Proof of the principle of mathematical induction

First recall the well-ordering axiom:

Axiom 16 (WO). $\boxed{\big(S \subseteq \mathbb{N}\big) \wedge \big(S \neq \emptyset\big) \Rightarrow \big(\exists\, m \in S\ \forall x \in S \quad m \leq x\big)}$

In the above statement of Axiom 16 we used a common convention that the exclusive disjunction $(m < x) \oplus (m = x)$ is abbreviated as $m \leq x$.

In the next theorem the universe of discourse is the set $\mathbb{Z}_+$ of positive integers.

Theorem 1. Let $P(n)$ be a propositional function involving a positive integer n. Then

$$\boxed{P(1) \wedge \Big(\forall\, k\ \big(P(k) \Rightarrow P(k+1)\big)\Big)} \;\Rightarrow\; \boxed{\forall\, n\ P(n)}$$

Proof. We will prove the contrapositive:

$$\boxed{\exists\, j\ \neg P(j)} \;\Rightarrow\; \boxed{\neg P(1) \vee \Big(\exists\, k\ \big(P(k) \wedge \neg P(k+1)\big)\Big)} \tag{1}$$

Assume $\boxed{\exists\, j\ \neg P(j)}$. That is, assume that there exists $j \in \mathbb{Z}_+$ such that $\neg P(j)$. Now consider the set

$$S = \big\{ n \in \mathbb{Z}_+ \,|\, \neg P(n) \big\}.$$

Clearly $S \subseteq \mathbb{Z}_+$ and $j \in S$. Therefore $S \subseteq \mathbb{N}$ and $S \neq \emptyset$. Hence

$$\boxed{\big(S \subseteq \mathbb{N}\big) \wedge \big(S \neq \emptyset\big)}$$

is true. By the well-ordering axiom we conclude

$$\boxed{\exists\, m \in S\ \forall x \in S\ m \leq x} \tag{2}$$

It is important to note that such m is called a *minimum* of S.

Next we make two observations about the proposition (2). First, we notice that the proposition

$$\forall x \in S \quad m \leq x$$

is equivalent to

$$\forall x \quad x \in S \Rightarrow m \leq x,$$

which is further equivalent to

$$\forall x \quad x < m \Rightarrow x \notin S.$$

Thus (2) is equivalent to

$$\boxed{\exists\, m \in S \;\; \forall\, x \; \big(x < m \Rightarrow x \notin S\big)} \tag{3}$$

Second, we notice that $m \in \mathbb{Z}_+$. Therefore, $(m = 1) \oplus (1 < m)$. In other words, there are two cases for m: either $m = 1$ or $m > 1$. Consider these two cases separately.

Case 1. Assume $\boxed{m = 1}$. Then, since $\boxed{m = 1 \in S}$, we have that $\boxed{\neg P(1)}$ is true. Consequently,

$$\boxed{\neg P(1) \vee \Big(\exists\, k \; \big(P(k) \wedge \neg P(k+1)\big)\Big)}$$

is true. Thus, we have proved the implication (1) in this case.

Case 2. Assume $\boxed{m > 1}$. Then $m - 1 > 0$ and thus $m - 1 \in \mathbb{Z}_+$. Define $k = m - 1$. Then $\boxed{k \in \mathbb{Z}_+}$. Further, since $\boxed{k < m}$, (3) implies $\boxed{k \notin S}$. Since $n \in S$ is equivalent to $(n \in \mathbb{Z}_+) \wedge (\neg P(n))$, $\boxed{k \notin S}$ is equivalent to $\boxed{\big(k \notin \mathbb{Z}_+\big) \vee P(k)}$. Since $\boxed{k \in \mathbb{Z}_+}$, the last disjunction implies that $\boxed{P(k)}$ is true. Recall that $\boxed{k + 1 = m \in S}$. Hence $\boxed{\neg P(k+1)}$ is true. Thus we just proved that

$$\boxed{\exists\, k \; \big(P(k) \wedge \neg P(k+1)\big)}$$

Consequently,

$$\boxed{\neg P(1) \vee \Big(\exists\, k \; \big(P(k) \wedge \neg P(k+1)\big)\Big)}$$

is true. Thus, we have proved the implication (1) in Case 2, as well. This completes the proof. $\square$