BCMM I : EXTRA PROBLEMS

1 論理

1.1 記号論理

1.1.1 真理表をつくり次の論理式が等値であることを証明せよ。

(a) $P \wedge Q \equiv \sim((\sim P) \vee (\sim Q))$.

(b) $P \vee Q \equiv \sim((\sim P) \wedge (\sim Q))$.

(c) $P \Rightarrow Q \equiv (\sim P) \vee Q$.

(d) $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$.

(e) $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$.

1.1.2 次の論理式の組み X, Y が等値 $(X \equiv Y)$ であるか、$X \Rightarrow Y$ であるか、$Y \Rightarrow X$ であるかどうか判定せよ。

(a) $P \Rightarrow Q$, $\sim(P \wedge \sim Q)$.

(b) $P \wedge (Q \vee R)$, $(P \wedge Q) \vee R$.

(c) $(P \wedge Q) \Rightarrow R$, $P \Rightarrow (Q \vee R)$.

(d) $P \Rightarrow (Q \vee R)$, $(P \wedge \sim Q) \Rightarrow R$.

(e) $(P \Rightarrow Q) \wedge (Q \Rightarrow R)$, $P \Rightarrow R$.

1.1.3 X, Y を命題とするとき、$X \oplus Y = (X \vee Y) \wedge \sim(X \wedge Y)$ とする。また 1 つねに真の命題、0 は常に偽の命題とする。P, Q, R を命題とするとき、次を示せ。

(a) $P \vee \sim P \equiv 1$, $P \vee 1 \equiv 1$, $P \wedge 1 \equiv P$.

(b) $P \wedge \sim P \equiv 0$, $P \wedge 0 \equiv 0$, $P \vee 0 \equiv P$.

(c) $P \oplus P \equiv 0$.

(d) $P \oplus 0 \equiv P$.

(e) $P \oplus 1 \equiv \sim P$.

(f) $P \oplus Q \equiv Q \oplus P$.

(g) $(P \oplus Q) \oplus R \equiv P \oplus (Q \oplus R)$.

1.1.4 $\boldsymbol{R}$ で実数をあらわすものとする。以下のうち、正しいものは証明し、誤っているものについてはその命題の否定を記述し、それを証明せよ。

(a) $(\forall x \in \boldsymbol{R})[x^2 > 0]$.

(b) $(\exists x \in \boldsymbol{R})[x^2 > 0]$.

(c) $(\forall x \in \boldsymbol{R})(\exists y \in \boldsymbol{R})[x + y = 0]$.

(d) $(\exists x \in \boldsymbol{R})(\forall y \in \boldsymbol{R})[x + y = 0]$.

(e) $(\forall x \in \boldsymbol{R})(\exists y \in \boldsymbol{R})[x + y = y]$.

(f) $(\exists x \in \boldsymbol{R})(\forall y \in \boldsymbol{R})[x + y = y]$.

(g) $(\forall x \in \boldsymbol{R})(\exists y \in \boldsymbol{R})[xy = 1]$.

(h) $(\exists x \in \boldsymbol{R})(\forall y \in \boldsymbol{R})[xy = 1]$.

(i) $(\forall x \in \boldsymbol{R})(\exists y \in \boldsymbol{R})[xy = 0]$.

(j) $(\exists x \in \boldsymbol{R})(\forall y \in \boldsymbol{R})[xy = 0]$.

(k) $(\forall x \in \boldsymbol{R})(\exists y \in \boldsymbol{R})[xy = y]$.

(l) $(\exists x \in \boldsymbol{R})(\forall y \in \boldsymbol{R})[xy = y]$.

1.1.5 命題 $P_1, P_2, \ldots, P_n$ に関する二つの論理式 $F(P_1, P_2, \ldots, P_n)$, $G(P_1, P_2, \ldots, P_n)$ が等値（すなわち $P_1, P_2, \ldots, P_n$ の真理値にかかわらず、それぞれの真理値が等しい）であることと、次が成り立つことは同値である（すなわち、等値であれば次が成り立ち、次が成り立てば、等値である）ことを証明せよ。

$$F(P_1, P_2, \ldots, P_n) \Leftrightarrow G(P_1, P_2, \ldots, P_n) \text{ の真理値はすべて「真」}$$

1.1.6 次のそれぞれの列が真理値になるような論理式を求めよ。

P	Q	R	X_1	X_2	X_3	X_4	X_5	X_6	X_7
T	T	T	F	T	T	F	F	T	F
T	T	F	F	F	T	T	F	T	F
T	F	T	T	T	F	T	F	T	F
T	F	F	T	F	T	F	F	T	F
F	T	T	T	T	F	T	T	T	F
F	T	F	T	F	T	F	F	T	F
F	F	T	F	F	F	F	F	T	F
F	F	F	F	F	T	T	F	T	F

1.1.7 前問で得られた論理式をなるべく短くなるよう変形せよ。($\Rightarrow$, $\Leftrightarrow$ は用いず、$\sim$, $\wedge$, $\vee$ を使う回数を一番少なく。)

チャレンジ問題 1.1 命題 $P_1, P_2, \ldots, P_n$ に関する論理式で真理値がどのようになるものも $\sim$ と $\vee$ および括弧だけを用いて構成することができることを証明せよ。

チャレンジ問題 1.2 前問で $\sim$ と $\vee$ を用いる回数を最小にしたい。$n = 3$ のとき一番多く必要とするのはどんな場合か。$\sim$ と $\vee$ と $\wedge$ を使った場合はどうか。

2 集合

2.1 集合

2.1.1 次の式を証明せよ。(Venn 図ではなく、定義またはそれまでに証明した式を用いて証明せよ。)

(a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

(b) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

(c) $\overline{A \cap B} = \overline{A} \cup \overline{B}$

(d) $\overline{A \cup B} = \overline{A} \cap \overline{B}$

(e) $(A \subseteq A_1) \wedge (B \subseteq B_1) \Rightarrow A \cup B \subseteq A_1 \cup B_1$.

(f) $A \subseteq B \Leftrightarrow A \cup B = B$

(g) $A \cap B = A - (A - B)$

(h) $(A-B)-C = (A-C)-(B-C) = A-(B \cup C)$

(i) $A \cup B \cup C = (A-B) \cup (B-C) \cup (C-A) \cup (A \cap B \cap C)$

(j) $A \cap (A \cup B) = A \cup (A \cap B) = A$

(k) $(A \cup B) \cap (B \cup C) \cap (C \cup A) = (A \cap B) \cup (B \cap C) \cup (C \cap A)$

(l) $A-(B-A) = A$

(m) $(A \cup B)-C = (A-C) \cup (B-C)$

(n) $A-(B-(C-D)) = (A-B) \cup ((A \cap C)-D)$

(o) $A \cup (B-C) = ((A \cup B)-C) \cup (A \cap C)$

(p) $A-(B-(C-D)) = (A-B) \cup (A \cap C-D)$

(q) $A-(B-(C-(D-E))) = (A-B) \cup (A \cap C-D) \cup (A \cap C \cap E)$.

2.1.2 次の関係式は正しいか。正しければ証明し、正しくなければ、反例を与えよ。

(a) $(A-B) \cap C = (A \cap C)-(B \cap C) = (A \cap C)-B$

(b) $A \cup (B-C) = (A \cup B)-C$

(c) $(A-B) \cup C = A-(B-C)$

2.1.3 A を 2 の倍数である整数全体、B を 3 の倍数である整数全体、C を 4 の倍数である整数全体、D を 5 の倍数である整数全体、E を 6 の倍数である整数全体とする。整数に関する命題を次のように定義する。$P(x)$: x は 2 の倍数である。$Q(x)$: x は 3 の倍数である。$R(x)$: x は 4 の倍数である。$S(x)$: x は 5 の倍数である。このとき、論理式を用いながら、次を証明せよ。

(a) $A \cap B = E$.

(b) $A \cup B \cup D \neq \boldsymbol{Z}$.

(c) $C \subseteq A$.

(d) $A \cap C \subseteq E$.

(e) $E \neq A \cap C$.

2.1.4 $A \triangle B = (A \cup B) - (A \cap B)$ と定義する。次のことを証明せよ。

(a) $A \triangle A = \emptyset$, $A \triangle B = B \triangle A$.

(b) $(A \triangle B) \triangle C = A \triangle (B \triangle C)$.

(c) $(A \triangle B) \cap C = (A \cup C) \triangle (B \cap C)$.

2.1.5 次を証明せよ。

(a) $A \subseteq C$, $B \subseteq D$ のとき、$A \times B \subseteq C \times D$.

(b) $A \times B \subseteq C \times D$ で $A \neq \emptyset$, $B \neq \emptyset$ のとき $A \subseteq C$, $B \subseteq D$.

(c) $(A \times B) - (C \times D) = ((A - C) \times B) \cup (A \times (B - D)) = ((A - C) \times (B - D)) \cup ((A - C) \times (B \cap D)) \cup ((A \cap C) \times (B - D))$

(d) $A \times A = B \times B$ ならば $A = B$.

(e) $A \neq \emptyset$, $B \neq \emptyset$ で $(A \times B) \cup (B \times A) = C \times C$ ならば $A = B = C$.

2.1.6 Λ, M を添字の集合、任意の $\lambda \in \Lambda$, $\mu \in M$ について、$A_\lambda, B_\mu \subseteq X$ とする。次のことを証明せよ。

(a) $\left(\bigcup_{\lambda \in \Lambda} A_\lambda\right) \cap \left(\bigcup_{\mu \in M} B_\mu\right) = \bigcup_{(\lambda, \mu) \in \Lambda \times M} A_\lambda \cap B_\mu$.

(b) $\left(\bigcap_{\lambda \in \Lambda} A_\lambda\right) \cup \left(\bigcap_{\mu \in M} B_\mu\right) = \bigcap_{(\lambda, \mu) \in \Lambda \times M} A_\lambda \cap B_\mu$.

2.1.7 $\boldsymbol{N}$ を自然数の集合とする。次のことを証明せよ。

(a) $\bigcup_{n \in \boldsymbol{N}} \left(0,\ 1 - \frac{1}{n}\right) = (0, 1)$.

(b) $\bigcap_{n \in \boldsymbol{N}} \left(0,\ \frac{1}{n}\right) = \emptyset$.

(c) $\bigcap_{n \in \boldsymbol{N}} \left[-\frac{1}{n},\ \frac{1}{n}\right] = \{0\}$.

チャレンジ問題 2.1 $A \cup B \cup C = (A - B) \cup (B - C) \cup (C - A) \cup (A \cap B \cap C)$ を n 個の集合の和集合 $A_1 \cup A_2 \cup \cdots \cup A_n$ に拡張し、証明を与えよ。

3　同値関係、半順序、数学的帰納法

3.1　同値関係 (equivalence relation)、半順序 (partial order)

以下の問題において、$\boldsymbol{Z}$ は整数全体の集合、$\boldsymbol{Q}$ は有理数全体の集合、$\boldsymbol{R}$ は実数全体の集合、$\boldsymbol{C}$ は複素数全体の集合、$\boldsymbol{Z}^+ = \{0, 1, 2, \ldots\}$ を負または 0 の整数全体とする。また、X を集合とするとき、$P(X)$ で X の部分集合全体からなる集合を表すとする。n を正の整数とするとき、$\mathrm{Mat}_n(\boldsymbol{C})$ で複素数を成分とする n 次正方行列全体からなる集合を表し、$\mathrm{GL}_n(\boldsymbol{C})$ で複素数を成分とする n 次正則行列[1]全体からなる集合を表すものとする。

$a, b \in \boldsymbol{Z}$ に対して、$b = ca$ となる $c \in \boldsymbol{Z}$ が存在するとき、$a \mid b$ と書き、a は b を割り切る（整除する）と言う。(英語では "a divides b". と読む。)

$$(\forall a \in \boldsymbol{Z})(\forall b \in \boldsymbol{Z})[a \mid b \Leftrightarrow (\exists c \in \boldsymbol{Z})[b = ca]].$$

3.1.1 m を正の整数とする。$a, b \in \boldsymbol{Z}$ に対して、$a \equiv b$ を $b - a$ は m の倍数、すなわち、

$$a \equiv b \Leftrightarrow (\exists q \in \boldsymbol{Z})[b - a = qm] \Leftrightarrow m \mid b - a$$

とする。

(a) $\equiv$ は $\boldsymbol{Z}$ 上の同値関係であることを示せ。

(b) $[a]$ で a を含む同値類を表すとすると、$[0], [1], \ldots, [m-1]$ はすべて相異なる同値類で、かつ、$\boldsymbol{Z} = [0] \cup [1] \cup \cdots \cup [m-1]$ であることを示せ。

3.1.2 X を集合とする。X の部分集合に対して、$A \subseteq B$ で関係を定めると、$\subset$ は $P(X)$ の順序関係であることを示せ。

3.1.3 $(A, \sim)$ によって集合 A に同値関係 $\sim$ が定義されているとする。このとき、$[a] = \{x \mid (x \in A) \wedge (x \sim a)\}$ とすると、次が成立することを示せ。

(a) $(\forall a \in A)[a \in [a]]$.

(b) $(\forall a \in A)(\forall b \in A)[b \in [a] \Rightarrow [a] = [b]]$.

(c) $(\forall a \in A)(\forall b \in A)[[a] \cap [b] \neq \emptyset \Rightarrow [a] = [b]]$.

(d) $A = \bigcup_{a \in A} [a]$.

3.1.4 以下のそれぞれの集合上に定義された関係が、順序関係であるか、同値関係であるか、そのどちらでもないか判定せよ。ある条件を満たさないときは、そのような例をあげよ。

(a) $(P(X), \sim_A)$: X を集合、$P(X)$ をその部分集合全体、A を X の一つの部分集合とする。$B, C \in P(X)$ に対して、$B \sim_A C$ を、$A \cap B = A \cap C$ で定義する。

[1] n 次正方行列で逆行列が存在するもの。

(b) $(P(X), \subset_A)$: X を集合、$P(X)$ をその部分集合全体、A を X の一つの部分集合とする。$B, C \in P(X)$ に対して、$B \subset_A C$ を、$A \cap B \subseteq A \cap C$ で定義する。

(c) $(\boldsymbol{R}, \simeq)$: 実数 $a, b \in \boldsymbol{R}$ に対して、$|a| = |b|$ によって $a \simeq b$ を定める。

(d) $(\boldsymbol{R}, \fallingdotseq)$: 実数 $a, b \in \boldsymbol{R}$ に対して、$|b - a| < 0.01$ によって $a \fallingdotseq b$ を定める。

(e) $(\boldsymbol{R}, \dashv)$: 実数 $a, b \in \boldsymbol{R}$ に対して、$|a| \leq |b|$ によって $a \dashv b$ を定める。

(f) $(\boldsymbol{R}, \leq_e)$: 実数 $a, b \in \boldsymbol{R}$ に対して、$e^a \leq e^b$ のとき、$a \leq_e b$ と定める。

(g) $(\mathcal{L}, \|)$: $\mathcal{L}$ を平面上の直線全体の集合、直線 $\ell, m \in \mathcal{L}$ に対して、$\ell = m$ または、ℓ と m が平行（交差しない）のとき $\ell \| m$ とする。

(h) $(\mathcal{L}^*, \|^*)$: $\mathcal{L}^*$ を 3 次元空間の直線全体の集合、直線 $\ell, m \in \mathcal{L}$ に対して、$\ell = m$ または、ℓ と m が交差しないとき $\ell \|^* m$ とする。

(i) $(\mathcal{P}, \|)$: $\mathcal{P}$ を 3 次元空間の平面全体の集合、平面 $P_1, P_2 \in \mathcal{P}$ に対して、$P_1 = P_2$ または、P_1 と P_2 が平行（交差しない）のとき $P_1 \| P_2$ とする。

(j) $(\mathcal{T}, \equiv)$: $\mathcal{T}$ を平面内の三角形全体とする。三角形 $T_1, T_2 \in \mathcal{T}$ に対して、T_1 と T_2 が合同のとき $T_1 \equiv T_2$ とする。

(k) $(\mathcal{T}, \backsim)$: $\mathcal{T}$ を平面内の三角形全体とする。三角形 $T_1, T_2 \in \mathcal{T}$ に対して、T_1 と T_2 が相似のとき $T_1 \backsim T_2$ とする。

(l) $(\mathcal{C}, \sim)$: $\mathcal{C}$ を微分可能な一変数関数全体とする。$f(x), g(x) \in \mathcal{C}$ にたいして、$f'(x) = g'(x)$ すなわち、それぞれの導関数が等しいとき、$f(x) \sim g(x)$ とする。

(m) $(\mathcal{F}, \approx)$: $\mathcal{F}$ は実数上で定義された一変数関数全体とする。$f(x), g(x) \in \mathcal{F}$ に対して、$\{x \mid (x \in \boldsymbol{R}) \wedge (f(x) \neq g(x))\}$ は有限集合（元の数が有限）のとき、$f(x) \approx g(x)$ とする。

(n) $(\mathcal{S}, \approx)$: $\mathcal{S}$ は、収束する数列 $\{a_n\}$ 全体とする。$\{a_n\}, \{b_n\} \in \mathcal{S}$ に対して、ある番号以降は同じであるときこれらの数列は収束する数列として等しいと定義する。すなわち、

$$\{a_n\} \approx \{b_n\} \Leftrightarrow (\exists m \in \boldsymbol{N})(\forall k \in \boldsymbol{N})[(k \geq m) \Rightarrow (a_k = b_k)].$$

(o) $(\mathcal{S}, \preceq)$: $\mathcal{S}$ は、収束する数列 $\{a_n\}$ 全体とする。$\{a_n\}, \{b_n\} \in \mathcal{S}$ に対して、ある番号以降は $a_k \leq b_k$ であるとき $\preceq$ であるとする。すなわち、

$$\{a_n\} \preceq \{b_n\} \Leftrightarrow (\exists m \in \boldsymbol{N})(\forall k \in \boldsymbol{N})[(k \geq m) \Rightarrow (a_k \leq b_k)].$$

ただし、収束する数列が等しいことの定義は前問の $\approx$ を用いる。

(p) $(\mathrm{Mat}_n(\boldsymbol{C}), \preceq)$: M_1, M_2 を n 次正方行列としたとき、n 次正方行列 N で $M_2 = NM_1$ となるものが存在するとき、$M_2 \preceq M_1$ と定義する。

3.1.5 以下のそれぞれの集合上に定義された関係が、順序関係であることを示せ。全順序（$a \leq b$ または $b \leq a$ のいずれかが必ず成り立つ）かどうか判定せよ。

(a) $(\boldsymbol{Z}^+, |)$: $a, b \in \boldsymbol{Z}^+$ に対して、$b = ac$ となる $c \in \boldsymbol{Z}^+$ が存在するとき[2]、$a \mid b$ とする。

(b) $(\boldsymbol{Z}, |_+)$: $a, b \in \boldsymbol{Z}$ に対して、$b = ac$ となる 非負の整数 $c \in \boldsymbol{Z}^+$ が存在する時 $a \mid_+ b$ とする。

(c) $(\boldsymbol{R} \times \boldsymbol{R}, \leq)$: $(a, b), (c, d) \in \boldsymbol{R} \times \boldsymbol{R}$ に対して、$a < c$ であるか、または、$a = c$ かつ $b \leq d$ のときに、$(a, b) \leq (c, d)$ と定義する。

(d) $(\mathcal{P}^2, \Rightarrow)$: $\mathcal{P}^2$ は P と Q の二つの命題の結合命題全体とする。$X \Rightarrow Y$ は、この命題が P, Q の真偽にかかわらず真であることを意味するとする。ただし、結合命題が等しいのは等値のときであるとする。

(e) $(\mathcal{P}^3, \Rightarrow)$: $\mathcal{P}^3$ は P、Q、R の三つの命題の結合命題全体とする。$X \Rightarrow Y$ は、この命題が P, Q, R の真偽にかかわらず真であることを意味するとする。ただし、結合命題が等しいのは等値のときであるとする。

3.1.6 以下のそれぞれの集合上に定義された関係が、同値関係であることを示せ。

(a) $(\boldsymbol{R}^*, R)$: $\boldsymbol{R}^*$ を 0 以外の実数の集合とする。$a, b \in \boldsymbol{R}^*$ に対し、$ab > 0$ のとき、aRb と定義する。

(b) $(\boldsymbol{R}, T)$: $a, b \in \boldsymbol{R}$ に対して、$b - a \in \boldsymbol{Z}$ のとき aTb と定義する。

(c) $(\boldsymbol{R}, S)$: $a, b \in \boldsymbol{R}$ に対して、$\cos a = \cos b$ かつ $\sin a = \sin b$ のとき aSb と定義する。

(d) $(\boldsymbol{Z} \times \boldsymbol{Z}, R)$: $(a, b), (c, d) \in \boldsymbol{Z} \times \boldsymbol{Z}$ に対して、$a + d = b + c$ のとき、$(a, b)R(c, d)$ と定義する。

(e) $(\boldsymbol{Z} \times \boldsymbol{Z}^*, Q)$: $\boldsymbol{Z}^*$ は 0 以外の整数全体を表すとする。$(a, b), (c, d) \in \boldsymbol{Z} \times \boldsymbol{Z}^*$ に対して、$ad = bc$ のとき、$(a, b)Q(c, d)$ と定義する。

(f) $(\boldsymbol{C}, \sim)$: $z_1, z_2 \in \boldsymbol{C}$ とするとき、零ではない実数 c で $z_2 = cz_1$ と書けるとき、$z_1 \sim z_2$ と定義する。

(g) $(\mathrm{Mat}_n(\boldsymbol{C}), \sim_L)$: M_1, M_2 を n 次正方行列としたとき、n 次正則行列 $N \in \mathrm{GL}_n(\boldsymbol{C})$ で $M_2 = NM_1$ となるものが存在するとき、$M_1 \sim_L M_2$ と定義する。

(h) $(\mathrm{Mat}_n(\boldsymbol{C}), \sim)$: M_1, M_2 を n 次正方行列としたとき、n 次正則行列 $N \in \mathrm{GL}_n(\boldsymbol{C})$ で $M_2 = NM_1N^{-1}$ となるものが存在するとき、$M_1 \sim M_2$ と定義する。

(i) $(\mathrm{Mat}_n(\boldsymbol{C}), \sim_{RL})$: M_1, M_2 を n 次正方行列としたとき、n 次正則行列 $N_1, N_2 \in \mathrm{GL}_n(\boldsymbol{C})$ で $M_2 = N_1M_1N_2$ となるものが存在するとき、$M_1 \sim_{RL} M_2$ と定義する。

3.1.7 前問のそれぞれについて、同値類を決定せよ。

[2] $a \mid b$ すなわち $c \in \boldsymbol{Z}$ としてもこの場合は $c \in \boldsymbol{Z}^+$ となるので同じ。しかし次の問題では、この定義では順序関係にならない。何故でしょうか。

3.1.8 順序集合 $(X, \leq)$ で X の要素の数が有限であるとする、X の要素を点とし、$a, b \in X$ について $a \leq b$ のとき、b を上に、a を下に書き、線で結んだ図を Hasse Diagram という。以下のそれぞれについて、Hasse Diagram を描け。

(a) $A = \{1, 2, 3, 4\}$ として、$(P(A), \subset)$ とした順序集合。

(b) $A = \{1, 2, 3, \ldots, 12\}$ とする。a が b を割り切るとき $a \preceq b$ とした順序集合。

(c) $(\mathcal{P}^2, \Rightarrow)$: $\mathcal{P}^2$ は P と Q の二つの命題の結合命題全体。ただし、結合命題が等しいのは等値のときであるとする。

4 写像 (functions)

4.1 写像の定義・全射・単射・全単射とその個数

4.1.1 X を 4 個の元からなる集合、Y を 3 個の元からなる集合とする。そのとき、それぞれの写像がいくつあるかを下の表に書き込め。

	$X \longrightarrow Y$	$Y \longrightarrow X$	$X \longrightarrow X$	$Y \longrightarrow Y$
写像 (function)				
単射 (injective function)				
全射 (surjective function)				
全単射 (bijective function)				

4.1.2 X を m 個の元からなる集合、Y を n 個の元からなる集合とする。

(a) X から Y への写像はいくつあるか。

(b) X から Y への単射はいくつあるか。

(c) X から Y への全射はいくつあるか。

(d) X から Y への全単射はいくつあるか。

必要ならば、$m > n$, $m < n$, $m = n$ など場合分けして考えよ。m と n に関する簡単な式で表現できないときは、その数を $f(m,n)$ などとおき、$f(m-1,n)$, $f(m,n-1)$, $f(m-1,n-1)$ などを用いて表現せよ。

4.1.3 $a, b \in \boldsymbol{Z}$ としたとき、$a \equiv b$ を $12 \mid b-a$ すなわち、$b-a$ は 12 の倍数で定義すると、$\equiv$ は $\boldsymbol{Z}$ 上に同値関係を定める。この同値類全体を $\boldsymbol{Z}_{12}$ で表すものとする。すると、$\boldsymbol{Z}_6 = \{[0],[1],[2],[3],\ldots,[10],[11]\}$ となる。ここで $[a]$ は a を含む同値類で、$[a] = \{a + 12q \mid q \in \boldsymbol{Z}\}$ である。このとき、以下の対応は、まず写像であるか判定し、写像であれば、単射であるか、全射であるか判定せよ。

(a) $f : \boldsymbol{Z} \longrightarrow \boldsymbol{Z}_{12} \quad (a \mapsto [a])$.

(b) $f : \boldsymbol{Z}_{12} \longrightarrow \boldsymbol{Z} \quad ([a] \mapsto a)$.

(c) $f : \boldsymbol{Z}_{12} \longrightarrow \boldsymbol{Z} \quad ([a] \mapsto (-1)^a)$.

(d) $f : \boldsymbol{Z}_{12} \longrightarrow \boldsymbol{Z}_{12} \quad ([a] \mapsto [a+1])$.

(e) $f : \boldsymbol{Z}_{12} \longrightarrow \boldsymbol{Z}_{12} \quad ([a] \mapsto [2a])$.

(f) $f : \boldsymbol{Z}_{12} \longrightarrow \boldsymbol{Z}_{12} \quad ([a] \mapsto [-a])$.

(g) $f : \boldsymbol{Z}_{12} \longrightarrow \boldsymbol{Z}_{12} \quad ([a] \mapsto [5a])$.

(h) $f : \boldsymbol{Z}_{12} \longrightarrow \boldsymbol{Z}_{12} \quad ([a] \mapsto [a^2])$.

4.1.4 次のそれぞれの写像は単射か全射か判定し、その事実を証明せよ。ただし $P(\boldsymbol{R})$ は実数の部分集合全体を表すものとする。

(a) $f : \boldsymbol{R} \longrightarrow \boldsymbol{R} \quad (x \mapsto x^3 + 2x - 1)$.

(b) $f : \boldsymbol{R} \longrightarrow \boldsymbol{R} \quad (x \mapsto e^{-x} - 2x)$.

(c) $f : \boldsymbol{R}-\{1\} \longrightarrow \boldsymbol{R} \quad (x \mapsto \dfrac{x}{x-1})$.

(d) $f : \boldsymbol{R}-\{1\} \longrightarrow \boldsymbol{R}-\{1\} \quad (x \mapsto \dfrac{x+1}{x-1})$.

(e) $f : \boldsymbol{R} \longrightarrow \boldsymbol{R} \quad (x \mapsto \dfrac{x}{x^2+1})$.

(f) $f : \boldsymbol{R} \longrightarrow P(\boldsymbol{R}) \quad (x \mapsto \{y \mid y < x\})$。

(g) $f : \boldsymbol{R} \longrightarrow P(\boldsymbol{R}) \quad (x \mapsto \{y \mid y^2 < x\})$。

(h) $f : \boldsymbol{R} \longrightarrow P(\boldsymbol{R}) \quad (x \mapsto \{y \mid y < x^2\})$。

4.1.5 $f : \boldsymbol{R} \to \boldsymbol{R}\,(x \mapsto \sin x)$, $g : \boldsymbol{R} \to \boldsymbol{R}\,(x \mapsto \cos x)$, $h : \boldsymbol{R} \to \boldsymbol{R} \times \boldsymbol{R}\,(x \mapsto (\cos x, \sin x))$ とする。このとき次のそれぞれの集合を求めよ。

(a) $f^{-1}(1)$, $f^{-1}(-1)$.

(b) $g^{-1}(1)$, $g^{-1}(-1)$.

(c) $f^{-1}(\sqrt{3}/2)$, $f^{-1}(-\sqrt{3}/2)$.

(d) $g^{-1}(\sqrt{3}/2)$, $g^{-1}(-\sqrt{3}/2)$.

(e) $h^{-1}((1,0))$, $h^{-1}((0,1))$, $h^{-1}((-1,0))$, $h^{-1}((0,-1))$.

(f) $B = \{(x,0) \mid x \in \boldsymbol{R}\}$ としたとき、$h^{-1}(B)$.

(g) $f^{-1}(f(a))$, a はある実数.

(h) $g^{-1}(g(a))$, a はある実数.

4.2 写像の性質

4.2.1 f を集合 X から集合 Y への写像、A, A' を X の部分集合、B, B' を Y の部分集合とする。ここで、$f(A)$ とは $f(A) = \{f(x) \mid x \in A\} \subseteq Y$、$f^{-1}(B)$ とは $f^{-1}(B) = \{x \mid f(x) \in B\} \subseteq X$ のことである。($f(A')$, $f^{-1}(B')$ も同様。)

(a) $A \subseteq A' \Rightarrow f(A) \subseteq f(A')$ を示せ。

(b) $B \subseteq B' \Rightarrow f^{-1}(B) \subseteq f^{-1}(B')$ を示せ。

(c) $f(A \cup A') = f(A) \cup f(A')$ を示せ。

(d) $f^{-1}(B \cup B') = f^{-1}(B) \cup f^{-1}(B')$ を示せ。

(e) $f(A \cap A') \subseteq f(A) \cap f(A')$ を示せ。

(f) $f^{-1}(B \cap B') = f^{-1}(B) \cap f^{-1}(B')$ を示せ。

(g) $f(A \cap A') \neq f(A) \cap f(A')$ である例をあげよ。

(h) $f(A \cap A') = f(A) \cap f(A')$ となる f の条件は何か。全射、単射など。

4.2.2 f を X から Y への写像、$A \subseteq X$、$B \subseteq Y$ とする。

(a) $f(f^{-1}(B)) \subseteq B$ を示せ。

(b) $f^{-1}(f(A)) \supseteq A$ を示せ。

(c) f が全射ならば、$f(f^{-1}(B)) = B$ であることを証明せよ。

(d) $f(f^{-1}(B)) \neq B$ である例をあげよ。

(e) f が単射ならば、$f^{-1}(f(A)) = A$ であることを証明せよ。

(f) $f^{-1}(f(A)) \neq A$ である例をあげよ。

4.2.3 次の条件を満たす写像の例をあげよ。

(a) 写像 $f : \boldsymbol{Z} \longrightarrow \boldsymbol{Z}$ であって、単射であるが全射ではない。

(b) 写像 $f : \boldsymbol{Z} \longrightarrow \boldsymbol{Z}$ であって、全射であるが単射ではない。

(c) 写像 $f : \boldsymbol{R} \longrightarrow \boldsymbol{R}$ であって、単射であるが全射ではない。

(d) 写像 $f : \boldsymbol{R} \longrightarrow \boldsymbol{R}$ であって、全射であるが単射ではない。

(e) 写像 $f : \boldsymbol{R} \longrightarrow \boldsymbol{Z}$ であって、全射であるもの。

4.2.4 $V = \boldsymbol{R}^n$ を n 次元実列ベクトル空間、$f : V \longrightarrow V$ が線形写像（一次写像）とするとき次を示せ。

$$\{\boldsymbol{v} \mid (\boldsymbol{v} \in V) \wedge f(\boldsymbol{v}) = \boldsymbol{0}\} = \{\boldsymbol{0}\} \Leftrightarrow f \text{ は単射}$$

4.3 写像の合成

4.3.1 $f : X \longrightarrow Y$ を集合 X から集合 Y への写像とする。$g : Y \longrightarrow X$ を集合 Y から集合 X への写像で、$g \circ f = id_X$ が成り立つものとする。id_X は集合 X 上の恒等写像（すなわち $(\forall x \in X)[id_X(x) = x]$）を表すものとする。

(a) f は単射であることを証明せよ。

(b) g は全射であることを証明せよ。

4.3.2 $f : X \longrightarrow Y$ を集合 X から Y への写像とする。$g : Y \longrightarrow Z$ を集合 Y から集合 Z への写像とする。

(a) f および g が単射ならば、$g \circ f$ も単射であることを示せ。

(b) f および g が全射ならば、$g \circ f$ も全射であることを示せ。

(c) $g \circ f$ が単射ならば、f は単射であることを証明せよ。

(d) $g \circ f$ が単射であって、かつ g が単射ではない例をあげよ。

(e) $g \circ f$ が全射ならば、g は全射であることを証明せよ。

(f) $g \circ f$ が全射であって、かつ f が全射ではない例をあげよ。

チャレンジ問題 **4.1** $f : X \longrightarrow Y$ を集合 X から集合 Y への写像とする。

(1) f が全射としたとき、写像 $g : Y \longrightarrow X$ で $f \circ g = id_Y$ となるものが存在するかどうか判定せよ。

(2) f が単射としたとき、写像 $g : Y \longrightarrow X$ で $g \circ f = id_X$ となるものが存在するかどうか判定せよ。

4.4 写像と同値関係

4.4.1 $\sim$ を集合 X 上に定義した同値関係とする。$\sim$ は X の同値関係である。$x \in X$ の属する $\sim$ による同値類を $[x] = [x]_\sim$ で表し、同値類全体の集合を $X/\sim = \{[x] \mid x \in X\} \subseteq P(X)$ で表す。

(a) $f : X \to X/\sim$ $(x \mapsto [x])$ は全射であることを示せ。

(b) $f^{-1}([x]) = [x]$ であることを示せ。

4.4.2 $f : X \longrightarrow Y$ を全射とする。$a, b \in X$ について $a \sim b \Leftrightarrow f(a) = f(b)$ とする。

(a) $\sim$ は X の同値関係であることを示せ。

(b) 上の同値関係について a の属する同値類を $[a]$ で表すとする。このとき、任意の $a \in X$ について、$f^{-1}(f(a)) = [a]$ であることを示せ。

(c) Y の要素は $f(a), a \in X$ と表されるから、$g : Y \to P(X)$ を $g(f(a)) = [a]$ と定義するとこれは、写像 (well-defined) であって[3]、かつ単射であることを示せ。

(d) 上で定めた同値関係の同値類全体の集合を $X/\sim = \{[x] \mid x \in X\} \subseteq P(X)$ で表す。このとき、$\bar{f}$ を

$$\bar{f} : X/\sim \longrightarrow Y \ ([x] \mapsto f(x))$$

と定義する。すると $\bar{f}$ は全単射であることを示せ[4]。

[3] Y の要素 b を $f(a)$ と表す表し方は一通りではないかも知れない。$b = f(a) = f(a')$ とすると $g(f(a)) = g(b) = g(f(a'))$ であることを示して下さい。

[4] $x \neq x'$ であっても $[x] = [x']$ である場合もあるので、$[x] = [x']$ ならば $f(x) = f(x')$ も確かめる必要があることに注意。

5　数学的帰納法 (Mathematical Induction)

以下の命題・公式を数学的帰納法を用いて証明せよ。

5.0.1 $q_1, q_w, \ldots, q_n$ を命題とする。このとき、

(a) $\sim(q_1 \wedge q_2 \wedge \cdots \wedge q_n) \equiv (\sim q_1) \vee (\sim q_2) \vee \cdots \vee (\sim q_n)$.

(b) $\sim(q_1 \vee q_2 \vee \cdots \vee q_n) \equiv (\sim q_1) \wedge (\sim q_2) \wedge \cdots \wedge (\sim q_n)$.

5.0.2 $1 + 2 + 3 + \cdots + n = \dfrac{1}{2}n(n+1)$.

5.0.3 $1^2 + 2^2 + 3^2 + \cdots + n^2 = \dfrac{1}{6}n(n+1)(2n+1)$.

5.0.4 $1^3 + 2^3 + 3^3 + \cdots + n^3 = (\dfrac{1}{2}n(n+1))^2$.

5.0.5 $\displaystyle\sum_{k=1}^{n} k^5 + \sum_{k=1}^{n} k^7 = 2\Big(\sum_{k=1}^{n} k\Big)^4$.

5.0.6 $11^{n+2} + 12^{2n+1}$ は、$n \geq 0$ の時、133 で割り切れる。

5.0.7 $x = \cos\theta$ とすると、$n \in \boldsymbol{Z}^+$ について、$\cos n\theta$ は、x に関する丁度 n 次の x に関する多項式 $T_n(x)$ で表すことができることを証明せよ[5]。次数が丁度 n となることも忘れずに。$T_0(x) = 1$, $T_1(x) = x$, $T_2(x) = \cos 2\theta = 2\cos^2\theta - 1 = 2x^2 - 1$, $T_3(x) = 4x^3 - 3x, \ldots$.　（ヒント：$\cos(n+1)\theta + \cos(n-1)\theta = 2\cos n\theta\cos\theta$. ）

5.0.8 $x = \cos\theta$ とすると、$n \in \boldsymbol{Z}^+$ について $\sin(n+1)\theta / \sin\theta$ は、丁度 n 次の x に関する多項式、$U_n(x)$ で表すことができることを証明せよ[6] 。

5.0.9 サイズ $2^n \times 2^n$ のチェス盤から一ますを抜き取ったものを B_n と呼ぶことにすると、すべての、B_n は、B_1 で敷き詰めることができる。

5.0.10 サイズ $2^n \times 2^n \times 2^n$ のブロックから一ブロックを抜き取ったものを T_n と呼ぶことにすると、すべての、T_n は、T_1 で埋め尽くすことができる。

5.0.11 $\displaystyle 1 + \frac{1}{2^3} + \frac{1}{3^3} + \cdots + \frac{1}{n^3} \leq \frac{1}{2}\left(3 - \frac{1}{n^2}\right)$.

5.0.12 $F_1 = 1$, $F_2 = 1$, $F_{n+2} = F_{n+1} + F_n$ で定まる数列をフィボナッチ数列 (Fibonacci Series) という。

(a) F_n は偶数 $\Leftrightarrow$ n は 3 の倍数。

---

[5] $\{T_n(x) \mid n = 0, 1, \ldots\}$ は第一種のチェビシェフ多項式 (Tchebichef polynomials of the first kind) と言います。$m \neq n$ のとき、$\int_{-1}^{1} T_m(x)T_n(x)(1-x^2)^{-1/2}dx = 0$ となっています。

[6] $\{U_n(x) \mid n = 0, 1, \ldots\}$ は第二種のチェビシェフ多項式 (Tchebichef polynomials of the second kind) と言います。$m \neq n$ のとき $\int_{-1}^{1} U_m(x)U_n(x)(1-x^2)^{1/2}dx = 0$ となっています。

(b) $F_n = \dfrac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{2^n\sqrt{5}}$.

6　集合の濃度

この節では特に断らない限り $\boldsymbol{N}$ は正の整数を表すものとする。また、集合 A から集合 B への全単射が存在するとき、$A \sim B$ と書く。集合 A から 集合 B への写像全体からなる集合を B^A または $\mathrm{Map}(A, B)$ と書く。

6.1　集合の対等

6.1.1 集合に定義された関係 $\sim$ は同値関係であることを証明せよ。

6.1.2 A, B, C, D を $A \sim C$ かつ $B \sim D$ なる集合とする。

(a) $A \cap B = \emptyset = C \cap D$ ならば $A \cup B \sim C \cup D$ であることを示せ。

(b) $A \times B \sim C \times D$ であることを示せ。

(c) $P(A) \sim P(C)$ であることを示せ。

(d) $B^A \sim D^C$ すなわち $\mathrm{Map}(A, B) \sim \mathrm{Map}(C, D)$ であることを示せ。

(e) $P(A) \sim \mathrm{Map}(C, \{0, 1\})$ であることを示せ。

6.1.3 $n \in \boldsymbol{N}$ のとき $I(n) = \{x \mid (x \in \boldsymbol{N}) \wedge (x \leq n)\}$ とする。 $m, n \in \boldsymbol{N}$ に対して、$I(m) \sim I(n)$ ならば $m = n$ であることを証明せよ。(ヒント：$m \geq n$ とし、n に関する数学的帰納法を用いよ。)

6.2　可算集合

6.2.1 $F = \{x \mid (x \in \boldsymbol{N}) \wedge (x \geq 5)\}$ とすると、$F \sim \boldsymbol{N}$ すなわち、 $|F| = \aleph_0$ であることを示せ。

6.2.2 $\boldsymbol{Z} \sim \boldsymbol{N}$ すなわち $|\boldsymbol{Z}| = \aleph_0$ であることを示せ。

6.2.3 $E = \{x \mid (x \in \boldsymbol{Z}) \wedge (\exists q)[(q \in \boldsymbol{Z}) \wedge (x = 2q)\}$ とする。このとき、$E \sim \boldsymbol{N}$ すなわち、$|E| = \aleph_0$ であることを示せ。(E は $2\boldsymbol{Z}$ とも書かれる。ここでは、the set of even integers の E を用いた。)

6.2.4 $T = \{x \mid (x \in \boldsymbol{Z}) \wedge (\exists q)[(q \in \boldsymbol{Z}) \wedge (x = 3q + 1)\}$ とする。このとき、$T \sim \boldsymbol{N}$ すなわち、$|T| = \aleph_0$ であることを示せ。(T は、$1 + 3\boldsymbol{Z}$ とも書かれる。)

6.2.5 $S = \{x \mid (x \in \boldsymbol{Z}) \wedge (\exists y)[(y \in \boldsymbol{Z}) \wedge (x = y^2)\}$ とする。このとき、$S \sim \boldsymbol{N}$ すなわち、$|S| = \aleph_0$ であることを示せ。(Hint: $S = \{0, 1, 4, 9, \cdots\}$)

6.2.6 $n \in \boldsymbol{N}$ としたとき、$I(n)$ は $\boldsymbol{N}$ とは対等ではないことを示せ。(ヒント：$I(n)$ の空でない部分集合で、$I(n)$ と異なるものに対しては、ある自然数 m で $I(m)$ と等値となるものが存在することを用いよ。)

6.2.7 X を可算無限集合とする。集合 A から X への単射が存在すれば、A は可算集合（有限または可算無限）であることを示せ。

6.2.8 X を可算無限集合とする。集合 X から A への全射が存在すれば、A は可算集合（有限または可算無限）であることを示せ。

6.3 無限集合

6.3.1 任意の無限集合は可算無限部分集合を含むことを証明せよ。

6.3.2 無限集合はそれ自身と対等な真部分集合を含むことを証明せよ。

6.3.3 X が無限集合、A が X の高々可算な部分集合で、$X-A$ が無限集合ならば $X-A$ と X は対等であることを証明せよ。

6.3.4 X が無限集合、Y が可算集合（高々可算）ならば $X \cup Y$ と X は対等であることを証明せよ。

6.4 いろいろな集合の対等

6.4.1 $X = \{(a,b,c,d) \mid a,b,c,d \in \boldsymbol{Z},\ 1 \leq a \leq b \leq c \leq d \ \leq 10\}$、$Y = \{(\alpha,\beta,\gamma,\delta) \mid \alpha,\beta,\gamma,\delta \in \boldsymbol{Z},\ 1 \leq \alpha < \beta < \gamma < \delta \leq 13\}$ としたとき、X から Y への全単射を与えることによって、$|X| = |Y|$ であることを示せ。

6.4.2 $g : \boldsymbol{N} \times \boldsymbol{N} \longrightarrow \boldsymbol{N}$ $((m,n) \mapsto g(m,n) = 2^{m-1}(2n-1))$ は 全単射であることを証明せよ。

6.4.3 $h : \boldsymbol{N} \times \boldsymbol{N} \longrightarrow \boldsymbol{N}$ $((m,n) \mapsto h(m,n) = \dfrac{(m+n-1)(m+n-2)}{2} + n)$ は 全単射であることを証明せよ。（ヒント：具体的に、m, n が小さいときに、$h(m,n)$ を計算してみよ。）

6.4.4 前問の逆写像 $h^{-1} : \boldsymbol{N} \longrightarrow \boldsymbol{N} \times \boldsymbol{N}$ を決定せよ。

6.4.5 $f : \boldsymbol{N}^4 = \boldsymbol{N} \times \boldsymbol{N} \times \boldsymbol{N} \times \boldsymbol{N} \to \boldsymbol{N}$ $((a,b,c,d) \mapsto 2^{a-1} \cdot 3^{b-1} \cdot 5^{c-1} \cdot 7^{d-1})$ は単射であることを示せ。これより、$|\boldsymbol{N}^4| = \aleph_0$ であることが証明できる。

6.4.6 $\boldsymbol{Z} \times \boldsymbol{Z} \sim \boldsymbol{Z}$ であることを具体的な全単射を定義することによって示せ。

6.4.7 $|\boldsymbol{Z} \times \boldsymbol{Z} \times \boldsymbol{Z}| = \aleph_0$ であることを示せ。

6.4.8 $|\boldsymbol{Q}| = \aleph_0$ であることを示せ。

6.4.9 A および B を可算集合とすると、$A \times B$ も可算集合であることを示せ。

6.4.10 A および B が可算集合でそのうち一方が無限集合ならば $|A \times B| = \aleph_0$ であることを示せ。

6.4.11 $f(x) = e^x$ を用いて、$R = (-\infty, \infty)$ と、$(0, \infty)$ の濃度が等しいことを示せ。

6.4.12 $a < b$ なる実数 a, b に対して、開区間 (a, b) を $(a, b) = \{x \mid x \in \boldsymbol{R}, a < x < b\}$ と定義する。任意の実数 c, d $(c < d)$ に対して、(a, b) と (c, d) が対等 (equipollent) であることを示せ。(Hint: $f(x) = mx + n$ が (a, b) から (c, d) への全単射になるように $m, n \in \boldsymbol{R}$ を決めよ。)

6.4.13 閉区間 $[-\pi/2, \pi/2]$ と $[-1, 1]$ が対等になることを三角関数を用いて示せ。

6.4.14 閉区間 $[a, b]$ と $[c, d]$ $(a < b,\ c < d)$ が対等となることを三角関数を用いて示せ。

6.4.15 開区間 $(-1, 1)$ と実数全体の集合 $\boldsymbol{R}$ が対等であることを具体的に全単射を与えることによって示せ。(Hint: $f(x) = \frac{x}{1-x^2}$)

6.4.16 開区間 (a, b) と 実数全体の集合 $\boldsymbol{R}$ が対等であることを、三角関数を用いて具体的な全単射を与えることによって示せ。

6.4.17 閉区間 $[0, 1]$ と、開区間 $(0, 1)$ は同じ濃度をもつことを具体的な全単射を構成して証明せよ。(ヒント：例えば $A = \{(1/2)^n \mid n = 0, 1, 2, \ldots\} \cup \{0\}$ とし A から $A \cap (0, 1)$ への全単射を構成し、あとは、$[0, 1] - A = (0, 1) - A$ を用いる。)

6.4.18 閉区間 $[a, b]$ と実数全体の集合 $\boldsymbol{R}$ は同じ濃度を持つことを具体的な全単射を構成して証明せよ。

6.4.19 閉区間 $[a, b]$ と開区間 (c, d) $(a < b,\ c < d)$ が同じ濃度を持つことを具体的な全単射を構成して証明せよ。

7 濃度の比較

7.1 濃度の大小

7.1.1 $A \sim C$, $B \sim D$ である集合 A, B, C, D において、A から B への単射が存在すれば、C から D への単射も存在することを示せ。

7.1.2 $|A| \leq |C|$, $|B| \leq |D|$ なる集合 A, B, C, D について次を示せ。

(a) $|P(A)| \leq |P(C)|$。

(b) $|A \times B| \leq |C \times D|$。

(c) $|B^A| \leq |D^C|$ すなわち、$|Map(A, B)| \leq |Map(C, D)|$。

7.1.3 A を集合とするとき、$|A| \leq |P(A)|$。

7.2 Cantor–Bernsteinの定理

以下のそれぞれの問題を Cantor–Bernstein の定理を用いて示せ。

7.2.1 集合の濃度の間の関係 $\leq$ が順序関係になることを示せ。

7.2.2 a, b を $a < b$ なる実数とする。閉区間 $[a, b] = \{x \mid x \in \boldsymbol{R}, a \leq x \leq b\}$ は $\boldsymbol{R}$ と対等であることを示せ。

7.2.3 閉区間 $[0, 1]$ と閉区間 $(0, 1)$ とが対等であることを示せ。

7.2.4 閉区間 $[a, b]$ $(a < b)$ と、$\boldsymbol{R}$ は対等であることを示せ。

7.2.5 閉区間 $I_n = [2n, 2n + 1]$ とする。この時、$I_0 = [0, 1]$ は、$\bigcup_{n=0}^{\infty} I_n$ と対等であることを示せ。

7.2.6 集合 A, B, C について $|A| \leq |B| \leq |C|$ かつ $|A| = |C|$ ならば $|A| = |B|$, $|B| = |C|$ であることを示せ。

7.2.7 $\boldsymbol{Q}$ を有理数全体の集合、$\boldsymbol{Z}$ を整数全体の集合とする。$|\boldsymbol{N}| \leq |\boldsymbol{Q}| \leq |\boldsymbol{Z} \times \boldsymbol{N}|$ を示せ。

7.2.8 A, B, C, D を集合とする。

(a) $A \sim C$ かつ $A \times B \sim C \times D$ ならば $B \sim D$ か。正しければ証明し、誤っていれば、反例をあげよ。

(b) $A \sim C$、$A \cap B = \emptyset = C \cap D$ かつ $A \cup B \sim C \cup D$ であるとき、$B \sim D$ か。正しければ証明し、誤っていれば、反例をあげよ。

(c) $A \sim C$ かつ $\mathrm{Map}(A, B) \sim \mathrm{Map}(C, D)$ ならば $B \sim D$ か。正しければ証明し、誤っていれば、反例をあげよ。

(d) $B \sim D$ かつ $\mathrm{Map}(A, B) \sim \mathrm{Map}(C, D)$ ならば $A \sim C$ か。正しければ証明し、誤っていれば、反例をあげよ。

7.3 非可算集合

7.3.1 $|\boldsymbol{Q}| < |\boldsymbol{R}|$ であることを示せ。

7.3.2 $|P(\boldsymbol{Q})| < |P(\boldsymbol{R})|$ であることを示せ。

7.3.3 A を空でない集合とするとき、$|A| < |\mathrm{Map}(A, A)|$ であることを示せ。

7.3.4 E を正の偶数全体の集合、O を正の奇数全体の集合とする。$\boldsymbol{N} = E \cup O$ かつ $E \cap O = \emptyset$ であるが、$A \subseteq \boldsymbol{N}$ に対して、$(A \cap E, A \cap O)$ を対応させる $P(\boldsymbol{N})$ から $P(E) \times P(O)$ への写像は全単射であることを示せ。

7.3.5 無理数全体の集合は実数全体の集合と対等であることを証明せよ。

7.3.6 $|\boldsymbol{R}| = |\boldsymbol{R} \times \boldsymbol{R}|$ を示せ。

7.3.7 $|\boldsymbol{C}| = |\boldsymbol{R}|$ を示せ。

7.3.8 $\boldsymbol{R}$ の n 個の直積 $\boldsymbol{R} \times \boldsymbol{R} \times \cdots \times \boldsymbol{R}$ を $\boldsymbol{R}^n$ とかく。任意の自然数 n に対して $|\boldsymbol{R}^n| = |\boldsymbol{R}|$ を示せ。

7.3.9 $x \in \boldsymbol{R}$ に対して、$B(x) = \{r \mid (r \in \boldsymbol{Q}) \wedge (r > x)\}$ とおく。すると、$B : \boldsymbol{R} \to P(\boldsymbol{Q})$ は単射であることを示せ。これより、$|\boldsymbol{R}| \leq |P(\boldsymbol{Q})|$ がわかる。

7.3.10 $\boldsymbol{N}$ の有限部分集合全体を $P_0(\boldsymbol{N})$ で表すとする。このとき、$|P_0(\boldsymbol{N})| = |\boldsymbol{Q}| = |\boldsymbol{N}|$ であることを証明せよ。

7.3.11 整数係数の多項式全体の濃度は、$\aleph_0$ であることを示せ。(Hint: $f(x) = a_0, +a_1 x + \cdots + a_n x^n$ $(a_0, a_1, \ldots, a_n \in \boldsymbol{Z},\ a_n \neq 0)$ を n 次の整数係数の多項式とする。$h(f) = |a_0| + |a_1| + \cdots + |a_n|$ を f の高さ (height) と呼ぶことにする。$X_{n,h}$ で次数が n で高さが h の整数係数の多項式全体を表すとすると、$|X_{n,h}|$ は有限であることを利用せよ。)

7.3.12 整数係数の多項式の根となるような複素数を代数的数という。それ以外を超越数という。A を代数的数の全体からなる集合とすると、A の濃度は $\aleph_0$ であることを示せ。

7.3.13 超越数全体の濃度は $\aleph$ であることを証明せよ。すなわち、T を超越数の集合とすると、$T \sim \boldsymbol{C}$。

7.3.14 RT を超越数で実数であるもの全体のなす集合とする。このとき、$RT \sim \boldsymbol{R}$ すなわち、$|RT| = \aleph$ であることを示せ。

7.3.15 $\mathrm{Map}(X, \mathrm{Map}(Y, Z)) \sim \mathrm{Map}(X \times Y, Z)$ を示せ。

7.3.16 $|P(\boldsymbol{N})| = |\mathrm{Map}(\boldsymbol{N}, \boldsymbol{N})| = |\mathrm{Map}(\boldsymbol{N}, \boldsymbol{R})|$ であることを示せ。

7.3.17 $|P(\boldsymbol{R})| = |\mathrm{Map}(\boldsymbol{R}, \boldsymbol{N})| = |\mathrm{Map}(\boldsymbol{R}, \boldsymbol{R})| = |\mathrm{Map}(\boldsymbol{R}, P(\boldsymbol{R}))|$ であることを示せ。

8 整数

以下において、$a, b \in \boldsymbol{Z}$ に対し、$a \mid b \Leftrightarrow (\exists c \in \boldsymbol{Z})[b = ac]$、また、$a_1, a_2, \ldots, a_n \in \boldsymbol{Z}$ に対し、$\gcd\{a_1, a_2, \ldots, a_n\}$ は、授業 (Handout 参照) で定義した最大公約数、$\langle a_1, a_2, \ldots, a_n\rangle = \{a_1x_1 + a_2x_2 + \cdots + a_nx_n \mid x_1, x_2, \ldots, x_n \in \boldsymbol{Z}\}$、 すなわち、$a_1, a_2, \ldots, a_n$ の 整数係数の一次結合で書けるもの全体の集合を表すものとする。また、次の性質を満たす $\ell \in \boldsymbol{Z}$ を $a_1, a_2, \ldots, a_n$ の最小公倍数 (the least common multiple) といい $\ell = \mathrm{lcm}\{a_1, a_2, \ldots, a_n\}$ と書く。 (i) $\ell \geq 0$. (ii) $a_1 \mid \ell, a_2 \mid \ell, \ \ldots\ , \ a_n \mid \ell$. (iii) $a_1 \mid c, a_2 \mid c, \ \ldots\ , \ a_n \mid c$ ならば $\ell \mid c$.

8.1 整数の整除

8.1.1 $\langle 28, 35\rangle = \{7m \mid m \in \boldsymbol{Z}\}$ であることを示せ。

8.1.2 $\langle 21, -15\rangle = \{3m \mid m \in \boldsymbol{Z}\}$ であることを示せ。

8.1.3 $\langle 8, -12, 18\rangle = \{2m \mid m \in \boldsymbol{Z}\}$ であることを示せ。

8.1.4 $a, b, q, r \in \boldsymbol{Z}$ で、$a = bq + r$ が成立しているとする。このとき、$\langle a, b\rangle = \langle b, r\rangle$ であることを示せ。

8.1.5 $a, b \in \boldsymbol{Z}$ とし、$d = \gcd\{a, b\}$ とするとき、$\langle a, b\rangle = \{dm \mid m \in \boldsymbol{Z}\}$ であることを示せ。

8.1.6 a, b, cを整数とする。方程式$ax+by = c$が整数解x, yをもつこと（すなわち、$ax+by = c$ となる整数 x, y が存在すること）と、a と bの最大公約数 $\gcd\{a, b\}$ が c を割り切ることとは同値であることを証明せよ。

8.1.7 次の整数の組 (a, b) に対して、ユークリッドの互除法を用いて a, b の最大公約数 d を求め、d を $ar + bs$ $(r, s \in \boldsymbol{Z})$ の形に表せ。

(a) $a = 7$, $b = 11$. (b) $a = -28$, $b = -63$. (c) $a = 91$, $b = 126$.
(d) $a = 7245$, $b = 4784$.

8.1.8 $a_1, a_2, \ldots, a_n, a_{n+1}, k \in \boldsymbol{Z}$ とする。この時、次が成立することを示せ。

(a) $\gcd\{a_1, a_2, \ldots, a_n, 1\} = 1$, $\gcd\{a_1, a_2, \ldots, a_n, 0\} = \gcd\{a_1, a_2, \ldots, a_n\}$.

(b) $\gcd\{k \cdot a_1, k \cdot a_2, \ldots, k \cdot a_n\} = |k| \cdot \gcd\{a_1, a_2, \ldots, a_n\}$.

(c) $\gcd\{a_1, a_2, \ldots, a_n, a_{n+1}\} = \gcd\{\gcd\{a_1, a_2, \ldots, a_n\}, a_{n+1}\}$.

(d) $\langle a_1, a_2, \ldots, a_n, a_{n+1}\rangle = \{ax + a_{n+1}y \mid a \in \langle a_1, a_2, \ldots, a_n\rangle, x, y \in \boldsymbol{Z}\}$.

8.1.9 3 つの整数 $6, 14, 21$ の最大公約数 d を求め、d を $6r + 14s + 21t$ $(r, s, t \in \boldsymbol{Z})$ の形で表せ。

8.1.10 $a_1, a_2, \ldots, a_n \in \boldsymbol{Z}$ は全ては零でない（少なくとも一つは零でない）とする。このとき、$\langle a_1, a_2, \ldots, a_n \rangle$ の元のうちで、正の整数で一番小さいものを d とすると、$d = \gcd\{a_1, a_2, \ldots, a_n\}$ であることを示せ。

8.1.11 $a_1, a_2, \ldots, a_n \in \boldsymbol{Z}$ とする。このとき、$c \in \langle a_1, a_2, \ldots, a_n \rangle$、すなわち、$a_1x_1 + a_2x_2 + \cdots + a_nx_n = c$ が整数解、$x_1, x_2, \ldots, x_n$ を持つこと（すなわち、$a_1x_1 + a_2x_2 + \cdots + a_nx_n = c$ となる整数の組み $x_1, x_2, \ldots, x_n$ が存在すること）と、$d \mid c$ であることとは同値であることを示せ。ただし、$d = \gcd\{a_1, a_2, \ldots, a_n\}$ とする。

8.1.12 $a, b, c \in \boldsymbol{Z}$ とするとき、次を示せ。

(a) $\gcd\{a, b\} = 1 \Leftrightarrow \gcd\{a + bc, b\} = 1$.

(b) $\gcd\{a, c\} = \gcd\{b, c\} = 1 \Leftrightarrow \gcd\{ab, c\} = 1$.

(c) $\gcd\{a, b\} = 1 \wedge a \mid c \wedge b \mid c \Rightarrow ab \mid c$.

(d) p を素数（すなわち、$(p \in \boldsymbol{Z}) \wedge (p \geq 2) \wedge (\forall x \in \boldsymbol{Z})[(x > 0) \wedge (x \mid p) \Rightarrow (x = 1) \vee (x = p)]$、2 以上の整数で、正の約数は 1 またはそれ自身であるもの）とする。このとき、 $p \mid ab \Rightarrow (p \mid a) \vee (p \mid b)$.

8.1.13 p を素数とする。$\sqrt{p}$ は無理数であることを示せ。

8.1.14 p と q を相異なる素数とする。$\sqrt{pq}$ は無理数であることを示せ。

8.1.15 $a, b \in \boldsymbol{Z}$ とし、$\ell = \mathrm{lcm}\{a, b\}$ とする。この時、次を示せ。

$$\{ax \mid x \in \boldsymbol{Z}\} \cap \{by \mid y \in \boldsymbol{Z}\} = \{\ell z \mid z \in \boldsymbol{Z}\}$$

8.1.16 $a_1, a_2, \ldots, a_n, a_{n+1} \in \boldsymbol{Z}$ とする。この時、次が成立することを示せ。

(a) $\mathrm{lcm}\{a_1, a_2, \ldots, a_n, 1\} = \mathrm{lcm}\{a_1, a_2, \ldots, a_n\}$, $\mathrm{lcm}\{a_1, a_2, \ldots, a_n, 0\} = 0$.

(b) $\mathrm{lcm}\{k \cdot a_1, k \cdot a_2, \ldots, k \cdot a_n\} = |k| \cdot \mathrm{lcm}\{a_1, a_2, \ldots, a_n\}$.

(c) $\mathrm{lcm}\{a_1, a_2, \ldots, a_n, a_{n+1}\} = \mathrm{lcm}\{\mathrm{lcm}\{a_1, a_2, \ldots, a_n\}, a_{n+1}\}$.

8.1.17 a, b を 0 でない整数とする。$\gcd\{a, b\} \cdot \mathrm{lcm}\{a, b\} = ab$ を示せ。

8.1.18 $2^n - 1$ が素数ならば、n は素数であることを示せ。

8.1.19 $2^n + 1$ $(n \geq 1)$ が素数ならば、非負の整数 k を用いて、$n = 2^k$ と表せることを示せ。

8.1.20 次のそれぞれについて、正しければ証明し、常には成立しなければ反例を示せ。

(a) すべての整数 n に対して、$\gcd\{4n + 5, 3n + 4\} = 1$。

(b) $a, b \in \boldsymbol{Z}$ とするとき、$a^2 \mid b^2 \Leftrightarrow a \mid b$。

(c) $a, b \in \boldsymbol{Z}$ とするとき、$\gcd\{a, b\} = \gcd\{a + b, \mathrm{lcm}\{a, b\}\}$。

(d) $a, b, c \in \boldsymbol{Z}$ とするとき、$\gcd\{a, b\} \cdot \gcd\{ab, c\} = \gcd\{a.c\} \cdot \gcd\{b, c\}$。

(e) $a, b, c \in \boldsymbol{Z}$ とするとき、$\mathrm{lcm}\{\gcd\{a, b\}, \gcd\{a, c\}\} = \gcd\{a, \mathrm{lcm}\{b, c\}\}$。

9 m を法とした合同

m を正の整数とする。$a, b \in \boldsymbol{Z}$ に対して、$a \equiv b \Leftrightarrow m \mid b-a$ とすると、$\equiv$ は、$\boldsymbol{Z}$ 上の同値関係となる。m を明記するため、$a \equiv b \pmod{m}$ と書くこともある。$a \in \boldsymbol{Z}$ を含む同値類を $[a] = [a]_{\equiv}$ と書き、この同値類全体を、$\boldsymbol{Z}_m = \{[a] \mid a \in \boldsymbol{Z}\}$ とする。

9.1 整数の合同 (congruences)

9.1.1 $m \in \boldsymbol{Z}$, $m > 0$ とし、$\boldsymbol{Z}_m$ において、次を示せ。

(a) $a \equiv b \Leftrightarrow a \in [b] \Leftrightarrow [a] = [b]$.

(b) $[a] = [a'] \wedge [b] = [b'] \Rightarrow [a+b] = [a'+b']$. （この事実により、$[a] + [b] = [a+b]$ として、$\boldsymbol{Z}_m$ に和を定義する。）

(c) $[a] = [a'] \wedge [b] = [b'] \Rightarrow [a \cdot b] = [a' \cdot b']$. （この事実により、$[a] \cdot [b] = [a \cdot b]$ として、$\boldsymbol{Z}_m$ に積を定義する。）

9.1.2 $m \in \boldsymbol{Z}$, $m > 0$, $[a], [b], [c] \in \boldsymbol{Z}_m$ とする。次を示せ：

(a) $([a] + [b]) + [c] = [a] + ([b] + [c])$.

(b) $[0] + [a] = [a] = [a] + [0]$.

(c) $[a] + [-a] = [0]$.

(d) $[a] + [b] = [b] + [a]$,

(e) $([a][b])[c] = [a]([b][c])$.

(f) $[1][a] = [a]$.

(g) $([a] + [b])[c] = [a][c] + [b][c]$, $[c]([a] + [b]) = [c][a] + [c][b]$.

(h) $[a][b] = [b][a]$.

9.1.3 $\boldsymbol{Z}_6$ の加法表 (addition table) と乗法表 (multiplication table) を作れ。

9.1.4 $a \in \boldsymbol{N}$ を 10 進法であらわしたものを、$a = \sum_{i=0}^{n} a_i 10^i$ $(a_i \in \{0, 1, 2, \ldots, 9\})$ とする。このとき、以下を示せ。

(a) $a \equiv \sum_{i=0}^{n} a_i \pmod{3}$ である。すなわち、a を 3 で割った余り（剰余）は、桁ごとに足したものを 3 で割った余りと等しい。

(b) $a \equiv \sum_{i=0}^{n} a_i \pmod{9}$ である。すなわち、a を 9 で割った余り（剰余）は、桁ごとに足したものを 9 で割った余りと等しい。

(c) $a \equiv \sum_{i=0}^{n} (-1)^i a_i \pmod{11}$ である。すなわち、a を 11 で割った余り（剰余）は、一桁目から２桁目を引き、３桁目を足し、と交互に和と差を取っていたものを、 11 で割った余りと等しい。

9.1.5 一般に、$\boldsymbol{Z}_m$ の元 $[x]$ に対して、$[x][y] = [1]$ をみたす $[y]$ を $[x]$ の逆元 (inverse) といい、逆元をもつような元 $[x]$ のことを正則元 (invertible element) とよぶ。$\boldsymbol{Z}_m$ の正則元全体の集合を $\boldsymbol{Z}_m^*$ と書く。

(a) $[x]$ の逆元は存在するならば、一意的 (unique) に存在することを示せ。

(b) $[x]$ と $[y]$ が正則元ならば、$[x][y]$ も正則元であることを示せ。

(c) $\boldsymbol{Z}_6$ の正則元と、それぞれの逆元をすべて求めよ。

(d) $\boldsymbol{Z}_7$ の正則元と、それぞれの逆元をすべて求めよ。

(e) $\boldsymbol{Z}_9$ の正則元と、それぞれの逆元をすべて求めよ。

(f) $\boldsymbol{Z}_{24}$ における、[7], [13] の逆元をそれぞれ求めよ。

(g) p を素数とすると、$\boldsymbol{Z}_p^* = \boldsymbol{Z}_p - \{[0]\}$ であることを示せ。

(h) $\boldsymbol{Z}_m^* = \{[a] \mid a \in \boldsymbol{Z},\ \gcd\{a, m\} = 1\}$ であることを示せ。

9.1.6 $a \in \boldsymbol{Z}$ とし、$\ell_a : \boldsymbol{Z}_m \to \boldsymbol{Z}_m$ $([x] \mapsto [a + x])$ とする。このとき、ℓ_a は全単射であることを示せ。

9.1.7 $a \in \boldsymbol{Z}$ とし、$\mu_a : \boldsymbol{Z}_m \to \boldsymbol{Z}_m$ $([x] \mapsto [a \cdot x])$ とする。このとき、μ_a が全単射であることと $[a] \in \boldsymbol{Z}_m^*$ すなわち、$[a]$ が正則元であることとは同値であることを示せ。

9.1.8 $a \in \boldsymbol{Z}_m^*$ とし、$\psi_a : \boldsymbol{Z}_m^* \to \boldsymbol{Z}_m^*$ $([x] \mapsto [ax])$ は、全単射であることを示せ。

9.1.9 p を素数とする。$a \in \boldsymbol{Z}$ で、a は p で割り切れないものとする。このとき、$\boldsymbol{Z}_p$ において、$\{[1], [2], \ldots, [p-1]\} = \{[a], [2a], \ldots, [(p-1)a]\}$ であることを示せ。

9.1.10 p を素数とする。$a \in \boldsymbol{Z}$ で、a は p で割り切れないものとする。このとき、$\boldsymbol{Z}_p$ において、$[a^{p-1}] = [1]$、すなわち、$a^{p-1} \equiv 1 \pmod{p}$ であることを示せ。

9.1.11 p を素数とする。$a \in \boldsymbol{Z}$ とする。このとき、$\boldsymbol{Z}_p$ において、$[a^p] = [a]$、すなわち、$a^p \equiv a \pmod{p}$ であることを示せ。

9.1.12 $a \in \boldsymbol{Z}_m^*$ とし、$|\boldsymbol{Z}_m^*| = t$ と書くことにすると、$[a^t] = [1]$ であることを示せ。すなわち、$a^t \equiv 1 \pmod{m}$。この定理をオイラーの定理という。(ヒント：前問をもちい、$\boldsymbol{Z}_m^* = \{[a_1], [a_2], \ldots, [a_t]\}$ とすると、$\boldsymbol{Z}_m^* = \{[aa_1], [aa_2], \ldots, [aa_t]\}$。これらの元をすべてかけ、それらが等しいことを用いよ。)

9.1.13 $n^2 \equiv a \pmod{7}$ となる整数 n が存在するならば、$a \equiv 0, 1, 2, 4 \pmod{7}$ であることを示せ。

9.1.14 $3n^7 + n^2 + 4n + 2 \equiv 0 \pmod{7}$ となる整数 n は存在しないことを示せ。

9.1.15 $n \in \boldsymbol{Z}$ とするとき、$3n^7 + 7n^3 + 11n \equiv 0 \pmod{21}$ であることを示せ。(ヒント：$\boldsymbol{Z}_3$ と、$\boldsymbol{Z}_7$ でまず考えよ。)

9.1.16 $n \in \boldsymbol{Z}$ とすると、$\boldsymbol{Z}_4$ において、$[n^2] \in \{[0],[1]\}$ であることを示せ。

9.1.17 n が奇数のとき、$n^2 \equiv 1 \pmod 8$ を証明せよ。

9.1.18 整数 x, y, z が $x \neq 0, y \neq 0, z \neq 0$ かつ $\gcd\{x, y, z\} = 1$ をみたすものとする。$x^2+y^2 = 6z^2$ が成立するような x, y, z は存在するか。

9.1.19 n を整数とする。$4n+3$ は二つの平方数の和で表せないことを示せ。

9.1.20 p を奇素数とする。$\boldsymbol{Z}_p$ において、$[x]^2 = [1]$ の解 $[x]$ は二つしか存在しないことを示せ。

9.1.21 $4n+3$ と書ける素数は無限に存在することを示せ。(ヒント：そのような素数は有限個だとし、$p_1 = 3, p_2 = 7, \ldots, p_n$ とする。ここで、$\ell = 4 \cdot 7 \cdot p_3 \cdots p_n + 3$ とし、$\boldsymbol{Z}_4$ で考え、ℓ の約数の中に、$4n+3$ の形の素数で、$p_1, p_2, \ldots, p_n$ のいずれでもないものがあることを示せ。)

9.1.22 $6n+5$ と書ける素数は無限に存在することを示せ。

9.1.23 ISBN (International Standard Book Number) $a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}$ は、4つに区切られた 0 から 10 までの 10 桁の数字で表される。ただし、10 は X で記される。たとえば、$3-11-017544-4$、$4-7561-1667-1$。最初の一桁は言語、次の組が出版社、次が本の番号、最後は次のようにして決められた数である。

$$a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6 + 7a_7 + 8a_8 + 9a_9 + 10a_{10} \equiv 0 \pmod{11}$$

次のそれぞれの最後または途中の桁を決定せよ。

(a) $0-13-184868-?$、(b) $4-?77-01651-X$。

9.1.24 次の連立合同式を解け。

$$\text{(a)} \begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 4 \pmod 5 \end{cases} \qquad \text{(b)} \begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 3 \pmod 5 \\ x \equiv 3 \pmod 7 \end{cases} \qquad \text{(c)} \begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 5 \pmod{11} \\ x \equiv 12 \pmod{13} \end{cases}$$