s_j are powers of 2. Then the lowest possible value of $\frac{|x_j|}{s_j}$ is 2, since $\delta_j<|x_j|$ and

s_j is the highest possible power of 2 less than or equal to δ_j. Then,

$$\begin{aligned}(1+P(\delta))^2 = 1 &\text{ if and only if } 1+\Pi_{j=1}^{d}(x_j^2+1)^{\delta_j} = 1\\ &\text{ if and only if } \Pi_{j=1}^{d}(x_j^2+1)^{\delta_j} = 0\\ &\text{ if and only if } (x_j^2+1)^{\delta_j} = 0 \text{ for some } j,\ 1 \le j \le d\end{aligned}$$

and this occurs if and only if $\delta_j \ge \dfrac{|x_j|}{2}$ for some j, $1 \le j \le d$. Thus $\dfrac{|x_j|}{2} \le \delta_j < |x_j|$ for some j. As a result s_j is equal to $\dfrac{|x_j|}{2}$. Therefore, $\dfrac{|x_j|}{s_j} = 2$ when $1+P(\delta))^2 = 1$. If $\delta_j < \dfrac{|x_j|}{2}$ for all j then $(1+P(\delta))^2 = 1+\Pi_{j=1}^{d}(x_j^2+1)^{\delta_j} \ne 1$ and it is an element of $1+P(D(G^2))$. Now $\exp G^2 < \exp G$, so by induction hypothesis $|(1+P(\delta))^2| = \min\{|x_j^2|/s_j\} = \frac{1}{2}\min\{|x_j|/s_j\}$ and $|1+P(\delta)| = \min\{|x_j|/s_j\}$. Therefore by the principle of mathematical induction for all $n \ge 1$ and G with exponent equal to 2^n the order of the element $1+P(\delta) = 1+\prod(x_j+1)^{\delta_j}$ is the minimum of numbers $\dfrac{|x_j|}{s_j}$, taken over those j for which $\delta_j \ne 0$. □

Let $\overline{G} = G/G' = \langle\overline{x_1}\rangle \times \langle\overline{x_2}\rangle \times \cdots \times \langle\overline{x_d}\rangle$. Recall that $1+P(D(\overline{G}))$ is the set of elements of the form $1+P(\delta) = 1+\prod_{j=1}^{d}(\overline{x}_j+1)^{\delta_j}$ with $\delta = (\delta_1,\ldots,\delta_d)$ and $\delta \in D(\overline{G})$ i.e. $0 \le \delta_j < |\overline{x}_j|$ and 2 does not divide δ_j for some j.

Theorem 2.2.6. *$V(F_2\overline{G}) = \overline{W(G)} \times \overline{G}$.*

Proof. From Theorem 2.1.11, $1+P(D(\overline{G}))$ is a basis for $V(F_2\overline{G})$. Notice that when $\sum\delta_j = 1$, $1+P(\delta) = 1+\prod(\overline{x}_j+1)^{\delta_j} = 1+(\overline{x}_j+1) = \overline{x}_j \in \overline{G}$, hence the result. □

Theorem 2.2.7. *$W(G) \cap (1+(1+s)F_2G) = 1+J$.*

PROOF. Choose $\mu \in W(G) \cap (1 + (1+s)F_2G)$. Since $\mu \in W(G)$ and $1 + J$ is a normal subgroup in $V(F_2G)$ we can write $\mu = \sigma(1+j)$, where $j \in J$ and σ is a product of preimages of terms of the form $1 + P(\delta)$ where $\delta \in D(\overline{G})$ and $\sum \delta_i > 1$. Each $P(\delta)$ is in Δ^2, so using Lemma 2.2.1 we can assume that σ is the product of preimages of $(1+P(\delta_1))^{\alpha_1}, (1+P(\delta_2))^{\alpha_2}, \ldots, (1+P(\delta_s))^{\alpha_s}$ for different $P(\delta_i)$. Since $1 + J \subset 1 + (1+s)F_2G$ and $\mu \in 1 + (1+s)F_2G$ it follows that $\sigma = \mu(1+j)^{-1}$ is in $1 + (1+s)F_2G$. Since $(1+s)F_2G$ is in the kernel of the natural epimorphism from F_2G to $F_2(\frac{G}{G'})$ it follows from Theorem 2.1.11 that each α_i can be assumed to be a multiple of $|1 + P(\delta_i)|$ in $V(F_2(\frac{G}{G'}))$. We will complete the proof by showing that the preimage of each $(1+P(\delta_i))^{\alpha_i}$ is in $1 + J$.

First let us assume that a $1 + P(\delta_i)$ term in the above product is of the form $1 + (1+\overline{x})^\theta$ for some θ (i.e. involves only one x). In that case θ is necessarily odd and greater than 1. Lemma 2.2.5 tells us that $\theta|1 + P(\delta)| > |\overline{x}|$. The corresponding term that is actually in the product of σ is $(1 + (1+x)^\theta + r)^{\alpha_i}$ where $r \in (1+s)F_2G$. Since $(1+x)^{|\overline{x}|}$ belongs to $(1+s)F_2G$, this term is clearly in $1 + J$.

If a $1 + P(\delta_i)$ term involves more than one $\overline{x}$ but all x's involved commute, a similar argument to the one just given still works (note that $(1+x_i)^{|\overline{x_i}|}(1+x_j) \in J$ if $i \neq j$).

Finally observe that if f is the preimage of a $1 + P(\delta_i)$ term involving x's which do not commute and g is obtained from f by allowing the x's to commute then $f - g$ is in $(1+s)F_2G$, so f and g are preimages of the same $1 + P(\delta_i)$ term. Hence the difference $f - g$ can be considered as part of the "r" term in the earlier case. In other words, we may assume the x's commute.

We have completed the proof that $\sigma \in 1 + J$. Hence $\mu = \sigma(1+j)$ also belongs to $1 + J$ and we're done. □

LEMMA 2.2.8. $G \cap (1+J) = 1$.

PROOF. Let $g = 1+(s+1)\alpha$ with $\alpha \in \Delta$. Then $(1+s)g = (1+s)(1+(1+s)\alpha) = 1+s$. Hence $sg+g+s+1 = 0$ and $g = s$ or $g = sg$, or $g = 1$. If $g = sg$ then $s = 1$ which is a contradiction. If $g = s$, then $s = 1+(1+s)\alpha$. Thus $(s+1)(1+\alpha) = 0$. Now α is in Δ. So $1+\alpha$ is a unit by Theorem 1.2.16. Thus there exists $\gamma \in F_2G$ such that $(1+\alpha)\gamma = 1 = \gamma(1+\alpha)$. Then $(s+1)(1+\alpha) = 0$ and $(s+1)(1+\alpha)\gamma = 0$. As a result $s+1 = 0$ and $s = 1$ which is a contradiction. So $g = 1$, and $G \cap (1+J) = 1$. □

In the next lemma we follow an argument of de Barros and Policino Milies [**dBM95**].

LEMMA 2.2.9. $1+(1+s)F_2G = G'(1+J)$.

PROOF. Since $J = (1+s)\Delta \subseteq (1+s)F_2G$ and $s = 1+(1+s) \in 1+(1+s)F_2G$, we have one containment. For the other, let $\alpha \in 1+(1+s)F_2G$. Then $\alpha = 1+\sum_{g\in G}\alpha_g g(1+s)$ where $\alpha_g \in F_2$. Now $\alpha_g = 1$ or 0. So we will let the sum of all non-zero coefficients of $\sum_{g\in G}\alpha_g$ equal f. If $f = 2h+1$ is odd,

$$\begin{aligned}
\alpha &= 1+\sum_{g\in G}\alpha_g g(1+s)\\
&= s(s+\sum_{g\in G}\alpha_g g(1+s))\\
&= s(s+\sum_{g\in G}\alpha_g g(1+s)+\underbrace{(1+s)+(1+s)\cdots(1+s)}_{2h \text{ times}}+1+1)\\
&= s(1+\sum_{g\in G}\alpha_g g(1+s)+\underbrace{(1+s)+(1+s)\cdots(1+s))}_{2h+1 \text{ times}}\\
&= s(1+\sum_{g\in G}\alpha_g g(1+s)+\sum_{g\in G}\alpha_g(1+s))
\end{aligned}$$

$$= s(1 + \textstyle\sum_{g\in G} \alpha_g(g+1)(1+s)) \in G'(1+\Delta(1+s)).$$

If f is even, then

$$\begin{aligned}
\alpha &= 1 + \sum_{g\in G} \alpha_g g(1+s) + \underbrace{(1+s) + (1+s) + \cdots + (1+s)}_{f \text{ times}} \\
&= 1 + \sum_{g\in G} \alpha_g g(1+s) + \sum_{g\in G} \alpha_g (1+s) \\
&= 1 + \sum_{g\in G} \alpha_g (g+1)(1+s) \in G'(1+\Delta(1+s)).
\end{aligned}$$

In both cases $\alpha \in G'(1+\Delta(1+s)) = G'(1+J)$. □

THEOREM 2.2.10. $V = G \cdot W(G)$.

PROOF. Extend the mapping $\mu\colon G \longrightarrow G/G'$ to the modular group algebra by $\mu\colon \sum \alpha_g g \longrightarrow \sum \alpha_g \overline{g}$. Then $\ker\mu = \Delta(G, G') = F_2G(1+s)$. By restriction, we obtain a mapping $\mu_0\colon V(F_2G) \to V(F_2\overline{G})$. If $x \in \ker\mu_0$, then $\mu_0(x) = 1$, so $x+1 \in \ker\mu$. Thus $\ker\mu_0 = 1+(1+s)F_2G$. By Theorem 2.2.6, $V(F_2\overline{G}) = \overline{G}\times\overline{W}$. Let $v \in V$. There exist $g \in G$, $w \in W$ such that $\overline{v} = \overline{g}\,\overline{w}$. Thus $v^{-1}gw \in \ker\mu_0$, so $v^{-1}gw = 1+(1+s)\alpha$ for some $\alpha \in F_2G$. Hence, $v = gw(1+(1+s)\alpha)^{-1} = gw(1+(1+s)\alpha) \in GW(1+(1+s)F_2G)$. Therefore $V \subseteq GW(1+(1+s)F_2G) = GWG'(1+J)$ by Lemma 2.2.9. The result follows because $G' \subseteq G$ and $1+J \subseteq W$. □

THEOREM 2.2.11. *The subgroup $W(G)$ is a normal complement to G in $V(F_2G)$.*

PROOF. It remains only to prove that $G \cap W(G) = 1$. Now $\overline{G} \cap \overline{W} = \{1\}$ so $G \cap W \subseteq G' \cap W \subseteq W \cap G'(1+J) = W \cap (1+(1+s)F_2G)$ by Lemma 2.2.9. Using Theorem 2.2.7, $G \cap W \subseteq G \cap (1+J) = \{1\}$ by Lemma 2.2.8. □

CHAPTER 3

The Structure of Some Unit Groups of Small Order

The purpose of this chapter is to exhibit the unit group of various group rings F_2G, for certain groups G of order $|G| \leq 31$. We will do this by first finding the decomposition of the group ring. Our results rely heavily on the Wedderburn Artin Theorem, which states that every semisimple artinian ring is the direct sum of matrix rings over division rings. We also use the Wedderburn Principal Theorem which says that if R is a finite dimensional algebra over a perfect field (for example, a finite field) then R can be written as $R = S + N$ where N is the Jacobson radical of R and $S \cong R/N$ [**Row88**].

3.1. F_2C_n when n is odd

In this section we will look at the unit group of group rings of the form F_2C_n where n is odd. Now $|C_n|$ is invertible in F_2 since $\gcd\{|C_n|, \operatorname{char} F_2\} = 1$, so by Maschke's Theorem F_2C_n is semisimple [**MS02**]. Then by the Wedderburn-Artin theorem F_2C_n is a direct sum of matrix rings over division rings. Since F_2C_n is abelian F_2C_n is actually the direct sum of fields. In particular, $F_2C_n \cong \frac{F_2[x]}{(q_1(x))} \oplus \frac{F_2[x]}{(q_2(x))} \oplus \cdots \oplus \frac{F_2[x]}{(q_s(x))}$, where the decomposition of x^n+1 into irreducible polynomials over $F_2[x]$ is $x^n+1 = q_1(x)q_2(x)\cdots q_s(x)$[**MS02**]. In their book "The Theory of Error-Correcting Codes", MacWilliams and Sloane list the irreducible factors of x^n+1 in $F_2[x]$ for odd $n \leq 63$ [**MS78**]. Some of these we reproduce in Table 1. From these factorizations, we obtain decompositions of the group algebras. Consider, for example, the case $n = 9$. The

TABLE 1. Factorizations of $1 + x^n$ in $F_2[x]$

n	$1 + x^n$
3	$(1+x)(1+x+x^2)$
5	$(1+x)(1+x+x^2+x^3+x^4)$
7	$(1+x)(1+x^2+x^3)(1+x+x^3)$
9	$(1+x)(1+x+x^2)(1+x^3+x^6)$
11	$(1+x)(1+x+x^2+\cdots+x^{10})$
13	$(1+x)(1+x+x^2+\cdots+x^{12})$
15	$(1+x)(1+x+x^2)(1+x^3+x^4)(1+x+x^4)(1+x+x^2+x^3+x^4)$
17	$(1+x)(1+x^3+x^4+x^5+x^8)(1+x+x^2+x^4+x^6+x^7+x^8)$
19	$(1+x)(1+x+x^2+\cdots+x^{18})$
21	$(1+x)(1+x+x^2)(1+x^2+x^3)(1+x+x^3)(1+x+x^4+x^5+x^6)$
21	$(1+x+x^4+x^5+x^6)$
23	$(1+x)(1+x^2+x^4+x^6+x^{10}+x^{11})(1+x+x^5+x^6+x^7+x^9+x^{11})$
25	$(1+x)(1+x+x^2+x^3+x^4)(1+x^5+x^{10}+x^{15}+x^{20})$
27	$(1+x)(1+x+x^2)(1+x^3+x^6)(1+x^9+x^{18})$
29	$(1+x)(1+x+x^2+\cdots+x^{28})$
31	$(1+x)(1+x^3+x^5)(1+x^2+x^5)(1+x^2+x^3+x^4+x^5)$
31	$(1+x+x^3+x^4+x^5)(1+x+x^2+x^4+x^5)(1+x+x^2+x^3+x^5)$

factorization $(1+x)^9 = (1+x)(1+x+x^2)(1+x^3+x^6)$ into the product of irreducible polynomials gives $F_2C_9 \cong F_2 \oplus F_2[x]/(1+x+x^2) \oplus F_2[x]/(1+x^3+x^6)$. Now the set $\{1, x\}$ is a basis for $F_2[x]/(1+x+x^2)$, so this algebra is the unique field $GF(2^2)$ of dimension 2 over F_2 and order $2^2 = 4$. Similarly, the set $\{1, x, x^2, x^3, x^4, x^5\}$ is a basis for $F_2[x]/(1+x^3+x^6)$ which is therefore the unique field $GF(2^6)$ of dimension 6 over F_2 and order $2^6 = 64$. Similarly, we obtain the following decompositions.

$$
\begin{aligned}
F_2C_3 &\cong F_2 \oplus F_2[x]/(1+x+x^2) \\
F_2C_5 &\cong F_2 \oplus F_2[x]/(1+x+x^2+x^3+x^4) \\
F_2C_7 &\cong F_2 \oplus F_2[x]/(1+x^2+x^3) \oplus F_2[x]/(1+x+x^3) \\
F_2C_9 &\cong F_2 \oplus F_2[x]/(1+x+x^2) \oplus F_2[x]/(1+x^3+x^6) \\
F_2C_{11} &\cong F_2 \oplus F_2[x]/(1+x+x^2+\cdots+x^{10}) \\
F_2C_{13} &\cong F_2 \oplus F_2[x]/(1+x+x^2+\cdots+x^{12}) \\
F_2C_{15} &\cong F_2 \oplus F_2[x]/(1+x+x^2) \oplus F_2[x]/(1+x^3+x^4) \\
&\qquad \oplus F_2[x]/(1+x+x^4) \oplus F_2[x]/(1+x+x^2+x^3+x^4) \\
F_2C_{17} &\cong F_2 \oplus F_2[x]/(1+x^3+x^4+x^5+x^8) \oplus \\
&\qquad F_2[x]/(1+x+x^2+x^4+x^6+x^7+x^8) \\
F_2C_{19} &\cong F_2 \oplus F_2[x]/(1+x+x^2+\cdots+x^{18}) \\
F_2C_{21} &\cong F_2 \oplus F_2[x]/(1+x+x^2) \oplus F_2[x]/(1+x^2+x^3) \\
&\qquad \oplus F_2[x]/(1+x+x^3) \oplus F_2[x]/(1+x+x^4+x^5+x^6) \\
&\qquad \oplus F_2[x]/(1+x+x^4+x^5+x^6) \\
F_2C_{23} &\cong F_2 \oplus F_2[x]/(1+x^2+x^4+x^6+x^{10}+x^{11}) \\
&\qquad \oplus F_2[x]/(1+x+x^5+x^6+x^7+x^9+x^{11}) \\
F_2C_{25} &\cong F_2 \oplus F_2[x]/(1+x+x^2+x^3+x^4) \\
&\qquad \oplus F_2[x]/(1+x^5+x^{10}+x^{15}+x^{20}) \\
F_2C_{27} &\cong F_2 \oplus F_2[x]/(1+x+x^2) \oplus F_2[x]/(1+x^3+x^6) \\
&\qquad \oplus F_2[x]/(1+x^9+x^{18}) \\
F_2C_{29} &\cong F_2 \oplus F_2[x]/(1+x+x^2+\cdots+x^{28}) \\
F_2C_{31} &\cong F_2 \oplus F_2[x]/(1+x^3+x^5) \oplus F_2[x]/(1+x^2+x^5) \\
&\qquad \oplus F_2[x]/(1+x^2+x^3+x^4+x^5) \oplus F_2[x]/(1+x+x^3+x^4+x^5) \\
&\qquad \oplus F_2[x]/(1+x+x^2+x^4+x^5) \oplus F_2[x](1+x+x^2+x^3+x^5)
\end{aligned}
$$

From these decompositions, we obtain the structure of the unit groups. See Table 2.

TABLE 2. The structure of $V(F_2C_n)$, $n \leq 31$ odd

n	$V(F_2C_n)$
3	C_3
5	$C_{15} \cong C_3 \times C_5$
7	$C_7 \times C_7$
9	$C_3 \times C_{63} \cong C_3 \times C_7 \times C_9$
11	$C_{2^{10}-1} \cong C_{11} \times C_{93}$
13	$C_{2^{12}-1} \cong C_{13} \times C_{315}$
15	$C_3 \times C_{15} \times C_{15} \times C_{15}$
17	$C_{255} \times C_{255} \cong C_{17} \times C_{15} \times C_{17} \times C_{15}$
19	$C_{2^{18}-1} \cong C_{19} \times C_{13797}$
21	$C_3 \times C_7 \times C_7 \times C_{63} \times C_{63} \cong C_3 \times C_7 \times C_7 \times C_{21} \times C_3 \times C_{21} \times C_3$
23	$C_{2^{11}-1} \times C_{2^{11}-1} \cong C_{23} \times C_{89} \times C_{23} \times C_{89}$
25	$C_{15} \times C_{2^{20}-1} \cong C_{15} \times C_{25} \times C_{41943}$
27	$C_3 \times C_{63} \times C_{2^{18}-1} \cong C_3 \times C_{63} \times C_{27} \times C_{9709}$
29	$C_{2^{28}-1} \cong C_{29} \times C_{9256395}$
31	$C_{31} \times C_{31} \times C_{31} \times C_{31} \times C_{31} \times C_{31}$

For example, from the decomposition of F_2C_9 as the direct sum of fields and using the fact that the multiplicative group of a finite field is cyclic, it is easy to discover that

$$V(F_2C_9)$$
$$\cong V(F_2) \times V(GF(2^2)) \times V(GF(2^6)) \cong 1 \times C_3 \times C_{63} \cong 1 \times C_3 \times C_7 \times C_9.$$

3.2. F_2C_n when $n = 2q$, q odd

When $C_n = \langle a \rangle$ with $n = 2q$, q odd, the element $1 + a^q$ generates a nilpotent ideal. The next theorem gives us the structure of F_2C_n in a special case.

THEOREM 3.2.1. *Let F_2C_n be a group ring, where $n = 2q$, q odd. Then $F_2C_n \cong F_2C_q + N$ where N is a nilpotent ideal generated by $1 + a^q$.*

PROOF. In F_2C_n, $(1 + a^q)^2 = 0$, so the ideal N generated by $1 + a^q$ is nilpotent. It is clear that N is spanned by the set $\{a^j(1 + a^q) \mid 0 \leq j \leq q - 1\}$. In fact, N has basis $\{a^j(1+a^q) \mid 0 \leq j \leq q-1\}$ since $a^{q+j}(1+a^q) = a^{q+j} + a^j = a^j(1+a^q)$ for all j, $0 \leq j < q$ and $\{1, a, \ldots, a^{n-1}\}$ is linearly independent in F_2C_n. Also $\alpha^2 = 0$ for each $\alpha \in N$ since this is true for basis elements and we are in characteristic 2.

Now N has dimension q. Let H be the subgroup generated by a^2, then $|H| = q$ and F_2H has dimension q. We want to show that $F_2C_n \cong F_2H + N$. Since F_2C_n has dimension $2q$ it is sufficient to show that $N \cap F_2H = \{0\}$. Choose $\alpha = \alpha_0 + \alpha_1 a^2 + \alpha_2 a^4 + \cdots + \alpha_{q-1}a^{2(q-1)} \in N \cap F_2H$. Since $\alpha \in N$, $\alpha(1 + a^q) = 0$. But, $\alpha(1 + a^q) = \alpha_0 + \alpha_1 a^2 + \alpha_2 a^4 + \cdots + \alpha_{q-1}a^{2(q-1)} + \alpha_0 a^q + \alpha_1 a^{2+q} + \alpha_2 a^{4+q} + \cdots + \alpha_{q-1}a^{2(q-1)+q}$. The exponents $q, 2+q, 4+q, \ldots, 2(q-1)+q$ are all odd (and remain so modulo n) so they must be distinct from $0, 2, \cdots, 2(q-1)$. Hence, $\alpha_i = 0$ for all i and $\alpha = 0$. Thus, $F_2C_n \cong F_2H + N \cong F_2C_q + N$. □

In the presence of a nonzero nilpotent radical, knowing the structure of F_2G again gives us knowledge of the unit group.

LEMMA 3.2.2. *Let G be a group with $F_2G \cong S+N$ with N nilpotent. Then $V(F_2G) \cong V(S)(1 + N)$.*

PROOF. Let $v \in V(F_2G)$, and write $v = s+n$. Then there exists $s_1+n_1 \in S+N$ such that $(s+n)(s_1+n_1) = 1$. Now

$$(s+n)(s_1+n_1) = ss_1 + \underbrace{sn_1 + ns_1 + nn_1}_{\in N}$$

Thus $ss_1 = 1$ and as a result s, s_1 are both units. Hence, $s+n = s(1+s^{-1}n) \in V(S)(1+N)$. Conversely, choose $v(1+n) \in V(S)(1+N)$. From Lemma 1.2.15, $1+n$ is a unit, so $v(1+n) \in V(F_2G)$. □

Now let $C_n = \langle a \rangle$, $n = 2q$, q odd and let N be the nilpotent ideal generated by $1+a^q$. Using Lemma 3.2.2 together with Theorem 3.2.1, $V(F_2C_n) \cong V(F_2C_q)(1+N)$. We claim that the product is even direct. For this, let $v \in V(F_2C_q) \cap (1+N)$. Then $v = 1+n$ for some $n \in N$. So $1+v = n$ and as a result $(1+v)^2 = n^2 = 0$. Therefore, $1+v \in F_2C_q$ is a nilpotent element in a direct sum of fields. So $1+v = 1$, $v = 0$ and we have our desired result.

Since $1+N$ has exponent 2, $1+N \cong \underbrace{C_2 \times C_2 \times \cdots \times C_2}_{q\text{-times}}$ by the fundamental theorem of abelian groups. Lemma 3.2.2, together with Table 2, leads us to Table 3, which shows the structure of the unit groups under consideration.

3.3. Abelian Group Rings

In this section we will show that any abelian group G of order less than 31 is isomorphic to a direct factor of $V(F_2G)$. In the previous two sections, we proved that C_n is isomorphic to a direct factor in $V(F_2C_n)$ if n is an integer less than 31 and either n is odd or $n = 2q$, where q is odd. In Theorem 2.1.11 and Remark 2.1.14 we showed the same thing for any abelian 2-group G when $F = F_2$, so we only need to consider $C_{12} \cong C_4 \times C_3$, $C_{20} \cong C_4 \times C_5$, $C_{24} \cong C_8 \times C_3$, $C_{28} \cong C_4 \times C_7$, $C_3 \times C_3$, $C_2 \times C_6$, $C_3 \times C_6$, $C_2 \times C_{10}$, $C_2 \times C_{12}$, $C_2 \times C_2 \times C_6$, $C_5 \times C_5$, $C_3 \times C_9$, $C_3 \times C_3 \times C_3$ and

TABLE 3. The structure of $V(F_2C_n)$, $n = 2q \leq 30$, q odd

n	$V(F_2C_n)$
6	$C_3 \times C_2 \times C_2 \times C_2$
10	$C_3 \times C_5 \times \underbrace{C_2 \times \cdots \times C_2}_{5 \text{ copies}}$
14	$C_7 \times C_7 \times \underbrace{C_2 \times \cdots \times C_2}_{7 \text{ copies}}$
18	$C_3 \times C_7 \times C_9 \times \underbrace{C_2 \times \cdots \times C_2}_{9 \text{ copies}}$
22	$C_{11} \times C_{93} \times \underbrace{C_2 \times \cdots \times C_2}_{11 \text{ copies}}$
26	$C_{13} \times C_{315} \times \underbrace{C_2 \times \cdots \times C_2}_{13 \text{ copies}}$
30	$C_3 \times C_{15} \times C_{15} \times C_{15} \times \underbrace{C_2 \times \cdots \times C_2}_{15 \text{ copies}}$

$C_{14} \times C_2$. To do this we will use the following properties of tensor products which can be found, for instance, in [**GJM96**].

$$E \cong F \otimes_F E \tag{3.1}$$

$$(K_1 \oplus K_2) \otimes_F F \cong (K_1 \otimes_F F) \oplus (K_2 \otimes_F F) \tag{3.2}$$

$$E \otimes_F F[x]/(f) \cong E[x]/(f) \text{ where } f \in F[x] \tag{3.3}$$

$$F[G \times H] = FG \otimes_F FH \tag{3.4}$$

Here we understand $F \subsetneq E$ to be a field extension, K_1, K_2 to be modules over F, and G and H to be groups.

EXAMPLE 3.3.1. Now suppose we want the structure of the unit group of F_2G, $G \cong C_3 \times C_3$. We have

$$\begin{aligned}
F_2[C_3 \times C_3] &\cong F_2C_3 \otimes_{F_2} F_2C_3 && \text{by (3.4)} \\
&\cong (F_2 \oplus GF(2^2)) \otimes_{F_2} (F_2 \oplus GF(2^2)) \\
&\cong (F_2 \otimes_{F_2} F_2) \oplus (F_2 \otimes_{F_2} GF(2^2)) \oplus (GF(2^2) \otimes_{F_2} F_2) \\
&\qquad \oplus (GF(2^2) \otimes_{F_2} GF(2^2)) && \text{by (3.2)} \\
&\cong F_2 \oplus GF(2^2) \oplus GF(2^2) \\
&\qquad \oplus (GF(2^2) \otimes_{F_2} F_2[x]/(1+x+x^2)) && \text{by (3.1)} \\
&\cong F_2 \oplus GF(2^2) \oplus GF(2^2) \oplus GF(2^2)[x]/(1+x+x^2) && \text{by (3.3)} \\
&\cong F_2 \oplus GF(2^2) \oplus GF(2^2) \oplus GF(2^2) \oplus GF(2^2)
\end{aligned}$$

because $1 + x + x^2$ is the product of two linear polynomials over $GF(2^2)$. So

$$\begin{aligned}
V(F_2[C_3 \times C_3]) &\cong V(F_2) \times V(GF(2^2)) \times V(GF(2^2)) \times V(GF(2^2)) \times V(GF(2^2)) \\
&\cong 1 \times C_3 \times C_3 \times C_3 \times C_3 \cong C_3 \times C_3 \times C_3 \times C_3.
\end{aligned}$$

Clearly, the original group G is isomorphic to a direct factor of $V(F_2G)$.

We will now generalize this example.

THEOREM 3.3.2. *Let G and H be groups that are direct factors in the unit groups of their group rings over F_2 and assume in each case that the decomposition of these group rings as a sum of fields includes at least one copy of F_2. Then $G \times H$ is a direct factor of $V(F_2[G \times H])$.*

PROOF. By assumption, $F_2G \cong F_2 \oplus \sum E_i$ with the E_i fields and $F_2H \cong F_2 \oplus \sum K_i$ with the K_i fields. Then,

$$\begin{aligned} F_2[G \times H] &\cong F_2G \otimes_{F_2} F_2H \\ &\cong (F_2 \oplus \sum E_i) \otimes_{F_2} (F_2 \oplus \sum K_i) \end{aligned}$$

$$\begin{aligned} &\cong (F_2 \otimes_{F_2} F_2) \oplus (F_2 \otimes_{F_2} \sum K_i) \oplus (\sum E_i \otimes_{F_2} F_2) \oplus (\sum E_i \otimes_{F_2} \sum K_i) \\ &\cong F_2 \oplus \sum K_i \oplus \sum E_i \oplus (\sum E_i \otimes_{F_2} K_j) \text{ by (3.1).} \end{aligned}$$

So,

$$\begin{aligned} V(F_2[G \times H)] &\cong 1 \times V(\sum E_i) \times V(\sum K_i) \times V((\sum E_i \otimes_{F_2} K_j)) \\ &\cong V(F_2G) \times V(F_2H) \times V((\sum E_i \otimes_{F_2} K_j)). \end{aligned}$$

By assumption both G and H are direct factors in their respective unit groups. As a result $G \times H$ is a direct factor in $V(F_2[G \times H])$. □

From Theorem 3.3.2, it follows that $C_5 \times C_5$, $C_3 \times C_9$, $C_3 \times C_3 \times C_3 \cong C_3 \times (C_3 \times C_3)$ are all direct factors in the respective unit groups. The next theorem allows us to extend this list.

THEOREM 3.3.3. *Let G be any group that is isomorphic to a direct factor of $V(F_2G)$ and let n be a power of 2. Then $C_n \times G$ is isomorphic to a direct factor of $V(F_2[C_n \times G])$.*

PROOF. We have $F_2C_n \cong F_2 + N$ with N a nilpotent ideal. Note that $\alpha^n = 0$ for all $\alpha \in N$ and also there exists an $\alpha \in N$ with $\alpha^{n-1} \neq 0$. So $F_2[C_n \times G] \cong (F_2C_n)G \cong$

$(F_2 + N)G \cong F_2G + NG$. It follows that $1 + NG$ is an abelian group of exponent n, hence contains at least one copy of C_n in its representation as the direct product of cyclic groups. By assumption G is isomorphic to a direct factor in $V(F_2G)$. So $C_n \times G$ is isomorphic to a direct factor of $V(F_2[C_n \times G])$. □

COROLLARY 3.3.4. *The groups* $C_{12} \cong C_4 \times C_3$, $C_{20} \cong C_4 \times C_5$, $C_{28} \cong C_4 \times C_7$, $C_2 \times C_6$, $C_2 \times C_{10}$, $C_2 \times C_{12}$, $C_2 \times C_{14}$, $C_2 \times (C_2 \times C_6)$, $C_6 \times C_3 \cong C_2 \times (C_3 \times C_3)$ *and* $C_{24} \cong C_8 \times C_3$ *are all isomorphic to direct factors of their respective unit groups over* F_2.

We have now shown that every abelian group G of order less than 31 is a direct factor in $V(F_2G)$.

3.4. F_2D_n where n is odd

In this section, we examine group rings of the form F_2D_n where n is odd.

THEOREM 3.4.1. *Let* F_2 *be the field of two elements and* $D_n = \langle a, b \mid a^n = 1, b^2 = 1, ba = a^{-1}b\rangle$, *the dihedral group of order* $2n$, n *odd. Let* $e = 1 + a + \cdots + a^{n-1}$. *Then*

$$F_2D_n \cong (F_2e + F_2(1 + b)e) \oplus F_2D_n(1 + e).$$

PROOF. Let $S = \langle a\rangle$ be the subgroup generated by a. Since $|D_n/S| = 2$, S is normal in D_n. Since it is the sum of the elements in a normal subgroup, e is central. Notice that $a^ie = e$ for all $a^i \in S$, so $e^2 = ne = e$. Thus e is a central idempotent in F_2D_n giving $F_2D_n = F_2D_ne \oplus F_2D_n(1 + e)$. Since $a^ie = e$ for all i, we have $a^ibe = a^ieb = eb = be$ for all i making clear that the set $\{e, be\}$ is a basis of F_2D_ne. For any $\alpha \in F_2D_ne$, we have $\alpha = \alpha_0e + \alpha_1be = (\alpha_0 + \alpha_1)e + \alpha_1(1 + b)e$. Thus $F_2D_ne \cong F_2e + F_2(1 + b)e$ giving the result. □

Let $N = F_2(1+b)e$. Since $(1+b)^2 = 0$, this ideal is nilpotent. We claim it is maximal and hence the radical of F_2D_n. In showing this, we make use of the map $\alpha \mapsto \alpha^*$, where for $\alpha = \sum \alpha_g g$ in a group ring, $\alpha^* = \sum \alpha_g g^{-1}$. It is easy to see that $\alpha \mapsto \alpha^*$ is an involution, that is an antiautomorphism of order 2.

LEMMA 3.4.2. *Let F_2 be the field of two elements and D_n the dihedral group of order $2n$, n odd, presented as in Theorem 3.4.1. Then F_2D_n/N is semisimple.*

PROOF. Let J be an ideal in F_2D_n such that $J^2 \subseteq N$ and let $x \in J$. We can write $x = \alpha + \beta b$ where $\alpha, \beta \in F_2\langle a\rangle$. It is easy to see that $b\beta = \beta^* b$ and $b\alpha = \alpha^* b$, so $x^2 = \alpha^2 + \beta\beta^* + (\beta\alpha^* + \alpha\beta)b$ is an element of $N = F_2(1+b)e$. Thus $\alpha^2 + \beta\beta^* = k_1 \in F_2e$. Now J is an ideal, so $ax = a\alpha + a\beta b \in J$ and

$$(ax)^2 = a^2\alpha^2 + a^2\alpha\beta b + a\beta a^{-1}\alpha^* b + a\beta a^{-1}\beta^* = a^2\alpha^2 + \beta\beta^* + (a^2\alpha\beta + \beta\alpha^*)b \in N.$$

So $a^2\alpha^2 + \beta\beta^* = k_2 \in F_2e$. Hence, $\alpha^2 + a^2\alpha^2 = k_1 + k_2 = 0$ or e. Now $\alpha^2 + a^2\alpha^2 = \alpha^2(1+a^2)$ has even augmentation while $e = 1 + a + \cdots + a^{n-1}$ has augmentation n which is odd. Thus $\alpha^2 + a^2\alpha^2 = 0 = (\alpha(1+a))^2 = 0$ in F_2C_n, which is a direct sum of fields. So $\alpha(1+a) = 0$ giving $\alpha = \alpha a$. Writing $\alpha = \sum_{i=1}^n \alpha_i a^i$, $\alpha_i \in F_2$, we have $\alpha a = \sum_{i=1}^n \alpha_i a^i a = \sum_{i=1}^n \alpha_i a^{i+1}$, so $\alpha_k = \alpha_{k+1}$ for every k, $1 \le k \le n$. Therefore, $\alpha = k_3 e$, where $k_3 \in F_2$. Now $xb = \beta + \alpha b \in J$ and an argument similar to the above shows $\beta = k_4 e$, with $k_4 \in F_2$. Thus $x = k_3 e + k_4 eb$. If $k_3 \neq k_4$ then either $x = e$ or $x = eb$, a contradiction in either case because $x \in J$, a nilpotent ideal. Thus $k_3 = k_4$ and $x = k_3(1+b)e \in N$. All this shows that F_2D_n/N has no nontrivial nilpotent ideals, so N is the radical of F_2D_n and F_2D_n/N is semisimple, as claimed. $\square$

LEMMA 3.4.3. *Let F_2, D_n and e be as above. Then $\{a^i(1+e), a^ib(1+e) \mid 0 \le i \le n-2\}$ is a basis for $F_2D_n(1+e)$.*

PROOF. As shown in the proof of Lemma 3.4.1 F_2D_ne has dimension 2. Thus $F_2D_n(1+e)$ has dimension $2n-2$. Clearly, $\{1+e, a(1+e), a^2(1+e), \ldots, a^{n-1}(1+e), b(1+e), ab(1+e), \ldots, a^{n-1}b(1+e)\}$ spans $F_2D_n(1+e)$. Notice that $(1+e)+a(1+e)+\cdots+a^{n-1}(1+e) = (1+a+\cdots+a^{n-1})(1+e) = e(1+e) = 0$. Thus $a^{n-1}(1+e) = (1+e)+a(1+e)+\cdots+a^{n-2}(1+e)$. By a similar argument, $a^{n-1}b(1+e) = b(1+e)+ab(1+e)+\cdots+a^{n-2}b(1+e)$, so the set $\{1-e, a(1+e), a^2(1+e), \ldots, a^{n-2}(1+e), b(1+e), ab(1+e), \ldots, a^{n-2}b(1+e)\}$ spans $F_2D_n(1+e)$ and it has dimension $2n-2$. $\square$

Now we will describe the conjugacy classes in D_n, for odd n. Elements in D_n are either of the form a^i or a^ib where $0 \leq i \leq n-1$. Since $a^ja^ia^{-j} = a^ja^{-j}a^i = a^i$ and $(a^jb)a^i(a^jb)^{-1} = a^jba^iba^{-j} = a^ja^{-i}a^{-j} = a^{-i}$, the conjugacy class of a^i is $\{a^i, a^{-i}\}$. Since $a^jb(a^j)^{-1} = a^ja^jb = a^{2j}b$ and $(a^jb)b(a^jb)^{-1} = a^jbbba^{-j} = a^jba^{-j} = a^{2j}b$ and n is odd, the conjugacy class of b is $\{b, ab, a^2b, \ldots, a^{n-1}b\}$.

Recall that any class sum, that is, the sum of all the elements in a conjugacy class, is central in F_2G. The class sums actually form a basis for the centre of F_2G. So, for example, $\gamma+\gamma^*$ is central for any $\gamma \in F_2\langle a\rangle$. We use $Z(A)$ to denote the centre of an algebra A.

LEMMA 3.4.4. *For any $\alpha, \beta \in F_2D_n$, $(\alpha\beta+\beta\alpha)^2 \in Z(F_2D_n)$.*

PROOF. Choose $\alpha = \alpha_1+\alpha_2b$ and $\beta = \beta_1+\beta_2b \in F_2D_n$ where $\alpha_1, \alpha_2, \beta_1, \beta_2 \in F_2\langle a\rangle$. Then $b\alpha = \alpha^*b$ and $b\beta = \beta^*b$, so $\alpha\beta = \alpha_1\beta_1+\alpha_1\beta_2b+\alpha_2\beta_1^*b+\alpha_2\beta_2^*$ and $\beta\alpha = \beta_1\alpha_1+\beta_1\alpha_2b+\beta_2\alpha_1^*b+\beta_2\alpha_2^*$.

Thus,

$$\begin{aligned}\alpha\beta+\beta\alpha &= (\alpha_1\beta_2+\alpha_2\beta_1^*+\beta_1\alpha_2+\beta_2\alpha_1^*)b+\beta_2\alpha_2^*+\alpha_2\beta_2^* \\ &= (\alpha_1\beta_2+\alpha_2\beta_1^*+\beta_1\alpha_2+\beta_2\alpha_1^*)b+\beta_2\alpha_2^*+(\beta_2\alpha_2^*)^*.\end{aligned}$$

Now $\zeta = \beta_2\alpha_2^* + (\beta_2\alpha_2^*)^*$ is central, so we have

$$\begin{aligned}(\alpha\beta+\beta\alpha)^2 &= ((\alpha_1\beta_2+\alpha_2\beta_1^*+\beta_1\alpha_2+\beta_2\alpha_1^*)b+\zeta)^2\\ &= \zeta^2 + ((\alpha_1\beta_2+\alpha_2\beta_1^*+\beta_1\alpha_2+\beta_2\alpha_1^*)b)^2.\end{aligned}$$

Thus, to show that this is in the centre, it suffices to show that for any $\gamma \in F_2\langle a\rangle$, $(\gamma b)^2 = \gamma\gamma^*$ is central. To show this it is sufficient to show that $\gamma\gamma^*$ commutes with both a and b. Clearly, $\gamma\gamma^*$ commutes with a. But also $\gamma\gamma^* b = \gamma b\gamma = b\gamma^*\gamma = b\gamma\gamma^*$. Thus, $\gamma\gamma^*$ is central. □

Now note that every 2×2 matrix with trace 0 squares to a multiple of the identity matrix and $XY - YX$ has trace zero for any square matrices X and Y. Thus, if X, Y are 2×2 matrices then $(XY - YX)^2$ is a multiple of the identity and hence central. Conversely, if $(XY - YX)^2$ is central in $M_r(K)$ for all $X, Y \in M_r(K)$ (where $\mathrm{char}(K) = 2$) then $r \leq 2$. To see why, it's sufficient to show $(XY - YX)^2$ is not necessarily central when $r = 3$. For this, take $X = \begin{bmatrix}1&1&0\\0&1&1\\1&0&0\end{bmatrix}$ and $Y = \begin{bmatrix}0&1&0\\1&0&1\\0&0&1\end{bmatrix}$. Then $(XY - YX)^2 = \begin{bmatrix}1&0&0\\0&1&0\\0&1&0\end{bmatrix} \neq kI$.

COROLLARY 3.4.5. *F_2D_n/N is the direct sum of fields and 2×2 matrix rings over fields.*

PROOF. By Corollary 3.4.2 F_2D_n/N is semisimple. By the Wedderburn-Artin theorem, F_2D_n/N is the direct sum of matrices over division rings which are necessarily fields because they are finite. By Lemma 3.4.4 $(\alpha\beta + \beta\alpha)^2$ is central in F_2D_n for all $\alpha, \beta \in F_2D_n$. By the above, this means F_2D_n/N is the direct sum of $r \times r$ matrix rings, where $r \leq 2$. □

Consider the group ring F_2D_5. From Theorem 3.4.1, we know $F_2D_5 = F_2D_5e \oplus F_2D_5(1+e) = (F_2e + F_2(1+b)e) \oplus F_2D_5(1+e)$ where $e = 1 + a + a^2 + a^3 + a^4$. From

Corollary 3.4.2 $F_2D_5(1+e)$ is semisimple. The conjugacy classes of D_5 are 1, $\{a, a^4\}$, $\{a^2, a^3\}$, $\{b, ab, a^2b, a^3b, a^4b\}$. So the class sums 1, $a+a^4$, a^2+a^3, $(1+a+a^2+a^3+a^4)b = be$ form a basis for the centre of F_2D_5 which has, therefore, dimension 4. Now $Z(F_2D_5) = Z(F_2e+F_2(1+b)e) \oplus Z(F_2D_5(1+e)) = (F_2e+F_2(1+b)e) \oplus Z(F_2D_5(1+e))$. Thus $Z(F_2D_5(1+e))$ has dimension 2. The set $\{f_0 = 1+e, f_1 = (a^2+a^3)(1+e)\}$ is a basis for the centre of $F_2D_5(1+e)$ since the centre is spanned by $1+e$, $(a+a^4)(1+e)$, $(a^2+a^3)(1+e)$ and $be(1+e) = 0$ and $(a+a^4)(1+e) = (1+a^2+a^3)(1+e)$. Let $f = \alpha_0 f_0 + \alpha_1 f_1$. Then $f^2 = \alpha_0^2 f_0^2 + \alpha_1^2 f_1^2 = \alpha_0 f_0 + \alpha_1(f_0 + f_1)$. Therefore f is an idempotent if and only if $\alpha_0 = \alpha_0 + \alpha_1$. So the only central idempotents are $1+e$ and 0, giving that $F_2D_5(1+e)$ is simple. By Corollary 3.4.5 (and since $F_2D_5(1+e)$ is not commutative) $F_2D_5(1+e) \cong M_2(K)$, K a field. Since $\dim F_2D_5(1+e) = 8$, $K = GF(2^2)$. So we get $F_2D_5 \cong (F_2e + F_2(1+b)e) \oplus M_2[GF(2^2)]$ and hence

$$V(F_2D_5) \cong V(F_2 + F_2(1+b)e) \times GL(2,4) \cong C_2 \times GL(2,4).$$

Note that $|GL(2,4)| = (4^2-1)(4^2-4) = 180$, so $|V(F_2D_5)| = 360$. Similar calculations give the unit groups for F_2D_n, $n \leq 15$ odd, shown below.

D_n	$V(F_2D_n)$
D_3	$C_2 \times S_3$
D_5	$C_2 \times GL(2,4)$
D_7	$C_2 \times GL(2,8)$
D_9	$C_2 \times GL(2,2) \times GL(2,8)$
D_{11}	$C_2 \times GL(2,32)$
D_{13}	$C_2 \times GL(2,64)$
D_{15}	$C_2 \times GL(2,4) \times GL(2,128)$

We would still like to determine whether any of D_5, D_7, D_9,D_{11},D_{13},D_{15} have a normal complement in their unit groups.

THEOREM 3.4.6. *If $F_2D_n \cong (F_2 \oplus F_2(1+b)e) \oplus M_2[K]$, where $K = GF(q)$, $q > 3$, then D_n does not have a normal complement in $V(F_2D_n)$.*

PROOF. The given information says that $|D_n| = 2 + 4q$ and $V(F_2D_n) \cong C_2 \times GL(2,q)$. Assume that $V(F_2D_n) \cong N \rtimes D_n$. Let $S = \{1\} \times SL(2,q)$ where $SL(2,q)$ denotes the (normal) subgroup of $GL(2,q)$ consisting of matrices with determinant 1. Since $S \cap N \trianglelefteq S$ and S is simple for $q > 3$ [**Row88**, p. 167], $S \cap N = \{1\}$ or S. If $S \cap N = S$, then $S \subseteq N$. Then

$$D_n \cong \frac{C_2 \times GL(2,q)}{N} \cong \frac{\frac{C_2 \times GL(2,q)}{S}}{\frac{N}{S}} \cong \frac{C_2 \times K^*}{\frac{N}{S}},$$

where $K^* = K \setminus \{0\}$. Since $C_2 \times K^*$ is an abelian group, $\frac{C_2 \times K*}{\frac{N}{S}} \cong D_n$ is abelian, a contradiction. Therefore $S \cap N = \{1\}$ and so $|NS| = \frac{|N||S|}{|S \cap N|} = |N||S| > |N \rtimes D_n|$ because $|S| = q(q^2-1) > 4q + 2 = |D_n|$ for $q > 3$. This contradiction gives the result. $\square$

The theorem shows that none of $G = D_5$, D_7,D_{11}, or D_{13} has a normal complement in its unit group. In fact, neither does D_9 or D_{15}. In the case of D_9, for example, we have $F_2D_9 \cong (F_2 + N) \oplus M_2(F_2) \oplus M_2[GF(2^3)]$ so $V(F_2D_9) \cong C_2 \times S_3 \times GL(2,8)$. A proof similar to the one given for Theorem 3.4.6 can be used to give the result.

3.5. F_2D_n where n is even

In this section we will look at the unit group of group rings of the form F_2D_n where n is even. Consider first the case that $n = 2k$ with k odd. Recall from Section 3.4 that the conjugacy class of a^k is $\{a^k, a^{-k}\} = \{a^k\}$. Thus $1 + a^k$ is a central element in F_2D_n which generates a nilpotent ideal N spanned by $(1+a^k)$, $a(1+a^k)$, $a^2(1+a^k)$,..., $a^{k-1}(1+a^k)$, $b(1+a^k)$, $ab(1+a^k)$, $a^2b(1+a^k)$, ..., $a^{k-1}b(1+a^k)$. These elements are linearly independent so they constitute a basis for N.

THEOREM 3.5.1. *Let D_n be the dihedral group of order $2n$, where $n = 2k$ and k is odd. Let N be the nilpotent ideal of F_2D_n generated by $1 + a^k$. Then,*

$$V(F_2D_n) \cong V(F_2D_k)(1 + N).$$

[Note that the groups $V(F_2D_k)$ were determined in Section 3.4.]

PROOF. Now N has dimension $2k = n$ and F_2D_n has dimension $2n$, so F_2D_n/N has dimension $2n - n = n$. Writing $\overline{x} = x + N$,

$$\{\overline{1}, \overline{a}, \dots, \overline{a^{k-1}}, \overline{b}, \overline{ab}, \dots \overline{a^{k-1}b}\} \cong D_k$$

spans F_2D_n/N and contains $2k = n$ elements, so it's a basis for F_2D_n/N. As a result $F_2D_n/N \cong F_2D_k$ and $F_2D_n \cong F_2D_k + N$, so, by Lemma 3.2.2, $V(F_2D_n) \cong V(F_2D_k)(1 + N)$. □

In this chapter, we have been concerned with groups of order $n \leq 31$ and, to this point, we have found the structure of $V(F_2D_n)$ with n odd and $n = 2k$, k odd. Since D_4 and D_{16} have unique commutators, the structure of $V(F_2D_4)$ and $V(F_2D_{16})$ was considered in Chapter 2. This leaves D_8 and D_{12} for investigation.

EXAMPLE 3.5.2. In F_2D_8, the nilpotent ideal N generated by $1 + a^2$ is spanned by the set $\{1 + a^2, a(1 + a^2), \dots, a^5(1 + a^2), b(1 + a^2), ab(1 + a^2), \dots, a^5b(1 + a^2)\}$ and it is straightforward to show that this is linearly independent. The quotient F_2D_8/N has basis $\{\overline{1}, \overline{a}, \overline{b}, \overline{ab}\} \cong C_2 \times C_2$. Therefore, $F_2D_8 \cong N + F_2(C_2 \times C_2)$ and $V(F_2D_8) \cong (1 + N)(V(F_2(C_2 \times C_2)) \cong (1 + N)(C_2 \times C_2 \times C_2)$.

EXAMPLE 3.5.3. In F_2D_{12}, the nilpotent ideal N generated by $1 + a^3$ has basis

$$\{1 + a^3, a(1 + a^3), \dots, a^8(1 + a^3), \dots, b(1 + a^3), ab(1 + a^3), \dots, a^8b(1 + a^3)\},$$

so F_2D_{12}/N has basis $\{\overline{1}, \overline{a}, \overline{a^2}, \overline{b}, \overline{ab}, \overline{a^2b}\} \cong S_3$. Hence, $F_2D_{12} \cong N + F_2S_3$ and $V(F_2D_{12}) \cong (1+N)(C_2 \times S_3)$.

CHAPTER 4

Summary

In this thesis we examined the unit group $V(F_2G)$ for many different groups G of order $|G| \leq 31$. The intention was to determine if G had a normal complement in the unit group $V(F_2G)$ or not. To do this, we found a semisimple algebra S and a nilpotent ideal N with $F_2G = S \oplus N$, as in the Wedderburn Principal Theorem. We show the structures with G cyclic or dihedral below. Here N_i is a nilpotent ideal of dimension i.

$$F_2C_2 \cong F_2 + N_1, \qquad N_1 = \Delta$$

$$F_2C_3 \cong F_2 \oplus F_2[x]/(1 + x + x^2)$$

$$F_2C_4 \cong F_2 + N_3, \qquad N_3 = \Delta$$

$$F_2C_5 \cong F_2 \oplus F_2[x]/(1 + x + x^2 + x^3 + x^4)$$

$$F_2C_6 \cong F_2C_3 + N_3$$

$$F_2D_3 \cong F_2 \oplus M_2[F_2] + N_1$$

$$F_2C_7 \cong F_2 \oplus F_2[x]/(1 + x^2 + x^3) \oplus F_2[x]/(1 + x + x^3)$$

$$F_2C_8 \cong F_2 + N_7, \qquad N_7 = \Delta$$

$$F_2C_9 \cong F_2 \oplus F_2[x]/(1 + x + x^2) \oplus F_2[x]/(1 + x^3 + x^6)$$

$$F_2C_{10} \cong F_2C_5 + N_5$$

$$F_2D_5 \cong F_2 \oplus M_2[GF(2^2)] + N_1$$

$$F_2C_{11} \cong F_2 \oplus F_2[x]/(1 + x + x^2 + \cdots + x^{10})$$

$$F_2C_{12} \cong F_2C_3 + N_9$$

$$F_2D_6 \cong F_2 \oplus M_2[F_2] + N_7$$

$$F_2C_{13} \cong F_2 \oplus F_2[x]/(1 + x + x^2 + \cdots + x^{12})$$

$$F_2C_{14} \cong F_2C_7 + N_7$$

$$F_2D_7 \cong F_2 \oplus M_2[GF(2^3)] + N_1$$

$$\begin{aligned} F_2C_{15} \cong{} & F_2 \oplus F_2[x]/(1 + x + x^2) \oplus F_2[x]/(1 + x^3 + x^4) \\ & \oplus F_2[x]/(1 + x + x^4) \oplus F_2[x]/(1 + x + x^2 + x^3 + x^4) \end{aligned}$$

$$F_2C_{16} \cong F_2 + N_{15}, \qquad N_{15} = \Delta$$

$$F_2D_8 \cong F_2 + N_{15}, \qquad N_{15} = \Delta$$

$$\begin{aligned} F_2C_{17} \cong{} & F_2 \oplus F_2[x]/(1 + x^3 + x^4 + x^5 + x^8) \oplus \\ & F_2[x]/(1 + x + x^2 + x^4 + x^6 + x^7 + x^8) \end{aligned}$$

$$F_2C_{18} \cong F_2C_9 + N_9$$

$$F_2D_9 \cong F_2 \oplus M_2[GF(2^3)] + N_1$$

$$F_2C_{19} \cong F_2 \oplus F_2[x]/(1 + x + x^2 + \cdots + x^{18})$$

$$F_2C_{20} \cong F_2C_5 + N_{15}$$

$$F_2D_{10} \cong F_2 \oplus M_2[GF(2^2)] + N_{11}$$

$$\begin{aligned} F_2C_{21} \cong{} & F_2 \oplus F_2[x]/(1 + x + x^2) \oplus F_2[x]/(1 + x^2 + x^3) \oplus F_2[x]/(1 + x + x^3) \\ & \oplus F_2[x]/(1 + x + x^4 + x^5 + x^6) \oplus F_2[x]/(1 + x + x^4 + x^5 + x^6) \end{aligned}$$

$$F_2C_{22} \cong F_2C_{11} + N_{11}$$

$$F_2D_{11} \cong F_2 \oplus M_2[GF(2^5)] + N_1$$

$$
\begin{aligned}
F_2C_{23} &\cong F_2 \oplus F_2[x]/(1+x^2+x^4+x^6+x^{10}+x^{11}) \\
&\qquad \oplus F_2[x]/(1+x+x^5+x^6+x^7+x^9+x^{11}) \\
F_2C_{24} &\cong F_2C_3 + N_{21} \\
F_2D_{12} &\cong F_2 \oplus M_2[F_2] + N_{19} \\
F_2C_{25} &\cong F_2 \oplus F_2[x]/(1+x+x^2+x^3+x^4) \\
&\qquad \oplus F_2[x]/(1+x^5+x^{10}+x^{15}+x^{20}) \\
F_2C_{26} &\cong F_2C_{13} + N \\
F_2D_{13} &\cong F_2 \oplus M_2[F_2] \oplus M_2[GF(2^6)] + N_1 \\
F_2C_{27} &\cong F_2 \oplus F_2[x]/(1+x+x^2) \oplus F_2[x]/(1+x^3+x^6) \\
&\qquad \oplus F_2[x]/(1+x^9+x^{18}) \\
F_2C_{28} &\cong F_2C_7 + N_{21} \\
F_2D_{14} &\cong F_2 \oplus M_2[GF(2^3)] + N_{15} \\
F_2C_{29} &\cong F_2 \oplus F_2[x]/(1+x+x^2+\cdots+x^{28}) \\
F_2C_{30} &\cong F_2C_{15} + N_{15} \\
F_2D_{15} &\cong F_2 \oplus M_2[GF(2^2)] \oplus M_2[GF(2^7)] + N_1 \\
F_2C_{31} &\cong F_2 \oplus F_2[x]/(1+x^3+x^5) \oplus F_2[x]/(1+x^2+x^5) \\
&\qquad \oplus F_2[x]/(1+x^2+x^3+x^4+x^5) \oplus F_2[x]/(1+x+x^3+x^4+x^5) \\
&\qquad \oplus F_2[x]/(1+x+x^2+x^4+x^5) \oplus F_2[x](1+x+x^2+x^3+x^5)
\end{aligned}
$$

We were able to prove that every abelian group G of order less than 31 is isomorphic to a direct factor of $V(F_2G)$. This is not the case over the field $GF(3)$. For example, consider the group ring KC_4, $K = GF(3)$. The order of C_4 is invertible in K so by Maschke's Theorem KC_3 is semisimple and commutative **[MS02]** hence the direct sum of fields. In fact, $KC_4 \cong K/(1+x^4) \cong K/2(1+x) + K/(2+x) + K/(x^2+1)$, so $V(KC_3) \cong C_2 \times C_2 \times C_8$. Clearly C_4 is not a direct factor.

We showed that $D_3 = S_3$ has a normal complement in its unit group but that D_n does not in the cases $n = 5, 7, 9, 11, 13$. The two nonabelian groups of order 8, D_4 and the quaternions, are both 2-groups with order two commutator subgroups, so they have normal complements as we showed in Section 2.2. All this implies that D_5 is the smallest group that is not a direct factor of its unit group.

We had hoped to extend our results to all groups of "small order" and even to certain classes of loops, but this is work for another day.

Bibliography

[CG90] Orin Chein and Edgar G. Goodaire, *Code loops are RA2 loops*, J. Algebra **130** (1990), no. 2, 385–387.

[Chr04] Borge Inger Christin, *A cohomological approach to the modular isomorphism problem*, Journal of Pure and Applied Algebra **189** (2004), 7–25.

[CSW81] G. H. Cliff, S. K. Sehgal, and A. R. Weiss, *Units of integral group rings of metabelian groups*, Journal of Algebra **73** (1981), 167–183.

[dBM95] Luiz G. X. de Barros and César Policino Milies, *Modular loop algebras of RA loops*, Journal of Algebra **175** (1995), 1027–1040.

[Des56] W. E. Deskins, *Finite abelian groups with isomorphic group algebras*, Duke Mathematical Journal **23** (1956), 35–40.

[GJM96] E. G. Goodaire, E. Jespers, and C. Polcino Milies, *Alternative loop rings*, Elsevier, Netherlands, 1996.

[Goo83] Edgar G. Goodaire, *Alternative loop rings*, Publ. Math. Debrecen **30** (1983), 31–38.

[GR95] Edgar G. Goodaire and D. A. Robinson, *A class of loops with right alternative loop rings*, Comm. Algebra **22** (1995), no. 14, 5623–5634.

[HS06] Martin Hertweck and Marcos Soriano, *On the modular isomorphism problem: groups of order* 2^6, Contemp. Math **420** (2006), 141–161.

[Joh78] D. L. Johnston, *The modular group-ring of a finite p-group*, Proceedings of American Mathematical Society **68** (1978), 19–22.

[Mil82] C. Policino Milies, *Units of group rings: A short survey*, London Math Soc. Lecture Notes **71** (1982), 281–297.

[MS78] F. J. Macwilliams and N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland Publishing, New York, 1978.

[MS02] César Polcino Milies and Sudarshan K. Sehgal, *An introduction to group rings: A survey*, Kluwer Academic Publishers, Netherlands, 2002.

[Pai55] Lowell J. Paige, *A theorem on commutative power associative loop algebras*, Proc. Amer. Math. Soc. **6** (1955), 279–280.

[Pas65] D. S. Passman, *The group algebras of groups of order p^4 over a modular field*, Michigan Math. J. **12** (1965), 405–415.

[PS72] I. B. S. Passi and S. K. Sehgal, *Isomorphism of modular group algebras*, Math.Z. **129** (1972), 65–73.

[PS81] D. S. Passman and P. F. Smith, *Units in integral group rings*, Journal of Algebra **69** (1981), 213–239.

[Row88] Louis Rowen, *Ring theory volume I*, Academic Press, Inc, San Diego, 1988.

[San84a] R. Sandling, *The isomorphism problem for group rings: a survey*, Lecture Notes in Math., vol. 1142, Springer, Berlin, 1984.

[San84b] Robert Sandling, *Units in the modular group algebra of a finite abelian p-group*, Journal of Pure and Applied Algebra **33** (1984), 337–346.

[San89] R. Sandling, *The modular group algebra of a central-elementary-by-abelian p-group*, Archiv der Mathematik **52** (1989), 22–27.

[San96] Robert Sandling, *The modular group algebra problem for metacyclic p-groups*, Proceedings of the American Mathematical Society **124** (1996), 1347–1350.

[Seh90] Sudarshan Sehgal, *Units of integral group rings a survey*, Algebraic structures and number theory: proceeding of first international symposium, Hong Kong, August 8-13, 1988, vol. 1, World Sci. Publishing, Berlin, 1990.

[Seh93] S. K. Sehgal, *Units in integral group rings : A survey*, Longman Group UK limited, New York, 1993.

[SS96] Mohamed A. M Salim and Robert Sandling, *The modular group algebra problem for groups of order p^5*, J. Austral. Math. Soc. (Series A) **16** (1996), 229–237.

[Wur93] Martin Wursthorn, *Isomorphisms of modular group algebras: An algorithm and its application to groups of order 2^6*, J. Symbolic Computation **15** (1993), 211–227.