Numbers and Vector spaces

September 30, 2011

In the definition of a Vector space, multiplication of vectors by numbers is present. This note explains what we exactly mean by "numbers".

You are probably familiar with rational numbers, real numbers, and complex numbers. Here I explain what is "numbers" in general, for the purposes of Linear Algebra.

A *field* is a set F with two operations, called *addition* and *multiplication*. An "operation" means a rule which to every two elements of F puts into correspondence an element of F (their sum, or their product). The operations must have the following properties:

$$(x+y)+z = z+(y+z),$$
$$x+y = y+x,$$

There exits 0 in F such that

$$x+0 = x \quad \text{for every} \quad x \quad \text{in} \quad F,$$

For every x in F there exists a y in F such that

$$x+y = 0.$$

This y is denoted by $-x$.

These are the properties of addition.

$$(xy)z = x(yz),$$

$$xy = yx,$$

There exists an element $1 \neq 0$ in F such that

$$1 \cdot x = x \quad \text{for every} \quad x \quad \text{in} \quad F.$$

For every $x \neq 0$ in F there exists y in F such that

$$xy = 1.$$

This y is called x^{-1}. These are the properties of multiplication. Now the properties relating addition and multiplication:

$$x(y+z) = zy + xz.$$

This are all properties.

In general, "numbers" are elements of some field. Here are examples of fields.

1. Field of rational numbers, denoted by Q. Operations are defined as usual. You can check that all properties listed above are satisfied.

2. The set of all integers with usual operations of addition and multiplication *is not* a field. One of the properties of multiplication from the definition of the field does not hold. For an integer 2, there is no such integer y that $2y = 1$.

3. Field of real numbers, denoted by R. Operations are defined as usual. You can check that al properties listed above are satisfied.

4. Field of complex numbers, denoted by C. Complex numbers are expressions of the form $a + ib$, where a and b are real numbers. Operations are defined in the following way:

$$(a_1 + ib_1) + (a_2 + ib_2) = (a_1 + a_2) + i(b_1 + b_2).$$

$$(a_1 + ib_1)(a_2 + ib_2) = (a_1a_2 - b_1b_2) + i(a_1b_2 + a_2b_2).$$

Verify that all properties are satisfied. Of course, $0 = 0 + i0$ and $1 = 1 + i0$. Hint: $(a + ib)^{-1} = a/(a^2 + b^2) - ib/a^2 + b^2)$.

5. The next example is the simplest field of all. It contains only two elements 0 and 1. The operations are defined as follows:

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

$$0 \cdot 0 = 0, \quad 0 \cdot 1 = 1 \cdot 0 = 0, \quad 1 \cdot 1 = 1.$$

Verify that all properties hold.

6. This is a generalization of the previous example. Let p be a positive integer. Then every integer (positive or negative or zero!) n can be divided by p with remainder. Let us call this reminder $\bar{n}$. There are p possible reminders: $\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{p-1}$. We define a set F_p with two operations. The elements of F_p are reminders $\bar{0}, \ldots, \overline{p-1}$. So there are p elements. Addition is defined in the following way: $\bar{x} + \bar{y}$ is the reminder of the sum of $x + y$ considered as an integer. Product is defined similarly. For example, if $p = 2$, we obtain the same field as in example 5.

Let $p = 3$. Then we have 3 elements $0, 1, 2$, and here are some examples of addition and multiplication in F_3:

$$1 + 2 = 0, \quad 2 + 2 = 1, \quad 2 \cdot 2 = 1.$$

Verify that F_3 is a field.

Let $p = 4$. Then $2 \cdot 2 = 0$. Show that there is no $y \in F_4$ such that $2 \cdot y = 1$. So F_4 *is not a field.*

Verify that F_p is a field if and only if p is prime.

7. Rational functions are ratios of polynomials. Like $(x + 1)/(x^2 + 1)$. Strictly speaking, they are not functions on the real line, because the denominator can be zero at some point. Nevertheless it is clear what is a sum or product of two rational functions. Verify that all rational functions with rational (or real or complex) coefficients form a field (these are three different fields, of course). You can also consider rational functions with coefficients from F_q, or with coefficients from any field. They form a field.

There are infinitely many other examples. In linear algebra, "numbers" in the definition of a vector space can be elements of any field. When we wish to specify a field, we say "a vector space *over* such and such field". This indicates what numbers are we using to multiply vectors. We also can use the term F-vector space, where F is a field, meaning that the ubers used in the definition are elements of F. Of course, some properties of vector spaces depend on the field is used in their definition.

Examples.

A. Every field is a vector space (of dimension 1) over itself.

B. Real numbers form a vector space over rational numbers. Think, what is the dimension of this vector space.

C. Complex numbers form a vector space over real numbers. The dimension of this vector space is 2. A basis is $0 + 1 \cdot i$ and $1 + 0 \cdot i$. Complex numbers also make a complex vector space of dimension 1, see example A. This is a different vector space, though it consists of the same elements.

D. The set of all columns of n complex numbers with usual addition and multiplication is called C^n. It is a complex vector space of dimension n. It is also a real vector space of dimension $2n$ (find a basis!). It is also a rational vector space of dimension ∞. (I am not asking you to find a basis:-). So C^n can be a vector space in three ways. All these three spaced are *different*.

In this curse we will deal mainly with real vector spaces, just in few instances with complex ones.