APPENDIX C

Well Ordering and Induction

We assume that you are familiar with ordinary arithmetic in the set $\mathbb{Z}$ of integers and with the usual order relation ($<$) on $\mathbb{Z}$. The subset of nonnegative integers will be denoted by $\mathbb{N}$. Thus

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}.$$

Finally, we assume this fundamental axiom:

WELL-ORDERING AXIOM *Every nonempty subset of* $\mathbb{N}$ *contains a smallest element.*

Most people find this axiom quite plausible, but it is important to note that it may not hold if $\mathbb{N}$ is replaced by some other set of numbers; see page 2 of the text for examples.

An important consequence of the Well-Ordering Axiom is the method of proof known as mathematical induction. It can be used to prove statements such as

A set of n elements has 2^n subsets.

Denote this statement by the symbol $P(n)$ and observe that there are really infinitely many statements, one for each possible value of n:

$P(0)$: A set of 0 elements has $2^0 = 1$ subset.
$P(1)$: A set of 1 element has $2^1 = 2$ subsets.
$P(2)$: A set of 2 elements has $2^2 = 4$ subsets.
$P(3)$: A set of 3 elements has $2^3 = 8$ subsets.

And so on. To prove the original proposition we must prove that

$P(n)$ is a true statement for every $n \in \mathbb{N}$.

Here's how it can be done.

THEOREM C.1 (THE PRINCIPLE OF MATHEMATICAL INDUCTION) *Assume that for each nonnegative integer n, a statement P(n) is given. If*

(i) P(0) is a true statement; and

(ii) Whenever P(k) is a true statement, then P(k + 1) is also true,

then P(n) is a true statement for every $n \in \mathbb{N}$.

The example of the number of subsets of a set of n elements is continued after the proof of the theorem. You may want to read that example now to see how Theorem C.1 is *applied*, which is quite different from the manner in which it is proved.

Proof of Theorem C.1 Let S be the subset of $\mathbb{N}$ consisting of those integers j for which $P(j)$ is *false*. To prove the theorem we need only show that S is empty; we shall use proof by contradiction to do this. Suppose S is nonempty. Then by the Well-Ordering Axiom, S contains a smallest element, say d. Since $P(d)$ is false by the definition of S and $P(0)$ is true by property (i), we must have $d \neq 0$. Consequently, $d \geq 1$ (because d is a nonnegative integer), and, hence, $d - 1 \geq 0$, that is, $d - 1 \in \mathbb{N}$. Since $d - 1 < d$ and d is the smallest element in S, $d - 1$ cannot be in S. Therefore, $P(d - 1)$ must be true (otherwise $d - 1$ would be in S). Property (ii) (with $k = d - 1$) implies that $P((d - 1) + 1) = P(d)$ is also a true statement. This is a contradiction since $d \in S$. Therefore, S is the empty set, and the theorem is proved. ◆

In order to apply the Principle of Mathematical Induction to a series of statements, you must verify that these statements satisfy *both* properties (i) and (ii). Note that property (ii) does *not* assert that any particular $P(k)$ is actually true, but only that a conditional relationship holds: *If* $P(k)$ is true, *then* $P(k + 1)$ must also be true. So to verify property (ii), you assume the truth of $P(k)$ and use this assumption to prove that $P(k + 1)$ is true. As we shall see in the examples below, it is often possible to prove this conditional statement even though you may not be able to prove directly that a particular $P(j)$ is true. The assumption that $P(k)$ is true is called the **induction assumption** or the **induction hypothesis.**

You may have seen induction used to prove statements such as "the sum of the first n nonnegative integers is $\frac{n(n+1)}{2}$"; here $P(n)$ is the statement: "$0 + 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$." Although such examples make nice exercises for beginners, they are not typical of the way induction is used in advanced mathematics. The examples below will give you a more comprehensive

picture of inductive proof. They are a bit more complicated than the usual elementary examples but are well within your reach.

EXAMPLE We shall use the Principle of Mathematical Induction to prove that for each $n \geq 0$,

$$\text{A set of } n \text{ elements has } 2^n \text{ subsets.}$$

If $n = 0$, then the set must be the empty set (the only set with no elements). Its one and only subset is itself (since $\varnothing$ is a subset of every set). So the statement

$$P(0)\text{: A set of 0 elements has } 2^0 = 1 \text{ subset}$$

is true (property (i) holds).

In order to verify property (ii) of Theorem C.1, we assume the truth of

$$P(k)\text{: A set of } k \text{ elements has } 2^k \text{ subsets}$$

and use this induction hypothesis to prove

$$P(k+1)\text{: A set of } k+1 \text{ elements has } 2^{k+1} \text{ subsets.}$$

To do this, let T be any set of $k + 1$ elements and choose some element c of T. Every subset of T either contains c or does not contain c. The subsets of T that do not contain c are precisely the subsets of $T - \{c\}$. Since the set $T - \{c\}$ has one fewer element than T, it is a set of k elements and, therefore, has exactly 2^k subsets (because the induction hypothesis $P(k)$ is assumed true). Now every subset of T that contains c must be of the form $\{c\} \cup D$, where D is a subset of $T - \{c\}$. There are 2^k possible choices for D and, hence, 2^k subsets of T that contain c. Consequently, the total number of subsets of T is

$$\begin{aligned}\begin{pmatrix}\text{Number of subsets}\\ \text{that contain } c\end{pmatrix} + \begin{pmatrix}\text{Number of subsets that}\\ \text{do not contain } c\end{pmatrix} &= 2^k + 2^k\\ &= 2(2^k)\\ &= 2^{k+1}.\end{aligned}$$

Thus any set T of $k + 1$ elements has 2^{k+1} subsets, that is, $P(k + 1)$ is a true statement. We have now verified property (ii) and can, therefore, apply Theorem C.1 to conclude that $P(n)$ is true for every $n \in \mathbb{N}$; that is, every set of n elements has 2^n subsets.

The Principle of Mathematical Induction cannot be conveniently used on certain propositions, even though they appear to be suitable for inductive proof. In such cases a variation on the procedure is needed:

THEOREM C.2 (THE PRINCIPLE OF COMPLETE INDUCTION) *Assume that for each nonnegative integer n, a statement P(n) is given. If*

(i) P(0) is a true statement; and

(ii) Whenever P(j) is a true statement for all j such that $0 \leq j < t$, then P(t) is also true,

then P(n) is a true statement for every $n \in \mathbb{N}$.

Although commonly used, the title "complete induction" is a bit of a misnomer since, as we shall see, this form of induction is equivalent to the previous one.

Proof of Theorem C.2 For each $n \in \mathbb{N}$, let $Q(n)$ be the statement

$$P(j) \text{ is true for all } j \text{ such that } 0 \leq j \leq n.$$

Note carefully that the last inequality sign in this statement is $\leq$ and not $<$. We shall use the Principle of Mathematical Induction (Theorem C.1) to show that $Q(n)$ is true for every $n \in \mathbb{N}$. This will mean, in particular, that $P(n)$ is true for every $n \in \mathbb{N}$. Now $Q(0)$ is the statement

$$P(j) \text{ is true for all } j \text{ such that } 0 \leq j \leq 0.$$

In other words, $Q(0)$ is just the statement "$P(0)$ is true." But we know that this is the case by hypothesis (i) in the theorem. Suppose that $Q(k)$ is true, that is,

$$P(j) \text{ is true for all } j \text{ such that } 0 \leq j \leq k.$$

By hypothesis (ii) (with $t = k + 1$), we conclude the $P(k + 1)$ is also true. Therefore, $P(j)$ is true for all j such that $0 \leq j \leq k + 1$, that is, $Q(k + 1)$ is a true statement. Thus we have shown that whenever $Q(k)$ is true, then $Q(k + 1)$ is also true. By the Principle of Mathematical Induction, $Q(n)$ is true for every $n \in \mathbb{N}$, and the proof is complete. ◆

In the formal description of induction (either principle), the notation $P(n)$ is quite convenient. But it is rarely used in actual proofs by induction. The next example is more typical of the way inductive proofs are usually phrased. But even here we include more detail than is customary in such proofs.

EXAMPLE We shall use the Principle of Complete Induction to prove:

If $n, b \in \mathbb{N}$ and $b > 0$, then there exist $q, r \in \mathbb{N}$ such that

$$(*) \qquad n = bq + r \quad \text{and} \quad 0 \leq r < b.$$

This statement (called the **Division Algorithm** for nonnegative integers) is just a formalization of grade-school long division: When n is divided by

b, there is a quotient q and remainder r (smaller than the divisor b) such that $n = bq + r$; see the discussion on page 3 of the text.

Statement (*) is true for $n = 0$ and any positive b (let $q = 0$ and $r = 0$). So property (i) of Theorem C.2 holds. Suppose that (*) is true for all n such that $0 \le n < t$ (this is the induction hypothesis). We must show that (*) is true for $n = t$. If $t < b$, then $t = b0 + t$, so (*) is true with $q = 0$ and $r = t$. If $b \le t$, then $0 \le t - b < t$, and by the induction hypothesis, (*) is true for $n = t - b$. Therefore, there exist integers q_1 and r_1 such that

$$t - b = q_1 b + r_1 \quad \text{and} \quad 0 \le r_1 < b.$$

Consequently,

$$t = b + q_1 b + r_1 = (1 + q_1)b + r_1 \quad \text{and} \quad 0 \le r_1 < b.$$

Therefore, (*) is true for $n = t$ (with $q = 1 + q_1$ and $r = r_1$). Hence, property (ii) of Theorem C.2 is satisfied. By the Principle of Complete Induction, (*) is true for every $n \in \mathbb{N}$.

Some mathematical statements are false (or undefined) for $n = 0$ or other small values of n but are true for $n = r$ and all subsequent integers. For instance, it can be shown that

$$3n > n + 1 \text{ for every integer } n \ge 1.$$
$$2^n > n^2 + 2 \text{ for every integer } n \ge 5.$$

Such statements can often be proved by using a variation of mathematical induction (either principle):

In order to prove that statement $P(n)$ is true for each integer $n \ge r$, follow the same basic procedure as before, starting with $P(r)$ instead of $P(0)$.

The validity of this procedure is a consequence of

THEOREM C.3 *Let r be a positive integer and assume that for each $n \ge r$ a statement $P(n)$ is given. If*

(i) $P(r)$ is a true statement;

and either

(ii) Whenever $k \ge r$ and $P(k)$ is true, then $P(k + 1)$ is true;

or

(ii') Whenever $P(j)$ is true for all j such that $r \le j < t$, then $P(t)$ is true,

Proof Conditions (i) and (ii) are the analogue of Theorem C.1. Verify that the proof of Theorem C.1 carries over to the present case verbatim if 0 is replaced by r, 1 by $r + 1$, and $\mathbb{N}$ by the set $\mathbb{N}_r = \{n \mid n \in \mathbb{N} \text{ and } n \geq r\}$. Conditions (i) and (ii′) are the analogue of Theorem C.2; its proof carries over similarly. ◆

The final theorem to be proved here is not necessary in order to read the rest of the book. But it is a result that every serious mathematics student ought to know. It is also a good illustration of the fact that intuition can sometimes be misleading. Most people feel that the Well-Ordering Axiom is obvious, whereas the Principle of Complete Induction seems deeper and in need of some proof. But as we shall now see, these two statements are actually equivalent. Among other things, this suggests that the Well-Ordering Axiom is a good deal deeper than it first appears.

THEOREM C.4 *The following statements are equivalent:*

(1) The Well-Ordering Axiom.

(2) The Principle of Mathematical Induction.

(3) The Principle of Complete Induction.

Proof The proof of Theorem C.1 shows that (1) $\Rightarrow$ (2), and the proof of Theorem C.2 shows that (2) $\Rightarrow$ (3). To prove (3) $\Rightarrow$ (1), we assume the Principle of Complete Induction and let S be any subset of $\mathbb{N}$. To prove that the Well-Ordering Axiom holds, we must show

If S is nonempty, then S has a smallest element.

To do so, we shall prove the equivalent contrapositive statement

If S has no smallest element, then S is empty.

Assume S has no smallest element; to prove that S is empty we need only show that the following statement is true for every $n \in \mathbb{N}$:

(**) n is not an element of S.

Since 0 is the smallest element of $\mathbb{N}$, it is also the smallest element of any subset of $\mathbb{N}$ containing 0. Since S has no smallest element, 0 cannot be in S, and, hence, (**) is true when $n = 0$ (property (i) of Theorem C.2 holds). Suppose (**) is true for all j such that $0 \leq j < t$. Then none of the integers $0, 1, 2, \ldots, t - 1$ is in S, or equivalently, every element in S must be greater than or equal to t. If t were in S, then t would be the smallest element in S since $s \geq t$ for all $s \in S$. Since S has no smallest element, t is not in S. In other words, (**) is true when $n = t$. Thus the truth of (**) when $j < t$ implies its truth for t (property (ii) of Theorem C.2 holds). By the Principle of Complete Induction, (**) is true for all $n \in \mathbb{N}$. Therefore, S is empty, and the proof is complete. ◆

◆ EXERCISES

A. **1.** Prove that the sum of the first n nonnegative integers is $n(n + 1)/2$. [*Hint:* Let $P(k)$ be the statement:

$$0 + 1 + 2 + \cdots + k = k(k + 1)/2.]$$

2. Prove that for each nonnegative integer n, $2^n > n$.

3. Prove that $2^{n-1} \leq n!$ for every nonnegative integer n. [Recall that $0! = 1$ and for $n > 0$, $n! = 1 \cdot 2 \cdot 3 \cdots (n - 1)n$.]

4. Let r be a real number, $r \neq 1$. Prove that for every integer $n \geq 1$,

$$1 + r + r^2 + r^3 + \cdots + r^{n-1} = \frac{r^n - 1}{r - 1}.$$

B. **5.** Prove that 4 is a factor of $7^n - 3^n$ for every positive integer n. [*Hint:* $7^{k+1} - 3^{k+1} = 7^{k+1} - 7 \cdot 3^k + 7 \cdot 3^k - 3^{k+1} = 7(7^k - 3^k) + (7 - 3)3^k$.]

6. Prove that 3 is a factor of $4^n - 1$ for every positive integer n.

7. Prove that 3 is a factor of $2^{2n+1} + 1$ for every positive integer n.

8. Prove that 5 is a factor of $2^{4n-2} + 1$ for every positive integer n.

9. Prove that 64 is a factor of $9^n - 8n - 1$ for every nonnegative integer n.

10. Use the Principle of Complete Induction to show that every integer greater than 1 is a product of primes. [Recall that a positive integer p is prime provided that $p > 1$ and that the only positive integer factors of p are 1 and p.]

11. Let B be a set of n elements. Prove that the number of different injective functions from B to B is $n!$. [$n!$ was defined in Exercise 3.]

12. True or false: $n^2 - n + 11$ is prime for every nonnegative integer n. Justify your answer. [Primes were defined in Exercise 10.]

13. Let B be a set of n elements.

(a) If $n \geq 2$, prove that the number of two-element subsets of B is $n(n - 1)/2$.

(b) If $n \geq 3$, prove that the number of three-element subsets of B is $n(n - 1)(n - 2)/3!$.

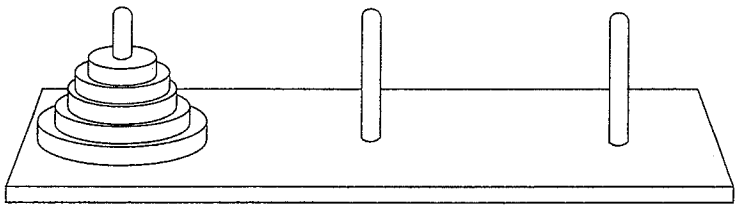
(c) Make a conjecture as to the number of k-element subsets of B when $n \geq k$. Prove your conjecture.

14. At a social bridge party every couple plays every other couple exactly once. Assume there are no ties.

(a) If n couples participate, prove that there is a "best couple" in the following sense: A couple u is "best" provided that for every couple v, u beats v *or* u beats a couple that beats v.

15. What is wrong with the following "proof" that all roses are the same color. It suffices to prove the statement: In every set of n roses, all the roses in the set are the same color. If $n = 1$, the statement is certainly true. Assume the statement is true for $n = k$. Let S be a set of $k + 1$ roses. Remove one rose (call it rose A) from S; there are k roses remaining, and they must all be the same color by the induction hypothesis. Replace rose A and remove a different rose (call it rose B). Once again there are k roses remaining that must all be the same color by the induction hypothesis. Since the remaining roses include rose A, all the roses in S have the same color. This proves that the statement is true when $n = k + 1$. Therefore, the statement is true for all n by induction.

16. Let n be a positive integer. Suppose that there are three pegs and on one of them n rings are stacked, with each ring being smaller in diameter than the one below it, as shown here for $n = 5$:



The game is to transfer all the rings to another peg according to these rules: (i) only one ring may be moved at a time; (ii) a ring may be moved to any peg but may never be placed on top of a smaller ring; (iii) the final order of the rings on the new peg must be the same as their original order on the first peg. Prove that the game can be completed in $2^n - 1$ moves and cannot be completed in fewer moves.

17. Let x be a real number greater than -1. Prove that for every positive integer n, $(1 + x)^n \geq 1 + nx$.

C. 18. Consider maps in the plane formed by drawing a finite number of straight lines (entire lines, not line segments). Use induction to prove that every such map may be colored with just two colors in such a way that any two regions with the same line segment as a common border have different colors. Two regions that have only a single point on their common border may have the same color. [This problem is a special case of the so-called Four-Color Theorem, which states that every map in the plane (with any continuous curves or segments of curves as boundaries) can be colored with at most four colors in such a way that any two regions that share a common border have different colors.]