AXIOMS FOR VECTOR SPACES
MATH 108A, March 28, 2010

Among the most basic structures of algebra are fields and vector spaces over fields. It is well worth the effort to memorize the axioms that define fields and vector spaces.

1 Field axioms

Definition. A *field* is a set F together with two operations (functions)

$$f : F \times F \to F, \qquad f(x, y) = x + y$$

and

$$g : F \times F \to F, \qquad g(x, y) = xy,$$

which satisfy the following axioms:

1. addition is commutative: $x + y = y + x$, for all $x, y \in F$.
2. addition is associative: $(x + y) + z = x + (y + z)$, for all $x, y, z \in F$.
3. existence of additive identity: there is an element $0 \in F$ such that $x + 0 = x$, for all $x \in F$.
4. existence of additive inverses: if $x \in F$, there is an element $-x \in F$ such that $x + (-x) = 0$.
5. multiplication is commutative: $xy = yx$, for all $x, y \in F$.
6. multiplication is associative: $(xy)z = x(yz)$, for all $x, y, z \in F$.
7. existence of multliplicative identity: there is an element $1 \in F$ such that $1 \neq 0$ and $x1 = x$, for all $x \in F$.
8. existence of multliplicative inverses: if $x \in F$ and $x \neq 0$, there is an element $(1/x) \in F$ such that $x(1/x) = 1$.
9. distributivity: $x(y + z) = xy + xz$, for all $x, y, z \in F$.

Example 1. Recall that a *rational number* is simply the ration of two integers. The set of rational numbers (denoted by $\mathbb{Q}$) is a field, when it is given the usual operations of addition and multiplication.

Example 2. The real numbers are the set of all numbers that can be expressed by infinite decimal expansions. Thus for example

$$\sqrt{2} = 1.41421356237309504880168872420969807857\ldots$$

is a real number. It is definitely NOT a rational number, because if

$$\sqrt{2} = \frac{m}{n}, \quad \text{then} \quad 2 = \frac{m^2}{n^2}.$$

We could then assume that m and n have no common factors. Since $m^2 = 2n^2$, m is even, say $m = 2r$. Then $4r^2 = 2n^2$ or $2r^2 = n^2$, so n is also even. But if m and n are both even, they have a common factor, a contradiction. Then $\sqrt{2}$ cannot be rational.

In fact, you learned in Math 8 that the set $\mathbb{R}$ of real numbers has uncountably many elements, while $\mathbb{Q}$ is countable, so $\mathbb{R}$ is a much larger set than $\mathbb{Q}$.

The set of real numbers $\mathbb{R}$ with the usual operations of addition and multiplication give us a second important example of field.

Example 3. Unfortunately, it is not possible to take the square roots of a negative real number and get a real number. This makes it impossible to find solutions to polynomial equations like

$$x^2 + 1 = 0.$$

In order to remedy this problem, we need introduce the complex numbers $\mathbb{C}$. We can regard a complex number as a 2×2 matrix of the form

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix},$$

where a and b are real numbers. Although matrix do not commute in general, it is the case that

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} c & -d \\ d & c \end{pmatrix} \begin{pmatrix} a & -b \\ b & a \end{pmatrix},$$

for any choice of a, b, c and d,as you can verify by direct multiplication. We often use the notation

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad i = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

so that

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} = a + bi.$$

The set $\mathbb{C}$ of complex numbers is a field under matrix addition and matrix multiplication. Needless to say, it is indispensable for solving differential equations, as you may have seen.

Example 4. Suppose that p is a prime, and let $\mathbb{Z}_p$ be the set

$$\{0, 1, 2, \ldots, p-1\}$$

with addition and multiplication modulo p. Thus to add or multiply two elements of $\mathbb{Z}_p$, you simply take the ordinary sum or product and then subtract a suitable integer multiple of p to get back into the set $\mathbb{Z}_p$. Can you figure out why $\mathbb{Z}_p$ is NOT a field when p is not a prime?

2 Vector space axioms

Definition. Suppose that F is a field. A *vector space* over F is a set V together with two operations (functions)

$$f : V \times V \to V, \qquad f(\mathbf{v}, \mathbf{w}) = \mathbf{v} + \mathbf{w}$$

and

$$g : F \times V \to V, \qquad g(a, \mathbf{v}) = a\mathbf{v},$$

called vector addition and scalar multiplication, which satisfy the following axioms:

1. vector addition is commutative: $\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$, for all $\mathbf{u}, \mathbf{v} \in V$.
2. vector addition is associative: $(\mathbf{u}+\mathbf{v})+\mathbf{w} = \mathbf{u}+(\mathbf{v}+\mathbf{w})$, for all $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$.
3. existence of additive identity: there is an element $\mathbf{0} \in V$ such that $\mathbf{v}+\mathbf{0} = \mathbf{v}$, for all $\mathbf{v} \in V$.
4. existence of additive inverses: if $\mathbf{v} \in V$, there is an element $\mathbf{w} \in V$ such that $\mathbf{v} + \mathbf{w} = \mathbf{0}$.
5. scalar multiplication is associative: $(ab)\mathbf{v} = a(b\mathbf{v})$, for all $a, b \in F$, $\mathbf{v} \in V$.
6. multliplicative identity: $1\mathbf{v} = \mathbf{v}$, for all $\mathbf{v} \in V$.
7. distributivity 1: $a(u + \mathbf{v}) = a\mathbf{u} + a\mathbf{v}$, for all $a \in F$, $\mathbf{u}, \mathbf{v} \in V$.
8. distributivity 2: $(a + b)\mathbf{v} = a\mathbf{v} + b\mathbf{v}$ for all $a, b \in F$, $\mathbf{v} \in V$.

A vector space over the field $\mathbb{Q}$ is called a *rational vector space*. A vector space over $\mathbb{R}$ is called a *real vector space*. A vector space over $\mathbb{C}$ is called a *complex vector space*.

Example 1. If F is a field and n is a positive integer, we let F^n denote the set of lists of elements of F of length n. If

$$\mathbf{x} = (x_1, \ldots, x_n) \qquad \text{and} \qquad \mathbf{y} = (y_1, \ldots, y_n)$$

are elements of F^n, we define vector addition by

$$\mathbf{x} + \mathbf{y} = (x_1 + y_1, \ldots, x_n + y_n).$$

If $a \in F$, we define scalar multiplication by

$$a\mathbf{x} = (ax_1, \ldots, ax_n).$$

You have already encountered the vector space $\mathbb{R}^n$ over $\mathbb{R}$ in Math 3ABC and 5A. But the vector space $\mathbb{C}^n$ over $\mathbb{C}$ is equally important in applications.

Example 2. If F is a field, we can also let F^∞ be the set of infinite sequences of elements of F. If

$$\mathbf{x} = (x_1, x_2, \ldots) \qquad \text{and} \qquad \mathbf{y} = (y_1, y_2, \ldots)$$

are elements of F^∞, we define vector addition by

$$\mathbf{x} + \mathbf{y} = (x_1 + y_1, x_2 + y_2, \ldots).$$

If $a \in F$, we define scalar multiplication by

$$a\mathbf{x} = (ax_1, ax_2, \ldots).$$

Example 3. Suppose that $F = \mathbb{R}$ and let

$$V = \{ \text{ functions } f : \mathbb{R} \to \mathbb{R} \ \}.$$

If f and g are elements of V and $a \in \mathbb{R}$, we can define vector addition $f + g$ and scalar multiplication af by

$$(f + g)(t) = f(t) + g(t), \qquad (af)(t) = af(t).$$

One can check that these operations satisfy the axioms for a vector space over $\mathbb{R}$. Needless to say, this is an important vector space in calculus and the theory of differential equations.

Remark. an obvious advantage to proving theorems for general vector spaces over arbitrary fields is that the resulting theorems apply all of the cases at once.