TRIVIAL UNITS IN \( RG \)

By

**Jürgen Ritter**
Institut für Mathematik, Universität Augsburg, 86135 Augsburg, Germany

and

**Sudarshan K. Sehgal**
Department of Mathematical and Statistical Sciences, University of Alberta, Edmonton-Alberta T6G 2G1, Canada

[Received 12 August 2003. Read 21 August 2004. Published 11 March 2005.]

**Abstract**

A characterisation of group rings \( RG \) with trivial units is given when \( R \) is a \( G \)-adapted ring. A formula for the rank of the centre of \( \mathcal{U}(\mathbb{Z}G) \) is given. A characterisation of \( RG \) with trivial central units is given for some \( G \)-adapted rings \( R \).

1. Introduction

Let \( \mathbb{Z}G \) be the integral group ring of a finite group \( G \). It is a classical result of G. Higman [5; 9, p. 57] that the unit group of \( \mathbb{Z}G \) is trivial if and only if \( G \) is abelian of exponent 2, 3, 4 or 6 or is a Hamiltonian 2-group. A unit of \( RG \) is said to be trivial if it is of the form \( rg, r \in R, g \in G \). Thus the trivial units of \( \mathbb{Z}G \) are simply \( \pm g, g \in G \). It is also known that central units of \( \mathbb{Z}G \) are trivial if and only if \( G \) satisfies the following condition [8]:

\[
(j, |G|) = 1 \Rightarrow g^j \sim g^\varepsilon, \quad \varepsilon = \pm 1 \quad (\forall g \in G). \tag{1.1}
\]

This result has been extended to arbitrary groups in [3].

The purpose of this paper is threefold. First, we extend the Higman result to \( G \)-adapted rings of coefficients. A ring \( R \) is said to be \( G \)-adapted if it is an integral domain of characteristic zero and if no prime divisor of \( |G| \) is contained in the unit group \( R^\times \) of \( R \). Recently, Hertweck [4] has studied central units of \( RG \) for arbitrary \( G \) and \( G \)-adapted \( R \). Our rings \( R \) will be \( G \)-adapted and \( G \) will be finite throughout this paper.

The second result computes the rank of the group of central units of \( \mathbb{Z}G \). The special case when \( G \) is abelian is due to Ayoub and Ayoub see [1; 9, p. 54]. Also, as a corollary we see the classification of groups with trivial central units in \( \mathbb{Z}G \).

Finally, imposing a further assumption on \( R \), we extend the trivial central units result to \( RG \).

*Corresponding author; e-mail: sehgal@ualberta.ca

The concrete statements are these:

**Theorem 1.** Suppose that $R$ is $G$-adapted and that $G$ is a finite group. Then $\mathcal{U}(RG)$ is trivial if and only if one of the following holds:

1. $G$ is abelian of exponent 2, and $R_2^\times = \{a \in R^\times : a \equiv 1 \pmod{2}\}$ is torsion.
2. $G$ is abelian of exponent 3, and $R_3^\times = \{u = a + b\omega \in R[\omega] : u \equiv 1 \pmod{\pi}, a^2 + b^2 - ab \in R^\times\}$ is torsion. Here, $\omega$ is a primitive 3rd root of unity and $\pi = \omega - 1$.
3. $G$ is abelian of exponent 4, and $R_4^\times = \{u = a + bi \in R[i] : u \equiv 1 \pmod{i - 1}, a^2 + b^2 \in R^\times\}$ is torsion.
4. $G$ is abelian of exponent 6, and $R_3^\times$ and $R_2^\times$ are torsion.
5. $G$ is a Hamiltonian 2-group, $G = Q_8 \times E$, where $Q_8$ is the quaternion group of order 8 and $E$ is an elementary abelian 2-group and the following three conditions are satisfied:
   a. the field $K$ of quotients of $R$ has no solution to the equation $x^2 + y^2 + z^2 = -1$
   b. $R_2^\times$ is torsion
   c. the kernel of the norm map $R[i, j, k] \to R$, $N(a + bi + cj + dk) = a^2 + b^2 + c^2 + d^2$ is torsion.

**Theorem 2.** The rank $\rho = \rho(\mathcal{U}(RG))$ of the centre of the unit group of the integral group ring of a finite group $G$ is given by

$$\rho = \frac{1}{2} (c - 2h,Q + h,R)$$

where $c$ is the number of conjugacy classes in $G$, $h,Q$ is the number of $\mathbb{Q}$-conjugate classes in $G$ and $h,R$ is the number of real classes in $G$.

**Theorem 3.** Let $R$ be $G$-adapted. Suppose that the unit group $(R \otimes \mathbb{Z}[\chi(G)]^\times / |G|)^\times$ is torsion. Then $\mathcal{U}(RG)$ is trivial if and only if $(R \otimes \mathbb{Z}[\chi])^\times$ is torsion for all complex characters $\chi$.

Our notations are standard as in [10]. As has been said already, our ring $R$ is $G$-adapted throughout. We set $K = \text{Quot}(R)$ for its field of fractions. We denote by $\zeta_n$ a primitive $n$th root of unity, and we write $\omega = \zeta_3$, $\pi = \omega - 1$ and $i = \zeta_4$. Also, $R^\times$ denotes the group of units of $R$. By $\mathcal{U}(RG)$, $\mathcal{U}_1(RG)$ we mean the groups of units of $RG$, respectively of units of $RG$ having augmentation one. The cyclic group of order $n$ will be denoted by $C_n$. It needs to be mentioned that $R[\omega]$ is the subring of the field $K(\omega)$ consisting of elements $a + b\omega$, $a, b \in R$. This representation is not necessarily unique, since $\omega$ may be contaiomed in $K$. When we consider a set $S = \{u = a + b\omega \in R[\omega] : u$ has property $P\}$ we simply understand the set of all those $u$ that have a representation satisfying property $P$. 


2. Some lemmas

We collect some known results and prove preliminary lemmas. The following result and its corollaries are well known.

**Lemma 2.1.** If $R$ is a $G$-adapted ring and $u = \sum u(g)g \in U(RG)$ is a torsion element with $u_1 \neq 0$ then $u = u_1$.

**Proof.** See [9, corollary 1.4, p. 45]. □

**Corollary 2.2.** If $R$ is a $G$-adapted ring, then any torsion central unit of $RG$ is of the form $rg$, $r \in R$, $g \in G$.

**Corollary 2.3.** Let $V$ be a finite subgroup of $U_1(RG)$, the group of augmentation one units, then $|V|$ is a divisor of $|G|$.

**Proof.** Let $e = \frac{1}{|V|} \sum_{v \in V} v$. Then $e = e^2 \in KG$, where $K$ is the field of quotients of $R$. We compute the trace of the matrix of the regular representation of $e$. We see by Lemma 2.1 that

$$\text{tr}(e) = \frac{1}{|V|} \sum_{v \in V} \text{tr}(v) = \frac{1}{|V|} \text{tr}(1) = \frac{|G|}{|V|}.$$ 

On the other hand, this trace is an integer. So $|V|$ is a divisor of $|G|$ as claimed. □

**Lemma 2.4.** $R^\times_1 = \{ a + b\omega \in R[\omega] : a + b\omega \equiv 1 (\text{mod } \pi), a^2 - ab + b^2 \in R^\times \}$ is a subgroup of $R[\omega]^\times$.

**Proof.** This is directly checked. The inverse of $a + b\omega$ is $c(a - b) - cb\omega$ with $c = (a^2 - ab + b^2)^{-1}$; the product of $a + b\omega, c + d\omega \in R^\times_1$ is $(ac - bd) + (ad + bc - bd)\omega$, and $(ac - bd)^2 - (ac - bd)(ad + bc - bd) + (ad + bc - bd)^2 = (a^2 - ab + b^2)(c^2 - cd + d^2)$. Note that only $\omega^2 = -1 - \omega$ is used and not that $\omega \mapsto \omega^2$ induces an automorphism of $R[\omega]$, which need not be true. □

Similarly, we have

**Lemma 2.5.** $R^\times_4 = \{ a + bi \in R[i] : a + bi \equiv 1 (\text{mod } i - 1), a^2 + b^2 \in R^\times \}$ is a subgroup of $R[i]^\times$.

We shall implicitly be using the next result throughout.

**Lemma 2.6.** Suppose that the ring $S$ is an integral extension of $R$. Suppose $u \in R$ has an inverse in $S$. Then $u$ has an inverse in $R$.

**Proof.** If $u$ was not in $R^\times$, then $u \in \mathfrak{p}$ for some prime ideal $\mathfrak{p}$ of $R$ and thus, by [7, proposition 9, p. 9], also in $\mathfrak{P}$ for some prime ideal $\mathfrak{P}$ of $S$, which is a contradiction. □
Lemma 2.7. Suppose that $R$ is $G$-adapted. Then $\mathcal{U}(RC_2)$ is trivial if and only if $R_2^\times = \{u \in R^\times : u \equiv 1 (\text{mod } 2)\}$ is torsion.

Proof. Write $C_2 = \langle x \rangle$. Then we have an embedding
\[
\lambda : RC_2 \to R \oplus R, \quad \lambda(x) = (1, -1).
\]
a) ($\Rightarrow$) Suppose $\mathcal{U}(RC_2)$ is trivial. Then $\mathcal{U}_1(RC_2) = C_2$. Suppose we have an element $u$ of infinite order in $R_2^\times$. Let $\gamma = \frac{1+u}{2} + \frac{1-u}{2} x \in RC_2$. Then $\lambda(\gamma) = (1, u)$. Therefore, $\mathcal{U}(RC_2)$ has an element of infinite order, which is a contradiction, proving this implication.

b) ($\Leftarrow$) Let $\gamma \in \mathcal{U}_1(RC_2)$. Write $\gamma = a + bx$. Then $\lambda(\gamma) = (a + b, a - b) = (1, a - b)$. Therefore, $a - b$, which is $\equiv 1 (\text{mod } 2)$, is a unit of $R$. By assumption, it is torsion. Thus there exists an integer $k$ so that $\lambda(\gamma^k) = 1$, and therefore $\gamma^k = 1$. It follows by Lemma 2.1 that $\gamma \in C_2$, as desired. \hfill \blacksquare

Lemma 2.8. Suppose that $R$ is $G$-adapted. Then $\mathcal{U}(RC_3)$ is trivial if and only if $R_3^\times = \{u = r + s\omega \in R[\omega] : u \equiv 1 (\text{mod } \pi), r^2 - rs + s^2 \in R^\times\}$ is torsion.

Proof. ($\Rightarrow$) Assume that $\mathcal{U}(RC_3)$ is trivial. Suppose we have in $R_3^\times$ an element $u \equiv 1 (\text{mod } \pi)$, $u = A + B\omega$, $A, B \in R$, $A^2 - AB + B^2 \in R^\times$, and $o(u) = \infty$ (i.e., order of $u$ is infinite). Let $C_3 = \langle x \rangle$. Consider the embedding
\[
\lambda : RC_3 \to R \oplus R[\omega] \oplus R[\omega], \quad \lambda(x) = (1, \omega, \omega^2).
\]
Indeed, if $a + bx + cx^2 \mapsto 0$, then $a + b + c = 0$, $(a - c) + (b - c)\omega = 0 = (a - b) + (c - b)\omega$, so $a - c = b - a = -c - a - a$, and $a = 0 = b = c$ follows.

Now, $u^3 = A_1 + B_1\omega$ with $A_1 = A^3 + B^3 - 3AB^2$, $B_1 = 3(A^2B - AB^2)$. Let us find the preimage of $(1, u^3, A_1 + B_1\omega^2)$ under $\lambda$. We wish to find $a, b, c \in R$ so that $\lambda(a + bx + cx^2) = (1, u^3, x)$, $x = A_1 + B_1\omega^2$. Remember that $u \equiv 1 (\text{mod } \pi)$ gives $u^3 \equiv 1 (\text{mod } \pi^3)$, and so $u^3 \equiv 1 (\text{mod } 3)$. It follows that $A_1 \equiv 1 (\text{mod } 3)$. Then the elements
\[
a + b + c = 1, \quad a + b\omega + c\omega^2 = A_1 + B_1\omega, \quad a + b\omega^2 + c\omega = A_1 + B_1\omega^2 = x.
\]
Set $\gamma = a + bx + cx^2$. Then $\lambda(\gamma) = (1, u^3, x)$. Since $u^3 \in R_3^\times$, $u^3x \equiv A_1^2 - A_1B_1 + B_1^2 \in R^\times$. It follows that $x \in R[\omega]^\times$ as well. Also, $x = A_1 + B_1\omega^2 = (A_1 - B_1) - B_1\omega \in R_3^\times$.

Then we can find $\mu \in RC_3$ so that $\lambda(\mu) = (1, u^{-3}, x^{-1})$. It follows that $\gamma$ is a unit of $RC_3$ having augmentation one and infinite order. This is a contradiction, proving this implication.

($\Leftarrow$) Let $\gamma = a + bx + cx^2 \in \mathcal{U}_1(RC_3)$. Then
\[
\gamma = a + bx + cx^2 \mapsto (a + b + c, a + b\omega + c\omega^2, a + b\omega^2 + c\omega).
\]
In fact,
\[ \lambda(y) = (1, 2a + b - 1 + (a + 2b - 1)\omega, 2a + b - 1 + (a + 2b - 1)\omega^2) = (1, u, v), \]

where \( u, v \) are units of \( R[\omega] \). Also, \( u \equiv 1 \pmod{\pi} \) and \( v \equiv 1 \pmod{\pi} \). Moreover, \( u \) and \( v \) are units of \( R[\omega] \), and thus \( uv \) (being an element of \( R \)) is in \( R^* \) by Lemma 2.6. Hence \( u, v \in R_3^* \). Thus \( u \) and \( v \) are torsion and hence \( \gamma \) is torsion. Since \( R \) is \( G \)-adapted, \( \gamma \in C_3 \), as desired. \( \blacksquare \)

3. The quaternion group \( Q_8 \) of order 8

In this section we characterise when \( RQ_8 \) has trivial units only. We fix notation. \( R \) is a \( G \)-adapted ring and \( K \) is its field of quotients. Also,

\[ Q_8 = \langle x, y : x^4 = y^4 = 1, xy = x^{-1} \rangle. \]

We have

**Proposition 3.1.** \( U_1(RQ_8) = Q_8 \iff \) the three conditions below are satisfied:

1. \( R_2^2 = \{ u \in R^* : u \equiv 1 \pmod{2} \} \) is torsion, and
2. the kernel of the norm map \( N[i, j, k] \rightarrow R \) given by \( N(a + bi + cj + dk) = a^2 + b^2 + c^2 + d^2 \), is torsion. Here, \( i, j, k \) are the usual quaternions in the division ring \( \mathbb{H}_K = K \otimes \mathbb{Q} \mathbb{H}_0 \supset R \otimes \mathbb{Z}[i, j, k] = R[i, j, k] \).

**Proof.** Note that due to 0) \( \mathbb{H}_K \) is a division ring.

(a) \( \Rightarrow \) If \( K \) has a solution as in 0), then \( KQ_8 \) splits [9, p. 169] and contains nontrivial nilpotent elements. By removing denominators we can assume that \( RQ_8 \) has a nonzero element \( \eta \) with \( \eta^2 = 0 \). Then \( 1 + \eta \) is a unit of \( RQ_8 \). By assumption, \( 1 + \eta = g \) and \( (g - 1)^2 = 0 \). This gives \( g = 1 \) and \( \eta = 0 \), a contradiction, proving 0).

Since \( RC_2 \subset RQ_8 \) we have 1) by Lemma 2.7. It remains only to prove 2). The isomorphism \( KQ_8 \simeq K \oplus K \oplus K \oplus K \oplus \mathbb{H}_K \) induces an injection

\[ \lambda : RQ_8 \rightarrow R \oplus R \oplus R \oplus R \oplus R[i, j, k] \]

\[ \lambda(x) = (1, 1, -1, -1, i), \quad \lambda(y) = (1, -1, 1, -1, j). \]

Suppose we have \( u = a + bi + cj + dk \in R[i, j, k] \), \( a^2 + b^2 + c^2 + d^2 = 1 \) and \( o(u) = \infty \).

We observe that \( u^2 = a^2 - b^2 - c^2 - d^2 + 2abi + 2acj + 2adk \), so that the coefficients of \( i, j, k \) in \( u^2 \) are \( \equiv 0 \pmod{2} \) and the first coefficient is \( \equiv 1 \pmod{2} \). Replace \( u \) by \( u^2 \). We want to lift \( u \) to \( \gamma \in RQ_8 \) with augmentation one. Write \( \gamma = (a_0 + a_1 x + a_2 x^2 + a_3 x^3 + b_1 y + b_2 y^3 + c_1 xy + c_2 x^3 y) \in RQ_8 \). Then

\[ \lambda(\gamma) = (a_0 + a_1 + a_2 + a_3 + b_1 + b_2 + c_1 + c_2, a_0 + a_1 + a_2 + a_3 - b_1 - b_2 - c_1 - c_2, a_0 - a_1 + a_2 - a_3 + b_1 + b_2 - c_1 - c_2, a_0 - a_1 + a_2 - a_3 - b_1 - b_2 + c_1 + c_2, (a_0 - a_2) + (a_1 - a_3)i + (b_1 - b_2)j + (c_1 - c_2)k). \]

We wish to solve for \( \gamma \in U_1(RQ) \) the equation \( \lambda(\gamma) = (1, 1, 1, 1, u) \). The augmented matrix of this system of linear equations in \( a_0, a_1, a_2, a_3, b_1, b_2, c_1, c_2 \) is
We consider the two cases separately.

If we now take a unit $g$ of infinite order. Since the first four components of $g$ is torsion. Hence it follows by the assumption 1) that $g$ has infinite order, this is a contradiction, proving 2).

(b) $\equiv$ First, we show that $U_1(RQ_8)$ is torsion. Suppose there exists a $\gamma \in U_1(RQ_8)$ of infinite order. Since the first four components of $\lambda(\gamma)$ can be viewed as the components of $\overline{\gamma}$ in $R(Q_8/\mathcal{Q})$, we have $\lambda(\gamma) = (1, \pm 1, \pm 1, \pm 1, \pm 1)$. Replace $\gamma$ by $\gamma^2$ to obtain

$$\lambda(\gamma) = (1, 1, 1, 1, u), \quad u = (a_0 - a_2) + (a_1 - a_3)i + (b_1 - b_2)j + (c_1 - c_2)k,$$

where $\gamma = a_0 + a_1x + a_2x^2 + a_3x^3 + b_1y + b_2y^2 + c_1xy + c_2x^2y \in U_1(RQ_8)$. Also, $a_0 + a_1 + a_2 + a_3 + b_1 + b_2 + c_1 + c_2 = 1$. Then

$$N(u) = (a_0 - a_2)^2 + (a_1 - a_3)^2 + (b_1 - b_2)^2 + (c_1 - c_2)^2$$

$$= \sum a_i^2 \pm \sum b_i^2 \pm \sum c_i^2 \equiv 1 \pmod{2}.$$

It follows by the assumption 1) that $N(u^k) = 1$, which implies by 2) that $u^k$ is torsion. Hence $\gamma$ is of finite order, which is a contradiction.

If we now take a unit $\gamma \in U_1(RQ_8)$, then $o(\gamma)$ must divide 8 by Corollary 2.3, but it can not be 8 (as $RQ_8$ is non-commutative). Thus we may suppose that $o(\gamma) = 2$ or 4. We consider the two cases separately.

\[
\begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 \\
1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 \\
1 & 0 & -1 & 0 & 0 & 0 & 0 & a \\
0 & 1 & 0 & -1 & 0 & 0 & 0 & b \\
0 & 0 & 0 & 0 & 1 & -1 & 0 & c \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & -1
\end{bmatrix}
\]

which is equivalent to

\[
\begin{bmatrix}
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
1 & 0 & -1 & 0 & 0 & 0 & 0 & a \\
0 & 1 & 0 & -1 & 0 & 0 & 0 & b \\
0 & 0 & 0 & 0 & 1 & -1 & 0 & c \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & -1
\end{bmatrix}
\]

This gives the equations

\[
\begin{align*}
a_0 + a_2 &= 1, \quad a_0 - a_2 &= a \\
b_1 + b_2 &= 0, \quad b_1 - b_2 &= c \\
c_1 + c_2 &= 0, \quad c_1 - c_2 &= d \\
a_1 + a_3 &= 0, \quad a_1 - a_3 &= b.
\end{align*}
\]

These can be solved as $b, c, d \equiv 0 \pmod{2}$ and $a \equiv 1 \pmod{2}$. The element $\gamma$ is a unit, as $(1, 1, 1, 1, u^{-1})$ can also be lifted. Because $\gamma$ has infinite order, this is a contradiction, proving 2).
(i) Suppose \( o(\gamma) = 2 \). If \( \lambda(\gamma) = (1, 1, 1, 1, \ast) \), then \( \ast = -1 \) and \( \gamma = x^2 \). Otherwise, \( \lambda(\gamma) = (1, -1, -1, 1, \pm 1) \) is a typical expression—the middle triple might be \((1, -1, -1)\) or \((-1, 1, -1)\). We choose an element \( g \in Q_8 \) of order 4 so that \( \lambda(\gamma g) = (1, 1, 1, 1, u) \) with \( o(u) = 4 \); in the expression this is given by \( g = xy \) and \( u = k \).

We claim

\[
\text{if } o(u) = 4 \text{ then } (1, 1, 1, 1, u) \text{ has no preimage.} \tag{3.1}
\]

Since \( K[i, j, k] \) is a division ring, \( u^2 = -1 \). Write \( u = a + bi + cj + dk \). Then

\[
a^2 - b^2 - c^2 - d^2 + 2abi + 2acj + 2adk = -1.
\]

It follows that \( a^2 - b^2 - c^2 - d^2 = -1, 0 = ab = ac = ad \). Thus either \( a \neq 0, b = 0 = c = d \), \( a^2 = -1 \) or \( a = 0 \) and \( b^2 + c^2 + d^2 = 1 \). The first case is not possible due to 0).

We are left with the possibility \( b^2 + c^2 + d^2 = 1 \); \( (1, 1, 1, 1, u) = \lambda(\gamma), u^2 = -1 \). If we could solve this for \( \gamma \) then it follows from the equation (1.1) that \( b, c \) and \( d \) are \( \equiv 0(\mod 2) \). This contradiction completes the proof in this case.

(ii) It remains to consider the case when \( o(\gamma) = 4 \). We know from (3.1) that \( \lambda(\gamma) \neq (1, 1, 1, 1, \ast) \). Then a typical expression for \( \lambda(\gamma) \) is \( \lambda(\gamma) = (1, -1, -1, 1, u) \). Then \( \lambda(\gamma \text{xy}) = (1, 1, 1, 1, uk) \).

We have \( N(u)^4 = 1 = N(uk)^4 \). It follows that \( uk \) is torsion. The situation is \( \lambda(\gamma \text{xy}) = (1, 1, 1, 1, uk) \). As before, \( o(u) \) can be 1, 2 or 4. It follows by (3.1) that \( o(uk) \neq 4 \). If \( uk = 1 \) then \( \gamma \in Q_8 \). If \( o(uk) = 2 \) then \( uk = -1 \) and \( \lambda(\gamma \text{xy}) = (1, 1, 1, 1, -1) \). It follows that \( \gamma \text{xy} = x^2 \) and \( \gamma \in Q_8 \). This completes the proof of the proposition. \( \square \)

4. Proof of Theorem 1

We know from Higman’s theorem (see [9, p. 57]) that \( U(\mathbb{Z} G) \) is trivial if and only if one of the following holds:

1. \( G \) is abelian of exponent 2, 3, 4 or 6;
2. \( G = E \times Q_8 \) where \( E \) is an elementary abelian 2-group.

We have to find necessary and sufficient conditions on the \( G \)-adapted ring \( R \) so that \( U(RG) \) is trivial for the groups in Higman’s theorem. We have already taken care of some of the basic groups in Sections 2 and 3. We also need to handle \( C_4 \), which we do below.

**Lemma 4.1.** \( U_1(RC_4) = C_4 \iff R_4^* = \{ u = x_1 + x_2 i \in R[i], \ u \equiv 1 \mod (i - 1), \ x_1^2 + x_2^2 \in R^* \} \) is torsion.

**Proof:**

(a) \( \Rightarrow \) Write \( C_4 = \langle x \rangle \). We have an injection

\[
\lambda : RC_4 \to R \oplus R \oplus R[i] \oplus R[i]
\]

given by \( \lambda(x) = (1, -1, i, -i) \). Suppose we have \( u = x_1 + x_2 i \in R_4^* \) of infinite order. Note that \( u^2 \equiv 1(\mod 2) \) by \( (i - 1)^2 = -2i \). So \( u^2 = x_1^2 - x_2^2 + 2x_1x_2i \equiv 1(\mod 2) \).
and consequently, \( x_1^2 - x_2^2 \equiv 1 \pmod{2} \). Replace \( u \) by \( u^2 \) to assume
\[
u = x + \beta \implies x \equiv 1 \pmod{2} \quad \text{and} \quad \beta \equiv 0 \pmod{2}.
\]

We solve \( \gamma = a + bx + cx^2 + dx^3 \) with \( \lambda(\gamma) = (1, 1, x + \beta i, x - \beta i) \), namely, by taking \( a = \frac{x+1}{2}, b = \beta / 2, c = \frac{x-1}{2}, d = -\beta / 2 \) all in \( R \). Then \( \gamma \in \mathcal{U}_1(RC_4) \), as similarly \( (1, 1, (x + \beta i)^{-1}, (x - \beta i)^{-1}) \) can be lifted. Also, \( \sigma(\gamma) \) is infinite, which is a contradiction, proving the implication.

(b) \( \Leftarrow \) Let \( \gamma = a + bx + cx^2 + dx^3 \in \mathcal{U}_1(RC_4) \). Going modulo \( C_2 \) we have \( RC_4 \rightarrow (R \oplus R), \quad \overline{\lambda}(\overline{\gamma}) = (1, x), \quad \overline{\lambda}(\overline{\gamma}) = (1, x, -x, -x) \). Then \( \lambda(\gamma^2) = (1, 1, u, v), \) with \( u = A + Bi, v = A - Bi, A, B \in R \). We have \( uv = A^2 + B^2 \in R[\overline{\gamma}] \) and hence \( \in R^\times \). Both \( u \) and \( v \) are \( \equiv 1 \pmod{(i-1)} \) and are torsion by assumption. So \( \gamma^2 \) is torsion and \( \gamma \) is a torsion element of \( \mathcal{U}_1(RC_4) \). Thus \( \gamma \in C_4 \) by Corollary 2.2. ■

**Lemma 4.2.** Suppose \( G \) is abelian of exponent three. Suppose that \( R \) is \( G \)-adapted and \( RC_3 \times C_3 = \{ u = a + 3v \in R[w] : u \equiv 1 \pmod{\pi}, a^2 - ab + b^2 \in R^\times \} \) is torsion. Then \( \mathcal{U}_1(RG) = G \).

**Proof.** We proceed by induction on \(|G|\). In view of Lemma 2.8, it suffices to prove that if \( G = C_3 \times G_1, \quad C_3^1 = 1, \quad \mathcal{U}_1(RG_1) = G_1 \), then \( \mathcal{U}_1(RG) = G \). Let us write \( C_3 = \langle x \rangle \). Then we have an embedding
\[
RG = R(C_3 \times G_1) = (RC_3)G_1 \overset{\lambda}{\twoheadrightarrow} RG_1 \oplus R[\omega]G_1 \oplus R[\omega]G_1
\]
given by
\[
\gamma = x_0 + x_1x + x_2x^2 \mapsto (x_0 + x_1 + x_2, x_0 + x_1\omega + x_2\omega^2, x_0 + x_1\omega^2 + x_2\omega).
\]
Suppose \( \gamma \in \mathcal{U}_1(RG) \). Then the augmentation, \( \sigma(\gamma) = 1 = \sum_0^2 \sigma(x_i) \). Thus \( \sum_0^2 x_i \) is a trivial unit of \( RG_1 \). Replacing \( \gamma \) by a suitable power we get \( \lambda(\gamma) = (1, x, \beta) \), where \( \sigma(x) = \sum_0^2 \sigma(x_i)\omega^i \equiv \sum \sigma(x_i)(\mod \pi) \equiv 1(\mod \pi) \). The element \( x \in R[\omega]G_1 \), \( \sigma(x) \in R[\omega] \), so \( \sigma(x) \in R^\times \). The condition \( a^2 - ab + b^2 \in R^\times \) is checked by observing that \( x \mapsto x^{-1} \) is an automorphism of \( G \) and by using Lemma 2.6. Thus \( \sigma(x) \) is torsion. There exists a \( k \) so that \( \sigma(x^k) = 1 \) so that \( x^k \in G_1 \). Therefore, \( x \) is a torsion and we get \( \lambda(\gamma^k) = (1, 1, 1, 1, \ldots) \) for some \( k \). Repeating, we get that \( \lambda(\gamma^{k/m}) = (1, 1, 1, 1, \ldots) \) for some \( m \). Consequently, \( \gamma \) is torsion. It follows by Corollary 2.2 that \( \gamma \in G_1 \) as desired. ■

Using Lemma 4.1, the above proof gives

**Lemma 4.3.** If \( G \) is a product of cyclic groups of order 4 and \( RC_3 \times C_3 = \{ u = a + bi \in R[i] : u \equiv 1 \pmod{(i-1)}, a^2 + b^2 \in R^\times \} \) is torsion then \( \mathcal{U}_1(RG) = G \).

We need one more result.

**Lemma 4.4.** Suppose that \( R \) is a \( G \)-adapted ring, \( G = C_2 \times G_1 \). Suppose that \( \mathcal{U}(RG_1) \) and \( \mathcal{U}(RC_2) \) are trivial. Then \( \mathcal{U}(RG) \) is also trivial.
PROOF: Write $C_2 = \langle x \rangle$, $G = C_2 \times G_1$. Then we have an embedding $RG \hookrightarrow RG_1 \oplus RG_1$ given by $\lambda(x + \beta x) = (x + \beta, x - \beta)$ for $x, \beta \in RG_1$. Suppose that $\gamma = x + \beta x \in U_1(RG)$. Then $x + \beta$ and $x - \beta$ are both units of $RG_1$ with the augmentation $\varepsilon(x + \beta) = 1$. Thus by assumption $x + \beta = g \in G_1$. Multiplying by $g^{-1}$ we can assume $\gamma \mapsto (1, \text{unit}) = (1, rg_1)$, $r \in R$, $g_1 \in G_1$. Then $x + \beta = 1$, $x - \beta = rg_1$, $2x = 1 + rg_1$. It follows that $g_1 = 1$. We have $x = \frac{1 + \sqrt{2}}{2}$, $\beta = \frac{1 - \sqrt{2}}{2}$ and $\gamma = \frac{1 + \sqrt{2}}{2} + \frac{1 - \sqrt{2}}{2} x$ is a unit of $RC_2$. This implies that either $1 + r = 0$ and $\gamma = x$ or $1 - r = 0$ and $\gamma = 1$, which completes the proof. \[\blacksquare\]

4.5. Completion of the proof of Theorem 1

The proof now follows from Proposition 3.1, Lemma 4.4, Lemma 4.3 and Lemma 4.2.

5. Rank of $\mathfrak{Z}(U(\mathbb{Z}G))$

In this section we compute the rank of the group of central units of the integral group ring of a finite group. From this the formula for the abelian case due to Ayoub and Ayoub [1] easily follows, as does the criterion for the triviality of central units due to the authors [10]. We collect a couple of well-known results below.

Two elements $a$ and $b$ of $G$ are said to be $Q$-conjugate ($a \sim_Q b$) if there exists an $x \in G$ such that $x^{-1}bx = ax$ for some $r \in (\mathbb{Z}/|G|) \times$ in the Galois group of the cyclotomic field $\mathbb{Q}(\zeta_{|G|})$. Then it is known (see [2, pp 282, 306]), that

(5.1) The number of $Q$-conjugate classes of $G$ equals the number of irreducible $QG$-modules and equals the number of non-conjugate cyclic subgroups of $G$. We denote this number by $h_Q$.

A conjugacy class $C_g$ is said to be a real class if $g^{-1} \in C_g$. A character of $G$ is said to be real valued if all its values $\chi(g)$ are real. Then we know (see [6, p. 537]) that

(5.2) The number of real classes of $G$ is equal to the number of real valued complex irreducible characters of $G$.

We denote this number by $h_R$.

Now, we can state the main result of this section.

**Theorem 2.** The rank $\rho = \rho(\mathfrak{Z}(U(\mathbb{Z}G)))$ of the centre of the unit group of the integral group ring of a finite group $G$ is given by

$$\rho = \frac{1}{2} (c - 2h_Q + h_R),$$

where $c$ is the number of conjugacy classes in $G$, $h_Q$ is the number of $Q$-conjugate classes in $G$ and $h_R$ is the number of real classes in $G$. 
PROOF. Let us decompose $\mathbb{Q}G$ as a direct sum of simple rings:

$$\mathbb{Q}G = \bigoplus S.$$ 

Then we know, for the centres, (see [6, p. 545]) that

$$3\mathbb{Q}G = \bigoplus \mathbb{Q}(\chi), \quad (5.3)$$

a direct sum of character fields, with the sum ranging over the irreducible complex characters $\chi$ of $G$ modulo Galois conjugation over $\mathbb{Q}$. Let us denote the degree $[\mathbb{Q}(\chi) : \mathbb{Q}]$ by $d_\chi$. Let $O_\chi$ be the ring of algebraic integers of $\mathbb{Q}(\chi)$. Then we have a containment of orders

$$3(\mathbb{Z}G) \subset \bigoplus O_\chi.$$ 

Therefore, $\rho = \sum \rho(O_\chi^\times)$, whereby the rank of an abelian group is understood, simply the rank of its torsion-free part. By Dirichlet’s unit theorem, if $\mathbb{Q}(\chi)$ is complex then $\rho(O_\chi^\times) = \frac{d_\chi}{2} - 1$, and if it is real then $\rho(O_\chi^\times) = d_\chi - 1$. Thus we have

$$\rho = \sum_{\chi \text{ nonreal}} \left(\frac{d_\chi}{2} - 1\right) + \sum_{\chi \text{ real}} (d_\chi - 1) \quad (5.4)$$

where $\sum$ denotes the sum modulo Galois conjugacy over $\mathbb{Q}$. We claim

$$\sum d_\chi = h_{\mathbb{R}}. \quad (5.5)$$

We know from (5.3) that

$$3(\mathbb{R}G) = \cdots \bigoplus \mathbb{R} \otimes \mathbb{Q} \mathbb{Q}(\chi) \bigoplus \cdots.$$ 

If $\chi$ is real then $\mathbb{R} \otimes \mathbb{Q} \mathbb{Q}(\chi) = d_\chi \mathbb{R}$, otherwise $\mathbb{R} \otimes \mathbb{Q} \mathbb{Q}(\chi) = \frac{d_\chi}{2} \mathbb{C}$. Thus

$$3(\mathbb{R}G) = \cdots \bigoplus \mathbb{R} \bigoplus \cdots \bigoplus \mathbb{R} \bigoplus \mathbb{C} \bigoplus \cdots \bigoplus \mathbb{C}$$

and (5.5) follows. We also have

$$\sum_{\chi \text{ real}} d_\chi + \sum_{\chi \text{ nonreal}} d_\chi = c,$$

the number of conjugacy classes in $G$. Thus

$$\sum_{\chi \text{ nonreal}} d_\chi = c - h_{\mathbb{R}}. \quad (5.6)$$

Combining 5.4 and 5.6, we have

$$\rho = \sum_{\chi \text{ nonreal}} \left(\frac{d_\chi}{2} - 1\right) + \sum_{\chi \text{ real}} (d_\chi - 1)$$

$$= \sum_{\chi \text{ nonreal}} \frac{d_\chi}{2} + \sum_{\chi \text{ real}} d_\chi - \sum 1.$$
Corollary 5.7. (Ayoub and Ayoub [1]). If $G$ is a finite abelian group then the rank of the unit group $U(\mathbb{Z}G)$ of the integral group ring $\mathbb{Z}G$ is given by 
\[ r = \frac{1}{2}(c - h_R) + h_R - h_Q \]
\[ = \frac{1}{2}(c + h_R - 2h_Q) \] 

PROOF. Clearly $c = |G|$ and $h_Q = \ell$ in the abelian case. Also, in this case, $g \sim g^{-1}$ if and only if $g = g^{-1}$. Consequently, $h_R = (n_2 + 1)$.

Corollary 5.8. (Ritter and Sehgal [8]). Let $G$ be a finite group. Then all central units of $\mathbb{Z}G$ are trivial (equivalently $\rho(U(\mathbb{Z}G)) = 0$) if and only if $G$ satisfies the following condition:

given $a \in G$ and $(j, |a| = 1)$, then $a^j \sim a^e, e = \pm 1$.

PROOF. Let us first assume that $\rho = 0$ and deduce the condition of the corollary. We have

\[ \rho = 0 \iff \frac{c - h_R}{2} + h_R = h_Q. \]

A class $C_g$ is real if and only if $g^{-1} \in C_g$ (see [6, p. 587]). Also, we have $(c - h_R)$ non-real conjugacy classes $C_g$, in this case, $C_g \neq C_{g^{-1}}$. Then $C_g \cup C_{g^{-1}}$ belong to the same $\mathbb{Q}$-conjugate class. We have thus $(c - h_R)/2$ pairs. This gives us in all $h_Q$ subsets of $\mathbb{Q}$-conjugate classes, all disjoint. These must be all the $\mathbb{Q}$-conjugate classes. Hence $g^j \sim g$ or $g^{-1}$ for all $(j, |g|) = 1$.

For the proof of the converse, let us assume the condition. For $(j, |g|) = 1$ we can only have $g^j \sim g^e, e = 1, -1$. Thus the only $\mathbb{Q}$-conjugate classes are $C_g$ or $C_g \cup C_{g^{-1}}$. Their total number $h_Q = h_R + \frac{c - h_R}{2}$. Thus $\rho = 0$ as desired. ■

6. Trivial central units

Let $G$ be a finite group. Express $\mathbb{Q}G$ as a direct sum

\[ \mathbb{Q}G = \bigoplus S_i \]

of simple rings $S_i$; the sum ranges over the irreducible complex characters of $G$ modulo Galois conjugation over $\mathbb{Q}$. Let $\chi$ be one such and $D$ the corresponding representation. So there exists a unique $S$ so that $D(S) \neq 0$. There is an isomorphism

\[ 3 \mathbb{Q}G \cong \bigoplus \mathbb{Q}(\chi), \]

which on class sums $C_g$ is
where $h_g = |C|$. Moreover

$$ \mathfrak{Z}(ZG) \leq \sum_{\chi} Z[\chi]. $$

Let $R$ be a $G$-adapted ring. Then

$$ \mathfrak{Z}(RG) = R \otimes \mathfrak{Z}(ZG) \leq \sum_{\chi} R \otimes Z[\chi]. $$

If the centre of $U(ZG)$ is trivial then every $Q$ is rational or imaginary quadratic (see [10, p. 22]). For an imaginary quadratic field $Q(\sqrt{m})$ the integers are given by $Z \oplus \sqrt{m} Z$ or $Z \oplus \frac{1+\sqrt{m}}{2} Z$. In this case we enlarge the direct sum on the right by another copy of $Q(\chi)$ or $Z[\chi]$ with the corresponding projection the algebraic conjugate. Then we have

$$ \mathfrak{Z}(RG) \leq \sum_{\chi} R \otimes Z[\chi] \quad (6.1) $$

with $c$ (= the number of conjugacy classes in $G$) summands (so the sum now ranges over all irreducible complex $\chi$). Remember the map is

$$ \sum_{\chi_1, C_i \mapsto \sum_{\chi} h_i C_i \mapsto \sum_{\chi} h_i \chi_1(g_i) \chi_1(1), \ldots, \sum_{\chi} h_i \chi_c(g_i) \chi_c(1) \quad (6.2) $$

where $h_i = |C_i|$ and $\chi_1, \ldots, \chi_c$ are the irreducible complex characters.

We shall now characterise groups $G$ so that central units $\mathfrak{U}(ZG)$ are trivial, namely, of the form $rg, r \in R, g \in G$. Unfortunately, we need to impose a rather strong condition on $R$. As before, $\zeta_n$ is a primitive $n^{th}$ root of unity.

**Theorem 3.** Let $R$ be a ring that is $G$-adapted. Suppose that the unit group $(R \otimes Z[\chi])^\times$ is torsion. Then $\mathfrak{U}(RG)$ is trivial if and only if $(R \otimes Z[\chi])^\times$ is torsion for all complex characters $\chi$.

**Proof.**

a) ($\Rightarrow$) Suppose that $(R \otimes Z[\chi])^\times$ is torsion. From the embedding

$$ \mathfrak{Z}(RG) \leq \sum_{\chi} R \otimes Z[\chi] $$

we conclude that $\mathfrak{U}(\mathfrak{Z}(RG))$ is torsion. It follows by (2.2) that all central units of $RG$ are trivial as $R$ is $G$-adapted.

b) ($\Rightarrow$) Now we assume that all central units of $RG$ are trivial. Then $\mathfrak{Z}(RG)$ is trivial. We have (6.1) and (6.2). Suppose that there exists an $\varepsilon \in (R \otimes Z[\chi])^\times$ of infinite order for some $\chi \neq 1$. By assumption, we can find an $n$ so that $\varepsilon^n \equiv 1(\text{mod } |G|)$, hence also an $n$ so that $\varepsilon^n \equiv 1(\text{mod } |G|^d)$ for some given exponent $d$. Let us replace $\varepsilon$ by $\varepsilon^n$. 
We represent the map (6.2) as
\[
\sum \varepsilon_i C_i \mapsto \begin{bmatrix} h_i \varepsilon_i(g_j) \\ \varepsilon_i(1) \end{bmatrix}_{i,j} \begin{bmatrix} \varepsilon_1 \\ \vdots \\ \varepsilon_c \end{bmatrix} = M \begin{bmatrix} \varepsilon_1 \\ \vdots \\ \varepsilon_c \end{bmatrix},
\]
where
\[
M = \begin{bmatrix} 1 & h_1 & \cdots & h_c \\ 1 & \vdots & \star \\ 1 \end{bmatrix}.
\]
We define \( \hat{Z} = \mathbb{Z}[\varepsilon_i(g_j) : 1 \leq i, j \leq c] \) and claim for the determinant that there exists an exponent \( d \) such that
\[
|M| = \det M \text{ is a divisor of } |G|^d \text{ in } \hat{Z}.
\]
Let \( M^* \) be the conjugate transpose. Then the orthogonality relations yield
\[
|M| = \left| \frac{h_i \varepsilon_i(g_j)}{\varepsilon_i(1)} \right| = \frac{\prod h_j}{\prod \varepsilon_i(1)} |\varepsilon_i(g_j)|,
\]
\[
|MM^*| = \left( \frac{\prod h_j}{\prod \varepsilon_i(1)} \right)^2 |\varepsilon_i(g_j)\varepsilon_j(g_p)| = \frac{\prod h_j}{(\prod \varepsilon_i(1))^2} \left| \sum_k h_k \varepsilon_i(g_k) \varepsilon_j(g_k) \right| = \frac{|G|^c \cdot \prod h_j}{(\prod \varepsilon_i(1))^2}.
\]
Thus we have \( |MM^*| (\prod \varepsilon_i(1))^2 = |G|^c (\prod h_j) \), and the claim follows from \( h_j | G |, \varepsilon_i(1) | G \) and \( M \in (\mathbb{Z})_{c \times c} \) (see [6, p. 481]).

We wish to find \( \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_c \) so that
\[
M \begin{bmatrix} \varepsilon_1 \\ \vdots \\ \varepsilon_c \end{bmatrix} = \begin{bmatrix} \vdots \\ \bar{\varepsilon} \end{bmatrix}
\]
with the dots on the right representing ones,

where \( \bar{\varepsilon} \) is the algebraic conjugate of \( \varepsilon \). We have
\[
\begin{bmatrix} 1 & h_2 \cdots h_c \\ 1 & \vdots & \star \\ 1 \end{bmatrix} \begin{bmatrix} \varepsilon_1 \\ \vdots \\ \varepsilon_c \end{bmatrix} = \begin{bmatrix} \vdots \\ \bar{\varepsilon} \end{bmatrix}.
\]
Subtracting the first row from all others gives
where the dots on the right now represent zeros. We forget the first equation
\[ \sum_i h_i \alpha_i = 1 \]
and are left with
\[ M = \begin{bmatrix} \alpha_1 & \ldots & \alpha_c \\ \vdots & \ddots & \vdots \\ \alpha_1 & \ldots & \alpha_c \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_c \end{bmatrix} = \begin{bmatrix} 1 \\ \vdots \\ \varepsilon - 1 \\ \varepsilon - 1 \end{bmatrix}, \]

Note that \( \det M = \det M' \). Multiplication with the adjoint matrix of \( M' \) from the
left yields
\[ (\text{Adj } M')M' \begin{bmatrix} \alpha_2 \\ \vdots \\ \alpha_c \end{bmatrix} = (\text{Adj } M') \begin{bmatrix} \vdots \\ \varepsilon - 1 \\ \varepsilon - 1 \end{bmatrix}, \]
i.e.,
\[ |M'| \begin{bmatrix} \alpha_2 \\ \vdots \\ \alpha_c \end{bmatrix} = (\text{Adj } M') \begin{bmatrix} \vdots \\ \varepsilon - 1 \\ \varepsilon - 1 \end{bmatrix}. \]

Since \( \det M = \det M' \) is a divisor of \( |G|^d \) and \( \varepsilon \equiv 1 \mod |G|^d \), the system of equations
can be solved in \( R \otimes_{\mathbb{Z}} \hat{\mathbb{Z}} \). In order to see that the unique solution actually belongs to
\( R = R \otimes_{\mathbb{Z}} \hat{\mathbb{Z}} \), we apply the automorphisms \( \sigma \) from the Galois group \( A \) of \( \mathbb{Q}(\chi) \) to it. Note that \( A \) is an elementary abelian 2-group and that, to \( \chi \) with \( \hat{\mathbb{Z}} \neq \mathbb{Z}[\chi] \), there exists a \( \sigma_\chi \in A \), which is trivial on all \( \mathbb{Z}[\chi'] \), \( \chi' \neq \chi \) but \( \neq 1 \) on \( \mathbb{Z}[\chi] \) itself; in particular, \( \sigma_\chi(\epsilon) = \varepsilon \) for our \( \chi \). Since the \( \sigma_\chi \neq 1 \) just interchange two rows of our system of linear equations, they have no influence on its solution. And since they generate \( A \), we find that the solution belongs to \( R \) as desired. The fact that
the solution is a unit follows by considering \( \varepsilon^{-1} \).

**Corollary.** Let \( R \) be the ring of integers in an algebraic number field \( K \). Then the central
units of \( RG \) are trivial if and only if either \( K = \mathbb{Q} \) and all character fields \( \mathbb{Q}(\chi) \) are rational or imaginary quadratic or \( K \) itself is imaginary quadratic and \( \mathbb{Q}(\chi) \subseteq K \) for all \( \chi \).

This is because \( R \) is a finitely generated \( \mathbb{Z} \)-module, and thus \( R[\varepsilon_{|G|}] / |G| \) is finite.

**REFERENCES**


