Finite Rings and Loop Rings
Involving the Commuting Regular Elements

H. Doostie
Mathematics Department
Teacher Training University
49 Mofateh Ave., Tehran 15614, Iran
doostih@saba.tmu.ac.ir

L. Pourfaraj
Department of Mathematics
Science and Research Branch
Islamic Azad University
P. O. Box 14515/1775, Tehran, Iran
L.pourfaraj@iauctb.ac.ir

Abstract
Two elements $x$ and $y$ of a ring $R$ are commuting regular if for some $a \in R$, $xy = yxayx$ holds. In this paper we study the finite rings $\mathbb{Z}_p[S]$ and $\mathbb{Z}_{p_1p_2}[L_n(m)]$, and prove that the first one is commuting regular and the second ring contains the commuting regular element and idempotents as well (where $p, p_1$ and $p_2$ are odd primes. Moreover, $i, m$ and $n$ are positive integers such that $m < n$, $(m,n) = 1$ and $(m-1,n) = 1$).

Mathematics Subject Classification: 16E50, 12E15, 16N60

Keywords: Commuting regular rings, group rings, loop ring

1. Introduction
We use $R$ and $S$ to denote a ring and a semigroup, respectively. A quasi group is a set $Q$ with a binary operation, here denoted by ",", with the property that for all $a, b \in Q$, there are unique solutions to the equations $a \cdot x = b$ and $y \cdot a = b$. A quasi group with an identity element is called a loop. A ring $R$ is called commuting regular if and only if for each $x, y \in R$ there exists an element $a$ of $R$ such that $xy = yxax$ (see [6]). The commuting regular semigroup is defined
in a similar way in [2]. A positive integer \( n \) is said to be a perfect number if \( n \) is equal to the sum of all its positive divisors, excluding \( n \) itself (see [1]). Let \( R \) be a ring, \( G \) is a group and \( R[G] \) be the set of all linear combinations of the form \( \alpha = \sum_{g \in G} \alpha(g)g \) where \( \alpha(g) \in R \) and \( \alpha(g) = 0 \) except of a finite number of coefficients. The sum and product of elements of \( R[G] \) are defined by:

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

\[
\left( \sum_{g \in G} \alpha(g)g \right) \left( \sum_{h \in G} \beta(h)h \right) = \sum_{g, h \in G} \alpha(g)\beta(h)gh.
\]

\( R[G] \) is called the group ring of \( G \) over \( R \) (see [4]). If we replace the group \( G \) in the above definition by a semigroup \( S \) (or loop \( L \)) we get \( R[S] \) (or \( R[L] \)) the semigroup ring (or loop ring). Following [6], let \( L_n(m) = \{e, 1, 2, \ldots, n\} \) be a set where \( n > 3 \), \( n \) is an odd integer and \( m \) is a positive integer such that \((m, n) = 1 \) and \((m - 1, n) = 1 \) with \( m < n \). Define on \( L_n(m) \), a binary operation “.” as follows:

1. \( e \cdot i = i \cdot e = i \) for all \( i \in L_n(m) - \{e\} \),
2. \( i^2 = e \) for all \( i \in L_n(m) \),
3. \( i \cdot j = t \) where \( t \equiv (mj - (m - 1)i)(\mod n) \) for all \( i, j \in L_n(m), i \neq e \) and \( j \neq e \).

Then \( L_n(m) \) is a loop.

2. The commuting regular semigroup ring \( Z_p[S] \)

Definition 2.1. A group ring \( R[G] \) is said to be a commuting regular group ring if \( R \) be a commuting regular ring. Also, we define the commuting regular semigroup ring, commuting regular loop ring and commuting regular groupoid ring in the same way.

Definition 2.2. Two elements \( x \) and \( y \) of a ring \( R \) (or semigroup \( S \)) are commuting regular if for some \( a \in R \) (or \( a \in S \)), \( xy = yxax \).

Proposition 2.3. Let \( S = \{a, b, c\} \) be the semigroup given by the table,

<table>
<thead>
<tr>
<th></th>
<th>a</th>
<th>b</th>
<th>c</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>a</td>
<td>a</td>
<td>a</td>
</tr>
<tr>
<td>b</td>
<td>a</td>
<td>a</td>
<td>a</td>
</tr>
<tr>
<td>c</td>
<td>a</td>
<td>a</td>
<td>c</td>
</tr>
</tbody>
</table>

then for all prime \( p \), \( Z_p[S] \) is commuting regular semigroup ring.
Proof. If \( p = 2 \), \( Z_2[S] \) is a Boolean ring and so \( Z_2[S] \) is a commuting regular semigroup ring. Now, let \( p \) be an odd prime, then \( 2^p \equiv 2 \pmod{p} \) and so

\[
(\alpha a + \beta b + \gamma c)^p \equiv (\alpha a + \beta b + \gamma c)(\mod{p}),
\]

where \( \alpha, \beta, \gamma \in \mathbb{Z}_p \). Therefore \( x^p = x \) for all \( x \in Z_p[S] \) and so

\[
x y = x^p y^p = (yx)(x^{p-2}y^{p-2})(yx)
\]

for all \( x, y \in Z_p[S] \). Then \( Z_p[S] \) is commuting regular semigroup ring.

**Corollary 2.4.** Let \( S = \{a, b, c\} \) be the semigroup given by the table,

\[
\begin{array}{ccc}
a & b & c \\
a & a & a \\
b & a & b \\
c & a & a \\
\end{array}
\]

then \( R = \prod_{i \in I} Z_{p_i} \) is a commuting regular ring where \( p_i \) is a prime number for all \( i \).

**Proof.** By the Proposition 3.1 of [2] and the Proposition 2.3.

**Proposition 2.5.** Let \( S = \{a, b, c\} \) be the semigroup given by the table,

\[
\begin{array}{ccc}
a & b & c \\
a & a & a \\
b & a & b \\
c & a & a \\
\end{array}
\]

then

\[
I = \{0, a, b, c, (p-1)a + b, (p-1)a + c, (p-1)a + b + c, (p-2)a + b + c\},
\]

is the set of all idempotent elements of commuting regular semigroup ring \( Z_p[S] \).

**Proof.** Assume that \( x \) be an idempotent of \( Z_p[S] \), then \( x = (\alpha a + \beta b + \gamma c) \) where \( \alpha, \beta, \gamma \in \mathbb{Z}_p \). By \( x^2 = x \), we have \( (\alpha^2 + 2\alpha\beta + 2\alpha\gamma + 2\beta\gamma) = \alpha, \beta^2 = \beta \) and \( \gamma^2 = \gamma \). Then \( \beta, \gamma \in \{0, 1\} \).

(1) If \( \beta = \gamma = 0, \alpha \in \{0, 1\} \) and so \( x = 0 \) or \( x = a \),

(2) If \( \beta = 0 \) and \( \gamma = 1, \alpha \in \{0, (p-1)\} \) and so \( x = c \) or \( x = (p-1)a + c \),

(3) If \( \beta = \gamma = 1, \alpha \in \{(p-1), (p-2)\} \) and so \( x = (p-1)a + b + c \) or \( x = (p-2)a + b + c \).
Example 2.6. Let \( M = \{a, b, c\} \) be the groupoid given by the table,

\[
\begin{array}{ccc}
   & a & b & c \\
   a & a & b & c \\
b & c & a & b \\
c & b & c & a
\end{array}
\]

then \( Z_2[M] \) is the commuting regular groupoid ring having only 8 elements given by

\[ \{0, a, b, c, a + b, a + c, b + c, a + b + c\} \]

Clearly, \( Z_2[M] \) is a non associative ring without identity and non commuting regular ring. But center of \( Z_2[M] \) (i.e; \( Z(Z_2[M]) = \{0, a+b+c\} \) is commuting regular ring.

3. The loop ring \( Z_{p_1p_2}[L_n(m)] \)

In this section we will prove that existence of commuting regular elements for the loop ring \( Z_t[L_n(m)] \) when \( t \) is an even perfect number. Also we will prove that the loop ring \( Z_t[L_n(m)] \) have commuting regular elements when \( t \) is of the form \( 2^i p \) or \( 3^i p \) (where \( p \) is an odd prime) or in general when \( t = p_1^i p_2 \) (\( p_1 \) and \( p_2 \) are distinct odd primes).

Proposition 3.1. Let \( Z_t[L_n(m)] \) be a loop ring where \( t \) is an even perfect number of the form \( t = 2^r(2^{r+1}-1) \) for some \( r > 1 \), then there exists an idempotent element \( e \in Z_t[L_n(m)] \) such that \( e \neq 0, 1 \).

Proof. As \( t \) be an even perfect number, \( t \) must be of the form

\[ t = 2^r(2^{r+1}-1), \text{ for some } r > 1 \]

where \( (2^{r+1}-1) \) is a prime. Consider \( e = 2^r(1+l) \in Z_t[L_n(m)] \) where \( l \in L_n(m) \). Now

\[ e^2 = (2^r(1+l))^2 = 2.2^{2r}(1+l) \]

by \( 2^{r+2r+1} \equiv 2^r \) (mod \( t \)). Therefore \( e^2 = e \).

Example 3.2. The loop ring \( Z_6[L_n(m)] \) has an idempotent \( e = 2(1+l) \) where \( l \in L_n(m) \).

Proposition 3.3. Let \( Z_t[L_n(m)] \) be a loop ring where \( t \) is an even perfect number of the form \( t = 2^r(2^{r+1}-1) \) for some \( r > 1 \), then there exist commuting regular elements \( a, b \in Z_t[L_n(m)] \) such that \( a \neq b \).
Proof. As $t$ be an even perfect number, $t$ must be of the form

$$t = 2^r(2^{r+1} - 1), \text{ for some } r > 1$$

where $(2^{r+1} - 1)$ is a prime. Assume that $a = 2^r(1+l)$ and $b = (t - 2^r)(1+l) \in Z_t[L_n(m)]$. Now

$$b^2 = [(t - 2^r)(1+l)]^2 = (t - 2^r)^2(1+l) \equiv 2^r(1+l)(\text{mod } t)$$

by $2^r2^{r+1} \equiv 2^r(\text{mod } t)$, so $b^2 = a$. Also,

$$ab = [2^r(1+l)][(t - 2^r)(1+l)] \equiv -2^r.2^r(1+l)(\text{mod } t)$$

by $-2^r.2^r(1+l) \equiv (t - 2^r)(1+l)(\text{mod } t)$ and so $ab = b$. Similarly, $ba = b$.  

By the Proposition 3.1, $a^2 = a$. Therefore

$$ab = (ba)b(ba).$$

Example 3.4. The loop ring $Z_6[L_n(m)]$ have commuting regular elements $a = 2(1+l)$ and $b = (6 - 2)(1+l)$ where $l \in L_n(m)$.

Proposition 3.5. Let $Z_{2p}[L_n(m)]$ be a loop ring where $p$ is an odd prime such that $p \mid 2^{r+1} - 1$ for some $r \geq 1$, then there exists an idempotent element $e \in Z_{2p}[L_n(m)]$ such that $e \neq 0, 1$.

Proof. Suppose that $p \mid 2^{r+1} - 1$ for some $r \geq 1$ and $e = 2^r(1+l) \in Z_{2p}[L_n(m)]$. Therefore

$$e^2 = (2^r(1+l))^2 = 2.2^r(1+l) = 2^{r+1}.2^r(1+l) \equiv 2^r(1+l)(\text{mod } 2p)$$

by $2^r2^{r+1} \equiv 2^r(\text{mod } 2p)$, so $e^2 = e$.

Example 3.6. The loop ring $Z_{10}[L_n(m)]$ has an idempotent $e = 2^3(1+l)$ where $r = 3, 5 \mid 2^{3+1} - 1$ and $l \in L_n(m)$.

Proposition 3.7. Let $Z_{2p}[L_n(m)]$ be a loop ring where $p$ is an odd prime such that $p \mid 2^{r+1} - 1$ for some $r \geq 1$, then there exist commuting regular elements $a, b \in Z_{2p}[L_n(m)]$ such that $a \neq b$. 
Proof. Suppose that $p \mid 2^{r+1} - 1$ for some $r \geq 1$ and $a = 2^r(1 + l), b = (2p - 2^r)(1 + l) \in Z_{2p}[L_n(m)]$. Therefore

$$b^2 = [(2p - 2^r)(1 + l)]^2 = 2(2p - 2^r)^2(1 + l) \equiv 2.2^{2r}(1 + l)(\mod 2p)$$

and

$$2^{r+1}2^r(1 + l) \equiv 2^r(1 + l)(\mod 2p)$$

by $2^r2^{r+1} \equiv 2^r(\mod 2p)$ and so $b^2 = a$. Also,

$$ab = [2^r(1 + l)][(2p - 2^r)(1 + l)] \equiv -2^r(1 + l)2^r(1 + l)(\mod 2p)$$

and

$$-2.2^{2r}(1 + l) \equiv (2p - 2^r)(1 + l)(\mod 2p).$$

Hence $ab = b$. Similarly, $ba = b$. By the Proposition 3.6, $a^2 = a$. Therefore

$$ab = (ba)b(ab).$$

Example 3.8. The loop ring $Z_{10}[L_n(m)]$ have commuting regular elements $a = 2^4(1 + l)$ and $b = 2(1 + l)$ where $l \in L_n(m)$.

Proposition 3.9. Let $Z_{2p}[L_n(m)]$ be a loop ring where $p$ is an odd prime such that $p \mid 2^{r+1} - 1$ for some $r \geq i$, then there exists an idempotent element $e \in Z_{2p}[L_n(m)]$ such that $e \neq 0, 1$.

Proof. Suppose that $p \mid 2^{r+1} - 1$ for some $r \geq i$ and $e = 2^r(1 + l) \in Z_{2p}[L_n(m)]$. Since

$$2^{r+1} \equiv 1(\mod p)$$

for some $r \geq i \Leftrightarrow 2^r2^{r+1} \equiv 2^r(\mod 2^ip)$ as $(2^r, 2^ip) = 2^i, r \geq i$

then $e^2 = e$.

Example 3.10. The loop ring $Z_{23,7}[L_n(m)]$ has an idempotent $e = 2^5(1 + l)$ where $5, 7 \mid 25^{1+1} - 1$ and where $l \in L_n(m)$.

Proposition 3.11. Let $Z_{2p}[L_n(m)]$ be a loop ring where $p$ is an odd prime such that $p \mid 2^{r+1} - 1$ for some $r \geq 1$, then there exist commuting regular elements $a, b \in Z_{2p}[L_n(m)]$ such that $a \neq b$.

Proof. Suppose that $p \mid 2^{r+1} - 1$ for some $r \geq 1$ and $a = 2^r(1 + l), b = (2^p - 2^r)(1 + l) \in Z_{2p}[L_n(m)]$. Since $2^r2^{r+1} \equiv 2^r(\mod 2^ip)$ as $(2^r, 2^ip) = 2^i, r \geq i$,

$$b^2 = a$$

and $ab = ba = b$.

By the Proposition 3.9, $a^2 = a$. Therefore

$$ab = (ba)b(ab).$$
Example 3.12. The loop ring $Z_{2^i 7}[L_n(m)]$ have commuting regular elements $a = 2^i(1 + l)$ and $b = (2^3 7 - 2^i)(1 + l)$ where $r = 5, 7 | 2^{5+1} - 1$ and $l \in L_n(m)$.

Proposition 3.13. Let $Z_{3^i p}[L_n(m)]$ be a loop ring where $p$ is an odd prime such that $p \mid 2.3^r - 1$ for some $r \geq i$, then there exists an idempotent element $e \in Z_{3^i p}[L_n(m)]$ such that $e \neq 0, 1$.

Proof. Suppose that $p \mid 2.3^r - 1$ for some $r \geq i$ and $e = 3^r(1 + l) \in Z_{3^i p}[L_n(m)]$. Since

$$2.3^r \equiv 1 \pmod{p}$$

for some $r \geq i$ $\iff$ $2.3^r \equiv 3^r(\mod 3^ip)$ as $(3^i, 3^ip) = 3^i, r \geq i$

then

$$e^2 = (3^r(1 + l))^2 = 2.3^{2r}(1 + l) = 2.3^r.3^r(1 + l) \equiv 3^r(1 + l)(\mod 3^ip),$$

so $e^2 = e$.

Example 3.14. The loop ring $Z_{3^2 5}[L_n(m)]$ has an idempotent $e = 3^5(1 + l)$ where $r = 5, 5 | 2.3^5 - 1$ and $l \in L_n(m)$.

Proposition 3.15. Let $Z_{3^i p}[L_n(m)]$ be a loop ring where $p$ is an odd prime such that $p \mid 2.3^r - 1$ for some $r \geq i$, then there exist commuting regular elements $a, b \in Z_{3^i p}[L_n(m)]$ such that $a \neq b$.

Proof. Suppose that $p \mid 2.3^r - 1$ for some $r \geq i$ and $a = 3^r(1 + l), b = (3^i p - 3^r)(1 + l) \in Z_{3^i p}[L_n(m)]$. Since $2.3^r \equiv 3^r(\mod 3^ip)$ as $(3^i, 3^ip) = 3^i, r \geq i, a^2 = a$ by the Proposition 3.13. Similarly,

$$b^2 = a \text{ and } ab = ba = b.$$ 

Therefore

$$ab = (ba)b(ba).$$

Example 3.16. The loop ring $Z_{3^2 5}[L_n(m)]$ have commuting regular elements $a = 3^5(1 + l)$ and $b = (3^2 5 - 3^5)(1 + l)$ where $r = 5, 5 | 2.3^5 - 1$ and $l \in L_n(m)$.

Proposition 3.17. Let $Z_{p_1 p_2}[L_n(m)]$ be a loop ring where $p_1$ and $p_2$ are distinct odd primes and $p_2 \mid 2.3^r - 1$ for some $r \geq i$, then there exists an idempotent element $e \in Z_{p_1 p_2}[L_n(m)]$ such that $e \neq 0, 1$. 
**Proof.** Suppose that \( p_2 \mid 2.p_1^r - 1 \) for some \( r \geq i \) and \( e = p_1^i(1 + l) \in Z_{p_1^i.p_2}[L_n(m)] \). Since

\[
2.p_1^i \equiv 1 \pmod{p_2}
\]

for some \( r \geq i \) ⇔ \( 2.p_1^i.p_1^r \equiv p_1^i \pmod{p_1^i.p_2} \) as \((p_1^i, p_1^i.p_2) = p_1^i, r \geq i\) then

\[
e^2 = (p_1^i(1 + l))^2 = 2.p_1^{2r}(1 + l) = 2.p_1^r.p_1^r(1 + l) \equiv p_1^r(1 + l)(\pmod{p_1^i.p_2}).
\]

So \( e^2 = e \).

**Proposition 3.18.** Let \( Z_{p_1^i.p_2}[L_n(m)] \) be a loop ring where \( p_1 \) and \( p_2 \) are distinct odd primes and \( p_2 \mid 2.p_1^r - 1 \) for some \( r \geq i \), then there exist commuting regular elements \( a, b \in Z_{p_1^i.p_2}[L_n(m)] \) such that \( a \neq b \).

**Proof.** Suppose that \( p_2 \mid 2.p_1^r - 1 \) for some \( r \geq i \) and \( a = p_1^i(1 + l), b = (p_1^i.p_2 - p_1^i)(1 + l) \in Z_{p_1^i.p_2}[L_n(m)] \). Since \( 2.p_1^r.p_1^r \equiv p_1^r \pmod{p_1^i.p_2} \) as \((p_1^i, p_1^i.p_2) = p_1^i, r \geq i, a^2 = a \) by the Proposition 3.18. Similarly,

\[
b^2 = a \text{ and } ab = ba = b.
\]

Therefore

\[
ab = (ba)b(ba).
\]

**References**


Received: March 15, 2007