CLARK
UNIVERSITY

Kinds of proofs
Math 225 Modern Algebra

D Joyce, Fall 2017

Kinds of proofs. In linear algebra you looked at some of the theorems that come from the axioms for vector spaces. For reference, here are the eight axioms for vector spaces.

a. Vector addition is commutative: $\mathbf{v}+\mathbf{w}=\mathbf{w}+\mathbf{v}$
b. Vector addition is associative: $(\mathbf{u}+\mathbf{v})+\mathbf{w}=\mathbf{u}+(\mathbf{v}+\mathbf{w})$
c. There is a vector, denoted $\mathbf{0}$ such that $\mathbf{v}+\mathbf{0}=\mathbf{v}=\mathbf{0}+\mathbf{v}$
d. For each $\mathbf{v}$, there is another vector $-\mathbf{v}$ such that $\mathbf{v}+(-\mathbf{v})=\mathbf{0}$
e. Scalar multiplication distributes over vector addition: $c(\mathbf{v}+\mathbf{w})=c\mathbf{v}+c\mathbf{w}$
f. Scalar multiplication distributes over real addition: $(c+d)\mathbf{v}=c\mathbf{v}+d\mathbf{v}$
g. Multiplication and scalar multiplication associate: $c(d\mathbf{v})=(cd)\mathbf{v}$
h. 1 acts as the identity for scalar multiplication: $1\mathbf{v}=\mathbf{v}$

In linear algebra you looked at some of the theorems that follow from these axioms.

The theorem $0\mathbf{v}=\mathbf{0}$. One of the first theorems states that $0\mathbf{v}=\mathbf{0}$ for all vectors $\mathbf{v}$. We'll look at three forms of that proof. They're essentially the same proof, but they look different. Even in a proof as straightforward as this one, some insight is needed to get started, and for this one, it's $0+0=0$, a fact of real numbers, or, for that matter, any field. The first proof is in the standard form you see in college textbooks and in research mathematics, but with a couple extra comments inserted.

Proof. Since $0+0=0$, therefore $(0+0)\mathbf{v}=0\mathbf{v}$. By axiom f, that implies $0\mathbf{v}+0\mathbf{v}=0\mathbf{v}$. If we could subtract $0\mathbf{v}$ from each side, we'd be done, but subtraction isn't yet defined. Still, we can add the negation of $0\mathbf{v}$ to each side which should accomplish about the same thing. Thus,

$$(0\mathbf{v}+0\mathbf{v})+(-0\mathbf{v})=0\mathbf{v}+(-0\mathbf{v}).$$

Next, we can associate the paretheses differently by axiom b to get

$$0\mathbf{v}+(0\mathbf{v}+(-0\mathbf{v}))=0\mathbf{v}+(-0\mathbf{v}).$$

That equation simplifies by axiom d to $0\mathbf{v}+\mathbf{0}=\mathbf{0}$, and by axiom c, that further simplifies to $0\mathbf{v}=\mathbf{0}$ which is what was to be proved. Q.E.D.

Next, let's look at the same proof but in a different form. It's called a two-column proof where the statements in the left column are justified in the right column. You've probably seen this kind of proof in plane geometry courses. It's main advantage is that it requires justification for every statement. It's also pretty easy to read and follow.

1. $0 = 0 + 0$	Property of $\mathbf{R}$
2. $0\mathbf{v} + 0\mathbf{v} = 0\mathbf{v}$	Line 1 and axiom f
3. $(0\mathbf{v} + 0\mathbf{v}) + (-0\mathbf{v}) = 0\mathbf{v} + (-0\mathbf{v})$	Line 2
4. $0\mathbf{v} + (0\mathbf{v} + (-0\mathbf{v})) = 0\mathbf{v} + (-0\mathbf{v})$	Line 3 and axiom b
5. $0\mathbf{v} + \mathbf{0} = \mathbf{0}$	Line 4 and axiom d
6. $0\mathbf{v} = \mathbf{0}$	Line 5 and axiom c

Some proofs can be made entirely equational, that is, one long continued equation. They're easy to check, but they have to be constructed from other proofs. When you read one you're often puzzled as to where it came from. Here's what this one looks like as an equation where each equality has an associated justification.

$$\begin{array}{rcll} 0\mathbf{v} & = & 0\mathbf{v} + \mathbf{0} & \text{by axiom c} \\ & = & 0\mathbf{v} + (0\mathbf{v} + (-0\mathbf{v})) & \text{by axiom d} \\ & = & 0(\mathbf{v} + 0\mathbf{v}) + (-0\mathbf{v}) & \text{by axiom b} \\ & = & (0+0)\mathbf{v} + (-0\mathbf{v}) & \text{by axiom f} \\ & = & 0\mathbf{v} + (-0\mathbf{v}) & \text{property of } \mathbf{R} \\ & = & \mathbf{0} & \text{by axiom d} \end{array}$$

The theorem $(-1)\mathbf{v} = -\mathbf{v}$. Another early theorem says that

$$(-1)\mathbf{v} = -\mathbf{v}$$

for every vector $\mathbf{v}$. This is not an automatic statement. The left side of the equation is the product of a scalar and a vector while the right side is a vector whose sum with $\mathbf{v}$ yields $\mathbf{0}$.

If we added $\mathbf{v}$ to each side, we would have

$$\mathbf{v} + (-1)\mathbf{v} = \mathbf{v} + (-\mathbf{v}).$$

The left side, by use of the axioms, can be written $1\mathbf{v} + (-1)\mathbf{v} = (1 + (-1))\mathbf{v} = 0\mathbf{v}$, which equals, by the previous thereom, $\mathbf{0}$, while the right side, by one of the axioms, also equals $\mathbf{0}$. If we could just reverse the steps, we'd have a proof of the theorem.

Here's such a proof in the 2-column form, but I couldn't create it without doing the analysis just described.

1. $(-1) + 1 = 0$	Property of $\mathbf{R}$
2. $(-1)\mathbf{v} + 1\mathbf{v} = 0\mathbf{v}$	Line 1 and axiom f
3. $(-1)\mathbf{v} + \mathbf{v} = \mathbf{0}$	Line 2, axiom h, and the previous theorem
4. $(-1)\mathbf{v} + \mathbf{v} + (-\mathbf{v}) = \mathbf{0} + (-\mathbf{v})$	Line 3 and, implicitly, axiom b
5. $(-1)\mathbf{v} + \mathbf{0} = \mathbf{0}$	Line 4 and axioms d and c
6. $(-1)\mathbf{v} = -\mathbf{v}$	Line 5 and axiom c

Math 225 Home Page at `http://math.clarku.edu/~djoyce/ma225/`