Fields and Vector Spaces

Fields:

Informally, you should think of a **field** as somewhere you can add, subtract, multiply, and divide (except by 0). Formally, a field is a set F which has special elements, called 0 and 1, two operations, $+$ and $\times$ (which take two elements of F and return an element of F), and two functions, $-$ and $^{-1}$ (which take a single element of F and return an element of F, except that $^{-1}$ is only defined on *non-zero* elements of F), satisfying the following properties for any x, y, and z in F:

$x + y = y + x$	commutativity of addition
$(x + y) + z = x + (y + z)$	associativity of addition
$x + 0 = x$	0 is identity for addition
$x + (-x) = 0$	additive inverses (subtraction)
$x \times y = y \times x$	commutativity of multiplication
$(x \times y) \times z = x \times (y \times z)$	associativity of multiplication
$x \times 1 = x$	1 is identity for multiplication
$x \times x^{-1} = 1$	multiplicative inverses (division)
$x \times (y + z) = (x \times y) + (x \times z)$	multiplication distributes over addition
$0 \neq 1$	non-triviality.

Warning: in physics and applied maths, the terms "scalar field" and "vector field" are used to describe certain types of function on a surface or space. This is a totally different use of the word "field" and has nothing to do with the notion discussed here.

Examples of fields include $\mathbb{Q}$ (the rational numbers), $\mathbb{R}$ (the real numbers), and $\mathbb{C}$ (the complex numbers). There are many other examples of fields; if you know modular arithmetic, the integers modulo a prime are a field (don't worry if you don't know modular arithmetic); the set of numbers of the form $a + b\sqrt{2}$, where a and b are rational, is a field, and many more.

Non-examples of fields include the integers, $\mathbb{Z}$, because division fails (2 is an integer, but 2^{-1} isn't), or the integers modulo any non-prime (*e.g.*, 3 is non-zero

modulo 6, but there is no 3^{-1} modulo 6; again, don't worry about this if you haven't seen modular arithmetic). If you've seen matrices, the set of 2×2 matrices with real entries, for instance, is not a field for two reasons; one reason is that multiplication does not commute, and the other is that division fails, since not all non-zero matrices are invertible. Don't worry if you haven't seen matrices.

The last condition, non-triviality, is not hugely important; some people do not include that condition, and allow fields where $0 = 1$. In fact, it can be shown that there is only one structure satisfying the conditions of a field with $0 = 1$; so allowing trivial fields only gives you one extra field, and it's an incredibly simple one! For a tricky (optional) exercise, figure out what the trivial field is and why it is the only field with $0 = 1$.

Vector Spaces:

Let F be any field. We will call elements of F **scalars** are use Greek letters to denote them. A **vector space** over F is, informally, somewhere you can add and subtract, and multiply by scalars (from F). Formally, a vector space over F is a set V (the elements of which we call **vectors** and denote with Latin letters), which has a special element $\underline{0}$ (the **zero vector**) an operation $\oplus$ ("vector addition"—taking two elements of V and giving an element of V as output), a function $\sim$ ("vector minus"—taking one element of V and giving another), and an operation $.$ (taking a scalar from F and a vector from V and giving a vector in V). These must satisfy the following conditions for any λ and μ in F, and u, v, w in V:

$u \oplus v = v \oplus u$	commutativity of vector addition
$(u \oplus v) \oplus w = u \oplus (v \oplus w)$	associativity of vector addition
$u \oplus \underline{0} = u$	$\underline{0}$ is identity for vector addition
$u \oplus (\sim u) = \underline{0}$	additive inverses (subtraction)
$(\lambda \times \mu).u = \lambda.(\mu.u)$	associativity of scalar multiplication
$1.u = u$	1 is identity for scalar multiplication
$\lambda.(u + v) = (\lambda.u) \oplus (\lambda.v)$	scalar multiplication distributes over vector addition
$(\lambda + \mu).u = (\lambda.u) + (\mu.u)$	scalar multiplication distributes over scalar addition.

Here, we have written $\oplus$ for vector addition and $\sim$ for vector minus to make it clear that these are not necessarily the same operations as $+$ and $-$ in the field F. However, normally we just write $+$ and $-$ regardless of whether we mean scalar addition/minus or vector addition/minus; it is clear from the context which is meant (since the things we're adding will either be vectors or scalars). Similarly, the zero vector has been written as $\underline{0}$ to emphasise that it is different from the

zero scalar, but normally we write them both as 0 and let context make it clear which is meant.

For example, $\mathbb{R}^2$ is a vector space over $\mathbb{R}$; then the zero scalar is literally the number 0, whereas the zero vector is actually the pair $(0,0)$; so an equation like $0.u = 0$ would more precisely be written as $0.u = \underline{0}$, or $0u = (0,0)$; but it is clear what is meant by $0u = 0$. An equation like $(1,2) + (-1,-2) = 0$ would more precisely be written as $(1,2) \oplus (-1,-2) = (0,0)$, but again, it is clear what is meant.

Given any field F and positive integer n, F^n, the set of n-tuples (ordered lists of n elements) with entries from n is a vector space over F. For example, if we take our field to be $\mathbb{Q}$, the rationals, then $\mathbb{Q}^3$, the set of ordered triples (a,b,c), where a, b, and c are rational, is a vector space over $\mathbb{Q}$.

There are more exciting examples of vector spaces though; *anywhere* we can add, subtract, and multiply by scalars, subject to the conditions above, qualifies as a vector space. For instance, the set of all polynomials with real coefficients is a vector space over $\mathbb{R}$ (and the set of polynomials with complex coefficients is a vector space over $\mathbb{C}$), because we can add or subtract two polynomials and get a polynomial, there is a zero polynomial, and we can multiply a polynomial by a scalar, and all the technical conditions above are satisfied.

For another example, let S be any set. Then the set of all functions from S to $\mathbb{R}$ is a vector space over $\mathbb{R}$! The zero vector is just the constant function sending every element of S to 0, we can add two functions f and g by the rule $(f+g)(s) = f(s) + g(s)$ for any s in S, and we can multiply any function f by a scalar λ by the rule $(\lambda f)(s) = \lambda(f(s))$ for any s in S. Exercise: check that the conditions of a vector space are satisfied.

As another example, let $\mathbb{F}_2$ be the integers modulo 2; if you don't know modular arithmetic, $\mathbb{F}_2$ is just the set containing two elements, 0 and 1, with addition defined as you would expect, except that $1 + 1 = 0$, and multiplication exactly as you would expect (exercise: check that $\mathbb{F}_2$ satisfies the conditions to be a field). Let V be the set of all messages of length n in binary; then V is a vector space over $\mathbb{F}_2$ (exercise: figure out what the zero vector, vector addition, and scalar multiplication should be, and check they satisfy the conditions of a vector space). This has important applications in computer science; if we want to send a message but are worried about errors in transmission, we can find a large vector space over $\mathbb{F}_2$, and take a subspace consisting of possible messages we might want to send, which are "spread out," so no two valid messages are close to each other (in some suitable sense of closeness, called the Hamming metric if you want to read up more on this). Then when we transmit, if errors are made, the receiving computer takes

the vector in V it receives and finds the closest element of the subspace of valild messages; this allows it to recover the (most probable) original message from the garbled message it receives.

Technically speaking, we should always specifiy the field when talking about a vector space. We should always say "vector space over F" (where F is some field), not just "vector space." However, often we have only one field we're interested in for a particular problem or application, so that just stays in the background; for instance, in our work on Fourier analysis, we will (to start with) work only over the field of real numbers, so when we say "vector space," we always mean "vector space over $\mathbb{R}$." In the book you sent me, "vector space" always means "vector space over $\mathbb{C}$," and we will probably switch to working over $\mathbb{C}$ in a week or two. I'll say when we start working with complex vector spaces instead of real ones; for now, always assume when I say "vector space" that it is over $\mathbb{R}$.