2025年度春夏学期 大阪大学 理学部数学科
幾何学基礎1演義 演習問題(応用問題)

岩井雅崇 (大阪大学)

April 13, 2025 ver 1.00

Contents

1　集合と集合の演算・集合の直積・写像 (応用問題)

問 1.1 (ラッセルのパラドックス)

$$V = \{X | X \text{ は集合 }\} \quad M := \{X \in V | X \notin X\}$$

とおく. M, V は集合ではないことを示せ. つまり”集合の集合”は集合ではない.

問 1.2 *〜**(公理的集合論) 上の問題より集合を”ものの集まり”として定義するのは良くないことがわかる. 今日では ZF (ツェルメロ=フレンケル) 公理系という 8 つの公理によって, 集合の定義や空集合・和集合などの存在を保証している. (8 つの公理に関しては [田中] 参照)
ZF 公理系の一つに正則性公理がある. これは「空でない集合は必ず自分自身と交わらない要素を持つ」ことを要請するものである. 正則性公理を論理式で書くならば,

$$\forall A(A \neq \varnothing \to \exists x \in A, \forall t \in A(t \notin x)).$$

である. 任意の集合 A について $A \notin A$ であることを正則性公理を用いて示せ. また公理的集合論において集合の集合 $V = \{X | X \text{ は集合 }\}$ は集合ではないことを示せ. [1]

問 1.3 集合 A, B について, 対称差

$$A \circ B := (A \setminus B) \cup (B \setminus A)$$

と定義する. 次の問いに答えよ. ただし板書で解答する際はある程度省略して書いて良い.(”以下同様”などで議論を省略して良い.)

(1). $A \circ B = B \circ A$ を示せ.
(2). $(A \circ B) \circ C = A \circ (B \circ C)$ を示せ.
(3). $A \circ A = \varnothing$, $A \circ \varnothing = A$ をそれぞれ示せ.
(4). A, B を任意に与えたとき, $A \circ X = B$ となる集合 X がただ一つ存在することを示せ.

問 1.4 集合 L と L 上の二項演算[2] 結び $\vee$ と交わり $\wedge$ の組 $(L, \vee, \wedge)$ が次を満たすとき, 束 (lattice)と言う.

- (ベキ等律): $x \wedge x = x$, $x \vee x = x$
- (交換則): $x \wedge y = y \wedge x$, $x \vee y = y \vee x$
- (結合則): $(x \wedge y) \wedge z = x \wedge (y \wedge z)$, $(x \vee y) \vee z = x \vee (y \vee z)$
- (吸収則): $(x \wedge y) \vee x = x$, $(x \vee y) \wedge x = x$

さらに (分配則): $(x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z), (x \wedge y) \vee z = (x \vee z) \wedge (y \vee z)$ を満たすとき, $(L, \vee, \wedge)$ を分配束と呼ぶ
また L の特別な元 $0, 1$ と単項演算[3] $\neg$ について (補元則)

$$x \vee \neg x = 1 \quad x \wedge \neg x = 0$$

が成り立つとき, 組 $(L, \vee, \wedge, \neg, 0, 1)$ を ブール束 (ブール代数, 可補分配束)と呼ぶ.
任意の集合 X についてその冪集合 $\mathfrak{P}(X)$ はブール束 (ブール代数) の構造を持つことを示せ. ただし板書で解答する際はある程度省略して書いて良い.(”以下同様”などで議論を省略して良い.)

---

[1] V はクラスというものになる.
[2] 二項演算とは写像 $\mu : L \times L \to L$ のこと.
[3] 単行演算とは写像 $\neg : L \to L$ のこと

問 1.5 集合 R 上の 2 つの二項演算 $(+,\cdot)$ を持つ代数系 $(R,+,\cdot)$ が(単位的) 環 (ring with unit)であるとは、以下の条件を満たすことをいう。

(a). (加法の結合法則): 任意の $a,b,c \in R$ について $(a+b)+c = a+(b+c)$.
(b). (加法の可換法則): 任意の $a,b \in R$ について $a+b = b+a$.
(c). (加法単位元の存在): ある $0_R \in R$ があって, 任意の $a \in R$ について $0_R + a = a + 0_R = a$.
(d). (加法の逆元の存在): 任意の $a \in R$ について, $a+(-a) = (-a)+a = 0$ となる $-a \in R$ が存在する.
(e). (乗法の結合法則): 任意の $a,b,c \in R$ について $(a\cdot b)\cdot c = a\cdot(b\cdot c)$.
(f). (乗法単位元の存在): ある $1_R \in R$ があって, 任意の $a \in R$ について $1_R \cdot a = a \cdot 1_R = a$.
(g). (分配法則): 任意の $a,b,c \in R$ について $a\cdot(b+c) = (a\cdot b)+(a\cdot c)$ かつ $(b+c)\cdot a = (b\cdot a)+(c\cdot a)$.

以下, 環 $(R,+,\cdot)$ について $xy := x\cdot y$ と書くことにする.
さらに, 任意の $x \in X$ について $x^2 = x$ が成り立つとき, 環 $(R,+,\cdot)$ をブール環 (Boolean ring) と呼ぶ.
次の問いに答えよ. ただし板書で解答する際はある程度省略して書いて良い.((a)-(g) の証明を全てする必要はなく, 以下同様などである程度省略して良い.)

(1). $x \in R$ について $2x := x+x$ と定める. $(R,+,\cdot)$ がブール環ならば $2x = 0$ が成り立つことを示せ.
(2). $(R,+,\cdot)$ がブール環ならば, $x,y \in R$ について $xy = yx$ が成り立つことを示せ.
(3). 任意の集合 X についてその冪集合 $\mathfrak{P}(X)$ はブール環の構造を持つことを示せ.

問 1.6 *~** 次の問いに答えよ. ただし板書で解答する際はある程度省略して書いて良い.(”以下同様”などである程度省略して良い.)

(1). ブール束 (ブール代数)$(L,\vee,\wedge,\neg,0,1)$ について, 二項演算 $(+,\cdot)$ を

$$x+y := (x\wedge\neg y)\vee(\neg x\wedge y) \quad x\cdot y := x\wedge y$$

で定めると $(L,+,\cdot)$ はブール環になることを示せ.
(2). 逆にブール環 $(R,+,\cdot)$ について

$$x\wedge y := xy \quad x\vee y := x+y+xy \quad \neg x := 1-x$$

で定めると, $(R;\vee,\wedge,\neg,0_R,1_R)$ はブール束 (ブール代数) となることを示せ. よってブール束 (ブール代数) とブール環は一対一に対応する.

問 1.7 ** 冪集合 $\mathfrak{P}(X)$ と同型でないブール環は存在するか? [4]

[4] 「”ストーンの表現定理”を見る限り存在するだろう」と思ったがわからず, TA さんに質問したら, 具体的な例を教えてくれた.

問 1.8 *(Zagier's one sentence proof) p を 4 で割って 1 余る素数とする. $S = \{(x, y, z) \in \mathbb{N}^3 : x^2+4yz = p\}$ とし $f : S \to S$ を

$$(x, y, z) \mapsto \begin{cases} (x + 2z, z, y - x - z) & x < y - z \text{ のとき} \\ (2y - x, y, x - y + z) & y - z < x < 2y \text{ のとき} \\ (x - 2y, x - y + z, y) & x > 2y \text{ のとき} \end{cases}$$

で定める. 次の問いに答えよ.

(1). S は有限集合であることを示せ.
(2). $f : S \to S$ について, $f((x, y, z)) = (x, y, z)$ となる点はただ一つであることを示せ.
(3). S の元の数 (位数 $|S|$) は奇数であることを示せ.
(4). $\nu : S \to S$ を $\nu((x, y, z)) = (x, z, y)$ とすると, $\nu((x, y, z)) = (x, y, z)$ となる点も存在することを示せ.
(5). 4 で割って 1 余る素数は二つの平方数の和 ($n^2 + m^2$ という形) で表せられることを示せ.

以下の問題は私が最近勉強したことをそのまま出した. なお問題が難易度順に並んでいないため, 「問 1.9 を仮定して問 1.13 を解く」など解答の順番が前後して良い.

問 1.9 *~** 集合 α が次の 2 つを満たすとき, α は順序数 (ordinal number) という.

(a). (推移的) $x \in \alpha$ かつ $y \in x$ ならば, $y \in \alpha$ である.
(b). (全順序性) 任意の $x, y \in \alpha$ について, $x \in y$ または $x = y$ または $y \in x$.

次の問いに答えよ.

(1). $x, y, z \in \alpha$ について, $x \in y$ かつ $y \in z$ ならば, $x \in z$ であることを示せ
(2). (整列性)「任意の空でない部分集合 $S \subset \alpha$ について, ある $a \in S$ があって, 任意の $x \in S$ について, $a \in x$ または $a = x$」であることを示せ.

ただし以後, 順序数に関する問題の解答に関して, 正則性公理 (問 1.2) や次を仮定して良い. (これは正則性公理から導かれ, $\in$ 無限下降列の非存在と呼ばれる.)

集合列 $X_1, X_2, \ldots,$ について $X_1 \ni X_2 \ni \ldots$ となる無限下降列は存在しない.

以上により順序数 α は $\in$ に関して整列順序を持つ. つまり $x, y \in \alpha$ について順序 $x < y$ を $x \in y$ として定めることができる.

問 1.10 *~** α を順序数, $x, y \in \alpha$ とする. 「$x \subset y$」は「$x \in y$ または $x = y$」と同値であることを示せ. よって順序数 α は $\subset$ に関して整列順序を持つ. つまり $x, y \in \alpha$ について順序 $x \leq y$ を $x \subset y$ として定めることができる. (それは問 1.9 の順序と同じである.)

問 1.11 *~**α を順序数とする. 任意の $\beta \in \alpha$ について β もまた順序数であることを示せ. よって $\alpha = \{\beta | \beta$ は順序数かつ $\beta \in \alpha\}$ と書くことができる.

問 1.12 *~** 順序数 α, β について $\alpha \subset \beta$ または $\beta \subset \alpha$ が成り立つことを示せ.

問 1.13 *~** α を順序数とする.

$$\alpha + 1 := \alpha \cup \{\alpha\}$$

と定義する. 次の問いに答えよ.

(1). α を順序数とするとき, $\alpha + 1$ も順序数であることを示せ.
(2). $\alpha \in \beta \in \alpha + 1$ となる順序数 β は存在しないことを示せ. よって $\alpha + 1$ は α の直後順序数となる.

問 1.14 *~** (ブラリ・フォルティのパラドックス)

$$\mathrm{OR} := \{\alpha | \alpha \text{ は順序数 }\}$$

とする. OR について次が成り立つことを示せ.

(a). (推移的) $x \in \mathrm{OR}$ かつ $y \in x$ ならば, $y \in \mathrm{OR}$ である.
(b). (全順序性) 任意の $x, y \in \mathrm{OR}$ について, $x \in y$ または $x = y$ または $y \in x$.
(c). (整列性) 任意の空でない部分"集合"$S \subset \mathrm{OR}$ について, ある $a \in S$ があって, 任意の $x \in S$ について $a \in x$ または $a = x$ である.

また OR は"集合ではない"ことを示せ.

問 1.15 *~** α を順序数とする.

(a). α が後続型順序数 (第一種順序数) とは,「$\alpha = \varnothing$」または「ある順序数 β があって $\alpha = \beta + 1$ となる」こと. ($\beta + 1$ については問 1.13 参照.)
(b). α が極限順序数 (第二種順序数) とは, α が後続型順序数でないこと.
(c). α が自然数とは, α が後続型順序数であり「任意の $s \in \alpha$ について s は後続型順序数となる」こと.

次の問いに答えよ.

(1). 0 という順序数を $0 := \varnothing$ とする. 順序数 1 を $1 := 0 + 1$ と定義し, 順序数 $2, 3$ を $2 := 1 + 1$, $3 := 2 + 1$ と定義する. $1, 2, 3$ をそれぞれ"$\varnothing$"と"$\{$"と"$\}$"のみを用いて表せ.
(2). $1, 2, 3$ は自然数であることを示せ.
(3). $\omega := \{\alpha | \alpha$ は順序数かつ自然数 $\}$ とする. ω は極限順序数であることを示せ. ただし ω が集合になることは認めて良い.[5]

問 1.16 *~** 問 1.15 と同様に, $\omega := \{\alpha | \alpha$ は順序数かつ自然数 $\}$, $0 := \varnothing$ とする. ω は次のペアノの公理を全て満たすことを示せ. [6]

(1). $0 \in \omega$.
(2). $n \in \omega$ ならば $n + 1 \in \omega$. ($n + 1$ の定義は問 1.13 での定義である.)
(3). $n + 1 = 0$ となる $n \in \omega$ は存在しない.
(4). $n, m \in \omega$ かつ $n + 1 = m + 1$ ならば, $n = m$.
(5). $E \subset \omega$ を部分集合とする. $0 \in E$ であり「任意の $e \in E$ について $e + 1 \in E$」であるとする. このとき $E = \omega$ である.

---

[5]"$\varnothing \in A$"かつ"$x \in A$ ならば $x \cup \{x\} \in A$"なる集合 A をとると (無限公理から存在する), $\omega = \{\alpha \in A | \alpha$ は順序数かつ自然数 $\}$ が成り立つ. よって分出公理から ω は集合になる. 実際は逆で, まず A を用いて $\omega = \{\alpha \in A | \alpha$ は順序数かつ自然数 $\}$ と定義したのちに, ω は集合 A の取り方によらないことを示す. これは整列性からわかる.

[6]つまり順序数を用いた自然数の構成である. 今後「自然数とはなんですか?」と聞かれたら, 「順序数 x で, x や x のすべての元は後続型順序数であるもの」と答えれば良い. この ω の構成はフォン・ノイマンによる自然数の構成らしい ([田中] にそう書いてた). 調べてみるとペアノの公理を満たすものは同型を除いて唯一であるらしく, 自然数の構成はいろいろあるとのこと.(例えば"$\varnothing \in A$"かつ"$x \in A$ ならば $x \cup \{x\} \in A$"なる集合 A の最小のものとして構成できる. これは全ての共通部分を取れば良い.) またペアノの公理から頑張って順序構造や和を入れることができる.([尾畑] 参照.)

2　集合系の演算・全射・単射・濃度の大小 (応用問題)

問 2.1 集合の写像 $f : X \to Y$ がモニック (左簡約可能)であるとは, 「任意の写像 $g_1, g_2 : W \to X$ について, $f \circ g_1 = f \circ g_2$ ならば $g_1 = g_2$」が成り立つこととする. 次の問いに答えよ.

(1). f が単射ならばモニックであることを示せ.
(2). f がモニックならば単射であることを示せ. つまり集合においては二つの概念は同じである.

問 2.2 集合の写像 $f : X \to Y$ がエピ (右簡約可能)であるとは, 「任意の写像 $g_1, g_2 : Y \to W$ について, $g_1 \circ f = g_2 \circ f$ ならば $g_1 = g_2$」が成り立つこととする. 次の問いに答えよ.

(1). f が全射ならばエピであることを示せ.
(2). f がエピならば全射であることを示せ. つまり集合においては二つの概念は同じである.

問 2.3 集合 A, B, C について $F(A \times B, C) \sim F(A, F(B, C))$ を示せ. ここで集合 C, D について, $F(C, D)$ を以下のように定義する.

$$F(C, D) := \{g : C \to D | g \text{ は写像 }\}$$

問 2.4 $\mathbb{R} \setminus \mathbb{Q} \sim \mathbb{R}$ を示せ. これより無理数は存在する.

問 2.5 Λ を可算集合とし, 任意の $\lambda \in \Lambda$ について A_λ も可算集合とする. このとき $\bigcup_{\lambda \in \Lambda} A_\lambda$ も可算であることを示せ.[7]

問 2.6 $\mathbb{R} \sim \mathfrak{P}(\mathbb{N})$ を示せ.

問 2.7 $F(\mathbb{N}, \mathbb{N}) \sim F(\mathbb{N}, \mathbb{R}) \sim \mathbb{R}$ を示せ.

問 2.8 $F(\mathbb{R}, \mathbb{R}) \sim \mathfrak{P}(\mathbb{R})$ を示せ.

問 2.9 連続関数 $f : \mathbb{R} \to \mathbb{R}$ からなる集合の濃度は $\mathbb{R}$ に等しいことを示せ.

問 2.10 係数が全て整数である代数方程式 $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ の解となる複素数を代数的数という. 代数的数の集合は可算であることを示せ.

問 2.11 超越数 (代数的ではない複素数) の集合の濃度は $\mathbb{R}$ に等しいことを示せ. よって超越数は存在する.

問 2.12 $X = (\mathbb{R} \setminus \mathbb{Q})^2$ とおく. X 上の相異なる 2 点は X 上の線分二つで結べることを示せ. つまり任意の $x, y \in X$ についてある $a \in X$ があって, x と a を結ぶ線分 L と a と y を結ぶ線分 M について $L \subset X, M \subset X$ とできることを示せ.

[7] 実は証明には選択公理 (後述) が必要である. なんと ZF 公理系ではこの問題 (可算和定理) は証明できないらしい ([alg6] 参照). ただ多くの数学者は選択公理を仮定するので, 暗黙のうちに選択公理を使って良い.

3　同値関係 (二項関係)・商集合 (応用問題)

問 3.1 集合 X 上の冪集合 $\mathfrak{P}(X)$ の二項関係を

$$A \sim B \Longleftrightarrow (A \setminus B) \cup (B \setminus A) \text{ が有限集合}$$

として定義すると, これは $\mathfrak{P}(X)$ 上の同値関係になることを示せ.

問 3.2 半順序集合 $(X, \leq)$ について, 任意の二つの元が上限と下限を持つとき, $(X, \leq)$ は束 (lattice) と呼ばれる. 次の問いに答えよ. ただし板書で解答する際はある程度省略して書いて良い.(”以下同様”などである程度省略して良い.)

(1). $x, y \in L$ について

$$x \vee y := \sup(x, y) \quad x \wedge y := \inf(x, y)$$

とする. このとき以下の 4 つが成り立つことを示せ.

- (ベキ等律): $x \wedge x = x$, $x \vee x = x$
- (交換則): $x \wedge y = y \wedge x$, $x \vee y = y \vee x$
- (結合則): $(x \wedge y) \wedge z = x \wedge (y \wedge z)$, $(x \vee y) \vee z = x \vee (y \vee z)$
- (吸収則): $(x \wedge y) \vee x = x$, $(x \vee y) \wedge x = x$

(2). 逆に集合 L と L 上の二項演算 $\vee$ と $\wedge$ が上の 4 つを満たすとする. このとき

$$x \leq y \Longleftrightarrow x = x \wedge y$$

として定義すると $(L, \leq)$ は束になることを示せ.

問 3.3 $(R, +, \cdot)$ をブール環とする. (問 1.5 参照.)

$$x \leq y \Longleftrightarrow x = xy$$

として定義すると $(R, \leq)$ は束になることを示せ. ただし板書で解答する際はある程度省略して書いて良い.(”以下同様”などである程度省略して良い.)

問 3.4 半順序集合 $(X, \leq)$ が完備束とは $(X, \leq)$ が束で任意の空でない部分集合の上限と下限が常に存在するものとする. 集合 A について $\mathfrak{P}(A)$ は包含関係に関して完備束になることを示せ. (つまり $X, Y \in \mathfrak{P}(A)$ について $X \leq Y$ を $X \subset Y$ で定めるとき, $(\mathfrak{P}(A), \leq)$ は完備束であることを示せ.)

問 3.5 X を集合とし, $\varphi : \mathfrak{P}(X) \to \mathfrak{P}(X)$ を包含関係による順序を保つ写像とする. ($\mathfrak{P}(X)$ の順序に関しては問 3.4 参照.)

$$E := \bigcap_{\{A \in \mathfrak{P}(X) \mid \varphi(A) \subset A\}} A$$

とおくとき $\varphi(E) = E$ であることを示せ.

問 3.6 R を環とする. (問 1.5 参照.) 任意の $x, y \in R$ について $xy = yx$ が成り立つとき, R を可換環という.

可換環 R の部分集合 $I \subset R$ が次の二つを満たすときイデアル (ideal) と呼ばれる.

- $x, y \in I$ ならば, $x + y \in I$.
- $x \in R$ かつ $a \in I$ ならば, $xa \in I$

さらにイデアル $\mathfrak{p} \subset R$ が次を満たすとき素イデアル (prime ideal) と呼ばれる.

- $\mathfrak{p} \neq R$[8]
- $xy \in \mathfrak{p}$ ならば, $x \in \mathfrak{p}$ または $y \in \mathfrak{p}$.

次の問いに答えよ.

(1). 整数の集合 $\mathbb{Z}$ は可換環の構造を持つことがわかる. そこで整数 a について

$$(a) := \{an | n \in \mathbb{Z}\}$$

とする. このとき (a) は $\mathbb{Z}$ のイデアルであることを示せ.

(2). (a) が素イデアルになるような a を全て求めよ.

(3). $\mathbb{Z}$ の素イデアルを全て求めよ.

問 3.7 次の問いに答えよ.

(1). R を可換環とし, I をイデアルとする. $x, y \in R$ について

$$x \sim y \Leftrightarrow x - y \in I$$

と定める. $\sim$ は同値関係であることをしめせ.

(2). 商集合 $R/I := R/\sim$ と置くとき, R/I は可換環になることを示せ. ただし板書で解答する際はある程度省略して書いて良い.(”以下同様”などである程度省略して良い.)

(3). 整数 a について $\mathbb{Z}/a\mathbb{Z} := \mathbb{Z}/(a)$ とする. ((a) については上を参照すること.) $\mathbb{Z}/a\mathbb{Z}$ の元の個数を求めよ.

(4). $p \in \mathbb{Z}$ を正の素数とする. $\mathbb{Z}/p\mathbb{Z}$ は (1) より可換環になる. このとき任意の 0 でない元 $x \in \mathbb{Z}/p\mathbb{Z}$ についてある $y \in \mathbb{Z}/p\mathbb{Z}$ があって $xy = 1$ となることをしめせ.

問 3.8 可換環 R についてイデアル $\mathfrak{m} \subset R$ が次の二つを満たすとき極大イデアル (maximal ideal) と呼ばれる.

- $\mathfrak{m} \neq R$.
- イデアル I が $\mathfrak{m} \subset I \subset R$ を満たすならば, $\mathfrak{m} = I$ または $I = R$.

次の問いに答えよ.

(1). 極大イデアル $\mathfrak{m}$ は素イデアルであることを示せ.

(2). $\mathbb{Z}$ の (0) ではない素イデアルは極大であることを示せ.

(3). $\mathfrak{m}$ を極大イデアルとする. 可換環 $R/\mathfrak{m}$ について, 任意の 0 でない元 $x \in R/\mathfrak{m}$ についてある $y \in R/\mathfrak{m}$ があって $xy = 1$ となることをしめせ.[9]

[8] 今回は [Atiyah-MacDonald] の定義に従う.

[9] ちなみに逆も言える. 要は $R/\mathfrak{m}$ が体になるということである. また $\mathfrak{p}$ が素イデアルならば $R/\mathfrak{p}$ は整域 (integral domain) になる. これも逆が言える. [Atiyah-MacDonald] 参照のこと.

問 3.9 * ブール環 R の素イデアル $\mathfrak{p}$ は極大であり, $R/\mathfrak{p}$ は 2 つの元しか持たないことを示せ.

問 3.10 $p \in \mathbb{Z}$ を正の素数とし, $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ とおく. n を 0 以上の整数とする. $(x_1, \ldots, x_{n+1}), (y_1, \ldots, y_{n+1}) \in \mathbb{F}_p^{n+1} \setminus \{(0, 0, \ldots, 0)\}$ について二項関係 $\sim$ を

$(x_1, \ldots, x_{n+1}) \sim (y_1, \ldots, y_{n+1}) \Leftrightarrow 0$ でない $\lambda \in \mathbb{F}_p$ があって, 任意の $1 \leq i \leq n+1$ について $x_i = \lambda y_i$.

とする. 次の問いに答えよ

(1). $\sim$ は $\mathbb{F}_p^{n+1} \setminus \{(0, 0, \ldots, 0)\}$ における同値関係であることを示せ.
(2). $\mathbb{F}_p\mathbb{P}^n := (F_p^{n+1} \setminus \{(0, 0, \ldots, 0)\})/\sim$ とおく. $\mathbb{F}_p\mathbb{P}^n$ の元の個数を求めよ.

問 3.11 *(ドブル 1) 次の問いに答えよ.

(1). $\mathbb{F}_2\mathbb{P}^2$ の元で $(0 : x_2 : x_3)$ と書けるものの個数を求めよ. ここで $x = (x_1, x_2, \ldots, x_{n+1})$ を $\mathbb{F}_p\mathbb{P}^n$ の元とみなしたものを $(x_1 : \cdots : x_{n+1})$ と書き同次座標と呼ぶ.
(2). 7 色 (赤, 橙, 黄, 緑, 青, 藍, 紫) のペンと 7 枚のカードある. 次のルールを考える.
- どのカードにも相異なる 3 色の ● 印がある.
- どの 2 枚のカードを取っても, 1 つだけ共通する色の ● 印がある.

上のルール 2 つを満たすように色ペンを使ってカードに ● 印を書くことはできるだろうか?

問 3.12 * (ドブル 2) 次の問いに答えよ.

(1). $\mathbb{F}_7\mathbb{P}^2$ の元で $(0 : x_2 : x_3)$ と書けるものの個数を求めよ.
(2). ポケモンのドブルの説明書にはこう書かれていた.
「8 匹のポケモンが描かれたカードが 55 枚入っているよ。 2 枚のカードに 1 つだけ共通するポケモンを誰よりも早く見つけよう！[10]」
さらにポケモンのドブルの説明書を読むとドブルに描かれているポケモンの総数は計 57 匹である. なぜこのようなことが可能なのだろうか. このドブルの仕組みを $\mathbb{F}_7\mathbb{P}^2$ の視点から論ぜよ.
(3). 実はポケモンのドブルのカード数は 57 枚でも可能である. その理由を答えよ.

[10]要は二つのカード A, B について, ただ一つのポケモン x が存在して, x は A にも B にも描かれている, ということ.

4　整列集合・選択公理・ツォルンの補題・整列可能定理 (応用問題)

問 4.1 X を空でない集合 $\sim$ を同値関係とする. $x \in X$ について $C(x) \subset X$ を x の同値類とする. X の部分集合 $S \subset X$ が

(1). $X/\sim = \{C(x) | x \in S\}$
(2). $x, y \in S$ かつ $x \neq y$ ならば $C(x) \neq C(y)$

を満たすとき, S は $X/\sim$ の完全代表系という. このとき $X = \cup_{x \in S} C(x)$ とかける.

選択公理を仮定すれば, 完全代表系は存在することを示せ. (ヒント: $\Lambda = X/\sim$ とし, $\lambda = C(x) \in X/\sim$ として $A_\lambda = C(x)$ と定める.)

問 4.2 $n \in \mathbb{N}$ について集合 X_n を

$$X_0 := \varnothing \quad X_n := \{0, 1, \ldots, n-1\} \quad (n \geq 1 \text{ のとき.})$$

として定義する. 集合 A について次の用語を定義する.

- A が有限とは, ある全単射 $f : X \to X_n$ が存在すること.
- A が無限とは, A が有限ではないこと.
- A がデデキンド無限とは, ある全射ではない単射 $f : A \to A$ が存在すること.

選択公理を仮定すれば, 「A が無限であること」と「A がデデキンド無限である」ことは同値であることを示せ.

問 4.3 関数 $f : \mathbb{R} \to \mathbb{R}$ が任意の $x, y \in \mathbb{R}$ について

$$f(x+y) = f(x) + f(y)$$

を満たしているとする. 次の問いに答えよ.

(1). f が連続ならば, ある $\lambda \in \mathbb{R}$ があって $f(x) = \lambda x$ とかけることを示せ
(2). f が連続でなければ (1) は必ずしも成り立たない. そのような例を構成せよ. つまり「$f(x+y) = f(x) + f(y)$ であるが $f(x) = \lambda x$ とかけない関数 f の例」を一つあげよ. なお選択公理を仮定して良い.

問 4.4 選択公理を仮定すれば, 任意の 0 でない可換環 R には極大イデアル $\mathfrak{m}$(問 3.8 参照) が存在することを示せ.

問 4.5 選択公理を仮定すると次のような定理が証明できる.

> 定理 **1** (バナッハ・タルスキー 1924)). 3 次元空間内の半径 1 の球体を有限個 (実は 5 個でいい) に分割したのち、それらを回転・平行移動操作のみを使ってうまく組み合わせることにより半径 1 の球体を 2 個作ることが出来る.

バナッハ・タルスキーの定理を用いた 1=2 の証明というものがある.

> [証明?] D を半径 1 の球体とする. バナッハ・タルスキーの定理から, 互いに交わらない

部分集合 A_i, B_j があって

$$D = \bigcup_{i=1}^{n} A_i \cup \bigcup_{j=1}^{m} B_j$$

かつ, $\{A_i | 1 \leq i \leq n\}$ を回転・平行移動の操作のみを使って半径 1 の球体 D にでき, $\{B_j | 1 \leq j \leq n\}$ を回転・平行移動の操作のみを使って半径 1 の球体 D にできる.
部分集合 $X \subset \mathbb{R}^3$ に対して $v(X)$ を X の体積 (測度) 表すものとする. すると

$$v(D) = v\left(\bigcup_{i=1}^{n} A_i \cup \bigcup_{j=1}^{m} B_j\right) = \sum_{i=1}^{n} v(A_i) + \sum_{j=1}^{m} v(B_j)$$

であり, $\{A_i | 1 \leq i \leq n\}$ を回転・平行移動操作のみを使って半径 1 の球体 D にできるので $\sum_{i=1}^{n} v(A_i) = v(D)$ となる. よって

$$v(D) = v(D) + v(D)$$

となる. $v(D) = \frac{4\pi}{3}$ であり 0 でないので, 両辺を $v(D)$ でわって $1 = 2$ を得る.

しかし $1{=}2$ は明らかに間違いである. この証明のどの部分に間違いがあるか指摘せよ. ただし選択公理を仮定し, 選択公理を仮定すればバナッハ・タルスキーの定理は成り立つ.

問 4.6 * 地獄に囚人が可算無限人いる. 獄卒の鬼が言うには, 翌日に次のようなゲームを行い囚人側が勝てば囚人たち全員を解放し, 負ければ全員を拷問にかけるとのことである.

[ゲーム内容] 鬼は先ず囚人全員を広場に集め, 囚人各人に赤または白の帽子を被せる. 囚人たちは自分の帽子の色を知ることはできないが, 他の囚人の帽子の色は全て見ることができる. 囚人たちは自分の帽子の色を推測し, 全員で一斉にそれが赤か白かを答える. もし自分の帽子の色を間違えた囚人の数が有限なら, 囚人側の勝ちである. もし間違えた囚人の数が無限なら, 囚人側の負けである. ただし, 囚人たちはゲームの開始前にはいくらでも作戦を相談してよいが, ゲームが始まったら意思の疎通は一切禁止されるものとする.

囚人たちがこのゲームに勝てる作戦が必ず存在することを示せ. なお選択公理を仮定して良い.(ヒント: 問 3.1 の同値関係と問 4.1.)[11]

問 4.7 *** 整列集合 $(X, \leq)$ で $X \sim \mathbb{R}$ となるものの具体的な例を一つあげよ. [12]

問 4.8 *「任意の全射 $f : X \to Y$ についてある $g : Y \to X$ があって, $f \circ g = id_Y$」という命題は選択公理と同値であることを示せ.

問 4.9 ***「任意の体上の任意のベクトル空間は基底を持つ」という命題は選択公理と同値であることを示せ.[13]

問 4.10 ***「帰納的順序集合 X 上の順序を保つ写像 $f : X \to X$ は不動点 ($f(a) = a$ となる $a \in X$) を持つ」という命題は選択公理と同値であることを示せ.

[11]実は「囚人は一列に並んでいて, 前の人は後ろの人の帽子の色がわからない」という条件をつけても良い.
[12]整列集合の例は可算なものが多い. では非加算なものはどうなるのか? ちょっと考えてもわからなかった. なお選択公理を認めれば, 存在に関しては言える.
[13]この命題は正しいが, 私には証明がわからなかった. 問 4.10 も同様. 証明を教えてほしい.

以下の問題は私が最近勉強したことをそのまま出した.

問 4.11 *~** 授業では「X と Y の濃度が等しい」など濃度の大小を定義していたが, 濃度自体は定義していなかった. この問題では濃度を定義することを考える.(以下, 選択公理を仮定する.)

$\mathrm{OR} := \{\alpha | \alpha$ は順序数 $\}$ とおき順序数 (問 1.9 参照)α, β について

$$\alpha \leq \beta \Longleftrightarrow \alpha \in \beta \text{ または } \alpha = \beta$$

として定義する. OR は集合ではないが”整列集合”と同じような性質を満たす (問 1.14 参照. 整列クラスと呼ばれる.)

X を集合として

$$|X| = \min\{\alpha \in \mathrm{OR} | X \text{ にある順序 } \leq \text{ があって } (X, <) \text{ と } (\alpha, \in) \text{ は順序同型 } \}$$

と定義し, $|X|$ を X の濃度 (cardinality)という.[14] X, Y を集合とするとき, 次の問いに答えよ.

(1). $X \sim Y$ であることは $|X| = |Y|$ と同値であることを示せ.
(2). 集合 α が順序数ならば, $|\alpha| \leq \alpha$ であることを示せ.
(3). $X \subset Y$ ならば, $|X| \leq |Y|$ であることを示せ.
(4). 単射 $f : X \to Y$ が存在することは, $|X| \leq |Y|$ と同値であることを示せ.

よって「X と Y の濃度が等しい」を $|X| = |Y|$ と定義でき, 「X は Y より濃度が小さい」を $|X| < |Y|$ として定義できる.

問 4.12 *~** 順序数 α が基数 (cardinal number)であるとは $\alpha = |X|$ となる集合 X が存在することとする. 次の問いに答えよ.

(1). κ を基数とする. 順序数 α が $\alpha < \kappa$ を満たすならば $\alpha \not\sim \kappa$ であることを示せ.
(2). 順序数 κ が基数であることは, $\kappa = |\kappa|$ であることと同値であることを示せ.
(3). κ を基数とする. 集合 Y について $Y \sim \kappa$ ならば $|Y| = \kappa$ であることを示せ.

問 4.13 *~** 問 1.15 と同様に, $\omega := \{\alpha | \alpha$ は順序数かつ自然数 $\}$ とする. 次の問いに答えよ.

(1). 順序数 α, β について $\alpha+1 \sim \beta+1$ ならば $\alpha \sim \beta$ である. (ヒント. 全単射 $f : \alpha+1 \to \beta+1$ について α の行き先を考える.)
(2). $n \in \omega$ とする. 順序数 β について $\beta \sim n$ ならば $\beta = n$ であることを示せ. (ヒント. 順序数 n は整列集合なので超限帰納法を用いる. $\beta \geq \omega$ ならば $\beta \sim \beta + 1$ も使う.)
(3). ω の元 n は基数であることを示せ. ω の元である基数を有限基数といい, そうでない基数を無限基数という.
(4). ω は無限基数であり, 無限基数の中で最小であることを示せ. そのため ω は $\aleph_0$(アレフゼロ)とも書かれる.

[14] min が存在するのは OR が整列クラスになることからわかる. min の右側の集合が空でないことの証明は難しい. つまり「任意の整列集合はある順序数と順序同型になる」ことの証明は難しい. 詳しくは [田中] か [alg1] を参照のこと.

(コラム 1. 連続体仮説) 無限基数の集まり (クラス) を $\mathrm{Incard} := \{\aleph | \aleph \text{ は無限基数 }\}$ とおく. すると順序数の集まり (クラス)$\mathrm{OR} := \{\alpha | \alpha \text{ は順序数 }\}$ と順序同型であることが示せる. つまり無限基数もまた整列されており, 「0 番目, 1 番目, 2 番目, ...」と並べることができる:

$$\omega = |\mathbb{N}| = \aleph_0 < \aleph_1 < \aleph_2 < \cdots < \aleph_\omega < \aleph_{\omega+1} < \cdots$$

問 4.13 から $\aleph_0 = \omega = |\mathbb{N}|$ である. 一方カントールの定理から $\aleph_0 = |\mathbb{N}| < |\mathfrak{P}(\mathbb{N})| = |\mathbb{R}|$ である. 連続体仮説とは次のような命題である.

仮説 **2** (連続体仮説)**.** $\aleph_1 = \mathbb{R}$? つまり集合 Y について $|\mathbb{N}| \leq |Y| \leq |\mathfrak{P}(\mathbb{N})| = |\mathbb{R}|$ ならば $|Y| = |\mathbb{N}|$ または $|Y| = |\mathbb{R}|$ か?

連続体仮説に関しては次が知られている.

定理 **3.** (ゲーデル 1940, コーエン 1963) 連続体仮説は ZFC 公理系 (ZF 公理系+選択公理) からは肯定も否定もできない.

一般連続体仮説 ($\aleph_{\alpha+1} = |\mathfrak{P}(\aleph_\alpha)|$?) もあり, これも ZFC 公理系 (ZF 公理系+選択公理) からは肯定も否定もできない. ちなみに選択公理もまた ZF 公理系からは肯定も否定もできない.

(コラム 2. 宇宙)

定義 **4.** 集合 U が次を満たすとき, U をグロタンディーク宇宙 (Grothendieck universe) という.
(a). $\omega \in U$ であり, $u \in U$ かつ $x \in u$ ならば $x \in U$.
(b). $u, v \in U$ ならば, $\cup_{x \in u} x, \mathfrak{P}(u), \{u, v\}, (u, v), u \times v \in U$.
(c). 全射 $f : a \to b$, $a \in U$, $b \subset U$ ならば, $b \in U$.

要はグロタンディーク宇宙とはまともな集合演算で閉じている集合である. 「マックレーン 圏論の基礎」でも存在を仮定している. グロタンディーク宇宙は基数との関係がある.

定義 **5.** 非可算極限 (問 1.15) な基数 κ が次を満たすとき, 強到達不能基数という.
(a). (正則性) $|\Lambda| < \kappa$ かつ任意の $\lambda \in \Lambda$ について $|A_\lambda| < \kappa$ ならば, $|\cup_{\lambda \in \Lambda} A_\lambda| < \kappa$.
(b). (強極限性) $|X| < \kappa$ ならば $|\mathfrak{P}(X)| < \kappa$.

定理 **6.** (1). "グロタンディーク宇宙の存在"と"強到達不能基数の存在"は同値である.
(2). 強到達不能基数の存在は ZFC 公理系で証明することができない. (ただし ZFC は無矛盾と仮定する.)

なのでグロタンディーク宇宙の存在を ZFC で示すことができない. 「別にグロタンディーク宇宙の存在くらい仮定していいのでは?」と思っていたが, 「ZFC が無矛盾であっても, グロタンディーク宇宙の存在を仮定した ZFC は矛盾するかもしれない」とのことである. [15] 調べれば調べるほど, 「今研究している数学は果たして大丈夫なのか?」と心配する限りである.[16]

[15] この辺りは巨大基数の話に繋がるらしい. 私は全くの素人なので, alg-d さんの動画 [alg4] に委ねる. ちなみに定理 6 の (1) を演習問題にしようとしたが解けなかったのでやめた.

[16] ここ最近調べたり勉強したりして「基礎論・(公理的) 集合論は難しいなあ」と思った. ある集会でとある数学者が「数学者は公理的集合論に疎かである」と言っていた. 身にしみる言葉である.

5　ユークリッド空間・距離空間 (応用問題)

問 5.1 (X,d) を距離空間とし, 部分集合 $M \subset X$ とする. 次の問いに答えよ.

(1). M^i は M に含まれる最大の開集合であることを示せ.
(2). $\overline{M}$ は M を含む最小の閉集合であることを示せ.

問 5.2 (X,d) を距離空間とする. X の部分集合 A が有界とは, ある正の数 M があって任意の $x,y \in A$ について $d(x,y) \leqq M$ であることとする. $\mathcal{B}(X)$ を X の有界閉集合のなす集合とする. 次の問いに答えよ.

(1). $A,B \in \mathcal{B}(X)$ について $\sup_{x\in A} d(x,B) < +\infty$ であることを示せ.
(2). $A,B \in \mathcal{B}(X)$ について

$$d_H(A,B) := \max\{\sup_{x\in A} d(x,B), \sup_{y\in B} d(A,y)\}$$

とする. 任意の $x \in X$ について $d(x,A) \leqq d(x,B) + d_H(A,B)$ が成り立つことを示せ.

問 5.3 問 5.2 での $(\mathcal{B}(X), d_H)$ は距離空間になることを示せ. (ハウスドルフ距離と呼ばれる.)

問 5.4 p を素数とする. 0 でない有理数 $r \in \mathbb{Q}$ について, $r = p^e \frac{n}{m}$ (m,n はともに p と互いに素な整数) と表せるとき, $v_p(r) := e$ と定義する. $r \in \mathbb{Q}$ について

$$|r|_p = \begin{cases} p^{-v_p(r)} & (r \neq 0) \\ 0 & (r = 0) \end{cases}$$

とおく. 次の問いに答えよ.

(1). 0 でない有理数 $r,s \in \mathbb{Q}$ について, $r+s \neq 0$ ならば $v_p(r+s) \geqq \min(v_p(r), v_p(s))$ であることを示せ.
(2). $x,y \in \mathbb{Q}$ について $d_p(x,y) := |x-y|_p$ とおくと d_p は $\mathbb{Q}$ の距離になることを示せ.
(3). $a,r \in \mathbb{Q}$ かつ $r > 0$ について, 開球 $B(a,r) = \{x \in \mathbb{Q} | d_p(x,a) < r\}$ で定める. $B(a,r)$ は閉集合であることを示せ.
(4). $a_n := \sum_{i=0}^{n-1} 2^i = 1 + 2 + \cdots + 2^{n-1}$ とおく. $d_2(-1, a_n)$ の値を求めよ.

問 5.5 *(ハミング符号・グレイコード) $\mathbb{F}_2 = \{0,1\}$ を標数 2 の体とする. ($\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ である.) $x, y \in \mathbb{F}_2^n$ について

$$d(x,y) := (x_i \neq y_i \text{ となる } i \text{ の個数})$$

とおく. (ただし, $x = \{x_i\}_{i=1}^n$, $y = \{y_i\}_{i=1}^n$ とする.) 次の問いに答えよ.

(1). $(\mathbb{F}_2^n, d)$ は距離空間であることを示せ.
(2). $\mathbb{F}_2^n$ の相異なる元からなる数列 $a_1, \ldots, a_{2^n}$ で $a_1 = \{0\}_{i=1}^n$, $d(a_{2^n}, a_1) = 1$, 任意の $2 \leqq k \leqq 2^n$ について $d(a_{k-1}, a_k) = 1$ となるものが存在することを示せ.

以下 $f : \mathbb{F}_2^4 \to \mathbb{F}_2^7$ を次で定める.

$$\begin{array}{ccccc} f: & \mathbb{F}_2^4 & \to & \mathbb{F}_2^7 \\ & (a,b,c,d) & \longmapsto & (a,b,c,d,a+b+d,a+c+d,b+c+d) \end{array}$$

(3). $x, y \in \mathbb{F}_2^4$ について, $x \neq y$ ならば $d(f(x), f(y)) \geqq 3$ であることを示せ.
(4). 任意の $z \in \mathbb{F}_2^7$ について, $d(f(x), z) \leqq 1$ となる $x \in \mathbb{F}_2^4$ がただ一つ存在することを示せ.
(5). I 教官は TA から $f(a,b,c,d)$ の値を聞きメモをした. ところがメモをする際に $\mathbb{F}_2^7$ の一つの成分を間違ってしまった. I 教官のメモには $(1,0,0,1,0,1,0)$ とかかれている. (a,b,c,d) の値を求めよ.

References

[Atiyah-MacDonald] M.F.Atiyah, I.G.MacDonald 可換代数入門 共立出版

[alg1] alg-d 順序数入門 https://alg-d.com/math/ordinal_number.pdf

[alg2] alg-d 選択公理と同値な命題とその証明 https://alg-d.com/math/ac/

[alg3] alg-d 【実数の闇】本当は怖い $\mathbb{R}$ の濃度 https://www.youtube.com/watch?v=iLBJ0AGluIU

[alg4] alg-d 最強の巨大基数「0=1」について【集合論】https://www.youtube.com/watch?v=z7jXyjFnjfU&t=665s

[alg5] alg-d 有限集合・無限集合の定義【選択公理】https://www.youtube.com/watch?v=U0BGmKdCzak

[alg6] alg-d 可算和定理 https://alg-d.com/math/ac/countable_union.html

[内田] 内田伏一 集合と位相 裳華房

[小澤] 小澤登高 バナッハ=タルスキーのパラドックス https://www.kurims.kyoto-u.ac.jp/~kenkyubu/kokai-koza/H27-ozawa.pdf

[尾畑] 尾畑伸明 2022 年度 解析学入門のノート 15 章 https://www.math.is.tohoku.ac.jp/~obata/student/subject/TaikeiBook/Taikei-Book_15.pdf

[田中] 田中尚夫 公理的集合論　培風館

[ドブル] ”ドブル ポケットモンスター” ポケモンセンターオンラインで購入可能
https://www.pokemoncenter-online.com/4970381803407.html?srsltid=AfmBOoqlTFoiTZH-k2ea7zID0u39ZuX3pKW7_m6q4x0e64r1V8nDYXAL

[マックレーン] S. マックレーン 圏論の基礎 丸善出版

[Zagier] D. Zagier A One-Sentence Proof That Every Prime $p \equiv 1(\mod 4)$ Is a Sum of Two Squares The American Mathematical Monthly, Vol. 97, No. 2 (Feb., 1990), p. 144.