On Duo Group Rings[1]

Weidong Gao
Center for Combinatorics, Nankai University
Tianjin, 300071, P.R. China
Email: gao@cfc.nankai.edu.cn

Yuanlin Li
Department of Mathematics, Brock University, St. Catharines,
Ontario, L2S 3A1, Canada
E-mail: yli@brocku.ca

Abstract. It is shown that if the group ring RQ_8 of the quaternion group Q_8 of order 8 over an integral domain R is duo, then R is a field for the following cases: (1) char $R \neq 0$, and (2) char $R = 0$, and $S \subseteq R \subseteq K_S$, where S is a ring of algebraic integers and K_S is its quotient field. Hence we confirm that the field $\mathbb{Q}$ of rational numbers is the smallest integral domain R of characteristic zero such that RQ_8 is duo. A non-field integral domain R of characteristic zero for which RQ_8 is duo is also identified.

2000 Mathematics Subject Classification: 16S34, 16S99, 16U80

Keywords: Duo ring, Group ring, Reversible ring

1. Introduction

An associative ring R is called left (right) duo if every left (right) ideal is an ideal, and R is said to be duo if it is both left and right duo. R is defined to be reversible if $\alpha\beta = 0$ implies $\beta\alpha = 0$ for all $\alpha, \beta \in R$.

Let k be a commutative ring with identity and G be any group. Using the standard involution $*$ on the group ring kG, defined by $(\sum a_i g_i)^* = \sum a_i g_i^{-1}$ for all $a_i \in k$ and $g_i \in G$, we can easily see that the three duo conditions defined on kG are equivalent.

It follows from a result of Marks [4] and a remark of Bell and the second author [1] that if the group ring kG of an arbitrary group G over a commutative ring k is duo, then it is reversible. The question of when a reversible group ring kG is duo was investigated and all duo group algebras KG of torsion groups G over fields K were characterized in [1]. It was shown that such a group algebra is duo if and only if it is reversible (see [2, 3] for the discussion of the reversibility of group rings). It was also pointed out that a reversible group ring kG is not necessarily duo; for example, the integral group ring $\mathbb{Z}Q_8$ of the quaternion group Q_8 of order 8 is a reversible ring,

[1]The first author was supported in part by the Natural Science Foundation of China and the second author was supported in part by a Discovery Grant from the Natural Sciences and Engineering Research Council of Canada.

but not a duo ring [1, Example 1.1]. A natural question which arises is as follows:

Question 1.1. *Is there any ring R between $\mathbb{Z}$ and $\mathbb{Q}$ (in addition to $\mathbb{Q}$ the field of all rational numbers), such that RQ_8 is duo.*

In this paper, we investigate a more general question of when an integral domain R is a field under the assumption that RQ_8 is duo. We give an affirmative answer to the question for many cases. Our main result is Theorem 2.4, showing that if R is an integral domain such that RQ_8 is duo, then R is a field for the following cases: (1) char $R \neq 0$, and (2) char $R = 0$, and $S \subseteq R \subseteq K_S$, where S is a ring of algebraic integers and K_S is its quotient field. In particular, this shows that there does not exist any ring R between $\mathbb{Z}$ and $\mathbb{Q}$ (except for $\mathbb{Q}$) such that RQ_8 is duo. Thus, $\mathbb{Q}$ is the smallest integral domain R (up to isomorphism) of characteristic zero for which the group ring RQ_8 is duo. It is also proved that there exists an integral domain R that is not a field for which RQ_8 is duo (Proposition 2.6). We remark that for a non-abelian torsion group G, if RG is duo, then RQ_8 is always duo (Remark 2.8). So we will use the latter weaker assumption when it is required.

Throughout the paper, R and R_K denote an integral domain and its quotient field respectively. $\mathcal{U}(R)$ denotes the unit group of R and, as mentioned before, $Q_8 = \langle a, b | a^4 = 1, a^2 = b^2, a^b = a^{-1}\rangle$ denotes the quaternion group of order 8. Our other notation is standard and follows that in [6].

2. Main result

We begin with two lemmas which will be required later. The first lemma is a well known result in number theory and it is a consequence of [5, Theorem 5.14].

Lemma 2.1. $1 + x^2 + y^2 \equiv 0$ *(mod p) is solvable in $\mathbb{Z}$ for every prime p.*

Lemma 2.2. *Let R be an integral domain such that RQ_8 is duo. If $1+x^2+y^2 \neq 0$ for some $x, y \in R$, then $1 + x^2 + y^2$ is invertible in R.*

Proof. If R is finite, then R is a field, and thus the result holds. From now on we may assume that R is infinite.

For $x, y \in R$, let $L = (RQ_8)(1 + xa + yb)$ be a left ideal. Since RQ_8 is duo, we know that L is also a right ideal. Thus,

$$(1 + xa + yb)a = (\sum_{i=0}^{3} a_i a^i + \sum_{j=4}^{7} a_j a^{j-4} b)(1 + xa + yb) \in L,$$

where $a_i \in R$ for $i = 0, 1, \cdots, 7$, or

$$a + xa^2 + ya^3 b = (\sum_{i=0}^{3} a_i a^i + \sum_{j=4}^{7} a_j a^{j-4} b)(1 + xa + yb) \tag{2.1}$$

Simplifying and then comparing the coefficients of group elements on both sides of the above equation, we obtain the following system.

$$
\begin{cases}
a_0 + xa_3 + ya_6 = 0 \\
xa_0 + a_1 + ya_7 = 1 \\
xa_1 + a_2 + ya_4 = x \\
xa_2 + a_3 + ya_5 = 0 \\
ya_0 + a_4 + xa_5 = 0 \\
ya_1 + a_5 + xa_6 = 0 \\
ya_2 + a_6 + xa_7 = 0 \\
ya_3 + xa_4 + a_7 = y
\end{cases}
\tag{2.2}
$$

It is not hard to see that the determinant of the coefficient matrix A of System (2.2) is as follows:

$$
\det(A) = y^8 - 2y^4 - 8y^4x^2 - 2y^4x^4 - 8y^2x^2 - 8y^2x^4 - 2x^4 + x^8 + 1. \tag{2.3}
$$

If $\det(A) \neq 0 \in R$, then solving System (2.2) in the quotient field of R, we obtain the following result.

$$
\begin{aligned}
a_0 &= 0 \\
a_1 &= \tfrac{1+x^2}{1+y^2+x^2} \\
a_2 &= 0 \\
a_3 &= \tfrac{y^2}{1+y^2+x^2} \\
a_4 &= \tfrac{yx}{1+y^2+x^2} \\
a_5 &= -\tfrac{y}{1+y^2+x^2} \\
a_6 &= -\tfrac{yx}{1+y^2+x^2} \\
a_7 &= \tfrac{y}{1+y^2+x^2}
\end{aligned}
$$

In particular, if $\det(A) \neq 0$, then

$$
(1 + x^2 + y^2)a_1 = 1 + x^2. \tag{2.4}
$$

We first prove that if $1 + y_0^2 \neq 0$ for some $y_0 \in R$, then $1 + y_0^2$ is invertible in R. Set $z = 1 + y_0^2$. Then z is a factor of $1 + (y_0 + wz)^2$ for all $w \in R$. Let $x = 0$. Then $\det(A) = (y^4 - 1)^2$ and it has only finite zeros in R (in fact, it has at most 4 distinct zeros in R). Since R is infinite, its subset $S = \{y_0 + wz|\ w \in R\}$ has infinite many elements, so we can always choose an element $y \in S$ such that $\det(A) \neq 0$. Now by (2.4), $(1 + y^2)a_1 = 1$. Therefore, $1 + y^2$ is invertible in R, and hence $z = 1 + y_0^2$ (as a factor of $1 + y^2$) is also invertible in R.

Let $u = (1 + x^2 + y^2) \neq 0$ for some $x, y \in R$. Then as before, u is a factor of $1 + (x + wu)^2 + y^2$ for all $w \in R$. Note that for a fixed $y \in R$, $\det(A)$ has at most finite zeros in R. Since R is infinite, as before, we can choose an element $x_1 \in \{x + wu|\ w \in R\}$ such that $1 + x_1^2 \neq 0$ and $\det(A) \neq 0$. Substituting x by x_1 in (2.4), we have $(1 + x_1^2 + y^2)a_1 = 1 + x_1^2$. Since

$1 + x_1^2 \neq 0$, by what we just proved, it must be invertible in R, and thus $1+x_1^2+y^2$ is also invertible in R. Since $1+x^2+y^2$ is a factor of the invertible element $1 + x_1^2 + y^2$, it is also invertible in R and we are done. □

We note that if R is an integral domain such that RQ_8 is duo, then RQ_8 is reversible. It follows from [3, Theorem 2.5] that the characteristic of R is either 2 or 0. In the latter case, by [3, Theorem 4.2] (see also [2, Theorem 3.1]), we have $1 + x^2 + y^2 \neq 0$, for all $x, y \in R$. As a consequence of the above lemma, we obtain

Corollary 2.3. *Let R be an integral domain such that RQ_8 is duo. Then char $R = 2$ or char $R = 0$. In the latter case, we have $1 + x^2 + y^2 \in \mathcal{U}(R)$, for all $x, y \in R$.*

We are now ready to show our main result.

Theorem 2.4. *Let R be an integral domain such that RQ_8 is duo. Then the following statements hold.*

(1) *If $char(R) \neq 0$, then R must be a field.*
(2) *If S is a ring of algebraic integers with its quotient field K_S such that $S \subseteq R \subseteq K_S$, then $R = K_S$. In particular, if $\mathbb{Z} \subseteq R \subseteq \mathbb{Q}$, then $R = \mathbb{Q}$.*

Proof. (1) We note that $char(R) = 2$ by Corollary 2.3. Let $\alpha \neq 0 \in R$ and $x = \alpha - 1 \in R$. Then $1 + x^2 = (1 + x)^2 = \alpha^2 \neq 0$. It follows from Lemma 2.2 that α^2 is invertible in R and so is α. Therefore, R is a field.

(2) We need only show that $K_S \subseteq R$. To do this, it suffices to prove that every nonzero element $\alpha \in S$ is invertible in R. We first prove that if $0 \neq \alpha \in \mathbb{Z}$, then α is invertible in R. Let p be any prime. By Lemma 2.1, $p|1 + x^2 + y^2$ for some integers $x, y \in \mathbb{Z}$. It follows from Corollary 2.3 that $1 + x^2 + y^2$, and thus p is invertible in R. Since every integer greater than 1 can be expressed as a product of primes, it follows that α is invertible in R.

We now turn to the general case when $0 \neq \alpha \in S$. By the definition of algebraic integers, there is a monic polynomial $f(x) \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$. Suppose that

$$f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0,$$

where all $c_i \in \mathbb{Z}$ and $c_0 \neq 0$. Then

$$\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 = 0,$$

or

$$(\alpha^{n-1} + c_{n-1}\alpha^{n-2} + \cdots + c_1)\alpha = -c_0.$$

As proved above, $-c_0$ is invertible in R, so α is also invertible in R. This completes the proof. □

Corollary 2.5. *Let R be an integral domain of char $R = 0$ such that RQ_8 is duo, and let M be any maximal ideal of R. Then char $(R/M) = 0$ and $(R/M)Q_8$ is duo.*

Proof. Since M is a maximal idea of R, R/M is a field. By Lemma 2.1 and Corollary 2.3, we know that every prime is invertible in R, so it is not in M. Therefore, char $(R/M) = 0$. Again by Corollary 2.3, we know that for any $x_0, y_0 \in R$, $1 + x_0^2 + y_0^2$ is invertible, so it is not in M. This shows that the equation $1 + x^2 + y^2 = 0$ has no solutions in R/M. By [1, Theorem 2.1], we conclude that $(R/M)Q_8$ is duo. □

The following proposition shows that there exists an integral domain R which is not a field such that RQ_8 is duo.

Proposition 2.6. *Let $S = \mathbb{Q}[x]$ be the polynomial ring over the rational field, and S_P be the localization of S at the maximal ideal $P = \langle x \rangle$. Then $R = S_P$ is a local integral domain of characteristic 0, but not a field, such that RQ_8 is duo.*

Proof. Clearly R is a local integral domain of characteristic 0, but not a field (as x is not invertible in R).

We next make the following easy observations:

For all $z_1, \cdots, z_r \in R$, we have

(1) $z_1^2 + \cdots + z_r^2 = 0$ if and only if $z_1 = \cdots = z_r = 0$.

(2) $z_1^2 + \cdots + z_r^2$ is invertible in R if and only if at least one of z_i, $1 \le i \le r$ is invertible in R

The first observation follows from the fact that R is totally real. To prove the second observation, without loss of generality we may assume that all z_i are in $\mathbb{Q}[x]$. Now $z_1^2 + \cdots + z_r^2$ is invertible if and only if the constant term of $z_1^2 + \cdots + z_r^2$ is not zero if and only if the constant term of at least one of z_i is not zero if and only if at least one of z_i is invertible.

We now show that RQ_8 is duo. To do so, it suffices to prove that every left principal ideal in RQ_8 is a right ideal. Let $\alpha = \sum_{i=0}^{3} x_i a^i + \sum_{j=4}^{7} x_j a^{j-4} b$ be any element in RQ_8 and $L = (RQ_8)\alpha$. We will prove that L is a right ideal. Clearly, it suffices to prove that both $\alpha a \in L$ and $\alpha b \in L$.

We first prove that $\alpha a \in L$. We need to show that there exists $\beta = \sum_{i=0}^{3} a_i a^i + \sum_{j=4}^{7} a_j a^{j-4} b \in RQ_8$ such that $\alpha a = \beta\alpha$, or

$$(\sum_{i=0}^{3} x_i a^i + \sum_{j=4}^{7} x_j a^{j-4} b)a = (\sum_{i=0}^{3} a_i a^i + \sum_{j=4}^{7} a_j a^{j-4} b)(\sum_{i=0}^{3} x_i a^i + \sum_{j=4}^{7} x_j a^{j-4} b) \in L.$$

Simplifying and then comparing the coefficients of group elements on both sides of the above equation, we obtain the following system.

$$
(2.5)\quad \begin{cases}
x_0a_0 + x_3a_1 + x_2a_2 + x_1a_3 + x_6a_4 + x_7a_5 + x_4a_6 + x_5a_7 = x_3 \\
x_1a_0 + x_0a_1 + x_3a_2 + x_2a_3 + x_5a_4 + x_6a_5 + x_7a_6 + x_4a_7 = x_0 \\
x_2a_0 + x_1a_1 + x_0a_2 + x_3a_3 + x_4a_4 + x_5a_5 + x_6a_6 + x_7a_7 = x_1 \\
x_3a_0 + x_2a_1 + x_1a_2 + x_0a_3 + x_7a_4 + x_4a_5 + x_5a_6 + x_6a_7 = x_2 \\
x_4a_0 + x_7a_1 + x_6a_2 + x_5a_3 + x_0a_4 + x_1a_5 + x_2a_6 + x_3a_7 = x_5 \\
x_5a_0 + x_4a_1 + x_7a_2 + x_6a_3 + x_3a_4 + x_0a_5 + x_1a_6 + x_2a_7 = x_6 \\
x_6a_0 + x_5a_1 + x_4a_2 + x_7a_3 + x_2a_4 + x_3a_5 + x_0a_6 + x_1a_7 = x_7 \\
x_7a_0 + x_6a_1 + x_5a_2 + x_4a_3 + x_1a_4 + x_2a_5 + x_3a_6 + x_0a_7 = x_4
\end{cases}
$$

Thus, $\alpha a \in L$ if and only if System (2.5) has a solution $(a_0, \cdots, a_7)$ in R. We distinguish two cases.

Case 1. $(x_0 - x_2)^2 + (x_1 - x_3)^2 + (x_4 - x_6)^2 + (x_5 - x_7)^2 \neq 0$. It is not hard to check that the following is a solution of System (2.5) in the quotient field of R.

$$
(2.6)\quad \begin{aligned}
a_0 &= 0 \\
a_1 &= \tfrac{(x_0-x_2)^2+(x_1-x_3)^2}{(x_0-x_2)^2+(x_1-x_3)^2+(x_4-x_6)^2+(x_5-x_7)^2} \\
a_2 &= 0 \\
a_3 &= \tfrac{(x_4-x_6)^2+(x_5-x_7)^2}{(x_0-x_2)^2+(x_1-x_3)^2+(x_4-x_6)^2+(x_5-x_7)^2} \\
a_4 &= \tfrac{(x_1-x_3)(x_4-x_6)+(x_0-x_2)(x_5-x_7)}{(x_0-x_2)^2+(x_1-x_3)^2+(x_4-x_6)^2+(x_5-x_7)^2} \\
a_5 &= \tfrac{(x_1-x_3)(x_5-x_7)-(x_0-x_2)(x_4-x_6)}{(x_0-x_2)^2+(x_1-x_3)^2+(x_4-x_6)^2+(x_5-x_7)^2} \\
a_6 &= -\tfrac{(x_1-x_3)(x_4-x_6)+(x_0-x_2)(x_5-x_7)}{(x_0-x_2)^2+(x_1-x_3)^2+(x_4-x_6)^2+(x_5-x_7)^2} \\
a_7 &= -\tfrac{(x_1-x_3)(x_5-x_7)-(x_0-x_2)(x_4-x_6)}{(x_0-x_2)^2+(x_1-x_3)^2+(x_4-x_6)^2+(x_5-x_7)^2}
\end{aligned}
$$

We verify only that (2.6) satisfies the first equation of System (2.5). The rest of verifications can be done similarly. Let $A = x_0 - x_2, B = x_1 - x_3, C = x_4 - x_6$, $D = x_5 - x_7$, and $E = A^2 + B^2 + C^2 + D^2$. Then $a_4 = -a_6 = \frac{BC+AD}{E}$ and $a_5 = -a_7 = \frac{BD-AC}{E}$. Substituting (2.6) into the left side of the first equation in System (2.5) and then simplifying, we obtain the following.

$$
\begin{aligned}
&\tfrac{1}{E}(x_3(A^2 + B^2) + x_1(C^2 + D^2) - (x_4 - x_6)(BC + AD) - (x_5 - x_7)(BD - AC)) \\
&= \tfrac{1}{E}(x_3(A^2 + B^2) + x_1(C^2 + D^2) - C(BC + AD) - D(BD - AC)) \\
&= \tfrac{1}{E}(x_3(A^2 + B^2) + x_1(C^2 + D^2) - BC^2 - BD^2) \\
&= \tfrac{1}{E}(x_3(A^2 + B^2) + (x_1 - B)(C^2 + D^2) = x_3,
\end{aligned}
$$

which is equal to the right side of the first equation in System (2.5). This completes our verification.

We claim that all a_i given in (2.6) are, in fact, in R. We need only check that $a_i \in R$ for $i \in \{1, 3, 4, 5, 6, 7\}$. Since $(x_0 - x_2)^2 + (x_1 - x_3)^2 + (x_4 -$

$x_6)^2 + (x_5 - x_7)^2 \neq 0$, we know that at least one of $x_0 - x_2, x_1 - x_3, x_4 - x_6$ and $x_5 - x_7$ is not zero. If $x_i - x_{i+2} \neq 0$ for some $i \in \{0, 1, 4, 5\}$, then $x_i - x_{i+2} = x^{n_i} u_i$, where $n_i \geq 0$ is an integer and u_i is invertible in R. Otherwise, write $x_i - x_{i+2} = x^{n_i} u_i$, where $u_i = 0$ and $n_i \in \mathbb{Z}$ can be chosen as large as we want. Define $n = \min\{n_0, n_1, n_4, n_5\} = \min\{n_i | x_i - x_{i+2} \neq 0\}$. Then $a_4 = \frac{x^{n_1+n_4-2n} u_1 u_4 + x^{n_0+n_5-2n} u_0 u_5}{(x^{n_0-n} u_0)^2 + (x^{n_1-n} u_1)^2 + (x^{n_4-n} u_4)^2 + (x^{n_5-n} u_5)^2}$. We note that at least one of $(x^{n_i-n} u_i)^2$ is invertible, so it follows from observation (2) that $(x^{n_0-n} u_0)^2 + (x^{n_1-n} u_1)^2 + (x^{n_4-n} u_4)^2 + (x^{n_5-n} u_5)^2$ is invertible in R. Therefore, $a_4 \in R$ and hence $a_6 = -a_4 \in R$. Similarly, we can prove that $a_i \in R$ for $i \in \{1, 3, 5, 7\}$. This completes the proof of Case 1.

Case 2. $(x_0 - x_2)^2 + (x_1 - x_3)^2 + (x_4 - x_6)^2 + (x_5 - x_7)^2 = 0$. By observation (1), we now have $x_0 = x_2, x_1 = x_3, x_4 = x_6$, and $x_5 = x_7$, so $\alpha = (x_0 + x_1 a + x_4 b + x_5 ab)(1 + a^2)$ is a central element in RQ_8, and hence $\alpha a = a\alpha \in L$.

We have just proved that $\alpha a \in L$. Since elements a and b are symmetric in Q_8, by using a symmetric argument we can easily show that $\alpha b \in L$. Therefore, L is an ideal, and thus RQ_8 is duo. □

Remark 2.7. *We note that the ring R in Proposition 2.6 is a principal local integral domain such that RQ_8 is duo. However, for any prime p, $\mathbb{Z}_{(p)}$ the localization of $\mathbb{Z}$ at the ideal generated by p, is a principal local integral domain, but $\mathbb{Z}_{(p)} Q_8$ is not duo.*

Let G be a non-abelian torsion group and R be a commutative ring with identity. If RG is duo, then as mentioned before, RG is reversible, so it follows from [3] that $G = Q_8 \times E_2 \times E_2'$ is a Hamiltonian group, where E_2 is an elementary abelian 2-group, and E_2' is an abelian group all of whose elements are of odd order. Since $RG = (RQ_8)(E_2 \times E_2')$ can be regarded as a group ring over the ring RQ_8, the coefficient ring RQ_8 is an homomorphic image of RG under the standard augmentation mapping [6]. As a homomorphic image of a duo ring RG, RQ_8 is clearly duo.

Remark 2.8. *Let G be a non-abelian torsion group and R be a commutative ring with identity. If RG is duo, then RQ_8 is also duo.*

We note that it follows from Theorem 2.4 and [1, Theorem 3.1] that if R is an integral domain with $char(R) \neq 0$, then RQ_8 is duo if and only if R is a field of $char(R) = 2$ and $1 + x + x^2 \in \mathcal{U}(R)$ for all $x \in R$. If $char(R) = 0$, a necessary condition for RQ_8 to be duo is given in Corollary 2.3, i.e. $1 + x^2 + y^2 \in \mathcal{U}(R)$ for all $x, y \in R$. We are not aware of any example of an integral domain R of $char(R) = 0$ satisfying this necessary condition for which RQ_8 is not duo. We close this paper by proposing the following question.

Question 2.9. *Assume that R is an integral domain of $char(R) = 0$ such that $1 + x^2 + y^2 \in \mathcal{U}(R)$ for all $x, y \in R$. Is RQ_8 duo?*

References

[1] H. Bell and Y. Li, Duo group rings, *J. Pure Appl. Algebra*, **209** (2007), 833 - 838.

[2] M. Gutan and A. Kisielewicz, Reversible group rings, *J. Algebra* **279** (2004), 280–291.

[3] Y. Li and M.M. Parmenter, Reversible group rings over commutative rings, *Comm. Algebra* **35** (2007), 4096–4104.

[4] G. Marks, Reversible and symmetric rings, *J. Pure Appl. Algebra* **174** (2002), 311 - 318.

[5] I. Niven, H.S. Zuckerman and H.L. Montgomery, *An introduction to the theory of numbers*, Fifth edition, John Wiley & Sons, Inc., New York, 1991.

[6] C. Polcino Milies and S.K. Sehgal, *An Introduction to Group Rings*, Kluwer Academic Publishers, Dordrecht, 2002.