Math 4310 Handout - Fields

Dan Collins

In this course the main object of study will be *vector spaces*. Concretely,vector spaces are modeled after n-dimensional real space, where we think of a vector as being an "arrow" connecting the origin to a point in space. There are two fundamental algebraic operations we know how to do with vectors: we can add two of them together, and we can multiply a vector by a scalar.

In earlier classes (and in the course's textbook), you mostly see vector spaces over the real numbers, i.e. where we can multiply a vector by a scalar in $\mathbb{R}$. If you're just thinking of things in terms of $\mathbb{R}^n$ then there's no problems, but if you start thinking about complex numbers then it might get a bit confusing. What's the dimension of $\mathbb{C}$, for instance - is it 1-dimensional because you just have one coordinate, or is it 2-dimensional because it's represented by a plane? Relatedly, are the complex numbers 1 and i linearly independent or linearly dependent? The answer depends on whether you only consider scalar multiplication by real numbers, or allow scalar multiplication by complex numbers too. Any time you're doing linear algebra, your choice of scalars are implicit. $\mathbb{R}$ and $\mathbb{C}$ aren't the only choices of scalars, either; we can do linear algebra with scalars in any structure called a *field*.

Definition 1. A *field* is a set F together with binary operations of addition and multiplication which satisfy the following list of axioms:

1. (Associativity of addition): For any $a, b, c \in F$ we have $(a + b) + c = a + (b + c)$.
2. (Commutativity of addition): For any $a, b \in F$ we have $a + b = b + a$.
3. (Additive identity): There exists an element $0 \in F$ such that for every $a \in F$, we have $a + 0 = a$.
4. (Additive inverses): For each $a \in F$ there exists an element $-a \in F$ such that $a + (-a) = 0$.
5. (Distributivity of multiplication over addition): For any $a, b, c \in F$ we have $(a + b)c = ac + bc$.
6. (Associativity of multiplication): For any $a, b, c \in F$ we have $(ab)c = a(bc)$.
7. (Commutativity of multiplication): For any $a, b \in F$ we have $ab = ba$.
8. (Multiplicative identity): There exists an element $1 \in F$ (which is not equal to 0) such that for every $a \in F$, we have $a \cdot 1 = a$.
9. (Multiplicative inverses): For each nonzero $a \in F$ there exists an element $a^{-1} \in F$ such that $a \cdot a^{-1} = 1$.

We then define subtraction of two elements by $a - b = a + (-b)$ and division of a by $b \neq 0$ by $a/b = a \cdot b^{-1}$.

At first glance this may look like an intimidating list of requirements, but it's really just a bunch of familiar properties that you know are true for $\mathbb{R}$ - the idea is that a field is something where we're insisting that addition and multiplication *behave like* they do in $\mathbb{R}$ and $\mathbb{C}$, and to do this we need to write down a bunch of these rules.

Example 2. The real numbers $\mathbb{R}$ and the complex numbers $\mathbb{C}$ each are fields with their usual addition and multiplication. The set of rational numbers $\mathbb{Q}$ is a field as well.

Non-Example 3. The integers $\mathbb{Z}$ are *not* a field - they satisfy axioms (1) through (8), but not axiom (9) because, for instance, 2 does not have a multiplicative inverse in the integers. A structure which satisfies the first 8 axioms is called a *commutative ring*, so the integers are one of those - you'll see more about rings if you take Math 4320. (Fields are a special case of commutative rings, and are definitely the nicest ones, which is why we're focusing on them).

Since the axioms of a field are set up to mimic $\mathbb{R}$ and $\mathbb{C}$, it's not surprising that we can prove that they imply many other basic algebraic properties we might expect. For instance:

Lemma 4. *Let F be a field. Then for any element $a \in F$ we have $a \cdot 0 = 0 \cdot a = 0$.*

Proof. To see $a \cdot 0 = 0 \cdot a = 0$ we first notice that $0 + 0 = 0$ by applying the additive identity axiom to 0 itself. Multiplying this identity by a we get $(0 + 0) \cdot a = 0 \cdot a$, and applying the distributivity axiom gives $0 \cdot a + 0 \cdot a = 0 \cdot a$. Finally, subtracting $0 \cdot a$ from both sides (i.e. adding its multiplicative inverse) we conclude $0 \cdot a + 0 = 0$ and thus $0 \cdot a = 0$. Commutativity of multiplication tells us $a \cdot 0 = 0 \cdot a$, finishing the proof. □

This is a lot of detail for proving a very simple fact, but that's what we need to do if we really want to justify every single algebraic manipulation we make. To start off you'll probably want to think through all of the details carefully, and once you get comfortable with them you can write less verbose proofs by combining steps. For instance the following proof is a lot less detailed - you might want to think how you'd use the axioms more carefully to get between the different steps.

Lemma 5. *A field F has the "cancellation property" that if $a, b, c \in F$ are such that $ab = ac$, then either $a = 0$ or $b = c$.*

Proof. Rearranging the equation $ab = ac$ gives $ab - ac = 0$. Using distributivity (plus the fact that $-(ac) = (-a)c = a(-c)$, which needs to be justified) we get $a(b - c) = 0$. Then we have two possibilities: either $a = 0$ (one of the conclusions we want) or $a \neq 0$, in which case we can multiply both sides by a^{-1} to get $b - c = 0$ and thus $b = c$. □

So most of the algebraic manipulations you'd do with numbers in $\mathbb{Q}$ or $\mathbb{R}$ or $\mathbb{C}$ remain valid over an arbitrary field F. But there are some surprising things that can happen! We can see some of them by looking at the example we've been building up to.

Proposition 6. *Let p be a prime number. Then $\mathbb{Z}/p\mathbb{Z}$, the integers modulo p, is a field.*

Proof. As we mentioned above, $\mathbb{Z}$ is a "commutative ring" and satisfies axioms (1)-(8). Since $\mathbb{Z}/p\mathbb{Z}$ is constructed as a quotient set from $\mathbb{Z}$ it's entirely formal to check that each of those axioms stays true in $\mathbb{Z}/p\mathbb{Z}$ (or any $\mathbb{Z}/n\mathbb{Z}$); for instance we have commutativity of addition because

$$[a] + [b] = [a + b] = [b + a] = [b] + [a]$$

(with the first and third equalities by definition of addition in $\mathbb{Z}/p\mathbb{Z}$, and the middle one by commutativity in $\mathbb{Z}$).

So the only thing we really need to check is axiom (9), that every nonzero element of $\mathbb{Z}/p\mathbb{Z}$ has a multiplicative inverse. This really is something new, since in $\mathbb{Z}$ most elements do not have multiplicative inverses - but by "collapsing" things using our equivalence relation some start to appear. So, let $[a]$ be a nonzero element of $\mathbb{Z}/p\mathbb{Z}$, i.e. not equal to the equivalence class $[0]$. This means $a \not\equiv 0 \pmod{p}$, and thus $p \nmid a$; since p is prime we can actually conclude $\gcd(a, p) = 1$, i.e. a and p are coprime. Then we showed in class that there exists x with $ax \equiv 1 \pmod{p}$, and therefore $[a] \cdot [x] = [1]$, so $[x]$ is a multiplicative inverse of $[a]$. □

Since $\mathbb{Z}/p\mathbb{Z}$ is a field and also has a finite number of elements (namely, p of them), it's an example of a *finite field*.

Definition 7. For any prime number p, we call $\mathbb{Z}/p\mathbb{Z}$ the *finite field with p elements*, and we often denote it $\mathbb{F}_p$.

As the notation suggests, we can show that *any* finite field with p elements is essentially the same as $\mathbb{Z}/p\mathbb{Z}$, in the sense that any such field is "isomorphic" to $\mathbb{Z}/p\mathbb{Z}$. It turns out there are other finite fields, too - we may come back to this topic later in the course, once we've built up enough theory to understand them.

For now we want to focus on a feature of $\mathbb{F}_p$ that may be surprising: if we add 1 to itself enough times, we get back to zero! To be careful about this we set the following notation:

Definition 8. Let F be a field. We let $0_F = 0$ and $1_F = 1$ be the additive and multiplicative identities in F, respectively. Then, for any $n > 1$ we define n_F as the sum of n copies of 1_F; i.e. $2_F = 1_F + 1_F$ and $3_F = 1_F + 1_F + 1_F$. For $n < 0$ we set $n_F = -(-n)_F$.

If we think about what happens for $F = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, we have

$$p_F = 1_F + \cdots + 1_F = [1] + \cdots + [1] = [p] = [0] = 0_F$$

(where these are sums over p terms). This is why we it's helpful to have this n_F notation - we can think of integers as "being inside" any field F in this way, but distinct integers can become equal when we do this.

Definition 9. Let F be a field. If p is the smallest positive integer such that $p_F = 0_F$, we say F has *characteristic* p; if there is no positive integer with $p_F = 0_F$ we say F has *characteristic* 0.

As the notation suggests, the characteristic of a field will always be a prime number (or zero); you're asked to prove this on your homework. The terminology "characteristic 0" probably seems a bit strange ("characteristic ∞" seems like it would fit better) but it makes sense in the context of studying ring theory in general.

So, we now have a few different examples of fields. If we look at the "smallest" ones, we have the rational numbers $\mathbb{Q}$ (of characteristic zero) and, for each prime p, a finite field $\mathbb{F}_p$ (of characteristic p). We also have $\mathbb{R}$ and $\mathbb{C}$ (both of characteristic zero) which contain $\mathbb{Q}$ inside of them. This isn't a coincidence; it turns out that every field of characteristic zero contains a copy of $\mathbb{Q}$, and every field of characteristic p contains a copy of $\mathbb{F}_p$. So if we start with $\mathbb{Q}$ or $\mathbb{F}_p$, how do we "build up" something bigger on top of it, and get more examples of fields? That turns out to be a bit too hard to answer now (and leads to a lot of interesting mathematics in the subjects of "field theory" and "algebraic number theory"), but I'll give one example:

Example 10. Let $\sqrt{2}$ be the usual positive square root of 2. We define a subset of $\mathbb{R}$ that we denote $\mathbb{Q}(\sqrt{2})$ as follows:

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a \in \mathbb{Q}, b \in \mathbb{Q}\} \subseteq \mathbb{R}.$$

I claim that this is actually a field. First of all, for this to make sense we need to check that addition and multiplication are actually binary operations *on* $\mathbb{Q}(\sqrt{2})$ *itself*, i.e. that if we add or multiply two elements we get something back in $\mathbb{Q}(\sqrt{2})$. For addition this is pretty obvious, and for multiplication it isn't much harder because we know $\sqrt{2}^2 = 2$ is in $\mathbb{Q}$ again:

$$(a + b\sqrt{2})(c + d\sqrt{2}) = ac + ad\sqrt{2} + bc\sqrt{2} + bd\sqrt{2}^2 = (ac + 2bd) + (ad + bc)\sqrt{2} \in \mathbb{Q}(\sqrt{2}).$$

So then we need to check the axioms for fields. The five axioms about associativity, commutativity, and distributivity are immediate: they identities we want are true because they hold in the larger set $\mathbb{R}$.

We need to pay a bit more attention to the axioms about identities and inverses, since they require *existence* of something; we know these things exist in $\mathbb{R}$ but we need to make sure we actually included them in $\mathbb{Q}(\sqrt{2})$! For existence of additive and multiplicative identities, this is still easy since we clearly have $0, 1 \in \mathbb{Q}(\sqrt{2})$. Additive inverses also aren't too bad, since $-(a + b\sqrt{2}) = (-a) + (-b)\sqrt{2}$. Multiplicative inverses are a bit more surprising, but it turns out that we have

$$\frac{1}{a + b\sqrt{2}} = \frac{(a - b\sqrt{2})}{(a - b\sqrt{2})(a + b\sqrt{2})} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}(\sqrt{2}).$$

Vector spaces. So now we have an abstract definition of a field, and some examples to keep in mind. Now we can give the abstract definition of a vector space over any field, and (finally!) get to doing actual linear algebra.

Definition 11. Let F be a field. A *vector space* with F as its field of scalars (usually "a vector space over F") is a set V with a binary operation of addition and a "scalar multiplication" operation $F \times V \to V$ (i.e. which takes a pair (a, v) with $a \in F$ and $v \in V$ as inputs, and outputs a single element $av \in V$) which satisfy the following list of axioms:

1. (Associativity of addition): For any $u, v, w \in V$ we have $(u + v) + w = u + (v + w)$.
2. (Commutativity of addition): For any $v, w \in V$ we have $v + w = w + v$.
3. (Additive identity): There exists an element $0 \in V$ such that for every $v \in V$, we have $v + 0 = v$.
4. (Additive inverses): For each $v \in V$ there exists an element $-v \in V$ such that $v + (-v) = 0$.
5. (Distributivity of scalar multiplication over vector addition): For for any $a \in F$ and $v, w \in V$ we have $a(v + w) = av + aw$.
6. (Distributivity of scalar multiplication over scalar addition): For for any $a, b \in F$ and $v \in V$ we have $(a + b)v = av + bv$.
7. (Compatibility of multiplications): For any $a, b \in F$ and $v \in V$ we have $(ab)v = a(bv)$.
8. (Compatibility of the multiplicative identity): For any $v \in V$ we have $1v = v$.

This list of axioms is identical to the one at the beginning of Chapter 2 of the textbook, except that we're now allowing F to be any field while the book only considers scalars in $\mathbb{R}$. We're now going to pick up in the book from there, except everywhere that the book uses $\mathbb{R}$ we'll work with an arbitrary field F. Essentially everything through Chapter 14 works identically for any field F as it does for $\mathbb{R}$! (The only exceptions are occasional things like examples talking about geometric things like areas and angles, or about continuous functions).