Mathematical Reasoning

Chapter 6. Number Theory

6.1. Operations—Proofs of Theorems

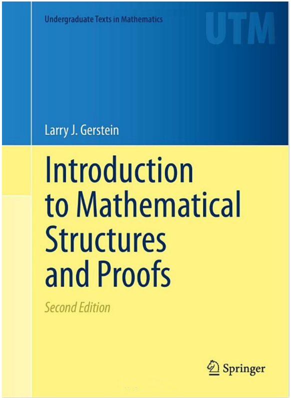

Table of contents

Theorem 6.4

Theorem 6.4. An operation has at most one identity.

Proof. Suppose binary operation $*$ has more than one identity, say e and e_1 are identities. Then $e * e_1 = e_1$ since e is an identity. Also, $e * e_1 = e$ since e_1 is an identity. Therefore, $e_1 = e * e_1 = e$ and so any two identities are actually equal. That is, $*$ has at most one identity, as claimed. $\square$

Theorem 6.4

Theorem 6.4. An operation has at most one identity.

Proof. Suppose binary operation $*$ has more than one identity, say e and e_1 are identities. Then $e * e_1 = e_1$ since e is an identity. Also, $e * e_1 = e$ since e_1 is an identity. Therefore, $e_1 = e * e_1 = e$ and so any two identities are actually equal. That is, $*$ has at most one identity, as claimed. $\square$

Theorem 6.6

Theorem 6.6. Suppose $*$ is an associative operation on S with identity e. If an element $a \in S$ has an inverse, then it has only one inverse.

Solution. Suppose element a has more than one inverse, say b and c. Then

$$\begin{aligned} b &= b * e \text{ since } e \text{ is the identity} \\ &= b * (a * c) \text{ because } a * c = e \text{ since } c \text{ is an inverse of } a \\ &= (b * a) * c \text{ by associativity} \\ &= e * c \text{ because } b * a = e \text{ since } b \text{ is an inverse of } a \\ &= c \text{ since } e \text{ is the identity.} \end{aligned}$$

So $b = c$ and any two inverses of a are equal. That is, a has only one inverse, as claimed. $\square$

Theorem 6.6

Theorem 6.6. Suppose $*$ is an associative operation on S with identity e. If an element $a \in S$ has an inverse, then it has only one inverse.

Solution. Suppose element a has more than one inverse, say b and c. Then

$$\begin{aligned} b &= b * e \text{ since } e \text{ is the identity} \\ &= b * (a * c) \text{ because } a * c = e \text{ since } c \text{ is an inverse of } a \\ &= (b * a) * c \text{ by associativity} \\ &= e * c \text{ because } b * a = e \text{ since } b \text{ is an inverse of } a \\ &= c \text{ since } e \text{ is the identity.} \end{aligned}$$

So $b = c$ and any two inverses of a are equal. That is, a has only one inverse, as claimed. □