

them (together with the set-theoretic principles we have already met) it is possible to define integers, rational numbers, real numbers, and complex numbers, and to derive their usual arithmetic and analytic properties. Such a program is not within the scope of this book; the interested reader should have no difficulty in locating and studying it elsewhere.

Induction is often used not only to prove things but also to define things. Suppose, to be specific, that f is a function from a set X into the same set X , and suppose that a is an element of X . It seems natural to try to define an infinite sequence $\{u(n)\}$ of elements of X (that is, a function u from ω to X) in some such way as this: write $u(0) = a$, $u(1) = f(u(0))$, $u(2) = f(u(1))$, and so on. If the would-be definer were pressed to explain the "and so on," he might lean on induction. What it all means, he might say, is that we define $u(0)$ as a , and then, inductively, we define $u(n^+)$ as $f(u(n))$ for every n . This may sound plausible, but, as justification for an existential assertion, it is insufficient. The principle of mathematical induction does indeed prove, easily, that there can be at most one function satisfying all the stated conditions, but it does not establish the existence of such a function. What is needed is the following result.

Recursion theorem. *If a is an element of a set X , and if f is a function from X into X , then there exists a function u from ω into X such that $u(0) = a$ and such that $u(n^+) = f(u(n))$ for all n in ω .*

Proof. Recall that a function from ω to X is a certain kind of subset of $\omega \times X$; we shall construct u explicitly as a set of ordered pairs. Consider, for this purpose, the collection \mathcal{C} of all those subsets A of $\omega \times X$ for which $(0, a) \in A$ and for which $(n^+, f(x)) \in A$ whenever $(n, x) \in A$. Since $\omega \times X$ has these properties, the collection \mathcal{C} is not empty. We may, therefore, form the intersection u of all the sets of the collection \mathcal{C} . Since it is easy to see that u itself belongs to \mathcal{C} , it remains only to prove that u is a function. We are to prove, in other words, that for each natural number n there exists at most one element x of X such that $(n, x) \in u$. (Explicitly: if both (n, x) and (n, y) belong to u , then $x = y$.) The proof is inductive. Let S be the set of all those natural numbers n for which it is indeed true that $(n, x) \in u$ for at most one x . We shall prove that $0 \in S$ and that if $n \in S$, then $n^+ \in S$.

Does 0 belong to S ? If not, then $(0, b) \in u$ for some b distinct from a . Consider, in this case, the set $u - \{(0, b)\}$. Observe that this diminished set still contains $(0, a)$ (since $a \neq b$), and that if the diminished set contains (n, x) , then it contains $(n^+, f(x))$ also. The reason for the second assertion is that since $n^+ \neq 0$, the discarded element is not equal to

$(n^+, f(x))$. In other words, $u - \{(0, b)\} \in \mathcal{C}$. This contradicts the fact that u is the smallest set in \mathcal{C} , and we may conclude that $0 \in S$.

Suppose now that $n \in S$; this means that there exists a unique element x in X such that $(n, x) \in u$. Since $(n, x) \in u$, it follows that $(n^+, f(x)) \in u$. If n^+ does not belong to S , then $(n^+, y) \in u$ for some y different from $f(x)$. Consider, in this case, the set $u - \{(n^+, y)\}$. Observe that this diminished set contains $(0, a)$ (since $n^+ \neq 0$), and that if the diminished set contains (m, b) , say, then it contains $(m^+, f(b))$ also. Indeed, if $m = n$, then t must be x , and the reason the diminished set contains $(n^+, f(x))$ is that $f(x) \neq y$; if, on the other hand, $m \neq n$, then the reason the diminished set contains $(m^+, f(t))$ is that $m^+ \neq n^+$. In other words, $u - \{(n^+, y)\} \in \mathcal{C}$. This again contradicts the fact that u is the smallest set in \mathcal{C} , and we may conclude that $n^+ \in S$.

The proof of the recursion theorem is complete. An application of the recursion theorem is called *definition by induction*.

EXERCISE. Prove that if n is a natural number, then $n \neq n^+$; if $n \neq 0$, then $n = m^+$ for some natural number m . Prove that ω is transitive. Prove that if E is a non-empty subset of some natural number, then there exists an element k in E such that $k \in m$ whenever m is an element of E distinct from k .

Halmos