Math 24
Spring 2012
Monday, March 26

We are going to use Appendix C from the textbook, "Fields," to take a look at the process of reading mathematics. Mostly this is practice. You will, however, need to know a few things about fields.

Every vector space is associated with a field. The vector spaces you studied in calculus are associated with the field of real numbers.

Because we are studying the abstract theory of vector spaces, for us, a vector space can be associated with any field. When we work with specific examples, our fields will usually be either the real numbers $\mathbb{R}$ or the complex numbers $\mathbb{C}$, although sometimes we will consider other fields.

We will use the following facts about fields in the rest of the course:

1. There are many different fields.

2. Examples of fields include the real numbers $\mathbb{R}$, the rational numbers $\mathbb{Q}$, the complex numbers $\mathbb{C}$, many other sets of complex numbers (such as the set given in Example 3 of Appendix A), and the field $\mathbb{Z}_2$ given in Example 4 of Appendix A.

3. There are some strange fields, like $\mathbb{Z}_2$, in which you can add 1 to itself finitely many times and get 0. (In $\mathbb{Z}_2$, we have $1 + 1 = 0$.) Fields like $\mathbb{R}$, $\mathbb{Q}$, and $\mathbb{C}$ in which you cannot add 1 to itself finitely many times and get 0 are said to have *characteristic zero*. Fields in which $1 + 1 = 0$ are said to have *characteristic* 2.

In the following pages, we'll see an excerpt from the text, followed by some questions. These are examples of the kinds of questions you should be asking yourself as you read a mathematics text. You may have heard that you should always read a math book with paper and pencil at hand; you may need them to answer some of these questions.

Appendix C
Fields

From your textbook: Friedberg, Insel, and Spence, *Linear Algebra*, fourth edition

The set of real numbers is an example of an algebraic structure called a *field*. Basically, a field is a set in which four operations (called addition, multiplication, subtraction, and division) can be defined so that, with the exception of division by zero, the sum, product, difference, and quotient of any two elements in the set is an element of the set. More precisely, a field is defined as follows.

****

Are there any words or phrases you don't know the meanings of?
Is there anything you don't understand?
What is an algebraic structure? Can you tell from this paragraph?
What can you conclude from this paragraph? In particular, what is coming next?

If you don't know what an algebraic structure is, you can at least tell from this paragraph that a field is an example of an algebraic structure.

You can conclude from this paragraph that the author is about to give a formal definition of the word *field*. (In mathematical writing, it is common, when giving a definition, to italicize the word or phrase being defined.)

You can conclude that a field will consist of a collection of things you can add, subtract, multiply, and divide.

You can also conclude that the real numbers are an example of a field. You should keep this example in mind as you read the formal definition that is to follow.

From your textbook:

Definitions: A field F is a set on which two operations $+$ and $\cdot$ (called **addition** and **multiplication** respectively) are defined so that, for each pair of elements x, y in F, there are unique elements $x + y$ and $x \cdot y$ in F for which the following conditions hold for all elements a, b, c in F.

****

Are there any words or phrases you don't know the meaning of?
Is there anything you don't understand?
What does the word "unique" mean in this sentence?
Does this definition, so far, apply to the real numbers?
What can you conclude from this sentence?

The word "unique" here means "one and only one." That is, for each pair x, y in F, there is one and only one element $x + y$ that is the result of adding x and y.

In addition to the obvious (that a field consists of a set F with two operations $+$ and $\cdot$ as described), you can conclude that the definition is going to continue by giving conditions that must hold. There might be a set with operations $+$ and $\cdot$ that did not satisfy these conditions, but it would not be a field.

As you read the conditions, you should continue to check that they do hold for the real numbers.

From your textbook:

(F1) $a + b = b + a$ and $a \cdot b = b \cdot a$

(commutativity of addition and multiplication)

(F2) $(a + b) + c = a + (b + c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

(associativity of addition and multiplication)

(F3) There exist distinct elements 0 and 1 in F such that

$$0 + a = a \text{ and } 1 \cdot a = a$$

(existence of identity elements for addition and multiplication)

(F4) For each element a in F and each nonzero element b in F there exist elements c and d in F such that

$$a + c = 0 \text{ and } b \cdot d = 1$$

(existence of inverses for addition and multiplication)

(F5) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

(distributivity of multiplication over addition)

****

Is there anything here you do not understand?
What is the meaning of "distinct" here?
Does this definition apply to the real numbers?
What's with the phrases in parentheses?

"Distinct elements 0 and 1" means that 0 and 1 are distinct from each other; that is, $0 \neq 1$.

The phrases in parentheses are the names of the properties expressed in (F1)-(F5), which are useful to know when you are talking about fields. For example, suppose you are writing a proof, and you need to use the fact that $(a + b) + c = a + (b + c)$. You can say "by (F2)" if you know your reader is familiar with the presentation of the definition of field given in this book (and remembers which condition is (F2)). However, if you say "by the associativity of addition," you will be generally understood.

From your textbook:

The elements $x + y$ and $x \cdot y$ are called the **sum** and **product**, respectively, of x and y. The elements 0 (read **"zero"**) and 1 (read **"one"**) mentioned in (F3) are called **identity elements** for addition and multiplication, respectively, and the elements c and d referred to in (F4) are called an **additive inverse** for a and a **multiplicative inverse** for b, respectively.

****

Is there anything you don't understand here?
Is this paragraph part of the definition of field?

This is not part of the definition of field. It is a definition of the words and phrases printed in boldface. This vocabulary is useful for talking about fields.

Now you have seen the definition of a field, and you know one example of a field. Can you think of any other examples?

Can you think of examples of something that is like a field in some ways, but fails to have some of the properties of a field?

The more examples you have, and the more different kinds, the better. Also the more counterexamples (non-fields), and the more different kinds, the better. You should *always* think about examples and counterexamples when you encounter a mathematical definition.

The textbook is actually about to provide some examples.

From your textbook:

Example 1: The set of real numbers $\mathbb{R}$ with the usual definitions of addition and multiplication is a field.

Example 2: The set of rational numbers with the usual definitions of addition and multiplication is a field.

****

Convince yourself that these are actually examples of fields.

If you've been reading attentively, you have already checked the first example.

From your textbook:

Example 3: The set of all real numbers of the form $a + b\sqrt{2}$, where a and b are rational numbers, with addition and multiplication as in $\mathbb{R}$ is a field.

****

Is this an example of a field?

In particular, does every nonzero element in this set have a multiplicative inverse *in this set*?

To check for multiplicative inverses, you need to check that for every element $a + b\sqrt{2}$ where a and b are rational numbers (and not both zero), there is an element $c + d\sqrt{2}$ where c and d are rational numbers, such that $(a + b\sqrt{2})(c + d\sqrt{2}) = 1$.

Alternatively, you need to show that if a and b are rational numbers (and not both zero), you can write the multiplicative inverse $\dfrac{1}{a + b\sqrt{2}}$ in the form $c + d\sqrt{2}$, for some rational numbers c and d.

A hint: Remember "rationalizing the denominator"?

From your textbook:

Example 4: The field $\mathbb{Z}_2$ consists of the two elements 0 and 1 with the operations of addition and multiplication defined by the equations

$$0+0=0,\ \ 0+1=1+0=1,\ \ 1+1=0,$$

$$0\cdot 0=0,\ \ 0\cdot 1=1\cdot 0=0,\ \ \text{and}\ \ 1\cdot 1=1.$$

****

Is this an example of a field?

If you think of 0 as "even" and 1 as "odd" this might make more intuitive sense. You may have learned principles like "even times odd is even" in elementary school; here this takes the form $0 \cdot 1 = 0$.

If you know about "arithmetic mod n," you can see that this is just addition and multiplication mod 2.

From your textbook:

Example 5: Neither the set of positive integers nor the set of integers with the usual definitions of addition and multiplication is a field, for in either case (F4) does not hold.

****

Can you show that these are not fields?

Give a specfic counterexample; that is, an element of the set that does not have an additive inverse in the set, or a nonzero element of the set that does not have a multiplicative inverse in the set.

From your textbook:

The identity and inverse elements guaranteed by (F3) and (F4) are unique; this is a consequence of the following theorem:

****

What does "unique" mean here?
Can you think of relevant examples of non-uniqueness?
What is a theorem?
What can you conclude from this sentence?

Once again, "unique" means "one and only." Additive inverses are unique means that if $a + b = 0$ and $a + c = 0$ then $b = c$, and similarly for multiplicative inverses.

A theorem is a mathematical fact that is proven using relevant mathematical definitions, and perhaps previously proven facts. There are other names for such facts, such as lemmas, propositions, corollaries. Generally, proposition and theorem mean the same thing (although some writers reserve the word theorem for particularly important results, a lemma is something you prove just because you want to use it to prove a theorem, and a corollary to a theorem is something you prove using that theorem.

Among other things, you can conclude that the author is about to prove a theorem, and that from that theorem you can prove the uniqueness of additive and multiplicative inverses.

From your textbook:

Theorem C.1 (Cancellation Laws). For arbitrary elements a, b, and c in a field, the following statements are true.

(a) If $a + b = c + b$, then $a = c$.

(b) If $a \cdot b = c \cdot b$ and $b \neq 0$, then $a = c$.

****

Anything you don't understand?
What does arbitrary mean here?
Does this fit in with what you know about the fields you are familiar with?
Why are these called cancellation laws?

Arbitrary elements means any elements whatsoever.

These are called cancellation laws because they allow you to "cancel out" a term that occurs on both sides of an equation, going (for example) from $a + b = c + b$ to $a = c$ by "cancelling out" the term $+b$. Sometimes this is phrased as "the $+b$'s cancel each other out."

From your textbook:

Proof. (a) The proof of (a) is left as an exercise.

(b) If $b \neq 0$, then (F4) guarantees the existence of an element d in the field such that $b \cdot d = 1$. Multiply both sides of the equation $a \cdot b = c \cdot b$ by d to obtain $(a \cdot b) \cdot d = (c \cdot b) \cdot d$. Consider the left side of this equality: by (F2) and (F3), we have

$$(a \cdot b) \cdot d = a \cdot (b \cdot d) = a \cdot 1 = a.$$

Similarly, the right side of the equality reduces to c. Thus $a = c$.

****

Anything you don't understand?

Could you write out a proof of part (a)? (You don't need to actually write it out — unless that's the only way to convince yourself that you could.)

The form of a proof is not set in stone. Here are other examples:

****

Theorem C.1 (Cancellation Laws). For arbitrary elements a, b, and c in a field, the following statements are true.

(a) If $a + b = c + b$, then $a = c$.

(b) If $a \cdot b = c \cdot b$ and $b \neq 0$, then $a = c$.

Proof A of part (b):

Since $b \neq 0$, b has a multiplicative inverse, d, such that $b \cdot d = 1$. Beginning with the original equation $a \cdot b = c \cdot b$, we can multiply both sides by d, then apply the associativity of multiplication and the definitions of multiplicative inverse and multiplicative identity to show $a = c$, as follows.

$$\begin{aligned} a \cdot b &= c \cdot b \\ (a \cdot b) \cdot d &= (c \cdot b) \cdot d \\ a \cdot (b \cdot d) &= c \cdot (b \cdot d) \\ a \cdot 1 &= c \cdot 1 \\ a &= c. \end{aligned}$$

****

Theorem C.1 (Cancellation Laws). For arbitrary elements a, b, and c in a field, the following statements are true.

(a) If $a + b = c + b$, then $a = c$.

(b) If $a \cdot b = c \cdot b$ and $b \neq 0$, then $a = c$.

Proof B of part (b):

By (F4), let d be a multiplicative inverse of b. The following sequence of equations demonstrates that if $a \cdot b = c \cdot b$ then $a = c$.

$$\begin{aligned} a \cdot b &= c \cdot b && \text{(given)} \\ (a \cdot b) \cdot d &= (c \cdot b) \cdot d && \text{(multiply both sides by } d\text{)} \\ a \cdot (b \cdot d) &= c \cdot (b \cdot d) && \text{(F2, associativity)} \\ a \cdot 1 &= c \cdot 1 && \text{(F4, multiplicative inverse)} \\ a &= c && \text{(F3, multiplicative identity).} \end{aligned}$$

****

Theorem C.1 (Cancellation Laws). For arbitrary elements a, b, and c in a field, the following statements are true.

(a) If $a + b = c + b$, then $a = c$.

(b) If $a \cdot b = c \cdot b$ and $b \neq 0$, then $a = c$.

Proof of part (b):
Let d be a multiplicative inverse of b. We are given

$$a \cdot b = c \cdot b$$

and we want to show $a = c$. Multiplying both sides of the original equation by d gives

$$(a \cdot b) \cdot d = (c \cdot b) \cdot d.$$

Because multiplication is associative, we get

$$a \cdot (b \cdot d) = c \cdot (b \cdot d).$$

Because d is a multiplicative inverse of b, we get

$$a \cdot 1 = c \cdot 1.$$

Finally, because 1 is a multiplicative identity, we get

$$a = c.$$

****

Two things ARE set in stone.

1. You must state the result before proving it, or restate the problem before solving it.
2. A proof is written in English. A sequence of equations (even with justifications included, as in Proof B above) may be part of a proof, but it is not a proof.

Corollary. The elements 0 and 1 mentioned in (F3) , and the elements c and d mentioned in (F4), are unique.

****

We know now what "unique" means. How would you go about proving the additive identity element 0 is unique? What might you try?

Here is a standard method for proving something is unique: We need to prove that 0 is the only additive identity element. We can do this by assuming there is another one, giving it a name (say $0'$), and then proving that in fact $0' = 0$ after all.

You would then start with what you know, that is, for every $a \in F$ you have $0 + a = a$ and, because you're assuming $0'$ is an additive identity, for every $a \in F$ you have $0' + a = a$.

Since this is supposed to be a corollary to Theorem C1, you could now try to see whether you can use a cancellation law to get to your desired conclusion, namely, $0' = 0$.

Proof. Suppose that $0' \in F$ satisfies $0' + a = a$ for each $a \in F$. Since $0 + a = a$ for each $a \in F$, we have $0' + a = 0 + a$ for each $a \in F$. Thus $0' = 0$ by Theorem $C1$.

The proofs of the remaining parts are similar.

****

Questions?

Here is a slightly different proof that the additive identify of a field is unique. To find this proof I started with the usual method of proving something is unique, assuming there are two additive identities 0 and $0'$, and trying to show they are equal. Then I considered what I knew from the definition of additive identity, namely, for any element a we have $a + 0 = a$ and $a + 0' = a$. Then I could have looked for a way to use the Cancellation Theorem. Instead, I considered that since these equations hold for any a, I could plug anything I wanted in for a, and thought about what it might be useful to plug in.

Proposition: The additive identity element 0 of a field is unique.

Proof: By (F3) there is an additive identity element called 0. Suppose $0'$ is another additive identity element. We must show that $0' = 0$.

Because 0 and $0'$ are additive identity elements, for any element a we have

1. $0 + a = a$, and
2. $0' + a = a$.

Setting $a = 0'$ in (1) and $a = 0$ in (2), we get

1. $0 + 0' = 0'$, and
2. $0' + 0 = 0$.

Because addition is commutative, $0 + 0' = 0' + 0$, and therefore $0' = 0$.

Exercise: Show that if V is a vector space over the field F, and $a\vec{x} = \vec{0}$ (where $a \in F$ and $\vec{x} \in V$), then either $a = 0$ or $\vec{x} = \vec{0}$. (Hint available to anyone who asks.)

****

Here is an example of a possible proof.

Proposition: If $\vec{x}$ is a vector and a is a scalar such that $a\vec{x} = \vec{0}$, then either $a = 0$ or $\vec{x} = \vec{0}$.

Proof: Suppose that $a \neq 0$. Then we must prove that $\vec{x} = \vec{0}$.

Because $a \neq 0$, we know a has a multiplicative inverse, a^{-1}. Then we can multiply both sides of $a\vec{x} = \vec{0}$ by a^{-1} to show $\vec{x} = \vec{0}$, as the following sequence of equations shows.

$$\begin{aligned}
a\vec{x} &= \vec{0} && \text{(given)} \\
a^{-1}(a\vec{x}) &= a^{-1}\vec{0} && \text{(multiply both sides by } a^{-1}\text{)} \\
a^{-1}(a\vec{x}) &= \vec{0} && \text{(Theorem 1.2(c))} \\
(a^{-1}a)\vec{x} &= \vec{0} && \text{(VS 6)} \\
1\vec{x} &= \vec{0} && \text{(definition of multiplicative inverse)} \\
\vec{x} &= \vec{0} && \text{(VS 5)}
\end{aligned}$$

Note: Another possible approach here is to use $a\vec{0} = \vec{0}$ (from Theorem 1.2) to rewrite the original equation as $a\vec{x} = a\vec{0}$. Then it is tempting to "cancel out" the a on each side to get $\vec{x} = \vec{0}$. However, we have not proved a cancellation law of this form. You could easily prove a cancellation law for scalar multiplication:

For any vectors $\vec{x}$ and $\vec{y}$ and any nonzero scalar a, if $a\vec{x} = a\vec{y}$ then $\vec{x} = \vec{y}$.

Or, you could just multiply both sides of $a\vec{x} = a\vec{0}$ by a^{-1}.

The nice thing about proving a cancellation law is that you can then use it again and again.

Exercise: Show, as a corollary, that if $a\vec{x} = b\vec{x}$, and $\vec{x} \neq \vec{0}$, then $a = b$. (This question came up in class, when we decided that "In any vector space, $a\vec{x} = b\vec{x}$ implies that $a = b$" is false because $\vec{x}$ could be $\vec{0}$. Then we asked whether this was the only way it could be false.)

****

Here is an example of a possible proof.

Proposition: If a and b are any scalars and $\vec{x}$ is any nonzero vector such that $a\vec{x} = b\vec{x}$, then $a = b$.

Proof: Let $-b$ be the additive inverse of b. Add $(-b)\vec{x}$ to both sides of the equation $a\vec{x} = b\vec{x}$ to get

$$a\vec{x} + (-b)\vec{x} = b\vec{x} + (-b)\vec{x}.$$

Now we will use Theorem 1.2(b), which says that $(-b)\vec{x} = -(b\vec{x})$, to rewrite our equation as

$$a\vec{x} + (-b)\vec{x} = b\vec{x} + (-(b\vec{x})).$$

Since $-(b\vec{x})$ is the additive inverse of $b\vec{x}$, this gives us

$$a\vec{x} + (-b)\vec{x} = \vec{0}.$$

We can use (VS 8), a distributivity property, to rewrite this as

$$(a + (-b))\vec{x} = \vec{0}.$$

Now, since $\vec{x} \neq \vec{0}$, our previous proposition tells us that $(a + (-b)) = 0$. By the definition of $-b$ we know that $(b + (-b)) = 0$. By the cancellation law for addition (Theorem C.1), applied to $(a + (-b)) = 0$ and $(b + (-b)) = 0$, we see that $a = b$.