Maths-1: Linear Algebra

Vector Spaces over the Finite Field $\mathbb{Z}/2\mathbb{Z}$

The concept of a vector space can be extended to fields other than $\mathbb{R}$ and $\mathbb{C}$. We will not dwell on the theoretical aspects of this.

The field $\mathbb{Z}/2\mathbb{Z}$ is simply the set $\{0,1\}$ on which the operation of addition is defined by:

$$0+0=0, \quad 0+1=1, \quad 1+0=1, \quad 1+1=0 \tag{$*$}$$

and multiplication is defined by:

$$0.0=0, \quad 0.1=0, \quad 1.0=0, \quad 1.1=1 \tag{$**$}$$

Interested students should feel free to look up the definition of a field in any standard university level Algebra text. For the purpose of this assignment you can take it on faith that $\mathbb{Z}/2\mathbb{Z}$ is a field.

Axler's Definitions 1.18 and 1.19 can be now applied with $F = \mathbb{Z}/2\mathbb{Z}$ to get a vector space over $\mathbb{Z}/2\mathbb{Z}$. Students may take this on faith for now.

An example of such a vector space is the set $V = (\mathbb{Z}/2\mathbb{Z})^4$, the set of all 4-tuples of 0s and 1s, with component-wise addition and scalar multiplication defined using the relations in $(*)$ and $(**)$.

A *non-empty* subset $W \subset (\mathbb{Z}/2\mathbb{Z})^4$ is said to be a *subspace* of $(\mathbb{Z}/2\mathbb{Z})^4$ if W is closed the component-wise addition and component-wise scalar mutiplication as defined using the relations specified by $(*)$ and $(**)$.

Example Let us verify that the set

$$W = \{(0,0,0,0),(1,0,0,0),(0,1,0,0),(1,1,0,0)\}$$

is a subspace of $(\mathbb{Z}/2\mathbb{Z})^4$ by verfiying that (i) it is closed under vector addition:

$$\begin{aligned}
(0,0,0,0)+(0,0,0,0) &= (0,0,0,0)\\
(0,0,0,0)+(1,0,0,0) &= (1,0,0,0)\\
(0,0,0,0)+(0,1,0,0) &= (0,1,0,0)\\
(0,0,0,0)+(1,1,0,0) &= (1,1,0,0)\\
(1,0,0,0)+(1,0,0,0) &= (0,0,0,0)\\
(1,0,0,0)+(0,1,0,0) &= (1,1,0,0)\\
(1,0,0,0)+(1,1,0,0) &= (0,1,0,0)\\
(0,1,0,0)+(0,1,0,0) &= (0,0,0,0)\\
(0,1,0,0)+(1,1,0,0) &= (1,0,0,0)\\
(1,1,0,0)+(1,1,0,0) &= (0,0,0,0)
\end{aligned}$$

(ii) it is closed under scalar multiplication:

$$
\begin{aligned}
0.(0,0,0,0) &= (0,0,0,0)\\
0.(1,0,0,0) &= (0,0,0,0)\\
0.(0,1,0,0) &= (0,0,0,0)\\
0.(1,1,0,0) &= (0,0,0,0)\\
1.(0,0,0,0) &= (0,0,0,0)\\
1.(1,0,0,0) &= (1,0,0,0)\\
1.(0,1,0,0) &= (0,1,0,0)\\
1.(1,1,0,0) &= (1,1,0,0)
\end{aligned}
$$

Please note that the above computations are done for the sake of explanation only. You do not need to print any explicit computations in your assignment. It is not recommended at all.