http://ijgt.ui.ac.ir

**International Journal of Group Theory**
ISSN (print): 2251-7650, ISSN (on-line): 2251-7669
Vol. 11 No. 4 (2022), pp. 253-257.

www.ui.ac.ir

# ON THE PROBABILITY OF ZERO DIVISOR ELEMENTS IN GROUP RINGS

HAVAL M. MOHAMMED SALIH

Abstract. Let $R$ be a non trivial finite commutative ring with identity and $G$ be a non trivial group. We denote by $P(RG)$ the probability that the product of two randomly chosen elements of a finite group ring $RG$ is zero. We show that $P(RG) < \frac{1}{4}$ if and only if $RG \ncong \mathbb{Z}_2C_2, \mathbb{Z}_3C_2, \mathbb{Z}_2C_3$. Furthermore, we give the upper bound and lower bound for $P(RG)$. In particular, we present the general formula for $P(RG)$, where $R$ is a finite field of characteristic $p$ and $|G| \leq 4$.

## 1. Introduction

Throughout this paper, a ring $R$ will denote a non trivial finite commutative ring with identity 1. The set of all invertible elements of a ring $R$ form a group called the unit group of $R$ denoted by $\mathcal{U}(R)$. Let $G$ be a non trivial finite group and $RG$ denote the group ring of group $G$ over the ring $R$. If $R = K$ is a field then $KG$ is the group algebra of $G$ over the field $K$. Let $C_n$ denote the cyclic group of order $n$. There are many known results about the group unit of $KG$ in [1, 3, 6, 7, 8]. The main objects of study here will be the nullity degree (probability) of $RG$, is the probability that the multipication of two randomly chosen elements of $RG$ is zero. That is

$$P(RG) = \frac{|(a, b) \in RG \times RG \ : ab = 0|}{|RG|^2}.$$

where $a := \sum_{g\in G} r_g g$ and $b := \sum_{g\in G} \bar{r}_g g$ $(\bar{r}_g, r_g \in R, g \in G)$. Since $RG$ contains an identity, then we have that $RG = \{0\} \cup \mathcal{U}(RG) \cup \mathcal{ZD}(RG)$, where $\mathcal{ZD}(RG)$ is the set of nonzero zero divisors of $RG$. The homomorphsim $\varepsilon\colon RG \to R$ given by $\varepsilon(\sum_{g\in G} a_g g) = \sum_{g\in G} a_g$ is called the augmentation mapping of $RG$. Its kernel, denoted by $\triangle(G)$ is called the augmentation ideal of $RG$. It is clear that

Communicated by: Victor Bovdi.

MSC(2010): Primary: 16S34; Secondary: 16U60.

Keywords: group ring, probability, unit group, zero divisor.

Received: 28 December 2020, Accepted: 25 October 2021.

Article Type: Research Paper.

http://dx.doi.org/10.22108/IJGT.2021.126694.1664 .

$\varepsilon$ is surjective and $RG/\triangle(G) \cong R$. Furthermore, it sends unit elements (zero divisors) in $RG$ to unit elements (zero divisors) in $R$. For $x \in RG$, $Ann(x) = \{b \in RG \ : xb = 0\}$ denote the annihilator of $x$ in $RG$. Now

$$P(RG) = \frac{\sum_{x\in RG} |Ann(x)|}{|RG|^2} \tag{1.1}$$

$$= \frac{|Ann(0)| + \sum_{x\in \mathcal{U}(RG)} |Ann(x)| + \sum_{0\neq x\in \mathcal{ZD}(RG)} |Ann(x)|}{|RG|^2} \tag{1.2}$$

$$= \frac{|RG| + |\mathcal{U}(RG)| + \sum_{0\neq x\in \mathcal{ZD}(RG)} |Ann(x)|}{|RG|^2}. \tag{1.3}$$

It obvious that $P(RG) = 1$ if and only if $R$ is a trivial ring. Also if $RG$ is a semi simple and $G$ is a trivial group, then $RG \cong R$. The probability of $RG$ can be found in [2].

## 2. **Preliminary**

Of course, our goal is to find the upper and lower bound of the probability of group ring. For that purpose, we will first need the known results of the unit groups in the group ring.

**Theorem 2.1.** [1] $\mathcal{U}(\mathbb{F}_{3^k}(C_3 \times C_2)) \cong C_3^{4k} \times C_{3^k-1}^2$.

**Theorem 2.2.** [1] $\mathcal{U}(\mathbb{F}_{3^k}(C_3 \times D_6)) \cong [(C_3^{9k} \rtimes C_3^{3k}) \rtimes (C_3^{4k} \times C_{3^k-1})] \times C_{3^k-1}$.

**Theorem 2.3.** [4] $\mathcal{U}(\mathbb{F}_{3^k} D_6) = ((C_3^{3k} \rtimes C_3^k) \rtimes C_{3^k-1}) \times C_{3^k-1}$.

**Theorem 2.4.** [5] $\mathcal{U}(\mathbb{F}_{2^k} D_8) = [(((C_2^k \times C_4^k) \rtimes C_4^k) \times C_2^k) \rtimes C_{2^k})] \times C_{2^k-1}$.

**Theorem 2.5.** [6] $|\mathcal{U}(\mathbb{F}_{p^k} D_{2p^m})| = p^{2k(p^m-1)}(p^k-1)^2$, *where* $p$ *is an odd prime and* $m \in N_0$.

**Theorem 2.6.** [8] *If* $|F| = p^n$, *where* $charF = p > 3$, *then the unit group* $\mathcal{U}(FS_4)$ *is isomorphic to* $GL(3,F) \times GL(3,F) \times GL(2,F) \times F^* \times F^*$.

**Theorem 2.7.** [7] *If* $|F| = p^n$, *where* $charF = p > 3$, *then the unit group* $\mathcal{U}(FD_{12})$ *is isomorphic to* $GL(2,F) \times GL(2,F) \times GL(2,F) \times F^* \times F^* \times F^* \times F^*$.

There are some kinds of basic properties of the unit groups of group ring $RG$, where $G$ is abelian group that will be given in the following results.

**Theorem 2.8.** [3] *If* $gcd(n,p) = 1$ *and* $q = p^m$, *then* $\mathcal{U}(\mathbb{F}_q C_n) \cong C_{q-1} \times (\prod_{l|n,l>1} C_{q^{d_l}-1}^{el})$ *where* $d_l$ *is the multiplicative order of* $q$ *modulo* $l$ *and* $e_l = \frac{\varphi(l)}{d_l}$.

Now consider the case $p|n$.

**Lemma 2.9.** [3] *Let* $k \in \mathbb{N}$. *Then* $\mathcal{U}(\mathbb{F}_{p^m} C_{p^k}) \cong \begin{cases} C_{p^m-1} \times C_p^{m(p-1)} & if k = 1 \\ C_{p^m-1} \times \prod_{n=1}^{k} C_{p^t}^{n_t} & otherwise \end{cases}$

*where* $n_k = m(p-1)$ *and* $n_t = mp^{k-t-1}(p-1)^2$, *for all* $t, 1 \leq t < k$.

http://dx.doi.org/10.22108/IJGT.2021.126694.1664

**Theorem 2.10.** [3] *Let $n = p^k n_1$, where $gcd(n_1, p) = 1$ and $k \geq 1$. Then*
$\mathcal{U}(\mathbb{F}_{p^m} C_n) \cong \mathcal{U}(\mathbb{F}_{p^m} C_{p^k}) \times (\prod_{l|n_1, l>1} \mathcal{U}(\mathbb{F}_{p^{md_l}} C_{p^k})^{e_l})$

**Theorem 2.11.** *)*[9, (Maschke's Theorem] *Let $G$ be a group. Then the group ring $RG$ is semi-simple if and only if one the following conditions hold:*

i) *$R$ is a semi-simple ring.*
ii) *$G$ is finite.*
iii) *$|G|$ is inversable in $R$.*

## 3. **Results**

**Theorem 3.1.** *Let $R$ be a field of characteristic $p$, where $q = p^m$. Then*
$$P(\mathbb{F}_q C_2) \cong \begin{cases} \frac{3q-2}{q^3} & if\ p|2. \\ \frac{4q^2-4q+1}{q^4} & if\ gcd(p,2) = 1. \end{cases}$$

*Proof.* Since $|Ann(x)| = q$ for all $0 \neq x \in \mathcal{ZD}(RG)$, then from Equation (3), we obtain

$$P(RG) = \frac{|RG| + |\mathcal{U}(RG)| + q(|RG| - |\mathcal{U}(RG)| - 1)}{|RG|^2} \tag{3.1}$$

From Theorem 2.8, we have $|\mathcal{U}(\mathbb{F}_q C_2)| = (q-1)^2$ and by Lemma 2.9, we obtain $|\mathcal{U}(\mathbb{F}_q C_2)| = q(q-1)$. Substituting these in Equation (3.1) and the result follows. □

**Theorem 3.2.** *Let $R$ be a field of characteristic $p$, where $q = p^m$. Then*
$$P(\mathbb{F}_q C_3) \cong \begin{cases} \frac{4q-3}{q^4} & if\ p|3. \\ \frac{8q^3-12q^2+6q-1}{q^6} & q \equiv 1 \mod 3\ and\ if\ gcd(p,3) = 1. \\ \frac{4q^3-2q^2-2q+1}{q^6} & q \equiv 2 \mod 3\ and\ if\ gcd(p,3) = 1. \end{cases}$$

*Proof.* Let $0 \neq x \in \mathcal{ZD}(RG)$, then either $|Ann(x)| = q$ or $q^2$. If $p|3$, then there are $q^2 - q$ elements of size $q$ and $q-1$ elements of size $q^2$. By Lemma 2.9, we obtain $|\mathcal{U}(\mathbb{F}_q C_3)| = q^2(q-1)$. If $gcd(p,3) = 1$, then we have two cases as follows:

Case 1 if $q \equiv 1 \mod 3$, then there are $3(q-1)^2$ elements of size $q$ and $3(q-1)$ elements of size $q^2$. Also, by Theorem 2.8, we obtain $|\mathcal{U}(\mathbb{F}_q C_3)| = (q-1)^3$.

Case 2 if $q \equiv 2 \mod 3$, then there are $q^2 - 1$ elements of size $q$ and $q-1$ elements of size $q^2$. So $|\mathcal{U}(\mathbb{F}_q C_3)| = (q^2-1)(q-1)$ by Theorem 2.8.

The rest follows from Equation (1.3). □

**Theorem 3.3.** *Let $R$ be a field of characteristic $p$, where $q = p^m$. Then*
$$P(\mathbb{F}_q C_4) \cong \begin{cases} \frac{5q-4}{q^5} & if\ p|4. \\ \frac{16q^4-32q^3+24q^2-8q+1}{q^8} & q \equiv 1 \mod 4\ and\ if\ gcd(p,4) = 1. \\ \frac{8q^4-8q^3-2q^2+4q-1}{q^8} & q \equiv 3 \mod 4\ and\ if\ gcd(p,4) = 1. \end{cases}$$

*Proof.* The proof is similar as Theorem 3.2. □

http://dx.doi.org/10.22108/IJGT.2021.126694.1664

**Theorem 3.4.** *Let $R$ be a field of characteristic $p$, where $q = p^m$. Then*

$$P(\mathbb{F}_q(C_2 \times C_2)) \cong \begin{cases} \frac{q^2+3q-3}{q^5} & if\ p|4. \\ \frac{16q^4-32q^3+24q^2-8q+1}{q^8} & otherwise. \end{cases}$$

*Proof.* The proof is similar as Theorem 3.2. □

**Lemma 3.5.** *Let $RG$ be a finite group ring. Then $\sum_{x\in RG} |Ann(x)| \geq \sum_{x\in R} |Ann(x)|$.*

*Proof.* The proof is clear. □

**Lemma 3.6.** *If $R$ is a ring and $G$ is a group, then $P(R) \geq P(RG)$.*

*Proof.* Since $RG/\triangle(G) \cong R$ and $\triangle(G)$ is non empty and non zero, then $|RG|^2 \geq (\frac{|RG|}{|\triangle(G)|})^2$ and so $(\sum_{x\in R} |Ann(x)|)|RG|^2 \geq (\sum_{x\in R} |Ann(x)|)(\frac{|RG|}{|\triangle(G)|})^2 = (\sum_{x\in R} |Ann(x)|)|R|^2$. Thus $P(R) = \frac{\sum_{x\in R} |Ann(x)|}{|R|^2} \geq \frac{\sum_{x\in R} |Ann(x)|}{|RG|^2} = \frac{\sum_{x\in RG} |Ann(x)|}{|RG|^2} = P(RG)$, as required. □

**Remark 3.7.** *Since $RG$ is a semi-simple, then a consequence of Theorem 2.11, we have that $RG \cong R^n$. However $P(RG) \neq P(R^n)$. For instance, $R = \mathbb{Z}_3$ and $G = C_4$. So $P(RG) = \frac{425}{6561}$ and $P(R^4) = P(R)^4 = \frac{625}{6561}$.*

**Lemma 3.8.** *If $RG$ is a group ring, then*

$$P(RG) \leq \frac{5|RG| - 4}{2|RG|^2}.$$

*Proof.* Since $|Ann(x)| \leq \frac{|RG|}{2}$ for $0 \neq x \in RG$, then

$$P(RG) \leq \frac{|RG| + |\mathcal{U}(RG)| + \frac{|RG|}{2}(|RG| - |\mathcal{U}(RG)| - 1)}{|RG|^2} = \frac{|RG| + |RG|^2 + |\mathcal{U}(RG)|(2 - |RG|)}{2|RG|^2}.$$

Also $|\mathcal{U}(RG)| \leq |RG| - 2$. Therefore,

$$P(RG) \leq \frac{|RG| + |RG|^2 + (|RG| - 2)(2 - |RG|)}{2|RG|^2} = \frac{5|RG| - 4}{2|RG|^2}.$$

This completes the proof. □

**Lemma 3.9.** *If $RG$ is a group ring, then*

$$P(RG) \geq \frac{2|RG| - |\mathcal{ZD}(RG)|}{|RG|^2}.$$

*Proof.* The proof is clear. □

In [4, 3, 5, 6, 1, 8], they give the size of $\mathcal{U}(RG)$ and then we obtain the size of $\mathcal{ZD}(RG)$. Thus we achieve the lower bound of $P(RG)$.

**Theorem 3.10.** *Let $RG$ be a finite group ring. Then $P(RG) \geq \frac{1}{4}$ if and only if $RG$ is isomorphic to one of the following rings: $\mathbb{Z}_2C_2, \mathbb{Z}_3C_2, \mathbb{Z}_2C_3$.*

http://dx.doi.org/10.22108/IJGT.2021.126694.1664

*Proof.* Let $m = |RG|$. Then Lemma 3.8 gives upper bound for $P(RG)$ and then $\frac{1}{4} \leq P(RG) \leq \frac{5m-4}{2m^2}$. Solving this inequality gives $m \leq 9$. That is $m = |RG| = |R|^{|G|} \leq 9$. This force that $RG$ is isomorphic to one of the following rings: $\mathbb{Z}_2C_2, \mathbb{Z}_3C_2, \mathbb{Z}_2C_3$.

Conversely, if $RG$ is isomorphic to one of the following rings: $\mathbb{Z}_2C_2, \mathbb{Z}_3C_2, \mathbb{Z}_2C_3$, then $P(RG) \geq \frac{1}{4}$ by Theorem 3.1 and Theorem 3.2. Hence the result is proved. □

## Acknowledgments

I would like thank to the referee for careful reading of the article and detailed report including corrections and comments; and I appreciate his/her effort on reviewing the article.

## References

[1] J. Gildea, The structure of the unit group of the group algebra $\mathbb{F}_{3^K}(C_3 \times D_6)$, *Comm. Algebra*, **38** (2010) 3311–3317.

[2] M. A. Esmkhani and S. M. Jafarian Amiri, The probability that the multiplication of two ring elements is zero, *J. Algebra Appl.*, **17** (2018) pp. 9.

[3] N. Makhijani, R. K. Sharma and J. B. Srivastava, The unit group of algebra of circulant matrices, *Int. J. Group Theory*, **3** no. 4 (2014) 13–16.

[4] J. Gildea and L. Creedon, The structure of the unit group of the group algebra $F3^kD_6$, *Int. J. Pure Appl. Math*, **45**, no. 2, (2008) 315-320.

[5] J. Gildea, The structure of the unitary units of the group algebra $\mathbb{F}_{2^k}D_8$, *Int. Electron. J. Algebra*, **9** (2011) 171–176.

[6] J. Gildea, On the order of $U(\mathbb{F}_{p^k}D_{2p^m})$, *Int. J. Pure Appl. Math.*, **46** (2008) 267–272.

[7] G. Tang and Y. Gao, The unit groups of $FG$ of groups with order 12, *Int. J. Pure Appl. Math.*, **73** (2011) 143–158.

[8] M. Khan, R. K. Sharma and J. B. Srivastava, The unit group of $FS_4$, *Acta Math. Hungar.*, **118** (2008) 105–113.

[9] C. P. Milies and S. K. Sehgal, *An introduction to group rings*,Springer Science and Business Media, **1**, Kluwer Academic publishers Dordrecht/Boston/London, 2002.

**Haval M. Mohammed Salih**

Department of Mathematics, Faculty of Science, Soran University , Kawa St, Soran, Erbil, Iraq

Email: havalmahmood07gmail.com

http://dx.doi.org/10.22108/IJGT.2021.126694.1664