Appendix A

Mathematical Induction

Mathematical induction is the name of a method of proof based on a specific principle which can be explained as follows. Suppose \( P(n) \) is a sequence of propositions dependent on the integral index \( n \), usually nonnegative. If the two statements below can be proved, then \( P(n) \) is true for all \( n \geq k \).

\((S1)\) \( P(k) \) is true.

\((S2)\) \( P(n) \) implies \( P(n+1) \) for any \( n \geq k \).

The second statement says that if \( P(n) \) holds for some \( n \geq k \) then \( P(n+1) \) holds as well. Intuitively, since by \((S1)\), \( P(k) \) is true, then \( P(k+1) \) is true by \((S2)\). And since \( P(k+1) \) is true then \( P(k+2) \) is true, again by \((S2)\), and hence \( P(k+3) \) is also true, and so on.

Example. Prove that the number \( n^3 - n \) is divisible by 3 for all \( n \geq 1 \).

Proof. Let \( P(n) \) stand for the statement “\( n^3 - n \) is divisible by 3.” Then \( P(1) \) says “0 is divisible by 3.” This is trivially true.

Next, we assume that \( P(n) \) is true—this is called the induction hypothesis—and seek to establish \( P(n+1) \). Now \( P(n+1) \) is the statement “\((n+1)^3 - (n+1) \) is divisible by 3.” This part of the proof might be written as follows. Note first the right-hand side of the following equality.

\[
(n+1)^3 - (n+1) = (n^3 - n) + 3(n^2 + n)
\]

By our hypothesis, \( n^3 - n \) is divisible by 3. And clearly, \( 3(n^2 + n) \) is also a multiple of 3. Hence the quantity on the left, \( (n+1)^3 - (n+1) \), is divisible by 3. This completes the proof that \( P(n) \) is true for all \( n \geq 1 \). □

With practice, we can write an induction proof with less explicit declaration of the induction steps. In fact, doing so is sometimes best for the flow of the proof. We give another example.
Example. Every set with $n \geq 1$ elements have a total of $2^n$ subsets.

Proof. If a set has only one element, then it has exactly two subsets: itself and the empty set. Hence the claim is true for $n = 1$. We proceed by induction: Assume that the statement holds for some $n > 1$ and consider a set $S$ with $n+1$ elements. Let $x$ be one of these elements. Some subsets of $S$ contains $x$ and some do not. Those that do not are subsets $S - \{x\}$, which is the set of the remaining $n$ elements of $S$ after removing $x$. By the induction hypothesis, there are $2^n$ of these subsets. Meanwhile, the subsets of $S$ which do contain $x$ can be enumerated just like those which don’t, by joining $x$ into each of them. Hence the subsets containing $x$ are also $2^n$ in number. It follows that, in all, there are $2^n + 2^n = 2^{n+1}$ subsets of $S$. ▽

Exercise A.1. Use mathematical induction to prove the following claims.

a) The formula $1 + 2 + 4 + \cdots + 2^{n-1} = 2^n - 1$ holds for all $n \geq 1$.

b) The number $3^{2^n} - 1$ is a multiple of 8 for all $n \geq 1$.

c) The number $\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15}$ is an integer for all $n \geq 0$.

d) The inequality $n! > 2^n$ holds for all $n \geq 4$.

Exercise A.2. Let $k \geq 2$ and $n_1, n_2, \ldots, n_k$ be $k$ integers such that for each pair $i \neq j$, $\gcd(n_i, n_j) = 1$. Let $m$ be another integer and $N = n_1n_2 \cdots n_k$. Use mathematical induction on the index $k$, to prove that

a) If $n_i \mid m$ for each $1 \leq i \leq k$ then $N \mid m$.

b) If $\gcd(m, n_i) = 1$ for each $1 \leq i \leq k$ then $\gcd(m, N) = 1$.

Exercise A.3. For three integers or more, define their greatest common divisor recursively by $\gcd(n_1, n_2, \ldots, n_k) = \gcd(\gcd(n_1, n_2, \ldots, n_{k-1}), n_k)$. Prove that $\gcd(n_1, n_2, \ldots, n_k)$ is a linear combination of $n_1, n_2, \ldots, n_k$.

There is a second version of the principle of mathematical induction, in which the statement $(S2)$ is replaced by another:

$(S3)$ If $P(k), P(k+1), \ldots, P(n)$ all hold, then $P(n+1)$ holds.

This is the version which we use, for instance, to prove Proposition 2.1(2) and Theorem 2.4 in the text. This seemingly stronger principle is actually equivalent to the first, and both are logically equivalent to the well-ordering principle, which states that every nonempty set of positive integers contains a least element. In most mathematical subjects, this principle—induction or well-ordering—is taken as an axiom, that is, assumed valid without proof.

Exercise A.4. The well-ordering principle has been implicitly employed, twice, in the proofs of Chapter 1. Go and investigate.