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]:

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

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

 © Royal Irish Academy

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 $R_2^\times = \{a \in R^\times : a \equiv 1 (\mathrm{mod}\ 2)\}$ is torsion.*
(2) *G is abelian of exponent 3, and $R_3^\times = \{u = a + b\omega \in R[\omega] : u \equiv 1 (\mathrm{mod}\ \pi), a^2 + b^2 - ab \in R^\times\}$ is torsion. Here, ω is a primitive 3^{rd} root of unity and $\pi = \omega - 1$.*
(3) *G is abelian of exponent 4, and $R_4^\times = \{u = a + bi \in R[i] : u \equiv 1\ \mathrm{mod}(i-1), a^2 + b^2 \in R^\times\}$ 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 $\rho = \rho(\mathfrak{Z}(\mathcal{U}(\mathbb{Z}G)))$ of the centre of the unit group of the integral group ring of a finite group G is given by*

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

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

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

Our notations are standard as in [10]. As has been said already, our ring R is G-adapted throughout. We set $K = \mathrm{Quot}(R)$ for its field of fractions. We denote by ζ_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 ω may be contained in K. When we consider a set $S = \{u = a + b\omega \in R[\omega] : u \text{ has property } P\}$ 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 $u = \sum u_g g \in \mathcal{U}(RG)$ 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 $\mathcal{U}_1(RG)$, 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

$$\mathrm{tr}(e) = \frac{1}{|V|} \sum \mathrm{tr}(v) = \frac{1}{|V|} \mathrm{tr}(1) = \frac{|G|}{|V|} .$$

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

Lemma 2.4. $R_3^\times = \{a + b\omega \in R[\omega] : a + b\omega \equiv 1 (\mathrm{mod}\ \pi),\ a^2 - ab + b^2 \in R^\times\}$ *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 $a + b\omega, c + d\omega \in R_3^\times$ 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. $R_4^\times = \{a + bi \in R[i] : a + bi \equiv 1 (\mathrm{mod}\ i - 1),\ a^2 + b^2 \in R^\times\}$ *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 $R_2^\times = \{u \in R^\times : u \equiv 1 (\mathrm{mod}\ 2)\}$ 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 $\equiv 1 (\mathrm{mod}\ 2)$, 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. ■

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

Proof. ($\Rightarrow$) Assume that $\mathcal{U}(RC_3)$ is trivial. Suppose we have in $R_3^\times$ an element $u \equiv 1 (\mathrm{mod}\ \pi)$, $u = A + B\omega$, $A, B \in R$, $A^2 - AB + B^2 \in R^\times$ 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 λ. We wish to find $a, b, c \in R$ so that $\lambda(a + bx + cx^2) = (1, u^3, \alpha)$, $\alpha = A_1 + B_1\omega^2$. Remember that $u \equiv 1 (\mathrm{mod}\ \pi)$ gives $u^3 \equiv 1 (\mathrm{mod}\ \pi^3)$, and so $u^3 \equiv 1 (\mathrm{mod}\ 3)$. It follows that $A_1 \equiv 1 (\mathrm{mod}\ 3)$. Then the elements $a = \frac{1}{3}(2A_1 - B_1 + 1)$, $b = \frac{1}{3}(2B_1 - A_1 + 1)$, $c = 1 - a - b$ belong to R and they solve the equations

$$a + b + c = 1, \quad a + b\omega + c\omega^2 = A_1 + B_1\omega, \quad a + b\omega^2 + c\omega = A_1 + B_1\omega^2 = \alpha.$$

Set $\gamma = a + bx + cx^2$. Then $\lambda(\gamma) = (1, u^3, \alpha)$. Since $u^3 \in R_3^\times, u^3\alpha = A_1^2 - A_1B_1 + B_1^2 \in R^\times$. It follows that $\alpha \in R[\omega]^\times$ as well. Also, $\alpha = A_1 + B_1\omega^2 = (A_1 - B_1) - B_1\omega \in R_3^\times$. Then we can find $\mu \in RC_3$ so that $\lambda(\mu) = (1, u^{-3}, \alpha^{-1})$. It follows that γ 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

$$\gamma = a + bx + cx^2 \overset{\lambda}{\mapsto} (a + b + c,\ a + b\omega + c\omega^2,\ a + b\omega^2 + c\omega).$$

In fact,

$$\lambda(\gamma) = (1, 2a + b - 1 + (a + 2b - 1)\omega,\ 2a + b - 1 + (a + 2b - 1)\omega^2) = (1, u, v),$$

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

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,

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

We have

Proposition 3.1. $\mathcal{U}_1(RQ_8) = Q_8 \Longleftrightarrow$ *the three conditions below are satisfied:*

(0) *K has no solution of* $x_1^2 + y_1^2 + z_1^2 = -1$,
(1) $R_2^{\times} = \{u \in R^{\times} : u \equiv 1 (\mathrm{mod}\ \ 2)\}$ *is torsion, and*
(2) *the kernel of the norm map* $R[i, j, k] \to R$ *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* $\mathbb{H}_K = K \otimes_{\mathbb{Q}} \mathbb{H}_{\mathbb{Q}} \supset R \otimes_{\mathbb{Z}} \mathbb{Z}[i, j, k] = R[i, j, k]$.

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 η 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

$$\lambda : RQ_8 \to R \oplus R \oplus R \oplus R \oplus R[i, j, k]$$
$$\lambda(x) = (1, 1, -1, -1, i), \quad \lambda(y) = (1, -1, 1, -1, j).$$

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 $\equiv 0 (\mathrm{mod}\ \ 2)$ and the first coefficient is $\equiv 1 (\mathrm{mod}\ \ 2)$. 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

$$\begin{aligned} \lambda(\gamma) = (&a_0 + a_1 + a_2 + a_3 + b_1 + b_2 + c_1 + c_2, \\ &a_0 + a_1 + a_2 + a_3 - b_1 - b_2 - c_1 - c_2, \\ &a_0 - a_1 + a_2 - a_3 + b_1 + b_2 - c_1 - c_2, \\ &a_0 - a_1 + a_2 - a_3 - b_1 - b_2 + c_1 + c_2, \\ &(a_0 - a_2) + (a_1 - a_3)i + (b_1 - b_2)j + (c_1 - c_2)k). \end{aligned}$$

We wish to solve for $\gamma \in \mathcal{U}_1(RQ)$ 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

$$\left[\begin{array}{cccccccc|c} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 \\ 1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & a \\ 0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 & b \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & c \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & d \end{array}\right],$$

which is equivalent to

$$\left[\begin{array}{cccccccc|c} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & a \\ 0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 & b \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & c \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & d \end{array}\right],$$

This gives the equations

$$\begin{aligned} a_0 + a_2 &= 1, & a_0 - a_2 &= a \\ b_1 + b_2 &= 0, & b_1 - b_2 &= c \\ c_1 + c_2 &= 0, & c_1 - c_2 &= d \\ a_1 + a_3 &= 0, & a_1 - a_3 &= b. \end{aligned}$$

These can be solved as $b, c, d \equiv 0 \pmod 2$ and $a \equiv 1 \pmod 2$. The element γ is a unit, as $(1, 1, 1, 1, u^{-1})$ can also be lifted. Because γ has infinite order, this is a contradiction, proving 2).

(b) ($\Leftarrow$) First, we show that $\mathcal{U}_1(RQ_8)$ is torsion. Suppose there exists a $\gamma \in \mathcal{U}_1(RQ_8)$ of infinite order. Since the first four components of $\lambda(\gamma)$ can be viewed as the components of $\bar{\gamma}$ in $R(Q_8/Q_8')$, we have $\lambda(\gamma) = (1, \pm 1, \pm 1, \pm 1, *)$. Replace γ by γ^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 $\gamma = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + b_1 y + b_2 y^3 + c_1 xy + c_2 x^3 y \in \mathcal{U}_1(RQ_8)$. Also, $a_0 + a_1 + a_2 + a_3 + b_1 + b_2 + c_1 + c_2 = 1$. Then

$$\begin{aligned} N(u) &= (a_0 - a_2)^2 + (a_1 - a_3)^2 + (b_1 - b_2)^2 + (c_1 - c_2)^2 \\ &\equiv \textstyle\sum_0^3 a_i^2 + \sum_1^2 b_i^2 + \sum_1^2 c_i^2 \pmod 2 \\ &\equiv \left(\textstyle\sum a_i + \sum b_i + \sum c_i\right)^2 \pmod 2 \\ &\equiv 1 \pmod 2. \end{aligned}$$

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

If we now take a unit $\gamma \in \mathcal{U}_1(RQ_8)$, 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.

(i) Suppose $o(\gamma) = 2$. If $\lambda(\gamma) = (1, 1, 1, 1, *)$, then $* = -1$ 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 γ then it follows from the equation (1.1) that b, c and d are $\equiv 0 (\text{mod } 2)$. 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 $\lambda(\gamma) \neq (1, 1, 1, 1, *)$. Then a typical expression for $\lambda(\gamma)$ is $\lambda(\gamma) = (1, -1, -1, 1, u)$. Then $\lambda(\gamma xy) = (1, 1, 1, 1, uk)$.

We have $N(u)^4 = 1 = N(uk)^4$. It follows that uk is torsion. The situation is $\lambda(\gamma xy) = (1, 1, 1, 1, uk)$. 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 $\lambda(\gamma xy) = (1, 1, 1, 1, -1)$. It follows that $\gamma xy = x^2$ and $\gamma \in Q_8$. This completes the proof of the proposition. ■

4. Proof of Theorem 1

We know from Higman's theorem (see [9, p. 57]) that $\mathcal{U}(\mathbb{Z}G)$ 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 $\mathcal{U}(RG)$ 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. *$\mathcal{U}_1(RC_4) = C_4 \Longleftrightarrow R_4^\times = \{u = x_1 + x_2 i \in R[i]\,,\quad u \equiv 1 \,\mathrm{mod}(i-1),\ x_1^2 + x_2^2 \in R^\times\}$ 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 $u = x_1 + x_2 i \in R_4^\times$ of infinite order. Note that $u^2 \equiv 1 (\text{mod } 2)$ by $(i-1)^2 = -2i$. So $u^2 = x_1^2 - x_2^2 + 2x_1x_2 i \equiv 1 (\text{mod } 2)$, and consequently, $x_1^2 - x_2^2 \equiv 1 (\text{mod } 2)$. Replace u by u^2 to assume

$$u = \alpha + \beta i, \quad \alpha \equiv 1 (\text{mod } 2) \quad \text{and} \quad \beta \equiv 0 (\text{mod } 2).$$

We solve $\gamma = a + bx + cx^2 + dx^3$ with $\lambda(\gamma) = (1, 1, \alpha + \beta i, \alpha - \beta i)$, namely, by taking $a = \frac{\alpha+1}{2}$, $b = \beta/2$, $c = \frac{1-\alpha}{2}$, $d = -\beta/2$ all in R. Then $\gamma \in \mathcal{U}_1(RC_4)$, as similarly $(1, 1, (\alpha + \beta i)^{-1}, (\alpha - \beta i)^{-1})$ can be lifted. Also, $o(\gamma)$ 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 $R\overline{C}_4 \to (R \oplus R)$, $\overline{\lambda}(\overline{\gamma}) = (1, \alpha)$, $\lambda(\gamma) = (1, \alpha, \cdot, \cdot)$. Then $\lambda(\gamma^2) = (1, 1, u, v)$, with $u = A + Bi$, $v = A - Bi$, $A, B \in R$. We have $uv = A^2 + B^2 \in R[i]^\times$ and hence $\in R^\times$. Both u and v are $\equiv 1 (\text{mod } (i-1))$ and are torsion by assumption. So γ^2 is torsion and γ 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 $R_3^\times = \{u = a + b\omega \in R[w] : u \equiv 1 (\text{mod } \pi),\ a^2 - ab + b^2 \in R^\times\}$ 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 $G = C_3 \times G_1$, $G_1^3 = 1$, $\mathcal{U}_1(RG_1) = G_1$, then $\mathcal{U}_1(RG) = G$. Let us write $C_3 = \langle x \rangle$. Then we have an embedding

$$RG = R(C_3 \times G_1) = (RC_3)G_1 \xrightarrow{\lambda} RG_1 \oplus R[\omega]G_1 \oplus R[\omega]G_1$$

given by

$$\gamma = \alpha_0 + \alpha_1 x + \alpha_2 x^2 \overset{\lambda}{\mapsto} (\alpha_0 + \alpha_1 + \alpha_2, \alpha_0 + \alpha_1\omega + \alpha_2\omega^2, \alpha_0 + \alpha_1\omega^2 + \alpha_2\omega).$$

Suppose $\gamma \in \mathcal{U}_1(RG)$. Then the augmentation, $\varepsilon(\gamma) = 1 = \sum_0^2 \varepsilon(\alpha_i)$. Thus $\sum_0^2 \alpha_i$ is a trivial unit of RG_1. Replacing γ by a suitable power we get $\lambda(\gamma) = (1, \alpha, \beta)$, where $\varepsilon(\alpha) = \sum_0^2 \varepsilon(\alpha_i)\omega^i \equiv \sum \varepsilon(\alpha_i) (\text{mod } \pi) \equiv 1 (\text{mod } \pi)$. The element $\alpha \in R[\omega]G_1$, $\varepsilon(\alpha) \in R[\omega]$, so $\varepsilon(\alpha) \in R_3^\times$. The condition $a^2 - ab + b^2 \in R^\times$ is checked by observing that $x \to x^{-1}$ is an automorphism of G and by using Lemma 2.6. Thus $\varepsilon(\alpha)$ is torsion. There exists a k so that $\varepsilon(\alpha^k) = 1$ so that $\alpha^k \in G_1$. Therefore, α is torsion and we get $\lambda(\gamma^{k\ell}) = (1, 1, *)$ for some ℓ. Repeating, we get that $\lambda(\gamma^{k\ell m}) = (1, 1, 1)$ for some m. Consequently, γ 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 $R_4^\times = \{u = a + bi \in R[i] : u \equiv 1 (\text{mod}(i-1)),\ a^2 + b^2 \in R^\times\}$ 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 $RG \xrightarrow{\lambda} RG_1 \oplus RG_1$ given by $\lambda(\alpha + \beta x) = (\alpha + \beta, \alpha - \beta)$ for $\alpha, \beta \in RG_1$. Suppose that $\gamma = \alpha + \beta x \in \mathcal{U}_1(RG)$. Then $\alpha + \beta$ and $\alpha - \beta$ are both units of RG_1 with the augmentation $\varepsilon(\alpha + \beta) = 1$. Thus by assumption $\alpha + \beta = g \in G_1$. Multiplying by g^{-1} we can assume $\gamma \overset{\lambda}{\mapsto} (1, \text{unit}) = (1, rg_1)$, $r \in R$, $g_1 \in G_1$. Then $\alpha + \beta = 1$, $\alpha - \beta = rg_1$, $2\alpha = 1 + rg_1$. It follows that $g_1 = 1$. We have $\alpha = \frac{1+r}{2}$, $\beta = \frac{1-r}{2}$ and $\gamma = \frac{1+r}{2} + \frac{1-r}{2} x$ 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. ■

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 $\mathfrak{Z}(\mathcal{U}(\mathbb{Z}G))$

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 $\mathbb{Q}$-conjugate ($a \sim_{\mathbb{Q}} b$) if there exists an $x \in G$ such that $x^{-1}bx = a^r$ 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 $\mathbb{Q}$-conjugate classes of G
equals the number of irreducible $\mathbb{Q}G$-modules and
equals the number of non-conjugate cyclic subgroups of G. We denote this number by $h_{\mathbb{Q}}$.

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 $h_{\mathbb{R}}$.

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

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

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

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

PROOF. Let us decompose $\mathbb{Q}G$ as a direct sum of simple rings:

$$\mathbb{Q}G = \sum^{\oplus} S .$$

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

$$\mathfrak{Z}\mathbb{Q}G = \sum^{\oplus} \mathbb{Q}(\chi), \tag{5.3}$$

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

$$\mathfrak{Z}(\mathbb{Z}G) \subset \sum^{\oplus} O_\chi .$$

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

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

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

$$\sum_{\chi \text{ real}}' d_\chi = h_{\mathbb{R}}. \tag{5.5}$$

We know from (5.3) that

$$\mathfrak{Z}(\mathbb{R}G) = \cdots \oplus \mathbb{R} \otimes_{\mathbb{Q}} \mathbb{Q}(\chi) \oplus \cdots .$$

If χ 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

$$\mathfrak{Z}(\mathbb{R}G) = \cdots \oplus \mathbb{R} \oplus \cdots \oplus \mathbb{R} \oplus \mathbb{C} \oplus \cdots \oplus \mathbb{C}$$

and (5.5) follows. We also have

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

the number of conjugacy classes in G. Thus

$$\sum_{\text{nonreal}}' d_\chi = c - h_{\mathbb{R}}. \tag{5.6}$$

Combining 5.4 and 5.6, we have

$$\begin{aligned} \rho &= \textstyle\sum_{\text{nonreal}}' \left(\frac{d_x}{2} - 1\right) + \sum_{\text{real}}' (d_x - 1) \\ &= \textstyle\sum_{\text{nonreal}}' \frac{d_x}{2} + \sum_{\text{real}}' d_x - \sum' 1 \end{aligned}$$

$$= \tfrac{1}{2}(c - h_{\mathbb{R}}) + h_{\mathbb{R}} - h_{\mathbb{Q}}$$
$$= \tfrac{1}{2}(c + h_{\mathbb{R}} - 2h_{\mathbb{Q}}) \quad \blacksquare$$

Corollary 5.7. (Ayoub and Ayoub [1]). *If G is a finite abelian group then the rank of the unit group $\mathcal{U}(\mathbb{Z}G)$ of the integral group ring $\mathbb{Z}G$ is given by $\rho = \frac{1}{2}(|G| - 2\ell + n_2 + 1)$, where ℓ is the number of cyclic subgroups of G and n_2 is the number of elements of order 2 in G.*

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

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

$$\text{given } a \in G \text{ and } (j, |a|{=}1), \text{ then } a^j \sim a^{\varepsilon}, \varepsilon = \pm 1.$$

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

$$\rho = 0 \Longleftrightarrow \frac{c - h_{\mathbb{R}}}{2} + h_{\mathbb{R}} = h_{\mathbb{Q}}.$$

A class C_g is real if and only if $g^{-1} \in C_g$ (see [6, p. 587]). Also, we have $(c - h_{\mathbb{R}})$ 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 $(c - h_{\mathbb{R}})/2$ pairs. This gives us in all $h_{\mathbb{Q}}$ 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 $g^j \sim g^{\varepsilon}$, $\varepsilon = 1, -1$. Thus the only $\mathbb{Q}$-conjugate classes are C_g or $C_g \cup C_{g^{-1}}$. Their total number $h_{\mathbb{Q}} = h_{\mathbb{R}} + \frac{c - h_{\mathbb{R}}}{2}$. Thus $\rho = 0$ as desired. $\blacksquare$

6. Trivial central units

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

$$\mathbb{Q}G = \sum^{\oplus} S_i$$

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

$$\mathfrak{Z}\mathbb{Q}G \simeq \sum^{\oplus} \mathbb{Q}(\chi),$$

which on class sums C_g is

$$C_g \mapsto \sum \frac{h_g}{\chi(1)} \chi(g),$$

where $h_g = |C|$. Moreover

$$\mathfrak{Z}(\mathbb{Z}G) \hookrightarrow \sum^{\oplus} \mathbb{Z}[\chi].$$

Let R be a G-adapted ring. Then

$$\mathfrak{Z}(RG) = R \otimes_{\mathbb{Z}} \mathfrak{Z}(\mathbb{Z}G) \hookrightarrow \sum^{\oplus} R \otimes_{\mathbb{Z}} \mathbb{Z}[\chi].$$

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

$$\mathfrak{Z}(RG) \hookrightarrow \sum_{\chi}^{\oplus} R \otimes_{Z} \mathbb{Z}[\chi] \tag{6.1}$$

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

$$\sum \alpha_i C_i \mapsto \frac{\sum \alpha_i h_i \chi_1(g_i)}{\chi_1(1)}, \ldots, \frac{\sum \alpha_i h_i \chi_j(g_i)}{\chi_j(1)}, \ldots, \frac{\sum \alpha_i h_i \chi_c(g_i)}{\chi_c(1)} \tag{6.2}$$

where $h_i = |C_{g_i}|$ and $\chi_1, \ldots, \chi_c$ are the irreducible complex characters.

We shall now characterise groups G so that central units $\mathfrak{Z}(\mathcal{U}(RG))$ 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, ζ_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 $(R \otimes_Z Z[\zeta_{|G|}]/|G|)^\times$ is torsion. Then $\mathfrak{Z}(\mathcal{U}(RG))$ is trivial if and only if $(R \otimes_{\mathbb{Z}} \mathbb{Z}[\chi])^\times$ is torsion for all complex characters χ.*

Proof.

a) ($\Leftarrow$) Suppose that $(R \otimes_{\mathbb{Z}} \mathbb{Z}[\chi])^\times$ is torsion. From the embedding

$$\mathfrak{Z}(RG) \hookrightarrow \sum^{\oplus} R \otimes_{\mathbb{Z}} \mathbb{Z}[\chi]$$

we conclude that $\mathcal{U}(\mathfrak{Z}(RG))$ 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 $\mathfrak{Z}(\mathcal{U}(\mathbb{Z}G))$ is trivial. We have (6.1) and (6.2). Suppose that there exists an $\varepsilon \in (R \otimes_{\mathbb{Z}} \mathbb{Z}[\chi])^\times$ 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 ε by ε^n.

We represent the map (6.2) as

$$\sum \alpha_i C_i \mapsto \left[\frac{h_j \chi_i(g_j)}{\chi_i(1)}\right]_{i,j} \begin{bmatrix}\alpha_1\\ \vdots \\ \alpha_c\end{bmatrix} = M \begin{bmatrix}\alpha_1\\ \vdots \\ \alpha_c\end{bmatrix},$$

where

$$M = \begin{bmatrix} 1 & h_1 & \cdots & h_c \\ 1 & & & \\ \vdots & & * & \\ 1 & & & \end{bmatrix}.$$

We define $\tilde{\mathbb{Z}} = \mathbb{Z}[\chi_i(g_j) : 1 \le i,j \le c]$ and claim for the determinant that there exists an exponent d such that

$$|M| = \det\ M \text{ is a divisor of } |G|^d \text{ in } \tilde{\mathbb{Z}}.$$

Let M^* be the conjugate transpose. Then the orthogonality relations yield

$$|M| = \left|\frac{h_j \chi_i(g_j)}{\chi_i(1)}\right| = \frac{\prod h_j}{\prod \chi_i(1)}\ |\chi_i(g_j)|,$$

$$|MM^*| = \left(\frac{\prod h_j}{\prod \chi_i(1)}\right)^2\ |[\chi_i(g_j)]_{i,j}||[\ \overline{\chi_\nu(g_\mu)}\ ]_{\mu,\nu}|$$

$$= \frac{\prod h_j}{\left(\prod \chi_i(1)\right)^2}\ \left|\left[\sum_k\ h_k \chi_i; (g_k)\ \overline{\chi_j(g_k)}\ \right]\right|$$

$$= \frac{\prod h_j}{\left(\prod \chi_i(1)\right)^2}\ |[\delta_{ij}|G|]| = \frac{|G|^c \cdot \prod_j\ h_j}{\left(\prod_i\ \chi_i(1)\right)^2}.$$

Thus we have $|MM^*|\left(\prod_i\ \chi_i(1)\right)^2 = |G|^c\left(\prod_j\ h_j\right)$, and the claim follows from $h_j \big|\ |G|\ , \chi_i(1) \big|\ |G|$ and $M \in (\tilde{\mathbb{Z}})_{c\times c}$ (see [6, p. 481]).

We wish to find $\alpha_1, \alpha_2, \ldots, \alpha_c$ so that

$$M \begin{bmatrix}\alpha_1\\ \vdots \\ \alpha_c\end{bmatrix} = \begin{bmatrix}\vdots\\ \varepsilon \\ \bar{\varepsilon} \\ \vdots\end{bmatrix} \text{ with the dots on the right representing ones,}$$

where $\bar{\varepsilon}$ is the algebraic conjugate of ε. We have

$$\begin{bmatrix} 1 & h_2 \ldots h_c \\ 1 & \\ \vdots & * \\ 1 & \end{bmatrix} \begin{bmatrix}\alpha_1\\ \vdots \\ \alpha_c\end{bmatrix} = \begin{bmatrix}\vdots\\ \varepsilon \\ \bar{\varepsilon} \\ \vdots\end{bmatrix}.$$

Subtracting the first row from all others gives

$$\begin{bmatrix} 1 & h_2 \cdots h_c \\ 0 & \\ 0 & M' \\ \vdots & \\ 0 & \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_c \end{bmatrix} = \begin{bmatrix} 1 \\ \vdots \\ \varepsilon - 1 \\ \overline{\varepsilon} - 1 \\ \vdots \end{bmatrix},$$

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

$$M' \begin{bmatrix} \alpha_2 \\ \vdots \\ \alpha_c \end{bmatrix} = \begin{bmatrix} \vdots \\ \varepsilon - 1 \\ \overline{\varepsilon} - 1 \\ \vdots \end{bmatrix}.$$

Note that det $M =$ det M'. Multiplication with the adjoint matrix of M' from the left yields

$$(\text{Adj } M')M' \begin{bmatrix} \alpha_2 \\ \vdots \\ \alpha_c \end{bmatrix} = (\text{Adj } M') \begin{bmatrix} \vdots \\ \varepsilon - 1 \\ \overline{\varepsilon} - 1 \\ \vdots \end{bmatrix},$$

i.e.,

$$|M'| \begin{bmatrix} \alpha_2 \\ \vdots \\ \alpha_c \end{bmatrix} = (\text{Adj } M') \begin{bmatrix} \vdots \\ \varepsilon - 1 \\ \overline{\varepsilon} - 1 \\ \vdots \end{bmatrix}.$$

Since det $M =$ det M' is a divisor of $|G|^d$ and $\varepsilon \equiv 1 \bmod |G|^d$, the system of equations can be solved in $R \otimes_{\mathbb{Z}} \tilde{\mathbb{Z}}$. In order to see that the unique solution actually belongs to $R = R \otimes_{\mathbb{Z}} \mathbb{Z}$, we apply the automorphisms σ from the Galois group A of $\mathbb{Q}(\chi_i(g_j))/\mathbb{Q}$ to it. Note that A is an elementary abelian 2-group and that, to χ with $\mathbb{Z} \neq \mathbb{Z}[\chi]$, 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, $\sigma_\chi(\varepsilon) = \overline{\varepsilon}$ for our χ. 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 ε^{-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 χ.*

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

References

[1] R.G. Ayoub and C. Ayoub, On the group ring of a finite abelian group, *Bulletin of the Australiam Mathematical Society* **1** (1969), 245–61.

[2] C.W. Curtis and I. Reiner, Representation theory of finite groups and associative algebras, *Interscience*, New York, 1962.

[3] M. Dokuchaev, C. Polcino Milies and S.K. Sehgal, Integral group rings with trivial central units II, *Communications in Algebra* **32** (2004), 4579–85.

[4] M. Hertweck, Contributions to the integral representation theory of groups, Habilitation thesis, University of Stuttgart, Germany, 2003.

[5] G. Higman, The units of group rings, *Proceedings of the London Mathematical Society* **46** (1940), 231–48.

[6] B. Huppert, *Endliche gruppen I*, Springer Verlag, Heidelberg, 1967.

[7] S. Lang, *Algebraic number theory,* Addison-Wesley, Reading, 1970.

[8] J. Ritter and S.K. Sehgal, Integral group rings with trivial central units, *Proceedings of the American Mathematical Society* **108** (1990), 327–9.

[9] S.K. Sehgal, *Topics in group rings,* M. Dekker, New York, 1978.

[10] S.K. Sehgal, *Units in integral group rings,* Longman, New York, 1993.