

0 「数学」の講義について

この講義で取り扱う内容は

- ・ 集合と写像
- ・ 命題と論理
- ・ 代数学の話 (整数の話, 出来れば暗号の話)
- ・ 幾何学の話 (一筆書きや多面体の Euler の定理など)
- ・ 解析学の話 (数列と関数の極限, 実数の話)

を扱う.

教材はプリントをインターネットにて配布する. PDF ファイルなので, Acrobat Reader が必要 (たいていのパソコンにはインストールされている)

ホームページのアドレスは

<http://www.ne.jp/asahi/kitty/shiro/>

mail address : ibuki@kobe.email.ne.jp

ibuki@econ.u-hyogo.ac.jp

k.ibuki@ezweb.ne.jp (ケイタイからのメールのみ受信可能)

関連図書

- [1] 樋口禎一ほか著「現代数学の基礎」牧野書店 1994 年
数理情報科学シリーズ 7 1,700 円
- [2] 日本大学文理学部数学科編「数学基礎セミナー」日本評論社 2,200 円
- [3] 小川 洋子, 「博士の愛した数式」, 新潮社, 2003 年 1,500 円
- [4] G. Toth 著 (蟹江幸博訳) 「数学名所案内 ～代数と幾何のきらめき～」
(上・下) シュプリンガー・フェアラーク東京, 上下各 2,700 円
- [5] Neal Koblitz, *A Course in Number Theory and Cryptography*
(second edition), Springer, 1994 年

[1] は昨年度のこの講義のテキスト. この授業で配布するプリントはほとんどこの本の内容と同じ. [2] は [1] と同様の材料を扱っていて, 少し高度. [3] は整数の話を盛り込んだ面白い小説. [4] は友人の訳した本で数学的には高度. 興味深い内容が書かれているが難しい. [5] は整数と暗号を扱った本で, 英語で書かれた数学的には高度な本.

1 集合と写像

1.1 集合の演算

ものの集まりで、それに属しているか属していないかが定まっているものを **集合 (set)** という。集合を表わす記号は中括弧 ($\{ \}$) を用いて、

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

のように列挙したり、

$$\{n \mid n \text{ は } 0 \text{ 以上で } 10 \text{ 未満の整数}\}$$

$$\{n^2 \mid n \text{ は自然数}\}$$

のように、

$$\{\text{変数の式} \mid \text{変数に関する条件}\}$$

の形で表わす。

集合そのものは A や B のようにアルファベットの大文字で表わすことが多い。

$$A = \{n \mid n \text{ は } 0 \text{ 以上で } 10 \text{ 未満の整数}\}, \quad B = \{n^2 \mid n \text{ は自然数}\}$$

集合を構成しているものを **要素** とか **元** という。

よく用いられる数の集合の記号

$\mathbf{N}$: 自然数 (natural number) の全体

$\mathbf{Z}$: 整数 (integer) の全体 (ドイツ語の Zahlen(数) からきている)

$\mathbf{Q}$: 有理数 (rational number) の全体 (Quotient(商) からきている)

$\mathbf{R}$: 実数 (real number) の全体

$\mathbf{C}$: 複素数 (complex number) の全体

a が A の元であるとき、すなわち、 a が A に属しているとき、

$$a \in A \quad \text{あるいは} \quad A \ni a$$

と書く。また、 a が A に属していないときは、

$$a \notin A \quad \text{あるいは} \quad A \not\ni a$$

と書く。

2つの集合 A と B に対して A の元がすべて B の元でもあるとき、すなわち、 A に属している元がすべて B にも属しているとき、

$$A \subset B \quad \text{あるいは} \quad B \supset A$$

と書き、 A は B に含まれる とか A は B の部分集合 (subset) であるという。

A が B に含まれないとき、すなわち、 A に属してはいるが、 B には属さない元があるとき、

$$A \not\subset B \quad \text{あるいは} \quad B \not\supset A$$

と書く.

$A \subset B$ かつ $A \supset B$ であるとき, A と B は等しいといい,

$$A = B$$

と書く.

$A \subset B$ ではあるが, A と B が等しくない($A \neq B$)とき, A は B の真部分集合である
といい,

$$A \subsetneq B$$

と表わす.

次の2つの定理が成り立つことは容易に分かる.

定理 1.1

- (1) $A = A$
- (2) $A = B$ ならば $B = A$
- (3) $A = B$ かつ $B = C$ ならば $A = C$

定理 1.2

- (1) $A \subset A$
- (2) $A \subset B$ かつ $B \subset C$ ならば $A \subset C$

和集合

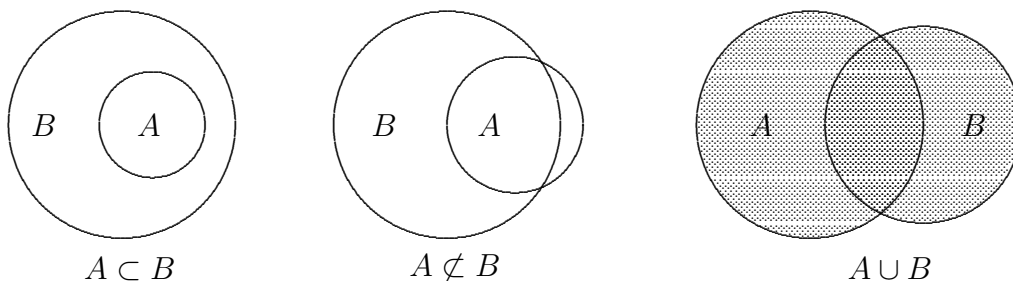
集合 A の元と集合 B の元を併せた集合を A と B の 和集合 (union) といい,

$$A \cup B$$

と表わす, すると $A \cup B$ は, 次のようなものである.

$$A \cup B = \{x \mid x \in A \quad \text{または} \quad x \in B\}$$

次のように, 集合を図で表現したものを Venn 図 という.



次の定理が成り立つ.

定理 1.3

- (1) $A \subset A \cup B$, $B \subset A \cup B$
- (2) $A \cup B = B \cup A$
- (3) $(A \cup B) \cup C = A \cup (B \cup C)$
- (4) $A \subset B \iff A \cup B = B$

問 1 定理 1.3 の (4) を証明しなさい.

共通部分

集合 A と集合 B の両方に属する元からなる集合を A と B の 共通部分 (intersection) といい,

$$A \cap B$$

と表わす, すると $A \cap B$ は, 次のようなものである.

$$A \cap B = \{x \mid x \in A \text{ かつ } x \in B\}$$

次の定理が成り立つ.

定理 1.4

- (1) $A \cap B \subset A$, $A \cap B \subset B$
- (2) $A \cap B = B \cap A$
- (3) $(A \cap B) \cap C = A \cap (B \cap C)$
- (4) $A \subset B \iff A \cap B = A$

問 2 定理 1.4 の (4) を証明しなさい.

また, $\cup$ と $\cap$ の間には次の分配法則が成り立つ.

定理 1.5

- (1) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- (2) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

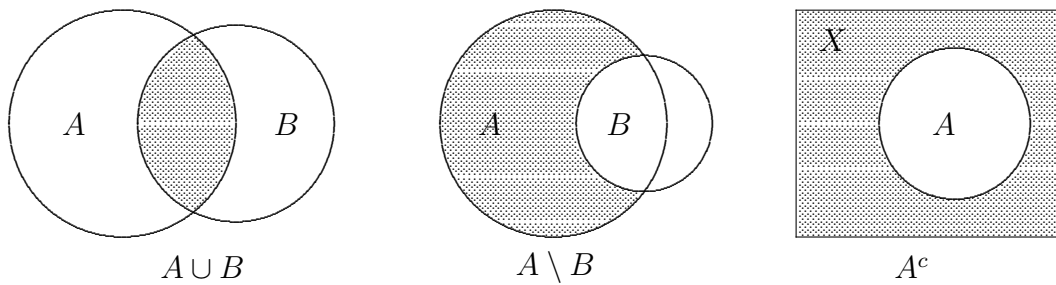
差集合

2つの集合 A と B があるとき, A に属して, B に属さないものの全体を 差集合 といい,

$$A \setminus B$$

と表わす. すなわち,

$$A \setminus B = \{x \mid x \in A \text{ かつ } x \notin B\}$$

**空集合, 全体集合, 補集合**

属する元が1つも無いものも集合とみなしてこれを **空集合 (empty set)** といい,

$$\emptyset$$

と表わす.

また, ある定まった集合 X の中でその部分集合だけを考えるとき, この X を **全体集合** という.

全体集合 X が定まっているとき, その部分集合 A に対して $X \setminus A$ を A の **補集合 (complement)** といい,

$$A^c$$

と表わす (TEXT によっては $\bar{A}$ と表わすことがある).

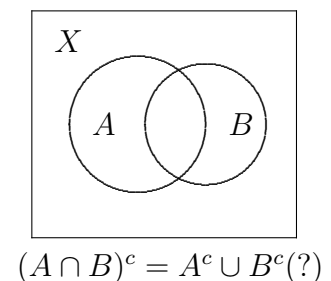
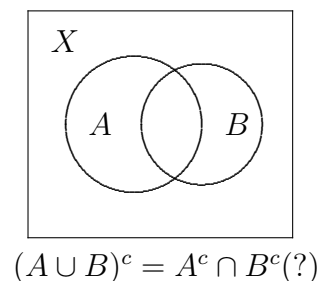
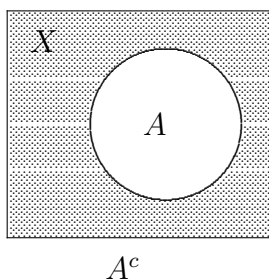
次の **de Morgan の法則** が成り立つ.

定理 1.6

$$(1) \quad (A \cup B)^c = A^c \cap B^c$$

$$(2) \quad (A \cap B)^c = A^c \cup B^c$$

問 3 定理 1.6 を下の右の 2 つの Venn 図を用いて確かめよ.



練習問題 1-1

全体集合を

$$X = \{\text{cat, rat, pig, dog, elephant, mouse, horse, cow, panda, zebra, bear, tiger}\}$$

また, A, B, C を X の部分集合で次のようなものとする.

A :最後が母音 (a, e, i, o, u) で終わる英単語

B :最初が c で始まる英単語

C :文字 e を含む英単語

次の集合を求めよ.

- (1) $A \cap B$ (2) $A \cap C$ (3) $B \cap C$ (4) $A \cup B$
 (5) $A \cup C$ (6) $B \cup C$ (7) $C \setminus A$ (8) A^c
 (9) C^c (10) $A^c \cup C^c$ (11) $(A \cap C)^c$ (12) $A^c \cap C^c$
 (13) $(A \cup C)^c$

練習問題 1-2

全体集合を $X = \{x \mid x \in \mathbf{Z} \text{ かつ } 0 \leq x \leq 100\}$ とする. また,

$$A = \{x \mid x \in X \text{ かつ } x \text{ は } 2 \text{ の倍数}\}$$

$$B = \{x \mid x \in X \text{ かつ } x \text{ は } 3 \text{ の倍数}\}$$

$$C = \{x \mid x \in X \text{ かつ } x \text{ は } 5 \text{ の倍数}\}$$

とすると, 次の集合の個数を求めよ. また, 個数が 10 個以下のものは元 (要素) をすべて列挙せよ.

- (1) $A \cap B$ (2) $A \cap C$ (3) $B \cap C$ (4) $A \cup B$ (5) $A \cup C$
 (6) $B \cup C$ (7) $A^c \cap C$ (8) $A^c \cup C$ (9) $B^c \cap C^c$ (10) $(A \cap C)^c$

1.2 写像

2つの集合 X と Y について, X の勝手な元 x に対して Y の元 y が唯一つ定まるとき, この対応を X から Y への **写像 (mapping または map)** という. この写像を f で表わすとき, x に対応する Y の元 y を $f(x)$ と表わし, x の写像 f による **像 (image)** という. また, X を **定義域**, X の f による像全体

$$\{f(x) \mid x \in X\}$$

を **値域** といい, $f(X)$ と表わすことにする.

集合 X と Y が数の集合のとき, 写像を **関数 (function)** という (X が数の集合でないときも関数ということがある).

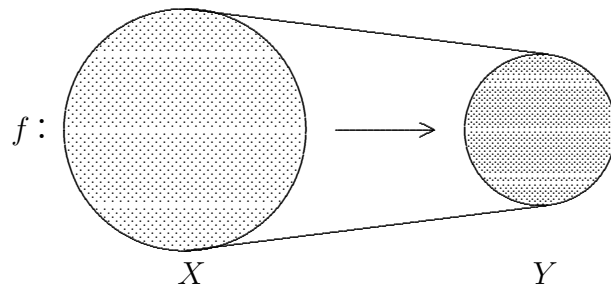
恒等写像 (identity mapping)

集合 X の任意の元 x に対して、自分自身 x を対応させる写像を **恒等写像** といい、 id_X と表わす.

$$id_X : X \longrightarrow X, \quad id_X(x) = x \text{ for } x \in X$$

全射

集合 Y の勝手な元 y に対して、 $y = f(x)$ となるような X の元 x があるとき、写像 f は **全射** であるという. このことは、 X が写像 f によって Y 全体に写されていることを意味する. すなわち、 $f(X) = Y$ となっている.

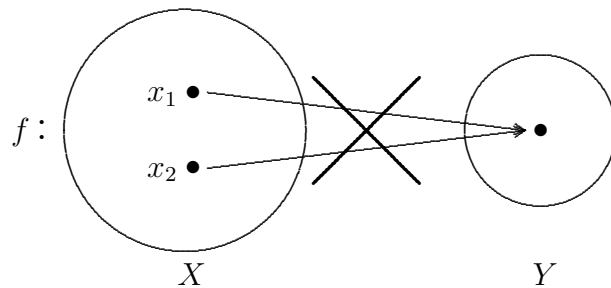
**単射**

集合 X の勝手な2つの元 x_1 と x_2 に対して、

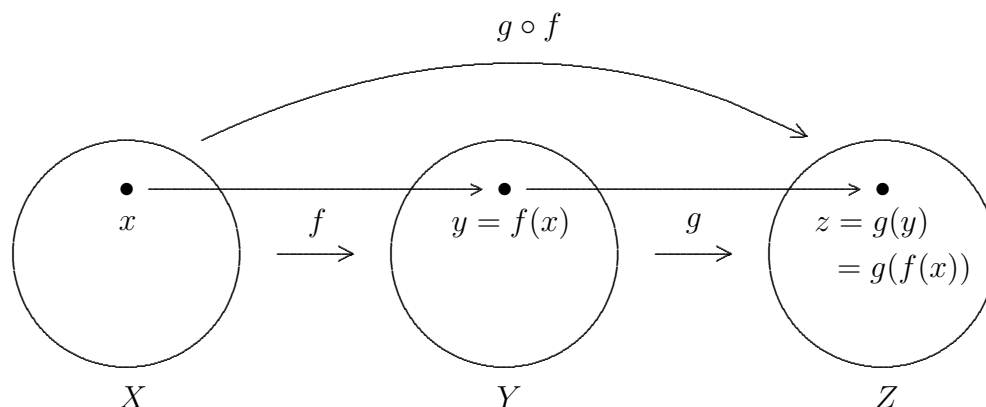
$$f(x_1) = f(x_2) \implies x_1 = x_2$$

となっているとき、写像 f は **単射** であるという. 言い換えると、

$$x_1 \neq x_2 \implies f(x_1) \neq f(x_2)$$

**合成写像**

集合 X から集合 Y への写像 f と Y から集合 Z への写像 g が与えられているとき、 X の元 x を f によって Y の元 $f(x)$ に写し、さらにこれを g によって Z の元 $g(f(x))$ に移すことによって、 X から Z への写像が出来る. この写像を f と g の **合成写像** といい、 $g \circ f$ で表わす.



全単射, 逆写像

集合 X から集合 Y への写像 f が全射でありかつ単射になっているとき, f は **全単射** (または **1対1の対応**) であるという.

このとき, Y の任意の元 y に対して, $y = f(x)$ となるような X の元 x が唯一つ定まる. このような y から x が定まる対応を f の **逆写像** といい, f^{-1} で表す.

$$f^{-1}(f(x)) = x \text{ for } x \in X, \text{ すなわち } f^{-1} \circ f = id_X$$

$$f(f^{-1}(y)) = y \text{ for } y \in Y, \text{ すなわち } f \circ f^{-1} = id_Y$$

次の定理が成り立つ.

定理 1.7 $f: X \rightarrow Y, g: Y \rightarrow Z$ とする.

- (1) $g \circ f: \text{全射} \implies g: \text{全射}$
- (2) $g \circ f: \text{単射} \implies f: \text{単射}$
- (3) $g \circ f: \text{全単射} \text{ かつ } f \circ g: \text{全単射} \implies f \text{ と } g \text{ は全単射}$

練習問題 1-3 次の写像は全射になっているか, 単射になっているかを調べよ.

(1) $f: X = \mathbf{N} \rightarrow Y = 2\mathbf{N} \quad y = f(x) = 2x + 10$

(2) $f: X = \mathbf{N} \rightarrow Y = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

$y = f(x) = x$ を 10 で割った余り

(3) $f: X = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\} \rightarrow Y = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

$y = f(x) = x$ を 3 倍して 10 で割った余り

(4) $f: X = \{\text{cat}, \text{dog}, \text{panda}, \text{zebra}, \text{puma}, \text{tiger}\} \rightarrow Y = \{a, e, i, o, u\}$

$y = f(x) = x$ の最初の母音

上で, 全射になっていないものは, Y から適当に要素を取り除き, 全射になるようにしなさい.

また、単射になっていないものは、 X から適当に要素を取り除き、単射になるようにしなさい。

練習問題 1-4 次の写像 $f: X \rightarrow Y$ は全射になっているか、単射になっているかを調べよ。全射になっていない場合や単射になっていない場合にはその理由を説明しなさい。

$$(1) f: X = [0, \infty) = \{x \mid 0 \leq x\} \rightarrow Y = \mathbf{R} \quad y = f(x) = x^2 + 1$$

$$(2) f: X = \{0, 1, 2, 3, 4, 5\} \rightarrow Y = \{0, 1, 2, 3, 4, 5\}$$

$$y = f(x) = x \text{ を } 2 \text{ 倍して } 6 \text{ で割った余り}$$

練習問題 1-5 次の2つの写像 $f: X \rightarrow Y$, $g: Y \rightarrow Z$ の合成写像 $g \circ f$ を作りなさい。

$$(1) X = \mathbf{R} , Y = \mathbf{R} , Z = \mathbf{R} , y = f(x) = a^x , z = g(y) = \frac{1}{y^2 + 1}$$

$$(2) X = \{\text{cat}, \text{dog}, \text{panda}, \text{zebra}, \text{puma}\}$$

$$Y: \text{アルファベット 26 文字}$$

$$Z = \mathbf{N}$$

$$y = f(x) = x \text{ の } 3 \text{ 番目の文字} , z = g(y) = y \text{ の } abc \text{ 順による順番}$$

$$g \circ f(\text{cat}), g \circ f(\text{dog}), g \circ f(\text{panda}), g \circ f(\text{zebra}), g \circ f(\text{puma}) \text{ を求めよ。}$$

練習問題 1-6 次の写像 $f: X \rightarrow Y$ は全単射になっている。 $y = f(x)$ の逆写像 $x = f^{-1}(y)$ を作りなさい。

$$(1) X = [0, 1) , Y = [1, \infty) \quad y = f(x) = \frac{1}{1-x}$$

$$(2) X = \mathbf{R} , Y = \mathbf{R} \quad y = f(x) = \frac{10^x - 10^{-x}}{2}$$

1.3 集合の濃度 (個数)

集合 X が有限集合のときその個数 n を **濃度** と呼び、 $\#X$ で表わす。このことは、集合 X から次の集合

$$\{1, 2, 3, \dots, n\}$$

への全単射が存在することを意味する。

無限集合の場合も、2つの集合 X と Y に対して、 X から Y への全単射が存在するとき、2つの集合の濃度 $\#X$ と $\#Y$ は等しいと定め、 $\#X = \#Y$ と書く。

自然数全体の集合 $\mathbf{N}$ を **可算濃度** といい、 $\aleph_0$ (アレフゼロ) と書く。

例 1 (1) 正の偶数 $2\mathbf{N}$ の全体の集合の濃度は可算濃度 $\aleph_0$ である。

$$f: \mathbf{N} \longrightarrow 2\mathbf{N} (\text{全単射}), \quad y = f(n) = 2n$$

(2) 整数全体の集合 $\mathbf{Z}$ の濃度は可算濃度 $\aleph_0$ である.

$$\begin{array}{cccccccc} \mathbf{N} & \cdots & \textcircled{5} & \textcircled{3} & \textcircled{1} & \textcircled{2} & \textcircled{4} & \cdots \\ \mathbf{Z} & \cdots & -2 & -1 & 0 & 1 & 2 & \cdots \end{array}$$

$$f: \mathbf{N} \longrightarrow \mathbf{Z} (\text{全単射}), \quad y = f(x) = \begin{cases} 0 & n = 1 \text{ のとき} \\ n/2 & n: \text{正の偶数のとき} \\ -(n-1)/2 & n: \text{正の奇数のとき} \end{cases}$$

(3) 正の有理数全体の集合の濃度は可算濃度 $\aleph_0$ である.

$$\begin{array}{ccccc} \frac{1}{1} & \rightarrow & \frac{2}{1} & \rightarrow & \frac{3}{1} & \rightarrow & \frac{4}{1} & \rightarrow & \frac{5}{1} \\ \downarrow & \swarrow & \nearrow & \downarrow & \nearrow & \downarrow & \nearrow & \downarrow & \nearrow \\ \frac{1}{2} & & \frac{2}{2} & & \frac{3}{2} & & \frac{4}{2} & & \frac{5}{2} \\ \downarrow & \swarrow & \nearrow & \downarrow & \nearrow & \downarrow & \nearrow & \downarrow & \nearrow \\ \frac{1}{3} & & \frac{2}{3} & & \frac{3}{3} & & \frac{4}{3} & & \frac{5}{3} \\ \downarrow & \swarrow & \nearrow & \downarrow & \nearrow & \downarrow & \nearrow & \downarrow & \nearrow \\ \frac{1}{4} & & \frac{2}{4} & & \frac{3}{4} & & \frac{4}{4} & & \frac{5}{4} \\ \downarrow & \swarrow & \nearrow & \downarrow & \nearrow & \downarrow & \nearrow & \downarrow & \nearrow \\ \frac{1}{5} & & \frac{2}{5} & & \frac{3}{5} & & \frac{4}{5} & & \frac{5}{5} \end{array}$$

(4) 有理数全体 $\mathbf{Q}$ の集合の濃度は可算濃度 $\aleph_0$ である.

問 1 例 1 の (4) を証明しなさい.

定義 2つの集合 X と Y に対して, X から Y への単射が存在するとき,

$$\#X \leq \#Y$$

と定める. また, $\#X \leq \#Y$ であって, $\#X \neq \#Y$ であるとき, $\#X < \#Y$ と書こう.

定理 1.8 2つの集合 X と Y に対して, X から Y への全射が存在すれば, Y から X への単射が存在し, $\#Y \leq \#X$ が成り立つ.

定理 1.9(Cantor-Bernstein) 2つの集合 X と Y に対して, X から Y への単射と全射が存在すれば, X から Y への全単射が存在し, $\#X = \#Y$ が成り立つ. このことから, X から Y への単射と全射が存在すれば, 2つの集合の濃度は等しいことがわかる.

定理 1.8 と定理 1.9 の証明は難しいので省略する.

実数の濃度 (連続体の濃度)

集合 I を 0 と 1 の間の実数全体とする. すなわち,

$$I = \{x \mid x \in \mathbf{R} \text{ かつ } 0 < x < 1\}$$

$n \in \mathbf{N}$ に対して, $f(n) = 1/n$ とすると, これは $\mathbf{N}$ から I への単射となっている. このことと, 定理 1.8 より, $\aleph_0 \leq \#I$ である. しかし, $\#I \neq \aleph_0$ であることを以下に示そう.

背理法によって示す. $\#I = \aleph_0$ とすると, $\mathbf{N}$ から I への全単射 f が存在する. $f(n)$ を少数表示して,

$$\begin{aligned} f(1) &= a_1 = 0 . \underline{a_{11}} \ a_{12} \ a_{13} \ a_{14} \ a_{15} \ \cdots \\ f(2) &= a_2 = 0 . a_{21} \ \underline{a_{22}} \ a_{23} \ a_{24} \ a_{25} \ \cdots \\ f(3) &= a_3 = 0 . a_{31} \ a_{32} \ \underline{a_{33}} \ a_{34} \ a_{35} \ \cdots \\ f(4) &= a_4 = 0 . a_{41} \ a_{42} \ a_{43} \ \underline{a_{44}} \ a_{45} \ \cdots \\ f(5) &= a_5 = 0 . a_{51} \ a_{52} \ a_{53} \ a_{54} \ \underline{a_{55}} \ \cdots \\ &\dots\dots\dots \end{aligned}$$

ただし, $0.2 = 0.1999999\cdots$ のように, 無限小数でないものは 2通りの表わし方があるが, 無限小数として表わすことにする.

いま, アンダーライン部分の a_{ii} によって, 次のように b_i を定める.

$$b_i = \begin{cases} 1 & a_{ii}: \text{偶数のとき} \\ 2 & a_{ii}: \text{奇数のとき} \end{cases}$$

$b = 0 . b_1 \ b_2 \ b_3 \ b_4 \ b_5 \ \cdots$ とおくと, b はどの $f(n)$ とも異なるので, f は全射になっていない(矛盾).

このようにして, I の濃度は $\aleph_0$ より大きいことがわかる. I から実数全体の集合 $\mathbf{R}$ へは全単射が存在するので, $\aleph_0 < \#I = \#\mathbf{R}$ となる. 実数 $\mathbf{R}$ の濃度を 連続体の濃度 といひ, $\aleph$ とか $\aleph_1$ で表わす.

ベキ集合とベキ集合の濃度

集合 X に対して空集合を含めた X の部分集合の全体を X のベキ集合といい 2^X で表わす.

例 2 $X = \{1, 2, 3\}$ とする. すると, その部分集合全体 2^X は

$\emptyset$	$\longleftrightarrow$	000
$\{1\}$	$\longleftrightarrow$	100
$\{2\}$	$\longleftrightarrow$	010
$\{3\}$	$\longleftrightarrow$	001
$\{1, 2\}$	$\longleftrightarrow$	110
$\{1, 3\}$	$\longleftrightarrow$	101
$\{2, 3\}$	$\longleftrightarrow$	011
$\{1, 2, 3\}$	$\longleftrightarrow$	111

であり, $\#(2^X) = 2^3$

一般に, X が有限集合で, $\#X = n$ とするとき, $\#(2^X) = 2^n$ である. また, 連続体の濃度 $\#R$ は $\#(2^N)$ と等しい.

定理 1.10 集合 X に対して,

$$\#X < \#(2^X)$$

である.

(証明) X から部分集合の集合 2^X への写像

$$f: X \longrightarrow 2^X, \quad f(x) = \{x\}$$

は単射となっているので, $\#X \leq \#(2^X)$ が言える.

背理法で $\#X \neq \#(2^X)$ を示そう. もし, $\#X = \#(2^X)$ とすれば, X から 2^X への全単射 g が存在する. いま, 次のような X の部分集合 A を考える.

$$A = \{x \mid x \notin g(x)\}$$

g は全射であるので, X の元 a で, $g(a) = A$ となるものが存在する. この a が A に属しているのか属していないのかを調べよう.

もし, $a \in A$ であるとすれば, $a \in A = g(a)$ となり, $a \notin A$ で矛盾.

もし, $a \notin A$ であるとすれば, $a \notin A = g(a)$ となり, $a \in A$ で矛盾.

以上より, $\#X \neq \#(2^X)$ が言え, $\#X < \#(2^X)$ となることがわかる. (証明終)

練習問題 1-7 次の 2 つの集合 X, Y は濃度が等しい. X から Y への全単射を作りなさい.

(1) $X = (0, 1) = \{x \mid 0 < x < 1\}$, $Y = (-1, 1) = \{y \mid -1 < y < 1\}$

(2) $X = (0, 1] = \{x \mid 0 < x \leq 1\}$, $Y = [0, 2) = \{y \mid 0 \leq y < 2\}$

(3) $X = \mathbf{Z}$, $Y = \mathbf{N}$

(4) $X = [0, 1)$, $Y = [0, \infty) = \{y \mid 0 \leq y\}$ (hint: 練習問題 1-5(1) 参照)

(5) $X = I = (0, 1)$, $Y = \mathbf{R}$

(6) $X = (0, 1]$, $Y = \{(x, y) \mid x^2 + y^2 = 1\}$

2 代数の話 (整数)

2.1 b -進法

. 10 進法

$$(357.062\cdots)_{10} = 3 \cdot 10^2 + 5 \cdot 10^1 + 7 \cdot 10^0 + 0 \cdot 10^{-1} + 6 \cdot 10^{-2} + 2 \cdot 10^{-3} + \cdots$$

. b -進法

$$(d_{k-1}d_{k-2}\cdots d_0.d_{-1}d_{-2}\cdots)_b = d_{k-1} \cdot b^{k-1} + d_{k-2} \cdot b^{k-2} + \cdots + d_0 \cdot b^0 + d_{-1} \cdot b^{-1} + d_{-2} \cdot b^{-2} + \cdots$$

$$b : \text{base(基数)} \quad d_i : \text{digit(数字)}$$

$$2 \text{ 進法 (binary system)} \quad \text{bit: binary digit を縮めた言い方} \quad 0 \text{ or } 1$$

$11 \leq b \leq 26$ の時は $0 \sim 25$ までの数字に $A \sim Z$ を割り当てる. あるいは

$11 \leq b \leq 36$ の時は $0 \sim 9$ まではそのまま用い, $10 \sim 35$ の数字に $A \sim Z$ を割り当てる.

コンピュータで 16 進法は

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A(10), B(11), C(12), D(13), E(14), F(15)$$

を用いる.

例 1 (1) $(11001001)_2 = 1 \cdot 2^7 + 1 \cdot 2^6 + 1 \cdot 2^3 + 1 = 128 + 64 + 8 + 1 = 201$

(2) $(BAD)_{26} = 1 \cdot 26^2 + 0 \cdot 26^1 + 3 \cdot 26^0 = 676 + 3 = 679$

$$(B.AD)_{26} = 1 \cdot 26^0 + 0 \cdot 26^{-1} + 3 \cdot 26^{-2} = 1 + \frac{3}{676}$$

例 2 160 と 199 を 7 進法で表わし, 7 進法で掛け算せよ.

$\begin{array}{r} 7 \overline{) 160} \cdots 6 \\ 7 \overline{) 22} \cdots 1 \\ 7 \overline{) 3} \cdots 3 \\ \hline 0 \end{array}$	$\begin{array}{r} 7 \overline{) 199} \cdots 3 \\ 7 \overline{) 28} \cdots 0 \\ 7 \overline{) 4} \cdots 4 \\ \hline 0 \end{array}$	$\begin{array}{r} (316)_7 \\ (403)_7 \\ \hline (1254)_7 \\ (1603)_7 \\ \hline (161554)_7 \end{array}$
---	---	---

$$160 = (316)_7$$

$$199 = (403)_7$$

$$(316)_7 \times (403)_7 = (161554)_7$$

例 4 10^6 を 26 進法で表わせ.

$$\begin{array}{r} 26 \overline{) 1000000} \cdots 14(O) \\ 26 \overline{) 38461} \cdots 7(H) \\ 26 \overline{) 1479} \cdots 23(X) \\ 26 \overline{) 56} \cdots 4(E) \\ 26 \overline{) 2} \cdots 2(C) \\ \hline 0 \end{array}$$

$$10^6 = (\text{CEXHO})_{26}$$

例 5 $\pi = 3.1415926 \dots$ を 7 進法で小数点以下 5 桁まで表わせ. また, 26 進法で小数点以下 3 桁まで表わせ.

$$3 = (3)_2$$

$$0.1415926 \dots = d_{-1} \cdot 7^{-1} + d_{-2} \cdot 7^{-2} + d_{-3} \cdot 7^{-3} + \dots$$

$$\times 7 \quad 0.991148 \dots = d_{-1} + d_{-2} \cdot 7^{-1} + d_{-3} \cdot 7^{-2} + \dots \quad \text{より} \quad d_{-1} = 0$$

$$\times 7 \quad 6.93804 \dots = d_{-2} + d_{-3} \cdot 7^{-1} + d_{-4} \cdot 7^{-2} + \dots \quad \text{より} \quad d_{-2} = 6$$

$$6 \text{ を引いて } \times 7 \quad 6.5662 \dots = d_{-3} + d_{-4} \cdot 7^{-1} + d_{-5} \cdot 7^{-2} + \dots \quad \text{より} \quad d_{-3} = 6$$

$$6 \text{ を引いて } \times 7 \quad 3.963 \dots = d_{-4} + d_{-5} \cdot 7^{-1} + d_{-6} \cdot 7^{-2} + \dots \quad \text{より} \quad d_{-4} = 3$$

$$3 \text{ を引いて } \times 7 \quad 6.74 \dots = d_{-5} + d_{-6} \cdot 7^{-1} + d_{-7} \cdot 7^{-2} + \dots \quad \text{より} \quad d_{-5} = 6$$

$$\text{以上より} \quad \pi = 3.1415926 \dots = (3.06636 \dots)_7$$

$$3 = (D)_{26}$$

$$0.1415926 \dots = d_{-1} \cdot 26^{-1} + d_{-2} \cdot 26^{-2} + d_{-3} \cdot 26^{-3} + \dots$$

$$\times 26 \quad 3.6814076 \dots = d_{-1} + d_{-2} \cdot 26^{-1} + d_{-3} \cdot 26^{-2} + \dots \quad \text{より} \quad d_{-1} = 3 = (D)_{26}$$

$$3 \text{ を引いて } \times 26 \quad 17.716597 \dots = d_{-2} + d_{-3} \cdot 26^{-1} + \dots \quad \text{より} \quad d_{-2} = 17 = (R)_{26}$$

$$17 \text{ を引いて } \times 26 \quad 18.6315227 \dots = d_{-3} + d_{-4} \cdot 26^{-1} + \dots \quad \text{より} \quad d_{-3} = 18 = (S)_{26}$$

$$\text{以上より} \quad \pi = 3.1415926 \dots = (D.DRS \dots)_{26}$$

練習問題 2-1 次の数を 10 進法で表わせ.

$$(1) \quad (471)_8 \qquad (2) \quad (11011011)_2 \qquad (3) \quad (165)_7$$

練習問題 2-2 次の問いに答えよ. ただし, 16 進法のときは 10 を A で, 11 を B で, 12 を C で, 13 を D で, 14 を E で, 15 を F とする.

$$(1) \quad 1000 \text{ を } 2 \text{ 進法で表わせ.} \qquad (2) \quad 1000 \text{ を } 16 \text{ 進法で表わせ.}$$

$$(3) \quad 10.25 \text{ を } 2 \text{ 進法で表わせ.} \qquad (4) \quad 123.5 \text{ を } 8 \text{ 進法で表わせ.}$$

練習問題 2-3 次の 26 進法 ($A=0 \sim Z=25$) で表わされた数を 10 進法で表わせ.

$$(1) \quad (KOB E)_{26} \qquad (2) \quad (YAMA)_{26}$$

練習問題 2-4 次の数を 26 進法 ($A=0 \sim Z=25$) で表わせ.

$$(1) \quad 176332 \qquad (2) \quad 3687172$$

練習問題 2-5 $e = 2.7182818 \dots$ を 7 進法で小数点以下 5 桁まで表わせ. また, 26 進法で小数点以下 3 桁まで表わせ.

2.2 整除性と Euclid の互除法

定義 a, b : 整数 (integer) とする.

$$a|b \stackrel{\text{def}}{\iff} \exists d: \text{整数} \quad s.t. \quad b = ad$$

このとき, 「 a は b を割り切る」, 「 a は b の約数 (diviser) である」, 「 b は a の倍数 (multiple) である」という.

真の約数 (proper diviser): 自分自身以外の約数

非自明な約数 (non-trivial diviser): 自分自身と 1 以外の約数

素数 (prime number): 1 より大きな整数で, 1 と自分自身以外に正の約数をもたないもの

合成数 (composite number): 少なくとも 1 つの非自明な約数を持つ整数

p を素数とする.

$$p^\alpha || b \stackrel{\text{def}}{\iff} p^\alpha | b \quad \text{かつ} \quad p^{\alpha+1} \nmid b$$

整除性の基本的性質

1. $a|b$ かつ $\forall c: \text{整数} \implies a|bc$
2. $a|b$ かつ $b|c \implies a|c$
3. $a|b$ かつ $a|c \implies a|(b \pm c)$

算術の基本定理 (The Fundamental Theorem of Arithmetic)

任意の自然数は (因子の順序を無視すれば) 一通りに素因数分解が出来る. 小さい素数の順番に書くのが通常である. (例 $4200 = 2^3 \cdot 3 \cdot 5^2 \cdot 7$)

整除性の基本的性質 (続き)

4. p : 素数, $a|bc \implies a|b$ または $p|c$
5. $m|a$, $n|a$ かつ m と n が共通の約数 (公約数) をもたない $\implies mn|a$

自然数 n の約数は何通りあるか?

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \text{ (素因数分解)}$$

とすると, n の任意の約数 d は

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r} \quad (0 \leq \beta_i \leq \alpha_i)$$

の形である. よって, $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ の約数の個数は

$$(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1)$$

である. (例 $4200 = 2^3 \cdot 3 \cdot 5^2 \cdot 7$ の約数の個数は $(3+1)(1+1)(2+1)(1+1) = 48$ 個)

定義 0 と異なる 2 つの整数 a と b について, a と b の両方を割り切る最大の整数を 最大公約数 (greatest common divider) といい, $g.c.d.(a, b)$ と書く.

$g.c.d.(a, b)$: a と b を割り切り, a と b の任意の公約数によって割り切られる唯一つの正の数

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$$

とすると,

$$g.c.d.(a, b) = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_r^{\gamma_r} \quad \text{ここで, } \gamma_i = \min(\alpha_i, \beta_i)$$

a と b の両方が割り切る最小整数を 最小公倍数 (least common multiple) といい, $l.c.m.(a, b)$ と書く.

$$l.c.m.(a, b) = p_1^{\delta_1} p_2^{\delta_2} \cdots p_r^{\delta_r} \quad \text{ここで, } \delta_i = \max(\alpha_i, \beta_i)$$

$$l.c.m.(a, b) = \frac{|a \cdot b|}{g.c.d.(a, b)} \quad (\max(\alpha, \beta) + \min(\alpha, \beta) = \alpha + \beta)$$

$$\text{例 } 4200 = 2^3 \cdot 3^1 \cdot 5^2 \cdot 7^1, \quad 10780 = 2^2 \cdot 5^1 \cdot 7^2$$

$$g.c.d.(4200, 10780) = 2^2 \cdot 5^1 \cdot 7^1$$

$$l.c.m.(4200, 10780) = 2^3 \cdot 3^1 \cdot 5^2 \cdot 7^2$$

Euclid の互除法 (Euclidean algorithm)

大きな数に対して素因数分解が分からない時でも, 2 つの数 a と b の最大公約数 $g.c.d.(a, b)$ を簡単な方法で求める事が出来る.

原理

$a \geq b$ とする. $a \div b$: 商を q , 余りを r とする. すなわち, $a = bq + r$ ($0 \leq r \leq b - 1$)

このとき. $g.c.d.(a, b) = g.c.d.(b, r)$ ($\because d : a$ と b の公約数 $\iff d : b$ と r の公約数)

algorithm

$a \geq b$ とする.

- (1) $a \div b$: 商 q_1 , 余り $r_1 (r_1 > 0)$ $a = bq_1 + r_1$ $g.c.d.(a, b) = g.c.d.(b, r_1)$
- (2) $b \div r_1$: 商 q_2 , 余り $r_2 (r_2 > 0)$ $b = r_1q_2 + r_2$ $g.c.d.(b, r_1) = g.c.d.(r_1, r_2)$
- (3) $r_1 \div r_2$: 商 q_3 , 余り $r_3 (r_3 > 0)$ $r_1 = r_2q_3 + r_3$ $g.c.d.(r_1, r_2) = g.c.d.(r_2, r_3)$
- (4) $r_2 \div r_3$: 商 q_4 , 余り $r_4 (r_4 > 0)$ $r_2 = r_3q_4 + r_4$ $g.c.d.(r_2, r_3) = g.c.d.(r_3, r_4)$
-
- (k) $r_{k-2} \div r_{k-1}$: 商 q_k , 余り $r_k (r_k > 0)$ $r_{k-2} = r_{k-1}q_k + r_k$
 $g.c.d.(r_{k-2}, r_{k-1}) = g.c.d.(r_{k-1}, r_k)$
- (k+1) $r_{k-1} \div r_k$: 商 q_{k+1} , 余り $r_{k+1} = 0$ $r_{k-1} = r_kq_{k+1}$
 $d = g.c.d.(a, b) = g.c.d.(r_{k-1}, r_k) = r_k$: 最大公約数

例 6 $g.c.d.(1547, 560)$ を見つけよ.

$$1547 = 560 \cdot 2 + 427$$

$$560 = 427 \cdot 1 + 133$$

$$427 = 133 \cdot 3 + 28$$

$$133 = 28 \cdot 4 + 21$$

$$28 = 21 \cdot 1 + 7$$

$$21 = 7 \cdot 3$$

$$g.c.d.(1547, 560) = 7$$

定理 2.1 $d = g.c.d.(a, b) \implies \exists u, v : \text{integer} \text{ s.t. } d = au + bv$

すなわち, 2つの整数 a と b の最大公約数 d は a と b の整数係数の 1 次結合表わせる.

Outline of proof(以下の方法を **拡張 Euclid の互除法** という) Euclid の互除法の式を逆にたどって,

$d = r_k = r_{k-2} - r_{k-1}q_k$ の式に $r_{k-1} = r_{k-3} - r_{k-2}q_{k-1}$ を代入. それに, $r_{k-2}, r_{k-3}, \dots$ を次々に代入していけば, d は a と b の整数係数の 1 次結合表わせる.

例 6(続き)

$$\begin{aligned} 7 &= 28 - 21 \cdot 1 = 28 - (133 - 28 \cdot 4) \cdot 1 \\ &= 5 \cdot 28 - 1 \cdot 133 = 5 \cdot (427 - 133 \cdot 3) - 1 \cdot 133 \\ &= 5 \cdot 427 - 16 \cdot 133 = 5 \cdot 427 - 16 \cdot (560 - 427 \cdot 1) \\ &= 21 \cdot 427 - 16 \cdot 560 = 21 \cdot (1547 - 560 \cdot 2) - 16 \cdot 560 \\ &= 21 \cdot 1547 - 58 \cdot 560 \end{aligned}$$

定義 a, b 整数 (integer) とする.

a と b は互いに素 (relatively prime)

$\stackrel{\text{def}}{\iff} g.c.d.(a, b) = 1$ (i.e. a と b は 1 より大きな公約数を持たない)

定義 (Euler の φ 関数)

n : 自然数 (natural number) とする.

$$\varphi(n) \stackrel{\text{def}}{=} \# \{b \in \mathbf{Z} \mid 1 \leq b \leq n \text{ かつ } g.c.d.(b, n) = 1\}$$

($\#$ は集合の個数を表わすこと事にする)

$\varphi(n)$ は n 以下の n と互いに素である数の個数である.

例 $\varphi(1) = \# \{1\} = 1$, $\varphi(2) = \# \{1\} = 1$, $\varphi(3) = \# \{1, 2\} = 2$,

$\varphi(4) = \# \{1, 3\} = 2$, $\varphi(5) = \# \{1, 2, 3, 4\} = 4$, $\varphi(6) = \# \{1, 5\} = 2$

p : 素数のとき, $\varphi(p) = \# \{1, 2, \dots, p-1\} = p-1$

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha \left(1 - \frac{1}{p}\right)$$

($\because$ $1 \sim p^\alpha$ のうち, p^α と素でないものは $\{1 \cdot p, 2 \cdot p, \dots, p^{\alpha-1} \cdot p\}$ の $p^{\alpha-1}$ 個)

練習問題 2-6 (1) つぎのことを証明せよ.

$$(i) \quad p^\alpha \parallel a \text{ かつ } p^\beta \parallel b \implies p^{\alpha+\beta} \parallel a \cdot b$$

$$(ii) \quad p^\alpha \parallel a, p^\beta \parallel b \text{ かつ } \alpha < \beta \implies p^\alpha \parallel (a \pm b)$$

(2) 次の命題の反例を示せ. 「 $p^\alpha \parallel a$ かつ $p^\alpha \parallel b \implies p^\alpha \parallel (a+b)$ 」

練習問題 2-7 945 の約数は何個あるか? それらをすべて挙げよ.

練習問題 2-8 (1) $n!$ を正確に割り切る (exactly divide) 素数 p の巾は

$$\left[\frac{n}{p} \right] + \left[\frac{n}{p^2} \right] + \left[\frac{n}{p^3} \right] + \dots \quad (\text{有限和})$$

であることを示せ.

(2) 100! は 2 の何乗で割り切れるか?

100! は 3 の何乗で割り切れるか?

100! は 5 の何乗で割り切れるか?

100! は 7 の何乗で割り切れるか?

100! を素因数分解せよ.

練習問題 2-9 $d = g.c.d.(360, 294)$ を 2 つの方法で求めよ.

(1) 2 つの数を素因数分解して求める方法

(2) Euclid の互除法

練習問題 2-10 つぎの 2 つの数の最大公約数を Euclid の互除法を用いて求め, その最大公約数を 2 つの数の 1 次結合で表わせ.

- (1) 26, 18 (2) 187, 34 (3) 841, 160 (d) 2613, 2171

練習問題 2-11 実数係数の多項式 (polynomial) について考える.

f, g : 多項式

$f|g \stackrel{\text{def}}{\iff} \exists h: \text{多項式} \quad s.t. \quad g = f \cdot h \quad (f \text{ は } g \text{ を割り切る})$

$g.c.d.(f, g)$: f と g を割り切る最大次数の多項式

一意的ではないが, 0 でない実数倍の違いだけ.

最高次数の係数を 1 にする (monic) 多項式とすれば, 一意的

f と g は互いに素 $\stackrel{\text{def}}{\iff} g.c.d.(f, g) = 1$

Euclid の互除法が整数の場合と同様に可能

(1) $g.c.d.(x^4 + x^2 + 1, x^2 + 1) = ?$

(2) $g.c.d.(x^4 - 4x^3 + 6x^2 - 4x + 1, x^3 - x^2 + x - 1) = ?$

(1) と (2) の場合に最大公約数を f と g の多項式係数の 1 次結合で表わせ.

($g.c.d. = u(x)f(x) + v(x)g(x)$ となる多項式 $u(x)$ と $v(x)$ を見つけよ)

練習問題 2-12 $f(x) = 0$ が重根をもつとき,

「 $\alpha: f(x) = 0$ の重根 $\implies \alpha: g.c.d.(f(x), f'(x)) = 0$ の根」

であることを示せ. さらに, $x^4 - 2x^3 - x^2 + 2x + 1 = 0$ の重根を求めよ.

2.3 合同式

定義

$$a \equiv b \pmod{m} \stackrel{\text{def}}{\iff} m \mid (a - b) \quad (\text{i.e. } (a - b) \text{ が } m \text{ の倍数})$$

このとき, a は m を法として b と合同である という.

合同式の基本的性質

1. (i) $a \equiv a \pmod{m}$
 (ii) $a \equiv b \pmod{m} \iff b \equiv a \pmod{m}$
 (iii) $a \equiv b \pmod{m}$ かつ $b \equiv c \pmod{m} \implies a \equiv c \pmod{m}$
 (i)~(iii) をみたす関係 $\equiv$ を 同値関係 という.

2. 集合に同値関係があるとき, 同じ関係をもつものを集めたものを 同値類 という.
 いまの場合, m で割った余りが同じであるものを集めたものであるので, これを m を法とする剰余類 といい, $\mathbb{Z}/m\mathbb{Z}$ で表わす. $\mathbb{Z}/m\mathbb{Z}$ は

0 と合同な同値類

1 と合同な同値類

2 と合同な同値類

.....

$(m - 1)$ と合同な同値類

の m 個の同値類が出来る.

3. $a \equiv b \pmod{m}$ かつ $c \equiv d \pmod{m}$
 $\implies (a \pm c) \equiv (b \pm d) \pmod{m}$ かつ $ac \equiv bd \pmod{m}$
4. $d \mid m$ (d が m の約数) であるとき, $a \equiv b \pmod{m} \implies a \equiv b \pmod{d}$
5. m と n が互いに素であるとき ($\text{g.c.d.}(m, n) = 1$)
 $a \equiv b \pmod{m}$, $a \equiv b \pmod{n} \implies a \equiv b \pmod{m \cdot n}$

定理 2.2 $\mathbb{Z}/m\mathbb{Z}$ において,

a が掛け算の逆元 $b = a^{-1}$ (i.e. $a \cdot b \equiv a \cdot a^{-1} \equiv 1 \pmod{m}$) をもつ

$$\iff \text{g.c.d.}(a, m) = 1$$

proof $\implies$ の証明

背理法 $\text{g.c.d.}(a, m) = d > 1$ とする.

$ab - 1$ は m の倍数 $\implies ab - 1$ は d の倍数 $\implies 1$ は d の倍数 (矛盾)

$\Leftarrow$ の証明

$g.c.d.(a, m) = 1$ とすると, $ua + vm = 1$ となる u, v がある ($u, v \in \mathbf{Z}$).
 $b = u$ とおくと, $ab - 1 = -vm$ より, $ab \equiv 1 \pmod{m}$ である.

Remark $g.c.d.(a, m) = 1$, $ab \equiv 1 \pmod{m}$ とするとき, a^{-n} で $b^n \equiv (a^{-1})^n$ の剰余類を表わす.

例 7 841 を法とする 160 の逆元 160^{-1} を見つけよ.

問題 2-6(c) より,

$$841 = 160 \cdot 5 + 41$$

$$160 = 41 \cdot 3 + 37$$

$$41 = 37 \cdot 1 + 4$$

$$37 = 4 \cdot 9 + 1$$

$$4 = 1 \cdot 4 + 0$$

より,

$$\begin{aligned} 1 &= 37 - 4 \cdot 9 = 37 - (41 - 37 \cdot 1) \cdot 9 \\ &= 37 \cdot 10 - 41 \cdot 9 = (160 - 41 \cdot 3) \cdot 10 - 41 \cdot 9 \\ &= 160 \cdot 10 - 41 \cdot 39 = 160 \cdot 10 - (841 - 160 \cdot 5) \cdot 39 \\ &= 160 \cdot 205 - 841 \cdot 39 \end{aligned}$$

以上より, $160 \cdot 205 \equiv 1 \pmod{841}$ すなわち, $160^{-1} \equiv 205 \pmod{841}$

定理 2.3

$a \equiv b \pmod{m}$ $g.c.d.(a, m) = 1 (\Rightarrow g.c.d.(b, m) = 1)$ とすると,
 $a^{-1} \equiv b^{-1} \pmod{m}$

が成り立つ.

proof

$ab(a^{-1} - b^{-1}) \equiv b - a \equiv 0 \pmod{m}$ である. $ab(a^{-1} - b^{-1})$ が m の倍数となり, $g.c.d.(ab, m) = 1$ より, $(a^{-1} - b^{-1})$ が m の倍数で, $a^{-1} \equiv b^{-1} \pmod{m}$ が成り立つ.

定理 2.4 $0 \leq a, b < m$ のとき, 一次合同方程式

$$ax \equiv b \pmod{m}$$

について考える.

(1) $g.c.d.(a, m) = 1$ のとき, ある解 x_0 が存在し, すべての解 x は $x = x_0 + mn$ の形である.

(2) $g.c.d.(a, m) = d > 1$ のとき, $d|b$ であるときのみ解をもち,

$$a = a'd, \quad b = b'd, \quad m = m'd$$

とすると, $g.c.d.(a', m') = 1$ となり,

$$ax \equiv b \pmod{m} \iff a'x \equiv b' \pmod{m'}$$

定理 2.5(Fermat の小定理) p を素数とし, a を任意の整数とすると,

$$a^p \equiv a \pmod{p}$$

が成り立つ, さらに, a が p の倍数でなければ,

$$a^{p-1} \equiv 1 \pmod{p}$$

が成り立つ,

proof

$p \nmid a$ (a が p の倍数でない) とする.

$$0 \cdot a, \quad 1 \cdot a, \quad 2 \cdot a, \quad (p-1) \cdot a$$

はすべて異なる剰余類に属する. [なぜなら, $i \cdot a \equiv j \cdot a \pmod{p}$ ($0 \leq i, j \leq p-1$) とすると, $(i-j) \cdot a$ は p の倍数となり, a は p と互いに素であることから, $(i-j)$ が p の倍数となり, $0 \leq i, j \leq p-1$ より, $i = j$ でなければならない.]

$\{1 \cdot a, 2 \cdot a, 3 \cdot a, (p-1) \cdot a\}$ を並べ替えると, p を法として, $\{1, 2, 3, (p-1)\}$ と等しい. このことから,

$$(1 \cdot a) \cdot (2 \cdot a) \cdot (3 \cdot a) \cdots ((p-1) \cdot a) \equiv (p-1)! \pmod{p}$$

$$(p-1)! \cdot a^{p-1} \equiv (p-1)! \pmod{p}$$

$(p-1)!$ は p と互いに素であるので,

$$a^{p-1} \equiv 1 \pmod{p}$$

となる. この両辺に a をかければ, $a^p \equiv a \pmod{p}$ が得られ, これは a が p の倍数のときも成り立つ.

定理 2.5 の系 p を素数とし, a を p の倍数でない ($p \nmid a$) とする. また,

$$n \equiv m \pmod{p-1}$$

とすると,

$$a^n \equiv a^m \pmod{p}$$

が成り立つ.

proof $n \equiv m \pmod{p-1}$ であることより, $n = m + c(p-1)$ と書ける.

$$a^n = a^m \cdot (a^{p-1})^c \equiv a^m \pmod{p} \quad (\because a^{p-1} \equiv 1 \pmod{p})$$

例 8 $2^{1000000}$ を 7 進法で表示するとき, 第 1 位の数字は何か? ($2^{1000000}$ を 7 で割った余りを求めよ)

$$p = 7 \text{ とすると, } 1000000 \div (7 - 1) = 166666 \cdots 4 \quad i.e. \quad 1000000 = 6 \times 166666 + 4$$

$$1000000 \equiv 4 \pmod{7-1} \text{ より, } 2^{1000000} \equiv 2^4 \equiv 2 \pmod{7}$$

定理 2.6(中国剰余定理=Chinese Remainder Theorem)

連立合同方程式

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots\dots\dots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

を考える

$i \neq j$ のとき $\text{g.c.d.}(m_i, m_j) = 1$ (どの異なる m_i と m_j も互いに素) をみたせば, $M = m_1 m_2 \cdots m_r$ を法として一意的に解は存在する.

proof

M を法として解は一意的であることの証明

x' と x'' を 2 つの解とする.

すべての i について,

$$x = x' - x'' \equiv 0 \pmod{m_i}$$

どの m_i も互いに素であるので, 合同式の基本的性質 5 より,

$$x = x' - x'' \equiv 0 \pmod{M = m_1 m_2 \cdots m_r}$$

解の存在証明

$M_i = M/m_i$ とおく. $\text{g.c.d.}(M_i, m_i) = 1$ より, $\exists N_i \text{ s.t. } N_i M_i \equiv 1 \pmod{m_i}$

$$x = \sum_{j=1}^r a_j M_j N_j$$

$i \neq j$ のとき, M_i は m_i の倍数になっており, $M_i N_i \equiv 1 \pmod{m_i}$ より,

$$x \equiv a_i M_i N_i \equiv a_i \pmod{m_i}$$

例 9 連立合同方程式

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

上の解の存在証明に当てはめて解こう.

$$M = 3 \times 5 \times 7 = 105, \quad M_1 = M/3 = 35, \quad M_2 = M/5 = 21, \quad M_3 = M/7 = 15$$

$$35 \times 2 = 70 \equiv 1 \pmod{3} \text{ より, } N_1 \equiv M_1^{-1} \equiv 2 \pmod{3}$$

$$21 \times 1 = 21 \equiv 1 \pmod{5} \text{ より, } N_2 \equiv M_2^{-1} \equiv 1 \pmod{5}$$

$$15 \times 1 = 15 \equiv 1 \pmod{7} \text{ より, } N_3 \equiv M_3^{-1} \equiv 1 \pmod{7}$$

$$\text{以上より, } x \equiv 2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1 = 233 \equiv 23 \pmod{105}$$

定理 2.6 の系

$$m \text{ と } n \text{ が互いに素 } (g.c.d.(m, n) = 1) \implies \varphi(mn) = \varphi(m)\varphi(n)$$

proof

$$0 \sim (mn - 1) \text{ に } mn \text{ と互いに素な数があるか? } \varphi(mn)$$

$$0 \leq \forall j \leq (mn - 1) \quad j_1 : j \text{ を } m \text{ で割ったときの余り}$$

$$j_2 : j \text{ を } n \text{ で割ったときの余り}$$

Proposition II.3.3 より, j と (j_1, j_2) は 1 対 1 に対応する.

$$(\because \exists! j \text{ s.t. } j \equiv j_1 \pmod{m} \text{ かつ } j \equiv j_2 \pmod{n})$$

また,

$$j \text{ と } mn \text{ と互いに素} \iff j_1 \text{ が } m \text{ と互いに素} \text{ かつ } j_2 \text{ が } n \text{ と互いに素}$$

以上より,

$$\begin{aligned} \varphi(mn) &= (mn \text{ と互いに素な } j \text{ の個数}) \\ &= (m \text{ と互いに素な } j_1 \text{ の個数}) \times (n \text{ と互いに素な } j_2 \text{ の個数}) \\ &= \varphi(m)\varphi(n) \end{aligned}$$

この定理 2.6 の系を用いると, 素因数分解された $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ とすると,

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}) \\ &= \varphi(p_1^{\alpha_1}) \varphi(p_2^{\alpha_2}) \cdots \varphi(p_r^{\alpha_r}) \\ &= p_1^{\alpha_1} \left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2} \left(1 - \frac{1}{p_2}\right) \cdots p_r^{\alpha_r} \left(1 - \frac{1}{p_r}\right) \\ &= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right) \\ \varphi(n) &= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right) = n \times \prod_{p|n: \text{素数}} \left(1 - \frac{1}{p}\right) \end{aligned}$$

例 $\varphi(12) = 12 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) = 4$, $\varphi(100) = 100 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right) = 40$

定理 2.7(Euler) a が m と素 $(g.c.d.(a, m) = 1)$ であるとき,

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

が成り立つ.

proof(i) $m = p^\alpha$ (p : 素数) のとき, α に関する帰納法で証明する.

$$\alpha = 1 \text{ のとき, } a^{\varphi(m)} = a^{\varphi(p)} = a^{p-1} \equiv 1 \pmod{p = m}$$

$$\alpha = k \text{ のとき, 成り立つと仮定すると } a^{\varphi(p^k)} = a^{p^k - p^{k-1}} \equiv 1 \pmod{p^k}$$

$$\alpha = k + 1 \text{ のときは } a^{\varphi(p^{k+1})} = a^{p^{k+1} - p^k} = a^{p(p^k - p^{k-1})} = \left(a^{p^k - p^{k-1}}\right)^p$$

帰納法の仮定より, $a^{p^k - p^{k-1}} = 1 + b \cdot p^k$ と書け,

$$a^{\varphi(p^{k+1})} = (1 + b \cdot p^k)^p = {}_pC_0 + {}_pC_1 b \cdot p^k + {}_pC_2 (b \cdot p^k)^2 + \cdots + {}_pC_p (b \cdot p^k)^p$$

この右辺の第1項目を除けばすべての項は p^{k+1} で割り切れるので,

$$a^{\varphi(p^{k+1})} \equiv {}_pC_0 = 1 \pmod{p^{k+1}}$$

(ii) $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ のとき, 任意の i について,

$$a^{\varphi(m)} = a^{\varphi(p_1^{\alpha_1}) \varphi(p_2^{\alpha_2}) \cdots \varphi(p_r^{\alpha_r})} \equiv 1 \pmod{p_i^{\alpha_i}} \quad (\because a^{\varphi(p_i^{\alpha_i})} \equiv 1 \pmod{p_i^{\alpha_i}})$$

合同式の基本的性質5より,

$$a^{\varphi(m)} \equiv 1 \pmod{m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}}$$

が成り立つ.

定理 2.7 の系 a と m が互いに素 ($\gcd(a, m) = 1$) とし, n を $\varphi(m)$ で割った余りを n' とするとき,

$$a^n \equiv a^{n'} \pmod{m}$$

が成り立つ.

proof $n = n' + c \cdot \varphi(m)$ と書けるので,

$$a^n = a^{n'} \cdot \left(a^{\varphi(m)}\right)^c \equiv a^{n'} \pmod{m} \quad (\because a^{\varphi(m)} \equiv 1 \pmod{m})$$

Remark a と m が互いに素であるとき, $a^{\varphi(m)} \equiv 1 \pmod{m}$ であるが, $a^x \equiv 1 \pmod{m}$ となるもっと小さな x を見つけたい.定理 2.7(Euler) の証明から, $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ のとき, x として, $\varphi(p_1^{\alpha_1}), \varphi(p_2^{\alpha_2}), \dots, \varphi(p_r^{\alpha_r})$ の最小公倍数をとれば, $a^x \equiv 1 \pmod{m}$ となる.**例 9** $m = 105 = 3 \cdot 5 \cdot 7$, a を m と互いに素であるとすれば, $\varphi(3) = 2$, $\varphi(5) = 4$, $\varphi(7) = 6$ の最小公倍数 12 をとれば, $a^{12} \equiv 1 \pmod{105}$ ($\varphi(105) = 2 \cdot 4 \cdot 6 = 48$)**例 10** $2^{1000000} \equiv ? \pmod{77}$ 解法 1(上の Remark を用いる方法) $77 = 7 \cdot 11$, $\varphi(7) = 6$, $\varphi(11) = 10$, 6 と 10 の最小公倍数は 30

$$2^{30} \equiv 1 \pmod{77}, \quad 1000000 = 30 \cdot 33333 + 10$$

$$2^{1000000} = (2^{30})^{33333} \cdot 2^{10} \equiv 2^{10} = 1024 = 77 \cdot 13 + 23 \equiv 23 \pmod{77}$$

解法 2(定理 2.5 の系と定理 2.6(中国剰余定理) を用いる方法)

$$2^{1000000} \equiv ? \pmod{7}$$

$$1000000 = (7 - 1) \cdot 166666 + 4 \quad \text{より,} \quad 2^{1000000} \equiv 2^4 = 16 \equiv 2 \pmod{7}$$

$$2^{1000000} \equiv ? \pmod{11}$$

$$1000000 = (11 - 1) \cdot 100000 + 0 \quad \text{より,} \quad 2^{1000000} \equiv 2^0 \equiv 1 \pmod{11}$$

$$x = 2^{1000000} \equiv 2 \pmod{7}, \quad x \equiv 1 \pmod{11}, \quad \text{中国剰余定理の証明と,}$$

$$11^{-1} \equiv 2 \pmod{7}, \quad 7^{-1} \equiv 8 \pmod{11} \quad \text{より,}$$

$$x = 2^{1000000} \equiv 2 \cdot 2 \cdot 11 + 1 \cdot 8 \cdot 7 = 100 \equiv 23 \pmod{77}$$

問題 2-13 次の解を求めよ.

$$(1) \quad 3x \equiv 4 \pmod{7}$$

$$(2) \quad 3x \equiv 4 \pmod{12}$$

$$(3) \quad 9x \equiv 12 \pmod{21}$$

$$(4) \quad 27x \equiv 25 \pmod{256}$$

$$(5) \quad 27x \equiv 72 \pmod{900}$$

$$(6) \quad 103x \equiv 612 \pmod{676}$$

問題 2-14 完全平方数を 16 進法で表わすとき, 第 1 位の数字は何になるか? 可能な数字をすべてあげよ.

問題 2-15 連続する 2 つの正の奇数の積を 12 進法で表わすとき, 第 1 位の数字は何になるか? 可能な数字をすべてあげよ.

問題 2-16 n を 10 進法で表わすとき, 次のことを証明せよ.

$$3|n \iff 3|(\text{各桁の数字の和})$$

$$9|n \iff 9|(\text{各桁の数字の和})$$

問題 2-17 $30|(n^5 - n)$ であることを証明せよ.

問題 2-18 次の連立合同方程式の解を求めよ.

$$(1) \quad \begin{cases} x \equiv 4 \pmod{7} \\ x \equiv 4 \pmod{9} \\ x \equiv 4 \pmod{11} \end{cases}$$

$$(2) \quad \begin{cases} x \equiv 1 \pmod{11} \\ x \equiv 2 \pmod{12} \\ x \equiv 3 \pmod{13} \end{cases}$$

$$(3) \quad \begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 4 \pmod{11} \\ x \equiv 5 \pmod{16} \end{cases}$$

問題 2-19 $\varphi(90), \varphi(91), \varphi(92), \dots, \varphi(100)$ を求めよ.

問題 2-20 $\varphi(n) \leq 12$ となる n をすべて求めよ.

また, それらがすべてであることを示せ.

2.4 群

集合 G とその任意の 2 つの元 a と b に対して 2 項演算 $\cdot$ が定義され, 次の条件 (1-1)~(1-3) を満たすとき, $(G, \cdot)$ を 群 (group) であるという.

$$(1-1) \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$$

(1-2) G にある元 e が存在して, G の任意の元 a に対して,

$$a \cdot e = e \cdot a = a$$

となる. (e を 単位元 という)

(1-3) G の任意の a に対して, G にある元 a^{-1} が存在して

$$a \cdot a^{-1} = a^{-1} \cdot a = e$$

となる. (a^{-1} を a の 逆元 という)

さらに, 次の (1-4) を満たす群を 可換群, 満たさない群を 非可換群 という.

(1-4) G の任意の 2 つの元 a と b に対して,

$$a \cdot b = b \cdot a$$

となる.

例 10(群の例)

$$(1) \quad (\mathbf{Z}, +)$$

$$(2) \quad (\mathbf{Q}, +)$$

$$(3) \quad (\mathbf{Q} \setminus \{0\}, \times) \quad (\mathbf{Q} \text{ の代わりに } \mathbf{R} \text{ や } \mathbf{C} \text{ でも同じ})$$

$$(4) \quad (\mathbf{Z}/p\mathbf{Z} \setminus \{0\}, \times) \quad (\text{ただし, } p \text{ は素数})$$

置換群

集合 X からそれ自身への全単射を集合 X の置換という. いま, $X = \{1, 2, \dots, n\}$ とする. この X の置換全体を S_n と書くことにする. (S_n は何個の元からなるか?)

置換の記号

1 つの置換を σ とする.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ j_1 & j_2 & j_3 & \cdots & j_n \end{pmatrix} \quad \text{は} \quad \sigma(1) = j_1, \sigma(2) = j_2, \dots, \sigma(n) = j_n \text{ を表わす.}$$

$$\sigma = \begin{pmatrix} j_1 & j_2 & j_3 & \cdots & j_n \\ k_1 & k_2 & k_3 & \cdots & k_n \end{pmatrix} \quad \text{は} \quad \sigma(j_1) = k_1, \sigma(j_2) = k_2, \dots, \sigma(j_n) = k_n \text{ を表わす.}$$

$$\sigma = \begin{pmatrix} j_1 & j_2 & j_3 & \cdots & j_n \\ k_1 & k_2 & k_3 & \cdots & k_n \end{pmatrix} \quad \text{は} \quad \sigma(j_1) = k_1, \sigma(j_2) = k_2, \dots, \sigma(j_n) = k_n \text{ を表わす.}$$

自分自身に移る元は省略することがある. 例えば,

$$\sigma = \begin{pmatrix} 2 & 3 & 5 \\ 3 & 5 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 4 & 2 \end{pmatrix}$$

次のような置換を 巡回置換 という.

$$\sigma = \begin{pmatrix} j_1 & j_2 & j_3 & \cdots & j_r \\ j_2 & j_3 & j_4 & \cdots & j_1 \end{pmatrix} \quad \text{これを } (j_1, j_2, j_3, \dots, j_r) \text{ と表わす.}$$

次のような2つだけの入れ替えの置換を 互換 という.

$$\sigma = \begin{pmatrix} j_1 & j_2 \\ j_2 & j_1 \end{pmatrix} = (j_1, j_2)$$

置換の積

$$\sigma = \begin{pmatrix} j_1 & j_2 & j_3 & \cdots & j_n \\ k_1 & k_2 & k_3 & \cdots & k_n \end{pmatrix}, \quad \tau = \begin{pmatrix} i_1 & i_2 & i_3 & \cdots & i_n \\ j_1 & j_2 & j_3 & \cdots & j_n \end{pmatrix} \text{ とするとき,}$$

$$\sigma \cdot \tau = \begin{pmatrix} j_1 & j_2 & j_3 & \cdots & j_n \\ k_1 & k_2 & k_3 & \cdots & k_n \end{pmatrix} \cdot \begin{pmatrix} i_1 & i_2 & i_3 & \cdots & i_n \\ j_1 & j_2 & j_3 & \cdots & j_n \end{pmatrix} = \begin{pmatrix} i_1 & i_2 & i_3 & \cdots & i_n \\ k_1 & k_2 & k_3 & \cdots & k_n \end{pmatrix}$$

これは置換を写像とみなしたとき, τ で写してから σ で写す写像の積である.

このように定義すると $(S_n, \cdot)$ は群になる.

問題 2-21 S_3 の元をすべて挙げよ. 単位元を $e = \sigma_0$ とし, そのほかを $\sigma_1, \sigma_2, \dots, \sigma_5$ とせよ. また, 積の演算表を作れ. さらに, 非可換な元の組をすべて挙げよ.

問題 2-22 互換の積 $(k_1, k_r)(k_1, k_{r-1}) \cdots (k_1, k_2)$ が巡回置換であることを確かめよ. また, 巡回置換 $(1, 2, 3, 4, 5)$ を互換の積で表わせ.

問題 2-23 置換 $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 3 & 4 & 2 & 6 & 7 & 1 \end{pmatrix}$ を巡回置換の積で表わし, さらに互換の積で表わせ.

問題 2-22 と問題 2-23 のように, すべての置換は互換の積で表わせる (表わし方は1通りではない). この積が偶数個の積であるか奇数個の積であるかは与えられた置換によって定まる. 偶数個の積で表わせる置換を 偶置換, 奇数個の積で表わせる置換を 奇置換 とよぶ.

問題 2-24 S_3 の各置換が偶置換か奇置換か判定せよ.

2.5 環と体

集合 R と 2 つの 2 項演算, 加法 $+$ と乗法 $\cdot$ が定義され, 次の条件を満たすとき, $(R, +, \cdot)$ を **環 (ring)** であるという.

$$(2-1) \quad (a + b) + c = a + (b + c) \quad (\text{加法の結合法則})$$

$$(2-2) \quad a + b = b + a \quad (\text{加法の可換法則})$$

$$(2-3) \quad R \text{ にある元 } 0 \text{ が存在して, } R \text{ の任意の元 } a \text{ に対して,}$$

$$a + 0 = 0 + a = a$$

となる. (0 を **加法の単位元** あるいは **零元** という)

$$(2-4) \quad R \text{ の任意の } a \text{ に対して, } R \text{ にある元 } -a \text{ が存在して}$$

$$a + (-a) = (-a) + a = 0$$

となる. ($-a$ を a の **加法の逆元** という)

$$(2-5) \quad (a \cdot b) \cdot c = a \cdot (b \cdot c) \quad (\text{乗法の結合法則})$$

$$(2-6) \quad a \cdot (b + c) = a \cdot b + a \cdot c, \quad (a + b) \cdot c = a \cdot c + b \cdot c \quad (\text{分配法則})$$

また, (2-1)~(2-6) に加えて, 次の (2-7) が成り立つ環を **可換環** という.

$$(2-7) \quad a \cdot b = b \cdot a \quad (\text{乗法の可換法則})$$

例 11(環の例)

$$(1) \quad (\mathbf{Z}, +, \times) \quad (\mathbf{Z} \text{ の代わりに } \mathbf{Q}, \mathbf{R}, \mathbf{Z} \text{ でも同じ})$$

$$(2) \quad (\text{整数係数の多項式の全体}, +, \times)$$

(”整数係数”の代わりに ”有理数係数”でも”実数係数”でも”複素数係数”でも同じ)

$$(3) \quad (n \text{ 次正方行列の全体}, +, \cdot)$$

$$(4) \quad (\mathbf{Z}/n\mathbf{Z}, +, \times) \quad (\text{ただし, } n \text{ は } 2 \text{ 以上の自然数})$$

(2-1)~(2-6) に加えて, 次の (2-8) と (2-9) が成り立つ環を **体 (field)** という.

$$(2-8) \quad R \text{ にある元 } e \text{ が存在して, } R \text{ の任意の元 } a \text{ に対して,}$$

$$a \cdot e = e \cdot a = a$$

となる. (e を **乗法の単位元** という)

$$(2-9) \quad R \text{ の } 0 \text{ と異なる任意の } a \text{ に対して, } R \text{ にある元 } a^{-1} \text{ が存在して}$$

$$a \cdot a^{-1} = a^{-1} \cdot a = e$$

となる. (a^{-1} を a の **乗法の逆元** という)

(2-7) も満たす体を, **可換体** という.

例 12(体の例)

$$(1) \quad (\mathbf{Q}, +, \times) \quad (\mathbf{Q} \text{ の代わりに } \mathbf{R}, \mathbf{Z} \text{ でも同じ})$$

$$(2) \quad (\mathbf{Z}/p\mathbf{Z}, +, \times) \quad (\text{ただし, } p \text{ は素数})$$

3 命題と論理

3.1 命題論理学

命題とは 真 (True) であるか 偽 (False) であるかが定まる文章のことである。疑問文や命令文や感嘆文は命題とは考えられない。

例 次の文章が命題であるか命題でないか考えて見なさい。また命題であれば、その命題が真であるか偽であるか判定しなさい。(あまり、厳密には考えない)

- ・「3は自然数である」
- ・「 $\frac{3}{5}$ は自然数である」
- ・「小泉首相は偉大な人である」
- ・「大阪は日本の首都である」
- ・「人間は必ず死ぬ」
- ・「明日は雨が降る」
- ・「昨日風が強かった」
- ・「学校へ行きなさい」
- ・「明石公園の桜はなんときれいなんでしょう」

命題は p, q などとアルファベットの小文字で表わすことにする。

(1) 否定 (～ではない) (記号 $\neg$)

p = 「大阪は日本の首都である」

とするととき,

$\neg p$ = 「大阪は日本の首都ではない」

否定の真偽表

p	$\neg p$
T	F
F	T

(2) 論理和 (=選言 または) (記号 $\vee$)

p = 「人間は魚類である」

q = 「人間は哺乳類である」

とするととき,

$p \vee q$ = 「人間は魚類であるかまたは人間は哺乳類である」

を表わす。

論理和の真偽表

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

(3) 論理積 (= 連言 かつ) (記号 $\wedge$) p = 「クジラは魚類である」 q = 「人間は哺乳類である」

とすると,

 $p \wedge q$ = 「クジラは魚類でありかつ人間は哺乳類である」

を表わす.

論理積の真偽表

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

(4) 含意 (ならば) (記号 $\implies$) p = 「風が吹く」 q = 「桶屋が儲かる」

とすると,

 $p \implies q$ = 「風が吹けば桶屋が儲かる」

を表わす.

含意の真偽表

p	q	$p \implies q$
T	T	T
T	F	F
F	T	T
F	F	T

「 $p \implies q$ 」は「 $(\neg p) \vee q$ 」と同じであることは次の真偽表から分かる.

p	q	$\neg p$	$(\neg p) \vee q$
T	T	F	T
T	F	F	F
F	T	T	T
F	F	T	T

(5) 同値 (記号 $\iff$) p = 「Aさんは生きている」 q = 「Aさんは死んでいない」

とすると,

 $p \iff q$ = 「Aさんは生きていることと Aさんは死んでいないことは同値である」

を表わす.

同値の真偽表

p	q	$p \iff q$
T	T	T
T	F	F
F	T	F
F	F	T

いくつかの命題と $\neg$, $\vee$, $\wedge$, $\implies$, $\iff$ を用いて書かれた式を **論理式** という.「 $\neg(\neg p)$ 」と「 p 」「 $p \implies q$ 」と「 $(\neg p) \vee q$ 」のように、どのような場合でも真偽が等しい論理式を **論理的に同値** であるといい、次のように記号「 $\equiv$ 」で表わす.

$$\neg(\neg p) \equiv p, \quad p \implies q \equiv (\neg p) \vee q$$

次の3つの定理が成り立つ.

定理 3-1

- (1) $\neg(\neg p) \equiv p$
- (2) $p \vee p \equiv p$, $p \wedge p \equiv p$
- (3) $p \vee q \equiv q \vee p$, $p \wedge q \equiv q \wedge p$ (交換法則)
- (4) $(p \vee q) \vee r \equiv p \vee (q \vee r)$, $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$ (結合法則)
- (5) $p \wedge (\neg p) \equiv F$ (矛盾律), $p \vee (\neg p) \equiv T$ (排中律)
- (6) $p \wedge T \equiv p$, $p \vee T \equiv T$
- (7) $p \wedge F \equiv F$, $p \vee F \equiv p$

定理 3-2(de Morgan の法則)

- (8) $\neg(p \vee q) \equiv (\neg p) \wedge (\neg q)$
- (9) $\neg(p \wedge q) \equiv (\neg p) \vee (\neg q)$

定理 3-3(分配法則)

- (10) $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
- (11) $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

逆・対偶・裏

命題「 $p \implies q$ 」に対して,

- 「 $q \implies p$ 」を 逆 ($q \implies p \equiv (\neg q) \vee p$)
- 「 $(\neg p) \implies (\neg q)$ 」を 裏 ($(\neg p) \implies (\neg q) \equiv p \vee (\neg q)$)
- 「 $(\neg q) \implies (\neg p)$ 」を 対偶 ($(\neg q) \implies (\neg p) \equiv q \vee (\neg p)$)

という. $p \implies q \equiv (\neg p) \vee q$ より,

「元の命題」と「対偶」は論理的に同値,

「裏」と「逆」は論理的に同値

であることが分かる.

3.2 変数を含んだ命題 (命題関数)

「 $x \geq 0$ 」, 「 x は人間である」などのように変数を含んだ命題を考える. 変数は複数個ある場合もある. 変数を含んだ命題を **命題関数** という. それらを, $p(x)$ のように表わす. 命題関数の場合も前の3つの定理はそのまま成り立つ. x の定義域 (考える範囲) を **対象領域** とよぶことにする.

$p(x)$ = 「 x は有理数である」とするとき, $p(7)$ = 「7 は有理数である」, $p(\pi)$ = 「 π は有理数である」となる.

全称記号 ($\forall$) と存在記号 ($\exists$) と否定

$p(x)$ に対して,

$$\forall x p(x) = \text{「すべての } x \text{ に対して, } p(x)\text{」}$$

を表わし,

$$\exists x p(x) = \text{「} p(x) \text{ であるような } x \text{ が存在する」} = \text{「ある } x \text{ が存在して } p(x)\text{」}$$

例えば, $p(x)$ = 「 x は有理数である」とするとき,

$$\forall x p(x) = \text{「すべての } x \text{ は有理数である」}$$

$$\exists x p(x) = \text{「有理数であるような } x \text{ が存在する」}$$

定理 3-4 (de Morgan ?)

$$(12) \quad \neg(\forall x p(x)) = \exists x(\neg p(x))$$

$$(13) \quad \neg(\exists x p(x)) = \forall x(\neg p(x))$$

例 (1) 「すべての実数 x に対して $x^2 \geq 0$ 」の否定は

「ある実数 x に対して, $x^2 \not\geq 0$ 」 = 「 $x^2 \not\geq 0$ となる実数 x が存在する」

(2) 「ある実数 x に対して $x^2 \geq 0$ 」の否定は「すべての実数 x に対して, $x^2 \not\geq 0$ 」

2つ以上の変数を含んだ命題

$p(x, y)$ = 「 $x > y$ 」 とするとき,

$$\begin{aligned} \forall x \forall y p(x, y) &= \forall x(\forall y p(x, y)) = \forall y \forall x p(x, y) = \forall y(\forall x p(x, y)) \\ &= \text{「すべての } x \text{ とすべての } y \text{ に対して } x > y \text{ である」} \end{aligned}$$

$$\begin{aligned} \exists x \exists y p(x, y) &= \exists x(\exists y p(x, y)) = \exists y \exists x p(x, y) = \exists y(\exists x p(x, y)) \\ &= \text{「ある } x \text{ とある } y \text{ が存在して } x > y \text{ である」} \end{aligned}$$

$$\begin{aligned} \forall x \exists y p(x, y) &= \forall x(\exists y p(x, y)) \\ &= \text{「すべての } x \text{ に対して, ある } y \text{ が存在して } x > y \text{ である」} \end{aligned}$$

(このとき, y は x に関係してよい)

$$\exists y \forall x p(x, y) = \exists y (\forall x p(x, y))$$

= 「ある y が存在して、すべての x に対して $x > y$ である」

= 「「すべての x に対して $x > y$ となる」ような x が存在する」

(このとき, y は x に関係してはいけない)

以上のように, $\forall x$ と $\forall y$ の順番は入れ替えてもよい.

同様に, $\exists x$ と $\exists y$ も順番を入れ替えてもよい.

しかし, $\forall x$ と $\exists y$ の順番は入れ替えることは出来ない.

2つ以上の変数を含んだ命題の否定

$$\neg(\forall x \forall y p(x, y)) = \exists x \exists y (\neg p(x, y))$$

$$\neg(\exists x \exists y p(x, y)) = \forall x \forall y (\neg p(x, y))$$

$$\neg(\forall x \exists y p(x, y)) = \exists x \forall y (\neg p(x, y))$$

$$\neg(\exists x \forall y p(x, y)) = \forall x \exists y (\neg p(x, y))$$

3.3 命題の記号化と仮定のもとでの真偽

次の4つの type の命題を考えよう.

- ・すべてのアメリカ人は野球が好きである。(全称肯定命題)
- ・どのアメリカ人も野球は好きでない。(全称否定命題)
- ・あるアメリカ人は野球が好きである。(特称肯定命題)
- ・あるアメリカ人は野球が好きでない。(特称否定命題)

これらの命題を記号で表わそう (**命題の記号化**).

x の対象領域を「すべてのアメリカ人」とし, $p(x)$ = 「 x は野球が好きである」とすれば,

「すべてのアメリカ人は野球が好きである」は「 $\forall x p(x)$ 」

「どのアメリカ人も野球は好きでない」は「 $\forall x (\neg p(x))$ 」

「あるアメリカ人は野球が好きである」は「 $\exists x p(x)$ 」

「あるアメリカ人は野球が好きでない」は「 $\exists x (\neg p(x))$ 」

また, x の対象領域を「すべてのアメリカ人」に限定しないとき,

$p(x)$ = 「 x はアメリカ人である」

$q(x)$ = 「 x は野球がすきある」

とすると,

「すべてのアメリカ人は野球が好きである」は「 $\forall x (p(x) \implies q(x))$ 」

「どのアメリカ人も野球は好きでない」は「 $\forall x (p(x) \implies \neg q(x))$ 」

「あるアメリカ人は野球が好きである」は「 $\exists x(p(x) \wedge q(x))$ 」

「あるアメリカ人は野球が好きでない」は「 $\exists x(p(x) \wedge (\neg q(x)))$ 」

ある命題を「真」であると仮定したとき、それに関連した命題の「真偽」について調べよう。以下では、 x の対象領域は空でないとする。

「 $\forall x p(x)$ 」が「真」であることを仮定すると、

「 $\exists x p(x)$ 」は「真」.

「 $\forall x(\neg q(x))$ 」は「偽」.

「 $\exists x(\neg q(x))$ 」は「偽」.

「 $\exists x p(x)$ 」が「真」であることを仮定すると、

「 $\forall x p(x)$ 」は「真偽不明」.

「 $\forall x(\neg q(x))$ 」は「偽」.

「 $\exists x(\neg q(x))$ 」は「真偽不明」.

「 $\forall x(p(x) \implies q(x))$ 」が「真」であることを仮定すると、

「 $\exists x(p(x) \wedge q(x))$ 」は「真」.

「 $\forall x(p(x) \implies \neg q(x))$ 」は「偽」.

「 $\exists x(p(x) \wedge (\neg q(x)))$ 」は「偽」.

「 $\forall x(q(x) \implies p(x))$ 」は「真偽不明」.

「 $\exists x(p(x) \wedge q(x))$ 」が「真」であることを仮定すると、

「 $\forall x(p(x) \implies q(x))$ 」は「真偽不明」.

「 $\forall x(p(x) \implies \neg q(x))$ 」は「偽」.

「 $\exists x(p(x) \wedge (\neg q(x)))$ 」は「真偽不明」.