Math 108a | Professor: Padraic Bartlett

Lecture 2: Fields, Formally

Week 1 | *UCSB 2013*

In our first lecture, we studied $\mathbb{R}$, the real numbers. In particular, we examined how the real numbers interacted with the operations of addition and multiplication, listing a number of properties that we believed the real numbers satisfied. From there, we showed that some of those properties were "superfluous:" i.e. we showed that we could prove that some of these properties were necessary consequences of other properties, and therefore that listing them was unnecessary [1].

Finally, at the end of class, we defined the mathematical concept of **fields**. We restate this here, as fields will be the subject of today's talk:

1 Fields: Definitions and Examples

Definition. A **field** is a set F along with a pair of operations $+$, $\cdot$, typically thought of as addition and multiplication, such that the following properties hold:

- **Closure**$(+)$: $\forall a, b \in F$, we have $a+b \in F$.
- **Identity**$(+)$: $\exists 0 \in F$ such that $\forall a \in F$, $0 + a = a$.
- **Commutativity**$(+)$: $\forall a, b \in F, a + b = b + a$.
- **Associativity**$(+)$: $\forall a, b, c \in F, (a + b) + c = a + (b + c)$.
- **Inverses**$(+)$: $\forall a \in F, \exists$ some $-a \in F$ such that $a + (-a) = 0$.
- **Closure**$(\cdot)$: $\forall a, b \in F$, we have $a \cdot b \in F$.
- **Identity**$(\cdot)$: $\exists 1 \in F$ such that $\forall a \in F$, $1 \cdot a = a$.
- **Commutativity**$(\cdot)$: $\forall a, b \in F, a \cdot b = b \cdot a$.
- **Associativity**$(\cdot)$: $\forall a, b, c \in F, (a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- **Inverses**$(\cdot)$: $\forall a \neq 0 \in F, \exists$ some$a^{-1} \in F$ such that $a \cdot a^{-1} = 1$.

- **Distributivity**$(+, \cdot)$: $\forall a, b, c \in F, (a + b) \cdot c = (a \cdot c) + (b \cdot c)$

Typically, when we write down a field, we do so in the form $\langle F, +, \cdot \rangle$, so that we understand that F is a field with respect to those two operations $+$ and $\cdot$. This may seem odd at first — why would we need to talk about what addition and multiplication are? — but this comes in handy later, when we want to work on sets where what addition and multiplication even **are** can be tricky to understand.

[1] To make an analogy: this would be like listing a set of properties of the UCSB campus, and listing separately that (a) we have a building called Phelps Hall and (b) that we have a class called Math 108a that is taught in Phelps Hall, room 3505. Sure, these are both true properties: but if you know the second property than the first one falls as a logical consequence! So there's no need to list the first property, if you have the second.

As we discussed in our last class, the real numbers $\mathbb{R}$ along with standard addition and multiplication form a field. What other objects are fields? What objects are not fields?

- Let's consider $\langle \mathbb{N}, +\cdot \rangle$, the **natural numbers**: i.e. the nonnegative whole numbers $\{0, 1, 2, 3, \ldots\}$. Does this set form a field, along with the typical operations of addition and multiplication?

  As it turns out: no! This set does not have **additive inverses**. In specific, 1 is a natural number, and yet there is no natural number that we can add to 1 to get to 0.

- Now, let's consider $\langle \mathbb{Z}, +, \cdot \rangle$, the **integers**, i.e. the whole numbers where we allow negative and positive values: $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$. Unlike $\mathbb{N}$, this set satisfies the additive inverse property: given any $a \in \mathbb{Z}$, we know that $-a$ is also an integer, and furthermore that $a + (-a) = 0$.

  However, this set is also not a field, because it fails the property of having **multiplicative inverses**. In particular, 2 is an integer, and yet there is no integer a such that $a \cdot 2 = 1$.

- Now, let's try $\langle [-1, 1], +, \cdot \rangle$, the closed interval containing all of the real numbers between -1 and 1, along with the standard operations of $+$ and $\cdot$. This set has additive inverses: for any number $x \in [-, 1, 1]$, the number $-x$ is also in $[-1, 1]$, because this interval is symmetric. However, it also fails to have multiplicative inverses: $\frac{1}{2} \in [-1, 1]$, and yet there is no $x \in [-1, 1]$ such that $x \cdot \frac{1}{2} = 1$. Moreover, this set fails to be additively **closed**: i.e. it is possible to add two numbers in our set and get a number outside of our set! For example, $\frac{1}{2}$ and $\frac{2}{3}$ are in our set, while $\frac{1}{2} + \frac{2}{3} = \frac{7}{6}$ is not in our set.

So: we have a lot of examples of things that are **not** fields. How about an example of something that **is** a field? In particular, let's consider $\langle \mathbb{Q}, +, \cdot \rangle$, the **rational numbers**. If you haven't seen these before, here's a definition:

Definition. $\mathbb{Q}$, the **rational numbers**, is the collection of all numbers of the form $\frac{p}{q}$ such that:

1. Both p and q are integers.
2. q is nonzero. We don't want to accidentally divide by 0.

We define addition on this set as normal by declaring

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd},$$

for any $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$.

Similarly, we define multiplication by

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd},$$

for any $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$.

Finally, take any element $\frac{p}{q} \in \mathbb{Q}$, and suppose that both p and q share a common factor $r \in \mathbb{Z}$. In other words, suppose that we can write $p = r \cdot a$ and $q = r \cdot b$, for some set of integers $r, a, b \in \mathbb{Z}$. Then we consider $\frac{p}{q}$ and $\frac{a}{b}$ to be the same fraction. Essentially, this is like saying that

$$\frac{p}{q} = \frac{r \cdot a}{r \cdot b} = \frac{a}{b}.$$

In other words, we can cancel out common factors.

This defines $\mathbb{Q}$. Is this a field? Well: let's check!

- Does **closure**$(+)$ hold: i.e. is it additively closed? Well: let's take any pair of fractions $\frac{a}{b}, \frac{c}{d}$. We know, because of how addition is defined on fractions, that $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$. Both $ad+cb$ and bd are integers, because a, b, c, d are all integers; furthermore, because neither b or d are zero, we know that bd is also nonzero. Therefore, we satisfy the properties required to be a rational number listed above. Consequently, we have shown that adding any two rational numbers together yields another rational number: in other words, we've proven that addition is closed!

- How about **closure**$(\cdot)$? Again: let's take any pair of fractions $\frac{a}{b}, \frac{c}{d}$. We know, because of how addition is defined on fractions, that $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$. Again, both ac and bd are integers, because a, b, c, d are all integers; furthermore, bd is still not zero because neither b nor d are zero. Therefore, we've shown that the product of any two rational numbers is still rational: i.e. that our field is multiplicatively closed.

- **Commutativity**$(+)$ is relatively simple. All you have to do is notice that for any $\frac{a}{b}, \frac{c}{d}$, we can use the fact that multiplication in the integers is commutative to see that

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} = \frac{da + cb}{db} = \frac{c}{d} + \frac{a}{b}.$$

- **Commutativity**$(\cdot)$ is pretty much the same argument: for any $\frac{a}{b}, \frac{c}{d}$, we again use the fact that multiplication in the integers is commutative to see that

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} = \frac{ca}{db} = \frac{c}{d} \cdot \frac{a}{b}.$$

- **Identity**$(+)$: The fraction $\frac{0}{1}$ is the identity. To see this, take any $\frac{a}{b} \in \mathbb{Q}$, and notice that

$$\frac{0}{1} + \frac{a}{b} = \frac{0 \cdot b + 1 \cdot a}{1 \cdot b} = \frac{a}{b}.$$

  We will often write 0 instead of $\frac{0}{1}$, for convenience's sake.

- **Identity**$(\cdot)$: The fraction $\frac{1}{1}$ is the identity. To see this, take any $\frac{a}{b} \in \mathbb{Q}$, and notice that

$$\frac{1}{1} \cdot \frac{a}{b} = \frac{1 \cdot a}{1 \cdot b} = \frac{a}{b}.$$

  We will often write 1 instead of $\frac{1}{1}$, for convenience's sake.

- **Associativity**$(+)$ is a pain to write down, but not actually any more complicated than the above arguments: all we have to notice is that for any $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbb{Q}$, we have

$$\left(\frac{a}{b}+\frac{c}{d}\right)+\frac{e}{f}=\frac{ad+bc}{bd}+\frac{e}{f}=\frac{(ad+bc)f+(bd)e}{(bd)f}=\frac{adf+bcf+bde}{bdf}, \text{ and}$$
$$\frac{a}{b}+\left(\frac{c}{d}+\frac{e}{f}\right)=\frac{a}{b}+\frac{cf+de}{df}=\frac{a(df)+b(cf+de)}{b(df)}=\frac{adf+bcf+bde}{bdf}.$$

- **Associativity**$(\cdot)$ is similar: for any $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbb{Q}$, we have

$$\left(\frac{a}{b}\cdot\frac{c}{d}\right)\cdot\frac{e}{f}=\frac{ac}{bd}\cdot\frac{e}{f}=\frac{(ac)e}{(bd)f}=\frac{ace}{bdf}, \text{ and}$$
$$\frac{a}{b}\cdot\left(\frac{c}{d}\cdot\frac{e}{f}\right)=\frac{a}{b}\cdot\frac{ce}{df}=\frac{a(ce)}{b(df)}=\frac{ace}{bdf}.$$

- **Inverses**$(+)$ is pretty easy, also. For any $\frac{p}{q} \in \mathbb{Q}$, consider the fraction $\frac{-p}{q}$. Because p is an integer and q is a nonzero integer, this is a well-defined fraction. Furthermore, we can easily see that

$$\frac{p}{q}+\frac{-p}{q}=\frac{pq+(-p)q}{q^2}=\frac{pq-pq}{q^2}=\frac{0}{q^2}=\frac{0\cdot q^2}{q^2}=\frac{0}{1}.$$

  Because $\frac{0}{1}$ is the additive identity, we have just shown that every element has an additive inverse.

- **Inverses**$(\cdot)$ is similarly simple. Take any $\frac{p}{q} \in \mathbb{Q}$ that is not equal to $\frac{0}{1}$. Notice that this means that $p \neq 0$, because if $p = 0$, we would have

$$\frac{0}{q}=\frac{0\cdot q}{q}=\frac{0}{1}.$$

  Now consider the fraction $\frac{q}{p}$. Because p and q are nonzero integers, this is a well-defined fraction. Then, we have

$$\frac{p}{q}\cdot\frac{q}{p}=\frac{pq}{qp}=\frac{pq}{pq}=\frac{1}{1}.$$

  Because $\frac{1}{1}$ is the multiplicative identity, we have just shown that every element has a multiplicative inverse.

- Last one! **Distributivity**$(+,\cdot)$ is proven just like the rest: : all we have to notice is that for any $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbb{Q}$, we have

$$\left(\frac{a}{b}+\frac{c}{d}\right)\cdot\frac{e}{f}=\frac{ad+bc}{bd}\cdot\frac{e}{f}=\frac{(ad+bc)e}{(bd)f}=\frac{ade+bce}{bdf}, \text{ and}$$
$$\left(\frac{a}{b}\cdot\frac{e}{f}\right)+\left(\frac{c}{d}\cdot\frac{e}{f}\right)=\frac{ae}{bf}+\frac{ce}{df}=\frac{(ae)(df)+(bf)(ce)}{(bf)(df)}=\frac{adef+bfce}{bdf^2}=\frac{ade+bce}{bdf}.$$

This should persuade you of three things:

1. $\mathbb{Q}$ is a field!
2. It can be really tedious to check if something is a field.
3. Despite the fact that it's tedious, it's not actually that **hard** to check if something is a field: every single property we tested was pretty trivial to prove, there were just a **lot** of them to check.

So: we've discovered two fields, $\mathbb{R}$ and $\mathbb{Q}$. Are there more?

2 Complex Numbers

A commonly-asked question in mathematics is the following: "Given some polynomial $P(x)$, what are its roots?" Depending on the polynomial, we've seen several techniques for finding these roots (Rolle's theorem, quadratic/cubic formulas, factorization.) However, at times we have encountered polynomials that have no roots at all, like

$$x^2 + 1.$$

Yet, despite the observation that this polynomial's graph never crossed the x-axis, we can still use the quadratic formula to find that this polynomial had the "formal" roots

$$\frac{-0 \pm \sqrt{-4}}{2} = \pm\sqrt{-1}.$$

The number $\sqrt{-1}$, unfortunately, isn't a real number (because $x^2 \geq 0$, for any real x) — so this polynomial has no roots over $\mathbb{R}$. This was a rather frustrating block to run into; often, we like to factor polynomials entirely into their roots, and it would be quite nice if we could always do so, as opposed to having to worry about irreducible functions like $x^2 + 1$.

So: what if we just "add in" $\sqrt{-1}$ into the real numbers? Formally, define the set of **complex numbers**, $\mathbb{C}$, as follows:

Definition. The set of **complex numbers**, denoted $\mathbb{C}$, is the set of all objects of the form $a + bi$, where a, b are real numbers and $i = \sqrt{-1}$. We call the "a"-piece of a complex number the **real part** of the complex number, and the "bi"-piece of a complex number the **imaginary part** of the complex number. Given two complex numbers $a + bi, c + di$, we define their sum as the object

$$(a + bi) + (c + di) = (a + c) + (b + d)i.$$

Because $a+c$, $b+d$ are both real numbers, this result is in the form that we request complex numbers to be in, and therefore is a complex number.

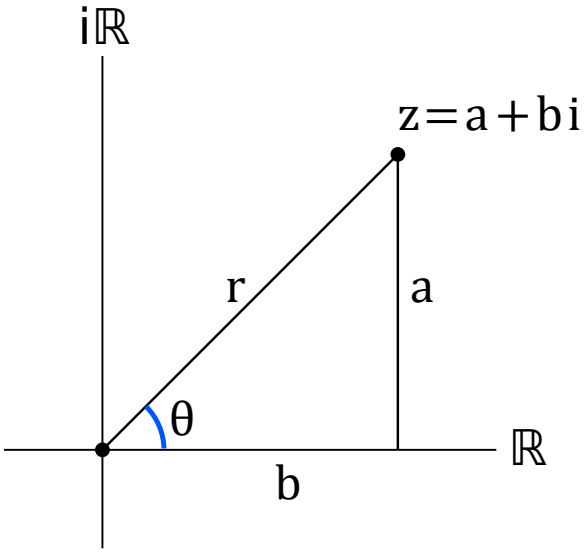
Similarly, given two complex numbers $a+bi, c+di$, we define their product as the object

$$\begin{aligned}(a + bi) \cdot (c + di) &= ac + a(di) + (bi)c + (bi)(di) = ac + (ad + bc)i + (bd)i^2 \\ &= ac + (ad + bc)i + bd(\sqrt{-1})^2 = ac + (ad + bc)i - bd \\ &= (ac - bd) + (ad + bc)i.\end{aligned}$$

Because $ac - bd$ and $ad + bc$ are both real numbers, the result is again in the form that we request complex numbers to be in, and therefore is a complex number.

As a special case, the definition of the product means that $i^2 = -1$; check this with the above formula if you don't believe it!

Graphically, we can visualize the complex numbers as a plane, where we identify one axis with the real line $\mathbb{R}$, the other axis with the imaginary-real line $i\mathbb{R}$, and map the point $a + bi$ to (a, b):



We've mentioned the complex numbers in the middle of a lecture about the concept of **fields**. Lecture theory suggests the following question: Is $\mathbb{C}$ a field?

The answer, as you may have guessed, is yes! We've already shown that a few of the required properties of fields are satisfied: for instance, we've already shown that both addition and multiplication are closed, because when we defined these operations we took special care to note that the output of both operations was a complex number.

Things like associativity, distributivity and commutativity are shown just like how we did for the rational numbers; we reserve a few of these proofs for the homework, and leave the others for the interested reader to pursue on their own. Similarly, you can easily show that the additive identity is $0 + 0i$ and that the multiplicative identity is $1 + 0i$; we again reserve these proofs for the reader to check on their own. It bears noting that like with $\mathbb{Q}$, we will often write 0 instead of $0 + 0i$ and 1 instead of $1 + 0i$, for brevity's sake.

Inverses, however, are weirder. Well: the additive inverse is exactly what we'd expect: given any $a + bi$, the number $(-a) + (-b)i$ is its inverse, because

$$(a + bi) + ((-a) + (-b)i) = (a + (-a) + (b + (-b))i = 0 + 0i = 0.$$

But the multiplicative one is weirder! Suppose we have any $a + bi \neq 0$; what can we multiply it by to get 1?

This is tricky to figure out at first. Accordingly, because we are mathematicians, the first response we have to a problem being tricky is to **try working on a simpler problem.** In

particular, maybe 1 is hard to get. What if we just wanted to multiply $a+bi$ by something to get a **real** number?

This seems more promising. In particular, a trick that you might remember from polynomial multiplication is the observation that

$$(a+bi)(a-bi) = a^2 - abi + abi - b^2i^2 = a^2 - b^2(\sqrt{-1})^2 = a^2 + b^2.$$

This is a real number, as it doesn't have any imaginary part! So we've achieved our easier goal: we can multiply any complex number $a+bi$ by the quantity $a-bi$, and get something that's **real**, even if it's not necessarily 1.

This is useful. (So useful, in fact, that mathematicians have a name for it! Given any complex number $z = a+bi$, we call the complex number $a-bi$ the **conjugate** of z, and write it as $\overline{z}$.) In fact, it's pretty much our answer! We know how to form the inverse of a real number r: as long as the real number r in question is nonzero, then its inverse is just $\frac{1}{r}$.

We know that because $a+bi \neq 0$, one of a or b is nonzero; therefore, we know that a^2+b^2 is nonzero, because one of a^2, b^2 is nonzero and they're both nonnegative (because they're squared real numbers!) Therefore, we know that $\frac{1}{a^2+b^2}$ is the inverse of a^2+b^2, and therefore that

$$\begin{aligned}(a+bi)(a-bi)\cdot\frac{1}{a^2+b^2} &= \left(a^2 - abi + abi - b^2i^2\right)\cdot\frac{1}{a^2+b^2}\\ &= \left(a^2 - b^2(\sqrt{-1})^2\right)\cdot\frac{1}{a^2+b^2}\\ &= \frac{a^2+b^2}{a^2+b^2}\\ &= 1.\end{aligned}$$

Therefore, we have that

$$(a-bi)\cdot\frac{1}{a^2+b^2} = \frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}i$$

is the inverse of $a+bi$, for any i. Because a, b are real numbers such that one of them is nonzero, we know that both $\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}$ are both real numbers; therefore this inverse is a complex number! So we have shown that complex numbers have multiplicative inverses.

3 Other fields?

We have shown that $\mathbb{R}$ and $\mathbb{Q}$ are fields, and (after doing the HW) you should be convinced that $\mathbb{C}$ is a field too. This covers pretty much all of the examples that we're going to use in this class.

However, in our last bit of lecture, I should mention that there are far stranger fields out there that we actively use in modern research[2]! To understand them, consider the following object:

[2]Specifically, the research area of **elliptic curve cryptography**, one of the pieces of technology that you use every day in encrypting your wifi, relies heavily on the fields we study here.

Definition. The set $\mathcal{C}$, of "clock numbers," is defined along with an addition operation $+$ and multiplication operation $\cdot$ as follows:

- Our set is the numbers $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$.
- Our addition operation is the operation "addition mod 12," or "clock arithmetic," defined as follows: we say that $a + b \cong c \mod 12$ if the two integers $a + b$ and c differ by a multiple of 12. Another way of thinking of this is as follows: take a clock, and replace the 12 with a 0. To find out what the quantity $a + b$ is, take your clock, set the hour hand so that it points at a, and then advance the clock b hours; the result is what we call $a + b$.

  For example, $3 + 5 \equiv 8 \mod 12$, and $11 + 3 \equiv 2 \mod 12$. This operation tells us how to add things in our set.
- Similarly, our multiplication operation is the operation "multiplication mod 12," written $a \cdot b \cong c \mod 12$, and holds whenever $a + b$ and c differ by a multiple of 12. Again, given any pair of numbers a, b, to find the result of this "clock multiplication," look at the integer $a \cdot b$, and add or take away copies of 12 until you get a number between 0 and 11.

  For example, $2 \cdot 3 \equiv 6 \mod 12$, $4 \cdot 4 \equiv 4 \mod 12$, and $6 \cdot 4 \equiv 0 \mod 12$.

We often will denote this object as $\langle \mathbb{Z}/12\mathbb{Z}, +, \cdot \rangle$, instead of as $\mathcal{C}$.

This is not a field. To see this, first show that 1 is the multiplicative identity of this field: this is not very hard, and is a good exercise to make sure you understand what's going on. Now, because 1 is the multiplicative identity, we know that if this is a field, any element $x \in \mathbb{Z}/12\mathbb{Z}$ should have a multiplicative inverse x^{-1} that we can multiply x by to get to 1.

However, you can check that no such multiplicative inverse exists for 2. This is not hard to see: take any other element y in $\mathbb{Z}/12\mathbb{Z}$, and multiply 2 by y: you get $2y$, an even integer. Adding or subtracting multiples of 12 to $2y$ will not change this property: because both 12 and $2y$ are even, the result of these operations will always be even.

1, however, is not an even number. Therefore, there is no way for $2y$ to be equal to 1, no matter what y we pick from our set. Therefore, 2 has no multiplicative inverse!

However, some small variations on this object **are** fields:

Definition. The object $\langle \mathbb{Z}/n\mathbb{Z}, +, \cdot \rangle$,i.e.s defined as follows:

- Your set is the numbers $\{0, 1, 2, \ldots n - 1\}$.
- Your addition operation is the operation "addition mod n," defined as follows: we say that $a + b \cong c \mod n$ if the two integers $a + b$ and c differ by a multiple of n.

  For example, suppose that $n = 3$. Then $1 + 1 \equiv 2 \mod 3$, and $2 + 2 \equiv 1 \mod 3$.
- Similarly, our multiplication operation is the operation "multiplication mod n," written $a \cdot b \cong c \mod n$, and holds whenever $a + b$ and c differ by a multiple of n.

  For example, if $n = 7$, then $2 \cdot 3 \equiv 6 \mod 7$, $4 \cdot 4 \equiv 2 \mod 7$, and $6 \cdot 4 \equiv 3 \mod 7$.

There are many values of n for which this is always a field! You will study some of these values on the homework. We run one sample calculation here:

Claim 1. *$\langle \mathbb{Z}/5\mathbb{Z}, +, \cdot \rangle$ is a field.*

Proof. So: we're working with the set $\{0, 1, 2, 3, 4\}$, with the operations $+$ and $\cdot$ taken mod 5.

We first note that the operations $+, \cdot$ are closed. This is because given any pair of numbers in $\{0, 1, 2, 3, 4\}$, their sum and product are positive integers. If we take away copies of 5 one-by-one from any positive integer, we must eventually land in the set $\{0, 1, 2, 3, 4\}$, as it is impossible to subtract 5 from a positive integer that is not in this set (i.e. an integer greater than or equal to 5) and get a negative integer. (If you don't see why, draw a number line and try "subtract copies of five one by one" algorithm with some sample numbers!)

We also note that the commutativity, associativty and distribuitivity axioms all hold. To see this, notice that before taking the mod operation, our $+$ and $\cdot$ operations are precisely the same as those for $\mathbb{R}$; therefore, before applying mods, these two operations preserve these properties.

So: all of these properties are equality statements (i.e. $(a + b) + c = a + (b + c)$). These statements all hold before we apply the mod operation, because they hold in $\mathbb{R}$. Therefore, when we apply the mod operation to both sides, we're applying it to the same thing on both sides! Because we're starting from the same number on both sides when we perform our "add or take away copies of 5" algorithm, we can't possibly get these two sides to go to different numbers in $\{0, 1, 2, 3, 4\}$: we're starting from the same place and performing the same algorithm that always has a unique output! (If you don't see why our mod algorithm of "add or take away multiples of 5 until you are in the set $\{0, 1, 2, 3, 4\}$ always has the same output from any set input, prove this to yourself.) Therefore, we preserve these axioms.

To see the identity and inverse properties for $+$ and $\cdot$, consider the following addition and multiplication tables:

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Notice how in the 0-row of the addition table, adding 0 to any element doesn't change that element. Therefore 0 is an additive identity! Similarly, notice that there is a 0 in every row and column in the addition table: this means that given any element in $\mathbb{Z}/5\mathbb{Z}$, there is some other element we can add to it to get to 0. Therefore, we have additive inverses.

As well, notice how in the 1-row of the multiplication table, multiplying 1 by any element doesn't change that element. Therefore, 1 is a multiplicative identity. Similarly, notice that there is a 1 in every row and column of the multiplication table not corresponding to a 0: this means that given any element in $\mathbb{Z}/5\mathbb{Z}$, there is some other element we can multiply by it to get to 1. Therefore, we have multiplicative inverses. □

So this is a field! A field with **finitely many elements,** which is weird.