Units of Truncated Group Rings of Higman Groups

by

Brian C. Rich

A Dissertation
Submitted to the University at Albany, State University of New York
in Partial Fulfillment of
the Requirements for the Degree of
Doctor of Philosophy

College of Arts and Sciences
Department of Mathematics and Statistics

2020

Abstract

In this thesis an analogue of the triviality of units of group rings of finite abelian groups is proved for truncated group rings. A Higman group is a group of exponent 2, 3, 4 or 6. The truncated group ring $\mathbb{Z}G_t$ is the quotient of the group ring by the ideal generated by the formal sum of all group elements. We show that in the case of finite abelian G that $\mathbb{Z}G_t$ has only trivial units; i.e, that any unit in $\mathbb{Z}G_t$ is an image under the quotient map of a unit of the form $\pm g$, where $g \in G$, if (and only if) G is a Higman group. We additionally show several results that follow from this pertaining to Swan subgroups.

Acknowledgements

I am extremely grateful to Professor Anupam Srivastav, my advisor, whose enthusiasm, support, and above all wisdom and expertise were indispensable in helping me organize my path. Srivastav was always available, even in the midst of the pandemic, which as of this writing is still a huge issue in these turbulent times.

I am also very grateful to Professor Marco Varisco, without whom I would have probably never overcome the last of my more procrastinating tendencies in time, and who never failed to motivate me to complete this labor. He has also been instrumental in guiding me as to where to go in the near future.

I am extremely thankful to Professor Emeritus Karl Zimmermann from Union college, who having overseen my undergraduate work, continued to encourage me and keep in touch even years after I had graduated from Union. I am happy and grateful that he was able to see me through to the end, and I strongly intend to keep in touch with him on future developments.

I am also extremely thankful to the rest of the Department of Mathematics at SUNY Albany, both for the financial support which allowed this all to be possible, and for the encouragement, knowledge, and advice I learned along the way. In particular I wish to thank Professors Antun Milas and Boris Goldfarb for their work on my thesis committee, and to Joan Mainwaring and JoAnna Aveyard for their work both with me and in keeping the department organized and functional.

I would also like to thank my colleagues, current and former, in the graduate department, including James Sidoli, J.P. LeBlanc, and Daniel Wood. They have all been great colleagues and great friends, and I am grateful for that.

I would also like to thank my parents, Dr. Steven Rich and Dr. Sandra Eckhert. Since March, I have stayed with them during these difficult times, something which I am forever grateful for; nonetheless, both of them (particularly my mother) still managed to encourage me in ways that I sorely needed.

Finally, I wish most of all to thank the late Professor Mark Steinberger, who during my first several at the university was perhaps the professor I admired most of all, and who in turn consoled me in some of my most stressful moments. Without him being there, I would never have reached this point.

Contents

Abstract ii

Acknowledgements iii

Chapter 1. Introduction and Preliminary Definitions 1

Chapter 2. Trivial Units of Group Rings over the Integers 7

Chapter 3. Application to Swan Subgroups 13

Chapter 4. Trivial Units of Group Rings over Integer Rings of Quadratic Imaginary Fields 19

Chapter 5. Trivial Units of Truncated Group Rings 24

Appendix: Sage Code 44

Bibliography 49

CHAPTER 1

Introduction and Preliminary Definitions

We begin by discussing some basic definitions and establishing notations used in the paper. We then discuss some relevant background material which motivated the question which this paper answers, particularly the Hilbert-Speiser theorem and its converse. We then discuss the main theorem under consideration (Theorem 9) and discuss the general method by which we prove it. Finally, we discuss the definitions, results, and other essential machinery used to discuss Swan subgroups.

NOTATION 1. The following notational conventions will be used:

- G — a finite abelian group
- C_n — a cyclic group of order n
- K — a number field
- $\mathcal{O}_K$ — ring of integers of K
- R — either $\mathbb{Z}$ or $\mathcal{O}_K$
- KG — the group algebra of G over K
- $\mathcal{O}_{KG}$, $\mathscr{M}(KG)$ — the maximal order in KG
- $S^{\times}$— unit group of a ring S
- $\mathcal{O}_K G$ — group ring
- θ — an algebraic number
- ζ, ξ — roots of unity
  - ζ and ζ_α will be primitive roots of unity
- $\operatorname{rank}(H)$ — rank of an abelian group H

DEFINITION 2. Given a commutative ring R and a finite group G, we define the *group ring* or *group algebra* as the set of all formal sums

$$\left\{\sum_{g\in G} \alpha[g]\, g : g \in G, \alpha[g] \in R\right\}$$

with addition defined by

$$\sum_{g\in G}\alpha\left[g\right]g+\sum_{g\in G}\beta\left[g\right]g=\sum_{g\in G}\left(\alpha\left[g\right]+\beta\left[g\right]\right)g$$

and multiplication defined by linear extension of multiplication on the group.

NOTATION 3. Given $\alpha \in RG$, we refer to $\alpha\left[g\right]$ as the coefficient of g in α.

DEFINITION 4. A group ring RG is said to have *only trivial units* if the only units in RG are of the form ug for $g \in G$ and u a unit in R.

DEFINITION 5. Given a group ring RG, we define the truncated group ring RG_t as the quotient ring of RG by the ideal $R\Sigma G$ generated by $\Sigma G = \sum_{g\in G} G$.

DEFINITION 6. An *idempotent* e in an algebra A is a non-zero element such that $e^2 = e$. A *primitive idempotent* e in an algebra A is an element such that e is the only idempotent element in eAe.

LEMMA 7. **[Higman, Wedderburn]** *The following hold:*

(1) If G is finite, then $\mathbb{Q}(\theta)G$ is semisimple.

(2) Commutative simple algebras over $\mathbb{Q}\left(\theta\right)$ are isomorphic to algebraic extensions of $\mathbb{Q}\left(\theta\right)$.

(3) For any $\mathbb{Q}\left(\theta\right)G$, there exists an extension $\mathbb{Q}\left(\theta,\zeta\right)$ of $\mathbb{Q}\left(\theta\right)$ such that

$$\mathbb{Q}\left(\theta\right)G=\bigoplus_{i=1}^{|G|}\mathbb{Q}(\theta,\zeta)\eta_i$$

with $\mathbb{Q}(\theta,\zeta)\eta_i$ simple for each η_i and each η_i a primitive idempotent. In other words,

$$\eta_i\eta_j=\begin{cases}0 & i\neq j\\ \eta_i & i=j\end{cases}$$

and $\sum\eta_i = 1$.

DEFINITION 8. We define a *Higman group* as any finite abelian group with exponent 2, 3, 4, or 6. (Note that this is a different from the other, well-known use of the term “Higman group”, which refers to a class of infinite groups.)

In the subsequent chapter, we discuss a proof given by Higman of a result which states, in the terminology we have used, that

> *given a finite abelian group G, $\mathbb{Z}G$ has only trivial units if and only if G is a Higman group.*

The main theorem proven in this thesis, on the other hand, concerns *truncated* group rings:

THEOREM 9. *Let G be a finite abelian group. Then $\mathbb{Z}G_t$ has only trivial units if and only if G is a Higman group.*

Our general approach to this relies on two theorems. The first is the aforementioned result of [**Higman**] regarding $\mathbb{Z}G$, the proof of which is discussed in Chapter 2, and the other is a result in [**Herm-Li-Par**] and [**Herm-Li**] regarding group rings of the form RG where R is the ring of integers of a quadratic field, which is discussed in Chapter 4.

In Chapter 5, we prove Theorem 9 via induction. For each of $n = 2, 3, 4$, we first prove certain base cases explicitly via calculations in the maximal order. These base cases are C_2, C_3 and C_4, which are relatively easy, as well as $C_2 \times C_2$, $C_3 \times C_3$, and $C_4 \times C_4$. For some of these latter results, we employ SageMath, an open-source computer algebra application, to do the heavy lifting of calculation. We then go to the inductive step: if G is a Higman group of exponent dividing n and $G' = G \times C_n$, then if $\mathbb{Z}G_t$ and $\mathbb{Z}(\zeta)\, G$ have only trivial units (where ζ is a primitive root of order n) then so does $\mathbb{Z}G'_t$. This last calculation involves relatively straightforward (though tedious) calculations in group algebras.

The following preliminary material is relevant for corollaries to the main theorem which are discussed in Chapter 3. Let K be a number field, G a finite group, and L/K a Galois extension with Galois group isomorphic to G.

DEFINITION 10. L/K is said to have *trivial Galois module structure* if $\mathcal{O}_L$ is a free $\mathcal{O}_K G$ module — i.e., if there exists an α in $\mathcal{O}_L$ such that $\{g(\alpha) : g \in G\}$ forms a basis — called a *normal integral basis* — over $\mathcal{O}_K$.

DEFINITION 11. L/K is said to be *tame* if for every prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ the ramification index is relatively prime to the characteristic of the residue field $\mathcal{O}_K/\mathfrak{p}$. It is well know that L/K is tame if and only if there exists an element of $\mathcal{O}_L$ with trace 1.

Definition 12. A number field K is called a *Hilbert-Speiser field* if each finite tame abelian extension has trivial Galois module structure.

Theorem 13 (Hilbert-Speiser Theorem). *The field $K = \mathbb{Q}$ is a Hilbert-Speiser field.*

In [**GRRS**], the converse to this theorem is proved:

Theorem 14 (Converse to the Hilbert-Speiser Theorem). *Let K be a number field. Then K is a Hilbert Speiser field if and only if $K = \mathbb{Q}$.*

Remark. The converse of the Hilbert-Speiser theorem was proved by showing the existence of non-trivial realizable Swan classes (i.e, elements of the intersection of the set of realizable classes and the Swan subgroup) for cyclic groups of prime order for some prime numbers.

Definition 15. An RG-module M is *locally free* if $M_{\mathfrak{p}}$ is a free $R_{\mathfrak{p}}G$-module for every prime ideal $\mathfrak{p}$ of R.

Theorem 16. *Let L be a finite Galois extension of K and let $G \cong \mathrm{Gal}\,(L/K)$. Then L/K is tame if and only if O_L is a locally free $O_K G$ module.*

Let $K_0(RG)$ be the Grothendieck group of all finitely generated locally free RG-modules modulo $[P] + [N] = [M]$ whenever there is a short exact sequence

$$0 \to P \to M \to N \to 0$$

Definition 17. Let $\Psi : K_0(RG) \to \mathbb{Z}$ be the map that assigns each element its rank r. The *class group* $\mathrm{Cl}\,(RG)$ is the kernel of Ψ; i.e., the members of $K_0(RG)$ corresponding to modules of zero rank. Similarly, the class group $\mathrm{Cl}\,(\mathfrak{M})$ is defined as the kernel of the map assigning each element of $K_0\,(\mathfrak{M})$ its rank r.

Definition 18. Let $[\mathcal{O}_L]$ be the class determined by the locally free $O_K G$ module $\mathcal{O}_L$ in $\mathrm{Cl}\,(O_K G)$. Let $\mathfrak{R}\,(O_K G)$ — the *realizable classes* of $\mathcal{O}_K G$ — denote the set of classes in in $\mathrm{Cl}\,(O_K G)$ that can be realized as Galois module classes of rings of integers $\mathcal{O}_L$ in tame Galois extensions L/K with $G \cong \mathrm{Gal}\,(L/K)$.

Definition 19. The *kernel group* of $O_K G$ is the kernel of the map $\mathrm{Cl}\,(O_K G) \to \mathrm{Cl}\,(\mathfrak{M})$. It is denoted by $D\,(O_K G)$.

Definition 20. Let $r \in R$ satisfy $(r,n)=1$. Let $\sigma = \Sigma G = \sum_{g\in G} g$. Then we define a *Swan module* $\langle r,\sigma\rangle = RGr + RG\sigma = RGr + R\Sigma G$.

Theorem 21. *Swan modules are locally-free RG-modules of rank* 1.

Definition 22. The *Swan subgroup*, denoted $T(RG)$, is the subset of $D(RG)$ comprised by all classes of Swan modules. It is a subgroup of $K_0(RG)$.

Theorem 23 (Milnor's Theorem). *Let $A, A_1, A_2, \bar{A}$ be any rings and suppose we have a fiber product of ring homomorphisms*

$$\begin{array}{ccc} A & \xrightarrow{f_1} & A_1 \\ \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle g_1} \\ A_2 & \xrightarrow{g_2} & \bar{A} \end{array}$$

where g_1, g_2 are surjective. Then there is an exact Mayer-Vietoris sequence

$$K_1 A \xrightarrow{(f_1,f_2)} K_1(A_1)\times K_1(A_2) \xrightarrow{g_1\times(1/g_2)} K_1\left(\bar{A}\right)$$
$$\xrightarrow{\delta} K_0(A) \xrightarrow{(f_1,f_2)} K_0(A_1)\oplus K_0(A_2) \xrightarrow{g_1-g_2} K_0\left(\bar{A}\right)$$

We have the following fiber product diagram

$$\begin{array}{ccccc} RG & \longrightarrow & RG/(\sigma) & = & \Gamma \\ \downarrow{\scriptstyle \varepsilon} & & \downarrow{\scriptstyle \bar{\varepsilon}} & & \\ R & \xrightarrow{\pi} & R/nR & = & \bar{R} \end{array}$$

where $\bar{\varepsilon}$ is induced by the augmentation map $\varepsilon\left(\sum_{g\in G} r_g G\right) = \sum r_g$ and Γ is the truncated group ring $RG/R\Sigma G$.

This gives rise to the exact sequence

$$RG^{\times} \to \Gamma^{\times}\times R^{\times} \xrightarrow{h} \bar{R}^{\times} \xrightarrow{\delta} Cl(RG) \to Cl(\Gamma)\oplus Cl(R) \to 0 \tag{1.0.1}$$

from which the following corollary is derived.

Corollary 24.

$$T(RG) = \operatorname{Im}\delta \cong \bar{R}^{\times}/\operatorname{Ker}\delta \cong \frac{\bar{R}}{h\left(\Gamma^{\times} \times R^{\times}\right)}$$

Remark 25. From Milnor's theorem, we can see that $h : \Gamma^{\times} \times R^{\times} \to \bar{R}^{\times}$ is given by $[u, v] \to \bar{u}\bar{v}^{-1}$.

CHAPTER 2

Trivial Units of Group Rings over the Integers

THEOREM 26. [**Higman**] *Let G be a finite abelian group. Then the group ring $\mathbb{Z}G$ has only trivial units if and only if it is a Higman group. That is to say, $\mathbb{Z}G$ has only trivial units if and only if either*

(1) $G = C_2^n$;

(2) $G = C_3^m \times C_2^n$;

(3) $G = C_4^m \times C_2^n$.

To prove this, we will prove a series of lemmas, summarized from [**Higman**]. However, we first need to discuss some character theory, which will be relevant to the thesis as a whole.

Since G is abelian, we have $|G|$ irreducible representations of G up to isomorphism, each into a space of dimension 1. Let $X = \left\{\Gamma_1, \cdots, \Gamma_{|G|}\right\}$ be the set of these representations, and let $\chi_g^i = \Gamma_i(g)$. If m is the exponent of G, then for all $g \in G$, χ_g^i is an mth root of unity. Note that Γ_i in each case is a representation of dimension 1, so we can treat the image of each Γ_i as a field. If we do have that the character and the representation are the same thing, and we can apply character theory directly to the pursuit of our goal! In what follows, we therefore write χ_g^i for $\Gamma_i(g)$ exclusively.

REMARK 27 (Orthogonality relations).

- $\sum_{g\in G} \chi_g^i \overline{\chi_g^j} = [G:1]\delta_{ij}$. As a consequence,

$$\sum_{g\in G} \chi_g^i \overline{\chi_g^j} = \delta_{ij}|G|$$

- $\sum_{\Gamma_k\in X} |C(g)|\, \chi_g^k \overline{\chi_h^k} = [G:1]\delta_{gh}$. Now since $C(g) = \{g\}$ since G is abelian, we have that this becomes

$$\sum_{\Gamma_k\in X} \chi_g^k \overline{\chi_h^k} = |G|\,\delta_{gh}$$

Lemma 28. **[Higman]** *Let*

$$\eta_i = \frac{1}{|G|} \sum_{g \in G} \chi_g^i g$$

Then $\mathbb{Q}(\theta, \zeta) G \cong \oplus_{i=0}^{|G|-1} \mathbb{Q}(\theta, \zeta) \eta_i$.

Proof. Let $g \in G$. Now, since G is a group, for any $h \in G$, $g = g'h$ for some $g' \in G$. Since χ^i is a representation, we have that $\chi_g^i = \chi_{g'}^i \chi_h^i$. Thus,

$$\begin{aligned}
\eta_i &= \frac{1}{|G|} \sum_{g \in G} \chi_g^i g \\
&= \frac{1}{|G|} \sum_{g' \in G} \chi_{g'}^i \chi_h^i g' h \\
&= \chi_h^i \left(\frac{1}{|G|} \sum_{g' \in G} \chi_{g'}^i g' \right) h \\
&= \chi_h^i \eta_i h
\end{aligned}$$

Multiplying by χ_h^j, we have

$$\chi_h^j \overline{\chi_h^i} \eta_i = \chi_h^j \eta_i h$$

Summing over $h \in G$ gives

$$\sum_{h \in G} \chi_h^j \overline{\chi_h^i} \eta_i = \sum_{h \in G} \chi_h^j \eta_i h$$

or

$$\begin{aligned}
\delta_{ij} |G| \eta_i &= \sum_{h \in G} \chi_h^j h \eta_i \\
&= |G| \eta_i \eta_j
\end{aligned}$$

or

$$\begin{aligned}
\eta_i \eta_j &= \delta_{ij} \eta_i \\
&= \begin{cases} \eta_i & i = j \\ 0 & i \neq j \end{cases}
\end{aligned}$$

$\square$

Since the η_i form a basis for $\mathbb{Q}(\theta,\zeta)G$, if $z \in \mathbb{Q}(\theta,\zeta)G$, then

$$z = \sum_{\Gamma^i \in X} b_i \eta_i$$

We will write b_i as $z[\eta_i]$ in the sequel.

LEMMA 29. We have $\mathbb{Q}(\theta)G \cong \bigoplus_{i=0}^{p-1} \mathbb{Q}(\theta,\xi_\alpha)$ where ξ_α has order

$$h = \operatorname{lcm}(\{\operatorname{ord}(\chi_\alpha(g)) : g \in G\}) \, Swansubgroup$$

and p is the number of non-conjugate (in $\mathbb{Q}(\theta)$) representations of G.

PROOF. Let $\sigma \in \operatorname{Gal}(\mathbb{Q}(\theta,\zeta) : \mathbb{Q}(\theta))$. Let $\Gamma^i \in X$ be one of the aforementioned representations. Then $\sigma \circ \Gamma^i : \mathbb{Q}(\theta,\zeta)G \to \mathbb{Q}(\theta,\zeta)$ is a homomorphism, and thus $\sigma \circ \Gamma^i =: \Gamma^{\sigma(i)} \in X$. We say $\Gamma^{\sigma(i)}$ is conjugate to Γ^i. Let ξ_i be a root of unity of order $h = \operatorname{lcm}(\{\operatorname{ord}(\chi_\alpha(g)) : g \in G\})$. Then $\mathbb{Q}(\theta,\xi_i)$ is the smallest extension of $\mathbb{Q}(\theta)$ in which Γ^i exists, in the sense that $\operatorname{im}(\Gamma^i) \subseteq \mathbb{Q}(\theta,\xi_i)$. Since h is the maximum order of any element in G, we have, by the fundamental theorem of finite abelian groups, that $G \cong \mathbb{Z}_h \times G'$. If we set Γ^i to be the representation mapping the generator of G to ζ, and all elements of G' to 1, then we have that ξ_i is a primitive root.

From this it follows that the maximal order of $\mathbb{Q}(\theta)G$ is isomorphic to the maximal order of $\bigoplus_{i=0}^{p-1} \mathbb{Q}(\theta,\xi_\alpha)$

Let U_k denote the subgroup of all $\sigma \in \operatorname{Gal}(\mathbb{Q}(\theta,\zeta) : \mathbb{Q}(\theta))$ such that $\Gamma^{\sigma(k)} = \Gamma^k$. We have that $\sigma \in U_k$ if and only if $\sigma(\chi_g^k) = \chi_g^k$ for all $g \in G$. By the fundamental theorem of Galois theory, we have that the fixed field of U_k is $\mathbb{Q}(\theta,\xi_k)$. $\square$

Recall that

$$z[\eta_i] = \sum_{\Gamma^i \in X} z[g] \, \overline{\chi}_g^i$$

Then $E \in \mathbb{Q}(\theta)G$ iff $\sigma(E[\eta_i]) = E[\eta_{\sigma(i)}]$ for every $\Gamma^i \in X$ and every $\sigma \in \operatorname{Gal}(\mathbb{Q}(\theta,\zeta) : \mathbb{Q}(\theta))$. Thus, we can choose some subset $X' \subseteq X$ consisting of non-conjugate representations Γ^i. If our previous condition is met, then $E[\eta_k] \in \mathbb{Q}(\theta,\xi_k)$ for all $\Gamma^k \in X'$. Furthermore, for a given set of values $\{b_k \in \mathbb{Q}(\theta,\xi_k) : \Gamma^k \in X'\}$, there is a unique $E \in \mathbb{Q}(\theta)G$ such that $E[\eta_k] = b_k$ and $\sigma(E[\eta_i]) = E[\eta_{\sigma(i)}]$ for every $\Gamma^i \in X$ and every $\sigma \in \operatorname{Gal}(\mathbb{Q}(\theta,\zeta) : \mathbb{Q}(\theta))$.

LEMMA 30. $\mathcal{O}^{\times}_{\mathbb{Q}(\zeta)G} \cong \prod_{i=0}^{p-1} \mathcal{O}\left(\mathbb{Q}\left(\zeta_i\right)\right)^{\times}$.

PROOF. We note that there is a $1-1$ correspondence between elements of $\mathbb{Q}\left(\theta\right)$ and sequences of values of $z\left[\eta_i\right]$ for $\Gamma^i \in X'$, a set of p non-conjugate representations. Furthermore, multiplication and addition are preserved.

Define $\Phi : \mathbb{Q}\left(\theta\right) G \cong \bigoplus_{i=0}^{p-1} \mathcal{O}\left(\mathbb{Q}(\theta, \xi_\alpha)\right)$ by mapping

$$E \mapsto \left(E\left[\eta_i\right] \in \mathcal{O}\left(\mathbb{Q}\left(\theta, \xi_k\right)\right) : \Gamma^k \in X'\right)$$

Since the η_i are basis elements, we have that this is an isomorphism of rings. Indeed, if F is any other member of $\mathbb{Q}\left(\theta\right) G$, then since $\eta_i \eta_i \eta_j = \delta_{ij}\eta_i$,

$$\begin{aligned} \Phi\left(EF\right) &= \left(E\left[\eta_i\right] F\left[\eta_i\right] \in \mathcal{O}\left(\mathbb{Q}\left(\theta, \xi_k\right)\right) : \Gamma^k \in X'\right) \\ \Phi\left(E+F\right) &= \left(E\left[\eta_i\right] + F\left[\eta_i\right] \in \mathcal{O}\left(\mathbb{Q}\left(\theta, \xi_k\right)\right) : \Gamma^k \in X'\right) \end{aligned}$$

□

LEMMA 31. *A unit of finite order in $\mathcal{O}_{\mathbb{Q}(\zeta)}G$ is trivial.*

PROOF. Let $x \in \left(\mathcal{O}_{\mathbb{Q}(\theta)}G\right)^{\times}$ be of finite order. Then

$$x\left[\eta_i\right]^m = 1$$

for all $\Gamma^i \in X$. Then $x\left[\eta_i\right]$ is a complex number with absolute value 1, and so is χ^i_g for any $g \in G$. Since x is a unit, we can choose $g \in G$ such that $x[g] \neq 0$. Then

$$\begin{aligned} |x[g]| &= \left| \frac{1}{|G|} \sum_{\Gamma^i \in X} \left(x\left[\eta_g\right]\right) \chi^i_g \right| \\ &\leq \frac{1}{|G|} \sum_{\Gamma^i \in X} \left|\left(x\left[\eta_g\right]\right) \chi^i_g\right| \\ &= 1 \end{aligned}$$

Similarly, each conjugate of $x[g]$ satisfies this relation for $x[g]$ as well. But the product of these conjugates is the norm of $x[g]$, a non-zero integer, so $|x[g]| = 1$ and the above becomes an equality. Thus,

$$x[g] = \left(x\left[\eta_i\right]\right) \chi^i_g, \forall \Gamma^i \in X$$

$$x[\eta_i] = (x\,[h])\,\overline{\chi}_h^i, \forall \Gamma^i \in X$$

□

LEMMA 32. *There exists an n such that for all $u \in \mathcal{O}_{\mathbb{Q}(\zeta)G}^{\times}$, $u^n \in \left(\mathcal{O}_{\mathbb{Q}(\zeta)}G\right)^{\times}$.*

PROOF. Choose n to be the number of residue classes modulo $|G|$ in $\mathbb{Q}(\theta, \zeta)$ relatively prime to $|G|$. Let x be a unit in the integer ring of $\mathbb{Q}(\theta)\,G$. Then $x[\eta_i]$ is a unit in $\mathbb{Q}(\theta, \zeta)$ for all $\Gamma^i \in \mathbb{Q}(\theta, \zeta)$ and is therefore relatively prime to G. Then $x\,[\eta_i]^n \equiv 1 \pmod{|G|}$, so $x\,[\eta_i]^n\,1 = c_i|G|$ for some $c_i \in \mathcal{O}\left(\mathbb{Q}(\theta, \zeta)\right)$. Then $x^n = 1 + \sum_{\Gamma^i \in X} c_i|G|\eta_i$. The coefficients in $|G|\eta_i$ are algebraic integers, so therefore the coefficients in x^n are as well, so $x^n \in \mathcal{O}_{\mathbb{Q}(\theta)}G$. □

LEMMA 33. *$\mathcal{O}_{\mathbb{Q}(\zeta)G}^{\times}$ and $\left(\mathcal{O}_{\mathbb{Q}(\zeta)}G\right)^{\times}$ have the same rank as abelian groups.*

PROOF. Let $x \in \mathcal{O}_{\mathbb{Q}(\theta)G}^{\times}$. Then $x^{-n} = \left(x^{-1}\right)^n \in \mathcal{O}_{\mathbb{Q}(\theta)}G$. Then x^n is a unit in $\mathcal{O}_{\mathbb{Q}(\theta)}G$. Since the set of nth powers of a given independent set of units is itself an independent set of units, we have that $\operatorname{rank}\left(\left(\mathcal{O}_{\mathbb{Q}(\theta)}G\right)^{\times}\right) \geq \operatorname{rank}\left(\mathcal{O}_{\mathbb{Q}(\theta)G}^{\times}\right)$.

But $\operatorname{rank}\left(\left(\mathcal{O}_{\mathbb{Q}(\theta)}G\right)^{\times}\right) \leq \operatorname{rank}\left(\mathcal{O}_{\mathbb{Q}(\theta)G}^{\times}\right)$ since $\left(\mathcal{O}_{\mathbb{Q}(\theta)}G\right)^{\times} \subseteq \mathcal{O}_{\mathbb{Q}(\theta)G}^{\times}$, so we have that the ranks are equal. □

Theorem 26 then follows from the preceding lemmas via the following reasoning: Using Lemma 33 and setting $\theta = 1$, we have that $\operatorname{rank}\left((\mathbb{Z}G)^{\times}\right) = 0$ if and only if $\operatorname{rank}\left(\mathbb{Q}(\zeta)^{\times}\right) = 0$.

Dirichlet's Unit Theorem states that if K is a number field then $\operatorname{rank}\left(\mathcal{O}_K^{\times}\right) = r_1 + r_2 - 1$, r_1 being the number or real embeddings of K, r_2 the number of complex embeddings. Thus, we have that if ζ is of order h,

$$\operatorname{rank}\left(\mathbb{Q}(\zeta)^{\times}\right) = r_1 + r_2 - 1$$

where

$$r_1 = \begin{cases} 1 & h \text{ odd} \\ 2 & h \text{ even} \end{cases}$$

and

$$r_2 = \begin{cases} \frac{h-1}{2} & h \text{ odd} \\ \\ \frac{h}{2} - 1 & h \text{ even} \end{cases}$$

The rank equals zero when $h = 2, 3, 4, 6$. These are in fact the only such h. For $r_1 + 2r_2 = \phi(h)$ since this is the number of embeddings of the field; therefore, $r_1 + r_2 - 1 = 0$ implies $r_1 + r_2 = 1$. Then either $r_2 = 0$ or $r_1 = 0$. If $r_2 = 0$ then we have $r_1 = 1$ so $\phi(h) = 1 + 0 = 1$ which happens if and only if $h = 2$. If $r_1 = 0$ then $r_2 = 1$, so $\phi(h) = 0 + 2 = 2$, which happens if $h = 3$, 4, or 6.

CHAPTER 3

Application to Swan Subgroups

We calculate the Swan subgroups $T(\mathbb{Z}G)$ for Higman groups of the forms so far discussed. We first present some known results mentioned in [**Guzman**].

THEOREM 34. *For $m \geq 2$,*

$$T(\mathbb{Z}C_2) = \frac{\left(\mathbb{Z}/2^m\mathbb{Z}\right)^\times}{\operatorname{Im}(\mathbb{Z}^\times)}$$

.

PROPOSITION 35. *$T(RG)$ is the homomorphic image of $\bar{R}/\operatorname{Im}(R^\times)$. If $R = \mathbb{Z}$ and $|G| > 2$, then*

$$|T(RG)| \mid \frac{\phi(n)}{2}$$

PROOF. By Corollary 24 we have that

$$\begin{aligned} T(RG) &\cong \frac{\bar{R}}{h(\Gamma^\times \times R^\times)} \\ &= \frac{\bar{R}}{\operatorname{Im}(\Gamma^\times)\operatorname{Im}(R^\times)} \\ &\twoheadleftarrow \bar{R}/\operatorname{Im}(R^\times) \end{aligned}$$

If $R = \mathbb{Z}$, then

$$|T(\mathbb{Z}G)| \mid \left|\frac{\bar{\mathbb{Z}}^\times}{\operatorname{Im}(\mathbb{Z}^\times)}\right|$$

and for $n \geq 2$, $1 \not\equiv -1 \pmod 2$ so $\operatorname{Im}(\mathbb{Z}^\times) = \{\pm 1\}$. □

PROPOSITION 36. *If G is cyclic then $T(\mathbb{Z}G) = 0$.*

PROOF. Let $G = C_n = \langle x \rangle$ and let $r \in Z$ such that $(r, n) = 1$. Consider

$$\begin{aligned} u &= \frac{x^{r-1} - 1}{x - 1} \\ &= \sum_{i=0}^{r-1} x^i \in \mathbb{Z}G \end{aligned}$$

Since $(r,n)=1$. there exists $s,t\in\mathbb{Z}$ such that $rs+tn=1$. Then

$$\begin{aligned} u^{-1} &= \frac{x-1}{x^{r-1}-1} \\ &= \frac{x^{rs}-1}{x^{r}-1}\in\mathbb{Z}G \end{aligned}$$

Then $u+\mathbb{Z}\Sigma=\sum_{i=0}^{r-1}x^i+\mathbb{Z}\Sigma\in\Gamma^\times$ and $\varepsilon(u)=r$ so

$$h:\Gamma^\times\times\mathbb{Z}^\times\to\bar{\mathbb{Z}}^\times$$

$\square$

Applying Corollary 24 we have the desired result

Corollary 37. *When $G=C_2$, C_3, or C_4, $T(\mathbb{Z}G)=0$.*

Theorem 38. [**MT-LJM**] *If G is a non-cyclic group of order p^m for some $m\in\mathbb{Z}$ and some odd prime p, then $T(\mathbb{Z}G)$ is a cyclic group of order p^{n-1}.*

An analogue of Theorem 38 is also known for $p=2$ and is proved by Taylor in [**MT-LJM**]. The following theorem is a special case, proven as a corollary of Theorem 9.

Theorem 39. *For $m\geq 2$*

$$\begin{aligned} T\left(\mathbb{Z}C_2^m\right) &= \frac{\left(\mathbb{Z}/2^m\mathbb{Z}\right)^\times}{\operatorname{Im}\left(\mathbb{Z}^\times\right)} \\ &= \frac{\left(\mathbb{Z}/2^m\mathbb{Z}\right)^\times}{\operatorname{Im}\left(\{\pm1\}\right)} \\ &\cong \mathbb{Z}/2^{m-2}\mathbb{Z} \end{aligned}$$

$$\left|T\left(\mathbb{Z}C_2^m\right)\right|=2^{m-2}$$

In [**Ullom**], as cited by [**Guzman**], it is shown that:

Proposition. *In the exact sequence found in Equation 24, $\operatorname{Im}\delta=T(RG)$. δ is given by $\delta(\bar{r})=\langle r,\sigma\rangle\in D(RG)$.*

Proposition 40. *By the exact sequence above, we have*

$$T(RG)\cong\bar{R}^\times/h\left(\Gamma^\times\times R^\times\right)$$

$$\cong \bar{R}^{\times}/\operatorname{im}\left(\Gamma^{\times}\right)$$

where $\operatorname{im}(\Gamma^{\times}) = \bar{\varepsilon}(\Gamma^{\times})$ *and* Γ *is the truncated group ring* RG_t*.*

Finally, we have the following well-known result:

Proposition 41. *The Swan subgroup* $T(RG)$ *is the homomorphic image of* $\bar{R}/\operatorname{Im}(R^{\times})$*. Furthermore, when* $R = \mathbb{Z}$ *and* $|G| = n > 2$*, then* $|T(RG)| \mid \frac{\varphi(n)}{2}$ *where* φ *is the Euler totient function.*

We now discuss the cases $G = C_3 \times C_2^n$ and $G = C_4 \times C_2^n$.

For the first, let $G = \left\langle b, a_1, \cdots, a_n : a_i^2 = b^3 = 1, xy = yx \text{ for all } x, y \in G\right\rangle$. Then the pullback diagram becomes

$$\begin{tikzcd}
\mathbb{Z}G \arrow[r] \arrow[d, "\varepsilon"] & \mathbb{Z}G/\mathbb{Z}\Sigma \arrow[d, "\bar{\varepsilon}"] \\
\mathbb{Z} \arrow[r, "\pi"] & \mathbb{Z}/n\mathbb{Z}
\end{tikzcd}$$

Now

$$\operatorname{im}\left(\Gamma^{\times}\right) = \operatorname{im}\left(\left(\mathbb{Z}G/\mathbb{Z}\Sigma\right)^{\times}\right)$$

By Theorem 9 we have that $\mathbb{Z}G/\mathbb{Z}\Sigma$ has only trivial units in this case, so

$$\begin{aligned}
\operatorname{im}\left(\Gamma^{\times}\right) &= \operatorname{im}\left(\{\pm g : g \in G\}\right) \\
&= \bar{\varepsilon}\left(\{\pm g : g \in G\}\right) \\
&= \{\pm\bar{1}\}
\end{aligned}$$

Thus,

$$\begin{aligned}
T(\mathbb{Z}G) &\cong \frac{\left(\mathbb{Z}/|G|\mathbb{Z}\right)^{\times}}{\{\pm\bar{1}\}} \\
&\cong \frac{\left(\mathbb{Z}/(3\cdot 2^n)\mathbb{Z}\right)^{\times}}{\{\pm\bar{1}\}}
\end{aligned}$$

Since $|T(\mathbb{Z}G)| \mid \frac{\varphi(3\cdot 2^n)}{2}$ and $\frac{\varphi(3\cdot 2^n)}{2} = \frac{\varphi(3)\varphi(2^n)}{2} = \varphi(2^n) = 2^{n-1}$, we have that $|T(\mathbb{Z}G)| \mid 2^{n-1}$.

When $n = 1$, $\left(\mathbb{Z}/6\mathbb{Z}\right)^{\times} = \langle \pm\bar{1} \rangle$ so $T(\mathbb{Z}G)$ is trivial. (This can also be seen by the fact that in this case $G = C_3 \times C_2 \cong C_6$ is a cyclic group, so $T(\mathbb{Z}G)$ is trivial by Theorem 1.23 in [**Guzman**].

In general,

$$\begin{aligned}\left(\mathbb{Z}/(3\cdot 2^n)\mathbb{Z}\right)^{\times} &\cong \left(\mathbb{Z}/3\mathbb{Z}\right)^{\times} \times \left(\mathbb{Z}/(2^n)\mathbb{Z}\right)^{\times} \\ &\cong \mathbb{Z}/2\mathbb{Z} \times \left(\mathbb{Z}/(2^{n-2})\mathbb{Z}\right) \times \mathbb{Z}/2\mathbb{Z}\end{aligned}$$

with the two cyclic groups of order 2 being generated by $2^{n+1} + (-1)^{n+1}$ and $2^n + (-1)^n$. The product of these generators is

$$\left(2^{n+1} + (-1)^{n+1}\right)\left(2^n + (-1)^n\right) = 2^{2n+1} + (-1)^{2n+1} - (-2)^{n+1} - (-2)^n$$

Modulo $3 \cdot 2^n$, we have

$$\begin{aligned}2^{n+k} &\equiv 3 \cdot 2^{n+k-1} - 2^{n+k-1} \\ &\equiv -2^{n+k-1} = (-1)^k\, 2^n\end{aligned}$$

If n is even, then

$$\begin{aligned}2^{2n+1} + (-1)^{2n+1} - (-2)^{n+1} - (-2)^n &= 2^{2n+1} - 1 + 2^{n+1} - 2^n \\ &= 2^{2n+1} + 2^n - 1\end{aligned}$$

Since $2^{2n+1} \equiv -2^n \pmod{3 \cdot 2^n}$ we have that

$$2^{2n+1} + 2^n - 1 \equiv -1 \pmod{3 \cdot 2^n}$$

If n is odd, then

$$\begin{aligned}2^{2n+1} + (-1)^{2n+1} - (-2)^{n+1} - (-2)^n &= 2^{2n+1} - 1 - 2^{n+1} + 2^n \\ &= 2^{2n+1} - 1 - 2^n\end{aligned}$$

and modulo $3 \cdot 2^n$ we have

$$2^{2n+1} - 1 - 2^n \equiv 2^n - 2^n - 1 \pmod{3 \cdot 2^n}$$

$$\equiv 1 \pmod{3 \cdot 2^n}$$

In either case, we have that $T(\mathbb{Z}G)$ is the quotient of ${}^{\mathbb{Z}}/_{2\mathbb{Z}} \times \left({}^{\mathbb{Z}}/_{(2^{n-2})\mathbb{Z}}\right) \times {}^{\mathbb{Z}}/_{2\mathbb{Z}}$ by the subgroup generated by the product of the firSst and last cyclic components. Thus, $T(\mathbb{Z}G) \cong \left({}^{\mathbb{Z}}/_{(2^{n-2})\mathbb{Z}}\right) \times {}^{\mathbb{Z}}/_{2\mathbb{Z}}$, and therefore

$$|T(\mathbb{Z}G)| = 2^{n-1}$$

For the second case, let $G = C_4 \times C_2^n$. By our work in Chapter 5, we have that ${}^{\mathbb{Z}G}/_{\mathbb{Z}\Sigma}$ has only trivial units in this case, so

$$\begin{aligned}
\operatorname{im}\left(\Gamma^{\times}\right) &= \operatorname{im}\left(\{\pm g : g \in G\}\right) \\
&= \bar{\varepsilon}\left(\{\pm g : g \in G\}\right) \\
&= \{\pm \bar{1}\}
\end{aligned}$$

Thus,

$$\begin{aligned}
T(\mathbb{Z}G) &\cong \frac{\left({}^{\mathbb{Z}}/_{|G|\mathbb{Z}}\right)^{\times}}{\{\pm\bar{1}\}} \\
&\cong \frac{\left({}^{\mathbb{Z}}/_{(2^{n+2})\mathbb{Z}}\right)^{\times}}{\{\pm\bar{1}\}}
\end{aligned}$$

Now,

$$\left({}^{\mathbb{Z}}/_{(2^{n+2})\mathbb{Z}}\right)^{\times} \cong {}^{\mathbb{Z}}/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}/_{2^n\mathbb{Z}}$$

with the generator of the first component being the image of $-\bar{1}$. Thus,

$$T(\mathbb{Z}G) \cong {}^{\mathbb{Z}}/_{2^n\mathbb{Z}}$$

THEOREM 42. *If $G = C_3^m \times C_2^n$, $m, n \geq 1$, then $|T(\mathbb{Z}G)| = 3^{m-1} \cdot 2^{n-1}$.*

PROOF. Let $G = C_3^m \times C_2^n$ By our work in Chapter 5, we have that ${}^{\mathbb{Z}G}/_{\mathbb{Z}\Sigma}$ has only trivial units in this case, so

$$\begin{aligned}
\operatorname{im}\left(\Gamma^{\times}\right) &= \operatorname{im}\left(\{\pm g : g \in G\}\right) \\
&= \bar{\varepsilon}\left(\{\pm g : g \in G\}\right) \\
&= \{\pm \bar{1}\}
\end{aligned}$$

and

$$
\begin{aligned}
T(\mathbb{Z}G) &\cong \frac{\left(\mathbb{Z}/|G|\mathbb{Z}\right)^{\times}}{\{\pm\bar{1}\}} \\
&\cong \frac{\left(\mathbb{Z}/(3^m \cdot 2^n)\mathbb{Z}\right)^{\times}}{\{\pm\bar{1}\}}
\end{aligned}
$$

Now,

$$
\begin{aligned}
\left(\mathbb{Z}/(3^m \cdot 2^n)\mathbb{Z}\right)^{\times} &\cong \left(\mathbb{Z}/3^m\mathbb{Z}\right)^{\times} \times \left(\mathbb{Z}/2^n\mathbb{Z}\right)^{\times} \\
&\cong \mathbb{Z}/2\mathbb{Z} \times \left(\mathbb{Z}/3^{m-1}\mathbb{Z}\right) \times \mathbb{Z}/2\mathbb{Z} \times \left(\mathbb{Z}/2^{n-2}\mathbb{Z}\right)
\end{aligned}
$$

so

$$
\left| \frac{\left(\mathbb{Z}/(3^m \cdot 2^n)\mathbb{Z}\right)^{\times}}{\{\pm\bar{1}\}} \right| = 3^{m-1} \cdot 2^{n-1}
$$

Since $|T(\mathbb{Z}G)| \mid \frac{\varphi(3^m \cdot 2^n)}{2} = 3^{m-1} \cdot 2^{n-1}$, and $\left(\mathbb{Z}/(3^m \cdot 2^n)\mathbb{Z}\right)^{\times}$ has cardinality $3^{m-1} \cdot 2^n$, we have that $|T(\mathbb{Z}G)| = 3^{m-1} \cdot 2^{n-1}$. $\square$

CHAPTER 4

Trivial Units of Group Rings over Integer Rings of Quadratic Imaginary Fields

THEOREM 43 ([**Herm-Li**]). *Let G be a finite abelian group and $R = \mathcal{O}_K$ for K an algebraic number field. Then RG has only trivial units if and only if one of the following holds:*

(1) *$G = C_2^n$ and $K = \mathbb{Q}$ or $K = \mathbb{Q}\left(\sqrt{-d}\right)$ for d either 1 or a squarefree positive integer;*

(2) *$G = C_4^m \times C_2^n$ and $K = \mathbb{Q}$ or $K = \mathbb{Q}(i)$;*

(3) *$G = C_3^m \times C_2^n$ and $K = \mathbb{Q}$ or $K = \mathbb{Q}(\zeta_3)$ where $\zeta_3 = \frac{-1+i\sqrt{3}}{2}$.*

To prove this theorem, found in [**Herm-Li**] we prove yet another series of lemmas from both [**Herm-Li**] and [**Herm-Li-Par**].

LEMMA 44. *Let R be a commutative ring. Then the following are equivalent:*

(1) *RC_2 has nontrivial units;*

(2) *There exist $a, b \neq 0$ in R such that $a^2 - b^2 \in R^\times$;*

(3) *There exists $a \neq 0, 1$ in R such that $2a - 1 \in R^\times$.*

PROOF.

- ((1) $\Leftrightarrow$ (2)): Suppose u is an nontrivial unit in RC_2. Then $u = a + bx$ where $a, b \neq 0$, and since u is a unit, we have that for all $s, t \in R$ there exists $v, w \in R$ such that

$$(a + bx)(v + wx) = s + tx$$

Equating coefficients, this is equivalent to saying that v, w exist and satisfy

$$av + bw = s$$

$$bv + aw = t,$$

or equivalently that the matrix $\begin{bmatrix} a & b \\ b & a \end{bmatrix}$ has an inverse in $M_2(R)$. By the determinant property this holds if and only if $a^2 - b^2 \in R^{\times}$.

- $((1) \Leftrightarrow (3))$: Suppose $u = a + bx$ is an nontrivial unit in RC_2. Assume without loss of generality that $\varepsilon(u) = 1$: i.e, that $a + b = 1$. Then $u = a + (1 - a)x$. By the preceding proof this is non-trivial if and only if $a^2 - (1-a)^2 = a^2 - 1 + 2a - a^2 = 2a - 1 \in R^{\times}$.

$\square$

Lemma 45. *Suppose $R = \mathcal{O}(K)$ for K an algebraic number field and suppose RC_2 has only trivial units. Then either $K = \mathbb{Q}$ or K is an imaginary quadratic number field.*

Proof. By the preceding lemma, for all $r \in R$, if $2r - 1$ is a unit, then $r = 0$ or $r = 1$. Then $\Gamma = \{u \in R^{\times} : u = 2r - 1\} = \{\pm 1\}$. But this is the kernel of the homomorphism $\pi : R^{\times} \to (R/2R)^{\times}$ given by $u \to u + 2R$ above. Since $R/2R$ is finite we have that Γ is of finite index. The only way for Γ to be finite is for $R^{\times}$ to be finite. Since K is a finite extension of $\mathbb{Q}$, it follows from Dirichlet's unit theorem that that in order for this to happen, $K = \mathbb{Q}$ or $K = \mathbb{Q}\left(\sqrt{-d}\right)$, where d is a square-free positive integer. $\square$

Lemma 46. *Let R be a commutative ring with unity with characteristic 0. Then if RC_2 and RG have only trivial units, then $R[G \times C_2]$ has only trivial units.*

Proof. Let $u \in R[G \times C_2]^{\times}$. Without loss of generality assume that u has augmentation 1. Then $u = a + bx$, $\langle x \rangle = C_2$, $a, b \in RG$, and $\omega(a) + \omega(b) = 1$, where $\omega : RG \to R$ is the augmentation map. Similarly, the inverse $u^{-1} = c + dx$ satisfies $\omega(c) + \omega(d) = 1$. Then we have that

$$ac + bd = 1$$

$$ad + bc = 0$$

or

$$(a + b)(c + d) = 1$$

$$(a - b)(c - d) = 1$$

Thus, $a+b$ is a unit of augmentation 1 in RG and thus $a+b=g\in G$. Similarly, $a-b\in(RG)^{\times}$ so $a-b=vh$ for some $v\in R^{\times}$, $h\in G$. Now this implies

$$v=2\omega(a)-1$$

is a unit in R and since RC_2 has trivial units, we have $\omega(a)=0$ or 1, so $v=\pm1$. Thus,

$$2a=g+vh$$

$$2b=g-vh$$

If $g=h$, then either $2a=0$ or $2b=0$. By assumption, R has characteristic 0 and RC_2 has only trivial units, so 2 is not a zero divisor, so $a=0$ or $b=0$. If $b=0$, then $u=a\in RG^{\times}$ is trivial. If $a=0$, then $ux\in RG^{\times}$ is a trivial unit, and hence so is u.

On the other hand, if $g\neq h$, then $2a=g+vh$ implies that 2 is invertible in R. Setting $a=-2^{-1}$ gives us that $-2^{-1}=1$, implying R is of characteristic 3, a contradiction of our initial assumption. □

Corollary. *Suppose RC_2 has only trivial units. Then RE_2, where E is an elementary abelian 2-group, also has trivial units. In fact, RE_2 has trivial units if and only if $K=\mathbb{Q}$ or $K=\mathbb{Q}\left(\sqrt{-d}\right)$ for d a square-free positive integer.*

Lemma 47. *Let R be a commutative ring with unity. Then RC_3 has nontrivial units if and only if there exist $a,b\in R$ such that $(a,b)\notin\{(0,0),(-1,0),(-1,-1)\}$ and $1+3a+3a^2+3b^2-3ab\in R^{\times}$.*

Proof. Let $\langle x\rangle=C_3$. Let $u\in RC_3$ have augmentation 1. Then $u=1+(1-x)(a+bx)$ for some $a,b\in R$ and u is nontrivial if and only if $(a,b)\notin\{(0,0),(-1,0),(-1,-1)\}$. Consider the quotient ring $\frac{R\langle x\rangle}{1+x+x^2}\cong R[y]$, where $y^2+y+1=0$ and $y^3=1\neq y$ we have that the image of u in $R\langle y\rangle$ is

$$\begin{aligned}v&=1+(1-y)(a+by)\\&=1+a+by-ay-by^2\\&=1+a+by-ay+by+b\\&=1+a+b+(2b-a)y\end{aligned}$$

Now, since v is a unit, for any element $s+ty \in R[y]$ we can find $p+qy$ such that $v(p+qy) = s+ty$. Since

$$\begin{aligned} v(p+qy) &= [1+a+b+(2b-a)y](p+qy) \\ &= (1+a+b)p-(2b-a)q+((2b-a)p+(1-b+2a)q)y \end{aligned}$$

we have that the system

$$\begin{aligned} (1+a+b)p-(2b-a)q &= s \\ ((2b-a)p+(1-b+2a)q) &= t \end{aligned}$$

in p and q has a solution in R for all $s,t \in R$, so the determinant of

$$\begin{bmatrix} (1+a+b) & (2b-a) \\ (2b-a) & (1-b+2a) \end{bmatrix}$$

must be a unit of R. This determinant is exactly $1+3a+3a^2+3b^2-3ab$, so this condition is indeed necessary. It is also sufficient, as if a,b satisfy the condition, then if

$$\begin{aligned} e &= a^2+b^2+a-ab \\ d &= 1+3e \in R^\times \\ u &= 1+(1-x)(a+bx) \\ w &= \frac{(1+a+e)+(e-b)x+(e+b-a)x^2}{d} \end{aligned}$$

then $uw=1$ and u is therefore a non-trivial unit of R. □

Lemma 48. *Let R be a commutative ring with unity of characteristic 0, and suppose RC_3 has trivial units and that G is a finite elementary abelian 3-group. Then RG has only trivial units.*

Proof. The proof is by induction and analoguous to Lemma 46. □

Lemma 49. *Let R be a commutative ring with unity. Then RC_4 has non-trivial units if and only if either RC_2 has nontrivial units or there are nonzero $a,b \in R$ with $a \neq -1$ such that $2a^2+2b^2+2a=0$.*

Proof. If $\langle g \rangle = C_4$ then let $f : RC_4 \to RC_2$ be the R-linear extension of the group homomorphism $C_4 \to C_2$. Suppose $u \in RC_4$ is an nontrivial unit, and suppose RC_2 has only trivial units. Since f is a group ring homomorphism and maps units to units, we can assume without loss of generality that $f(u) = 1$. We can also assume that $u = 1 + \left(1 - x^2\right)(a + bx)$ for some nonzero $a, b \in R$ such that $a \neq -1$.

Now let $u^* = 1 + \left(1 - x^2\right)\left(a + bx^3\right)$. We have that

$$\begin{aligned} u^* &= 1 + \left(1 - x^2\right)\left(a + bx^3\right) \\ &= 1 + \left(a - ax^2 + bx^3 - bx\right) \\ &= 1 + \left(1 - x^2\right)(a - bx) \end{aligned}$$

so therefore

$$\begin{aligned} uu^* &= \left[1 + \left(1 - x^2\right)(a + bx)\right]\left[1 + \left(1 - x^2\right)(a - bx)\right] \\ &= 1 + \left(1 - x^2\right)\left(2a + 2a^2 + 2b^2\right) \in \left(R\left\langle x^2 \right\rangle\right)^\times \end{aligned}$$

Since $\left(R\left\langle x^2 \right\rangle\right)^\times$ has only trivial units, we have that $2a+2a^2+2b^2 = 0$ or $2a+2a^2+2b^2 = -1$. If $2a + 2a^2 + 2b^2 = -1$, then $a + a^2 + b^2 = -\frac{1}{2}$ so 2 is invertible, contradicting Lemma 46. If $2a + 2a^2 + 2b^2 = 0$ then we have that u is a non-trivial unit of RC_4.

From this, using either Dirichlet's Unit Theorem or Pell's equations, one derives the theorem statement. □

Corollary. *Suppose R is the integer ring of an algebraic number field and G is an abelian group of exponent 4. Then RG has trivial units if and only if $R = \mathbb{Z}$ or $R = \mathbb{Z}[i]$.*

Proof. This follows from Theorem 26 and the previous lemma, together with an induction lemma similar to Lemma 46. □

CHAPTER 5

Trivial Units of Truncated Group Rings

Proposition 50. *$\mathbb{Z}G_t$ has trivial units when $G = C_2$ since $(\mathbb{Z}C_2)_t \cong \mathbb{Z}$*

Proof. If $C_2 = \langle e \rangle$ then

$$\begin{aligned}\frac{\mathbb{Z}G}{\mathbb{Z}\Sigma G} &= \frac{\mathbb{Z}[1] \oplus \mathbb{Z}[1+e]}{\mathbb{Z}[1+e]} \\ &\cong \mathbb{Z}\end{aligned}$$

□

Proposition 51. *$\mathbb{Z}(\omega)[C_2]_t$ has only trivial units.*

Proof. If $C_2 = \langle e \rangle$ then

$$\mathbb{Q}(\omega)G = \mathbb{Q}(\omega)\left[\frac{1+e}{2}\right] \oplus \mathbb{Q}(\omega)\left[\frac{1-e}{2}\right]$$

so

$$\begin{aligned}\frac{\mathbb{Q}(\omega)G}{\mathbb{Q}(\omega)\Sigma G} &= \frac{\mathbb{Q}(\omega)\left[\frac{1+e}{2}\right] \oplus \mathbb{Q}(\omega)\left[\frac{1-e}{2}\right]}{\mathbb{Q}(\omega)\left[\frac{1+e}{2}\right]} \\ &\cong \mathbb{Q}(\omega)\end{aligned}$$

The corresponding maximal order is

$$\mathscr{M} = \mathbb{Z}(\omega)\left[\frac{1+e}{2}\right] \oplus \mathbb{Z}(\omega)\left[\frac{1-e}{2}\right]$$

and the corresponding truncated maximal order is

$$\mathbb{Z}(\omega)\left[\frac{1-e}{2}\right] \cong \mathbb{Z}(\omega)$$

which has 6 units. Since there are 6 trivial units in $\mathbb{Z}(\omega)[C_2]_t$, it follows that $\mathbb{Z}(\omega)[C_2]_t$ has only trivial units. □

Proposition 52. *$\mathbb{Z}[C_3]_t$ has only trivial units.*

Proof. Let $G = C_3 = \langle e \rangle$. Let ω be a primitive 3rd root of unity. In the group algebra $\mathbb{Q}(\omega) G$ we have that

$$\begin{aligned}\mathbb{Q}(\omega) G = \mathbb{Q}(\omega) \left[\frac{1+e+e^2}{3}\right] \oplus \mathbb{Q}(\omega) \left[\frac{1+\omega e+\omega^2 e^2}{3}\right] \\ \oplus \mathbb{Q}(\omega) \left[\frac{1+\omega^2 e+\omega e^2}{3}\right]\end{aligned}$$

so passing to $\mathbb{Q}G$, we have

$$\begin{aligned}\mathbb{Q}G &= \mathbb{Q}\left[\frac{1+e+e^2}{3}\right] \oplus \mathbb{Q}\langle e \rangle \left[\frac{1+\omega e+\omega^2 e^2}{3} + \frac{1+\omega^2 e+\omega e^2}{3}\right] \\ &= \mathbb{Q}\left[\frac{1+e+e^2}{3}\right] \oplus \mathbb{Q}\langle e \rangle \left[1 - \frac{1+e+e^2}{3}\right]\end{aligned}$$

Thus

$$\begin{aligned}\frac{\mathbb{Q}G}{\mathbb{Q}\Sigma G} &= \frac{\mathbb{Q}\left[\frac{1+e+e^2}{3}\right] \oplus \mathbb{Q}\langle e \rangle \left[1 - \frac{1+e+e^2}{3}\right]}{\mathbb{Q}\left(\frac{1+e+e^2}{3}\right)} \\ &= \mathbb{Q}\langle e \rangle [1 - \mathbb{Q}\Sigma G]\end{aligned}$$

Since

$$e + e^2 \equiv -1 \pmod{\mathbb{Q}\Sigma G},$$

we have that $\mathbb{Q}(e)[1 - \mathbb{Q}\Sigma G] \cong \mathbb{Q}(\omega)$ via the map

$$e - \mathbb{Q}\Sigma G \mapsto \omega$$

where ω is a primitive cube root of unity.

The maximal order is then

$$\mathscr{M} = \mathbb{Z}\left[\frac{1+e+e^2}{3}\right] \oplus \mathbb{Z}\langle e \rangle \left[1 - \frac{1+e+e^2}{3}\right]$$

and the truncated maximal order is isomorphic to $\mathbb{Z}[\omega]$. $\mathbb{Z}[\omega]$ has six units, all trivial, which must correspond to the trivial units in $\mathscr{M}$. □

Proposition 53. *$\mathbb{Z}[C_4]_t$ has only trivial units.*

PROOF. We have that if $G = C_4 = \langle e \rangle$ and if i is the primitive 4th root of unity, then for the group algebra $\mathbb{Q}(i)G$ we have that

$$\begin{aligned}\mathbb{Q}(i)\,G = \mathbb{Q}(i)\left(\frac{\Sigma}{4}\right) \oplus \mathbb{Q}(i)\left(\frac{1-e+e^2-e^3}{4}\right)\\ \oplus\, \mathbb{Q}(i)\left(\frac{1+ie-e^2-ie^3}{4}\right) \oplus \mathbb{Q}(i)\left(\frac{1-ie-e^2+ie^3}{4}\right)\end{aligned}$$

so passing to $\mathbb{Q}G$ we have that

$$\begin{aligned}\mathbb{Q}G &= \mathbb{Q}\langle e\rangle\left(\frac{\Sigma}{4}\right) \oplus \mathbb{Q}\langle e\rangle\left(\frac{1-e+e^2-e^3}{4}\right)\\ &\oplus \mathbb{Q}\langle e\rangle\left(\frac{1+ie-e^2-ie^3}{4}+\frac{1+ie-e^2-ie^3}{4}\right)\\ &= \mathbb{Q}\left(\frac{\Sigma}{4}\right) \oplus \mathbb{Q}\left(\frac{1-e+e^2-e^3}{4}\right) \oplus \mathbb{Q}\langle e\rangle\left(\frac{1-e^2}{2}\right)\end{aligned}$$

$$\begin{aligned}\frac{\mathbb{Q}G}{\mathbb{Q}\Sigma G} &= \frac{\mathbb{Q}\left(\frac{\Sigma}{4}\right) \oplus \mathbb{Q}\left(\frac{1-e+e^2-e^3}{4}\right) \oplus \mathbb{Q}\langle e\rangle\left(\frac{1-e^2}{2}\right)}{\mathbb{Q}\left(\frac{\Sigma}{4}\right)}\\ &= \mathbb{Q}\left(\frac{1-e+e^2-e^3}{4}\right) \oplus \mathbb{Q}\langle e\rangle\left(\frac{1-e^2}{2}\right)\\ &\cong \mathbb{Q}\oplus\mathbb{Q}(i)\end{aligned}$$

The corresponding maximal order is

$$\mathscr{M} = \mathbb{Z}\left(\frac{\Sigma}{4}\right) \oplus \mathbb{Z}\left(\frac{1-e+e^2-e^3}{4}\right) \oplus \mathbb{Z}\langle e\rangle\left(\frac{1-e^2}{2}\right)$$

and the corresponding truncated maximal order is $\mathbb{Z}\left(\frac{1-e+e^2-e^3}{4}\right) \oplus \mathbb{Z}\langle e\rangle\left(\frac{1-e^2}{2}\right) \cong \mathbb{Z}\oplus\mathbb{Z}[i]$. This has eight units, which clearly correspond to the eight trivial units in $\mathbb{Z}G$. ☐

PROPOSITION 54. *$\mathbb{Z}[C_2 \times C_2]_t$ has only trivial units*

PROOF. Let $G = \langle f, g\rangle = C_2 \times C_2$. Then for the group ring, we have

$$\begin{aligned}\mathbb{Q}G = \mathbb{Q}\frac{\Sigma G}{4} \oplus \mathbb{Q}\left(\frac{1-f+g-fg}{4}\right)\\ \oplus\, \mathbb{Q}\left(\frac{1+f-g-fg}{4}\right) \oplus \mathbb{Q}\left(\frac{1-f-g+fg}{4}\right)\end{aligned}$$

so

$$\begin{aligned}\frac{\mathbb{Q}G}{\mathbb{Q}\Sigma G} &= \mathbb{Q}\left(\frac{1-f+g-fg}{4}\right) \oplus \mathbb{Q}\left(\frac{1+f-g-fg}{4}\right) \oplus \mathbb{Q}\left(\frac{1-f-g+fg}{4}\right) \\ &\cong \mathbb{Q}^3\end{aligned}$$

The maximal order corresponding to this is

$$\mathscr{M} = \mathbb{Z}\frac{\Sigma G}{4} \oplus \mathbb{Z}\left(\frac{1-f+g-fg}{4}\right) \oplus \mathbb{Z}\left(\frac{1+f-g-fg}{4}\right) \oplus \mathbb{Z}\left(\frac{1-f-g+fg}{4}\right)$$

and the truncated maximal order is

$$\mathbb{Z}\left(\frac{1-f+g-fg}{4}\right) \oplus \mathbb{Z}\left(\frac{1+f-g-fg}{4}\right) \oplus \mathbb{Z}\left(\frac{1-f-g+fg}{4}\right)$$

which is isomorphic to $\mathbb{Z}^3$. $\mathbb{Z}^3$ has $2^3 = 8$ units, and $\mathbb{Z}G_t$ has 8 trivial units, so it follows that $\mathbb{Z}G_t$ has only trivial units. □

PROPOSITION 55. *$\mathbb{Z}[C_3 \times C_3]_t$ has only trivial units.*

PROOF. We have that if $G = \langle f, g\rangle$ and if ω is the primitive cube root of unity, then for the group algebra $\mathbb{Q}(\omega)G$ we have that

$$\begin{aligned}\mathbb{Q}(\omega)G = \mathbb{Q}(\omega)&\left[\frac{(1+f+f^2)(1+g+g^2)}{9}\right] \oplus \mathbb{Q}(\omega)\left[\frac{(1+f+f^2)(1+\omega g+\omega^2 g^2)}{9}\right] \\ &\oplus \mathbb{Q}(\omega)\left[\frac{(1+f+f^2)(1+\omega^2 g+\omega g^2)}{9}\right] \\ &\oplus \mathbb{Q}(\omega)\left[\frac{(1+\omega f+\omega^2 f^2)(1+g+g^2)}{9}\right] \oplus \mathbb{Q}(\omega)\left[\frac{(1+\omega^2 f+\omega f^2)(1+g+g^2)}{9}\right] \\ &\oplus \mathbb{Q}(\omega)\left[\frac{(1+\omega f+\omega^2 f^2)(1+\omega g+\omega^2 g^2)}{9}\right] \\ &\oplus \mathbb{Q}(\omega)\left[\frac{(1+\omega f+\omega^2 f^2)(1+\omega^2 g+\omega g^2)}{9}\right] \\ &\oplus \mathbb{Q}(\omega)\left[\frac{(1+\omega^2 f+\omega f^2)(1+\omega g+\omega^2 g^2)}{9}\right] \\ &\oplus \mathbb{Q}(\omega)\left[\frac{(1+\omega^2 f+\omega f^2)(1+\omega^2 g+\omega g^2)}{9}\right]\end{aligned}$$

Passing to $\mathbb{Q}G$ we have

$$\begin{aligned}\mathbb{Q}G = \mathbb{Q}&\left[\frac{\left(1+f+f^2\right)\left(1+g+g^2\right)}{9}\right] \oplus \mathbb{Q}\langle g\rangle \left[\frac{\left(1+f+f^2\right)}{3}\left(1-\frac{1+g+g^2}{3}\right)\right]\\ \oplus\, \mathbb{Q}\langle f\rangle &\left[\left(1-\frac{1+f+f^2}{3}\right)\frac{\left(1+g+g^2\right)}{3}\right]\\ \oplus\, \mathbb{Q}\langle f\rangle &\left[\frac{2-f-f^2-g-fg+2f^2g-g^2+2fg^2-f^2g^2}{9}\right]\\ \oplus\, \mathbb{Q}\langle f\rangle &\left[\frac{2-f-f^2-g+2fg-f^2g-g^2-fg^2+2f^2g^2}{9}\right]\end{aligned}$$

Thus,

$$\begin{aligned}\frac{\mathbb{Q}G}{\mathbb{Q}\Sigma G} = \mathbb{Q}\langle g\rangle &\left[\frac{\left(1+f+f^2\right)}{3} - \mathbb{Q}\Sigma G\right]\\ \oplus\, \mathbb{Q}\langle f\rangle &\left[\frac{\left(1+g+g^2\right)}{3} - \mathbb{Q}\Sigma G\right]\\ \oplus \mathbb{Q}\langle f\rangle &\left[\frac{1+f^2g+fg^2}{3} - \mathbb{Q}\Sigma G\right]\\ \oplus\, \mathbb{Q}\langle f\rangle &\left[\frac{1+fg+f^2g^2}{3} - \mathbb{Q}\Sigma G\right]\end{aligned}$$

The corresponding maximal order is

$$\begin{aligned}\mathscr{M} = \mathbb{Z}&\left[\frac{\left(1+f+f^2\right)\left(1+g+g^2\right)}{9}\right] \oplus \mathbb{Z}\langle g\rangle \left[\frac{\left(1+f+f^2\right)}{3}\left(1-\frac{1+g+g^2}{3}\right)\right]\\ \oplus\, \mathbb{Z}\langle f\rangle &\left[\left(1-\frac{1+f+f^2}{3}\right)\frac{\left(1+g+g^2\right)}{3}\right]\\ \oplus\, \mathbb{Z}\langle f\rangle &\left[\frac{2-f-f^2-g-fg+2f^2g-g^2+2fg^2-f^2g^2}{9}\right]\\ \oplus\, \mathbb{Z}\langle f\rangle &\left[\frac{2-f-f^2-g+2fg-f^2g-g^2-fg^2+2f^2g^2}{9}\right]\end{aligned}$$

and the truncated maximal order is

$$\begin{aligned}\mathbb{Z}\langle g\rangle &\left[\frac{\left(1+f+f^2\right)}{3} - \mathbb{Q}\Sigma G\right]\\ \oplus\, \mathbb{Z}\langle f\rangle &\left[\frac{\left(1+g+g^2\right)}{3} - \mathbb{Q}\Sigma G\right]\end{aligned}$$

$$\oplus\,\mathbb{Z}\langle f\rangle\left[\frac{1+f^2g+fg^2}{3}-\mathbb{Q}\Sigma G\right]$$
$$\oplus\,\mathbb{Z}\langle f\rangle\left[\frac{1+fg+f^2g^2}{3}-\mathbb{Q}\Sigma G\right]$$

This is isomorphic to $\mathbb{Z}(\omega)^4$, which has 6^4 units. However, an enumeration of the corresponding elements in the maximal order shows that there are only trivial units in the truncated group ring. □

THEOREM 56. *Suppose $G' = G \times C_2$, where $C_2 = \langle f\rangle$, and suppose $\mathbb{Z}G$ has only trivial units and $|G| > 2$. Then if $\mathbb{Z}G_t$ has only trivial units, then $\mathbb{Z}G'_t$ has only trivial units*

PROOF. Suppose $\mathbb{Z}G_t$ has only trivial units; equivalently, we say that

$$(x-\mathbb{Z}\Sigma G)(y-\mathbb{Z}\Sigma G) = 1-\mathbb{Z}\Sigma G.$$

In other words,

$$xy-1 = m\Sigma G$$

for some $m\in\mathbb{Z}$ if and only if

$$x-u = m'\Sigma G$$

for some $m'\in\mathbb{Z}$, $u=\pm g\in G$.

Let $x = a+bf+\mathbb{Z}\Sigma G(1+f)\in\mathbb{Z}G'_t$ be a unit. Suppose $c,d\in\mathbb{Z}G$ exist such that

$$(a+bf+\mathbb{Z}\Sigma G(1+f))(c+df+\mathbb{Z}\Sigma G(1+f)) = 1+\mathbb{Z}\Sigma G(1+f)$$

Then

$$ac+bd+bcf+adf+\mathbb{Z}\Sigma G(1+f) = 1+\mathbb{Z}\Sigma G(1+f),$$

or equivalently

$$ac+bd+bcf+adf-1 = \frac{m}{2}\Sigma G(1+f)$$

for some $\frac{m}{2}\in\mathbb{Z}$ This implies

$$ac+bd-1 = \frac{m}{2}\Sigma G$$
$$bc+ad = \frac{m}{2}\Sigma G$$

In other words,

$$(a+b)(c+d)-1 = m\Sigma G$$
$$(a-b)(c-d)-1 = 0$$

Since $\mathbb{Z}G_t$ has only trivial units, we have

$$a+b-u = m_1\Sigma G$$
$$a-b-u' = 0$$

where $u = \pm g$, $u' = \pm g'$, for some $m_1 \in \mathbb{Z}$. Then

$$a - \frac{u+u'}{2} = \left(\frac{m_1}{2}\right)\Sigma G$$

By definition of ΣG, we have that for all $h \in G$,

$$\left(a - \frac{u+u'}{2}\right)[h] = \left(\frac{m_1}{2}\right)$$

Now suppose for a contradiction that $g \neq g'$. Then we have

$$\left(a - \frac{u+u'}{2}\right)[g] = a\,[g] \pm \frac{1}{2}$$
$$\left(a - \frac{u+u'}{2}\right)[g'] = a\,[g'] \pm \frac{1}{2}$$

Since $|G| > 2$ we can choose yet another element $g'' \in G$. Then

$$\left(a - \frac{u+u'}{2}\right)[g''] = a\,[g''] = a\,[g'] \pm \frac{1}{2}$$

contradicting the fact that $a\,[g''] \in \mathbb{Z}$ and $a\,[g'] \pm \frac{1}{2} \notin \mathbb{Z}$. Thus, $g' = g$, so

$$u = \pm u' = \pm g,$$

and therefore

$$a+b-u = m_1\Sigma G \tag{5.0.1}$$
$$a-b \pm u = 0 \tag{5.0.2}$$

so $a+b \equiv \pm(a-b) \pmod{\Sigma G}$. As an additional consequence, we note that $\frac{m_1}{2} \in \mathbb{Z}$

If $a+b \equiv a-b \equiv u \pmod{\Sigma G}$ we have $a \equiv u \pmod{\Sigma G}$,$b \equiv 0 \Sigma G$. Indeed, we have

$$a = u + \frac{m_1 \Sigma G}{2}$$
$$b = \frac{m_1 \Sigma G}{2}$$

so

$$\begin{aligned} a + bf &= \left(u + \frac{m_1 \Sigma G}{2}\right) + \frac{m_1 \Sigma G}{2} f \\ &= u + \frac{m_1 \Sigma G\,(1+f)}{2} \end{aligned}$$

On the other hand, if $a+b \equiv u \equiv b-a \pmod{\Sigma G}$,we have $b \equiv u \pmod{\Sigma G}$ and $a \equiv 0 \pmod{\Sigma G}$. Indeed, by equations (5.0.1) and (5.0.2), we have

$$a = \frac{m_1 \Sigma G}{2}$$
$$b = u + \frac{m_1 \Sigma G}{2}$$

so

$$\begin{aligned} a + bf &= \left(\frac{m_1 \Sigma G}{2}\right) + \left(u + \frac{m_1 \Sigma G}{2}\right) f \\ &= uf + \frac{m_1 \Sigma G\,(1+f)}{2} \end{aligned}$$

In both cases $a+bf$ is a trivial unit modulo $\Sigma G\,(1+f)$, as was sought to prove. $\square$

THEOREM 57. *Suppose $G' = G \times C_3$, where $|G| > 3$ and $C_3 = \langle f \rangle$. Then if $\mathbb{Z}G_t$ and $\mathbb{Z}(\omega)G$ have only trivial units, where ω is the primitive cube root of unity , then $\mathbb{Z}G'_t$ has only trivial units.*

PROOF. Suppose $\mathbb{Z}G_t$ has only trivial units; i.e,

$$xy - 1 = m\Sigma G$$

for some $m \in \mathbb{Z}$ if and only if

$$x - u = m' \Sigma G$$

for some $m' \in \mathbb{Z}$, $u = \pm g \in G$. Let

$$x = a + bf + cf^2 + \mathbb{Z}\Sigma G\left(1 + f + f^2\right) \in \mathbb{Z}G_t'$$

be a unit. Suppose $a', b', c' \in \mathbb{Z}G$ exist such that

$$y = a' + b'f + c'f^2 + \mathbb{Z}\Sigma G\left(1 + f + f^2\right)$$

satisfies

$$xy = 1 + \mathbb{Z}\Sigma G\left(1 + f + f^2\right)$$

Then

$$\begin{aligned} aa' + bc' + cb' + \left(ab' + ba' + cc'\right)f + \left(ac' + bb' + ca'\right)f^2 + \mathbb{Z}\Sigma G\left(1 + f + f^2\right) \\ = 1 + \mathbb{Z}\Sigma G\left(1 + f + f^2\right) \end{aligned}$$

or equivalently

$$\begin{aligned} aa' + bc' + cb' + \left(ab' + ba' + cc'\right)f + \left(ac' + bb' + ca'\right)f^2 - 1 \\ = \frac{m}{3}\Sigma G\left(1 + f + f^2\right) \end{aligned}$$

for some $\frac{m}{3} \in \mathbb{Z}$. This implies

$$\begin{aligned} aa' + bc' + cb' - 1 &= \frac{m}{3}\Sigma G \\ ab' + ba' + cc' &= \frac{m}{3}\Sigma G \\ ac' + bb' + ca' &= \frac{m}{3}\Sigma G \end{aligned}$$

Since $\mathbb{Z}G_t$ and $\mathbb{Z}(\omega)G$ each have only trivial units, we have that

$$\begin{aligned} (a + b + c)\left(a' + b' + c'\right) - 1 &= m\Sigma G \\ \left(a + \omega b + \omega^2 c\right)\left(a' + \omega b' + \omega^2 c'\right) - 1 &= 0 \\ \left(a + \omega^2 b + \omega c\right)\left(a' + \omega^2 b' + \omega c'\right) - 1 &= 0 \end{aligned}$$

so

$$a+b+c-u_1 = m_1\Sigma G$$
$$a+\omega b+\omega^2 c-u_2 = 0$$
$$a+\omega^2 b+\omega c-u_3 = 0$$

for some $m_1 \in \mathbb{Z}$, where $u_i = \pm\omega^{b_i} g_i \in G$. Then

$$a - \frac{u_1+u_2+u_3}{3} = \left(\frac{m_1}{3}\right)$$

By definition of ΣG, we have that for all $h \in G$,

$$\left(a - \frac{u_1+u_2+u_3}{3}\right)[h] = \left(\frac{m_1}{3}\right)$$

Now suppose that there does not exist a $g \in G$ such that $g_i = g$ for all $1 \leq i \leq 3$. Then

$$\left(a - \frac{u_1+u_2+u_3}{3}\right)[g_i] = a\,[g_i] \pm \frac{h_i}{3}$$

where $(3, h_i) = 1$, and since $|G| > 3$, we can pick $g' \neq g_i$ for any i. Then

$$\left(a - \frac{u_1+u_2+u_3}{3}\right)[g'] = a\,[g'] = a\,[g_i] \pm \frac{h}{3}$$

a contradiction. Thus, the g_i are equal to g so therefore

$$a+b+c \pm \omega^{b_1} g = m_1\Sigma G$$
$$a+\omega b+\omega^2 c \pm \omega^{b_2} g = 0$$
$$a+\omega^2 b+\omega c \pm \omega^{b_3} g = 0$$

Note that $b_1 = 0$ and $\frac{m_1}{3} \in \mathbb{Z}$ follow as consequences of the above and the fact that $a+b+c \in \mathbb{Z}G$, so

$$a+b+c \pm g = m_1\Sigma G$$
$$a+\omega b+\omega^2 c \pm \omega^{b_2} g = 0$$
$$a+\omega^2 b+\omega c \pm \omega^{b_3} g = 0$$

Adding all three rows and dividing by 3 gives

$$a + \frac{\left(\pm 1 \pm \omega^{b_2} \pm \omega^{b_3}\right)}{3} g = \frac{m_1}{3} \Sigma G$$

Then $\frac{\left(\pm 1 \pm \omega^{b_2} \pm \omega^{b_3}\right)}{3} \in \mathbb{Z}(\omega)$. Without loss of generality assume the first sign is positive. Under these restrictions there are three cases to deal with satisfying these constraints. $\square$

Case 1. All signs are positive and $b_2 = 1, b_3 = 2$. Then $\left(1 + \omega + \omega^2\right) = 0$ so $a = \frac{m_1}{3} \Sigma G \equiv 0 \pmod{\mathbb{Z}\Sigma G}$. Then

$$\begin{aligned} b + c + g &= \frac{2m_1}{3} \Sigma G \\ \omega b + \omega^2 c + \omega g &= -\frac{m_1}{3} \Sigma G \\ \omega^2 b + \omega c + \omega^2 g &= -\frac{m_1}{3} \Sigma G \end{aligned}$$

Subtracting the third equation from the second and dividing by $\omega - \omega^2$ gives

$$b - c + g = 0$$

so either $b \equiv -g + \frac{m_1}{3} \Sigma G$ and $c \equiv \frac{m_1}{3} \Sigma G$, in which case

$$\begin{aligned} a + bf + cf^2 &= \left(\frac{m_1}{3} \Sigma G\right) + \left(-g + \frac{m_1}{3} \Sigma G\right) f + \left(\frac{m_1}{3} \Sigma G\right) f^2 \\ &= -gf + m_1 \Sigma G \frac{\left(1 + f + f^2\right)}{3} \end{aligned}$$

or $b \equiv \frac{m_1}{3} \Sigma G$ and $c \equiv g + \frac{m_1}{3} \Sigma G$, in which case

$$\begin{aligned} a + bf + cf^2 &= \left(\frac{m_1}{3} \Sigma G\right) + \left(\frac{m_1}{3} \Sigma G\right) f + \left(g + \frac{m_1}{3} \Sigma G\right) f^2 \\ &= gf^2 + m_1 \Sigma G \frac{\left(1 + f + f^2\right)}{3} \end{aligned}$$

In both these cases $a + bf + cf^2$ is a trivial unit modulo $\Sigma G \left(1 + f + f^2\right)$.

Case 2. All signs are positive and $b_2 = 2, b_3 = 1$. The proof is entirely analogous to that for the previous case.

Case 3. All signs are positive and $b_2 = 0, b_3 = 0$. Then $\frac{\left(\pm 1 \pm \omega^{b_2} \pm \omega^{b_3}\right)}{3} = 1$ so $a = -g + \frac{m_1}{3} \Sigma G \pmod{\mathbb{Z}\Sigma G}$. Then

$$b + c = 2 \frac{m_1 \Sigma G}{3}$$

$$b - c = 0$$

so we have

$$\begin{aligned} a + bf + cf^2 &= \left(-g + \frac{m_1}{3}\Sigma G\right) + \frac{m_1}{3}\Sigma G f + \frac{m_1}{3}\Sigma G f^2 \\ &= -g + m_1 \Sigma G \frac{\left(1 + f + f^2\right)}{3} \end{aligned}$$

which is a trivial unit modulo $m_1 \Sigma G \frac{\left(1+f+f^2\right)}{3}$.

Since all cases have been covered, the proof is complete.

PROPOSITION 58. *$\mathbb{Z}\left[C_4 \times C_4\right]_t$ has only trivial units.*

PROOF. We have that if $G = \langle f, g \rangle$ and i is the imaginary unit, then

$$\begin{aligned} \mathbb{Q}(i)\, G = \mathbb{Q}(i) &\left[\frac{\left(1+f+f^2+f^3\right)\left(1+g+g^2+g^3\right)}{16}\right] \\ \oplus\, \mathbb{Q}(i) &\left[\frac{\left(1+f+f^2+f^3\right)\left(1+ig-g^2-ig^3\right)}{16}\right] \\ \oplus\, \mathbb{Q}(i) &\left[\frac{\left(1+f+f^2+f^3\right)\left(1-g+g^2-g^3\right)}{16}\right] \\ \oplus\, \mathbb{Q}(i) &\left[\frac{\left(1+f+f^2+f^3\right)\left(1-ig+g^2+ig^3\right)}{16}\right] \\ \oplus\, \mathbb{Q}(i) &\left[\frac{\left(1+if-f^2-if^3\right)\left(1+g+g^2+g^3\right)}{16}\right] \\ \oplus\, \mathbb{Q}(i) &\left[\frac{\left(1+if-f^2-if^3\right)\left(1+ig-g^2-ig^3\right)}{16}\right] \\ \oplus\, \mathbb{Q}(i) &\left[\frac{\left(1+if-f^2-if^3\right)\left(1-g+g^2-g^3\right)}{16}\right] \\ \oplus\, \mathbb{Q}(i) &\left[\frac{\left(1+if-f^2-if^3\right)\left(1-ig+g^2+ig^3\right)}{16}\right] \\ \oplus\, \mathbb{Q}(i) &\left[\frac{\left(1-f+f^2-f^3\right)\left(1+g+g^2+g^3\right)}{16}\right] \\ \oplus\, \mathbb{Q}(i) &\left[\frac{\left(1-f+f^2-f^3\right)\left(1+ig-g^2-ig^3\right)}{16}\right] \end{aligned}$$

$$\oplus\,\mathbb{Q}(i)\left[\frac{\left(1-f+f^2-f^3\right)\left(1-g+g^2-g^3\right)}{16}\right]$$

$$\oplus\,\mathbb{Q}(i)\left[\frac{\left(1-f+f^2-f^3\right)\left(1-ig+g^2+ig^3\right)}{16}\right]$$

$$\oplus\,\mathbb{Q}(i)\left[\frac{\left(1-if-f^2+if^3\right)\left(1+g+g^2+g^3\right)}{16}\right]$$

$$\oplus\,\mathbb{Q}(i)\left[\frac{\left(1-if-f^2+if^3\right)\left(1+ig-g^2-ig^3\right)}{16}\right]$$

$$\oplus\,\mathbb{Q}(i)\left[\frac{\left(1-if-f^2+if^3\right)\left(1-g+g^2-g^3\right)}{16}\right]$$

$$\oplus\,\mathbb{Q}(i)\left[\frac{\left(1-if-f^2+if^3\right)\left(1-ig+g^2+ig^3\right)}{16}\right]$$

Passing to $\mathbb{Q}G$ we have

$$\mathbb{Q}G=\mathbb{Q}\left[\frac{\left(1+f+f^2+f^3\right)\left(1+g+g^2+g^3\right)}{16}\right]\oplus\mathbb{Q}\left[\frac{\left(1+f+f^2+f^3\right)\left(1-g+g^2-g^3\right)}{16}\right]$$

$$\oplus\,\mathbb{Q}\langle g\rangle\left[\frac{\left(1+f+f^2+f^3\right)\left(1-g^2\right)}{8}\right]\oplus\mathbb{Q}\langle f\rangle\left[\frac{\left(1-f^2\right)\left(1+g+g^2+g^3\right)}{8}\right]$$

$$\oplus\,\mathbb{Q}\langle f\rangle\left[\frac{\left(1-f^2\right)\left(1-g+g^2-g^3\right)}{8}\right]$$

$$\oplus\,\mathbb{Q}\langle g\rangle[z_1]\oplus\mathbb{Q}\langle g\rangle[z_1]$$

$$\oplus\,\mathbb{Q}\left[\frac{\left(1-f+f^2-f^3\right)\left(1+g+g^2+g^3\right)}{16}\right]$$

$$\oplus\,\mathbb{Q}\langle f\rangle\left[\frac{\left(1-f+f^2-f^3\right)\left(1-g+g^2-g^3\right)}{16}\right]$$

$$\oplus\,\mathbb{Q}\langle g\rangle\left[\frac{\left(1-f+f^2-f^3\right)\left(1-g^2\right)}{8}\right]$$

where

$$z_1=\frac{\left(1+if-f^2-if^3\right)\left(1+ig-g^2-ig^3\right)}{16}+\frac{\left(1-if-f^2+if^3\right)\left(1-ig-g^2+ig^3\right)}{16}$$
$$z_2=\frac{\left(1-if-f^2+if^3\right)\left(1+ig-g^2-ig^3\right)}{16}+\frac{\left(1+if-f^2-if^3\right)\left(1-ig-g^2+ig^3\right)}{16}$$

and truncation gives us

$$\begin{aligned}
\frac{\mathbb{Q}G}{\mathbb{Q}\Sigma G} = \mathbb{Q}&\left[\frac{\left(1+f+f^2+f^3\right)\left(1-g+g^2-g^3\right)}{16} - \mathbb{Q}\Sigma G\right] \\
&\oplus \mathbb{Q}\left\langle g\right\rangle\left[\frac{\left(1+f+f^2+f^3\right)\left(1-g^2\right)}{8} - \mathbb{Q}\Sigma G\right] \\
&\oplus \mathbb{Q}\left\langle f\right\rangle\left[\frac{\left(1-f^2\right)\left(1+g+g^2+g^3\right)}{8} - \mathbb{Q}\Sigma G\right] \\
&\oplus \mathbb{Q}\left\langle f\right\rangle\left[\frac{\left(1-f^2\right)\left(1-g+g^2-g^3\right)}{8} - \mathbb{Q}\Sigma G\right] \\
&\oplus \mathbb{Q}\left\langle g\right\rangle\left[z_1 - \mathbb{Q}\Sigma G\right] \oplus \mathbb{Q}\left(g\right)\left[z_2 - \mathbb{Q}\Sigma G\right] \\
&\oplus \mathbb{Q}\left[\frac{\left(1-f+f^2-f^3\right)\left(1+g+g^2+g^3\right)}{16} - \mathbb{Q}\Sigma G\right] \\
&\oplus \mathbb{Q}\left[\frac{\left(1-f+f^2-f^3\right)\left(1-g+g^2-g^3\right)}{16} - \mathbb{Q}\Sigma G\right] \\
&\oplus \mathbb{Q}\left\langle g\right\rangle\left[\frac{\left(1-f+f^2-f^3\right)\left(1-g^2\right)}{8} - \mathbb{Q}\Sigma G\right] \\
&\cong \mathbb{Q}^3 \times \mathbb{Q}\left(i\right)^6
\end{aligned}$$

The corresponding truncated maximal order is thus isomorphic to $\mathbb{Z}^3 \times \mathbb{Z}\left(i\right)^6$ which has $2^3 \cdot 4^6 = 2^{15} = 32768$ units. A computer search of these units gives us that all units in the maximal order also in the truncated group ring are trivial. $\square$

THEOREM 59. *Suppose $G' = G \times C_4$, where $C_4 = \langle f\rangle$ and $|G| > 4$. Then if $\mathbb{Z}G_t$ and $\mathbb{Z}\left(i\right)G$ have only trivial units, then $\mathbb{Z}G'_t$ has only trivial units.*

PROOF. Suppose $\mathbb{Z}G_t$ has only trivial units; i.e,

$$xy - 1 = m\Sigma G$$

for some $m \in \mathbb{Z}$ if and only if

$$x - u = m'\Sigma G$$

for some $m' \in \mathbb{Z}$, $u = \pm g \in G$. Let

$$x = a + bf + cf^2 + df^3 + \mathbb{Z}\Sigma G\left(1+f+f^2+f^3\right) \in \mathbb{Z}G'_t$$

be a unit. Suppose $a', b', c', d' \in \mathbb{Z}G$ exist such that

$$y = a' + b'f + c'f^2 + d'f^3 + \mathbb{Z}\Sigma G\left(1 + f + f^2 + f^3\right)$$

satisfies

$$xy = 1 + \mathbb{Z}\Sigma G\left(1 + f + f^2 + f^3\right)$$

Then

$$\begin{aligned} aa' + bd' + cc' + db' + \left(ab' + ba' + cd' + dc'\right) f \\ + \left(ac' + bb' + ca' + dd'\right) f^2 + \left(ad' + bc' + cb' + da'\right) f^3 \\ + \mathbb{Z}\Sigma G\left(1 + f + f^2 + f^3\right) = 1 + \mathbb{Z}\Sigma G\left(1 + f + f^2 + f^3\right) \end{aligned}$$

or equivalently

$$\begin{aligned} aa' + bd' + cc' + db' + \left(ab' + ba' + cd' + dc'\right) f \\ + \left(ac' + bb' + ca' + dd'\right) f^2 + \left(ad' + bc' + cb' + da'\right) f^3 - 1 \\ = \frac{m}{4}\Sigma G\left(1 + f + f^2 + f^3\right) \end{aligned}$$

for some $\frac{m}{4} \in \mathbb{Z}$. This implies

$$\begin{aligned} aa' + bd' + cc' + db' - 1 &= \frac{m}{4}\Sigma G \\ ab' + ba' + cd' + dc' &= \frac{m}{4}\Sigma G \\ ac' + bb' + ca' + dd' &= \frac{m}{4}\Sigma G \\ ad' + bc' + cb' + da' &= \frac{m}{4}\Sigma G \end{aligned}$$

Since $\mathbb{Z}G_t$ and $\mathbb{Z}(i)\,G$ each have only trivial units, we have that

$$(a + b + c + d)\left(a' + b' + c' + d'\right) - 1 = m\Sigma G$$

$$(a + ib - c - id)\left(a' + ib' - c' - id'\right) - 1 = 0$$

$$(a - b + c - d)\left(a' - b' + c' - d'\right) - 1 = 0$$

$$(a - ib - c + id)\left(a' - ib' - c' + id'\right) - 1 = 0$$

so

$$a+b+c+d-u_1 = m_1\Sigma G$$

$$a+ib-c-id-u_2 = 0$$

$$a-b+c-d-u_3 = 0$$

$$a-ib-c+id-u_4 = 0$$

for some $m_1 \in \mathbb{Z}$, where $u_i = i^{b_i} g_i \in G$. Then

$$a - \frac{u_1+u_2+u_3+u_4}{4} = \left(\frac{m_1}{4}\right)$$

By definition of ΣG, we have that for all $h \in G$,

$$\left(a - \frac{u_1+u_2+u_3+u_4}{4}\right)[h] = \left(\frac{m_1}{4}\right)$$

Now suppose that there does not exist a $g \in G$ such that $g_i = g$ for all $1 \le i \le 4$. Then

$$\left(a - \frac{u_1+u_2+u_3+u_4}{4}\right)[g_i] = a\,[g_i] \pm \frac{h_i}{4}$$

where $(4, h_i) = 1$, and since $|G| > 4$, we can pick $g' \neq g_i$ for any i. Then

$$\left(a - \frac{u_1+u_2+u_3+u_4}{4}\right)\left[g'\right] = a\left[g'\right] = a\,[g_i] \pm \frac{h}{4}$$

a contradiction. Thus, the g_i are equal to g so therefore

$$a+b+c+d-i^{b_1}g = m_1\Sigma G$$

$$a+ib-c-id-i^{b_2}g = 0$$

$$a-b+c-d-i^{b_3}g = 0$$

$$a-ib-c+id-i^{b_4}g = 0$$

Note that $b_1 = 0$ or $b_1 = 2$ and that $b_3 = 0$ or $b_3 = 2$, and that $\frac{m_1}{4} \in \mathbb{Z}$ follow as consequences of the above and the fact that $a+b+c+d \in \mathbb{Z}G$, so

$$a+b+c+d \pm g = m_1\Sigma G$$

$$a+ib-c-id-i^{b_2}g = 0$$

$$a - b + c - d - i^{b_3} g = 0$$

$$a - ib - c + id - i^{b_4} g = 0$$

Adding all four rows and dividing by 4 gives

$$a + \frac{\left(\pm 1 - i^{b_2} - i^{b_3} - i^{b_4}\right)}{4} g = \frac{m_1}{4} \Sigma G$$

Then $\frac{\left(\pm 1 - i^{b_2} - i^{b_3} - i^{b_4}\right)}{4} \in \mathbb{Z}$. Without loss of generality assume the first sign is negative. Under these restrictions there are 6 cases to deal with satisfying these constraints: $\square$

Case 1. $b_2 = b_3 = b_4 = 0$. Then we have $a = g + \frac{m_1}{4} \Sigma G$ and so

$$b + c + d = \frac{3m_1}{4} \Sigma G$$
$$ib - c - id = -\frac{m_1}{4} \Sigma G$$
$$-b + c - d = -\frac{m_1}{4} \Sigma G$$
$$-ib - c + id = -\frac{m_1}{4} \Sigma G$$

Subtracting the fourth equation from the second and dividing by $2i$ gives

$$b - d = 0$$

so $b = d = \frac{m_1}{4} \Sigma G$ and $c = \frac{m_1}{4} \Sigma G$, so we have

$$\begin{aligned} a + bf + cf^2 + df^3 &= \left(g + \frac{m_1}{4} \Sigma G\right) + \frac{m_1}{4} \Sigma G f + \frac{m_1}{4} \Sigma G f^2 + \frac{m_1}{4} \Sigma G f^3 \\ &= g + \frac{m_1}{4} \Sigma G \left(1 + f + f^2 + f^3\right) \end{aligned}$$

which is a trivial unit modulo $\frac{m_1}{4} \Sigma G \left(1 + f\right)$

Case 2. $b_2 = 1$, $b_3 = 2, b_4 = 3$ Then we have $a = \frac{m_1}{4} \Sigma G$ so

$$b + c + d - g = \frac{3m_1}{4} \Sigma G$$
$$ib - c - id - ig = -\frac{m_1}{4} \Sigma G$$
$$-b + c - d + g = -\frac{m_1}{4} \Sigma G$$
$$-ib - c + id + ig = -\frac{m_1}{4} \Sigma G$$

Subtracting the fourth equation from the second and dividing by $2i$ gives

$$b - d - g = 0$$

so $c = \frac{m_1}{4}\Sigma G$ and the equations become

$$\begin{aligned} b + d - g &= \frac{m_1}{2}\Sigma G \\ b - d - g &= 0 \\ -b - d + g &= -\frac{m_1}{2}\Sigma G \end{aligned}$$

so $b = \frac{m_1}{4}\Sigma G + g$ and $d = \frac{m_1}{4}\Sigma G$. We thus have

$$\begin{aligned} a + bf + cf^2 + df^3 &= \frac{m_1}{4}\Sigma + \left(g + \frac{m_1}{4}\right)\Sigma G f + \frac{m_1}{4}\Sigma G f^2 + \frac{m_1}{4}\Sigma G f^3 \\ &= gf + \frac{m_1}{4}\Sigma G\left(1 + f + f^2 + f^3\right) \end{aligned}$$

Case 3. $b_2 = 3$, $b_3 = 2$, $b_4 = 1$. Then we have $a = \frac{m_1}{4}\Sigma G$ so

$$\begin{aligned} b + c + d - g &= \frac{3m_1}{4}\Sigma G \\ ib - c - id + ig &= -\frac{m_1}{4}\Sigma G \\ -b + c - d + g &= -\frac{m_1}{4}\Sigma G \\ -ib - c + id - ig &= -\frac{m_1}{4}\Sigma G \end{aligned}$$

We immediately have that $c = \frac{m_1}{4}\Sigma G$, so the equations become

$$\begin{aligned} b + d - g &= \frac{m_1}{2}\Sigma G \\ b - d + g &= 0 \\ -b - d + g &= -\frac{m_1}{2}\Sigma G \\ -b + d - g &= 0 \end{aligned}$$

so $b = \frac{m_1}{4}\Sigma G$ and $d = \frac{m_1}{4}\Sigma G + g$. We thus have

$$\begin{aligned} a + bf + cf^2 + df^3 &= \frac{m_1}{4}\Sigma G + \frac{m_1}{4}\Sigma G f + \frac{m_1}{4}\Sigma G f^2 + \left(g + \frac{m_1}{4}\right)\Sigma G f^3 \\ &= gf^3 + \frac{m_1}{4}\Sigma G\left(1 + f + f^2 + f^3\right) \end{aligned}$$

Case 4. $b_2 = 2, b_3 = 2,\ b_4 = 0$. Then we have $a = \frac{m_1}{4}\Sigma G$ so

$$\begin{aligned} b + c + d - g &= \frac{3m_1}{4}\Sigma G \\ ib - c - id + g &= -\frac{m_1}{4}\Sigma G \\ -b + c - d + g &= -\frac{m_1}{4}\Sigma G \\ -ib - c + id - g &= -\frac{m_1}{4}\Sigma G \end{aligned}$$

so $c = \frac{m_1}{4}\Sigma G$ and the equations become

$$\begin{aligned} b + d - g &= \frac{m_1}{2}\Sigma G \\ ib - id + g &= 0 \end{aligned}$$

or

$$\begin{aligned} b + d - g &= \frac{m_1}{2}\Sigma G \\ b - d - ig &= 0 \end{aligned}$$

contradicting that b and d are in $\mathbb{Z}G$.

Case 5. $b_2 = 2, b_3 = 0,\ b_4 = 2$. Then we have $a = \frac{m_1}{4}\Sigma G$ so

$$\begin{aligned} b + c + d - g &= \frac{3m_1}{4}\Sigma G \\ ib - c - id + g &= -\frac{m_1}{4}\Sigma G \\ -b + c - d - g &= -\frac{m_1}{4}\Sigma G \\ -ib - c + id + g &= -\frac{m_1}{4}\Sigma G \end{aligned}$$

so $c = g + \frac{m_1}{4}\Sigma G$, $b = d = \frac{m_1}{4}\Sigma G$, and we have that

$$\begin{aligned} a + bf + cf^2 + df^3 &= \frac{m_1}{4}\Sigma + \frac{m_1}{4}\Sigma G f + \left(g + \frac{m_1}{4}\Sigma G f^2\right) + \frac{m_1}{4}\Sigma G f^3 \\ &= gf^2 + \frac{m_1}{4}\Sigma G\left(1 + f + f^2 + f^3\right) \end{aligned}$$

Case 6. $b_2 = 0, b_3 = 2, b_4 = 2$. Then we have $a = \frac{m_1}{4}\Sigma G$ so

$$b + c + d - g = \frac{3m_1}{4}\Sigma G$$

$$ib - c - id - g = -\frac{m_1}{4}\Sigma G$$
$$-b + c - d + g = -\frac{m_1}{4}\Sigma G$$
$$-ib - c + id + g = -\frac{m_1}{4}\Sigma G$$

so $c = \frac{m_1}{4}\Sigma G$ and the equations become

$$b + d - g = \frac{m_1}{2}\Sigma G$$
$$ib - id - g = 0$$

or

$$b + d - g = \frac{m_1}{2}\Sigma G$$
$$b - d + ig = 0$$

contradicting that b and d are in $\mathbb{Z}G$.

Since all cases have been covered, the proof is complete.

Appendix: Sage Code

The following are listings of the SageMath code used to calculate the base cases in Chapter 5 for $n = 3$ and $n = 4$. This consists of a file `truncated_group_rings.sage`, which serves as a library for working with truncated group rings and the elements thereof, and the actual commands used to perform the calculations in this paper. A Git repository containing this code can be found at `https://github.com/mathlover2/truncated-group-rings`. Please note that this code is rather slow at the time of this writing.

```
## Begin file: truncated_group_rings.sage
from itertools import islice, product as iprod
from operator import add

## Code for the truncating ideal

def _reducer(x,R,G,sigma_element):


    # Gives $\sum_{g \in G} \left| \left\[ x \right\]_{g} \right|}$.

    def weight(v):
        return sum(abs(x) for x in v.coefficients(False))

    def length(v):
        return v.length()

    def val_ident(v):
        return -abs(v.coefficient(G.identity()))
```

```
    def weed_out(f, l):
        m = f(min(l, key=f))
        return [v for v in l if f(v) == m]

    n = length(x)
    coeffs = sorted(x.coefficients())
    n1 = len(coeffs)

    # A simple case of x being already reduced.
    if 2*n1 < n:
        return x

    else:
        coeffs = set(coeffs) | {0}
        candidate_reductions = [x - y*sigma_element for y in coeffs]
        for weeder_function in [length,  weight, val_ident]:
            candidate_reductions = weed_out(weeder_function,
                                            candidate_reductions)
            if len(candidate_reductions) == 1:
                return candidate_reductions[0]
        return x - x.coefficient(G.identity())*sigma_element



def TruncatingIdeal(group_ring):
    sigma_element = sum(group_ring.basis())
    I = group_ring.ideal([sigma_element])
    I.sigma_element = sigma_element
    def reduce(self, x):
        return _reducer(group_ring(x), self.base_ring(),
```

```
                        self.ring().group(), self.sigma_element)
    I.reduce = reduce.__get__(I)
    return I

def _reducer_2(x, R, G, sigma_element):
    # Alternative version of _reducer_. Works but isn't as pretty.
    ident = G.identity()
    xx = x - x.coefficient(ident) * sigma_element
    return xx

def TruncatingIdeal_quick(group_ring):
    sigma_element = sum(group_ring.basis())
    I = group_ring.ideal([sigma_element])
    I.sigma_element = sigma_element
    def reduce(self, x):
        return _reducer_2(group_ring(x), self.base_ring(),
                        self.ring().group(), self.sigma_element)
    I.reduce = reduce.__get__(I)
    return I
## end file
```

The commands for the calculation.

```
## begin file
load('truncated_group_rings.sage')
from itertools import product as iprod
class TGRExample(object):
    def __init__(self, G, R):
        self.G = G
        self.R = R
        self.RG = self.G.algebra(self.R)
        self.I = TruncatingIdeal(self.RG)
        self.Iq = TruncatingIdeal_quick(self.RG)
```

```
        self.RGt = QuotientRing(self.RG, self.I)
        self.RGtq = QuotientRing(self.RG, self.Iq)
        self.fs = self.RG.gens()
        self.fts = self.RGt.gens()
        self.sigma = self.I.gen()

Qw = CyclotomicField(3)
Qi = CyclotomicField(4)
QC3 = TGRExample(AbelianGroup([3]), QQ)
QC3C2 = TGRExample(AbelianGroup([3,2]), QQ)
QC3C3 = TGRExample(AbelianGroup([3,3]), QQ)
QwC3C3 = TGRExample(AbelianGroup([3,3]), Qw)
QwC3C2 = TGRExample(AbelianGroup([3,2]), Qw)
QiC4C4 = TGRExample(AbelianGroup([4,4]), Qi)
w = Qw.gen()
f, g = QwC3C3.fts
basis = [(1+f+f^2) * (1/3), (1+g+g^2) * (1/3),
         (1+f^2*g+f*g^2) * (1/3), (1+f*g+f^2*g^2) * (1/3)]
for units in iprod([1,g,g^2,-1,-g,-g^2], [1,f,f^2,-1,-f,-f^2],
                   [1,f,f^2,-1,-f,-f^2],[1,f,f^2,-1,-f,-f^2]):
    z = (sum(map(lambda x,y: x*y, units, basis)))
    if all(c in ZZ for c in QwC3C3.RGt.lift(z).coefficients()):
        show(z)
f, g = QiC4C4.fts
ii = Qi.gen()
z1 = (1 + ii*f - f^2 - ii*f^3)*(1 + ii*g - g^2 - ii*g^3) \
        + (1 - ii*f - f^2 + ii*f^3)*(1 - ii*g - g^2 + ii*g^3)
z2 = (1 - ii*f - f^2 + ii*f^3)*(1 + ii*g - g^2 - ii*g^3) \
        + (1 + ii*f - f^2 - ii*f^3)*(1 - ii*g - g^2 + ii*g^3)
basis = [(1+f+f^2+f^3)*(1-g+g^2-g^3) * (1/16),
         (1+f+f^2+f^3)*(1-g^2) * (1/8),
```

```
        (1+g+g^2+g^3)*(1-f^2) * (1/8),
        (1-g+g^2-g^3)*(1-f^2) * (1/8),
        z1 * (1/16),
        z2 * (1/16),
        (1-f+f^2-f^3)*(1+g+g^2+g^3) * (1/16),
        (1-f+f^2-f^3)*(1-g+g^2-g^3) * (1/16),
        (1-f+f^2-f^3)*(1-g^2) * (1/8)]
for units in iprod([1,-1], [1,g,-1,-g], [1,f,-1,-f], [1,f,-1,-f],
                   [1,g,-1,-g], [1,g,-1,-g], [1,-1],
                   [1,-1], [1,g,-1,-g]):
    z = (sum(map(lambda x,y: x*y, units, basis)))
    if all(c.is_integer()
           for c in QiC4C4.RGt.lift(z).coefficients()):
        show(z)
## End file
```

Bibliography

[Higman] Graham Higman. "The Units of Group Rings". Proc. London Math. Soc., (2)46, (1940), 231–248.

[Herm-Li] Allen Herman and Yuanlin Li. *Trivial Units for Group Rings over Rings of Algebraic Integers.* Proceedings of the American Mathematical Society, Vol. 134, No. 3 (Mar. 2006), pp. 631–635.

[Herm-Li-Par] Allen Herman, Yuanlin Li, and M. M. Parmenter. *Trivial Units for Group Rings with G-adapted Coefficient Rings.* Canad. Math. Bull. Vol. 48 (1), 2005, pp. 80–89.

[Wedderburn] J. H. M. Wedderburn. *Lectures on Matrices.* American Mathematical Society Colloquium Publications, Vol. 17, 1934, pp. 158–168.

[MT-LJM] Martin Taylor. *Classgroups of Group Rings.* London Mathematical Society Lecture Note Series, 91, (1984).

[Guzman] Maxine Guzman. *Swan Modules of Elementary Abelian 2-Groups over Quadratic Imaginary Fields.* Ph.D. Thesis, State University of New York at Albany, 2015.

[GRRS] Cornelius Greither, Daniel R. Replogle, Karl Rubin and Anupam Srivastav. *Swan modules and Hilbert–Speiser number fields.* Journal of Number Theory, 79 (1999), pg. 164–173.

[Ullom] S. Ullom. *Nontrivial Lower bounds for class groups of integral group rings.* Illinois Journal Mathematics 20 (1976), 361-371.