

Mathematics MATH 236, Winter 2007
Linear Algebra
Fields and vector spaces/ definitions and examples

Most of linear algebra takes place in structures called vector spaces. It takes place *over* structures called fields, which we now define.

DEFINITION 1. A *field* is a set (often denoted F) which has two binary operations $+_F$ (*addition*) and \cdot_F (*multiplication*) defined on it. (So for any $a, b \in F$, $a +_F b$ and $a \cdot_F b$ are elements of F .) They must satisfy the following rules:

1. There is an element $0_F \in F$ such that $0_F +_F a = a$ for any $a \in F$. (0_F is the *additive identity*, or just the *zero* of the field.)
2. For any element $a \in F$, there is an element $-a \in F$ such that $(-a) +_F a = 0_F$. ($-a$ is the *additive inverse* or the *negative* of a .)
3. For any $a, b, c \in F$, $a +_F (b +_F c) = (a +_F b) +_F c$. (This is the *associative law* for addition.)
4. For any $a, b \in F$, $a +_F b = b +_F a$ (the *commutative law* of addition).
5. There is an element $1_F \in F$ with $1_F \neq 0_F$ such that $1_F \cdot a = a$ for any $a \in F$. (1_F is the *multiplicative identity*, or just the *identity* or (sometimes) *unity* of the field.)
6. For any element $0_F \neq a \in F$, there is an element $a^{-1} \in F$ such that $(a^{-1}) \cdot_F a = 1_F$. (a^{-1} is the *multiplicative inverse* or the *inverse* of a .)
7. For any $a, b, c \in F$, $a \cdot_F (b \cdot_F c) = (a \cdot_F b) \cdot_F c$. (This is the *associative law* for multiplication.)
8. For any $a, b \in F$, $a \cdot_F b = b \cdot_F a$ (the *commutative law* of multiplication).
9. For any $a, b, c \in F$, $a \cdot_F (b +_F c) = (a \cdot_F b) +_F (a \cdot_F c)$ (the *distributive law*).

REMARKS.

1. All of these rules are true for the reals (we will denote the set of reals, and the field, by \mathcal{R}), the complex numbers (denoted \mathcal{C}), and the rationals (denoted \mathcal{Q}). So each of these is an example of a field. (This is with the usual, familiar, operations.) I will list some other, less familiar, examples below.
2. Contrarily, the integers (positive, negative and zero — we will use \mathcal{Z} for the integers) with the usual operations, *don't* make a field. The only problem is the multiplicative inverse — while any nonzero integer has a multiplicative inverse (in \mathcal{Q}), it isn't always in \mathcal{Z} , e.g., $\frac{1}{2}$ is not an integer. (\mathcal{Z} is not *closed under multiplicative inverses*, to use the technical term.)

3. In this definition, I should emphasize that the elements 0_F and 1_F *may not* be the usual 0 and 1. Similarly, even if there is a standard $+$ and \cdot , it is possible that $+_F$ and \cdot_F are different operations. (For instance, it's quite possible to define unusual operations $+_Z$ and \cdot_Z on the integers that make them into a field. I can do it, but it's messy.)
4. The exception for 0_F in the article regarding multiplicative inverses is necessary; it's not hard to prove from the other rules that $b \cdot 0_F = 0_F$ for any $b \in F$. (See below.)
5. Terminology alert! The first four axioms don't say anything about multiplication. They state that F is a *commutative group* (a.k.a. an *abelian group*, after Jens Abel) under addition. (Without the fourth one, it would just be a *group*). Similarly, the next four say that $F \setminus \{0_F\}$ is a commutative group under multiplication. (We toss out 0_F for this because every element of a group should have an inverse.) The distributive law connects the additive structure to the multiplicative structure.

Here are some other basic rules about fields.

PROPOSITION 1. Suppose that F is a field (with operations $+_F$ and \cdot_F).

1. The additive identity 0_F is unique. (That is, if $\hat{0}$ and $\bar{0}$ satisfy $a +_F \hat{0} = a$ and $a +_F \bar{0} = a$ for all $a \in F$, then $\hat{0} = \bar{0}$.)
2. The multiplicative identity 1_F is unique. (That is, if $\hat{1}$ and $\bar{1}$ satisfy $a \cdot_F \hat{1} = a$ and $a \cdot_F \bar{1} = a$ for all $a \in F$, then $\hat{1} = \bar{1}$.)
3. For any $a \in F$, the additive inverse $-a$ is unique. (That is, if \hat{a} and \bar{a} satisfy $a +_F \hat{a} = 0_F$ and $a +_F \bar{a} = 0_F$, then $\hat{a} = \bar{a}$.)
4. For any nonzero $a \in F$, the multiplicative inverse a^{-1} is unique. (That is, if a^* and a^{**} satisfy $a \cdot a^* = 1_F$ and $a \cdot a^{**} = 1_F$, then $a^* = a^{**}$.)
5. Addition is cancellative; if $a +_F b = a +_F c$ (for any $a, b, c \in F$), then $b = c$.
6. Multiplication is basically cancellative. If $a \cdot_F b = a \cdot_F c$ and $a \neq 0_F$, then $b = c$. (This for any nonzero a and any $b, c \in F$.)
7. $0_F \cdot a = a \cdot 0_F = 0_F$ for any $a \in F$.
8. The other distributive law. For any $a, b, c \in F$, $(a +_F b) \cdot_F c = (a \cdot_F c) +_F (b \cdot_F c)$.
9. Any other reasonable version of commutativity/associativity/distributivity that you like. For instance, $a + (b + (c + d)) = (b + d) + (a + c)$.

Some words on the proofs. I will omit all the F 's. For 1), consider $\hat{0} = \bar{0} + \hat{0}$ (because $\bar{0}$ is an additive identity) and this equals (or "is equal to"; but to paraphrase Soul Brother Number One, please, please, please, not "equals to") $\hat{0} + \bar{0}$ by commutativity, which equals $\bar{0}$ as $\hat{0}$ is an additive identity. 2) is almost the same.

3) and 4) are also similar. For 3), consider $\hat{a} = \hat{a} + 0 = \hat{a} + (\bar{a} + a) = (\hat{a} + \bar{a}) + a = (\bar{a} + \hat{a}) + a = \bar{a} + (\hat{a} + a) = \bar{a} + 0 = \bar{a}$.

5) and 6) are again virtually identical. For 6), suppose that $a \neq 0$, so a^{-1} exists. (For 5), we don't need to consider 0 separately.) Then if $a \cdot b = a \cdot c$, we have $a^{-1} \cdot (a \cdot b) = a^{-1} \cdot (a \cdot c)$. So $(a^{-1} \cdot a) \cdot b = (a^{-1} \cdot a) \cdot c$ by associativity; thus $1 \cdot b = 1 \cdot c$, which is the same as $b = c$.

For 7), first note that $0 + 0 = 0$. So $a \cdot (0 + 0) = a \cdot 0 = a \cdot 0 + 0$. Now $a \cdot (0 + 0) = (a \cdot 0) + (a \cdot 0)$ by distributivity, so by cancellation $a \cdot 0 = 0$. The other equality follows from commutativity of \cdot .

For 8), $(a + b) \cdot c = c \cdot (a + b)$ because multiplication is commutative, and this equals $(c \cdot a) + (c \cdot b)$ by the given distributive law. Using commutativity of \cdot twice more, we see that this equals $(a \cdot c) + (b \cdot c)$, as advertized.

Things like 9) are easy but tedious. You can make up (and I hope, prove) a million of them. For this one, using associativity and commutativity of $+$ a few times, we get that $a + (b + (c + d)) = a + (b + (d + c)) = a + ((b + d) + c) = (a + (b + d)) + c = ((b + d) + a) + c = (b + d) + (a + c)$.

I could go on. (For instance, I hope you can easily show that $-a = (-1) \cdot a$ for any a in a field. And that $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$. And that $a^{-1} + b^{-1} = (a + b) \cdot (a^{-1} \cdot b^{-1})$ as long as $a, b \neq 0$. And — this one's very useful — $a \cdot b = 0$ only if $a = 0$ or $b = 0$, or both. And, ...) We will be assuming this kind of simple algebra for fields; if you have any doubt at all whether one of the usual algebra rules holds for every field, try to prove it, or look for a counterexample. (It's best to do both of these at the same time if you're really not sure.)

Here are some other fields for your delectation. The rather important, if simple, \mathbb{Z}_2 , to start. The only elements of the set \mathbb{Z}_2 are 0 and 1, but they are not the standard 0 and 1 in \mathbb{Q} . Here are the addition and multiplication tables

for \mathbb{Z}_2 .

+	0	1
0	0	1
1	1	0

 and

·	0	1
0	0	0
1	0	1

. Except for $1 + 1 = 0$, these look the

same as usual. Although we use the same symbols 0, 1, + and \cdot as if we were operating in the real numbers or rationals, obviously something doesn't mean the same as usual. (In fact, we don't consider any of these symbols as having the same meaning as in the reals.) One way to think of \mathbb{Z}_2 is to regard the operations as having the usual results, just that $0 = 2 = -2 = 4 = \dots$ and $1 = -1 = 3 = -3 = \dots$ in \mathbb{Z}_2 , that is 0 represents all even numbers and 1 all odds.

Another way to consider \mathbb{Z}_2 (which is also called F_2 , and sometimes GF_2 , where the G is for Evariste Galois) is as your basic 2-element Boolean algebra.

(Then \cdot becomes “and” and $+$ becomes “exclusive or”.)

One can vary this example to get a finite field \mathcal{Z}_p for any prime number p . The distinct elements are usually denoted $0, 1, \dots, p-1$, and we operate “as usual” except that in \mathcal{Z}_p , $0 = p = 2p = -p$ and so on. (In \mathcal{Z}_5 we would have $0 = 5 = -5 = 10$, etc., but also $1 = 6 = -4 = 11 = \dots$, $2 = 7 = -3 = 12 = \dots$; two numerals stand for the same object in \mathcal{Z}_5 if they differ by a multiple of

		$+$					
			0	1	2	3	4
5.) The addition and multiplication tables for \mathcal{Z}_5 are	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

[The same definitions could be — and are — given for non-prime natural numbers, but don’t yield fields; in \mathcal{Z}_6 neither 2 nor 3 is 0, but $6 = 2 \cdot 3 = 0$. There is no multiplicative inverse for 2 or for 3 in \mathcal{Z}_6 .]

There are loads of *subfields* of the real numbers. These would be subsets of the real numbers which are fields in their own right, with the standard addition and multiplication. \mathcal{Q} is the obvious one, and in fact the *smallest* one; it’s a subset of any other. (This is easy to show, but a pain to write out.) Another one is $F = \mathcal{Q}[\sqrt{2}]$, consisting of all numbers of the form $a + b\sqrt{2}$ where a and b are rationals — it’s trivial to show that this is a field, except maybe for showing that $(a + b\sqrt{2})^{-1}$ is in F . To see this, rationalize the denominator, by which I mean (of course) multiply $\frac{1}{a+b\sqrt{2}}$ by $\frac{a-b\sqrt{2}}{a-b\sqrt{2}}$ and see what transpires. Similarly, $\mathcal{Q}[\sqrt{3}]$ can be defined, and so can $\mathcal{Q}[\sqrt[3]{2}]$, whose elements are $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ for a, b, c rational. (It’s not quite so easy to show that this is closed under multiplicative inverses.) And so on.

It is often useful to consider the field of *rational functions*, which are functions defined on a *big part* of the reals (or complexes, if you prefer). f is a rational function if $f(x) = \frac{P(x)}{Q(x)}$ for some polynomial functions P and Q . (f will not be defined anywhere Q is zero.) This is slightly cheating — we must exclude $Q = 0$ (the constant) and agree that $f_1 = f_2$ if $f_1(x) = \frac{P_1(x)}{Q_1(x)}$ and $f_2(x) = \frac{P_2(x)}{Q_2(x)}$ in case the polynomials $P_1(x)Q_2(x)$ and $P_2(x)Q_1(x)$ are identical. Thus, if $f_1(x) = \frac{x}{x-1}$ and $f_2(x) = \frac{x^2}{x^2-x}$ we pretend that $f_1 = f_2$ even though technically f_1 is defined at 0 and f_2 isn’t. It’s not hard (but it is fussy)

to make the identification precise and then show that we have a field with the usual operations of adding and multiplying functions (i.e., pointwise).

[I might mention that the reason the polynomial functions by themselves don't comprise a field is that there aren't generally multiplicative inverses — $\frac{1}{x^2-2x-3}$ is not a polynomial.]

Now for vector spaces. We suppose that in the following F is a field.

DEFINITION 2. A *vector space* over F — a.k.a. an F -space — is a set (often denoted V) which has a binary operation $+_V$ (*vector addition*) defined on it, and an operation $\cdot_{F,V}$ (*scalar multiplication*) defined from $F \times V$ to V . (So for any $\vec{v}, \vec{w} \in V$, $\vec{v} +_V \vec{w}$ is in V , and for any $\alpha \in F$ and $\vec{v} \in V$ $\alpha \cdot_{F,V} \vec{v} \in V$. In this context an element α of F is called a *scalar*.) They must satisfy the following rules, besides the rules that F itself must obey to join the grand fellowship of fields:

1. There is an element $\vec{0}_V \in V$ such that $\vec{0}_V +_V \vec{v} = \vec{v}$ for any $\vec{v} \in V$. ($\vec{0}_V$ is the *zero vector*.)
2. For any element $\vec{v} \in V$, there is an element $-\vec{v} \in V$ such that $(-\vec{v}) +_V \vec{v} = \vec{0}_V$. ($-\vec{v}$ is the *additive inverse* or the *negative* of \vec{v} .)
3. For any $\vec{u}, \vec{v}, \vec{w} \in V$, $\vec{u} +_V (\vec{v} +_V \vec{w}) = (\vec{u} +_V \vec{v}) +_V \vec{w}$. (This is the *associative law* for vector addition.)
4. For any $\vec{v}, \vec{w} \in V$, $\vec{v} +_V \vec{w} = \vec{w} +_V \vec{v}$ (the *commutative law* of vector addition).
5. $1_F \cdot_{F,V} \vec{v} = \vec{v}$ for any $\vec{v} \in V$. (1_F still acts like a multiplicative identity on the space.)
6. For any elements $\alpha, \beta \in F$ and $\vec{v} \in V$, $\alpha \cdot_{F,V} (\beta \cdot_{F,V} \vec{v}) = (\alpha \cdot_F \beta) \cdot_{F,V} \vec{v}$. (This is a kind of associative law for scalar multiplication.)
7. For any $\alpha, \beta \in F$, and $\vec{v} \in V$. $(\alpha +_F \beta) \cdot_{F,V} \vec{v} = (\alpha \cdot_{F,V} \vec{v}) +_V (\beta \cdot_{F,V} \vec{v})$. (This is a distributive law.)
8. For any $\alpha \in F$, and $\vec{v}, \vec{w} \in V$, $\alpha \cdot_{F,V} (\vec{v} +_V \vec{w}) = (\alpha \cdot_{F,V} \vec{v}) +_V (\alpha \cdot_{F,V} \vec{w})$. (The other distributive law.)

The first comment to make is that we will drop all those subscripts on the operations whenever we can (especially on scalar multiplication); they are there just to emphasize where the inputs are coming from. The field has its own operations, the vector space has its own addition, and the scalar multiplication is distinct from the field multiplication in that it involves both field and space. But my text editor easily overdoses on subscripts; it would be cruel to feed it too many. For $\alpha \in F$ and $\vec{v} \in V$, we will write $\alpha \cdot \vec{v}$ or just $\alpha \vec{v}$ for the scalar multiple, trusting to the context to save us from any ambiguity.

You will notice that the first four axioms (rules) here are identical to those for fields, except that they involve vectors. A vector space is in particular an abelian group under vector addition.

There is no multiplication just involving vectors on a vector space, necessarily. In many of the important examples of vector spaces (functions, matrices, etc.) there is a natural multiplication that occurs, but this is always something extra. More on this later.

Worth noting is that if F is any field and K is a smaller field (a subfield), then any F -space V can be regarded as a K -space with the same vector addition and scalar multiplication. Again, more later.

Here are some basic properties of vector spaces.

PROPOSITION 2. Suppose that V is an F -space (where F is any particular field.)

1. The zero vector is unique.
2. For any $\vec{v} \in V$, the negative $-\vec{v}$ is unique; in fact, it's equal to $(-1) \cdot \vec{v}$.
3. Vector addition is cancellative — for any \vec{u}, \vec{v} and \vec{w} in V , if $\vec{u} + \vec{v} = \vec{u} + \vec{w}$, then $\vec{v} = \vec{w}$.
4. $0_F \cdot \vec{v} = \vec{0}_V$ and $\alpha \cdot \vec{0}_V = \vec{0}_V$ for any $\vec{v} \in V$ and any scalar α .
5. Conversely, if $\alpha \cdot \vec{v} = \vec{0}$ (for α a scalar and \vec{v} a vector), then either $\alpha = 0_F$ or $\vec{v} = \vec{0}_V$.

The proofs of the first three parts of this are basically the same as for fields. We will leave off all the subscripts for a while. To see that $0\vec{v} = \vec{0}$, note that $\vec{0} + 0\vec{v} = 0\vec{v} = (0 + 0)\vec{v} = 0\vec{v} + 0\vec{v}$ and apply cancellation to get rid of a $0\vec{v}$ on each side. (We used one distributive law here, and also commutativity of $+$.) The other distributive law helps us see that $\vec{0} + \alpha\vec{0} = \alpha\vec{0} = \alpha(\vec{0} + \vec{0}) = \alpha\vec{0} + \alpha\vec{0}$; again, cancel to see that 4) is true.

For 5), suppose that $\alpha\vec{v} = \vec{0}$ but $\alpha \neq 0$. Then $\alpha^{-1}(\alpha\vec{v}) = \alpha^{-1}\vec{0} = \vec{0}$. But by the funny associate law, $\alpha^{-1}(\alpha\vec{v}) = (\alpha^{-1}\alpha)\vec{v}$ and this equals $1\vec{v} = \vec{v}$. So $\vec{v} = \vec{0}$. That does it.

The BASIC EXAMPLE of a vector space over a field F is F^n for a natural number n . Really, of course, this is an infinite collection of examples, one for each n . The elements of F^n are n -vectors (duh!), which we will by default take

as column vectors ($n \times 1$ matrices). Thus $F^3 = \left\{ \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} : a_1, a_2, a_3 \in F \right\}$. In

case $F = \mathcal{R}$, this is just ordinary Euclidean 3-space. [It is on occasion natural or convenient to consider “row vectors”, which are $1 \times n$ matrices; we will do so sometimes, but the default setting is columns.]

Specifying the set (and the field) by itself doesn't tell us what the vector space is; we need to know what the operations are. Here they are completely

familiar; we add coordinatewise and multiply every entry by the scalar for multiplication. Thus in F^3 , if $\vec{v} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix}$ and $\vec{w} = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix}$, we define $\vec{v} + \vec{w}$ as $\begin{pmatrix} a_1 + b_1 \\ a_2 + b_2 \\ a_3 + b_3 \end{pmatrix}$. (Here $a_1 + b_1$ should be written $a_1 +_F b_1$, as the addition is carried out in the field, but let's go easy on those subscripts.) If α is a scalar (id est, an element of F), then $\alpha\vec{v}$ is defined to be $\begin{pmatrix} \alpha a_1 \\ \alpha a_2 \\ \alpha a_3 \end{pmatrix}$.

It is utter wrist exercise — the socially acceptable kind — to verify that with these operations F^n is a vector space over F . (To verify associativity of vector addition, for instance, use associativity of addition in F .) In case $n = 1$, we will often lie a little and pretend $F^1 = F$. (Technically, a one-by one matrix (a) is different from a itself, but not all that different.)

A variation on this example is the set of $m \times n$ matrices over the field F , where m and n are fixed but arbitrary natural numbers. This set (and space) is denoted $M_{m,n}(F)$ or $F^{m \times n}$; in the square case $m = n$ we may just write $M_n(F)$. If A and B are $m \times n$ matrices with entries from F and $1 \leq j \leq m$, $1 \leq k \leq n$, then the (j, k) -entry of $A + B$ is $a_{j,k} + b_{j,k}$ where $a_{j,k}$ is the (j, k) -entry of A and $b_{j,k}$ the (j, k) -entry of B . If $\alpha \in F$, then the (j, k) -entry of αA is $\alpha a_{j,k}$. (I trust this is all familiar; I spelled it out partly to fix notation for future reference.) F^n above is $M_{n,1}(F)$.

Again, checking that this is a v.s./ F (a vector space over F) is nothing. Note that I didn't put little arrows over A and B here — I won't in such cases, or if the vectors are functions, but if I'm dealing with F^n or some arbitrary space V , I generally will. I find this kind of “typing” useful to keep vectors and scalars separate.

Note that in some cases we can multiply matrices, and of course this is a crucial aspect of linear algebra, but it is not part of the vector space structure of $M_{m,n}(F)$ even if $m = n$. It's something more. In the vector space itself, we can only multiply by scalars.

Another important class of examples arises from functions. We will usually be considering functions from \mathcal{R} to \mathcal{R} , but at this stage we may as well be general.

Let X be any nonempty set, and F any field. The set F^X is defined to be the collection all functions $f : X \rightarrow F$. $F^X = \{f | f : X \rightarrow F \text{ is a function}\}$. (If $f \in F^X$, then for any $x \in X$, $f(x)$ is an element of F ; there's no other constraint on f here.) We define the operations on F^X pointwise — to wit, if $f, g \in F^X$, then $f + g$ is the element $h \in F^X$ such that $h(x) = f(x) + g(x)$ for every $x \in X$; if $f \in F^X$ and $\alpha \in F$, then αf is the function $k \in F^X$ such that $k(x) = \alpha \cdot f(x)$. $f(x) + g(x)$ and $\alpha \cdot f(x)$ are evaluated in the field F .

We summarize these definitions by saying $(f + g)(x) = f(x) + g(x)$ and

$(\alpha f)(x) = \alpha \cdot f(x)$; in case $F = \mathcal{R}$ and $X = \mathcal{R}$, or for that matter X is some interval in \mathcal{R} , these definitions are familiar (I hope!) from calculus. I mean, if $f(x) = \sin x$ and $g(x) = x^3$ for every real x , then $(f + g)(x) = \sin x + x^3$ for every real x and this *defines* what $f + g$ is. Capiche?

I will now go through the gory details of verifying that F^X is a vector space over F .

1. The zero vector here is the constant function whose value is 0_F ; we will as usual just call it 0, even though writing $0(x) = 0$ for all x looks funny (and *does not mean* zero times x is zero; we're defining a particular function here). It's trivial to see that this works; for any $f \in F^X$, $0 + f = f$ since $(0 + f)(x) = 0(x) + f(x) = 0_F + f(x) = f(x)$ for every $x \in X$. (Note the use of the basic property of 0_F here.)
2. For any $f \in F^X$, we let $-f$ be the function defined by $(-f)(x) = -(f(x))$ for every $x \in X$. To see that $(-f) + f = 0$ we need to check that $[(-f) + f](x) = 0(x)$ for every x . But by definition of function addition, $[(-f) + f](x) = (-f)(x) + f(x)$; by our definition of $-f$, this is $-(f(x)) + f(x)$. As $-a + a = 0$ for every element of F , $-(f(x)) + f(x) = 0 = 0(x)$, so indeed $(-f) + f = 0$ in F^X . (I belaboured these two, very simple, cases because the point here is not that any of the verifications are difficult — they're all wrist exercise — but to emphasize what it means to check the rules here. I promise to be briefer below.)
3. To see that $f + (g + h) = (f + g) + h$ for any $f, g, h \in F^X$, we check that for any $x \in X$, $[f + (g + h)](x) = [(f + g) + h](x)$. But the left-hand side is by definition $f(x) + (g + h)(x)$, which is $f(x) + (g(x) + h(x))$ and this — by associativity in F — is $(f(x) + g(x)) + h(x)$ and that's $(f + g)(x) + h(x) = [(f + g) + h](x)$.
4. For any $f, g \in F^X$ and any $x \in X$, $(f + g)(x) = f(x) + g(x) = g(x) + f(x)$ (using commutativity in F) and this equals $(g + f)(x)$. So $f + g = g + f$.
5. To see that $1_F \cdot f = f$ for any $f \in F^X$, note that $(1_F f)(x) = 1_F(f(x)) = f(x)$ for any $x \in X$.
6. Suppose that α and β are scalars and $f \in F^X$. Then for any $x \in X$, $[\alpha \cdot (\beta f)](x) = \alpha([\beta f](x)) = \alpha(\beta f(x)) = (\alpha \cdot \beta)f(x) = [(\alpha \cdot \beta)f](x)$; hence $\alpha \cdot (\beta f) = (\alpha \cdot \beta)f$. (The third equality uses associativity of multiplication in F .)
7. If α and β are scalars and $f \in F^X$, we should show that $(\alpha + \beta)f = (\alpha f) + (\beta f)$. Let $x \in X$. Then $[(\alpha + \beta)f](x) = (\alpha + \beta)f(x) = (\alpha f(x)) + (\beta f(x))$ (this by distributivity in F) and this is the same as $(\alpha f)(x) + (\beta f)(x) = [(\alpha f) + (\beta f)](x)$. Right?

8. Finally, suppose that α is a scalar and that $f, g \in F^X$. To see that $\alpha(f + g) = (\alpha f) + (\alpha g)$, we check your favourite $x \in X$. $[\alpha(f + g)](x) = \alpha[(f + g)(x)] = \alpha[f(x) + g(x)]$ (all by definition) which is $(\alpha f(x)) + (\alpha g(x))$ by distributivity in F , and this is $(\alpha f)(x) + (\alpha g)(x) = [(\alpha f) + (\alpha g)](x)$. Done.

WHEW! Lots of writing, not much thought (I hope). I am not actually opposed to thought, but one should reserve deep thinking for deep matters. This “proof” is long and involved because the definition of a vector space is, but it (the proof) is very shallow.

Almost every vector space we will see is either one of the above, some minor variation on one of them, or a subspace of one of these. (Coming attractions.)

Before passing on examples (for now) we pause to consider the complex field \mathcal{C} and the spaces \mathcal{C}^n . As mentioned above, each of these can be considered as a vector space over \mathcal{C} , but they can also be thought of as vector spaces over \mathcal{R} (or over \mathcal{Q} if we like). \mathcal{C} , regarded as a vector space over itself, is one-dimensional; as a vector space over \mathcal{R} , it’s two-dimensional. (One of the first things anyone studying \mathcal{C} sees is the representation of complex numbers as \mathcal{R}^2 with “real” and “imaginary” axes.)

So these spaces are not exactly the same thing, even though the underlying set is the same in both cases. In the first, $2 + 17i$ is a scalar; in the second, only real numbers are scalars. The fact that we can multiply complex numbers is of course significant — it is part of the v.s. structure of \mathcal{C} and \mathcal{C}^n when we regard these as complex vector spaces. It is something extra when we consider them as \mathcal{R} -spaces.

In case $F = X = \mathcal{R}$, there are various significant *subspaces* of F^X . Among them are the space $C(\mathcal{R})$ (sometimes $C^0(\mathcal{R})$) of all continuous functions. We will also consider $C([a, b])$ for a closed interval $[a, b] \subseteq \mathcal{R}$, which is the space of real-valued functions defined and continuous on the interval. $C^1(\mathcal{R})$ is the space of functions with continuous first derivatives, and generally $C^n(\mathcal{R})$ is fairly standard notation for the collection of real-valued functions defined on (all of) \mathcal{R} which have continuous n th derivatives. (We can also consider $C^n([a, b])$.) $C^\infty(\mathcal{R})$ stands for the space of all functions defined on \mathcal{R} with derivatives of all orders. We will use the notation $P(x)$ and for the collection of all polynomial functions with real coefficients (if x is the variable); we may also call this space $\mathcal{R}[x]$. More generally, for any field F , $F[x]$ may be used to denote the collection of all polynomials with coefficients in F .

Here, a *subspace* of a vector space V (over F) is a subset $S \subseteq V$ which contains 0_F and is *closed under vector addition* and *closed under scalar multiplication*.

The first closure condition means that, whenever \vec{v} and \vec{w} are in S , then so is $\vec{v} + \vec{w}$. The second means that, whenever $\vec{v} \in S$ and $\alpha \in F$, then $\alpha \cdot \vec{v} \in S$. It is trivial to see that if S is a subspace of an F -space V , then S is itself an F -space; the rules are automatic.