International Journal of Mathematics And its Applications
Volume 4, Issue 1–B (2016), 169–171.
ISSN: 2347-1557
Available Online: http://ijmaa.in/

International Journal of Mathematics And its Applications

Dual and Non-Dual Elements in Finite Fields (Rings)

Research Article

S.K.Pandey[1] *

1 Department of Mathematics, Sardar Patel University of Police, Security and Criminal Justice, Daijar, Jodhpur, Rajasthan, India.

Abstract: Let F be a finite field (ring) and $a, b \in F$. We call a and b as dual elements if $a^2 = b^2 = -1$ (where 1 is the identity element of F). The term dual elements refers to the dual properties of a and b as a and b are the additive as well as multiplicative inverse of each other. If $a^2 = b^2 = -c$, where $c \neq 1$ is any element of F then we call a and b as non-dual elements of F. We note that if $a \in F$ such that $a^2 = -a$ then a is not necessarily the zero element of F.

MSC: 12E20, 16P10.

Keywords: Finite ring, finite field, Galois field, dual elements.

1. Introduction

The theory of finite rings and finite fields are important aspects of modern algebra for study and research. One may refer [1–3] for further details. The idea behind this note is simple and has originated through [4, 5]. In [4] we have given a simple technique to obtain a finite matrix field of order p for every prime $p > 0$. In [5] we have given a technique to construct a finite matrix field of order p^2 for every positive prime $p \neq 2$. In this article we introduce the concept of dual inverse and dual elements in a finite ring and finite field and provide some examples. In this article by a finite ring we mean a finite commutative ring. In the section two, all the definitions and propositions are given for finite fields but they equally hold for finite rings as well.

2. Dual Elements and Dual Inverse

Definition 2.1. *Let F be a finite field and $a, b \in F$ then b is called the dual inverse of a if b is the additive as well as multiplicative inverse of a. If b is the dual inverse of a then a is also the dual inverse of b.*

Definition 2.2. *Let F be a finite field and $a, b \in F$ then a and b are called dual elements of F if $a^2 = b^2 = -1$. In other words, a and b are called dual elements of F if a and b are the dual inverse of each other.*

Definition 2.3. *An element a of a finite field F is called the self dual element if a is the additive as well as multiplicative inverse of itself.*

Definition 2.4. *Let F be a finite field and $a, b \in F$ then a and b are called non-dual elements of F if $a^2 = b^2 \neq -1$.*

* *E-mail: skpandey12@gmail.com*

Proposition 2.5. *If F is a finite field of characteristic p and c is an element of F then*

(1). $a^2 + b^2 = (p-2)ab$,

(2). $a^3 + b^3 = 0$,

(3). $a^2 = b^2 = -c$

forall $a, b \in F$ *and* $a + b = 0$.

Proposition 2.6. *Let a and b are dual elements of a finite field F then*

(1). $a^2 + b^2 = (p-2).1$,

(2). $a^3 + b^3 = 0$

(3). $a^2 = b^2 = -1$.

Here 1 is the multiplicative identity of F and p is the characteristic of F.

Proposition 2.7. *The dual inverse of every $a \in F$ (if it exists) is unique.*

Proposition 2.8. *Every finite field of characteristic two has self dual element.*

Proposition 2.9. *Let F be a finite field and $a, b \in F$ with $a + b = 0$ then $a^2 = b^2 = -1$ or $a^2 = b^2 = -c$, where 1 is the identity element of F and c is an element of F.*

Proposition 2.10. *Let F be a finite field(ring) and $a \in F$ such that $a^2 = -a$ then a is not necessarily the zero element of F. Refer Example 2.16.*

Example 2.11. *Let* $R = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}$. *One can see that R is a finite commutative ring under matrix addition and multiplication modulo 2. Let* $a = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. *Then a and b are self dual elements of R.*

Example 2.12.

$$R = \left\{ \begin{matrix} \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 3 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}, \\ \begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix}, \begin{pmatrix} 3 & 1 \\ 3 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 3 \\ 1 & 3 \end{pmatrix} \end{matrix} \right\}.$$

Then R is a finite commutative ring under matrix addition and multiplication modulo 4. Let $a = \begin{pmatrix} 0 & 3 \\ 1 & 0 \end{pmatrix}$, $b = \begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix}$ *then a and b are dual elements of R.*

Example 2.13. *A finite matrix field of order 9 as given in [2] is*

$$M_9 = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix} \right\}.$$

Let $a = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$ *and* $b = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$ *then it is easy to verify that a and b are dual elements of* M_9*. It may be noted that addition and multiplication in* M_9 *are defined as matrix addition modulo* 3 *and matrix multiplication modulo* 3 *respectively.*

Example 2.14. *Let* $a = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$, $b = \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}$; $c = \begin{pmatrix} 0 & 1 \\ 4 & 0 \end{pmatrix}$, $d = \begin{pmatrix} 0 & 4 \\ 1 & 0 \end{pmatrix}$. *One may refer [2] to see that these are elements of* M_{25}*.* M_{25} *is a finite field of order* 25 *under matrix addition and multiplication modulo* 5*. One can see that a and b; c and d are dual elements of* M_{25}*.*

Example 2.15. *Since every finite field of characteristic p contains a finite field of order p therefore every field of characteristic* 2 *has a subfield of order* 2*. One can easily see that a finite field of order* 2 *has a self dual element. Thus it directly follows that every finite field of characteristic* 2 *has a self dual element. For two distinct matrix representations of a finite field of order* 2 *one may refer [1].*

Example 2.16. *Let* $F_5 = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}, \begin{pmatrix} 3 & 3 \\ 3 & 3 \end{pmatrix}, \begin{pmatrix} 4 & 4 \\ 4 & 4 \end{pmatrix} \right\}$*, then it is a finite field of order* 5 *under matrix addition and multiplication modulo* 5 *[1]. Let*

$$F_{11} = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}, \begin{pmatrix} 3 & 3 \\ 3 & 3 \end{pmatrix}, \begin{pmatrix} 4 & 4 \\ 4 & 4 \end{pmatrix}, \begin{pmatrix} 5 & 5 \\ 5 & 5 \end{pmatrix}, \begin{pmatrix} 6 & 6 \\ 6 & 6 \end{pmatrix}, \begin{pmatrix} 7 & 7 \\ 7 & 7 \end{pmatrix}, \begin{pmatrix} 8 & 8 \\ 8 & 8 \end{pmatrix}, \begin{pmatrix} 9 & 9 \\ 9 & 9 \end{pmatrix}, \begin{pmatrix} 10 & 10 \\ 10 & 10 \end{pmatrix} \right\}.$$

It is easy to see that F_{11} *is a finite field under matrix addition and multiplication modulo* 11 *[1].*
One may verify that F_5 *has dual elements however* F_{11} *does not have dual elements. Therefore* F_{11} *contains only non-dual elements and one can also verify that there are non-zero elements in* F_{11} *satisfying* $a^2 = -a$*.*

References

[1] M.Artin, *Algebra*, Prentice Hall of India Private Limited, New Delhi, (2000).

[2] R.Lidl and H.Niederreiter, *Introduction to Finite Fields and their Applications*, Cambridge University Press, (1987).

[3] T.W.Hungerford, *Algebra*, Springer-India, New Delhi, (2005).

[4] S.K.Pandey, *Matrix Field of Finite and Infinite Order*, International Research Journal of Pure Algebra, 5(12)(2015), 214-216.

[5] S.K.Pandey, *Visualizing Finite Field of Order* p^2 *through Matrices*, Global Journal of Science Frontier Research (F), XVI(1-1)(2016), 27-30.