8.4 Peano's axioms and proof by induction

Peano's axioms for the natural numbers, actually due to Dedekind, are not only one of most well-known axiomatic systems in the history of mathematics, but they give rise to the *Principle of Mathematical Induction* and the technique of *proof by induction* or *inductive proof*, a conceptually important tool which further helps to highlight the close affinity between recursive definitions and axiomatic systems.

In this section we introduce Peano's axioms and the method of proof by induction; we will come back to Peano's axioms from a model-theoretic perspective in 8.5.7.

In Part A, Appendix A, we saw a *constructive* approach to the natural numbers, with set theory assumed as a basis. We review that construction here, putting it in the form of a recursive definition of NN

(8–25) 1. $\emptyset \in NN$
2. For all X, if $X \in NN$, then $X \cup \{X\} \in NN$
3. Nothing else is in NN

The set NN defined in this way has many useful properties which make it a reasonable, if artificial, set-theoretic reconstruction of the natural numbers. Zero is identified with $\emptyset$, 1 with $\{\emptyset\}$, 2 with $\{\emptyset, \{\emptyset\}\}$, and so on, each natural number n being identified with the unique member of NN having n members. The definition endows the natural numbers with appropriate structure and can be used as the basis for defining further arithmetical relations and operations and extending the number system as discussed in Appendix A.

In the axiomatic approach to natural numbers, the aim was rather to set forth some essential properties of the natural numbers from which all their

other properties should be derivable as theorems, just as in the Euclidean axiomatization of plane geometry. In stating the basic axioms, only logical concepts (including, in this case, equality) are assumed, and a set of axioms involving two primitive predicates and one primitive constant is given. The primitives are (1) the one-place predicate 'is a natural number' and the two-place predicate 'is the successor of' and (2) the constant 0. It is to be emphasized that these are primitives; the only meaning they have is given to them in the axiomatization. The concept of a natural number is, therefore, implicitly defined by the axioms: they are those things of which, in some model of the system, the interpretation of the predicate 'is a natural number' is true. Let us write Nx for 'x is a natural number' and Sxy for 'x is a successor of y'. The axioms are:

P1) $N0$ (zero is a natural number)

P2) $(\forall x)(Nx \rightarrow (\exists y)(Ny \,\&\, Syx \,\&\, (\forall z)(Szx \rightarrow z = y)))$ (every natural number has a unique successor)

P3) $\sim(\exists x)(Nx \,\&\, S0x)$ (0 is not the successor of any number)

P4) $(\forall x)(\forall y)(\forall z)(\forall w)((Nx \,\&\, Ny \,\&\, Szx \,\&\, Swy \,\&\, z = w) \rightarrow x = y)$ (no two distinct natural numbers have the same successor

P5) If Q is a property such that

(i) $Q0$ (zero has Q), and

(ii) $(\forall x)(\forall y)((Nx \,\&\, Qx \,\&\, Ny \,\&\, Syx) \rightarrow Qy)$, (if a natural number has Q then its successor has Q, i.e. Q is a 'hereditary' property)

then $(\forall x)(Nx \rightarrow Qx)$ (every natural number has Q)

These axioms together characterize the set of all natural numbers in certain important respects in which they differ from other infinite sets. Although we will not go into the proof here, it can be shown that this axiomatization of the natural numbers is also sufficient for proving the equivalence of the notions *ordinary infinite* and *Dedekind infinite*, which used only the notion of one-to-one correspondence, defined in Section 4.2.

The fifth Peano postulate is very important. It introduces the notion of *mathematical induction*. Intuitively, this axiom says that the natural numbers are subject to the 'domino-effect': whenever you find a property

that knocks down zero, and makes each number knock down its successor, you can conclude that all numbers are knocked down. There are no natural numbers outside this single infinite chain. The first four axioms guarantee the existence of an infinite chain of successors starting at zero, but do not preclude the existence of additional natural numbers, e.g. a second infinite chain unconnected to the first. The fifth axiom precludes the existence of any more numbers than are required by the first four axioms.

Now let us look more closely at the Principle of Mathematical Induction and its application. Let us first restate the principle, i.e. Peano's fifth axiom, in a slightly simpler form by (i) suppressing the predicate N and assuming that our domain of quantification is restricted to just the natural numbers, and (ii) using the notation $S(\boldsymbol{x})$ to denote the successor of $\boldsymbol{x}$, something we can legitimately do since the first four axioms guarantee that the successor-of relation is a function.

For any predicate Q, if the following statements are both true of Q:

(8–26) 1. $Q0$
2. $(\forall \boldsymbol{x})(Q\boldsymbol{x} \rightarrow Q(S(\boldsymbol{x})))$

then the following statement is also true of Q:

3. $(\forall \boldsymbol{x})Q\boldsymbol{x}$

The similarity between (8-26) 1 and 2 and the base and recursion step, respectively, of a recursive definition is readily apparent. The Principle of Mathematical Induction is not a definition, however, but a rule of inference to be applied to statements about the integers. A proof that employs this rule of inference is known as a *proof by induction* or an *inductive proof*.

Let us examine the structure of such a proof in more detail. Suppose we have been given a predicate $P(\boldsymbol{x})$ such that (8-27) 1 and 2 hold. These form the premises of the argument.

(8–27) 1. $P(0)$
2. $(\forall \boldsymbol{x})(P(\boldsymbol{x}) \rightarrow P(\boldsymbol{x}+1))$

From $P(0)$ and a substitution instance of line 2

3. $P(0) \rightarrow P(1)$ 2, U.I.

we can derive

4. $P(1)$ 1, 3, M.P.

and from this and another substitution instance of line 2

5. $P(1) \rightarrow P(2)$ 2, U.I.

we can derive

6 $P(2)$ 4, 5, M.P

and so on

To prove the statement $(\forall x)P(x)$ would require an infinite number of steps, and we would ordinarily not want to consider an infinitely long sequence of lines a proof, if for no other reason than that it would be impossible to examine it in order to verify its correctness. Thus, there is no proof of $(\forall x)P(x)$ that can be constructed by using only the rules of inference we have considered up to now. Nevertheless, (8-26) 3 is intuitively a valid conclusion to draw from the premises (8-26) 1 and 2, and the Principle of Mathematical Induction is a formal assertion that this inference is legitimate. It should be noted that the Principle of Mathematical Induction itself is not susceptible of proof but only acceptance or rejection on the grounds of its effectiveness in separating intuitively valid from intuitively invalid arguments. With this additional rule of inference, the proof of $(\forall x)P(x)$ is simply as follows:

(8–28)
1. $P(0)$
2. $(\forall x)(P(x) \rightarrow P(x+1))$
3 $(\forall x)(P(x))$ 1, 2, Math. Ind.

As an example we prove by induction that for every integer n the sum of the series $0 + 1 + 2 + \ldots + (n-1) + n$ equals $[n(n+1)]/2$.

The premises of the argument are the propositions stating all the usual arithmetic properties of the integers (the commutativity of addition, etc), which can be deduced as theorems from Peano's Axioms. As is usual in inductive proofs almost all the work comes in establishing the truth of the statements corresponding to (8-28) 1 and 2, known as the *base* and the *induction step*, respectively. Once these have been derived, the remainder of the proof consists of just one inferential step justified by the Principle of Mathematical Induction. We begin by demonstrating the truth of the base, i.e., that $0 + 1 + \ldots + n = [n(n+1)]/2$ is true for $n = 0$. In this case the sequence to the left of the equals sign consists of just 0, and the expression to the right becomes $[0(0+1)]/2$, which is equal to 0.

The induction step to be established is

$$(8\text{–}29) \quad (\forall n)\left(0 + 1 + \ldots + n = \frac{n(n+1)}{2} \rightarrow 0 + 1 + \ldots + n + (n+1) = \frac{(n+1)(n+1+1)}{2}\right)$$

that is, if the equation is true for any integer n, it is also true for $n+1$, the successor of n. To prove (8-29) we use a conditional proof in which we assume the antecedent of the conditional in (8-29) for an arbitrary integer k.

(8-30) 1 $0+1+\ldots+k=\dfrac{k(k+1)}{2}$ C.P.

2. $0+1+\ldots+k+(k+1)=\dfrac{k(k+1)}{2}+(k+1)$
1, adding $(k+1)$ to both sides

3 $0+1+\ldots+k+(k+1)=\dfrac{k(k+1)+2(k+1)}{2}$
2, converting right side to common denominator

4. $0+1+\ldots+k+(k+1)=\dfrac{(k+1)(k+2)}{2}$
3, factoring $(k+1)$ in numerator

5. $0+1+\ldots+k+(k+1)=\dfrac{(k+1)((k+1)+1)}{2}$
4, expressing $k+2$ as $(k+1)+1$

6. $0+1+\ldots+k=\dfrac{k(k+1)}{2}\rightarrow$
$0+1+\ldots+k+(k+1)=\dfrac{(k+1)(k+1)+1}{2}$

Since k was chosen arbitrarily, line 6 can be universally generalized to (8-29). Having now established the truth of the base and the induction step, the Principle of Mathematical Induction allows us to conclude:

(8-31) $$(\forall n)\left(0+1+\ldots+n=\frac{n(n+1)}{2}\right)$$

Proof by induction can be applied not only to theorems about the set of integers but to theorems about any set that can be put into one-to-one correspondence with the integers, i.e., the denumerably infinite sets. As an example of this sort we prove a generalized form of the Distributive Law for union and intersection of sets.

(8-32) $A\cup(B_1\cap B_2\cap\ldots\cap B_n)=(A\cup B_1)\cap(A\cup B_2)\cap\ldots\cap(A\cap B_n)$

The form in which the Distributive Law was given in Chapter 2 is a special case of (8-32) in which $n = 2$; that is

$$(8\text{–}33) \quad A \cup (B_1 \cap B_2) = (A \cup B_1) \cap (A \cup B_2)$$

Equation (8-32) is meaningless for $n = 0$ and trivial for $n = 1$ We take as the base of the inductive proof that (8-32) holds for $n = 2$, i.e., that (8-33) is true. This is easily shown by expressing the sets in terms of predicates and applying the Distributive Law of disjunction over conjunction in statement logic.

To prove the induction step we assume that (8-32) holds for an arbitrarily chosen integer k:

$$(8\text{–}34) \quad A \cup (B_1 \cap B_2 \cap \ldots \cap B_k) = (A \cup B_1) \cap (A \cup B_2) \cap \ldots \cap (A \cup B_k)$$

We wish to show that (8-34) implies (8-35).

$$(8\text{–}35) \quad A \cup (B_1 \cap B_2 \cap \ldots \cap B_{k+1}) = (A \cup B_1) \cap (A \cup B_2) \cap \ldots \cap (A \cup B_k) \cap (A \cup B_{k+1})$$

The left side of (8-35) can be rewritten by the Associative Law as

$$(8\text{–}36) \quad A \cup ((B_1 \cap B_2 \cap \ldots \cap B_k) \cap B_{k+1})$$

which is equal to

$$(8\text{–}37) \quad (A \cup (B_1 \cap B_2 \cap \ldots \cap B_k)) \cap (A \cup B_{k+1})$$

by an application of the Distributive Law for the case $n = 2$, which has already been proved By the induction hypothesis (8-34), expression (8-37) is equal to

$$(8\text{–}38) \quad ((A \cup B_1) \cap (A \cup B_2) \cap \ldots \cap (A \cup B_k)) \cap (A \cup B_{k+1})$$

By the Associative Law we can omit one set of parentheses to obtain the right side of (8-35). This shows that (8-35) holds if (8-34) does. From this and the base by the Principle of Mathematical Induction the generalized form of the Distributive Law is shown to be true for all n equal to or greater than 2 (or greater than 1 if we include this trivial case).

In this last example induction is used to prove a theorem about a class of equations of the form given in (8-32), which can be put into one-to-one correspondence with the integers. The mapping is between an equation and an integer n representing its length—specifically, the number of terms in the expression $B_1 \cap B_2 \cap \ldots \cap B_n$. Proof by induction on the length of a string is the commonest use of this method of proof in mathematical linguistics

Problem: Prove by induction the following generalized form of one of DeMorgan's Laws:

$$(A_1 \cap A_2 \cap \ldots \cap A_n)' = A_1' \cup \ldots \cup A_n'$$