

Assignment 10

Adarsh Srivastava

The link to the solution is

<https://github.com/Adarsh1310/EE5609>

Abstract—This documents solves a problem based on fields.

1 PROBLEM

Let \mathbb{F} be a set which contains exactly two elements, 0 and 1. Define an addition and multiplication by tables.

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

Verify that the set \mathbb{F} , together with these two operations, is a field.

2 SOLUTION

To prove that $(\mathbb{F}, +, \cdot)$ is a field we need to satisfy the following,

- 1) $+$ and \cdot should be closed
 - For any a and b in \mathbb{F} , $a+b \in \mathbb{F}$ and $a \cdot b \in \mathbb{F}$. For example $0+0=0$ and $0 \cdot 0=0$.
- 2) $+$ and \cdot should be commutative
 - For any a and b in \mathbb{F} , $a+b = b+a$ and $a \cdot b = b \cdot a$. For example $0+1=1+0$ and $0 \cdot 1=1 \cdot 0$.
- 3) $+$ and \cdot should be associative
 - For any a and b in \mathbb{F} , $a+(b+c) = (a+b)+c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$. For example $0+(1+0)=(0+1)+0$ and $0 \cdot (1 \cdot 0)=(0 \cdot 1) \cdot 0$.
- 4) $+$ and \cdot operations should have an identity element
 - If we perform $a + 0$ then for any value of a from \mathbb{F} the result will be a itself. Hence 0

is an identity element of $+$ operation. If we perform $a \cdot 1$ then for any value of a from \mathbb{F} the result will be a itself. Hence 1 is an identity element of \cdot operation.

- 5) $\forall a \in \mathbb{F}$ there exists an additive inverse
 - For additive inverse to exist, $\forall a$ in \mathbb{F} $a+(-a)=0$. For example. $1-1=0$ and $0-0=0$.
- 6) $\forall a \in \mathbb{F}$ such that a is non zero there exists a multiplicative inverse
 - For multiplicative inverse to exist, $\forall a$ such that a is non zero in \mathbb{F} , $a \cdot a^{-1}=1$. For example $1 \cdot 1^{-1} = 1$.
- 7) $+$ and \cdot should hold distributive property
 - For any a, b and c in \mathbb{F} the property $a \cdot (b+c)=a \cdot b+a \cdot c$ should always hold true. For example $0 \cdot (1+2)=0 \cdot 1+0 \cdot 2$.

3 RESULT

Since the above properties are satisfied we can say that $(\mathbb{F}, +, \cdot)$ is a field.