

Abstract proofs

A student asked me, “What does the star mean in the statement and proof of Theorem 11.3.2?”

By way of a roundabout answer, I ask you to first consider the following two proofs:

Theorem: The only identity element in the group $[\mathbb{R}; +]$ is 0.

Proof (indirect): Suppose $r \in \mathbb{R}$, $r \neq 0$, and r is an identity of $[\mathbb{R}; +]$. We'll show that $r = 0$, which is a contradiction, completing the proof.

$$\begin{aligned} r &= r + 0 && \text{since } 0 \text{ is an identity} \\ &= 0 && \text{since } r \text{ is an identity} \end{aligned}$$

which is the required contradiction.

Theorem: The only identity element in the group $[\mathbb{R}^*; \times]$ is 1.

Proof (indirect): Suppose $s \in \mathbb{R}^*$, $s \neq 1$, and s is an identity of $[\mathbb{R}^*; \times]$. We'll show that $s = 1$, which is a contradiction, completing the proof.

$$\begin{aligned} s &= s \times 1 && \text{since } 1 \text{ is an identity} \\ &= 1 && \text{since } s \text{ is an identity} \end{aligned}$$

which is the required contradiction.

At a conceptual level, it's the same proof in a new guise.

Mathematicians don't like writing the same proof over and over; instead, they try to prove one theorem that's so general that it covers all the individual cases. In this instance, we can give a proof that applies not just to the group $[\mathbb{R}; +]$ or the group $[\mathbb{R}^*; \times]$ but to *any* group.

Theorem: Suppose $[G; *]$ is any group, with identity element e . Then the only identity element in the group is e .

Proof (indirect): Suppose that $f \in G$, $f \neq e$, and f is an identity of $[G; *]$. We'll show that $f = e$, which is a contradiction, completing the proof.

$$\begin{aligned} f &= f * e && \text{since } e \text{ is an identity} \\ &= e && \text{since } f \text{ is an identity} \end{aligned}$$

which is the required contradiction.

Now perhaps Theorem 11.3.2 makes more sense. In particular, my reply to the question “What does $*$ mean in the statement of the theorem?” is, Pretty much whatever you want it to be, as long as it satisfies all the axioms of a group! Could $*$ mean addition of real numbers? Yup. Could $*$ mean multiplication of nonzero real numbers? Yup. (Could it mean subtraction of real numbers? Nope, because for one thing subtraction isn’t associative!) In any context where the axioms of group theory hold, the theorems of group theory apply as well, one of which is Theorem 11.3.2.