Subspace of $M_n(\mathbb{Z}_2)$

Yanita and A Adrianda
Department of Mathematics, Faculty of Mathematics and Natural Sciences, Andalas University, Kampus Unand Limau Manis Padang 25163, Indonesia
Email: yanita3010@gmail.com

Abstract. This paper discusses the subspace of the set of matrices over the set of integers modulo 2, symbolized by $M_n(\mathbb{Z}_2)$. This set $M_n(\mathbb{Z}_2)$ is a vector space over $\mathbb{Z}_n$ with scalar matrix multiplication and addition modulo n on matrices of $M_n(\mathbb{Z}_2)$. Will be given properties that proper subset and proper a subgroup of $M_n(\mathbb{Z}_2)$ which is a subspace of $M_n(\mathbb{Z}_2)$. It’s used $M_2(\mathbb{Z}_2)$ to illustration the proof of the theorems.

1. Introduction
Let’s begin with the definition vector space and subspace and then the theorem about subspaces used in this article.

Definition 1.1 [1] Let $F$ be a field, whose elements are referred to a scalars. A vector space over $F$ is a nonempty set $V$, whose element are referred to as vectors, together with two operations. The first operation, called addition and denoted by $+$, assign to each pair $(u, v)$ of vectors in $V$ a vector $u + v$ in $V$. The second operation, called scalar multiplication and denoted by juxtaposition, assigns to each pair $(r, u) \in F \times V$ a vector $ru$ in $V$. Furthermore, the following properties must be satisfied: associativity of addition, commtativity of addition, existence of a the zero, existence of additive invers and properties of scalar.

Definition 1.2 [1] A subspace of a vector space $V$ is a subset $S$ of $V$ that is a vector space in its own right under the operations obtained by restricting the operations of $V$ to $S$.

Theorem 1.1 [1] A nonempty subset $S$ of a vector space $V$ is a subspace of $V$ if and only if $S$ is closed under addition and scalar multiplication.

If $S$ and $T$ are subspaces of vector space $V$, then we may always say that the sum $S + T$ exists, and the fact is that $S + T$ is a subspace of $V$ too.

2. Vector Space $M_2(\mathbb{Z}_2)$
We give an illustration to this article with the $M_2(\mathbb{Z}_2)$ vector space.

The first, we list element of $M_2(\mathbb{Z}_2) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{Z}_2 \right\}$, that is

$A_0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, A_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, A_2 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, A_3 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, A_4 = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, A_5 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, A_6 = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, A_7 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, A_8 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, A_9 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, A_{10} = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}, A_{11} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, A_{12} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, A_{13} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, A_{14} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, A_{15} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$
Using combinatoric theory, we can get the element of $M_2(\mathbb{Z}_2)$ using formula $2^4$, since there are 4 elements in matrix $2 \times 2$, and there are 2 elements in $\mathbb{Z}_2$.

Next, if we apply addition modulo 2 on $\mathbb{Z}_2$ on matrices of $M_2(\mathbb{Z}_2)$, then we have that $M_2(\mathbb{Z}_2)$ is a group (see Table 1).

| Table 1. | Table Cayley of on matrices of $M_2(\mathbb{Z}_2)$ over addition modulo 2 |
| --- | --- |
| $+$ | $A_0$ $A_1$ $A_2$ $A_3$ $A_4$ $A_5$ $A_6$ $A_7$ $A_8$ $A_9$ $A_{10}$ $A_{11}$ $A_{12}$ $A_{13}$ $A_{14}$ $A_{15}$ |
| $A_0$ | $A_0$ | $A_1$ | $A_2$ | $A_3$ | $A_4$ | $A_5$ | $A_6$ | $A_7$ | $A_8$ | $A_9$ | $A_{10}$ | $A_{11}$ | $A_{12}$ | $A_{13}$ | $A_{14}$ | $A_{15}$ |
| $A_1$ | $A_0$ | $A_1$ | $A_2$ | $A_3$ | $A_4$ | $A_5$ | $A_6$ | $A_7$ | $A_8$ | $A_9$ | $A_{10}$ | $A_{11}$ | $A_{12}$ | $A_{13}$ | $A_{14}$ | $A_{15}$ |
| $A_2$ | $A_2$ | $A_5$ | $A_6$ | $A_7$ | $A_8$ | $A_9$ | $A_{10}$ | $A_{11}$ | $A_{12}$ | $A_{13}$ | $A_{14}$ | $A_{15}$ | $A_1$ | $A_2$ | $A_3$ | $A_4$ |
| $A_3$ | $A_3$ | $A_6$ | $A_9$ | $A_2$ | $A_{11}$ | $A_{14}$ | $A_7$ | $A_1$ | $A_{15}$ | $A_{10}$ | $A_{13}$ | $A_{12}$ | $A_{14}$ | $A_{11}$ | $A_{12}$ |
| $A_4$ | $A_4$ | $A_{13}$ | $A_{12}$ | $A_{14}$ | $A_{15}$ | $A_8$ | $A_0$ | $A_2$ | $A_3$ | $A_4$ | $A_{15}$ | $A_{12}$ | $A_{14}$ | $A_{15}$ | $A_1$ |
| $A_5$ | $A_5$ | $A_2$ | $A_9$ | $A_{10}$ | $A_{12}$ | $A_{13}$ | $A_{14}$ | $A_8$ | $A_0$ | $A_2$ | $A_3$ | $A_{15}$ | $A_{12}$ | $A_{14}$ | $A_{15}$ |
| $A_6$ | $A_6$ | $A_9$ | $A_3$ | $A_{11}$ | $A_{12}$ | $A_{13}$ | $A_{14}$ | $A_8$ | $A_0$ | $A_2$ | $A_3$ | $A_4$ | $A_{15}$ | $A_{12}$ |
| $A_7$ | $A_7$ | $A_{10}$ | $A_{11}$ | $A_{12}$ | $A_{13}$ | $A_{14}$ | $A_{15}$ | $A_8$ | $A_0$ | $A_2$ | $A_3$ | $A_4$ | $A_{15}$ | $A_{12}$ |
| $A_8$ | $A_8$ | $A_{15}$ | $A_{11}$ | $A_{13}$ | $A_{14}$ | $A_{15}$ | $A_8$ | $A_0$ | $A_2$ | $A_3$ | $A_4$ | $A_{15}$ | $A_{12}$ |
| $A_9$ | $A_9$ | $A_{16}$ | $A_{15}$ | $A_{14}$ | $A_{13}$ | $A_{12}$ | $A_{11}$ | $A_{10}$ | $A_{13}$ | $A_{14}$ | $A_{15}$ | $A_1$ | $A_2$ | $A_3$ | $A_4$ |
| $A_{10}$ | $A_{10}$ | $A_{17}$ | $A_{15}$ | $A_{14}$ | $A_{13}$ | $A_{12}$ | $A_{11}$ | $A_{10}$ | $A_{13}$ | $A_{14}$ | $A_{15}$ | $A_1$ | $A_2$ | $A_3$ | $A_4$ |
| $A_{11}$ | $A_{11}$ | $A_{14}$ | $A_{13}$ | $A_{12}$ | $A_{11}$ | $A_{10}$ | $A_{11}$ | $A_{13}$ | $A_{14}$ | $A_{15}$ | $A_1$ | $A_2$ | $A_3$ | $A_4$ |
| $A_{12}$ | $A_{12}$ | $A_{13}$ | $A_{14}$ | $A_{15}$ | $A_7$ | $A_{12}$ | $A_{13}$ | $A_{14}$ | $A_{15}$ | $A_1$ | $A_2$ | $A_3$ | $A_4$ |
| $A_{13}$ | $A_{13}$ | $A_{10}$ | $A_{14}$ | $A_{15}$ | $A_7$ | $A_{12}$ | $A_{13}$ | $A_{14}$ | $A_{15}$ | $A_1$ | $A_2$ | $A_3$ | $A_4$ |
| $A_{14}$ | $A_{14}$ | $A_{11}$ | $A_{15}$ | $A_{10}$ | $A_{12}$ | $A_{13}$ | $A_{14}$ | $A_{15}$ | $A_1$ | $A_2$ | $A_3$ | $A_4$ |
| $A_{15}$ | $A_{15}$ | $A_{11}$ | $A_{14}$ | $A_{13}$ | $A_{12}$ | $A_{11}$ | $A_{10}$ | $A_{13}$ | $A_{14}$ | $A_{15}$ | $A_1$ | $A_2$ | $A_3$ |

Furthermore, if we apply scalar multiplication on the element of $\mathbb{Z}_2$ moreover, matrices on $M_2(\mathbb{Z}_2)$, then we have

| Table 2. | Scalar multiplication on the element of $\mathbb{Z}_2$ moreover, matrices on $M_2(\mathbb{Z}_2)$ |
| --- | --- |
| $\times 2$ | $A_0$ $A_1$ $A_2$ $A_3$ $A_4$ $A_5$ $A_6$ $A_7$ $A_8$ $A_9$ $A_{10}$ $A_{11}$ $A_{12}$ $A_{13}$ $A_{14}$ $A_{15}$ |
| $0A$ | $A_0$ | $A_0$ | $A_0$ | $A_0$ | $A_0$ | $A_0$ | $A_0$ | $A_0$ | $A_0$ | $A_0$ | $A_0$ |
| $1A$ | $A_0$ | $A_1$ | $A_2$ | $A_3$ | $A_4$ | $A_5$ | $A_6$ | $A_7$ | $A_8$ | $A_9$ | $A_{10}$ | $A_{11}$ |

Based on Table 1. and Table 2. It is concluded that $M_2(\mathbb{Z}_2)$ is vector space over $\mathbb{Z}_2$. It’s known that set $M_2(\mathbb{Z}_2)$ has $2^{16}$ subsets, and certainly not all are subspaces.

This paper aims to identify the subsets of $M_n(\mathbb{Z}_2)$ which is a subspace of $M_n(\mathbb{Z}_2)$. We provide illustrations on $M_2(\mathbb{Z}_2)$. There are 3 properties given in this case; it gives a condition a subset of $M_2(\mathbb{Z}_2)$ is subspace of $M_2(\mathbb{Z}_2)$. It’s shown that three conditions for proper a subset of $M_2(\mathbb{Z}_2)$ which is subspacea of $M_2(\mathbb{Z}_2)$.

**Lemma 2.1** Let $U = \{A_0, B| A_0, B \in M_2(\mathbb{Z}_2), A_0 \neq B \}$, then $U$ is subspace of $M_2(\mathbb{Z}_2)$.

**Proof.** Clear that $U \subset M_2(\mathbb{Z}_2)$ and $U \neq \emptyset$. Let $A, B \in U$, and set $A = A_0$. Note that for each $B \in M_2(\mathbb{Z}_2)$, $B + B = A_0$, so $B + B + B^{-1} = A_0 + B^{-1} = B^{-1}$ and we have $B = B^{-1}$. Thus, for each $A, B \in U$, $A + B \in U$. Furthermore, if $k = 0$ we have $kA = A_0$ and if $k = 1$, we have $kA = A$ for every $A \in U$. Thus, for every $A \in U$ and $k \in \mathbb{Z}_2$, $kA \in U$.

**Lemma 2.2** Let $U = \{A_0, B, C, D| A_0, B, C, D \in M_2(\mathbb{Z}_2), \text{and different}, B + C = D \}$, then $U$ is subspace of $M_2(\mathbb{Z}_2)$.
Proof.  
Clear that $(\text{I})$ and $(\text{II})$. Let $A, B \in U$. Since $M_2(\mathbb{Z}_2)$ is vector space, so $A_0 + A = A + A_0 = A$ for each $A \in U$. Note that, if $B, C, D \in U$ and $B + C = D$, we have $B = D + C$ (remember that $B + C + C^{-1} = D + C^{-1}$ and imply that $B + A_0 = D + C^{-1}$, and based on Lemma 1.1, $C^{-1} = C$ ). Analogously, we have $C = B + D$. Based on this, it’s found that for every $A, B \in U$, $A + B \in U$. Furthermore, if $k = \bar{0}$ we have $kA = A_0$ and if $k = \bar{1}$, we have $kA = A$ for every $A \in U$. Thus, for every $A \in U$ and $k \in \mathbb{Z}_2$, $kA \in U$.

**Lemma 2.3** Let $U = \{A_0, B, C, D, E, F, G, H | A_0, B, C, D, F, G, H \in M_2(\mathbb{Z}_2), \text{ and all different} \}$, then $U$ is subspace of $M_2(\mathbb{Z}_2)$ whenever $B + C = D, B + E = F, C + E = G, D + E = H, B + G = H, C + F$.

Proof.  
Analogously with Lemma 2.2.

The next properties associates to subgroup of $M_2(\mathbb{Z}_2)$, that is condition of proper subgroup of $M_2(\mathbb{Z}_2)$ which is subspace of $M_2(\mathbb{Z}_2)$.

Based on Lemma 2.1, 2.2 and 2.3, it’s concluded that subspace of $M_2(\mathbb{Z}_2)$ is subgroup of $M_2(\mathbb{Z}_2)$.

**Theorem 2.1** Let $U$ subset of $M_2(\mathbb{Z}_2)$, if $U$ is a subgroup of $M_2(\mathbb{Z}_2)$ then $U$ is a subspace of $M_2(\mathbb{Z}_2)$.

Proof.  
Lagrange Theorem states that for any finite group $G$, the order (number of elements) of every subgroup $H$ of $G$ divides the order of $G$ [2]. Thus, for the group $M_2(\mathbb{Z}_2)$ over addition modulo 2 can be concluded that the order of subgroups are 1, 2, 4, 8 and 16. Every group $G$ has 2 subgroup trivial, that is $\{e\}$ ($e$ is identity element) and $G$, so group $M_2(\mathbb{Z}_2)$ over addition modulo 2 has $\{A_0\}$ and $M_2(\mathbb{Z}_2)$ as trivial subgroup.

Thus $\{A_0\}$ and $M_2(\mathbb{Z}_2)$ are subspace in $M_2(\mathbb{Z}_2)$, see [1]. Let $U$ be a subgroup of $M_2(\mathbb{Z}_2)$. Lemma 2.1, Lemma 2.2, and Lemma 2.3 describes a subset of $M_2(\mathbb{Z}_2)$ whose number of elements is 2, 4 and 8 which satisfies the subspace properties and it’s known that $U$ is a subgroup. This complete the proof.

3. **Vector Space $M_n(\mathbb{Z}_n)$**

We repeat Theorem 2.1 in general case

**Theorem 3.1** Let $U$ subset of $M_n(\mathbb{Z}_2)$, if $U$ is a subgroup of $M_n(\mathbb{Z}_2)$ ($n \geq 2$) then $U$ is subspace of $M_n(\mathbb{Z}_2)$.

Proof.  
Proof has been given for $n = 2$.

For $n = 3$, we have number of elements of $M_n(\mathbb{Z}_2)$ are $2^9$ and in general we, have $2^n \times n$ elements for $M_n(\mathbb{Z}_2)$. From this, explicit that the number of elements from $M_n(\mathbb{Z}_2)$ has no prime number. Thus, based on proof of $n = 2$, it can be done for $n > 2$.

In group theory also has the property that the sum of 2 or more subgroups is also subgroup ([3] and [4]). We use Lagrange Theorem to find the whole of order subgroup of $M_n(\mathbb{Z}_2)$. Let $H$ be a proper subgroup of $M_n(\mathbb{Z}_2)$ and $|H| = d \leq n \times n$ and $d | (n \times n)$. We write that $H = \{I, A_1, A_2, ..., A_{k-1}\}$, $I$ is identity matrix in $M_n(\mathbb{Z}_2)$. Since $H$ is group under matrix multiplication modulo $n$ and $H$ is closed under scalar multiplication matrix and element of $\mathbb{Z}_2$, so this complete the proof.

References
[1] Roman S 2008 *Advanced Linear Algebra* (New York: Springer Sciences+Bussiness Media).
[2] Roth R 2001 *Mathematics Magazine* 74 99
[3] Gallian J 2006 *Contemporary Abstract Algebra* 6th ed. Boston: Houghton Mifflin).
[4] Grillet P 2007 *Abstract Algebra* 2nd ed. (New York: Springer, Sciences+Bussiness Media).