Fields and Vector Spaces

Aryaman Maithani

Semester: Spring 2020
Latest update: January 15, 2020

§1 Fields

1.1 Axioms

Let $\mathbb{F}$ be a set and let $+, \cdot$ be binary operations on $\mathbb{F}$.
That is, $+, \cdot : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$ are functions from $\mathbb{F} \times \mathbb{F}$ to $\mathbb{F}$.
For the sake of better notation, we will write $a + b$ instead of $+(a, b)$ for $a, b \in \mathbb{F}$. Similarly, we will write $a \cdot b$ instead of $\cdot(a, b)$. In fact, later on, we will even drop the $\cdot$ and simply write ab instead of $a \cdot b$.

Now, we say that $(\mathbb{F}, +, \cdot)$ is a *field* if the following axioms (properties) hold:

(A1) $a + b = b + a$ for all $a, b \in \mathbb{F}$.

(A2) $a + (b + c) = (a + b) + c$ for all $a, b \in \mathbb{F}$.

(A3) $\exists 0 \in \mathbb{F}$ such that $a + 0 = a = 0 + a$ for all $a \in \mathbb{F}$.

(A4) For every $a \in \mathbb{F}$, there exists $b \in \mathbb{F}$ such that $a + b = 0 = b + a$.

(A5) $a \cdot b = b \cdot a$ for all $a, b \in \mathbb{F}$.

(A6) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in \mathbb{F}$.

(A7) $\exists 1 \in \mathbb{F}$ such that $a \cdot 1 = a = 1 \cdot a$ for all $a \in \mathbb{F}$.

(A8) For every $a \in \mathbb{F} \setminus \{0\}$, there exists $b \in \mathbb{F}$ such that $a \cdot b = 1 = b \cdot a$.

(A9) $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$ for all $a, b, c \in \mathbb{F}$.

(A10) $1 \neq 0$.

Notation abuse: If it is clear from context, one often writes $\mathbb{F}$ is a field instead of $(\mathbb{F}, +, \cdot)$.

1.2 Remarks

I have given the definition of a *commutative* field. Some books don't require commutativity of multiplication (A5) to be a part of the axioms. However, we shall not go with that definition.

As you may have observed, some of the statements contain redundant information. For example, I could've simply written $a + 0 = a$ instead of $a + 0 = a = 0 + a$, for the last part would've followed from (A1). You are right in believing so. Perhaps someday you will realise why I had specifically written it in this case (even though it would've been perfectly correct without).
Before getting into more explanation, one can observe that $(\mathbb{R}, +, \cdot)$ is a field. (Assuming that $+$ and $\cdot$ are defined in the *usual* sense.)
In fact, I might even stretch the truth enough to describe a field to be something which "behaves" like $\mathbb{R}$. Indeed, for the sake of intuition, this is a nice starting point.

Now, if you see the axioms, it really is telling that $(\mathbb{F}, +, \cdot)$ should have some sort of properties that we have seen $\mathbb{R}$ having. To name them, addition and multiplication should be additive as well as commutative. On top of that, both the operations must have their "identities", that is, an element that "does nothing" to the other element when operated together. After that, we also demand "inverses". Note that here too, we only demand *multiplicative* inverses of non-zero elements to exist, just like what we saw in $\mathbb{R}$. To finally connect $\cdot$ and $+$, we demand that $\cdot$ *distributed* over $+$.

Note that without this axiom, the two operations were more or less disconnected. (But not exactly. We demanded every $a \neq 0$ to have a multiplicative inverse, where 0 was the *additive* identity.)

The last axiom, as silly as it may seem, is there simply to avoid the pathological example of a one-element field. (What do I mean by this?)

Lastly, note that I did *not* demand that the identities or inverses must be unique, to begin with. That is, just from (A3) alone, I cannot conclude that if $a + 0 = a = 0' + a$ for every $a \in \mathbb{F}$, then $0 = 0'$. However, in the case of $\mathbb{R}$, we do know that that is true.
In fact, nicely enough, it *is* true in general and can be proven using just (A2) and (A3). (Check!)
Similarly, it can shown that the b described in (A4) is indeed unique using just (A2) - (A4). (Check!)
Analogous results also hold for (A7) and (A8).

Thus, keeping in mind the above results, we introduce the following notations:
For any $a \in \mathbb{F}$, $-a$ denotes *the* additive inverse of a, that is, the unique element such that $a + (-a) = 0$.
For any $a \in \mathbb{F} \setminus \{0\}$, a^{-1} denotes *the* multiplicative inverse of a, that is, the unique element such that $a \cdot a^{-1} = 1$.

1.3 Examples

Let us now look at some examples, old and new.
As noted earlier, $(\mathbb{R}, +, \cdot)$ is a field with the usual $+$ and $\cdot$.
In fact, so is $(\mathbb{Q}, +, \cdot)$.
On the other hand, not everything we know is a field. For example, $(\mathbb{N}, +, \cdot)$ is not and neither is $(\mathbb{Z}, +, \cdot)$. (Why?)
It doesn't make much sense to talk about $(\mathbb{R} \setminus \mathbb{Q}, +, \cdot)$ being a field since $+$ and $\cdot$ aren't even binary operations on $\mathbb{R} \setminus \mathbb{Q}$. (The sum of two irrationals need not be irrational and same for multiplication.)
One more example of a field you must've seen already is $(\mathbb{C}, +, \cdot)$.
Note that if you define multiplication on $\mathbb{R}^2$ as $(a, b) \cdot (c, d) = (ab, cd)$, it does *not* form a field under the usual addition. One can observe that $(0, 1)$ is a non-zero element (which, in this case, is $(0, 0)$) but it does not have a multiplicative inverse.
Does the set all of 2×2 matrices with real entries form a field, under the usual addition and multiplication?

We also have some examples of finite fields. For $n \in \mathbb{N} \setminus \{1\}$, let us define $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ and define addition and multiplication *modulo* n.
For example, if $n = 3$, then $2 + 2 = 1 \in \mathbb{Z}_3$ and $2 \times 2 = 1 \in \mathbb{Z}_3$.
Now, a natural question to ask is whether $(\mathbb{Z}_n, +, \cdot)$ always a field?
The answer is *no*. That is, it is not *always* a field.
For example, $\mathbb{Z}_4$ is not a field. One can verify that $2 \in \mathbb{Z}_4$ has no multiplicative inverse.
On the other hand, $\mathbb{Z}_3$ indeed is a field. This can be verified by making the multiplication and addition table and manually checking all the (finitely many) combinations.
In fact, it is easy to show that all axioms except (A8) always hold for any n. Thus, it is only the existence of multiplicative inverses that one needs to check. ((A10) holds as $n > 1$.)

The next natural question is the following - For *what* values of n is $\mathbb{Z}_n$ a field?
Before continuing, the reader is encouraged to answer this themselves.
This question has a nice answer - $\mathbb{Z}_n$ is a field if and only if n is a prime.
To prove both the directions, you would have to show the following:

1. If n is not a prime, then there exists some non-zero element $a \in \mathbb{Z}_n$ such that a has no multiplicative inverse.
2. If n is a prime, then every non-zero element $a \in \mathbb{Z}_n$ has a multiplicative inverse.

The above is not too tough and I encourage the reader to prove this.

The next question that one could ask is - Do all finite fields have a prime cardinality? The answer is - no.
As an example, consider the four element set $\{0, 1, x, x + 1\}$. Consider the addition and multiplications of elements as addition and multiplication of polynomials with the following rules: x^2 is replaced with $x + 1$. 2 is replaced with 0.
To illustrate the nontrivial addition and multiplications, we have:
$x + (x + 1) = 1,\ x(x + 1) = 1,\ 1 + (x + 1) = x.$
The sum (resp. product) of 0 (resp. 1) and any element gives the same element. The product of 0 with any element gives 0.
It can be verified that this too is a field.

As before, the next natural question would be - Precisely what cardinalities can a finite field have?
We certainly know that it can be a prime number. The answer is - once again - quite nice.

Theorem 1. *If $\mathbb{F}$ is a finite field, then $|\mathbb{F}| = p^n$ for some prime p and $n \in \mathbb{N}$.*

Proof. The proof is trivial and is left as an exercise to the reader. □

Actually, the proof *isn't* trivial and requires some more algebraic knowledge and we shall not get into it.

1.4 Exercises

These are some (fun!) exercises that you can try. These will illustrate that some familiar properties of $\mathbb{R}$ do hold in general as well.
For the following questions, assume that $(\mathbb{F}, +, \cdot)$ be a field. Show that the following holds:

1. For all $a, b, c \in \mathbb{F}$, $a + b = a + c$ implies $b = c$.
2. For all $a, b, c \in \mathbb{F}$ and $a \neq 0$, $a \cdot b = a \cdot c$ implies $b = c$.
3. For all $a \in \mathbb{F}$, $a \cdot 0 = 0$.
4. If for any $a, b \in \mathbb{F}, a \cdot b = 0$ then $a = 0$ or $b = 0$. (Note that this would fail for $\mathbb{Z}_n$ if n is not a prime.)
5. For all $a \in \mathbb{F}, -a = (-1) \cdot a$.
6. For all $a, b \in \mathbb{F} \setminus \{0\}$, $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$.

Note that we observed earlier that $\mathbb{Z}_n$ is not a field if n isn't a prime. This was due to the fact that some nonzero elements may not have a multiplicative inverse. Towards this direction, characterise all elements of $\mathbb{Z}_n$ which do have a multiplicative inverse.

§2 Vector spaces

2.1 Axioms

As before, we start with the definition of what a vector space is.
Let V be a set and $\mathbb{F}$ a field. Let $+ : V \times V \to V$ be a binary operation on V and $\cdot : \mathbb{F} \times V \to V$ be a function. Note that this is ***not*** a binary operation on either V or $\mathbb{F}$.
We say that $(V, +, \cdot)$ is a *vector space over* $\mathbb{F}$ if the following axioms (properties) hold.

(A1) For all $u, v \in V : u + v = v + u$.

(A2) For all $u, v, w \in V : u + (v + w) = (u + v) + w$.

(A3) There exists $0 \in V$ such that for all $v \in V : v + 0 = v = 0 + v$.

(A4) For every $v \in V$, there exists $w \in V$ such that $v + w = 0 = w + v$.

(A5) For all $a \in \mathbb{F}$ and all $u, v \in V : a \cdot (u + v) = a \cdot u + a \cdot v$.

(A6) For all $a, b \in \mathbb{F}$ and all $v \in V : (a + b) \cdot v = a \cdot v + b \cdot v$.

(A7) For all $a, b \in \mathbb{F}$ and all $v \in V : (ab) \cdot v = a \cdot (b \cdot v)$.

(A8) For all $v \in V : 1 \cdot v = v$.

Note that as before, I have used $u + v$ to denote $+(u, v)$ for elements $u, v \in V$.
Also note that I have used the symbol $+$ to denote both the vector space addition as well as the field addition. This is abuse of notation but it is clear from context as to what is meant.
As before, we usually say that V is a vector space over $\mathbb{F}$ when it is clear what the operations are.

Also, the elements of the vector space are called *vectors*, whereas the elements of the field are called *scalars*.
In this course (MA 106), the scalars you will see will either be real numbers or complex numbers.
The function $+$ (defined on $V \times V$) is also called the vector addition and $\cdot$ (defined on $\mathbb{F} \times V$) is called the scalar multiplication.

2.2 Examples

Let us first consider the field to be $\mathbb{F} = \mathbb{R}$.
The most familiar examples of vector spaces are $\mathbb{R}^2$, $\mathbb{R}^3$, et cetera.
You can verify that all the eight axioms do indeed hold with the vector addition and scalar multiplication defined in the usual sense.

In fact given any field $\mathbb{F}$, there is a natural way to make $\mathbb{F}^n$ a vector space using the same idea. (How?)
What may be more surprising is that $\mathbb{R}$ is in fact a vector space over $\mathbb{R}$ itself!
In fact, in general, any field can be regarded as a vector space over itself by just considering the vector addition to be the same as field addition and the same for scalar multiplication.

Here is something perhaps even more interesting - recall that $\mathbb{Q}$ is a field that sits inside $\mathbb{R}$.
We can also regard $\mathbb{R}$ as a vector space over $\mathbb{Q}$. Define the vector addition to just be the standard addition of real numbers and scalar multiplication to be the standard multiplication. Note that you only need to define the product of a rational number and a real number. The fact that you can multiply any two real numbers isn't even required.
How would you generalise this? (Note that in this case, we didn't just use the fact that $\mathbb{Q} \subset \mathbb{R}$ but also that the addition and multiplication of $\mathbb{Q}$ as a field "agree" with that of $\mathbb{R}$. You may want to look up the definition of a "subfield" to understand this better.)

2.3 Exercises

1. Show that the identity element 0 of a vector space is unique.
2. Show that the additive inverse of every element in a vector space is unique.
3. Let V be a vector space over $\mathbb{F}$.
   Show that $0 \cdot v = \mathbf{0}$ for every $v \in V$.
   (It should be clear that $0 \in \mathbb{F}$ and $\mathbf{0} \in V$.)
4. Let V be a vector space over $\mathbb{F}$.
   Let $\alpha \in \mathbb{F}$ and $v \in V \setminus \{\mathbf{0}\}$.
   Show that if $\alpha \cdot v = \mathbf{0}$, then $\alpha = 0$.
5. Let V be a vector space over $\mathbb{F}$.
   Let $\alpha \in \mathbb{F} \setminus \{0\}$ and $v \in V$.
   Show that if $\alpha \cdot v = \mathbf{0}$, then $v = \mathbf{0}$.