集合論

花木 章秀

2007 年度後期 (2007/12/14)

目次

Chapter 4

関係

世の中には、色々な “関係” がある。例えば、人と人との関係にも、

- A さんは B さんを知っている
- A さんは B さんのことが好きである
- A さんと B さんは同じ高校を卒業している
- A さんは B さんよりも将棋が強い

など、いくら書いてもきりがない。これは数学的な対象についても同様である。同じ集合に属する二つの元の “関係” について、それを数学的に定義し、議論する。

4.1 関係

定義 4.1.1 (関係)**.** A を集合とする。直積集合 $A \times A$ の部分集合 R を A 上の**二項関係**、または単に**関係**という。A 上に関係 R が定められていることを明示したい場合には (A, R) と書く。

R を関係とするとき $(x, y) \in R$ であることを xRy とも書くことにする。

例 4.1.2. (1) $\leq := \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \leq y\}$ は $\mathbb{R}$ 上の関係である。

(2) $< := \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x < y\}$ は $\mathbb{R}$ 上の関係である。

(3) 集合 A に対してべき集合 2^A を考える。$\subset := \{(S, T) \in 2^A \times 2^A \mid S \subset T\}$ は 2^A 上の関係である。

(4) $| := \{(n, m) \in \mathbb{N} \times \mathbb{N} \mid n \text{ は } m \text{ の約数 }\}$ は $\mathbb{N}$ 上の関係である。

この例において、(1), (2), (3) では “$\leq$” などを定義する右辺で “$\leq$” 自身を使っていて、好ましい記述ではないが、例を理解するには十分であろう。

例 4.1.3. $\mathbb{N}\times\mathbb{Z}$ 上に

$$\sim := \{((m,a),(n,b)) \in (\mathbb{N}\times\mathbb{Z})\times(\mathbb{N}\times\mathbb{Z}) \mid mb = na\}$$

で関係 $\sim$ を定義できる。

ここに挙げた例は (例 4.1.3 を除いて) よく知られた性質を用いて関係を定義しているが、一般に A 上の関係は $A\times A$ の部分集合と言うだけでよいので、かなり自由に関係を定義できる。

4.2 順序関係

通常の生活でも、順序という言葉はよく用いられる。例えば、小学生でも背の低い順に列に並んだりする。この順序について考えよう。順序を表す記号として、よく使われるものを用いると、いろいろな先入観が入りやすいので、ここでは $\preceq$ という、あまり使われない記号を用いることにする。

定義 4.2.1 (順序関係)**.** 集合 A 上の関係 $\preceq$ が**順序関係**、または単に**順序**であるとは、以下の条件を満たすこととする。

(1) [**反射律**] 任意の $x\in A$ に対して $x\preceq x$

(2) [**推移律**] $x\preceq y,\ y\preceq z$ ならば $x\preceq z$

(3) [**非対称律**] $x\preceq y,\ y\preceq x$ ならば $x=y$

このとき $(A,\preceq)$ を**順序集合**という。

例 4.2.2. 「ジャンケン」を考えよう。「グー」は「チョキ」に強く、「チョキ」は「パー」に強く、「パー」は「グー」に強い。これは推移律が成り立たないことを意味しており、ジャンケンにおける「強い」ということは、関係を定めてはいるが、それは順序関係ではない。

例 4.2.3. 例 4.1.2 の $(\mathbb{R},\leq)$, $(\mathbb{N},|)$, $(2^A,\subset)$ はすべて順序集合である。例 4.1.2 の $(\mathbb{R},<)$ は条件 (1) を満たさないので順序集合ではない。例 4.1.3 $(\mathbb{N}\times\mathbb{Z},\sim)$ は条件 (3) を満たさないので順序集合ではない。

練習のため例 4.1.2 の $(\mathbb{N},|)$ が順序集合であることを示しておこう。

(1) まず、任意の $n\in\mathbb{N}$ に対して n は n の約数であるから $n\mid n$ である。

(2) $\ell,m,n\in\mathbb{N}$ に対して $\ell\mid m,\ m\mid n$ とすると ℓ は m の約数であり m は n の約数であるから ℓ は n の約数である。したがって $\ell\mid n$ が成り立つ。

(3) $m,n\in\mathbb{N}$ に対して $m\mid n$ かつ $n\mid m$ とすると m は n の約数で n は m の約数なので $m=n$ である。

以上より $(\mathbb{N}, |)$ が順序集合であることが示される。

ここで注意したいのは、例えば 2 と 3 については $2 \mid 3$ も $3 \mid 2$ も成り立たないということである。一般に順序集合の任意の二つの要素について「どちらかが大きい」という順序が定まるわけではない。

定義 4.2.4 (全順序)**.** 順序集合 $(A, \preceq)$ の任意の二つの要素 $x, y \in A$ に対して $x \preceq y$ または $y \preceq x$ が成り立つとき、この順序を**全順序**といい、この順序集合を**全順序集合**という。単なる順序を全順序とはっきり区別したいときには**半順序**という言い方もする。

例 4.2.5. 例 4.1.2 $(\mathbb{R}, \leq)$ は全順序集合であるが、例 4.1.2 $(\mathbb{N}, |)$, $(2^A, \subset)$ は全順序集合ではない。

例 4.2.6. 前述の「小学生を背の低い順に並べる」ということを考えよう。ある小学校のクラスの生徒を、ある身体測定の際の身長の小さい順に並べるとする。より一般に、集合 X と写像 $f : X \to \mathbb{R}$ が与えられ、f による値によって、集合 X の順序を決めるということを考えよう。自然に考えられる順序 $\preceq$ の決め方として

(1) $f(A) < f(B)$ のとき $A \preceq B$、すなわち

$$\preceq = \{(A, B) \in X \times X \mid f(A) < f(B)\}$$

(2) $f(A) \leq f(B)$ のとき $A \preceq B$、すなわち

$$\preceq = \{(A, B) \in X \times X \mid f(A) \leq f(B)\}$$

が考えられる。(1) は推移律、非対称律をみたすが、反射律をみたさないので順序ではない。(2) は反射律、推移律をみたすが、非対称律をみたさないので、やはり順序ではない。順序を定義するには

$$\preceq = \{(A, A) \in X \times X \mid A \in X\} \cup \{(A, B) \in X \times X \mid f(A) < f(B)\}$$

とすればよい。このとき $A \neq B$ で $f(A) = f(B)$ であるものに対しては $A \preceq B$ でも $B \preceq A$ でもなく、よってこの順序は全順序ではない。

順序集合 $(A, \preceq)$ を考える。$B \subset A$ に対して B の順序を A の順序で定めれば、B はまた順序集合になる。これを**順序部分集合**と呼ぶ。

順序集合 $(A, \preceq)$ の元 x に対して $x \preceq y$ ならば $x = y$ が成り立つとき x を A の**極大元**という。同様に $y \preceq x$ ならば $x = y$ であるとき x を A の**極小元**という。任意の $y \in A$ に対して $y \preceq x$ のとき x を A の**最大元**という。任意の $y \in A$ に対して $x \preceq y$ のとき x を A の**最小元**という。最大元は極大元、最小元は極小元であるが、逆は成り立つとは限らない。最大元、最小元は存在するとは限らないが、存在すれば唯一つに定まる。

例 4.2.7. 例 4.1.2 の順序集合 $(2^A, \subset)$ を考える。2^A には最大元 A と最小元 ϕ が存在する。

例 4.2.8. 例 4.1.2 の順序集合 $(2^A, \subset)$ を考え、その順序部分集合 $B = 2^A - \{\phi, A\}$ を考える。ここで $|A| > 1$ と仮定する。このとき B には最大元も最小元も存在しない。任意の $a \in A$ に対して $\{a\}$ は B の極小元であり、$A - \{a\}$ は B の極大元である。

命題 4.2.9. 全順序集合の極大元 (極小元) は最大元 (最小元) である。

証明. 極大元についてのみ示せば、極小元についても同様である。A を全順序集合とし $a \in A$ をその極大元とする。A が全順序集合なので、任意の $b \in A$ に対して $b \preceq a$ または $a \preceq b$ が成り立つが、a が極大であることから $b \preceq a$ である。よって a は最大元である。 □

順序集合 $(A, \preceq)$ の部分集合 B に対して $x \in A$ が $y \preceq x$ $(\forall y \in B)$ を満たすとき、x を B の**上界**という。B の上界が存在するとき B は**上に有界である**という。

例 4.2.10. 順序集合 $(\mathbb{R} \leq)$ を考える。$B = (0, 1)$ (開区間) とすれば、例えば 2 は B の上界であり、よって B は上に有界である。ここで $2 \notin B$ でもよいことに注意しておく。

定義 4.2.11 (整列順序)**.** 集合 A 上の順序 $\preceq$ が**整列順序**であるとは任意の空でない部分集合に最小元が存在することである。整列順序によって順序が与えられた順序集合を**整列集合**という。

例 4.2.12. $\mathbb{N}$ や $\{-1, 0\} \cup \mathbb{N}$ は通常の $\leq$ という順序で整列集合である。しかし $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Q}$ は整列集合ではない。

問 4.2.13. $\{r \in \mathbb{Q} \mid r \geq 0\}$ は整列集合ではないことを示せ。

例 4.2.14. $A = \{1, 2\}$ としてべき集合 2^A を考える。このとき $B = \{\{1\}, \{2\}\} \subset 2^A$ を考えれば B に最小元はないので 2^A は整列集合ではない。

命題 4.2.15. 整列集合は全順序集合である。

証明. A を全順序集合ではない順序集合とする。このとき $a \preceq b$ でも $b \preceq a$ でもない $a, b \in A$ が存在する。例 4.2.14 と同じように $B = \{a, b\}$ を考えれば B には最小元は存在しない。 □

$B = [a_1, a_2, \cdots]$ を順序集合 A の元の列とする。(同じ元を含んでもよい。よって B は部分集合ということではないので異なる記号を用いている。) B が**単調減少列** (**単調増加列**) であるとは $a_{i+1} \preceq a_i$ $(a_i \preceq a_{i+1})$ が任意の $i \in \mathbb{N}$ について成り立つこととする。また B が**狭義単調減少列** (**狭義単調増加列**) であるとは減少列 (増加列) であって $a_i \neq a_{i+1}$ が任意の $i \in \mathbb{N}$ について成り立つこととする。

命題 4.2.16. 整列集合には無限の狭義単調減少列は存在しない。

証明. 整列集合 A に無限の狭義単調減少列 $B = [a_1, a_2, \cdots]$ が存在したとする。このとき A の部分集合 $C = \{a_1, a_2, \cdots\}$ を考える。A が整列集合だから C には最小元が存在する。$a \in C$ を C の最小元とする。$a \in C$ だから、ある $n \in \mathbb{N}$ があって $a = a_n$ である。しかし $a_{n+1} \preceq a_n = a$, $a_{n+1} \neq a$ となり、a が最小元であることに矛盾する。よって A に無限の狭義単調減少列は存在しない。 □

例 4.2.17 (辞書式順序)**.** $X = \mathbb{N} \times \mathbb{N}$ に次のように順序を定める。

(1) $a_0 = a_1$ ならば $b_0 \leq b_1$ のとき $(a_0, b_0) \leq (a_1, b_1)$ である。

(2) $a_0 \neq a_1$ のとき $a_0 \leq a_1$ ならば $(a_0, b_0) \leq (a_1, b_1)$ である。

この順序は整列順序である。これを**辞書式順序**という。

やや分かりにくいと思うので具体的に書くと以下のようになる。$(a_0, b_0) \leq (a_1, b_1)$ かつ $(a_0, b_0) \neq (a_1, b_1)$ であることを簡単のために $<$ とかく。

$$(1,1) < (1,2) < (1,3) < \cdots < (2,1) < (2,2) < (2,3) < \cdots < (3,1) < \cdots$$

辞書の語順と似ていることも分かるだろう。

これが整列順序であることを示そう。Y を X の空でない部分集合とする。

$$Y_1 = \{a \in \mathbb{N} \mid \text{ある } b \in \mathbb{N} \text{ があって } (a, b) \in Y\}$$

とおく。言い換えれば、写像 $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ を $f(a, b) = a$ で定めて $Y_1 = f(Y)$ としているのである。Y が空でないから Y_1 も空でない。Y_1 は $\mathbb{N}$ の部分集合で、$\mathbb{N}$ は整列集合なので Y_1 には最小元 a_1 が存在する。

$$Y_2 = \{b \in \mathbb{N} \mid (a_1, b) \in Y\}$$

とおく。言い換えれば、写像 $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ を $g(a, b) = b$ で定めて $Y_2 = g(f^{-1}(a_1))$ としているのである。a_1 の決め方から Y_2 は空でない $\mathbb{N}$ の部分集合で、したがって Y_2 は最小元 b_1 をもつ。このとき a_1, b_1 の決め方から (a_1, b_1) は Y の最小元である。

例 4.2.18. 例 4.2.17 で $\mathbb{N} \times \mathbb{N}$ に辞書式順序を定めたが、これは次のように一般化される。$(A, \leq), (B \leq)$ をそれぞれ整列順序とする。このとき例 4.2.17 と同様に $A \times B$ に順序を定めれば、これも整列順序となる。この順序も**辞書式順序**と呼ばれる。これによって $\mathbb{N}^n$ なども辞書式順序で整列集合と見ることができる。

定義 4.2.19 (帰納的順序)**.** 集合 A 上の順序 $\preceq$ が**帰納的順序**であるとは A の任意の空でない全順序部分集合が上に有界であることをいう。このとき A を**帰納的順序集合**という。

命題 4.2.20. 順序集合 A が最大元をもてば、A は帰納的順序集合である。

証明. 最大元は任意の部分集合の上界であるから、任意の部分集合は上に有界である。 □

例 4.2.21. $\mathbb{R}$ の開区間 $A = (0, 1)$ に自然な順序を考える。A は帰納的ではない。なぜならば A 自身は A の全順序部分集合であるがそれは上界をもたない。

4.3 数学的帰納法と超限帰納法

数学的帰納法の通常の形は以下の通りである。

自然数 n に関する命題は

(1) 1 のとき正しい。

(2) n より小さいすべての自然数に対して正しければ n についても正しい。

が成り立てば、任意の n に対しても正しい。(2) は

(2') $n-1$ に対して正しければ n についても正しい。

という形で考えられることもある。

これは整列集合に一般化される。すなわち A を整列集合とするとき $a \in A$ に関する命題は

(1) A の最小元に対して正しい。

(2) この順序に関して a より小さいすべて元に対して正しければ a についても正しい。

が成り立つとき、任意の a に対しても正しい。これは整列集合には無限の狭義単調減少列が存在しないことによる。すなわち $a \in A$ を決めると、狭義単調減少列は有限回で最小元に達する。したがって命題は有限回の手続きで証明されることになる。数学的帰納法を整列集合に一般化したものを**超限帰納法**という。

例 4.3.1. $\mathbb{N} \times \mathbb{N}$ に例 4.2.17 の整列順序を考える。二つの自然数の組 (a, b) に関する命題は

(1) $\mathbb{N} \times \mathbb{N}$ の最小元 $(a, b) = (1, 1)$ で正しい。

(2) $(a_0, b_0) < (a, b)$ である任意の (a_0, b_0) で正しければ (a, b) で正しい。

が成り立てば、任意の (a, b) で正しい。

考える順序集合が整列集合ではない場合、例えば通常の順序を考えた実数体 $\mathbb{R}$ など、では数学的帰納法や超限帰納法は使えない。以下の論法は正しくない。

例 4.3.2 (正しくない帰納法)**.** 非負の実数 a に関する命題は

(1) 0 で正しい。

(2) $a/2$ で正しいなら a で正しい。

となっていても正しいとは限らない。なぜならば無限の狭義単調減少列が存在するからである。

しかし、例えば以下の論法は正しい。

例 4.3.3. 非負の実数 a に関する命題は

(1) 区間 $[0, 1)$ で正しい。

(2) $a-1$ で正しければ a で正しい。

が成り立てば、任意の a に対して正しい。

4.4 同値関係と類別

定義 4.4.1 (同値関係)**.** 集合 A 上の関係 $\sim$ が**同値関係**であるとは、以下の条件を満たすこととする。

(1) [**反射律**] 任意の $x \in A$ に対して $x \sim x$

(2) [**対称律**] $x \sim y$ ならば $y \sim x$

(3) [**推移律**] $x \sim y,\ y \sim z$ ならば $x \sim z$

数学においては (数学以外でもそうであると思うが) 色々な意味で「同じである」という概念を用いる。例えば分数 $1/2$ と $3/6$ は同じ数であるが、明らかにその表記は異なる。他にも例えば合同な二つの三角形はある意味では「同じ」と言える。しかし、同じと言う概念をあまり勝手に使うと感覚的に理解しがたいことになる。同値関係は「同じ」という概念を数学的に定式化したものと考えられる。主張していることは

(1) 勝手な要素は自分自身と「同じ」である。

(2) x と y が「同じ」ならば y と x も「同じ」である。

(3) x と y が「同じ」で y と z が「同じ」ならば x と z は「同じ」である。

という当たり前のことである。これが成り立たない場合に「同じ」という言葉を使うのが感覚的に受け入れがたいということも理解できるだろう。

例 4.4.2. 例 4.1.3, $\mathbb{N} \times \mathbb{Z}$ 上の関係 $\sim$ は同値関係である。これを示そう。

$$\sim := \{((m,a),(n,b)) \in (\mathbb{N} \times \mathbb{Z}) \times (\mathbb{N} \times \mathbb{Z}) \mid mb = na\}$$

であった。

(1) 任意の $(m,a) \in \mathbb{N} \times \mathbb{Z}$ に対して $ma = ma$ は成立するので $(m,a) \sim (m,a)$ である。

(2) $(m,a) \sim (n,b)$ とすると $mb = na$ であるから $na = mb$ である。よって $(n,b) \sim (m,a)$ である。

(3) $(m,a) \sim (n,b),\ (n,b) \sim (\ell,c)$ とする。このとき $mb = na,\ nc = \ell b$ である。よって $mnc = m\ell b = \ell na$ である。ここで $n \in \mathbb{N}$ より $n \neq 0$ なので $mc = \ell a$ が成り立ち $(m,a) \sim (\ell,c)$ である。

以上より $\sim$ は同値関係である。

$\sim$ を集合 A 上の同値関係とする。$x \in A$ に対して

$$C_x := \{y \in A \mid x \sim y\}$$

とおいて、これを x を含む ($\sim$ に関する) **同値類**と呼ぶ。すなわち C_x は $\sim$ に関して x と「同じ」もの全体の集合である。このとき次が成り立つ。

定理 4.4.3. $\sim$ を集合 A 上の同値関係とし、C_x を $x \in A$ を含む同値類とする。このとき

(1) 任意の $x \in A$ に対して $x \in C_x$

(2) $x, y \in A$ に対して $y \in C_x$ ならば $C_x = C_y$

(3) $x, y \in A$ に対して $C_x \cap C_y \neq \phi$ ならば $C_x = C_y$

(4) $x, y \in A$ に対して $C_x \neq C_y$ ならば $C_x \cap C_y = \phi$

証明. (1) は反射律より明らか。

(2) $y \in C_x$ と仮定する。定義より $x \sim y$ である。また対称律より $y \sim x$ である。
$z \in C_x$ とする。このとき $x \sim z$ である。よって $y \sim x,\ x \sim z$ となり、推移律より $y \sim z$ であり $z \in C_y$ である。したがって $C_x \subset C_y$ である。
$z \in C_y$ とする。このとき $y \sim z$ である。$x \sim y,\ y \sim z$ であるから推移律により $x \sim z$ である。よって $z \in C_x$ であり $C_y \subset C_x$ が成り立つ。
以上より $C_x = C_y$ である。

(3) $C_x \cap C_y \neq \phi$ なので $z \in C_x \cap C_y$ とする。このとき $z \in C_x$ なので (2) より $C_x = C_z$ であり、同様に $z \in C_y$ より $C_y = C_z$ である。よって $C_x = C_y$ である。

(4) は (3) の対偶である。 □

定理 4.4.3 より A の異なる同値類の全体を $\{C_\lambda \mid \lambda \in \Lambda\}$ とおくと

$$A = \bigcup_{\lambda \in \Lambda} C_\lambda, \quad \lambda \neq \mu \text{ ならば } C_\lambda \cap C_\mu = \phi$$

となる。これを A の同値関係 $\sim$ による**類別**という。各同値類 C_λ から一つずつ元 a_λ を選ぶとき a_λ を C_λ の**代表元**という。また集合 $\{a_\lambda \mid \lambda \in \Lambda\}$ をこの類別の**完全代表系**という。

例 4.4.4. 例 4.1.3 の同値関係 $\sim$ は実はよく知られたものである。それは (m, a) を有理数 a/m に対応させると分かる。

$$a/m = b/n \Leftrightarrow mb = na \Leftrightarrow (m, a) \sim (n, b)$$

となっているのである。$m \in \mathbb{N}$ となっているので分母が 0 にならないことにも注意しておく。(m, a) を含む同値類は分数として $a/m = b/n$ となる (n, b) の全体である。すなわち

$$C_{(m,a)} = \{(n, b) \mid mb = na\} = \{(n, b) \mid a/m = b/n\}$$

である。有理数は既約分数として一意的に書けるので $C_{(m,a)}$ の代表元として、例えば a/m が既約分数であるものを取ることができる。ただし 0 の既約分数表示は $(1, 0)$ としておく。したがって既約分数の全体がこの同値関係による類別の完全代表系である。

注意. 一般に同値類の代表元の取り方は一意的ではない。この例では既約分数を代表元に取ったが、他の代表元をとっても構わず、その場合には完全代表系も違うものになる。

例 4.4.4 をもう少し考える。$(m,a) \sim (n,b)$ であるとき、有理数としては $a/m = b/n$ であるが $\mathbb{N}\times\mathbb{Z}$ では $(m,a) = (n,b)$ という訳ではない。写像 $f : \mathbb{N}\times\mathbb{Z} \to \mathbb{Q}$ $((m,a) \mapsto a/m)$ を定めることは出来るがこれは全単射ではない。同値類全体の集合 $\{C_{(m,a)} \mid (m,a) \in \mathbb{N}\times\mathbb{Z}\}$ を考えれば写像 $g : \{C_{(m,a)} \mid (m,a) \in \mathbb{N}\times\mathbb{Z}\} \to \mathbb{Q}$ $(C_{(m,a)} \mapsto a/m)$ は矛盾なく定義でき (well-defined) かつ全単射であることを示そう。

$C_{(m,a)} = C_{(n,b)}$ であるならば $(m,a) \sim (n,b)$ であるから $a/m = b/n$ である。したがって $g(C_{(m,a)}) = a/m$ は定まり、写像は矛盾なく定義できる。

任意の有理数 a/m $(a, m \in \mathbb{Z},\ m \neq 0)$ に対して、$m > 0$ ならば $(m,a) \in \mathbb{N}\times\mathbb{Z}$ で $g(C_{(m,a)}) = a/m$ である。また $m < 0$ ならば $(-m,-a) \in \mathbb{N}\times\mathbb{Z}$ で $g(C_{(-m,-a)}) = a/m$ である。よって g は全射である。

$g(C_{(m,a)}) = g(C_{(n,b)})$ とすると $a/m = b/n$ であるから $(m,a) \sim (n,b)$ であり $C_{(m,a)} = C_{(n,b)}$ が成り立つ。よって g は単射である。

以上より g は矛盾なく定義でき、かつ全単射であることが示された。

この例では $\mathbb{N}\times\mathbb{Z}$ 自身は $\mathbb{Q}$ との間に全単射がないが、その同値類の全体は $\mathbb{Q}$ との間に全単射がある。すなわち一つの同値類を一つのものと見ることが有効である。これは数学では多く見られる方法である。一般に集合 A の上に同値関係 $\sim$ が定義されているとき、その同値類全体の集合を $A/\sim$ と書き、**集合 A を同値関係 $\sim$ で割った集合**という。先の例では $(\mathbb{N}\times\mathbb{Z})/\sim$ と $\mathbb{Q}$ の間に全単射があったのである。

4.4.1 整数の合同

$n \in \mathbb{N}$ を一つ固定する。$a, b \in \mathbb{Z}$ に対して

$$a \equiv b \pmod{n} \iff \text{ある } \ell \in \mathbb{Z} \text{ があって } a - b = n\ell$$

という関係を定義する。この関係は同値関係である。

問 4.4.5. 上の関係が同値関係であることを示せ。

$a \in \mathbb{Z}$ に対して、この関係による a を含む同値類は $\{a + n\ell \mid \ell \in \mathbb{Z}\}$ と書くことができる。これを $a + n\mathbb{Z}$ と書き n を法とする a を含む**剰余類**という。特に $0 + n\mathbb{Z}$ は単に $n\mathbb{Z}$ と書かれる。任意の剰余類 $a + n\mathbb{Z}$ に対して、その代表元 b を $0 \leq b < n$ の範囲で取ることができることは明らかだろう。また $0 \leq a < b < n$ ならば $a + n\mathbb{Z} \neq b + n\mathbb{Z}$ であることも明らかである。したがって $\{n\mathbb{Z},\ 1 + n\mathbb{Z}, \cdots, (n-1) + n\mathbb{Z}\}$ が同値類のすべてである。この集合を $\mathbb{Z}/n\mathbb{Z}$ と書く。

$\mathbb{Z}/n\mathbb{Z}$ に二項演算 “+” を次のように定義しよう。

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) := (a + b) + n\mathbb{Z}$$

二項演算は写像 $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ であるから、これが矛盾なく定義されていることを示そう。$(a + b) + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ は問題ないが、演算が代表元の取り方に依存しないことを示す必要がある。すなわち $a + n\mathbb{Z} = a' + n\mathbb{Z}$, $b + n\mathbb{Z} = b' + n\mathbb{Z}$ であるときに $(a + b) + n\mathbb{Z} = (a' + b') + n\mathbb{Z}$ でなければならない。

$a+n\mathbb{Z}=a'+n\mathbb{Z}$, $b+n\mathbb{Z}=b'+n\mathbb{Z}$ と仮定する。これは、ある $\ell, m \in \mathbb{Z}$ があって $a-a'=n\ell$, $b-b'=nm$ と書けるということである。このとき

$$(a+b)-(a'+b')=(a-a')+(b-b')=n(\ell+m)$$

となるから $(a+b)+n\mathbb{Z}=(a'+b')+n\mathbb{Z}$ である。よって、この演算は矛盾なく定義できる。

問 4.4.6. (1) $\mathbb{Z}/n\mathbb{Z}$ に二項演算 "$-$" を $(a+n\mathbb{Z})-(b+n\mathbb{Z}):=(a-b)+n\mathbb{Z}$ で矛盾なく定義できることを示せ。

(2) $\mathbb{Z}/n\mathbb{Z}$ に二項演算 "$\times$" を $(a+n\mathbb{Z})\times(b+n\mathbb{Z}):=ab+n\mathbb{Z}$ で矛盾なく定義できることを示せ。

(3) 上で定義した $\mathbb{Z}/n\mathbb{Z}$ の加法と乗法は交換法則、結合法則を満たすことを示せ。また減法は一般には交換法則、結合法則を満たさないことを示せ。

4.5 演習問題

(1) $X=\{1,2,3,4\}$ とする。

(a) $\preceq=\{(1,1),(1,2),(1,3),(1,4),(2,2),(2,4),(3,3),(3,4),(4,4)\}$ は X 上の順序関係であることを確認せよ。この順序は全順序かどうかを判定せよ。また最大元、最小元、極大元、極小元をそれぞれ求めよ。

(b) $\preceq=\{(1,1),(1,2),(2,1),(2,2),(3,3),(3,4),(4,3),(4,4)\}$ は X 上の同値関係であることを確認せよ。またこの同値関係による類別を求めよ。

(2) $\mathbb{R}$ の元を成分に持つ n 次正方行列の全体を $M_n(\mathbb{R})$ と書く。$A,B\in M_n(\mathbb{R})$ に対して、関係 $A\sim B$ を「ある正則行列 P があって $B=P^{-1}AP$ となる」ということで定義する。このとき $\sim$ は同値関係であることを示せ。

(3) (2) の同値関係による同値類の集合 $M_n(\mathbb{R})/\sim$ を考える。$A\in M_n(\mathbb{R})$ を含む同値類を C_A と書くことにする。このとき $\det: M_n(\mathbb{R})/\sim \to \mathbb{R}$ $(\det(C_A)=\det A)$ が矛盾なく定義できることを説明せよ。ただし $\det A$ は A の行列式である。

(4) $f:\mathbb{Z}/n\mathbb{Z}\to\mathbb{Z}/m\mathbb{Z}$ を $f(a+n\mathbb{Z})=a+m\mathbb{Z}$ で定義したい。f が矛盾なく定義されるための必要十分条件を求めよ。

(5) $\mathbb{R}^2=\mathbb{R}\times\mathbb{R}=\{(a,b)\mid a,b\in\mathbb{R}\}$ を考え、$A=\mathbb{R}^2-\{(0,0)\}$ とする。A に

$$(a,b)\sim(c,d)\Leftrightarrow ad-bc=0$$

で関係 $\sim$ を定める。$\sim$ は同値関係であり、その同値類の完全代表系として座標平面上の単位円 (半径 1 の円) 上の点 (a,b) のうち $a>0$ であるもの、および $(a,b)=(0,1)$ からなる集合をとることができる。これを示せ。(この同値類全体の集合を $P^1(\mathbb{R})$ と書いて**射影空間**という。)

参考文献

[1] 入門 集合と位相, 竹之内修, 実教出版, 1971.

[2] 無限集合 (数学ワンポイント双書 4), 森殻, 共立出版, 1976.

Akihide Hanaki (hanaki@math.shinshu-u.ac.jp)
2004/10/24
2005/5/11 (誤りの訂正)
2005/10/26 (誤りの訂正)
2006/03/23
2006/08/21
2007/02/25 (加筆)