Associativity of addition of natural numbers from Peano axioms

We want to prove the following statement:

\[ a, b, c \in \mathbb{Z}^+ \Rightarrow (a + b) + c = a + (b + c) \]  

(1)

We shall use the Peano definition of the set of natural numbers i.e. defined as a set \( \mathbb{N} \) with a distinguished element \( 1 \in \mathbb{N} \) and an injective map \( s : \mathbb{N} \rightarrow \mathbb{N} \) such that \( 1 \) does not belong to \( s(\mathbb{N}) \) and such that the following induction axiom \((\text{ind})\) is satisfied:

\[(\text{ind}) \text{ If } A \subseteq \mathbb{N} \text{ such that } 1 \in \mathbb{N} \text{ and } a \in A \Rightarrow s(a) \in A \text{ then } A = \mathbb{N}.
\]

In such a set \( \mathbb{N} \) one defines addition of \( b \in \mathbb{N} \) to \( a \in \mathbb{N} \) so that the following two properties are satisfied:

(i) \( a + 1 = s(a) \)

(ii) If \( a + b \) is defined, then \( a + (b + 1) \) is defined as \( s(a + b) \).

Note that the set \( B \) of \( b \in \mathbb{N} \) for which \( a + b \) is defined contains \( 1 \) and by (ii) if \( b \in B \) then \( b + 1 \in B \). Therefore, by (ind) \( B = \mathbb{N} \) and hence \( a + b \) is defined for all \( a, b \in \mathbb{N} \).

We shall prove the identity (1) using induction over \( c \) i.e. we show that the set \( C \) defined as subset of \( \mathbb{N} \) consisting of \( c \in \mathbb{N} \) for which (1) is true is equal to the set \( \mathbb{N} \) (this is the same as to say that (1) is true for any \( c \in \mathbb{N} \)).

Claim 1: \( 1 \in C \) i.e. associativity takes place for \( c = 1 \) i.e.

\[ (a + b) + 1 = a + (b + 1) \]

Indeed, LHS by part (i) of definition of addition is \( s(a + b) \) and RHS is \( s(a + b) \) by part (ii). Hence both sides are the values of function \( s \) at \( a + b \) and hence are equal (by definition of a function).

Claim 2: if \( (a + b) + c = a + (b + c) \) then \( (a + b) + (c + 1) = a + (b + (c + 1)) \).

Indeed

\[ (a + b) + (c + 1) = s((a + b) + c) \]  

(by (ii) in definition of addition)

\[ = s(a + (b + c)) \]  

(by assumption of Claim 2)

\[ = a + ((b + c) + 1) \]  

(by (ii) of definition of addition)

\[ = a + (b + (c + 1)) \]  

(by Claim 1 i.e. associativity of addition when last summand equals 1)

QED.