Axioms for Fields and Vector Spaces

The subject matter of Linear Algebra can be deduced from a relatively small set of first principles called "Axioms" and then applied to an astonishingly wide range of situations in which those few axioms hold. An alternative approach to the subject is to study several typical or archetypal situations and draw conclusions that generalize to other situations that seem at first unrelated. An example of an archetypal situation is matrix multiplication. Neither approach is fully satisfactory by itself. The first can be too dry, the second drowned in inessential details. In this course both approaches are pursued, thus combining the best with the worst of both worlds.

Linear Algebra begins with a *Field* of *Scalars*, which are entities $\alpha, ß, \gamma, \ldots$ analogous to numbers that obey the following rules:

0 and 1 are scalars.
Any two scalars α and $ß$ have a sum $\alpha + ß$ which is also a scalar; $\alpha + 0 = \alpha$.
If α is a scalar so is $-\alpha$; and $ß - \alpha := ß + (-\alpha)$; and $\alpha - \alpha = \alpha + (-\alpha) = 0$.
Addition is commutative, $\alpha + ß = ß + \alpha$, and associative, $(\alpha + ß) + \gamma = \alpha + (ß + \gamma)$.
Any two scalars α and $ß$ have a product $\alpha \cdot ß$ which is also a scalar; $\alpha \cdot 1 = \alpha$; $\alpha \cdot 0 = 0$.
If scalar $\alpha \neq 0$ so is α^{-1} ; and $ß/\alpha := ß \cdot (\alpha^{-1})$; $\alpha/\alpha = \alpha \cdot (\alpha^{-1}) = 1$. But there is no 0^{-1} .
Multiplication is commutative, $\alpha \cdot ß = ß \cdot \alpha$, and associative, $(\alpha \cdot ß) \cdot \gamma = \alpha \cdot (ß \cdot \gamma)$.
Multiplication distributes over addition; $\alpha \cdot (ß + \gamma) = \alpha \cdot ß + \alpha \cdot \gamma$.
(We often omit the dot $\cdot$ from multiplications.)

A few examples of fields are …
The Rational numbers, ratios of Integers. (The Integers do *not* constitute a field.)
The Algebraic numbers, roots of polynomial equations with integer coefficients.
The Real numbers, limits of bounded monotonic sequences of rational numbers.
The Complex numbers, roots of polynomial equations with real coefficients.
Rational functions, ratios of polynomials with coefficients from one of the previous fields.
The integers modulo a prime; this field has just finitely many members.

There are many other fields, but this course will use the first four almost exclusively.
(That the algebraic numbers form a field can be inferred from unobvious properties of *symmetric functions*.)

A *Vector Space* over a field of scalars $\alpha, ß, \mu, \ldots$ is a set of entities $\mathbf{x}, \mathbf{y}, \mathbf{z}, \ldots$ called "vectors" that obey the following rules:

If $\mathbf{x}$ is a vector so is $ß \circ \mathbf{x} = \mathbf{x} \circ ß$ for any scalar $ß$, and $1 \circ \mathbf{x} = \mathbf{x}$, and $(ß\mu) \circ \mathbf{x} = ß \circ (\mu \circ \mathbf{x})$.
If $\mathbf{x}$ and $\mathbf{y}$ are vectors so is $\mathbf{x} \dotplus \mathbf{y}$.
Addition is commutative, $\mathbf{x} \dotplus \mathbf{y} = \mathbf{y} \dotplus \mathbf{x}$, and associative, $(\mathbf{x} \dotplus \mathbf{y}) \dotplus \mathbf{z} = \mathbf{x} \dotplus (\mathbf{y} \dotplus \mathbf{z})$.
There is a zero vector $\mathbf{o}$ that satisfies $\mathbf{x} \dotplus \mathbf{o} = \mathbf{x}$ and $0 \circ \mathbf{x} = \mathbf{o}$ for every vector $\mathbf{x}$.
If $\mathbf{x}$ is a vector so is $-\mathbf{x} = (-1) \circ \mathbf{x}$; and $\mathbf{y} \dotminus \mathbf{x} := \mathbf{y} \dotplus (-\mathbf{x})$; $\mathbf{x} \dotminus \mathbf{x} = \mathbf{x} \dotplus (-\mathbf{x}) = \mathbf{o}$.
Multiplication distributes over addition: $ß \circ (\mathbf{x} \dotplus \mathbf{y}) = ß \circ \mathbf{x} \dotplus ß \circ \mathbf{y}$; $(ß + \mu) \circ \mathbf{x} = ß \circ \mathbf{x} \dotplus \mu \circ \mathbf{x}$.
(We usually omit the dot $\circ$, and drop the distinction between $\dotplus$ and $+$, and between $\dotminus$ and $-$.)

(Multiplying two vectors yields another in the same space only if the space is an *Algebra* too.)

The axioms for an abstract vector space are intentionally *not categorical* ; they tell us something about a vector space without saying exactly what it is. Consequently they tell us what is common to a vast variety of vector spaces some of them very peculiar. For instance, the axioms do not say how the vector operations $\{ \dotplus , \dotminus , \circ \}$ are to be implemented so long as they follow the rules. An implementation can appear perverse at first, as does the following example:

Start with a space V of column vectors x, y, z, … over the Real field with vector operations defined elementwise in the usual way: vector $x = \mu\circ y \dotplus ß\circ z$ just when $x_j = \mu\cdot y_j + ß\cdot z_j$ for the corresponding components x_j of x , y_j of y and z_j of z . Here there is no need to distinguish $\{ \dotplus , \dotminus , \circ \}$ from $\{ + , – , \cdot \}$; we might as well write $x = \mu\cdot y + ß\cdot z$. Next choose any function f that maps the Real field one-to-one upon itself, so f has an inverse Ω that satisfies $f(\Omega(ß)) = ß = \Omega(f(ß))$ for every real ß . One possibility is $f(ß) := ß + 7$, and then $\Omega(ß) = ß – 7$. A second possibility is $f(ß) := ß^3$, and then $\Omega(ß) = \sqrt[3]{ß}$. Reject trivial cases for which function $f(ß)/ß$ is constant. Next map V one-to-one onto a space **V** of column vectors **x**, **y**, **z**, … and *vice-versa* thus:

with every x in V associate **x** := (Ω(x) elementwise) in **V** ;
with every **x** in **V** associate x := (f(**x**) elementwise) in V .

Now write " $\mathbf{x} = \mu\circ\mathbf{y} \dotplus ß\circ\mathbf{z}$ " to mean " $\mathbf{x} = \Omega(\mu\cdot f(\mathbf{y}) + ß\cdot f(\mathbf{z}))$ elementwise ". Implemented perversely this way, the operations $\{ \dotplus , \dotminus , \circ \}$ in **V** must be distinguished from the Real field's operations $\{ + , – , \cdot \}$. The spaces V and **V** are really the same vector space in which the elements of every vector x are its components relative to an obvious basis for V , but **V** has no basis for which the elements of every column vector **x** are its components.

The axioms for a vector space bigger than { **o** } imply that it must have a *basis*, a set of *linearly independent* vectors that *span* the space. The meanings of "basis", "linearly independent" and "span" are quite clear if the space has finite *dimension* — this is the number of vectors in a basis. Every linearly independent set of vectors from a given space can be augmented by choosing more vectors, if necessary, to fill out a basis that spans this space, and every basis for this space turns out to have the same number of vectors in it. (You should know how to prove this.)

Infinite-dimensional spaces pose interesting challenges. The first concerns the sum of infinitely many basis vectors; it makes sense only if accompanied by an apt notion of *convergence*. This challenge can be postponed by insisting at first upon finite sums; then every vector in the space must be obtainable as a linear combination of finitely many basis vectors. Such a basis may exist only as a result of infinitely many choices of new vectors to augment previously chosen linearly independent vectors that do not yet span the space. Perhaps the word "exist" is too strong here.

For example, the field of Real numbers (including Algebraic and Transcendental) can be regarded as a vector space over the Rational field; for this purpose a basis consists of a proper subset $\{ \mathbf{r}_j \}$ of Reals which permits the expression of every other Real $\mathbf{r} = \sum_j ß_j\cdot\mathbf{r}_j$ as a sum of finitely many terms in which each coefficient $ß_j$ is a rational number determined uniquely by **r** . Such a basis, named after an early 20th century German mathematician G. Hamel, must contain *uncountably* many members; *i.e.*, the subscript j must range over a set more infinite than the integers or Rationals. There is no way to exhibit a Hamel basis because there is no way to decide for every set of Reals whether it is linearly independent. Like Spiritualism and Physics, Mathematics has its invisible presences.

With a few exceptions, every vector space considered in this course is finite dimensional. Its vectors and linear operators map to numerical column vectors and matrices via bases. Thus the course really concerns matrix multiplication. The point of the course is to learn how to tell which multiplications deserve doing and then do on a computer those that cannot be avoided. To keep the work from becoming unmanageable, Applied Mathematicians devote much of their time to choosing bases well. Their choices are guided by deductions from axioms but motivated partly by experience with archetypal examples and partly by geometric insights. We'll look at them all.