MATH 2513–002 The Least Principle

We introduce a very fundamental property of the natural numbers

$$\mathbb{N} = \{1, 2, 3, \ldots\}$$

called the *least principle.* It is also known as the *well ordering principle.*

The Least Principle. Every non-empty subset of $\mathbb{N}$ has a least element.

Example. The set of even natural numbers has 2 as its least element. The set of prime numbers bigger than 8 has 11 as its least element.

Looking at examples as above, we conclude that the Least Principle appears to be a fairly "self-evident" statement about $\mathbb{N}$. But keep in mind it is a statement about all possible subsets of the infinite set $\mathbb{N}$, so it is saying a lot.

Remarks.

1. The Least Principle does not hold for the set of all integers $\mathbb{Z}$. For example, the set of all even integers contains $-2, -4, \ldots$ and so does not have a least element.

2. The Least Principle does not hold for the set of all positive real numbers $\mathbb{R}^+ = (0, \infty)$. For example, the set $(0, \infty)$ has no smallest element. For any element x in $(0, \infty)$ we can always find a smaller element in $(0, \infty)$, for example, $x/2$.

3. Check that the Least Principle also holds for the set of non-negative integers, $\{0, 1, 2, \ldots\}$.

4. The phrase "well ordering principle" refers to the fact that one can use the least principle to describe a nice ordering: the least element, the next smallest element, and so on.

   These elements are produced by repeated applications of the Least Principle as follows. Start with the whole set $\mathbb{N}$; its least element is 1. Now remove 1 from consideration. We still have a non-empty subset of $\mathbb{N}$, which has (by the Least Principle) a smallest element, namely 2. Now also remove 2 from consideration. Continue.

5. Note that the set of non-negative real numbers $[0, \infty)$ has a least element, namely 0, but does not have a next smallest element.

The Least Principle is very useful in providing proofs of statements involving natural numbers. We will see how it is used in the following situations.

1. In proving irrationality of certain numbers.

2. In proving the Division Algorithm.

3. In proving that Greatest Common Divisors are linear combinations.

4. It is equivalent to the Principle of Mathematical Induction (in all its incarnations).

The Least Principle is an universally and existentially quantified statement. It states that a least element exists (existential portion) for any (universal portion) non-empty set of natural numbers. The existential content is useful for proving the existence of integers (such as the quotient and remainder in the Division Algorithm, or the greatest common divisor in Bézout's Theorem). It is also ideal for use in proofs by contradiction. This least element is the focus of a proof by contradiction in the case of the irrationality proofs. In the proof of the Division Algorithm, the least element of a particular set turns out to be the remainder, and a proof by contradiction is used to show that this remainder is strictly smaller than the divisor d. In the proof of Bézout's Theorem about greatest common divisors, the least element of another particular set turns out to be the greatest common divisor, and the proof that it is indeed a common divisor is given by contradiction. We will see that the Least Principle is equivalent to the (various formulations of the) Principle of Mathematical Induction. More details are given below.

The Least Principle in Irrationality Proofs

Our first three examples of the Least Principle in action involve proofs that $\sqrt{2}$ is irrational. The general framework for these proofs is the same in all three examples. We used this template in the group work proofs in class. These notes are a recap of those group work exercises.

Proposition. $\sqrt{2}$ is irrational.

Proof Template. We argue by contradiction. Suppose that $\sqrt{2}$ is rational. This means that

$$\sqrt{2} \;=\; \frac{l}{m} \qquad\qquad (*)$$

for some positive integers $l, m \in \mathbb{N}$. Thus, the collection of denominators m of such fractions is a non-empty subset of $\mathbb{N}$. By the Least Principle there is a least such denominator, q say. This means that there exist positive integers $p, q \in \mathbb{N}$ so that

$$\sqrt{2} \;=\; \frac{p}{q}$$

and q is the least denominator among the fractions $(*)$.

$$\vdots$$

Some mathematical manipulations.

$$\vdots$$

The calculations above show that $\sqrt{2}$ is a ratio of two positive integers, and the denominator is strictly smaller than q above. This is a contradiction. Thus the original assumption that $\sqrt{2}$ was rational is false. □

Proof I. This uses facts about even integers that we have proven in class.

Prop. $\sqrt{2}$ *is irrational.*

Proof I. We argue by contradiction. Suppose that $\sqrt{2}$ is rational. This means that

$$\sqrt{2} \;=\; \frac{l}{m} \qquad\qquad (*)$$

for some positive integers $l, m \in \mathbb{N}$. Thus, the collection of denominators m of such fractions is a non-empty subset of $\mathbb{N}$. By the Least Principle there is a least such denominator, q say. This means that there exist positive integers $p, q \in \mathbb{N}$ so that

$$\sqrt{2} \;=\; \frac{p}{q}$$

and q is the least denominator among the fractions $(*)$.

Squaring both sides of the equation

$$\sqrt{2} \;=\; \frac{p}{q}$$

gives

$$2 \;=\; \frac{p^2}{q^2}$$

and multiplying across by q^2 gives

$$2q^2 \;=\; p^2$$

Now the left hand side (LHS) of this equation is an even integer (by definition). Therefore, the RHS is also even. Thus, p^2 is even. From a previous result in class, we conclude that p is even. This means that $p = 2k$ for some integer k. Substituting this into the equation above gives

$$2q^2 \;=\; (2k)^2 \;=\; 4k^2$$

Dividing across by 2 gives

$$q^2 \;=\; 2k^2$$

Now the RHS of this equation is even. Therefore so is the LHS. Thus q^2 is even, and we conclude that q is even. By definition of even, $q = 2r$ for some integer r.

In summary, we have

$$\sqrt{2} \;=\; \frac{p}{q} \;=\; \frac{2k}{2r} \;=\; \frac{k}{r}$$

Note that since p and q are positive, then k and r are also positive.

The calculations above show that $\sqrt{2}$ is a ratio of two positive integers, and the denominator $r = q/2$ is strictly smaller than q above. This is a contradiction. Thus the original assumption that $\sqrt{2}$ was rational is false. □

Proof II. This uses a nice geometric observation.

Prop. *$\sqrt{2}$ is irrational.*

Proof II. We argue by contradiction. Suppose that $\sqrt{2}$ is rational. This means that

$$\sqrt{2} \;=\; \frac{l}{m} \qquad\qquad (*)$$

for some positive integers $l, m \in \mathbb{N}$. Thus, the collection of denominators m of such fractions is a non-empty subset of $\mathbb{N}$. By the Least Principle there is a least such denominator, q say. This means that there exist positive integers $p, q \in \mathbb{N}$ so that

$$\sqrt{2} \;=\; \frac{p}{q}$$

and q is the least denominator among the fractions $(*)$.

Squaring both sides of the equation

$$\sqrt{2} \;=\; \frac{p}{q}$$

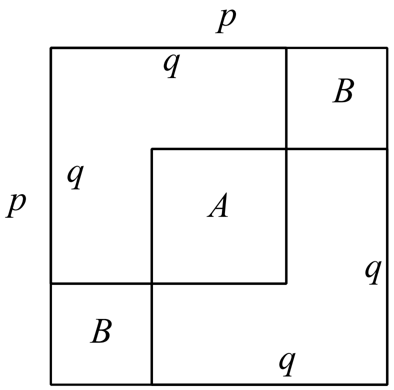
gives

$$2 \;=\; \frac{p^2}{q^2}$$

and multiplying across by q^2 gives

$$2q^2 \;=\; p^2$$

Consider a square of slide length p and two smaller squares of side length q. The equation above shows that the area of the large square is equal to the sum of the areas of the two smaller squares. Now try to "tile" the larger square with the two smaller squares as shown below.



There is an overlap square of area A and two missed squares, each of area B. Now the area of the big square is equal to the sum of the areas of the two tile squares, minus the area of the overlap square, plus the areas of the two missed squares. In symbols this gives

$$p^2 \;=\; q^2 + q^2 - A + B + B$$

or

$$p^2 \;=\; 2q^2 - A + 2B$$

But we know that $p^2 = 2q^2$, and subtracting this from the equation above gives $0 = -A + 2B$. Thus $A = 2B$.

Let a be the edge length of the overlap square, and b be the edge length of one of the missed squares. Then $A = 2B$ rewrites as $a^2 = 2b^2$ or

$$\sqrt{2} \;=\; \frac{a}{b}$$

Finally we show that a and b are positive integers, and that $b < q$. Indeed, we can read off these edge lengths as differences of other lengths in the diagram as follows. First, we have $b = p - q$, and then we can solve for a to get $a = q - (p - q) = 2q - p$. Thus a and b are integers.

It is evident from the geometry of the picture that a and b are positive and $b < q$, but here is an algebraic proof. Start with $1 < \sqrt{2} < 2$. Substituting p/q for $\sqrt{2}$ and multiplying across by q gives

$$q < p < 2q$$

The right hand inequality $p < 2q$ gives $(2q - p) > 0$; that is, $a > 0$. Subtracting q from all terms in $q < p < 2q$ gives $0 < (p - q) < q$. This tells us that $b > 0$ and also that $b < q$.

The calculations above show that $\sqrt{2}$ is a ratio a/b of two positive integers, and the denominator b is strictly smaller than q above. This is a contradiction. Thus the original assumption that $\sqrt{2}$ was rational is false. □

Proof III. This extracts the key algebra ingredients from the geometric proof above.

Prop. $\sqrt{2}$ *is irrational.*

Proof III. We argue by contradiction. Suppose that $\sqrt{2}$ is rational. This means that

$$\sqrt{2} = \frac{l}{m} \qquad (*)$$

for some positive integers $l, m \in \mathbb{N}$. Thus, the collection of denominators m of such fractions is a non-empty subset of $\mathbb{N}$. By the Least Principle there is a least such denominator, q say. This means that there exist positive integers $p, q \in \mathbb{N}$ so that

$$\sqrt{2} = \frac{p}{q}$$

and q is the least denominator among the fractions $(*)$.

Squaring both sides of the equation

$$\sqrt{2} = \frac{p}{q}$$

gives

$$2 = \frac{p^2}{q^2}$$

and multiplying across by q^2 gives

$$2q^2 = p^2$$

Subtract pq from both sides to get

$$2q^2 - pq = p^2 - pq$$

and then factor both sides to obtain

$$(2q - p)q = (p - q)p \qquad (**)$$

We know that $1 < \sqrt{2} < 2$. Substituting p/q for $\sqrt{2}$ and multiplying across by q gives

$$q < p < 2q$$

The right hand inequality $p < 2q$ gives $(2q - p) > 0$. Subtracting q from all terms in $q < p < 2q$ gives $0 < (p - q) < q$. Now we can divide across equation $(**)$ by the non-zero quantity $(p - q)q$ to get

$$\frac{(2p - q)}{(p - q)} = \frac{p}{q} = \sqrt{2}$$

The calculations above show that $\sqrt{2}$ is a ratio of two positive integers, and the denominator $(p - q)$ is strictly smaller than q above. This is a contradiction. Thus the original assumption that $\sqrt{2}$ was rational is false. □

Remark. Here is another way to think of proof III. It is very fast and efficient. (Needless to say, it should be couched in the language of a proof by contradiction.).

1. We assume that $\sqrt{2}$ is rational and that
$$\sqrt{2} \;=\; \frac{p}{q}$$
where p and q are positive integers and q is the least possible denominator.

2. We start from the observation $1 < \sqrt{2} < 2$. Thus $0 < \sqrt{2} - 1 < 1$.

3. Thus
$$\sqrt{2} \;=\; \frac{p}{q} \;=\; \frac{p(\sqrt{2}-1)}{q(\sqrt{2}-1)} \;=\; \frac{p(p/q-1)}{q(p/q-1)} \;=\; \frac{(p^2/q-p)}{(p-q)} \;=\; \frac{(2q^2/q-p)}{(p-q)} \;=\; \frac{(2q-p)}{(p-q)}$$

4. Because $\sqrt{2}-1$ is positive, we know that the terms in the fraction on the right are all positive. We know they are integers by closure properties of $\mathbb{Z}$ under multiplication (by 2) and addition (subtraction). Because $\sqrt{2}-1 < 1$ we know that the denominator in the fraction on the right is strictly less than q. Done!

Homework/class activity.

1. **Q1.** Use the outline in the remark above to give a proof by contradiction of the following result.

   Prop. *If m is a positive integer which is not a square of another integer, then $\sqrt{m}$ is irrational.*

   Hint. If m is a positive integer which is not a square of another integer, then its square root is not an integer. This means that it lies strictly between two consecutive integers
$$a \;<\; \sqrt{m} \;<\; a+1$$
   Hmmm. . . two things. Are we sure that such an a exists? Can you argue that the set $\{n \in \mathbb{N} \mid n \geq \sqrt{m}\}$ is non-empty? What does the least principle say about this set? Second thing. Suppose that we have proven that there is an integer a such that $a < \sqrt{m} < a+1$, how do we proceed?

The Least Principle and the proof of the Division Algorithm

We have talked about the Division Algorithm in class, and have seen some of its first applications. Here is the statement again.

The Division Algorithm. *For all integers a and all positive integers d, there exist unique integers q, r so that*
$$a \;=\; dq + r \qquad \text{where } 0 \leq r < d$$

Intuitively, this says that one can divide any given integer a by any positive integer d to obtain a quotient q and a remainder r satisfying $0 \leq r < d$. This seems plausable, particularly if we think of the integral multiples of d as being highlighted on the number line. If we take any integer a, either it will lie on one of these highlighted integers (in which case we have found a q and $r = 0$) or it lies between two. In the latter case, we look at the highlighted integer to the left. This gives dq and the difference is $r < d$.

This seems reasonable, but it is a claim about all integers a and all positive integers d. We had promised to avoid unnecessarily accepting any more claims of an infinite nature. Let's see if we can use the Least Principle (which is another claim of an infinite nature) to justify the Division Algorithm. The intuition of the previous paragraph gives us an insight about how to apply the least principle. We chose the multiple dq which was either equal to or just to the left of a. If we think in terms of differences $a - dq$, the phrase "equal to or just to the left" translates into the requirement that $a - dq$ is as small as possible among all non-negative differences. This sounds like the ideal setup for using the Least Principle. We use the version of the Least Principle for the set of non-negative integers, $\{0, 1, 2, \ldots\}$.

Proof of Division Algorithm. We are given an arbitrary integer a, and an arbitrary positive integer d. We have two things to to. Firstly, we have to establish the *existence* of the integers q, r as in the Division Algorithm. Secondly, we have to establish that q and r are *uniquely* determined.

We focus on existence now. Given a and $d > 0$, consider the following set of differences

$$R = \{a - dq \,|\, q \in \mathbb{Z}, \text{ and } a - dq \geq 0\}$$

Note that the set R is not empty. For instance, if a is not negative we can take $q = 0$ and $a - dq = a \geq 0$ is in R. If $a < 0$ then we can take $q = a$; in this case $a - dq = a - da = (-a)(d-1) \geq 0$ since $(-a) > 0$ and $d \geq 1$ (recall d is a positive integer) implies that $(d-1) \geq 0$.

We have shown that R is a non-empty subset of the set of all non-negative integers $\{0, 1, 2, \ldots\}$. By the Least Principle, the set R has a least element, call it r. Because r belongs to the set R we can conclude that it has two immediate properties: one is that $r \geq 0$, and the second is that $r = a - dq$ for some integer q. Rewriting this from the perspective of a and d we have the following: there exist $q, r \in \mathbb{Z}$ so that

$$a = dq + r \qquad \text{where } 0 \leq r$$

Note that this is *almost* the existence portion of the statement of the Division Algorithm. We only need to show that $r < d$ to get an exact match. To establish this last claim, we argue by contradiction. Suppose $r \geq d$. Then we could subtract d to get a non-negative number which is strictly smaller than r; namely, $0 \leq r - d < r$. Substituting $r = a - dq$ gives $0 \leq a - dq - d < r$, which cleans up to give $0 \leq a - d(q+1) < r$. This means that the number $a - d(q+1)$ is also in R and is strictly smaller than r. This contradicts the fact that r is the least element of R. We conclude that the assumption $r \geq d$ is false, and so $r < d$. We add this extra piece of information to obtain the existence portion of the Division Algorithm: there exist $q, r \in \mathbb{Z}$ so that

$$a = dq + r \qquad \text{where } 0 \leq r < d$$

Next we turn to proving uniqueness. Suppose that there exist $q', r' \in \mathbb{Z}$ so that

$$a = dq' + r' \qquad \text{where } 0 \leq r' < d$$

To establish uniqueness, we need to prove that these two equations imply that $q = q'$ and $r = r'$. Subtracting one equation from the other gives

$$a - a = d(q - q') + (r - r') \qquad \text{where } 0 \leq |r - r'| < d$$

This becomes

$$d(q' - q) \;=\; (r - r') \qquad \text{where } 0 \leq |r - r'| < d$$

Taking absolute values (remembering that $d > 0$) gives

$$d|q' - q| \;=\; |r - r'| \qquad \text{where } 0 \leq |r - r'| < d$$

Since $|q' - q|$ is a non-negative integer, the LHS of the equation is either 0 or $\geq d$. Note that the RHS of the equation is either 0 or $< d$. Since a number can't be simultaneously $\geq d$ and $< d$, the only way the equation holds is if both sides are 0.

Thus $d|q' - q| = 0$ and $|r - r'| = 0$. This gives $q' - q = 0$ (since $d \neq 0$) and $r - r' = 0$; that is, $q = q'$ and $r = r'$. We have established uniqueness. □

The Least Principle and properties of Greatest Common Divisors

We start with the definition of greatest common divisor.

Definition. Let a, b be non-zero integers. The *greatest common divisor* of a and b is the greatest integer which is a divisor of both a and b. The greatest common divisor of a and b is denoted by $\gcd(a, b)$.

In this section we use the Least Principle to prove the following lovely fact about greatest common divisors.

Proposition (Bézout). *The greatest common divisor of non-zero integers a and b, is the least positive, integer linear combination of a and b. In particular,*

$$\gcd(a, b) \;=\; la + mb$$

for some integers l, m.

Proof. Given two integers $a \neq 0$ and $b \neq 0$, consider the set of all positive, integer linear combinations of a and b:

$$S \;=\; \{la + mb \,|\, l, m \in \mathbb{Z},\, la + mb > 0\}$$

By definition, S is a subset of $\mathbb{N}$. We show that S is not empty. For example, taking $l = a$ and $m = b$, we see that the positive integer $a^2 + b^2$ is in S.

By the Least Principle, S has a least element; denote it by d. Since $d \in S$ we have that $d = la + mb$ for some $l, m \in \mathbb{Z}$. We argue that d is a divisor of a as follows. The hypotheses of the Division Algorithm hold since $d > 0$, and we conclude that there exist integers q, r such that

$$a \;=\; dq + r \qquad \text{where } 0 \leq r < d$$

If $r \neq 0$ then $0 < r < d$ and $r = a - dq = a - (la + mb)q = (1 - lq)a + (-mq)b$, then r would be a strictly smaller element of S, contradicting the fact that d was the least element. Therefore, $r = 0$ and so $a = dq$; that is, d divides a and we are done.

A similar argument by contradiction shows that d is a divisor of b.

At this stage we know that d is a positive, integer linear combination of a and b, and that d is a common divisor of a and b. How do we see that d is the greatest common divisor of a and b? We use the integer linear combination property. We have seen that $d = la + mb$ for some $l, m \in \mathbb{Z}$. If c is a common divisor of a and b, then c also divides $la+mb$ (proven in class). That is, c divides d. Thus, every other common divisor of a and b must divide the positive number d, and so $d = \gcd(a,b)$.

In summary, $\gcd(a,b)$ is the least positive, integer linear combination of a and b. In particular, $\gcd(a,b) = la + mb$ for some integers $l, m \in \mathbb{Z}$. □

This has nice consequences. For example, the following

Prop. *If a, b, c are positive integers such that $a \mid bc$ and $\gcd(a,b) = 1$, then $a \mid c$.*

Proof. We are told that $\gcd(a,b) = 1$. By the result above, there are $l, m \in \mathbb{Z}$ such that $la + mb = \gcd(a,b) = 1$. Multiply across by c to get

$$c \;=\; c(1) \;=\; lac + mbc$$

We are told that $a \mid bc$ and so, $a \mid lac + mbc$. That is, $a \mid c$. □

Definition. An integer $p \geq 2$ is said to be *prime* if its only divisors are itself and 1.

As an immediate consequence of the proposition above, we obtain this great property of prime numbers, which will be crucial in our proof of the Fundamental Theorem of Arithmetic.

Prop. (Key divisibility property of primes) *If b, c are positive integers and p is a prime number such that $p \mid bc$ and $p \nmid b$, then $p \mid c$.*

Proof. By definition of prime $p \nmid b$ means that p and b have only got the factor 1 in common, and so $(p,b) = 1$. The previous proposition applies to give the result. □

The Least Principle and Mathematical Induction

We have seen in class discussion that given a statement that is amenable to a proof by induction, it is possible instead to give a proof by contradiction using the Least Principle. In particular, we gave a proof by contradiction using the Least principle of the statement

$$1 \;+\; \cdots \;+\; n \;=\; \frac{n(n+1)}{2} \qquad \text{for all } n \in \mathbb{N}.$$

Take the time now to revisit that proof in your notes. It is also available on the course web page.

In this section we formalize the observation above, and prove that the following three principles are equivalent:

1. The Least Principle (LP). *Every nonempty subset of $\mathbb{N}$ has a smallest (least) element.*

2. The Principle of Induction (I). *Suppose $P(n)$ is a sentence about positive integers n.*

$$\left.\begin{array}{l} \bullet\;\; P(1) \text{ true} \\ \bullet\;\; P(k) \text{ true} \;\rightarrow\; P(k+1) \text{ true} \end{array}\right\} \;\rightarrow\; P(n) \text{ true}, \forall n \in \mathbb{N}$$

3. The Principle of Strong Induction (SI). *Suppose $P(n)$ is a sentence about positive integers n.*

$$\left.\begin{array}{l} \bullet\;\; P(1) \text{ true} \\ \bullet\;\; (P(1) \text{ true}) \wedge \cdots \wedge (P(k) \text{ true}) \;\rightarrow\; P(k+1) \text{ true} \end{array}\right\} \;\rightarrow\; P(n) \text{ true}, \forall n \in \mathbb{N}$$

Prop. *The following statements are equivalent: (LP), (I), and (SI).*

Proof. We shall establish this equivalence by proving a circle of implications:

$$\text{(LP)} \;\to\; \text{(I)} \;\to\; \text{(SI)} \;\to\; \text{(LP)}$$

First Part. [(LP) $\to$ (I)]

Proof. Given the sentence $P(n)$ and the two inductive assumptions "$P(1)$ true" and "$P(k)$ true implies $P(k+1)$ true," we want to prove that $P(n)$ is true for all positive integers n. That is, we want to establish that the following set of positive integers

$$F \;=\; \{n \in \mathbb{N} \,|\, P(n) \text{ is false}\}$$

is empty, and so conclude that the set $T = \{n \in \mathbb{N} \,|\, P(n) \text{ is true}\}$ is all of $\mathbb{N}$.

We argue by contradiction. Assume that F is nonempty. Then by (LP) we there is a least element n_0 in F. Note that since $P(1)$ is true $1 \notin F$, and so $n_0 \geq 2$. Subtracting 1 gives $1 \leq n_0 - 1$ is still a positive integer, and $n_0 - 1 \notin F$ (since n_0 was least). By definition of F, we conclude that $P(n_0 - 1)$ is true. Now, the second induction hypothesis (with $k = n_0$) gives us that $P((n_0 - 1) + 1)$ is true. But this says that $P(n_0)$ is true, a contradiction. This contradiction ("$P(n_0)$ is false and $P(n_0)$ is true") arose from the assumption that F is nonempty. Therefore, F is empty and so the set $T = \{n \in \mathbb{N} \,|\, P(n) \text{ is true}\}$ is all of $\mathbb{N}$. □

Second Part. [(I) $\to$ (SI)]

Proof. Given the sentence $P(n)$ and the two inductive assumptions "$P(1)$ true" and "$(P(1) \text{ true}) \wedge \cdots \wedge (P(k) \text{ true})$ implies $P(k+1)$ true," we want to prove that $P(n)$ is true for all positive integers n.

Let $Q(n)$ be the sentence $(P(1) \text{ true}) \wedge \cdots \wedge (P(n) \text{ true})$. We use ordinary induction to prove that $Q(n)$ is true for all $n \in \mathbb{N}$.

Base case. Note that $Q(1)$ is the sentence $P(1)$ is true. This is the first of the two (strong) induction hypotheses, and so is true.

Induction step. Assume that $Q(k)$ is true. By definition of $Q(k)$ this means that $(P(1) \text{ true}) \wedge \cdots \wedge (P(k) \text{ true})$ is true. By the second (strong) induction hypotheses we conclude that $P(k+1)$ is true. Therefore $(P(1) \text{ true}) \wedge \cdots \wedge (P(k) \text{ true})$ is true and $P(k+1)$ is true. Combining together gives $(P(1) \text{ true}) \wedge \cdots \wedge (P(k) \text{ true}) \wedge (P(k+1) \text{ true})$ is true. That is, $Q(k+1)$ is true. We have shown that $Q(k)$ true implies $Q(k+1)$ true.

By the principle of induction (regular form) we conclude that $Q(n)$ is true for all $n \in \mathbb{N}$. That is $(P(1) \text{ true}) \wedge \cdots \wedge (P(n) \text{ true})$ is true for all $n \in \mathbb{N}$ and, in particular, $P(n)$ is true for all $n \in \mathbb{N}$. □

Third Part. [(SI) $\to$ (LP)]

Proof. We can assume the principle of strong induction and we have to deduce the Least Principle. We have to prove that every nonempty subset of $\mathbb{N}$ has a least element. We shall prove the contrapositive statement:

If a subset S of $\mathbb{N}$ has no least element, then S is empty.

Consider the sentence $P(n) : n \notin S$. If we show that $P(n)$ is true for all $n \in \mathbb{N}$, then we will have shown that $n \notin S$ for all $n \in \mathbb{N}$, and so will have shown that S is empty. We argue by strong induction.

Base case. $P(1)$ is true. This is because 1 is the least element of $\mathbb{N}$ and so if $1 \in S$ it would be the least element of S too. But S does not have a least element by hypothesis. Therefore, $1 \notin S$.

Inductive step. Suppose $(P(1)$ true$) \wedge \cdots \wedge (P(k)$ true$)$ is true. This means $1 \notin S, 2 \notin S, \ldots, k \notin S$. We note that $(k+1)$ is the next smallest integer of $\mathbb{N}$ after $1, 2, \ldots, k$. Therefore $(k+1) \notin S$, because otherwise it would be the least element of S. This would contradict the hypothesis that S has no least element. So we have shown that $P(k+1)$ is true.

By the principle of strong induction, we conclude that $P(n)$ is true for all $n \in \mathbb{N}$. That is $n \notin S$ for all $n \in \mathbb{N}$. Thus S is empty. □

In conclusion, the three implications proven above establish the equivalence of the Least Principle, the Principle of Induction, and the Principle of Strong Induction. □