

TRIVIAL UNITS FOR GROUP RINGS OVER RINGS OF ALGEBRAIC INTEGERS

ALLEN HERMAN AND YUANLIN LI

(Communicated by Martin Lorenz)

ABSTRACT. Let G be a nontrivial torsion group and R be the ring of integers of an algebraic number field. The necessary and sufficient conditions are given under which RG has only trivial units.

1. INTRODUCTION

If R is a ring with unity and G is a group, we say that the group ring RG has only trivial units if $U(RG) = U(R)G$. A well-known theorem of Higman states that the integer group ring $\mathbb{Z}G$ for a finite group G can have only trivial units only when G is either an abelian group of exponent dividing 4 or 6, or the direct product of an elementary abelian 2-group E_2 with a quaternion group Q_8 of order 8 [5, Theorem 8.2.6]. In [1], for each such group G , conditions on commutative rings with unity R were given which guarantee that RG has only trivial units. In this note, we give a complete description of the rings of integers of algebraic number fields which satisfy these conditions. Surprisingly, it turns out that the examples among quadratic number fields described in [1] are the only ones among all algebraic number fields. We remark that although [1] considered finite groups G only, the conditions mentioned above still hold when G is a torsion group and the above Higman's Theorem also holds for torsion groups. Our main result is as follows.

Theorem 1.1. *Let G be a nontrivial torsion group and let R be the ring of integers of an algebraic number field. Then RG has only trivial units if and only if one of the following conditions holds.*

- (1) G is an abelian group of exponent 2, and R is the ring of algebraic integers of either \mathbb{Q} or $\mathbb{Q}(\sqrt{-d})$, where d is either 1 or a square-free positive integer.
- (2) G is an abelian group of exponent 4, and R is either \mathbb{Z} or $\mathbb{Z}[\sqrt{-1}]$.
- (3) G is an abelian group of exponent 3 or 6, and R is either \mathbb{Z} or $\mathbb{Z}[\zeta_3]$, where $\zeta_3 = \frac{-1+\sqrt{-3}}{2}$.
- (4) $G = E_2 \times Q_8$ is a Hamiltonian 2-group, and $R = \mathbb{Z}$.

Received by the editors August 6, 2004 and, in revised form, October 1, 2004.

2000 *Mathematics Subject Classification.* Primary 16S34; Secondary 16U60.

Key words and phrases. Group rings, units, rings of algebraic integers.

This research was supported in part by Discovery Grants from the Natural Sciences and Engineering Research Council of Canada.

Throughout this paper, R always denotes the ring of integers of an algebraic number field unless otherwise mentioned, and G is an arbitrary torsion group. We will prove the main theorem by using case by case arguments in the following two sections.

2. ABELIAN GROUPS OF EXPONENT DIVIDING 4

This section deals with the case where G is an abelian group of exponent dividing 4. By using Theorem 2.2 and some other results proved in [1], we are also able to handle the case where G is a Hamiltonian 2-group.

Let C_2 be a cyclic group of order 2, and let R be a commutative ring with unity. In [1, Proposition 1], the authors and M.M. Parmenter showed that the group ring RC_2 has only trivial units if and only if R satisfies the condition stated in the next proposition.

Proposition 2.1. *Let R be a commutative ring with unity. Then RC_2 has only trivial units if and only if whenever $2r - 1 \in U(R)$ for $r \in R$, then $r = 0, 1$. Here the element $r \in R$ occurs as the coefficient of g in the unit $(1 - r) + rg$.*

Examples among polynomial rings and the rings of integers of quadratic number fields were considered in [1]. It was shown there that when d is a square-free positive integer greater than 1, then $\mathbb{Z}[\sqrt{d}]C_2$ has nontrivial units. On the other hand, if d is a square-free positive integer, then it was shown there that $\mathbb{Z}[\sqrt{-d}]C_2$ has only trivial units. If R is the ring of integers of $\mathbb{Q}(\sqrt{-d})$ and $d \not\equiv 3 \pmod{4}$, then $R = \mathbb{Z}[\sqrt{-d}]$, so RC_2 has only trivial units. If $d \equiv 3 \pmod{4}$, then every element of R can be written as $\frac{1}{2}(m + n\sqrt{-d})$, with $m, n \in \mathbb{Z}$ being either both even or both odd. If $r = \frac{1}{2}(m + n\sqrt{-d}) \in R$ with the property that $2r - 1 \in U(R)$, then the norm of $2r - 1$ has to be an integer unit, and hence be ± 1 . This implies that $(m - 1)^2 + dn^2 = \pm 1$. The right side clearly cannot be -1 , so $(m - 1)^2 = 1 - dn^2$. This forces $n = 0$, and $m = 0$ or 2 . Therefore, r has to be 0 or 1 . We can conclude, therefore, that if R is the ring of integers of an imaginary quadratic number field, then RC_2 has only trivial units. The next result shows that these are the only algebraic number fields other than \mathbb{Q} with this property.

Theorem 2.2. *Suppose R is the ring of integers in an algebraic number field K , with the property that RC_2 has only trivial units. Then K is either \mathbb{Q} or an imaginary quadratic number field.*

Proof. It follows from Proposition 2.1 that for each $r \in R$, if $2r - 1$ is a unit, then $r = 0$ or 1 . Hence $\Gamma = \{u \in U(R) : u = 2r - 1, r \in R\} = \{\pm 1\}$. However, this is the congruence subgroup of $R \pmod{2}$, i.e., the kernel of the homomorphism $U(R) \rightarrow U(R/2R)$ given by $u \mapsto u + 2R$. It is well known that $R/2R$ is finite (see, for example, [3, Proposition 12.2.3]), so Γ is a subgroup of $U(R)$ of finite index. Thus the only way that Γ can be finite is for $U(R)$ to be finite.

Since K is a finite extension of \mathbb{Q} , it follows from a corollary of Dirichlet's Unit Theorem [5, Corollary 2.8.3] that either $K = \mathbb{Q}$ or $K = \mathbb{Q}(\sqrt{-d})$ for some square-free positive integer d . \square

It was shown in [1] that if RC_2 has only trivial units, then RE_2 also has only trivial units, where E_2 is an elementary abelian 2-group. We now have the following.

Corollary 2.3. *Let R be the ring of integers in an algebraic number field K and let $G = E_2$ be an elementary abelian 2-group. Then RG has only trivial units if and only if K is either \mathbb{Q} or $\mathbb{Q}[\sqrt{-d}]$, where d is a square-free positive integer.*

When G is an abelian group of exponent 4, it was shown in [1] that \mathbb{Z} and $\mathbb{Z}[i]$ (here $i = \sqrt{-1}$) are the only examples of rings R of integers in quadratic number fields for which RC_4 and thus RG have only trivial units. By the above, these are also the only two rings of integers in algebraic number fields for which RG has only trivial units.

Corollary 2.4. *Suppose R is the ring of algebraic integers in an algebraic number field and G is an abelian group of exponent 4. RG has only trivial units if and only if R is either \mathbb{Z} or $\mathbb{Z}[i]$.*

We note that if RQ_8 has only trivial units, then RC_4 has only trivial units. Since $\mathbb{Z}[i]Q_8$ has nontrivial units [1, paragraph following Corollary 3], it follows from Corollary 2.4 that \mathbb{Z} is the unique ring of integers in an algebraic number field for which RQ_8 (and thus also $R[Q_8 \times E_2]$) has only trivial units.

Corollary 2.5. *Suppose R is the ring of algebraic integers of an algebraic number field and $G = Q_8 \times E_2$ is a Hamiltonian 2-group. Then RG has only trivial units if and only if $R = \mathbb{Z}$.*

One can also reach this conclusion using the following recent result of Mazur.

Theorem 2.6 ([4, Theorem 5]). *Let R be an integrally closed subring of an algebraic number field K such that $\frac{1}{2} \notin R$. Then Q_8 is normal in $U(RQ_8)$ if and only if K is totally real and R is its ring of algebraic integers.*

An alternative proof of Corollary 2.5 is as follows.

Proof. Assume that $R(Q_8 \times E_2)$ has only trivial units, so does RQ_8 . In order for $U(RQ_8) = U(R)Q_8$, it is necessary that Q_8 be a normal subgroup of $U(RQ_8)$. By Theorem 2.6, this forces K to be totally real. Since C_2 is a subgroup of Q_8 , RC_2 must also have only trivial units. Since K is totally real, by Theorem 2.2 we must have $K = \mathbb{Q}$, and so $R = \mathbb{Z}$. The other direction is obvious. \square

Using Mazur's result, we can relax the assumptions of Corollary 2.5 to conclude that \mathbb{Z} is the only integrally closed C_2 -adapted subring R of an algebraic number field such that RQ_8 has only trivial units.

3. ABELIAN GROUPS OF EXPONENT 3 OR 6

In this section, we deal with the case where G is an abelian group of exponent 3 or 6. Let C_3 denote a cyclic group of order 3. The condition on R which guarantees that RC_3 has only trivial units is the following [1, Proposition 3].

Proposition 3.1. *Let R be a commutative ring with unity. Then RC_3 has only trivial units if and only if for each pair $a, b \in R$ such that $1 + 3(a + a^2 + b^2 - ab) \in U(R)$, (a, b) is either $(0, 0)$, $(-1, 0)$, or $(-1, -1)$. Here the elements $a, b \in R$ occur in the expression of the unit $1 + (1 - g)(a + bg)$.*

Lemma 3.2. *Let R be a commutative ring of characteristic 0, and suppose $x \in R$ is such that $1 + 3x \in U(R)$. Let $a = 2x$ and $b = x$. Then $1 + 3(a + a^2 + b^2 - ab) \in U(R)$.*

Proof. Since $1+3x \in U(R)$, $(1+3x)^2 \in U(R)$, and thus $(1+3x)^2 = 1+3(2x+3x^2) = 1+3(2x+4x^2+x^2-2x^2) = 1+3(a+a^2+b^2-ab) \in U(R)$. \square

Theorem 3.3. *Suppose R is the ring of algebraic integers in an algebraic number field K , with the property that RC_3 has only trivial units. Then K is either \mathbb{Q} or an imaginary quadratic number field.*

Proof. If the algebraic number field K is not \mathbb{Q} or an imaginary quadratic number field, then by Dirichlet's unit theorem $U(R)$ is infinite. Since the 3-congruence subgroup of $U(R)$ has finite index, it follows that there are infinitely many units of the form $1+3x$, for $x \in R$. If we choose $x \neq 0$ such that $1+3x \in U(R)$, then by Lemma 3.2 there exists $a, b \in R$ such that $1+3(a+a^2+b^2-ab) \in U(R)$ and (a, b) is not one of $(0, 0)$, $(-1, 0)$, and $(-1, -1)$. Thus the condition in Proposition 3.1 fails, and thus RC_3 has nontrivial units. This contradiction finishes the proof. \square

It was remarked in [1] that $\mathbb{Z}[\zeta_3]$ (here $\zeta_3 = \frac{-1+\sqrt{-3}}{2}$) is the only ring of integers in an imaginary quadratic number field that satisfies the condition in Proposition 3.1. We include a proof of this statement for completeness.

Proposition 3.4. *Let R be the ring of integers in an imaginary quadratic number field $K = \mathbb{Q}(\sqrt{-d})$ where d is a square-free positive integer. Then RC_3 has only trivial units if and only if $R = \mathbb{Z}[\zeta_3]$.*

Proof. We first show that if $\mathbb{Z}[\sqrt{-d}]C_3$ has only trivial units, then $d = 3$. If $d = 1$, then in the ring of Gaussian integers $\mathbb{Z}[i]$, we can take $a = i$ and $b = 1$ to obtain $a^2+b^2-ab+a = 0$, so $\mathbb{Z}[i]C_3$ has nontrivial units. In the case of rings $R = \mathbb{Z}[\sqrt{-d}]$, d a square-free positive integer > 1 . Then it follows from norm considerations that the only unit of R of the form $1+3(m+n\sqrt{-d})$ for $m, n \in R$ is 1. This is because the norm of $1+3(m+n\sqrt{-d})$, which is $1+6m+9m^2+9dn^2$, has to be ± 1 , so the only solution is to have $m+n\sqrt{-d} = 0$. So the condition under which $\mathbb{Z}[\sqrt{-d}]C_3$ has nontrivial units is equivalent to solving $a^2+b^2+a-ab = 0$ with $(a, b) \neq (0, 0)$, $(-1, 0)$, or $(-1, -1)$. Solving for b produces

$$b = \frac{a \pm \sqrt{-3a^2 - 4a}}{2}.$$

If d is not divisible by 3, then we claim that this equation is always solvable with a an even nonzero integer and $b \in \mathbb{Z}[\sqrt{-d}]$. Since $(d, 3) = 1$, $3d$ is square-free, and so the Pell equation $x^2 - 3dy^2 = 1$ has infinitely many integer solutions. Let (s, t) be any solution, and consider the quadratic equation $-3a^2 - 4a + 4dt^2 = 0$. Solving for a we have

$$a = \frac{4 \pm \sqrt{16 + 48dt^2}}{-6} = -\frac{2}{3} \pm \frac{2}{3}\sqrt{1 + 3dt^2} = -\frac{2}{3} \pm \frac{2}{3}s.$$

If $s \equiv 1 \pmod{3}$, then by choosing the positive sign we have that a is an even integer. If $s \equiv -1 \pmod{3}$, then choosing the negative sign we get that a is an even integer. When a is even, we have that $b = \frac{a \pm 2t\sqrt{-d}}{2} \in \mathbb{Z}[\sqrt{-d}]$. This shows that there are infinitely many solutions to $a^2+b^2+a-ab = 0$ in $\mathbb{Z}[\sqrt{-d}]$, so the condition is satisfied.

Now suppose $d > 3$ and 3 divides d . Write $d = 3e$, and note that $(3, e) = 1$ since d is square-free. Consider the Pell equation $x^2 - ey^2 = 1$. We claim that there exists a solution (s, t) such that t is divisible by 3. If (s, t) is a solution with t not divisible by 3, then set $(s+t\sqrt{e})^2 = (s^2+et^2) + (2st)\sqrt{e} := s_1 + t_1\sqrt{e}$. From

standard results on Pell equations, we know that (s_1, t_1) is another solution to the Pell equation $x^2 - ey^2 = 1$. If s is divisible by 3, then we now have that t_1 is divisible by 3. If s is also not divisible by 3, then t_1 is not divisible by 3, and so it follows from $(s_1)^2 - e(t_1)^2 = 1$ that $2 + e \equiv 1 \pmod{3}$, and hence $e \equiv 2 \pmod{3}$. Then $s_1 = s^2 + et^2$ is divisible by 3, so we are back in the previous case. Now let (s, t) be a solution to the Pell equation $s^2 - et^2 = 1$ with t divisible by 3, and let $t = 3u$. Then we have $s^2 = 1 + 9eu^2 = 1 + 3du^2$. Considering the quadratic equation $-3a^2 - 4a + du^2 = 0$, we have

$$a = \frac{4 \pm \sqrt{16 + 12du^2}}{-6} = -\frac{2}{3} \pm \frac{2}{3} \sqrt{1 + 3du^2} = -\frac{2}{3} \pm \frac{2}{3}s,$$

and again by choosing the sign appropriately we can arrange for a to be an even integer. So as in the previous paragraph the condition is satisfied.

Now if RC_3 has only trivial units, so does $\mathbb{Z}[\sqrt{-d}]C_3$. By the above, $d = 3$ and thus $R = \mathbb{Z}[\zeta_3]$, the ring of algebraic integers of $\mathbb{Q}(\sqrt{-3})$. Conversely, if $R = \mathbb{Z}[\zeta_3]$, it follows from [2, Theorems 2 and 3] that RC_3 has only trivial units. We are done. \square

(It is a consequence of the above that the only solutions to $a + a^2 + b^2 - ab = 0$ in $\mathbb{Z}[\zeta_3]$ are $(a, b) = (0, 0)$, $(0, -1)$, and $(-1, -1)$. We know of no elementary proof of this, which necessitates our appeal to Higman's results to complete the proof.)

It follows from Theorem 3.3 and Proposition 3.4 that \mathbb{Z} and $\mathbb{Z}[\zeta_3]$ are the only rings of integers of algebraic number fields for which RC_3 has only trivial units. If R is the ring of integers of an algebraic number field for which RC_6 and thus both RC_2 and RC_3 have only trivial units, then $R = \mathbb{Z}$ or $\mathbb{Z}[\zeta_3]$. Of course, the same conclusion holds for abelian groups of exponent 6 by [1, Propositions 2 and 4].

Corollary 3.5. *Let R be the ring of algebraic integers in an algebraic number field and let G be an abelian group of exponent 3 or 6. Then RG has only trivial units if and only if R is either \mathbb{Z} or $\mathbb{Z}[\zeta_3]$.*

REFERENCES

- [1] A. Herman, Y. Li and M.M. Parmenter, *Trivial units in group rings with G -adapted coefficient rings*, *Canad. Math. Bull.*, (1) **48** (2005), 80–89. MR2118765
- [2] G. Higman, *The units of group-rings*, *Proc. London Math. Soc.*, (2)**46**, (1940), 231 - 248. MR0002137 (2:5b)
- [3] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory, 2nd Ed.*, Springer-Verlag, 1990. MR1070716 (92e:11001)
- [4] M. Mazur, *Groups normal in the unit groups of their group rings*, preprint.
- [5] C. Polcino Milies and S.K. Sehgal, *An Introduction to Group Rings*, Kluwer Academic Publishers, Dordrecht, 2002. MR1896125 (2003b:16026)

DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY OF REGINA, REGINA, SASKATCHEWAN, CANADA S4S 0A2

E-mail address: aherman@math.uregina.ca

DEPARTMENT OF MATHEMATICS, BROCK UNIVERSITY, ST. CATHARINE'S, ONTARIO, CANADA L2S 3A1

E-mail address: yli@brocku.ca