1111: Linear Algebra I

Dr. Vladimir Dotsenko (Vlad)

Lecture 16

Consequences of properties of vector operations

The properties 1-8 altogether allow to operate with elements of V as though they were vectors in $\mathbb{R}^n$, that is create linear combinations, take summands in an equation from the left hand side to the right hand side with opposite signs, collect similar terms etc. For that reason, we shall refer to elements of an abstract vector space as vectors, and to real numbers as scalars.

These properties also allow to prove various theoretical statements about vectors. There will be some of those in your next homework, and for now let me give several examples.

Lemma 1. *For all $v \in V$, we have $0 \cdot v = 0$.*

Proof. Denote $u = 0 \cdot v$. We have $u+u = 0 \cdot v + 0 \cdot v = (0+0) \cdot v = 0 \cdot v = u$ (we used property 6 in the middle equality). But now we can "subtract u from both sides": $(u + u) + (-u) = u + (-u) = 0$ (property 4). Finally, $(u+u)+(-u) = u+(u+(-u)) = u+0 = u$ (properties 1, 4, and 3). We conclude that $u = 0$. □

The following lemma proved similarly with property 5 instead of property 6:

Lemma 2. *For all $c \in \mathbb{R}$, we have $c \cdot 0 = 0$.*

Let us prove another statement that is sometimes useful.

Lemma 3. *Suppose that for a scalar c and a vector v we have $c \cdot v = 0$. Then $c = 0$ or $v = 0$.*

Proof. If $c = 0$ there is nothing to prove. Suppose $c \neq 0$. Then $0 = c^{-1} \cdot 0 = c^{-1}(c \cdot v) = (c^{-1}c)v = 1 \cdot v = v$ (by Lemma 2 above, and properties 7 and 8). Therefore, $v = 0$, as required. □

Fields

It is also worth mentioning that sometimes we shall use other scalars, not just real numbers. In order for all the arguments to work, we need that scalars have arithmetics similar to that of real numbers. Let us be precise about what that means.

Definition 1. A *field* is a set F equipped with the following data:

- a rule assigning to each elements $f_1, f_2 \in F$ an element of F denoted $v_1 + v_2$, and
- a rule assigning to each elements $f_1, f_2 \in F$ an element of F denoted $f_1 \cdot f_2$ (or sometimes $f_1 f_2$),

for which the following properties are satisfied:

1. for all $f_1, f_2, f_3 \in F$ we have $(f_1 + f_2) + f_3 = f_1 + (f_2 + f_3)$,
2. for all $f_1, f_2 \in F$ we have $f_1 + f_2 = f_2 + f_1$,
3. there is a designated element of F denoted by 0 for which $0 + f = f + 0 = f$ for all f,
4. for each $f \in F$, there exists $g \in F$, denoted $-f$ and called *the opposite of* f, such that $f+(-f) = (-f)+f = 0$,
5. for all $f_1, f_2, f_3 \in F$ we have $(f_1 f_2) f_3 = f_1(f_2 f_3)$,

6. for all $f_1, f_2 \in F$ we have $f_1 f_2 = f_2 f_1$,
7. there is a designated element of F denoted by 1 for which $1 \cdot f = f \cdot 1 = f$ for all f,
8. for each $f \neq 0 \in F$, there exists $g \in F$, denoted f^{-1} and called *the inverse of* f, such that $ff^{-1} = f^{-1}f = 1$,
9. for all $f_1, f_2, f_3 \in F$, we have $f_1 \cdot (f_2 + f_3) = f_1 \cdot f_2 + f_1 \cdot f_3$.

Example 1. The field of rational numbers $\mathbb{Q}$ consists of fractions with integer numerator and integer nonzero denominator (like $1/2$, $-5/3$, etc.).

Example 2. The field of real numbers $\mathbb{R}$ is our main example of a field; I assume that you know what it stands for.

Example 3. The field of complex numbers $\mathbb{C}$ consists, as you know, of expressions $a + bi$, where $a, b \in \mathbb{R}$ with obvious addition and multiplication that is completely defined by the rule $i^2 = -1$.

Example 4. An example which is absolutely foundational for computer science is the binary arithmetic: $\mathbb{F}_2 = \{\bar{0}, \bar{1}\}$ with the operations $\bar{0} + \bar{0} = \bar{1} + \bar{1} = \bar{0}$, $\bar{0} + \bar{1} = \bar{1} + \bar{0} = \bar{1}$, $\bar{0} \cdot \bar{0} = \bar{0} \cdot \bar{1} = \bar{1} \cdot \bar{0} = \bar{0}$, $\bar{1} \cdot \bar{1} = \bar{1}$.

Given a field F, one can consider vector spaces over F, that is vector spaces where elements of F play the role of scalars. The flexibility of choosing scalars for the vector space can sometimes be very useful.

Coin weighing problem

Let us look at the following question.

> Given 101 coins of various shapes and denominations, one knows that if you remove any one coin, the remaining 100 coins can be divided into two groups of 50 of equal total weight. Show that all the coins are of the same weight.

Let us prove this in several steps. An important observation that we shall use many times is that if $x_1, \ldots, x_{101}$ are weights of the coins satisfying our assumption, then $x_1 + k$, $\ldots$, $x_{101} + k$ are weights that also satisfy our assumption, and lx_1, $\ldots$, lx_{101} are weights that also satisfy our assumption, for all k and l.

Let us suppose that weights are not all equal to each other.

First, we consider the case when all weights $x_1, \ldots, x_{101}$ of all coins are positive integers. Then among all the lists of weights which are not all equal to each other, let us choose the list with the least possible total weight.

Lemma 4. *The weights of the coins are either all even or all odd.*

Proof. Denote $S = x_1 + \cdots + x_{101}$. Then $S - x_i$ is divisible by 2 for all i, because we can split all coins except for the coin number i into two groups of equal total weight, so $S - x_i$ is twice that weight. Therefore, $x_i - x_j = (S - x_j) - (S - x_i)$ is divisible by 2 also. $\square$

If all the weights are even, we can divide them by 2, and get a set of coins satisfying our assumption of smaller total weight. If all the weights are odd, we can subtract 1 from each, and get a set of coins satisfying our assumptions of smaller total weight. In either case we get a contradiction with the minimality of the total weight in our set.

Second, we suppose all weights are rational. Then, multiplying by common denominator, we get a set of coins satisfying our assumptions where all weights are integers, and adding to all weights a large integer N we can ensure that they are positive, and we are back to the case we already dealt with.

Finally, suppose weights are arbitrary real numbers. Note that the conditions we impose can be expressed as a system of linear equations with rational coefficients! Saying that there is a solution where not all weights are equal is essentially saying that if we let $x_1 = 1$, there is a solution where not all coordinates are equal to 1, so this system of equations has at least 2 solutions. But this is a property that "does not depend on scalars", — whether we view our system of equations as a system with rational coefficients or with real coefficients, we do the same, compute the reduced row echelon form. If there is a solution different from the solution $x_1 = x_2 = \cdots = x_{101} = 1$ over real numbers, there must be free unknowns! Setting all these free unknowns equal to zero, we shall obtain a solution with rational coordinates where not all coordinates are equal. But we already proved that the latter was impossible.