数学基礎論サマースクール2019
選択公理と連続体仮説

導入：完全性定理，不完全性定理，ZFC 集合論

2019年9月3日 静岡大学

菊池 誠（神戸大）

数学基礎論の歴史

19世紀後半

- 実数論の算術化（デデキント，カントール）
- 素朴集合論の誕生と連続体仮説（カントール）
- 証明の形式化（フレーゲ）
- 素朴集合論の逆理

1900年代から1920年代

- ヒルベルトのプログラム
- 選択公理と公理的集合論の構築
- 1階述語論理の誕生

1930年：ゲーデルの完全性定理

- 述語論理の構文論と意味論の調和.
- 述語論理の妥当性の根拠.

数学基礎論の歴史

1931年：ゲーデルの不完全性定理

T：再帰的（何が公理か計算可能）で算術を含む公理系とする.

- T がω無矛盾ならば，T は不完全.
- T が無矛盾ならば，T の無矛盾性は T では証明できない.

1930年代〜40年代

- チューリング機械の誕生と計算論の発生
- ゲンツェンによる算術の無矛盾性の証明
- ゲーデルの構成可能集合の世界

1950年代〜60年代

- ヘンキンによる完全性定理の証明とモデル論の発生
- 竹内の基本予想（解析学の無矛盾性）
- コーエンの強制法（現代的な集合論の完成）

証明の形式化

論理的記号

- 命題結合子：¬ 否定，∧ かつ，∨ または，→ ならば
- 量化子：∀ 全て，∃ 存在
- 等号：=（項数 2 の関係記号），変数：x, y, z, ⋯

非論理的記号

- 関数記号：f(x, y, ⋯), g(x, y, ⋯), ⋯
- 定数記号：a, b, c, ⋯
- 関係記号：P(x, y, ⋯), Q(x, y, ⋯), ⋯

言語

- 非論理的記号の集合を言語という.
- 順序の言語 {<}，群論の言語 { · }，集合論の言語 {∈}, 算術の言語 {+, · , 0, 1, <}

証明の形式化

項

- 変数および定数記号は項
- f が項数 n の関数記号で $t_1, \cdots, t_n$ が項のとき, $f(t_1, \cdots, t_n)$ は項

論理式

- P が項数 n の関係記号で $t_1, \cdots, t_n$ が項のとき, $P(t_1, \cdots, t_n)$ は論理式（原子的論理式）
- A, B が論理式のとき, $\neg A$, $A \wedge B$, $A \vee B$, $A \rightarrow B$ は論理式
- A が論理式で x が変数のとき, $\forall xA$, $\exists xA$ は論理式

束縛変数と自由変数

- 束縛変数：$\forall xA$, $\exists xA$ における A 中の変数 x
- 自由変数：束縛変数でない変数
- 文：自由変数を持たない論理式

証明の形式化

論理的公理

- 論理的記号の意味から正しさが明らかな論理式
  $A\to(A\vee B)$, $(A\wedge B)\to A$ など

推論規則

- 仮定から結論を導く規則

$$\text{MP}\ \frac{A \quad A\to B}{B} \qquad \frac{A \quad B}{A\wedge B} \qquad \text{など}$$

- 横線の上が仮定，下が結論

理論と非論理的公理

- 非論理的公理：非論理的記号の意味を定める仮定
- 理論：非論理的公理の集合
  全順序の理論，群の理論，ZFC 集合論，ペアノ算術など
- T：理論，A：論理式のとき，$T\cup\{A\}$ を T+A と書く．

証明の形式化

注意　MP があれば非論理的推論規則は不要

証明と定理

- 証明：論理的公理と仮定から出発して，推論規則を用いて論理式を書き換えて得られる論理式の列.
- 定理：証明の最後に現れる論理式

証明の例

以下の論理式の列は，　MP を推論規則，
{A, B, A→(B→C)} を仮定の集合とする C の証明.

1. A→(B→C)　（仮定）
2. A　（仮定）
3. B→C　(MP, 1, 2)
4. B　（仮定）
5. C　(MP, 3, 4)

証明の形式化

証明可能性

T を論理式の集合，A を論理式とする．
仮定が T に含まれ，結論が A である証明が存在するとき，
A は T の定理であるといい $T \vdash A$ と書く．

例　$\{A, B, A \to (B \to C)\} \vdash C$

形式的体系

論理的公理と推論規則を定めると形式的体系が定まる．

- ヒルベルト流（フレーゲのものを改変）
- 自然演繹（ゲンツェン他．自然な形式化）
- シーケント計算 LK（ゲンツェン，綺麗な対称性）

ヒルベルト流の形式的体系

論理的公理（有限だが沢山）

- [$\wedge$]
  $A \to (B \to A \wedge B)$,
  $A \wedge B \to A$,
  $A \wedge B \to B$
- [$\vee$]
  $A \to A \vee B$,
  $B \to A \vee B$,
  $(A \to C) \to ((B \to C) \to (A \vee B \to C))$
- [$\to$]
  $A \to (B \to A)$,
  $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$
- [$\neg$]
  $(\neg A \to \neg B) \to (B \to A)$

ヒルベルト流の形式的体系

論理的公理（続き）

- [∀]
  $\forall x A(x) \to A(t)$,
  $\forall x (A^* \to B(x)) \to (A^* \to \forall x B(X))$
- [∃]
  $\forall x (A \to B^*) \to (\exists x A(x) \to B^*)$,
  $A(t) \to \exists x A(x)$

ただし A^*, B^* に x は自由変数としては現れない.

推論規則（二つ）

（分離規則, MP） $\dfrac{A \quad A \to B}{B}$　　（一般化） $\dfrac{A(y)}{\forall x A(x)}$

注意　等号の扱いは今回は省略.

ヒルベルト流の形式的体系

欠点　証明が著しく書きにくい.

演繹定理（証明を書きやすくする）

Tを理論，Ａ を文，Ｂ を論理式とする.

$T \cup \{A\} \vdash B \Leftrightarrow T \vdash A \to B$

自然演繹 NK

- 全て推論規則．演繹定理も推論規則.
- λ計算と対応（Curry-Howard の isomorphism）

(→導入)

$$\dfrac{\begin{matrix}[A]\\ \vdots \\ B\end{matrix}}{A \to B}$$

（演繹定理）

(→除去)

$$\dfrac{A \qquad A \to B}{B}$$

(分離規則）

ヒルベルト流の形式的体系

シーケント計算 LK

- 「NK の証明の構成」は「仮定と結論の組み」の書き換え.

[NK]

$$\dfrac{\begin{array}{c}\Gamma \\ \vdots \\ A\end{array} \quad \begin{array}{c}\Gamma \\ \vdots \\ B\end{array}}{A \land B} \quad \Rightarrow$$

[LK]

$$\dfrac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \land B}$$

シーケント

- ⊢ が左右対称になるように一般化
- $A_1, \cdots, A_n \vdash B_1, \cdots, B_m$: シーケント
- 意味「 $A_1 \land \cdots \land A_n$ ならば $B_1 \lor \cdots \lor B_m$ 」

完全性定理

根本的な問題　論理的公理と推論規則は十分か？

言語 L 構造　L の解釈を伴う集合

意味論 (真理値/構造)

T：理論，A：論理式，M：構造とする．

- 定義：$M \vDash A \Leftrightarrow$ M 上で A が真
- 定義：$M \vDash T$ (M は T のモデル) $\Leftrightarrow B \in T$ ならば $M \vDash B$
- 定義：$T \vDash A \Leftrightarrow$ 全ての構造 M について $M \vDash T$ ならば $M \vDash A$

完全性定理（ゲーデル1930）

T：理論，A：論理式とする．$T \vdash A \Leftrightarrow T \vDash A$

根本的な問題に対する答　論理的公理と推論規則は十分．

完全性定理

定義　T：理論とする.

- T は矛盾する $\Leftrightarrow$ すべての論理式 A について $T \vdash A$
- T は無矛盾である $\Leftrightarrow$ T は矛盾しない
- T は完全 $\Leftrightarrow$ 全ての論理式 A について $T \vdash A$ または $T \vdash \neg A$

注意　Tを理論とする.

- T は矛盾する $\Leftrightarrow$ $T \vdash A$ かつ $T \vdash \neg A$ となる論理式 A が存在
- A を論理式とする. $T \vdash A \Leftrightarrow T + \neg A$ は矛盾する

完全性定理（Another Form）

T：理論とする. T は無矛盾 $\Leftrightarrow$ T はモデルを持つ

系　T：理論，A：論理式とする.

$T \vdash A \Leftrightarrow T + \neg A$ はモデルを持たない.

完全性定理

完全性定理の証明

$T \vdash A$ でない $\Leftrightarrow$ $T + \neg A$ は無矛盾

$\Leftrightarrow$ $T + \neg A$ はモデルを持つ $\Leftrightarrow$ $T \vDash A$ でない

完全性定理（Another Form）の証明

T は無矛盾とする．T はモデルを持つことを示す．

1. 論理式 A(x) 毎に $\exists x A(x) \rightarrow A(c)$ となる新しい定数記号 c を用意し，この論理式を T に付け加えて，T' を作る．
2. T' を無矛盾で完全な理論 T'' に拡張する．
3. 「新しい定数記号の全体」からなる集合に構造を定めて，T'' のモデルにする．
4. そのモデルが T のモデルになる．□

レーベンハイム-スコーレムの定理

- T はモデルを持てば，可算濃度のモデルを持つ．

不完全性定理

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] でない．
- [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）

同型なものを同一視すれば，単純無限列は唯一．

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．

不完全性定理

<u>ペアノ算術</u>

以下の非論理的公理からなる算術の言語 {+, · , 0, 1, <} の理論をペアノ算術 PA という.

[和積]

- $(x+y)+z=x+(y+z)$, $x+y=y+x$, $x+0=x$
- $(x\cdot y)\cdot z=x\cdot(y\cdot z)$, $x\cdot y=y\cdot x$, $x\cdot 0=0$, $x\cdot 1=x$, $x\cdot(y+z)=x\cdot y+x\cdot z$

[順序]

- $x<y\wedge y<z\rightarrow x<z$, $\neg x<x$, $x<y\vee x=y\vee y<x$
- $x<y\rightarrow x+z<y+z$, $0<x\wedge x<y\rightarrow x\cdot z<y\cdot z$, $x<y\rightarrow\exists z(x+z=y)$
- $0<1$, $0<x\rightarrow 1=x\vee 1<x$

[数学的帰納法] A(x) を L の論理式とする.

- $A(0)\wedge\forall x(A(x)\rightarrow A(x+1))\rightarrow\forall xA(x)$

<u>注意</u>　数学的帰納法の適用範囲には制限がある.

不完全性定理

表現可能性

- $f(x)$ を再帰的 (＝計算可能) な関数とすると,
  $f(m)=n \Leftrightarrow PA \vdash A(m, n)$ となる論理式 $A(x, y)$ が存在.
- 注意： $PA \vdash \forall x \exists y\, A(x, y)$ とは限らない.
- T の無矛盾性を表す論理式 Con(T) が存在

ω無矛盾性

T を $PA \subseteq T$ である L の理論とする.

- T がω無矛盾 $\Leftrightarrow$ L のどのような論理式 $A(x)$ についても,
  $T \vdash A(0), T \vdash A(1), \cdots$ ならば $T \vdash \exists x \neg A(x)$ でない.

不完全性定理（ゲーデル1931）

T を再帰的で $PA \subseteq T$ である L の理論とする.

- 第一不完全性定理　T はω無矛盾なら不完全.
- 第二不完全性定理　T が無矛盾なら $T \vdash Con(T)$ でない.

ZFC 集合論

集合という見方

- 関数 f: A→B とは集合 $\{(a, b)\in A\times B : f(a) = b\}$ のこと.
- 順序対 (a, b) とは集合 $\{\{a\}, \{a, b\}\}$ のこと.
- 自然数 0, 1, 2, ⋯ とは集合 $\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}$ のこと.
- 全ては集合

素朴集合論

- 外延性公理：$\forall xy(x=y \leftrightarrow \forall v(v\in x \leftrightarrow v\in y))$
- 内包公理： $P(v, w_1, \cdots, w_n)$ を確定的性質とすると，すべての $y_1, \cdots, y_n$ について，集合 $\{v : P(v, y_1, \cdots, y_n)\}$ が存在.

提唱　確定的性質＝論理式で書ける

ZFC 集合論

ラッセルの逆理

- $\neg v \in v$ に内包公理を適用すると，
  $\forall v (v \in R \leftrightarrow \neg v \in v)$ を満たす集合 R が存在.
- $R \in R$ としても，$\neg R \in R$ としても矛盾.

ラッセルの分岐型理論　S を集合とする.

- 型：S, S の冪集合 P(S), P(S) の冪集合 P(P(S)), … の区別.
- 階：S を用いて定義可能な S の部分集合，それを用いて定義可能な S の部分集合, … の区別.
- 還元性公理「後で定義されるものは，前から入っている」
- そもそも $v \in v$ は不適切な表現.

ZFC 集合論

ZFC 集合論

以下の非論理的公理からなる集合論の言語 $\{\in\}$ の理論を選択公理を持つツェルメロ-フレンケル集合論 ZFC とう.

- 外延性公理：$\forall xy(x=y \leftrightarrow \forall v(v\in x \leftrightarrow v\in y))$
- 分出公理図式：$P(v, w_1, \cdots, w_n)$ を論理式とする． すべての $x, y_1, \cdots, y_n$ について， 集合 $\{v\in x : P(v, y_1, \cdots, y_n)\}$ が存在.
- 対公理：$\forall x\forall y$(集合 $\{x, y\}$ が存在)
- 和集合公理：$\forall x$(集合 $\cup x$ が存在)
- 冪集合公理：$\forall x$(集合 $P(x)$ が存在)
- 置換公理図式：集合の「関数」の像は集合として存在
- 無限公理：無限集合が存在
- 基礎公理：$\in$ の無限下降列は「存在しない」
- 選択公理：$\forall x(f(u)\in u$ を満たす $x-\{\emptyset\}$ 上の関数 f が存在)

ZFC 集合論

記号の導入

集合論の言語 $\{\in\}$ に

- 定数記号：$\varnothing$ 空集合，ω 自然数全体の集合
- 関数記号：$\cup x$ 和集合，$P(x)$ 冪集合

などを追加しても大丈夫.

スコーレムの逆理

- ZFC で $P(\omega)$ は非可算無限集合
- ZFC は無矛盾なら可算モデル M を持ち，$P(\omega) \in M$.
- M：二項関係「$\in$」が定まった「点」の集まり
- $\{a \in M : M \vDash a \in P(\omega)\}$ は可算無限集合であるが，この集合と ω を結ぶ全単射は M には入っていない.

ZFC 集合論

ZFC 上の独立性証明

- 経験的事実「数学的に証明可能 = ZFC で証明可能 」
- 「ZFC $\vdash$ A でない」を証明したい．しかし証明できたら，
- ZFC 上で ZFC + ¬A の無矛盾性が証明できることになり，
- ZFC が無矛盾であれば，第二不完全性定理に反する．

二つの可能性

[1]　ZFC + A $\vdash$ Con(ZFC)

[2]　ZFC $\vdash$ Con(ZFC) $\rightarrow$ Con(ZFC + ¬A)

- [1] が成り立ち，ZFC が無矛盾なら，ZFC $\vdash$ A でない．
- その議論が ZFC で形式化できれば，[2] が得られる．

読書案内

初めて述語論理を学ぶ人のために

- Enderton, H.B., A Mathematical Introduction to Logic (2nd ed.), Academic Press, 2000.
- van Dalen, D., Logic and Structure (5th ed.), Springer, 2012.

数学基礎論を包括的に学ぶために

- Shoenfield, J.R., Mathematical Logic, Routledge, 2001.

その他「雑談」に関して

- 菊池誠, 不完全性定理, 共立出版, 2014.
- 菊池誠, 数と論理の物語 – 不完全性定理について考えるための10の定理, 数学セミナー, 2019年4月号から連載中.