Recursion, Arithmetic

Please read LST 80-86 or NST 95-103.

Theorem 1. *(Recursion on $\mathbb{N}$) Assume that A is a set, $a_0 \in A$, and $g\colon \mathbb{N} \times A \to A$ is a function. There is a unique function $f\colon \mathbb{N} \to A$ satisfying the conditions*

(1) $f(0) = a_0$, *and*
(2) $f(S(n)) = g(n, f(n))$.

We say that f is defined by recursion (from g). (For a generalization of this theorem, see Theorem 8.7 of NST/LST.)

Example 2. The following data defines a unique function $f\colon \mathbb{N} \to \mathbb{N}$.

(1) $f(0) = 1$, and
(2) $f(S(n)) = S(n) \cdot f(n)$.

We typically write this function $f(n) = n!$.

Generalizations of Theorem 1.

(1) Recursion with parameters.
(2) Course-of-values recursion.
(3) Definition by recursion using well-founded set-like relations in place of $\langle \mathbb{N}; < \rangle$.

Application: Definitions and Laws of Arithmetic.

Addition

$$\begin{aligned} m+0 &:= m && \text{(IC)} \\ m+S(n) &:= S(m+n) && \text{(RR)} \end{aligned}$$

Multiplication

$$\begin{aligned} m \cdot 0 &:= 0 && \text{(IC)} \\ m \cdot S(n) &:= m \cdot n + m && \text{(RR)} \end{aligned}$$

Exponentiation

$$\begin{aligned} m^0 &:= 1 && \text{(IC)} \\ m^{S(n)} &:= m^n \cdot m && \text{(RR)} \end{aligned}$$

Each of these operations is defined by recursion on its *second* variable with the first variable as a parameter.

Exercises. Prove the statements below.

Laws of successor.

(a) 0 is not a successor. Every nonzero natural number is a successor.
(b) Successor is injective. ($S(m) = S(n)$ implies $m = n$.)

Laws of addition.

(a) $S(n) = n + 1$
(b) (Associative Law) $m + (n + k) = (m + n) + k$
(c) (Unit Law for 0) $m + 0 = 0 + m = m$
(d) (Commutative Law) $m + n = n + m$
(e) (+-Irreducibility of 0) $m + n = 0$ implies $m = n = 0$.
(f) (Cancellation) $m + k = n + k$ implies $m = n$.

Laws of multiplication (and addition).

(a) (Associative Law) $m \cdot (n \cdot k) = (m \cdot n) \cdot k$
(b) (Unit Law for 1) $m \cdot 1 = 1 \cdot m = m$
(c) (Commutative Law) $m \cdot n = n \cdot m$
(d) (0 is absorbing) $m \cdot 0 = 0 \cdot m = 0$
(e) (·-Irreducibility of 1) $m \cdot n = 1$ implies $m = n = 1$
(f) (Distributive Law) $m \cdot (n + k) = (m \cdot n) + (m \cdot k)$

Laws of exponentiation (and multiplication and addition).

(a) $m^0 = 1$, $m^1 = m$, $0^m = 0$ (if $m > 0$), and $1^m = 1$.
(b) $m^{n+k} = m^n \cdot m^k$
(c) $(m \cdot n)^k = m^k \cdot n^k$
(d) $(m^n)^k = m^{n \cdot k}$