ABSTRACT

In the literature one can find several examples of a matrix group as well as matrix ring. However examples of a matrix field are generally not found. We provide some examples of matrix fields of finite as well as infinite order. In addition this article provides a technique to obtain finite matrix fields of order $p$ for every positive prime $p$.

MSC2010: 12Exx, 12E20.

Key-Words: Algebra, binary operation, matrix group, matrix ring, matrix field, Galois field.

INTRODUCTION

A non empty set $R$ together with two binary operations ‘$+$’ and ‘$\cdot$’ is called a ring if

1. $(R, +)$ is an Abelian group.
2. $(R, \cdot)$ is a semigroup.
3. $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$,  $\forall a, b, c \in R$.

If in addition

4. $a.b = b.a$, $\forall a, b \in R$

A ring $R$ having this property is known as a commutative ring.

5. $\exists$ an element $1$ in $R$ such that

   $1.a = a.1 = a$,  $\forall a \in R$

   $1$ is called the multiplicative identity of $R$.

6. for every non-zero element $b$ in $R$ $\exists$ an element $c$ in $R$ such that $b \cdot c = 1$

then $R$ is known as a field.

In the literature of abstract (modern) algebra ([1], [2], [3], [4], [5]) it is not very common to find examples of a field of matrices. The purpose of this article is to provide few examples of a field of matrices.

Condition (6) asserts that in a field $R$ the product of any two non-zero elements is never zero. However in the case of a ring $R$ one may find two non-zero elements $b$ and $c$ in $R$ such that $b \cdot c = 0$. A ring $R$ having this property is known as a ring with zero divisors. The ring $M = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in K \right\}$ where $K$ denotes the set of all rational (real or complex) numbers, is an example of a ring with zero divisors under the ordinary addition and multiplication of matrices.

It is well known that the ring of all square matrices of order 2 is a non- commutative ring with zero-divisors. Due to this it does not form a field and one does not generally think about matrix field. However we shall provide some examples of matrix fields in the next sections.

*Corresponding Author: S. K. PANDEY*

Dept of Mathematics, Sardar Patel University of Police, Security and Criminal Justice, Daijar, Jodhpur, (Raj.), India.
This Ring $M$ contains several matrix fields. All the examples of infinite matrix field given in the next section are subsets of the above ring $M$.

**SOME EXAMPLES OF MATRIX FIELD OF INFINITE ORDER**

**Example 1:** Let $F = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in K \right\}$. It is easy to see that $F$ is a ring under usual addition and multiplication of matrices. $I = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ is the multiplicative identity of this ring. It is a commutative ring and $\forall A = \begin{pmatrix} a \\ 0 \\ 0 \end{pmatrix} \in F$ with $a \neq 0$ we can find $B = \begin{pmatrix} 1 \\ a \\ 0 \\ 1/a \end{pmatrix} \in F$ such that $AB = I$. Therefore $F$ is a field with respect to usual addition and multiplication of matrices.

Let $Q$, $R$ and $C$ denote the field of rational, real and complex numbers respectively.

Let $F_1 = \left\{ \begin{pmatrix} a \\ 0 \\ a \end{pmatrix} : a \in Q \right\}$.

$F_2 = \left\{ \begin{pmatrix} a \\ 0 \\ a \end{pmatrix} : a \in R \right\}$ and

$F_3 = \left\{ \begin{pmatrix} a \\ 0 \\ a \end{pmatrix} : a \in C \right\}$

then $F_2$ is an extension of $F_1$ and $F_3$ is an extension of $F_2$.

It is known from ring theory that every ring $R$ has a centre $Z(R)$. If $R$ is an $T$-algebra where $T$ is a field then $Z(R)$ contains a copy of the field $T$. One may conclude that field $F$ given in this example is the centre of ring $M$ given above. However it may be noted that the following two fields are not the centre of $M$ but both are subsets of $M$.

**Example 2:** Let $F = \left\{ \begin{pmatrix} a \\ a \\ a \end{pmatrix} : a \in K \right\}$. One can easily verify that $F$ is a ring with respect to addition and multiplication of matrices. $I = \begin{pmatrix} 1/2 \\ 1/2 \\ 1/2 \end{pmatrix}$ is the multiplicative identity of this ring. It is a commutative ring and $\forall A = \begin{pmatrix} a \\ 1 \\ a \\ 1 \\ 1/a \end{pmatrix} \in F$ with $a \neq 0$ we can find $B = \begin{pmatrix} 1/4a \\ 1 \\ 1 \\ 4a \\ 4a \end{pmatrix} \in F$ such that $AB = I$. Therefore $F$ is a field with respect to usual addition and multiplication of matrices.

**Example 3:** Let $F = \left\{ \begin{pmatrix} a \\ 0 \\ 0 \\ a \end{pmatrix} : a \in K \right\}$. It is a ring with respect to addition and multiplication of matrices. $I = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ is the multiplicative identity of this ring. It is a commutative ring and $\forall A = \begin{pmatrix} a \\ 0 \\ 0 \end{pmatrix} \in F$ with
Let $p$ be a prime number. Then $Z_p = \{0,1,2,3,4,5...p-1\}$ is a field under addition and multiplication modulo $p$. Using this field we can obtain different matrix fields of order $p$ for every positive prime $p$. We shall consider only few different matrix fields of prime order. These fields provide matrix representations for Galois field of prime order. Let $A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$ and $B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}$ are any two $2 \times 2$ matrices defined over $Z_p$ then the sum of $A$ and $B$ is defined as $A + B = (A + B) \mod p = \begin{pmatrix} (a_1 + b_1) \mod p & (a_2 + b_2) \mod p \\ (a_3 + b_3) \mod p & (a_4 + b_4) \mod p \end{pmatrix}$.

Similarly we can define the product of $A$ and $B$. In the following examples we shall consider these operations for matrix addition and multiplication respectively.

**Example 1:** Let $F = \{a \in Z_2 : a \in \{0,1\}\}$. Then $F$ is a finite field of order two with respect to addition and multiplication of matrices modulo 2. If we replace $Z_2$ by $Z_3$, then we will get a matrix field of order three. Similarly we can find a finite matrix field of higher order.

**Example 2:** If we take $F = \{a \in Z_2 : a \in \{0,1\}\}$ then we will get a matrix field of order two. By replacing $Z_2$ with $Z_3$ we shall get a matrix field of order three. Similarly we can get a matrix field of order five, seven and eleven etc..

**Example 3:** By taking $F = \{a \in Z_3 : a \in \{0,1,2\}\}$ we can get a matrix field of order three. If we replace $Z_3$ by $Z_4$ then we will get a finite matrix field of order five. The identity element of this field will be given by $I = \begin{pmatrix} 3 & 3 \\ 3 & 3 \end{pmatrix}$.

Similarly if we replace $Z_3$ by $Z_p$ in the above examples then we shall get finite matrix fields of order $p$. In the same way we can get a finite matrix field of order $p(\neq 2)$ from example 3. Thus this article provides a technique to obtain matrix representations for a finite field of prime order. One may find several such representations but all such fields are algebraically equivalent for a given prime $p$.

**REFERENCES**


[Source of Support: Nil, Conflict of interest: None Declared]