Proof If this were definable, we could take $A = \operatorname{Th} \mathfrak{N}$ in the preceding theorem to obtain a contradiction. ■

§ 3.1 NATURAL NUMBERS WITH SUCCESSOR

We begin with a situation which is simple enough to let us give reasonably complete answers to our questions. We reduce the set of parameters to just $\forall$, $\mathbf{0}$, and $\mathbf{S}$, eliminating $<$, $+$, $\cdot$, and $\mathbf{E}$. The corresponding reduct of $\mathfrak{N}$ is

$$\mathfrak{N}_S = (N, 0, S).$$

In this restricted language we still have the numerals, naming each point in N. But the sentences we can express in the language are, from the viewpoint of arithmetic, uninteresting.

We want to ask about $\mathfrak{N}_S$ the same questions that interest us in the case of $\mathfrak{N}$. We want to know about the complexity of the set $\operatorname{Th} \mathfrak{N}_S$; we want to study definability in $\mathfrak{N}_S$; and we want to survey the nonstandard models of $\mathfrak{N}_S$.

To study the theory of the natural numbers with successor ($\operatorname{Th} \mathfrak{N}_S$), we begin by listing a few of its members, i.e., sentences true in $\mathfrak{N}_S$. (These sentences will ultimately provide an axiomatization for the theory.)

S1. $\forall x\, \mathbf{S}x \not\approx \mathbf{0}$, a sentence asserting that zero has no predecessor.

S2. $\forall x\, \forall y(\mathbf{S}x \approx \mathbf{S}y \to x \approx y)$. This asserts that the successor function is one-to-one.

S3. $\forall y(y \not\approx \mathbf{0} \to \exists x\, y \approx \mathbf{S}x)$. This asserts that any nonzero number is the successor of something.

S4.1 $\forall x\, \mathbf{S}x \not\approx x$.

S4.2 $\forall x\, \mathbf{SS}x \not\approx x$.

...

S4.n $\forall x\, \mathbf{S}^n x \not\approx x$, where the superscript n indicates that the symbol $\mathbf{S}$ occurs at n consecutive places.

Let A_S be the set consisting of the above sentences S1, S2, S3, S4.n ($n = 1, 2, \ldots$). Clearly these sentences are true in $\mathfrak{N}_S$; i.e., $\mathfrak{N}_S$ is a model of A_S. Hence

$$\operatorname{Cn} A_S \subseteq \operatorname{Th} \mathfrak{N}_S.$$

(Anything true in every model of A_S is true in this model.) What is not so obvious is that equality holds. We will prove this by considering arbitrary models of A_S.

What can be said of an arbitrary model

$$\mathfrak{A} = (|\mathfrak{A}|, 0^{\mathfrak{A}}, \mathbf{S}^{\mathfrak{A}})$$

of the axioms A_S? $\mathbf{S}^{\mathfrak{A}}$ must be a one-to-one map of $|\mathfrak{A}|$ onto $|\mathfrak{A}| - \{0^{\mathfrak{A}}\}$, by S1, S2, and S3. And by S4.n, there can be no loops of size n. Thus $|\mathfrak{A}|$ must contain the "standard" points:

$$0^{\mathfrak{A}} \to \mathbf{S}^{\mathfrak{A}}(0^{\mathfrak{A}}) \to \mathbf{S}^{\mathfrak{A}}(\mathbf{S}^{\mathfrak{A}}(0^{\mathfrak{A}})) \to \cdots,$$

which are all distinct. The arrow here indicates the action of $\mathbf{S}^{\mathfrak{A}}$. There may or may not be other points. If there is another point a in $|\mathfrak{A}|$, then there will be the successor of a, its successor, etc. Not only that, but since (by S3) each nonzero element has a predecessor (something of which it is the successor) which is (by S2) unique, $|\mathfrak{A}|$ must contain the predecessor of a, its predecessor, etc. These must all be distinct lest there be a finite loop. Thus a belongs to a "Z-chain":

$$\cdots * \to * \to a \to \mathbf{S}^{\mathfrak{A}}(a) \to \mathbf{S}^{\mathfrak{A}}(\mathbf{S}^{\mathfrak{A}}(a)) \to \cdots.$$

(We refer to these as Z-chains because they are arranged like the set Z of all integers $\{\ldots, -1, 0, 1, 2, \ldots\}$.) There can be any number of Z-chains. But any two Z-chains must be disjoint, as S2 prohibits merging. Similarly, any Z-chain must be disjoint from the standard part.

This can be restated in another way. Say that two points a and b in $|\mathfrak{A}|$ are *equivalent* if the function $\mathbf{S}^{\mathfrak{A}}$ can be applied a finite number of times to one point to yield the other point. This *is* an equivalence relation. (It is clearly reflexive and symmetric; the transitivity follows from the fact that $\mathbf{S}^{\mathfrak{A}}$ is one-to-one.) The standard part of $|\mathfrak{A}|$ is the equivalence class containing $0^{\mathfrak{A}}$. For any other point (if any) a in $|\mathfrak{A}|$, the equivalence class of a is the set generated from $\{a\}$ by $\mathbf{S}^{\mathfrak{A}}$ and its inverse. This equivalence class is the Z-chain described above.

Conversely, any structure $\mathfrak{B}$ (for this language) which has a standard part

$$0^{\mathfrak{B}} \to \mathbf{S}^{\mathfrak{B}}(0^{\mathfrak{B}}) \to \mathbf{S}^{\mathfrak{B}}(\mathbf{S}^{\mathfrak{B}}(0^{\mathfrak{B}})) \to \cdots$$

and a nonstandard part consisting of any number of separate Z-chains, is a model of A_S. (Check through the list of axioms in A_S, and note that each is true in $\mathfrak{B}$.) We thus have a complete characterization of what the models of A_S must look like.

If a model $\mathfrak{A}$ of A_S has only countably many Z-chains, then $|\mathfrak{A}|$ is countable. In general, if the set of Z-chains has cardinality λ, then altogether

the number of points in $|\mathfrak{A}|$ is $\aleph_0 + \aleph_0 \cdot \lambda$. By facts of cardinal arithmetic (cf. Chapter 0) this number is the larger of $\aleph_0$ and λ. Hence

$$\operatorname{card}|\mathfrak{A}| = \begin{cases} \aleph_0 & \text{if } \mathfrak{A} \text{ has countably many } Z\text{-chains,} \\ \lambda & \text{if } \mathfrak{A} \text{ has an uncountable number } \lambda \text{ of } Z\text{-chains.} \end{cases}$$

Lemma 31A If $\mathfrak{A}$ and $\mathfrak{A}'$ are models of A_S having the same number of Z-chains, then they are isomorphic.

Proof There is a unique isomorphism between the standard part of $\mathfrak{A}$ and the standard part of $\mathfrak{A}'$. By hypothesis we are given a one-to-one correspondence between the set of Z-chains of $\mathfrak{A}$ and the set of Z-chains of $\mathfrak{A}'$; thus each chain of $\mathfrak{A}$ is paired with a chain of $\mathfrak{A}'$. Clearly any two Z-chains are isomorphic. By combining all the pieces (which uses the axiom of choice) we have an isomorphism of $\mathfrak{A}$ onto $\mathfrak{A}'$. ■

Thus a model of $\mathfrak{N}_S$ is determined to within isomorphism by its number of Z-chains. For $\mathfrak{N}_S$ this number is zero, but any number is possible.

The reader should note that there is no sentence of the language which says, "There are no Z-chains." In fact, there is no set Σ of sentences such that a model $\mathfrak{A}$ of A_S satisfies Σ iff $\mathfrak{A}$ has no Z-chains. For by the LST theorem there is an uncountable structure $\mathfrak{A}$ with $\mathfrak{A} \equiv \mathfrak{N}_S$. But $\mathfrak{A}$ has uncountably many Z-chains and $\mathfrak{N}_S$ has none.

Theorem 31B Let $\mathfrak{A}$ and $\mathfrak{B}$ be uncountable models of A_S of the same cardinality. Then $\mathfrak{A}$ is isomorphic to $\mathfrak{B}$.

Proof By the above discussion, $\mathfrak{A}$ has card $\mathfrak{A}$ Z-chains, and $\mathfrak{B}$ has card $\mathfrak{B}$ Z-chains. Since card $\mathfrak{A}$ = card $\mathfrak{B}$, they have the same number of Z-chains and hence are isomorphic. ■

Theorem 31C Cn A_S is a complete theory.

Proof Apply the Łoś–Vaught theorem of Section 2.6. The preceding theorem asserts that the theory Cn A_S is categorical in any uncountable power. Furthermore, A_S has no finite models. Hence the Łoś–Vaught theorem applies. ■

Corollary 31D Cn A_S = Th $\mathfrak{N}_S$.

Proof We have Cn $A_S \subseteq$ Th $\mathfrak{N}_S$; the first theory is complete and the second is satisfiable. ■

***Corollary 31E** Th $\mathfrak{N}_S$ is decidable.

Proof Any complete and axiomatizable theory is decidable (by Corollary 25G). A_S is a decidable set of axioms for this theory. ■

Elimination of quantifiers

Once one knows a theory to be decidable, it is tempting to try to find a realistically practical decision procedure. We will give such a procedure for Th $\mathfrak{N}_S$, based on "elimination of quantifiers."

Definition A theory T admits elimination of quantifiers iff for every formula φ there is a quantifier-free formula ψ such that

$$T \models (\varphi \leftrightarrow \psi).$$

Actually it is enough to consider only formulas φ of a rather special form:

Theorem 31F Assume that for every formula φ of the form

$$\exists x(\alpha_0 \wedge \cdots \wedge \alpha_n),$$

where each α_i is an atomic formula or the negation of an atomic formula, there is a quantifier-free formula ψ such that $T \models (\varphi \leftrightarrow \psi)$. Then T admits elimination of quantifiers.

Proof First we claim that we can find a quantifier-free equivalent for any formula of the form $\exists x\, \theta$ for quantifier-free θ. We begin by putting θ into disjunctive normal form (Corollary 15C). The resulting formula,

$$\exists x[(\alpha_0 \wedge \cdots \wedge \alpha_m) \vee (\beta_0 \wedge \cdots \wedge \beta_n) \vee \cdots \vee (\xi_0 \wedge \cdots \wedge \xi_t)],$$

is logically equivalent to

$$\exists x(\alpha_0 \wedge \cdots \wedge \alpha_m) \vee \exists x(\beta_0 \wedge \cdots \wedge \beta_n) \vee \cdots \vee \exists x(\xi_0 \wedge \cdots \wedge \xi_t).$$

By assumption, each disjunct of this formula can be replaced by a quantifier-free formula.

We leave it to the reader to show (in Exercise 2) that by using the above paragraph one can obtain a quantifier-free equivalent for an arbitrary formula. ■

In the special case where the theory in question is the theory Th $\mathfrak{A}$ of a structure $\mathfrak{A}$, the definition can be restated: Th $\mathfrak{A}$ admits elimination of

quantifiers iff for every formula φ there is a quantifier-free formula ψ such that φ and ψ are "equivalent in $\mathfrak{A}$"; i.e.,

$$\models_{\mathfrak{A}} (\varphi \leftrightarrow \psi)\,[s]$$

for any map s of the variables into $|\mathfrak{A}|$.

Theorem 31G Th $\mathfrak{N}_S$ admits elimination of quantifiers.

Proof By the preceding theorem, it suffices to consider a formula

$$\exists x(\alpha_0 \wedge \cdots \wedge \alpha_q),$$

where each α_i is atomic or is the negation of an atomic formula. We will describe how to replace this formula by another which is quantifier-free. The equivalence of the new formula to the given one will, in fact, be a consequence of A_S; see Exercise 3.

In the language of $\mathfrak{N}_S$ the only terms are of the form $\mathbf{S}^k u$, where u is $\mathbf{0}$ or a variable. The only atomic formulas are equations. We may suppose that the variable x occurs in each α_i. For if x does not occur in α, then

$$\exists x(\alpha \wedge \beta) \models \dashv \alpha \wedge \exists x\, \beta.$$

Thus each α_i has the form

$$\mathbf{S}^m x \approx \mathbf{S}^n u$$

or the negation of this equation, where u is $\mathbf{0}$ or a variable. We may further suppose u is different from x, since $\mathbf{S}^m x \approx \mathbf{S}^n x$ could be replaced by $\mathbf{0} \approx \mathbf{0}$ if $m = n$, and by $\mathbf{0} \not\approx \mathbf{0}$ if $m \neq n$.

Case 1: Each α_i is the negation of an equation. Then the formula may be replaced by $\mathbf{0} \approx \mathbf{0}$.

Case 2: There is at least one α_i not negated; say α_0 is

$$\mathbf{S}^m x \approx t,$$

where the term t does not contain x. Since the solution for x must be non-negative, we replace α_0 by

$$t \not\approx \mathbf{0} \wedge \cdots \wedge t \not\approx \mathbf{S}^{m-1}\mathbf{0}$$

(or by $\mathbf{0} \approx \mathbf{0}$ if $m = 0$). Then in each other α_j we replace, say,

$$\mathbf{S}^k x \approx u$$

first by

$$\mathbf{S}^{k+m} x \approx \mathbf{S}^m u,$$

which in turn becomes

$$\mathbf{S}^k t \approx \mathbf{S}^m u.$$

We now have a formula in which x no longer occurs, so the quantifier may be omitted. ■

There are several interesting by-products of the quantifier elimination procedure. For one, we get an alternative proof of the completeness of Cn A_S. For suppose we begin with a sentence σ. The quantifier elimination procedure gives a quantifier-free *sentence* τ such that (by Exercise 3) $A_S \models (\sigma \leftrightarrow \tau)$. Now we claim that either $A_S \models \tau$ or $A_S \models \neg\tau$. For τ is built up from atomic sentences by means of $\neg$ and $\rightarrow$. An atomic sentence must be of the form $\mathbf{S}^k\mathbf{0} \approx \mathbf{S}^l\mathbf{0}$ and is deducible from A_S if $k = l$, but is refutable (i.e., its negation is deducible) from A_S if $k \neq l$. (In fact, just {S1, S2} suffices for this.) Since every atomic sentence can be deduced or refuted, so can every quantifier-free sentence. This establishes the claim. And so either $A_S \models \sigma$ or $A_S \models \neg\sigma$.

Another by-product concerns the problem of definability in $\mathfrak{N}_S$; see Exercises 4 and 5. For any formula φ in which just $\mathbf{v}_1$ and $\mathbf{v}_2$ occur free we now can find a quantifier-free ψ (with the same variables free) such that

$$\text{Th } \mathfrak{N}_S \models \forall \mathbf{v}_1 \forall \mathbf{v}_2 (\varphi \leftrightarrow \psi);$$

i.e.,

$$\models_{\mathfrak{N}_S} \forall \mathbf{v}_1 \forall \mathbf{v}_2 (\varphi \leftrightarrow \psi).$$

Thus the relation φ defined is also definable by a quantifier-free formula.

EXERCISES

1. Let A_S^* be the set of sentences consisting of S1, S2, and all sentences of the form

$$\varphi(\mathbf{0}) \rightarrow \forall \mathbf{v}_1(\varphi(\mathbf{v}_1) \rightarrow \varphi(\mathbf{S}\mathbf{v}_1)) \rightarrow \forall \mathbf{v}_1\, \varphi(\mathbf{v}_1),$$

where φ is a wff (in the language of $\mathfrak{N}_S$) in which no variable except $\mathbf{v}_1$ occurs free. Show that $A_S \subseteq \text{Cn } A_S^*$. Conclude that Cn $A_S^* = \text{Th } \mathfrak{N}_S$. (Here $\varphi(t)$ is by definition $\varphi_t^{\mathbf{v}_1}$. The sentence displayed above is called the *induction axiom* for φ.)

2. Complete the proof of Theorem 31F.

3. The proof of quantifier elimination for Th $\mathfrak{N}_S$ showed how, given a formula φ, to find a quantifier-free ψ. Show that

$$A_S \vdash (\varphi \leftrightarrow \psi)$$

without using the completeness of Cn A_S. (This yields an alternative proof of the completeness of Cn A_S, not involving Z-chains or the Łoś-Vaught theorem.)

4. Show that a subset of N is definable in $\mathfrak{N}_S$ iff either it is finite or its complement (in N) is finite.

5. Show that the ordering relation $\{\langle m, n\rangle : m < n \text{ in } N\}$ is not definable in $\mathfrak{N}_S$.

6. Show that Th $\mathfrak{N}_S$ is not finitely axiomatizable. *Suggestion*: Show that no finite subset of A_S suffices, and then apply Section 2.6.

§ 3.2 OTHER REDUCTS OF NUMBER THEORY[1]

First let us add the ordering symbol $<$ to the language. The intended structure is

$$\mathfrak{N}_L = (N, 0, S, <).$$

We want to show that the theory of this structure is (like Th $\mathfrak{N}_S$) decidable and also admits elimination of quantifiers. But unlike Th $\mathfrak{N}_S$, it is finitely axiomatizable and is not categorical in any infinite power.

As axioms of Th $\mathfrak{N}_L$ we will take the finite set A_L consisting of the six sentences listed below. Here $x \leq y$ is, of course, an abbreviation for $(x < y \vee x \approx y)$, and $x \not\leq y$ abbreviates the negation of this formula.

S3.	$\forall y$	$(y \not\approx 0 \rightarrow \exists x\, y \approx Sx)$
L1.	$\forall x\, \forall y$	$(x < Sy \leftrightarrow x \leq y)$
L2.	$\forall x$	$x \not< 0$
L3.	$\forall x\, \forall y$	$(x < y \vee x \approx y \vee y < x)$
L4.	$\forall x\, \forall y$	$(x < y \rightarrow y \not< x)$
L5.	$\forall x\, \forall y\, \forall z$	$(x < y \rightarrow y < z \rightarrow x < z)$

[1] This section may be omitted without disastrous effects.

We begin by listing some consequence of these axioms.

(1) $A_L \vdash \forall x\, x < Sx$.

Proof In L1 take y to be x. ■

(2) $A_L \vdash \forall x\, x \not< x$.

Proof In L4 take y to x. ■

(3) $A_L \vdash \forall x\, \forall y (x \not< y \leftrightarrow y \leq x)$ (trichotomy).

Proof For "$\rightarrow$" use L3. For "$\leftarrow$" use L4 and (2). ■

(4) $A_L \vdash \forall x\, \forall y (x < y \leftrightarrow Sx < Sy)$.

Proof From A_L we can deduce the biconditionals:

$$\begin{aligned} x < y &\leftrightarrow y \not\leq x && \text{by (3);} \\ &\leftrightarrow y \not< Sx && \text{by L1;} \\ &\leftrightarrow Sx \leq y && \text{by (3);} \\ &\leftrightarrow Sx < Sy && \text{by L1.} \end{aligned}$$ ■

(5) $A_L \vdash$ S1 and $A_L \vdash$ S2.

Proof S1 follows from L2 and (1). S2 comes from (4) by use of L3 and (2). ■

(6) $A_L \vdash$ S4.n for $n = 1, 2, \ldots$.

Proof This follows from (1) and (2), using L5. ■

Thus any model $\mathfrak{A}$ of A_L is (when we ignore $<^{\mathfrak{A}}$) also a model of A_S. So it must consist of a standard part plus zero or more Z-chains. In addition, it is ordered by $<^{\mathfrak{A}}$.

Theorem 32A The theory Cn A_L admits elimination of quantifiers.

Proof Again we consider a formula

$$\exists x(\beta_0 \wedge \cdots \wedge \beta_p),$$

where each β_i is atomic or the negation of an atomic formula. The terms are, as in Section 3.1, of the form $S^k u$, where u is 0 or a variable. There are

two possibilities for atomic formulas,

$$S^k u \approx S^l t \quad \text{and} \quad S^k u < S^l t.$$

1. We can eliminate the negation symbol. Replace $t_1 \not< t_2$ by $t_2 < t_1 \vee t_1 \approx t_2$ and replace $t_1 \not\approx t_2$ by $t_1 < t_2 \vee t_2 < t_1$. (This is justified by L3 and L4.) By regrouping the atomic formulas and noting that

$$\exists x(\varphi \vee \psi) \models\dashv \exists x\, \varphi \vee \exists x\, \psi,$$

we may again reach formulas of the form

$$\exists x(\alpha_0 \wedge \cdots \wedge \alpha_q),$$

where now each α_i is atomic.

2. We may suppose that the variable x occurs in each α_i. This is because if x does not occur in α, then

$$\exists x(\alpha \wedge \beta) \models\dashv \alpha \wedge \exists x\, \beta.$$

Furthermore, we may suppose that x occurs on only one side of the equality or inequality α_i. For $S^k x \approx S^l x$ can be dealt with as in Section 3.1. $S^k x < S^l x$ can be replaced by $\mathbf{0} \approx \mathbf{0}$ if $k < l$, and $\mathbf{0} \not\approx \mathbf{0}$ otherwise. (This is justified by L1 and L4.)

Case 1: Suppose that some α_i is an equality. Then we can proceed as in case 2 of the quantifier-elimination proof of Theorem 31G.

Case 2: Otherwise each α_i is an inequality. Then the formula can be rewritten

$$\exists x\left(\bigwedge_i t_i < S^{m_i} x \wedge \bigwedge_j S^{n_j} x < u_j\right).$$

(Here $\bigwedge_i$ indicates the conjunction of formulas indexed by i, so $\gamma_0 \wedge \gamma_1 \wedge \cdots \wedge \gamma_k$ can be abbreviated $\bigwedge_i \gamma_i$.) In the first conjunction, $\bigwedge_i t_i < S^{m_i} x$, we have the lower bounds on x, in the second conjunction, $\bigwedge_j S^{n_j} x < u_j$, we have the upper bounds. If the second conjunction is empty (i.e., if there are no upper bounds on x), then we can replace the formula by $\mathbf{0} \approx \mathbf{0}$. (Why?) If the first conjunction is empty (i.e., if there are no lower bounds on x), then we can replace the formula by

$$\bigwedge_j S^{n_j} \mathbf{0} < u_j,$$

which asserts that zero satisfies the upper bounds. Otherwise, we rewrite

the formula successively as

(1) $$\exists x \bigwedge_{i,j} (t_i < S^{m_i} x \wedge S^{n_j} x < u_j).$$

(2) $$\exists x \bigwedge_{i,j} (S^{n_j} t_i < S^{m_i + n_j} x < S^{m_i} u_j).$$

(3) $$\left(\bigwedge_{i,j} S^{n_j+1} t_i < S^{m_i} u_j\right) \wedge \bigwedge_j S^{n_j} \mathbf{0} < u_j.$$

This last formula says "any lower bound plus one satisfies any upper bound, and furthermore zero satisfies any upper bound." This implies that there is a gap between the greatest lower bound and the least upper bound, whence there is a solution for x. The second part guarantees that the solution for x is not forced to be negative.

In each case, we have arrived at a quantifier-free version of the given formula. ■

Corollary 32B (a) Cn A_L is complete.
(b) Cn A_L = Th $\mathfrak{N}_L$.
*(c) Th $\mathfrak{N}_L$ is decidable.

Proof (a) The argument which followed the proof of Theorem 31G is applicable here also. (b) This follows from (a), since Cn $A_L \subseteq$ Th $\mathfrak{N}_L$ and Th $\mathfrak{N}_L$ is satisfiable. For (c), we can use the fact that any complete axiomatizable theory is decidable. But the quantifier elimination proof yields a more efficient decision procedure. ■

Corollary 32C A subset of N is definable in $\mathfrak{N}_L$ iff it is either finite or has finite complement.

Proof Compare Exercise 4 of the preceding section. ■

On the other hand, $\mathfrak{N}_L$ has more definable binary relations than has $\mathfrak{N}_S$. For the ordering relation $\{\langle m, n\rangle : m < n\}$ is not definable in $\mathfrak{N}_S$, by Exercise 5 of the preceding section.

Corollary 32D The addition relation,

$$\{\langle m, n, p\rangle : m + n = p\},$$

is not definable in $\mathfrak{N}_L$.

Proof If we could define addition, we could then define the set of even natural numbers. But this set is neither finite nor has finite complement. ■

Now suppose we augment the language by the addition symbol $+$. The intended structure is

$$\mathfrak{N}_A = (N, 0, S, <, +).$$

The theory of this structure is also decidable, as we will prove shortly. But to keep matters from getting even more complicated, we will avoid listing any convenient set of axioms for the theory.

The nonstandard models of Th $\mathfrak{N}_A$ must also be models of Th $\mathfrak{N}_L$. So they have a standard part, followed by some Z-chains. But ordering among the Z-chains can no longer be arbitrary. Let $\mathfrak{A}$ be a nonstandard model of Th $\mathfrak{N}_A$. The ordering $<^{\mathfrak{A}}$ induces a well-defined ordering on the set of Z-chains. (See Exercise 3.) We claim that there is no largest Z-chain, there is no smallest Z-chain, and there is between any two Z-chains another one. The reasons, in outline, can be stated simply: If a belongs to some Z-chain (i.e., is an infinite element of $\mathfrak{A}$), then $a +^{\mathfrak{A}} a$ is in a larger Z-chain. There must be some b such that $b +^{\mathfrak{A}} b$ is either a or its successor; b must be in a smaller Z-chain. If a_1 and a_2 belong to different Z-chains, then there must be some b such that $b +^{\mathfrak{A}} b$ is either $a_1 +^{\mathfrak{A}} a_2$ or its successor. And b will lie in a Z-chain between that of a_1 and that of a_2. (These statements should seem quite plausible. The reader who enjoys working with infinite numbers might supply some details.)

***Theorem 32E (Presburger, 1929)** The theory of the structure $\mathfrak{N}_A = (N, 0, S, <, +)$ is decidable.

The proof is again based on a quantifier elimination procedure. The theory of $\mathfrak{N}_A$ itself does *not* admit elimination of quantifiers. For example, the formula defining the set of even numbers

$$\exists y\, v_1 \approx y + y$$

is not equivalent to any quantifier-free formula. We can overcome this by adding a new symbol $\approx_2$ for congruence modulo 2. Similarly, we add symbols $\approx_3, \approx_4, \ldots$. The intended structure for this expanded language is

$$\mathfrak{N}^+ = (N, 0, S, <, +, \equiv_2, \equiv_3, \ldots),$$

where $\equiv_k$ is the binary relation of congruence modulo k. It turns out that the theory of this structure does admit elimination of quantifiers.

This by itself does not imply that the theory of either structure is decidable. After all, we can start with *any* structure, and expand it to a structure having additional relations until a structure is obtained that admits elimination of quantifiers. To obtain decidability, we must show that we can, given a sentence σ, (1) effectively find a quantifier-free equivalent σ', and then (2) effectively decide if σ' is true.

We will now give the quantifier elimination procedure for $\mathfrak{N}^+$. For a term t and a natural number n, let nt be the term $t + t + \cdots + t$, with n summands. $0t$ is $\mathbf{0}$. Then any term can be expanded to one of the form

$$\mathbf{S}^{n_0}\mathbf{0} + n_1x_1 + \cdots + n_kx_k$$

for $k \geq 0$, $n_i \geq 0$. For example,

$$\mathbf{S}(x + \mathbf{S}0)$$

becomes

$$\mathbf{S}^2\mathbf{0} + x.$$

As usual we begin with a formula $\exists y(\beta_1 \wedge \cdots \wedge \beta_n)$, where β_i is an atomic formula or the negation of one.

1. Eliminate negation. Replace $\neg(t_1 \approx t_2)$ by $(t_1 < t_2 \vee t_2 < t_1)$. Replace $\neg(t_1 < t_2)$ by $(t_1 \approx t_2 \vee t_2 < t_1)$. And replace $\neg(t_1 \approx_m t_2)$ by

$$t_1 \approx_m t_2 + \mathbf{S}^1\mathbf{0} \vee \cdots \vee t_1 \approx_m t_2 + \mathbf{S}^{m-1}\mathbf{0}.$$

Then regroup into a disjunction of formulas of the form

$$\exists y(\alpha_1 \wedge \cdots \wedge \alpha_m),$$

where each α_i is atomic. We may further suppose that y occurs in each α_i, and in fact that α_i has one of the four forms

$$\begin{aligned} ny + t &\approx u, \\ ny + t &\approx_m u, \\ ny + t &< u, \\ u &< ny + t, \end{aligned}$$

where u and t are terms not containing y. In what follows we will take the liberty of writing these formulas with a subtraction symbol:

$$\begin{aligned} ny &\approx u - t, \\ ny &\approx_m u - t, \\ ny &< u - t, \\ u - t &< ny. \end{aligned}$$

These are merely abbreviations for the formulas without subtraction obtained by transposing terms.

For example, we might have at this point the formula

$$\exists y(w < 4y \wedge 2y < u \wedge 3y < v \wedge y \approx_3 t),$$

where t, u, v, and w are terms not containing y.

2. Uniformize the coefficients of y. Let p be the least common multiple of the coefficients of y. Each atomic formula can be converted to one in which the coefficient of y is p, by "multiplying through" by the appropriate factor. This is obviously legitimate for equalities and inequalities. In the case of congruences one must remember to raise the modulus also:

$$a \equiv_m b \quad \text{iff } ka \equiv_{km} kb.$$

In the example above p is 12, and we obtain

$$\exists y(3w < 12y \wedge 12y < 6u \wedge 12y < 4v \wedge 12y \approx_{36} 12t).$$

3. Eliminate the coefficient of y. Replace py by x and add the new conjunct $x \approx_p \mathbf{0}$. (In place of $\exists y \cdots 12y \cdots$ we can equally well have, "There exists a multiple x of 12 such that $\ldots x \ldots$.") Our example is now converted to

$$\exists x(3w < x \wedge x < 6u \wedge x < 4v \wedge x \approx_{36} 12t \wedge x \approx_{12} \mathbf{0}).$$

4. Special case. If one of the atomic formulas is an equality, $x + t \approx u$, then we can replace

$$\exists x\, \theta$$

by

$$\theta^x_{u-t} \wedge t \leq u.$$

Here replacement of x by "$u - t$" is the natural thing; we transpose terms to compensate for the absence of subtraction. For example,

$$(x \approx_m v)^x_{u-t} \quad \text{is} \quad u \approx_m v + t.$$

5. We may assume henceforth that $\approx$ does not occur. So we have a formula of the form

$$\begin{aligned}\exists x[&r_0 - s_0 < x \wedge \cdots \wedge r_{l-1} - s_{l-1} < x\\ &\wedge x < t_0 - u_0 \wedge \cdots \wedge x < t_{k-1} - u_{k-1}\\ &\wedge x \approx_{m_0} v_0 - w_0 \wedge \cdots \wedge x \approx_{m_{n-1}} v_{n-1} - w_{n-1}],\end{aligned}$$

where r_i, s_i, t_i, u_i, v_i, and w_i are terms not containing x. This can be abbreviated

$$\exists x\Big[\bigwedge_{j<l} r_j - s_j < x \wedge \bigwedge_{i<k} x < t_i - u_i \wedge \bigwedge_{i<n} x \approx_{m_i} v_i - w_i\Big].$$

If there are no congruences (i.e., $n = 0$), then the formula asserts that there is a nonnegative space between the lower and upper bounds. We can replace the formula by the quantifier-free formula:

$$\bigwedge_{i<k}\bigwedge_{j<l}(r_j - s_j) + \mathbf{S0} < t_i - u_i \wedge \bigwedge_{i<k} \mathbf{0} < t_i - u_i.$$

Let M be the least common multiple of the moduli $m_0, \ldots, m_{n-1}$. Then $a + M \equiv_{m_i} a$. So as a increases, the pattern of residues of a modulo $m_0, \ldots, m_{n-1}$ has period M. Thus, in searching for a solution to the congruences, we need only search M consecutive integers.

We now have a formula which asserts the existence of a natural number which is not less than certain lower bounds $L_1, \ldots, L_l$ and which satisfies certain congruences and certain upper bounds. If there is such a solution, then one of the following is a solution:

$$\begin{aligned}&L_1, L_1 + 1, \ldots, L_1 + M - 1,\\ &L_2, L_2 + 1, \ldots, L_2 + M - 1,\\ &\cdots\\ &L_l, L_l + 1, \ldots, L_l + M - 1,\\ &0, 1, \ldots, M - 1.\end{aligned}$$

(The last line is needed to cover the case in which every L_j is negative. To avoid having to treat this line as special case, we will add a new lower bound of 0. That is, let $r_l = \mathbf{0}$ and $s_l = \mathbf{S0}$ so that

$$r_l - s_l < x$$

is a formula $\mathbf{0} < x + \mathbf{S0}$ asserting that x is nonnegative. We now have $l + 1$ lower bounds.)

Our formula (asserting the existence of a solution for x) can now be replaced by a quantifier-free disjunction which asserts that one of the numbers in the above matrix is a nonnegative solution:

$$\bigvee_{j\leq l}\bigvee_{q\leq M}\Big[\bigwedge_{i\leq l} r_i - s_i < (r_j - s_j) + \mathbf{S}^q\mathbf{0} \wedge \bigwedge_{i<k}(r_j - s_j) + \mathbf{S}^q\mathbf{0} < t_i - u_i \wedge \bigwedge_{i<n}(r_j - s_j) + \mathbf{S}^q\mathbf{0} \approx_{m_i} v_i - w_i\Big].$$

In our continuing example we have, after adding the new lower bound on x,

$$\exists x(3w < x \wedge \mathbf{0} < x + \mathbf{S0} \wedge x < 6u \wedge x < 4v \wedge x \approx_{36} 12t \wedge x \approx_{12} \mathbf{0}).$$

The quantifier-free equivalent is a disjunction of seventy-two conjunctions. Each conjunction has six constituents.

This proves half of the theorem. If we are given a sentence σ, the above procedure tells us how to find effectively a quantifier-free sentence τ (in the language of $\mathfrak{N}^+$) which is true (in the intended structure) iff σ is. Now we must decide if τ is true.

But this is easy. It is enough to look at atomic sentences. Any variable-free term can be put in the form $\mathbf{S}^n\mathbf{0}$. Then, for example,

$$\mathbf{S}^n\mathbf{0} \approx_m \mathbf{S}^p\mathbf{0}$$

is true iff $n \equiv_m p$. ■

A set D of natural numbers is *periodic* if for some positive p, a number n is in D iff $n + p$ is in D. D is *eventually periodic* iff there exist positive numbers M and p such that for all n greater than M, $n \in D$ iff $n + p \in D$.

Theorem 32F A set of natural numbers is definable in $(N, 0, S, <, +)$ iff it is eventually periodic.

Proof Exercise 1 asserts that every eventually periodic set is definable. Conversely, suppose D is definable. Then D is definable in $\mathfrak{N}^+$ by a quantifier-free formula (whose only variable is v_1). Since the class of eventually periodic sets is closed under union, intersection, and complementation, it suffices to show that every atomic formula in the language of $\mathfrak{N}^+$ whose only variable is v_1 defines an eventually periodic set. There are only four possibilities:

$$nv_1 + t \approx u,$$
$$nv_1 + t < u,$$
$$u < nv_1 + t,$$
$$nv_1 + t \approx_m u,$$

where u and t are numerals. The first two formulas define finite sets (which eventually have period 1), the third defines a set with finite complement, and the last formula defines a periodic set with period m. ■

Corollary 32G The multiplication relation

$$\{\langle m, n, p\rangle : p = m \cdot n \text{ in } N\}$$

is not definable in $(N, 0, S, <, +)$.

Proof If we had a definition of multiplication, we could then use that to define the set of squares. But the set of squares is not eventually periodic. ■

EXERCISES

1. Show that any eventually periodic set of natural numbers is definable in the structure $\mathfrak{N}_A$.

2. Show that in the structure $(N, +)$ the following relations are definable:
   (a) Ordering, $\{\langle m, n\rangle : m < n\}$.
   (b) Zero, $\{0\}$.
   (c) Successor, $\{\langle m, n\rangle : n = S(m)\}$.

3. Let $\mathfrak{A}$ be a model of Th $\mathfrak{N}_L$ (or equivalently a model of A_L). For a and b in $|\mathfrak{A}|$ define the equivalence relation:

$a \sim b \Leftrightarrow \mathbf{S}^{\mathfrak{A}}$ can be applied a finite number of times to one of a, b to reach the other.

Let $[a]$ be the equivalence class to which a belongs. Order equivalence classes by

$$[a] < [b] \quad \text{iff } a <^{\mathfrak{A}} b \text{ and } a \not\sim b.$$

Show that this is a well-defined ordering on the set of equivalence classes.

4. Show that the theory of the real numbers with its usual ordering, Th$(R, <)$, admits elimination of quantifiers. (Assume that the language includes equality.)

§ 3.3 A SUBTHEORY OF NUMBER THEORY

We now return to the full language of number theory, as described in Section 3.0. The parameters of the language are $\forall, 0, \mathbf{S}, <, +, \cdot$, and $\mathbf{E}$. The intended structure for this language is

$$\mathfrak{N} = (N, 0, S, <, +, \cdot, E).$$