

Assignments are due at the start of class on the given Due date.

Please Note! *Special problems are like “term papers.” They must be well-written, in ink, on standard 8.5 x 11 paper, and must be succinct - with exactly enough detail.*

Paper torn from spiral notebooks is not acceptable.

Err in the direction of slightly excessive detail at first,

but prolixity is not acceptable.

Solution for the second part.

We have to **define** addition and multiplication so that the field axioms are satisfied. There are some things we can say “in advance” of making our addition and multiplications tables:

- 0 and 1 have to act as identities for + and \times
thus each table will have an appropriate “repeated row”
- Since $0 \times a = 0$ for all a , the \times table will have a row and column of zeroes
- Inverses are needed, so each (appropriate) row and column
- has to contain just one copy of each (appropriate) element

This means we get the following tables, with \circ denoting an element to be filled in:

+	0	1	2	3
0	0	1	2	3
1	1	\circ	\circ	\circ
2	2	\circ	\circ	\circ
3	3	\circ	\circ	\circ

\times	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	\circ	\circ
3	0	3	\circ	\circ

In the \times table, we have to put a 1 or 3 in the first place to fill in (row 4, column 4)., because there’s already a 2 in the row and the column. If we try to put a 1 there, then we have to put a 3 in the last column, and that won’t work, because there’s already a 3 in column 5. So we have to put a 3 then a 1. Then in the last row we have to put 1 and 2. So now we know what the multiplication table has to be:

\times	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Now, how do we fill in the addition table so that it works, and so that both tables work together? We can take advantage of the fact that proved, in the first part of the problem, that we had a field with two elements. That field is usually called \mathbb{Z}_2 , and its operations are exactly what we get when we add and multiply in the usual way, but we only record whether the answers are even (i.e., zero) or odd (i.e., one). We are now going to use the idea of how to make the complex numbers, by considering polynomials $ax + b$, $ax^3 + bx^2 + cx + d$ and so on, where x is a variable that we will later give a meaning to. (In the complex numbers, we do this, using i instead of x , and we require that $i^2 = -1$.) We define *equality* of two of these polynomials by demanding that the coefficients of corresponding powers are equal.

Now we **define addition and multiplication** of these polynomials by:

$$(ax + b) + (cx + d) := (a + c)x + (b + d) \quad \text{and} \quad (ax + b) \times (cx + d) := acx^2 + adx + bcx + bd = ax^2 + (ad + bc)x + bd.$$

We followed this rule when writing these definitions: treat all quantities, including x , as commuting and associating quantities, with respect to addition and multiplication, then group them as a sum of coefficients (from \mathbb{Z}_2) times

powers of x . This immediately gives commutativity, by inspection of the formulas, keeping in mind the question “what happens when we interchange a and c , b and d ?” In particular, we may have to write down the steps showing that $ad+bc=cb+da$. Later we will replace x^2 by $Ax+B$ and rearrange again, to get a “quantity” of the form $gx+h$. If necessary, we replace x^3 by $xx^2=x(Ax+B)=Ax^2+Bx=A(Ax+B)+Bx=A^2+Bx+AB=Bx+(A^2+AB)$. Higher powers would be treated similarly, but we won’t encounter them. All our coefficients here are elements of the field \mathbb{Z}_2 from the first part of the problem, and the operations of addition and multiplication involving pairs of those elements are the operations from the field \mathbb{Z}_2 . For example, $(x+1)+(0x+1)=x+(1+1)=x+0(=x)$ and $(x+1)\times x=x^2+x$. When we later replace x^2 by $Ax+B$, we will have $x^2+x=(Ax+B)+x=(A+1)x+B$.

Because of the way we defined addition, we can take advantage of associativity in \mathbb{Z}_2 to check associativity here:

$$\begin{aligned}(ax+b)+((cx+d)+(ex+f)) &= (ax+b)+((c+e)x+(d+f)) \\ &= (a+(c+e))x+(b+(d+f)) \\ &= ((a+c)+e)x+((b+d)+f).\end{aligned}$$

and, grouping the other way,

$$\begin{aligned}((ax+b)+(cx+d))+ (ex+f) &= ((a+c)x+(b+d))+ (ex+f) \\ &= ((a+c)+e)x+((b+d)+f).\end{aligned}$$

Either grouping thus gives the same result, so addition of these polynomials is associative.

We can handle multiplication the same way, but we get higher powers of x :

$$\begin{aligned}(ax+b)\times((cx+d)\times(ex+f)) &= (ax+b)\times(cex^2+(cf+de)x+df) \\ &= a(ce)x^3+a(cf+de)x^2+a(df)x+b(ce)x^2+b(cf+de)x+b(df) \\ &= a(ce)x^3+(a(cf+de)+b(ce))x^2+(a(df)+b(cf+de))x+b(df) \\ &= acex^3+(acf+ade+bce)x^2+(adf+bcf+bde)x+buf.\end{aligned}$$

and, grouping the other way, following the rules,

$$\begin{aligned}((ax+b)\times(cx+d))\times(ex+f) &= (acx^2+(ad+bc)x+bd)\times(ex+f) \\ &= (ac)ex^3+(ac)fx^2+(ad+bc)ex^2+(ad+bc)fx+(bd)ex+(bd)f \\ &= (ac)ex^3+((ac)f+(ad+bc)e)x^2+((ad+bc)f+(bd)e)x+b(df) \\ &= acex^3+(acf+ade+bce)x^2+(adf+bcf+bde)x+buf.\end{aligned}$$

Either grouping thus gives the same result, so multiplication of the polynomials of the form $ax+b$ is associative.

Next we match polynomials with our symbols 0, 1, 2, 3. We will match $0x+0=0$ with 0 and $0x+1=1$ with 1. It seems natural to match $1x+0=x$ with 2 and match $1x+1=x+1$ with 3. Does this work – when we multiply these polynomials together, do we get the right matches with the multiplication table that we that we know is the only one possible? Because of commutativity we only have to check that the matchings for 2×2 , 2×3 and 3×3 result in matches for 3, 1 and 2, respectively.

We get: 2×2 corresponds to x^2 , 2×3 corresponds to $x(x+1)=x^2+x$ and 3×3 corresponds to

$$(x+1)(x+1)=x^2+x+x+1=x^2+(1+1)x+1=x^2+0x+1=x^2+1.$$

This is not a match yet! What we need is to see whether we can arrange for what we got, x^2 , x^2+x and x^2+1 , respectively, to match 3, 1 and 2, respectively. Considering the matches we started with, we thus ask: is it true that

$$x^2=x+1 \text{ and } x^2+x=1 \text{ and } x^2+1=x,$$

because the left-side polynomials are what we got by multiplying the polynomials assigned to the products $2\times 2=3$ and $2\times 3=1$ and $3\times 3=2$, and the right-side polynomials are the polynomials assigned to 3, 1 and 2, respectively.

So now we will replace x^2 , whenever it appears, by $x + 1$ (from the first equation). This makes $x^2 = x + 1$ true. In the second equation, the left side becomes $x^2 + x = (x + 1) + x = (1 + 1)x + 1 = 0x + 1 = 1$, which agrees with the right side. Thus setting $x^2 = x + 1$ makes $x^2 + x = 1$. We next substitute $x + 1$ for x^2 on the left side in the third (hoped for) equation: $x^2 + 1 = (x + 1) + 1 = x + (1 + 1) = x + 0 = x$, and so the equation $x^2 + 1 = x$ is also true, so the multiplication table for our polynomials matches. We can now fill in the missing spots in the addition table by adding polynomials in the usual way: we get $1 + 1 = 0$, $1 + 2 \leftrightarrow (0x + 1) + (1x + 0) = x + 1 \leftrightarrow 3$, $1 + 3 \leftrightarrow (0x + 1) + (1x + 1) = x + (1 + 1) = x + 0 = x \leftrightarrow 2$, $2 + 1 = 1 + 2 = 3$ by commutativity, $2 + 2 \leftrightarrow x + x = 0$, $2 + 3 \leftrightarrow x + (x + 1) = (x + x) + 1 = 1$, and $3 + 3 \leftrightarrow (x + 1) + (x + 1) = (x + x) + (1 + 1) = 0$. The skipped cases are OK, by commutativity.

On the set $\{0, 1, 2, 3\}$ we can now define addition and multiplication by the following tables:

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

We have shown already that addition and multiplication are commutative and associative, and this is reflected in the tables. The addition and multiplication tables show the existence of additive and multiplicative identities, and the existence of inverses (each row and column in the addition table contains all 4 elements, each row and column of the multiplication table that involves non-zero elements contains all three non-zero elements). We know also that $1 \neq 0$, from the tables. It remains to prove the distributive law. We do this abstractly, returning to the polynomials, remembering that we have to replace x^2 by $x + 1$:

$$(ax + b)((cx + d) + (ex + f)) = (ax + b)((c + e)x + (d + f)) = a(c + e)x^2 + a(d + f)x + b(c + e)x + b(d + f),$$

which simplifies to

$$\begin{aligned} (ax + b)((cx + d) + (ex + f)) &= (ac + ae)(x + 1) + (ad + af + bc + be)x + b(d + f) \\ &= (ac + ae + ad + af + bc + be)x + (ac + ae + bd + bf). \end{aligned}$$

And we have

$$\begin{aligned} (ax + b)(cx + d) + (ax + b)(ex + f) &= acx^2 + (ad + bc)x + bd + aex^2 + (af + be)x + bf \\ &= ac(x + 1) + (ad + bc)x + bd + ae(x + 1) + (af + be)x + bf \\ &= acx + ac + (ad + bc)x + bd + aex + ae + (af + be)x + bf \\ &= (ac + ad + bc + ae + af + be)x + (ac + bd + ae + bf). \end{aligned}$$

By tedious inspection of the two (using “extended” associativity and repeated commutativity), we see that distributivity holds. Hence this system is a field.

There are other possibilities for an addition table, for example, arithmetic modulo 4. But that does not satisfy the distributive law, since $3(2 + 2) = 3 \cdot 0 = 0$ and $3 \cdot 2 + 3 \cdot 2 = 1 + 1 = 2$ if we use addition modulo 4 instead of the addition from our table, which gives $3(2 + 2) = 3 \cdot 0 = 0$ and $3 \cdot 2 + 3 \cdot 2 = 1 + 1 = 0$.

There is a field with N elements if and only if N is a power of a prime. Thus there is no field with six elements.