Natural Numbers

Mariusz Wodzicki

October 12, 2023

Contents

1 The category of twisted objects $\mathcal{C}^{\langle 1\rangle}$

1.1 Twisted objects

1.1.1

Let $c \in \operatorname{Ob}\mathcal{C}$ be an object of a category $\mathcal{C}$ and

$$\tau \in \operatorname{End}_{\mathcal{C}} c$$

be its endomorphism. We shall refer to (c,τ) as a *twisted object* (in $\mathcal{C}$).

1.1.2 Morphisms between twisted objects

Given two *twisted objects* (c,τ) and (c',τ'), a morphism $\alpha \in \operatorname{Hom}_{\mathcal{C}}(c,c')$ defines a *morphism*

$$(c,\tau) \longrightarrow (c',\tau')$$

if $\alpha\circ\tau = \tau'\circ\alpha$, i.e., if the following diagram commutes

$$\begin{tikzcd}
c \arrow[r, "\alpha"] & c' \\
c \arrow[u, "\tau"] \arrow[r, "\alpha"] \arrow[ur, phantom, "\circlearrowright"] & c' \arrow[u, "\tau'"']
\end{tikzcd}$$

1.1.3

We shall denote the category of twisted objects in $\mathcal{C}$ by $\mathcal{C}^{\langle 1\rangle}$.

1.2 The category of unary structures

1.2.1 $\mathbf{Set}^{\langle 1\rangle}$

The category of *twisted sets* is the same as the category of *unary algebraic structures*. We shall denote it $\mathbf{Set}^{\langle 1\rangle}$.

1.2.2 Example: the canonical unary structure $(X,{}^{+})$ on a well-ordered set $(X,\preccurlyeq)$

Let $(X,\preccurlyeq)$ be a well-rdered set. We define the associated *successor operation* as follows

$$x \;\longmapsto\; x^{+} := \inf\{y \in X \mid x \prec y\} \qquad (x \in X)\,. \tag{1}$$

Exercise 1 *Show that*

$$x^{+} = \begin{cases} x & \text{\textit{when x is the greatest element of} } (X,\preccurlyeq) \\ \min\{y \in X \mid x \prec y\} & \text{\textit{otherwise}} \end{cases} \tag{2}$$

Solution. In any ordered set $(X, \preccurlyeq)$ the infimum of the empty subset is the greatest element of $(X, \preccurlyeq)$ and the set

$$\{y \in X \mid x \prec y\} \tag{3}$$

is empty precisely when x is a *maximal* element of $(X, \preccurlyeq)$. A well-ordered set is linearly ordered, hence any two maximal elements are equal. In particular, a maximal element in a well-ordered set is the greatest element of $(X, \preccurlyeq)$.

Any other element x' is *smaller* than the greatest element, hence

$$\{y \in X \mid x' \prec y\}$$

is not empty. In a well-ordered set every nonempty subset has the smallest element, hence

$$\inf\{y \in X \mid x' \prec y\} = \min\{y \in X \mid x' \prec y\}\,.$$

□

1.2.3 Invariant subsets

We say that a subset $A \subseteq X$ is *invariant under* τ or, τ*-invariant*, if $\tau_* A \subseteq A$, i.e., if

$$\tau(x) \in A \qquad (x \in A)\,. \tag{4}$$

1.2.4 A remark about notation

Displayed expression (4) is an abreviated form of the statement:

$$\tau(x) \in A \quad \textit{whenever} \quad x \in A\,.$$

Equivalently, the same can be stated as

$$\textit{for every } x \in A\textit{, one has } \tau(x) \in A$$

and, in an abbreviated form,

$$\forall_{x \in A}\, \tau(x) \in A\,.$$

1.2.5

A subset A of X is invariant if and only if the diagram

$$\begin{tikzcd}
A \arrow[r, hook] & X \\
A \arrow[r, hook] & X \arrow[u, "\tau"']
\end{tikzcd}$$

admits a completion to a commutative diagram

$$\begin{tikzcd}
A \arrow[r, hook] & X \\
A \arrow[r, hook] \arrow[u] \arrow[ur, phantom, "\circlearrowright"] & X \arrow[u, "\tau"']
\end{tikzcd}$$

1.2.6 The *induced* operation on an invariant subset

The operation represented by the blue arrow is unique. We refer to it as the operation *induced by* τ *on* A.

Indeed, if τ' and τ'' are two such operations and ι denotes the canonical inlusion of X' into X, then

$$\iota \circ \tau' = \tau \circ \iota = \iota \circ \tau''.$$

Since ι is *injective*, it is a monomorphism in the category of sets. Hence, $\tau' = \tau''$.

Generally, the induced operation on an invariant subset $A \subseteq X$ is denoted τ, the same way as the operation on X.

Exercise 2 *Show that, for any homomorphism* $f : (X, \tau) \longrightarrow (X', \tau')$, *one has*

$$f_*(\tau_* X) \subseteq \tau'_* X'. \tag{5}$$

Exercise 3 *Show that* $\tau_* X$ *is an invariant subset of* (X, τ).

2 The category of nullary-unary structures

2.1 $\mathbf{Set}^{\langle 01\rangle}$

2.1.1 Objects

We shall denote by $\mathbf{Set}^{\langle 01\rangle}$ the category of *algebraic structures* consisting of a set X equipped with a single *nullary* operation, i.e., a distinguished element

$$a \in X,$$

and a single *unary* operation

$$\tau\colon X \to X.$$

2.1.2 Morphisms

Homomorphisms $f\colon (X,a,\tau) \longrightarrow (X',a',\tau')$, i.e., functions $f : X \to X'$ such that

$$f(a) = a'$$

and

$$f(\tau(x)) = \tau'(f(x)) \qquad (x \in X),$$

are declared to be morphisms.

2.1.3 Example: $(X, \min X, {}^{+})$

If $(X, \preccurlyeq)$ is a nonempty well-rdered set, then $(X, \min X, {}^{+})$ is nullary-unary structure. We shall refer to it as the *canonical nullary-unary* structure of a well-ordered set.

2.1.4 Example: $\big(\mathrm{End}_{\mathcal{C}^{\langle 1\rangle}}(c,\tau), \tau, \tau_{\bullet}\big)$

For any twisted object (c,τ), post-composition with τ,

$$\lambda \longmapsto \tau_{\bullet}\lambda := \tau \circ \lambda \qquad (\lambda \in \mathrm{End}_{\mathcal{C}^{\langle 1\rangle}} c)$$

defines a unary operation $\tau_{\bullet}$ on the set $X = \mathrm{End}_{\mathcal{C}^{\langle 1\rangle}}(c,\tau)$ of endomorphisms of (c,τ) while τ is a distinguished element of $\mathrm{End}_{\mathcal{C}^{\langle 1\rangle}}(c,\tau)$.

2.1.5 Example: $\big(\mathrm{End}_{\mathcal{C}^{\langle 1\rangle}}(c,\tau), \mathrm{id}_c, \tau_{\bullet}\big)$

If c admits an identity endomorphism, then id_c is another distinguished element of $\mathrm{End}_{\mathcal{C}^{\langle 1\rangle}}(c,\tau)$.

2.2 An initial object of $\mathbf{Set}^{\langle 01\rangle}$

2.2.1 $(N, 0, \sigma)$

In this chapter $(N, 0, \sigma)$ denotes an initial object of category $\mathbf{Set}^{\langle 01\rangle}$.

2.2.2

Since **Set**$^{\langle 01\rangle}$ is a unital category, any two initial objects in **Set**$^{\langle 01\rangle}$ are isomorphic and such an isomorphism is *unique*. The question of existence of initial objects in **Set**$^{\langle 01\rangle}$ will be addressed later.

2.2.3 '0'

We shall denote the distinguished element of an initial object by 0 and will refer to the unary operation as the *successor operation*. To keep notation simple, we will often omit the parentheses around the argument of σ when the argument is denoted by a single symbol.

2.2.4 '1', '2', etc.

It is convenient to have separate notation for $\sigma 0$ and $\sigma(\sigma 0)$: we shall denote $\sigma 0$ by digit 1 and $\sigma 1$ by digit 2. We can similarly denote $\sigma 2$ by digit 3, and so on.

2.3 *Minimal* algebraic structures

2.3.1

We shall say that an algebraic structure $\bigl(X, (\mu_i)_{i\in I}\bigr)$ is *minimal* if X is the *only* subset of X that is closed under each operation μ_i. If we separate nullary and nonnullary operations,

$$I = I_0 \cup I_{>0},$$

where

$$\forall_{i\in I_0} \operatorname{arity}(\mu_i) = 0 \qquad \text{and} \qquad \forall_{i\in I_{>0}} \operatorname{arity}(\mu_i) > 0,$$

then $\bigl(X, (\mu_i)_{i\in I}\bigr)$ is a minimal structure precisely when the set of *distinguished elements*

$$\{\mu_i \mid i \in I_0\}$$

generates the algebraic structure $\bigl(X, (\mu_i)_{i\in I_{>0}}\bigr)$.

In particular, a minimal algebraic structure is nonempty precisely when at least one operation μ_i is nullary.

2.3.2 Initial objects in the categories of algebraic structures are minimal

The following lemma is a simple corollary of the definitions of an initial object and of a minimal algebraic structure.

Lemma 2.1 *An initial object in the category of algebraic structures of any type is a minimal structure.*

Proof. Suppose that an algebraic structure $\bigl(X, (\mu_i)_{i\in I}\bigr)$ is an initial object and let $A \subseteq X$ be a subset closed under all operations μ_i. Then, the canonical inclusion $\iota : A \hookrightarrow X$ is a homomorphism. In view of $\bigl(X, (\mu_i)_{i\in I}\bigr)$ being an initial object, there exists a homomorphism $f : X \to A$. The composite $\iota \circ f$ is an endomorphism of $\bigl(X, (\mu_i)_{i\in I}\bigr)$. An initial object in a unital category has only one endomorphism, namely the identity endomorphism. It follows that

$$\iota \circ f = \mathrm{id}_X \ .$$

In particular, ι is surjective and this means that $A = X$. □

2.3.3 The Principle of Mathematical Induction

In the special case of nullary-unary structures, we obtain the following corollary.

Corollary 2.2 (The Principle of Mathematical Induction) *If $E \subseteq N$, $0 \in E$ and $\sigma_* E \subseteq E$, then $E = N$.*

Corollary 2.3 *One has*

$$N = \{0\} \cup \sigma_* N\,. \tag{6}$$

In other words, if $n \neq 0$, then there exists $m \in N$ such that $\sigma m = n$.

Proof. The subset $E = \{0\} \cup \sigma_* N$ is closed under 0 and σ, hence Corollary 2.2 applies. □

2.3.4

Consider the canonical nullary-unary structure $(X, a, {}^+)$ of the well-ordered set $X = \{a, b\}$ where $a \prec b$.

Exercise 4 *Show that the unique homomorphism*

$$f : (N, 0, \sigma) \longrightarrow (X, a, {}^+)$$

sends every $n \neq 0$ to b.

Solution. In view of Corollary 2.3, every $n \neq 0$ belongs to $\sigma_* N$. By Exercise 2

$$f_*(\sigma_* N) \subseteq (\ )^+_* X = \{b\}\,.$$

□

Corollary 2.4 *One has*

$$0 \notin \sigma_* N\,. \tag{7}$$

In particular,

$$N \supsetneq \sigma_* N\,. \tag{8}$$

Lemma 2.5 *Let X be a set and $f : X \longrightarrow \mathscr{P}X$ be any function Then the subset*

$$A := \{x \mid x \notin f(x)\} \tag{9}$$

is not in the image of f. In particular, f is not surjective.

Exercise 5 *Prove Lemma 2.5.*

Corollary 2.6 *For every set X, there exists a set Y such that $X \neq Y$.*

Proof. Suppose that there exists a set X, such that every set Y is a subset of X. Then

$$\mathscr{P}X \subseteq X\,.$$

If so, then the function

$$f : X \longrightarrow \mathscr{P}X\,, \qquad f(x) = \begin{cases} x & \text{if } x \in \mathscr{P}X \\ \emptyset & \text{otherwise} \end{cases}\,.$$

is surjective. That contradicts Lemma 2.5. □

Corollary 2.7 *For every set X, there exists a set $X' \neq X$ such that*

$$X' = X \cup \{y\}\,.$$

Proof. A set Y is not equal to a set X precisely when there exists $y \in Y$ such that $y \notin X$. Thus, the set $X \cup \{y\}$ is not equal to X. □

2.3.5

Recall that a set X is *infinite* if there exists a left-invertible unary operation $\tau \in \mathrm{Op}_1 X$ that is not rright-invertible.

Exercise 6 *Show that $\tau \in \mathrm{Op}_1 X$ is left-invertible and not right-invertible if and only if τ is injective and $X \supsetneq \tau_* X$.*

Theorem 2.8 *If $(N, 0, \sigma)$ is an initial object in the category of nullary-unary structures, then σ is injective and*

$$N \setminus \sigma_* N = \{0\}\,. \tag{10}$$

In particular, N is an infinite set.

Proof. In view of Corollary 2.7, there exists a set

$$N' = N \cup \{y\}$$

such that $y \notin N$. Let $f : N' \longrightarrow N$ be the function

$$f(x) = \begin{cases} \sigma x & \text{if } x \in N \\ 0 & \text{if } x = y \end{cases}$$

and $\tau = \iota \circ f$ be the composite of f and the canonical inclusion $\iota : N \hookrightarrow N'$.

Exercise 7 *Show that f is a homomorphism $(N', y, \tau) \longrightarrow (N, 0, \sigma)$.*

The composite of f with the unique homomorphism

$$g : (N, 0, \sigma) \longrightarrow (N', y, \tau) \tag{11}$$

is an endomorphism of $(N, 0, \sigma)$ and, therefore, is the identity function,

$$f \circ g = \mathrm{id}_N \,. \tag{12}$$

Consider the subset of N,

$$E = \{n \in N \mid g(\sigma n) = n\}\,.$$

Since g is a homomorphism (11), one has

$$g(1) = g(\sigma 0) = \tau(g(0)) = \tau(y) = 0\,,$$

i.e., $0 \in E$. If $n \in N$, then

$$g(\sigma\sigma n) = \tau(g(\sigma n)) = \tau(n) = \sigma n\,,$$

i.e., $\sigma n \in E$. By Corollary 2.2, one has $E = N$. It follows that

$$\pi : N \longrightarrow N\,, \qquad \pi(n) = \begin{cases} g(n) & \text{if } n \in \sigma_* N \\ 0 & \text{if } n = 0 \end{cases} \tag{13}$$

is a left-inverse of σ. In view of $0 \notin \sigma_* N$, cf. Corollary 2.4, successor operation σ is not surjective and, thus, is not right-invertible. □

2.3.6 The *predecessor* operation

We shall refer to the left-inverse of σ defined in (13) as the *predecessor* operation.

Note that g is, by definition, surjective. In view of Identity (12), g is injective, hence g is an isomorphism and f is its inverse.

2.4 Recursively defined sequences

2.4.1 ‘Sequences’

Any function

$$N \longrightarrow X, \qquad n \longmapsto x_n \qquad (n \in N),$$

from the underlying set of an initial object to a set X will be called a *sequence of elements of* X. Generic notation for a sequence is $(x_n)_{n \in N}$ or, in an abbreviated form, (x_n).

2.4.2 A recursive definition

We say that a sequence (x_n) is *recursively defined* if there are given: an element $a \in X$, and a sequence of unary operations (τ_n) on X, such that

$$x_0 = a \tag{14}$$

and

$$x_{\sigma n} = \tau_n(x_n) \qquad (n \in N)\,. \tag{15}$$

2.4.3 Recursive data: the *initial term* and the *recursive step sequence*

Here, a is called the *initial term* of the sequence while (τ_n) is referred to as the *recursive step sequence*. We shall refer to (14) as the *initial condition* and to (15) as the *recursive step condition*.

2.4.4 Uniqueness of a recursively defined sequence

Uniqueness of a sequence defined by given recursive data is an immediate consequence of Corollary 2.2.

Lemma 2.9 *If* (x_n) *and* (x'_n) *are two sequences defined by the same recursive data, cf.* (14)–(15)*, then they are equal.*

Proof. Consider the set

$$E = \{n \in N \mid x_n = x'_n\}.$$

The two sequences satisfy the same initial condition precisely when $0 \in E$. For any $n \in E$, we have

$$x_{\sigma n} = \tau_n(x_n) = \tau_n(x'_n) = x'_{\sigma n},$$

since both sequences satisfy the same recursive step condition. It follows that $E = N$, cf. Corollary 2.2. □

2.4.5

A homomorphism

$$\mathbf{x} : (N, 0, \sigma) \longrightarrow (X, a, \tau), \qquad n \longmapsto x_n,$$

in $\mathbf{Set}^{\langle 01 \rangle}$ is the same as a sequence (x_n) defined by recursive data with the *constant* recursive step sequence

$$\tau_n = \tau \qquad (n \in N).$$

Existence as well as uniqueness of such a sequence is, therefore, equivalent to $(N, 0, \sigma)$ being an initial object of category $\mathbf{Set}^{\langle 01 \rangle}$.

2.4.6

Existence of a sequence defined by *any* recursive step sequence will be established later.

2.5 Powers of an element in a binary structure

2.5.1 The left-multiplication-by-an-element operation

Let $(B, \cdot)$ be a *binary structure* and λ_b be the operation on the underlying set B

$$x \longmapsto \lambda_b(x) := bx \qquad (x \in B), \tag{16}$$

that multiplies an element $x \in B$ on the left by a given element $b \in B$.

2.5.2 The left powers sequence

Let (p_n) be the sequence in B defined by the unique homomorphism

$$\mathbf{p} : (N, 0, \sigma) \longrightarrow (B, b, \lambda_b) . \tag{17}$$

Note that

$$p_0 = b, \quad p_1 = b{\cdot}b, \quad p_2 = b(b{\cdot}b), \quad p_3 = b(b(b{\cdot}b)), \quad \dots$$

2.5.3 The centralizer of an element

The set of elements $x \in B$ that commute with a given element $a \in B$,

$$C_a(B, \cdot) := \{x \in B \mid ax = xa\}, \tag{18}$$

is called the *centralizer of* a.

Exercise 8 *Show that the monoid of endomorphisms of a twisted set* (X, τ) *coincides with the centralizer of* τ,

$$\mathrm{End}_{\mathbf{Set}^{(1)}}(X, \tau) = C_\tau\left(\mathrm{Op}_1 X, \circ\right) ,$$

in the monoid of unary operations on X

$$\mathrm{Op}_1 X := \mathrm{End}_{\mathbf{Set}} X .$$

Exercise 9 *Suppose that binary operation* $\cdot$ *is associative. Show that the centralizer of every element is closed under operation* $\cdot$.

In other words, the centralizer of every element in a semigroup is a subsemigroup.

2.5.4

In particular, in a semigroup, if a commutes with b, then the centralizer $C_a(B, \cdot)$ is invariant under λ_b. It follows that there exists a homomorphism

$$(N, 0, \sigma) \longrightarrow (C_a(B, \cdot), b, \lambda_b) . \tag{19}$$

Its composition with the inclusion homomorphism $C \hookrightarrow B$ must coincide, in view of $(N, 0, \sigma)$ being an initial object, with homomorphism (17). It follows that

$$p_n \in C_a(B, \cdot) \qquad (n \in N),$$

i.e.,

$$p_n a = a p_n \qquad (n \in N)$$

and we establish the following important fact.

Lemma 2.10 *In a semigroup:*

(a) *if* b *commutes with* a, *then each* p_n *commutes with* a;

(b) *powers* p_n *of any element commute with each other, i.e.,*

$$p_m p_n = p_n p_m \qquad (m, n \in N) . \tag{20}$$

Part (b) is a corollary of Part (a): b commutes with itself, hence b commutes with every p_n. This in turn, implies, by Part (a) again, that every p_m commutes with every p_n. □

2.5.5 The right powers sequence

Let (q_n) be the sequence in B defined by the unique homomorphism

$$\mathbf{q} : (N, 0, \sigma) \longrightarrow (B, b, \rho_b) \tag{21}$$

where ρ_b is the operation of right multiplication by b

$$x \longmapsto \rho_b(x) := xb \qquad (x \in B)\,. \tag{22}$$

Note that

$$q_0 = b\,, \quad q_1 = b{\cdot}b\,, \quad q_2 = (b{\cdot}b)b\,, \quad q_3 = ((b{\cdot}b)b)b\,, \quad \ldots$$

Exercise 10 *Show that in a semigroup the left and the right powers of an element coincide*

$$p_n = q_n \qquad (n \in N)\,.$$

Solution. Consider the set

$$E = \{n \in N \mid p_n = q_n\}\,.$$

The initial terms of both sequences coincide,

$$p_0 = b = q_0\,,$$

hence $0 \in E$. If $n \in E$, then

$$p_{\sigma n} = bp_n = p_n b = q_n = q_{\sigma n}$$

in view of the fact that p_n commutes with b, cf. Lemma 2.10. Thus, E is closed under 0 and σ and, by Corollary 2.2, $E = N$. □

2.5.6 Powers of an element in a monoid

Suppose that $e \in B$ is an identity element in a semigroup $(B, \cdot)$. Define the sequence (b^n) to be the unique homomorphism

$$\mathbf{b} : (N, 0, \sigma) \longrightarrow (B, e, \lambda_b)\,.$$

Note that

$$b^0 = e\,, \qquad b^1 = b^{\sigma 0} = b \cdot b^0 = b \cdot e = b\,, \qquad b^2 = \sigma^{\sigma 1} = b \cdot b^1 = b \cdot b\,, \qquad \ldots \tag{23}$$

2.5.7 A relation between the sequence of powers in a semigroup and in a monoid

Uniqueness of a homomorphism $(N, 0, \sigma) \longrightarrow (B, b, \lambda_b)$ implies that the following diagram

$$\begin{tikzcd}
 & (B, b, \lambda_b) \\
(N, 0, \sigma) \arrow[ur, "\mathbf{p}"] \arrow[dr, "\mathbf{b}"'] \arrow[r, phantom, "\circlearrowleft"] & \\
 & (B, e, \lambda_b) \arrow[uu, "\lambda_b"']
\end{tikzcd}$$

commutes. In other words,

$$p_n = \lambda_b(b^n) = b^{\sigma n} \qquad (n \in N)\,. \tag{24}$$

In particular, we have the following corollary of Lemma 2.10.

Corollary 2.11 *In a monoid:*

(a) *if b commutes with a, then each b^n commutes with a;*

(b) *if b commutes with a, then, for any $m, n \in N$, b^n commutes with a^m;*

(c) *powers b^n of any element commute with each other, i.e.,*

$$b^m b^n = b^n b^m \qquad (m, n \in N)\,. \tag{25}$$

Proof. If either m or n are equal 0, then one of the factors in Equality (25) is the identity element, hence that Equality holds. If both m and n are not zero, then there exist $k, l \in N$ such that

$$\sigma k = m \qquad \text{and} \qquad \sigma l = n\,,$$

cf. Corollary 2.3, and therefore

$$b^m b^n = p_k p_l = p_l p_k = b^n b^m\,,$$

in view of Identity (24) combined with Lemma 2.10.

Parts (b) and (c) are immediate consequences of Part (a). □

2.5.8 Injectivity and surjectivity of the powers of a unary operation

Let $\tau \in \mathrm{Op}_1$ be a unary operation on a set X.

Exercise 11 *Show that*

$$\textit{if } \tau \textit{ is injective, then } \tau^n \textit{ is injective for every } n \in N\,. \tag{26}$$

Exercise 12 *Show that*

$$\textit{if there exists } n \neq 0\textit{, such that } \tau^n \textit{ is injective, then } \tau \textit{ is injective.} \tag{27}$$

Exercise 13 *Show that*

$$\textit{if } \tau \textit{ is surjective, then } \tau^n \textit{ is surjective for every } n \in N\,. \tag{28}$$

Exercise 14 *Show that*

$$\textit{if there exists } n \neq 0\textit{, such that } \tau^n \textit{ is surjective, then } \tau \textit{ is surjective.} \tag{29}$$

2.6 The sequence of products of elements of a semigroup

2.6.1 $(B^N, \mathbf{b}, \lambda_{\mathbf{b}}\circ\sigma^\bullet)$

Consider the semigroup $(B^N, \cdot)$ of sequences of elements of a semigroup $(B,,)$ equipped with the unary operation

$$\lambda_{\mathbf{b}}\circ\sigma^\bullet : \mathbf{x} \longmapsto \lambda_{\mathbf{b}}(\sigma^\bullet \mathbf{x}) = (b_n x_{\sigma n})\,. \tag{30}$$

2.6.2

Let

$$(N, 0, \sigma) \longrightarrow \left(B^N, \mathbf{b}, \lambda_{\mathbf{b}} \circ \sigma^{\bullet}\right), \qquad m \longmapsto \mathbf{p}_m = (p_{mn})_{n \in N}, \tag{31}$$

be the unique homomorphism. It is a unique sequence-of-sequences of elements of B that satisfies the identity

$$\mathbf{p}_{\sigma m} = \mathbf{b}\sigma^{\bullet}\mathbf{p}_m \qquad (m \in N). \tag{32}$$

Lemma 2.12 *One has the identity*

$$\mathbf{p}_{\sigma m} = \mathbf{p}_m \left(\sigma^{\sigma m}\right)^{\bullet} \mathbf{b} \qquad (m \in N) \tag{33}$$

Explicitly, Identity (33) *has the form*

$$p_{\sigma m, n} = p_{mn} b_{\sigma^{\sigma m}(n)}, \qquad (mn, \in N). \tag{34}$$

Proof. Consider the set

$$E = \left\{ m \in N \mid \mathbf{p}_{\sigma m} = \mathbf{p}_m \left(\sigma^{\sigma m}\right)^{\bullet} \mathbf{b} \right\}.$$

One has

$$\mathbf{p}_{\sigma 0} = \mathbf{b}\sigma^{\bullet}\mathbf{p}_0 = \mathbf{b}\sigma^{\bullet}\mathbf{b} = \mathbf{p}_0 (\sigma^1)^{\bullet}\mathbf{b} = \mathbf{p}_0 (\sigma^{\sigma 0})^{\bullet}\mathbf{b},$$

i.e., $0 \in E$.

The following short calculation, where we use Identity (32) and assume that $m \in E$,

$$\mathbf{p}_{\sigma\sigma m} = \mathbf{b}\sigma^{\bullet}\mathbf{p}_{\sigma m} = \mathbf{b}\sigma^{\bullet}\left(\mathbf{p}_m \left(\sigma^{\sigma m}\right)^{\bullet}\mathbf{b}\right) = \left(\mathbf{b}\sigma^{\bullet}\mathbf{p}_m\right)\left(\sigma^{\bullet} \circ \left(\sigma^{\sigma m}\right)^{\bullet}\mathbf{b}\right) = \mathbf{p}_{\sigma m}\left(\sigma^{\sigma\sigma m}\right)^{\bullet}\mathbf{b} \qquad (m \in N),$$

demonstrates that $\sigma m \in E$. Invocation of Corollary 2.2 proves that $E = N$. □

2.6.3 The (right) product sequence $\left(\prod_{i=0}^{n} b_i\right) = (b_0 \cdots b_n)$

Sequence Q_n, traditionally denoted

$$\prod_{i=0}^{n} b_i \qquad \text{or} \qquad b_0 \cdots b_n,$$

is defined by the recursive data

$$Q_0 = b_0 \qquad \text{and} \qquad Q_{\sigma n} = Q_n b_{\sigma n} \qquad ({}_n\!\in N). \tag{35}$$

By substituting $n = 0$ into Identity (32) and noticing that

$$\sigma^{\sigma m}(0) = \sigma m,$$

we obtain the following corollary.

Corollary 2.13 *One has*

$$\prod_{i=0}^{m} b_i = p_{m0} \qquad (m \in N).$$

In particular, the product sequence exists for any sequence (b_n) *of elements in a semigroup.*

□

2.6.4 The (left) product sequence $\left(\prod_{i=n}^{0} b_i\right) = (b_n \cdots b_0)$

The left product sequence P_n is defined by the recursive data

$$P_0 = b_0 \qquad \text{and} \qquad P_{\sigma_n} = b_{\sigma_n} P_n \qquad ({}_n\in N)\,. \tag{36}$$

The left product sequence coincides with the (right) product sequence in the *opposite* semigroup $(B,,)^{\mathrm{op}}$.

2.6.5 The sum sequence $\left(\sum_{i=0}^{n} b_i\right) = (b_0 + \cdots + b_n)$

In a commutative semigroup the product sequence becomes, in additive notation, the *sum sequence*, denoted

$$\sum_{i=0}^{n} b_i \qquad \text{or} \qquad b_0 + \cdots + b_n \qquad (n \in N)\,. \tag{37}$$

Proposition 2.14 *For any recursive data* (14)–(15)*, there exists a unique sequence defined by those data.*

Proof. Let

$$\bar{\tau}_n = \begin{cases} \tau_m & \text{if } \sigma m = n \\ \mathrm{id}_X & \text{if } n = 0 \end{cases}$$

and

$$T_n = \bar{\tau}_n \circ \cdots \circ \bar{\tau}_0 \qquad (n \in N)$$

be the left product sequence in the semigroup of unary operations $(\mathrm{Op}_1 X, \circ)$. The sequence

$$x_n := T_n(x_0) \qquad (n \in N) \tag{38}$$

satisfies recursive data (14)–(15). Uniqueness was proved earlier, cf. Lemma 2.9. □

2.7 Homomorphisms $(N, \sigma) \longrightarrow (X, \tau)$

2.7.1

Any homomorphism

$$\mathbf{x} : (N, \sigma) \longrightarrow (X, \tau) \tag{39}$$

of twisted sets is simultaneously a homomorphism of nullary-unary structures

$$(N, 0, \sigma) \longrightarrow (X, x, \tau) \tag{40}$$

where $x := x_0$. Thus, the set of homomorphisms (39) is the union

$$\mathrm{Hom}_{\mathbf{Set}^{\langle 1\rangle}}((N, \sigma), (X, \tau)) \;=\; \bigcup_{x \in X} \mathrm{Hom}_{\mathbf{Set}^{\langle 1\rangle}}\big((N, 0, \sigma), (X, x, \tau)\big) \tag{41}$$

of the disjoint family, indexed by elements of X, of the sets of homomorphisms (40).

2.7.2

Each set

$$\mathrm{Hom}_{\mathbf{Set}^{\langle 1\rangle}}\big((N, 0, \sigma), (X, x, \tau)\big)$$

has exactly one element, namely the unique homomorphism (40). We established the following important fact.

Lemma 2.15 *For every twisted set* (X, τ)*, there exists a canonical bijective correspondence*

$$\mathrm{Hom}_{\mathbf{Set}^{\langle 1\rangle}}\big((N, \sigma), (X, \tau)\big) \longleftrightarrow X\,, \qquad \mathbf{x} \longmapsto x_0\,. \tag{42}$$

The reverse correspondence assigns to an element $x \in X$ *the unique homomorphism* (40).

Corollary 2.16 *There exists a canonical bijective correspondence*

$$\mathrm{End}_{\mathbf{Set}^{\langle 1\rangle}}(N, \sigma) \longleftrightarrow N\,, \qquad \sigma^m \longleftrightarrow \sigma^m(0) = m\,. \tag{43}$$

Proof. Consider the set

$$E = \{m \in N \mid \sigma^m(0) = m\}\,.$$

Since $\sigma^0 = \mathrm{id}_N$, one has $0 \in E$. If $m \in N$, then

$$\sigma^{\sigma m}(0) = \sigma\,(\sigma^m(0)) = \sigma m\,,$$

i.e., E is closed under 0 and σ. By Corollary 2.2, E equals N.

By combining this with Lemma 2.15, we deduce that powers of σ are the only unary operations on N that commute with σ,

$$\sigma^m = \sigma^n \qquad \text{if and only if} \qquad m = n \qquad (m, n \in N)\,. \tag{44}$$

and

$$\mathrm{End}_{\mathbf{Set}^{\langle 1\rangle}}(N, \sigma) \;=\; \bigcup_{m \in N} \mathrm{Hom}_{\mathbf{Set}^{\langle 1\rangle}}\,((N, 0, \sigma), (N, m, \sigma)) \;=\; \bigcup_{m \in N} \{\sigma^m\}\,. \tag{45}$$

□

2.7.3 The canonical commutative monoid structure on N

Since composition of endomorphisms makes $\mathrm{End}_{\mathbf{Set}^{\langle 1\rangle}}(N, \sigma)$ a monoid, canonical bijection (43) equips N with a canonical monoid structure:

$$\mathrm{id}_N = \sigma^0 \longleftrightarrow 0 \qquad \text{and} \qquad \sigma^m \circ \sigma^n \longleftrightarrow m + n \qquad (m, n \in N)\,. \tag{46}$$

Exercise 15 *Prove that*

$$\sigma n = 1 + n\,. \tag{47}$$

Solution. Under Correspondence (46), one has

$$\sigma^{\sigma n} \longleftrightarrow \sigma n \qquad \text{and} \qquad \sigma^1 \circ \sigma^n \longleftrightarrow 1 + n \qquad (n \in N)\,.$$

By the definition of the power sequence (σ^n), one has

$$\sigma^{\sigma n} = \sigma \circ \sigma^n = \sigma^1 \circ \sigma^n \qquad (n \in N)$$

in view of $\sigma^1 = \sigma$, cf. (23). Since $\sigma^{\sigma n} = \sigma^1 \circ \sigma^n$, one has $\sigma n = 1 + n$. □

2.7.4

Since powers σ^n are the only endomorphisms of (N, σ), all elements of $\mathrm{End}_{\mathbf{Set}^{\langle 1 \rangle}}(N, \sigma)$ commute with each other, cf. Lemma 2.10. In particular, $(N, 0, +)$ is a commutative monoid.

2.7.5 Additive notation for commutative semigroups and monoids

The binary operation in a commutative semigroup is frequently referred to as *addition* and $+$ is used as the generic symbol for additiion. The identity element of addition is frequently referred to as the *zero* element and is denoted 0.

Lemma 2.17 *Addition in* $(N, 0, +)$ *has the property*

$$\textit{if} \quad l + m = l + n\,, \quad \textit{then} \quad m = n \qquad (l, m, n \in N)\,. \tag{48}$$

The above lemma says that $(N, 0, +)$ is a *cancellative* monoid.

2.7.6 Cancellative binary structures

A binary algebraic structure $(B, \cdot)$ is said to be *left-cancellative* if it has the following property:

$$\text{if} \quad ab = ac, \quad \text{then} \quad b = c \qquad (a, b, c \in B)\,, \tag{49}$$

and it is said to be *right-cancellative* if it has the following property:

$$\text{if} \quad ac = bc, \quad \text{then} \quad a = b \qquad (a, b, c \in B)\,. \tag{50}$$

We refer to (49) and (50) as the *Left-Cancellation Property* and, respectively, the *Right-Cancellation Property*. When the binary operation is commutative, the two cancellation properties coincide.

Proof of Lemma 2.17. One has

$$l + m = \sigma^{l+m}(0) = (\sigma^l \circ \sigma^m)(0) = \sigma^l(m)$$

and, similarly,

$$l + n = \sigma^{l+n}(0) = (\sigma^l \circ \sigma^n)(0) = \sigma^l(n)\,.$$

Thus, equality $l + m = l + n$ is equivalent to the equality

$$\sigma^l(m) = \sigma^l(n)\,.$$

According to Theorem 2.8, successor operation σ is injective. It follows that σ^l is injective, cf. Exercise 11, hence $m = n$. □

2.8 The canonical well-ordering of N

2.8.1 The canonical order relation $\leq$ on N

Consider the binary relation on N,

$$\leq : m, n \longmapsto \text{“ } \exists_{l \in N}\ l + m = n \text{ ”} . \tag{51}$$

Since addition in $(N, 0, +)$ is cancellative, cf. Lemma (2.17), an element $l \in N$ such that $l+m = n$ is unique when it exists.

Exercise 16 *Show that relation $\leq$ is reflexive.*

Exercise 17 *Show that relation $\leq$ is transitive.*

Exercise 18 *Show that, for any $l, m \in N$,*

$$\textit{if} \quad l + m = 0 \,, \quad \textit{then} \quad l = m = 0 \,. \tag{52}$$

Exercise 19 *Show that relation $\leq$ is weakly antisymmetric.*

2.8.2 *Remarks concerning valid solutions of the above exercises*

Use exclusively the facts established in these notes, and only those facts that were established prior to the statement of the above exercises. Your proofs should provide explicit, clear references to the facts you are relying upon at various places of your proofs. References must be correct and they must be mentioned where they are relevant.

2.8.3 The associated sharp order relation $<$ on N

We shall use symbol $<$ to denote the relation

$$< : m, n \longmapsto \text{“ } m{\leq}n \wedge m \neq n \text{ ”} . \tag{53}$$

Since $l \neq 0$ implies that $l = \sigma k$, for some $k \in N$, cf. Corollary 2.3, relation (53) is equipotent with the relation

$$m, n \longmapsto \text{“ } \exists_{k \in N}\ \sigma k + m = n \text{ ”} \tag{54}$$

which, in turn, is equipotent with the relation

$$m, n \longmapsto \text{“ } \sigma m \leq n \text{ ”} \tag{55}$$

in view of the identity

$$\sigma k + m = (1 + k) + m = (k + 1) + m = k + (1 + m) = k + \sigma m \,.$$

Exercise 20 *Show that $m \leq n$ if and only if $m < \sigma n$.*

Exercise 21 *Show that*

$$\textit{if} \quad m < n \,, \quad \textit{then} \quad k + m < k + n \,. \tag{56}$$

2.8.4 Ordered semigroups

. Commutative semigroups equipped with an order relation that satisfy Property (56) are called *ordered semigroups.*

Proposition 2.18 $(N, \leq)$ *is a well-ordered set.*

Proof. Consider the subset

$$E = \{n \in N \mid \forall_{m \in N}\, m \leq n \vee n \leq m\}\,.$$

Since $n + 0 = n$, element 0 is the smallest element of $(N, \leq)$ and $0 \in E$.

If $m \nleq \sigma n$, then $m \nleq n$, in view of the inequality $n < \sigma n$. If, additionally, $n \in E$, then $n < m$ or, equivalently, cf. Section 2.8.3,

$$\sigma n \leq m\,,$$

i.e., $\sigma n \in E$. Invocation of Corollary 2.2 proves that $E = N$. That means that $\leq$ is a *linear order* relation.

Consider the subset

$$F = \left\{n \in N \mid \forall_{A \subseteq N}\, (\exists_{k \in A}\, k \leq n) \Rightarrow (\exists_{m \in A}\, m = \min A)\right\}\,.$$

Since 0 is the smallest element of $(N, \leq)$, it is the smallest element of any subset $A \ni 0$. In particular, $0 \in F$.

The condition

$$\exists_{k \in A}\, k \leq \sigma n$$

is equivalent to the alternative

$$\left(\exists_{k \in A}\, k \leq n\right) \vee \left(\sigma n \in A \wedge \forall_{k \leq n}\, k \notin A\right) \tag{57}$$

If $n \in F$ and the first part of alternative statemnt (57) holds, then A has the smallest element.

If the second part of alternative (57) holds, then the already proven linear-ordering of $(N, \leq)$ implies that

$$\forall_{m \in A}\, n < m$$

and, accordingly, σn is the smallest element of A. This demonstartes that $\sigma n \in F$. Yet another invocation of Corollary 2.2 proves that $F = N$. □

2.9 Homomorphisms $(N, 0, +) \longrightarrow (B, e, \cdot)$

2.9.1

Homomorphisms

$$(N, 0, +) \longrightarrow (B, e, \cdot) \tag{58}$$

are precisely the sequences $\mathbf{x} : N \longrightarrow B$ such that

$$x_0 = e \qquad \text{and} \qquad x_{m+n} = x_m x_n \qquad (m, n \in N)\,. \tag{59}$$

Lemma 2.19 *For any $b \in B$, the sequence of powers (b^n) is a homomorphism of monoids* (58).

Proof. Let $b \in B$. Consider the set

$$E = \left\{m \in N \mid \forall_{n \in N}\, b^{m+n} = b^m b^n\right\}$$

In view of equalities

$$0 + n = n \qquad \text{and} \qquad b^0 = e$$

one has

$$b^{0+n} = b^n = eb^n = b^0 b^n ,$$

i.e, $0 \in E$. If $m \in E$, then

$$b^{\sigma m+n} = b^{(1+m)+n} = b^{1+(m+n)} = b^{\sigma(m+n)} = bb^{m+n} = bb^m b^n = b^{\sigma m} b^n , \tag{60}$$

i.e., E is closed under σ. Hence, by Corollary 2.2, $E = N$.

Note that calculation (60) used associativity of addition in N, Identity (47), and equality $\sigma^1 = \sigma$.

□

2.9.2

Consider the *evaluation-at-1* function,

$$\mathrm{ev}_1 : \mathrm{Hom}_{\mathrm{Mon}}\big((N, 0, +), (B, e, \cdot)\big) \longrightarrow B , \qquad \mathbf{x} \longmapsto x_1 . \tag{61}$$

Lemma 2.20 *Canonical correspondence* (61) *is bijective and the reverse correspondence assigns to an element $b \in B$ the sequence of powers (b^n).*

Proof. It suffices to prove injectivity of the evaluation-at-1 function. Let $\mathbf{x}$ and $\mathbf{x}'$ be two homomorphisms (58) such that $x_1 = x'_1$. Consider the set

$$E = \{n \in N \mid x_n = x'_n\} .$$

Since $x_0 = 0$, for any homomorphism (58), one has $0 \in E$. If $n \in E$, then

$$x_{\sigma n} = x_{1+n} = x_1 x_n = x'_1 x'_n = x'_{1+n} = x'_{\sigma n} ,$$

i.e., E is closed under σ. Hence, by Corollary 2.2, $E = N$. □

2.9.3 $(N, 0, 1, +)$ is an initial object in the category of monoids with a distinguished element

Note that Lemmata 2.19–2.20 imply that, for any element b in any monoid $(B, e, \cdot)$, there exists a unique homomorphism

$$(N, 0, 1, +) \longrightarrow (B, e, b, \cdot) , \tag{62}$$

i.e., $(N, 0, 1, +)$ is an initial object in the category of monoids with a distinguished element.

2.9.4

Homomorphisms (58) are sequences of elements of B. Seqeuences can be multiplied using multiplication in B,

$$(x_n)\cdot(y_n) := (x_n y_n)\,. \tag{63}$$

The set of homomorphisms is closed under multiplication when multiplication is commutative.

2.9.5

Let X be a set and $(B,\cdot)$ be a semigroup. The set of B-valued functions

$$\mathrm{Funct}(X,B)$$

is equipped with the induced binary operation

$$(f\cdot g)(x) := f(x)\cdot g(x)\,. \tag{64}$$

Exercise 22 *Let $(X,\cdot)$ be a binary structure and $(B,\cdot)$ be a semigroup. Show that if f and g are homomorphisms*

$$(X,\cdot)\longrightarrow(B,\cdot) \tag{65}$$

such that,

$$f(x)\cdot g(y) = g(y)\cdot f(x) \qquad (x,y\in X)\,, \tag{66}$$

then $f\cdot g$ is a homomomorphism (65).

Lemma 2.21 *If elements a and b of a monoid $(B,e,\cdot)$ commute with each other, then*

$$a^n b^n = (ab)^n \qquad (n\in N)\,. \tag{67}$$

Proof. If a and b commute, then, a^m and b^n commute for all $m,n\in N$, cf. Part (b) of Corollary 2.11. Therefore, the product sequence

$$(a^n b^n)$$

is, by Exercise 22, a homomorphism (58). Its value at $n=1$ equals

$$a^1 b^1 = ab\,.$$

Since there is only one homomorphism (58) that takes this value, namely the sequence of powers

$$(ab)^n\,,$$

Identity (67) folows. □

2.9.6

Note how brilliant is this purely algebraic proof of a nontrivial identity.

Lemma 2.22 *For any element $b \in B$ of a monoid, one has the following identity*

$$(b^m)^n = (b^m)^n \qquad (m, n \in N)\,. \tag{68}$$

Proof. Consider the set

$$E = \{n \in N \mid \forall_{m \in N}\, (b^m)^n = (b^m)^n\}\,.$$

One has

$$(b^m)^0 = e = e^m = (b^0)^m \qquad (m \in N)\,,$$

hence $0 \in E$. If $n \in N$, then

$$(b^m)^{\sigma n} = (b^m)^{1+n} = b^m (b^m)^n = (b^1)^m (b^n)^m\,.$$

Since b^1 commutes with b^n, we have, in view of Lemma 2.21,

$$(b^1)^m (b^n)^m = (b^{1+n})^m = (b^{\sigma n})^m\,,$$

i.e., $\sigma n \in E$. Corollary 2.2 implies that $E = N$. □

2.9.7 $\mathrm{Hom}_{\mathrm{Mon}}((N, 0, +), (A, 0, +))$

When the target is a commutative monoid and we use additive notation, the n-th power of an element $a \in A$ is then denoted na and referred to as *n times a*. In additive notation and terminology, Lemma 2.20 reads as follows.

Lemma 2.23 *For a commutative monoid $(A, 0, +)$, the reverse correspondence to* (61) *assigns to an element $a \in A$ the sequence of n*-tuples (na).

□

2.10 Semirings: terminology

2.10.1 Semirings

An algebraic structure $(S, +, \cdot)$ is said to be an (associative) *semiring* if it satisfies the following three conditions:

(a) $(S, +)$ is a commutative semigroup;

(b) $(S, \cdot)$ is a semigroup;

(c) operation $\cdot$, referred to as *multiplication*, right- and left-distibutes over operation $+$, referred to as *addition*.

2.10.2 Unital semirings

An algebraic structure $(S, 1, +, \cdot)$ is said to be a *unital semiring* if it satisfies the following two conditions:

(a_1) $(S, +, \cdot)$ is a semiring;

(b_1) $(S, 1, \cdot)$ is a monoid.

2.10.3 Semirings-with-zero

An algebraic structure $(S, 0, +, \cdot)$ is said to be a *semiring-with-zero* if it satisfies the following two conditions:

(a_0) $(S, +, \cdot)$ is a semiring;

(b_0) $(S, 0, +)$ is a monoid.

Usually, one also adds the requirement that

(c_0) $(S, 0, \cdot)$ is a semigroup with *sink*, i.e.,

$$0 \cdot s = 0 = s \cdot 0 \qquad (s \in S)\,. \tag{69}$$

2.10.4 Unital semirings-with-zero

An algebraic structure $(S, 0, 1, +, \cdot)$ is said to be a *unital semiring-with-zero* if it satisfies the following three conditions:

(a_{01}) $(S, +, \cdot)$ is a semiring;

(b_{01}) $(S, 0, +)$ is a monoid;

(c_{01}) $(S, 1, \cdot)$ is a monoid.

2.11 The unital semiring of endomorphisms of a commutative semigroup $(A, +)$

2.11.1 Commutative semigroup $(\mathrm{Funct}(X, A), +)$

Let $(A, +)$ be a commutative semigroup. The set

$$\mathrm{Funct}(X, A)$$

of A-valued functions on a set X, equipped with the induced binary operation,

$$(f + g)(x) := f(x) + g(x) \qquad (f, g \in \mathrm{Funct}(X, A)\,; x \in X)\,, \tag{70}$$

becomes a commutative semigroup.

2.11.2 $(\mathrm{Op}_1 A, \mathrm{id}_A, +, \circ)$

Consider a special case $X = A$. In this case $\mathrm{Funct}(X, A)$ is the set of unary operations on A, equipped with the canonical monoid structure $(\mathrm{Op}_1 A, \mathrm{id}_A, \circ)$. The subset of $\mathrm{Op}_1 A$ consisting of endomorphisms of semigroup $(A, +)$ contains the identity operation id_A and is closed under composition, i.e., is a *submonoid* of $(\mathrm{Op}_1 A, \mathrm{id}_A, \circ)$.

2.11.3 Right-distributivity of $\circ$ over $+$

Addition of unary operations on A equips $\mathrm{Op}_1 A$ with another binary operation that is both associative and commutative. Composition is *right-distributive* with respect to addition.

Exercise 23 *Show that, for any $f, g, h \in \mathrm{Op}_1 A$, one has*

$$(f+g)\circ h = f\circ h + g\circ h\,. \tag{71}$$

2.11.4 Limited left-distributivity of $\circ$ over $+$

Composition, in general, is *left-distributive* with respect to addition only when the left factor h is an endomorphism of semigroup $(A, +)$.

Exercise 24 *Show that, for any $f, g \in \mathrm{Op}_1 A$ and $h \in \mathrm{End}_{\mathrm{Sgr}}(A, +)$, one has*

$$h\circ(f+g) = h\circ f + h\circ g\,. \tag{72}$$

2.11.5 The unital semiring $\left(\mathrm{End}_{\mathrm{Sgr}}(A, +), \mathrm{id}_A, +, \circ\right)$

The subset consisting of endomorphisms $(A, +)$ is closed under addition.

Exercise 25 *Show that, if f and g are endomorphisms of $(A, +)$, then $f + g$ is an endomorphism.*

By combining previous three exercises, we deduce that the algebraic structure $\left(\mathrm{End}_{\mathrm{Sgr}}(A, +), \mathrm{id}_A, +, \circ\right)$ is a *unital semiring.*

2.11.6 The unital semiring-with-zero $(\mathrm{End}_{\mathrm{Mon}}(A, 0, +), \mathbf{0}, \mathrm{id}_A, +, \circ)$

If $(A, 0, +)$ is a commutative monoid, then the subset in $\mathrm{Op}_1 A$ consisting of endomorphisms of $(A, 0, +)$ is unital semiring with the the constant zero function

$$\mathbf{0} : A \longrightarrow A\,, \qquad x \longmapsto 0\,, \tag{73}$$

being its zero element.

Exercise 26 *Show that, for any operation $f \in \mathrm{Op}_1 A$, one has*

$$\mathbf{0}\circ f = \mathbf{0}\,,$$

and, for any endomorphism of nullary structures $g : (A, 0) \to (A, 0)$, one has also

$$g\circ\mathbf{0} = \mathbf{0}\,.$$

It follows that the constant zero function $\mathbf{0}$ is a sink for the operation of composition of endomorphisms of a commutative monoid $(A, 0, +)$.

2.11.7 The canonical commutative unital semiring-with-zero structure on N

Since $\mathrm{End}_{\mathrm{Mon}}(N, 0, +)$ is naturally equipped with a structure of a unital semiring-with-zero, canonical bijection (61) equips N with a canonical structure of a commutative unital semiring-with-zero.

By recalling that the monoid stucture $(N, 0, +)$ is a translation, via bijective correspondence (43), of the monoid structure on $\mathrm{End}_{\mathbf{Set}^{\langle 01\rangle}}(N, \sigma)$, we shall now describe the operations of $(N, 0, 1, +, \cdot)$ in terms the corresponding operations on the set of endomorphisms of

$$\mathrm{End}_{\mathbf{Set}^{\langle 01\rangle}}(N, \sigma) = \{\sigma^n \mid n \in N\}\,.$$

Addition in $(N, 0, 1, +, \cdot)$ corresponds to the composition operation

$$m + n \longleftrightarrow \sigma^m \circ \sigma^n \tag{74}$$

and multiplication in $(N, 0, 1, +, \cdot)$ corresponds to the exponentiation operation

$$mn \longleftrightarrow \sigma^m * \sigma^n := (\sigma^m)^n\,. \tag{75}$$

Commutativity of multiplication in $(N, 0, 1, +, \cdot)$ is an immediate corollary of Lemma 2.22

Corollary 2.24 *Multiplication in $(N, 0, 1, +, \cdot)$ is commutative.*

□

2.11.8

The canonical semiring structure on the underlying set of an initial object $(N, 0, \sigma)$ of the category of nullary-unary structures is what we know, on informal level, as "Arithmetic of Natural Numbers."

Lemma 2.25 *Semiring $(N, 0, 1, +, \cdot)$ has the following property*

$$\textit{if} \quad 0 < m, n\,, \quad \textit{then} \quad 0 < mn\,. \tag{76}$$

Proof. If $0 < m, n$, then $m = \sigma k = 1 + k$ and $n = \sigma l = 1 + l$, cf.Corollary 2.3 and Exercise 15. Distributivity of multiplication over addition yields

$$0 < 1 \leq 1 + kl + km = (1 + k)(1 + l) = mn\,.$$

□

2.11.9 Ordered semirings

Semirings equipped with an order relation such that the additive semigroup is an ordered semigroup, i.e., it satisfies Property (56), and the multiplicative semigroup satisfies Property (76), are called *ordered semirings*.

3 Peano's axiomatic theory of Natural Numbers

3.1 Peano structures

3.1.1 The definition

We shall say that a minimal nullary-unary structure $(P, 0, \sigma)$ is a *Peano* structure if σ is left-invertible and $0 \notin P$.

3.1.2 Existence and constructions

Let (X, τ) be a unary structure with τ left-invertible but not right-invertible. By definition, *every* infinite set admits such an operation. Let 0 be *any* element of the subset

$$X \setminus \tau_* X\,.$$

The intersection

$$P := \bigcap \{E \subseteq X \mid 0 \in E \text{ and } E \text{ is invariant}\} \tag{77}$$

of the family of invariant subsets of X that contain 0 is the smallest invariant subset such that $0 \in P$. Let us denote by σ the operation on P induced by τ. By construction, $(P, 0, \sigma)$ is a Peano structure.

3.1.3 Characterization of initial objects in the category of nullary-unary structures

The main objective of the present chapter is a proof of the following theorem.

Theorem 3.1 *A structure (X, a, τ) is an initial object in the category of nullary-unary structures if and only if it is a Peano structure.*

Necessity was proved before, cf. Theorem 2.8. The rest of this chapter will be devoted to the proof of sufficienncy.