Definition (Axiom): An axiom is an statement or proposition which is being regarded as being established, accepted or self-evidently true.

The mathematician Peano (1858-1932) elaborated the whole theory of numbers starting from three axioms, known as Peano's Axioms. They characterize the set of natural numbers.

Peano's Axioms:

The set $\mathbb{N}$ of natural numbers is characterized by the following axioms:

(1) There exists an injective function $S : \mathbb{N} \to \mathbb{N}$.
The image $S(n)$ of each natural number $n \in \mathbb{N}$ is called the successor of n.

(2) There exists an element $1 \in \mathbb{N} \setminus S(\mathbb{N})$

(3) (Induction) If $A \subseteq \mathbb{N}$ is such that $1 \in A$ and $S(A) \subseteq A$, then $A = \mathbb{N}$

This last property is saying that any subset of $\mathbb{N}$ which contains 1 and the successor of all its elements is equal to $\mathbb{N}$.
In other words, every element in $\mathbb{N}$ can be obtained from 1 by iterating the function S.

Informally, the induction property says that
$\mathbb{N} = \{1, S(1), S(S(1)), S(S(S(1))), \dots\}$.

Observation: 1 is the unique element in $\mathbb{N} \setminus S(\mathbb{N})$.

Indeed, let $A = \{1\} \cup S(\mathbb{N}) \subseteq \mathbb{N}$.

We have $1 \in A$. Let $n \in A$. Note that $S(n) \in S(\mathbb{N}) \subseteq A$. Thus, we obtain $S(n) \in A$. By Axiom 3, $A = \mathbb{N}$ and hence $\mathbb{N} \setminus S(\mathbb{N}) = \{1\}$.

Induction is used to construct functions recursively.
In particular, we can define what is sum.

Definition (Sum) We define $n+1 := S(n)$ for every $n \in \mathbb{N}$
Recursively, $n + S(k) := S(n+k)$ for all $n, k \in \mathbb{N}$
(for which $n+k$ was already defined).

Therefore, $k+1$ is the successor of k. If we know $k+n$, we know $k+S(n)$: by definition, we have $k+S(n) = S(k+n)$. This allows us to know $k+n$ for every $n \in \mathbb{N}$ and $k \in \mathbb{N}$.

(Observe that we don't know yet any of the properties such as associativity or commutativity)

Definition (Product) We define $n \cdot 1 := n$ for every $n \in \mathbb{N}$ and $n \cdot S(k) := n \cdot k + n$.

↑ As we have already defined sum, we could write $n \cdot (k+1) := n \cdot k + n$.

Now we need to show that the following properties hold:

Associativity: $m + (n+k) = (m+n) + k$ and
$m \cdot (n \cdot k) = (m \cdot n) \cdot k \quad \forall\, m, n, k \in \mathbb{N}$.

Distributivity: $m \cdot (n+k) = m \cdot n + m \cdot k \quad \forall\, m, n, k \in \mathbb{N}$

Comutativity: $m + n = n + m$ and $m \cdot n = n \cdot m \quad \forall\, m, n \in \mathbb{N}$.

Cancellation law: $m+p = n+p \Rightarrow m = n$; $m \cdot p = n \cdot p \Rightarrow m = n$
$\forall\, m, n, p \in \mathbb{N}$.

We will prove a few of these properties and leave the others as an exercise.

Associativity of the sum: we will prove it by induction on K.

$$m+(n+1) = m+S(n) = S(m+n) = (m+n)+1$$

This implies that the property holds for $K=1$.

Let $A = \{K \in \mathbb{N} : m+(n+K) = (m+n)+K \quad \forall\, m,n \in \mathbb{N}\}$.

Let $K \in A$. Our goal is to show that $K+1 \in A$, because this implies $A = \mathbb{N}$ by the axiom of induction.

In other words, suppose our property holds for K:

$$m+(n+K) = (m+n)+K \quad \forall\, m,n \in \mathbb{N}.$$

(This is usually called induction hypothesis, or base of induction)

Then, we have

$$m+(n+S(K)) \overset{\text{def}}{=} m+S(n+K) \overset{\text{def}}{=} S(m+(n+K))$$
$$\overset{\text{I.H.}}{=} S((m+n)+K)$$
$$= (m+n)+S(K)$$

Therefore, $S(K) \in A$. This is usually called the induction step.

By the induction axiom, we have $A = \mathbb{N}$. ∎

Distributivity: we will prove by induction on K that

$$m\cdot(n+K) = m\cdot n + m\cdot K \quad \forall\, m,n \in \mathbb{N}.$$

By definition, it holds for $K=1$:

$$m\cdot(n+1) = m\cdot n + m = m\cdot n + m\cdot 1$$

$\forall\, m,n \in \mathbb{N}$.

Induction hypothesis: suppose our property holds for k:

$$m(n+k) = m \cdot n + m \cdot k \qquad \forall\, m, n \in \mathbb{N}.$$

Note that

$$\begin{aligned} m \cdot \big(n + (k+1)\big) &= m \cdot \big((n+k)+1\big) \\ &\overset{\text{def}}{=} m \cdot (n+k) + m \\ &\overset{\text{I.H.}}{=} (m \cdot n + m \cdot k) + m \\ &\overset{\text{Assoc.}}{=} m \cdot n + (m \cdot k + m) \\ &\overset{\text{Def}}{=} m \cdot n + m \cdot (k+1) \end{aligned}$$

Therefore, the property holds for $k+1$ and hence it holds for every natural number.