第四回関西すうがく徒のつどい

代数学における選択公理

@alg_d　http://alg-d.com/math/ac/

2013 年 9 月 21 日

※ この PDF は第四回関西すうがく徒のつどいにて発表する予定の内容を書いたものです．大体この内容の通りに話すと思いますが，多少は変わる可能性もあります．

代数学において，選択公理は無くてはならないものである．これは良く知られている事実です．何故ならば「環の極大イデアルが存在する」「線型空間の基底が存在する」という，選択公理と同値な有名な定理があるからです．しかし，代数学にはまだまだ選択公理に関するヤバい事実が存在するのです．本講演では以下の論文の解説を行います．これらは「代数学における選択公理」に関するヤバい論文トップ 3(と勝手に私が思っているもの) です．

[1] W. Hodges, Six Impossible Rings
[2] A. Blass, Injectivity, projectivity, and the axiom of choice
[3] W. Hodges, Läuchli's algebraic closure of Q

1 Six Impossible Rings

ZFC では存在できないとよく知られている環を 6 つ《構成》したという論文である．(正確に言えば，そのような環が存在する ZF のモデルを構成したということ．) 以下，環とは単位元を持つ可換環を指す．

定理. ZF では以下のような環が存在しうる．

(1) 極大イデアルを持たない整域で，任意のイデアルが有限生成となるもの．
(2) 原子を持たないブール環で，任意のイデアルが単項イデアルであり，イデアルの無限降下列を持たないもの．
(3) 原子的な無限ブール環で，真のイデアルは極大イデアルの共通部分で書けて，イデアルの無限降下列・無限上昇列を持たないもの．
(4) 局所環で，イデアルの非空集合は極小元を持ち，イデアルの無限上昇列が存在するもの．
(5) イデアルの無限降下列・無限上昇列を持たない局所環 $(R, \mathfrak{m})$ で，以下を満たす．
  - $\mathfrak{m}$ は nil イデアルかつ冪等イデアル．
  - $\mathfrak{m}$ は有限生成でない．
  - $\mathfrak{m}$ は R の唯一つの素イデアル．
(6) 整域 R と非零元 $x \in R$ で素イデアル $\mathfrak{p} \supset (x)$ が存在し極小素イデアル $\mathfrak{q} \supset (x)$ が存在しないもの □

定義. $\mathrm{N}_{\max}$：R のイデアルの非空集合は極大元をもつ (極大条件)

$\mathrm{N_{fin}}$：R の任意のイデアルは有限生成である
$\mathrm{N_{acc}}$：R のイデアルの上昇列が必ず有限で止まる (昇鎖条件)
C：R の任意の素イデアルは有限生成である
$\mathrm{A_{min}}$：R のイデアルの非空集合は極小元をもつ (極小条件)
$\mathrm{A_{dcc}}$：R のイデアルの降下列が必ず有限で止まる (降鎖条件)
D：R のイデアルは準素分解を持つ
nil：R の nil イデアルは冪零イデアル
M：R の極小素イデアルはある非零元 $x \in R$ の annihilator

定理. 環 R に関する以下のよく知られている定理は ZF で証明できない.

- $\mathrm{A_{dcc}} \Longrightarrow \mathrm{A_{min}}$
- $\mathrm{A_{min}} \Longrightarrow \mathrm{N_{acc}}$，即ち「Artin 環は Noeher 環」
- $\mathrm{N_{acc}} \Longrightarrow \mathrm{N_{fin}}$
- $\mathrm{N_{fin}} \Longrightarrow \mathrm{N_{max}}$
- $\mathrm{C} \Longrightarrow \mathrm{N_{max}}$
- $\mathrm{N_{fin}} \Longrightarrow \mathrm{D}$
- $\mathrm{N_{acc}} \Longrightarrow \mathrm{nil}$
- $\mathrm{N_{acc}} \Longrightarrow \mathrm{M}$

$$\begin{tikzcd}
\mathrm{D} & \mathrm{N_{max}} \arrow[d, shift right] & \\
\mathrm{A_{min}} \arrow[d, shift right] \arrow[dr, dashed] & \mathrm{N_{fin}} \arrow[ul, dashed] \arrow[u, dashed, shift right] \arrow[r] \arrow[d, shift right] & \mathrm{C} \arrow[dl, dashed] \\
\mathrm{A_{dcc}} \arrow[u, dashed, shift right] & \mathrm{N_{acc}} \arrow[u, dashed, shift right] \arrow[d, dashed] \arrow[dr, dashed] & \\
 & \mathrm{nil} & \mathrm{M}
\end{tikzcd}$$

※ 実は $\mathrm{C} \Longrightarrow \mathrm{N_{max}}$ より強い $\mathrm{C} \Longrightarrow \mathrm{N_{acc}}$ が ZF + DC で証明できないことが知られている.

証明. ($\mathrm{A_{dcc}} \Longrightarrow \mathrm{A_{min}}$) 環 2 による．原子を持たないブール環の，零でないイデアル全体がなす集合は極小元を持たない.

($\mathrm{A_{min}} \Longrightarrow \mathrm{N_{acc}}$) 環 4 による.

($\mathrm{N_{acc}} \Longrightarrow \mathrm{N_{fin}}$) 環 5 による.

($\mathrm{N_{fin}} \Longrightarrow \mathrm{N_{max}}$) 環 1 による.

($\mathrm{C} \Longrightarrow \mathrm{N_{acc}}$) 冪集合代数 $\mathcal{P}(\omega)$ の任意の素イデアルが単項イデアルとなるような ZF + DC のモデルが存在する．即ち $\mathcal{P}(\omega)$ は C を満たす．明らかに $\mathcal{P}_{\mathrm{fin}}(\omega) \subset \mathcal{P}(\omega)$ は有限生成でないイデアルだから，この $\mathcal{P}(\omega)$ は $\mathrm{N_{fin}}$ をみたさない．ところで ZF + DC では $\mathrm{N_{acc}} \Longrightarrow \mathrm{N_{fin}}$ であるから，$\mathcal{P}(\omega)$ は $\mathrm{N_{acc}}$ も満たさない.

($\mathrm{N_{fin}} \Longrightarrow \mathrm{D}$) 環 2 による．ブール環において，準素イデアルは極大イデアルである．一

方 atomless なブール環の単項イデアルは極大でない．故に環 2 には準素イデアルは存在せず，D も成り立たない．

($N_{acc} \Longrightarrow$ nil) 環 5 による．

($N_{acc} \Longrightarrow$ M) 環 3 による．略． $\square$

2 Injectivity, projectivity, and the axiom of choice

定義. アーベル群 G が入射的

$\Longleftrightarrow$ 任意の単射準同型 $f\colon A \longrightarrow B$ と任意の準同型 $g\colon A \longrightarrow G$ に対し，ある準同型 $h\colon B \longrightarrow G$ が存在して $g = h \circ f$ となる．

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "f"] \arrow[d, "g"'] & B \arrow[dl, dashed, "h"] \\ & G & \end{tikzcd}$$

命題 (EI($\mathbf{Ab}$))**.** 任意のアーベル群 A に対し, ある入射的アーベル群 B と単射 $f\colon A \longrightarrow B$ が存在する．

EI($\mathbf{Ab}$) の証明は

(1) 任意のアーベル群 A に対し，可除アーベル群 B と単射準同型 $f\colon A \longrightarrow B$ が存在する．

(2) 可除アーベル群は入射的

という手順で与えられる．

※ アーベル群 G が可除 $\Longleftrightarrow$ 任意の $x \in G$ が可除元.
$x \in G$ が可除元 $\Longleftrightarrow$ 任意の $n \in \mathbb{Z} \setminus \{0\}$ に対してある $y \in G$ が存在して $x = ny$ と書ける．

(1) の証明は選択公理を使わずに (ZF で) できる．問題は (2) である．

定理. 次の命題は (ZF 上) 同値

(1) 選択公理

(2) 任意の可除アーベル群は入射的

では，選択公理を使わずに EI($\mathbf{Ab}$) を証明できるであろうか，というと次の恐ろしい定理が証明できる．

定理. 「injective な非自明アーベル群の存在」は ZF では証明できない．故に EI($\mathbf{Ab}$) も

ZF では証明できない. $\square$

3 Läuchli's algebraic closure of Q

命題. 任意の体 k に対し代数閉包 $\overline{k}/k$ が一意に存在する.

この命題は ZF では証明できないことが知られている. 但し, 体 k の濃度を可算に制限すれば, 代数閉包の「存在」は ZF で証明できる.

一方一意性は可算であっても証明できないのであるが, 更に ZF では $\mathrm{Gal}(\overline{k}/k) \neq 1$ や $\overline{k}$ の非自明絶対値の存在が証明できないことが知られているのである.

定理. ZF において, 次のような代数閉包 $L/\mathbb{Q}$ が存在し得る.
L 上の任意の関係 R は support を持つ. $\square$

> ※ $S \subset L$ が R の support
> $\Longleftrightarrow$ S が有限集合で, 自己同型 $\sigma\colon L \longrightarrow L$ が「任意の $x \in S$ に対して $\sigma(x) = x$」を満たすならば $\sigma(R) = R$ である.

以下, このような L を取り固定する.

定理. (1) L の非自明絶対値は存在しない.
(2) $\mathrm{Gal}(L/\mathbb{Q}) = 1$ $\square$

系. 以下のよく知られている定理は ZF で証明できない.

(1) 代数閉包 $\overline{\mathbb{Q}}/\mathbb{Q}$ の非自明絶対値が存在する
(2) 代数閉包 $\overline{\mathbb{Q}}/\mathbb{Q}$ に対して $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \neq 1$ $\square$

ところで,「単項イデアル整域ならば一意分解聖域」の証明は選択公理を使っている, という Twitter で稀によく話題になる事実があるが, この証明で選択公理が要ることが以下のようにして分かる.

定理. ZF では「体でない単項イデアル整域で, 素元を持たないもの」が存在し得る.

> ※ 代数体 $K/\mathbb{Q}$ に対して, 絶対類体と呼ばれる代数体 H/K が一意に存在する. H/K は最大不分岐アーベル拡大である. H/K は以下を満たす.

単項化定理　K のイデアルを H へ延長すれば単項イデアルとなる　$\square$

分解定理　K の素イデアル $\mathfrak{p}$ は H/K で完全分解する $\Longleftrightarrow$ $\mathfrak{p}$ は単項イデアル　$\square$

$K_0/\mathbb{Q}$ を代数体として，K_{n+1} を K_n の絶対類体とすれば代数体の上昇列 $K_0 \subset K_1 \subset K_2 \subset \cdots$ が得られる．これを類体塔という．「任意の n について $K_n \subsetneq K_{n+1}$ となるような代数体 K_0 は存在するか?」という問題を類体塔問題という．

Golod-Shafarevich の定理 (1964)
類体塔の長さが無限となる代数体 K_0 が存在する．　$\square$

例えば $K_0 = \mathbb{Q}(\sqrt{-5 \cdot 11 \cdot 461})$ ならよい．

証明. $K_0 \subset L$ を Golod-Shafarevich の定理を満たす代数体とする．K_{n+1}/K_n を K_n の絶対類体，$\mathcal{O}_n \subset K_n$ を整数環とする．$K := \bigcup_{n \in \mathbb{N}} K_n$，$\mathcal{O} := \bigcup_{n \in \mathbb{N}} \mathcal{O}_n$ と定める．R を K 上の関係とすれば，R は support $S \subset \mathcal{O}$ を持つことが分かる．この $\mathcal{O}$ は (体でない) 単項イデアル整域である．

$\because$) $I \subset \mathcal{O}$ をイデアルとすれば，一項関係 I は support $S \subset \mathcal{O}$ を持つ．S は有限集合だから，ある番号 n が存在して $S \subset \mathcal{O}_n$ となる．このとき $I = \mathcal{O}(I \cap \mathcal{O}_{n+1})$ が分かる．単項化定理により $\mathcal{O}_{n+2}(I \cap \mathcal{O}_{n+1}) \subset \mathcal{O}_{n+2}$ は単項イデアルである．それを $x\mathcal{O}_{n+2}$ と書けば

$$I = \mathcal{O}(I \cap \mathcal{O}_{n+1}) = \mathcal{O}\mathcal{O}_{n+2}(I \cap \mathcal{O}_{n+1}) = \mathcal{O}(x\mathcal{O}_{n+2}) = x\mathcal{O}$$

となり $I \subset \mathcal{O}$ は単項イデアルである．

$\mathcal{O}$ は素元を持たない．

$\because$) $p \in \mathcal{O}$ を素元とする．ある番号 n が存在して $p \in \mathcal{O}_n$ である．$(p) = p\mathcal{O}_n$ は素イデアルである．類体論により (p) は K_{n+1} で完全分解する．即ち素イデアル $\mathfrak{p}_i \subset \mathcal{O}_{n+1}$ が存在して $(p) = \mathfrak{p}_1 \ldots \mathfrak{p}_s$ $(s = [K_{n+1} : K_n] > 1)$ となる．$x_i \in \mathfrak{p}_i \setminus (p)$ を取れば $p \mid x_1 \ldots x_s$ かつ $p \nmid x_i$ である．故に p は素元でなく矛盾する．

$\square$

系. 以下のよく知られている定理は ZF で証明できない．

(1) 単項イデアル整域は一意分解整域である．

(2) 単項イデアル整域は極大イデアルを持つ． $\square$

ところで，「可算な体の代数閉包の一意性」が ZF で証明できないことは次の命題から分かる．

命題. 代数閉包 $\overline{\mathbb{Q}}/\mathbb{Q}$ が一意に存在する
$\Longrightarrow$ 二元集合の族 $\{X_n\}_{n=0}^{\infty}$ は選択関数を持つ

証明. まず準備として，p_n を n 番目の素数とする ($p_0 = 2,\ p_1 = 3, \cdots$)．可算個の不定元を持つ多項式環 $R := \mathbb{Q}[x_0, x_1, \cdots]$ を考える．$I \subset R$ を $\{x_n^2 - p_n \mid n \in \mathbb{N}\}$ で生成されるイデアルとすれば，$I \subset R$ は極大イデアルである．よって $K := R/I$ は $\mathbb{Q}$ の代数拡大体となる．K の代数閉包 $\overline{K}/K$ は勿論 $\mathbb{Q}$ の代数閉包でもあるから仮定より $\overline{K} \cong \overline{\mathbb{Q}}$.

さて $\{X_n\}_{n=0}^{\infty}$ を二元集合の族とする．各 X_n は互いに素としてよい．$X := \bigcup_{n=0}^{\infty} X_n$ と置いて多項式環 $\mathbb{Q}[X]$ を考える．$f_n, g_n \in \mathbb{Q}[X]$ を

$$f_n := \sum_{x \in X_n} x, \quad g_n := \prod_{x \in X_n} x + p_n$$

で定める．$J \subset \mathbb{Q}[X]$ を $\{f_n \mid n \in \mathbb{N}\} \cup \{g_n \mid n \in \mathbb{N}\}$ で生成されるイデアルすれば $J \subset \mathbb{Q}[x]$ は極大イデアルである．よって $L := \mathbb{Q}[X]/J$ は $\mathbb{Q}$ の代数拡大体となり，先ほどと同様に $\overline{L} \cong \overline{\mathbb{Q}}$ である．故に $\overline{L} \cong \overline{K}$ だから，同型写像 $\varphi\colon \overline{L} \longrightarrow \overline{K}$ が存在する．任意の $x \in X$ を取る．ある $n \in \mathbb{N}$ が存在して $x \in X_n$ である．$|X_n| = 2$ だから $X_n = \{x, y\}$ と書くと $x + y \in J,\ xy + p_n \in J$ であり

$$(x + J)^2 = x^2 + J = -xy + J = p_n + J$$

だから $\varphi((x + J)^2) = \varphi(p_n + J) = p_n + I = x_n^2 + I$ より $\varphi(x + J) = \pm x_n + I$ でなければならない．このとき勿論 $\varphi(y + J) = \mp x_n + I$ である．従って各 $n \in \mathbb{N}$ に対し，ある $x \in X_n$ が一意に存在して $\varphi(x + J) = x_n + I$ となる．そこで

$$f(n) := (\varphi(x + J) = x_n + I \text{ となる } x \in X_n)$$

とすれば $f : \mathbb{N} \longrightarrow X$ が選択関数である． $\square$

参考文献

[1] Wilfrid Hodges, "Six Impossible Rings," Journal of Algebra 31 (1974), 218–244, `http://www.sciencedirect.com/science/article/pii/0021869374900659`

[2] Andreas Blass, "Injectivity, projectivity, and the axiom of choice," Trans. Amer. Math. Soc. 255 (1979), 31–59
`http://www.ams.org/journals/tran/1979-255-00/S0002-9947-1979-0542870-6/home.html`

[3] Wilfrid Hodges, "Läuchli's algebraic closure of Q," Math. Proc. Camb. Phil. Soc. 79 (1976), 289–297

[4] Läuchli, "Auswahlaxiom in der Algebra," Comment. Math. Helv. 37 (1969), 388–394