数の構成 自然数から複素数まで

MATHEMATICS.PDF

2011-07-08

目 次

1　自然数

1.1　自然数の定義

自然数は, Peano の公理を満たす集合の元として定義される. 自然数に 0 を含める流儀とそうでないものとあるが, この文書では 0 を自然数の出発点として構成していく.

集合 N が **Peano の公理を満たす**とは, N の元 0 と単射 $\sigma : N \to N$ が存在して, 次の 2 つの条件を満たすときにいう.

(N1) $0 \notin \sigma(N)$.
(N2) N の任意の部分集合 S に対して次のことが成り立つ：

$$0 \in S,\ \sigma(S) \subseteq S \Longrightarrow S = N.$$

条件 (N1), (N2) のことを **Peano の公理**という.

以下, この節 (§1.1) では, N は Peano の公理を満たす集合であるとする.

X を集合, x_0 を X の元, $\varphi : X \to X$ を写像とする. $N \times X$ の部分集合 A で次の条件 (a), (b) を満たすものを考える.

(a) $(0, x_0) \in A$.
(b) $(n, x) \in A \Longrightarrow (\sigma(n), \varphi(x)) \in A$.

また, このような A の全体を $\mathcal{A}$ とおく. さらに

$$B = \bigcap_{A \in \mathcal{A}} A$$

とおく.

[補題 1.1] B は $\mathcal{A}$ に属する集合のうち, 包含関係について最小のものである.

[証明] $B \in \mathcal{A}$ さえ示せれば, 最小性は B の定め方から明らかである.

条件 (a) より, すべての $A \in \mathcal{A}$ に対して $(0, x_0) \in A$ だから, $(0, x_0) \in B$ である. すなわち B は条件 (a) を満たす. また, 条件 (b) より

$$\begin{aligned}(n, x) \in B &\Longrightarrow \text{すべての } A \in \mathcal{A} \text{ に対して } (n, x) \in A \\ &\Longrightarrow \text{すべての } A \in \mathcal{A} \text{ に対して } (\sigma(n), \varphi(x)) \in A \\ &\Longrightarrow (\sigma(n), \varphi(x)) \in B.\end{aligned}$$

よって B は条件 (b) を満たす. したがって $B \in \mathcal{A}$ である. □

各 $n \in N$ に対して

$$X_n = \{x \in X \mid (n, x) \in B\}$$

とおく.

[補題 1.2] 任意の $n \in N$ に対して, X_n は 1 元集合である.

[証明] X_n が 1 元集合であるような $n \in N$ の全体からなる集合を S とおく. $S = N$ を証明することが目標である.

S は N の部分集合なので, $0 \in S$ かつ $\sigma(S) \subseteq S$ であることが示せれば, Peano の公理の条件 (N2) を適用して $S = N$ が得られる. 以下, $0 \in S$ かつ $\sigma(S) \subseteq S$ であることを示そう.

$0 \in S$ であること： $0 \in S$ とは, X_0 が 1 元集合であるということである. そこで, X_0 が 1 元集合でないと仮定して矛盾を導こう. そうすれば, 背理法によって X_0 が 1 元集合であることがいえる.

B は $\mathcal{A}$ の元 (補題 1.1) なので, 条件 (a) より $(0, x_0) \in B$. したがって $x_0 \in X_0$.

いま, X_0 が x_0 以外の元 y を含むと仮定する.

$(0, y) \in B$ なので, B の部分集合

$$B' = B \setminus \{(0, y)\}$$

を考えると, B' は B の真部分集合である.

B' がもし $\mathcal{A}$ の元だとすると, B が $\mathcal{A}$ に属する集合のうちで包含関係について最小のものであること (補題 1.1) に矛盾する. それこそが私たちの狙いである. そこで以下, B' が $\mathcal{A}$ の元であること, すなわち条件 (a), (b) を満たすことを示そう.

まず, $(0, x_0) \in B$ かつ $(0, x_0) \neq (0, y)$ より, $(0, x_0) \in B'$. よって B' は条件 (a) を満たす.

次に, $(n, x) \in B'$ とすると, $(n, x) \in B$ なので, 条件 (b) より $(\sigma(n), \varphi(x)) \in B$. 一方, Peano の公理の条件 (N1) より $0 \neq \sigma(n)$. ゆえに $(\sigma(n), \varphi(x)) \neq (0, y)$. したがって $(\sigma(n), \varphi(x)) \in B'$ となる. よって B' は条件 (b) も満たし, $B' \in \mathcal{A}$ が成り立つ.

ところが, B' は B の真部分集合であるから, $B' \in \mathcal{A}$ は B の最小性 (補題 1.1) に反する. よって X_0 が x_0 以外の元を含むことはない. すなわち X_0 は x_0 のみを元にもつ 1 元集合である. ゆえに $0 \in S$.

$\sigma(S) \subseteq S$ であること： 任意の $k \in S$ に対して $\sigma(k) \in S$ を示せばよいが, $\sigma(k) \in S$ は $X_{\sigma(k)}$ が 1 元集合であることを意味するから, 任意の $k \in S$ に対して $X_{\sigma(k)}$ が 1 元集合であることを示せばよいことになる.

$k \in S$ とすると, X_k は 1 元集合である. X_k のただ 1 つの元を u とおく. $(k, u) \in B \in \mathcal{A}$ なので条件 (b) より $(\sigma(k), \varphi(u)) \in B$. よって $\varphi(u) \in X_{\sigma(k)}$.

$X_{\sigma(k)}$ は少なくとも 1 つの元をもつわけだが, $0 \in S$ を示したときと同様に, $X_{\sigma(k)}$ が $\varphi(u)$ とは別の元をもつと仮定して矛盾を導こう. そうすれば $X_{\sigma(k)}$ が 1 元集合であることがいえる.

いま, $X_{\sigma(k)}$ が $\varphi(u)$ 以外の元 z を含むと仮定すると, $(\sigma(k), z) \in B$. そこで, B の真部分集合

$$B'' = B \setminus \{(\sigma(k), z)\}$$

を考える.

(N1) より $0 \notin \sigma(N)$ だから $(\sigma(k), z) \neq (0, x_0)$. よって $(0, x_0) \in B''$, すなわち B'' は条件 (a) を満たす.

次に, $(n,x) \in B''$ とすると, $(n,x) \in B \in \mathcal{A}$ なので条件 (b) より $(\sigma(n), \varphi(x)) \in B$. もし仮に $(\sigma(n), \varphi(x)) = (\sigma(k), z)$ ならば, $\sigma(n) = \sigma(k)$ であるが, σ が単射であることから $n = k$. よって $(k,x) = (n,x) \in B$. したがって $x \in X_k = \{u\}$. ゆえに $x = u$. よって $z = \varphi(x) = \varphi(u) \neq z$. これは矛盾であるから, $(\sigma(n), \varphi(x)) \neq (\sigma(k), z)$ でなければならない. したがって $(\sigma(n), \varphi(x)) \in B''$. よって B'' は条件 (b) も満たし, $B'' \in \mathcal{A}$ が成り立つ.

ところが B'' は B の真部分集合であるから, B の最小性 (補題 1.1) に反する. ゆえに $X_{\sigma(k)} = \{\varphi(u)\}$, したがって $\sigma(k) \in S$ である. k の取り方は任意なので, $\sigma(S) \subseteq S$.

以上で, $0 \in S$ かつ $\sigma(S) \subseteq S$ が証明された. S は N の部分集合だから, 条件 (N2) より, $S = N$ である. すなわち, 任意の $n \in N$ に対して集合 X_n はただ 1 つの元からなる. □

[定理 1.3] X を集合, x_0 を X の元, $\varphi : X \to X$ を写像とする. このとき, 次の 2 つの条件を満たすような写像 $f : N \to X$ がただ 1 つ存在する.

(i) $f(0) = x_0$.
(ii) $f \circ \sigma = \varphi \circ f$. すなわち, すべての $n \in N$ に対して $f(\sigma(n)) = \varphi(f(n))$.

[証明] 写像 f が存在すること：補題 1.2 より, 各 $n \in N$ に対して, X_n は 1 元集合である. $X_n = \{x_n\}$ とおき, $f(n) = x_n$ によって写像 $f : N \to X$ を定義する. $f(0) = x_0$ であることは f の定め方から明らかである. 次に,

$$\begin{aligned} x_n \in X_n &\Longrightarrow (n, x_n) \in B \\ &\Longrightarrow (\sigma(n), \varphi(x_n)) \in B \\ &\Longrightarrow \varphi(x_n) \in X_{\sigma(n)} = \{x_{\sigma(n)}\} \\ &\Longrightarrow \varphi(x_n) = x_{\sigma(n)}. \end{aligned}$$

よって

$$f(\sigma(n)) = x_{\sigma(n)} = \varphi(x_n) = \varphi(f(n)).$$

したがって f は定理の条件 (i), (ii) を満たす. これで写像 f の存在が示された.

写像 f が一意的であること：f の一意性をいうためには, 条件 (i), (ii) を満たす任意の 2 つの写像が等しいことをいえばよい.

そこで, 条件 (i), (ii) を満たすような 2 つの写像 $f : N \to X$, $f' : N \to X$ を任意にとる. 写像として $f = f'$ であるとは, 任意の $n \in N$ に対して $f(n) = f'(n)$ が成り立つことである.

$S = \{n \in N \mid f(n) = f'(n)\}$ とおく. 任意の $n \in N$ に対して $f(n) = f'(n)$ が成り立つことをいうためには, $S = N$ を示せばよい.

S は N の部分集合なので, $0 \in S$ かつ $\sigma(S) \subseteq S$ がいえれば, Peano の公理の条件 (N2) より $S = N$ が導かれる. 以下, $0 \in S$ かつ $\sigma(S) \subseteq S$ を示そう.

条件 (i) より $f(0) = x_0 = f'(0)$ だから $0 \in S$.

次に, $n \in S$, すなわち $f(n) = f'(n)$ とすると, 条件 (ii) より,

$$f(\sigma(n)) = \varphi(f(n)) = \varphi(f'(n)) = f'(\sigma(n)).$$

よって $\sigma(n) \in S$. したがって $\sigma(S) \subseteq S$.

S は N の部分集合だから, Peano の公理の条件 (N2) より $S = N$. ゆえに写像として $f = f'$ である. よって f は一意的である. □

[定理 1.4] 集合 N', その元 $0'$, 単射 $\sigma' : N' \to N'$ もまた Peano の公理を満たしているとする. このとき, 次の 2 つの条件を満たすような全単射 $f : N \to N'$ がただ 1 つ存在する.

(i) $f(0) = 0'$.

(ii) $f \circ \sigma = \sigma' \circ f$. すなわち, すべての $n \in N$ に対して $f(\sigma(n)) = \sigma'(f(n))$.

[証明] 写像 f の存在と一意性：定理 1.3 における X, x_0, φ としてそれぞれ N', $0'$, σ' をとると, 条件 (i), (ii) を満たす写像 $f : N \to N'$ がただ 1 つだけ得られる.

写像 f が全単射であること：f が全単射であることの必要十分条件は, ある写像 $f' : N' \to N$ が存在して, 合成写像 $f' \circ f$ が N の恒等写像になり, $f \circ f'$ が N' の恒等写像になることである.

N と N' の役割を交換し, 再び定理 1.3 を用いれば, 写像 $f' : N' \to N$ が存在して, $f(0') = 0$ かつ任意の $n' \in N'$ に対して $f'(\sigma'(n')) = \sigma(f'(n'))$ を満たす.

$g = f' \circ f$ とおくと, g は N から N 自身への写像である. そして, $g(0) = 0$ であり, 任意の $n \in N$ に対して

$$\begin{aligned} g(\sigma(n)) &= f' \circ f(\sigma(n)) = f'(\sigma'(f(n))) \\ &= \sigma(f' \circ f(n)) = \sigma(g(n)) \end{aligned}$$

が成り立つ. よって g は定理 1.3 の条件 (i), (ii) を満たす. 定理 1.3 の一意性によって, g は N の恒等写像に一致する.

同様にして, $f \circ f'$ が N' の恒等写像に一致することもいえる. したがって, 写像 $f : N \to N'$ は全単射である. □

上の定理により, Peano の公理を満たす集合 N は, 存在すれば本質的にはただ 1 つであることがわかる. Peano の公理を満たす集合 N を $\mathbb{N}$ で表す. そして, $\mathbb{N}$ の元を**自然数**という.

1.2 自然数の加法

[補題 1.5] 各 $n \in \mathbb{N}$ に対して, 写像 $\sigma_n : \mathbb{N} \to \mathbb{N}$ が一意的に存在して, 次の 2 つの条件を満たす.

(i) $\sigma_n(0) = n$,

(ii) $\sigma_n \circ \sigma = \sigma \circ \sigma_n$.

[証明] 定理 1.3 における X, x_0, φ としてそれぞれ $\mathbb{N}$, n, σ をとり, 定理 1.3 を適用すれば, f として σ_n が得られる. □

$m, n \in \mathbb{N}$ に対し, $\sigma_n(m)$ を m, n の**和**とよび, $m + n$ で表す. また, $\sigma(0)$ を 1 と書く.

[補題 1.6] (i) $\sigma_0 = \mathrm{id}_{\mathbb{N}}$. ただし $\mathrm{id}_{\mathbb{N}}$ は $\mathbb{N}$ の恒等写像.

(ii) $\sigma_1 = \sigma$.

(iii) 任意の $n \in \mathbb{N}$ に対して, $\sigma_{\sigma(n)} = \sigma \circ \sigma_n$.

[証明] (i) $\mathrm{id}_{\mathbb{N}}(0) = 0$, $\mathrm{id}_{\mathbb{N}} \circ \sigma = \sigma \circ \mathrm{id}_{\mathbb{N}}$ であるから, 定理 1.3 の一意性より $\mathrm{id}_{\mathbb{N}} = \sigma_0$.

(ii) $\sigma(0) = 1$, $\sigma \circ \sigma = \sigma \circ \sigma$ はともに自明である. 定理 1.3 の一意性より $\sigma = \sigma_1$.

(iii) $n \in \mathbb{N}$ とする. 補題 1.5 より,

$$\sigma \circ \sigma_n(0) = \sigma(n),$$
$$(\sigma \circ \sigma_n) \circ \sigma = \sigma \circ (\sigma_n \circ \sigma) = \sigma \circ (\sigma \circ \sigma_n).$$

定理 1.3 の一意性より $\sigma \circ \sigma_n = \sigma_{\sigma(n)}$. □

[補題 1.7] 任意の $n \in \mathbb{N}$ に対して $\sigma(n) = n + 1$ が成り立つ.

[証明] 補題 1.6 (ii) と和の定義より $\sigma(n) = \sigma_1(n) = n + 1$. □

[補題 1.8] N の部分集合 S が

(i) $0 \in S$,

(ii) $n \in S \Longrightarrow n + 1 \in S$

を満たすとする. このとき, $S = \mathbb{N}$ である.

[証明] S が条件 (i), (ii) を満たすと仮定する. $n \in S$ とすると, 補題 1.7 と上の条件 (ii) より $\sigma(n) = n + 1 \in S$. したがって $\sigma(S) \subseteq S$. ゆえに, Peano の公理の条件 (N2) によって $S = \mathbb{N}$ が得られる. □

[定理 1.9] 各 $n \in \mathbb{N}$ に対して命題 $P(n)$ が与えられ, 次のことが成り立つとする.

(i) $P(0)$ は正しい.

(ii) $P(n)$ が正しいならば $P(n + 1)$ も正しい.

このとき $P(n)$ はすべての $n \in \mathbb{N}$ に対して正しい. この定理を利用した証明の方法を**数学的帰納法**という.

[証明] 条件 (i), (ii) が成り立つと仮定する.

$S = \{n \in \mathbb{N} \mid P(n)\}$ とおく. 条件 (i) より $P(0)$ は正しいから $0 \in S$. また, 条件 (ii) より

$$\begin{aligned} n \in S &\Longrightarrow P(n) \\ &\Longrightarrow P(n+1) \\ &\Longrightarrow n+1 \in S. \end{aligned}$$

したがって, S は補題 1.8 の条件 (i), (ii) を満たす. よって $S = \mathbb{N}$ となる. ゆえに, すべての $n \in \mathbb{N}$ に対して $P(n)$ が成り立つ. □

[定理 1.10] 任意の $m, n \in \mathbb{N}$ に対して次のことが成り立つ.

(i) $0 + n = n + 0 = n$.

(ii) $(m+1) + n = m + (n+1) = (m+n) + 1$.

[証明] (i) 和の定義より $0 + n = \sigma_n(0)$. 補題 1.5 (i) より $\sigma_n(0) = n$. さらに, 和の定義と補題 1.6 (i) より

$$n + 0 = \sigma_0(n) = \mathrm{id}_{\mathbb{N}}(n) = n.$$

ゆえに, $0 + n = n + 0 = n$.

(ii) 和の定義, 補題 1.5, 補題 1.6, 補題 1.7 を次々に適用する.

$$\begin{aligned} (m+1) + n &= \sigma(m) + n = \sigma_n(\sigma(m)) = \sigma(\sigma_n(m)), \\ m + (n+1) &= m + \sigma(n) = \sigma_{\sigma(n)}(m) = \sigma(\sigma_n(m)), \\ (m+n) + 1 &= \sigma_n(m) + 1 = \sigma(\sigma_n(m)). \end{aligned}$$

ゆえに, $(m+1) + n = m + (n+1) = (m+n) + 1$. □

[定理 1.11] 任意の $m, n \in \mathbb{N}$ に対して

$$m + n = n + m$$

が成り立つ. この等式を $\mathbb{N}$ の加法に関する**交換法則**という.

[証明] n は任意の自然数をとって固定する. m に関する数学的帰納法により証明する.

まず, 定理 1.10 (i) より

$$0 + n = n + 0$$

であるから, $m = 0$ のとき主張は正しい.

次に, m のとき主張が正しいと仮定すると,

$$m + n = n + m.$$

$m + 1$ のときを考えると,

$$\begin{aligned}(m + 1) + n &= (m + n) + 1 \\ &= (n + m) + 1 \\ &= n + (m + 1).\end{aligned}$$

よって, $m + 1$ のときも正しい.

したがって, すべての $m \in \mathbb{N}$ に対して主張は正しい. □

[定理 1.12] 任意の k, m, $n \in \mathbb{N}$ に対して

$$(k + m) + n = k + (m + n)$$

が成り立つ. この等式を $\mathbb{N}$ の加法に関する**結合法則**という.

[証明] m, n は任意の自然数をとって固定する. k に関する数学的帰納法により証明する.

まず, 定理 1.10 (i) より

$$(0 + m) + n = m + n = 0 + (m + n)$$

であるから, $k = 0$ のとき主張は正しい.

次に, k のとき主張が正しいと仮定すると,

$$(k + m) + n = k + (m + n).$$

$k + 1$ のときを考えると, k のときの仮定と定理 1.10 (ii) を適用して

$$\begin{aligned}((k + 1) + m) + n &= ((k + m) + 1) + n \\ &= ((k + m) + n) + 1 \\ &= (k + (m + n)) + 1 \\ &= (k + 1) + (m + n).\end{aligned}$$

よって, $k + 1$ のときも正しい.

したがって, すべての $k \in \mathbb{N}$ に対して主張は正しい. □

[定理 1.13] 任意の k, m, $n \in \mathbb{N}$ に対して

$$m + k = n + k \Longrightarrow m = n$$

が成り立つ. これを $\mathbb{N}$ の加法に関する**簡約法則**という.

[証明] 主張は, 任意の k, m, $n \in \mathbb{N}$ に対して

$$\sigma_k(m) = \sigma_k(n) \Longrightarrow m = n$$

であることと言い換えることができる (和の定義). このことはまさに任意の $k \in \mathbb{N}$ に対して $\sigma_k : \mathbb{N} \to \mathbb{N}$ が単射であるということにほかならない. 以下, そのことを k に関する数学的帰納法で示す.

$k = 0$ のとき, 補題 1.6 (i) より $\sigma_0 = \mathrm{id}_{\mathbb{N}}$ なので, σ_0 は単射である.

次に, 一般の k について, σ_k が単射であると仮定する. $\sigma(k) = k + 1$ なので, 補題 1.6 (iii) より $\sigma_{k+1} = \sigma \circ \sigma_k$ である. σ は単射であり, 2 つの単射の合成もまた単射であるから, σ_{k+1} も単射である.

したがって, すべての $k \in \mathbb{N}$ に対して σ_k は単射である. □

自然数の和に関する基本的な性質 (定理 1.10, 定理 1.11, 定理 1.12, 定理 1.13) は, 以後, 断りなしに使う.

1.3 自然数の順序

2 つの自然数 m, n に対して, 関係 $\leq$ を次のように定義する.

$$n \leq m \iff \text{ある } k \in \mathbb{N} \text{ が存在して } m = n + k.$$

$n \leq m$ のことを $m \geq n$ と書くこともある.

[定理 1.14] 任意の自然数 $m \in \mathbb{N}$ に対して, $m \leq m$ が成り立つ.

[証明] $m = m + 0$ より明らかである. □

[定理 1.15] 任意の自然数 k, m, $n \in \mathbb{N}$ に対して, $n \leq m$ かつ $m \leq k$ ならば, $n \leq k$ が成り立つ.

[証明] $n \leq m$ かつ $m \leq k$ とすると, ある l, $l' \in \mathbb{N}$ が存在して

$$m = n + l, \quad k = m + l'$$

となる. 1 番目の式を 2 番目に代入すると,

$$k = (n + l) + l' = n + (l + l').$$

よって $n \leq k$ である. □

[補題 1.16] $\sigma(\mathbb{N}) = \mathbb{N} \setminus \{0\}$.

[証明] $S = \{0\} \cup \sigma(\mathbb{N})$ とおく. Peano の公理の条件 (N1) より $0 \notin \sigma(\mathbb{N})$ だから, $\sigma(\mathbb{N}) = S \setminus \{0\}$ が成り立つ.

S の定め方から $0 \in S$. また, 補題 1.7 より

$$m \in S \Longrightarrow m + 1 = \sigma(m) \in \sigma(\mathbb{N}) \subseteq S.$$

ゆえに補題 1.8 より $S = \mathbb{N}$. したがって $\sigma(\mathbb{N}) = \mathbb{N} \setminus \{0\}$. □

[補題 1.17] 自然数 n について, $n \neq 0$ であることと, ある自然数 k が存在して $n = k + 1$ が成り立つこととは同値である.

[証明] 補題 1.7, 補題 1.16 より,

$$\begin{aligned} n \neq 0 &\Longleftrightarrow n \in \mathbb{N} \setminus \{0\} \\ &\Longleftrightarrow n \in \sigma(\mathbb{N}) \\ &\Longleftrightarrow \text{ある } k \in \mathbb{N} \text{ が存在して } n = \sigma(k) \\ &\Longleftrightarrow \text{ある } k \in \mathbb{N} \text{ が存在して } n = k + 1. \end{aligned}$$

□

[補題 1.18] 任意の自然数 n, k について, 次のことが成り立つ.

(i) $n + k = n \Longrightarrow k = 0$.

(ii) $n + k = 0 \Longrightarrow n = k = 0$.

[証明] (i)　加法に関する簡約法則により,

$$n + k = n \Longrightarrow n + k = n + 0 \Longrightarrow k = 0.$$

(ii)　補題 1.17 より, $n \neq 0$ のとき, ある $l \in \mathbb{N}$ が存在して $n = l + 1$. 再び補題 1.17 を用いると,

$$n + k = (l + 1) + k = (l + k) + 1 \neq 0.$$

よって

$$n \neq 0 \Longrightarrow n + k \neq 0$$

が成り立ち, その対偶

$$n + k = 0 \Longrightarrow n = 0$$

も成り立つ.

$n+k=0$ を仮定したとき, $n=0$ が成り立つから,

$$k=0+k=n+k=0$$

となる. □

[定理 1.19] 任意の自然数 $m, n \in \mathbb{N}$ に対して, $n \leq m$ かつ $m \leq n$ ならば, $m=n$ が成り立つ.

[証明] $n \leq m$ かつ $m \leq n$ とすると, ある $l, l' \in \mathbb{N}$ が存在して

$$m=n+l, \quad n=m+l'$$

となる. 1 番目の式を 2 番目に代入すると,

$$n=(n+l)+l'=n+(l+l').$$

加法に関する簡約法則より, $0=l+l'$. 補題 1.18 (ii) より $l=l'=0$. したがって $m=n$ が得られる. □

以上より, $\leq$ が実際に $\mathbb{N}$ 上の順序関係であること, すなわち反射法則 (定理 1.14), 推移法則 (定理 1.15), 対称法則 (定理 1.19) が成り立つことが示された.

2 つの自然数 m, n について, $n \leq m$ かつ $m \neq n$ であることを $n<m$ や $m>n$ で表す. このとき, m は n より**大きい**といい, n は m より**小さい**という.

[定理 1.20] 任意の自然数 $m, n \in \mathbb{N}$ に対して,

$$n<m \iff \text{ある } k \in \mathbb{N},\ k \neq 0 \text{ が存在して } m=n+k.$$

[証明] $n<m$ とすると, $n \leq m$ なので, ある $k \in \mathbb{N}$ が存在して $m=n+k$. もし $k=0$ ならば $m=n$ となり $n<m$ に反する. よって $k \neq 0$.

逆に, ある $k \in \mathbb{N}$ が存在して $m=n+k$ が成り立てば $n \leq m$. もし $m=n$ ならば $n=n+k$ なので, $k=0$ が得られる. したがって, $k \neq 0$ ならば $x \neq y$. ゆえに $x<y$ である. □

[定理 1.21] 任意の自然数 $k, m, n \in \mathbb{N}$ に対して, $n<m$ かつ $m<k$ ならば, $n<k$ が成り立つ.

[証明] $n<m$ かつ $m<k$ とすると, 定理 1.20 より, ある $l, l' \in \mathbb{N}$, $l \neq 0$, $l' \neq 0$ が存在して

$$m=n+l, \quad k=m+l'$$

となる. 1 番目の式を 2 番目に代入すると,

$$k=(n+l)+l'=n+(l+l').$$

$l \neq 0$, $l' \neq 0$ だから, 補題 1.18 (ii) より $l+l' \neq 0$. よって, 定理 1.20 より $n<k$ となる. □

[定理 1.22] 任意の自然数 k, m, $n \in \mathbb{N}$ に対して,

$$n < m \Longrightarrow n + k < m + k.$$

[証明] $n < m$ とすると, 定理 1.20 より, ある $l \in \mathbb{N}$, $l \neq 0$ が存在して $m = n + l$. このとき, $m + k = (n + l) + k = (n + k) + l$. よって, 定理 1.20 より $n + k < m + k$ となる. □

[定理 1.23] 任意の自然数 m, $n \in \mathbb{N}$ に対して,

(i) $n < m \Longrightarrow n + 1 \leq m$.
(ii) $n < m + 1 \Longrightarrow n \leq m$.

[証明] (i) $n < m$ とすると, 定理 1.20 より, ある $k \in \mathbb{N}$, $k \neq 0$ が存在して $m = n + k$ が成り立つ. 補題 1.17 より, ある $l \in \mathbb{N}$ が存在して $k = l + 1$. よって $m = n + (l + 1) = (n + 1) + l$. したがって $n + 1 \leq m$.

(ii) $n < m + 1$ とすると, 定理 1.20 より, ある $k \in \mathbb{N}$, $k \neq 0$ が存在して $m + 1 = n + k$ が成り立つ. 補題 1.17 より, ある $l \in \mathbb{N}$ が存在して $k = l + 1$. よって $m + 1 = n + (l + 1) = (n + l) + 1$. $\mathbb{N}$ の加法に関する簡約法則を用いれば, $m = n + l$ が得られる. よって $n \leq m$. □

[定理 1.24] 任意の m, $n \in \mathbb{N}$ に対して, $n < m$, $m = n$, $m < n$ のいずれか 1 つ, しかも 1 つだけが成り立つ.

[証明] 3 つの場合のうちどの 2 つも同時に成り立たないこと：$n < m$ と $m = n$ の両方が同時に成り立たないこと, $m < n$ と $m = n$ の両方が同時に成り立たないことは $m > n$ や $m < n$ の定義から明らかである. また, 仮に $m < n$ と $n < m$ が両方とも成り立つとすると, $m \leq n$ かつ $n \leq m$ だから $m = n$ となり, $m < n$ と $m = n$ が同時に成り立つことになって矛盾が生じる. したがって 3 つの場合のうちどの 2 つも同時に成り立つことはない.

3 つの場合のどれかが成り立つこと：$m \in \mathbb{N}$ を任意にとって固定する. $n < m$, $m = n$, $m < n$ のいずれかが成り立つことを n に関する数学的帰納法で証明する.

$m = 0 + m$ であるから, $0 \leq m$. よって $n = 0$ のときは正しい.

次に, n のとき $n < m$, $m = n$, $m < n$ のいずれかが成り立つと仮定し, $n + 1$ のときも正しいこと, すなわち $n + 1 < m$, $m = n + 1$, $m < n + 1$ のいずれかが成り立つことを示す.

$n < m$ のとき, 定理 1.23 (i) より $n + 1 \leq m$.

$m = n$ のとき, $n + 1 = m + 1$. よって $m < n + 1$.

$m < n$ のとき, $n < n + 1$ と定理 1.21 から $m < n + 1$ が得られる[1)].

[1)] $n < n + 1$ は, $n + 1 = n + 1$ という自明な式と定理 1.20 からわかる.

以上で $n+1<m$, $m=n+1$, $m<n+1$ のいずれかが成り立つことが示された. よって $n+1$ のときも正しい.

ゆえに n に関する数学的帰納法によって, 任意の $n \in \mathbb{N}$ に対して $n<m$, $m=n$, $m<n$ のいずれかが成り立つことが示された.

さらに, m の取り方は任意だったから, 任意の m, $n \in \mathbb{N}$ に対して $n<m$, $m=n$, $m<n$ のいずれかが成り立つ. □

[定理 1.25] $\mathbb{N}$ の任意の空でない部分集合 S は最小元をもつ[2)]. この性質を $\mathbb{N}$ の**整列性**という.

[証明] S を $\mathbb{N}$ の空でない部分集合とする.

$$T = \{n \in \mathbb{N} \mid \text{任意の } x \in S \text{ に対して } n \leq x\}$$

とおく.

まず, $0 \in T$ である. なぜなら, 任意の $k \in \mathbb{N}$ に対して, $k = 0+k$ すなわち $0 \leq k$ となるからである. 次に, S が空でないことから, ある $x \in S$ が存在する. $x < x+1$ より, $x+1 \notin T$. よって $T \neq \mathbb{N}$. ゆえに補題 1.8 より, $m \in T$ かつ $m+1 \notin T$ となる自然数 m が存在する.

もし仮に $m \notin S$ とすると, 任意の $x \in S$ に対して $m < x$ である. よって定理 1.23 より $m+1 \leq x$. ゆえに $m+1 \in T$ となり, 矛盾が生じる. したがって $m \in S$ であり, m は S の最小元である. □

[補題 1.26] $\mathbb{N}$ の部分集合 S が, 2 つの条件

(i) $0 \in S$.

(ii) $n \in \mathbb{N}$ とするとき, $k \leq n$ であるすべての $k \in \mathbb{N}$ について $k \in S$ ならば, $n+1 \in S$.

を満たすと仮定する. このとき, $S = \mathbb{N}$ となる.

[証明] $T = \{x \in \mathbb{N} \mid x \notin S\}$ とおく. $T = \emptyset$ を示せばよい.

背理法を用いる. もし仮に $T \neq \emptyset$ とすると, 整列性 (定理 1.25) によって T は最小元 n_0 をもつ. 仮定 (i) によって $0 \notin T$, よって $n_0 \neq 0$. 補題 1.17 より, ある $n_1 \in \mathbb{N}$ が存在して $n_0 = n_1 + 1$ である. 定理 1.20 より $n_1 < n_0$ だから, n_0 の最小性によって, $k \leq n_1$ なるすべての $k \in \mathbb{N}$ について $k \notin T$, すなわち $k \in S$ でなければならない. 仮定 (ii) によって $n_0 = n_1 + 1 \in S$. これは $n_0 \in T$ に反する. □

[定理 1.27] 各 $n \in \mathbb{N}$ に対して命題 $P(n)$ が与えられたとし，それについて次の 2 つのことが示されたとする.

[2)] 順序関係が定まった集合 X において, X の元 a が X の**最小元**であるとは, 任意の $x \in X$ に対して $a \leq x$ が成り立つときにいう.

(i) $P(0)$ が成り立つ.

(ii) $n \in \mathbb{N}$ とするとき, $0 \leq k \leq n$ であるすべての $k \in \mathbb{N}$ について $P(n)$ が成り立つならば, $P(n+1)$ が成り立つ.

このとき, すべての $n \in \mathbb{N}$ に対して $P(n)$ が成り立つ. この定理を利用した証明の方法も**数学的帰納法**と呼ばれる.

[証明] $S = \{n \in \mathbb{N} \mid P(n)\}$ とおく.

条件 (i) より, $0 \in S$. 条件 (ii) より, $n \in \mathbb{N}$ とするとき,

$$\begin{aligned} &0 \leq k \leq n\text{であるすべての } k \in \mathbb{N} \text{ について } k \in S \\ &\qquad \Longrightarrow 0 \leq k \leq n \text{ であるすべての } k \in \mathbb{N} \text{ について } P(k) \\ &\qquad \Longrightarrow P(k+1) \\ &\qquad \Longrightarrow n+1 \in S. \end{aligned}$$

したがって, 補題 1.26 より, $S = \mathbb{N}$. ゆえに, すべての $n \in \mathbb{N}$ に対して命題 $P(n)$ が成り立つ. □

1.4 自然数の乗法

[補題 1.28] 各 $n \in \mathbb{N}$ に対して, 写像 $\pi_n : \mathbb{N} \to \mathbb{N}$ が一意的に存在して, 次の 2 つの条件を満たす.

(i) $\pi_n(0) = 0$,

(ii) $\pi_n \circ \sigma = \sigma_n \circ \pi_n$.

[証明] 定理 1.3 における X, x_0, φ としてそれぞれ $\mathbb{N}$, 0, σ_m をとり, 定理 1.3 を適用すれば, f として π_n が得られる. □

$m, n \in \mathbb{N}$ に対し, $\pi_n(m)$ を m, n の**積**とよび, mn もしくは $m \cdot n$ で表す.

[定理 1.29] 任意の $m, n \in \mathbb{N}$ に対して, 次が成り立つ.

(i) $0 \cdot n = 0$.

(ii) $n \cdot 0 = 0$.

(iii) $1 \cdot n = n$.

(iv) $n \cdot 1 = n$.

(v) $(m+1)n = mn + n$.

(vi) $m(n+1) = mn + m$.

[証明] (i)　補題 1.28 (i) より, $0 \cdot n = 0$.

(ii)　補題 1.28 (i) より $\pi_0(0) = 0$. 次に, $\pi_0(n) = 0$ ならば, 補題 1.28 (ii) より

$$\begin{aligned}\pi_0(n+1) &= \pi_0 \circ \sigma(n) = \sigma_0 \circ \pi_0(n) \\ &= \mathrm{id}_{\mathbb{N}} \circ \pi_0(n) = \pi_0(n) = 0.\end{aligned}$$

ここで, $\mathrm{id}_{\mathbb{N}}$ は $\mathbb{N}$ 上の恒等写像である. n に関する数学的帰納法により, すべての $n \in \mathbb{N}$ に対して $\pi_0(n) = 0$, すなわち $n \cdot 0 = 0$.

(iii)　補題 1.28 (i), (ii) より

$$\begin{aligned}1 \cdot n = \pi_n(1) &= \pi_n \circ \sigma(0) \\ &= \sigma_n \circ \pi_n(0) = \sigma_n(0) = n.\end{aligned}$$

(iv)　補題 1.28 (i) より $0 \cdot 1 = \pi_1(0) = 0$. 次に, $n \cdot 1 = n$ ならば, 補題 1.28 (ii) より

$$\begin{aligned}(n+1) \cdot 1 = \pi_1(n+1) &= \pi_1 \circ \sigma_1(n) \\ &= \sigma \circ \pi_1(n) = \sigma_n(n \cdot 1) = \sigma(n) = n+1.\end{aligned}$$

n に関する数学的帰納法により, すべての $n \in \mathbb{N}$ に対して $n \cdot 1 = n$.

(v)　補題 1.28 (ii) より

$$\begin{aligned}(m+1)n = \pi_n(m+1) &= \pi_n \circ \sigma(m) \\ &= \sigma_n \circ \pi_n(m) = \sigma_n(mn) = mn + n.\end{aligned}$$

(vi)　$\tau_n(m) = mn + m$ とおく. (i) の結果を用いると

$$\tau_n(0) = 0 \cdot n + 0 = 0 + 0 = 0.$$

次に, $\mathbb{N}$ の加法に関する結合法則, 交換法則と (v) の結果を用いると

$$\begin{aligned}\sigma_{n+1} \circ \tau_n(m) = \sigma_{n+1}(mn+m) &= (mn+m) + (n+1) \\ &= (mn+n) + (m+1) = (m+1)n + (m+1) \\ &= \tau_n(m+1) = \tau_n \circ \sigma(m).\end{aligned}$$

よって補題 1.28 の一意性により, $\pi_{n+1} = \tau_n$. したがって $m(n+1) = mn + m$ が得られる.　□

[定理 1.30] 任意の $m, n \in \mathbb{N}$ に対して

$$mn = nm$$

が成り立つ. この等式を $\mathbb{N}$ の乗法に関する**交換法則**という.

[証明] n は任意の自然数をとって固定する. m に関する数学的帰納法により証明する.

まず, 定理 1.29 (i), (ii) より

$$0 \cdot n = 0, \quad n \cdot 0 = 0$$

であるから, $0 \cdot n = n \cdot 0$. よって $m = 0$ のとき主張は正しい.

次に, m のとき主張が正しいと仮定すると, 定理 1.29 (v), (vi) より

$$(m+1)n = mn + n = nm + n = n(m+1).$$

よって $m+1$ のときも正しい.

したがって, すべての $m \in \mathbb{N}$ に対して主張は正しい. □

[定理 1.31] 任意の k, m, $n \in \mathbb{N}$ に対して

$$m(n+k) = mn + mk, \quad (n+k)m = nm + km$$

が成り立つ. これらの等式を $\mathbb{N}$ の加法と乗法に関する**分配法則**という.

[証明] 乗法に関する交換法則により, 一方の式から他方が導かれるから, 最初の式について証明すれば十分である.

m, n は任意の自然数をとって固定する. k に関する数学的帰納法により証明する.

まず,

$$m(n+0) = mn = mn + 0 = mn + m \cdot 0$$

であるから, $k = 0$ のとき主張は正しい.

次に, k のとき主張が正しいと仮定すると,

$$\begin{aligned} m(n+(k+1)) &= m((n+k)+1) = m(n+k) + m \\ &= (mn + mk) + m = mn + (mk + m) \\ &= mn + m(k+1). \end{aligned}$$

よって $k+1$ のときも正しい.

したがって, すべての $k \in \mathbb{N}$ に対して主張は正しい. □

[定理 1.32] 任意の k, m, $n \in \mathbb{N}$ に対して

$$(mn)k = m(nk)$$

が成り立つ. この等式を $\mathbb{N}$ の乗法に関する**結合法則**という.

[証明] m, n は任意の自然数をとって固定する. k に関する数学的帰納法により証明する.

まず,

$$(mn)\cdot 0 = 0, \quad m(n\cdot 0) = m\cdot 0 = 0$$

であるから $(mn)\cdot 0 = m(n\cdot 0)$. よって $k = 0$ のとき主張は正しい.

次に, k のとき主張が正しいと仮定する. 分配法則を用いると,

$$\begin{aligned} m(n(k+1)) &= m(nk+n) = m(nk) + mn \\ &= (mn)k + mn = (mn)(k+1). \end{aligned}$$

よって $k+1$ のときも正しい.

したがって, すべての $k \in \mathbb{N}$ に対して主張は正しい. □

[定理 1.33] 任意の自然数 m, n に対して, $m \neq 0$ かつ $n \neq 0$ ならば, $mn \neq 0$.

[証明] $m \neq 0$, $n \neq 0$ とすると, ある k, $l \in \mathbb{N}$ が存在して $m = k+1$, $n = l+1$ となり,

$$mn = (k+1)(l+1) = (kl + k + l) + 1.$$

よって $mn \neq 0$. □

[定理 1.34] 任意の k, m, $n \in \mathbb{N}$ に対して, $k \neq 0$ ならば

$$n < m \Longrightarrow nk < mk.$$

[証明] $n < m$ とすると, ある $l \in \mathbb{N}$, $l \neq 0$ が存在して $m = n + l$. このとき,

$$mk = (n+l)k = nk + lk.$$

$l \neq 0$, $k \neq 0$ なので, 定理 1.33 より $lk \neq 0$. よって $nk < mk$. □

[定理 1.35] 任意の k, m, $n \in \mathbb{N}$ に対して, $k \neq 0$ ならば

$$mk = nk \Longrightarrow m = n$$

が成り立つ. これを $\mathbb{N}$ の乗法に関する**簡約法則**という.

[証明] 対偶を示す. $m \neq n$ ならば, $n < m$ または $m < n$. また, $k \neq 0$ だから, 定理 1.34 より

$$n < m \Longrightarrow nk < mk,$$
$$m < n \Longrightarrow mk < nk.$$

よって, $nk \neq mk$. □

2　整数

2.1　半群から生成される群

$\mathbb{N}$ から $\mathbb{Z}$ を構成するにあたって, より一般的に, 半群から群を構成する方法について述べる.

空でない集合 S が**簡約的可換半群**であるとは, 演算

$$S \times S \to S, \quad (x, y) \mapsto x + y$$

が定義されていて, 次の条件が成り立つときにいう.

(i) **結合法則**: 任意の x, y, $z \in S$ に対して $(x + y) + z = x + (y + z)$.

(ii) **交換法則**: 任意の x, $y \in S$ に対して $x + y = y + x$.

(iii) **簡約法則**: 任意の x, y, $z \in S$ に対して, $x + z = y + z$ ならば $x = y$.

結合法則 (i) を満たす演算をもつ集合が半群であり, その演算が交換法則 (ii) を満たすものが可換半群で, さらに簡約法則 (iii) も満たせば簡約的可換半群である.

S, T を簡約的可換半群とするとき, 写像 $f : S \to T$ が**準同型**であるとは, 任意の x, $y \in S$ に対して

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

が成り立つことをいう. ここで, 左辺の $+$ は S における演算であり, 右辺の $+$ は T における演算であることに注意せよ.

2 つの簡約的可換半群 S, T の間に単射準同型 $f : S \to T$ が存在するとき, S は T の**部分半群**であるという. さらに, f が全単射な準同型であるとき, S と T は**同型**であるといい, $S \simeq T$ で表す.

以後, この節では, S は簡約的可換半群を表すものとする.

[命題 2.1] 加法群は簡約的可換半群である[3].

[証明] M を加法群とし, その演算を $+$, 零元を 0 と書く[4]. 簡約的可換半群の定義の条件 (i), (ii) が成り立つことは, M が加法群であることから明らかである.

x, y, $z \in M$ を任意にとると, z の逆元 $-z$ が存在して,

$$\begin{aligned} x + z = y + z &\Longrightarrow (x + z) - z = (y + z) - z \\ &\Longrightarrow x + (z - z) = y + (z - z) \\ &\Longrightarrow x + 0 = y + 0 \\ &\Longrightarrow x = y. \end{aligned}$$

□

[3] 交換法則を満たす群が **Abel 群**であるが, その演算を $+$ と書くとき, Abel 群のことを**加法群**と呼ぶ.

[4] 加法群における単位元のことを**零元**という.

以後, この節では, 加法群の演算を $+$, 単位元を 0, その各元 x の逆元を $-x$ で表すことにする.

$S \times S$ 上の 2 項関係 $\sim$ を, 各 (x, y), $(z, w) \in S \times S$ に対して

$$(x, y) \sim (z, w) \Longleftrightarrow x + w = z + y$$

によって定める.

[命題 2.2] $\sim$ は $S \times S$ 上の同値関係である.

[証明] x, y, z, w, u, $v \in S$ とする.

$x + y = x + y$ より $(x, y) \sim (x, y)$. したがって $\sim$ に関して反射法則が成り立つ.

$(x, y) \sim (z, w) \Rightarrow x + w = z + y \Rightarrow z + y = x + w \Rightarrow (z, w) \sim (x, y)$. したがって $\sim$ に関して対称法則が成り立つ.

$(x, y) \sim (z, w)$, $(z, w) \sim (u, v)$ を仮定すれば,

$$x + w = z + y, \quad z + v = u + w.$$

これらの式を辺々加えると

$$x + w + z + v = z + y + u + w.$$

結合法則, 交換法則, 簡約法則により

$$x + v = u + y.$$

すなわち $(x, y) \sim (u, v)$. したがって $\sim$ に関して推移法則が成り立つ. □

直積集合 $S \times S$ を同値関係 $\sim$ により類別した同値類の集合を G とおく:

$$G = S \times S/\sim$$

また, $(x, y) \in S \times S$ を代表元とする G の同値類を $[x, y]$ と書く. つまり,

$$G = \{[x, y] \mid x, y \in S\}.$$

このとき, 任意の x, y, z, $w \in S$ に対して

$$[x, y] = [z, w] \Longleftrightarrow (x, y) \sim (z, w) \Longleftrightarrow x + w = z + y$$

が成り立つ.

[補題 2.3] (i) 任意の x, $y \in S$ に対して $[x, x] = [y, y]$.

(ii) 任意の x, y, $z \in S$ に対して $[x + z, y + z] = [x, y]$.

(iii) 任意の x, y, $z \in S$ に対して $[x + y, y] = [x + z, z]$.

[証明] x, y, $z \in S$ とする.

(i)　交換法則より $x + y = y + x$.

(ii)　結合法則と交換法則より $(x + z) + y = x + (y + z)$.

(iii)　結合法則と交換法則より $(x + y) + z = (x + z) + y$. □

G の演算 $+$ を

$$[x, y] + [z, w] = [x + z, y + w]$$

によって定義する.

[命題 2.4] G は加法群になる.

[証明] x, y, z, w, x', y', z', w', u, $v \in S$ とする.

S が結合法則と交換法則を満たすことを利用すれば,

$$\begin{aligned}
&[x, y] = [x', y'],\ [z, w] = [z', w'] \\
&\quad \Longrightarrow x + y' = x' + y,\ z + w' = z' + w \\
&\quad \Longrightarrow (x + y') + (z + w') = (x' + y) + (z' + w) \\
&\quad \Longrightarrow (x + z) + (y' + w') = (x' + z') + (y + w) \\
&\quad \Longrightarrow [x + z, y + w] = [x' + z', y' + w'].
\end{aligned}$$

よって G の演算は well-defined である.

S が結合法則を満たすことを利用すれば,

$$\begin{aligned}
([x, y] + [z, w]) + [u, v] &= [x + z, y + w] + [u, v] \\
&= [x + z + u, y + w + v] \\
&= [x, y] + [z + u, w + v] \\
&= [x, y] + ([z, w] + [u, v]).
\end{aligned}$$

よって G も結合法則を満たす.

S が交換法則を満たすことを利用すれば,

$$\begin{aligned}
[x, y] + [z, w] &= [x + z, y + w] \\
&= [z + x, w + y] \\
&= [z, w] + [x, y].
\end{aligned}$$

よって G も交換法則を満たす.

S の元 s を任意にとったとき, G の単位元は $[s, s]$ である. 実際,

$$\begin{aligned}
[s, s] + [z, w] &= [s + z, s + w] = [z, w], \\
[z, w] + [s, s] &= [z + s, w + s] = [z, w].
\end{aligned}$$

$[x, y]$ の逆元は $[y, x]$ である. 実際,

$$[x, y] + [y, x] = [x + y, y + x] = [x + y, x + y] = [s, s].$$

以上より, G が加法群であることが示された. □

$s \in S$ を 1 つとって固定し, 各 $x \in S$ に対して

$$\varphi(x) = [x + s, s]$$

とおくことにより写像 $\varphi : S \to G$ を定義する. 補題 2.3 (iii) より φ の定義は s の選び方に依存しない. また, S は空でないので, 元 s は少なくとも 1 つ存在する.

[補題 2.5] 任意の x, $y \in S$ に対して $[x, y] = \varphi(x) - \varphi(y)$.

[証明] $s \in S$ とするとき,

$$\begin{aligned}
[x, y] &= [x + s, s] + [s, y + s] \\
&= [x + s, s] - [y + s, s] \\
&= \varphi(x) - \varphi(y)
\end{aligned}$$

となる. □

[補題 2.6] φ は単射準同型である. したがって特に, S は G の部分半群である.

[証明] x, y を S の元とする. S が簡約法則を満たすことから,

$$\begin{aligned}
\varphi(x) = \varphi(y) &\Longrightarrow [x + s, s] = [y + s, s] \\
&\Longrightarrow x + s + s = y + s + s \\
&\Longrightarrow x = y.
\end{aligned}$$

よって, φ は単射である. また,

$$\begin{aligned}
\varphi(x) + \varphi(y) &= [x + s, s] + [y + s, s] \\
&= [x + y + s + s, s + s] \\
&= \varphi(x + y).
\end{aligned}$$

よって, φ は準同型である. □

[補題 2.7] M が加法群で, $\psi : S \to M$ を準同型とすると, 準同型 $g : G \to M$ で

$$\psi = g \circ \varphi$$

をみたすものがただ 1 つ存在する.

[証明] x, y, z, $w \in S$ とする.

$[x, y] = [z, w]$ とすると, $x + w = z + y$ である. ψ は準同型だから

$$\psi(x) + \psi(w) = \psi(x + w) = \psi(z + y) = \psi(z) + \psi(y).$$

M は加法群であるから

$$\psi(x) - \psi(y) = \psi(z) - \psi(w)$$

を得る. そこで,

$$g([x, y]) = \psi(x) - \psi(y)$$

によって写像 $g : G \to M$ を定義すれば, この値は x, y の選び方によらない. つまり g は well-defined である. また,

$$\begin{aligned} g([x, y] + [z, w]) &= g([x + z, y + w]) \\ &= \psi(x + z) - \psi(y + w) \\ &= (\psi(x) + \psi(z)) - (\psi(y) + \psi(w)) \\ &= (\psi(x) - \psi(y)) + (\psi(z) - \psi(w)) \\ &= g([x, y]) + g([z, w]). \end{aligned}$$

よって g は準同型である. さらに,

$$\begin{aligned} g(\varphi(x)) &= g([x + y, y]) \\ &= \psi(x + y) - \psi(y) \\ &= \psi(x) + \psi(y) - \psi(y) \\ &= \psi(x). \end{aligned}$$

よって $g \circ \varphi = \psi$ が成り立つ.

次に, $g' : G \to M$ を準同型とし, $g' \circ \varphi = \psi$ をみたすものとすると,

$$[x, y] = [x + z, z] + [z, z + y] = \varphi(x) - \varphi(y)$$

であるから,

$$\begin{aligned} g'([x, y]) &= g'(\varphi(x) - \varphi(y)) = g'(\varphi(x)) - g'(\varphi(y)) \\ &= \psi(x) - \psi(y) = g(\varphi(x)) - g(\varphi(y)) \\ &= g(\varphi(x) - \varphi(y)) = g([x, y]). \end{aligned}$$

x, y の取り方は任意であるから, $g = g'$ となる. □

[定理 2.8] G は, 簡約的可換半群 S を部分半群とする加法群のうちで最小のものである.

[証明] 補題 2.6 より, G は S を部分半群とする加法群である. 以下, G の最小性を示そう.

S を部分半群とする加法群 M を任意にとると, 単射準同型 $\psi : S \to M$ が存在する. 補題 2.7 より準同型 $g : G \to M$ で

$$\psi = g \circ \varphi$$

となるものがただ 1 つ存在する.

g が単射であることが示されたとしよう. すると, G は M の部分群である. M は任意なので, G は S を含むすべての加法群の部分群である. すなわち, G はそのような加法群のうちで最小のものである. よって, g の単射性がいえれば, 証明は完了する.

g が単射であることを示そう. x, y, z, $w \in S$ とし, $g([x,y]) = g([z,w])$ とする. このとき, 補題 2.5 より $[x,y] = \varphi(x) - \varphi(y)$, $[z,w] = \varphi(z) - \varphi(w)$ であるから,

$$\begin{aligned} g([x,y]) &= g(\varphi(x) - \varphi(y)) = g(\varphi(x)) - g(\varphi(y)) = \psi(x) - \psi(y), \\ g([z,w]) &= g(\varphi(z) - \varphi(w)) = g(\varphi(z)) - g(\varphi(w)) = \psi(z) - \psi(w). \end{aligned}$$

これらより,

$$\psi(x) - \psi(y) = g([x,y]) = g([z,w]) = \psi(z) - \psi(w).$$

したがって $\psi(x) + \psi(w) = \psi(z) + \psi(y)$ となる. ψ は単射準同型だから,

$$\begin{aligned} \psi(x) + \psi(w) = \psi(z) + \psi(y) &\Longrightarrow \psi(x+w) = \psi(z+y) \\ &\Longrightarrow x + w = z + y \\ &\Longrightarrow [x,y] = [z,w]. \end{aligned}$$

ゆえに, 任意の x, y, z, $w \in S$ に対して

$$g([x,y]) = g([z,w]) \Longrightarrow [x,y] = [z,w].$$

したがって, g は G から M への単射である.

以上より, G が S を部分半群とする加法群のうちで最小のものであることが示された. □

G を**簡約的可換半群 S から生成される加法群**と呼ぶ.

2.2 整数の定義

自然数の全体からなる集合 $\mathbb{N}$ は簡約的可換半群である. したがって, 定理 6.8 より $\mathbb{N}$ を部分半群とする最小の加法群

$$\mathbb{Z} = \mathbb{N} \times \mathbb{N} / \sim = \{[x,y] \mid x, y \in \mathbb{N}\}$$

が存在する. $\mathbb{Z}$ の元を**整数**という.

$\mathbb{Z}$ は加法群だから, 一般の加法群が満たすべき次の基本的な性質を $\mathbb{Z}$ も満たしている.

零元の存在と一意性: ある $0 \in \mathbb{Z}$ がただ 1 つ存在して, 任意の $a \in \mathbb{Z}$ に対して, $a+0 = 0+a = 0$. この 0 は $\mathbb{Z}$ の**零元**と呼ばれる.

逆元の存在と一意性: 任意の $a \in \mathbb{Z}$ に対して, ある $b \in \mathbb{Z}$ がただ 1 つ存在して $a+b = b+a = 0$. この b は a の**逆元**と呼ばれ, $-a$ と表される.

結合法則: 任意の a, b, $c \in \mathbb{Z}$ に対して, $(a+b)+c = a+(b+c) = 0$.

交換法則: 任意の a, $b \in \mathbb{Z}$ に対して, $a+b = b+a$.

簡約法則: 任意の a, b, $c \in \mathbb{Z}$ に対して, $a+c = b+c \Longrightarrow a = b$.

[定理 2.9] 任意の a, $b \in \mathbb{Z}$ に対して, 次が成り立つ.

(i) $-(-a) = a$.

(ii) $a = -b \Longleftrightarrow b = -a$.

(iii) $a = 0 \Longleftrightarrow -a = 0$.

[証明] (i)　$-a$ は a の加法における逆元なので, $0 = a+(-a) = (-a)+a$. 見方を変えれば, a が $-a$ の逆元である. よって逆元の一意性から $-(-a) = a$ が得られる.

(ii)　$a = -b$ とすれば, $a+b = (-b)+b = 0$. 逆元の一意性より $b = -a$. 逆に, $b = -a$ とすれば, $a = a+0 = a+(b-b) = (a+b)-b = (a-a)-b = 0-b = -b$.

(iii)　$0+0 = 0+0 = 0$ より, 0 の加法における逆元は 0 自身である. すなわち $-0 = 0$ である. (ii) において $b = 0$ とおくことにより, (iii) が得られる. □

単射準同型 $\varphi : \mathbb{N} \to \mathbb{Z}$ により, $\mathbb{N}$ を $\mathbb{Z}$ の部分集合とみなす. $x \in \mathbb{N}$ とすると, φ による x の像は

$$\varphi(x) = [x+0, 0] = [x, 0].$$

そこで, $x = [x, 0]$ とみなす. 特に, $0 = [0, 0]$ は $\mathbb{Z}$ の零元である.

$x \in \mathbb{N}$ に対して,

$$[x, 0] + [0, x] = [x, x] = [0, 0]$$

となるから, $[0, x]$ は $\mathbb{Z}$ の加法における $[x, 0]$ の逆元である. すなわち,

$$[0, x] = -[x, 0] = -x.$$

任意の x, $y \in \mathbb{N}$ に対して,

$$[x, y] = [x, 0] + [0, y] = x - y.$$

したがって,

$$\mathbb{Z} = \{x - y \mid x, y \in \mathbb{N}\}$$

と表すことができる.

[定理 2.10] $\mathbb{Z}$ のすべての元 a について, 次の (i), (ii), (iii) のいずれかが必ず成り立ち, 2 つの条件が同時に成り立つことはない.

(i) ある $k \in \mathbb{N}$, $k \neq 0$ が存在して $a = -k$.

(ii) $a = 0$.

(iii) ある $l \in \mathbb{N}$, $l \neq 0$ が存在して $a = l$.

[証明] a は, ある $x, y \in \mathbb{N}$ によって $a = [x, y]$ と表される.

(i), (ii), (iii) のいずれかが成り立つこと：$\mathbb{N}$ の順序の性質より, $x < y$, $x = y$, $y < x$ のいずれかが必ず成り立つ.

$x < y$ のとき, ある $k \in \mathbb{N}$, $k \neq 0$ が存在して $y = x + k$. よって

$$a = [x, x + k] = [0, k] = -k.$$

$x = y$ のとき,

$$a = [x, x] = [0, 0] = 0.$$

$y < x$ のとき, ある $l \in \mathbb{N}$, $l \neq 0$ が存在して $x = y + l$. よって

$$a = [y + l, y] = [l, 0] = l.$$

2 つの条件が同時に成り立たないこと：任意の m, $n \in \mathbb{N}$ に対して

$$[0, n] = [0, 0] \Longrightarrow 0 + 0 = 0 + n \Longrightarrow n = 0,$$
$$[m, 0] = [0, 0] \Longrightarrow m + 0 = 0 + 0 \Longrightarrow m = 0,$$
$$[0, n] = [m, 0] \Longrightarrow 0 + 0 = m + n \Longrightarrow m + n = 0 \Longrightarrow m = n = 0$$

となることから, もし (i), (ii) が同時に成り立つと仮定すると矛盾が生じる. 他も同様である. □

$-\mathbb{N} = \{-x \mid x \in \mathbb{N}\}$ とおくと, 定理 2.10 より

$$\mathbb{Z} = \mathbb{N} \cup -\mathbb{N}, \quad \mathbb{N} \cap -\mathbb{N} = \{0\}$$

が成り立つことがわかる. 特に, 1 番目の式より

$$\mathbb{Z} = \{\pm x \mid x \in \mathbb{N}\}$$

と表せる.

2.3 整数の順序

二つの整数 x, y に対して, 関係 $\leq$ を次のように定義する.

$$x \leq y \iff \text{ある } k \in \mathbb{N} \text{ が存在して } y = x + k.$$

$x \leq y$ のことを $y \geq x$ と書くこともある.

[定理 2.11] 任意の整数 $x \in \mathbb{Z}$ に対して, $x \leq x$ が成り立つ.

[証明] $x = x + 0$ より明らかである. □

[定理 2.12] 任意の整数 $x, y, z \in \mathbb{Z}$ に対して, $x \leq y$ かつ $y \leq z$ ならば, $x \leq z$ が成り立つ.

[証明] $x \leq y$ かつ $y \leq z$ とすると, ある $k, l \in \mathbb{N}$ が存在して

$$y = x + k, \quad z = y + l$$

となる. 1 番目の式を 2 番目に代入すると,

$$z = (x + k) + l = x + (k + l).$$

$k + l \in \mathbb{N}$ だから, $x \leq z$ である. □

[定理 2.13] 任意の整数 $x, y \in \mathbb{Z}$ に対して, $x \leq y$ かつ $y \leq x$ ならば, $x = y$ が成り立つ.

[証明] $x \leq y$ かつ $y \leq x$ とすると, ある $k, l \in \mathbb{N}$ が存在して

$$y = x + k, \quad x = y + l$$

となる. 1 番目の式を 2 番目に代入すると,

$$x = (x + k) + l = x + (k + l).$$

加法に関する簡約法則を用いれば $0 = k + l$ が得られる. k, l は自然数だから, $k = l = 0$. したがって $x = y$ が得られる. □

以上より, $\leq$ が実際に $\mathbb{Z}$ 上の順序関係であること, すなわち反射法則（定理 2.11）, 推移法則（定理 2.12）, 対称法則（定理 2.13）が成り立つことが示された.

二つの整数 x, y について, $x \leq y$ かつ $x \neq y$ であることを $x < y$ や $y > x$ で表す. このとき, y は x より**大きい**といい, x は y より**小さい**という.

[定理 2.14] 任意の整数 $x, y \in \mathbb{Z}$ に対して,

$$x < y \iff \text{ある } k \in \mathbb{N},\ k \neq 0 \text{ が存在して } y = x + k$$

が成り立つ.

[証明] $x < y$ とすると, $x \leq y$ なので, ある $k \in \mathbb{N}$ が存在して $y = x + k$. もし $k = 0$ ならば $y = x$ となり $x < y$ に反する. よって $k \neq 0$.

逆に, ある $k \in \mathbb{N}$ が存在して $y = x + k$ が成り立てば $x \leq y$. もし $x = y$ ならば, $x = x + k$ なので, 両辺に $-x$ を加えると $k = 0$ が得られる. したがって, $k \neq 0$ ならば $x \neq y$. ゆえに $x < y$ である. □

[定理 2.15] 任意の整数 x, y, $z \in \mathbb{Z}$ に対して, 次が成り立つ.

(i) $x \leq y$ かつ $y < z$ ならば, $x < z$.
(ii) $x < y$ かつ $y \leq z$ ならば, $x < z$.
(iii) $x < y$ かつ $y < z$ ならば, $x < z$.

[証明] $x \leq y$ かつ $y < z$ ならば, ある k, $l \in \mathbb{N}$, $l \neq 0$ が存在して $y = x + k$, $z = y + l$ となる. 1 番目の式を 2 番目に代入すると,

$$z = (x + k) + l = x + (k + l).$$

$k + l$ は 0 でない自然数だから, $x < z$. したがって (i) が成り立つ.

(ii), (iii) も (i) と同様にして示せる. □

[定理 2.16] 任意の整数 x, y, $z \in \mathbb{Z}$ に対して,

$$x < y \Longleftrightarrow x + z < y + z$$

が成り立つ.

[証明] ($\Rightarrow$) $x < y$ とすると, ある $k \in \mathbb{N}$, $k \neq 0$ が存在して $y = x + k$. このとき, $y + z = (x + k) + z = (x + z) + k$. よって $x + z < y + z$.

($\Leftarrow$) $x + z < y + z$ とすると, ある $l \in \mathbb{N}$, $l \neq 0$ が存在して $y + z = x + z + l$. このとき, 両辺に $-z$ を加えると $y = x + l$ が得られる. よって $x < y$. □

[定理 2.17] 任意の x, y, z, $w \in \mathbb{Z}$ に対して, 次が成り立つ.

(i) $x < y$ かつ $z < w$ ならば, $x + z < y + w$.
(ii) $x \leq y$ かつ $z < w$ ならば, $x + z < y + w$.
(iii) $x < y$ かつ $z \leq w$ ならば, $x + z < y + w$.
(iv) $x \leq y$ かつ $z \leq w$ ならば, $x + z \leq y + w$.

[証明] $x < y$, $z < w$ とすると, ある $k, l \in \mathbb{N}$, $k \neq 0$, $l \neq 0$ が存在して $y = x + k$, $w = z + l$ となる. よって

$$y + w = (x + k) + (z + l) = (x + z) + (k + l).$$

$k + l$ は 0 でない自然数だから, $x + z < y + w$. したがって (i) が成り立つ.

(ii), (iii), (iv) も (i) と同様にして示せる. □

[定理 2.18] 任意の $x, y \in \mathbb{Z}$ に対して, 次が成り立つ.

(i) $x < y$ ならば $x + 1 \leq y$.

(ii) $x < y + 1$ ならば $x \leq y$.

[証明] (i) $x < y$ とすると, ある $k \in \mathbb{N}$ が存在して $x = y + k$, $k \neq 0$ が成り立つ. k は 0 でない自然数だから, ある $l \in \mathbb{N}$ が存在して $k = l + 1$. よって $y = x + (l + 1) = (x + 1) + l$. したがって $x + 1 \leq y$.

(ii) $x < y + 1$ とすると, ある $k \in \mathbb{N}$ が存在して $y + 1 = x + k$, $k \neq 0$ が成り立つ. k は 0 でない自然数だから, ある $l \in \mathbb{N}$ が存在して $k = l + 1$. よって $y + 1 = x + l + 1$. 両辺に -1 を加えれば $y = x + l$ が得られる. よって $x \leq y$. □

[定理 2.19] 任意の $x, y \in \mathbb{Z}$ に対して, 次が成り立つ.

(i) $x < y \iff -y < -x$.

(ii) $x > 0 \iff -x < 0$.

(iii) $x < 0 \iff -x > 0$.

[証明] (i) ($\Rightarrow$) $x < y$ とするとき, 両辺に $-x - y$ を加えると, 定理 2.16 より,

$$-y = x - x - y < y - x - y = -x.$$

($\Leftarrow$) $-y < -x$ とするとき, 両辺に $x + y$ を加えると, 再び定理 2.16 より,

$$x = x + y - y < x + y - x = y.$$

(ii) (i) において $x = 0$, $y = x$ とおくことで得られる. ここで, $-0 = 0$ であることに注意せよ.

(iii) (i) において $y = 0$ とおくことで得られる. ここで再び, $-0 = 0$ であることに注意せよ.
□

[定理 2.20] $x \in \mathbb{Z}$ とするとき, 次のことが成り立つ.

(i) $x > 0 \iff x \in \mathbb{N}$ かつ $x \neq 0$.

(ii) $x < 0 \iff x \in -\mathbb{N}$ かつ $x \neq 0$.

[証明] (i)　$x > 0$ とすると, ある $k \in \mathbb{N}$, $k \neq 0$ が存在して $x = 0 + k = k$ となる. ゆえに $x \in \mathbb{N}$, $x \neq 0$ である. 逆に, $x \in \mathbb{N}$, $x \neq 0$ ならば, $x = 0 + x$ より $x > 0$.

(ii)　$x < 0$ とすると, $<$ の定義から $x \neq 0$ である. また, ある $k \in \mathbb{N}$, $k \neq 0$ が存在して $0 = x + k$ となる. 両辺に $-k$ を加えると $x = -k$ が得られる. ゆえに $x \in -\mathbb{N}$. 逆に, $-x \in \mathbb{N}$, $x \neq 0$ ならば, $0 = x + (-x)$ より $x < 0$. □

[定理 2.21] 任意の $x \in \mathbb{Z}$ に対して, $x > 0$, $x = 0$, $x < 0$ のいずれか 1 つ, しかも 1 つだけが成り立つ.

[証明]

$$\mathbb{Z}^+ = \{n \mid n \in \mathbb{N}, n \neq 0\},$$
$$\mathbb{Z}^- = \{-n \mid n \in \mathbb{N}, n \neq 0\}$$

とおくと, $\mathbb{Z} = \mathbb{N} \cup -\mathbb{N}$, $\mathbb{N} \cap -\mathbb{N} = \{0\}$ より

$$\mathbb{Z} = \mathbb{Z}^+ \cup \{0\} \cup \mathbb{Z}^- \quad \text{(集合の直和)}$$

となる. すなわち, 任意の $x \in \mathbb{Z}$ に対して, $x \in \mathbb{Z}^+$, $x \in \{0\}$, $x \in \mathbb{Z}^-$ のいずれか 1 つ, しかも 1 つだけが成り立つ.

一方, $x = 0 \Leftrightarrow x \in \{0\}$ であり, 定理 2.20 によって,

$$x > 0 \iff x \in \mathbb{N} \text{ かつ } x \neq 0 \iff x \in \mathbb{Z}^+,$$
$$x < 0 \iff x \in -\mathbb{N} \text{ かつ } x \neq 0 \iff x \in \mathbb{Z}^-.$$

したがって主張が成り立つ. □

$x \in \mathbb{Z}$ について, $x > 0$ であるとき, x は**正**であるという. また, $x < 0$ であるとき, x は**負**であるという.

[定理 2.22] 任意の $x, y \in \mathbb{Z}$ に対して, $x < y$, $x = y$, $y < x$ のいずれか 1 つ, しかも 1 つだけが成り立つ.

[証明] まず,

$$x < y \iff y - x > 0,$$
$$x = y \iff y - x = 0,$$
$$y < x \iff y - x < 0$$

である. 一方, 定理 2.21 より, $y - x > 0$, $y - x = 0$, $y - x < 0$ のいずれか 1 つ, しかも 1 つだけが成り立つ. したがって主張が成り立つ. □

[定理 2.23] S を空でない $\mathbb{Z}$ の部分集合とする.

(i) ある整数 $m \in \mathbb{Z}$ が存在して, 任意の $x \in S$ に対して $x < m$ が成り立つとする. このとき, S は最大元をもつ.

(ii) ある整数 $m \in \mathbb{Z}$ が存在して, 任意の $x \in S$ に対して $m < x$ が成り立つとする. このとき, S は最小元をもつ.

[証明] (i) $T = \{m - x \mid x \in S\}$ とおく. 仮定より, T の任意の元は正である. よって, T のすべての元は $\mathbb{N}$ に属する. ゆえに T は $\mathbb{N}$ の部分集合である. S は空集合ではないので, $\mathbb{N}$ の整列性により, T は最大元 t をもつ. すなわち, 任意の $x \in S$ に対して $m - x \leq t$ が成り立つ. 一方, t はある $s \in S$ によって $t = m - s$ と表せる. ゆえに任意の $x \in S$ に対して $m - s \leq m - x$ が成り立つ. したがって任意の $x \in S$ に対して $x \leq s$ が成り立つ. よって s が S の最大元である.

(ii) $T = \{x - m \mid x \in S\}$ とおけば, (i) と同様にして示せる. □

2.4 整数の乗法

[補題 2.24] 任意の x, y, z, w, x', y', z', $w' \in \mathbb{N}$ に対して, $\mathbb{Z}$ において

$$x - y = x' - y', \quad z - w = z' - w'$$

ならば

$$(xz + yw) - (xw + yz) = (x'z' + y'w') - (x'w' + y'z')$$

が成り立つ.

[証明] $x - y = x' - y'$, $z - w = z' - w'$ とすると,

$$x + y' = x' + y, \quad z + w' = z' + w$$

より,

$$\begin{aligned}&(x + y')z + (x' + y)w + x'(z + w') + y'(z' + w)\\ =&(x' + y)z + (x + y')w + x'(z' + w) + y'(z + w').\end{aligned}$$

$\mathbb{N}$ の加法, 乗法に関する交換法則, 結合法則, 分配法則を用いて計算し, 両辺から共通項を消去すれば,

$$xz + yw + x'w' + y'z' = xw + yz + x'z' + y'w'$$

が得られる. したがって,

$$(xz + yw) - (xw + yz) = (x'z' + y'w') - (x'w' + y'z')$$

が成り立つ. □

各 $a, b \in \mathbb{Z}$ に対して, ある $x, y, z, w \in \mathbb{N}$ が存在して $a = x - y$, $b = z - w$ と表すことができる. このとき, **積** ab を

$$ab = (xz + yw) - (xw + yz)$$

によって定義する. 補題 2.24 により, ab は x, y, z, w の選び方によらずに定まる. この積によって定まる演算を $\mathbb{Z}$ の**乗法**と呼ぶ.

[定理 2.25] 任意の $a, b \in \mathbb{Z}$ に対して $ab = ba$ が成り立つ. これを $\mathbb{Z}$ の乗法に関する**交換法則**という.

[証明] $a, b \in \mathbb{Z}$ とすると, ある $x, y, z, w \in \mathbb{N}$ によって $a = x - y$, $b = z - w$ と表すことができる. このとき, $\mathbb{N}$ の乗法に関する交換法則より

$$ab = (xz + yw) - (xw + yz) = (zx + wy) - (zy + wx) = ba$$

となる. よって, $\mathbb{Z}$ の乗法について交換法則が成り立つ. □

[定理 2.26] 任意の $a, b, c \in \mathbb{Z}$ に対して $(ab)c = a(bc)$ が成り立つ. これを $\mathbb{Z}$ の乗法に関する**結合法則**という.

[証明] $a, b, c \in \mathbb{Z}$ とすると, ある $x, y, z, w, u, v \in \mathbb{N}$ によって $a = x - y$, $b = z - w$, $c = u - v$ と表すことができる. このとき, $\mathbb{Z}$ の乗法の定義にしたがって計算し, $\mathbb{N}$ の乗法に関する分配法則を用いると,

$$\begin{aligned}(ab)c &= \big((xz + yw) - (xw + yz)\big)(u - v)\\ &= \big((xz + yw)u + (xw + yz)v\big) - \big((xz + yw)v + (xw + yz)u\big)\\ &= \big((xz)u + (yw)u + (xw)v + (yz)v\big) - \big((xz)v + (yw)v + (xw)u + (yz)u\big).\end{aligned}$$

同様に,

$$\begin{aligned}a(bc) &= (x - y)\big((zu + wv) - (zv + wu)\big)\\ &= \big(x(zu + wv) + y(zv + wu)\big) - \big(x(zv + wu) + y(zu + wv)\big)\\ &= \big(x(zu) + x(wv) + y(zv) + y(wu)\big) - \big(x(zv) + x(wu) + y(zu) + y(wv)\big).\end{aligned}$$

さらに, $\mathbb{N}$ の乗法に関する結合法則により

$$\begin{aligned}(xz)u + (yw)u + (xw)v + (yz)v &= x(zu) + x(wv) + y(zv) + y(wu),\\ (xz)v + (yw)v + (xw)u + (yz)u &= x(zv) + x(wu) + y(zu) + y(wv).\end{aligned}$$

したがって $(ab)c = a(bc)$ が成り立つ. □

[定理 2.27] $\mathbb{Z}$ の乗法における単位元は 1 である.

[証明] $a \in \mathbb{Z}$ とすると, ある $x, y \in \mathbb{N}$ が存在して $a = x - y$ と表すことができる. また, $1 = 1 - 0$ である. よって,

$$a \cdot 1 = (x - y)(1 - 0) = x \cdot 1 - y = x - y = a,$$
$$1 \cdot a = (1 - 0)(x - y) = 1 \cdot x - y = x - y = a.$$

したがって 1 は $\mathbb{Z}$ の乗法における単位元である. □

[定理 2.28] 任意の $a, b, c \in \mathbb{Z}$ に対して

$$a(b + c) = ab + ac, \quad (a + b)c = ac + bc.$$

が成り立つ. これらの等式を $\mathbb{Z}$ の加法と乗法に関する**分配法則**という.

[証明] $a, b, c \in \mathbb{Z}$ とすると, ある $x, y, z, w, u, v \in \mathbb{N}$ によって $a = x - y$, $b = z - w$, $c = u - v$ と表すことができる.

$\mathbb{Z}$ の乗法の定義にしたがって計算すると,

$$\begin{aligned} a(b + c) &= (x - y)\big((z + u) - (w + v)\big) \\ &= \big(x(z + u) + y(w + v)\big) - \big(x(w + v) + y(z + u)\big). \end{aligned}$$

同様に,

$$\begin{aligned} ab + ac &= (x - y)(z - w) + (x - y)(u - v) \\ &= \big((xz + yw) - (xw + yz)\big) + \big((xu + yv) - (xv + yu)\big) \\ &= \big((xz + yw) + (xu + yv)\big) - \big((xw + yz) + (xv + yu)\big). \end{aligned}$$

さらに, $\mathbb{N}$ の分配法則によって

$$x(z + u) + y(w + v) = (xz + yw) + (xu + yv),$$
$$x(w + v) + y(z + u) = (xw + yz) + (xv + yu).$$

したがって $a(b + c) = ab + ac$ が成り立つ.

$\mathbb{Z}$ は乗法に関して交換法則を満たす (定理 2.25) ので, 一方の等式から他方が得られる. □

[定理 2.29] 任意の $x, y, z \in \mathbb{Z}$ に対して, 次が成り立つ.

(i) $x \cdot 0 = 0 \cdot x = 0$.

(ii) $(-x)y = x(-y) = -(xy)$.

(iii) $(-x)(-y) = xy$.

(iv) $x(y-z) = xy - xz$, $(x-y)z = xz - yz$.

[証明] (i) $x \cdot 0 = x(0+0) = x \cdot 0 + x \cdot 0$. 両辺に $-x \cdot 0$ を加えると $x \cdot 0$ が得られる. 同様にして $0 \cdot x = 0$ も得られる.

(ii) 分配法則と (i) より $xy + (-x)y = (x-x)y = 0 \cdot y = 0$. 逆元の一意性により $(-x)y = -(xy)$. 同様にして $x(-y) = -(xy)$ も得られる.

(iii) 分配法則と (i) より $x(-y) + (-x)(-y) = (x-x)(-y) = 0 \cdot y = 0$. 一方, (ii) より $x(-y) = -(xy)$. ゆえに $-(xy) + (-x)(-y) = 0$. 両辺に xy を加えれば $(-x)(-y) = xy$ が得られる.

(iv) 分配法則と (ii) より $x(y-z) = xy + x(-z) = xy - xz$. 同様にして $(x-y)z = xz - yz$ も得られる. □

[定理 2.30] 任意の $x, y \in \mathbb{Z}$ に対して, $x \neq 0$ かつ $y \neq 0$ ならば, $xy \neq 0$.

[証明] $x \neq 0$ かつ $y \neq 0$ のとき, 次の 4 通りのいずれかが成り立つ.

- $x > 0$ かつ $y > 0$,
- $x > 0$ かつ $y < 0$,
- $x < 0$ かつ $y > 0$,
- $x < 0$ かつ $y < 0$.

$x > 0$ かつ $y > 0$ のとき, $x, y \in \mathbb{N}$, $x \neq 0$, $y \neq 0$ だから, $\mathbb{N}$ において $xy \neq 0$ となる.

$x > 0$ かつ $y < 0$ のとき, $-y > 0$ なので, $x, -y \in \mathbb{N}$, $x \neq 0$, $-y \neq 0$ だから, $\mathbb{N}$ において $x(-y) \neq 0$ となる. 一方, $-xy = x(-y)$ だから $-xy \neq 0$. よって $xy \neq 0$.

$x < 0$ かつ $y > 0$ のとき, $-x > 0$ なので, $-x, y \in \mathbb{N}$, $-x \neq 0$, $y \neq 0$ だから, $\mathbb{N}$ において $(-x)y \neq 0$ となる. 一方, 定理 2.29 (ii) より $-xy = (-x)y$ だから $-xy \neq 0$. よって $xy \neq 0$.

$x < 0$ かつ $y < 0$ のとき, $-x > 0$, $-y > 0$ なので, $-x, -y \in \mathbb{N}$, $-x \neq 0$, $-y \neq 0$ だから, $\mathbb{N}$ において $(-x)(-y) \neq 0$ となる. 一方, $xy = (-x)(-y)$. よって $xy \neq 0$. □

[定理 2.31] 任意の $x, y, z \in \mathbb{Z}$ に対して, $z \neq 0$ ならば

$$xz = yz \Longrightarrow x = y$$

が成り立つ. これを $\mathbb{Z}$ の乗法に関する**簡約法則**という.

[証明] $z \neq 0$ とし, さらに $xz = yz$ とする. $xz = yz$ の両辺に $-yz$ を加えると $xz - yz = 0$ となる. 一方, 分配法則より $(x-y)z = xz - yz$ であるから, $(x-y)z = 0$ である. このとき, 定理 2.30 の対偶により $x - y = 0$ または $z = 0$ である. $z \neq 0$ と仮定したから, $x - y = 0$. よって $x = y$. □

[定理 2.32] 任意の x, y, $z \in \mathbb{Z}$ に対して, 次が成り立つ.

(i) $x < y$ かつ $z > 0$ ならば, $xz < yz$.
(ii) $x < y$ かつ $z < 0$ ならば, $yz < xz$.
(iii) $x > 0$ かつ $y > 0$ ならば, $xy > 0$.
(iv) $x > 0$ かつ $y < 0$ ならば, $xy < 0$.
(v) $x < 0$ かつ $y > 0$ ならば, $xy < 0$.
(vi) $x < 0$ かつ $y < 0$ ならば, $xy > 0$.

[証明] (i) $x < y$ より, ある $k \in \mathbb{N}$, $k \neq 0$ が存在して $y = x + k$. 両辺に z を乗じると

$$yz = (x+k)z = xz + kz.$$

一方, $z > 0$ より $z \in \mathbb{N}$, $z \neq 0$. よって $kz \in \mathbb{N}$, $kz \neq 0$. したがって $xz < yz$.

(ii) $x < y$ とする. $z < 0$ ならば $-z > 0$ であるから, (i) より $x(-z) < y(-z)$. 一方, 定理 2.29 (ii) より $x(-z) = -(xz)$, $y(-z) = -(yz)$ である. よって $-(xz) < -(yz)$. したがって $yz < xz$.

(iii) (i) において, x, y, z をそれぞれ 0, x, y に置き換えればよい.

(iv) (ii) において, x, y, z をそれぞれ 0, x, y に置き換えればよい.

(v) (i) において, x, y, z をそれぞれ x, 0, y に置き換えればよい.

(vi) (ii) において, x, y, z をそれぞれ x, 0, y に置き換えればよい. □

[定理 2.33] 任意の x, y, $z \in \mathbb{Z}$ に対して, 次が成り立つ.

(i) $xz < yz$ かつ $z > 0$ ならば, $x < y$.
(ii) $xz < yz$ かつ $z < 0$ ならば, $y < x$.
(iii) $xy > 0$ かつ $x > 0$ ならば, $y > 0$.
(iv) $xy > 0$ かつ $x < 0$ ならば, $y < 0$.
(v) $xy < 0$ かつ $x > 0$ ならば, $y < 0$.
(vi) $xy < 0$ かつ $x < 0$ ならば, $y > 0$.

[証明] (i) 対偶を示す. すなわち, $y \leq x$ ならば, $z \leq 0$ または $yz \leq xz$ であることを示す. $y = x$ のときは $yz = xz$ である. $y < x$ のとき, $z \leq 0$ でなければ $z > 0$ であり, そのとき定理 2.32 (i) より $yz < xz$ となる.

(ii)　$xz < yz$ かつ $z < 0$ とすると, $(-x)(-z) < (-y)(-z)$ かつ $-z > 0$ であり, (i) より $-x < -y$. ゆえに $y < x$.

(iii)　(i) において, x, y, z をそれぞれ 0, y, x に置き換えればよい.

(iv)　(ii) において, x, y, z をそれぞれ 0, y, x に置き換えればよい.

(v)　(i) において, x, y, z をそれぞれ y, 0, x に置き換えればよい.

(vi)　(ii) において, x, y, z をそれぞれ y, 0, x に置き換えればよい. □

2.5　整数の絶対値

$x \in \mathbb{Z}$ に対して, x の**絶対値** $|x|$ を

$$|x| = \begin{cases} x & x > 0 \text{ のとき} \\ 0 & x = 0 \text{ のとき} \\ -x & x < 0 \text{ のとき} \end{cases}$$

と定義する.

[命題 2.34] 任意の x, $y \in \mathbb{Z}$ に対して, 次が成り立つ.

(i) $|x| \geq 0$.

(ii) $|x| = 0 \Longleftrightarrow x = 0$.

(iii) $x \leq |x|$.

(iv) $|-x| = |x|$.

(v) $|xy| = |x||y|$.

[証明] (i)　絶対値の定義と, $x < 0$ ならば $-x > 0$ であることからわかる.

(ii)　絶対値の定義から明らかである.

(iii)　$x = 0$ または $x > 0$ のときは $|x| = x$ である. $x < 0$ のときは $x < 0 < |x|$ である.

(iv)　$x = 0$ のときは $-x = x$ となることから明らか. $x > 0$ のとき, $-x < 0$ なので

$$|x| = -(-x) = x = |x|$$

となる. $x < 0$ のとき, $-x > 0$ なので

$$|-x| = -x = |x|$$

となる.

(v)　$x = 0$ または $y = 0$ のとき, $|x| = 0$ または $|y| = 0$ より $|x||y| = 0$. 一方, $xy = 0$ より $|xy| = 0$.

$x > 0$ かつ $y > 0$ のとき, $xy > 0$ より $|xy| = xy = |x||y|$.

$x > 0$ かつ $y < 0$ のとき, $xy < 0$ より $|xy| = -(xy) = x(-y) = |x||y|$.
$x < 0$ かつ $y > 0$ のとき, $xy < 0$ より $|xy| = -(xy) = (-x)y = |x||y|$.
$x < 0$ かつ $y < 0$ のとき, $xy > 0$ より $|xy| = xy = (-x)(-y) = |x||y|$. □

[命題 2.35] 任意の $x, y \in \mathbb{Z}$ に対して, 次が成り立つ.

(i) $|x + y| \leq |x| + |y|$. この不等式は**三角不等式**と呼ばれる.
(ii) $|x - y| \leq |x| + |y|$.
(iii) $|x| - |y| \leq |x + y|$.
(iv) $|x| - |y| \leq |x - y|$.

[証明] (i) $x \leq |x|$, $y \leq |y|$ より

$$x + y \leq |x| + |y|.$$

一方, $-x \leq |x|$, $-y \leq |y|$ より

$$-(x + y) \leq |x| + |y|.$$

$|x + y|$ は $x + y$ か $-(x + y)$ のどちらかに等しい. よって

$$|x + y| \leq |x| + |y|.$$

となる.

(ii) (i) において, y に $-y$ を代入すれば, $|-y| = |y|$ より (ii) が得られる.

(iii) (ii) において y に $x + y$ を代入すれば,

$$|x - (x + y)| \leq |x| + |x + y|.$$

これと $|-y| = |y|$ より (iii) が得られる.

(iv) (i) において x に $x - y$ を代入すれば,

$$|(x - y) + y| \leq |x - y| + |y|.$$

これより (iv) が得られる. □

2.6 整数の整除

この節では, 正なる整数の全体からなる集合を $\mathbb{Z}^+$ で表す. すなわち

$$\mathbb{Z}^+ = \{x \in \mathbb{Z} \mid x > 0\}$$

とする.

［定理 2.36］ $a, b \in \mathbb{Z}, b > 0$ とする．このとき

$$a = bq + r, \quad 0 \leq r < b$$

を満たすような $q, r \in \mathbb{Z}$ がただ 1 組だけ存在する．

q, r を，それぞれ a を b で割ったときの**商**，**剰余**という[5]．

［証明］ まず，整数の組 q, r の存在を示す．

$$r = \min\{x \in \mathbb{N} \mid \text{ある } q \in \mathbb{Z} \text{ が存在して } a = bq + x\}$$

とおく．$\mathbb{N}$ の整列性より，このような $r \in \mathbb{N}$ の存在が保証される．いま，$q \in \mathbb{Z}$ が存在して

$$a = bq + r$$

であるとする．もし仮に $b \leq r$ ならば，

$$0 \leq r - b < r, \quad a = b(q-1) + (r-b)$$

となって r の最小性に反する．ゆえに $r < b$ である．

次に，一意性を示す．

$$a = bq + r, \quad 0 \leq r < b,$$
$$a = bq' + r', \quad 0 \leq r' < b$$

とすると，

$$b(q' - q) = r' - r.$$

もし仮に $q \neq q'$ ならば，

$$b \leq b|q' - q| = |r' - r| \leq \max\{r, r'\} < b.$$

これは矛盾である．したがって $q = q'$, $r = r'$ でなければならない． □

$a, b \in \mathbb{Z}$ に対して，ある $q \in \mathbb{Z}$ が存在して

$$a = bq$$

が成り立つとき，a は b で**割り切れる**という．このことを記号で

$$b \mid a$$

と書く．またこのとき，a を b の**倍数**といい，b を a の**約数**という．

$b \neq 0$ のとき，$a = bq$ となる $q \in \mathbb{Z}$ は存在するならば，a, b に対してただ 1 つ定まる．このとき，q を a/b もしくは $\dfrac{a}{b}$ で表す．

[5] 剰余のことを**余り**ともいう．

[注意 2.1] $a,\ b \in \mathbb{Z}$ とする．$b = 0$ のとき，もし，ある整数 q が存在して $a = bq$ ならば，$a = 0$ でなければならない．よって，$a \neq 0$ かつ $b = 0$ のとき，$a = bq$ となる整数 q は存在しない．また，$a = b = 0$ のとき，どのような整数 q に対しても $a = bq$ となり，q はただ 1 つには定まらない．これがまさに，数を 0 で割ってはいけない理由である．

[定理 2.37] 任意の $a,\ b \in \mathbb{Z}$ に対して，次が成り立つ．

(i) $a \mid b \iff -a \mid b$.
(ii) $a \mid b \iff a \mid -b$.

[証明] (i)　$a \mid b$ とすると，ある $q \in \mathbb{Z}$ が存在して $b = aq$．このとき $b = (-a)(-q)$ である．逆も同様である．

(ii)　$a \mid b$ とすると，ある $q \in \mathbb{Z}$ が存在して $b = aq$．このとき $-b = a(-q)$ である．逆も同様である．　□

[定理 2.38] 任意の $a,\ b,\ c \in \mathbb{Z}$ に対して，次が成り立つ．

(i) $a \mid b$ ならば $a \mid bc$.
(ii) $c \neq 0$ のとき，$a \mid b \iff ac \mid bc$.
(iii) $a \mid b$ かつ $a \mid c$ ならば，$a \mid b + c$.

[証明] (i)　$a \mid b$ とすると，ある $q \in \mathbb{Z}$ が存在して $b = aq$．このとき $bc = a(qc)$ である．よって $a \mid bc$.

(ii)　$a \mid b$ とすると，ある $q \in \mathbb{Z}$ が存在して $b = aq$．このとき $bc = (ac)q$ である．よって $ac \mid bc$. 逆に，$ac \mid bc$ とすると，ある $q' \in \mathbb{Z}$ が存在して $bc = (ac)q'$．これより $c(b - aq') = 0$ が得られ，$c \neq 0$ より $b - aq' = 0$，したがって $b = aq'$ が得られる．よって $a \mid b$.

(iii)　$a \mid b,\ a \mid c$ とすると，ある $q,\ q' \in \mathbb{Z}$ が存在して $b = aq,\ c = aq'$．よって $b + c = aq + aq' = a(q + q')$．したがって $a \mid b + c$.　□

[定理 2.39] 任意の $a,\ b \in \mathbb{Z}^+$ に対して，$a \mid b$ ならば $a \leq b$.

[証明] $a \mid b$ とすると，ある $q \in \mathbb{Z}$ が存在して $b = aq$．このとき $q \geq 1$ だから[6)]，

$$b = aq \geq a \cdot 1 = a$$

となる．　□

[6)] もし仮に $q < 1$ とすると，q は整数だから $q \leq 0$ となる．$a > 0$ だから $b = aq \leq 0$．これは $b > 0$ に矛盾する．

[定理 2.40] 任意の a, b, $c \in \mathbb{Z}^+$ に対して, 次の 3 つの条件が成り立つ.

(i) $a \mid a$.

(ii) $a \mid b$ かつ $b \mid a$ ならば, $a = b$.

(iii) $a \mid b$ かつ $b \mid c$ ならば, $a \mid c$.

[証明] (i) $a = a \cdot 1$ より明らか.

(ii) $a \mid b$ のとき, ある $q \in \mathbb{Z}^+$ が存在して $b = aq$ となる. $q \geq 1$ より,

$$a \leq a + a(q-1) = aq = b.$$

同様にして $b \leq a$ もいえる. したがって, $a \leq b$ と $b \leq a$ とがともに成り立つから, $a = b$.

(iii) $a \mid b$ のとき, ある $q \in \mathbb{Z}^+$ が存在して $b = aq$ となる. 同様に, $b \mid c$ のとき, ある $q' \in \mathbb{Z}^+$ が存在して $c = bq'$ となる. よって,

$$c = bq' = aqq'.$$

$qq' \in \mathbb{Z}$ であるから, $c \mid a$. □

[注意 2.2] 上の定理の (i), (iii) は, その前の定理を適用することで, 負の整数にも拡張できる. しかし, (ii) は負の整数までは拡張できない. 例えば, $-1 = 1 \cdot (-1)$, $1 = (-1) \cdot (-1)$ より $(-1) \mid 1$ かつ $1 \mid (-1)$ であるが $-1 \neq 1$ である.

2.7 公約数・公倍数

整数 a, $b \in \mathbb{Z}$ に対して, a と b の両方を割り切る整数のことを a と b の**公約数**という.

$d \in \mathbb{Z}$ が a と b の**最大公約数**であるとは, 次の 3 つの条件が成り立つときにいう.

- d は a と b の公約数である.
- a と b の任意の公約数は d の約数になる.
- $d > 0$.

a と b の最大公約数を記号 $\gcd(a, b)$ で表す.

3 つ以上の整数に対しても, 同様にして公約数, 最大公約数を定義することができる. 例えば a, b, $c \in \mathbb{Z}$ に対して, a, b, c のすべてを割り切る整数を a, b, c の公約数という. また, $d \in \mathbb{Z}$ が a, b, c の最大公約数であるとは, 次の 3 つの条件が成り立つときにいう.

- d は a, b, c の公約数である.
- a, b, c の任意の公約数は d の約数になる.
- $d > 0$.

a, b, c の最大公約数を記号 $\gcd(a, b, c)$ で表す.

[定理 2.41] 任意の a, b, $c \in \mathbb{Z}$ に対して, 次のことが成り立つ.

(i) $\gcd(a,b) = \gcd(b,a)$.

(ii) $\gcd(a,b,c) = \gcd(\gcd(a,b),c)$.

[証明] (i) x を整数とする. 明らかに, x が a と b の公約数であることと, b と a の公約数であることとは同値である[7]. これより, a と b の任意の公約数が d の約数であることと, b と a の任意の公約数が d の約数であることとが同値であることも明らかである[8].

(ii) $d = \gcd(a,b,c)$, $d' = \gcd(\gcd(a,b),c)$, $d'' = \gcd(a,b)$ とおく.

$d \mid a$, $d \mid b$ より $d \mid d''$. また, $d \mid c$. ゆえに $d \mid d'$. 逆に, $d' \mid d''$ であり, $d'' \mid a$ だから $d' \mid a$. 同様に $d' \mid b$. 一方, $d' \mid c$ でもある. したがって $d' \mid d$. ゆえに, $d' \mid d$ かつ $d \mid d'$ より, $d = d'$. ここで, $d > 0$, $d' > 0$ であることに注意せよ. □

$m \in \mathbb{Z}$ に対して, m の倍数全体からなる集合を $m\mathbb{Z}$ とおく. すなわち

$$m\mathbb{Z} = \{mx \mid x \in \mathbb{Z}\}$$

とする.

[定理 2.42] a, $b \in \mathbb{Z}$ とし,

$$I = \{ax + by \mid x, y \in \mathbb{Z}\}$$

とおく. このとき, ある $d \in \mathbb{Z}$ が存在して

$$I = d\mathbb{Z}, \quad d = \gcd(a,b)$$

が成り立つ.

[証明] $S = \{x \in \mathbb{N} \mid x \in I, x \neq 0\}$ とおく. $\mathbb{N}$ の整列性により, S の最小元 $d > 0$ が存在する. このとき, ある x, $y \in \mathbb{Z}$ が存在して

$$d = ax + by$$

と書ける.

$I = d\mathbb{Z}$ を示せばよいが, $d\mathbb{Z} \subseteq I$ は明らかなので[9], $I \subseteq d\mathbb{Z}$ を示せば十分である.

$z \in I$ とする. ある q, $r \in \mathbb{Z}$ が存在して

$$z = dq + r, \quad 0 \leq r < d$$

[7] 二つの命題 P, Q について, 「P かつ Q」と「Q かつ P」とが同値であることに注意して, P として $x \mid a$ をとり, Q として $x \mid b$ をとればよい.

[8] きちんと証明すれば, a と b の公約数全体の集合を A とし, b と a の公約数全体の集合を B とし, d の約数全体の集合を D とするとき, x が a と b の公約数であることと, b と a の公約数であることとが同値であるから $A = B$. よって $A \subseteq D \Leftrightarrow B \subseteq D$.

[9] 任意の $z \in \mathbb{Z}$ に対して $dz = (ax + by)z = a(xz) + b(xz) \in I$ となるから.

となる. 適当な u, $v \in \mathbb{Z}$ をとって

$$z = ax + by$$

と書けば,

$$r = z - dq = a(u - xq) + b(v - yq) \in I.$$

ところが, d の最小性により $r = 0$ でなければならない. よって $z = dq \in d\mathbb{Z}$. ゆえに $I \subseteq d\mathbb{Z}$.

$a = a \cdot 1 + b \cdot 0$, $b = a \cdot 0 + b \cdot 1$ より a, $b \in I = d\mathbb{Z}$. よって d は a, b の公約数である. また, a, b の任意の公約数 w に対して

$$w \mid (ax + by) = d.$$

ゆえに d は a, b の最大公約数である. □

[定理 2.43] a, b, $c \in \mathbb{Z}$ とし, a, b の最大公約数を d をする. このとき, 次の 2 つの条件は同値である.

(i) ある x, $y \in \mathbb{Z}$ が存在して $ax + by = c$.
(ii) $d \mid c$.

[証明] I を前定理の通りとすると, (i) $\Leftrightarrow c \in I \Leftrightarrow c \in d\mathbb{Z} \Leftrightarrow$ (ii). □

a, b を整数とする. $\gcd(a, b) = 1$ が成り立つとき, a と b とは**互いに素**であるという.

[定理 2.44] a, $b \in \mathbb{Z}$, $m \in \mathbb{Z}^+$ とする. このとき

$$\gcd(ma, mb) = m \cdot \gcd(a, b)$$

が成り立つ.

[証明] $d = \gcd(a, b)$, $d' = \gcd(ma, mb)$ とおく.

適当な x, $y \in \mathbb{Z}$ をとって

$$d = ax + by$$

と書き, 両辺に m を掛けると,

$$md = (ma)x + (mb)y.$$

ゆえに $d' \mid md$.

逆に 適当な x', $y' \in \mathbb{Z}$ をとって

$$d' = (ma)x' + (mb)y'$$

と書けば,

$$d' = m(ax' + by').$$

$d \mid a$, $d \mid b$ より $d \mid ax' + by'$ であるから, $md \mid d'$. したがって $d' = md$. □

[定理 2.45] a, b, $c \in \mathbb{Z}$ とし, $\gcd(a,b) = 1$ とする. このとき, $a \mid bc$ ならば $a \mid c$.

[証明] $\gcd(a,b) = 1$ より, ある x, $y \in \mathbb{Z}$ が存在して

$$ax + by = 1.$$

両辺に c を掛ければ,

$$acx + bcy = c.$$

$a \mid bc$ であるから, この左辺は a の倍数である. ゆえに $a \mid c$. □

[定理 2.46] a, b, $c \in \mathbb{Z}$ とする. このとき

$$\gcd(a,b) = \gcd(a,c) = 1 \Longleftrightarrow \gcd(a,bc) = 1.$$

[証明] まず, $\gcd(a,b) = \gcd(a,c) = 1$ を仮定して $\gcd(a,bc) = 1$ を証明する. $d = \gcd(a,bc)$ とおくと, $d \mid a$, $d \mid bc$. もし仮に $\gcd(d,b) > 1$ ならば, $d \mid a$ より $\gcd(a,b) > 1$ となる. これは $\gcd(a,b) = 1$ に反する. よって $\gcd(d,b) = 1$. したがって前の定理より $d \mid c$. ところが, $d \mid a$ より d は a, c の公約数である. 仮定より $\gcd(a,c) = 1$ であったから, $d = 1$ でなければならない.

次に, $\gcd(a,b) > 1$ ならば $\gcd(a,bc) > 1$ となることは明らかである[10]. 同様に, $\gcd(a,c) > 1$ ならば $\gcd(a,bc) > 1$ となることも明らかである. よって,

$$\gcd(a,b) > 1 \text{ または } \gcd(a,c) > 1 \Longrightarrow \gcd(a,bc) > 1.$$

対偶をとれば

$$\gcd(a,bc) = 1 \Longrightarrow \gcd(a,b) = \gcd(a,c) = 1$$

となる. □

整数 a, $b \in \mathbb{Z}$ に対して, a と b の両方の倍数であるような整数のことを a と b の**公倍数**という. $l \in \mathbb{Z}$ が a と b の**最小公倍数**であるとは, 次の 3 つの条件が成り立つときにいう.

- l は a と b の公倍数である.
- a と b の任意の公倍数は l の倍数になる.
- $l > 0$.

a と b の最小公倍数を記号 $\mathrm{lcm}(a,b)$ で表す.

3 つ以上の整数に対しても, 同様にして公倍数, 最小公倍数を定義することができる. 例えば a, b, $c \in \mathbb{Z}$ に対して, a, b, c のそれぞれの倍数であるような整数を a, b, c の公倍数という. また, $l \in \mathbb{Z}$ が a, b, c の最小公倍数であるとは, 次の 3 つの条件が成り立つときにいう.

[10] $d = \gcd(a,b)$, $d' = \gcd(a,bc)$ とおく. $d \mid b$ ならば $d \mid bc$. よって $d \mid d'$ である. $d > 0$, $d' > 0$ だから, $d \leq d'$.

- l は a, b, c の公倍数である.
- a, b, c の任意の公倍数は l の倍数になる.
- $l > 0$.

a, b, c の最小公倍数を記号 $\mathrm{lcm}(a, b, c)$ で表す.

[定理 2.47] 任意の a, b, $c \in \mathbb{Z}$ に対して, 次のことが成り立つ.

(i) $\mathrm{lcm}(a, b) = \mathrm{lcm}(b, a)$.

(ii) $\mathrm{lcm}(a, b, c) = \mathrm{lcm}(\mathrm{lcm}(a, b), c)$.

[証明] (i) x を整数とする. 明らかに, x が a と b の公倍数であることと, b と a の公倍数であることとは同値である. これより, a と b の任意の公倍数が l の倍数であることと, b と a の任意の公倍数が l の倍数であることとが同値であることも明らかである.

(ii) $l = \mathrm{lcm}(a, b, c)$, $l' = \mathrm{lcm}(\mathrm{lcm}(a, b), c)$, $l'' = \mathrm{lcm}(a, b)$ とおく.

$a \mid l$, $b \mid l$ より $l'' \mid l$. また, $c \mid l$. ゆえに $l' \mid l$. 逆に, $l'' \mid l'$ であり, $a \mid l''$ だから $a \mid l'$. 同様に $b \mid l'$. 一方, $c \mid l'$ でもある. したがって $l \mid l'$. ゆえに, $l \mid l'$ かつ $l' \mid l$ より, $l = l'$. ここで, $l > 0$, $l' > 0$ であることに注意せよ. □

[定理 2.48] a, $b \in \mathbb{Z}^+$ の最大公約数を d, 最小公倍数を l とする. このとき

$$ab = dl$$

が成り立つ.

[証明] $a = a'd$, $b = b'd$ とおく.

$$d = \gcd(a, b) = \gcd(a'd, b'd) = d \cdot \gcd(a', b').$$

$d > 0$ なので $\gcd(a', b') = 1$. 一方, l は a の倍数であるから, ある $k \in \mathbb{Z}^+$ が存在して

$$l = ak = a'kd.$$

l は b の倍数でもあるから, $b \mid a'kd$ である. $b = b'd$ より $b'd \mid a'kd$ であり, $d \neq 0$ より $b' \mid a'k$ が得られる. $\gcd(a', b') = 1$ であるから, $b' \mid k$ である. したがって, ある $t \in \mathbb{Z}^+$ が存在して $k = b't$. このとき,

$$l = ak = ab't = a'db't = a'bt.$$

ゆえに,

$$\frac{l}{t} = ab' = ba'.$$

したがって l/t は a, b の公倍数である. l が最小公倍数であることから l は l/t の約数, よって $l \leq l/t$. したがって $t = 1$ でなければならない[11]. ゆえに $ab = ld$ が得られる. □

[11] $l > 0$, $t > 0$ のとき, $l/t < l \Leftrightarrow l < lt \Leftrightarrow l(t-1) > 0 \Leftrightarrow t - 1 > 0 \Leftrightarrow t > 1$.

2.8 素因数分解

$n \in \mathbb{Z}$, $n > 1$ とする.

n の正の約数が 1 と n だけであるとき, n は**素数**であるといい, そうでないとき, n は**合成数**であるという.

素数全体からなる集合を $\mathbb{P}$ とおく.

[定理 2.49] $p \in \mathbb{P}$, a, $b \in \mathbb{Z}$ とする. このとき

$$p \mid ab \Rightarrow p \mid a \text{ または } p \mid b.$$

[証明] 任意の $n \in \mathbb{Z}_{>0}$ に対して,

$$\gcd(p, n) = 1 \Leftrightarrow p \nmid n$$

が成り立つことに注意する.

$$\gcd(p, a) = \gcd(p, b) = 1 \Rightarrow \gcd(p, ab) = 1$$

なので

$$p \nmid a \text{ かつ } p \nmid b \Rightarrow p \nmid ab.$$

対偶をとれば

$$p \mid ab \Rightarrow p \mid a \text{ または } p \mid b.$$

□

[命題 2.50] $p \in \mathbb{P}$, $a_1, \ldots, a_n \in \mathbb{Z}_{>0}$ とする.

このとき, $p \mid (a_1 \cdots a_n)$ ならば, p はいずれかの a_i を割り切る.

[証明] n に関する数学的帰納法によって証明する.

$n = 2$ のときは上の定理より明らか.

$n = k$ のとき主張が成り立つと仮定する.

$p \mid (a_1 \cdots a_k a_{k+1})$ ならば, 上の定理より, $p \mid (a_1 \cdots a_k)$ または $p \mid a_{k+1}$ である.

$p \mid a_{k+1}$ ならば, これ以上すべきことはない.

$p \nmid a_{k+1}$ ならば $p \mid (a_1 \cdots a_k)$ である. 帰納法の仮定により p は $a_1, \ldots a_k$ のうちのいずれかを割り切る.

したがって, p は $a_1, \ldots a_k, a_{k+1}$ のいずれかを割り切る.

以上より, すべての n について系の主張が成り立つことが示された. □

[定理 2.51] $n \in \mathbb{Z}$, $n > 1$ とする.

n は素数の積として表せる. しかもその表し方は積の順序を除いて一意的である.

[証明] まず, n が素数の積として表せることを, n に関する数学的帰納法によって証明する.

$n = 2$ のとき, 2 は素数である.

$2 \leq k \leq n$ であるようなすべての $k \in \mathbb{Z}$ について, k が素数の積として表せると仮定する.

$n+1$ が素数ならば, これ以上すべきことはない.

$n+1$ が合成数ならば, 適当な l, $m \in \mathbb{Z}_{>0}$ をとって

$$n+1 = lm, \quad 2 \leq l < n+1, \quad 2 \leq m < n+1$$

と書ける. 帰納法の仮定から, l, m はそれぞれ素数の積で表せる. したがって $n+1$ も素数の積で表せる.

以上より, すべての $n \in \mathbb{Z}$, $n > 1$ について, n が素数の積として表せることが示された.

次に, 表し方の一意性を証明する.

上に述べたことから, $n \in \mathbb{Z}$, $n > 1$ なる任意の n に対して, ある $k \in \mathbb{Z}_{>0}$ が存在して, n は k 個の素数の積で表すことができる:

$$n = p_1 p_2 \cdots p_k.$$

そこで, k に関する数学的帰納法によって, 表し方の一意性を証明する.

n が素数のとき, $n = p_1 p_2 \cdots p_k$ (p_i は素数) と書けたとすると, $k = 1$, $p_1 = n$ でなければならない.

n が少なくとも k 個の素数の積で書けるならば, 表し方は一意的であると仮定する.

$$n = p_1 p_2 \cdots p_{k+1} = q_1 q_2 \cdots q_l, \quad p_i,\ q_j \text{ は素数}$$

のとき, 帰納法の仮定から $k+1 \leq l$ である. $p_1 \mid (q_1 q_2 \cdots q_l)$ より, ある i について $p_1 \mid q_i$. 積の順序を考えなければ, $p_1 \mid q_1$ としてもよい. q_1 は素数だから, $p_1 = q_1$. よって

$$\frac{n}{p_1} = p_2 \cdots p_{k+1} = q_2 \cdots q_l.$$

帰納法の仮定より, $l = k+1$, $p_i = q_i$ でなければならない.

以上より, すべての k に関して, 表し方の一意性が証明された.

したがって, すべての $n \in \mathbb{Z}$, $n > 1$ について, n の素数の積での表し方は一意的である. □

整数 n ($n > 1$) を素数の積として表すことを, n の**素因数分解**という.

また, n を割り切る素数を n の**素因数**という.

[定理 2.52] 素数は無限に存在する.

［証明］ 背理法により証明する.

いま, 素数が有限個しかないと仮定し, p_1, p_2, …, p_k が素数のすべてであるとする.

$$n = p_1 p_2 \cdots p_k + 1$$

とおく.

n は素因数分解できる. よって n は素数の約数を持つ.

ところが, p_1, p_2, …, p_k はすべて n を割らない. これは n が素数の約数を持つことに反する.

したがって素数は無限に存在する. □

3　有理数

3.1　商体

$\mathbb{Z}$ から $\mathbb{Q}$ を構成するにあたって, より一般的に, 整域から体を構成する方法について述べる.

この節の全体を通じて, R は整域を表すものとする.

$R^* = R \setminus \{0\}$ とおく. すなわち, 任意の $x \in R$ について

$$x \in R^* \Longleftrightarrow x \neq 0.$$

R^* は整域だから, 任意の $y,\ w \in R^*$ に対して $yw \in R^*$ であること, すなわち任意の $y,\ w \in R$ に対して, $y \neq 0$ かつ $w \neq 0$ ならば, $yw \neq 0$ であることに注意せよ.

$R \times R^*$ 上の 2 項関係 $\sim$ を, 各 $(x, y),\ (z, w) \in R \times R^*$ に対して

$$(x, y) \sim (z, w) \Longleftrightarrow xw = zy$$

によって定める.

[命題 3.1] $\sim$ は $R \times R^*$ 上の同値関係である.

[証明] $x,\ y,\ z,\ w,\ u,\ v \in R$ とする.

$xy = xy$ より $(x, y) \sim (x, y)$. したがって $\sim$ に関して反射法則が成り立つ.

$(x, y) \sim (z, w) \Rightarrow xw = zy \Rightarrow zy = xw \Rightarrow (z, w) \sim (x, y)$. したがって $\sim$ に関して対称法則が成り立つ.

$(x, y) \sim (z, w),\ (z, w) \sim (u, v)$ を仮定すれば,

$$xw = zy, \quad zv = uw.$$

$z \neq 0$ のとき, これらの式を辺々乗じると

$$xwzv = zyuw.$$

R の乗法に関する結合法則, 交換法則により

$$zw(xv - uz) = 0.$$

$zw \neq 0$ より, $xv - uz = 0$. よって $xv = uz$.

$z = 0$ のとき, $xw = uw = 0$ であるが, $w \in R^*$ すなわち $w \neq 0$ より, $x = u = 0$. よって $xv = uz$ が成り立つ.

ゆえに $(x, y) \sim (u, v)$. したがって $\sim$ に関して推移法則が成り立つ. □

直積集合 $R \times R^*$ を同値関係 $\sim$ により類別した同値類の集合を K とおく:

$$K = R \times R^* / \sim$$

また, $(x, y) \in R \times R^*$ を代表元とする K の同値類を $[x, y]$ と書く. つまり,

$$K = \{[x, y] \mid x, y \in R\}.$$

このとき, 任意の x, y, z, $w \in R$ に対して

$$[x, y] = [z, w] \Longleftrightarrow (x, y) \sim (z, w) \Longleftrightarrow xw = zy$$

が成り立つ.

[補題 3.2] (i) 任意の $x \in R$, $y \in R^*$ に対して, $[x, y] = [0, 1] \Longleftrightarrow x = 0$.
(ii) 任意の $x \in R$, $y \in R^*$ に対して, $[x, y] = [1, 1] \Longleftrightarrow x = y$.
(iii) 任意の $x \in R$, y, $w \in R^*$ に対して $[xw, yw] = [x, y]$.

[証明] (i) $[x, y] = [0, 1]$ と仮定すると, $x = x \cdot 1 = 0 \cdot y = 0$. 逆は明らか.
(ii) $[x, y] = [1, 1]$ と仮定すると, $x = x \cdot 1 = 1 \cdot y = y$. 逆は明らか.
(iii) R の乗法に関する結合法則と交換法則より $(xw)y = x(yw)$. □

K の各元 $[x, y]$, $[z, w]$, x, $z \in R$, y, $w \in R^*$ に対して, それらの和と積をそれぞれ

$$[x, y] + [z, w] = [xw + zy, yw], \quad [x, y][z, w] = [xz, yw]$$

によって定義する.

[命題 3.3] K は体になる.

[証明] x, z, x', z', $u \in R$, y, w, y', w', $v \in R^*$ とする. 以下, R の加法, 乗法に関する結合法則, 交換法則, 分配法則を利用して計算する.

まず, K の加法が体であるための条件を満たすことを確認する.

$$\begin{aligned}
[x, y] = [x', y'], [z, w] = [z', w'] &\Longrightarrow xy' = x'y,\ zw' = z'w \\
&\Longrightarrow xy'ww' + zw'yy' = x'yww' + z'wy'y \\
&\Longrightarrow (xw + zy)y'w' = (x'w' + z'y')(yw) \\
&\Longrightarrow [xw + zy, yw] = [x'w' + z'y', y'w'].
\end{aligned}$$

よって K の加法は well-defined である.

$$\begin{aligned}
([x, y] + [z, w]) + [u, v] &= [xw + zy, yw][u, v] = [(xw + zy)v + (yw)u, ywv] \\
&= [xwv + zyv + ywu, ywv] = [x(wv) + (zv + uw)y, ywv] \\
&= [x, y] + [zv + uw, wv] = [x, y] + ([z, w] + [u, v]).
\end{aligned}$$

よって K は加法に関して結合法則を満たす.

$$\begin{aligned}[x,y]+[z,w] &= [xw+zy, yw] = [zy+xw, wy] \\ &= [z,w]+[x,y].\end{aligned}$$

よって K は加法に関して交換法則を満たす.

R の零元を 0 とするとき, K の単位元は $[0,1]$ である. 実際

$$[x,y]+[0,1] = [x\cdot 1 + 0\cdot y, y\cdot 1] = [x,y].$$

$[x,y]$ の加法における逆元は $[-x,y]$ である. 実際,

$$[x,y]+[-x,y] = [xy+(-x)y, yy] = [0,yy] = [0,1].$$

次に, K の乗法が体であるための条件を満たすことを確認する.

$$\begin{aligned}[x,y]=[x',y'],\ [z,w]=[z',w'] &\Longrightarrow xy'=x'y,\ zw'=z'w \\ &\Longrightarrow (xy')(zw')=(x'y)(z'w) \\ &\Longrightarrow (xz)(y'w')=(x'z')(yw) \\ &\Longrightarrow [xz,yw]=[x'z',y'w'].\end{aligned}$$

よって K の乗法は well-defined である.

$$\begin{aligned}([x,y][z,w])[u,v] &= [xz,yw][u,v] = [xzu, ywv] \\ &= [x,y]+[zu,wv] = [x,y]([z,w][u,v]).\end{aligned}$$

よって K も乗法に関して結合法則を満たす.

$$[x,y]+[z,w] = [xz,yw] = [zx,wy] = [z,w]+[x,y].$$

よって K も乗法に関して交換法則を満たす.

R の乗法における単位元を 1 とするとき, K の単位元は $[1,1]$ である. 実際

$$[x,y][1,1] = [x\cdot 1, y\cdot 1] = [x,y].$$

$[y,w]$ の乗法に関する逆元は $[w,y]$ である. 実際,

$$[y,w][w,y] = [yw,wy] = [yw,yw] = [1,1].$$

ここで, 上の補題の (i) より, $[x,y]$ が零元でないための必要十分条件は $x\in R^*$ であることに注意せよ.

最後に, 上の補題の (ii) を用いると

$$\begin{aligned}[x,y][z,w]+[x,y][u,v] &= [xz,yw]+[xu,yv] = [xzyv+xuyw, ywyv]\\ &= [yx(zv+uw), y(ywv)] = [x(zv+uw), ywv]\\ &= [x,y][zv+uw, wv] = [x(zv+uw), ywv]\\ &= [x,y]([z,w]+[u,v]).\end{aligned}$$

よって K の加法と乗法に関して分配法則が成り立つ.

以上より, K が体であることが示された. □

各 $x \in R$ に対して

$$\varphi(x) = [x,1]$$

とおくことにより写像 $\varphi : R \to K$ を定義する.

[補題 3.4] 任意の $x \in R$, $y \in R^*$ に対して $[x,y] = \varphi(x)\varphi(y)^{-1}$.

[証明] $[x,y] = [x,1][1,y] = [x,1][y,1]^{-1} = \varphi(x)\varphi(y)^{-1}$. □

[定理 3.5] φ は単射準同型である. したがって特に, R は K の部分環である.

[証明] a, $b \in R$ とする.

$$\varphi(a) = \varphi(b) \Longrightarrow [a,1] = [b,1] \Longrightarrow a \cdot 1 = b \cdot 1 \Longrightarrow a = b.$$

よって, φ は単射である. また,

$$\begin{aligned}\varphi(a)+\varphi(b) &= [a,1]+[b,1] = [a\cdot 1 + b\cdot 1, 1\cdot 1] = [a+b,1] = \varphi(a+b),\\ \varphi(a)\varphi(b) &= [a,1]+[b,1] = [ab, 1\cdot 1] = [ab,1] = \varphi(ab).\end{aligned}$$

よって, φ は準同型である. □

[定理 3.6] L が体で, $\psi : R \to L$ を単射準同型とすると, 準同型 $g : K \to L$ で

$$\psi = g \circ \varphi$$

を満たすものがただ一つ存在する.

[証明] x, $z \in R$, y, $w \in R^*$ とする.

$[x,y] = [z,w]$ とすると, $xw = zy$ である. ψ は準同型だから

$$\psi(x)\psi(w) = \psi(xw) = \psi(zy) = \psi(z)\psi(y).$$

ψ は単射であり, $y \neq 0$, $w \neq 0$ であるから, $\psi(y) \neq 0$, $\psi(w) \neq 0$ である. よって L においてこれらの元に対する逆元が存在し,

$$\psi(x)\psi(y)^{-1} = \psi(z)\psi(w)^{-1}$$

を得る. そこで,

$$g([x,y]) = \psi(x)\psi(y)^{-1}$$

によって写像 $g : K \to L$ を定義すれば, この値は x, y の選び方によらない. つまり g は well-defined である. また,

$$\begin{aligned} g([x,y][z,w]) = g([xz,yw]) &= \psi(xz)\psi(yw)^{-1} \\ &= (\psi(x)\psi(z))(\psi(w)\psi(y))^{-1} \\ &= \psi(x)\psi(z)\psi(y)^{-1}\psi(w)^{-1} \\ &= \psi(x)\psi(y)^{-1}\psi(z)\psi(w)^{-1} \\ &= g([x,y])g([z,w]) \end{aligned}$$

が成り立つ. よって g は準同型である. さらに, $\psi(1) = 1$ だから,

$$g \circ \varphi(x) = g([x,1]) = \psi(x)\psi(1)^{-1} = \psi(x).$$

よって $g \circ \varphi = \psi$ が成り立つ.

次に, $g' : K \to L$ を準同型とし, $g' \circ \varphi = \psi$ をみたすものとすると, $[x,y] = \varphi(x)\varphi(y)^{-1}$ であるから,

$$\begin{aligned} g'([x,y]) = g'(\varphi(x)\varphi(y)^{-1}) &= g'(\varphi(x))\, g'(\varphi(y))^{-1} \\ &= \psi(x)\psi(y)^{-1} = g(\varphi(x))\, g(\varphi(y))^{-1} \\ &= g(\varphi(x)\varphi(y)^{-1}) = g([x,y]) \end{aligned}$$

を得る. x, y の取り方は任意であるから, $g = g'$ となる. □

[定理 3.7] K は, 整域 R を部分環とする体のうちで最小のものである.

[証明] L を, R を部分環とする体であるとすれば, R から L への単射準同型が存在する. それを ψ で表すことにする. 前定理より準同型 $g : K \to L$ で

$$\psi = g \circ \varphi$$

となるものがただ一つ存在する.

$x,\ z \in R,\ y,\ w \in R^*$ とし, $g([x,y]) = g([z,w])$ とする. このとき, 上の補題より $[x,y] = \varphi(x)\varphi(y)^{-1}$, $[z,w] = \varphi(z)\varphi(w)^{-1}$ であるから,

$$g([x,y]) = g(\varphi(x)\varphi(y)^{-1}) = g(\varphi(x))\, g(\varphi(y))^{-1} = \psi(x)\psi(y)^{-1},$$
$$g([z,w]) = g(\varphi(z)\varphi(w)^{-1}) = g(\varphi(z))\, g(\varphi(w))^{-1} = \psi(z)\psi(w)^{-1}.$$

これらより,

$$\psi(x)\psi(y)^{-1} = g([x,y]) = g([z,w]) = \psi(z)\psi(w)^{-1}.$$

したがって $\psi(x)\psi(w) = \psi(z)\psi(y)$ となる. ψ は単射準同型だから,

$$\begin{aligned}\psi(x)\psi(w) = \psi(z)\psi(y) &\Longrightarrow \psi(xw) = \psi(zy)\\ &\Longrightarrow xw = zy\\ &\Longrightarrow [x,y] = [z,w].\end{aligned}$$

ゆえに g は単射である.

よって, 整域 R を含む体 L はすべて, K を部分環とすることがわかる.

一方, 前の前の定理より K 自身が R を部分環とする体である. したがって K は, R を部分環とする体のうちで最小のものである. □

K を整域 R の**商体**と呼ぶ.

3.2 有理数の構成

整数の全体からなる集合 $\mathbb{Z}$ は整域である. したがって, 前節の定理より $\mathbb{Z}$ の商体, すなわち $\mathbb{Z}$ を部分環とする最小の体

$$\mathbb{Q} = \mathbb{Z} \times \mathbb{Z}^* / \sim = \{[a,b] \mid a,b \in \mathbb{Z}, b \neq 0\}$$

が存在する. $\mathbb{Q}$ の元を**有理数**という.

単射準同型 $\varphi : \mathbb{Z} \to \mathbb{Q}$ による $a \in \mathbb{Z}$ の像は $[a,1]$ である. そこで, $a = [a,1]$ であるとみなす. 特に, $0 = [0,1]$ は $\mathbb{Q}$ の零元であり, $1 = [1,1]$ は乗法における単位元である.

任意の $a \in \mathbb{Z}$ に対して,

$$[a,1] + [-a,1] = [a \cdot 1 + (-a) \cdot 1, 1 \cdot 1] = [a-a,1] = [0,1]$$

となるから, $[-a,1]$ は $\mathbb{Q}$ の加法における $[a,1]$ の逆元である. すなわち $[-a,1] = -[a,1] = -a$ である. また, $a \neq 0$ ならば,

$$[a,1][1,a] = [a \cdot 1, 1 \cdot a] = [a,a] = [1,1]$$

となるから, $[1,a]$ は $\mathbb{Q}$ の加法における $[a,1]$ の逆元である. すなわち $[1,a] = [a,1]^{-1} = a^{-1}$ である.

さらに, 任意の a, $b \in \mathbb{Z}$, $b \neq 0$ に対して,

$$[a, b] = [a, 1][1, b] = ab^{-1}.$$

したがって

$$\mathbb{Q} = \{ab^{-1} \mid a, b \in \mathbb{Z}, b \neq 0\}$$

と表すことができる.

$\mathbb{Q}$ の加法と乗法が満たす主な性質をまとめておく.

- 零元の存在と一意性:ある $0 \in \mathbb{Q}$ がただ1つ存在して, 任意の $x \in \mathbb{Q}$ に対して, $x+0 = 0+x = 0$.
- 加法における逆元の存在と一意性：任意の $x \in \mathbb{Q}$ に対して, ある $-x \in \mathbb{Q}$ がただ 1 つ存在して, $x + (-x) = (-x) + x = 0$.
- 加法における結合法則：任意の x, y, $z \in \mathbb{Q}$ に対して, $(x + y) + z = x + (y + z) = 0$.
- 加法における交換法則：任意の x, $y \in \mathbb{Q}$ に対して, $x + y = y + x$.
- 乗法における単位元の存在と一意性：ある $1 \in \mathbb{Q}$ がただ 1 つ存在して, 任意の $x \in \mathbb{Q}$ に対して, $x + 1 = 1 + x = 0$.
- 乗法における逆元の存在と一意性：任意の $x \in \mathbb{Q}$ に対して, ある $x^{-1} \in \mathbb{Q}$ がただ 1 つ存在して, $xx^{-1} = x^{-1}x = 1$.
- 乗法における結合法則：任意の x, y, $z \in \mathbb{Q}$ に対して, $(xy)z = x(yz) = 0$.
- 乗法における交換法則：任意の x, $y \in \mathbb{Q}$ に対して, $xy = yx$.
- 分配法則：任意の x, y, $z \in \mathbb{Q}$ に対して, $x(y + z) = xy + xz$, $(x + y)z = xz + yz$.

慣例にしたがって, 任意の x, $y \in \mathbb{Q}$, $y \neq 0$ に対して,

$$\frac{x}{y} = xy^{-1}$$

と定める. すると,

$$\frac{1}{y} = 1 \cdot y^{-1} = y^{-1}$$

となる.

特に, 任意の a, $b \in \mathbb{Z}$, $b \neq 0$ に対して, $[a, b] = a/b$ であり,

$$\mathbb{Q} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z}, b \neq 0 \right\}$$

と表せる. また, 任意の整数 $a \in \mathbb{Z}$ に対して, $a = a/1$ と表せる.

[命題 3.8] 任意の a, b, $c \in \mathbb{Z}$ に対して, $b \neq 0$, $c \neq 0$ ならば,

$$\frac{a}{b} = \frac{ac}{bc}$$

が成り立つ.

[証明] $a(bc) = (ac)b$ となることからわかる. □

[命題 3.9] 任意の $x \in \mathbb{Q}$ に対して, ある a, $b \in \mathbb{Z}$, $b > 0$ が存在して, $x = a/b$.

[証明] (i) $x \in \mathbb{Q}$ とすると, ある a, $b \in \mathbb{Z}$, $b \neq 0$ が存在して $x = a/b$ と書ける. $a(-b) = (-a)b$ なので, $b < 0$ のとき, $x = a/b = (-a)/(-b)$, $-b > 0$ となる. □

[定理 3.10] $x \in \mathbb{Q}$ とする. このとき, ある a_0, $b_0 \in \mathbb{Z}$, $b_0 > 0$ が一意的に存在して,

$$x = \frac{a_0}{b_0}, \quad \gcd(a_0, b_0) = 1$$

が成り立つ. またこのとき,

$$b_0 = \min\{b \in \mathbb{Z} \mid b > 0 \text{ かつ, ある } a \in \mathbb{Z} \text{ が存在して } x = a/b\}$$

である. 有理数 x がこのように表されるとき, a_0/b_0 を x の**既約分数による表示**といい, x は既約分数 a_0/b_0 で表されるという.

[証明] 前の命題より, ある a, $b \in \mathbb{Z}$, $b > 0$ が存在して, $x = a/b$. 一方, $d = \gcd(a, b)$ とおき, $a_0 = a/d$, $b_0 = b/d$ とおくと,

$$d = \gcd(a, b) = \gcd(a_0 d, b_0 d) = d \cdot \gcd(a_0, b_0)$$

より $\gcd(a_0, b_0) = 1$ が得られる. さらに,

$$x = \frac{a}{b} = \frac{a_0 d}{b_0 d} = \frac{a_0}{b_0}.$$

となる[12)].

次に, a_0, b_0, a_0', $b_0' \in \mathbb{Z}$, $b_0 > 0$, $b_0' > 0$ とし,

$$x = \frac{a_0}{b_0}, \quad \gcd(a_0, b_0) = 1,$$
$$x = \frac{a_0'}{b_0'}, \quad \gcd(a_0', b_0') = 1$$

であるとする. このとき, $a_0 b_0' = a_0' b_0$ である. $\gcd(a_0, b_0) = 1$ より, $b_0 \mid b_0'$ でなければならない. 同様に, $\gcd(a_0', b_0') = 1$ より, $b_0' \mid b_0$ でなければならない. $b_0 > 0$, $b_0' > 0$ であるから, $b_0 = b_0'$ が得られ, さらに $a_0 = a_0'$ も得られる. これで一意性が示された.

$$B_x = \{b \in \mathbb{Z} \mid b > 0 \text{ かつ, ある } a \in \mathbb{Z} \text{ が存在して } x = a/b\}$$

とおくと, $B_x \subseteq \mathbb{N}$ であり, 前の命題より $B_x \neq \emptyset$ である. よって $\mathbb{N}$ の整列性により最小元 b' が存在する. また, ある $a' \in \mathbb{Z}$ が存在して $x = a'/b'$ と書ける. $d' = \gcd(a', b')$ とおくとき, もし仮に $d' > 1$ ならば, $a'' = a'/d'$, $b'' = b'/d'$ とおくと, $x = a''/b''$, $b' > b'' > 0$ となって b' の最小性に反する. したがって $d' = 1$. さらに, 上で示した一意性により $b' = b_0$ となる. □

[12)] ここで, 最大公約数 d は正の整数であることに注意せよ.

[命題 3.11] $x \in \mathbb{Q}$ とし, a_0/b_0 を x の既約分数による表示とする. このとき, 任意の a, $b \in \mathbb{Z}$, $b > 0$ に対して, $x = a/b$ ならば, $d = \gcd(a, b)$ とおくと $a = a_0 d$, $b = b_0 d$ となる.

[証明] $d = \gcd(a, b)$ とおき, $a' = a/d$, $b' = b/d$ とおくと,

$$x = \frac{a'}{b'}, \quad \gcd(a', b') = 1$$

となり, x は既約分数 a'/b' で表される. 既約分数による表示の一意性により, $a_0 = a'$, $b_0 = b'$ となる. したがって $a = a_0 d$, $b = b_0 d$. □

[命題 3.12] (i) 任意の $a \in \mathbb{Z}$ に対して, $a/1$ は a の既約分数による表示である.
(ii) 任意の b, $c \in \mathbb{Z}$, $b \neq 0$ に対して,

$$\frac{c}{b} \in \mathbb{Z} \Longleftrightarrow c \text{ は } b \text{ の倍数}$$

が成り立つ.

[証明] (i) $\mathbb{Q}$ が $\mathbb{Z}$ の商体であることから, $a = a/1$ であることは明らかである. また,

$$B_x = \{b \in \mathbb{Z} \mid b > 0 \text{ かつ, ある } a \in \mathbb{Z} \text{ が存在して } x = a/b\}$$

とおくと, $1 \in B_x$ である. 1 が B_x の最小元であることはすぐにわかる[13]. よって $a/1$ は a の既約分数による表示である.

(ii) $a = c/b$ とおく. (i) より, c/b の既約分数による表示は $a/1$ である. 前の命題から, $d = \gcd(c, b)$ とおくと $c = ad$, $b = 1 \cdot d = d$ となる. よって $c = ab$. 逆に, c が b の倍数ならば, ある $t \in \mathbb{Z}$ が存在して $c = tb$ となる. よって $c/b = (tb)/b = t/1 = t$. □

3.3 有理数の順序

x, $y \in \mathbb{Q}$ とし, a/b, c/d をそれぞれ x, y の既約分数による表示とする. このとき, 関係 $\leq$ を次のように定義する.

$$x \leq y \Longleftrightarrow bc - ad \geq 0.$$

$x \leq y$ のことを $y \geq x$ と書くこともある.

[定理 3.13] 任意の $x \in \mathbb{Q}$ に対して, $x \leq x$ が成り立つ.

[証明] $x = a/b$ を既約分数による表示とするとき, $ba - ab = 0$ となることからわかる. □

[13] 任意の $b \in B_x$ に対して, $b > 0$ より $b \in \mathbb{N}$ かつ $b \neq 0$ であるから, ある $n \in \mathbb{N}$ が存在して $b = n + 1$, すなわち $b \geq 1$.

[定理 3.14] 任意の $x, y, z \in \mathbb{Q}$ に対して, $x \leq y$ かつ $y \leq z$ ならば, $x \leq z$ が成り立つ.

[証明] a/b, c/d, e/f をそれぞれ x, y, z の既約分数による表示とする. このとき,

$$\begin{aligned} x \leq y,\, y \leq z &\Longrightarrow bc - ad \geq 0,\, de - cf \geq 0 \\ &\Longrightarrow bcf - adf \geq 0,\, bde - bcf \geq 0 \\ &\Longrightarrow bde - adf \geq 0 \\ &\Longrightarrow be - af \geq 0 \\ &\Longrightarrow x \leq z \end{aligned}$$

となる. □

[定理 3.15] 任意の $x, y \in \mathbb{Q}$ に対して, $x \leq y$ かつ $y \leq x$ ならば, $x = y$ が成り立つ.

[証明] a/b, c/d をそれぞれ x, y の既約分数による表示とする. このとき,

$$\begin{aligned} x \leq y,\, y \leq x &\Longrightarrow bc - ad \geq 0,\, da - cb \geq 0 \\ &\Longrightarrow cb - ad \geq 0,\, cb - ad \leq 0 \\ &\Longrightarrow cb - ad = 0 \\ &\Longrightarrow ad = cb \\ &\Longrightarrow x = y \end{aligned}$$

となる. □

以上より, $\leq$ が実際に $\mathbb{Q}$ 上の順序関係であること, すなわち反射法則, 推移法則, 対称法則が成り立つことが示された.

二つの有理数 x, y について, $x \leq y$ かつ $x \neq y$ であることを $x < y$ や $y > x$ で表す. このとき, y は x より**大きい**といい, x は y より**小さい**という.

$x, y \in \mathbb{Z}$ とし, a/b, c/d をそれぞれ x, y の既約分数による表示とする. このとき, $x = y$ であることの定義から

$$x = y \Longleftrightarrow ad = cb \Longleftrightarrow bc - ad = 0.$$

さらに,

$$x < y \Longleftrightarrow x \leq y \text{ かつ } x \neq y \Longleftrightarrow bc - ad > 0.$$

このことを用いると, $\leq$ を $<$ に置き換えることで, 上の定理の証明と同様にして

$$x < y \text{ かつ } y < z \Longrightarrow x < z$$

を示すことができる.

[定理 3.16] 任意の x, $y \in \mathbb{Z}$ に対して, $x < y$, $x = y$, $x > y$ のいずれか一つ, しかも一つだけが成り立つ.

[証明] a/b, c/d をそれぞれ x, y の既約分数による表示とする. このとき,

$$\begin{aligned} x < y &\Longleftrightarrow bc - ad > 0, \\ x = y &\Longleftrightarrow bc - ad = 0, \\ x > y &\Longleftrightarrow da - bc > 0 \Longleftrightarrow bc - ad < 0. \end{aligned}$$

一方, $\mathbb{Z}$ において $bc - ad > 0$, $bc - ad = 0$, $bc - ad < 0$ のいずれか一つ, しかも一つだけが成り立つ. □

[定理 3.17] 任意の x, y, $z \in \mathbb{Q}$ に対して,

$$x < y \Longleftrightarrow x + z < y + z$$

が成り立つ.

[証明] x, y, z の既約分数による表示を a/b, c/d, e/f とする. まず,

$$\begin{aligned} x + z &= \frac{af + eb}{bf}, \\ y + z &= \frac{cf + ed}{df}. \end{aligned}$$

よって, $f > 0$ より

$$\begin{aligned} x + z < y + z &\Longleftrightarrow (cf + ed)bf - (af + eb)df > 0 \\ &\Longleftrightarrow (bc - ad)ff > 0 \\ &\Longleftrightarrow bc - ad > 0 \\ &\Longleftrightarrow x < y \end{aligned}$$

となる. □

[定理 3.18] 任意の x, y, $z \in \mathbb{Q}$ に対して, $z > 0$ ならば,

$$x < y \Longleftrightarrow xz < yz$$

が成り立つ.

[証明] x, y, z の既約分数による表示を a/b, c/d, e/f とする．まず，

$$xz = \frac{ae}{bf},$$
$$yz = \frac{ce}{df}.$$

$z > 0$ より，$e > 0$, $f > 0$ だから，$ef > 0$. よって

$$\begin{aligned} xz < +z &\iff cebf - aedf > 0 \\ &\iff (bc - ad)ef > 0 \\ &\iff bc - ad > 0 \\ &\iff x < y \end{aligned}$$

となる． □

[定理 3.19] 任意の x, $y \in \mathbb{Q}$ に対して，$x < y$ ならば，ある $z \in \mathbb{Q}$ が存在して $x < z < y$ が成り立つ．この性質を $\mathbb{Q}$ の**稠密性**という．

[証明] a/b, c/d をそれぞれ x, y の既約分数による表示とする．$b > 0$, $d > 0$ より $b + d > 0$. そこで，

$$z = \frac{a + c}{b + d}$$

とおく．$x < y$ より，$bc - ad > 0$ である．よって

$$b(a + c) - a(b + d) = bc - ad > 0,$$
$$(b + d)c - (a + c)d = bc - ad > 0.$$

したがって $x < z < y$. □

3.4 有理数の絶対値

各 $x \in \mathbb{Q}$ に対して，ある a, $b \in \mathbb{Z}$, $b \neq 0$ によって $x = a/b$ と表すとき，絶対値 $|x|'$ を

$$|x|' = \frac{|a|}{|b|}$$

によって定義する．ここで，右辺の $|*|$ は $\mathbb{Z}$ における絶対値である．特に，$b > 0$ ならば $|x|' = |a|/b$ である．

この定義は a, b の選び方によらない．実際，$b > 0$ のとき，x の既約分数による表示を a_0/b_0 とし，$d = \gcd(a, b)$ とすれば，$a = a_0 d$, $b = b_0 d$ が成り立つ．よって，整数の絶対値の性質から

$$\frac{|a|}{|b|} = \frac{|a_0 d|}{|b_0 d|} = \frac{|a_0|d}{|b_0|d} = \frac{|a_0|}{|b_0|}$$

となる. さらに, $b<0$ のときは, $x=a/b=(-a)/(-b)$ と $b>0$ のときの結果を用いて

$$\frac{|a|}{|b|}=\frac{|-a|}{|-b|}=\frac{|a_0|}{|b_0|}$$

が得られる.

任意の $a\in\mathbb{Z}$ に対して, $a=a/1$ だから,

$$|a|'=\left|\frac{a}{1}\right|'=\frac{|a|}{1}=|a|.$$

したがって, 有理数の絶対値は整数の絶対値の拡張になっている. そこで, 有理数の絶対値もまた $|*|$ で表すことにする.

[命題 3.20] 任意の $x\in\mathbb{Q}$ に対して,

$$|x|=\begin{cases}x & x>0 \text{ のとき}\\ 0 & x=0 \text{ のとき}\\ -x & x<0 \text{ のとき}\end{cases}$$

が成り立つ.

[証明] x の既約分数による表示を a/b とするとき, $b>0$ なので,

$$x>0\Longleftrightarrow a>0,$$
$$x=0\Longleftrightarrow a=0,$$
$$x<0\Longleftrightarrow a<0$$

であることから明らかである. 例えば, $x<0$ のとき, $a<0$ より $|a|=-a$ なので,

$$|x|=\frac{|a|}{b}=\frac{-a}{b}=-\frac{a}{b}=-x$$

となる. □

[命題 3.21] 任意の $x,\,y\in\mathbb{Q}$ に対して, 次が成り立つ.

(i) $|x|\geq 0$.
(ii) $|x|=0\Longleftrightarrow x=0$.
(iii) $x\leq|x|$.
(iv) $|-x|=|x|$.
(v) $|xy|=|x||y|$.
(vi) $y\neq 0$ ならば, $|x/y|=|x|/|y|$. 特に, $|1/y|=1/|y|$.

[証明] (i) 上の命題と, $x < 0$ ならば $-x > 0$ であることからわかる.

(ii) 上の命題から明らかである.

(iii) $x = 0$ または $x > 0$ のときは $|x| = x$ である. $x < 0$ のときは $x < 0 < |x|$ である.

(iv) $x = a/b$ を既約分数による表示とすると, $|-x| = |-a|/b = |a|/b = |x|$.

(v) $x = a/b$, $y = c/d$ を既約分数による表示とすると, $xy = (ac)/(bd)$, $bd > 0$ より,

$$|xy| = \frac{|ac|}{bd} = \frac{|a||c|}{bd} = \frac{|a|}{b}\frac{|c|}{d} = |x||y|$$

となる.

(vi) $y \cdot (x/y) = x$ であるから, (v) より $|y||x/y| = |x|$. 両辺を $|y|$ で割れば, $|x/y| = |x|/|y|$ が得られる. □

[定理 3.22] 任意の $x, y \in \mathbb{Q}$ に対して, 次が成り立つ.

(i) $|x + y| \leq |x| + |y|$. この不等式は**三角不等式**と呼ばれる.

(ii) $|x - y| \leq |x| + |y|$.

(iii) $|x| - |y| \leq |x + y|$.

(iv) $|x| - |y| \leq |x - y|$.

[証明] (i) $x \leq |x|$, $y \leq |y|$ より

$$x + y \leq |x| + |y|.$$

一方, $-x \leq |x|$, $-y \leq |y|$ より

$$-(x + y) \leq |x| + |y|.$$

$|x + y|$ は $x + y$ か $-(x + y)$ のどちらかに等しい. よって

$$|x + y| \leq |x| + |y|.$$

となる.

(ii) (i) において, y に $-y$ を代入すれば, $|-y| = |y|$ より (ii) が得られる.

(iii) (ii) において y に $x + y$ を代入すれば,

$$|x - (x + y)| \leq |x| + |x + y|.$$

これと $|-y| = |y|$ より (iii) が得られる.

(iv) (i) において x に $x - y$ を代入すれば,

$$|(x - y) + y| \leq |x - y| + |y|.$$

これより (iv) が得られる. □

4 実数

4.1 $\mathbb{Q}$ の Cauchy 列

X を集合とするとき, $\mathbb{N}$ から X への写像を X における**元の列**という. 写像

$$f : \mathbb{N} \longrightarrow X, \quad n \longmapsto f(n)$$

に対して, $x_n = f(n)$ とおくとき, f を $(x_n \mid n \in \mathbb{N})$ または (x_n) と書く. 特に, X が $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ のときには[14], (x_n) を**数列**という.

$\mathbb{Q}$ の元の列 (a_n) が $\mathbb{Q}$ の **Cauchy 列**であるとは, 任意の正の有理数 ε に対して, ある自然数 n_0 が存在して, 任意の自然数 m, n に対して, $m > n_0$ かつ $n > n_0$ ならば, $|a_m - a_n| < \varepsilon$ が成り立つときにいう. $\mathbb{Q}$ の Cauchy 列全体からなる集合を $\mathcal{C}$ とする.

[定理 4.1] (i) 任意の (a_n), $(b_n) \in \mathcal{C}$ に対して, $(a_n + b_n) \in \mathcal{C}$.
(ii) 任意の $(a_n) \in \mathcal{C}$ に対して, $(-a_n) \in \mathcal{C}$.

[証明] (i) (a_n), $(b_n) \in \mathcal{C}$ とすると, 任意の正の有理数 ε に対して, ある自然数 n_0, n_1 が存在して, 任意の自然数 m, n に対して

$$m > n_0, n > n_0 \Longrightarrow |a_m - a_n| < \frac{\varepsilon}{2},$$
$$m > n_1, n > n_1 \Longrightarrow |b_m - b_n| < \frac{\varepsilon}{2}.$$

したがって, $n_2 = \max\{n_0, n_1\}$ とおくと, m, $n > n_2$ ならば,

$$|(a_m + b_m) - (a_n + b_n)| \leq |a_m - a_n| + |b_m - b_n| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$$

が成り立つ.

(ii) $|a_m - a_n| = |(-a_m) - (-a_n)|$ より明らか. □

[補題 4.2] $(a_n) \in \mathcal{C}$ とする. このとき, ある $c \in \mathbb{Q}$ が存在して, 任意の $n \in \mathbb{N}$ に対して $|a_n| < c$ が成り立つ. これを **Cauchy 列の有界性**という.

[証明] $(a_n) \in \mathcal{C}$ とすると, ある自然数 n_0 が存在して, 任意の自然数 m, n に対して, $m > n_0$ かつ $n > n_0$ ならば, $|a_m - a_n| < 1$ が成り立つ. よって特に, 任意の $n > n_0$ に対して, $|a_n - a_{n_0+1}| < 1$ となるから,

$$|a_n| \leq |a_n - a_{n_0+1}| + |a_{n_0+1}| < 1 + |a_{n_0+1}|.$$

ゆえに,

$$c = \max\{|a_0|, |a_1|, \ldots, |a_{n_0}|, 1 + |a_{n_0+1}|\}$$

とおけば, すべての $n \in \mathbb{N}$ に対して $|a_n| < c$ が成り立つ. □

[14] $\mathbb{R}$, $\mathbb{C}$ は後で定義する.

[定理 4.3] 任意の (a_n), $(b_n) \in \mathcal{C}$ に対して, $(a_n b_n) \in \mathcal{C}$.

[証明] 上の補題より, ある a, $b \in \mathbb{Q}$ が存在して, 任意の $n \in \mathbb{N}$ に対して, $|a_n| < a$ かつ $|b_n| < b$ が成り立つ. $c = \max\{a, b\}$ とおく.

一方, 任意の正の有理数 ε に対して, ある自然数 n_0, n_1 が存在して, 任意の自然数 m, n に対して,

$$m > n_0, n > n_0 \Longrightarrow |a_m - a_n| < \frac{\varepsilon}{2c},$$
$$m > n_1, n > n_1 \Longrightarrow |b_m - b_n| < \frac{\varepsilon}{2c}.$$

$n_2 = \max\{n_0, n_1\}$ とすれば, 任意の自然数 m, n に対して, $m > n_2$ かつ $n > n_2$ ならば,

$$\begin{aligned} |a_m b_m - a_n b_n| &= |a_m(b_m - b_n) + b_n(a_m - a_n)| \\ &\leq |a_m||b_m - b_n| + |b_n||a_m - a_n| \\ &< c \cdot \frac{\varepsilon}{2c} + c \cdot \frac{\varepsilon}{2c} = \varepsilon. \end{aligned}$$

したがって $(a_n b_n) \in \mathcal{C}$. □

[補題 4.4] 任意の $(a_n) \in \mathcal{C}$ に対して, 次の三つの場合のいずれか一つ, しかも一つだけが成り立つ.

(i) 任意の正の有理数 ε に対して, ある $n_0 \in \mathbb{N}$ が存在して, 任意の $n \in \mathbb{N}$ に対して, $n > n_0$ ならば $|a_n| < \varepsilon$.

(ii) ある正の有理数 c と $n_0 \in \mathbb{N}$ が存在して, 任意の $n \in \mathbb{N}$ に対して, $n > n_0$ ならば $a_n \geq c$.

(iii) ある正の有理数 c と $n_0 \in \mathbb{N}$ が存在して, 任意の $n \in \mathbb{N}$ に対して, $n > n_0$ ならば $a_n \leq -c$.

[証明] まず, (ii), (iii) が同時に成り立つと仮定すると, (ii) より, ある正の有理数 c と $n_0 \in \mathbb{N}$ が存在して, 任意の $n \in \mathbb{N}$ に対して, $n > n_0$ ならば $a_n \geq c$ が成り立つ. (iii) より, ある正の有理数 c' と $n_0' \in \mathbb{N}$ が存在して, 任意の $n \in \mathbb{N}$ に対して, $n > n_0'$ ならば $a_n \leq -c'$ が成り立つ. $n_0'' = \max\{n_0, n_0'\} + 1$ とおくと, $a_{n_0''} \geq c > 0$ かつ $a_{n_0''} \leq -c' < 0$ となって矛盾する. したがって (ii) と (iii) は同時に成り立たない.

(i) の ε として (ii) の c をとれば, それは (ii) とは両立しえない. よって (i) と (ii) が同時に成り立つことはない. (i) と (iii) についても同様である.

次に, いずれかの条件が成立することを示すために, (ii), (iii) が成り立たないと仮定する. (i) が成り立つことをいえばよい.

正の有理数 ε を任意にとる. (a_n) は Cauchy 列であるから, ある $n_0 \in \mathbb{N}$ が存在して, 任意の m, $n \in \mathbb{N}$ に対して, $m > n_0$ かつ $n > n_0$ ならば,

$$|a_m - a_n| < \frac{\varepsilon}{2}$$

が成り立つ.

一方, (a_n) は (ii) を満たさないと仮定した[15]から, ある $n_1 \in \mathbb{N}$ が存在して, $n_1 > n_0$ かつ $a_{n_1} < \varepsilon/2$ となる. 同様に, (a_n) は (iii) を満たさないと仮定した[16]から, ある $n_2 \in \mathbb{N}$ が存在して, $n_2 > n_0$ かつ $a_{n_2} < -\varepsilon/2$ となる. よって $n > n_0$ ならば,

$$a_n = (a_n - a_{n_1}) + a_{n_1} \leq |a_n - a_{n_1}| + a_{n_1} < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon,$$
$$a_n = (a_n - a_{n_2}) + a_{n_2} \geq -|a_n - a_{n_2}| + a_{n_2} > -\frac{\varepsilon}{2} - \frac{\varepsilon}{2} = -\varepsilon.$$

ゆえに $|a_n| < \varepsilon$ となる. したがって (i) が成り立つ. □

4.2 実数の構成

$\mathcal{C}$ を, $\mathbb{Q}$ の Cauchy 列全体からなる集合とする. $\mathcal{C}$ 上の二項関係 $\sim$ を, 各 $(a_n), (b_n) \in \mathcal{C}$ に対して次のように定める.

$$(a_n) \sim (b_n) \Longleftrightarrow \text{任意の正の有理数 } \varepsilon \text{ に対して, ある自然数 } n_0 \text{ が存在して,}$$
$$\text{任意の自然数 } n \text{ に対して, } n > n_0 \text{ ならば } |a_n - b_n| < \varepsilon.$$

[命題 4.5] $\sim$ は $\mathcal{C}$ 上の同値関係である.

[証明] $|a_n - a_n| = 0$ より, $(a_n) \sim (a_n)$. したがって $\sim$ に関して反射法則が成り立つ.

$|a_n - b_n| = |b_n - a_n|$ より, $(a_n) \sim (b_n) \Rightarrow (b_n) \sim (a_n)$. したがって $\sim$ に関して対称法則が成り立つ.

$(a_n) \sim (b_n)$ かつ $(b_n) \sim (c_n)$ が成り立つとする. このとき, 任意の正の有理数 ε に対して, ある自然数 n_0, n_1 が存在して, 任意の自然数 n に対して

$$n > n_0 \Longrightarrow |a_n - b_n| < \frac{\varepsilon}{2},$$
$$n > n_1 \Longrightarrow |b_n - c_n| < \frac{\varepsilon}{2}$$

となる. したがって, $n_2 = \max\{n_0, n_1\}$ とおくと, $n > n_2$ ならば

$$|a_n - c_n| \leq |a_n - b_n| + |b_n - c_n| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$$

が成り立つ. よって $(a_n) \sim (c_n)$. したがって $\sim$ に関して推移法則が成り立つ. □

$\mathcal{C}$ を同値関係 $\sim$ により類別した同値類の集合を $\mathbb{R}$ とおく:

$$\mathbb{R} = \mathcal{C}/\sim .$$

[15] (ii) の否定は, 任意の正の有理数 c と任意の $n_0 \in \mathbb{N}$ に対して, ある $n \in \mathbb{N}$ が存在して, $n > n_0$ かつ $a_n < c$.
[16] (iii) の否定は, 任意の正の有理数 c と任意の $n_0 \in \mathbb{N}$ に対して, ある $n \in \mathbb{N}$ が存在して, $n > n_0$ かつ $a_n > -c$.

また, Cauchy 列 (a_n) を代表元とする $\mathbb{R}$ の同値類を $[a_n]$ と書く. すなわち,

$$\mathbb{R} = \{[a_n] \mid (a_n) \in \mathcal{C}\}.$$

$\mathbb{R}$ の元, すなわち $\mathbb{R}$ に属する各同値類 $[a_n]$ のことを**実数**という.

[定理 4.6] $[a_n]$, $[b_n]$, $[c_n]$, $[d_n] \in \mathbb{R}$ とする. $[a_n] = [c_n]$ かつ $[b_n] = [d_n]$ ならば, $[a_n + b_n] = [c_n + d_n]$.

[証明] (i) $[a_n] = [c_n]$ かつ $[b_n] = [d_n]$ のとき, 任意の正の有理数 ε に対して, ある自然数 n_0, n_1 が存在して, 任意の自然数 n に対して

$$n > n_0 \Longrightarrow |a_n - c_n| < \frac{\varepsilon}{2},$$
$$n > n_1 \Longrightarrow |b_n - d_n| < \frac{\varepsilon}{2}$$

となる. したがって, $n_2 = \max\{n_0, n_1\}$ とおくと, $n > n_2$ ならば

$$|(a_n + b_n) - (c_n + d_n)| \leq |a_n - c_n| + |b_n - d_n| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$$

が成り立つ. したがって $[a_n + b_n] = [c_n + d_n]$. □

[定理 4.7] $[a_n]$, $[b_n]$, $[c_n]$, $[d_n] \in \mathbb{R}$ とする. $[a_n] = [c_n]$ かつ $[b_n] = [d_n]$ ならば, $[a_n b_n] = [c_n d_n]$.

[証明] 補題より, ある a, $b \in \mathbb{Q}$ が存在して, 任意の $n \in \mathbb{N}$ に対して, $|b_n| < a$ かつ $|c_n| < b$ が成り立つ. $c = \max\{a, b\}$ とおく.

一方, $[a_n] = [c_n]$ かつ $[b_n] = [d_n]$ とすると, 任意の正の有理数 ε に対して, ある自然数 n_0, n_1 が存在して, 任意の自然数 n に対して,

$$n > n_0 \Longrightarrow |a_n - c_n| < \frac{\varepsilon}{2c},$$
$$n > n_1 \Longrightarrow |b_n - d_n| < \frac{\varepsilon}{2c}.$$

$n_2 = \max\{n_0, n_1\}$ とすれば, 任意の自然数 m, n に対して, $n > n_2$ ならば

$$\begin{aligned} |a_n b_n - c_n d_n| &= |b_n(a_n - c_n) + c_n(b_n - d_n)| \\ &\leq |b_n||a_n - c_n| + |c_n||b_n - d_n| \\ &< c \cdot \frac{\varepsilon}{2c} + c \cdot \frac{\varepsilon}{2c} = \varepsilon. \end{aligned}$$

したがってしたがって $[a_n b_n] = [c_n d_n]$. □

各 $[a_n]$, $[b_n] \in \mathbb{R}$ に対し, それらの和, 積をそれぞれ

$$[a_n] + [b_n] = [a_n + b_n], \quad [a_n][b_n] = [a_n b_n]$$

によって定義する. 上の定理により, 和, 積は同値類の代表元の選び方によらずに定まる.

[命題 4.8] 任意の $(a_n) \in \mathcal{C}$ に対して, $[a_n] \neq [0]$ ならば, ある $(b_n) \in \mathcal{C}$ が存在して $[a_n b_n] = [1]$ となる.

[証明] 補題により[17], ある正の有理数 c と $n_0 \in \mathbb{N}$ が存在して, 任意の $n \in \mathbb{N}$ に対して, $n > n_0$ ならば $|a_n| > c$ が成り立つ. 特に $a_n \neq 0$ である. そこで, 数列 (b_n) を次のように定義する.

$$b_n = \begin{cases} 1 & n \leq n_0 \text{ のとき,} \\ 1/a_n & n > n_0 \text{ のとき.} \end{cases}$$

ε を正の有理数とする. (a_n) は Cauchy 列であるから, ある $n_1 \in \mathbb{N}$ が存在して, 任意の $m, n \in \mathbb{N}$ に対して,

$$m > n_1, n > n_1 \Longrightarrow |a_m - a_n| < c^2 \varepsilon$$

が成り立つ. $n_2 = \max\{n_0, n_1\}$ とすると, $m > n_2$ かつ $n > n_2$ ならば

$$|b_m - b_n| = \left| \frac{1}{a_m} - \frac{1}{a_n} \right| = \frac{|a_n - a_m|}{|a_m||a_n|} < \frac{c^2 \varepsilon}{c^2} = \varepsilon.$$

したがって (b_n) は Cauchy 列である.

$n > n_0$ ならば, $a_n b_n = 1$ だから, $|a_n b_n - 1| = 0$. これより $[a_n b_n] = [1]$ となることは明らかである. □

[定理 4.9] $\mathbb{R}$ は体になる.

[証明] $[a_n], [b_n], [c_n] \in \mathbb{R}$ とする. 以下, $\mathbb{Q}$ の加法, 乗法に関する結合法則, 交換法則, 分配法則を利用して計算する.

まず, $\mathbb{R}$ の加法が, 体であるための条件を満たすことを確認する.

$$\begin{aligned} ([a_n] + [b_n]) + [c_n] &= [a_n + b_n] + [c_n] = [(a_n + b_n) + c_n] \\ &= [a_n + (b_n + c_n)] = [a_n] + [b_n + c_n] \\ &= [a_n] + ([b_n] + [c_n]). \end{aligned}$$

よって $\mathbb{R}$ は加法に関して結合法則を満たす.

$$\begin{aligned} [a_n] + [b_n] &= [a_n + b_n] = [b_n + a_n] \\ &= [b_n] + [a_n]. \end{aligned}$$

よって $\mathbb{R}$ は加法に関して交換法則を満たす.

[17] $[a_n] = [0]$ と補題の条件 (i) とは同値であることに注意せよ.

$\mathbb{Q}$ の零元を 0 とするとき, $\mathbb{R}$ の零元は $[0]$ である. つまり, 任意の $n \in \mathbb{N}$ に対して $d_n = 0$ であるような有理数列 (d_n) を代表元とする同値類である. 実際,

$$[a_n] + [0] = [a_n + 0] = [a_n].$$

$[a_n]$ の加法における逆元は $[-a_n]$ である. 実際,

$$[a_n] + [-a_n] = [a_n - a_n] = [0].$$

次に, $\mathbb{R}$ の乗法が体であるための条件を満たすことを確認する.

$$\begin{aligned}([a_n][b_n])[c_n] &= [a_n b_n][c_n] = [(a_n b_n)c_n] \\ &= [a_n(b_n c_n)] = [a_n][b_n c_n] \\ &= [a_n]([b_n][c_n]).\end{aligned}$$

よって $\mathbb{R}$ は加法に関して結合法則を満たす.

$$\begin{aligned}[a_n][b_n] &= [a_n b_n] = [b_n a_n] \\ &= [b_n][a_n].\end{aligned}$$

よって $\mathbb{R}$ は加法に関して交換法則を満たす.

$\mathbb{Q}$ の乗法における単位元を 1 とするとき, $\mathbb{R}$ の乗法における単位元は $[1]$ である. つまり, 任意の $n \in \mathbb{N}$ に対して $d_n = 1$ であるような有理数列 (d_n) を代表元とする同値類である. 実際,

$$[a_n][1] = [a_n \cdot 1] = [a_n].$$

$\mathbb{R}$ の乗法における逆元の存在は, 上の命題によって明らかである.

最後に,

$$\begin{aligned}[a_n][b_n] + [a_n][c_n] &= [a_n b_n] + [a_n c_n] = [a_n b_n + a_n c_n] \\ &= [a_n(b_n + c_n)] = [a_n][b_n + c_n] \\ &= [a_n]([b_n] + [c_n]).\end{aligned}$$

よって $\mathbb{R}$ の加法と乗法に関して分配法則が成り立つ.

以上より, $\mathbb{R}$ が体であることが示された. □

4.3 実数の順序

$\mathbb{R}$ 上の二項関係 $<$ を, 各 $[a_n], [b_n] \in \mathbb{R}$ に対して次のように定める.

$$\begin{aligned}[a_n] < [b_n] \Longleftrightarrow &\text{ある正の有理数 } c \text{ と自然数 } n_0 \text{ が存在して,} \\ &\text{任意の自然数 } n \text{ に対して, } n > n_0 \text{ ならば } b_n - a_n \geq c.\end{aligned}$$

$[a_n] < [b_n]$ が成り立つとき, $[b_n]$ は $[a_n]$ よりも**大きい**といい, $[a_n]$ は $[b_n]$ よりも**小さい**という. また,

$$[a_n] \leq [b_n] \Longleftrightarrow [a_n] < [b_n] \text{ または } [a_n] = [b_n]$$

と定める.

$[a_n] \in \mathbb{R}$ について, $[a_n] > 0$ が成り立つとき, $[a_n]$ は正であるという. また, $[a_n] < 0$ が成り立つとき, $[a_n]$ は負であるという.

[定理 4.10] 任意の $[a_n], [b_n] \in \mathbb{R}$ に対して, 次が成り立つ.

(i) $[a_n] \leq [a_n]$.
(ii) $[a_n] \leq [b_n]$ かつ $[b_n] \leq [c_n]$ ならば, $[a_n] \leq [c_n]$.
(iii) $[a_n] \leq [b_n]$ かつ $[b_n] \leq [a_n]$ ならば, $[b_n] = [a_n]$.

(i), (ii), (iii) より, $\leq$ が実際に $\mathbb{R}$ 上の順序関係であることがわかる. さらに, 任意の $[a_n], [b_n] \in \mathbb{R}$ に対して, $[a_n] < [b_n]$, $[a_n] = [b_n]$, $[a_n] > [b_n]$ のいずれか一つ, しかも一つだけが成り立つ.

[証明] (i) $[a_n] = [a_n]$ より明らかである.

(ii) $[a_n] \leq [b_n]$ かつ $[b_n] \leq [c_n]$ ならば, ある正の有理数 c, c' と自然数 n_0, n_1 が存在して, 任意の自然数 n に対して,

$$n > n_0 \Longrightarrow b_n - a_n \geq c$$
$$n > n_1 \Longrightarrow c_n - b_n \geq c'$$

が成り立つ. $n_2 = \max\{n_0, n_1\}$ とおくと, 任意の自然数 n に対して, $n > n_2$ ならば,

$$c_n - a_n = (c_n - b_n) + (b_n - a_n) \geq c + c'.$$

ところで, $c + c'$ および n_2 は n によらない. よって $[a_n] \leq [c_n]$.

(iii) $a_n - b_n \geq c \Leftrightarrow b_n - a_n \leq -c$ であるから, 補題より, $[a_n] < [b_n]$ と $[b_n] < [a_n]$ とは同時に成立しない. したがって $[a_n] = [b_n]$ でなければならない.

後半の主張は, 補題において a_n を $b_n - a_n$ と置き換えたとき, $[a_n] = [b_n]$, $[a_n] < [b_n]$, $[a_n] > [b_n]$ がそれぞれ補題の条件 (i), (ii), (iii) に対応することから明らかである.

□

$\mathbb{Q}$ から $\mathbb{R}$ への写像 φ を, 各 $a \in \mathbb{Q}$ に対して

$$\varphi(a) = [a]$$

によって定義する. ここで, $[a]$ は任意の $n \in \mathbb{N}$ に対して $a_n = a$ であるような有理数列 (a_n) を代表元とする同値類である.

[補題 4.11] $a \in \mathbb{Q}$ とする. $0 \leq a < \varepsilon$ が任意の正の有理数 ε に対して成り立つならば, $a = 0$ である.

[証明] 対偶を示す. $a \neq 0$ とすると, $a > 0$ なので, $\mathbb{Q}$ の稠密性により, ある $c \in \mathbb{Q}$ が存在して $0 < c < a$ となる. □

[定理 4.12] 写像 φ は単射準同型である. したがって特に, $\mathbb{Q}$ は $\mathbb{R}$ の部分体である. さらに, φ は順序を保つ.

[証明] $a, b \in \mathbb{Q}$ とする. $[a] = [b]$ ならば, 二つの Cauchy 列が同値であることの定義から, 任意の正の有理数 ε に対して $|a - b| < \varepsilon$ が成り立つことがわかる. よって, 上の補題より $|a - b| = 0$, したがって $a = b$ が得られる. これは φ の単射性を示している. また,

$$\varphi(a) + \varphi(b) = [a] + [b] = [a + b] = \varphi(a + b),$$
$$\varphi(a)\varphi(b) = [a][b] = [ab] = \varphi(ab).$$

よって, φ は準同型である.

さらに, $a < b$ ならば, $\mathbb{Q}$ の稠密性によって, ある有理数 c が存在して, $b - a > c$ かつ $c > 0$ となる. よって, $n_0 = 0$ とすれば, 当然のことながら, 任意の自然数 n に対して, $n > n_0$ ならば $b - a > c$ が成り立つ. このことは $[a] < [b]$, すなわち $\varphi(a) < \varphi(b)$ を意味する. □

以後, 有理数 a に対して, $a = [a]$ であるとみなす. 特に, $0 = [0]$ は $\mathbb{R}$ の零元であり, $1 = [1]$ は $\mathbb{R}$ の乗法における単位元である.

[補題 4.13] $[a_n], [b_n] \in \mathbb{R}$ とし, ある自然数 n_0 が存在して, 任意の自然数 n に対して, $n > n_0$ ならば $a_n \leq b_n$ が成り立つとする. このとき $[a_n] \leq [b_n]$.

[証明] ある自然数 n_0 が存在して, 任意の自然数 n に対して, $n > n_0$ ならば $a_n \leq b_n$ が成り立つとすれば, 補題において a_n を $b_n - a_n$ に置き換えたとき, 条件 (iii) は成り立たない. よって補題の条件の (i) または (ii) が成り立つ. よって $[a_n] \leq [b_n]$. □

[定理 4.14] 任意の $[a_n] \in \mathbb{R}$ に対して, ある自然数 m が存在して $[a_n] < m$. これを **Archimedes の性質**と呼ぶ.

[証明] Cauchy 列の有界性から, ある正の有理数 b が存在して, 任意の $n \in \mathbb{N}$ に対して $a_n < b$ が成り立つ. よって上の補題より $[a_n] \leq b$ がわかる. 一方, $b = c_0/d_0$ を既約分数による表示とし, $m = c_0 + 1$ とおけば, $0 < b \leq c_0 < m$. したがって $m \in \mathbb{N}$ かつ $[a_n] < m$ となる. □

[定理 4.15] 任意の $x, y \in \mathbb{R}$ に対して, $x < y$ ならば, ある $r \in \mathbb{Q}$ が存在して $x < r < y$. これを $\mathbb{R}$ における $\mathbb{Q}$ の稠密性という.

[証明] $\mathbb{R}$ は体であり, $x \neq y$ なので, $1/(y-x) \in \mathbb{R}$ である. Archimedes の性質により, ある自然数 n が存在して $1/(y-x) < n$ が成り立つ. $y - x > 0$ なので, $1 < n(y-x)$ となる.

次に, $m = \min\{k \in \mathbb{Z} \mid nx < k\}$ とおく. $nx < m$ より $x < m/n = r$. 一方, m の最小性から $m - 1 \leq nx$. よって

$$nx = n(y-x) + nx > 1 + (m-1) = m.$$

ゆえに $y > m/n = r$. したがって $x < r < y$. □

4.4 実数の絶対値

[補題 4.16] $|*|$ を $\mathbb{Q}$ における絶対値とする. このとき, 任意の $(a_n) \in \mathcal{C}$ に対して, $(|a_n|) \in \mathcal{C}$.

[証明] Cauchy 列の定義と不等式 $||a_m| - |a_n|| < |a_m - a_n|$ よりわかる. □

[補題 4.17] $|*|$ を $\mathbb{Q}$ における絶対値とする. このとき, 任意の $(a_n), (b_n) \in \mathcal{C}$ に対して, $[a_n] = [b_n]$ ならば $[|a_n|] = [|b_n|]$.

[証明] 同値類が等しいことの定義と不等式 $||a_n| - |b_n|| < |a_n - b_n|$ よりわかる. □

各 $x \in \mathbb{R}$ に対して, $x = [a_n]$ とするとき, **絶対値** $|x|'$ を

$$|x|' = [|a_n|]$$

によって定義する. ここで, 右辺の $|*|$ は $\mathbb{Q}$ における絶対値である. この定義が well-defined であること, すなわち同値類の代表元 $(a_n) \in \mathcal{C}$ の選び方によらないことは, 上の補題よりわかる.

任意の $a \in \mathbb{Q}$ に対して,

$$|a|' = [|a|] = |a|.$$

したがって, 実数の絶対値は有理数の絶対値の拡張になっている. そこで, 実数の絶対値もまた $|*|$ で表すことにする.

[命題 4.18] 任意の $x \in \mathbb{R}$ に対して,

$$|x| = \begin{cases} x & x > 0 \text{ のとき} \\ 0 & x = 0 \text{ のとき} \\ -x & x < 0 \text{ のとき} \end{cases}$$

が成り立つ.

[証明] $x=[a_n]$ とする. $x>0$ のとき, ある正の有理数 c と自然数 n_0 が存在して, 任意の自然数 n に対して,

$$n>n_0 \Longrightarrow a_n \geq c.$$

一方, $a_n \in \mathbb{Q}$ より, $a_n>0$ ならば $|a_n|=a_n$ であるから,

$$n>n_0 \Longrightarrow |a_n|-a_n=0.$$

したがって, 任意の正の有理数 ε に対して

$$n>n_0 \Longrightarrow ||a_n|-a_n|<\varepsilon.$$

これは $[|a_n|]=[a_n]$, すなわち $|x|=x$ を意味する.

$x=0$ のとき, 任意の正の有理数 ε に対して, ある自然数 n_0 が存在して, 任意の自然数 n に対して,

$$n>n_0 \Longrightarrow |a_n|<\varepsilon.$$

一方, $a_n \in \mathbb{Q}$ より, $|a_n| \geq 0$ であるから, $||a_n||=|a_n|$. よって

$$n>n_0 \Longrightarrow ||a_n||<\varepsilon.$$

これは $[|a_n|]=0$, すなわち $|0|=0$ を意味する.

$x<0$ のとき, ある正の有理数 c と自然数 n_0 が存在して, 任意の自然数 n に対して,

$$n>n_0 \Longrightarrow a_n \leq -c.$$

一方, $a_n \in \mathbb{Q}$ より, $a_n<0$ ならば $|a_n|=-a_n$ であるから,

$$n>n_0 \Longrightarrow |a_n|-(-a_n)=0.$$

したがって, 任意の正の有理数 ε に対して

$$n>n_0 \Longrightarrow ||a_n|-(-a_n)|<\varepsilon.$$

これは $[|a_n|]=[-a_n]=-[a_n]$, すなわち $|x|=-x$ を意味する. □

[命題 4.19] 任意の $x, y \in \mathbb{Q}$ に対して, 次が成り立つ.

(i) $|x| \geq 0$.

(ii) $|x|=0 \Longleftrightarrow x=0$.

(iii) $x \leq |x|$.

(iv) $|-x|=|x|$.

(v) $|xy|=|x||y|$.

(vi) $y \neq 0$ ならば, $|x/y|=|x|/|y|$. 特に, $|1/y|=1/|y|$.

[証明] 実数の絶対値が有理数の絶対値の拡張であることに注意して, 有理数の絶対値に関する性質を利用して証明する.

(i) $x = [a_n]$ とすると, $|x| = [|a_n|]$ である. 一方, 任意の自然数 n に対して, $a_n \in \mathbb{Q}$ なので, $|a_n| \geq 0$ であることがすでに分かっている. よって $[|a_n|] \geq 0$ が得られる.

(ii) 上の命題から明らかである.

(iii) $x = 0$ または $x > 0$ のときは $|x| = x$ である. $x < 0$ のときは $x < 0 < |x|$ である.

(iv) $x = [a_n]$ とすると, $-x = [-a_n]$ だから,

$$|-x| = [|-a_n|] = [|a_n|] = |x|.$$

(v) $x = [a_n]$, $y = [b_n]$ とすると, $xy = [a_n b_n]$ だから,

$$|xy| = [|a_n b_n|] = [|a_n||b_n|] = [|a_n|][|b_n|] = |x||y|$$

となる.

(vi) $y \cdot (x/y) = x$ であるから, (v) より $|y||x/y| = |x|$. 両辺を $|y|$ で割れば, $|x/y| = |x|/|y|$ が得られる. □

[定理 4.20] 任意の $x, y \in \mathbb{Q}$ に対して, 次が成り立つ.

(i) $|x + y| \leq |x| + |y|$. この不等式は三角不等式と呼ばれる.

(ii) $|x - y| \leq |x| + |y|$.

(iii) $|x| - |y| \leq |x + y|$.

(iv) $|x| - |y| \leq |x - y|$.

[証明] (i) $x \leq |x|$, $y \leq |y|$ より

$$x + y \leq |x| + |y|.$$

一方, $-x \leq |x|$, $-y \leq |y|$ より

$$-(x + y) \leq |x| + |y|.$$

$|x + y|$ は $x + y$ か $-(x + y)$ のどちらかに等しい. よって

$$|x + y| \leq |x| + |y|.$$

となる.

(ii) (i) において, y に $-y$ を代入すれば, $|-y| = |y|$ より (ii) が得られる.

(iii) (ii) において y に $x + y$ を代入すれば,

$$|x - (x + y)| \leq |x| + |x + y|.$$

これと $|-y| = |y|$ より (iii) が得られる.

(iv) (i) において x に $x-y$ を代入すれば,

$$|(x-y)+y| \leq |x-y|+|y|.$$

これより (iv) が得られる. □

4.5 $\mathbb{R}$ の完備性

$\mathbb{Q}$ の元の列を**有理数列**といい, $\mathbb{R}$ の元の列を**実数列**ということにする.

実数列 (x_n) が実数 x に**収束する**とは, 任意の正の実数 ε に対して, ある自然数 n_0 が存在して, 任意の自然数 n に対して, $n > n_0$ ならば $|x_n - x| < \varepsilon$ が成り立つときにいう.

実数列 (x_n) が $\mathbb{R}$ の **Cauchy 列**であるとは, 任意の正の実数 ε に対して, ある自然数 n_0 が存在して, 任意の自然数 m, n に対して, $m > n_0$ かつ $n > n_0$ ならば, $|x_m - x_n| < \varepsilon$ が成り立つときにいう.

[補題 4.21] (x_n) を実数列, x を実数とする. このとき, (x_n) が x に収束することの定義において, 「任意の正の実数 ε に対して」というところを, 「任意の正の有理数 ε に対して」に置き換えた条件さえ成り立てば, (x_n) は x に収束する.

[証明] 任意の正の有理数 e に対して, ある自然数 n_0 が存在して, 任意の自然数 n に対して, $n > n_0$ ならば $|x_n - x| < e$ が成り立つと仮定する.

ε を正の実数とする. $\mathbb{R}$ における $\mathbb{Q}$ の稠密性により, ある有理数 e が存在して $0 < e < \varepsilon$ が成り立つ. このとき, e に対して, ある自然数 n_0 が存在して, 任意の自然数 n に対して, $n > n_0$ ならば

$$|x_n - x| < e < \varepsilon$$

が成り立つ. これは (x_n) が x に収束することを意味する. □

[補題 4.22] (a_n) を有理数の Cauchy 列とし, $x = [a_n]$ とおく. このとき, (a_n) は $\mathbb{R}$ において a に収束する.

[証明] ε を正の有理数とする. (a_n) は有理数の Cauchy 列であるから, ε に対して, ある自然数 n_0 が存在して, 任意の自然数 m, n に対して,

$$m > n_0, n > n_0 \Longrightarrow |a_m - a_n| < \varepsilon$$

が成り立つ.

いま, m を固定し, $b = a_m$ とおくと, 任意の自然数 n に対して, $n > n_0$ ならば

$$|b - a_n| < \varepsilon,$$

すなわち

$$b-\varepsilon < a_n < b+\varepsilon$$

が成り立つ. したがって

$$b-\varepsilon \leq [a_n] \leq b+\varepsilon.$$

よって

$$|b-[a_n]| \leq \varepsilon.$$

$x=[a_n]$, $b=a_m$ とおいたから,

$$|a_m - x| < \varepsilon$$

となる. この不等式は, $m > n_0$ を満たす任意の自然数 m に対して成り立つ. ゆえに上の補題より, (a_n) は a に収束する. □

[定理 4.23] $\mathbb{R}$ の任意の Cauchy 列は, ある実数に収束する. これを $\mathbb{R}$ の**完備性**という.

[証明] (x_n) を $\mathbb{R}$ の Cauchy 列とする. ε を任意の正の有理数とする.

いま, n を固定し, 各 n に対して $x_n=[a_{n,i}]$ とおく. 上の補題より, $\mathbb{Q}$ の Cauchy 列 $(a_{n,i})$ は x_n に収束する. すなわち, ある自然数 i_0 が存在して, 任意の自然数 i に対して,

$$i > i_0 \Longrightarrow |a_{n,i} - x_n| < \frac{\varepsilon}{3}.$$

そこで,

$$a_n = a_{n,i_0+1}$$

によって有理数列 (a_n) を定義すると, 任意の自然数 n に対して

$$|a_n - x_n| < \frac{\varepsilon}{3}$$

が成り立つ. このとき, (a_n) が $\mathbb{Q}$ の Cauchy 列であることを示す.

ε を任意の有理数とする. (x_n) は $\mathbb{R}$ の Cauchy 列であるから, ある自然数 n_0 が存在して, 任意の自然数 m, n に対して

$$m > n_0, n > n_0 \Longrightarrow |x_m - x_n| < \frac{\varepsilon}{3}$$

が成り立つ. よって, 任意の自然数 m, n に対して, $m > n_0$, $n > n_0$ ならば

$$\begin{aligned} |a_m - a_n| &= |(a_m - x_m) + (x_m - x_n) + (x_n - a_n)| \\ &\leq |a_m - x_m| + |x_m - x_n| + |x_n - a_n| \\ &< \frac{\varepsilon}{3} + \frac{\varepsilon}{3} + \frac{\varepsilon}{3} = \varepsilon. \end{aligned}$$

ゆえに (a_n) は $\mathbb{Q}$ の Cauchy 列である.

$x = [a_n]$ とおくと, 上の補題より, (a_n) は x に収束する. よって, ε に対して, ある自然数 n_1 が存在して, 任意の自然数 n に対して

$$n > n_1 \Longrightarrow |a_n - x| < \frac{\varepsilon}{3}.$$

$n_2 = \max\{n_0, n_1\}$ とおくと, 任意の自然数 n に対して, $n > n_2$ ならば,

$$|x_n - x| = |x_n - a_n| + |a_n - x| < \frac{\varepsilon}{3} + \frac{\varepsilon}{3} < \varepsilon.$$

ゆえに (x_n) は x に収束する. □

[定理 4.24] 実数列 (x_n), (y_n) について, 任意の $n \in \mathbb{N}$ に対して

$$x_n \leq x_{n+1} \leq y_{n+1} \leq y_n$$

が成り立つと仮定する. このとき, もし数列 $(y_n - x_n)$ が 0 に収束すれば, ある実数 x がただ一つ存在して, (x_n), (y_n) はともに x に収束し, 任意の $n \in \mathbb{N}$ に対して

$$x_n \leq x \leq y_n$$

を満たす. これを**区間縮小法の原理**という.

[証明] まず, $(y_n - x_n)$ が 0 に収束することから, 任意の正の実数 ε に対して, ある n_0 が存在して, 任意の自然数 n に対して, $n > n_0$ ならば

$$|y_n - x_n| < \varepsilon.$$

n_1 を $n_1 > n_0$ なる自然数とすれば, 任意の自然数 m, n に対して, $m > n_1$, $n > n_1$ ならば,

$$x_{n_1} \leq x_m \leq y_{n_1}, \quad x_{n_1} \leq x_n \leq y_{n_1}$$

となるから,

$$|x_m - x_n| < |y_{n_1} - x_{n_1}| < \varepsilon.$$

よって (x_n) は $\mathbb{R}$ の Cauchy 列である. $\mathbb{R}$ の完備性から, ある実数 x が存在して, (x_n) は x に収束する.

ここでもし仮に, ある番号 n_2 が存在して $x < x_{n_2}$ ならば, $c = x_{n_2} - x$ とおくと, $n > n_2$ なる任意の自然数 n に対して

$$0 < c \leq |x_n - x|$$

となり, (x_n) が x に収束することに反する. よって, 任意の $n \in \mathbb{N}$ に対して $x_n \leq x$ が成り立つ.

一方, (y_n) もまた x に収束することは, (x_n) が x に収束すること, $(y_n - x_n)$ が 0 に収束すること, および, 任意の $n \in \mathbb{N}$ に対して成り立つ不等式

$$|y_n - x| \leq |y_n - x_n| + |x_n - x|$$

よりわかる.

もし仮に, ある番号 n_3 が存在して $y_{n_2} < x$ ならば, $c' = x - y_{n_3}$ とおくと, $n > n_3$ なる任意の自然数 n に対して

$$0 < c' \leq |x - y_n|$$

となり, (y_n) が x に収束することに反する. よって, 任意の $n \in \mathbb{N}$ に対して $x \leq y_n$ が成り立つ.

最後に, もし実数 x, y が, 任意の $n \in \mathbb{N}$ に対して

$$x_n \leq x \leq y_n, \quad x_n \leq y \leq y_n$$

を満たしているとすれば,

$$|y - x| < |y_n - x_n|.$$

したがって, 任意の正の実数 ε に対して $|y - x| < \varepsilon$ となる. もし仮に $|y - x| > 0$ であるとすると, $c'' = |y - x|/2$ とおけば $0 < c'' < |y - x|$ となって矛盾が生じる. よって $y = x$ が得られる. したがって x は存在すれば一意的である. □

[補題 4.25] 任意の $n \in \mathbb{N}$ に対して $n + 1 \leq 2^n$.

[証明] n に関する数学的帰納法により証明する. $n = 0$ のときは $n + 1 = 2^n = 1$ である. n のとき正しいとすると, $2^{n+1} = 2 \cdot 2^n \geq 2 \cdot (n + 1) \geq n + 2$. よって $n + 1$ のときも正しい. したがって, すべての $n \in \mathbb{N}$ について $n + 1 \leq 2^n$ が成り立つ. □

$\mathbb{R}$ の部分集合 S が**上に有界**であるとは, ある $c \in \mathbb{R}$ が存在して, 任意の $x \in S$ に対して $x \leq c$ が成り立つことである.

$\mathbb{R}$ の部分集合 S が**下に有界**であるとは, ある $c \in \mathbb{R}$ が存在して, 任意の $x \in S$ に対して $c \leq x$ が成り立つことである.

$\mathbb{R}$ の部分集合 S が**有界**であるとは, ある $c \in \mathbb{R}$, $c > 0$ が存在して, 任意の $x \in S$ に対して $|x| \leq c$ が成り立つことである[18].

a を実数, S を $\mathbb{R}$ の部分集合とする. a が S の**上界**であるとは, 任意の $x \in S$ に対して $x \leq a$ が成り立つときにいう. また, S の上界に最小のものが存在するとき, それを S の**上限**という.

a が S の**下界**であるとは, 任意の $x \in S$ に対して $a \leq x$ が成り立つときにいう. また, S の下界に最大のものが存在するとき, それを S の**下限**という.

[定理 4.26] $\mathbb{R}$ において上に有界な空でない任意の $\mathbb{R}$ の部分集合は上限をもつ.

[証明] S を $\mathbb{R}$ において上に有界な空でない $\mathbb{R}$ の部分集合とする. もし S が S 自身の上界を含めば, その上界は S の最大元であり, したがって S の上限である. そこで, S は S 自身の上界を含まないと仮定する.

[18] 明らかに, S が有界 $\Leftrightarrow$ S が上にも下にも有界.

S は空でないので, S の元を一つとりそれを x_0 とする. また, S は上に有界なので, S の上界が存在する. その一つをとり y_0 とおく. さらに, $z_0 = (x_0 + y_0)/2$ とおく. 次に, x_n, y_n, z_n が定義されたとき,

$$z_n \text{ が } S \text{ の上界のとき, } x_{n+1} = x_n,\ y_{n+1} = z_n,$$
$$z_n \text{ が } S \text{ の上界でないとき, } x_{n+1} = z_n,\ y_{n+1} = y_n$$

と定める. また, $z_{n+1} = (x_{n+1} + y_{n+1})/2$ とする. このようにして, 数列 (x_n), (y_n), (z_n) が帰納的に定まる. 数列の定め方から, 各 $n \in \mathbb{N}$ に対して y_n は S の上界であり, x_n は S の上界ではない. さらに,

$$x_n \leq x_{n+1} \leq y_{n+1} \leq y_n$$

であり, $n + 1 \leq 2^n$ より

$$y_n - x_n = \frac{y_{n-1} - x_{n-1}}{2} = \cdots = \frac{y_0 - x_0}{2^n} \leq \frac{y_0 - x_0}{n+1}.$$

Archimedes の性質から, 任意の正の実数 ε に対して, ある自然数 n_0 が存在して

$$\frac{y_0 - x_0}{\varepsilon} - 1 < n_0,$$

ゆえに

$$\frac{y_0 - x_0}{n_0 + 1} < \varepsilon$$

が成り立つので, 数列 $(y_n - x_n)$ が 0 に収束することがいえる. 上の定理より, ある実数 x がただ一つ存在して, 任意の $n \in \mathbb{N}$ に対して

$$x_n \leq x \leq y_n$$

を満たす.

もし仮に, x が S の上界でないとすると, S の元 s が存在して $x < s$. このとき任意の $n \in \mathbb{N}$ に対して

$$y_n - x_n \geq y_n - x \geq s - x > 0.$$

これは $(y_n - x_n)$ が 0 に収束することに矛盾する. したがって x は S の上界である.

さらに, もし仮に x が S の上限でないとすると, ある S の上界 y が存在して $y < x$ となる. 任意の $n \in \mathbb{N}$ に対して, x_n は S の上界ではないから $x_n < y$ となり,

$$y_n - x_n > y_n - y \geq x - y > 0.$$

これも $(y_n - x_n)$ が 0 に収束することに矛盾する. したがって x は S の上限である. □

実数列 (x_n) が**上に有界**であるとは, 集合 $\{x_n \mid n \in \mathbb{N}\}$ が上に有界となることである. すなわち, ある $c \in \mathbb{R}$ が存在して, 任意の $n \in \mathbb{N}$ に対して $x_n \leq c$ が成り立つことである.

実数列 (x_n) が**下に有界**であるとは, 集合 $\{x_n \mid n \in \mathbb{N}\}$ が下に有界となることである. すなわち, ある $c \in \mathbb{R}$ が存在して, 任意の $n \in \mathbb{N}$ に対して $c \leq x_n$ が成り立つことである.

実数列 (x_n) が**有界**であるとは, 集合 $\{x_n \mid n \in \mathbb{N}\}$ が有界となることである. すなわち, ある $c \in \mathbb{R}$, $c > 0$ が存在して, 任意の $n \in \mathbb{N}$ に対して $|x_n| \leq c$ が成り立つことである[19].

実数列 (x_n) が**単調増加**であるとは, 任意の $x \in \mathbb{N}$ に対して $x_n \leq x_{n+1}$ が成り立つときにいう.

実数列 (x_n) が**単調減少**であるとは, 任意の $x \in \mathbb{N}$ に対して $x_{n+1} \leq x_n$ が成り立つときにいう.

[定理 4.27] 上に有界な単調増加実数列は収束する.

[証明] (x_n) を上に有界な単調増加実数列とし, $S = \{x_n \mid n \in \mathbb{N}\}$ とおく. S は上に有界な $\mathbb{R}$ の部分集合である. よって前定理より上限 s をもつ.

S の上限は S の上界でもあるから, 任意の $n \in \mathbb{N}$ に対して $x_n \leq S$ である. 一方, 任意の正の実数 ε に対して, $s - \varepsilon < s$ だから, 上限の最小性によって $s - \varepsilon$ は S の上界ではない. よって, ある $n_0 \in \mathbb{N}$ が存在して $s - \varepsilon < x_{n_0}$ となる. (x_n) は単調増加だから, $n > n_0$ なる任意の $n \in \mathbb{N}$ に対して

$$s - \varepsilon < x_{n_0} \leq x_n \leq s < s + \varepsilon.$$

よって

$$|x_n - s| < \varepsilon.$$

したがって (x_n) は s に収束する. □

数列 (x_n) から有限個または無限個の項を取り除いてできた数列 (x_{i_n}) のことを, (x_n) の**部分列**という. 厳密に述べれば, (x'_n) が (x_n) の部分列であるとは, 順序を保つ単射

$$\mathbb{N} \longrightarrow \mathbb{N}, \quad n \longmapsto i_n$$

が存在して, $x'_n = x_{i_n}$ が成り立つときにいう.

[定理 4.28] $\mathbb{R}$ において有界な実数列は収束する部分列をもつ.

[証明] (w_i) を有界な実数列とすると, ある実数 a, b が存在して, 任意の $i \in \mathbb{N}$ に対して $a \leq w_i \leq b$ となる.

$x_0 = a$, $y_0 = b$, $z_0 = (x_0 + y_0)/2$ とおく. 次に, x_n, y_n, z_n が定義されたとき,

$$x_n \leq w_i \leq z_n \text{ なる } i \in \mathbb{N} \text{ が無数にあるとき, } x_{n+1} = x_n,\ y_{n+1} = z_n,$$
$$z_n \leq w_i \leq y_n \text{ なる } i \in \mathbb{N} \text{ が無数にあるとき, } x_{n+1} = z_n,\ y_{n+1} = y_n$$

と定める. 集合 $\{w_i \mid i \in \mathbb{N}\}$ は無限集合なので, いずれか一方が必ず成り立つ. 両方とも成り立つときは最初のほうの条件で定義する. また, $z_{n+1} = (x_{n+1} + y_{n+1})/2$ とする. このようにして, 数列 (x_n), (y_n), (z_n) が帰納的に定まる.

[19] 明らかに, (x_n) が有界 $\Leftrightarrow$ (x_n) が上にも下にも有界.

数列の定め方から,

$$x_n \leq x_{n+1} \leq y_{n+1} \leq y_n$$

であり, $n+1 \leq 2^n$ より

$$y_n - x_n = \frac{y_{n-1} - x_{n-1}}{2} = \cdots = \frac{y_0 - x_0}{2^n} \leq \frac{y_0 - x_0}{n+1}.$$

Archimedes の性質から, 任意の正の実数 ε に対して, ある自然数 n_0 が存在して

$$\frac{y_0 - x_0}{\varepsilon} - 1 < n_0,$$

ゆえに

$$\frac{y_0 - x_0}{n_0 + 1} < \varepsilon$$

が成り立つので, 数列 $(y_n - x_n)$ が 0 に収束することがいえる. 区間縮小法の原理より, ある実数 x がただ一つ存在して, 任意の $n \in \mathbb{N}$ に対して

$$x_n \leq x \leq y_n$$

を満たす.

各 $n \in \mathbb{N}$ に対して, $I_n = \{t \in \mathbb{R} \mid x_n \leq t \leq y_n\}$ とおく. I_n の定め方から, $w_i \in I_n$ なる w_i が無数に存在する. そこで, $w_{i_0} = w_0$ とし, w_{i_0}, w_{i_1}, …, w_{i_n} まで選んだとき, I_{n+1} に属する w_i のうち $i > i_n$ を満たすものをとってそれを $w_{i_{n+1}}$ とする. このとき, (w_{i_n}) は (w_n) の部分列であり, すべての $n \in \mathbb{N}$ に対して

$$x_n \leq w_{i_n} \leq y_n$$

が成り立つ. (w_{i_n}) が x に収束することは, $(y_n - x_n)$ が 0 に収束することと, 任意の $n \in \mathbb{N}$ に対して成り立つ不等式

$$|w_{i_n} - x| \leq |y_n - x_n|$$

よりわかる. □

5　複素数

5.1　複素数の構成

実数の全体からなる体 $\mathbb{R}$ の直積 $\mathbb{R}\times\mathbb{R}$ の各元 (a,b), (c,d) に対して, それらの**和**, **積**を次のように定義する.

$$\begin{aligned}(a,b)+(c,d)&=(a+c,b+d),\\(a,b)(c,d)&=(ac-bd,ad+bc).\end{aligned}$$

このような和, 積によって加法, 乗法が定義された $\mathbb{R}\times\mathbb{R}$ を $\mathbb{C}$ で表す. また, $\mathbb{C}$ の元を**複素数**という.

[定理 5.1] $\mathbb{C}$ は体になる.

[証明] a, b, c, d, e, $f\in\mathbb{R}$ とする. 以下, $\mathbb{R}$ の加法, 乗法に関する結合法則, 交換法則, 分配法則を利用して計算する.

$$\begin{aligned}\big((a,b)+(c,d)\big)+(e,f)&=(a+c,b+d)+(e,f)=\big((a+c)+e,(b+d)+f\big)\\&=\big(a+(c+e),b+(d+f)\big)=(a,b)+(c+e,d+f)\\&=(a,b)+\big((c,d)+(e,f)\big).\end{aligned}$$

よって $\mathbb{C}$ は加法に関して結合法則を満たす.

$$\begin{aligned}(a,b)+(c,d)&=(a+c,b+d)=(c+a,d+b)\\&=(c,d)+(a,b).\end{aligned}$$

よって $\mathbb{C}$ は加法に関して交換法則を満たす.

$\mathbb{R}$ の零元を 0 とするとき, $\mathbb{C}$ の零元は $(0,0)$ である. 実際,

$$(a,b)+(0,0)=(a+0,b+0)=(a,b).$$

(a,b) の加法における逆元は $(-a,-b)$ である. 実際,

$$(a,b)+(-a,-b)=(a-a,b-b)=(0,0).$$

$$\begin{aligned}\big((a,b)(c,d)\big)(e,f)&=(ac-bd,ad+bc)(e,f)\\&=\big((ac-bd)e-(ad+bc)f,(ac-bd)f+(ad+bc)e\big)\\&=(ace-bde-adf-bcf,adf-bdf+ade+bce)\\&=\big(a(ce-df)-b(cf+de),a(cf+de)+b(ce-df)\big)\\&=(a,b)(ce-df,cf+de)\\&=(a,b)\big((c,d)(e,f)\big).\end{aligned}$$

よって $\mathbb{C}$ は乗法に関して結合法則を満たす.

$$\begin{aligned}(a,b)(c,d) &= (ac-bd, ad+bc) = (ca-db, da+cb)\\ &= (c,d)(a,b).\end{aligned}$$

よって $\mathbb{C}$ は乗法に関して交換法則を満たす.

$\mathbb{R}$ の乗法における単位元を 1 とするとき, $\mathbb{C}$ の零元は $(1,0)$ である. 実際,

$$(a,b)(1,0) = (a\cdot 1 - b\cdot 0, a\cdot 0 + b\cdot 1) = (a,b).$$

$(a,b) \neq (0,0)$ の加法における逆元は

$$\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)$$

である. 実際, $a^2+b^2 > 0$ であり,

$$\begin{aligned}(a,b)\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right) &= \left(a\cdot\frac{a}{a^2+b^2} - b\cdot\frac{-b}{a^2+b^2}, a\cdot\frac{-b}{a^2+b^2} + b\cdot\frac{a}{a^2+b^2}\right)\\ &= (1,0).\end{aligned}$$

最後に,

$$\begin{aligned}(a,b)\big((c,d)+(e,f)\big) &= (a,b)(c+e, d+f)\\ &= \big(a(c+e)-b(d+f), a(d+f)+b(c+e)\big)\\ &= \big((ac-bd)+(ae-bf), (ad+bc)+(af+be)\big)\\ &= (ac-bd, ad+bc)+(ae-bf, af+be)\\ &= (a,b)(c,d)+(a,b)(e,f).\end{aligned}$$

よって $\mathbb{C}$ の加法と乗法に関して分配法則が成り立つ.

以上より, $\mathbb{C}$ が体であることが示された. □

$\mathbb{R}$ から $\mathbb{C}$ への写像 φ を, 各 $a \in \mathbb{R}$ に対して

$$\varphi(a) = (a,0)$$

によって定義すると, φ は単射準同型である. 実際, a, $b \in \mathbb{R}$ とするとき,

$$\varphi(a) = \varphi(b) \Longrightarrow (a,0) = (b,0) \Longrightarrow a = b$$

より φ は単射. また,

$$\begin{aligned}\varphi(a)+\varphi(b) &= (a,0)+(b,0) = (a+b,0) = \varphi(a+b),\\ \varphi(a)\varphi(b) &= (a,0)+(b,0) = (ab+0\cdot 0, a\cdot 0 + b\cdot 0) = \varphi(ab)\end{aligned}$$

より φ は準同型である．したがって特に，$\mathbb{R}$ は $\mathbb{C}$ の部分体になる．そこで，$a = (a, 0)$ とみなせば，$\mathbb{C}$ の任意の元 (a, b) は

$$(a, b) = (a, 0) + (b, 0)(0, 1) = a + b(0, 1)$$

と表せる．さらに，

$$(0, 1)^2 = (0 \cdot 0 - 1 \cdot 1, 1 \cdot 0 + 0 \cdot 1) = (-1, 0) = -1$$

が成り立つ．そこで，$(0, 1)$ を $\sqrt{-1}$ で表すことにすると，$(\sqrt{-1})^2 = -1$ である．$\sqrt{-1}$ のことを**虚数単位**と呼ぶ．このとき

$$(a, b) = a + b\sqrt{-1}$$

となる．順序対の性質により，任意の a, b, c, $d \in \mathbb{R}$ に対して

$$(a, b) = (c, d) \Longrightarrow a = b \text{ かつ } c = d.$$

したがって

$$a + b\sqrt{-1} = c + d\sqrt{-1} \Longrightarrow a = b \text{ かつ } c = d$$

となる．

任意の複素数 z は $a + b\sqrt{-1}$, a, $b \in \mathbb{R}$ の形に一意的に表される．a を z の**実数部分**あるいは**実部**といい，$\mathrm{Re}\, z$ で表す．また，b を z の**虚数部分**あるいは**虚部**といい，$\mathrm{Im}\, z$ で表す．

5.2 複素数の絶対値

複素数 $z = a + b\sqrt{-1}$, a, $b \in \mathbb{R}$ に対して

$$|z| = \sqrt{a^2 + b^2}$$

を z の**絶対値**という．

[定理 5.2] $z \in \mathbb{C}$ とする．

(i) $|z| \in \mathbb{R}$ は負でない実数である．

(ii) $|z| = 0 \Longleftrightarrow z = 0$.

[証明] $z = a + b\sqrt{-1}$, a, $b \in \mathbb{R}$ とおく．

(i) $a^2 + b^2 \geq 0$ が成り立つから，$\sqrt{a^2 + b^2}$ は負でない実数である．

(ii) $a = b = 0$ のとき，$a^2 + b^2 = 0$, したがって $\sqrt{a^2 + b^2} = 0$ である．

a, b のどちらか一方が 0 でないとき，$a^2 > 0$ または $b^2 > 0$. このとき $a^2 + b^2 > 0$, したがって $\sqrt{a^2 + b^2} > 0$ である． □

[定理 5.3] z, z_1, $z_2 \in \mathbb{C}$ とする．

(i) $|z_1 z_2| = |z_1|\,|z_2|$

(ii) $z \neq 0$ のとき, $\left|\dfrac{1}{z}\right| = \dfrac{1}{|z|}$.

[証明] (i)　$z_1 = a + b\sqrt{-1}$, $z_2 = c + d\sqrt{-1}$ とおく.

$$\begin{aligned}
|z_1 z_2| &= |(a + b\sqrt{-1})(c + d\sqrt{-1})| \\
&= |(ac - bd) + (ad + bc)\sqrt{-1}| \\
&= (ac - bd)^2 + (ad + bc)^2 \\
&= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 \\
&= (a^2 + b^2)(c^2 + d^2) \\
&= |z_1|\,|z_2|.
\end{aligned}$$

(ii)　(i) を用いると,

$$\left|\frac{1}{z}\right| |z| = \left|\frac{z}{z}\right| = |1| = 1.$$

$z \neq 0$ より $|z| \neq 0$. よって両辺を $|z|$ で割れば求める等式が得られる. □

[定理 5.4] $z \in \mathbb{C}$ とする.

(i) $\mathrm{Re}\, z \leq |\mathrm{Re}\, z|$. 等号は $\mathrm{Re}\, z \geq 0$ のとき.

(ii) $\mathrm{Im}\, z \leq |\mathrm{Im}\, z|$. 等号は $\mathrm{Im}\, z \geq 0$ のとき.

(iii) $|\mathrm{Re}\, z| \leq |z|$. 等号は z が実数のとき.

(iv) $|\mathrm{Im}\, z| \leq |z|$. 等号は z が 0 または純虚数とき.

(v) $\mathrm{Re}\, z \leq |z|$. 等号は z が負でない実数のとき.

(vi) $\mathrm{Im}\, z \leq |z|$. 等号は z が 0 であるか, または $\mathrm{Im}\, z > 0$ なる純虚数のとき.

[証明] (i)　$\mathrm{Re}\, z$ が実数であることから明らか.

(ii)　$\mathrm{Im}\, z$ が実数であることから明らか.

(iii)　$|\mathrm{Re}\, z|^2 \leq |\mathrm{Re}\, z|^2 + |\mathrm{Im}\, z|^2 = |z|^2$. 等号は $|\mathrm{Im}\, z|^2 = 0$ のとき.

(iv)　$|\mathrm{Im}\, z|^2 \leq |\mathrm{Re}\, z|^2 + |\mathrm{Im}\, z|^2 = |z|^2$. 等号は $|\mathrm{Re}\, z|^2 = 0$ のとき.

(v)　(i) と (iii) を合わせればよい.

(vi)　(ii) と (iv) を合わせればよい. □

[定理 5.5] $z_1, z_2 \in \mathbb{C}$ とする.

(i) $|z_1 + z_2| \leq |z_1| + |z_2|$. 等号は $\overline{z_1} z_2$ が負でない実数のとき. この不等式を**三角不等式**という.

(ii) $||z_1| - |z_2|| \leq |z_1 - z_2|$. 等号は $\overline{z_1} z_2$ が実数であって, $|z_1|^2 \leq \overline{z_1} z_2$ または $|z_2|^2 \leq \overline{z_1} z_2$ のとき.

[証明] (i)

$$\begin{aligned}|z_1+z_2|^2 &= (z_1+z_2)(\overline{z_1+z_2}) = (z_1+z_2)(\overline{z_1}+\overline{z_2})\\ &= z_1\overline{z_1}+\overline{z_1}\overline{z_2}+\overline{z_1}z_2+z_2\overline{z_2} = |z_1|^2+2\mathrm{Re}\,(\overline{z_1}z_2)+|z_2|^2\\ &\le |z_1|+2|\overline{z_1}z_2|+|z_2|^2 = |z_1|^2+2|z_1||z_2|+|z_2|^2\\ &= (|z_1|+|z_2|)^2.\end{aligned}$$

等号は $\mathrm{Re}\,(\overline{z_1}z_2) = |\overline{z_1}z_2|$ のとき.

(ii)　三角不等式により

$$|z_1| = |(z_1-z_2)+z_2| \le |z_1-z_2|+|z_2|.$$

同様に

$$|z_2| = |(z_2-z_1)+z_1| \le |z_2-z_1|+|z_1| = |z_1-z_2|+|z_1|.$$

等号は $\overline{(z_1-z_2)}z_2$ または $\overline{(z_2-z_1)}z_1$ が負でない実数のとき. □

[定理 5.6] $z \in \mathbb{C}$ とする.

(i) $|z| \le |\mathrm{Re}\,z|+|\mathrm{Im}\,z|$. 等号は $\mathrm{Re}\,z\,\mathrm{Im}\,z = 0$ のとき.

(ii) $|\mathrm{Re}\,z|+|\mathrm{Im}\,z| \le \sqrt{2}\,|z|$. 等号は $|\mathrm{Re}\,z| = |\mathrm{Im}\,z|$ のとき.

[証明] (i)　三角不等式により

$$|z| = |\mathrm{Re}\,z+\mathrm{Im}\,z\sqrt{-1}| \le |\mathrm{Re}\,z|+|\mathrm{Im}\,z\sqrt{-1}| = |\mathrm{Re}\,z|+|\mathrm{Im}\,z|.$$

等号は $(\overline{\mathrm{Re}\,z}\,\mathrm{Im}\,z)\sqrt{-1}$ が負でない実数のとき.

(ii)

$$\begin{aligned}&2|z|^2-(|\mathrm{Re}\,z|+|\mathrm{Im}\,z|)^2\\ &\quad= 2(\mathrm{Re}\,z+\mathrm{Im}\,z)(\mathrm{Re}\,z-\mathrm{Im}\,z)-(|\mathrm{Re}\,z|+|\mathrm{Im}\,z|)^2\\ &\quad= 2(|\mathrm{Re}\,z|^2+|\mathrm{Im}\,z|^2)-(|\mathrm{Re}\,z|^2+|\mathrm{Im}\,z|^2+2|\mathrm{Re}\,z||\mathrm{Im}\,z|)\\ &\quad= |\mathrm{Re}\,z|^2+|\mathrm{Im}\,z|^2-2|\mathrm{Re}\,z||\mathrm{Im}\,z|\\ &\quad= (|\mathrm{Re}\,z|-|\mathrm{Im}\,z|)^2\\ &\quad\ge 0.\end{aligned}$$

ゆえに $|\mathrm{Re}\,z|+|\mathrm{Im}\,z| \le \sqrt{2}\,|z|$. 等号は $(|\mathrm{Re}\,z|-|\mathrm{Im}\,z|)^2 = 0$ のとき. □

参考文献

[1] 織田進, 柳原弘志: 数をとらえ直す, 裳華房, 2005

[2] 松坂和夫: 代数系入門, 岩波書店. 1976

索 引