Exercise

On the set $\mathbf{Z}^+$ (positive integers), there are two natural binary operations $\mathbf{Z}^+ \times \mathbf{Z}^+ \to \mathbf{Z}^+$: namely, addition and multiplication.

1. Is the binary operation of addition an injective function? surjective function?
   Not injective: for example, $1 + 3 = 2 + 2$.
   Not surjective, because 1 is not the sum of any two positive integers.
   But if we changed the set to be all nonnegative integers, then addition would be surjective.
2. Is the binary operation of multiplication an injective function? surjective function?
   Not injective: for example $2 \times 2 = 1 \times 4$.
   Surjective because for every positive integer n, we have $1 \times n = n$, so n is in the image.

Exercise

Suppose $*$ is a binary operation on a set A. Write with quantifiers the *negation* of each of the following statements.

1. The binary operation $*$ is commutative.
   Negation: There exist elements a and b such that $a * b \neq b * a$.
2. The binary operation $*$ is associative.
   Negation: There exist elements a, b, and c such that $(a * b) * c \neq a * (b * c)$.
3. The element e of A is an identity element with respect to $*$.
   Negation: There exists an element a such that either $e * a \neq a$ or $a * e \neq a$.
4. The element a of A is invertible with respect to $*$.
   Negation, assuming that an identity element e exists: For every element b, either $a * b \neq e$ or $b * a \neq e$.

A puzzle

Suppose $*$ is a commutative and associative binary operation on the four-element set $\{a, b, c, d\}$, and $*$ has an identity element, and every element is invertible with respect to $*$. Complete the table:

$*$	a	b	c	d
a	c			
b		c		
c			c	
d				

Sketch of solution: Since a is invertible, multiplication by a is an injective function from A to A. An injective function from a finite set to itself is necessarily a bijection. Therefore the first row is a permutation of the four letters; so is the first column; similarly for each row and column. Since $c * c = c$, multiplying by c^{-1} shows that $c = e$, the identity; so the third row and third column are determined. Proceed as in solving sudoku.

Answer to the puzzle

$*$	a	b	c	d
a	c	d	a	b
b	d	c	b	a
c	a	b	c	d
d	b	a	d	c

A *group* is the technical term for a set equipped with an associative binary operation that has an identity element and additionally has the property that every element is invertible.

If the binary operation is commutative too, then the group is called *abelian* [after Niels Henrik Abel (1802–1829)].