Preliminaries

In this preliminary section, we first survey some basic facts from logic (and recursion theory) that are assumed to be known to the reader. Furthermore, we shall introduce the language of first order arithmetic and investigate first order definable sets of natural numbers. Finally, we shall present the beginnings of arithmetization of metamathematics by showing (or announcing) that various syntactic and some semantic logical notions can be understood as first order definable sets of natural numbers. To show that metamathematically interesting sets (like the set of all formulas, proofs, etc.) are (or can be understood as) first order definable sets of natural numbers is only the first step; the second step, more important and postponed until Chap. I, consists in investigating which first-order properties of these sets are provable in various systems of first order arithmetic. The fact that arithmetic can express its own syntax and partially its own semantics is of basic importance for the investigation of its metamathematics.

(a) Some Logic

0.1. Throughout the book, N is the set of all natural numbers (including zero). We shall denote natural numbers mainly by letters m, n, k, l, possibly indexed. The *least number principle* assures that each non-empty set of natural numbers has a least element. The *induction principle* says that if X is a set such that $0 \in X$ and X contains with each natural number n also its successor $n+1$, then $N \subseteq X$.

0.2. Our survey of logic will have a double purpose: on the one hand, we shall investigate axiomatic systems of arithmetic as first-order theories and therefore first order logic will be our main device, and, on the other hand, we shall develop our axiomatic systems as meaningful mathematical theories and shall, among other things, formalize parts of first order logic in these systems. The fact that reasonable parts of logic can be developed in first-order arithmetic is of basic importance, as we shall see in the future.

0.3. A first-order *language* consists of *predicates* and *function symbols* (each predicate and function symbol has its non-zero natural *arity*), *constants,* and *variables.* A particular predicate $=$ of *equality* (binary, i.e. of arity 2) is assumed to belong to each language. There are infinitely many variables. Constants and variables are *atomic terms*; if F is a k-ary function symbol and $t_o, \ldots, t_k$ are terms then $F(t_o, \ldots, t_k)$ is a *term.* An *atomic formula* is $P(t_o, \ldots, t_k)$ where P is a k-ary predicate and $t_o, \ldots, t_k$ are terms. If φ, ψ are formulas and x is a variable, then $\neg\varphi, \varphi \rightarrow \psi, (\forall x)\varphi$ are formulas. The symbols $\neg, \rightarrow$ are *connectives* (negation and implication); other usual connectives ($\&, \vee, \equiv, etc.$) are understood as abbreviations. $\forall$ is the *universal quantifier*; the *existential quantifier* $\exists$ is understood as an abbreviation. The notion of a *free* and *bound* variable in a formula is assumed to be known; e.g. x is free and y is bound in $P(x) \rightarrow (\forall y)Q(x, y)$. $Subst(\varphi, x, t)$ denotes the result of substitution of the term t for all free occurences of the variable x in the formula φ. We often write $\varphi(x)$ instead of φ and $\varphi(t)$ instead of $Subst(\varphi, x, t)$ if there is no danger of misunderstanding.

0.4. A *model* for a language L consists of a non-empty domain M together with the following: for each k-ary predicate P of L, a k-ary relation $P_M \subseteq M^k$, for each k-ary function symbol F of L, a k-ary mapping $F_M : M^k \rightarrow M$, for each constant c an element $c_M \in M$. We use the same symbol M to denote both the model and its domain if there is no danger of misunderstanding. M has *absolute equality* if the equality predicate is interpreted by the identity relation $\{\langle a, a\rangle | a \in M\}$. An *evaluation* of a term in M is a finite mapping e whose domain consists of some variables, among them all variables occuring in t, and whose range is included in M. Similarly for an evaluation of a formula ($dom(e)$ contains all variables free in φ).

0.5. The *value of a term* t in a model M given by an evaluation e is defined as follows:

$$
\begin{aligned}
t_M[e] \text{ is } & t_M \text{ if } t \text{ is a constant,}\\
& e(t) \text{ if } t \text{ is a variable,}\\
& F_M(t_{1M}[e], \ldots, t_{kM}[e]) \text{ if } t \text{ is } F(t_1, \ldots, t_k)\ .
\end{aligned}
$$

0.6. The following are *Tarski's conditions for satisfaction* ($M \models \varphi[e]$ is to be read "e satisfies φ in M").

(i) If φ is atomic, say $P(t_1, \ldots, t_k)$, then $M \models \varphi[e]$ if $\langle t_{1M}[e], \ldots, t_{kM}[e]\rangle \in P_M$ (the tuple of values of $t_1, \ldots, t_k$ is in the relation that is the meaning of P).

(ii) $M \models \neg\varphi[e]$ iff $M \not\models \varphi[e]$;

(iii) $M \models (\varphi \rightarrow \psi)[e]$ iff $M \not\models \varphi[e]$ or $M \models \psi[e]$;

(iv) $M \models (\forall x)\varphi[e]$ iff $M \models \varphi[e']$ for each e' coinciding with e on all arguments except x and defined for x.

0.7. Let Γ be a class of formulas of a language L, assume that Γ contains with each formula all its subformulas, let M be a model for L. A ternary relation $Sat$is a *satisfaction relation for Γ in M* if the following conditions hold:

(1) Sat consists of some pairs $\langle\varphi, e\rangle$, where $\varphi \in \Gamma$ and e is an evaluation of φ.

(2) Let $M \models \varphi[e]$ mean $\langle\varphi, e\rangle \in Sat$; then, for each $\varphi \in \Gamma$ and each evaluation e of φ, Tarski's conditions (i)–(iv) hold.

(Clearly, for each Γ and M, the satisfaction relation Sat for Γ in M is uniquely determined. But this is a rather strong fact; we shall investigate the provability of existence of various satisfaction classes in various axiomatic systems.)

0.8. φ is *true* in M ($M \models \varphi$) iff $M \models \varphi[e]$ for each e. We shall use various usual conventions in using the symbol $\models$; for example, if φ has the only free variable x and $a \in M$, we shall write $M \models \varphi[a]$ or $M \models \varphi(a)$ instead of $M \models \varphi[e]$ where e is the mapping defined only for x and giving x the value a.

0.9. A set $x \in M$ is *Γ-definable* in M (where M is a model for L and Γ is a class of L-formulas) if there is a $\varphi \in \Gamma$ having exactly one free variable, such that $X = \{a \in M | M \models \varphi(a)\}$. (This is non-parametrical definability; we shall deal with parametrical definability later on.) Occasionally, we shall denote by φ_M the set defined by φ, thus: $a \in \varphi_M$ iff $M \models \varphi(a)$.

0.10. We shall fix any usual set of (Hilbert-style) *logical axioms* and *deduction rules,* for example the following ones:

Axioms:

$$\varphi \to (\psi \to \varphi)$$
$$((\varphi \to (\psi \to \chi)) \to ((\varphi \to \psi) \to (\varphi \to \chi))$$
$$(\neg\psi \to \neg\varphi) \to (\varphi \to \psi)$$
$$(\forall x)\varphi(x) \to \varphi(t) \qquad (t \text{ free for } x \text{ in } \varphi)$$

Rules: From φ and $\varphi \to \psi$ infer ψ (modus ponens).
From $\nu \to \varphi(x)$ infer $\nu \to (\forall x)\varphi(x)$ if x is not free in ν.

0.11. An *axiomatic theory* in a language L is given by a set T of L-formulas called *special axioms* of the theory. Axioms for *equality* (saying that equality is reflexive, symmetric, transitive and is a congruence with respect to all predicates and function symbols) are assumed to belong to special axioms of each axiomatic theory; they will not be explicitly mentioned. $T \vdash \varphi$ means that φ is *provable* in T, i.e. there is a T-proof of φ (a sequence $\varphi_0, \ldots, \varphi_n$ of L-formulas such that φ_n is φ and for each $i \leq n$, either φ_i is an axiom (logical or special) or φ_i follows from some preceding members of the sequence using a rule of inference).

T is *consistent* if it does not prove any contradiction, i.e. for each $\varphi, T \nvdash \varphi$ or $T \nvdash \neg\varphi$ (or both).

M is a *model* of T if M is a model for the language L and each special axiom of T is true in M.

0.12 Gödel's Completeness Theorem. $T \vdash \varphi$ is true in each model of T iff φ is true in each countable model of T. Thus: T is consistent iff T has a model.

Convention. All models investigated in this book are countable (or finite).

Next we shall deal with Skolemizations. The reader is assumed to know how to convert each formula in a logically equivalent formula in the *prenex normal form,* i.e. a formula consisting of a block of quantifiers followed by an open (quantifier-free) formula.

0.13. Let T be a theory in a language L, let $\varphi(x_1, \ldots, x_k, y)$ be an L-formula and let F be a k-ary function symbol not in L; put $L' = L \cup \{F\}$. The formula

$$\varphi(x_1, \ldots, x_k, y) \rightarrow \varphi(x_1, \ldots, x_k, F(x_1, \ldots, x_k))$$

is the *Skolem axiom* for φ and y.

0.14 Lemma. If T is a theory in a language L and $\hat{T}$ results from T by adding a Skolem axiom, then $\hat{T}$ is a conservative extension of T, i.e. each L-formula provable in $\hat{T}$ is provable in T.

(A model-theoretic proof is trivial: each (countable) model of T has an expansion to a model of T. Indeed, let $M \models T$, and assume that the domain of M is N. For each $a \in N$, let $f(a)$ be the least $b \in N$ such that $M \models \varphi(a, b)$, if such a b exists; otherwise put $f(a) = 0$. Clearly, $(M, f) \vdash T$.)

0.15. Let Φ be the formula

$$(Q_1 x_1), \ldots, (Q_k x_k)\varphi(\mathbf{x}, \mathbf{y})$$

where Q_i is $\forall$ or $\exists$ $(= 1, \ldots, k)$. Let $\mathbf{x}$ mean $x_1, \ldots, x_k$; let $\leftarrow x_i$ mean $x_1, \ldots, x_i$ let $x_i \rightarrow$ mean $x_i, \ldots, x_k$. Define a sequence of terms as follows:

$$t_i = x_i \text{ if } Q_i \text{ is } \forall\ ,$$
$$t_i = F_i^{\Phi}(\leftarrow t_{i-1}) \text{ if } Q_i \text{ is } \exists\ ,$$

F_i^{Φ} being a new function symbol. Finally, put

$$sk(\Phi) = \varphi(t_1, \ldots, t_k, \mathbf{y})\ .$$

(Example: $sk(\forall x)(\exists y)(\forall u)(\exists v)\varphi(x,y,u,v)$ is $\varphi(x,F_1(x),u,F_2(x,F_1(x),u))$.) If T is a theory, then $sk(T)=\{sk(\Phi)|\Phi\in T\}$.

0.16 Corollary. $sk(T)$ is an open conservative extension of T, i.e. all axioms of $sk(T)$ are quantifier-free and each L-formula provable in $sk(T)$ is provable in T.

Proof. For $i=0,\dots,k$ let $\Phi^{(i)}$ result from Φ by deleting the first i quantifiers, thus $\Phi^{(i)}$ is $(Q_{i+1}x_{i+1})\dots\varphi(x,y)$. First extend T by adding, for $i=0,\dots,k$, the following Skolem axioms:

$$\Phi^{(i)}(\leftarrow x,y)\rightarrow\Phi^{(i)}(\leftarrow x_{i-1},F_i^{\Phi}(\leftarrow x_{i-1}),y)\ .$$

Do this for each axiom Φ of T. The new theory T' is a conservative extension of T. □

Claim 1. $T'\vdash sk(T)$.

Take a $\Phi\in T$ and prove by induction $\Phi^{(i)}(\leftarrow t_i,y)$ in T'. $\Phi^{(i)}$ is Φ; and $T',\Phi^{(i)}(\leftarrow t_i,y)\vdash\Phi^{(i+1)}(\leftarrow t_{(i+1)},y)$ either by predicate calculus (if Q_{i+1} is $\forall$) or by the above Skolem axiom (if Q_{i+1} is $\exists$). And obviously $\Phi^{(k)}(t_1,\dots,t_k)$ is $sk(\Phi)$.

Claim 2. $sk(T)\vdash T$.

Prove by induction $sk(\Phi)\vdash\Phi^{(i)}(\leftarrow t_i,y)$ for $i=k,\dots,0$. $\Phi^{(k)}(\leftarrow t_i,y)$ is $sk(\Phi)$; and $\Phi^{(i+1)}(\leftarrow t_{(i+1)},y)\vdash\Phi^{(i)}(\leftarrow t_i,y)$ either by generalization (if Q_i is $\forall$) or by the logical schema $\alpha(t)\vdash(\exists x)\alpha(x)$ (if Q_i is $\exists$).

0.17 Lemma. Each theory T has an open conservative extension $\hat{T}$ in which each formula is equivalent to an open formula.

Proof. Put $T_0=T,T_{n+1}$ is the extension of T_n by Skolem axioms for all open formulas of T_n, let $T_\infty=\bigcup_n T_n$ and $T'=T_\infty-T_0$. Clearly, T_∞ is a conservative extension of T. We shall show that each formula ψ of T' is equivalent in T' to an open formula. For this purpose it suffices to assume ψ to have the form $(\exists y)\varphi(\mathbf{x},y),\varphi$ open. But then the Skolem axiom for φ and y guarantees that, for an appropriate F, $T'\vdash(\exists y)\varphi(\mathbf{x},y)\equiv\varphi(\mathbf{x},F(\mathbf{x}))$. Now it suffices to replace in T_∞ each element of T_0 by its open equivalent; the resulting theory is $\hat{T}$. □

0.18. For any Φ, let the *Herbrand variant* of Φ, $He(\Phi)$ be the existential closure of $\neg sk(\neg\Phi)$: e.g. if Φ is $(\forall x)(\exists y)(\forall u)(\exists v)\varphi(x,y,u,v)$, then $He(\Phi)$ is $(\exists y)(\exists v)\varphi(c,y,F(c,y,v)$.

0.19 Theorem. Φ is provable (in logic, i.e. in the theory with no special axiom) iff $He(\Phi)$ is provable.

(Immediate from 0.16.)

0.20 Lemma. Let $\varphi(\mathbf{x})$ be an open L-formula ($\mathbf{x}$ is a tuple of variables). The formula $(\exists \mathbf{x})\varphi(\mathbf{x})$ is provable (in logic) iff there are tuples $\mathbf{t}_1, \ldots, \mathbf{t}_n$ of L-terms such that the disjunction

$$\varphi(\mathbf{t}_1) \vee \ldots \vee \varphi(\mathbf{t}_n)$$

is a propositional tautology. (Each $\varphi(\mathbf{t}_i)$ is called an *instance* of $\varphi(\mathbf{x})$.

Note that this also has an easy model-theoretic proof using Königs lemma; König's lemma will be studied in Chap. I, Sect. 3.

0.21 Herbrand's Theorem. A formula Φ is provable in logic iff there is a disjunction D of finitely many instances of the quantifier-free matrix of $He(\Phi)$ such that D is a propositional tautology.

This follows from the preceding. An elementary proof (not using model theory) can be found in Shoenfield's book. In I.4.15 we shall claim that Herbrand's theorem is (meaningful and) provable in a theory called $I\Sigma_1$ (defined in Chap. I, Sect. 1), again with the help of Shoenfield's book, and in III.3.30 we shall prove in $I\Sigma_1$ a theorem that has the implication $\Leftarrow$ of Herbrand's theorem as its corollary. (In fact, we shall elaborate Shoenfield's proof of that implication.) Finally, in Chap. V we prove Herbrand's theorem in a rather weak system of arithmetic.

We now turn to some basic notions and facts of recursion theory. Recall that N denotes the set of natural numbers.

0.22. Primitive recursive functions and general recursive functions are usually defined as follows:

$$\begin{aligned} &\textit{Basic PRF's:} \qquad \mathit{Zero}(n) = 0, \quad \mathit{Succ}(n) = n+1\ , \\ &I^i_m(n_0, \ldots, n_m) = n_i \qquad (\text{where} \quad 0 \le i \le m)\ . \end{aligned}$$

A function $F : N^n \to N$ results from $G : N^m \to N$ and $H_1, \ldots, H_m : N^n \to N$ by *composition* if

$$F(k_1, \ldots, k_n) \;=\; G(H_1(k_1, \ldots, k_n), \ldots H_m(k_1, \ldots, k_n))$$

for each $k_1, \ldots, k_n \in N$. An $F : N^{n+1} \to N$ results from $G : N_n \to N$ and $H : N_{n+2} \to N$ by *primitive recursion* if, for each $\mathbf{k} = (k_1, \ldots, k_n)$, and each m,

$$\begin{aligned} F(0, \mathbf{k}) &= G(\mathbf{k})\ , \\ F(m+1, \mathbf{k}) &= H(m, \mathbf{k}))\ . \end{aligned}$$

The class of all *primitive recursive functions* (PRF's) is the smallest class containing basic PRF's and closed under composition and primitive recursion.

An $F : N_{m+1} \to N$ results from $G : N^{m+2} \to N$ by *regular minimization* if for each $m, \mathbf{k} = (k_1, \ldots, k_n)$,

$$F(m, \mathbf{k}) = (\min q)(G(m, \mathbf{k}, q) = 0)$$

and for each $m, \mathbf{k}$ there exists a q such that $G(m, \mathbf{k}, q) = 0$ (so that F is total, i.e. defined for each $m, \mathbf{k}$).

The class of all *general recursive functions* is the smallest class containing the basic PRF's and closed under composition, primitive recursion and minimization.

0.23 Examples of PRF's: addition *Add*, multiplication *Mult*, exponentiation *Exp*, factorial *Fact*, difference *Diff*. We freely write $n + m, n * m, n_m, n!, n - m$ instead of $Add(n,m), Mult(n,m), Exp(n,m), Fact(n), Diff(n,m)$, respectively. (A word on difference: $n - m$ for natural numbers means $max(n - m, 0)$ as meaningful for integers; thus $5 - 3 = 2$ and $3 - 5 = 0$.)

0.24. A set $X \subseteq N_n$ is *primitive recursive* (PR) [*general recursive* (GR)] if its characteristic function

$$\chi_X(k_1, \ldots, k_n) = \begin{cases} 1 & \text{if } \langle k_1, \ldots, k_n \rangle \in X, \\ 0 & \text{otherwise}. \end{cases}$$

is PR [GR, respectively].

0.25 Examples. The equality relation as well as the less-than relation are both primitive recursive; both PR and GR sets are closed under Boolean operations. The set of all primes is a PR set; the increasing enumeration p_n of primes ($p_0 = 2, p_1 = 3, p_2 = 5, p_3 = 7, p_4 = 11$ etc.) is a PRF.

0.26. Let Γ be a class of functions such that each $F \in \Gamma$, $F : N^n \to N$ for some n. (We say that Γ is a class of *total number theoretic functions.* It is obvious what we mean by saying that Γ is closed under substitution, primitive recursion, regular minimization, etc. A Γ set *(relation)* is a set (relation) whose characteristic function is in Γ. If Γ contains basic PRF's and is closed under composition and primitive recursion (or: under composition and regular minimization) then it is closed under definitions of functions by cases (with a condition in Γ) and under bounded minimization. In more detail:

Let A be a Γ set, let $F_1, F_2 : N \to N$ be in Γ. Define

$$F(n) = F_1(n) \text{ if } n \in A,$$
$$F(n) = F_2(n) \text{ otherwise}.$$

Then $F \in \Gamma$. (Generalize for $F_1, \ldots, F_k$ of n arguments and $A_1, \ldots, A_k$ a partition of N^n.)

Let $R \subseteq N^{n+1}$, let R be a Γ-relation and put

$$F(k, \mathbf{q}) = (\min m \leq k)\ R(m, \mathbf{q}) \text{ if there is such an } m,$$
$$F(k, \mathbf{q}) = 0 \text{ otherwise };$$
$$S(k, \mathbf{q}) = \{\langle k, \mathbf{q}\rangle | (\exists m \leq k)\ R(m, \mathbf{q})\}\ .$$

Then $F \in \Gamma$ and S is a Γ-relation.

0.27. For each class Γ of number-theoretic total functions, let $Prim(\Gamma)$ (the class of all functions primitive recursive in Γ) be the minimal class containing all basic primitive recursive functions, all elements of Γ and closed under composition and primitive recursion. Similarly for the class $Rec(\Gamma)$ of all functions general recursive in Γ.

(b) The Language of Arithmetic, the Standard Model

0.28. Recall that N is the set of natural numbers. N also denotes the set of natural numbers together with the usual arithmetical structure:

the unary operation *Succ* of successor (adding one),
the binary operation *Add* of addition,
the binary operation *Mult* of multiplication,
the binary relation *Ord* of linear order,
the minimal element 0.

N is certainly a very natural and very mathematical structure, the ground stone of mathematics. We introduce a first order language L_0 such that N is a model of this language. L_0 has

a unary function symbol S,
binary function symbols $+, *$,
the equality predicate $=$,
a binary predicate $\leq$,
a constant 0.

L_0 is *the language of first-order arithmetic* and N is its *standard model.* Note that each natural number n is named by a variable-free term $\overline{n}$ of L_0: we can just take $\overline{n}$ to be $S(S(\ldots S(0)\ldots))$ (n occurrences of S). Thus 1 is $S(0)$, 4 is $S(S(S(S(0))))$, etc. For some investigations (in Chap. V) we need more economical names; this will be made explicit if the situation demands. The term $\overline{n}$ is the nth *numeral.*

Notational Conventions. We shall freely use obvious conventions in writing terms of L_0: *first,* we shall use the infix notation (we write $x + y$ rather than $+(x, y)$, the same for $*$), *second*, the multiplication sign may be omitted if there is no danger of misunderstanding (xy means $x * y$), *third*, we omit unnecessary parentheses, declaring $*$ to be superordinated to $+$ ($x * y + 2$ and $xy + 2$ both stand for $(x * y) + 2$ etc.).

0.29. Any model isomorphic to N is also called standard. It is easy to show that there is a model M which is elementarily equivalent to N (i.e. has the same true L_0-formulas) but is not standard: let $Th(N)$ be the set of all sentences true in N, let c be a new constant and let $T = Th(N) \cup \{\overline{n}\langle c \mid n \in N\}$. By compactness, T is consistent and hence has a model M. Show by induction that if f is an isomorphism of N to M then for each $n, f(n) = \overline{n}_M$ and therefore c_M has no preimage. Thus M is not isomorphic to N.

0.30 Bounded Quantifiers and Arithmetical Hierarchy. $(\exists x \leq y)\varphi$ is an abbreviation for $(\exists x)(x \leq y \,\&\, \varphi)$ and $(\forall x \leq y)$ is an abbreviation for $(\forall x)(x \leq y \rightarrow \varphi)$. By convention, x and y must be *distinct variables*. An L_0-formula is *bounded* if all quantifiers occuring in it are bounded, i.e. occur in a context as above. Furthermore, $(\forall x < y)\varphi$ is an abbreviation for $(\forall x \leq y)(x \neq y \rightarrow \varphi)$ and similarly for $(\forall x < y)$; $x \neq y$ is the same as $\neg(x = y)$.

We introduce a hierarchy of formulas called the *arithmetical hierarchy*. Σ_0-formulas $=$ Π_0-formulas $=$ bounded formulas; Σ_{n+1}-formulas have the form $(\exists x)\varphi$ where φ is Π_n, Π_{n+1}-formulas have the form $(\forall x)\varphi$ where φ is Σ_n. Thus a Σ_n-formula has a block of n alternating quantifiers, the first one being existential, and this block is followed by a bounded formula. Similarly for Π_n.

0.31. A set $X \subseteq N$ is Σ_n (or Π_n) if it is defined by a Σ_n-formula ((Π_n-formula) with exactly one free variable. Similarly for a relation $R \subseteq N^k$. X is Δ_n if it is both Σ_n and Π_n. A function $F : N^k \rightarrow N$ is Σ_n, etc., if it is Σ_n as a relation $\subseteq N^{k+1}$ (the graph of F).

In particular, X is Δ_0 iff it is Σ_0; Π_n relations are complements of Σ_n relations and vice versa.

0.32 Pairing. There is a Σ_0 pairing function, i.e. a one-one mapping OP of N_2 onto N, increasing in both arguments.

Indeed, the usual "diagonal" enumeration of ordered pairs of natural numbers

$$
\begin{array}{ccccccc}
 & 0 & 1 & 2 & 3 & \ldots \\
0 & 0 & 1 & 3 & 6 & \ldots \\
1 & 2 & 4 & 7 & \ldots \\
2 & 5 & 8 & \ldots \\
3 & 9 & \ldots
\end{array}
$$

satifies the following:

$$OP(m,n) = \frac{1}{2}(m+n+1)(m+n)+m\ .$$

Clearly, this function is defined by the formula

$$2z = (x+y+1)(x+y)+2x\ ;$$

we denote the last formula by $OP(x,y,z)$. Furthermore, we expand N by adding OP to its structure; and expand L_0 by a new binary function symbol (x,y) interpreted as OP. We keep the notation N, L_0 for the (inessentially) expanded structure and language. Thus we have

$$N \models (\forall x,y) OP(x,y,(x,y))$$

and for each $m,n \in N$ we have

$$OP(m,n) = (m,n)_N$$

If there is no danger of misunderstanding we omit the subscript N in $(m,n)_N$; thus we write also (m,n) for $OP(m,n)$.

0.33 Notation Conventions Continued. We give a detailed notational explanation on the pairing function since this exemplifies a general notational method common in the metamathematics of arithmetic and also used in the present book:

(1) The structure N and language L_0 is notationally not distinguished from its inessential expansions if not necessary.
(2) If we have a relation $R \subseteq N^k$ and exhibit a concrete definition of R in N formulated in L_0 then the defining formula is denoted by $R^\bullet$ (dot notation). Similarly for functions.
(3) Conversely, if we have a function symbol F and its interpretation F_N in N we often omit the subscript N and write $F(k,\ldots)$ instead of $F_N(k,\ldots)$. Similarly for relations.

Now that we have introduced the language of arithmetic we see that $m+n$ is shorthand for $m +_N n$ and that the formula $x+y=z$ could be denoted by *Add*$^\bullet$; similarly for *Succ* and *Mult*.

This convention will be used tacitly through the book; it will be generalized (and made more precise) in connection with axiomatic theories having N as one of their models.

Caution. Even if we expand the language we keep the notion of Σ_n and Π_n formulas unchanged, i.e. assume that they are formulated in L_0 in its original meaning. (A formula in the enriched language may or may not be *equivalent* to a Σ_n or Π_n formula; this needs further investigation).

0.34 Theorem. For each natural n,

(1) Σ_n, Π_n, Δ_n relations are closed under intersection and union;
(2) Δ_n relations are closed under complementation;
(3) if $n > 0$ then Σ_n relations are closed under existential projection and Π_n relations are closed under universal projection.

Proof. We prove (1) & (2) & (3) by induction on n. For $n = 0$ the assertion is evident. Assume it for n and consider $n + 1$. The claim (2) is trivial; let us prove (3) for Σ_{n+1} (the proof for Π_{n+1} is similar). Let R be defined by $(\exists z)\varphi(\mathbf{x}, y, z)$ where φ is Π_n, and let R' be defined by $(\exists y)(\exists z)\varphi(\mathbf{x}, y, z)$. Then R' is defined by

$$(\exists u)(\forall y)(\forall z)(u = (y, z) \rightarrow \varphi(x, y, z))$$

as well as by

$$(\exists u)(\forall y \leq u)(\forall z \leq u)(u = (y, z) \rightarrow \varphi(x, y, z)) .$$

If $n = 0$ then the latter formula is clearly Σ_1; if $n > 0$ then, by the induction assumption, the former formula is equivalent (in N) to a Σ_{n+1} formula. (Once and for all, let us elaborate details: φ is Π_n, both $u = (y, z)$ and its negation are Σ_0, hence Π_n, and by (3), the formula in question is also Π_n.)

To prove (1) let $(\exists y)\varphi(\mathbf{x}, y)$ and $(\exists z)\psi(\mathbf{x}, z)$ be Σ_{n+1} and assume y, z to be distinct variables. Then $(\exists y)\varphi(\mathbf{x}, y) \,\&\, (\exists z)\psi(\mathbf{x}, z)$ is logically equivalent to $(\exists y)(\exists z)(\varphi(\mathbf{x}, y) \,\&\, \psi(\mathbf{x}, z))$ and similarly for $\vee$; thus (1) for n and (3) for $(n + 1)$ give the result. □

0.35 Theorem. Each Σ_0 set is primitive recursive.

Proof. Since successor, addition and multiplication are PRF's, each term defines a PRF; since equality and ordering are PR relations, each atomic formula defines a PR relation. Dummy variables may be introduced using I^i_m. And PR relations are closed under Boolean operations and bounded projection. □

We shall now investigate the question whether each PRF, and moreover, each GRF, is definable in N. The result will be that general recursive functions coincide with Δ_1 functions; this appears to show that the choice of our language is natural. First note the following

0.36 Lemma. If a function $F : N^n \rightarrow N$ is Σ_1 then it is Δ_1.

Proof. Let F be defined by a Σ_1 formula $\varphi(\mathbf{x}, y)$, i.e. $F(m_1, \ldots) = k$ iff $N \models \varphi(m_1, \ldots, k)$. Then the complement of F in N^{n+1} is defined by $(\exists z)(z \neq$

$y \,\&\, \varphi(\mathbf{x}, z))$ which is again a Σ_1 formula. Note that the lemma does not generalize to partial functions, i.e. mappings *from* N^n into N. □

0.37 Lemma. Basic PRF's are defined by open formulas.

Proof. Take $y = 0$, $y = S(x)$, $y = x_i$. □

0.38 Lemma. Δ_1 functions are closed under composition.

Proof. For simplicity, let $F(k) = G(H(k))$ for each k, and let $\varphi(x, y), \psi(x, y)$ define G, H respectively, $\varphi, \psi \in \Sigma_1$. Then F is defined by the Σ formula

$$(\exists z)(\psi(x, z) \,\&\, \varphi(z, y)) \;. \qquad \square$$

0.39 Lemma. Σ_1 relations are closed under bounded universal projections.

Proof. Let $R \subseteq N^2$ be defined by a formula $(\exists z)\varphi(x, y, z)$ where φ is Σ_0 and let $S \subseteq N$ be defined by $(\forall x \leq y)(\exists z)\varphi(x, y, z)$. We show that S is also defined by $(\exists w)(\forall x \leq y)(\exists z \leq w)(\varphi(x, y, z)$, which is Σ_1. (Thus the quantifier $(\exists z)$ can be bounded.) Clearly the latter formula implies the former. Thus assume $k \in S$; we find a q such that $N \models (\forall x \leq \overline{k})(\exists z \leq \overline{q})\varphi(x, \overline{k}, z)$. To this end we show by induction that for each $i = 0, 1, \ldots k$ there is a q_i such that

$$N \models (\forall x \leq \overline{i})(\exists z \leq \overline{q}_i)\varphi(x, k, z) \;.$$

Since $k \in S$ we know $N \models (\forall x \leq k)(\exists z)\varphi(x, k, z)$; thus the case $i = 0$ is evident. Assume q_i has been found and let r be such that $N \models \varphi(\overline{i + 1}, \overline{k}, r)$. Put $q_{i+1} = \max\,(q_i, r)$. □

0.40 Lemma. Δ_1 functions are closed under regular minimization.

Proof. Let $F(k) = (\min q)(G(k, q) = 0)$, $F : N \to N$, G be Σ_1 defined by $\varphi((x, y, z)$. Then F is Σ_1 defined by

$$\varphi(x, y, 0) \,\&\, (\forall y' < y))(\exists z \neq \overline{0})\varphi(x, y', z) \;.$$

This shows that F is Σ_1, hence, by 0.36, it is Δ_1. □

The problem is to show that Δ_1 functions are closed under primitive recursion. If F results from G from G and H by primitive recursions then an explicit definition of $F(k)$ is easily made using the sequence $F(0), F(1), \ldots, F(k)$ since we can describe $F(0)$ and describe $F(i + 1)$ from $F(i)$. Thus some Δ_1 definable coding of finite sequences of natural numbers by natural numbers is desirable. In fact, such a coding is a device used very often in arithmetic. We shall state the existence of such a coding using the following

0.41 Definition. A *coding of finite sequences* (of natural numbers by natural numbers) consists of a PR set $Seq \subseteq N$ and PRF's

lh (unary; $lh(s)$ is called the length of s),
$memb$ (binary; $memb(s,i)$ is the ith *member* of s),
$prolong$ (binary; $prolong(s,k)$ is the *result of juxtaposing* k with s)

such that the following holds for each $s, s' \in Seq$:

(1) $lh(s) \leq s$ and, for each $i < lh(x)$, $memb(s,i) < s$;
(2) there is an *empty* sequence $\emptyset$ with $lh(\emptyset) = 0$;
(3) for each $k \in N$ if $s' = prolong(s,k)$ then $lh(s') = lh(s) + 1$, for $i < lh(s)$ we have $memb(s,i) = memb(s',i)$ and for $i = lh(s)$ we have $memb(s',i) = k$.
(4) (monotonicity): if $lh(s) \leq lh(s')$ and, for each $i < lh(s)$, $memb(s,i) \leq memb(s',i)$ then $s \leq s'$;
(5) the set $N - Seq$ is infinite.

(Note that (4) implies extensionality; if s, s' have the same length and the same corresponding members then they are equal.)

0.42 Theorem. There is a Δ_1 coding of finite sequences; i.e. a coding such that the set Seq and the functions $lh, memb, prolong$ are Δ_1 (besides being PR).

The proof of this theorem is put off until Chap. I, Sect. 1; we shall then show more, namely that the properties of the coding are *provable* in a suitable fragment of arithmetic.

For most investigations of Chaps. I–IV it is immaterial which concrete coding of sequences is taken; but for some more subtle results, especially on weak fragments, special care will be necessary. In fact, we prove in Chap. V that there is a Σ_0 coding of finite sequences.

Notation. The chosen Δ_1 definitions of Seq, lh, memb and prolong will be denoted by $Seq^\bullet, lh^\bullet, memb^\bullet$ and $prolong^\bullet$; $lh^\bullet$ and $prolong^\bullet$ will also be used as function symbols, thus we shall write $y = lh^\bullet(x)$ instead of $lh^\bullet(x,y)$.

We expand L_0 by a new function (symbol $(-)_-$ for the y-th member of x (thus in formulas we write $z = (x)_y$ for $memb^\bullet(x,y,z)$.

And if there is no danger of misunderstanding, we shall use this bracket notation also informally, thus $(s)_i$ will be the same number as $memb(s,i)$.

A similar convention for the function *prolong* will be made later.

0.43 Corollary. Δ_1 functions are closed under primitive recursion.

Proof. Assume $F(0) = m$ and $F(k+1) = H(k, F(k))$; let H be defined by $\kappa(x,y,z)$. Then F is defined by the following formula $\varphi(x,y)$:

$$(\exists z)(Seq^{\bullet}(z))\,\&\, lh^{\bullet}(z) = x+1\,\&\,(z)_{\overline{0}} = \overline{m}\,\&\\ (\forall u < lh^{\bullet}(z))(\forall v < u)(v+1 = u \rightarrow \kappa(v,(z)_v,(z)_u))$$

Similarly for the case of F having parameters. □

0.44 Remark. (1) In particular, *exponentiation* ($n = m^k$) is Δ_1 since it is primitive recursive. We shall show in Chap. V that exponentiation is Δ_0 (which is a rather non-trivial result).

(2) An apparently more general form of primitive recursion defines $F(k+1)$ from the course of values $F(0), \ldots, F(k)$ directly. Let, for each F, $\hat{F}(k, \mathbf{m}) = s$ iff s is the (code of the) sequence of length $k+1$ such that for each $i \leq k$, $(s)_i = F(i, \mathbf{m})$. F results from G, H by *primitive recursion on the course of values* if $F(0, \mathbf{m}) = G(\mathbf{m})$ and $F(k+1, \mathbf{m}) = H(k, \hat{F}(k), \mathbf{m})$. Clearly, Δ_1 functions are closed under this kind of primitive recursion.

(3) If the reader has a favourite primitive recursive coding of sequences he may keep it since now he knows that his coding is Δ_1 which is sufficient for most applications. But he should keep in mind that it might be rather difficult and cumbersome to show directly that his coding is Δ_1 (or even Σ_0).

0.45 Theorem. A function $F : N_n \rightarrow N$ is general recursive iff it is Δ_1.

Proof. Clearly, each GRF is Δ_1 since basic functions are and the class of Δ_1 functions is sufficiently closed.

Conversely, if $F : N \rightarrow N$ is Δ_1, thus $F(k) = n$ iff $N \models (\exists z)\varphi(\overline{k}, \overline{n}, z)$ where φ is Σ_0 then by 0.35, the relation $R \subseteq N^3$ defined by φ is primitive recursive. Define $F_0(k)$ to be the least sequence s of length 2 such that $R(k, (s)_0, (s)_1)$; then $F(k) = (F_0(k))_0$. F_0 results from F by a regular minimization and taking the 0-th member of a sequence is a primitive recursive function; thus F is a GRF. □

0.46 Fact. An infinite Δ_1 set $X \subseteq N$ has an infinite increasing enumeration (i.e. a $F : N \rightarrow N$ mapping N one-one and increasing onto X).

(The reader can either use the fact that this is true for recursive sets of natural members or prove that fact directly, which is easy using the available means.)

0.47 Some Useful PRFs Concerning Sequences.

(1) For each $n \geq 1$, there is an n-ary PRF associating with each $k_0, \ldots, k_{n-1} \in N$ the *n-tuple* $\langle k_0, \ldots, k_{n-1} \rangle$, i.e. the sequence s of length n such that, for each $i < n$, $(s)_i = k_i$.

(2) *Concatenation:* For $s, t \in Seq$, $s \frown t$ denotes the *concatenation* of s, t, i.e. the sequence w such that

$$\begin{aligned} lh(w) &= lh(s) + lh(t), \\ (w)_i &= (v)_i \text{ for each } i < lh(s), \\ (w)_{lh(s)+j} &= (t)_j \text{ for each } j < lh(t). \\ &\text{Put } s \frown t = 0 \text{ if } s \notin Seq \text{ or } t \notin Seq . \end{aligned}$$

We show that this function is primitive recursive.

$$\begin{aligned} \text{Define } C(s,t,0) &= s \\ C(s,t,i+1) &= prolong(C(s,t,i)), (t)_i) \text{ if } i < lh(t), \\ C(s,t,i+1)) &= C(s,t,i) \text{ if } i \geq lh(t), \\ \text{put } s \frown t &= C(s,t,lh(t)) . \end{aligned}$$

(3) *Concatentation of a sequence of sequences.* If $w \in Seq$ and for each $i < lh(w)$, $(w)_i \in Seq$ then put

$$Concseq\,(w) = (w)_0 \frown (w)_1 \frown \ldots \frown (w)_{lh(w)-1}$$

Concseq is primitive recursive:
Define

$$\begin{aligned} D(w,0) &= \emptyset, \\ D(w,i+1) &= D(w,i) \frown (w)_i \qquad \text{if } i < lh(w), \\ D(w,i+1) &= D(w,i) \qquad \text{if } i \geq lh(w), \\ Conseq(w) &= D(w,lh(w)) . \end{aligned}$$

The reader may easily verify the following facts for sequences s, t ($s \subseteq t$ means that s is an *initial segment* of t, i.e. $lh(s) \leq lh(t)$ and for each $i < lh(s)$, $(s)_i = (t)_i$);

(1) $s \frown t \subseteq s \frown t'$ implies $t \subseteq t'$,
(2) $s \frown t \subseteq s' \frown t'$ implies $s \subseteq s'$ or $s' \subseteq s$,
(3) $s \subseteq t$ implies the existence of a unique u such that $t = s \frown u$,
(4) $Concseq(s \frown t) = Concseq(s) \frown Concseq(t)$.

0.48 Matiyasevič(-Robinson-Davis-Putnam) Theorem. Σ_1 relations coincide with relations defined by existential L_0-formulas, i.e. formulas consisting of a block of existential quantifiers followed by an open formula.

We may additionally assume that the open formula in question does not contain the predicate $\leq$ (thus atomic formulas are only equalities of terms) since $x \leq y$ may be replaced by $(\exists z)(z = x = y)$ and $\neg(x \leq y)$ by $y \leq x \mathbin{\&} x \neq y$. Thus each open formula containing $\leq$ is equivalent to an existential formula not containing $\leq$.

A readable proof may be found in [Davis 73, Hilbert's tenth]. Note that this theorem (often called the MRDP theorem) is very famous; it implies recursive unsolvability of Hilbert's tenth problem.

0.49 Remark. Concerning the choice of the language L_0, observe that what we have said till now gives some justification to our choice of the language of arithmetic. In this language, all GRF's are first order definable (which is very natural for a first order arithmetic); and it can be shown that multiplication is not first order definable in the reduct of N to (L_0 without $*$) and similarly, addition is not first order definable using (L_0 without $+$).

This follows from the fact that the set of all sentences of (L without $*$) true in N is Δ_1 (i.e. recursive), the same for sentences of (L without $+$) and from the undecidability results of Chap. III.

On the other hand, zero, successor and ordering are easily definable in the reduct of N to $(+, *)$; the reasons for taking them as primitives are only technical and inessential variants are possible.

(c) Beginning Arithmetization of Metamathematics

0.50 Introduction. To *arithmetize metamathematics* means to make metamathematics a part of arithmetic (or at least to make important *parts* of metamathematics parts of arithmetic). It is Gödel's invention that this is possible. The first task consists in showing that important logical notions are *definable* in N by formulas of first order arithmetic; this is our task in the present subsection. The second task is then to show that important properties of these notions are provable in various systems of axiomatic arithmetic. (This task is postponed.)

To be able to define logical notions by arithmetical formulas we must identify objects of logic (as symbols, formulas, proofs, etc.) with numbers. There are two approaches to this task, not substantially different. First, we may think of logical objects as non-numbers (whatever they may be) and give some explicit rules on how to associate numbers to them. This procedure is usually called Gödel numbering and speaks of Gödel numbers of formulas, proofs, etc. Feferman observed that we have another apparently simpler possibility: just to *identify* logical objects with some numbers.

Recall our (pseudo)definition of terms: we defined some atoms (atomic terms) and specified operations (formation rules) under which the set of terms is closed. There are two tacit assumptions: first that the set of terms is the *least* set containing all atoms and closed under formation rules; and, second, that each non-atom t uniquely determines the formation rule and its components that give t according to the formation rule. Similarly for formulas; so let us speak generally about *expressions*. We have a set $At \neq 0$ of *atoms*, a set Op of *operations*, each operation e having its *arity* $Ar(e)$, and expressions are just elements of the free algebra generated by our atoms using our operations. More precisely, the *free algebra* of the type (Op, Ar) generated by At is a set $Expr \subseteq At$ together with a function $Appl$ (of application) associating with each operation o, and each sequence s of expressions such that $lh(s) = Ar(o)$, an expression $Appl(o, s) \in At$ such that $Appl$ is one-one (for such pairs (o, s)) and $Expr$ is the smallest set containing At and closed under $Appl$. Generalizing slightly, we replace the assumption $At \subset Expr$ by the assumption that we have a one-one embedding of At into $Expr$; it will be technically convenient to assume that for each atom $a \in At$ the one-element sequence $\langle a \rangle$ is an *atomic expression*. $Appl$ is then defined for pairs (o, s) as above and its range is the set of non-atomic expressions.

Finally, two free algebras given by At, Op, Ar are isomorphic in the obvious sense. Thus we may speak of *the* free algebra and its various *presentations*. We are interested in Δ_1 presentations.

0.51 Fact. Let $0 \neq At \subset N$, let (Op, Ar) be a type, $At \cap Op = 0$. Then there is a presentation $(Expr, Appl)$ of the free algebra of the type (Op, Ar) generated by At such that both the set $Expr$ and the function $Appl$ are primitive recursive in (At, Op, Ar).

Proof. For each $o \in Op$ and each sequence s of length $Ar(o)$ let $Appl(o, s)$ be $\langle o \rangle \frown Concseq(s)$, i.e. the sequence beginning by o and continuing by the concatenation of all members of s; let $Appl(o, s) = 0$ otherwise. (Note that this presentation is often called the Polish notation.) Clearly, $Appl$ is PR in (Op, Ar). Call w a *derivation* of z if w is a sequence, its last element is z and for each $i < lh(w)$ we have the following:

either $(w)_i$ is an atomic expression $\langle x \rangle$ or there are $o, s < w$ such that $(w)_i = \langle o \rangle\, Concseq(s), o \in Op, s$ is a sequence of length $Ar(o)$ and for each $k < lh(s)$, there is a $j < i$ such that $(s)_k = (w)_j$ (i.e. $(w)_i$ results from some preceding elements of w using an operation).

Let

$$Expr = \{z | (\exists w)(w \text{ is a derivation of } z)\}\ .$$

We show that $(Expr, Appl)$ is a presentation of the free algebra in question. $\square$

Lemma A. If e, e' are expressions and $e \subset e'$ then $e = e$.

Proof. Let e be the smallest expression such that there is an expression e' which is a proper initial seqment of e. Then $e = \langle o \rangle\, Concseq(s)$ and $e' = \langle o \rangle \frown Concseq(s'), s \neq s'$. Let i be the least number such that $(s)_i \neq (s')_i$;

show (using 0.47 (1)–(4)) that $(s)_i \subset (s')_i$ or $(s')_i \subset (s)_i$ and $(s)_i, (s')_i$ are expressions less than e. □

Lemma B. If $e = \langle o \rangle \frown Concseq((s)$ and $e' = \langle o \rangle \frown Concseq(s')$ are expressions and $e = e'$ then $s = s'$.

Proof. Assume not; then $Concseq(s) = Concseq(s')$ and if i is the least such that $(s)_i \neq (s')_i$ then $(s)_i \subset (s')_i$ or $(s')_i \subset (s)_i$, which contradicts Lemma A. Thus $(Expr, Appl)$ is a presentation.

It remains to show that $Expr$ is a set PR in (At, Op, Ar). For this it is sufficient to bound the quantifier $(\exists w)$ in the definition above, i.e. to find a function H PR in (At, Op, Ar) such that

$$Expr = \{e | (\exists w < H(e))(w \text{ is a derivation of } e)\} .$$

To this end show that if e has a derivation then it has a derivation w' without repetitions and such that each $(w)_i$ is a (non-initial) segment of e, i.e. for some s, t, $e = s \frown (w)_i \frown t$. (Just omit all superfluous members of w and show that the resulting sequence w' is a derivation of e).

We know from the preceding that for each s there is at most one expression e' and at most one t such that $e = s \frown e' \frown t$; thus sequence w' satisfies $lh(w') \leq lh(e)$. Thus we can choose $H(e) = \langle e, \ldots, e \rangle$ (e times); clearly, H is PR. This completes the proof of 0.51. □

0.52 Corollary. If (At, Op, Ar) is PR then $(Expr, Appl)$ is PR; if the former is Δ_1 then the latter is Δ_1.

0.53 Definition. A first order language is Δ_1 if the sets of all predicates, function symbols, constants and variables are (mutually disjoint) Δ_1 sets and the function Ar defined for each predicate and function symbol (arity) is a Δ_1 function. We additionally assume that no predicate, function symbol, constant and variable is a sequence and that there are two further non-sequences denoted $\neg$, $\rightarrow$.

0.54 Corollary. If a language L is Δ_1 then there are Δ_1 sets $Term$ (of all terms) and $Form$ (of all formulas) such that

(1) $Term$ is the free algebra given by variables and constants as atoms and function symbols with their arities as operations;
(2) The set of all atomic formulas is Δ_1; the functions associating with each atomic formula its predicate and its sequence of arguments respectively are Δ_1; and no atomic formula is a sequence.
(3) $Form$ is the free algebra given by atomic formulas as atoms and by the following operations: $\rightarrow$ (binary), $\neg$ (unary) and for each variable x an operation $(\forall x)$ (unary).

0.55 Discussion. Here we stop our preliminary development of arithmetization. We survey ideas that could follow; we shall not elaborate on them here since we shall prove stronger results in Chap. I that will imply the facts sketched below as corollaries. Namely, instead of showing that some things are Δ_1 definable in the standard model, i.e. that some definition have some properties in N we show that these properties are ***provable*** in some fragments of arithmetic. We shall prove in particular the following:

- the substitution function $Subst$ is Δ_1 in N;
- the set of all logical axioms is Δ_1 in N. A theory is ***axiomatized*** if its language is Δ_1 and its set of special axioms is also Δ_1.

It is easy to see that for each axiomatized theory T the set of all ***proofs in T*** (***T-proofs***) is Δ_1 and the set of all T-provable formulas is Σ_1. T is ***decidable*** if the set of T-provable formulas is Δ_1. (Undecidability of axiomatized systems of arithmetic is closely related to their incompleteness and will be studied in Part B of the book.)

Concerning semantics:

- the evaluation function Val of terms in N is Δ_1 in N;
- the satisfaction for Σ_0 formulas in N is Δ_1 in N.

In Chap. I we shall show that basic facts about arithmetization as sketched till now are provable in the theory $I\Sigma_1$ using induction for Σ_1 formulas. This will be basic for our investigations of systems of arithmetic containing $I\Sigma_1$, which are a matter of interest in the main part of the book. But note that Chap. V is devoted to theories weaker than $I\Sigma_1$; in these theories special care is necessary and special codings of sequences, formulas etc. are used. Chapters I–IV occasionally use some results from Chap. V; explicit reference will always be made.