The Well-Ordering Principle and its applications

- *Definition.* A nonempty subset S of $\mathbb{R}$ is **well–ordered** if every non-empty subset of S has a smallest element.
- **The Well-Ordering Principle**: The set $\mathbb{N}$ is well-ordered.
- *Example.* The following sets are well-ordered:
  (1) $\mathbb{N} \cup \{0\}$
  (2) $\mathbb{N} \cup \{-1, 0\}$
  (3) $\mathbb{N} \cup \{-3, -2, -1\}$
  (4) $\{n \in \mathbb{N} : n > 5\}$
- *Example.* The following sets are NOT well-ordered.
  (1) $\mathbb{R}$ (the open interval $(0, 2)$ is a non-empty subset of $\mathbb{R}$ but it has no smallest element)
  (2) $\mathbb{Z}$ (the set of negative integers is a non-empty subset of $\mathbb{Z}$ but with no smallest element)
  (3) the interval $[0, 1]$ (because $(0, 1)$ is a non-empty subset of $[0, 1]$ without smallest element)
- *Proposition.* Every non-empty subset of a well-ordered set is well-ordered.
- *Applications*
  (1) The Division Algorithm: Given $a, b \in \mathbb{Z}$ with $b > 0$, there exist $q, r \in \mathbb{Z}$ for which $a = qb + r$ and $0 \leq r < b$.

  Proof. Consider the set
  $$S = \{a - xb : x \in \mathbb{Z}, a - xb \geq 0\}.$$
  It holds
  $$S \subseteq \mathbb{N} \cup \{0\}.$$
  To see S is non-empty, take $x = -|a| \in \mathbb{Z}$, so
  $$a - xb = a + |a|b \geq 0$$
  because b is a positive integer (so $b \geq 1$), hence $a + |a|b \in S$. By the fact that $\mathbb{N} \cup \{0\}$ is well-ordered, there is a least element in S, call it r, so $r \geq 0$ and $r = a - qb$ for some $q \in \mathbb{Z}$. We now prove $r < b$. If $r \geq b$, then
  $$0 \leq r - b = (a - qb) - b = a - (q + 1)b$$
  would imply $r - b \in S$, which contradicts that r is the smallest in S. $\square$

  (2) Proposition 7.1 in the book (for the existence of smallest element).
  (3) *Theorem.* (Principle of Mathematical Induction) For every $n \in \mathbb{N}$ let $P(n)$ be a statement. If
  (a) $P(1)$ is a true statement, and
  (b) the implication $P(k) \Rightarrow P(k + 1)$ is true for all $k \in \mathbb{N}$
  then $P(n)$ is true for all $n \in \mathbb{N}$.

  Proof. We prove by contradiction. Assume that the set
  $$S = \{n \in \mathbb{N} : P(n) \text{ is false}\}$$
  is non-empty. Then there is a least element l in S by the Well-Ordering Principle. Since $P(1)$ is true by (a), we must have $l \geq 2$. So $l - 1 \in \mathbb{N}$. Since l is the least element in S, $l - 1 \notin S$, so $P(l - 1)$ is true. Then we must have $P(l)$ is true by (b). This contradicts that $l \in S$. We conclude that $S = \emptyset$. $\square$