数理情報学 6・講義ノート *

木原 貴行
名古屋大学 情報学部・情報学研究科

最終更新日: 2017 年 9 月 13 日

目次

* 本講義ノートは，2017 年度春期開講の名古屋大学情報文化学部 3 年生対象講義「数理情報学 6」の内容をまとめたものである．第 1 回から第 8 回までの講義内容である，命題論理，一階述語論理の入門的話題（シーケント計算の体系 LK の健全性，完全性，カット除去定理，コンパクト性定理，スコーレムの定理など）については，他に多数の教科書・講義ノート等があるので省略した．

1 自然数論の形式体系

1.1 離散順序半環

自然数上の演算の持つ性質を抽象化したい．自然数の代数的性質の分析を行うため，加法の単位元（乗法の零元）である 0 は自然数である $(0 \in \mathbb{N})$ と仮定する．考察する対象は，$(\mathbb{N}, +, \cdot, \leqslant)$ の構造である．たとえば，整数の加法 $(\mathbb{Z}, +)$ はアーベル群をなすが，$(\mathbb{N}, +)$ は逆元を持たないから，そもそも群ですらない．しかし，可換モノイドではある．$(\mathbb{Z}, +, \cdot)$ や $(\mathbb{R}, +, \cdot)$ は可換環であるが，先程と同じ理由により，$(\mathbb{N}, +, \cdot)$ は環ではない．しかし，環になるためには，加法的逆元が足りないだけであって，だいぶ環に近い．こういうものは**半環** (*semiring*) と呼ばれており，$(\mathbb{N}, +, \cdot)$ は可換半環となる．順序も考慮に入れると，$(\mathbb{Z}, +, \cdot, \leqslant)$ や $(\mathbb{R}, +, \cdot, \leqslant)$ は順序環と呼ばれるものになる．もう少し細かく述べると，$(\mathbb{Z}, +, \cdot, \leqslant)$ は離散順序環であり，$(\mathbb{R}, +, \cdot, \leqslant)$ は離散でない順序環である．そうすると，$(\mathbb{N}, +, \cdot, \leqslant)$ は**離散順序半環**というものであろうことは想像に難くない．

それでは，ここまで書き連ねた内容の正確な定義を述べよう．実際には，ここでは，離散順序半環というよりは，**離散順序環の非負部** (*non-negative parts of discretely ordered rings*) と言った方が正確なものの定義を与える．

定義 1.1 (可換モノイド)**.** $*$ を 2 変数関数記号，e を定数記号とする．このとき，$(*, e)$ に対する**可換モノイド** (*commutative monoid*) の公理は以下によって与えられる．

$$\begin{aligned} \text{結合法則:} &\quad \forall a, b, c((a * b) * c = a * (b * c)) \\ \text{単位元:} &\quad \forall a(a * e = e * a = a) \\ \text{可換性:} &\quad \forall a, b(a * b = b * a) \end{aligned}$$

定義 1.2 (可換半環)**.** $+$ と $\cdot$ を 2 変数関数記号とし，0 と 1 を定数記号とする．このとき，$(+, \cdot, 0, 1)$ に対する**可換半環** (*commutative semiring*) の公理は以下によって与えられる．

$$\begin{aligned} &(+, 0) \text{ は可換モノイドの公理を満たす.} \\ &(\cdot, 1) \text{ は可換モノイドの公理を満たす.} \\ \text{分配律:} &\quad \forall x, y, z(x \cdot (y + z) = x \cdot y + x \cdot z) \\ \text{零元:} &\quad \forall x(x \cdot 0 = 0) \end{aligned}$$

定義 1.3 (全順序)**.** $\leqslant$ を 2 変数関係記号とする．このとき，$\leqslant$ に対する**全順序** (*linear order*) の公理は以下によって与えられる．

$$\begin{aligned} \text{反射律:} &\quad \forall x(x \leqslant x) \\ \text{推移律:} &\quad \forall x, y, z(x \leqslant y \wedge y \leqslant z \to x \leqslant z) \\ \text{反対称律:} &\quad \forall x, y(x \leqslant y \wedge y \leqslant x \to x = y) \\ \text{比較可能律:} &\quad \forall x, y(x \leqslant y \vee y \leqslant x) \end{aligned}$$

定義 1.4 (順序半環)**.** $+$ と $\cdot$ を 2 変数関数記号とし，0 と 1 を定数記号とする．このとき，$(+, \cdot, 0, 1)$ に対する**順序半環** (*ordered semiring*) の公理は以下によって与えられる．

$(+, \cdot, 0, 1)$ は可換半環の公理を満たす.
$\leqslant$ は全順序の公理を満たす.

和の順序保存性: $\forall x, y, z(x \leqslant y \ \rightarrow \ x + z \leqslant y + z)$

非負積の順序保存性: $\forall x, y, z(0 \leqslant z \wedge x \leqslant y \ \rightarrow \ x \cdot z \leqslant y \cdot z)$

定義 1.5. $(+, \cdot, \leqslant, 0, 1)$ に対する以下の公理を考える.

非自明性: $0 < 1$

離散性: $\forall x(x > 0 \ \rightarrow \ x \geqslant 1)$

非負性: $\forall x(x \geqslant 0)$

加法的逆元: $\forall x \exists y(x + y = 0)$

減法: $\forall x, y(x \leqslant y \ \rightarrow \ \exists z(x + z = y))$

非負性を満たす順序半環を**正順序半環** (*positive ordered semiring*), 加法的逆元を持つ順序半環を**順序環** (*ordered ring*), 離散性を満たす順序環を**離散順序環** (*discretely ordered ring*) と呼ぶ.

定義 1.6. 順序半環の公理に非自明性，離散性，非負性，減法の公理を加えたものを**離散順序環の非負部**の公理と呼び，DOR^+ と書く.

つまり，公理 DOR^+ を満たす構造とは，減法の公理を満たす非自明な離散正順序半環である[*1].

例 1.7. 自然数全体のなす構造 $(\mathbb{N}, +, \cdot, \leqslant, 0, 1)$ は，DOR^+ を満たす.

離散順序環は $\mathbb{Z}$ 以外にも沢山ある．同様に，DOR^+ のモデルが $\mathbb{N}$ 以外にも沢山あることは予想できる.

例 1.8. $\mathbb{Z}[X]$ を $\mathbb{Z}$ 上の 1 変数多項式環とする，つまり，

$$\mathbb{Z}[X] = \left\{ a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 : n \in \mathbb{N} \ \wedge \ a_0, \ldots, a_n \in \mathbb{Z} \right\}.$$

このとき，$\mathbb{Z}[X]$ が環をなすことはよく知られているが，この上に順序 $\preceq$ を定義することもできる．まず，各多項式 $p \in \mathbb{Z}[X]$ について，$p \succ 0$ とは，p に現れる最大次数の項の係数が非負であることとする．つまり，

$$p = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \succ 0 \iff a_n > 0.$$

一般に，多項式 $p, q \in \mathbb{Z}[X]$ に対して，

$$p \prec q \ \Leftrightarrow \ q - p \succ 0$$

によって順序を定義する．このとき，$(\mathbb{Z}[X], +, \cdot, \preceq, 0, 1)$ は非自明な離散順序環である.

[*1] この公理は，ペアノ算術の公理系 PA と関連付けて語られることが多く，その場合には，DOR^+ ではなく PA^- と書かれることが多い.

例 1.9. 上で定義した順序 $\preceq$ に対して，次の集合を考える．

$$\mathbb{Z}[X]^+ = \{p \in \mathbb{Z}[X] : p \geq 0\}.$$

このとき，$(\mathbb{Z}[X]^+, +, \cdot, \preceq, 0, 1)$ は DOR^+ を満たす．

$\mathbb{Z}[X]$ や $\mathbb{Z}[X]^+$ において，順序だけに注目すると，変数 X を無限大の数のように扱っているように思える．たとえば，$\mathbb{Z}[X]^+$ の順序型としては，始切片として標準自然数 $\mathbb{N}$ があって，その無限の彼方に，無限大元たちの住む「整数の形の島」たちが無限に並んでいるような形をしている．より正確には，以下によって定義される $[p]$ を各 p の所属する “島” のように考える．

$$[p] = \{q \in \mathbb{Z}[X]^+ : (\exists k \in \mathbb{Z})\ q = p + k\}.$$

すると，自然数定数の所属する島 $[n]$ の無限の彼方に $\mathbb{Z}$-型の島 $[X]$ があって，その更に無限の彼方に $[2X]$, $[3X]$, といった島が無限に連なっており，といったことが見て取れるだろう．

$$[n] \prec [X] \prec [2X] \prec [3X] \prec \cdots \prec [X^2 - 2X] \prec [X^2 - X] \prec [X^2] \prec [X^2 + X] \prec \ldots$$
$$\cdots \prec [2X^2 - 6X] \prec [2X^2 + 3X] \prec [3X^2 - X] \prec \cdots \prec [X^3 - 6X^2 - 9X] \prec \ldots$$

例 1.10. 任意の非自明な離散順序環 $(R, +, \cdot, \leq, 0, 1)$ に対して，$R^+ = \{x \in R : x \geq 0\}$ と定義すると，$(R^+, +, \cdot, \leq, 0, 1)$ は DOR^+ を満たす．

豆知識. 逆に，DOR^+ の任意のモデル $\mathcal{M}$ に対して，ある非自明な離散順序環 R が存在して，$\mathcal{M}$ は R の非負部 R^+ と同型になる．これによって，DOR^+ を「離散順序環の非負部の公理」と呼ぶことは正当化されるであろう．

離散順序環の非負部の公理 DOR^+ は自然数の基本演算に関するかなりの部分を捉えるが，それでもやはり完璧には程遠い．たとえば，離散順序環の非負部の公理から「全ての元を偶数と奇数に類別できる」といったようなことを演繹することはできない．ちょうどよい《**証明不可能性の証明**》の練習問題なので，これを確認してみよう．

命題 1.11. $\mathsf{DOR}^+ \nvdash (\forall x)(\exists y)\ [2y = x \vee 2y + 1 = x]$.

Proof. DOR^+ のあるモデルが偶数でも奇数でもない元を持つことを示せばよい．実際，例 1.9 で定義した DOR^+ のモデル $\mathbb{Z}[X]^+$ には，偶数でも奇数でもない元が存在する．$q = a_n X^n + \cdots + a_0$ とすると，$2q = 2a_n X^n + \cdots + 2a_0$ であり，$2q + 1 = 2a_n X^n + \cdots + 2a_0 + 1$ である．したがって，多項式 p の次数正の項の係数が全て偶数でない限り，$p = 2q$ または $p = 2q + 1$ という形には書けないことが分かる．たとえば，X や $3X^2$ などは偶数でも奇数でもない． □

1.2 Σ_1-完全性

命題 1.11 で見たように，わりと自明そうな自然数の性質でも DOR^+ から導出できない可能性がある．しかし，実は，自然数 $\mathbb{N}$ に関する存在型の性質であれば，DOR^+ から導出できることを見ていこう．このために，自然数に関する性質の量化の複雑性による分類の概念を導入する．

言語 $\mathcal{L}_{\mathsf{arith}} = \{+, \cdot, \leqslant, 0, 1\}$ を考える．略記 $(\forall x \leqslant t)\varphi$ および $(\exists x \leqslant t)\varphi$ を以下によって定義する．

$$(\forall x \leqslant t)\varphi \iff (\forall x)\,[x \leqslant t \ \to\ \varphi],$$
$$(\exists x \leqslant t)\varphi \iff (\exists x)\,[x \leqslant t \ \wedge\ \varphi].$$

この形の量化を**有界量化** (*bounded quantification*) と呼ぶ．一方，$\forall x\varphi$ や $\exists x\varphi$ の形の量化を**非有界量化** (*unbounded quantification*) と呼ぶ．

定義 1.12. 非有界量化を用いずに構成される論理式を Δ_0 **論理式** (Δ_0-*formula*) と呼ぶ．本稿では，非有界全称量化を用いずに構成される論理式を Σ_1 **論理式** (Σ_1-*formula*) と呼ぶ．また，ある Δ_0 論理式 θ に対して $\exists x\theta$ の形で書ける論理式を**狭義の** Σ_1 **論理式** (*strict* Σ_1-*formula*) と呼ぶ[*2]．同様に，ある Δ_0 論理式 θ に対して $\forall x\theta$ の形で書ける論理式を Π_1 **論理式** (Π_1-*formula*) と呼ぶ．

豆知識. 広義と狭義の Σ_1 が同値であるという性質は，Σ_1-採集原理 $\mathrm{B}\Sigma_1$ と呼ばれる公理と同値である．この公理は，Σ_1-帰納法公理 $\mathsf{I}\Sigma_1$ (定義 1.25) から証明することができる．

例 1.13. 「x は素数である」ということを表す式 $\mathrm{Prime}(x)$ は Δ_0 論理式である．

$$\mathrm{Prime}(x) \equiv (\forall y \leqslant x)\,[[(\exists z \leqslant x)\ x = z \cdot y] \ \to\ (y = 1 \ \vee\ y = x)].$$

例 1.14. 以下，x^3 は項 $x \cdot x \cdot x$ の略記であるとする．

- 次の式は Σ_1 論理式である．

$$(\exists a, b, c, d)\,[a, b, c \geqslant 1 \ \wedge\ a^3 + b^3 + c^3 = d^3].$$

- フェルマーの最終定理の $n = 3$ のとき (オイラーの定理) を表す次の式は Π_1 論理式である．

$$(\forall a, b, c)\,[a, b \geqslant 1 \ \to\ a^3 + b^3 \neq c^3].$$

豆知識. 例 1.14 の Σ_1 論理式は真である．たとえば，$a = 3$, $b = 4$, $c = 5$, $d = 6$ がこれを満たすことはプラトンにより発見された．

問題 1.15. ゴールドバッハ予想，双子素数予想はいずれも Π_1 論理式で記述されていることを示せ．

定義 1.16. $\mathcal{L}_{\mathsf{arith}}$-理論 T が Σ_1**-完全** (Σ_1-*complete*) であるとは，$\mathbb{N}$ で真な Σ_1-閉論理式は必ず T で証明可能であることを意味する．つまり，任意の Σ_1-閉論理式 φ に対して，次が成立するときを言う．

$$\mathbb{N} \models \varphi \implies T \vdash \varphi.$$

[*2] 狭義の Σ_1 論理式のことを Σ_1 論理式と呼び，本稿の意味での Σ_1 論理式を $\Delta_0(\Sigma_1)$ 論理式と呼ぶ流儀もある．

定理 1.17. 離散順序環の非負部の公理 DOR^+ は Σ_1-完全である．

証明のアイデアを述べるために，離散順序環の非負部の構造を少し見てゆこう．まず，以下の略記を使用していたことを思い出そう．

$$\underline{n} = \underbrace{1+1+\cdots+1}_{n\text{ 個}}$$

さて，順序半環 $\mathcal{M} = (M, +, \cdot, \leqslant, 0, 1)$ が与えられたとき，$\underline{n}$ は M の要素である．つまり，

$$\mathbb{N}^{\mathcal{M}} = \{\underline{n} : n \in \mathbb{N}\} \subseteq M$$

が成立している．したがって，どんな順序半環を持ってきても，その中に $\mathbb{N}$ の複製のようなものがあるようである．

定理 1.18. $\mathcal{M}$ を非自明な順序半環とする．このとき，$(+, \cdot, \leqslant, 0, 1)$ を保つ $\mathbb{N}$ の $\mathcal{M}$ への埋め込みが存在する．さらに，もし $\mathcal{M}$ が離散順序環の非負部であれば．そのような埋め込みの像は $\mathcal{M}$ の始切片となる．

実際，$\mathbb{Z}[X]^+$ などでは，$\underline{n}$ は本物の自然数 n であり，$\mathbb{N}^{\mathbb{Z}[X]^+} = \mathbb{N}$ である．しかし，一般には，あくまで $\mathcal{M}$ はある種の順序半環でしかないので，1 や $1+1$ や $1+1+1$ などが $\mathcal{M}$ の中のどんな要素になっているかはよく分からない．そうすると，$n \mapsto \underline{n}$ が全ての構造を保つ埋め込みになっているというのは，そんなに自明なことではない．つまり，$\mathbb{N}^{\mathcal{M}}$ での演算が，本物の自然数の演算と同じとなっているかどうか，念のため確認する必要がある．非自明な順序半環の公理を OR^+ と書く．

補題 1.19. $\ell, k \in \mathbb{N}$ とする．

1. $\mathsf{OR}^+ \vdash \underline{\ell + k} = \underline{\ell} + \underline{k}$.
2. $\mathsf{OR}^+ \vdash \underline{\ell \cdot k} = \underline{\ell} \cdot \underline{k}$.
3. $\ell < k$ ならば，$\mathsf{OR}^+ \vdash \underline{\ell} < \underline{k}$.
4. $\mathsf{DOR}^+ \vdash (\forall x)\,[x \leqslant \underline{k} \;\to\; \bigvee_{m=0}^{k}(x = \underline{m})]$.

Proof. (1) 和に関する結合法則より自明である．(2) 帰納法を用いる．$\underline{\ell \cdot k} = \underline{\ell} \cdot \underline{k}$ は証明できたと仮定する．このとき，DOR^+ より次を導出できる．

$$\underline{\ell} \cdot (\underline{k+1}) = \underline{\ell} \cdot \underline{k} + \underline{\ell} = \underline{\ell \cdot k} + \underline{\ell} = \underline{\ell \cdot k + \ell} = \underline{\ell \cdot (k+1)}.$$

これらの等号は順に，分配律，帰納的仮定, (1) の性質より導かれる．

(3) まず，DOR^+ の非自明性より $\underline{0} < \underline{1}$ であり，順序半環の性質である和の順序保存性と推移律を利用して，任意の正整数 n について，$\underline{n} > \underline{0}$ であることを示せる．それでは，$\ell < k$ なる $k, \ell \in \mathbb{N}$ が与えられているとする．このとき，$k = \ell + n$ なる正整数 n が存在する．(1) を用いて，DOR^+

から $\underline{k} = \underline{\ell} + \underline{n}$ が導出される．すると，$\underline{n} > \underline{0}$ であることと和の順序保存性から，$\underline{k} = \underline{n} + \underline{\ell} > \underline{\ell}$ を得る．

(4) DOR^+ から $y < x \to y + 1 \leqslant x$ が導けることを確認する．これについては，$y < x$ なので，減法公理より $y = x + z$ なる z が存在する．このとき $z > 0$ である．なぜなら，$z \leqslant 0$ であると仮定すると，和の順序保存性より $x = y + z \leqslant y + 0 = y$ を得るが，これは $y < x$ に矛盾する．したがって，$z > 0$ なので，離散性より $z \geqslant 1$ である．再び和の順序保存性を用いて $x = y + z \geqslant y + 1$ を得る．

さて，帰納法より，$x \leqslant \underline{k} \to \bigvee_{m=0}^{k}(x = \underline{m})$ が示されていると仮定する．上の性質より，$x \leqslant \underline{k}$ または $x \geqslant \underline{k+1}$ が示される．したがって，もし $x \leqslant \underline{k+1}$ ならば，$x \leqslant \underline{k}$ または $x = \underline{k+1}$ である．帰納的仮定より，$x \leqslant \underline{k+1}$ ならば，$\bigvee_{m=0}^{k+1}(x = \underline{m})$ を得る． □

それでは，DOR^+ の Σ_1-完全性の証明に入ろう．

Proof (定理 1.17)．Σ_1-閉論理式 φ の構成に関する帰納法による．最初に，φ が論理記号を含まない場合を考える．まず，$a, b, c, d \in \mathbb{N}$ について，$a \leqslant b$ かつ $c \nleqslant d$ ならば $\mathsf{DOR}^+ \vdash \underline{a} \leqslant \underline{b}$ かつ $\mathsf{DOR}^+ \vdash \underline{c} \nleqslant \underline{d}$ である．これについては，補題 1.19 (3) から従う．項は和 $+$ と積 $\cdot$ から作られるので，補題 1.19 (1) と (2) を用いれば，項 s, t, u, v について，$\mathbb{N} \models s \leqslant t$ かつ $\mathbb{N} \models u \nleqslant v$ ならば $\mathsf{DOR}^+ \vdash s \leqslant t$ かつ $\mathsf{DOR}^+ \vdash u \nleqslant v$ であることが分かる．等号については，$s = t$ であることと $s \leqslant t$ かつ $t \leqslant s$ が同値であることを利用する．続いて，φ が $\psi \wedge \eta$ または $\psi \vee \eta$ の場合は，帰納法の仮定に還元できる．

続いて，有界量化の場合を考える．$\mathbb{N} \models (\forall x \leqslant t)\ \psi(x)$ を仮定する．いま，ある $n \in \mathbb{N}$ について $\mathbb{N} \models t = \underline{n}$ であるから，帰納的仮定より $\mathsf{DOR}^+ \vdash t = \underline{n}$ である．また，$\mathbb{N} \models \bigwedge_{k=0}^{n} \psi(\underline{k})$ であるが，同様に帰納的仮定より，$\mathsf{DOR}^+ \vdash \bigwedge_{k=0}^{n} \psi(\underline{k})$ である．補題 1.19 (4) より，$\mathsf{DOR}^+ \vdash (\forall x)\ [x \leqslant \underline{n} \to \bigvee_{k=0}^{n}(x = \underline{k})]$ が従う．これらを合わせて，$\mathsf{DOR}^+ \vdash (\forall x \leqslant t)\ \psi(x)$ が導かれる．有界存在量化の場合も同様にして示される．

最後に，$\mathbb{N} \models \exists x \psi(x)$ を仮定する．このとき，ある $n \in \mathbb{N}$ について $\mathbb{N} \models \psi(\underline{n})$ となる．帰納法の仮定より，$\mathsf{DOR}^+ \vdash \psi(\underline{n})$ であり，したがって，$\mathsf{DOR}^+ \vdash \exists x \psi(x)$ となる．よって，定理は示された． □

豆知識． $\mathcal{N}$ が $\mathcal{M}$ の始切片であるような部分 $\mathcal{L}_{\mathsf{arith}}$-構造であるとき，$\mathcal{M}$ を $\mathcal{N}$ の**終拡大** (*end extension*) であると言う．上の定理の証明を修正することで，$\mathcal{M}$ が $\mathcal{N}$ の終拡大ならば，$\mathcal{M}$ は $\mathcal{N}$ の Δ_0-**初等拡大** (Δ_0-*elementary extension*) である，ということを示すことができる．特に，$\mathcal{M}$ が離散順序環の非負部であるとき，$n \mapsto \underline{n}$ は $\mathbb{N}$ の $\mathcal{M}$ への Δ_0-**初等埋め込み** (Δ_0-*elementary embedding*) を与えている．

1.3 $\mathbb{Z}$-環と開帰納法

離散順序環の非負部の公理 DOR^+ は，まだ $\mathbb{N}$ とはかけ離れた構造をモデルに持つようである．もう少し $\mathbb{N}$ に近づくには，どのような公理を更に加えたらよいだろうか．まずは小学校の算数で習った割り算を思い出そう．小学校では，2 つの正整数 x, n が与えられたとき，$x \div n$ を問う問題

には，「q 余り r」のように答えていた．ここで，$x \div n =$ “q 余り r” とは，$x = qn + r$ かつ $r < n$ であることを思い出そう．この小学校の割り算は，以下のユークリッド除法の原理に基づくものである．

$$\text{除法の原理 } \mathsf{Div}(\underline{n}): \quad (\forall x)(\exists q, r)\ [x = q \cdot \underline{n} + r \ \&\ 0 \leqslant r < \underline{n}].$$

命題 1.11 で見たことは，DOR^+ のモデル $\mathbb{Z}[X]^+$ では 2 によるユークリッド除法が実行できないという点である．したがって，DOR^+ に除法の原理を加えれば，より強い体系を得ることができる．

定義 1.20. **$\mathbb{Z}$-環** ($\mathbb{Z}$-*ring*) とは，任意の正整数 n に対して除法の原理 $\mathsf{Div}(\underline{n})$ を満たす非自明な離散順序環のことを意味する．言い換えれば，$R/nR \simeq \mathbb{Z}/n\mathbb{Z}$ を満たす非自明な離散順序環である．

定義 1.21. 離散順序環の非負部の公理 DOR^+ に各正整数 n に対して除法の原理 $\mathsf{Div}(\underline{n})$ を加えたものを **$\mathbb{Z}$-環の非負部の公理**と呼び，ZR^+ と書く．標準的な名称ではないが，ここでは，$\mathbb{Z}$-環の非負部の公理を満たすモデルを **$\mathbb{N}$-半環** ($\mathbb{N}$-*semiring*) と呼ぶ．

例 1.22. $\mathbb{Z}[X]$ は $\mathbb{Z}$-環ではない．同様に，$\mathbb{Z}[X]^+$ は $\mathbb{N}$-半環ではない．

例 1.23. $\mathbb{Q}[X]$ を $\mathbb{Q}$ 上の 1 変数多項式環とし，$\mathbb{Q}[X]_Z$ を $\mathbb{Q}[X]$ の多項式のうち次数 0 の項が整数であるもの全体の集合とする．つまり，

$$\mathbb{Q}[X]_Z = \{a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 : n \in \mathbb{N} \ \wedge\ a_0 \in \mathbb{Z} \ \wedge\ a_1, \ldots, a_n \in \mathbb{Q}\}.$$

順序を $\mathbb{Z}[X]$ と同じように定義すると，$\mathbb{Q}[X]_Z$ は $\mathbb{Z}$-環となる．除法の原理については，多項式 $p = \sum_{i=0}^{n} a_i X^i \in \mathbb{Q}[X]_Z$ を自然数 n で割ることを考えよう．a_0 は整数なので，ある $0 \leqslant r < n$ に対して，$qn + r$ と書ける．よって，$p = (\sum_{i=1}^{n}(a_i/n)X^i + q) \cdot n + r$ となる．同様にして，$\mathbb{Q}[X]_Z$ の非負部 $\mathbb{Q}[X]_Z^+$ は $\mathbb{N}$-半環となる．

証明は省略するが，除法が全域には定義されないような $\mathbb{N}$-半環も存在する．そういうわけで，$\mathbb{N}$-半環もまだ $\mathbb{N}$ とはかなり異なる性質を持ち得る．さて，ここまでやってきたように公理を少しずつ加えていって $\mathbb{N}$ に地道に近づいていくのもよいが，それでは終わりが見えず，埒が明かないので，もう少し一般的な $\mathbb{N}$ 固有とおぼしき性質に着目しよう．以後，$\{+, \cdot, \leqslant, 0, 1\}$ を算術の言語と呼び，$\mathcal{L}_{\mathsf{arith}}$ と書く．

定義 1.24 (帰納法公理)**.** Γ を $\mathcal{L}_{\mathsf{arith}}$-論理式の集合とする．公理系 $\mathsf{I}\Gamma$ とは，離散順序環の非負部の公理 DOR^+ に，以下の**数学的帰納法**の公理を各 Γ-論理式 φ 毎に加えた公理図式である．

$$\text{数学的帰納法:} \quad [\varphi(0) \ \wedge\ (\forall x)\ \varphi(x) \to \varphi(x+1)] \ \to\ (\forall x)\ \varphi(x).$$

帰納法公理における φ は x 以外の自由変数を含んでもよい[*3]．Γ の例としては，量化記号を含まない $\mathcal{L}_{\mathsf{arith}}$-論理式全体の集合 Open，量化記号は有界存在量化 $\exists x \leqslant t$ のみを認める E_1, Σ_1 論理式全体の集合 Σ_1 などがあり，IOpen, IE_1 や $\mathsf{I}\Sigma_1$ などを考える．また，**ペアノ算術** (*Peano arithmetic*) とは，$\mathcal{L}_{\mathsf{arith}}$-論理式の集合 Arith に対する公理系 IArith のことを意味する．以後，PA によって，ペアノ算術を表す．

命題 1.25. IOpen から全域的な除法の原理を証明できる*:*

$$\mathsf{IOpen} \vdash (\forall x)(\forall y > 0)(\exists q, r)\ [x = q \cdot y + r \ \wedge\ r < y].$$

特に，IOpen の任意のモデルは $\mathbb{N}$-半環であるが，逆は成り立たない．たとえば，例 *1.23* の $\mathbb{N}$-半環 $\mathbb{Q}[X]_Z^+$ は IOpen のモデルではない．

Proof. x, y を任意に固定し，$\varphi(q)$ を $q \cdot y \leqslant x$ によって定義する．このとき，$\varphi \in$ Open である．まず，DOR^+ で明らかに $\varphi(0)$ かつ $\neg\varphi(x+1)$ が証明できる．したがって，Open-帰納法の対偶を用いることによって，IOpen で $\varphi(q)$ かつ $\neg\varphi(q+1)$ であるような q の存在が示される．つまり，DOR^+ における順序の比較可能性より，$qy \leqslant x$ かつ $(q+1)y > x$ である．$r = x - qy$ とおくと，$x = qy + r$ となる．$r < y$ については，$qy + r = x < (q+1)y = qy + y$ であることから分かる． □

IOpen のモデルの特徴付けとして，以下に述べる**シェファードソンの定理** (*Shepherdson's theorem*) は重要であるが，本講義のスコープを越えることと，後の節では用いないことから，証明は省略する．しかし，算術体系のモデルのイメージを鍛えるために有用であるから，シェファードソンの定理を応用した例に幾つか触れよう．

事実 1.26 (シェファードソンの定理)**.** IOpen のモデルとは，ある実閉体の整数部 Z の非負部 Z^+ に他ならない．

例 1.27. $\mathbb{R}$ 係数の**ピュイズー級数** (*Puiseux series*) たちが実閉体をなすことは知られている．したがって，シェファードソンの定理より，その整数部の非負部は IOpen のモデルであり，$\mathbb{N}$ と同型でないことも分かる．

例 1.28 (シェファードソンのモデル)**.** IOpen の可算モデルを得るためには，分数体 $\mathbb{Q}(X)$ の実閉包 $\mathrm{rcl}(\mathbb{Q}(X))$ を考えよう．これは，実代数的数を係数に持つ非負冪の有限ピュイズー級数たちのなす実閉体である．$\mathbb{R}_{\mathrm{alg}}$ を実代数的数全体を表すものとすると，$\mathrm{rcl}(\mathbb{Q}(X))$ の整数部として，以下を得る．

$$\begin{aligned} S :=& \mathrm{rcl}(\mathbb{Q}(X))_Z \\ =& \{a_n X^{\frac{n}{k}} + a_{n-1} X^{\frac{n-1}{k}} + \cdots + a_1 X^{\frac{1}{k}} + a_0 : n \in \mathbb{N},\ k \in \mathbb{N}\backslash\{0\},\ a_0 \in \mathbb{Z},\ a_i \in \mathbb{R}_{\mathrm{alg}}\}. \end{aligned}$$

[*3] x 以外の自由変数を許さない帰納法は，**パラメータなし帰納法** (*parameter-free induction*) と呼ばれ，対応する公理系は $\mathsf{I}\Gamma^-$ のようにマイナスを付けて表されることが多い．

S の非負部 S^+ は IOpen の可算モデルというだけではなく，計算可能モデルである．この S は**シェファードソンのモデル** (*Shepherdson's model*) と呼ばれる．

証明は省略するが，以下の事実が知られている．

命題 1.29. IOpen では，素数の無限性を証明できない．

$$\mathsf{IOpen} \nvdash (\forall x)(\exists p > x)(\forall a, b < p)\ p \neq a \cdot b.$$

実際，シェファードソンのモデル S^+ において，素数の無限性を表す上式は偽となる．しかし，上式は，S^+ の中で素数が有界であることを示すものであるが，各素数 $p \in \mathbb{N}$ は S^+ でも素数であるから，外から見れば，S^+ は素数を無限個持つことに注意する．

$$S^+ \models \neg(\forall x)(\exists p > x)\ \text{“}p \text{ は素数である”}.$$
$$(\forall x \in \mathbb{N})\ S^+ \models (\exists p > \underline{x})\ \text{“}p \text{ は素数である”}.$$

命題 1.30. IOpen では，フェルマーの最終定理を証明できない．実際，$n = 3$ の場合すら証明できない．

$$\mathsf{IOpen} \nvdash (\forall x, y, z > 0)\ [x^3 + y^3 \neq z^3].$$

Proof. シェファードソンのモデルの非負部 S^+ でフェルマーの最終定理の $n = 3$ の場合を証明できないことを示す．具体的に $x^3 + y^3 = z^3$ を満たす $x, y, z \in S^+$ を取ってこよう．これについては，$X, \sqrt[3]{2}X \in S^+$ であり，$X^3 + X^3 = (\sqrt[3]{2}X)^3$ であることから従う． □

IOpen のモデルの代数的性質に関して，もう一つ例を挙げておく．

例 1.31. シェファードソンのモデル S は**整閉** (*integrally closed*) ではない．

Proof. たとえば，$X, \sqrt{2}X \in S$ であるから，$\sqrt{2} = \sqrt{2}X/X$ は S で有理数であるが，これは S の分数体における S 係数モニック多項式 $x^2 - 2 = 0$ の根であり，つまり S 上整である．しかし，明らかに $\sqrt{2} \notin S$ であるから，S が整閉でないことが分かる． □

例 1.32 とは対照的に，有界存在量化帰納法 IE_1 のモデルは必ず整閉整域の非負部になることが知られている．したがって，S^+ は IE_1 のモデルではない．しかし，IE_1 くらいまで強い体系になると，これまでのように容易くモデルを構成する，ということができなくなる．実は，IE_1 には**テネンバウムの定理** (*Tennenbaum's theorem*) というものが成り立ってしまい，IE_1 の計算可能な超準モデルは存在しないのである．

以上のようにして，自然数をモデルとするような形式体系の階層が作られていく．その概要を表 1 にまとめた．

豆知識． ここで挙げた体系以外でも，$\mathbb{Z}$-環や IOpen の周辺のようなテネンバウムの定理の呪縛を受けない弱い体系では，たとえばベズー整域や GCD 整域といったような代数的な性質と絡み合ったモデル理論的研究が行われている．また，$\mathsf{I}\Delta_0$ 周辺は，**限定算術** (*bounded arithmetic*) と呼ばれる，算術体系と**計算量理論** (*computational complexity theory*) を結び付ける理論と関わりがある．$\mathsf{I}\Sigma_1$ と PA の中間の帰納法の階層構

形式体系	可算モデル	証明できない性質の例
離散順序環の非負部 DOR^+	$\mathbb{N}$, $\mathbb{Z}[X]^+$, $\mathbb{Q}[X]^+_Z$, S^+ など	任意の数が偶または奇
$\mathbb{Z}$-環の非負部 ZR^+	$\mathbb{N}$, $\mathbb{Q}[X]^+_Z$, S^+ など	全域的な除法の原理
開帰納法公理 IOpen	$\mathbb{N}$, S^+ など	整閉性，素数の無限性
Δ_0-帰納法公理 $\mathsf{I}\Delta_0$	$\mathbb{N}$ など	指数関数の全域性
Σ_1-帰納法公理 $\mathsf{I}\Sigma_1$	$\mathbb{N}$ など	アッカーマン関数の全域性
ペアノ算術 PA	$\mathbb{N}$ など	パリス・ハーリントンの定理

表 1　$\mathbb{N}$ をモデルとする形式体系の階層

造は，証明論や計算可能性理論などの分野で深く研究されており，前者ではたとえば**可証全域関数** (*provably total function*) であるとか，後者では算術の超準モデル上の計算論と**認容順序数** (*admissible ordinal*) 上の計算論の類似であるとかいったものである．PA より強い体系は二階算術などといったものと絡むことが多いが，その分析は証明論における不朽のテーマであり，数多の深遠な研究がなされている．

さて，これまでに，不足な公理を次々に追加していくことにより IOpen のような公理系を作り上げてきたが，未だ証明不可能な自然数の性質は無数に残る．$\mathsf{I}\Sigma_1$ くらいになると幾分か状況はよくなって，自然数について成り立つ閉論理式で，通常の数学的活動で取り扱うようなもののかなりの部分は証明できるといっても過言ではないだろう．しかし，たとえ $\mathsf{I}\Sigma_1$ や PA のような公理系といえど，まだ自然数を完全には捉えきれていないであろうことは容易に想像が付く．たとえば，有限ラムゼーの定理を技巧的に複雑化した主張である**パリス・ハーリントンの定理** (*Paris-Harrington theorem*) というものは，$\mathbb{N}$ で成立することが十分強い体系の下で証明できるが，PA では証明できない．実際，幾ら DOR^+ に公理を加えていったとしても，それが無矛盾であり，何を公理に加えたかを有限的なアルゴリズムによって判定できる限り，自然数に関する真な式を全て証明するということは決してできない．これについては，第 3 節で詳述する．

1.4　超準モデルの順序型

ここまでで，$\mathbb{N}$ の持つ様々な性質を公理化し，その公理を満たすが，$\mathbb{N}$ と非同型となるようなモデルを取り扱ってきた．それでは，そのような $\mathbb{N}$ と非同型なモデルについて，何か共有する性質はあるだろうか．離散順序環の非負部のことを思い出すと，$\mathbb{Z}[X]^+$ では，$\mathbb{N}$ の形の島の無限の彼方に，$\mathbb{Z}$ の形の島が $\mathbb{N}$ の形に並んだ列島 $\mathbb{Z}\cdot\mathbb{N}$ があり，その更に無限の彼方には $\mathbb{Z}\cdot\mathbb{Z}\cdot\mathbb{N}$ がある，さらに無限の彼方には $\mathbb{Z}\cdot\mathbb{Z}\cdot\mathbb{Z}\cdot\mathbb{N}$ があって，... といったようなことが見て取れる．それでは，他のモデルは，一体どのような形状をしているだろうか．

定理 1.32. 非自明な離散順序環の非負部の順序型は，最大元を持たない全順序 J が存在して，$\mathbb{N}+\mathbb{Z}\cdot J$ の形となる．$\mathbb{N}$-半環の順序型は，最大・最小元を持たない稠密全順序 Q が存在して，

$\mathbb{N}+\mathbb{Z}\cdot Q$ の形となる．

特に，$\mathbb{N}$ と非同型な可算 $\mathbb{N}$-半環の順序型は $\mathbb{N}+\mathbb{Z}\cdot\mathbb{Q}$ である．

Proof. $\mathcal{M}$ を非自明な離散順序環の非負部とする．$\mathcal{M}$ が $\mathbb{N}$ と同型ならば，$\mathbb{N}+\mathbb{Z}\cdot\varnothing$ である．$\mathcal{M}$ が $\mathbb{N}$ と非同型であると仮定する．定理 1.18 より，$\mathbb{N}$ の $\mathcal{M}$ への埋め込み像 $\mathbb{N}^{\mathcal{M}}=\{\underline{n}:n\in\mathbb{N}\}$ は $\mathcal{M}$ の始切片だった．簡単のために，$\mathbb{N}^{\mathcal{M}}$ を $\mathbb{N}$ と略記する．以前と同様に，$\mathcal{M}$ の元を標準整数差によって同値分類する．つまり，各 $x\in\mathcal{M}$ に対して，島 $[x]=\{y\in\mathcal{M}:(\exists n\in\mathbb{N})\ x+\underline{n}=y\ \vee\ y+\underline{n}=x\}$ を考える．また，$[x]<[y]$ によって，任意の $x'\in[x]$ と $y'\in[y]$ について，$x'<y'$ となることを意味する．超準元 $a\in\mathcal{M}\backslash\mathbb{N}$ を取ると，そこから任意の標準自然数 $n\in\mathbb{N}$ に対して，$a+n$ と $a-n$ が存在するので，$[a]$ の順序型は $\mathbb{Z}$ と等しい．また，$a\in\mathcal{M}\backslash\mathbb{N}$ ならば $[a]<[2a]$ なので，最上位の島が存在しないことは容易に分かる．したがって，最大元を持たないある全順序 J に対して，$\mathcal{M}$ の順序型は $\mathbb{N}+\mathbb{Z}\cdot J$ となっている．

続いて，$\mathcal{M}$ が $\mathbb{N}$-半環であると仮定する．標準自然数たちが住む $\mathbb{N}$ の島が最下位に位置するが，その次の島は存在しない．なぜなら，$\mathbb{N}$-半環であれば，任意の超準元 $a\in\mathcal{M}\backslash\mathbb{N}$ に対し，$a=2b$ または $a=2b+1$ なる b が存在する．このとき，$\mathbb{N}<[b]<[a]$ は容易に分かる．

稠密性を示すために，$[a]<[b]$ なる $a,b\in\mathcal{M}\backslash\mathbb{N}$ を取る．$\mathcal{M}$ は $\mathbb{N}$-半環であるから，$a+b=2c$ または $a+b=2c+1$ となるような $c\in\mathcal{M}$ が存在する．このとき，$[a]<[c]<[b]$ であることが確認できる．よって，島たちは稠密に存在する．

以上より，どんな $\mathbb{N}$-半環も，ある最大及び最小元を持たない稠密全順序 Q に対して，$\mathbb{N}+\mathbb{Z}\cdot Q$ の順序型を持つ．また，$\mathcal{M}$ が可算の場合，$Q\neq\varnothing$ ならば，そのような全順序の性質の $\aleph_0$-範疇性から，Q は有理数の順序 $\mathbb{Q}$ と同型になる．よって，$\mathbb{N}$ と非同型などんな可算 $\mathbb{N}$-半環も，その順序型は $\mathbb{N}+\mathbb{Z}\cdot\mathbb{Q}$ であることが分かった． □

注意．2 つの構造が同型ならば，初等同値である．したがって，$\mathbb{N}$ では偽となる閉論理式（たとえば，素数の有限性など）を 1 つでも満たす $\mathbb{N}$-半環 R は，$\mathbb{N}$ と初等非同値になるので，非同型になる．したがって，定理 1.33 より，そのような $\mathbb{N}$-半環 R の順序型は，最大・最小元を持たない稠密全順序 Q に対して，必ず $\mathbb{N}+\mathbb{Z}\cdot Q$ という形になっている．具体的には，例 1.23 の $\mathbb{N}$-半環 $\mathbb{Q}[X]_Z^+$ や例 1.29 の IOpen のモデル S^+ は $\mathbb{N}$ と初等非同値で可算であるから，その順序型は $\mathbb{N}+\mathbb{Z}\cdot\mathbb{Q}$ である．

しかし，最大・最小元を持たない稠密全順序ならどんなものでも良いかというと，そういうわけではない．

命題 1.33. IOpen のモデルで，順序型が $\mathbb{N}+\mathbb{Z}\cdot\mathbb{R}$ であるようなものは存在しない．

この主張を証明するためには少し準備が必要である．$\mathcal{M}$ を離散順序環の非負部とする．このとき，$I\subseteq\mathcal{M}$ が $\mathcal{M}$ の**カット** (*cut*) であるとは，$a\in I$ かつ $b<a$ ならば $b\in I$ であり，$a\in I$ ならば $a+1\in I$ であるもののことである．

補題 1.34 (溢れ出し)**.** $\mathcal{M} \models \mathsf{I}\Gamma$ かつ $I \neq \mathcal{M}$ を $\mathcal{M}$ のカットとする．$\varphi(x)$ を Γ-論理式とする．もし，任意の $a \in I$ で，$M \models \varphi(a)$ が成立しているならば，ある $c \in \mathcal{M} \backslash I$ で，$M \models \varphi(c)$ が成立する．

Proof. 結論が偽であると仮定する．このとき，$\varphi(x) \Leftrightarrow x \in I$ であり，I はカットなので，$0 \in I$ かつ $\forall x\ (x \in I \Rightarrow x+1 \in I)$ である．つまり，

$$\varphi(0)\ \wedge\ \forall x\ (\varphi(x)\ \rightarrow\ \varphi(x+1))$$

ここで $\varphi(x)$ は Γ-論理式なので，$M \models \mathsf{I}\Gamma$ を用いて $\forall x \varphi(x)$ を得る．これは $I = M$ を意味し，仮定に矛盾する． □

Proof (**定理** 1.34)*.* M を IOpen のモデルで，順序型が $\mathbb{N}+\mathbb{Z}\cdot\mathbb{R}$ だったとする．このとき，適当に超準元 $a \in M\backslash\mathbb{N}$ を取る．各 $b \in M$ について，$a \cdot b$ は，ある $x_b \in \mathbb{R}$ について，x_b 番目の $\mathbb{Z}$-島におり，$b < c \in M$ ならば $x_b < x_c$ である．数列 $(x_n)_{n\in\mathbb{N}}$ を考えると，任意の $n \in N$ と $b \in M\backslash\mathbb{N}$ について $x_n < x_b$ が成立するので，$(x_n)_{n\in\mathbb{N}}$ は有界な実数列である．$\mathbb{R}$ の完備性より，上限 $x = \sup_n x_n$ が存在する．x 番目の $\mathbb{Z}$-島の元 $b \in M$ を取る．$\varphi(n) \equiv a\underline{n} < b$ の溢れ出しによって，ある超準元 $c \in M\backslash\mathbb{N}$ が存在して，任意の $n \in \mathbb{N}$ について $a \cdot n < a \cdot (c-1) < a \cdot c < b$ となるが，これは b の性質に矛盾する． □

2 原始再帰関数

ここまでに自然数の半環構造に注目してきた．これはすなわち，自然数の足し算および掛け算という演算だけを取り扱うということである．しかし，このような基本的な演算から，**原始再帰法** (*primitive recursion*)[*4]と呼ばれる操作によって，様々な自然数上の関数を構成できることを本節では見ていこう．

このアイデアを説明するために，人類が「新しい演算」を創造していく過程をシミュレートしよう[*5]．まず，自然数 x が与えられたとき，「x の次」である数が何であるかを知っているとしよう．すると，「x の次の次」や「x の次の次の次」などを考えることができる．しかし，いくつも「の次」という文字を書くのは億劫なので，x の y 個次の数を $x+y$ と書くことにしよう．こうして，人類は，「足す」という演算を生み出した．

$$x + y = x \text{ の } \underbrace{\text{次の次の次} \ldots \text{の次の次}}_{y \text{ 個}}$$

[*4] Primitive recursion は伝統的には，原始再帰でなく**原始帰納**と訳されることがある．しかし，本講義ではそこまで辿り着かないが，再帰理論やその周辺の理論では， inductive と recursive が全く別概念として登場し，たとえば，「recursive ではないが inductive であるような集合が存在する」「Π^1_1-transfinite induction は Π^1_1-transfinite recursion を導かない」というような定理が成立する．したがって，inductive と recursive には異なる訳語を割り当てる必要があるが，ここでは inductive を**帰納**と訳し，recursive を**再帰**と訳す流儀を採用する．

[*5] 本稿の記述は現実の数学史に沿っているとは限らない．

このように「足す」という演算を知った人類は，$x+x+x$ や $x+x+x+x+x$ のように x を何度も足す，という演算が有用であることに次第に気づき始める．これを簡潔に表すために，人類は「掛ける」という演算を次のように定義した．

$$x \cdot y = \underbrace{x+x+\cdots+x+x}_{y\text{ 個}}$$

そして，「掛ける」という演算を知った人類は，$x \cdot x \cdot x$ のように x を何度も掛ける，という演算の有用性に気づく．そして「累乗」という演算を次のように定義した．

$$x^y = \underbrace{x \cdot x \cdot \cdots \cdot x \cdot x}_{y\text{ 個}}$$

すると，自然に x^{x^x} や $x^{x^{x^x}}$ のようなものを考える人も現れる．上方向にたくさん添字が付くのは見づらいので，x^y のことを今後は $x \uparrow y$ と書くこととしよう．たとえば，x^{x^x} は $x \uparrow (x \uparrow x)$ であり，$x^{x^{x^x}}$ は $x \uparrow (x \uparrow (x \uparrow x))$ である．また，以下，括弧は省略し，これらの演算は右から順に適用するものとする．さて，累乗でも飽き足らない一部の人類は，「テトレーション」という演算を編み出した．

$$x \uparrow\uparrow y = \underbrace{x \uparrow x \uparrow \ldots \uparrow x \uparrow x}_{y\text{ 個}}$$

飽くなき人類は，更なる演算「ペンテーション」を定義する．

$$x \uparrow\uparrow\uparrow y = \underbrace{x \uparrow\uparrow x \uparrow\uparrow \ldots \uparrow\uparrow x \uparrow\uparrow x}_{y\text{ 個}}$$

より一般に，クヌースの矢印記法というものは以下によって定義される．

$$x \uparrow^{n+1} y = \underbrace{x \uparrow^n x \uparrow^n \ldots \uparrow^n x \uparrow^n x}_{y\text{ 個}}$$

更なる高みを目指す人類の一部は，矢印記法を越えて続く演算を生み出している[*6]が，キリがないので，本講義で触れるのはここまでとしよう．

このような再帰的な関数構成を数学的に抽象化したものが，原始再帰法と呼ばれる概念である．

2.1 原始再帰法

さて，ここまで，何かの演算 $x \diamond y$ を元に，人類が新たな演算 $x \star y$ を創造する過程を見てきた．これらの過程が共有するものとは何であろうか．それは以下の性質である．

$$x \star y = \underbrace{x \diamond x \diamond \cdots \diamond x \diamond x}_{y\text{ 個}}$$

[*6] たとえば，コンウェイのチェーン記法と呼ばれるものがある．

$$x \to y \to z = x \uparrow^z y.$$

チェーンはより長く伸びてゆき，更なる演算が定義される．しかし，ここまでゆくと，既に原始再帰の枠組みを越えてしまう．たとえば，$x \mapsto x \uparrow^x x$ の増大速度は原始再帰でない関数として有名な**アッカーマン関数** (*Ackermann function*) のそれとおおよそ同程度である．

実際に，この値 $x \star y$ を計算する場合には，$x \star 2 = x \diamond x$ を求め，$x \star 3 = x \diamond x \diamond x = x \diamond (x \star 2)$ を求め，$x \star 4 = x \diamond x \diamond x \diamond x = x \diamond (x \star 3)$ を求め，... という手続きを行うこととなるだろう．たとえば，掛け算以降の演算の定義を少し書き直せば，次のようにして定義されていることがわかる．

$$\begin{cases} x \star 1 = x, \\ x \star (y+1) = x \diamond (x \star y). \end{cases}$$

上の定義では曖昧であるが，$x \star 0$ の場合も定義しておくのが自然である．たとえば，$x \cdot 0 = 0$ であるし，$x \uparrow 0 = x^0 = 1$ である．

問題 2.1. 以下のようにして，$x \uparrow^{n+1} y$ を定義する．

$$\begin{cases} x \uparrow^{n+1} 0 = 1, \\ x \uparrow^{n+1} (y+1) = x \uparrow^{n} (x \uparrow^{n+1} y). \end{cases}$$

このとき，$x \uparrow^{n+1} 1 = x$ であることを示せ．

さて，ここまでは演算の形式で書いてきたが，これらを関数として見直すこととする．つまり，今までのことを，関数 $h(x,y) = x \diamond y$ から新たな関数 $f(x,y) = x \star y$ を創造する過程を考えてきたものとしよう．また，$g(x) = x \star 0$ は与えられているものとする．これまでの内容を言い直せば，g と h からの新たな関数 f は以下のように生み出された．

$$\begin{cases} f(x,0) = g(x), \\ f(x,y+1) = h(x, f(x,y)). \end{cases}$$

それでは，原始再帰法の厳密な定義に入ろう．上では，f は 2 変数関数であったが，より多変数であってよい．

定義 2.2 (原始再帰法)**.** 関数 $g : \mathbb{N}^n \to \mathbb{N}$ と $h : \mathbb{N}^{n+2} \to \mathbb{N}$ が与えられているとする．さらに，$f : \mathbb{N}^{n+1} \to \mathbb{N}$ が，次のように定義されるとしよう: 任意の $\bar{x} \in \mathbb{N}^n$ と $y \in \mathbb{N}$ について，

$$\begin{cases} f(\bar{x},0) = g(\bar{x}), \\ f(\bar{x},y+1) = h(\bar{x}, y, f(\bar{x},y)). \end{cases}$$

このとき，f は g と h から**原始再帰法** (*primitive recursion*) によって定義されるという．

それでは，原始再帰関数の概念を導入しよう．

定義 2.3 (原始再帰関数)**.** 以下のように，**原始再帰関数** (*primitive recursive function*) を帰納的に定義する．

1. 以下によって定義される後続関数 $\mathsf{succ} : \mathbb{N} \to \mathbb{N}$, 零関数 $\mathsf{zero}^n : \mathbb{N}^n \to \mathbb{N}$ および射影関数

$\mathsf{proj}_i^n : \mathbb{N}^n \to \mathbb{N}$ は原始再帰関数である．

$$\mathsf{succ}(x) = x + 1, \quad \mathsf{zero}^n(x_1, \ldots, x_n) = 0, \quad \mathsf{proj}_i^n(x_1, \ldots, x_n) = x_i.$$

2. 原始再帰関数たちの合成は原始再帰関数である．つまり，$h : \mathbb{N}^m \to \mathbb{N}$ と $g_1, \ldots, g_m : \mathbb{N}^n \to \mathbb{N}$ が原始再帰的ならば，以下のように定義される関数 $f : \mathbb{N}^n \to \mathbb{N}$ もまた原始再帰的である．
$$f(\bar{x}) = h(g_1(\bar{x}), \ldots, g_m(\bar{x})).$$

3. 原始再帰関数 g, h から原始再帰法によって定義される関数は原始再帰的である．

例 2.4. 和 $(x, y) \mapsto x + y$, 積 $(x, y) \mapsto x \cdot y$, 冪乗 $(x, y) \mapsto x^y$, 第 n 矢印演算 $(x, y) \mapsto x \uparrow^n y$ はいずれも原始再帰的関数である．

例 2.5. ここでは自然数上の関数を考えるので，引き算は一般には定義されないが，部分的引き算 $x \dot{-} y = \max\{0, x - y\}$ を考えることはできる．これが原始再帰的であることを示そう．まず，「入力が正の数であれば，値を 1 減らす」という演算 pred が原始再帰的であることを確認する．これは，$g = \mathsf{zero}^0$ と $h = \mathsf{proj}_1^2$ から原始再帰法によって定義される関数を考えればよい．

$$\begin{cases} \mathsf{pred}(0) = \mathsf{zero}^0 = 0, \\ \mathsf{pred}(y + 1) = \mathsf{proj}_1^2(y, \mathsf{pred}(y)) = y. \end{cases}$$

このとき，部分的引き算 $f(x, y) = x \dot{-} y = \max\{0, x - y\}$ は，$g = \mathsf{proj}_1^1$ と $h = \mathsf{pred} \circ \mathsf{proj}_3^3$ から原始再帰法によって定義される．

$$\begin{cases} x \dot{-} 0 = \mathsf{proj}_1^1(x) = x, \\ x \dot{-} (y + 1) = \mathsf{pred}(\mathsf{proj}_3^3(x, y, x \dot{-} y) = \mathsf{pred}(x \dot{-} y). \end{cases}$$

例 2.6. 典型的な原始再帰関数として，総和と総乗がある．

$$f_0(\bar{x}, y) = \sum_{i=0}^{y-1} p(\bar{x}, i), \qquad f_1(\bar{x}, y) = \prod_{i=0}^{y-1} p(\bar{x}, i).$$

ここで，$p : \mathbb{N}^{n+1} \to \mathbb{N}$ は与えられた原始再帰関数とする．このとき，f_0 は $g_0 = \mathsf{zero}^n$ と $h_0(\bar{x}, y, z) = z + p(\bar{x}, y)$ から原始再帰法によって定義される．

$$\begin{cases} f_0(\bar{x}, 0) = \mathsf{zero}^n(\bar{x}) = 0, \\ f_0(\bar{x}, y + 1) = f_0(\bar{x}, y) + p(\bar{x}, y). \end{cases}$$

同様に，f_1 は $g_1 = \mathsf{succ} \circ \mathsf{zero}^n$ と $h_1(\bar{x}, y, z) = z \cdot p(\bar{x}, y)$ から原始再帰法によって定義される．

$$\begin{cases} f_1(\bar{x}, 0) = \mathsf{succ}(\mathsf{zero}^n(\bar{x})) = 1, \\ f_1(\bar{x}, y + 1) = f_0(\bar{x}, y) \cdot p(\bar{x}, y). \end{cases}$$

さて，新しい原始再帰関数を作るために，場合分けを自由に使用してよいことを示しておくと便利である．

命題 2.7 (原始再帰的場合分け)．$g, h, p : \mathbb{N}^n \to \mathbb{N}$ を原始再帰関数とする．このとき，次によって定義される $f : \mathbb{N}^n \to \mathbb{N}$ は原始再帰的である．

$$f(\bar{x}) = \begin{cases} g(\bar{x}) & \text{if } p(\bar{x}) = 0, \\ h(\bar{x}) & \text{if } p(\bar{x}) > 0. \end{cases}$$

Proof. まず，$\mathsf{sgn} : \mathbb{N} \to \mathbb{N}$ を zero^0 と $\mathsf{succ} \circ \mathsf{zero}^2$ から原始再帰法よって定義される関数とする．

$$\begin{cases} \mathsf{sgn}(0) = \mathsf{zero}^0 = 0, \\ \mathsf{sgn}(y+1) = \mathsf{succ}(\mathsf{zero}^2(y, \mathsf{sgn}(y))) = 1. \end{cases}$$

つまり，sgn は入力値が 0 であれば 0 を出力し，入力値が 0 以外であれば 1 を出力する．このとき，f は次のような合成によって定義する．

$$f(\bar{x}) = g(\bar{x}) \cdot (1 \dot{-} \mathsf{sgn}(p(\bar{x}))) + h(\bar{x}) \cdot \mathsf{sgn}(p(\bar{x})).$$

これが求める関数であることを確認しよう．もし $p(\bar{x}) = 0$ であれば，$\mathsf{sgn}(p(\bar{x})) = 0$ かつ $1 \dot{-} \mathsf{sgn}(p(\bar{x})) = 1$ であるから，

$$f(\bar{x}) = g(\bar{x}) \cdot 1 + h(\bar{x}) \cdot 0 = g(\bar{x})$$

である．もし $p(\bar{x}) > 0$ であれば，$\mathsf{sgn}(p(\bar{x})) = 1$ かつ $1 \dot{-} \mathsf{sgn}(p(\bar{x})) = 0$ であるから，

$$f(\bar{x}) = g(\bar{x}) \cdot 0 + h(\bar{x}) \cdot 1 = h(\bar{x})$$

である．よって f が求める関数であることが分かった．また，f は原始再帰関数 $+$, $\cdot$, $\dot{-}$, sgn, g, h, p から合成によって作られているので，原始再帰的である． □

2.2 算術的定義可能性

集合 $P \subseteq \mathbb{N}^n$ が**原始再帰的**であるとは，その特性関数

$$\chi_P(\bar{x}) = \begin{cases} 1 & \text{if } \bar{x} \in P, \\ 0 & \text{if } \bar{x} \notin P \end{cases}$$

が原始再帰的であることを意味する．しばしば，集合のことを**述語** (*predicate*) と同一視し，$\bar{x} \in P$ のとき $P(\bar{x})$ と書き，$\bar{x} \notin P$ のとき $\neg P(\bar{x})$ と書く．

例 2.8. 述語 $x < y$ は原始再帰的である．つまり，次の関数は原始再帰的である．

$$\chi_<(x,y) = \begin{cases} 1 & \text{if } x < y, \\ 0 & \text{otherwise.} \end{cases}$$

これはなぜなら，$\chi_<$ は次の原始再帰的場合分け (命題 2.7) によって定義できるからである．

$$\chi_<(x,y) = \begin{cases} 1 & \text{if } y \dot{-} x > 0, \\ 0 & \text{if } y \dot{-} x = 0. \end{cases}$$

一般に，どのような述語が原始再帰的かを確かめるために，$\mathbb{N}$ 上の算術的複雑性の概念を思い出そう．再び言語 $\mathcal{L}_{\mathsf{arith}} = \{+, \cdot, \leqslant, 0, 1\}$ を考える．非有界量化を用いずに構成される論理式を Δ_0 論理式と呼んだ．また，ある Δ_0 論理式 θ に対して $\exists x\theta$ の形で書ける論理式を Σ_1 論理式と呼んだ．

定義 2.9. 論理式 φ が $\mathbb{N}$ 上 Γ とは，ある Γ 論理式 ψ が存在して，$\mathbb{N} \models \varphi \leftrightarrow \psi$ が成立することを意味する．また，$\mathbb{N}$ 上 Σ_1 かつ Π_1 であるような論理式を，$\mathbb{N}$ 上 Δ_1 であると言う．集合 $P \subseteq \mathbb{N}^n$ が Γ であるとは，ある Γ 論理式 φ が存在して，$P = \{\bar{x} \in \mathbb{N}^n : \mathbb{N} \models \varphi(\bar{x})\}$ となることである．

補題 2.10. 論理式 φ, ψ が $\mathbb{N}$ 上 Σ_1 ならば，以下のいずれも $\mathbb{N}$ 上 Σ_1 である．

$$\varphi \wedge \psi, \quad \varphi \vee \psi, \quad (\exists a \leqslant u)\varphi, \quad (\forall a \leqslant u)\varphi.$$

Proof. たとえば，$(\forall a < u)(\exists b)\theta$ は，$(\exists v)(\forall a < u)(\exists b < v)\theta$ と同値である． □

定理 2.11. 任意の Δ_0 集合 $P \subseteq \mathbb{N}^n$ は原始再帰的である．

Proof. まず，もし P, Q が原始再帰的述語であれば，$\neg P, P \wedge Q, P \vee Q, P \to Q$ も原始再帰的であることを確認する．これについては，$\chi_{\neg P} = 1 \dot{-} \chi_P$ かつ $\chi_{P \wedge Q} = \chi_P \cdot \chi_Q$ である．残りは，$P \vee Q$ と $\neg(\neg P \wedge \neg Q)$ が同値であることと $P \to Q$ と $\neg P \vee Q$ が同値であることを用いればよい．続いて，有界量化が原始再帰性を保つことを示す．つまり，もし R が原始再帰的述語であれば，以下の述語も原始再帰的である．

$$P(\bar{x}, y) \iff (\exists z \leqslant y)\, R(\bar{x}, z),$$
$$Q(\bar{x}, y) \iff (\forall z \leqslant y)\, R(\bar{x}, z).$$

これについては，$\chi_Q(\bar{x}, y) = \prod_{z<y} \chi_R(\bar{x}, z)$ であるから，例 2.6 より，原始再帰性が分かる．P については，$\neg(\forall z \leqslant y)\neg R$ と同値であることを用いればよい． □

2.3 原始再帰法の算術化

原始再帰関数の算術的複雑性を確認しよう．この節では，次を証明することを目標とする．

定理 2.12. 原始再帰関数のグラフは $\mathbb{N}$ で Σ_1-定義可能である．

これから行うことは，算術の言語での原始再帰関数のコーディングであり，そのためには数列のコーディングが必要になる．自然数の有限列を一つの自然数でエンコードすることを考えよう．たとえば，$\langle 3, 10, 6, 4\rangle$ という数列が与えられているとする．エンコードの方法は幾らでも思いつくであろう．たとえば，これらの数をまず二進表記に直すと $\langle 11, 1010, 110, 100\rangle$ となる．カンマを 2 に置き換えた数列 112101021102100 を三進表記された一つの自然数だと考え，これを元の数列のコードであると考えよう．つまり，

$$\mathsf{code}_a(\langle 3, 10, 6, 4\rangle) = (112101021102100)_3.$$

数列の別のコード方法としては，次のようなものもある．

$$\mathsf{code}_b(\langle 3, 10, 6, 4\rangle) = p_1^3 \cdot p_2^{10} \cdot p_3^6 \cdot p_4^4.$$

ここで，p_n は n 番目の素数である．後者のコード方法は若干，効率が悪い．実際，限定算術などの文脈では code_b のような非効率的なコーディングは利用できず，まずは code_a の類によって基本的なコーディングが行われる．

さて，これらのコーディングで問題となるのは，どのように元の数列を復元するか，という点である．復元は算術の言語を用いて実行されなければならない．注意すべきことは，算術の言語 $\mathcal{L}_{\mathsf{arith}}$ が和，積，順序および $0, 1$ からなるものであって，指数などは記号としては含まれていない点である．例として，数列 $(x_1, x_2, \ldots, x_\ell)$ のコード c が与えられていたとしよう．この c から x_n を復元したい，という状況を考える．code_b でコード化していた場合，x_n とは「p_n^y が c を割り切るような最大の y」である．これを求める素朴な方法では，p_n^y について知る必要がある．code_a は幾分かマトモそうに見えるが，やはりどのように和，積，順序のみでデコードするかは明白ではない[*7]．

ここでコーディングに求めたいものは，

「c がコードしている列の n 番目の値が a である」という式が Δ_0 論理式で記述できる

という性質である．ただし，デコードの容易さだけを問題にするので，コード化の難しさについては，ここでは気にしないこととする．まず，対のコーディングを与えよう．

命題 2.13 (カントール)**.** 次のような全単射 $\mathsf{pair} : \mathbb{N}^2 \to \mathbb{N}$ と Δ_0 論理式 pr が存在する．$\pi_0, \pi_1 : \mathbb{N} \to \mathbb{N}$ を $\pi_0(\mathsf{pair}(x, y)) = x$ および $\pi_1(\mathsf{pair}(x, y)) = y$ なる唯一の関数としたとき，

$$\mathsf{pr}(n, a, b) \iff \pi_n(a) = b.$$

[*7] どちらのコード化についても原始再帰的な方法でコード・デコードできることを確認するのは難しくない．しかし，本節の目的は，原始再帰をアプリオリには持たない算術の言語で原始再帰を記述することであるから，その準備となるコード・デコードの部分で原始再帰を用いるわけにはいかない．

Proof. たとえば，対 $(x,y)\in\mathbb{N}^2$ を $x+y$ の値が小さいものから順に並べていく．また，$x+y=\ell$ なる対 (x,y) は

$$(\ell,0),\ (\ell-1,1),\ (\ell-2,2),\dots,(2,\ell-2),\ (1,\ell-1),\ (0,\ell)$$

という順に並べていこう．$x+y=\ell$ となる対 $(x,y)\in\mathbb{N}^2$ は ℓ 種類しか存在しないから，たとえば，$(\ell,0)$ には番号 $\sum_{k=0}^{\ell}k$ が割り当てられることが分かる．より一般に，対 (x,y) が配置される番号は以下となる．

$$\mathsf{pair}(x,y)=\left(\sum_{k=0}^{x+y}k\right)+y=\frac{1}{2}(x+y)(x+y+1)+y.$$

このとき，$\mathsf{pr}(0,a,b)$ は $(\exists c\leqslant a)\ a=\mathsf{pair}(b,c)$ によって与えられるが，これは明らかに Δ_0 である． □

以後は，$\langle x,y\rangle$ によって，命題 2.13 による対のコーディング $\mathsf{pair}(x,y)$ を表す．それでは，任意有限長さの自然数列のコーディングを始めよう．以下，$\mathbb{N}^*$ を自然数の有限列全体の集合を表すものとし，$\mathbb{N}^{\geqslant n}\subseteq\mathbb{N}^*$ を長さ n 以上の有限列全体の集合を表すものとする．

定理 2.14 (ゲーデル)**.** 次のような単射 $\mathsf{code}:\mathbb{N}^*\to\mathbb{N}$ と Δ_0 論理式 decode が存在する．$\pi_n:\mathbb{N}^{\geqslant n}\to\mathbb{N}$ を $n\leqslant\ell$ ならば $\pi_n(\mathsf{code}(x_0,\dots,x_\ell))=x_n$ なる関数とすると，任意の $a\in\mathbb{N}^{\geqslant n}$ について，

$$\mathsf{decode}(n,a,b)\iff\pi_n(a)=b.$$

Proof. まずは，有限集合のコーディングを行う．このために，階乗 $x!$ は以下の性質を持つことを確認しよう．

補題 2.15. 以下の相異なる 2 元は互いに素である．

$$m!+1,\ m!\cdot2+1,\ m!\cdot3+1,\ m!\cdot4+1,\dots,\ m!\cdot(m+1)+1.$$

Proof. まず，$a<b$ であり，a と b が共に v で割り切れるならば，$b-a$ も v で割り切れることに注意する．これはなぜなら，ある c,d が存在して $a=cv$ かつ $b=dv$ なので，$b-a=(d-c)v$ であるからである．それでは，$0<i<j\leqslant m+1$ とする．$m!\cdot i+1$ と $m!\cdot j+1$ を共に割り切る素数 u が存在しないことを示せばよい．u をそのような素数とすると，上の議論から，$m!\cdot(j-i)$ は u で割り切れる．u は素数であるから，$m!$ または $j-i$ のどちらか一方を割り切る．しかし，$j-i<j\leqslant m+1$ なので，$m!$ は $j-i$ で割り切れる．よって，どちらにせよ u は $m!$ を割り切るから，特に $m!\cdot i$ を割り切る．しがって，$m!\cdot i+1-m!\cdot i=1$ を割り切る．これより，u は 1 より大きい数では有り得ない． □

有限集合 $D \subseteq \mathbb{N}$ とその上界 $m \geqslant \max D$ が与えられているとしよう．この有限集合 D を次の自然数によってコードする．

$$\mathsf{code}(D) = \prod_{n \in D} (m! \cdot (n+1) + 1).$$

このとき，補題 2.15 と，a, b, c が互いに素ならば a と bc も互いに素であることを用いると，次のことが分かる．

$$n \in D \iff \mathsf{code}(D) \text{ は } m! \cdot (n+1) + 1 \text{ で割り切れる}.$$

したがって，D に対して，2 つの数 $y = \mathsf{code}(D)$ と $z = m!$ を知っていれば，

$$n \in D \iff (\exists u \leqslant y)\, [y = (z(n+1)+1) \cdot u].$$

として書けるので，つまり，D は自然数の対 $\langle y, z \rangle$ という “コード” から Δ_0 な方法で復元される．これが Δ_0-デコード可能なコーディングの 1 つである．以後，以下の記法を用いよう．

$$n \,\epsilon\, \langle y, z \rangle \iff (\exists u \leqslant y)\, [y = (z(n+1)+1) \cdot u].$$

有限列 $\sigma \in \mathbb{N}^*$ については，そのグラフをコードする．一般に，次を満たす自然数の対のコード $\langle y, z \rangle$ が，有限列 $\sigma \in \mathbb{N}^*$ のコードであると考えよう：任意の $n < |\sigma|$ について，

$$\sigma(n) = k \iff \langle n, k \rangle \,\epsilon\, \langle y, z \rangle \ \wedge\ (\forall \ell < k)\, \neg \langle n, \ell \rangle \,\epsilon\, \langle y, z \rangle.$$

したがって，以下，次の記法を用いる．

$$\mathsf{decode}(n, x, k) \iff \langle n, k \rangle \,\epsilon\, x \ \wedge\ (\forall \ell < k)\, \neg \langle n, \ell \rangle \,\epsilon\, x.$$

これが Δ_0 であり，求める性質を持つことは明らかであろう． □

以後，$\mathsf{decode}(n, x, k)$ という論理式を $(x)_n = k$ と表す．これは，自然数 x がコードしている列 $(a_i)_{i<\ell}$ の n 番目の要素 a_n の値が k であることを意味している．さて，これで原始再帰関数を算術的に記述するための準備は整った．

Proof (定理 2.12). 初期関数 succ, zero^n, proj^n_i のグラフが Δ_0-定義可能であることは自明である．次に，関数合成が Σ_1-定義可能性を保つことを示す．つまり，$g_1, \ldots, g_m : \mathbb{N}^n \to \mathbb{N}$ と $h : \mathbb{N}^m \to \mathbb{N}$ のグラフが Σ_1-定義可能であることを仮定し，$f(\bar{x}) = h(g_1(\bar{x}), \ldots, g_m(\bar{x}))$ のグラフも Σ_1-定義可能であることを確認する．これについては，$f(\bar{x}) = y$ が次と同値である．

$$(\exists u_1, \ldots, u_m) \left[\bigwedge_{i=1}^{m} (g_i(\bar{x}) = u_i) \ \wedge\ h(u_1, \ldots, u_m) = y \right].$$

補題 2.10 より，上の論理式は Σ_1 である．続いて，原始再帰法が Σ_1-定義可能性を保つことを示す．このために，$g : \mathbb{N}^n \to \mathbb{N}$ と $h : \mathbb{N}^{n+2} \to \mathbb{N}$ のグラフが Σ_1-定義可能であることを仮定し，$f : \mathbb{N}^{n+1} \to \mathbb{N}$ が以下の原始再帰法によって定義されているとする．

$$\begin{cases} f(\bar{x}, 0) = g(\bar{x}), \\ f(\bar{x}, y+1) = h(\bar{x}, y, f(\bar{x}, y)). \end{cases}$$

このとき，$f(\bar{x}, y) = z$ は以下の式と同値である．

$$(\exists u)\ \left[g(\bar{x}) = (u)_0\ \wedge\ (u)_y = z\ \wedge\ (\forall t < y)\ h(\bar{x}, t, (u)_t) = (u)_{t+1}\right].$$

これをもう少し丁寧に書けば，

$$\begin{aligned}(\exists u, v)\ \big[&g(\bar{x}) = v\ \wedge\ (u)_0 = v\ \wedge\ (u)_y = z \\ &\wedge\ (\forall t < y)(\exists r, s)\ \left[(u)_t = r\ \wedge\ (u)_{t+1} = s\ \wedge\ h(\bar{x}, t, r) = s\right]\big]\end{aligned}$$

であるから，補題 2.10 より，これは Σ_1 である． □

豆知識． 原始再帰関数の定義に **μ-再帰** (*μ-recursion*) というものを加えることによって，**部分再帰関数** (*partial recursive function*) の概念を定義することができる．部分再帰関数は（チューリング完全な）プログラミング言語を用いて計算可能な関数と正確に一致する，というものが計算可能性理論における基本定理の 1 つである．

定理 2.12 について，より一般に，任意の部分再帰関数のグラフは $\mathbb{N}$ で Σ_1-定義可能であることが知られている．逆に，部分関数のグラフが $\mathbb{N}$ で Σ_1-定義可能ならば，それは部分再帰関数であることも分かる．

つまり，グラフが $\mathbb{N}$ で Σ_1-定義可能な部分関数と，何らかのプログラミング言語を用いて計算可能な部分関数は正確に一致する．

3 ゲーデルの不完全性定理

3.1 算術の真理の公理化

第 1 節で，自然数に関して正しいと思われる性質の一部を抽出して，様々な算術の体系を取り扱ってきた．しかし，いずれの体系も，自然数に関する正しい式を全て証明できる，というわけではなかった．それでは，自然数に関する正しい式を全て証明できるような無矛盾な公理体系は存在するだろうか．この意味を明確にするために，以下の概念を導入しよう．

定義 3.1. 言語 $\mathcal{L}$ の構造 A が与えられているとする．このとき，A の**完全理論** (*complete theory*) とは，A で成立する $\mathcal{L}$-閉論理式全体の集合を意味し，$\mathrm{Th}(A)$ と書く．

まず，理論とはあくまで閉論理式の集合であったから，数学上では，$\mathrm{Th}(\mathbb{N})$ は理論である．定義から，任意の算術的な閉論理式 φ に対して，

$$\mathbb{N} \models \varphi \iff \mathrm{Th}(\mathbb{N}) \vdash \varphi$$

である．もちろん，スコーレムの定理より，$\mathrm{Th}(\mathbb{N})$ は $\mathbb{N}$ と非同型な可算モデルを持つから，$\mathrm{Th}(\mathbb{N})$ がモデル理論的に $\mathbb{N}$ を特徴づけるものではないが，とにかく $\mathrm{Th}(\mathbb{N})$ が自然数に関する正しい式を全て証明できる，ということに間違いはないだろう．しかし，$\mathrm{Th}(\mathbb{N})$ の公理とは，$\mathbb{N}$ に関する真な文そのもののことであり，一体，何が $\mathrm{Th}(\mathbb{N})$ の公理なのか，そう簡単に知る術は無さそうである．$\mathrm{Th}(\mathbb{N})$ のような超越的な理論を算術の公理体系と認めてよいだろうか．

これに対するひとつの解答としては，何が公理で何が公理でないのか，有限のアルゴリズムで判定する方法がある公理系だけに限定して考えよう，というものである．これが再帰的公理化可能性

のアイデアである．算術の言語 $\mathcal{L}_{\mathrm{arith}}$ は有限個の記号からなる有限言語である．一般に，$\mathcal{L}$ が可算言語であれば，$\mathcal{L}$-論理式は可算個しか存在しないので，$\mathcal{L}$-論理式 φ と自然数 $\ulcorner\varphi\urcorner \in \mathbb{N}$ を一対一に対応付けることができる．このように，文字列を数でコードするという手法については，現代社会に生きる読者には慣れ親しんだものであろうし，具体的な方法も簡単に思いつくと思う．アルゴリズム的判定の概念を導入するのは計算論が必要であるが，実は，再帰的公理化可能性と原始再帰的公理化可能性は同値になることは，**クレイグのトリック** (*Craig's trick*) としてよく知られているので，最初から以下のように定義してしまおう．

定義 3.2. 言語 $\mathcal{L}$ の理論 T の**公理化** (*axiomatization*) とは，$\mathcal{L}$-閉論理式の集合 S であって，任意の $\mathcal{L}$-閉論理式 φ に対して，以下が成立することである．

$$T \vdash \varphi \iff S \vdash \varphi.$$

理論 T が**再帰的公理化可能** (*recursively axiomatizable*) とは，原始再帰的公理化をもつことである．つまり，ある原始再帰的集合 $S \subseteq \mathbb{N}$ が存在して，$\{\varphi : \ulcorner\varphi\urcorner \in S\}$ が T の公理化となっている．

これが何が公理で何が公理でないかのアルゴリズム的判定可能性を数学的に形式化したものである．これくらいの条件を算術体系に要求することは妥当であろう．さて，我々は自然数に関する正しい式を全て証明できる無矛盾な再帰的公理化可能理論を求めていた．これは，次の問い掛けと同値である．

$$\mathbb{N} \text{ の完全理論 } \mathrm{Th}(\mathbb{N}) \text{ は再帰的公理化可能か？}$$

この分析のために，再帰的公理化可能理論における証明可能性の算術的複雑性の分析を始めよう．

定理 3.3. T を再帰的公理化可能理論とする．このとき，次を満たす Σ_1 論理式 $\mathsf{Provable}_T$ が存在する．

$$T \vdash \varphi \iff \mathbb{N} \models \mathsf{Provable}_T(\ulcorner\varphi\urcorner).$$

言い換えれば，以下の集合は $\mathbb{N}$ 上 Σ_1 である．

$$\mathrm{Th}(T) = \{\ulcorner\varphi\urcorner \in \mathbb{N} : T \vdash \varphi\}$$

Proof. この証明を一言で述べるならば，一階述語論理における「証明」というものが原始再帰法によって定義されていた，という点に尽きる．証明図とは，シーケントの有限列 $S_0, S_1, \ldots, S_n$ がツリー状に配置されているものであった．個々のシーケント S は論理式の列であるから，自然数 $\ulcorner S\urcorner \in \mathbb{N}$ でコードできる．有限列のコード $c \in \mathbb{N}$ が与えられれば，シーケントの列 $(S_0^c, S_1^c, \ldots, S_n^c)$ を復元できる．また，c の長さを求める関数 $lh(c)$ は原始再帰的である．c がコードしている最後のシーケントは，$S^c_{lh(c)-1}$ として書ける．以下，c^- を c から最後の値を取り除いたものとする．つまり，c^- は $(S_0^c, S_1^c, \ldots, S^c_{lh(c)-2})$ をコードする．

それでは，「c が理論 T でシーケント S を導く証明図をコードしている」ことを表す述語 $\mathsf{Proof}_T(c, \lceil S \rceil)$ が原始再帰的であることを示そう．$\mathsf{Proof}_T(c, \lceil S \rceil) = 1$ であるとは，次のいずれかの条件を満たすものである．

1. S が T の公理であり，$S^c_{lh(c)-1} = S$ である．
2. c^- の部分列 $d_0, \ldots, d_k$ が $S^c_{j_0}, \ldots S^c_{j_k}$ を導く証明図をコードしており，

$$\frac{S^c_{j_0}, \ldots, S^c_{j_k}}{S^c_{lh(c)-1}}$$

が上式から下式を導く推論規則であって，$S^c_{lh(c)-1} = S$ である．

第 1 の条件の原始再帰性は，再帰的公理化可能性より明らかである．第 2 の条件は，$\mathsf{Proof}_T(d_i, S^c_{j_i}) = 1$ を知る必要があるが，$d_i \leqslant c^- < c$ であるから，典型的な原始再帰法によって，第 2 の条件を満たすかどうかを判定する原始再帰関数を定義できる．したがって，補題 2.10 より，述語 $\mathsf{Proof}_T(c, \lceil S \rceil)$ が原始再帰的であることが分かる．T で φ が証明可能ということは，T におけるシーケント $\Rightarrow \varphi$ の証明図が存在する，ということであるから，

$$\lceil \varphi \rceil \in \mathrm{Th}(T) \iff (\exists c \in \mathbb{N})\ \mathsf{Proof}_T(c, \lceil \Rightarrow \varphi \rceil) = 1$$

と表すことができる．補題 2.12 より，原始再帰関数のグラフは Σ_1 であるから，$\mathrm{Th}(T)$ は Σ_1 であることが従う． □

豆知識． 定理 3.3 から我々が学べることは，自然数に関する非有界全称量化 $\forall$ を用いずに $\mathrm{Th}(T)$ を記述できる，ということである．一方，算術の論理式というものは，非有界存在量化と非有界全称量化を自在に用いてよい．算術の論理式における非有界量化記号の使用回数によって，以下のような**算術的階層** (*arithmetical hierarchy*) というものが定義される．

$$\Delta_0 \subsetneq \Sigma_1 \subsetneq \Sigma_2 \subsetneq \Sigma_3 \subsetneq \Sigma_4 \subsetneq \ldots$$

計算可能性理論を学んだ人であれば，$\mathrm{Th}(\mathbb{N})$ が有限の n について Σ_n の範囲に収まるわけはないことは知っている．これは，数学基礎論の文脈では，**タルスキの真理定義不可能性定理** (*Tarski's undefinability theorem*) として知られている．よって，定理 3.3 を用いれば，どんな再帰的公理化可能理論 T についても，$\mathrm{Th}(\mathbb{N}) \neq \mathrm{Th}(T)$ となることは自明に分かるだろう．つまり，$\mathrm{Th}(\mathbb{N})$ は再帰的公理化不可能である．

算術の完全理論 $\mathrm{Th}(\mathbb{N})$ の再帰的公理化不可能性を不完全性定理と呼ぶ人もいるが，この形の極めて弱い不完全性定理については，計算可能性理論における最も初歩的な定理の 1 つと言ってよいだろう．しかし，実際のゲーデルの不完全性定理はもう少し強い主張であるから，詳細は次以降の節で説明する．

3.2 停止問題を用いる証明

算術の完全理論 $\mathrm{Th}(\mathbb{N})$ が再帰的公理化不可能ということは，$\mathbb{N}$ をモデルに持つような再帰的公理化可能理論 T は不完全である，つまり $T \nvdash \varphi$ かつ $T \nvdash \neg\varphi$ なる閉論理式 φ が存在する，ということに他ならない．ここでは，理論が $\mathbb{N}$ をモデルに持つ，ということを少し弱めた概念を導入しよう．

定義 3.4. 理論 T が **ω-無矛盾** (ω-*consistent*) とは，どんな論理式 φ についても，以下が成立することである．

$$T \vdash \varphi(\underline{n}) \text{ for all } n \in \mathbb{N} \implies T \nvdash \exists x \neg\varphi(x).$$

理論 T が **Σ_1-健全** (Σ_1-*sound*) または **1-無矛盾** (1-*consistent*) とは，どんな Σ_1-閉論理式 φ についても，以下が成立することである．

$$T \vdash \varphi \implies \mathbb{N} \models \varphi.$$

上の性質が全ての算術的閉論理式 φ について成立するとき, 理論 T が**算術的健全** (*arithmetically sound*) であると言う．つまり，T が算術的健全とは，$T \subseteq \mathrm{Th}(\mathbb{N})$ となることである．

命題 3.5. T が離散順序環の非負部の公理 DOR^+ を含む理論であれば，次の関係が成立する．

$$\mathbb{N} \models T \implies T \text{ は } \omega\text{-無矛盾} \implies T \text{ は } \Sigma_1\text{-健全} \implies T \text{ は無矛盾}.$$

Proof. Σ_1-健全性が無矛盾性を導くことは，容易に分かる．念のために説明すると，矛盾した理論は任意の閉論理式を証明するので，特に Σ_1-閉論理式 φ についても，$\varphi \wedge \neg\varphi$ を証明する．よって，Σ_1-健全性より $\mathbb{N} \models \varphi \wedge \neg\varphi$ となるが，構造における否定の真偽の定義より，これは有り得ない．

続いて，T が ω-無矛盾であると仮定する．Σ_1-健全性を示すために，Σ_1-論理式 $\exists x\psi(x)$ に対して，$T \vdash \exists x\psi(x)$ を仮定する．T の ω-無矛盾性より，$T \nvdash \neg\psi(\underline{n})$ なる $n \in \mathbb{N}$ が存在する．もし $\mathbb{N} \not\models \exists x\psi(x)$ ならば $\mathbb{N} \models \forall x\neg\psi(x)$ であるから，$\mathbb{N} \models \neg\psi(\underline{n})$ が任意の $n \in \mathbb{N}$ について成立する．定理 1.17 より，DOR^+ は Σ_1-完全であるから，任意の $n \in \mathbb{N}$ について $T \vdash \neg\psi(\underline{n})$ である．よって，ω-無矛盾性より，$T \vdash \forall x\neg\varphi(x)$ である．

T が ω-矛盾していると仮定する．このとき，ある論理式 φ が存在して，全ての $n \in \mathbb{N}$ について $T \vdash \varphi(\underline{n})$ が成立するが，$T \vdash \exists x\neg\varphi(x)$ となる．もし，全ての $n \in \mathbb{N}$ について $\mathbb{N} \models \varphi(\underline{n})$ ならば，$\mathbb{N} \models \forall x\varphi(x)$ であるから，ある $n \in \mathbb{N}$ について，$\varphi(\underline{n}) \in \mathrm{Th}(T)\backslash\mathrm{Th}(\mathbb{N})$ であるか，さもなくば $\exists x\neg\varphi(x) \in \mathrm{Th}(T)\backslash\mathrm{Th}(\mathbb{N})$ である．つまり，$\mathrm{Th}(T) \not\subseteq \mathrm{Th}(\mathbb{N})$ を得る．よって $\mathbb{N} \not\models T$ である． □

ω-無矛盾性と無矛盾性に一体どんな違いがあるのか，と思う人もいるだろうから，ω-矛盾するが無矛盾な理論の簡単な例を挙げよう．

例 3.6. $\mathbb{Z}[X]^+$ の完全理論 $\mathrm{Th}(\mathbb{Z}[X]^+)$ は Σ_1-健全ではない．よって，$\mathrm{Th}(\mathbb{Z}[X]^+)$ は ω-矛盾している．

Proof. 命題 1.11 より，$\mathbb{Z}[X]^+$ には偶数でも奇数でもない元が存在した．つまり，次の閉論理式を考える．

$$\varphi \equiv (\exists x)(\forall y < x)\,[x \neq 2y \ \wedge \ x \neq 2y+1].$$

これは明らかに Σ_1 論理式である．一方，$\mathbb{Z}[X]^+ \models \varphi$ であるから，$\mathrm{Th}(\mathbb{Z}[X]^+) \vdash \varphi$ であるが，他方，$\mathbb{N} \models \neg\varphi$ である． □

実際，算術的健全だが ω-矛盾する理論を容易に構成できる．まず，算術的健全性については，次が成立する．

$$\mathbb{N} \models T \implies T \text{ は算術的健全} \implies T \text{ は } \Sigma_1\text{-健全} \implies T \text{ は無矛盾}.$$

例 3.7. T の言語が算術的言語より大きい場合，T の算術的健全性は一般には $\mathbb{N} \models T$ であることを導かない．たとえば，新しい定数記号 c を加えて，$T = \mathrm{Th}(\mathbb{N}) \cup \{c > \underline{n} : n \in \mathbb{N}\}$ を考えると，T は算術的健全だが，$\mathbb{N} \not\models T$ である．実際，T は ω-矛盾している．

ゲーデルのオリジナルの第一不完全性定理は，十分強い算術体系（たとえば離散順序環の非負部の公理 DOR^+ など）を含む ω-無矛盾な理論は不完全である，というものである．

定義 3.8. 言語 $\mathcal{L}$ の理論 T が**不完全** (*incomplete*) であるとは，T では証明も反証もできない論理式が存在することを意味する．つまり，ある $\mathcal{L}$-論理式 φ が存在して，次が成り立つことである．

$$T \not\vdash \varphi \ \wedge \ T \not\vdash \neg\varphi.$$

定理 3.9 (ゲーデルの第一不完全性定理)**.** 離散順序環の非負部の公理 DOR^+ を含む Σ_1-健全な再帰的公理化可能理論は不完全である

計算論を知っている人にとっては，この証明は容易である．本節では，計算論を使った証明の概略を与えよう．しかし，現代的には，ゲーデル-ロッサーの不完全性定理と呼ばれるもう少し強い形の主張が成り立つことが知られている．そちらについては，次節で計算論の知識を仮定しない証明を与えるので，計算論を学んだことのない読者は，本節を飛ばして次節に進むとよい．本節で要求する計算論の知識は，計算可能性理論における（歴史上においても，現代の教育課程においても）“最初の定理” である．

事実 3.10 (チューリングの定理)**.** 次のような集合 $K \subseteq \mathbb{N}$ が存在する．K は $\mathbb{N}$ 上 Σ_1 だが，その補集合 $\mathbb{N}\backslash K$ は $\mathbb{N}$ 上 Σ_1 ではない．

Proof. 以下の**停止問題** (*halting problem*) と呼ばれる集合 K を考える．

$$K = \{e \in \mathbb{N} : e \text{ 番目のチューリング機械に } 0 \text{ を入力したとき，} \\ \text{計算が有限時間で停止する}\}.$$

この K が求める性質を持つことはよく知られている． □

それでは，ゲーデルの第一不完全性定理の証明を与えよう．

定理 *3.9* の証明. K を事実 3.10 で得た集合とすると，K は Σ_1 なので，ある Σ_1 論理式 φ が存在して，$n \in K$ と $\mathbb{N} \models \varphi(\underline{n})$ が同値になる．T は DOR^+ を含むので，定理 1.17 より Σ_1-完全であるから，$T \vdash \varphi(\underline{n})$ を得る．一方，T の Σ_1-健全性より，もし $T \vdash \varphi(\underline{n})$ ならば，$\mathbb{N} \models \varphi(\underline{n})$ であるか

ら，$n \in K$ を得る．つまり，$n \in K$ と $T \vdash \varphi(\underline{n})$ は同値となる．一方，もし T が完全ならば，特に，任意の $n \in \mathbb{N}$ について $T \vdash \varphi(\underline{n})$ または $T \vdash \neg\varphi(\underline{n})$ が成立するから，以下を得る．

$$n \in \mathbb{N}\backslash K \iff T \nvdash \varphi(\underline{n}) \iff T \vdash \neg\varphi(\underline{n}).$$

つまり，$n \in \mathbb{N}\backslash K$ であることは $\ulcorner\neg\varphi(\underline{n})\urcorner \in \mathrm{Th}(T)$ である．$n \mapsto \ulcorner\neg\varphi(\underline{n})\urcorner$ は原始再帰的であり，定理 3.3 より $\mathrm{Th}(T)$ は Σ_1 であるから，この条件は Σ_1 である．これは $\mathbb{N}\backslash K$ が $\mathbb{N}$ 上 Σ_1 であることを導くため，事実 3.10 に反する． □

ちなみに弱い形のゲーデルの不完全性定理では，たとえば，$\mathbb{Z}[X]^+$ の完全理論 $\mathrm{Th}(\mathbb{Z}[X]^+)$ が再帰的公理化可能かどうかについては何も導かない．

3.3 表現可能性と対角化による証明

それでは，計算論の予備知識を前提としない，ゲーデル-ロッサーの不完全性定理の証明を始めよう．

定義 3.11. 関数 $f : \mathbb{N}^n \to \mathbb{N}$ が理論 T で **Σ_1-表現可能** (Σ_1-*representable*) であるとは，ある Σ_1-論理式 φ が存在して，任意の $\bar{x} \in \mathbb{N}^n$ および $y \in \mathbb{N}$ について，次を満たすことを意味する．

$$f(\bar{x}) = y \implies T \vdash \varphi(\underline{\bar{x}}, \underline{y}) \ \wedge \ (\forall z \neq y)\ \neg\varphi(\underline{\bar{x}}, z)$$

補題 3.12. 任意の原始再帰関数は離散順序環の非負部の公理 DOR^+ で Σ_1-表現可能である．

Proof. 原始再帰関数 $f : \mathbb{N}^n \to \mathbb{N}$ が与えられているとする．補題 2.12 より，f のグラフは Σ_1-論理式で与えられる．つまり，ある Δ_0 論理式 θ_f が存在して，

$$f(\bar{x}) = y \iff (\exists z)\ \theta_f(\bar{x}, y, z).$$

このとき，$\theta_f^{\min}(\bar{x}, y, z)$ を $\theta_f(\bar{x}, y, z)$ を満たすもののうち，$\langle y, z\rangle$ が最小であるものとする．より正確には，

$$\theta_f^{\min}(\bar{x}, y, z) \iff \theta_f(\bar{x}, y, z) \ \wedge \ (\forall u, v)\ [\langle u, v\rangle < \langle y, z\rangle \implies \neg\theta_f(\bar{x}, u, v)]$$

これは明らかに Δ_0 である．任意の $\bar{x}$ に対して，$\theta_f^{\min}(\bar{x}, y, z)$ を満たす対 $\langle y, z\rangle$ は高々 1 つであることが DOR^+ で証明できる：

$$\mathsf{DOR}^+ \vdash (\forall x, y, y', z, z')\ [[\langle y, z\rangle \neq \langle y', z'\rangle \ \wedge \ \theta_f^{\min}(\bar{x}, y, z)] \implies \neg\theta_f^{\min}(\bar{x}, y, z)].$$

それでは，f が Σ_1-論理式 $\psi(\bar{x}, y) \equiv \exists z\theta_f^{\min}(\bar{x}, y, z)$ によって表現されることを示す．まず，$f(\bar{x}) = y$ とすると，y は $\mathbb{N} \models \exists z\theta_f(\bar{x}, y, z)$ を満たす唯一の y であるから，$\exists z\theta_f(\bar{x}, y)$ を満たす最小の z について，$\theta_f^{\min}(\bar{x}, y, z)$ が成立し，つまり $\mathbb{N} \models \psi(\bar{x}, y)$ である．よって，DOR^+ の Σ_1-完全性より，$\mathsf{DOR}^+ \vdash \psi(\underline{\bar{x}}, \underline{y})$ が示される．

続いて，$f(\bar{x}) \neq y$ とする．このとき，ある $y' \neq y$ が存在して，$f(\bar{x}) = y'$ となるから，上と同様にして，ある $z' \in \mathbb{N}$ について $\mathsf{DOR}^+ \vdash \theta_f^{\min}(\underline{\bar{x}}, \underline{y'}, \underline{z'})$ を得る．$y \neq y'$ であることから，任意の z について $\langle \underline{y}, z \rangle \neq \langle \underline{y'}, \underline{z'} \rangle$ であることが DOR^+ で証明できるので，上で述べた $\theta_f^{\min}$ を満たす対の唯一性より，$\mathsf{DOR}^+ \vdash (\forall z)\, \neg\theta_f^{\min}(\underline{\bar{x}}, \underline{y}, z)$ が得られる．つまり，$\mathsf{DOR}^+ \vdash \neg\psi(\underline{\bar{x}}, \underline{y})$ である． □

豆知識． 補題 3.12 の証明は，Σ_1-グラフを持つ任意の全域関数は DOR^+ で Σ_1-表現可能であることを示している．したがって，実際には，任意の全域再帰関数は DOR^+ で Σ_1-表現可能である．

豆知識． 補題 3.12 の証明に多少の修正を施すことによって，$\mathsf{I}\Sigma_1$ において任意の原始再帰関数が可証全域再帰的（第 4.1 節を参照）であることを示すことができる．実際，$\mathsf{I}\Sigma_1$ における可証全域再帰関数は正確に原始再帰関数と一致する．したがって，たとえばアッカーマン関数などは $\mathsf{I}\Sigma_1$-可証全域再帰的でない．

それではゲーデルの不完全性定理の証明の準備を始めようと思うが，その前に，論理式の枚挙に対する注意をしよう．論理式は原始再帰的に定義されるものであるから，x のみを自由変数に持つ論理式を $\varphi_0(x), \varphi_1(x), \ldots$ と並べる関数 $(n, x) \mapsto \lceil \varphi_n(x) \rceil$ は原始再帰的である．したがって，定理 2.12 より，$\lceil \varphi_n(x) \rceil = y$ は $\mathbb{N}$ 上 Σ_1 である．それでは，ゲーデルの不完全性定理の鍵となる，対角化補題を証明する．

補題 3.13 (対角化補題)**.** T を離散順序環の非負部の公理 DOR^+ を含む任意の理論とする．このとき，任意の論理式 $\psi(x)$ に対して，ある閉論理式 σ が存在して，$T \vdash \sigma \leftrightarrow \psi(\underline{\lceil \sigma \rceil})$ となる．

一般の対角化補題を証明する前に，$T = \mathrm{Th}(\mathbb{N})$ のときを考える．実は，ここまでに示してきたことを用いると，$T = \mathrm{Th}(\mathbb{N})$ の対角化補題は，もはや自明である．なぜなら，$\mathbb{N}$ では，$\langle n, x \rangle \mapsto \lceil \varphi_n(x) \rceil$ は項と思えるから，$\psi(\lceil \varphi_x(x) \rceil)$ は x を自由変数とする論理式である．したがって，$\varphi_k(x) \leftrightarrow \psi(\lceil \varphi_x(x) \rceil)$ となる $k \in \mathbb{N}$ が存在する．これより，x に k を代入すれば，$\varphi_k(k) \leftrightarrow \psi(\lceil \varphi_k(k) \rceil)$ となるから，$\varphi_k(k)$ を σ とおけばよい．

このアイデアを T における形式証明として記述しよう．

補題 *3.13* の証明. 上で述べたように，$x \mapsto \lceil \varphi_x(x) \rceil$ は原始再帰的であるから，補題 3.12 より，DOR^+ を含む理論 T で Σ_1-表現可能である．つまり，次の性質を持つ論理式 χ が存在する．任意の $x, y \in \mathbb{N}$ について，

$$\underline{\lceil \varphi_x(x) \rceil} = y \implies T \vdash \chi(\underline{x}, \underline{y}) \wedge (\forall z \neq \underline{y})\, \neg\chi(\underline{x}, z).$$

このとき，論理式 $\exists y(\chi(x, y) \wedge \psi(y))$ は x のみを自由変数に持つので，ある k について $\varphi_k(x)$ となっている．これについて，$\varphi_k(\underline{k})$ を σ とおく．つまり，σ とは，$\exists y(\chi(\underline{k}, y) \wedge \psi(y))$ のことである．χ の性質により，T において，任意の y について次が証明できる．

$$\chi(\underline{k}, y) \leftrightarrow y = \underline{\lceil \varphi_k(k) \rceil} \leftrightarrow y = \underline{\lceil \sigma \rceil}$$

したがって，σ の存在量化の証拠となる y は必ず $\underline{\lceil \sigma \rceil}$ であるから，$T \vdash \sigma \to \psi(\underline{\lceil \sigma \rceil})$ を得る．逆に，

$\psi(\underline{\lceil\sigma\rceil})$ であるならば，$\chi(\underline{k}, \underline{\lceil\sigma\rceil})$ であることは分かっているから，$y = \underline{\lceil\sigma\rceil}$ を存在量化の証拠として σ が導かれることが T において証明できる．以上より，$T \vdash \sigma \leftrightarrow \psi(\underline{\lceil\sigma\rceil})$ を得る． □

定理 3.3 の証明で定義した Proof_T を思い出そう．このとき，次の**ロッサー述語** (*Rosser predicate*) を考える．

$$\mathsf{Provable}^*_T(x) \;\equiv\; (\exists y)\,[\mathsf{Proof}_T(y, x) \;\wedge\; (\forall z \leqslant y)\,\neg\mathsf{Proof}_T(z, \neg x)].$$

定理 3.3 で見たように，もし T が再帰的公理化可能ならば，$\mathsf{Provable}^*_T$ は Σ_1-論理式である．

補題 3.14. T を DOR^+ を含む再帰的公理化可能理論とする．このとき，任意の閉論理式 σ について，次が成立する．

$$T \vdash \sigma \implies T \vdash \mathsf{Provable}^*_T(\underline{\lceil\sigma\rceil}),$$
$$T \vdash \neg\sigma \implies T \vdash \neg\mathsf{Provable}^*_T(\underline{\lceil\sigma\rceil}).$$

Proof. T が矛盾している場合は明らかなので，T は無矛盾であると仮定する．$T \vdash \sigma$ ならば，T の無矛盾性より，$\mathbb{N} \models \mathsf{Provable}^*_T(\underline{\lceil\sigma\rceil})$ であるから，T の Σ_1-完全性より，$T \vdash \mathsf{Provable}^*_T(\underline{\lceil\sigma\rceil})$ である．一方，$T \vdash \neg\sigma$ の場合，$T \vdash \neg\sigma$ の証明図の最小コード c がある．このとき，

$$\mathbb{N} \models \mathsf{Proof}_T(\underline{c}, \underline{\lceil\neg\sigma\rceil}) \wedge (\forall z \leqslant \underline{c})\,\neg\mathsf{Proof}_T(z, \underline{\lceil\sigma\rceil})$$

であるが，この論理式は Σ_1 であるから，T の Σ_1-完全性より，T で証明可能である．これは

$$T \vdash (\forall y)\,[\mathsf{Proof}_T(y, \underline{\lceil\neg\sigma\rceil}) \;\to\; (\exists z < y)\,\mathsf{Proof}_T(z, \underline{\lceil\neg\sigma\rceil})]$$

を導く．つまり，$T \vdash \neg\mathsf{Provable}^*_T(\underline{\lceil\sigma\rceil})$ である． □

定理 3.15 (ゲーデル-ロッサーの不完全性定理)**.** 離散順序環の非負部の公理 DOR^+ を含む無矛盾かつ完全な再帰的公理化可能理論は存在しない．

Proof. T を DOR^+ を含む再帰的公理化可能理論とする．対角化補題 3.13 より，$T \vdash \sigma \leftrightarrow \neg\mathsf{Provable}^*_T(\underline{\lceil\sigma\rceil})$ となる閉論理式 σ が存在する．しかし，σ の定義と補題 3.14 を組み合わせると，

$$T \vdash \neg\mathsf{Provable}^*_T(\underline{\lceil\sigma\rceil}) \iff T \vdash \sigma \implies T \vdash \mathsf{Provable}^*_T(\underline{\lceil\sigma\rceil}),$$
$$T \vdash \mathsf{Provable}^*_T(\underline{\lceil\sigma\rceil}) \iff T \vdash \neg\sigma \implies T \vdash \neg\mathsf{Provable}^*_T(\underline{\lceil\sigma\rceil}).$$

となるから，$T \vdash \sigma$ または $T \vdash \neg\sigma$ が成立するならば，T は矛盾している． □

例 3.16. ゲーデル-ロッサーの不完全性定理の前提条件である (a) DOR^+ を含む; (b) 無矛盾である; (c) 完全である; (d) 再帰的公理化可能である; のいずれか一つを取り除けば，そのような理論は存在する．

1. DOR^+ を含む無矛盾かつ完全な理論は存在する．たとえば，$\mathsf{Th}(\mathbb{Z}[X]^+)$ や $\mathsf{Th}(\mathbb{N})$ などである．
2. DOR^+ を含まない無矛盾かつ完全な再帰的公理化可能理論は存在する．たとえば加法のみの算術として知られる**プレスバーガー算術** (*Presburger arithmetic*) や**実閉体** (*real closed field*) の理論 RCF などである．

豆知識．上で挙げたように，ペアノ算術を含む無矛盾かつ完全な理論の例として $\mathsf{Th}(\mathbb{N})$ がある．もちろん，$\mathsf{Th}(\mathbb{N})$ は再帰的公理化可能からは程遠いが，ペアノ算術を含む無矛盾かつ完全な理論が**どれくらい再帰的公理化可能に近い**ものとして作れるか，ということを議論することができる．つまり，再帰的公理化不可能さの**度合い** (*degree*) を測る指標があって，それが**低い** (*low*) ほど，再帰的公理化可能に近い．**次数の理論** (*degree theory*) においては，ペアノ算術を含む無矛盾かつ完全な理論の**次数** (*degree*) のことを **PA-次数** (PA-*degree*) と呼び，1970 年代始め頃から深く研究されている．たとえば，$\mathsf{Th}(\mathbb{N})$ の次数は $\mathbf{0}^{(\omega)}$ であるが，これより遥かに低い PA-次数が存在する．具体的には，停止問題の次数 $\mathbf{0}'$ より低い次数 $\mathbf{a}$ を神託とすることによって無矛盾かつ完全な理論 $T \supseteq \mathsf{PA}$ を構成することも可能である．

$$\mathbf{0} = \text{計算可能} < T \text{ の次数} < \mathbf{0}' = \text{停止問題の次数} < \mathbf{0}'' < \mathbf{0}''' < \cdots < \mathbf{0}^{(\omega)} = \mathsf{Th}(\mathbb{N}) \text{ の次数}.$$

この最初期の最も有名な定理が**低基底定理** (*low basis theorem*) と呼ばれるものである．これによって，ペアノ算術を含む無矛盾かつ完全な理論で再帰的公理化可能に極めて近いものが存在することが分かる．しかし，次数という観点は不完全性定理の詳細な分析に用いるには非常に粗く，そのような文脈で用いられることは現代的にはほぼ皆無といってよい．たとえば，ペアノ算術の代わりに ZFC 集合論に対する ZFC-次数のようなものを考えても結果は変わらない，というような粗さがある．

しかし，これによって PA-次数といった概念や低基底定理の重要性が霞むというものでは決してない．それどころか，時代を経るにつれ，その重要性は増している．その重要性は，数学基礎論よりはむしろ計算可能性理論におけるものであって，たとえば**アルゴリズム情報理論** (*algorithmic information theory*)，**計算可能解析学** (*computable analysis*) や**逆数学** (*reverse mathematics*) といった分野において広範な応用を持つことが知られている．

対角化補題 3.13 のように $\varphi_k(k)$ のような対角関数を取るという操作は，数学の至る所で行われてきた．たとえば，2 節の原始再帰関数の導入のように，人類は「足し算から倍増 $2x := x + x$ の概念を得る」「掛け算から自乗 $x^2 = x \cdot x$ の概念を得る」といった対角化を実践してきたことだろう．ゲーデルの不完全性定理 3.15 の証明は**対角線論法** (*diagonal argument*) と呼ばれることもあるが，関数の対角化による構成の文脈では，「掛け算は足し算より真に急増加する」「指数関数は掛け算より真に急増加する」「矢印関数は指数関数より真に急増加する」などが対角線論法である．

実際，数学において対角線論法の最初の利用とは，まさにこのようなものであり，1875 年のポール・デュ・ボア=レーモン (Paul du Bois-Reymond) による

与えられた $\mathbb{N}$ 上の関数の列のいずれよりも真に急増加する関数を構成できる

ということの証明が対角線論法の起源とされる．ちなみに対角線論法というとカントールが有名であり，カントールによる実数の非可算性証明は 1874 年である．しかし，1874 年の証明には対角線論法は現れず，カントールが初めて対角線論法を用いたのは 1891 年だそうである．

情報系の学生向けの講義であるから，最後に，情報学関連の分野における対角線論法に触れて締めるとしよう．最も有名な例は，**計算量理論** (*computational complexity theory*) において 1965 年

に証明された**時間階層定理** (*time hierarchy theorem*) である．この定理の結論の一例として，多項式時間計算可能な問題のクラス P と指数時間計算可能な問題のクラス EXP が異なるということ，つまり $\mathsf{P} \neq \mathsf{EXP}$ が示される．一方で，対角線論法はあくまで基本的な証明技法に過ぎず，そこまで強力な手法というわけでもない，ということも説明しよう．

計算機科学における最も重要な未解決問題で，数学のミレニアム問題の 1 つとも知られる P 対 NP 問題と呼ばれる難問がある．1950 年代に，ナッシュがアメリカ国家安全保障局に宛てた書簡，およびゲーデルがフォン・ノイマンに宛てた手紙において，この問題は言及されており，現在は，ナッシュとゲーデルが P 対 NP 問題の提唱者であると認識されている．

さて，クックがこの大問題に厳密な定式化を与えた 1970 年代になってすぐに，$\mathsf{P} \neq \mathsf{NP}$ には**相対化可能** (*relativizable*) な証明は存在しないことが知られるようになった．実際，上手く**神託** (*oracle*) A, B を取ると，その相対化によって $\mathsf{P}^A = \mathsf{NP}^A$ にも $\mathsf{P}^B \neq \mathsf{NP}^B$ にもなることが示されたのである．ところが，対角線論法とは，相対化可能な証明手法の代表選手のようなものである．したがって，対角線論法を用いて $\mathsf{P} \neq \mathsf{NP}$ のようなものを証明することはできないことが分かってしまう．

4 付録

4.1 可証全域関数

関数 $f : \mathbb{N}^n \to \mathbb{N}$ が理論 T において**可証全域** (*provably total*) とは，ある論理式 φ が存在して，$T \vdash \forall \bar{x} \exists! y \varphi(\bar{x}, y)$ かつ $\mathbb{N}$ において φ は f のグラフを定義する，つまり，$\mathbb{N} \models (\forall \bar{x}, y)\ [f(\bar{x}) = y \leftrightarrow \varphi(\bar{x}, y)]$ となることである．論理式 φ が Σ_1 であれば，**可証全域再帰的** (*provably recursive*) または**可証全域計算可能**という[*8]．大雑把に言えば，可証全域計算可能性は，全域計算可能性が証明できるということであるから，十分健全な理論では次が成立する．

命題 4.1. T を離散順序環の非負部の公理 DOR^+ を含む再帰的公理化可能理論とする．このとき，T が Σ_1-健全ならば，T-可証全域計算可能性は計算可能性を導く．

Proof. f が T-可証全域計算可能であると仮定する．T が Σ_1-健全ならば，$T \vdash \varphi(\underline{n}, \underline{m})$ は $\mathbb{N} \models \varphi(n, m)$ を導く．つまり，$f(n) = m$ である．逆に，$f(n) = m$ ならば $\mathbb{N} \models \varphi(n, m)$ であるから，DOR^+ の Σ_1-完全性より，$T \vdash \varphi(\underline{n}, \underline{m})$ を得る．$f(n) = \mu m.\mathrm{Provable}_T(\ulcorner \varphi(\underline{n}, \underline{m}) \urcorner)$ であるが，$\mathrm{Provable}_T$ は Σ_1 であるから，f のグラフは Σ_1 である．よって，T-可証全域計算可能関数は必ず計算可能である． □

注意すると，一般の論理式 φ については，$T \vdash \exists y \varphi(\underline{n}, y)$ だったとしても，具体的な m について $T \vdash \varphi(\underline{n}, \underline{m})$ となるとは限らない．たとえば，$(\mathrm{Con}(T) \leftrightarrow y = 0) \wedge (\neg \mathrm{Con}(T) \leftrightarrow y = 1)$ など

[*8] ほとんどの文献では，可証全域性といった場合，暗黙に全域計算可能関数についての可証全域性を議論している．このため，可証全域計算可能関数のことを単に可証全域関数と呼ぶことが多い．ただし上の定義の場合，当然ながら，可証全域だからといって計算可能とは限らない．

を考えるとよい．しかし，T が上の命題の条件を満たす理論であり，φ が Σ_1 であれば，この存在特性 (existential property) を持つ．

もちろん，かなり弱い理論 (ペアノ算術 PA 程度でよい) でも，停止問題の特性関数やビジービーバー関数などといった計算不可能関数の全域性を証明できる．これらの関数について，論理式 φ の複雑性は Σ_2 である．したがって，可証全域であっても可証全域計算可能とは限らない．

さて，T-可証全域でない全域計算可能関数の存在を示すには，少し工夫が必要である．

命題 4.2. T を離散順序環の非負部の公理 DOR^+ を含む再帰的公理化可能理論とする．このとき，T が Σ_1-健全ならば，T-可証全域計算可能でない全域計算可能関数が存在する．

Proof. φ_e を e 番目の Σ_1 論理式とする．このとき，$E = \{e \in \mathbb{N} : T \vdash (\forall x)(\exists! y)\varphi_e(x,y)\}$ は Σ_1 である．各 $e \in E$ と $n \in \mathbb{N}$ について，$T \vdash (\exists y)\varphi_e(\underline{n}, y)$ であるから，Σ_1-健全性より $\mathbb{N} \models (\exists y)\varphi_e(n,y)$ である．よって，$\mathbb{N} \models \exists m \varphi_e(n,m)$ なる最小の m を取ると，DOR^+ の Σ_1-完全性より $T \vdash \varphi_e(\underline{n}, \underline{m})$ を得る．

さて，E が有限集合であれば主張は自明であるから，E は無限集合であると仮定すると，これを $e(0), e(1), \ldots$ と計算可能に枚挙できる．このとき，各 n について，上の議論により，$T \vdash \varphi_{e(n)}(\underline{n}, \underline{m})$ なる最小の m が存在する．これは Σ_1 条件なので計算可能な方法で見つけられるから，$f(n) = m + 1$ として定義した関数 $f : \mathbb{N} \to \mathbb{N}$ は計算可能である．

この f が T-可証全域計算可能でないことを示す．もし f が T-可証全域計算可能ならば，f のグラフを $\mathbb{N}$ で定義する Σ_1-論理式 φ で，$T \vdash \forall x \exists! y \varphi(x,y)$ となるものが存在する．E の定義より，ある n について，$\varphi = \varphi_{e(n)}$ である．$T \vdash \varphi_{e(n)}(\underline{n}, \underline{m})$ なる最小の m を取る．f の定義より，$f(n) = m + 1$ である．しかし，T の Σ_1-健全性より，$\mathbb{N} \models \varphi_{e(n)}(n,m)$ であり，$\varphi_{e(n)}$ は f のグラフを定義しているから，$f(n) = m$ を得るが，これは矛盾を導く．よって，f は T-可証全域計算可能では有り得ない． □

一応注意しておくと，上で作った関数 f の全域性は証明されている．補題 3.12 の直後に注記したように，$\mathsf{I}\Sigma_1$-可証全域計算可能性は原始再帰性を特徴づける．

定理 4.3. 関数 $f : \mathbb{N} \to \mathbb{N}$ が原始再帰的であることと $\mathsf{I}\Sigma_1$-可証全域計算可能であることは同値である．

4.2 チャイティンの不完全性定理

チューリングは，停止問題の計算不可能性を利用することによって，ゲーデルの不完全性定理の弱い形の別証明を与えた．このような計算論の手法を用いることによって，チューリング型の不完全性定理の様々なバリエーションを示すことができる．

1944 年，エミール・ポストは不完全性定理の計算論的分析のために，自然数の集合の計算論的

性質を幾つか導入した．そのバリエーションとして，計算可能性理論では以下のような概念がよく知られている．自然数の集合 $A \subseteq \mathbb{N}$ が**免疫** (*immune*) とは，$B \subseteq A$ となるような無限 Σ_1 集合が存在しないことである．また，$A \subseteq \mathbb{N}$ が**双免疫** (*bi-immune*) とは，A と $\mathbb{N}\backslash A$ が共に免疫であることを意味する．

以後，算術的論理式 φ について，$\mathrm{Set}_\varphi = \{n \in \mathbb{N} : \mathbb{N} \models \varphi(n)\}$ と定義する．理論 T が算術的健全とは，$T \subseteq \mathrm{Th}(\mathbb{N})$ を満たすことであった．

命題 4.4. T を算術的健全な再帰的公理化可能理論とする．任意の算術的論理式 $\varphi(x)$ について，もし Set_φ が免疫ならば，$T \vdash \varphi(\underline{n})$ なる $n \in \mathbb{N}$ は有限個しか存在しない．

Proof. $\mathrm{Set}_\varphi^T = \{n \in \mathbb{N} : T \vdash \varphi(\underline{n})\}$ とおく．T の再帰的公理化可能ならば，Set_φ^T は Σ_1 である．また，T が算術的健全ならば，$\mathrm{Set}_\varphi^T \subseteq \mathrm{Set}_\varphi$ である．よって，Set_φ が免疫であることから，Set_φ^T が有限であることが導かれる． □

以下は，チューリング型の不完全性定理のバリエーションの 1 つで，**チャイティンの不完全性定理** (*Chaitin's incompleteness theorem*) と呼ばれることもある定理である．

系 4.5 (チャイティンの不完全性定理)**.** 任意の算術的健全な再帰的公理化可能理論 T は，次の条件を満たす定数 $c_T \in \mathbb{N}$ を持つ．理論 T では，コルモゴロフ複雑性が c_T 以上であるようなバイナリ列の存在を示すことができない．つまり，任意の σ について，

$$T \nvdash K(\sigma) \geqslant c_T.$$

Proof. $\{\langle \sigma, c\rangle : K(\sigma) \geqslant c\}$ が免疫集合であることはよく知られている．よって，命題 4.4 を応用すればよい． □

念のために述べておけば，任意の c に対して，$K(\sigma) \geqslant c$ を満たすバイナリ列 σ の存在は，極めて弱い理論 T において証明できる．なぜなら，$K(\sigma) < c$ を満たすバイナリ列 σ は 2^c 個未満しかないからである．つまり，系 4.5 とは，前節で触れた存在特性を強く否定する論理式の具体例を与えるものである．

もう一つ，チューリング型の不完全性定理を紹介しよう．

命題 4.6. T を算術的健全な再帰的公理化可能理論とする．任意の算術的論理式 $\varphi(x)$ について，もし Set_φ が双免疫ならば，$T \vdash \varphi(\underline{n})$ または $T \vdash \neg\varphi(\underline{n})$ となる $n \in \mathbb{N}$ は有限個しか存在しない．

Proof. 命題 4.4 の証明と同様である． □

最適マシンの停止確率を**チャイティンの定数** (*Chaitin's constant*) または**チャイティンのオメガ** (*Chaitin's Omega*) と呼び，Ω と表記する．この実数 Ω はランダムな振る舞いをすることが知られ，アルゴリズム的情報理論における興味深い対象の 1 つである．

系 4.7 (チャイティンの不完全性定理 2)**.** 任意の算術的健全な再帰的公理化可能理論 T は，チャイティンの定数 Ω の有限個の値しか特定できない．つまり，$\Omega(n)$ によって Ω を 2 進展開したときの小数点以下 n 桁目のを表すものとすると，有限個の n, i を除いて，

$$T \nvdash \Omega(n) = i$$

Proof. $\{n \in \mathbb{N} : \Omega(n) = 1\}$ が双免疫集合であることはよく知られている．よって，命題 4.6 を応用すればよい． □

また，比較的弱い理論（たとえば ACA_0 など）において，任意の $n \in \mathbb{N}$ について，$\Omega(n) = i$ なる $i \in \{0, 1\}$ が存在することは証明できる．したがって系 4.7 もまた存在特性に対する極めて強い反例を与えるものである．

さて，もちろん，双免疫な算術的集合はチャイティンの定数以前にも沢山知られているものであったから，系 4.7 はチャイティンの定数の何らかの特筆性を示すものではない．テクニカルなことを言えば，チャイティンの不完全性定理はゲーデルの不完全性定理（の弱い形のチューリングによる証明）を一歩も越えていない．

しかし，チャイティンの不完全性定理が公表された後にソロヴェイによって与えられた改良は，テクニカルには非自明で興味深い．まず，チャイティンの定数 Ω の値は厳密には最適マシン U の選択に依存するから，正確には Ω_U と表記される．ソロヴェイは，ZFC の算術的健全性の仮定の下で，その停止確率 Ω_U を ZFC では 1 ビットたりとも特定できないような最適マシン U を構成した．

定理 4.8 (ソロヴェイ)**.** T を算術的健全な再帰的公理化可能理論とする．このとき，ある最適マシン U が存在して，任意の $n, i \in \mathbb{N}$ について，

$$T \nvdash \Omega_U(n) = i.$$

■補足 上に挙げた例であるチャイティンの Ω の他，ビジービーバー関数 BB のように，全域関数であると証明されている，つまり値が確定していると考えられるにも関わらず，健全な再帰的公理化可能理論では具体的な値を証明できない部分のある関数の存在を気持ち悪く思う人もいるようである．一階算術では分かりづらいかもしれないので，より明示的に自然数の集合を扱える体系，たとえばペアノ算術の保存的拡大である ACA_0 を考えれば，

$$\mathsf{ACA}_0 \vdash (\forall x \in \mathbb{N})(\exists y \in \mathbb{N})\ BB(x) = y$$

である．

計算可能なシステム

再帰的公理化可能性

計算可能性はロバストな概念

ただし，上に挙げた定理の中で，ソロヴェイの定理だけはそれ以上のことを述べている．

4.3 参考文献

本講義ノートでは省略したが，第 1 回〜第 8 回の講義内容である命題論理・述語論理入門については，小野 [2] および江田 [1] を参考にした．共に優れた教科書である．

本講義ノートの第 1 節「自然数論の形式体系」および第 3 節「ゲーデルの不完全性定理」に記載した内容の一部は，和書では田中 [4] が詳しい．特に第 3 節の作成の際に参考にした．第 1 節の一部は，Kaye [6] を参考にしている．第 2 節「原始再帰関数」の一部は，篠田 [3] を参考にしたが，絶版となっており，入手は難しい．

一階算術の入門書としては, Hajek-Pudlak [5] は非常に評価が高い教科書であり, Project Euclid において出版社から無料で公開されている．本ノートの作成の際にも参考にしている．

参考文献

[1] 江田勝哉『数理論理学—使い方と考え方: 超準解析の入り口まで』内田老鶴圃, 2010 年.

[2] 小野寛晰『情報科学における論理』 日本評論社, 1994 年.

[3] 篠田寿一『帰納的関数と述語』河合文化教育研究所, 1997 年.

[4] 田中一之『数の体系と超準モデル』裳華房, 2002 年.

[5] Petr Hajek and Pavel Pudlak, “Metamathematics of First Order Arithmetic,” Springer-Verlag, Berlin, Heidelberg, 1993.

[6] Richard Kaye, “Models of Peano Arithmetic,” Oxford University Press, 1991.