数学基礎論サマースクール2018
証明論，特に算術の無矛盾性証明

2．ペアノ算術・ε_0・ゲンツェン

2018年9月3日 神戸大学

菊池 誠（神戸大）

ペアノ算術

自然数全体の集合の特徴付け

X：集合，f: X→X，a∈X とする．(X, f, a) が以下の条件をみたすとき (X, f, a) は単純無限列であるという．

- f は単射
- a∉f[X]
- （数学的帰納法）A⊆X とする．
  a∈A かつ ∀x∈X(x∈A→f(x)∈A) ならば A=X.

定理（デデキント）

単純無限列は同型なものを同一視すれば唯一．

事実

ℕ={0, 1, 2, …}：自然数全体の集合，s(x)=x+1とすると，
(ℕ, s, 0) は単純無限列．

ペアノ算術

算術の言語：$L=\{+, \cdot, 0, 1, <\}$

ペアノ算術：以下の非論理的公理からなる算術の言語の理論をペアノ算術といい，PA と書く．

- $(x+y)+z=x+(y+z)$, $x+y=y+x$
- $(x\cdot y)\cdot z=x\cdot(y\cdot z)$, $x\cdot y=y\cdot x$, $x\cdot(y+z)=x\cdot y+x\cdot z$
- $x+0=x$, $x\cdot 0=0$, $x\cdot 1=x$
- $x<y\wedge y<z\rightarrow x<z$, $\neg x<x$, $x<y\vee x=y\vee y<x$
- $x<y\rightarrow x+z<y+z$, $0<x\wedge x<y\rightarrow x\cdot z<y\cdot z$, $x<y\rightarrow\exists z(x+z=y)$
- $0<1$, $\forall x(0<x\rightarrow 1=x\vee 1<x)$, $0<x$
- （数学的帰納法）A(x) を L の論理式とする．
  $A(0)\wedge\forall x(A(x)\rightarrow A(x+1))\rightarrow\forall xA(x)$

注意：数学的帰納法の適用範囲には制限がある．

ペアノ算術

無矛盾性

T を PA⊆T である L の理論とする.

- 定義：T が無矛盾⇔T⊢0=1 でない.
- 定義：T がω無矛盾
  ⇔Lのどのような論理式 A(x) についても,
  T⊢A(0), T⊢A(1), … ならば, T⊢∃x¬A(x) でない.

不完全性定理（ゲーデル1931）

T を再帰的で PA⊆T である L の理論とする. このとき,

- T はω無矛盾なら不完全
- T の無矛盾性を表す論理式 Con(T) が存在して,
  T が無矛盾なら T⊢Con(T) でない.

問題：PA の無矛盾性を示したいが cut は取れない. どうする？

順序数

対角線論法

- 集合 X の冪集合を P(X) と書く.
- X から P(X) への単射は存在するが，X と P(X) の間には全単射は存在しない．X よりもP(X) の方が大きい.

問題

- 有限集合の大きさは自然数で測れる.
- 無限集合の相対的な大小でなく，絶対的な大きさを定められないか？
- 無限集合を測るための「目盛」を定めたい.

順序数と基数

- 順序数：自然数概念の無限への拡張
- 基数：集合の大きさを測るための順序数

順序数

二種類の $\mathbb{N}$ の理解

- 上から見下ろす（構造主義）
  $\mathbb{N}$ 全体を数学的帰納法で特徴付ける．その要素が自然数．
- 下から積み上げる（構成主義）
  自然数 0, 1, 2, … を順々に作る．それを集めたのが $\mathbb{N}$．

最小値原理

- どのような $A \subseteq \mathbb{N}$ にも $A \neq \emptyset$ なら A の最小値が存在する．
- 数学的帰納法からの帰結．

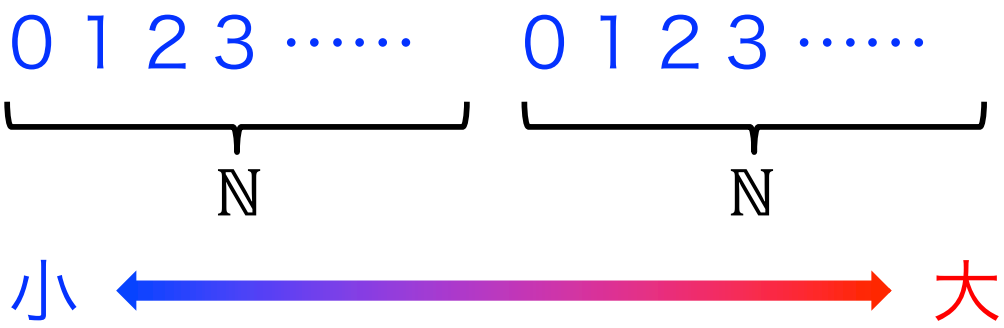
整列順序集合

- X を集合，$<$ を X 上の全順序とする．
  どのような $A \subseteq X$ にも $A \neq \emptyset$ なら A の最小値が存在するとき，
  $<$ は X 上の整列順序であるという．
- 整列順序集合は $\mathbb{N}$ の一般化．

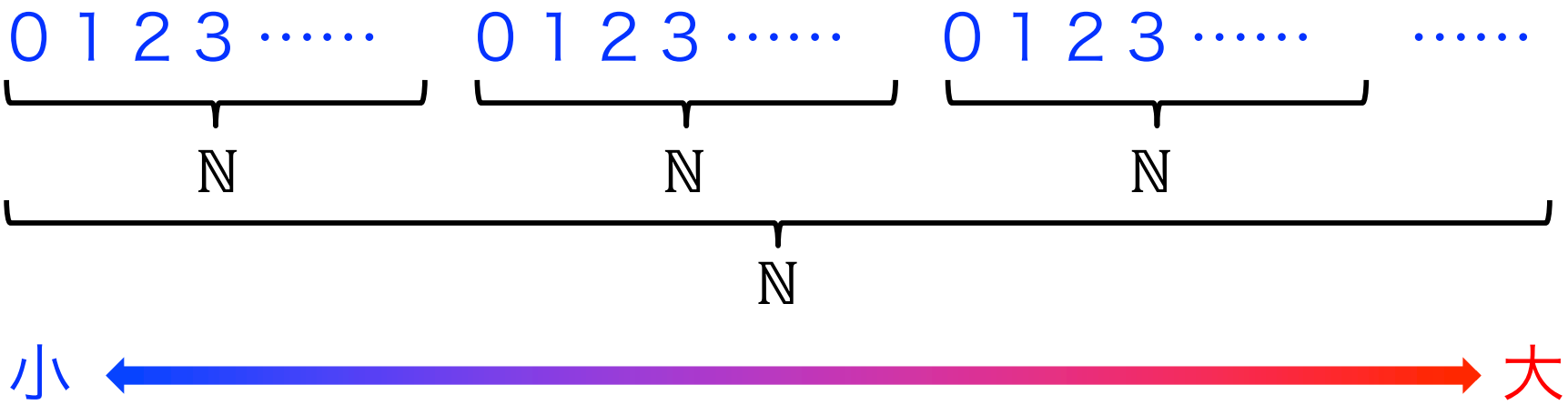
順序数

整列順序の例

- ℕ を二つ繋げたもの：



- ℕ を ℕ 個繋げたもの：



順序数

超限帰納法

$(X, <)$ を整列順序とする.

- $(X, <)$ 上では，次の形の数学的帰納法（超限帰納法）が成立.

  $A \subseteq X$ とする.

  $\forall x \in X(\forall y \in X(y<x \rightarrow y \in A) \rightarrow x \in A)$ ならば $A=X$

- 整列順序ならば無限下降列はない.

注意

- $\mathbb{N}$ には常に「直前の数」が存在.
- 整列順序集合には「直前の要素」がない場合がある.

０１２３……　０１２３……

⬆

直前の要素なし

順序数

順序数の構成

自然数 n を要素数 n の集合で表したい.

- 0 = ∅（空集合）
- 1 = {0}（= {∅} = 0∪{0}）
- 2 = {0, 1}（= {∅, {∅}} = 1∪{1}）
- 3 = {0, 1, 2}（= {∅, {∅}, {∅, {∅}}} = 2∪{2}）

  ⋮

- n+1 = {0, 1, 2, ⋯, n}（= n∪{n}）

  ⋮

順序数

順序数の構成

やがて $\mathbb{N}$ に辿り着き，乗り越えていく．

- $\omega = \{0, 1, 2, \cdots\}$
- $\omega{+}1 = \{0, 1, 2, \cdots, \omega\}$ $(= \omega \cup \{\omega\})$

  ⋮
- $\omega{+}\omega = \{0, 1, 2, \cdots, \omega, \omega{+}1, \omega{+}2, \cdots\}$

  ⋮

（フォンノイマン）順序数

このように構成される集合 α はつぎの性質を持つ．

- $\beta \in \alpha$ ならば $\beta \subseteq \alpha$（α は推移的）
- α は $\in$ で整列順序集合

この二つの性質を持つ集合を順序数という．

順序数

順序数の計算：α, β：順序数，　X：順序数の集合とする.

- $S(\alpha) = \alpha \cup \{\alpha\}$（$= \alpha+1$）
  $S(\alpha)$ の形でない順序数を極限順序数という.
- $\alpha+\beta$ = α と β を繋げて定められる順序数
- $\alpha \cdot \beta$ = α と β の直積集合で定められる順序数
- $\sup X = \cup X$
- $\alpha^1=\alpha$,　$\alpha^{\beta+1}=\alpha^\beta \cdot \alpha$
- $\alpha^\beta = \sup\{\alpha^\xi : \xi<\beta\}$（ただし α が極限順序数のとき）

計算例

- $\omega+1 \neq \omega$,　$1+\omega=\omega$,　$\omega \cdot 2=\omega+\omega$,　$2 \cdot \omega=\omega$
- $\omega^2=\omega \cdot \omega$,　$2^\omega=\omega$
- $\omega^\alpha=\alpha$ となる α（ε 数）が存在.

ε_0

自然数の10進数展開

m を 0 でない自然数とする．このとき，

- $a(1) \geq a(2) \geq \cdots \geq a(n)$
- $n = 10^{a(1)} + 10^{a(2)} + \cdots + 10^{a(n)}$

を満たす自然数 n と自然数列 a(1), …, a(n) が存在．

例：$m = 2018$ とする．$m = 2 \cdot 10^3 + 1 \cdot 10^1 + 8 \cdot 10^0$ なので，
3, 3, 1, 0, 0, 0, 0, 0, 0, 0, 0 が条件を満たす自然数列．

10進数展開に基づく自然数の定義

- 0 は自然数
- a が自然数のとき，10^a は自然数
- a(1), …, a(n) が 自然数のとき，$a(1) + \cdots + a(n)$ は自然数

ε_0

最小のε数

- 最小の ε 数を ε_0 と書く．　$\varepsilon_0 = \omega^{\omega^{\omega^{\cdot^{\cdot^{\cdot}}}}}$
- 以下，順序数は全て ε_0 未満の順序数とする．

順序数のω進数展開：カントール標準形

μ を 0 でない順序数とする．このとき，

- $\mu(1) \geq \mu(2) \geq \cdots \geq \mu(n)$
- $\mu = \omega^{\mu(1)} + \omega^{\mu(2)} + \cdots + \omega^{\mu(n)}$

を満たす自然数 n と順序数列 $\mu(1), \cdots, \mu(n)$ が一意的に存在．

カントール標準形に基づく順序数の定義

- 0 は順序数
- μ が順序数のとき，ω^{μ} は順序数
- $\mu(1), \cdots, \mu(n)$ が順序数のとき，$\mu(1) + \cdots + \mu(n)$ は順序数

ε_0

比べる.

10進数展開に基づく自然数の定義

- 0 は自然数
- a が自然数のとき，10^a は自然数
- a(1), …, a(n) が 自然数のとき，　a(1)+ … +a(n) は自然数

カントール標準形に基づく順序数の定義

- 0 は順序数
- μ が順序数のとき，ω^μ は順序数
- $\mu(1)$, …, $\mu(n)$ が順序数のとき，$\mu(1)+ \cdots +\mu(n)$ は順序数

10 も ω も「記号」でしかなく，二つの定義に違いはない.
違うのは「記法」ではなく「構造（演算）」.
どのように構造が定義されるのか（原始再帰的？）が大切.

ε_0

冪の繰り返し

α を順序数，n を自然数とする．$\omega_n(\alpha)$ を以下のように定める．

- $\omega_0(\alpha) = \alpha$
- $\omega_{n+1}(\alpha) = \omega^{\omega_n(\alpha)}$

自然和

$\mu = \omega^{\mu(1)} + \cdots + \omega^{\mu(m)}$，　$\nu = \omega^{\nu(1)} + \omega^{\nu(2)} + \cdots + \omega^{\nu(n)}$
をカントール標準形の順序数とする．

- $\lambda(1), \cdots\cdots, \lambda(m+n)$：
  $\mu(1), \cdots, \mu(m), \nu(1), \cdots, \nu(n)$ を大きい順に並べたもの
- $\mu\#\nu = \omega^{\lambda(1)} + \cdots + \omega^{\lambda(m+n)}$

と定め，$\mu\#\nu$ を μ と ν の自然和という．

注意：$\mu\#\nu = \nu\#\mu$

ゲンツェンの証明

目標

- PA の無矛盾性を示したい.
- LK の場合は grade と rank の二重帰納法.
  つまり，$\omega\cdot\omega$ までの超限帰納法.
- PA の場合は ε_0 までの超限帰納法.

数学帰納法

A(x) を L の論理式とする.

- 帰納法の公理：$A(0)\wedge\forall x(A(x)\rightarrow A(x+1))\rightarrow\forall xA(x)$
- 帰納法の規則：
$$\frac{A(x),\ \Gamma\vdash\Delta,\ A(x+1)}{A(0),\ \Gamma\vdash\Delta,\ A(t)}$$
  ただし x は Γ, Δ, A(0) の自由変数ではない.
  （A(0) と $A(x)\vdash A(x+1)$ から A(t) が導かれる）
- PA*：PA の帰納法の公理を帰納法の規則で置き換える.

ゲンツェンの証明

帰納法と cut

- PA = PA*（一般に規則は公理より弱いが，帰納法は大丈夫）
- 結論が具体的な自然数を表す項の場合は，
  帰納法の規則は cut で書き換えられる．

例：t = 3 の場合

$$\frac{A(x) \vdash A(x+1)}{A(0) \vdash A(3)}$$

⇨

$$\frac{\dfrac{A(0) \vdash A(1) \qquad A(1) \vdash A(2)}{A(0) \vdash A(2)} \qquad A(2) \vdash A(3)}{A(0) \vdash A(3)}$$

- cut が取れれば帰納法も消せる．

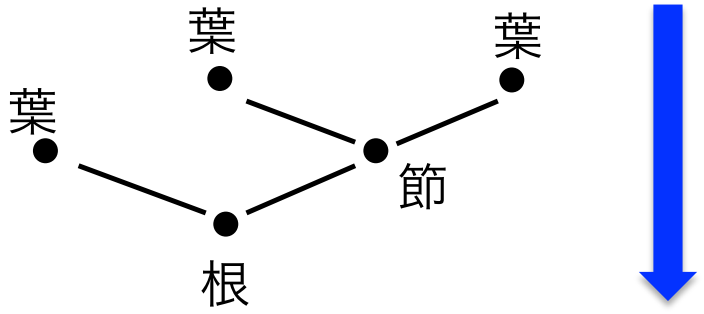
ゲンツェンの証明

無矛盾性証明の粗筋

PA* から　⊢　が証明できないことを示したい.

1. 全ての証明 P に順序数 o(P) を対応させる.
2. 　⊢　の証明 P を o(P)>o(Q) を満たす　⊢　の証明 Q に書き換える計算手順を与える.
3. 　⊢　の証明が一つでもあれば, 順序数の無限下降列が存在することになり矛盾.

証明の木構造



上から下に順序数を貼り付ける

ゲンツェンの証明

順序数の貼り付け

証明 P のシーケント S に順序数 o(S) を割り当てる．S が：

- 始式のとき，o(S)=1
- cut 以外の構造規則の下式で，上式の順序数が μ のとき，o(S)=μ
- 上式が 一つの論理規則の下式で，上式の順序数が μ のとき，o(S)=μ+1
- 上式二つの論理規則の下式で，上式の順序数が μ, νのとき，o(S)=$\mu \# \nu$
- cut の下式で，上式の順序数が μ, ν のとき，o(S)=$\omega_{m-n}(\mu \# \nu)$
- 帰納法の下式で，上式の順序数が μ，$\mu = \omega^{\mu(1)} + \cdots + \omega^{\mu(m)}$ のとき，o(S) = $\omega_{m-n+1}(\mu_1+1)$

P の終式を S とするとき，o(P) = o(S).

ゲンツェンの証明

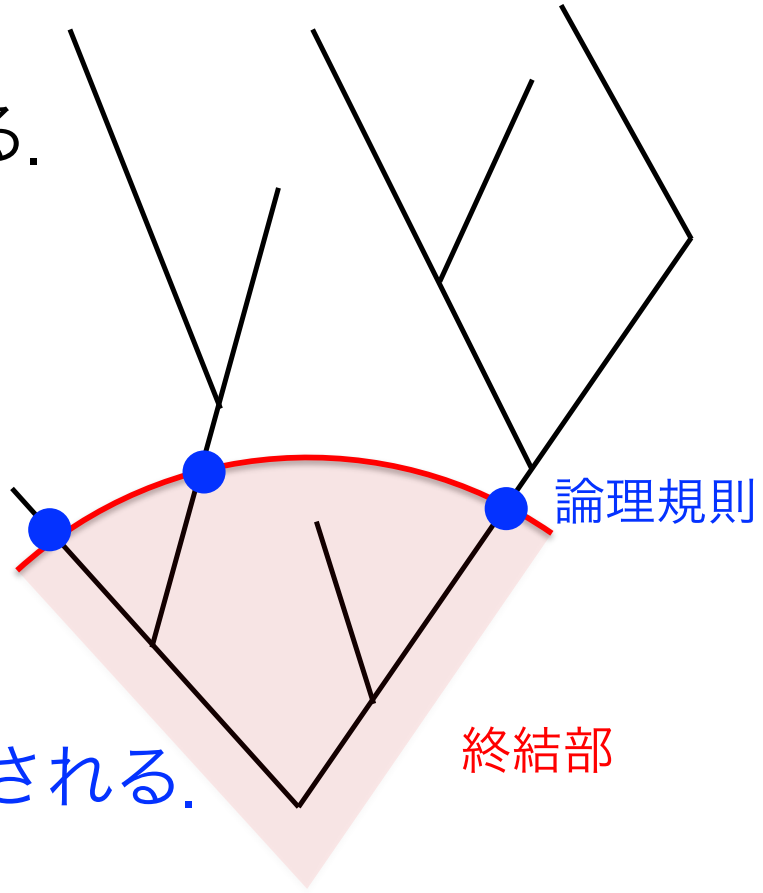
終結部

- $\vdash$ の証明を下から辿る．論理規則の下式までが終結部

$\vdash$ の証明の終結部を書き換える

1. 自由変数を含むとき，1 を代入する.
2. 帰納法があれば，
   一番下のを cut に書き換える.
3. Weakening があれば，取り除く.
4. 始式があれば，
   すぐ下に cut があるから取り除く.
5. 終結部に論理記号が現れる.
   その論理記号を含む論理式が cut される.
   その cut を書き換える.

順序数が下がる.



ゲンツェンの証明

参考文献

- G. Takeuti, Proof Theory (2nd edition), Dover, 2013.
- 竹内外史・八杉満利子, 復刊 証明論入門, 共立出版, 2010.
- 上江洲忠弘, 述語論理・入門–基礎からプログラムの理論へ, 遊星社, 2007.
- 小野寛晰, 情報科学における論理, 日本評論社, 1994.