Mathematics 2200H – Mathematical Reasoning
TRENT UNIVERSITY, Fall 2022
Solutions to Assignment #6
The Littlest Field

Please your complete reasoning in your solution. Recall that, unless stated otherwise on a given assignment, you are permitted to work together and look things up, so long as you write up your solution by yourself and acknowledge all sources and help that you ended up using.

$\mathbb{Z}_2$ is the system of integers modulo 2. Roughly, this means that all odd numbers are equal to 1 and all even numbers are equal to 0 when you do arithmetic. (Think of it as keeping time on a rapidly spinning planet with a two-hour day... :-) A little more technically, $\mathbb{Z}_2 = \{0, 1\}$, with the operations $+$ and $\cdot$ given by the following tables:

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \quad \text{and} \quad \begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$$

1. a. For each $a \in \mathbb{Z}_2$, what is $-a$, assuming that such exists? *[0.5]*
b. For each $a \in \mathbb{Z}_2$, what is a^{-1}, assuming that such exists? *[0.5]*

SOLUTIONS. *(Favoured by the Impressive Clergyman.)* **a.** $-0 = 0$ since $0 + 0 = 0$ and $-1 = 1$ since $1 + 1 = 0$. □

b. 0^{-1} does not exist since there is no $a \in \mathbb{Z}_2$ such that $0 \cdot a = 1$. On the other hand, $1^{-1} = 1$ since $1 \cdot 1 = 1$. ■

2. Show that $+$ and $\cdot$ on $\mathbb{Z}_2$ are both associative and commutative, and that the distributive law holds. *[4]*

SOLUTION THE FIRST. *(Favoured by the Brute Squad.)* Check them all!
Associativity of addition:

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

Commutativity of addition:

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

Associativity of multiplication:

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

Commutativity of multiplication:

$$
\begin{aligned}
0 \cdot 0 &= 0 = 0 \cdot 0 \\
0 \cdot 1 &= 0 = 1 \cdot 0 \\
1 \cdot 0 &= 0 = 0 \cdot 1 \\
1 \cdot 1 &= 1 = 1 \cdot 1
\end{aligned}
$$

Distribution from the left:

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

Distribution from the right:

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

That's that! Are your eyes thoroughly glazed over? ■

SOLUTION THE SECOND. *(Favoured by Miracle Max.)* Arithmetic in the integers modulo 2 respects the arithmetic operations in the integers. Since $+$ and $\cdot$ on the integers are associative and commutative, and satisfy the distributive law, it follows that so do their counterparts in $\mathbb{Z}$. ■

3. Use your answers to **1** and **2** to verify that $\mathbb{Z}_2$ is a *field*[†]. *[1]*

SOLUTION. *(Favoured by Vizzini.)* A remark on page 429 of the fourth edition of *Linear Algebra: A Modern Introduction*, by David Poole, tells us what a field is, at least informally:

> By "scalars" we will usually mean the real numbers. Accordingly, we should refer to V as a *real vector space* (or a *vector space over the real numbers*). It is also possible for scalars to be complex numbers or to belong to $\mathbb{Z}_p$, where p is prime. In these cases, V is called a *complex vector space* or a *vector space over* $\mathbb{Z}_p$, respectively. Most of our examples will be real vector spaces, so we will usually omit the adjective "real." If something is referred to as a "vector space," assume that we are working over the real number system.
>
> In fact, the scalars can be chosen from any number system in which, roughly speaking, we can add, subtract, multiply, and divide according to the usual laws of arithmetic. In abstract algebra, such a number system is called a *field*.

[†] You can look up the definition of a field in your old linear algebra textbook or online.

$\mathbb{Z}_p$, *i.e.* the integers modulo a prime p, is noted in this remark as a possible set of scalars, hence presumably a field. As 2 is a prime number, $\mathbb{Z}_2$ is a field.

Moreover, the solutions to **1** and **2** above demonstrate that the arithmetic operations on $\mathbb{Z}_2$ behave as expected: $+$ and $\cdot$ are associative and commutative, the distributive laws hold, both operations have unit or neutral elements (0 and 1, repectively), and inverses (except for 0 under multiplication). Thus $\mathbb{Z}_2$ has the same basic algebraic properties as the real numbers do, so it counts as a field. ■

4. $\mathbb{Z}_2^2$ is the usual two-dimensional vector space over $\mathbb{Z}_2$, in the same way that $\mathbb{R}^2$ is the usual two-dimensional vector space over the field of real numbers $\mathbb{R}$. What are all the subspaces of $\mathbb{Z}_2^2$? *[4]*

Hint: The most complete way to answer the last question is to simply write out each subspace as a set of vectors.

Solution. *(Favoured by Fezzik.)* Here they are:

$$\left\{ \begin{bmatrix} 0 \\ 0 \end{bmatrix} \right\}$$

$$\left\{ \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right\}$$

$$\left\{ \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}$$

$$\left\{ \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\}$$

$$\left\{ \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\}$$

We leave it to the Brute Squad to check that each of these sets of vectors of $\mathbb{Z}_2^2$ is actually a subspace, *i.e.* closed under the operations of multiplication by scalars and addition of vectors. ■