数の構成

平成 23 年 4 月
小澤　徹
http://www.ozawa.phys.waseda.ac.jp/index2.html
“Serious numbers will speak to us always,” Paul Simon

ペアノの公理を基礎とした自然数の定義から始めて、整数・有理数・実数・複素数の構成に就いて纏めて置こう。集合・写像・代数系の基礎概念は自由に用いる。

1. 自然数

集合 $\mathbb{N}$, $\mathbb{N}$ の元 e, 写像 $\varphi : \mathbb{N} \to \mathbb{N}$ が次の三つの性質 (P1)(P2)(P3) を持つとき**ペアノの公理**を満たすと謂う：

(P1) φ は単射である

(P2) $\varphi(\mathbb{N}) \subset \mathbb{N}\backslash\{e\}$

(P3) $\mathbb{N}$ の部分集合 M は次の二つの条件 (a)(b) を満たすならば $M = \mathbb{N}$

$$(a) \quad e \in M$$
$$(b) \quad \varphi(M) \subset M$$

定義　ペアノの公理を満たす $(\mathbb{N}, e, \varphi)$ を**ペアノ系**と定義する。集合 $\mathbb{N}$ の元を**自然数**と謂う。

註　(P3) の下で (P2) は $\varphi(\mathbb{N}) = \mathbb{N}\backslash\{e\}$ と同値である。実際 (P2)(P3) の下 $M = \varphi(\mathbb{N}) \cup \{e\}$ と置けば $e \in M, \varphi(M) \subset M$ であるから $M = \mathbb{N}$ となり $\varphi(\mathbb{N}) = \mathbb{N}\backslash\{e\}$ が従う。

定理１（加法の存在と一意性）　任意の $n \in \mathbb{N}$ に対し次の性質 (1)(2) を満たす写像 $f_n : \mathbb{N} \to \mathbb{N}$ が一意的に存在する。

(1) $f_n(e) = \varphi(n)$

(2) $f_n \circ \varphi = \varphi \circ f_n$

更にこのとき次が成立つ。

(3) $f_e = \varphi$

(4) $f_{\varphi(n)} = \varphi \circ f_n = f_n \circ \varphi$

（証明）　先ず (1)(2) を満たす写像の一意性を示そう。もう一つの写像 $f'_n : \mathbb{N} \to \mathbb{N}$ が $f'_n(e) = \varphi(n)$ 及び $f'_n \circ \varphi = \varphi \circ f'_n$ を満たしているとする。集合 M_n を

$$M_n = \{k \in \mathbb{N}; f_n(k) = f'_n(k)\}$$

と定義すると $f_n(e) = \varphi(n) = f'_n(e)$ 故 $e \in M_n$ が従う。任意の $k \in M_n$ を取る。$f_n(k) = f'_n(k)$ であるので (2) より等式

$$f_n(\varphi(k)) = \varphi(f_n(k)) = \varphi(f'_n(k)) = f'_n(\varphi(k))$$

が従う。これは $\varphi(k) \in M_n$ 即ち $\varphi(M_n) \subset M_n$ を意味する。(P3) により $M_n = \mathbb{N}$ 即ち $f_n = f'_n$ を得る。

次に (1)-(4) を満たす f_n を構成しよう。その為 $M = \{n \in \mathbb{N};$ 性質 (1)(2) を満たす写像 $f_n : \mathbb{N} \to \mathbb{N}$ が存在する $\}$ と定義する。$f_e = \varphi$ と置くと $f_e(e) = \varphi(e)$ であり $f_e \circ \varphi = \varphi \circ \varphi = \varphi \circ f_e$ 故 $e \in M$ が従う。任意の $k \in M$ に対し $\varphi(k) \in M$ となる事を示そう。仮定より (1)(2) を満たす $f_k : \mathbb{N} \to \mathbb{N}$ が存在する。そこで $f_{\varphi(k)} = \varphi \circ f_k$ と置くと $f_{\varphi(k)}(e) = (\varphi \circ f_k)(e) = \varphi(f_k(e)) = \varphi(\varphi(k))$ 及び $f_{\varphi(k)} \circ \varphi = (\varphi \circ f_k) \circ \varphi = \varphi \circ (f_k \circ \varphi) = \varphi \circ (\varphi \circ f_k) = \varphi \circ f_{\varphi(k)}$ となり $\varphi(k) \in M$ が従う。(P3) により $M = \mathbb{N}$ 即ち任意の $n \in \mathbb{N}$ に対し (1)-(4) を満たす $f_n : \mathbb{N} \to \mathbb{N}$ の存在が示された。

定義　二項演算 $f_\bullet : \mathbb{N} \times \mathbb{N} \ni (m, n) \mapsto f_m(n) \in \mathbb{N}$ を $\mathbb{N}$ に於ける**加法**と謂う。

定理２（加法の基本性質）

(1) 任意の $n \in \mathbb{N}$ に対し f_n は単射であり不動点を持たない。

(2) $\mathbb{N} \setminus \{e\} = \{f_n(e); n \in \mathbb{N}\}$

(3) **（加法の可換則）**　任意の $m, n \in \mathbb{N}$ に対し

$$f_m(n) = f_n(m)$$

(4) **（加法の結合則）**　任意の $m, n \in \mathbb{N}$ に対し

$$f_m \circ f_n = f_n \circ f_m = f_{f_m(n)} = f_{f_n(m)}$$

（証明）

(1) 集合 M を

$$M = \{n \in \mathbb{N}; f_n \text{は単射である}\}$$

と定義する。$\varphi = f_e$ は単射であるから $e \in M$ が従う。任意の $n \in M$ を取る。f_n は単射故 $f_{\varphi(n)} = \varphi \circ f_n$ も単射となり $\varphi(n) \in M$ が従う。故に $M = \mathbb{N}$ である。次に $n \in \mathbb{N}$ に対し

$$M_n = \{k \in \mathbb{N}; f_n(k) \neq k\}$$

と定義する。$f_n(e) = \varphi(n) \in \varphi(\mathbb{N}) = \mathbb{N} \setminus \{e\}$ 故 $e \in M$ が従う。任意の $k \in \mathbb{N}$ を取る。$f_n(k) \neq k$ であり φ は単射であるから $\varphi(f_n(k)) \neq \varphi(k)$ が従い左辺は $f_n(\varphi(k))$ に等しいので $\varphi(k) \in M_n$ が従う。故に $M_n = \mathbb{N}$ となる。

(2) 集合 M を

$$M = \{e\} \cup \{f_n(e); n \in \mathbb{N}\}$$

と定義する。$f_n(e) = \varphi(n) \in \varphi(\mathbb{N}) = \mathbb{N} \setminus \{e\}$ 故 $e \notin \{f_n(e); n \in \mathbb{N}\}$ が従う。任意の $m \in M$ を取る。$m = e$ なら $\varphi(e) = f_e(e)$ 故 $\varphi(e) \in M$ となる。$m \neq e$ なら $n \in \mathbb{N}$ が存在して $m = f_n(e)$ となる。このとき $\varphi(m) = (\varphi \circ f_n)(e) = f_{\varphi(n)}(e)$ より $\varphi(m) \in M$ となる。以上より $\varphi(M) \subset M$ を得るので $M = \mathbb{N}$ となる。これより (2) が従う。

(3) $n \in \mathbb{N}$ に対し

$$M_n = \{k \in \mathbb{N}; f_n(k) = f_k(n)\}$$

と定義する。$f_n(e) = \varphi(n) = f_e(n)$ 故 $e \in M$ が従う。任意の $k \in M_n$ を取る。等式 $f_n(k) = f_k(n)$ より $f_n(\varphi(k)) = \varphi(f_n(k)) = \varphi(f_k(n)) = (\varphi \circ f_k)(n) = f_{\varphi(k)}(n)$ を得るので $\varphi(k) \in M_n$ が従う。以上より $\varphi(M_n) \subset M_n$ 更に $M_n = \mathbb{N}$ が従う。

(4) $m, n \in \mathbb{N}$ に対し

$$M_{m,n} = \{k \in \mathbb{N}; (f_m \circ f_n)(k) = f_{f_m(n)}(k)\}$$

と定義する。$f_m(f_n(e)) = f_m(\varphi(n)) = \varphi(f_m(n)) = f_{f_m(n)}(e)$ 故 $e \in M_{m,n}$ が従う。任意の $k \in M_{m,n}$ を取る。等式 $f_m(f_n(k)) = f_{f_m(n)}(k)$ より

$$(f_m \circ f_n)(\varphi(k)) = \varphi(f_m(f_n(k))) = \varphi(f_{f_m(n)}(k)) = f_{f_m(n)}(\varphi(k))$$

を得るので $\varphi(k) \in M_{m,n}$ が従う。以上より任意の $m, n \in \mathbb{N}$ に対し

$$f_m \circ f_n = f_{f_m(n)}$$

が成立つ。(3) により $f_m(n) = f_n(m)$ であり上式で m と n を入れ替えると

$$f_m \circ f_n = f_{f_m(n)} = f_{f_n(m)} = f_n \circ f_m$$

が従う。

定理３（自然数の比較可能性）　任意の $m, n \in \mathbb{N}$ に対し、次の三つの場合の何れかの一つが成立つ：

(1) 唯一つの $j \in \mathbb{N}$ が存在して　$m = f_j(n)$

(2) $m = n$

(3) 唯一つの $k \in \mathbb{N}$ が存在して　$n = f_k(m)$

（証明）　定理２の (1) より、上の (1) と (2) は同時に成立せず、(2) と (3) も同時に成立しない。また (1) と (3) が同時に成立つと仮定すれば $m = f_j(n) = f_j(f_k(m)) = f_{f_j(k)}(m)$ となり定理２の (1) に矛盾する。さて任意の $n \in \mathbb{N}$ を取る。集合 M_n を

$$M_n = \{m \in \mathbb{N}; m \text{ は } n \text{ に対し (1)(2)(3) の何れか一つを満たす}\}$$

と定義する。先ず $e \in M_n$ を示そう。$n = e$ なら (2) が成立する事になる。$n \neq e$ なら $n \in \mathbb{N} \setminus \{e\}$ なので定理 2 の (2) により (3) が成立する事になる。次に $\varphi(M_n) \subset M_n$ を示そう。任意の $m \in M_n$ を取る。m は n に対し (1)(2)(3) の何れか一つを満たしている。

(1) の場合：唯一つの $j \in \mathbb{N}$ が在って $m = f_j(n)$ となる。このとき $\varphi(m) = (\varphi \circ f_j)(n) = f_{\varphi(j)}(n)$ となり $\varphi(m)$ は n に対し (1) を満たす。

(2) の場合：$m = n$ より $\varphi(m) = \varphi(n) = f_e(n)$ が従うので $\varphi(m)$ は n に対し (1) を満たす。

(3) の場合：唯一つの $k \in \mathbb{N}$ が在って $n = f_k(m)$ となる。このとき $k = e$ なら $\varphi(m) = f_e(m) = n$ 故 $\varphi(m)$ は n に対し (2) を満たす。$k \neq e$ なら $k \in \mathbb{N} \setminus \{e\}$ 故定理 2 の (2) により $\ell \in \mathbb{N}$ が存在し $k = f_\ell(e)$ となる。従って $n = f_k(m) = f_{f_\ell(e)}(m) = (f_\ell \circ f_e)(m) = f_\ell(\varphi(m))$ となり $\varphi(m)$ は n に対し (3) を満たす。

以上により $M_n = \mathbb{N}$ が従う。これが示すべき事であった。

定義　$n \in \mathbb{N}$ に依る $\mathbb{N}$ の**切片** $\mathbb{N}_{<n}$ を

$$\mathbb{N}_{<n} = \{m \in \mathbb{N}; \text{唯一つの } k \in \mathbb{N} \text{ が存在して } n = f_k(m)\}$$

で定義する。また

$$\mathbb{N}_{\leq n} = \{n\} \cup \mathbb{N}_{<n}$$

と表す。

命題１（切片の基本性質）

(1) $\mathbb{N}_{<e} = \emptyset, \quad \mathbb{N}_{\leq e} = \mathbb{N}_{<\varphi(e)} = \{e\}, \ \mathbb{N}_{\leq \varphi(e)} = \{e, \varphi(e)\}$

(2) 任意の $n \in \mathbb{N}$ に対し

$$\mathbb{N}_{<\varphi(n)} = \mathbb{N}_{\leq n} = \{n\} \cup \mathbb{N}_{<n}, \ \{n\} \cap \mathbb{N}_{<n} = \emptyset$$
$$\mathbb{N}_{\leq \varphi(n)} = \{\varphi(n)\} \cup \mathbb{N}_{\leq n} = \{n, \varphi(n)\} \cup \mathbb{N}_{<n}$$

(3)　任意の $n \in \mathbb{N}$ 及び任意の $m \in \mathbb{N}_{\leq n}$ に対し $\mathbb{N}_{\leq m} \subset \mathbb{N}_{\leq n}$

(4)　任意の $n \in \mathbb{N}$ 及び任意の $m \in \mathbb{N}_{<n}$ に対し $\mathbb{N}_{\leq m} \subset \mathbb{N}_{<n}$

(5)　任意の $n \in \mathbb{N}$ 及び任意の $m \in \mathbb{N}_{\leq n}$ に対し $\mathbb{N}_{<m} \subset \mathbb{N}_{<n}$

(6)　$m, n \in \mathbb{N}$ に対し次は同値

(i) $m = n$　(ii) $\mathbb{N}_{\leq m} = \mathbb{N}_{\leq n}$　(iii) $\mathbb{N}_{<m} = \mathbb{N}_{<n}$

(7)　任意の $n \in \mathbb{N} \setminus \{e\}$ 及び任意の $k \in \mathbb{N}_{<n}$ に対し $\varphi(k) \in \mathbb{N}_{\leq n}$

(8)　任意の $n \in \mathbb{N}$ に対し $\varphi(\mathbb{N}_{<n}) = \mathbb{N}_{<\varphi(n)} \setminus \{e\}, \ \varphi(\mathbb{N}_{\leq n}) = \mathbb{N}_{\leq \varphi(n)} \setminus \{e\}$

(9)　$\{e\} = \bigcap \{\mathbb{N}_{\leq n}; n \in \mathbb{N}\}$

（証明）

(1) $\mathbb{N}_{<e} \neq \emptyset$ ならば $m, k \in \mathbb{N}$ が存在して $e = f_k(m)$ を満たす。$k = e$ ならば $e = f_e(m) = \varphi(m) \in \mathbb{N}\backslash\{e\}$ となり矛盾。$k \neq e$ なら定理２の (2) により $\ell \in \mathbb{N}$ が存在して $k = f_\ell(e)$ と表される。このとき $e = f_k(m) = f_{f_\ell(e)}(m) = (f_e \circ f_\ell)(m) = \varphi(f_\ell(m)) \in \mathbb{N} \setminus \{e\}$ となり矛盾。よって $\mathbb{N}_{<e} = \emptyset$ が従う。$\varphi(e) = f_e(e)$ より $e \in \mathbb{N}_{<\varphi(e)}$ となる。一方 $\varphi(e) = f_k(m)$ なる $k, m \in \mathbb{N}$ が存在したとする。$k \neq e$ なら上と同様 $k = f_\ell(e)$ なる $\ell \in \mathbb{N}$ が存在するので $\varphi(e) = \varphi(f_\ell(m))$ が成立するが φ の単射性により $e = f_\ell(m)$ を得る事になり上の議論からこれは矛盾である。従って $k = e, \varphi(e) = f_e(m)$ の可能性のみ残される事となるが $f_e = \varphi$ の単射性により $e = m$ が従う。故に $\mathbb{N}_{<\varphi(e)} = \{e\}$ を得る。定義により $\mathbb{N}_{\leq e} = \{e\} \cup \mathbb{N}_{<e} = \{e\}$ 及び $\mathbb{N}_{\leq\varphi(e)} = \{\varphi(e)\} \cup \mathbb{N}_{<\varphi(e)} = \{e, \varphi(e)\}$ が従う。

(2) 定理２の (1) より $n \notin \mathbb{N}_{<n}$ であるので $\{n\} \cap \mathbb{N}_{<n} = \emptyset$ が従う。次に $\mathbb{N}_{<n} \subset \mathbb{N}_{<\varphi(n)}$ を示そう。任意の $m \in \mathbb{N}_{<n}$ に対し $k \in \mathbb{N}$ が存在し $n = f_k(m)$ となる。このとき $\varphi(n) = \varphi(f_k(m)) = f_{f_k(e)}(m)$ 故 $m \in \mathbb{N}_{<\varphi(n)}$ となり $\mathbb{N}_{<n} \subset \mathbb{N}_{<\varphi(n)}$ が従う。さて $n \in \mathbb{N}_{<\varphi(n)}$ である事は $\varphi(n) = f_e(n)$ より直ちに従う。$m \in \mathbb{N}_{<\varphi(n)}\backslash\mathbb{N}_{<n}$ とすると $k \in \mathbb{N}$ が存在して $\varphi(n) = f_k(m)$ を得る。ここで $k = e$ なら φ の単射性により $m = n$ となる。$k \neq e$ なら前と同様 $k = f_\ell(e)$ なる $\ell \in \mathbb{N}$ が在って $\varphi(n) = \varphi(f_\ell(m))$ となり φ の単射性により $n = f_\ell(m)$ が従うがこれは $m \notin \mathbb{N}_{<n}$ に矛盾する。以上より $\mathbb{N}_{<\varphi(n)} = \{n\} \cup \mathbb{N}_{<n}$ が従う。(2) の残りの関係式は定義より直ちに従う。

(3) $n \in \mathbb{N}$ 及び $m \in \mathbb{N}_{\leq n}$ を取る。$m = n$ ならば包含関係は等式として成立つ。$m \neq n$ ならば $m \in \mathbb{N}_{<n}$ 故 $k \in \mathbb{N}$ が在って $n = f_k(m)$ となる。任意の $j \in \mathbb{N}_{\leq m}$ に対し $j = m$ ならば $j = m \in \mathbb{N}_{<n} \subset \mathbb{N}_{\leq n}$ であり $j \in \mathbb{N}_{<m}$ ならば $\ell \in \mathbb{N}$ が在って $m = f_\ell(j)$ となる。このとき $n = f_k(m) = (f_k \circ f_\ell)(j) = f_{f_k(\ell)}(j)$ 故 $j \in \mathbb{N}_{<n}$ となる。以上より $\mathbb{N}_{\leq m} \subset \mathbb{N}_{\leq n}$ が従う。

(4) (3) の証明より従う。

(5) (3) の証明より従う。

(6) (i)⇒ (ii), (i)⇒ (iii) であるので (ii)⇒(i) 及び (iii)⇒(i) を示せば良い。$\mathbb{N}_{\leq m} = \mathbb{N}_{\leq n}$ であるとする。$m \in \mathbb{N}_{\leq n}$ 故 $m = n$ であるか或る $j \in \mathbb{N}$ に対して $n = f_j(m)$ であるかのどちらかである。一方 $n \in \mathbb{N}_{\leq m}$ 故 $n = m$ であるか或る $k \in \mathbb{N}$ に対して $m = f_k(n)$ であるかのどちらかである。このうち $m = n$ の場合以外 f_j または f_k が不動点を持つ事になり矛盾を生ずる。故に $m = n$ が成立つ。次に $\mathbb{N}_{<m} = \mathbb{N}_{<n}$ であるとする。$m \neq n$ とすると定理３により $m = f_j(n)$ なる $j \in \mathbb{N}$ が存在するか $n = f_k(m)$ なる $k \in \mathbb{N}$ が存在する。前者なら $m \in \mathbb{N}_{<n}$ であるが $m \notin \mathbb{N}_{<m}$ 故矛盾であり後者なら $n \in \mathbb{N}_{<m}$ であるが $n \notin \mathbb{N}_{<n}$ 故矛盾である。故に $m = n$ が成立つ。

(7) $n \in \mathbb{N} \setminus \{e\}$ 及び $k \in \mathbb{N}_{<n}$ に対し $\ell \in \mathbb{N}$ が在って $n = f_\ell(k)$ となる。このとき $\varphi(n) = \varphi(f_\ell(k)) = f_\ell(\varphi(k))$ 故 $\varphi(k) \in \mathbb{N}_{<\varphi(n)} = \mathbb{N}_{\leq n}$ が従う。

(8) (7) より $\varphi(\mathbb{N}_{<n}) \subset \mathbb{N}_{<\varphi(n)}$ が従う。$\varphi(\mathbb{N}_{<n}) \subset \varphi(\mathbb{N}) = \mathbb{N}\setminus\{e\}$ より $\varphi(\mathbb{N}_{<n}) \subset \mathbb{N}_{<\varphi(n)} \setminus \{e\}$ が従う。任意の $m \in \mathbb{N}_{<\varphi(n)} \setminus \{e\}$ に対し $j \in \mathbb{N}$ が在って $\varphi(n) = f_j(m)$ となる。

$m \in \mathbb{N} \setminus \{e\} = \varphi(\mathbb{N})$ 故 $k \in \mathbb{N}$ が在って $m = \varphi(k)$ となるので $\varphi(n) = f_j(\varphi(k)) = \varphi(f_j(k))$ が従う。φ の単射性により $n = f_j(k)$ となるので $k \in \mathbb{N}_{<n}$ となり $m = \varphi(k) \in \varphi(\mathbb{N}_{<n})$ が従う。以上より $\varphi(\mathbb{N}_{<n}) = \mathbb{N}_{<\varphi(n)} \setminus \{e\}$ となる。両辺に $\{\varphi(n)\}$ を合併すれば $\varphi(\mathbb{N}_{\leq n}) = \mathbb{N}_{\leq\varphi(n)} \setminus \{e\}$ が従う。

(9) 定理 2 の (2) より任意の $n \in \mathbb{N}$ に対し $e \in \mathbb{N}_{\leq n}$ となる。一方 $m \in \bigcap\{\mathbb{N}_{\leq n}; n \in \mathbb{N}\}$ なら $n = e$ として $m \in \mathbb{N}_{\leq e} = \{e\}$ となり $m = e$ が従う。

定理 4（帰納法に依る点列の定義）　X を集合とし a を X の元とする。$\Phi : \mathbb{N} \times X \to X$ を写像とする。このとき写像 $F : \mathbb{N} \to X$ で次の性質 (1)(2) を満たすものが唯一つ存在する。

(1) $F(e) = a$

(2) 任意の $n \in \mathbb{N}$ に対し $F(\varphi(n)) = \Phi(n, F(n))$

（証明）　先ず (1)(2) を満たす写像の一意性を示そう。もう一つの写像 $F' : \mathbb{N} \to X$ が $F'(e) = a$ 及び $F'(\varphi(n)) = \Phi(n, F'(n))$ を任意の $n \in \mathbb{N}$ に就いて満たしているとする。集合 M を

$$M = \{n \in \mathbb{N}; F(n) = F'(n)\}$$

と定義する。$F(e) = a = F'(e)$ 故 $e \in M$ が従う。任意の $n \in M$ を取る。$F(n) = F'(n)$ であるので $F(\varphi(n)) = \Phi(n, F(n)) = \Phi(n, F'(n)) = F'(\varphi(n))$ となり $\varphi(n) \in M$ が従う。以上より $M = \mathbb{N}$ 即ち $F = F'$ を得る。

次に (1)(2) を満たす F を構成しよう。その為

$M = \{n \in \mathbb{N}; $任意の$\ell \in \mathbb{N}_{\leq n}$に対し写像$F_\ell : \mathbb{N}_{\leq\ell} \to X$が存在し条件$(i)_n(ii)_n(iii)_n$を満たす$\}$

と定義する。ここに

$(\mathrm{i})_n$ $F_n(e) = a$

$(\mathrm{ii})_n$ 任意の $k \in \mathbb{N}_{<n}$ に対し $F_n(\varphi(k)) = \Phi(k, F_n(k))$

$(\mathrm{iii})_n$ 任意の $m \in \mathbb{N}_{<n}, k \in \mathbb{N}_{\leq m}$ に対し $F_n(k) = F_m(k)$

とする。

さて $F_e : \mathbb{N}_{\leq e} \to X$ を $F_e(e) = a$ と定義すると $e \in M$ が従う。任意に $n \in M$ を取る。このとき任意の $\ell \in \mathbb{N}_{\leq n}$ に対し $F_\ell : \mathbb{N}_{\leq\ell} \to X$ が存在して上の $(\mathrm{i})_n(\mathrm{ii})_n(\mathrm{iii})_n$ が満たされている。そこで $F_{\varphi(n)} : \mathbb{N}_{\leq\varphi(n)} \to X$ を

$$\begin{cases} F_{\varphi(n)}(k) = F_n(k), \quad k \in \mathbb{N}_{\leq n} \\ F_{\varphi(n)}(\varphi(n)) = \Phi(n, F_n(n)) \end{cases}$$

と定義する。$F_{\varphi(n)}(e) = F_n(e) = a$ 故 $F_{\varphi(n)}$ は $(\mathrm{i})_{\varphi(n)}$ を満たす。任意の $k \in \mathbb{N}_{<\varphi(n)} = \{n\} \cup \mathbb{N}_{<n}$ を取る。$k \in \mathbb{N}_{<n}$ なら $\varphi(k) \in \mathbb{N}_{\leq n}$ 故 $F_{\varphi(n)}$ の定義より $F_{\varphi(n)}(\varphi(k)) = F_n(\varphi(k))$ と

なり F_n は $(\mathrm{ii})_n$ を満たすから $F_n(\varphi(k)) = \Phi(k, F_n(k))$ であり $F_{\varphi(n)}(\varphi(k)) = \Phi(k, F_m(k)) = \Phi(k, F_{\varphi(n)}(k))$ が従う。$k = n$ なら $F_{\varphi(n)}$ の定義より $F_{\varphi(n)}(\varphi(n)) = \Phi(n, F_n(n)) = \Phi(n, F_{\varphi(n)}(n))$ が従う。故に $F_{\varphi(n)}$ は $(\mathrm{ii})_{\varphi(n)}$ を満たす。さて任意の $m \in \mathbb{N}_{<\varphi(n)},\ k \in \mathbb{N}_{\leq m}$ を取る。このとき $k \in \mathbb{N}_{\leq n}$ 故 $F_{\varphi(n)}$ の定義により $F_{\varphi(n)}(k) = F_n(k)$ であり $m = n$ ならこの等式は $F_{\varphi(n)}(k) = F_m(k)$ を意味し $m \in \mathbb{N}_{<n}$ なら $(\mathrm{iii})_n$ により $F_{\varphi(n)}(k) = F_m(k)$ が従う。故に $F_{\varphi(n)}$ は $(\mathrm{iii})_{\varphi(n)}$ を満たす。

以上より $\varphi(M) \subset M$ となり $M = \mathbb{N}$ が従う。
そこで $F : \mathbb{N} \to X$ を $F(n) = F_n(n), n \in \mathbb{N}$ と定めると

$$F(e) = F_e(e) = a$$

$$F(\varphi(n)) = F_{\varphi(n)}(\varphi(n)) = \Phi(n, F_n(n)) = \Phi(n, F(n))$$

となり性質 (1)(2) が満たされる事が分かる。

定理５（ペアノ系の一意性）

ペアノ系は同型を除いて一意的である。即ち $(\mathbb{N}, e, \varphi)$ と $(\mathbb{N}', e', \varphi')$ を二つの自然数の系とすると次の性質 (1)(2) を満たす全単射 $F : \mathbb{N} \to \mathbb{N}'$ が唯一つ存在する：

(1) $F(e) = e'$

(2) $F \circ \varphi = \varphi' \circ F$ 即ち任意の $n \in \mathbb{N}$ に対し $F(\varphi(n)) = \varphi'(F(n))$

$$\begin{array}{ccc} \mathbb{N} & \xrightarrow{F} & \mathbb{N}' \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi'} \\ \mathbb{N} & \xrightarrow{F} & \mathbb{N}' \end{array}$$

（証明）　定理４を $X = \mathbb{N}',\ \Phi(n, n') = \varphi(n'),\ (n, n') \in \mathbb{N} \times X$ に対して用いると $F : \mathbb{N} \to \mathbb{N}'$ が一意的に存在し (1)(2) が成立つ事が分かる。
次に F の全射性を示そう。$\mathbb{N}'$ の部分集合 M' を

$$M' = \{F(n) \in \mathbb{N}'; n \in \mathbb{N}\}$$

と定義する。(1) より $e' \in M'$ が従う。任意に $m' \in M'$ を取る。$n \in \mathbb{N}$ が在って $m' = F(n)$ となる。このとき $\varphi'(m') = (\varphi' \circ F)(n) = F(\varphi(n))$ 故 $\varphi'(m') \in M$ 即ち $\varphi'(M') \subset M'$ が従う。$(\mathbb{N}', e', \varphi')$ はペアノの公理を満たすので $M' = \mathbb{N}'$ となり f の全射性が従う。
　最後に F の単射性を示そう。$\mathbb{N}$ の部分集合 M を

$$M = \{n \in \mathbb{N}; m \in \mathbb{N} \text{ が存在し } F(n) = F(m) \text{ なるとき } m = n\}$$

と定義する。$M = \mathbb{N}$ を示せば良い。

$e \in M$ なること：　$m \in \mathbb{N}$ は $F(e) = F(m)$ を満たすとする。$m \neq e$ ならば $n \in \mathbb{N}$ が在って $m = \varphi(n)$ となる。このとき $F(m) = F(\varphi(n)) = \varphi'(F(n))$ より $e' = F(e) = F(m) = \varphi'(F(m)) \in \varphi'(\mathbb{N}') = \mathbb{N}' \setminus \{e'\}$ を得るが、これは矛盾である。

$\varphi(M) \subset M$ **なること：**　任意に $n \in M$ を取る。$m \in \mathbb{N}$ は $F(\varphi(n)) = F(m)$ を満たすとして $m \neq \varphi(n)$ を仮定する。$m = e$ なら $F(\varphi(n)) = F(e)$ となり $e \in M$ 故 $e = \varphi(n)$ が従い矛盾となる。$m \neq e$ なら $k \in \mathbb{N}$ が在って $m = \varphi(k)$ となる。このとき $\varphi'(F(n)) = F(\varphi(n)) = F(m) = F(\varphi(k)) = \varphi'(F(k))$ となり φ' は単射故 $F(n) = F(k)$ が従う。$n \in M$ 故 $n = k$ が従う。故に $\varphi(n) = \varphi(k) = m$ となり矛盾を生ずる。以上より $\varphi(n) = m$ となり $\varphi(n) \in M$ が従う。

定理６（乗法の存在と一意性）　任意の $n \in \mathbb{N}$ に対し次の性質 (1)(2) を満たす写像 $g_n : \mathbb{N} \to \mathbb{N}$ が一意的に存在する：

(1) $g_n(e) = n$

(2) $g_n \circ \varphi = f_n \circ g_n$

更にこのとき次が成立つ。

(3) $g_e = id$

(4) 任意の $m \in \mathbb{N}$ に対して $g_{\varphi(n)}(m) = f_m(g_n(m))$

（証明）　先ず (1)(2) を満たす写像の一意性を示そう。もう一つの写像 $g'_n : \mathbb{N} \to \mathbb{N}$ が $g'_n(e) = n$ 及び $g'_n \circ \varphi = f_n \circ g'_n$ を満たしているとする。集合 M_n を

$$M_n = \{k \in \mathbb{N}; g_n(k) = g'_n(k)\}$$

と定義すると $g_n(e) = n = g'_n(e)$ 故 $e \in M_n$ が従う。任意の $k \in M_n$ を取る。$g_n(k) = g'_n(k)$ であるので (2) より等式

$$g_n(\varphi(k)) = f_n(g_n(k)) = f_n(g'_n(k)) = g'_n(\varphi(k))$$

が従う。これは $\varphi(k) \in M_n$ 即ち $\varphi(M_n) \subset M_n$ を意味する。従って $M_n = \mathbb{N}$ 即ち $g_n = g'_n$ を得る。

次に (1)-(4) を満たす g_n を構成しよう。その為 $M = \{n \in \mathbb{N};$ 性質 (1)(2) を満たす写像 $g_n : \mathbb{N} \to \mathbb{N}$ が存在する $\}$ と定義する。$g_e = id$ と置くと $g_e(e) = e$ であり $g_e \circ \varphi = \varphi = f_e = f_e \circ g_e$ 故 $e \in M$ が従う。任意の $k \in M$ を取る。$\varphi(k) \in M$ となる事を示そう。仮定により (1)(2) を満たす $g_k : \mathbb{N} \to \mathbb{N}$ が存在する。そこで $g_{\varphi(k)} : \mathbb{N} \to \mathbb{N}$ を $g_{\varphi(k)}(m) = f_m(g_k(m)),\ m \in \mathbb{N}$ で定めると $g_{\varphi(k)}(e) = f_e(g_k(e)) = f_e(k) = \varphi(k)$ となり $g_{\varphi(k)}$ は (1) を満たす。また $g_k \circ \varphi = f_k \circ g_k$ であるから

$$\begin{aligned}(g_{\varphi(k)} \circ \varphi)(m) &= g_{\varphi(k)}(\varphi(m)) = f_{\varphi(m)}(g_k(\varphi(m))) = f_{\varphi(m)}(f_k(g_k(m))) \\ &= (f_m \circ \varphi \circ f_k)(g_k(m)) \\ &= (f_m \circ f_{\varphi(k)})(g_k(m)) \\ &= (f_{\varphi(k)} \circ f_m)(g_k(m)) \\ &= f_{\varphi(k)}(g_{\varphi(k)}(m)) = (f_{\varphi(k)} \circ g_{\varphi(k)})(m)\end{aligned}$$

となり $g_{\varphi(k)}$ は (2) も満たす。以上で $M = \mathbb{N}$ 即ち任意の $n \in \mathbb{N}$ に対し (1)-(4) を満たす $g_n : \mathbb{N} \to \mathbb{N}$ の存在が示された。

定義　二項演算 $g_\bullet : \mathbb{N} \times \mathbb{N} \ni (m, n) \mapsto g_m(n) \in \mathbb{N}$ を $\mathbb{N}$ に於ける**乗法**と謂う。

定理 7（乗法の基本性質）

(1) 任意の $n \in \mathbb{N}$ に対し g_n は単射であり $n \neq e$ ならば g_n は不動点を持たない。

(2) $\mathbb{N} = \{g_n(e); n \in \mathbb{N}\}$

(3) **（乗法の可換則）**任意の $m, n \in \mathbb{N}$ に対し

$$g_m(n) = g_n(m)$$

(4) **（乗法の結合則）**任意の $m, n \in \mathbb{N}$ に対し

$$g_m \circ g_n = g_n \circ g_m = g_{g_m(n)} = g_{g_n(m)}$$

(5) **（加法に対する乗法の分配則）**　任意の $m, n \in \mathbb{N}$ に対し

$$g_m \circ f_n = f_{g_m(n)} \circ g_m$$

（証明）　(2)(3)(5)(4)(1) の順に証明する。

(2) $g_n(e) = n$ より (2) が従う。

(3) 任意の $n \in \mathbb{N}$ に対し集合 M_n を

$$M_n = \{m \in \mathbb{N}; g_m(n) = g_n(m)\}$$

と定義する。$g_n(e) = n = g_e(n)$ 故 $e \in M_n$ が従う。任意に $m \in \mathbb{N}$ を取る。このとき $g_m(n) = g_n(m)$ であるので $g_{\varphi(m)}(n) = f_n(g_m(n)) = f_n(g_n(m)) = g_n(\varphi(m))$ となり $\varphi(m) \in M_n$ が従う。これより $M_n = \mathbb{N}$ となり (3) が従う。

(5) 任意の $m, n \in \mathbb{N}$ に対し集合 $M_{m,n}$ を

$$M_{m,n} = \{k \in \mathbb{N}; (g_m \circ f_n)(k) = (f_{g_m(n)} \circ g_m)(k)\}$$

と定義する。$(g_m \circ f_n)(e) = g_m(\varphi(n)) = (f_m \circ g_m)(n) = f_m(g_m(n)) = f_{g_m(n)}(m) = f_{g_m(n)}(g_m(e)) = (f_{g_m(n)} \circ g_m)(e)$ より $e \in M_{m,n}$ が従う。任意に $k \in M_{m,n}$ を取る。このとき $(g_m \circ f_n)(k) = (f_{g_m(n)} \circ g_m)(k)$ であるので $(g_m \circ f_n)(\varphi(k)) = (g_m \circ \varphi \circ f_n)(k) = (f_m \circ g_m \circ f_n)(k) = (f_m \circ f_{g_m(n)} \circ g_m)(k) = (f_{g_m(n)} \circ f_m \circ g_m)(k) = (f_{g_m(n)} \circ g_m)(\varphi(k))$ となり $\varphi(k) \in M_{m,n}$ が従う。これより $M_{m,n} = \mathbb{N}$ となり (5) が従う。

(4) 任意の $m, n \in \mathbb{N}$ に対し集合 $M_{m,n}$ を

$$M_{m,n} = \{k \in \mathbb{N}; (g_m \circ g_n)(k) = g_{g_m(n)}(k)\}$$

と定義する。$(g_m \circ g_n)(e) = g_m(n) = g_{g_m(n)}(e)$ より $e \in M_{m,n}$ が従う。任意に $k \in M_{m,n}$ を取る。このとき $(g_m \circ g_n)(k) = g_{g_m(n)}(k)$ であるので $(g_m \circ g_n)(\varphi(k)) = (g_m \circ f_n \circ g_n)(k) = (f_{g_m(n)} \circ g_m \circ g_n)(k) = (f_{g_m(n)} \circ g_{g_m(n)})(k) = g_{g_m(n)}(\varphi(k))$ となり $\varphi(k) \in M_{m,n}$ が従う。

これより $M_{m,n} = \mathbb{N}$ となり (4) が従う。

(1) 任意に $n \in \mathbb{N}$ を取る。$m, m' \in \mathbb{N}$ が在って $g_n(m) = g_n(m')$ が成立しているとする。定理 3 により次の三つの場合の何れか一つが成立している：

(a) $j \in \mathbb{N}$ が存在して $m = f_j(m')$

(b) $m = m'$

(c) $k \in \mathbb{N}$ が存在して $m' = f_k(m)$

(a) の場合 $f_{g_n(j)}(g_n(m')) = g_n(f_j(m')) = g_n(m) = g_n(m')$ となるが $f_{g_n(j)}$ は不動点を持たないから矛盾である。(c) の場合 $f_{g_n(k)}(g_n(m)) = g_n(f_k(m)) = g_n(m') = g_n(m)$ となるが $f_{g_n(k)}$ は不動点を持たないから矛盾である。従って (b) の場合のみ成立し g_n の単射性が従う。

最後に、不動点を持つ g_n は $n = e$ の場合に限る事を示そう。$m \in \mathbb{N}$ が存在して $g_n(m) = m$ が成立しているものとする。$n \neq e$ でなければ定理 2 の (2) により $j \in \mathbb{N}$ が在って $n = f_j(e)$ と表される。このとき

$$m = g_n(m) = g_m(n) = (g_m \circ f_j)(e) = f_{g_m(j)}(g_m(e)) = f_{g_m(j)}(m)$$

となるが $f_{g_m(j)}$ は不動点を持たないから矛盾である。よって $n = e$ が従う。

定理 8（算法の単調性）

(1) 任意の $m, n \in \mathbb{N}$ に対し $n \in \mathbb{N}_{\leq g_m(n)} \cap \mathbb{N}_{< f_m(n)}$

(2) 任意の $m, m' \in \mathbb{N}$ 及び任意の $n \in \mathbb{N}_{<m}, n' \in \mathbb{N}_{\leq m'}$ に対し

$$f_n(n') \in \mathbb{N}_{< f_m(m')}, \quad g_n(n') \in \mathbb{N}_{< g_m(m')}$$

（証明）(1)　任意の $n \in \mathbb{N}$ に対し集合 M_n を

$$M_n = \{m \in \mathbb{N}; n \in \mathbb{N}_{\leq g_m(n)}\}$$

と定義する。$g_e(n) = n$ 故 $e \in M_n$ が従う。任意に $m \in M_n$ を取る。このとき $n \in \mathbb{N}_{\leq g_m(n)}$ であるから $n = g_m(n)$ であるか $j \in \mathbb{N}$ が在って $g_m(n) = f_j(n)$ が成立つ。前者なら g_m の不動点が存在する事になるので $m = e$ であり $g_{\varphi(e)}(n) = f_n(g_e(n)) = f_n(n)$ より $n \in \mathbb{N}_{\leq g_{\varphi(e)}(n)}$

となり、後者なら $g_{\varphi(m)}(n)=f_n(g_m(n))=(f_n\circ f_j)(n)=f_{f_j(n)}(n)$ より $n\in\mathbb{N}_{\leq g_{\varphi(m)}(n)}$ となる。これより $\varphi(M_n)\subset M_n$ となり $M_n=\mathbb{N}$ が従う。次に任意の $n\in\mathbb{N}$ に対し集合 M_n を

$$M_n=\{m\in\mathbb{N};n\in\mathbb{N}_{<f_m(n)}\}$$

と定義する。$f_e(n)=\varphi(n)$ 及び $n\in\mathbb{N}_{\leq n}=\mathbb{N}_{<\varphi(n)}$ より $e\in M_n$ が従う。任意に $m\in M_n$ を取る。$n\in\mathbb{N}_{<f_m(n)}$ であるから $j\in\mathbb{N}$ が在って $f_m(n)=f_j(n)$ となる。これより $f_{\varphi(m)}(n)=(\varphi\circ f_m)(n)=(\varphi\circ f_j)(n)=f_{\varphi(j)}(n)$ となり $n\in\mathbb{N}_{<f_{\varphi(m)}(n)}$ 即ち $\varphi(m)\in M_n$ が従う。故に $M_n=\mathbb{N}$ が従う。

(2) $n\in\mathbb{N}_{<m}$ 及び $n'\in\mathbb{N}_{<m'}$ に対し j 及び k が在って $m=f_j(n)$ 及び $m'=f_k(n')$ が成立つ。このとき

$$\begin{aligned}&f_m(m')=f_m(f_k(n'))=f_{f_k(m)}(n')=f_{n'}(f_k(m))=f_{n'}(f_k(f_j(n)))\\&=f_k(f_j(f_{n'}(n)))=f_{f_j(k)}(f_{n'}(n))=f_{f_j(k)}(f_n(n'))\end{aligned}$$

より $f_n(n')\in\mathbb{N}_{<f_m(m')}$ が従い $\ell=f_{g_m(k)}(g_{n'}(j))$ とすれば

$$\begin{aligned}&g_m(m')=g_m(f_k(n'))=(f_{g_m(k)}\circ g_n)(n')=f_{g_m(k)}(g_{n'}(m))\\&=f_{g_m(k)}(g_{n'}(f_j(n)))=f_{g_m(k)}(f_{g_{n'}(j)}(g_{n'}(n)))=f_\ell(g_n(n'))\end{aligned}$$

が得られるので $g_n(n')\in\mathbb{N}_{<g_m(m')}$ が従う。

定理８の系（アルキメデス性）　任意の $m,n\in\mathbb{N}$ に対し $k\in\mathbb{N}$ が存在し $n\in\mathbb{N}_{\leq g_k(m)}$

（証明）　$k=\varphi(n)=f_e(n)$ と置くと $n\in\mathbb{N}_{<k}$ となる。$e\in\mathbb{N}_{\leq m}$ より $n=g_n(e)\in\mathbb{N}_{<g_k(m)}$ を得る。

定理９（切片の特徴付け）

(1) 任意の $m,n\in\mathbb{N}$ に対し次は同値である：

(i) $m\in\mathbb{N}_{<n}$

(ii) 或る $k\in\mathbb{N}$ に対し $f_k(m)\in\mathbb{N}_{<f_k(n)}$

(iii) 任意の $k\in\mathbb{N}$ に対し $f_k(m)\in\mathbb{N}_{<f_k(n)}$

(iv) 或る $k\in\mathbb{N}$ に対し $g_k(m)\in\mathbb{N}_{<g_k(n)}$

(v) 任意の $k\in\mathbb{N}$ に対し $g_k(m)\in\mathbb{N}_{<g_k(n)}$

(2) 任意の $m,n\in\mathbb{N}$ に対し次は同値である：

(i) $m\in\mathbb{N}_{\leq n}$

(ii) 或る $k\in\mathbb{N}$ に対し $f_k(m)\in\mathbb{N}_{\leq f_k(n)}$

(iii) 任意の $k\in\mathbb{N}$ に対し $f_k(m)\in\mathbb{N}_{\leq f_k(n)}$

(iv) 或る $k \in \mathbb{N}$ に対し $g_k(m) \in \mathbb{N}_{\leq g_k(n)}$

(v) 任意の $k \in \mathbb{N}$ に対し $g_k(m) \in \mathbb{N}_{<g_k(n)}$

（証明）

(1)　**(i)⇒(ii)**：$k = e$ とすれば (ii) は命題１の (8) より従う。

(ii)⇒(iii)：或る $k_0 \in \mathbb{N}$ に対し $f_{k_0}(m) \in \mathbb{N}_{<f_{k_0}(n)}$ であるとする。定義によって或る $j \in \mathbb{N}$ に対し $f_{k_0}(n) = f_j(f_{k_0}(m))$ が成立つ。このとき $f_{k_0}(n) = f_{k_0}(f_j(m))$ となり f_{k_0} の単射性より $n = f_j(m)$ が従う。よって任意の $k \in \mathbb{N}$ に対し $f_k(n) = f_k(f_j(m)) = f_j(f_k(m))$ となり $f_k(m) \in \mathbb{N}_{<f_k(n)}$ が従う。

(iii)⇒(i)：上と同様な議論で $n = f_j(m)$ なる $j \in \mathbb{N}$ の存在が従う。これは (i) を意味する。

(i)⇒(iv)：$k = e$ とすればよい。

(iv)⇒(i)：或る $k_0 \in \mathbb{N}$ に対し $g_{k_0}(m) \in \mathbb{N}_{<g_{k_0}(n)}$ であるとする。$j \in \mathbb{N}$ が在って $g_{k_0}(n) = f_j(g_{k_0}(m))$ が成立つ。もし $m \notin \mathbb{N}_{<n}$ ならば $m = n$ または $\ell \in \mathbb{N}$ が在って $m = f_\ell(n)$ と表される。前者ならば $g_{k_0}(n) = g_{k_0}(m)$ 故 f_j が不動点を持つ事になり矛盾。後者ならば $g_{k_0}(n) = f_j(g_{k_0}(m)) = f_j(g_{k_0}(f_\ell(n))) = f_j(f_{g_{k_0}(\ell)}(g_{k_0}(n))) = f_{f_j(g_{k_0}(\ell))}(g_{k_0}(n))$ となり $f_{f_j(g_{k_0}(\ell))}$ が不動点を持つ事になり矛盾。以上より $m \in \mathbb{N}_{<n}$ が従う。

(i)⇒(v)：$j \in \mathbb{N}$ が在って $n = f_j(m)$ となる。このとき $g_k(n) = g_k(f_j(m)) = f_{g_k(j)}(g_k(m))$ 故 $g_k(m) \in \mathbb{N}_{<g_k(n)}$ が従う。

(v)⇒(i)：(iv)⇒(i) の議論と同様。

(2)　f_k 及び g_k の単射性を用いれば良い。

定義：$\mathbb{N}$ の空でない部分集合 M に対し $m \in \mathbb{N}$ は

$$m \in M \cap \bigcap \{\mathbb{N}_{\leq n}; n \in M\}$$

を満たすとき m は M の**最小元**であると謂う。

定理１０（最小限の存在と一意性）
空でない部分集合 $M \subset \mathbb{N}$ は唯一つの最小限を持つ。

（証明）：集合 M_* を

$$M_* = \bigcap \{\mathbb{N}_{\leq n}; n \in M\}$$

と定義する。命題１の (9) により $e \in M_*$ が従う。M は空でないので一つの元 $m \in M$ が存在する。このとき $\varphi(m) \notin \mathbb{N}_{\leq m}$ 故 $\varphi(m) \notin M_*$ が従う。よって $M_* \neq \mathbb{N}$ が成立つ。さて

$$M_* = \mathbb{N} \Leftrightarrow \varphi(M_*) \subset M_* \Leftrightarrow \forall \ell \in M_*, \varphi(\ell) \in M_*$$

であり $M_* \neq \mathbb{N}$ が示されているので、$\ell \in M_*$ が存在して $\varphi(\ell) \notin M_*$ を満たす事が分かる。さて $\varphi(\ell) \notin M_*$ 故 $n \in M$ が存在し $\varphi(\ell) \notin \mathbb{N}_{\leq n}$ となる。定理３により $j \in \mathbb{N}$ が存在して

$\varphi(\ell) = f_j(n)$ を満たす。一方 $\ell \in M_*$ 故 $\ell \in \mathbb{N}_{\leq n}$ となり $\ell = n$ であるか $k \in \mathbb{N}$ が存在して $n = f_k(\ell)$ を満たす。後者ならば $\varphi(\ell) = f_j(n) = (f_j \circ f_k)(\ell) = f_{f_j(k)}(\ell)$ が従い $f_j(k) \neq e$ 故 $i \in \mathbb{N}$ が在って $f_j(k) = f_i(e)$ となるので $\varphi(\ell) = f_{f_i(e)}(\ell) = f_{f_e(i)}(\ell) = f_{\varphi(i)}(\ell) = \varphi(f_i(\ell))$ を得る。φ は単射故 $f_i(\ell) = \ell$ となり f_i は不動点を持つ事により矛盾を得る。よって $\ell = n$ であり、このとき $j = e$ である事も分かる。さて $\ell = n$ で $n \in M$ だったので $\ell \in M$ である。

最後に一意性を示そう。もう一つの元 $m' \in M \cap M_*$ が在ったとする。$m \neq m'$ なら $m = f_j(m')$ なる $j \in \mathbb{N}$ が存在するか $m' = f_k(m)$ なる $k \in \mathbb{N}$ が存在する。前者なら $m \notin \mathbb{N}_{\leq m'}$ となり $m \notin M_*$ により矛盾である。後者なら $m' \notin \mathbb{N}_{\leq m}$ となり $m' \notin M_*$ により矛盾である。よって $m = m'$ を得る。

定理１１（ペアノ系の代数的順序的同型）
二つのペアノ系 $(\mathbb{N}, e, \varphi)$ 及び $(\mathbb{N}', e', \varphi')$ に対し定理５で与えられる同型写像 $F : \mathbb{N} \to \mathbb{N}'$ は代数的にも順序的にも同型である。即ち

(1) **（加法に関する準同型）** 任意の $m, n \in \mathbb{N}$ に対し

$$F(f_m(n)) = f'_{F(m)}(F(m))$$

(2) **（乗法に関する準同型）** 任意の $m, n \in \mathbb{N}$ に対し

$$F(g_m(n)) = g'_{F(m)}(F(n))$$

(3) **（順序に関する準同型）** 任意の $n \in \mathbb{N}$ 及び $m \in \mathbb{N}_{\leq n}$ に対し

$$F(m) \in \mathbb{N}'_{\leq F(n)}$$

但し $f'_\bullet$ 及び $g'_\bullet$ は $\mathbb{N}'$ に於ける加法及び乗法を表すものとする。

（証明） 以下 $n \in \mathbb{N}$ を任意に取る。

(1) 集合 M_n を

$$M_n = \{m \in \mathbb{N}; F(f_n(m)) = f'_{F(n)}(F(m))\}$$

と定義する。$F(f_n(e)) = F(f_e(n)) = F(\varphi(n)) = \varphi'(F(n)) = f'_{e'}(F(n)) = f'_{F(n)}(e') = f'_{F(n)}(F(e))$ 故 $e \in M_n$ が従う。任意に $m \in M_n$ を取る。このとき $F(f_n(m)) = f'_{F(n)}(F(m))$ であるから $F(f_n(\varphi(m))) = F(\varphi(f_n(m))) = \varphi'(F(f_n(m)))$
$= \varphi'(f'_{F(n)}(F(m))) = f'_{F(n)}(\varphi'(F(m))) = f'_{F(n)}(F(\varphi(m)))$ となり $\varphi(m) \in M_n$ が従う。以上より $M_n = \mathbb{N}$ となり (1) が従う。

(2) 集合 M_n を

$$M_n = \{m \in \mathbb{N}; F(g_n(m)) = g'_{F(n)}(F(m))\}$$

と定義する。$F(g_n(e)) = F(n) = g'_{e'}(F(n)) = g'_{F(n)}(e') = g'_{F(n)}(F(e))$ 故 $e \in M_n$ が従う。任意に $m \in M_n$ を取る。このとき $F(g_n(m)) = g'_{F(n)}(F(m))$ であるから $F(g_n(\varphi(m))) = (F(f_n(g_n(m))) = f'_{F(n)}(F(g_n(m))) = f'_{F(n)}(g'_{F(n)}(F(m)))$
$= g'_{F(m)}(\varphi'(F(m))) = g'_{F(n)}(F(\varphi(m)))$ となり $\varphi(m) \in M_n$ が従う。以上より $M_n = \mathbb{N}$ となり (2) が従う。

(3) $m \in \mathbb{N}_{\leq n}$ を任意に取る。$m = n$ ならば $F(m) = F(n) \in \mathbb{N}'_{\leq F(n)}$ となる。$m \in \mathbb{N}_{<n}$ ならば $j \in \mathbb{N}$ が在って $n = f_j(m)$ となるので $F(n) = F(f_j(m)) = f'_{F(j)}(F(m))$ となるので $F(m) \in \mathbb{N}'_{\leq F(n)}$ が従う。

以上で自然数の基礎概念がペアノ系に基づいて構築されたので通常の記法で書き換えよう。特別な元であった e を 1 として

$$\varphi(n) = n + 1$$

$$f_m(n) = m + n$$

$$g_m(n) = mn$$

$$m < n \Leftrightarrow m \in \mathbb{N}_{<n}$$

$$m \leq n \Leftrightarrow m \in \mathbb{N}_{\leq n}$$

と表し、空でない部分集合 $M \subset \mathbb{N}$ の最小元を $\min M$ と表す。自然数の集合 $\mathbb{N}$ は**加法** $(m, n) \mapsto m+n$ に就いて（単位元を持たない）**可換半群**を成す。f_n の単射性により $f_n(\mathbb{N}) = \mathbb{N} \setminus \mathbb{N}_{\leq n}$ 上で**減法**が逆写像 $f_n^{-1} : \mathbb{N} \setminus \mathbb{N}_{\leq n} \ni m \mapsto f_n^{-1}(m) \in \mathbb{N}$ として定義される ($m = f_n(k) = n+k$ なるとき $k = f_n^{-1}(m) = m-n$ と表す)。自然数の集合 $\mathbb{N}$ は**乗法** $(m, n) \mapsto mn$ に就いて (単位元 1 を持つ) **可換半群**を成す。加法と乗法との間には**分配則**が成立つ。g_n の単射性により $g_n(\mathbb{N}) = \{g_n(k); k \in \mathbb{N}\}$ 上で**除法**が逆写像 $g_n^{-1} : g_n(\mathbb{N}) \ni m \mapsto g_n^{-1}(m) \in \mathbb{N}$ として定義される ($m = g_n(k) = nk$ なるとき $k = g_n^{-1}(m) = m/n$ と表し n を m の**約数**、m と n の**倍数**と謂う)。自然数 $\mathbb{N}$ に於ける関係 $\leq$ は順序の公理（反射律・反対称律・推移律）を満たし、この順序により $\mathbb{N}$ は全順序整列集合を成す。

2. 順序環と順序体

定義　乗法の単位元 1_R を持つ環 R は次の条件を満たす全順序を持つとき**順序環**と謂う：

(1) 任意の $a, b, c \in R$ に対し $a < b \Rightarrow a + c < a + b$

(2) 任意の $a, b, c \in R$ に対し $a < b,\ c > 0 \ \Rightarrow\ ac < bc,\ ca < cb$

順序環は体を成すとき**順序体**と謂う。

定義　R を順序環とする。$a \in R$ に対し、その**絶対値** $|a| \in R$ を次で定義する。

- $a = 0_R$ なら $|0_R| = 0_R$
- $a > 0_R$ なら $|a| = a$
- $a < 0_R$ なら $|a| = -a$

命題

(1) $a > 0_R \Leftrightarrow 0_R > -a$

(2) $a < b \Leftrightarrow -a > -b$

(3) $1_R > 0_R$

(4) $ab = 0_R \Leftrightarrow a = 0_R$ または $b = 0_R$

(5) $a = b \Leftrightarrow$ 任意の $c \neq 0_R$に対し $ac = bc$

$\Leftrightarrow$ 或る $c \neq 0_R$に対し $ac = bc$

(6) $|a + b| \leq |a| + |b|$

(7) $|ab| = |a|\ |b|$

(証明)

(1) $a > 0_R$ とする。このときもし $-a \geq 0_R$ なら $0_R = a + (-a) \geq a + 0_R = a > 0_R$ となり矛盾となる。従って $-a < 0_R$ である。逆に $0_R > -a$ とする。このときもし $a \leq 0_R$ なら $0_R = a + (-a) \leq 0_R + (-a) = -a < 0_R$ となり矛盾となる。従って $a > 0_R$ である。

(2) $a < b \Rightarrow 0_R = a + (-a) < b + (-a) = b - a$

$\Rightarrow 0_R > -(b - a) = a - b$

$\Rightarrow -b = (a - b) + (-a) < 0 + (-a) = -a,$

$-a > -b \Rightarrow 0_R = a + (-a) > a + (-b) = a - b$

$\Rightarrow 0_R < -(a - b) = b - a$

$\Rightarrow b = (b - a) + a > 0_R + a = a$

(3) $1_R < 0_R$ なら $-1_R > 0_R$ となる。$a = 0_R, b = -1_R, c = -1_R$ とおくと $a < b, c > 0_R$ であるから $ac < bc$ であり $ac = 0_R, bc = 1_R$ であるから $0_R < 1_R$ となり矛盾。よって $1_R > 0_R$ が従う。

(6) $a > 0_R, b > 0_R$ なら $a+b > 0_R$ 故 $|a+b| = a+b = |a|+|b|$ となる。$a < 0_R, b < 0_R$ なら $a+b < 0_R$ 故 $|a+b| = -(a+b) = (-a)+(-b) = |a|+|b|$ となる。$a > 0_R, b < 0_R$ なら $a+b < a+0_R = |a|+0_R < |a|+(-b) = |a|+|b|$ であり $-(a+b) = (-a)+(-b) = (-a)+|b| < 0_R+|b| < a+|b| = |a|+|b|$ となり $a + b \geq 0_R$ でも $a + b < 0_R$ でも $|a + b| < |a| + |b|$ が従う。$a < 0_R, b > 0_R$ なら a と b を入れ替えて $|a + b| < |a| + |b|$ を得る。

(7) $a > 0_R, b > 0_R$ なら $ab > 0_R$ 故 $|ab| = ab = |a||b|$ が従う。$a < 0_R, b < 0_R$ なら $-a > 0_R, -b > 0_R$ 故 $ab = (-a)(-b) > 0_R$ となり $|ab| = ab = (-a)(-b) = |a||b|$ が従う。$a > 0_R, b < 0_R$ なら $-b > 0_R$ 故 $-(ab) = a(-b) > 0_R$ であり $|ab| = -(ab) = a(-b) = |a||b|$ が従う。$a < 0_R, b > 0_R$ なら a と b を入れ替えて $|ab| = |a||b|$ を得る。

(4) $\Rightarrow$) を示せば良い。対偶を示そう。$a \neq 0_R, b \neq 0_R$ とする。このとき $|a| > 0_R, |b| > 0_R$ であるから (7) により $|ab| = |a||b| > 0_R$ が従う。よって $ab \neq 0_R$ となる。

(5) 或る $c \neq 0_R$ に対し $ac = bc$ なら $(a-b)c = 0_R$ となり (4) より $a = b$ が従う。

3. 整数

定理１（整数環の構成）　自然数全体の成す集合 $\mathbb{N}$ の直積集合 $\mathbb{N} \times \mathbb{N}$ に於いて、関係 $\sim$ を

$$(m,n) \sim (i,j) \underset{def}{\Longleftrightarrow} m + j = n + i$$

と定めると $\sim$ は同値関係を成す。$\mathbb{N} \times \mathbb{N}$ を関係 $\sim$ で割った商集合 $\mathbb{N} \times \mathbb{N}/\sim$ を $\mathbb{Z}$ と表し (m,n) の属す類を $[(m,n)]$ と表す：

$$[(m,n)] = \{(i,j) \in \mathbb{N} \times \mathbb{N}; (m,n) \sim (i,j)\}$$

$\mathbb{Z}$ の二つの元 $[(m,n)]$ 及び $[(k,\ell)]$ に対し和と積が

$$[(m,n)] + [(k,\ell)] \underset{\text{def.}}{=} [(m+k, n+\ell)]$$
$$[(m,n)] \cdot [(k,\ell)] \underset{\text{def.}}{=} [(mk + n\ell, m\ell + nk)]$$

によって（代表元の取り方に依らず）定まり $\mathbb{Z}$ に加法と乗法が定義される。加法及び乗法の単位元は夫々 $[(a,a)]$ 及び $[(a+1,a)]$ である。$[(m,n)]$ の加法に関する逆元は $[(n,m)]$ で与えられる。$\mathbb{Z}$ は可換環更には整域を成す。$\mathbb{Z}$ には

$$[(m,n)] \leq [(k,\ell)] \underset{def}{\Longleftrightarrow} m + \ell \leq n + k$$

によって（代表元の取り方に依らず）関係 $\leq$ が定義され順序の公理を満たす。$\mathbb{Z}$ は全順序集合で順序環を成す。$\mathbb{N}$ から $\mathbb{Z}$ への写像 ι が

$$\iota(n) = [(n+a, a)]$$

で（$a \in \mathbb{N}$ の取り方に依らず）定義される。ι は単射であり加法と乗法に関し準同型となる。値域を制限した写像 $\mathbb{N} \ni n \mapsto \iota(n) \in \iota(\mathbb{N})$ は全単射であり和と積と順序に関し同型となる。

定義　定理１で構成された可換環 $\mathbb{Z}$ を**整数環**と謂う。$\iota : \mathbb{N} \to \mathbb{Z}$ によって $\mathbb{N}$ は $\mathbb{Z}$ に埋め込まれる。加法の単位元（零元）$[(a,a)]$ を 0 と表し $[(m,n)]$ の逆元 $[(n,m)]$ を $-[(m,n)]$ と表す。乗法の単位元 $[(a+1,a)]$ を 1 と表す。$[(m,n)] \leq [(k,\ell)]$ 且つ $[(m,n)] \neq [(k,\ell)]$ なるとき $[(m,n)] < [(k,\ell)]$ と表す。通常 $[(m,n)]$ を $m - n$ と表す。

（証明）　関係 $\sim$ は $\mathbb{N} \times \mathbb{N}$ の同値関係を成す事：

反射性：$(m,n) \sim (m,n) \Leftrightarrow m + n = n + m$
対称性：$(m,n) \sim (i,j) \Leftrightarrow m + j = n + i$

$$\Leftrightarrow i+n=j+m \Leftrightarrow (i,j)\sim(m,n)$$

推移性：$(m,n)\sim(i,j),(i,j)\sim(k,\ell)$

$$\begin{aligned}&\Leftrightarrow m+j=n+i,\ i+\ell=j+k\\&\Rightarrow (m+\ell)+(i+j)=(m+j)+(i+\ell)=(n+i)+(j+k)=(n+k)+(i+j)\\&\Rightarrow m+\ell=n+k\Leftrightarrow(m,n)\sim(k,\ell)\end{aligned}$$

加法が代表元の取り方に依らず定まる事：

$$\begin{aligned}&(m,n)\sim(m',n'),(k,\ell)\sim(k',\ell')\\&\Leftrightarrow m+n'=n+m',k+\ell'=\ell+k'\\&\Rightarrow (m+k)+(n'+\ell')=(n+\ell)+(m'+k')\Leftrightarrow(m+k,n+\ell)\sim(m'+k',n'+\ell')\end{aligned}$$

乗法が代表元の取り方に依らず定まる事：

$$\begin{aligned}&(m,n)\sim(m',n'),(k,\ell)\sim(k',\ell')\\&\Leftrightarrow m+n'=n+m',k+\ell'=\ell+k'\\&\Rightarrow (mk+n\ell)+(m'\ell'+n'k')\\&\quad=\ m(k-\ell)+n(\ell-k)+m'(\ell'-k')+n'(k'-\ell')+(m\ell+nk+m'k'+n'\ell')\\&\quad=\ (m-n)(k-\ell)+(m'-n')(\ell'-k')+(m\ell+nk)+(m'k'+n'\ell')\\&\quad=\ (m\ell+nk)+(m'k'+n'\ell')\ \Rightarrow\ (mk+n\ell,m\ell+nk)\sim(m'k'+n'\ell',m'\ell'+n'k')\end{aligned}$$

加法の可換則:

$$[(m,n)]+[(k,\ell)]=[(m+k,n+\ell)]=[(k+m,\ell+n)]=[(k,\ell)]+[(m,n))]$$

加法の結合則:

$$\begin{aligned}&([(m,n)]+[(k,\ell)])+[(i,j)]=[(m+k,n+\ell)]+[(i,j)]=[(m+k+i,n+\ell+j)]\\&=[(m,n)]+[(k+i,\ell+j)]=[(m,n)]+([(k,\ell)]+[(i,j)])\end{aligned}$$

乗法の可換則:

$$\begin{aligned}[(m,n)]\cdot[(k,\ell)]&=[(mk+n\ell,m\ell+nk)]\\&=[(km+\ell n,\ell m+kn)]=[(k,\ell)]\cdot[(m,n)]\end{aligned}$$

乗法の結合則:

$$\begin{aligned}&([(m,n)]\cdot[(k,\ell)])\cdot[(i,j)]=[(mk+\ell n,\ell m+kn)]\cdot[(i,j)]\\&=[((mk+\ell n)i+(\ell m+kn)j,(mk+\ell n)j+(\ell m+kn)i)]\\&=[(m(ki+\ell j)+n(\ell i+kj),m(kj+\ell i)+n(ki+\ell j))]\\&=[(m,n)]\cdot[(ki+\ell j,\ell i+kj)]=[(m,n)]\cdot([(k,\ell)]\cdot[(i,j)])\end{aligned}$$

加法に関する乗法の分配則:

$$\begin{aligned}
&[(m,n)]\cdot([(k,\ell)])+[(i,j)])=[(m,n)]\cdot[(k+i,\ell+j)]\\
&=[(m(k+i)+n(\ell+j),m(\ell+j)+n(k+i))]\\
&=[((mk+n\ell)+(mi+nj),(m\ell+nk)+(mj+nj))]\\
&=[(mk+m\ell,m\ell+nk)]+[(mi+nj,mj+ni)]\\
&=[(m,n)]\cdot[(k,\ell)]+[(m,n)]\cdot[(i,j)]
\end{aligned}$$

加法の単位元が $[(a,a)]$ **である事**:

$$[(m,n)]+[(a,a)]=[(m+a,n+a)]=[(m,n)]$$

ここに最後の等式に於いて

$$(m+a,n+a)\sim(m,n)\Leftrightarrow\ (m+a)+n=(n+a)+m$$

なる事を用いた。

乗法の単位元が $[(a+1,a)]$ **である事**：

$$\begin{aligned}
[(m,n)]\cdot[(a+1,a)]&=[(m(a+1)+na,ma+n(a+1))]\\
&=[(a+1,a)]\cdot[(m,n)]
\end{aligned}$$

$[(m,n)]$ **の加法に関する逆元が** $[(n,m)]$ **である事**:

$$[(m,n)]+[(n,m)]=[(m+n,n+m)]=[(a,a)],\ a=m+n$$

$\mathbb{Z}$ **は整域を成す事**：

$$\begin{aligned}
&[(m,n)]\cdot[(k,\ell)]=[(a,a)]\\
\Leftrightarrow\ &[(mk+n\ell,m\ell+nk)]=[(a,a)]\\
\Leftrightarrow\ &k+n\ell+a=m\ell+nk+a\Leftrightarrow\ mk+n\ell=m\ell+nk
\end{aligned}$$

さて $k=\ell$ ならば $[(k,\ell)]=[(a,a)]$ となる。$k\neq\ell$ ならば $k<\ell$ または $k>\ell$ のどちらか一方が成立つ。$k<\ell$ ならば $\ell=k+i$ なる $i\in\mathbb{N}$ が存在するので

$$mk+n\ell=m\ell+nk\Leftrightarrow(m+n)k+ni=(m+n)k+mi\Leftrightarrow\ ni=mi\Leftrightarrow n=m$$

より $[(m,n)]=[(a,a)]$ を得る。$k>\ell$ ならば $k=\ell+j$ なる $j\in\mathbb{N}$ が存在するので

$$mk+n\ell=m\ell+nk\Leftrightarrow(m+n)\ell+mj=(m+n)\ell+nj\Leftrightarrow mj=nj\Leftrightarrow m=n$$

より $[(m,n)]=[(a,a)]$ を得る。

$\mathbb{Z}$ **に於ける関係** $\leq$ **が代表元の取り方に依らず定まる事**：

$$\begin{aligned}
&[(m,n)]\leq[(k,\ell)],\ (m,n)\sim(m',n'),(k,\ell)\sim(k',\ell')\\
\Leftrightarrow\ &(m,n)\sim(m',n'),\ (k,\ell)\sim(k',\ell'),\ m+\ell\leq n+k\\
\Leftrightarrow\ &m+n'=n+m',\ k+\ell'=\ell+k',\ m+\ell\leq n+k\\
\Rightarrow\ &(m'+\ell')+(n+k)=(n+m')+(k+\ell')=(m+n')+(\ell+k')\\
&=\ (m+\ell)+(n'+k')\leq(n+k)+(n'+k')\\
\Rightarrow\ &m'+\ell'\leq n+k'\Leftrightarrow\ [(m',n')]\leq[(\ell',k')]
\end{aligned}$$

$\mathbb{Z}$ に於ける関係 $\leq$ が順序を成す事：

反射性: $[(m,n)] \leq [(m,n)] \Leftrightarrow\ m+n=m+n$

反対称性: $[(m,n)] \leq [(k,\ell)],\ [(k,\ell)] \leq [(m,n)]$
$\Leftrightarrow\ m+\ell \leq n+k,\ k+n \leq \ell+m$
$\Rightarrow\ m+\ell = n+k \Rightarrow [(m,n)] = [(k,\ell)]$

推移性: $[(m,n)] \leq [(k,\ell)],\ [(k,\ell)] \leq [(i,j)]$
$\Leftrightarrow\ m+\ell \leq n+k,\ k+j \leq \ell+i$
$\Rightarrow\ (m+j)+\ell \leq (n+k)+j = (k+j)+n \leq (\ell+i)+n$
$\Leftrightarrow\ m+j \leq i+n \Rightarrow [(m,n)] \leq [(i,j)]$

$\mathbb{Z}$ に於ける順序 $\leq$ は全順序を成す事：

任意の $[(m,n)]$ 及び $[(k,\ell)]$ に対し $m+\ell, n+k \in \mathbb{N}$ であるから次の三つの場合の何れか一つが成立つ：

(i) $m+\ell > n+k$　　(ii) $m+\ell = n+k$　　(iii) $m+\ell < n+k$

(i) の場合は $[(m,n)] > [(k,\ell)]$、(ii) の場合は $[(m,n)] = [(k,\ell)]$、

(iii) の場合は $[(m,n)] < [(k,\ell)]$ となる。

$\mathbb{Z}$ は順序環を成す事:

$[(m,n)] < [(k,\ell)]$ なら $m+\ell < n+k$ であるから任意の $[(i,j)]$ に対し

$$(m+i)+(\ell+j) < (n+j)+(k+i) \Leftrightarrow\ [(m+i,n+j)] < [(k+i,\ell+j)]$$
$$\Leftrightarrow\ [(m,n)]+[(i,j)] < [(k,\ell)]+[(i,j)]$$

が従う。また $[(i,j)] > [(a,a)]$ に対して $i+a > j+a \Leftrightarrow i > j$ であるから
$[(m,n)]\cdot[(i,j)] = [(mi+nj,\ mj+ni)],\ [(k,\ell)]\cdot[(i,j)] = [(ki+\ell j, kj+\ell i)]$ に対し

$$\begin{aligned}
&(ki+\ell j)+(mj+ni) = (k+n)i+(\ell+m)j \\
&= (k+n)(i-j)+(k+n)j+(\ell+m)j \\
&= ((k+n)-(\ell+m))(i-j)+(\ell+m)(i-j)+(k+n)j+(\ell+m)j \\
&= ((k+n)-(\ell+m))(i-j)+(\ell+m)i+(k+n)j \\
&> (\ell+m)i+(k+n)j \\
&= (kj+\ell i)+(mi+nj)
\end{aligned}$$

となるので $[(m,n)]\cdot[(i,j)] < [(k,\ell)]\cdot[(i,j)]$ が従う。

$\mathbb{N}$ から $\mathbb{Z}$ への写像 ι が定まる事:

$$(n+b,b) \sim (n+a,a) \Leftrightarrow\ (n+b)+a = b+(n+a)$$

ι は単射である事：

$$\begin{aligned}\iota(m)=\iota(n) &\Leftrightarrow [(m+a,a)]=[(n+a,a)] \Leftrightarrow (m+a)+a=a+(n+a)\\ &\Leftrightarrow m=n\end{aligned}$$

ι は準同型である事：

$$\begin{aligned}\iota(m+n)&=[(m+n+a,a)]=[(m+n+a+a,a+a)]\\ &=[(m+a,a)]+[(n+a,a)]=\iota(m)+\iota(n)\\ \iota(mn)&=[(mn+a,a)]=[(mn+(m+n)a+2a^2,(m+n)a+2a^2)]\\ &=[((m+a)(n+a)+a^2,(m+a)a+a(n+a))]\\ &=[(m+a,a)]\cdot[(n+a,a)]=\iota(m)\cdot\iota(n)\end{aligned}$$

ι の順序保存性：

$$\begin{aligned}m\le n &\Leftrightarrow (m+a)+a\le(n+a)+a\\ &\Leftrightarrow \iota(m)=[(m+a,a)]\le[(n+a,a)]=\iota(n)\end{aligned}$$

定義　$[(m,n)]\in\mathbb{Z}$ が**正**であるとは $[(m,n)]>[(a,a)]$ である事と定義し正の整数全体の成す集合を $\mathbb{Z}_{>0}$ と表す：

$$\mathbb{Z}_{>0}=\{[(m,n)]\in\mathbb{Z};[(m,n)]>[(a,a)]\}$$

$[(m,n)]\in\mathbb{Z}$ が**非負**であるとは $[(m,n)]\ge[(a,a)]$ である事と定義し非負整数全体の成す集合を $\mathbb{Z}_{\ge0}$ と表す：

$$\mathbb{Z}_{\ge0}=\{[(m,n)]\in\mathbb{Z};[(m,n)]\ge[(a,a)]\}$$

命題　$\iota(\mathbb{N})=\mathbb{Z}_{>0}$
（証明）　任意の $n\in\mathbb{N}$ に対し

$$a+a<(n+a)+a\Leftrightarrow[(a,a)]<[(n+a,a)]$$

であるから $\iota(n)\in\mathbb{Z}_{>0}$ となる。一方、任意の $[(m,n)]\in\mathbb{Z}_{>0}$ に対し $m+a>n+a$ であるから $m=n+j$ なる $j\in\mathbb{N}$ が存在する。このとき $\iota(j)=[(j+a,a)]=[(j+n,n)]=[(m,n)]$ となり $[(m,n)]\in\iota(\mathbb{N})$ が従う。

系１　$[(m,n)]\in\mathbb{Z}$ に対し次は同値である。

(1) $[(m,n)]\in\mathbb{Z}_{>0}$

(2) $m-n\in\mathbb{N}$

系２　$[(m,n)]\in\mathbb{Z}$ に対し次は同値である。

(1) $[(m,n)]\in\mathbb{Z}\setminus\mathbb{Z}_{\ge0}$

(2) $[(n,m)] \in \mathbb{Z}_{\geq 0}$

(3) $n - m \in \mathbb{N}$

系３　$\mathbb{Z}$ は次の互いに素な合併で表される：

$$\mathbb{Z} = \mathbb{Z}_{>0} \cup \{[(a,a)]\} \cup (\mathbb{Z} \setminus \mathbb{Z}_{\geq 0})$$

定理２（整数環の特徴付け I）
順序環 R に対し次は同値である：

(1) R は $\mathbb{Z}$ と順序環として同型である。即ち、全単射 $f : \mathbb{Z} \to R$ が存在して任意の $[(m,n)], [(k,\ell)] \in \mathbb{Z}$ に対し次を満たす：

(i)　$f([(m,n)] + [(k,\ell)]) = f([(m,n)]) + f([(k,\ell)])$

$f([(m,n)] \cdot [(k,\ell)]) = f([(m,n)]) \cdot f([(k,\ell)])$

(ii)　$[(m,n)] \leq [(k,\ell)] \Rightarrow f([(m,n)]) \leq f([(k,\ell)])$

(2) $R_{>0} \equiv \{x \in R; x > 0_R\}$ は $\mathbb{N}$ と同型である。即ち、全単射 $g : \mathbb{N} \to R_{>0}$ が存在して任意の $m, n \in \mathbb{N}$ に対し次を満たす：

(i)　$g(m+n) = g(m) + g(n)$

$g(mn) = g(m) \cdot g(n)$

(ii)　$m \leq n \Rightarrow g(m) \leq g(n)$

（証明）(1) ⇒ (2)：$n \in \mathbb{N}$ に対し $g(n) = f(\iota(n))$ と定めると $\iota : \mathbb{N} \to \mathbb{Z}$ 及び $f : \mathbb{Z} \to R$ は単射であるから $g : \mathbb{N} \to R$ は単射である。任意の $x \in R_{>0}$ に対し $[(m,n)] \in \mathbb{Z}$ が存在して $f([(m,n)]) = x$ となる。$f([a,a]) = f([a+a, a+a]) = f([(a,a)] + [(a,a)]) = f([(a,a)]) + f([(a,a)])$ より $f([a,a)]) = 0_R$ を得る。これより $[(m,n)] > [(a,a)]$ が従う（実際 $[(m,n)] \leq [(a,a)]$ なら (ii) により $f([(m,n)]) \leq f([(a,a)]) = 0_R$ となり $x > 0_R$ に反する）。

さて $[(m,n)] \in \mathbb{Z}_{>0} = \iota(\mathbb{N})$ より $k \in \mathbb{N}$ が在って $x = f(\iota(k))$ となる。故に g は全射である。任意の $m, n \in \mathbb{N}$ に対し次が成立つ：

$$\begin{aligned} g(m+n) &= f(\iota(m+n)) = f(\iota(m) + \iota(n)) = f(\iota(m)) + f(\iota(n)) \\ &= g(m) + g(n) \\ g(mn) &= f(\iota(mn)) = f(\iota(m) \cdot \iota(n)) = f(\iota(m)) \cdot f(\iota(n)) = g(m) \cdot g(n) \\ m \leq n &\Rightarrow \iota(m) \leq \iota(n) \Rightarrow f(\iota(m)) \leq f(\iota(n)) \Rightarrow g(m) \leq g(n) \end{aligned}$$

(2) ⇒ (1)：$[(m,n)] \in \mathbb{Z}_{>0}$ に対し $m - n \in \mathbb{N}$ であるから $f([(m,n)]) = g(m-n)$ と置く。これは $[(m,n)]$ の代表元の取り方に依らず定まる。$\mathbb{N}$ 上 $f \circ \iota = g$ であり $\iota : \mathbb{N} \to \mathbb{Z}_{>0}$ は同型故 $f|\mathbb{Z}_{>0} = g \circ \iota^{-1}|\mathbb{Z}_{>0} : \mathbb{Z}_{>0} \ni [(m,n)] \mapsto f([(m,n)]) \in R_{>0}$ は全単射で (i)(ii) を満

たす。次に $f([(a,a)]) = 0_R$ と定める。最後に $[(m,n)] < [(a,a)]$ なる $[(m,n)] \in \mathbb{Z}$ に対し $f([(m,n)]) = -f([(n,m)])$ と置けば f は $\mathbb{Z} \setminus \mathbb{Z}_{\geq 0}$ から $R \setminus R_{\geq 0}(R_{\geq 0} = R_{>0} \cup \{0_R\})$ への同型を与える。$[(m,n)] \in \mathbb{Z}_{>0}, [(k,\ell)] \in \mathbb{Z} \setminus \mathbb{Z}_{\geq 0}$ に対し $[(m+k, n+\ell)] \in \mathbb{Z}_{>0}$ ならば

$$f([(m,n)] + [(k,\ell)]) = f([(m+k, n+\ell)]) = g((m+k) - (n+\ell))$$
$$f([(m,n)] + f([(k,\ell)]) = g(m-n) - f([(\ell,k)]) = g(m-n) - g(\ell - k)$$

であり $g(m-n) = g(((m+k) - (n+\ell)) + (\ell - k)) = g((m+k) - (n+\ell)) + g(\ell - k)$ となるから $f([(m,n)] + [(k,\ell)]) = f([(m,n)]) + f([(k,\ell)])$ を得る。
一方 $[(m+k, n+\ell)] = [(a,a)]$ ならば $[(m,n)] + [(k,\ell)] = [(a,a)]$ 即ち $[(k,\ell)] = [(n,m)] \in \mathbb{Z} \setminus \mathbb{Z}_{\geq 0}$ となり $f([(k,\ell)]) = -f([(m,n)])$ となるから

$$f([(m,n)] + [(k,\ell)]) = f([(m+k, n+\ell)]) = f([(a,a)]) = 0_R$$
$$f([(m,n)] + f([(k,\ell)]) = f([(m,n)]) - f([(m,n)]) = 0_R$$

が従い $f([(m,n)] + [(k,\ell)]) = f([(m,n)]) + f([(k,\ell)])$ を得る。
また $[(m+k, n+\ell)] \in \mathbb{Z} \setminus \mathbb{Z}_{\geq 0}$ ならば

$$f([(m,n)] + [(k,\ell)]) = -f([(n+\ell, m+k)]) = -g((n+\ell) - (m+k))$$
$$f([(m,n)] + f([(k,\ell)]) = g(m-n) - g(\ell - k)$$

であり $g(m-n) + g((n+\ell) - (m+k)) = g(\ell - k)$ となるから $f([(m,n)] + [(k,\ell)]) = f([(m,n)]) + f([(k,\ell)])$ を得る。
また $[(m,n)] \in \mathbb{Z}_{>0},\ [(k,\ell)] \in \mathbb{Z} \setminus \mathbb{Z}_{>0}$ に対し

$$(m\ell + nk) - (mk + n\ell) = m(\ell - k) - n(\ell - k) = (m-n)(\ell - k) \in \mathbb{N}$$

となるから $[(m,n)] \cdot [(k,\ell)] = [(mk + n\ell, m\ell + nk)] \in \mathbb{Z} \setminus \mathbb{Z}_{>0}$ である。故に

$$\begin{aligned} f([(m,n)] \cdot [(k,\ell)]) &= -f([(m\ell + nk, mk + n\ell)]) \\ &= -g((m-n)(\ell - k)) \\ &= -g(m-n) \cdot g(\ell - k) \\ &= -f([(m,n)]) \cdot f([(\ell,k)]) \\ &= f([(m,n)]) \cdot f([(k,\ell)]) \end{aligned}$$

を得る。$[(m,n)] \in \mathbb{Z}$ に対し

$$[(m,n)] \cdot [(a,a)] = [(ma + na, ma + na)] = [(a,a)]$$

であり

$$f([(m,n)] \cdot [(a,a)]) = f([(a,a)]) = 0_R = f([(m,n)]) \cdot f([(a,a)])$$

となる。以上で f は (i) を満たす事が分かった。(ii) は f の定義より直ちに従う。

定理３（整数環の特徴付け II）
任意の順序環 R に対し単射 $f : \mathbb{Z} \to R$ が存在し任意の $[(m,n)], [(k,\ell)] \in \mathbb{Z}$ に対し次を満たす：

(i) $f([(m,n)]+[(k,\ell)]) = f([(m,n)]) + f([(k,\ell)])$
$f([(m,n)]\cdot[(k,\ell)]) = f([(m,n)])\cdot f([(k,\ell)])$

(ii) $[(m,n)] \leq [(k,\ell)] \Rightarrow\ f([(m,n)]) \leq f([(k,\ell)])$

(iii) $|f([(m,n)])| \ = \ |m-n|$

註　単射 $f:\mathbb{Z}\to R$ によって $\mathbb{Z}\subset R$ と見做せば $\mathbb{Z}$ は最小の順序環と位置付ける事が出来る。

(証明)　R の乗法に関する単位元を 1_R と表す。写像 $\Phi: R\to R$ が $\Phi(x)=x+1_R$ により定まる。帰納法に依る点列 $F:\mathbb{N}\to R$ が一意的に定まり次を満たす：

$$(1)\ F(1)=1_R$$
$$(2)\ \text{任意の } n\in\mathbb{N} \text{ に対し } F(n+1)=\Phi(F(n))$$

この F に就いて次の性質を示そう：

$$(a)\ F(m+n)=F(m)+F(n)$$
$$(b)\ F(mn)=F(m)\cdot F(n)$$

(a) **の証明**：　任意の $n\in\mathbb{N}$ に対し集合 M_n を

$$M_n=\{m\in\mathbb{N}; F(m+n)=F(m)+F(n)\}$$

と定義する。$F(1+n)=\Phi(F(n))=F(n)+1_R=F(n)+F(1)$ より $1\in M_n$ が従う。任意に $m\in M_n$ を取る。このとき $F(m+n)=F(m)+F(n)$ が成立つ。
これより $F(m+1+n)=F(m+n)+1_R=F(m)+F(n)+1_R=\Phi(F(m))+F(n)=F(m+1)+F(n)$ を得るので $m+1\in M_n$ となり $M_n=\mathbb{N}$ が従う。

(b) **の証明**：　任意の $n\in\mathbb{N}$ に対し集合 M_n を

$$M_n=\{m\in\mathbb{N}; F(mn)=F(m)\cdot F(n)\}$$

と定義する。$F(1\cdot n)=F(n)=1_R\cdot F(n)=F(1)\cdot F(n)$ より $1\in M_n$ が従う。任意に $m\in M_n$ を取る。このとき $F(mn)=F(m)\cdot F(n)$ が成立つ。これより

$$\begin{aligned}F((m+1)n) &= F(mn+n)=F(mn)+F(n)=F(m)\cdot F(n)+F(n)\\ &=(F(m)+1_R)\cdot F(n)=\Phi(F(m))\cdot F(n)=F(m+1)\cdot F(n)\end{aligned}$$

を得るので $m+1\in M_n$ となり $M_n=\mathbb{N}$ が従う。

さて $[(m,n)]\in\mathbb{Z}_{>0}$ に対し $f([(m,n)])=F(m-n), f([a,a])=0_R, [(m,n)]\in\mathbb{Z}\setminus\mathbb{Z}_{\geq 0}$ に対し $f([(m,n)])=-F(n-m)$ と置くと、写像 $f:\mathbb{Z}\to R$ が定まる。このとき定理 2 の証明と同様な議論により (i) が従う。

(ii) は $[(m,n)],[(k,\ell)] \in \mathbb{Z}_{\geq 0}$ に就いて示せば充分である。集合 M を

$$M = \{m \in \mathbb{N}; F(m) > 0_R\}$$

と定義する。$\Phi(0) = F(1) = 1_R > 0_R$ より $1 \in M$ となる。任意に $m \in M$ を取る。このとき $F(m) > 0_R$ である。これより $F(m+1) = F(m) + F(1) = F(m) + 1_R > 1_R > 0_R$ となり $m+1 \in M$ が従い $M = \mathbb{N}$ を得る。故に任意の $m,n \in \mathbb{N}$ に対し $F(m+n) = F(m) + F(n) > F(m)$ が従う。これより (ii) が従う。

(iii) は $[(m,n)] \in \mathbb{Z}_{>0}$ に就いて示せば充分である。集合 M を

$$M = \{m \in \mathbb{N}; |F(m)| \ = F(m) = m1_R\}$$

と定義する。$F(1) = 1_R$ より $1 \in M$ となる。任意に $m \in M$ を取る。このとき $F(m) = m1_R$ である。これより $F(m+1) = F(m) + F(1) = m1_R + 1_R = (m+1)1_R$ となり $m+1 \in M$ が従い $M = \mathbb{N}$ を得る。これより (iii) が従う。

以下では通常の様に整数は $m,n\cdots$ の様に一つのローマ字で表す事にする。$\mathbb{Z}$ には加法 $(m,n) \mapsto m+n$ 及び乗法 $(m,n) \mapsto m \cdot n$ が定義され次の性質が成立する。

加法の可換則： $m+n = n+m$

加法の結合則： $(m+n)+k = m+(n+k)$

加法に関する単位元 0 の存在： $m+0 = m$

加法に関する逆元の存在： $m+(-m) = 0$

乗法の可換則： $m \cdot n = n \cdot m$

乗法の結合則： $(m \cdot n) \cdot k = m \cdot (n \cdot k)$

乗法に関する単位元１の存在： $m \cdot 1 = m$

加法に関する乗法の分配則： $m \cdot (n+k) = m \cdot n + m \cdot k$

このとき次が成立つ：

命題１

(1) $0 \cdot m = m \cdot 0 = 0$

(2) $-m = (-1) \cdot m = m \cdot (-1)$

(3) $(-1)^2 = 1$

(4) $(-m) \cdot (-n) = mn$

（証明）

(1) $0 \cdot m = 0 \cdot m + 0 = 0 \cdot m + (0 \cdot m + (-0 \cdot m))$
$= (0 \cdot m + 0 \cdot m) + (-0 \cdot m)$
$= (0 + 0) \cdot m + (-0 \cdot m) = 0 \cdot m + (-0 \cdot m) = 0$

(2) $m + (-1) \cdot m = 1 \cdot m + (-1) \cdot m = (1 + (-1)) \cdot m = 0 \cdot m = 0$ 及び逆元の一意性により $(-1) \cdot m = -m$ が従う。

(3) $(-1)^2 + (-1) = (-1) \cdot (-1) + (-1) \cdot 1 = (-1) \cdot ((-1) + 1) = (-1) \cdot 0 = 0$ より $(-1)^2 = -(-1)$ であり逆元の一意性より $(-1)^2 = 1$ が従う。

(4) $(-m) \cdot (-n) = (m \cdot (-1)) \cdot ((-1) \cdot n) = m \cdot ((-1) \cdot (-1)) \cdot n$
$= m \cdot 1 \cdot n = m \cdot n$

命題２（加法に関する簡約則） $m, n \in \mathbb{Z}$ に対し次は同値：

(1) $m = n$

(2) 或る $k \in \mathbb{Z}$ に対し $m + k = n + k$

(3) 任意の $k \in \mathbb{Z}$ に対し $m + k = n + k$

（証明） (1)⇒(3)⇒(2) は明らかであり (2)⇒(1) は k の加法に関する逆元 $-k$ を (2) の両辺に加え結合則を用いる。

命題３（乗法に関する簡約則） $m, n \in \mathbb{Z}$ に対し次は同値：

(1) $m = n$

(2) 或る $k \in \mathbb{Z} \setminus \{0\}$ に対し $m \cdot k = n \cdot k$

(3) 任意の $k \in \mathbb{Z} \setminus \{0\}$ に対し $m \cdot k = n \cdot k$

（証明） $\mathbb{Z}$ は整域である事から従う。

定義 $m, n \in \mathbb{N}$ に対し、その差を m と $-n$ との和 $m - n = m + (-n)$ で定義する。$\iota : \mathbb{N} \to \mathbb{Z}$ によって $\mathbb{N}$ を $\mathbb{Z}$ の部分集合 $\mathbb{Z}_{>0}$ と同一視する。これにより $\mathbb{Z}$ は $\mathbb{Z} = \mathbb{N} \cup \{0\} \cup (-\mathbb{N})$ と互いに素な集合の合併で表される。ここに $-\mathbb{N} = \{-m \in \mathbb{Z}; m \in \mathbb{N}\} = \mathbb{Z} \setminus \mathbb{Z}_{\geq 0}$ である。

命題４（大小関係の特徴付け）

(1) 任意の $m, n \in \mathbb{Z}$ に対し次は同値である：

(i) $m < n$

(ii) 或る $k \in \mathbb{Z}$ に対し $m + k < n + k$

(iii) 任意の $k \in \mathbb{Z}_{>0}$ に対し $m + k < n + k$

(iv) 或る $k \in \mathbb{Z}_{>0}$ に対し $mk < nk$

(v) 任意の $k \in \mathbb{Z}_{>0}$ に対し $mk < nk$

(vi) 或る $k \in \mathbb{Z} \setminus \mathbb{Z}_{\geq 0}$ に対し $mk > nk$

(vii) 任意の $k \in \mathbb{Z} \setminus \mathbb{Z}_{\geq 0}$ に対し $mk > nk$

(2) 任意の $m, n \in \mathbb{Z}$ に対し次は同値である：

(i) $m \leq n$

(ii) 或る $k \in \mathbb{Z}$ に対し $m + k \leq n + k$

(iii) 任意の $k \in \mathbb{Z}_{>0}$ に対し $m + k \leq n + k$

(iv) 或る $k \in \mathbb{Z}_{>0}$ に対し $mk \leq nk$

(v) 任意の $k \in \mathbb{Z}_{>0}$ に対し $mk \leq nk$

(vi) 或る $k \in \mathbb{Z} \setminus \mathbb{Z}_{\geq 0}$ に対し $mk \geq nk$

(vii) 任意の $k \in \mathbb{Z} \setminus \mathbb{Z}_{\geq 0}$ に対し $mk \geq nk$

命題５（アルキメデス性）　任意の $m \in \mathbb{Z}, n \in \mathbb{Z}_{>0}$ に対し $k \in \mathbb{Z}$ が存在し $kn \geq m$ を満たす。

（証明）　$m \leq 0$ なら $k = 1$ とする。$m > 0$ なら $k = m + 1$ とすれば $kn = (m + 1)n \geq m + 1 > m$ が従う。

命題６　$\mathbb{Z}$ は可算である。

（証明）　$n \in \mathbb{N}$ に対し $f(2n - 1) = n - 1, f(zn) = -n$ と置けば $f : \mathbb{N} \to \mathbb{Z}$ が定まる。$\mathbb{Z} = \mathbb{N} \cup \{0\} \cup (-\mathbb{N})$ から $\mathbb{N}$ への写像 $g(m) = 2m + 1, m \in \mathbb{N} \cup \{0\},\ g(-m) = 2m, m \in \mathbb{N}$ は f の逆写像となっており f は全単射である。

定義　$m \in \mathbb{Z}$ に対しその**絶対値** $|m|$ を $m \in \mathbb{N}$ なら $|m| = m, m = 0$ なら $|m| = 0, -m \in \mathbb{N}$ なら $|m| = -m$ と定める。

命題４（除法原理）　任意の $m \in \mathbb{Z}$ 及び任意の $n \in \mathbb{Z}_{>0}$ に対し $q \in \mathbb{Z}$ 及び $r \in \mathbb{Z}_{\geq 0}$ が一意的に存在し次を満たす：

$$m = qn + r,\ 0 \leq r < n$$

（証明）　$m = 0$ なら $q = r = 0$ とすれば良い。$m \in \mathbb{N}$ なるアルキメデス性により $k_0 \in \mathbb{N}$ を取って $k_0 n \geq m$ とする事が出来る。従って

$$M = \{k \in \mathbb{N}; kn \geq m\}$$

は空でなく、その最小元 $k_1 = \min M$ が存在する。これより $k_1 n \geq m$ となる。$k_1 n = m$ の場合は $q = k_1,\ r = 0$ とすれば良い。$k_1 n > m$ の場合は $q = k_1 - 1$ と置く。このとき $q \notin M$ 故 $qn < m$ である。そこで $r = m - qn$ と置くと $0 < r < m$ であり $m = qn + r$ が成立つ。$m \in -\mathbb{N}$ なら $-m \in \mathbb{N}$ 故 $q' \in \mathbb{Z}$ 及び $r' \in \mathbb{Z}_{\geq 0}$ が存在して $-m = q'n + r',\ 0 < r' < n$ が成

立つ。このとき $m=(-q')n-r'=(-q'-1)n+(n-r')$ となり $q=-q'-1,\ r=n-r'$ とすれば $m=qn+r,\ 0<r<n$ を満たす。

最後に $(q,r)\in\mathbb{Z}\times\mathbb{Z}_{\geq 0}$ の一意性を示そう。$(q',r')\in\mathbb{Z}\times\mathbb{Z}_{\geq 0}$ が存在して $m=q'n+r',\ 0\leq r'<n$ となっていたとすると

$$qn+r=q'n+r'\Leftrightarrow r-r'=(q'-q)n$$

もし $r<r'$ なら $0<r'-r<n$ であり $(q-q')n=r'-r>0$ より $q\neq q'$ となるから $q-q'\geq 1$ が従う。このとき $r'-r=(q-q')n\geq n$ となり矛盾を生ずる。もし $r'<r$ なら $0<r-r'<n$ であり $(q'-q)n=r-r'>0$ より $q'\neq q$ となるから $q'-q\geq 1$ が従う。このとき $r-r'=(q'-q)n\geq n$ となり矛盾を生ずる。以上より $r=r'$ を得る。このとき $(q'-q)n=r-r'=0$ より $q=q'$ が従う。

系　任意の $m\in\mathbb{Z}$ 及び任意の $n\in\mathbb{Z}\setminus\{0\}$ に対し $q\in\mathbb{Z}$ 及び $r\in\mathbb{Z}_{\geq 0}$ が一意的に存在し次を満たす：

$$m=qn+r,\ 0\leq r<|n|$$

（証明）　$-n\in\mathbb{N}$ に対し上の定理を適用する。$q'\in\mathbb{Z}$ 及び $r'\in\mathbb{Z}_{\geq 0}$ が一意的に存在し $m=q'(-n)+r',\ 0\leq r'<-n$ を満たす。そこで $q=-q',\ r=r'$ とすれば良い。一意性も上の定理に帰着される。

定義　$m\in\mathbb{Z},\ n\in\mathbb{Z}\setminus\{0\}$ に対し

$$m=qn+r,\ 0\leq r<|n|$$

で一意的に定まる $q\in\mathbb{Z}$ 及び $r\in\mathbb{Z}_{\geq 0}$ を夫々 m を n で割った**商**及び**余り**と謂う。$r=0$ 即ち $m=qn$ の場合 m は n で**割り切れる**と謂い $n|m$ と表し n を m の**約数**と謂う。

命題６

(1) $(\pm 1)|m,\ (\pm m)|m$

(2) $n|m, m|k\Rightarrow\ n|k$

(3) $n|m\Rightarrow\ n|mk$

(4) $k\neq 0, nk|mk\Rightarrow\ n|m$

(5) $n|m, \ell|k\Rightarrow\ n\ell|mk$

(6) $n|m, n|k\Rightarrow\ n|(mi+kj)\ \forall i,j\in\mathbb{Z}$

（証明）

(1) $m=(\pm 1)(\mp m)$

(2) $m=qn, k=q'm\Rightarrow\ k=(qq')n$

(3) $m = qn \Rightarrow\ mk = (kq)n$

(4) $mk = q(nk) \Rightarrow\ m = qn$

(5) $m = qn, k = q'\ell \Rightarrow\ mk = (qq')n\ell$

(6) $m = qn, k = q'n \Rightarrow\ mi + kj = (qi + q'j)n$

定義　$m \in \mathbb{Z}$ が**合成数**であるとは $j, k \in \mathbb{Z} \setminus \{\pm 1\}$ が存在して $m = jk$ と表される事を謂う。$m \in \mathbb{Z} \setminus \{\pm 1\}$ が**素数**であるとは合成数でない事を謂う。

定理５（最大公約数の存在）　任意の $m, n \in \mathbb{Z} \setminus \{0\}$ に対し集合 $M_{m,n}$ 及び $D_{m,n}$ を

$$M_{m,n} = \{mi + nj \in \mathbb{Z}; i, j \in \mathbb{Z}\}$$
$$D_{m,n} = \{k \in \mathbb{Z} \setminus \{0\}; k|m \text{ 且つ } k|n\}$$

と定義する。このとき唯一つの $d \in \mathbb{Z}_{>0}$ が存在し次を満たす：

(1) $d \in M_{m,n} \cap D_{m,n}$

(2) $M_{m,n} = \{\ell d \in \mathbb{Z}; \ell \in \mathbb{Z}\}$

(3) 任意の $c \in D_{m,n}$ に対し $c|d$

定義　$m, n \in \mathbb{Z} \setminus \{0\}$ に対し上で定まる d を m と n の**最大公約数**と謂い $d = GCD(m, n)$ と表す。また $m = GCD(m, 0) = GCD(0, m),\ 0 = GCD(0, 0)$ とする。

（証明）　$m = m1 + n0, n = m0 + n1$ 故 $m, n \in M_{m,n} \setminus \{0\}$ が従う。$mi + nj \in M_{m,n} \setminus \mathbb{Z}_{\geq 0}$ なら $-(mi + nj) = m(-i) + n(-j)$ 故 $-(mi + nj) \in M_{m,n} \cap \mathbb{N}$ が従う。故に $M_{m,n} \cap \mathbb{N}$ は $\mathbb{N}$ の空でない部分集合であり最小元を持つ。それを $d = \min(M_{m,n} \cap \mathbb{N})$ と表す。$d \in M_{m,n} \cap \mathbb{N}$ 故 $i, j \in \mathbb{Z}$ が存在し $d = mi + nj$ を満たす。

$M_{m,n} = \{\ell d \in \mathbb{Z}; \ell \in \mathbb{Z}\}$ **なる事**：　$P = \{\ell d\ ; \ell \in \mathbb{Z}\}$ と置く。$\ell d = \ell(mi + nj) = m(\ell i) + n(\ell j)$ 故 $P \subset M_{m,n}$ となる。もし $\ell_0 \in M_{m,n} \setminus P$ が存在したとすると $i_0, j_0 \in \mathbb{Z}$ によって $\ell_0 = mi_0 + nj_0$ と表される。ℓ_0 を d で割った商及び余りを q_0 と r_0 とすると $\ell_0 \notin P$ 故 ℓ_0 は

$$\ell_0 = dq_0 + r_0,\ 0 < r_0 < d$$

と表される。このとき

$$\begin{aligned} r_0 &= \ell_0 - dq_0 = (mi_0 + nj_0) - (mi + nj)q_0 \\ &= m(i_0 - iq_0) + n(j_0 - jq_0) \in M_{m,n} \cap \mathbb{N} \end{aligned}$$

となり d の最小性に反する。故に ℓ_0 は存在しない。即ち $M_{m,n} \subset P$ となる。

$d \in D_{m,n}$ **なる事**：　$m, n \in M_{m,n} = P$ 故 $m = \ell d, n = \ell' d$ なる $\ell, \ell' \in \mathbb{Z} \setminus \{0\}$ が存在する。即ち $d|m, d|n$ が成立つ。

任意の$c \in D_{m,n}$に対し$c|d$なる事:$c \in D_{m,n}$なら$m', n' \in \mathbb{Z}\setminus\{0\}$が存在し$m = m'c, n = n'c$と表される。このとき$d = mi + nj = (m'i + n'j)c$となるから$c|d$が従う。

一意性:もう一つの$d' \in \mathbb{Z}_{>0}$が(1)(2)を満たしていたとすると$\ell, \ell' \in \mathbb{Z}$が在って$d = d'\ell, d' = d\ell'$が成立つ。これより$d = d'\ell = (d\ell')\ell$即ち$d(1 - \ell\ell') = 0$が成立つ。$d \neq 0$故$\ell\ell' = 1$となり$\ell = \ell' = 1$即ち$d = d'$が従う。

系１　$p \in \mathbb{Z}_{>0}$を素数とし$m \in \mathbb{Z}_{>0}$とpは1以外の共通の約数を持たないとする。このとき$i, j \in \mathbb{Z}$が存在し$pi + mj = 1$が成立つ。

(証明)$d = GCD(p, m)$とすると$p, m \in M_{p,m} = \{\ell d; \ell \in \mathbb{Z}\}$であるから$\ell, \ell' \in \mathbb{N}$が存在し$p = \ell d, m = \ell' d$が成立つ。$p$と$m$は1以外の共通の約数を持たないから$d = 1$が従う。$1 = d \in M_{p,m}$より結論を得る。

系２　$m, n \in \mathbb{Z}_{>0}$とし$p \in \mathbb{Z}_{>0}$を素数とする。

$$\text{このとき } p|mn \Rightarrow p|m \text{ または } p|n$$

(証明)$p|mn$とし$p|m$ではないと仮定する。系１より$i, j \in \mathbb{Z}$が在って$pi + mj = 1$となる。$p|mn$故$k \in \mathbb{Z}_{>0}$が在って$mn = pk$となる。従って

$$n = n(pi + mj) = p(ni) + (pk)j = p(ni + kj)$$

となり$p|n$が成立つ。

定理６（算数の基本定理）任意の$m \in \mathbb{Z} \setminus \{-1, 0, 1\}$に対し有限個の素数$\{p_i; 1 \leq i \leq n\}$と正の整数$\{k_i \in \mathbb{Z}_{>0}; 1 \leq i \leq n\}$で次を満たすものが一意的に存在する：

(1)　$1 < p_1 < \cdots < p_n$

(2)　$m = \pm \prod_{i=1}^{n} p_i^{k_i}$

ここに$\pm$はmの正負に従う。

(証明)$m > 1$の場合を考える。集合D_mを

$$D_m = \{\ell \in \mathbb{N};\ \ell|m,\ \ell > 1\}$$

と定義する。$m \in D_m$故D_mは空でないので$p_1 = \min D_m$が存在する。最小性よりp_1は合成数ではなく素数である。故にmは

$$m = p_1 m_1,\ p_1\text{は素数},\ m_1 < m$$

と表される。$m_1 = 1$ならばこれで証明が完結する。$m_1 > 1$ならばmに就いての議論をm_1に対して行い

$$m_1 = p_2 m_2,\ p_2\text{は素数},\ m_2 < m_1$$

なる表現を得る。以下同様にして $j=2,3,\cdots$ に対し

$$m_{j-1}=p_j m_j,\ p_j\text{は素数},\ m_j<m_{j-1}$$

なる構成を繰り返す。$m>m_1>\cdots>m_j\geq 1$ であるからこの操作は有限回で終了する。
それを N 回とすると m は

$$m=p_1p_2\cdots p_N$$

と表される。右辺に現れる素数を小さい順に並べ、新たに $1<p_1<\cdots<p_n$ と書き直し p_i の現れる回数を正の整数 k_i とすれば (1)(2) が成立つ。
　一意性は定理 5 の系 2 と帰納法により示される。

系 1　$m\geq 2$ なる整数 m を

$$m=\prod_{i=1}^{n}p_i^{k_i}$$

と素因数分解表示する。ここに $\{p_i\,;1\leq i\leq n\}$ は互いに異なる n 個の素数で
$\{k_i\in\mathbb{Z}_{>0};1\leq i\leq n\}$ は n 個の正の整数であるとする。
このとき次は同値である：

(1) 全ての i に対し k_i は偶数である。

(2) 唯一つの $n\in\mathbb{Z}_{>0}$ が存在し $m=n^2$ を満たす。

(3) $\ell\in\mathbb{Z}\setminus\{0\}$ 及び $n\in\mathbb{Z}\setminus\{-1,0,1\}$ が存在し $\ell^2m=n^2$ を満たす。

系 2　$m\geq 2$ なる整数 m を

$$m=\prod_{i=1}^{n}p_i^{k_i}$$

と素因数分解表示する。ここに $\{p_i\,;1\leq i\leq n\}$ は互いに異なる n 個の素数で
$\{k_i\in\mathbb{Z}_{>0};1\leq i\leq n\}$ は n 個の正の整数であるとする。
このとき次は同値である：

(1) 或る i に対し k_i は奇数である。

(2) $m=n^2$ を満たす $n\in\mathbb{Z}\setminus\{0\}$ は存在しない。

(3) $\ell^2m=n^2$ を満たす $\ell\in\mathbb{Z}\setminus\{0\}$ 及び $n\in\mathbb{Z}\setminus\{-1,0,1\}$ は存在しない。

4. 有理数

定理 1（有理数体の構成） 整数環 $\mathbb{Z}$ 及び $\mathbb{Z}$ から 0 を除いた集合 $\mathbb{Z}\setminus\{0\}$ の直積集合 $\mathbb{Z}\times(\mathbb{Z}\setminus\{0\})$ に於いて、関係 $\sim$ を

$$(m,n)\sim(i,j)\underset{def}{\Longleftrightarrow}\ mj=ni$$

で定めると $\sim$ は同値関係を成す。$\mathbb{Z}\times(\mathbb{Z}\setminus\{0\})$ を関係 $\sim$ で割った商集合 $(\mathbb{Z}\times(\mathbb{Z}\setminus\{0\}))/\sim$ を $\mathbb{Q}$ と表し (m,n) の属す類を $[(m,n)]$ と表す：

$$[(m,n)]=\{(i,j)\in\mathbb{Z}\times(\mathbb{Z}\setminus\{0\});(m,n)\sim(i,j)\}$$

$\mathbb{Q}$ の二つの元 $[(m,n)]$ 及び $[(k,\ell)]$ に対し和と積が

$$[(m,n)]+[(k,\ell)] \underset{\text{def.}}{=} (m\ell+nk,n\ell)$$
$$[(m,n)]\cdot[(k,\ell)] \underset{\text{def.}}{=} [(mk,n\ell)]$$

によって（代表元の取り方に依らず）定まり $\mathbb{Q}$ に加法と乗法が定義される。加法及び乗法の単位元は夫々$[(0,1)]$ 及び $[(1,1)]$ である。$[(m,n)]$ の加法及び乗法（但し $[(m,n)]\neq[(0,1)]$）に関する逆元は夫々$[(-m,n)]$ 及び $[(n,m)]$ で与えられる。$\mathbb{Q}$ は可換体を成す。$\mathbb{Q}$ には

$$[(m,n)]\leq[(k,\ell)] \underset{def}{\Longleftrightarrow} \begin{cases} n\ell>0 \text{ なるとき } m\ell\leq nk \\ n\ell<0 \text{ なるとき } m\ell\geq nk \end{cases}$$

によって（代表元の取り方に依らず）関係 $\leq$ が定義され順序の公理を満たす。$\mathbb{Q}$ は全順序集合で順序体を成す。$\mathbb{Z}$ から $\mathbb{Q}$ への写像 ι が

$$\iota(m)=[(m,1)]$$

で定義される。ι は単射であり加法と乗法に関し準同型となる。値域を制限した写像 $\iota:\mathbb{Z}\ni m\mapsto\iota(m)\in\iota(\mathbb{Z})$ は全単射であり和と積と順序に関し同型となる。また $[(m,n)]=\iota(m)/\iota(n),\ |[(m,n)]|=|\iota(m)|/|\iota(n)|=\iota(|m|)/\iota(|n|)$ が成立つ。

定義　定理１で構成された可換体 $\mathbb{Q}$ を**有理数体**と謂う。$\iota:\mathbb{Z}\to\mathbb{Q}$ によって $\mathbb{Z}$ は $\mathbb{Q}$ に埋め込まれる。加法の単位元（零元）$[(0,1)]$ を 0 と表し $[(m,n)]$ の加法に関する逆元を $-[(m,n)]$ と表す。乗法の単位元 $[(1,1)]$ を 1 と表す。$[(m,n)]\leq[(k,\ell)]$ 且つ $[(m,n)]\neq[(k,\ell)]$ なるとき $[(m,n)]<[(k,\ell)]$ と表す。通常 $[(m,n)]$ を m/n と表す。よって $|[(m,n)]|=|[(|m|,|n|)]=|m|/|n|$ と表す事が出来る。

（証明）関係 $\sim$ は $\mathbb{Z}\times(\mathbb{Z}\setminus\{0\})$ の同値関係を成す事：

反射性：$(m,n)\sim(m,n)\Leftrightarrow mn=nm$

対称性：$(m,n)\sim(i,j)\Leftrightarrow\ mj=ni$
$\Leftrightarrow\ in=jm\Leftrightarrow(i,j)\sim(m,n)$

推移性：$(m,n)\sim(i,j),(i,j)\sim(k,\ell)$
$\Leftrightarrow mj=ni,i\ell=jk$
$\Rightarrow mj\ell=ni\ell=njk\Rightarrow m\ell=nk\Leftrightarrow(m,n)\sim(k,\ell)$

加法が代表元の取り方に依らず定まる事：

$$\begin{aligned}&(m,n)\sim(m',n'),\ (k,\ell)\sim(k',\ell')\\&\Leftrightarrow mn'=nm',\ k\ell'=\ell k'\\&\Rightarrow(m\ell+nk)n'\ell'=mn'\ell\ell'+nn'k\ell'=nm'\ell\ell'+nn'k'\ell=(m'\ell'+n'k')n\ell\\&\Rightarrow(m\ell+nk,n\ell)\sim(m'\ell'+n'k',n'\ell')\end{aligned}$$

乗法が代表元の取り方に依らず定まる事：

$$\begin{aligned}&(m,n)\sim(m',n'),\ (k,\ell)\sim(k',\ell')\\&\Leftrightarrow mn'=m'n',\ k\ell'=k'\ell\\&\Rightarrow mn'k\ell'=m'nk\ell'=m'nk'\ell\\&\Rightarrow(mk,n\ell)\sim(m'k',n'\ell')\end{aligned}$$

加法の可換則：

$$[(m,n)]+[(k,\ell)]=[(m\ell+nk,n\ell)]=[(kn+\ell m,\ell n)]=[(k,\ell)]+[(m,n)]$$

加法の結合則：

$$\begin{aligned}&([(m,n)]+[(k,\ell)])+[(i,j)]=[(m\ell+nk,n\ell)]+[(i,j)]\\&=[((m\ell+nk)j+(n\ell)i,(n\ell)j)]=[(m(\ell j)+n(kj+\ell i),n(\ell j))]\\&=[(m,n)]+[(kj+\ell i,\ell j)]=[(m,n)]+([(k,\ell)]+[(i,j)])\end{aligned}$$

乗法の可換則：$[(m,n)]\cdot[(k,\ell)]=[(mk,n\ell)]=[(k,\ell)]\cdot[(m,n)]$

乗法の結合則：$\begin{aligned}([(m,n)]\cdot[(k,\ell)])+[(i,j)]&=[(mk,n\ell)]\cdot[(i,j)]=[(mki,n\ell j)]\\&=\ [(m,n)]\cdot[(ki,\ell j)]=[(m,n)]\cdot([(k,\ell)]\cdot[(i,j)])\end{aligned}$

加法に関する乗法の分配則：

$$\begin{aligned}&[(m,n)]\cdot([(k,\ell)]+[(i,j)])=[(m,n)]\cdot[(kj+\ell i,\ell j)]=[(m(kj+\ell i),n\ell j)]\\&=[((mk)+(nj)+(n\ell)(mi),(n\ell)(nj))]\\&=[(mk,n\ell)]+[(mi,nj)]=[(m,n)]\cdot[(k,\ell)]+[(m,n)]\cdot[(i,j)]\end{aligned}$$

加法の単位元が $[(0,1)]$ **である事**：

$$[(m,n)]+[(0,1)]=[(m\cdot1+n\cdot0,n\cdot1)]=[(m,n)]$$

乗法の単位元が $[(1,1)]$ **である事**：

$$[(m,n)]\cdot[(1,1)]=[(m\cdot1,n\cdot1)]=[(m,n)]$$

$[(m,n)]$ **の加法に関する逆元が** $[(-m,n)]$ **である事**：

$$[(m,n)]+[(-m,n)]=[(mn+n(-m),n^2)]=[(0,n^2)]=[(0,1)]$$

$[(m,n)]$ **の乗法に関する逆元が** $[(n,m)]$ **である事**：$m,n\neq0$ ならば

$$[(m,n)]\cdot[(n,m)]=[(mn,nm)]=[(1,1)]$$

$\mathbb{Q}$ に於ける関係 $\leq$ が代表元の取り方に依らず定まる事：
$(m,n) \leq [(k,\ell)], (m,n) \sim (m',n'), (k,\ell) \sim (k',\ell')$ であるとする。先ず

$$\begin{aligned} & (m,n) \sim (m'n'),\ (k,\ell) \sim (k',\ell') \\ \Leftrightarrow\ & mn' = m'n, k\ell' = k'\ell \\ \Rightarrow\ & (m'\ell')nk = (m'n)(\ell'k) = (mn')(\ell k') = (n'k')m\ell \end{aligned}$$

なる関係に注意する。

(1) $k = 0$ **の場合**： 関係 $\leq$ の定義により $n\ell > 0$ なるとき $m\ell \leq 0$ であり $n\ell < 0$ なるとき $m\ell \geq 0$ である。これより

$n > 0, \ell > 0$ なら $m \leq 0$
$n > 0, \ell < 0$ なら $m \leq 0$
$n < 0, \ell > 0$ なら $m \geq 0$
$n < 0, \ell < 0$ なら $m \geq 0$

となる。上記全ての場合に $mn \leq 0$ 従って $m'n' \leq 0$ が成立する。

さて $k\ell' = k'\ell$ より $k' = 0$ であるから「$n'\ell' > 0$ なるとき $m'\ell' \leq 0$ であり $n'\ell' < 0$ なるとき $m'\ell' \geq 0$ である事」を示せば良い。$n'\ell'$ の符号と $m'n'$ の符号を与えたとき $m'\ell'(n')^2 = (n'\ell')(m'n')$ により $m'\ell'$ の符号が判別出来る。

さて $m'n' \leq 0$ であるから

$n'\ell' > 0$ なら $m'\ell' \leq 0$
$n'\ell' < 0$ なら $m'\ell' \geq 0$

が従い、順序 $\leq$ は代表元の取り方に依らない事が分かる。

(2) $k\ell > 0$ **の場合**：$n\ell > 0$ なるとき $m\ell \leq nk$ であり $n\ell < 0$ なるとき $m\ell \geq nk$ である。「$n'\ell' > 0$ なるとき $m'\ell' \leq n'k'$ であり $n'\ell' < 0$ なるとき $m'\ell' \geq n'k'$ である事」を示せば良い。$k'\ell = k'\ell$ より $k'\ell' > 0$ が従う。等式 $n'k'(\ell')^2 = (n'\ell')(k'\ell')$ により $n'k'$ の符号と $n'\ell'$ の符号は一致し、等式 $(m'\ell')nk = (n'k')m\ell$ 及び不等式 $m\ell \leq nk (n\ell > 0$ の場合$)$ または $m\ell \geq nk (n\ell < 0$ の場合$)$ より、$m'\ell'$ と $n'k'$ との大小関係が定まる。これより

(i) $n\ell > 0, k > 0$ なら $\ell > 0,\ n > 0$ であり
- $n'\ell' > 0$ なら $(m'\ell')nk = (n'k')m\ell \leq (n'k')nk$ より $m'\ell' \leq n'k'$ が従う。
- $n'\ell' < 0$ なら $(m'\ell')nk = (n'k')m\ell \geq (n'k')nk$ より $m'\ell' \geq n'k'$ が従う。

(ii) $n\ell > 0, k < 0$ なら $\ell < 0,\ n < 0$ であり
- $n'\ell' > 0$ なら $(m'\ell')nk = (n'k')m\ell \leq (n'k')nk$ より $m'\ell' \leq n'k'$ が従う。
- $n'\ell' < 0$ なら $(m'\ell')nk = (n'k')m\ell \geq (n'k')nk$ より $m'\ell' \geq n'k'$ が従う。

(iii) $n\ell < 0, k > 0$ なら $\ell > 0,\ n < 0$ であり

- $n'\ell' > 0$ なら $(m'\ell')nk = (n'k')m\ell \geq (n'k')nk$ より $m'\ell' \leq n'k'$ が従う。
- $n'\ell' < 0$ なら $(m'\ell')nk = (n'k')m\ell \leq (n'k')nk$ より $m'\ell' \geq n'k'$ が従う。

(iv) $n\ell < 0, k < 0$ なら $\ell < 0,\ n > 0$ であり

- $n'\ell' > 0$ なら $(m'\ell')nk = (n'k')m\ell \geq (n'k')nk$ より $m'\ell' \leq n'k'$ が従う。
- $n'\ell' < 0$ なら $(m'\ell')nk = (n'k')m\ell \leq (n'k')nk$ より $m'\ell' \geq n'k'$ が従う。

従って、順序 $\leq$ は代表元の取り方に依らない事が分かる。

(3) $k\ell < 0$ **の場合**: $k'\ell = k\ell'$ により $k'\ell' < 0$ が従う。等式 $n'k'(\ell')^2 = (n'\ell')(k'\ell')$ により $n'k'$ の符号と $n'\ell'$ の符号は反対であり、等式 $(m'\ell')nk = (n'k')m\ell$ 及び不等式 $m\ell \leq nk (n\ell > 0$ の場合) または $m\ell \geq nk (n\ell < 0$ の場合) より、$m'\ell'$ と $n'k'$ との大小関係が定まる。これより

(i) $n\ell > 0, k > 0$ なら $\ell < 0,\ n < 0$ であり

- $n'\ell' > 0$ なら $(m'\ell')nk = (n'k')m\ell \geq (n'k')nk$ より $m'\ell' \leq n'k'$ が従う。
- $n'\ell' < 0$ なら $(m'\ell')nk = (n'k')m\ell \leq (n'k')nk$ より $m'\ell' \geq n'k'$ が従う。

(ii) $n\ell > 0, k < 0$ なら $\ell > 0,\ n > 0$ であり

- $n'\ell' > 0$ なら $(m'\ell')nk = (n'k')m\ell \geq (n'k')nk$ より $m'\ell' \leq n'k'$ が従う。
- $n'\ell' < 0$ なら $(m'\ell')nk = (n'k')m\ell \leq (n'k')nk$ より $m'\ell' \geq n'k'$ が従う。

(iii) $n\ell < 0, k > 0$ なら $\ell < 0,\ n > 0$ であり

- $n'\ell' > 0$ なら $(m'\ell')nk = (n'k')m\ell \leq (n'k')nk$ より $m'\ell' \leq n'k'$ が従う。
- $n'\ell' < 0$ なら $(m'\ell')nk = (n'k')m\ell \geq (n'k')nk$ より $m'\ell' \geq n'k'$ が従う。

(iv) $n\ell < 0, k < 0$ なら $\ell > 0,\ n < 0$ であり

- $n'\ell' > 0$ なら $(m'\ell')nk = (n'k')m\ell \leq (n'k')nk$ より $m'\ell' \leq n'k'$ が従う。
- $n'\ell' < 0$ なら $(m'\ell')nk = (n'k')m\ell \geq (n'k')nk$ より $m'\ell' \geq n'k'$ が従う。

故に、順序 $\leq$ は代表元の取り方に依らない事が分かる。

$\mathbb{Q}$ に於ける関係 $\leq$ が順序を成す事:

反射性: $[(m,n)] \leq [(m,n)] \Leftrightarrow n^2 > 0$ であり $mn = nm$

反対称性: $[(m,n)] \leq [(k,\ell)],\ [(k,\ell)] \leq [(m,n)]$

$$\Leftrightarrow \begin{cases} n\ell > 0 \text{ なるとき } m\ell \leq nk \text{ 且つ } nk \leq m\ell \\ n\ell < 0 \text{ なるとき } m\ell \geq nk \text{ 且つ } nk \geq m\ell \end{cases}$$

$$\Leftrightarrow\ m\ell = nk \Leftrightarrow\ [(m,n)] = [(k,\ell)]$$

推移性: $[(m,n)] \leq [(k,\ell)],\ [(k,\ell)] \leq [(i,j)]$

$$\Leftrightarrow \begin{cases} n\ell > 0 \text{ なるとき } m\ell \leq nk,\ n\ell < 0 \text{ なるとき } m\ell \geq nk \\ \ell j > 0 \text{ なるとき } kj \leq \ell i,\ \ell j < 0 \text{ なるとき } kj \geq \ell i \end{cases}$$

ここで (1) $n_j > 0$　(2) $n_j < 0$　の二つの場合に分けて考える。

$$(1) \quad nj > 0 \Leftrightarrow nj\ell^2 > 0 \Leftrightarrow \left\{ \begin{array}{l} n\ell > 0 \text{ 且つ } \ell j > 0 \\ n\ell < 0 \text{ 且つ } \ell j < 0 \end{array} \right\} \text{の場合}$$

(i) $n\ell > 0, \ell j > 0, \ell > 0$ **の場合**

$n > 0, j > 0$ となるので $m\ell j \leq nkj \leq n\ell i$ であり $\ell > 0$ 故 $mj \leq ni$ が従う。

(ii) $n\ell > 0, \ell j > 0, \ell < 0$ **の場合**

$n < 0, j < 0$ となるので $m\ell j \geq nkj \geq n\ell i$ であり $\ell < 0$ 故 $mj \leq ni$ が従う。

(iii) $n\ell < 0, \ell j < 0, \ell > 0$ **の場合**

$n < 0, j < 0$ となるので $m\ell j \leq nkj \leq n\ell i$ であり $\ell > 0$ 故 $mj \leq ni$ が従う。

(iv) $n\ell < 0, \ell j < 0, \ell < 0$ **の場合**

$n > 0, j > 0$ となるので $m\ell j \geq nkj \geq n\ell i$ であり $\ell < 0$ 故 $mj \leq ni$ が従う。

$$(2) \quad nj < 0 \Leftrightarrow nj\ell^2 < 0 \Leftrightarrow \left\{ \begin{array}{l} n\ell > 0 \text{ 且つ } \ell j < 0 \\ n\ell < 0 \text{ 且つ } \ell j > 0 \end{array} \right\} \text{の場合}$$

(i) $n\ell > 0, \ell j < 0, j > 0$ **の場合**

$\ell < 0, n < 0$ となるので $m\ell j \leq nkj \leq n\ell i$ より $mj \geq ni$ が従う。

(ii) $n\ell > 0, \ell j < 0, j < 0$ **の場合**

$\ell > 0, n > 0$ となるので $m\ell j \geq nkj \geq n\ell i$ より $mj \geq ni$ が従う。

(iii) $n\ell < 0, \ell j > 0, j > 0$ **の場合**

$\ell > 0, n < 0$ となるので $m\ell j \geq nkj \geq n\ell i$ より $mj \geq ni$ が従う。

(iv) $n\ell < 0, \ell j > 0, j < 0$ **の場合**

$\ell < 0, n > 0$ となるので $m\ell j \leq nkj \leq n\ell i$ より $mj \geq ni$ が従う。

以上より

$$nj > 0 \text{ なるとき } mj \leq ni$$
$$nj < 0 \text{ なるとき } mj \geq ni$$

即ち $[(m,n)] \leq [(i,j)]$ が従う。

$\mathbb{Q}$ **は順序** $\leq$ **に於いて全順序を成す事**：任意の $[(m,n)], [(k,\ell)] \in \mathbb{Q}$ に対し $n\ell \neq 0$ 故 $n\ell > 0$ か $n\ell < 0$ かどちらか一方が成立つ。

(1) $n\ell > 0$ の場合：$m\ell, nk \in \mathbb{Z}$ 故

(i) $m\ell = nk$, (ii) $m\ell > nk$, (iii) $m\ell < nk$

の何れか一つが成立つ。(i) の場合は定義により $[(m,n)] = [(k,\ell)]$ となり (ii)(iii) の場合は順序の定義により夫々$[(m,n)] > [(k,\ell)], [(m,n)] < [(k,\ell)]$ となる。

(2) $n\ell < 0$ の場合：上と同様 (i)(ii)(iii) の何れか一つが成立ち夫々$[(m,n)] = [(k,\ell)]$, $[(m,n)] < [(k,\ell)], [(m,n)] > [(k,\ell)]$ が成立つ。

以上より $\mathbb{Q}$ は全順序集合となる。

$\mathbb{Q}$ は順序体を成す事：$[(m,n)] < [(k,\ell)]$ なる $[(m,n)], [(k,\ell)] \in \mathbb{Q}$ を取る。定義により $n\ell > 0$ なるとき $m\ell < nk, n\ell < 0$ なるとき $m\ell > nk$ となる。

(1) 任意の $[(i,j)] \in \mathbb{Q}$ に対し $[(m,n)] + [(i,j)] < [(k,\ell)] + [(i,j)]$ なる事：

これは $[(mj+ni, nj)] < [(kj+\ell i, \ell j)]$ 即ち

$$\begin{cases} n\ell > 0 \text{ なるとき } (mj+ni)\ell j < (kj+\ell i)nj \Leftrightarrow m\ell j^2 < nkj^2 \Leftrightarrow m\ell < nk \\ n\ell < 0 \text{ なるとき } (mj+ni)\ell j > (kj+\ell i)nj \Leftrightarrow m\ell j^2 > nkj^2 \Leftrightarrow m\ell > nk \end{cases}$$

と同値である。

(2) 任意の $[(i,j)] > [(0,1)]$ に対し $[(m,n)] \cdot [(i,j)] < [(k,\ell)] \cdot [(i,j)]$ なる事：

これは $[(mi, nj)] < [(ki, \ell j)]$ 即ち

$$\begin{cases} n\ell > 0 \text{ なるとき } mi\ell j < njki \\ n\ell < 0 \text{ なるとき } mi\ell j > njki \end{cases}$$

と同値であり $[(i,j)] > [(0,1)] \Leftrightarrow ij > 0$ 故これは $[(m,n)] < [(k,\ell)]$ と同値である。

埋込み写像 $\iota : \mathbb{Z} \ni m \mapsto \iota(m) = [(m,1)] \in \mathbb{Q}$ は単射である事：

$$\iota(m) = \iota(n) \Leftrightarrow [(m,1)] = [(n,1)] \Leftrightarrow m = n$$

ι は準同型である事：

$$\iota(m+n) = [(m+n,1)] = [(m,1)] + [(n,1)] = \iota(m) + \iota(n)$$

$$\iota(mn) = [(mn,1)] = [(m,1)] \cdot [(n,1)] = \iota(m) + \iota(n)$$

$m \leq n \Leftrightarrow \iota(m) \leq \iota(n)$ なる事：

$$m \leq n \Leftrightarrow [(m,1)] \leq [(n,1)] \Leftrightarrow \iota(m) \leq \iota(n)$$

$[(m,n)] = \iota(m)/\iota(n)$ なる事：

$$\iota(n) \cdot [(m,n)] = [(n,1)] \cdot [(m,n)] = [(mn,n)] = [(m,1)] = \iota(m)$$

$|[(m,n)]| = |\iota(m)/|\iota(n)| = \iota(|m|)/\iota(|n|)$ **なる事**

初めの等式は順序体$\mathbb{Q}$上の絶対値の性質である事から従う。次の等式は$m > 0$なら$\iota(|m|) = [(|m|,1)] = [(m,1)] = \iota(m) = |\iota(m)|, m < 0$なら$\iota(|m|) = [(-m,1)] = \iota(-m) = -\iota(m) = |\iota(m)|$より従う。

命題１： $\mathbb{Q}$は可算である。
（証明） $\mathbb{Z}$及び$\mathbb{Z} \setminus \{0\}$は可算であるから、その積集合$\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$も可算である。$\mathbb{Q}$は可算集合$\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$からの全射による像であるから可算である。

定理２（有理数体の特徴付け I）順序体Kに対し次は同値である：

(1) Kは$\mathbb{Q}$と順序体として同型である。即ち全単射$f : \mathbb{Q} \to K$が存在して任意の$[(m,n)], [(k,\ell)] \in \mathbb{Q}$に対し次を満たす：

(i) $$f([(m,n)] + [(k,\ell)]) = f([(m,n)]) + f([(k,\ell)])$$
$$f([(m,n)] \cdot [(k,\ell)]) = f([(m,n)]) \cdot f([(k,\ell)])$$

(ii) $$[(m,n)] \leq [(k,\ell)] \Rightarrow f([(m,n)]) \leq f([(k,\ell)])$$

(iii) $$|f([(m,n)])| = |[(m,n)]|$$

(2) Kは$\mathbb{Z}$と順序環として準同型で$\mathbb{Z}$の商体として実現される。即ち単射$g : \mathbb{Z} \to K$が存在して任意の$m, n \in \mathbb{Z}$に対し次を満たす：

(i) $$g(m+n) = g(m) + g(n)$$
$$g(mn) = g(m) \cdot g(n)$$

(ii) $$m \leq n \Rightarrow g(m) \leq g(n)$$

(iii) $$n \neq 0 \Leftrightarrow g(n) \neq 0_K$$

(iv) $$K = \{g(m)/g(n); (m,n) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})\}$$

(v) $$|g(m)| = |m|$$

（証明） **(1)** $\Rightarrow$ **(2)** : $\mathbb{Z}$から$\mathbb{Q}$への埋込み$\iota \ni m \mapsto \iota(m) = [(m,1)] \in \mathbb{Q}$によって$g = f \circ \iota$と置く。$f$は同型で$\iota$は準同型単射でどちらも順序を保つので$g$は準同型単射で順序を保つ。$g(0) = g(0+0) = g(0) + g(0)$故$g(0) = 0_K$であり$g$は単射故(iii)が成立つ。ま

た $g(1)=g(1\cdot 1)=g(1)\cdot g(1)\Leftrightarrow g(1)\cdot(1_K-g(1))=0_K\Leftrightarrow g(1)=1_K$ であり $m\in\mathbb{Z}\setminus\{0\}$ に対し

$$\begin{aligned}1_K=g(1)&=f([(1,1)])=f([(m,m)])=f([(m,1)]\cdot[(1,m)])\\&=f([(m,1)])\cdot f([(1,m)])\end{aligned}$$

であるから $(f([(m,1)]))^{-1}=1_K/f([(m,1)])=f([(1,m)])$ が成立つ。故に

$$f([(m,n)])=f([(m,1)]\cdot[(1,n)])=f([(m,1)])\cdot f([(1,n)])$$

$$=f([(m,1)])/f([(n,1)])=g(m)/g(n)$$

となり

$$K=f(\mathbb{Q})=\{g(m)/g(n);(m,n)\in\mathbb{Z}\times(\mathbb{Z}\setminus\{0\}\}$$

が従う。

(2) $\Rightarrow$ **(1)**：上と同様な議論で $g(0)=0_K$ 及び $g(1)=1_K$ が成立つ。$m\in\mathbb{Z},n\in\mathbb{Z}\setminus\{0\}$ に対し $f([(m,n)])=g(m)/g(n)$ と定義する。

$f([(m,n)])$ **は代表元の取り方に依らず定まる事**：

$$\begin{aligned}(m,n)\sim(k,\ell)&\Leftrightarrow m\ell=nk\Leftrightarrow g(m\ell)=g(nk)\Leftrightarrow g(m)g(\ell)=g(n)g(k)\\&\Leftrightarrow g(m)/g(n)=g(k)/g(\ell)\end{aligned}$$

f **は準同型なる事**：

$$\begin{aligned}&f([(m,n)]+[(k,\ell)])=f([(m\ell+nk,n\ell)])=g(m\ell+nk)/g(n\ell)\\&=(g(m)\cdot g(\ell)+g(n)\cdot g(k))/(g(n)\cdot g(\ell))=g(m)/g(n)+g(k)/g(\ell)\\&=f([(m,n)])+f([(k,\ell)]),\\&f([(m,n)]\cdot[(k,\ell)])=f([(mk,n\ell)])=g(mk)/g(n\ell)\\&=(g(m)\cdot g(k))/(g(n)\cdot g(\ell))=(g(m)/g(n))\cdot(g(k)/g(\ell))\\&=f([(m,n)])\cdot f([(k,\ell)])\end{aligned}$$

f **は順序を保つ事**：

$$[(m,n)]\le[(k,\ell)]\Leftrightarrow\begin{cases}n\ell>0\text{ なるとき }m\ell\le nk\\ n\ell<0\text{ なるとき }m\ell\ge nk\end{cases}$$

$$\Leftrightarrow\begin{cases}n\ell>0\text{ なるとき }g(m\ell)\le g(nk)\Leftrightarrow g(m)\cdot g(\ell)\le g(n)\cdot g(k)\\ n\ell<0\text{ なるとき }g(m\ell)\ge g(nk)\Leftrightarrow g(m)\cdot g(\ell)\ge g(n)\cdot g(k)\end{cases}$$

ここで $n\ell>0$ ならば $g(n)\cdot g(\ell)=g(n\ell)>g(0)=0_K$ であるから

$$\begin{aligned}g(m)\cdot g(\ell)\le g(n)\cdot g(k)\ &\Leftrightarrow g(m)/g(n)\le g(k)/g(\ell)\\&\Leftrightarrow f([(m,n)])\le f([(k,\ell)])\end{aligned}$$

が従い $n\ell < 0$ ならば $g(n)\cdot g(\ell) = g(n\ell) < g(0) = 0_K$ であるから

$$\begin{aligned} g(m)\cdot g(\ell) \geq g(n)\cdot g(k) &\Leftrightarrow g(m)/g(n) \leq g(k)/g(\ell) \\ &\Leftrightarrow f([(m,n)]) \leq f([(k,\ell)]) \end{aligned}$$

が従う。

f は単射なる事：

$$\begin{aligned} &f([(m,n)]) = f([(k,\ell)]) \Leftrightarrow g(m)/g(n) = g(k)/g(\ell) \\ &\Leftrightarrow g(m\ell) = g(m)\cdot g(\ell) = g(n)\cdot g(k) = g(nk) \Leftrightarrow m\ell = nk \\ &\Leftrightarrow [(m,n)] = [(k,\ell)] \end{aligned}$$

f は全射なる事：f の定義と (iv) より直ちに従う。

定理３（有理数体の特徴付け II）

(1) 任意の順序体 K に対し $\mathbb{Q}$ から K への順序を保つ準同型単射 $f : \mathbb{Q} \to K$ が存在する。f は $|f([(m,n)])| = |[(m,n)]|$ を満たす。

(2) 有理数体 $\mathbb{Q}$ の真部分体は存在しない。即ち $\mathbb{Q}$ の部分集合 K が同じ演算の下で体を成せば $\mathbb{Q} = K$ となる。

註　上の定理の意味で $\mathbb{Q}$ は最小の順序体と位置付ける事が出来る。

（証明）

(1) 前節の定理３によって順序を保つ準同型単射 $f : \mathbb{Z} \to K$ が存在する。定理２の (2)⇒(1) の議論と同様に $f([(m,n)]) = f(m)/f(n), [(m,n)] \in \mathbb{Q}$ によって f の定義域は $\mathbb{Q}$ に拡大され (1) が従う。

(2) $\mathbb{N}$ の部分集合 M を $M = \{k \in \mathbb{N}; k\cdot 1_K \in K\}$ と定義する。$1 \in M$ であり $k \in M \Rightarrow k+1 \in M$ となるから $M = \mathbb{N}$ 即ち $\mathbb{N} \subset \mathbb{Q}$ と見做した時 $\mathbb{N} \subset K \subset \mathbb{Q}$ となる。$0 \in K, -\mathbb{N} \subset -K = K$ 故 $\mathbb{Z} \subset K$ が従う。$(m,n) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ に対し $m/n \in K$ であるから $\mathbb{Q} \subset K$ 即ち $\mathbb{Q} = K$ が従う。

5. 順序体に於ける完備性

K を順序体とし $\mathbb{Q} \subset K$ と見做す。K に於ける点列の収束の概念は数列と同様に定義される。即ち K の点列 $\{a_n\}$ が $\alpha \in K$ に収束するとは任意の $\varepsilon \in K_{>0}$ に対し $N \in \mathbb{N}$ が存在し $n \geq N$ なる任意の $n \in \mathbb{N}$ に対し $|a_n - \alpha| < \varepsilon$ となる事と定義する。ここに $K_{>0} = \{k \in K; k > 0\}$ とする。

定理１（順序体のアルキメデス性）順序体 K に対し次は同値である：

(1) 任意の $k \in K_{>0}$ に対し $N \in \mathbb{N}$ が存在し $N > k$ を満たす。

(2) 任意の $m, n \in K_{>0}$ に対し $N \in \mathbb{N}$ が存在し $Nm > n$ を満たす。

(3) 点列 $\{1/n\}$ は $0 \in K$ に収束する： $\lim_{n\to\infty} 1/n = 0$

(4) $\mathbb{Q}$ は K に於いて稠密である。

（証明） **(1)⇒(2)**: 与えられた m, n に対し $k = n/m$ とすれば良い。

(2)⇒(3)： 任意の $\varepsilon \in K_{>0}$ に対し (2) に於いて $m = \varepsilon, n = 1$ とすると $N \in \mathbb{N}$ が存在し $N\varepsilon > 1$ となる。よって $n \geq N$ なる任意の $n \in \mathbb{N}$ に対し $n\varepsilon > 1$ となり $0 < 1/n < \varepsilon$ が従う。
(3)⇒(4)： $m, n \in K$ は $m > n$ を満たすとする。$\varepsilon = m - n$ と置けば $\varepsilon \in K_{>0}$ 故 (3) より $N \in \mathbb{N}$ が在って $\ell \geq N$ なる任意の $\ell \in \mathbb{N}$ に対し $0 < 1/\ell < m - n$ となる。$k = n\ell + 1$ と置けば $k \in \mathbb{N}$ であり $1/k < 1/(n\ell)$ となり $\mathbb{N}$ の部分集合 $M = \{k \in \mathbb{N}; k > n\ell\}$ は空でなく最小元 $k_0 \in \mathbb{N}$ が存在する。
このとき $k_0 - 1 \notin M$ 故 $k_0 > n\ell \geq k_0 - 1$ となり $m = n + (m - n) > (k_0 - 1)/\ell + 1/\ell = k_0/\ell > n$ が成立つ。
(4)⇒(1): (1) を否定して矛盾を導こう。$k_0 \in K_{>0}$ が存在し任意の $n \in \mathbb{N}$ に対し $n \leq k_0$ であるとする。(4) により $k_0 \in K_{>0}$ と $k_0+1 \in K_{>0}$ との間に $i/j \in \mathbb{Q}$ が存在し $k_0 < i/j < k_0+1$ を満たす。$j > 0$ ならば $k_0 < i/j \leq i$ が従い $i \in \mathbb{N}$ は $k_0 < i$ を満たす事となり矛盾を生ずる。$j < 0$ ならば $0 < k_0 < i/j$ 故 $i < 0$ となり $k_0 < |i|/|j| \leq |i|$ より $|i| \in \mathbb{N}$ は $k_0 < |i|$ を満たし再び矛盾を得る。

定義：定理１の同値な条件を満たす順序体を**アルキメデス的**と謂い、それら同値な条件を (A) と表す。

定理２（完備性の特徴付け）　順序体 K に対し次は同値である：

(D) **連結性（デデキント性）**
K の空でない互いに素な部分集合 A, B は $K = A \cup B$ 及び「$a \in A, b \in B \Rightarrow a < b$」なる条件を満たすとすると $c \in K$ が存在して次の (i)(ii) のどちらか一方が成立する：

(i) $A = \{k \in K; k \leq c\}, B = \{k \in K; k > c\}$

(ii) $A = \{k \in K; k < c\}, B = \{k \in K; k \geq c\}$

(W) **条件完備性（ワイエルストラス性）**
K の空でない部分集合は上に有界なら上限を持ち、下に有界なら下限を持つ。

(M) **単調収束性**
K の上に有界な単調増加列は収束列である。
K の下に有界な単調減少列は収束列である。

(A)(CI) **区間縮小法（カントル性）**
K はアルキメデス的であり K の有界閉区間の減少列の共通部分は空でない。

(A)(C) **完備性**
K はアルキメデス的であり K のコーシー列は収束列である。

(BW) **点列コンパクト性（ボルツァノ・ワイエルストラス性）**
K の有界列は収束部分列を持つ。

(BL) **コンパクト性（ボレル・ルベグ性）**
K の有界閉区間の任意の開（区間の成す）被覆は有限部分被覆を持つ。

（証明）(D) ⇒ (W)：$M \neq \emptyset$ は上に有界であるとする。M が一点集合 $\{c\}$ なら $c \in K$ が M の上限である。よって M が二点以上を含む場合を考える。$a, b \in M$ は $a < b$ を満たすとする。K の部分集合 A, B を $A = \{k \in K; \exists m \in M : k < m\}, B = \{k \in K; \forall m \in M, m \leq k\}$ と定義する。M は上に有界故 $B \neq \emptyset$ であり $b \in M$ は $a < b$ を満たすので $a \in A$ であり $A \cap B = \emptyset, A \cup B = K$ が成立する。ここで条件「$k \in A, \ell \in B \Rightarrow k < \ell$」を示そう。もしそうでなければ $k \in A, \ell \in B$ が在って $k \geq \ell$ となるが $\ell \in B, \ell \leq k$ より任意の $m \in M$ に対し $m \leq k$ が従い $k \in B = K \setminus A$ となって矛盾を生ずる。さて、仮定 (D) より $c \in K$ が存在して (i)$A = \{k \in K; k \leq c\}$ (ii)$A = \{k \in K; k < c\}$ のどちらかが成立つ。(i) ならば $c \in A$ 故 $m \in M$ が存在して $c < m$ となる。このとき $d = (c + m)/2$ と置くと $c < d < m$ となる。$c < d$ 故 $d \in K \setminus A = B = \{k \in K; c < k\}$ となる。一方 $d < m$ なる $m \in M$ が存在するので $d \in A$ となり矛盾が生ずる。従って (ii) が成立する。このとき $c \in B$ となり c は M の最小の上界となる。

$M \neq \emptyset$ は下に有界であるとする。M が一点集合 $\{c\}$ なら $c \in K$ が M の下限である。よって M が二点以上を含む場合を考える。$a, b \in M$ は $a < b$ を満たすとする。K の部分集合 A, B を $A = \{k \in K; \forall m \in M, k \leq m\}$ $B = \{k \in K; \exists m \in M : m < k\}$ と定義する。M は下に有界故 $A \neq \emptyset$ であり $a \in M$ は $a < b$ を満たすので $b \in B$ であり $A \cap B = \emptyset, A \cup B = K$ が成立する。ここで条件「$k \in A, \ell \in B \Rightarrow k < \ell$」を示そう。もしそうでなければ $k \in A, \ell \in B$ が在って $k \geq \ell$ となるが $k \in A, \ell \leq k$ より任意の $m \in M$ に対し $\ell \leq m$ が従い $\ell \in A = K \setminus B$ となって矛盾を生ずる。さて、仮定 (D) より $c \in K$ が存在して (i)$A = \{k \in K; k \leq c\}(ii)A = \{k \in K; k < c\}$ のどちらかが成立つ。(ii) ならば $c \in B$ 故 $m \in M$ が存在して $m < c$ となる。このき $d = (c + m)/2$ と置くと $m < d < c$ となる。$d < c$ 故 $d \in A$ となる。一方 $m < d$ なる $m \in M$ が存在するので $d \in B$ となり矛盾を生ずる。従って (i) が成立する。このとき $c \in A$ となり c は M の最大の下界となる。

(W) ⇒ (M)：$\{a_n\} \subset K$ を上に有界な単調増加列とする。仮定 (W) より $\{a_n\}$ は上限 $\alpha \in K$ を持つ。α は $\{a_n\}$ の最小上界であるから任意の $\varepsilon > 0$ に対し $\alpha - \varepsilon$ は上界ではなく $N \in \mathbb{N}$ が在って $\alpha \geq a_N > \alpha - \varepsilon$ を満たす。$\{a_n\}$ は単調増加列だから $n \geq N$ なる任意の $n \in \mathbb{N}$ に対し $\alpha \geq \alpha_n \geq \alpha_N > \alpha - \varepsilon$ となる。即ち $\{a_n\}$ は α に収束する。

$\{a_n\} \subset K$ を下に有界な単調減少列とする。仮定 (W) より $\{a_n\}$ は下限 $\beta \in K$ を持つ。β は $\{a_n\}$ の最大下界であるから任意の $\varepsilon > 0$ に対し $\beta + \varepsilon$ は下界ではなく $N \in \mathbb{N}$ が在って $\beta \leq a_N < \beta + \varepsilon$ を満たす。$\{a_n\}$ は単調減少列だから $n \geq N$ なる任意の $n \in \mathbb{N}$ に対し $\beta \leq a_n \leq a_N \leq +\varepsilon$ となる。即ち $\{a_n\}$ は β に収束する。

(M) ⇒ (A)：$M, \varepsilon \in K_{>0}$ が存在し任意の $n \in \mathbb{N}$ に対し $n\varepsilon \leq M$ であるとする。$a_n = n\varepsilon$ とした点列 $\{a_n\}$ は上に有界な単調増加列であり (M) により収束する。その極限を $\alpha \in K$

とする。$N \in \mathbb{N}$ が在って $n \geq N$ なる任意の $n \in \mathbb{N}$ に対し $\alpha - \varepsilon < n\varepsilon < \alpha + \varepsilon$ となる。特に $\alpha - \varepsilon < N\varepsilon$ より $\alpha < (N+1)\varepsilon$ を得る。一方 $n = N+2$ として $(N+2)\varepsilon < \alpha + \varepsilon$ を得る。以上より $(N+2)\varepsilon < \alpha + \varepsilon < (N+1)\varepsilon + \varepsilon = (N+2)\varepsilon$ となり矛盾が生ずる。

(M) ⇒ (CI)：有界閉区間 $I_n = [a_n, b_n] = \{k \in K; a_n \leq k \leq b_n\}$ の列 $\{I_n\}$ が減少列 $I_n \supset I_{n+1} (\forall n \in \mathbb{N})$ である事より $\{a_n\}$ は上に有界な単調増加列で $\{b_n\}$ は下に有界な単調減少列となる。仮定 (M) より $\{a_n\}$ 及び $\{b_n\}$ は収束列となり極限を持つので夫々 α 及び β と表す。任意の $m \in \mathbb{N}$ を取る。任意の $\varepsilon > 0$ に対し $N \in \mathbb{N}$ が在って $n \geq N$ なる任意の $n \in \mathbb{N}$ に対し $|a_n - \alpha| < \varepsilon,\ |b_n - \beta| < \varepsilon$ が成立つ。$\ell = \max(m, N)$ と置くと $a_m \leq a_\ell < \alpha + \varepsilon,\ \beta - \varepsilon < b_\ell \leq b_m$ となり $\varepsilon > 0$ は任意であるから $a_m \leq \alpha,\ \beta \leq b_m$ が従う。もし $\beta < \alpha$ ならば $\varepsilon = (\alpha - \beta)/2$ として対応する $N \in \mathbb{N}$ を取れば $a_N > \alpha - \varepsilon = \beta + \varepsilon > b_N$ となり矛盾である。従って $\alpha \leq \beta$ となる。故に $[\alpha, \beta] \subset \bigcap_{n \in \mathbb{N}} [a_m, b_m]$ が成立つ。一方 $c > \beta$ なる $c \in \bigcap_{n \in \mathbb{N}} I_n$ が存在したとすると $\varepsilon = (c - \beta)/2 > 0$ に対し $N \in \mathbb{N}$ が存在し $b_N < \beta + \varepsilon = \beta + (c - \beta)/2 = (c + \beta)/2 < c$ が従い $c \notin [a_N, b_N]$ なる矛盾を得る。また $c < \alpha$ なる $c \in \bigcap_{n \in \mathbb{N}} I_n$ が存在したとすると $\varepsilon = (\alpha - c)/2 > 0$ に対し $N \in \mathbb{N}$ が存在し $a_N > \alpha - \varepsilon = \alpha - (\alpha - c)/2 = (\alpha + c)/2 > c$ が従い $c \notin [a_N, b_N]$ なる矛盾を得る。以上より $\emptyset \neq [\alpha, \beta] = \bigcap_{n \in \mathbb{N}} I_n$ が従う。

(A)(CI) ⇒ (D)：$A \neq \emptyset, B \neq \emptyset, A \cap B = \emptyset, A \cup B = K$ なる K の部分集合 A, B は「$a \in A, b \in B \Rightarrow a < b$」なる条件を満たすものとする。

$\{a_n\} \subset A,\ \{b_n\} \subset B$ が存在して $b_n - a_n = (b_1 - a_1)/2^{n-1} > 0$ なる事：$A \neq \emptyset, B \neq \emptyset$ より $a_1 \in A, b_1 \in B$ が存在する。これより $a_1 < b_1$ が従う。$K = A \cup B, A \cap B = \emptyset$ 故 $(a_1 + b_1)/2 \in A$ または $(a_1 + b_1)/2 \in B$ のどちらか一方が成立する。前者の場合 $a_2 = (a_1 + b_1)/2, b_2 = b_1$ と置き、後者の場合 $a_2 = a_1, b_2 = (a_1 + b_1)/2$ と置く。このとき $a_1 \leq a_2 \leq b_2 \leq b_1, b_2 - a_2 = (b_1 - a_1)/2, a_2 \in A, b_2 \in B$ が従う。さて $\mathbb{N}$ の部分集合 M を

$$M = \{n \in \mathbb{N}; \exists\{a_j\}_1^n \in A, \exists\{b_j\}_1^n \in B : b_j - a_j = (b_1 - a_1)/2^{j-1}, 1 \leq j \leq n, \\ a_1 \leq a_2 \leq \cdots \leq a_n \leq b_n \leq \cdots \leq b_2 \leq b_1\}$$

と定義する。上の議論より $1, 2 \in M$ である。任意に $n \in M$ を取る。$(a_n + b_n)/2 \in A$ または $(a_n + b_n)/2 \in B$ のどちらか一方が成立する。前者の場合 $a_{n+1} = (a_n + b_n)/2, b_{n+1} = b_n$ と置き、後者の場合 $a_{n+1} = a_n, b_{n+1} = (a_n + b_n)/2$ と置く。このとき $a_n \leq a_{n+1} \leq b_{n+1} \leq b_n, b_{n+1} - a_{n+1} = (b_n - a_n)/2, a_{n+1} \in A, b_{n+1} \in B$ が従うので $M = \mathbb{N}$ となる事が分かる。

$\bigcap_{n \in \mathbb{N}} [a_n, b_n]$ は一点 $c \in K$ よりなる事：さて $I_n = [a_n, b_n]$ なる有界閉区間列は減少列である。$\{a_n\}$ 及び $\{b_n\}$ の極限を α 及び β とすると (CI) により $[\alpha, \beta] = \bigcap_{n \in \mathbb{N}} I_n$ となる。$b_n - a_n = (b_1 - a_1)/2^{n-1}$ 及び (A) により $\alpha = \beta$ となるので $c = \alpha = \beta$ と置いて $\{c\} = \bigcap_{n \in \mathbb{N}} I_n$ を得る。$c \in K = A \cup B, A \cap B = \emptyset$ 故 $c \in A$ または $c \in B$ のどちらか一方が成立つ。

$c \in A$ **の場合** $A = \{k \in K; k \leq c\}$ **である事**：任意の $k \in A$ を取る。もし $k > c$ であるなら $\varepsilon = (k-c)/2 > 0$ に対する $N \in \mathbb{N}$ を取り $b_N - a_N < \varepsilon$ とする事が出来る。このとき $b_N < a_N + \varepsilon \leq c + \varepsilon = (k+c)/2 < k$ となる。一方 $k \in A, b_N \in B$ 故 $k < b_N$ が従い矛盾が生ずる。故に $A \subset \{k \in K; k \leq c\}$ が成立つ。

さて $k \leq c$ なる任意の $k \in K$ を取る。$k \in B$ なら $c \in A$ 故 $c < k$ が従い矛盾となる。故に $k \in A$ となる。以上より $\{k \in K; k \leq c\} \subset A$ となる。

$c \in B$ **の場合** $B = \{k \in K; k \geq c\}$ **である事**：任意の $k \in B$ を取る。もし $k < c$ であるなら $\varepsilon = (c-k)/2$ に対する $N \in \mathbb{N}$ を取り $b_N - a_N < \varepsilon$ とする事が出来る。このとき $a_N > b_N - \varepsilon \geq c - \varepsilon = (c+k)/2 > k$ となる。一方 $a_N \in A, k \in B$ 故 $a_N < k$ が従い矛盾が生ずる。故に $B \subset \{k \in K; k \geq c\}$ が成立つ。

さて $k \geq c$ なる任意の $k \in K$ を取る。$k \in A$ なら $c \in B$ 故 $k < c$ が従い矛盾となる。故に $k \in B$ となる。以上より $\{k \in K; k \geq c\} \subset B$ となる。

(W)(M) $\Rightarrow$ **(C)**：$\{a_n\} \subset K$ をコーシー列とする。

$\{a_n\}$ **は有界である事**：$\varepsilon = 1$ に対する $N \in \mathbb{N}$ を取れば $n \geq N$ なる任意の $n \in \mathbb{N}$ に対し $|a_n - a_N| \leq 1$ であるから $M = \max(|a_1|, \cdots |a_{N-1}|, |a_N| + 1)$ とすれば任意の $n \in \mathbb{N}$ に対し $|a_n| \leq M$ となる。

$\{a_n\}$ **の上極限の存在**：任意の $n \in \mathbb{N}$ に対し $A_n = \{a_m \in K; m \geq n\}$ は上に有界だから (W) によって上限を持つ。これを $b_n = \sup_{m \geq n} a_m$ と置く。$\{b_n\}$ は下に有界な単調減少列であるから (M) によって或る $c \in K$ に収束する。

$\{a_n\}$ **の極限の存在**：任意に $\varepsilon > 0$ を取る。$N_1 \in \mathbb{N}$ が存在し $m, n \geq N_1$ なる任意の $m, n \in \mathbb{N}$ に対し $|a_m - a_n| < \varepsilon$ が成立つ。$N_2 \in \mathbb{N}$ が存在し $n \geq N_2$ なる任意の $n \in \mathbb{N}$ に対し $|b_n - c| < \varepsilon$ が成立つ。$N = \max(N_1, N_2)$ と置く。任意の $n \geq N$ に対し $b_n - \varepsilon$ は A_n の上限ではないので $m \geq n$ が存在して $b_n - \varepsilon < a_m \leq b_n$ となる。このとき

$$|a_n - c| \leq |a_n - a_m| + |a_m - b_n| + |b_n - c| < 3\varepsilon$$

が従う。これは $\{a_n\}$ が c に収束する事を意味する。

(A)(C) $\Rightarrow$ **(M)**：$\{a_n\} \subset K$ を上に有界な単調増加列とする。$k_0 \in K$ が存在し任意の $n \in \mathbb{N}$ に対し $a_n \leq k_0$ が成立つ。$\{a_n\}$ がコーシー列である事を示そう。もしそうでないとすると $\varepsilon_0 > 0$ が存在し任意の $N \in \mathbb{N}$ に対し $m, n \geq N$ が在って $|a_m - a_n| \geq \varepsilon_0$ とする事が出来る。$\{a_n\}$ は単調増加だから任意の $\ell \geq \max(m, n)$ に対し $a_\ell - a_N \geq a_\ell - a_n \geq a_m - a_n \geq \varepsilon_0$ となる。以上より任意の $N \in \mathbb{N}$ に対し $L \in \mathbb{N}$ が存在し $\ell \geq L$ なる任意の $\ell \in \mathbb{N}$ に対し $a_\ell - a_N \geq \varepsilon_0$ となる事が従う。これより $\{a_n\}$ の部分列 $\{a_{n_j}\}$ で任意の $j \in \mathbb{N}$ に対し $1 = n_1 < n_2 < \cdots < n_j < n_{j+1}$ かつ $a_{n_{j+1}} - a_{n_j} \geq \varepsilon_0$ なるものの存在が従う。
仮定 (A) より $j \in \mathbb{N}$ が在って $j\varepsilon_0 > \varepsilon_0 + k_0 - a_1$ を満たす。このとき

$$a_{n_j} = \sum_{k=1}^{j-1} (a_{n_{k+1}} - a_{n_k}) + a_1 \geq (j-1)\varepsilon_0 + a_1 > k_0$$

となり k_0 が $\{a_n\}$ の上界である事に反する。下に有界な単調減少列がコーシー列となる事も同様にして証明される。

(W)(M) ⇒ (BW)：$\{a_n\} \subset K$ を有界列とする。(W)(M) により $\{a_n\}$ の上極限 $c = \lim_{n\to\infty} b_n, b_n = \sup\{a_m \in K; m \geq n\}$ が存在する。$\mathbb{N}$ の部分集合を

$$M = \{j \in \mathbb{N}; \exists\{n_\ell \in \mathbb{N}; \ell = 1, \cdots, j\} : n_1 < \cdots < n_j, |a_{n_\ell} - c| < 1/\ell(^\forall\ell)\}$$

と定義する。$\varepsilon = 1$ に対して $N_1 \in \mathbb{N}$ が在って $n \geq N_1$ なる任意の $n \in \mathbb{N}$ に対し $c - 1 < b_n < c + 1$ となる。故に $n_1 \geq N_1$ が在って $c - 1 < a_{n_1} \leq b_{N_1}$ となり $1 \in M$ が従う。任意に $j \in M$ を取る。$\varepsilon = 1/(j+1)$ に対し $N_{j+1} \in \mathbb{N}$ が在って $n \geq N_{j+1}$ なる任意の $n \in \mathbb{N}$ に対し $c - 1/(j+1) < b_n < c + 1/(j+1)$ となる。故に $n_{j+1} > \max(n_j, N_{j+1})$ が在って $c - 1/(j+1) < a_{n_{j+1}} \leq b_{N_{j+1}}$ となり $j + 1 \in M$ が従う。以上より $M = \mathbb{N}$ であり $\{a_n\}$ の部分列 $\{a_{n_j}\}$ が定まる。この部分列は $c \in K$ に収束する。

(BW) ⇒ (A)：K がアルキメデス的でなければ $a_n = n$ なる数列 $\{a_n\}$ は有界であり (BW) により収束部分列を持つが $n \neq m$ なら $|a_m - a_n| \geq 1$ となり $\{a_n\}$ の任意の部分列はコーシー列にも成り得ない。

(BW) ⇒ (C)：$\{a_n\} \subset K$ をコーシー列とする。(BW) により部分列 $\{a_{n_j}\}$ は極限 $\alpha \in K$ を持つ。任意の $\varepsilon > 0$ に対し $N_1 \in \mathbb{N}$ が存在し $j \geq N_1$ ならば $|a_{n_j} - \alpha| < \varepsilon$ となる。また $N_2 \in \mathbb{N}$ が存在し、$j, k \geq N_2$ ならば $|a_j - a_k| < \varepsilon$ となる。$N = \max(N_1, N_2)$ と置く。任意の $j \geq N$ に対し $k = n_j$ とすれば $n_j \geq j$ より $|a_j - a_{n_j}| < \varepsilon$ となり $|a_j - \alpha| \leq |a_j - a_{n_j}| + |a_{n_j} - \alpha| < 2\varepsilon$ が従う。これは $\{a_n\}$ が α に収束する事を意味する。

(W) ⇒ (BL)：$I = [a, b] = \{k \in K; a \leq k \leq b\}$ を K の有界閉区間とし $\{U_\lambda : \lambda \in \Lambda\}$ を $[a, b]$ の開（区間の成す）被覆とする。K の部分集合 M を

$$M = \{m \in I; \exists\Lambda'\text{有限} \subset \Lambda : [a, m] \subset \bigcup_{\lambda\in\Lambda'} U_\lambda\}$$

と定義する。M は上に有界で $a \in M$ であるから (W) により上限を持つ。これを $c \in K$ とする。$c > b$ とすると b は M の上界ではないから $m \in M$ が在って $c > m > b$ となるが、これは $m \in I$ に矛盾する。故に $c \leq b$ である。$c \in I$ 故 $\lambda_0 \in \Lambda$ が在って $c \in U_{\lambda_0}$ となる。U_{λ_0} は $a_{\lambda_0}, b_{\lambda_0} \in K$ によって $U_{\lambda_0} = \{k \in K; a_{\lambda_0} < k < b_{\lambda_0}\}$ の形に表されるから $k < c$ なる $k \in U_{\lambda_0}$ を一つ取る。このとき $[k, c] \subset U_{\lambda_0}$ となる。k は M の上界ではないから $m \in M$ が在って $k < m < c$ となる。
このとき Λ の有限部分集合 Λ' が在って $\{U_\lambda; \lambda \in \Lambda'\}$ は $[a, m]$ を覆う。さて $c < b$ であるとすると $c \in U_{\lambda_0}$ 故 $\ell \in U_{\lambda_0}$ が在って $c < \ell < b$ となる。このとき $[c, \ell] \subset U_{\lambda_0}$ より $[k, \ell] = [k, c] \cup [c, \ell] \subset U_{\lambda_0}$ であり $[a, \ell] = [a, m] \cup [k, \ell]$ より $[a, \ell]$ は有限個の $\{U_\lambda; \lambda \in \Lambda' \cup \{\lambda_0\}\}$ で覆う事が出来る。従って $\ell \in M$ となるがこれは $c = \sup M$ である事に反する。よって $c = b$ である。さて $[a, b] = [a, m] \cup [k, c]$ 故 I は有限個の $\{U_\lambda; \lambda \in \Lambda' \cup \{\lambda_0\}\}$ で覆う事が出来る。

(BL) ⇒ (W)：

K **は** (A) **を満たす事**：そうでないとすると $\mathbb{N}$ は K の上に有界な部分集合となる。集合 B を $\mathbb{N}$ の上界の全体とする：$B = \{b \in K; \forall n \in \mathbb{N}, n \leq b\}$
仮定より B は空でないので元 $b_0 \in B$ を一つ取る。各 $n \in \mathbb{N}$ に対し $U_n = (n - 1/2, n + 1/2) = \{k \in K; n - 1/2 < k < n + 1/2\}$ と置く。$n < k < n + 1$ なる $k \in K$ に対し $U_k = (n, n + 1) = \{\ell \in K; n < \ell < n + 1\}$ と置く。これらを全て合せて $\{U_\lambda; \lambda \in \Lambda\}$ と表す。さて任意の $\ell \in [1, b_0] \setminus B$ に対し $\ell < n$ なる $n \in \mathbb{N}$ が存在する。$M_\ell = \{m \in \mathbb{N}; \ell < m\}$ は $n \in M_\ell$ より空でなく最小元 $\ell' = \min M_\ell$ を持つ。$\ell \in \mathbb{N}$ なら $\ell = \ell' + 1$ 故 $\ell \in U_{\ell'+1} = U_\ell$ となり $\ell \notin \mathbb{N}$ なら $\ell' - 1 < \ell < \ell'$ 故 $\ell \in (\ell' - 1, \ell') = U_\ell$ となる。以上より $[1, b_0] \setminus B \subset \bigcup_{\lambda \in \Lambda} U_\lambda$ が従う。
また $k \leq b_0$ なる $k \in B$ に対し $U_k = (k - 1/2, k + 1/2)$ と置くと $[1, b_0] \cap B \subset \bigcap \{U_k; k \in B, k \leq b_0\}$ となるので上の $\{U_\lambda : \lambda \in \Lambda\}$ と合せた開区間の族は有界閉区間 $[1, b_0]$ の開被覆となり (BL) より有限部分被覆を持つ。この有限部分被覆は $\mathbb{N}$ を覆う。一方 $n \in \mathbb{N}$ を含む開被覆は U_n だけでありこの有限部分被覆には有限個の自然数しか含まれず矛盾を生ずる。

K **の空でない上に有界な部分集合は上限を持つ事**：A_0 を空でない上に有界な部分集合とする。A_0 は上限を持たないと仮定し矛盾を導こう。$A = \{k \in K; \exists a \in A_0 : k \leq a\}$ と置く。A_0 及び A の上界の成す集合を夫々 B_0 及び B とする：

$$B_0 = \{k \in K; \forall a \in A_0, a \leq k\},\ B = \{k \in K; \forall a \in A, a \leq k\}$$

このとき $A_0 \subset A, B \subset B_0$ である。仮定より A_0 も B_0 も空でない。任意の $b_0 \in B_0$ を取る。任意の $a_0 \in A_0$ に対し $a_0 \leq b_0$ となる。任意の $a \in A$ に対し $a_0 \in A_0$ が在って $a \leq a_0$ となるので $a \leq b_0$ が従う。故に $b_0 \in B$ となり $B = B_0$ が成立つ。

A_0 の上限即ち B_0 の最小元は存在しないので B の最小元は存在しない。また A に最大元が存在したとするとそれは A_0 の最大元となり上限でもあるので矛盾である。故に A の最大元は存在しない。

$A \cap B$ が空でないとすると $k \in A \cap B$ は A の最大元となってしまい矛盾である。故に $A \cap B = \emptyset$ である。

$A \cup B = K$ でないとすると $k \notin A \cup B$ なる $k \in K$ が存在するが $k \notin A$ 故 $k \leq a$ なる $a \in A$ は存在しない事により任意の $a \in A$ に対し $a < k$ なる事が従い $k \in B$ となり矛盾。よって $A \cup B = K$ が成立つ。A の定義により $k \in A, \ell \in K$ に対し $\ell < k$ なら $\ell \in A$ となる事に注意する。同様には $k \in B, \ell \in K$ に対し $\ell > k$ なら $\ell \in B$ となる。

A には最大元が存在しないので任意の $a \in A$ に対し $a < k$ なる $k \in A$ が存在する。K のアルキメデス性により $(k - a)n > 1$ なる $n \in \mathbb{N}$ が存在する。従って $\mathbb{N}$ の部分集合 $M_a = \{n \in \mathbb{N}; a + 1/n \in A\}$ は空でなく最小元が存在する。M_a の最小元を $n(a)$ と表す：$n(a) = \min M_a$

B には最小元が存在しないので任意の $b \in B$ に対し $k < b$ なる $k \in B$ が存在し $(b - k)n > 1$ なる $n \in \mathbb{N}$ が存在する。従って $M_b = \{n \in \mathbb{N}; b - 1/n \in B\}$ は空でなく最小元 $n(b) = \min M_b$ が存在する。

任意の $a \in A$ に対し $U_a = (a - 1/n(a), a + 1/n(a)) = \{k \in K; a - 1/n(a) < k < a + 1/n(a)\}$ 及び任意の $b \in B$ に対し $U_b = (b - 1/n(b), b + 1/n(b)) = \{k \in K; b - 1/n(b) < k < b + 1/n(b)\}$ と置く。A 及び B から任意に二点 $a_0 \in A$ 及び $a_0 \in B$ を取る。このとき

$a_0 < b_0$ である。$\{U_k; k \in K\} = \{U_a; a \in A\} \cup \{U_b; b \in B\}$ は有界閉区間 $[a_0, b_0]$ の開被覆となり (BL) より有限部分被覆を持つ。そのうち $\{U_a; a \in A\}$ の成す部分を $\{U_{a_j}; i = 1, \cdots, n\}$ と表す事にすれば $c = \max\{a_i + 1/n(a_i) : i = 1, \cdots, n\}$ は A の最大元となる事が次の様にして示される。先ず $a_i + 1/n(a_i) \in A$ より $c \in A$ である。任意の $a \in A$ を取る。$a \leq a_0$ なら $a_0 \leq c$ 故 $a \leq c$ である。$a_0 < a$ なら $a \in [a_0, b_0] \cap A$ 故或る i に対し $a \in U_{a_i}$ となり $a < a_i + 1/n(a_i) \leq c$ が従う。

c は A の最大元となるが A は最大元を持たないので矛盾である。

定義：順序体 K は定理 2 の同値な条件を満たすとき**実数体**と謂い、その元を**実数**と謂う。定理 2 の同値な条件を**実数の連続性**と謂う。

6. 実数

定理１（実数体の構成）有理数体 $\mathbb{Q}$ のコーシー列の全体の成す集合 $\mathcal{C}$ に於いて、関係 $\sim$ を

$$\{a_m\} \sim \{b_n\} \underset{def.}{\Longleftrightarrow} \{a_n - b_n\} \text{ は } 0 \text{ に収束する}$$

と定めると $\sim$ は同値関係を成す。$\mathcal{C}$ を関係 $\sim$ で割った商集合 $\mathcal{C}/\sim$ を $\mathbb{R}$ と表し $\{a_n\}$ の属す類を $[\{a_n\}]$ と表す：

$$[\{a_n\}] = \{\{b_n\} \in \mathcal{C}; \{a_n\} \sim \{b_n\}\}$$

$\mathbb{Q}$ から $\mathbb{R}$ への写像 ι が $\iota(q) = [\{a_n\}]$ で定まる。ここに $\{a_n\}$ は $a_n = q(\forall n)$ で定まる $\mathcal{C}$ の元とする。

$\mathbb{R}$ の二つの元 $\{a_n\}$ 及び $[\{b_n\}]$ に対し和と積が

$$[\{a_n\}] + [\{b_n\}] \underset{\text{def.}}{=} [\{a_n + b_n\}]$$
$$[\{a_n\}] \cdot [\{b_n\}] \underset{\text{def.}}{=} [\{a_n + b_n\}]$$

によって（代表元の取り方に依らず）定まり $\mathbb{R}$ に加法と乗法が定義される。加法及び乗法の単位元は夫々 $\iota(0)$ 及び $\iota(1)$ であり $[\{a_n\}]$ の加法及び乗法（但し $[\{a_n\}] \neq \iota(0)$) に関する逆元は夫々 $[\{-a_n\}]$ 及び $[\{b_n\}]$（ここに $a_n = 0$ なる n に対し $b_n = 0, a_n \neq 0$ なる n に対し $b_n = 1/a_n$ と定める）で与えられる。
$\mathbb{R}$ は可換体を成す。$\mathbb{R}$ には

$$[\{a_n\}] < [\{b_n\}] \underset{def.}{\Longleftrightarrow} [\exists \varepsilon_0 \in \mathbb{Q}_{>0} \exists N \in \mathbb{N} : \forall n \geq N, b_n - a_n \geq \varepsilon_0]$$
$$[\{a_n\}] \leq [\{b_n\}] \underset{def.}{\Longleftrightarrow} [\{a_n\}] < [\{b_n\}] \text{ または } [\{a_n\}] = [\{b_n\}]$$

によって（代表元の取り方に依らず）関係 $\leq$ が定義され順序の公理を満たす。$\mathbb{R}$ は全順序集合で順序体を成す。任意の $[\{a_n\}] \in \mathbb{R}$ に対し $[\{a_n\}] \geq \iota(0)$ なら $|[\{a_n\}]| = [\{a_n\}], [\{a_n\}] < \iota(0)$ なら $|[\{a_n\}]| = -[\{a_n\}] = [\{-a_n\}]$ と置く。$\mathbb{R}$ はアルキメデス的で完備である。$\mathbb{Q}$ から $\mathbb{R}$ への写像 ι は単射であり加法と乗法に関し準同型であり値域 $\iota(\mathbb{Q})$ は $\mathbb{R}$ で稠密となる。値域を制限した写像 $\iota : \mathbb{Q} \ni q \mapsto \iota(q) \in \iota(\mathbb{Q})$ は全単射であり和と積と順序に関し同型となる。

（証明）　関係 $\sim$ は $\mathcal{C}$ の同値関係を成す事：

反射性：$\{a_n\} \sim \{a_n\}$ は $a_n - a_n = 0(\forall n)$ なる事より従う。

対称性：$\{a_n\} \sim \{b_n\} \Leftrightarrow$ $\{a_n - b_n\}$ は 0 に収束する

$\Leftrightarrow$ $\{b_n - a_n\}$ は 0 に収束する $\Leftrightarrow \{b_n\} \sim \{a_n\}$

推移性：$\{a_n\} \sim \{b_n\},\ \{b_n\} \sim \{c_n\}$

$\Leftrightarrow \{a_n - b_n\}, \{b_n - c_n\}$ は 0 に収束する

$\Rightarrow \{a_n - c_n\}$ は 0 に収束する $\Leftrightarrow \{a_n\} \sim \{c_n\}$

加法が代表元の取り方に依らず定まる事：$\{a_n\} \sim \{a'_n\}, \{b_n\} \sim \{b'_n\}$

$\Leftrightarrow \{a_n - a'_n\}, \{b_n - b'_n\}$ は 0 に収束する

$\Rightarrow \{(a_n - b_n) - (a'_n + b'_n)\}$ は 0 に収束する $\Leftrightarrow \{a_n + b_n\} \sim \{a'_n + b'_n\}$

乗法が代表元の取り方に依らず定まる事：$\{a_n\} \sim \{a'_n\}, \{b_n\} \sim \{b'_n\}$

$\Leftrightarrow \{a_n - a'_n\}, \{b_n - b'_n\}$ は 0 に収束する

$\Rightarrow \{a_n b_n - a'_n b'_n\}$ は 0 に収束する $\Leftrightarrow \{a_n b_n\} \sim \{a'_n b'_n\}$

最後の $\Rightarrow$ にはコーシー列が有界列である事と次の等式を用いる：

$$a_n b_n - a'_n b'_n = (a_n - a'_n)(b_n - b'_n) + a'_n(b_n - b'_n) + (a_n - a'_n)b'_n$$

加法の可換則：

$$[\{a_n\}] + [\{b_n\}] = [\{a_n + b_n\}] = [\{b_n + a_n\}] = [\{b_n\}] + [\{a_n\}]$$

加法の結合則：

$$\begin{aligned}
&([\{a_n\}] + [\{b_n\}]) + [\{c_n\}] = [\{a_n + b_n\}] + [\{c_n\}] \\
&= [\{(a_n + b_n) + c_n\}] = [\{a_n + (b_n + c_n)\}] = [\{a_n\}] + [\{b_n + c_n\}] \\
&= [\{a_n\}] + ([\{b_n\}] + [\{c_n\}])
\end{aligned}$$

乗法の可換則：

$$[\{a_n\}] \cdot [\{b_n\}] = [\{a_n b_n\}] = [\{b_n a_n\}] = [\{b_n\}] \cdot [\{a_n\}]$$

乗法の結合則：

$$\begin{aligned}
&([\{a_n\}] \cdot [\{b_n\}]) \cdot [\{c_n\}] = [\{a_n b_n\}] \cdot [\{c_n\}] = [\{(a_n b_n)c_n\}] \\
&= [\{a_n(b_n c_n)\}] = [\{a_n\}] \cdot [\{b_n c_n\}] = [\{a_n\}] \cdot ([\{b_n\}] \cdot [\{c_n\}])
\end{aligned}$$

加法に関する乗法の分配則：

$$\begin{aligned}&[\{a_n\}]\cdot([\{b_n\}]+[\{c_n\}])=[\{a_n\}]\cdot[\{b_n+c_n\}]\\&=[\{a_n(b_n+c_n)\}]=[\{a_nb_n+a_nc_n\}]=[\{a_nb_n\}]+[\{a_nc_n\}]\\&=[\{a_n\}]\cdot[\{b_n\}]+[\{a_n\}]\cdot[\{c_n\}]\end{aligned}$$

加法の単位元が $\iota(0)$ **である事**：

$$[\{a_n\}]+\iota(0)=[\{a_n+0\}]=[\{a_n\}]$$

乗法の単位元が $\iota(1)$ **である事**：

$$[\{a_n\}]\cdot\iota(1)=[\{a_n\cdot 1\}]=[\{a_n\}]$$

$[\{a_n\}]$ **の加法に関する逆元が** $[\{-a_n\}]$ **である事**：

$$[\{a_n\}]+[\{-a_n\}]=[\{a_n-a_n\}]=[\{0\}]=\iota(0)$$

$[\{a_n\}]\neq\iota(0)$ **の乗法に関する逆元**:

$$\begin{aligned}[\{a_n\}]=\iota(0)&\Leftrightarrow\{a_n\}\text{は}0\text{に収束する}\\&\Leftrightarrow\forall\varepsilon\in\mathbb{Q}_{>0}\ \exists N\in\mathbb{N}:\forall n\geq N,\ |a_n|<\varepsilon\end{aligned}$$

より

$$[\{a_n\}]\neq\iota(0)\Leftrightarrow\exists\varepsilon_0\in\mathbb{Q}_{>0}:\forall N\in\mathbb{N}\ \exists n\geq N:|a_n|\geq\varepsilon_0$$

が従う。$\{a_n\}\in\mathcal{C}$ であるから $\exists N_0\in\mathbb{N}:\forall m,n\geq N_0,|a_m-a_n|<\varepsilon_0/2$ となる。そこで N_0 に対し $|a_n|\geq\varepsilon_0$ なる $n\geq N_0$ を取ると $m\geq N_0$ なる任意の $m\in\mathbb{N}$ に対し $|a_m|\geq|a_n|-|a_m-a_n|>\varepsilon_0/2$ となる。従って $[\{a\}]\neq\iota(0)$ なら $a_n=0$ なる m は有限個であり特に $Z=\{n\in\mathbb{N};a_n=0\}$ とすれば $\sharp Z<N_0$ である。さて $\{b_n\}$ を

$$b_n=0\ (n\in Z),\ b_n=1/a_n\ (n\notin Z)\quad\text{と置くと}$$

$a_nb_n=0(n\in Z),a_nb_n=1(n\notin Z)$ となるので有限個の n を除き $a_nb_n=1$ で $[\{a_n\}]\cdot[\{b_n\}]=[\{a_nb_n\}]=\iota(1)$ が従う。

$\mathbb{R}$ **に於ける関係** $\leq$ **が代表元の取り方に依らず定まる事**：
$\{a_n\},\{b_n\}$ は条件

$$「\exists\varepsilon\in\mathbb{Q}_{>0},\exists N\in\mathbb{N}:\forall n\geq N,\ b_n-a_n\geq\varepsilon」$$

を満たしているとし $\{a_n\}\sim\{a'_n\},\{b_n\}\sim\{b'_n\}$ であるとすると

$$\begin{aligned}&\exists N_1\in\mathbb{N}:\forall n\geq N_1,|a_n-a'_n|<\varepsilon/3\\&\exists N_2\in\mathbb{N}:\forall n\geq N_2,|b_n-b'_n|<\varepsilon/3\end{aligned}$$

が成立つから $N_0 = \max(N, N_1, N_2)$ と置くと $n \geq N_0$ なる任意の $n \in \mathbb{N}$ に対し

$$\begin{aligned} b'_n - a'_n &= (b_n - a_n) + (b'_n - b_n) - (a'_n - a_n) \\ &\geq b_n - a_n - |b'_n - b_n| - |a'_n - a_n| > \varepsilon/3 \end{aligned}$$

が従い、関係 $<$ は代表元の取り方に依らないので関係 $\leq$ もそうである。

関係 $\leq$ は順序の公理を満たす事：$[\{a_n\}] < [\{a_n\}]$ ではない事は定義より直ちに従う。$[\{a_n\}] < [\{b_n\}]$ かつ $[\{b_n\}] < [\{a_n\}]$ ならば $\exists\varepsilon \in \mathbb{Q}_{>0}\ \exists N \in \mathbb{N} : \forall n \geq N, b_n - a_n > \varepsilon$ 且つ $a_n - b_n > \varepsilon$ となるので矛盾。最後に $[\{a_n\}] < [\{b_n\}], [\{b_n\}] < [\{c_n\}]$ ならば $\exists\varepsilon \in \mathbb{Q}_{>0} \exists N \in \mathbb{N} : \forall n \geq N, b_n - a_n > \varepsilon$ 且つ $c_n - b_n > \varepsilon$ となるので $c_n - a_n > 2\varepsilon$ が従う。これは $[\{a_n\}] < [\{c_n\}]$ を意味する。
以上により関係 $<$ は狭義順序であり $\leq$ は順序となる。

$\mathbb{R}$ は全順序集合を成す事：$\{a_n\}, \{b_n\} \in \mathcal{C}$ に対し $\{a_n\} \sim \{b_n\}$ は $[\{a_n - b_n\}] = \iota(0)$ 及び $[\{a_n\}] = [\{b_n\}]$ と同値である。$\{a_n\} \sim \{b_n\}$ でない事は $[\{a_n - b_n\}] \neq \iota(0)$ と同値であり上の議論より $\varepsilon_0 \in \mathbb{Q}_{>0}$ 及び $N_0 \in \mathbb{N}$ が存在し $m, n \geq N_0$ なる任意の $m, n \in \mathbb{N}$ に対し

$$|a_m - a_n| < \varepsilon/3,\ |b_m - b_n| < \varepsilon/3,\ |a_n - b_n| > \varepsilon$$

である事と同値である。さて $a_{N_0} - b_{N_0} < \varepsilon$ または $a_{N_0} - b_{N_0} < -\varepsilon$ のどちらか一方が成立つ。前者ならば任意の $m \geq N_0$ に対し $a_m - b_m = (a_{N_0} - b_{N_0}) + (a_m - a_{N_0}) + (b_{N_0} - b_m) > (a_{N_0} - b_{N_0}) - |a_m - a_{N_0}| - |b_{N_0} - b_m| > \varepsilon/3$ であり、後者ならば任意の $m \geq N_0$ に対し $a_m - b_m < (a_{N_0} - b_{N_0}) + |a_m - a_{N_0}| + |b_{N_0} - b_m| < -\varepsilon/3$ である。即ち前者ならば $[\{b_n\}] < [\{a_n\}]$ となり後者ならば $[\{a_n\}] < [\{b_n\}]$ となる。

$\mathbb{R}$ は順序体を成す事：$[\{a_n\}] < [\{b_n\}] \Rightarrow [\{a_n\}] + [\{c_n\}] < [\{b_n\}] + [\{c_n\}]$ なる事は

$$\begin{aligned} &\exists\varepsilon \in \mathbb{Q}_{>0}\ \exists N \in \mathbb{N} : \forall n \geq N,\ b_n - a_n > \varepsilon \\ &\Leftrightarrow \exists\varepsilon \in \mathbb{Q}_{>0}\ \exists N \in \mathbb{N} : \forall n \geq N,\ (b_n + c_n) - (a_n + c_n) > \varepsilon \end{aligned}$$

より従う。$[\{a_n\}] < [\{b_n\}], [\{c_n\}] > \iota(0) \Rightarrow [\{a\}] \cdot [\{c_n\}] < [\{b_n\}] \cdot [\{c_n\}]$ なる事は「$\exists\varepsilon_0 \in \mathbb{Q}_{>0}\ \exists N_0 \in \mathbb{N} : \forall n \geq N_0, c_n \geq \varepsilon_0$」及び「$\exists\varepsilon \in \mathbb{Q}_{>0}\ \exists N_1 \in \mathbb{N} : \forall n \geq N_1,\ b_n - a_n > \varepsilon$」なる事により「$n \geq N \equiv \max(N_0, N_1) \Rightarrow b_n c_n - a_n c_n > \varepsilon_0 \varepsilon$ 」が得られるからである。

$\mathbb{R}$ はアルキメデス的である事：$[\{a_n\}] \in \mathbb{R}$ を任意に取る。このとき $\{a_n\}$ は $\mathbb{Q}$ のコーシー列故有界である。従って $M \in \mathbb{Q}_{>0}$ が存在して任意の $N \in \mathbb{N}$ に対し $|a_n| \leq M$ となる。$\mathbb{Q}$ はアルキメデス的なので $N \in \mathbb{N}$ が在って $M < N$ となり $|a_n| < N$ が成立つ。$\varepsilon_0 = (N - M)/2$ とすれば $\varepsilon_0 \in \mathbb{Q}_{>0}$ で $N - a_n \geq N - M > \varepsilon_0$ となるので $[\{a_n\}] < \iota(N)$ が従う。

$\mathbb{R}$ は完備である事：$\{\alpha_k\} \subset \mathbb{R}$ をコーシー列とする。$\alpha_k \in \mathbb{R}$ は $\mathbb{Q}$ のコーシー列 $\{a_n^{(k)}\}$ を代表元として $\alpha_k = [\{a_n^{(k)}\}]$ と表される。任意に $\varepsilon \in \mathbb{R}_{>0}$ を取る。$\varepsilon = [\{\varepsilon_n\}] > \iota(0)$ と見做せば $\delta \in \mathbb{Q}_{>0}$ 及び $N \in \mathbb{N}$ を取って $n \geq N$ なる任意の $n \in \mathbb{N}$ に対し $\varepsilon_n > \delta$ と出来る。これより $\varepsilon > \iota(\delta)$ が従う。さて $\{a_n^{(k)}\}$ は $\mathbb{Q}$ のコーシー列だから $N \in \mathbb{N}$ が在って $m, n \geq N$ なる任意の $m, n \in \mathbb{N}$ に対し $|\{a_n^{(k)}\} - \{a_n^{(k)}\}| \leq \delta/2$ と出来る。$\mathbb{R}$ の元 $\iota(\{a_m^{(k)}\}) - \alpha_k$ は

$\iota(a_m^{(k)})-\alpha_k=[\{a_m^{(k)}-a_n^{(k)}\}_{n\in\mathbb{N}}]$ と表されるから $|\iota(a_m^{(k)})-\alpha_k|=|[\{a_m^{(k)}-a_n^{(k)}\}_{n\in\mathbb{N}}]|<\iota(\delta)<\varepsilon$ が従う。
さて $\mathbb{Q}$ は可算だから全単射 $\sigma:\mathbb{N}\to\mathbb{Q}$ が存在する。任意の $k\in\mathbb{N}$ に対し

$$M_k=\{k\in\mathbb{N};|\iota(\sigma(k))-\alpha_k|<\iota(1/k)\}$$

と置く。$\sigma^{-1}(a_m^{(k)})\in M_k$ 故 M_k は空でない。M_k の最小元を $m_k\in\mathbb{N}$ とする。このとき $\{\sigma(m_k)\}_{k\in\mathbb{N}}$ は $\mathbb{Q}$ のコーシー列である。実際任意の $\eta\in\mathbb{Q}_{>0}$ に対し $N\eta>1$ なる $N\in\mathbb{N}$ を取って $p,q\geq N$ なる任意の $p,q\in\mathbb{N}$ に対し $|\alpha_p-\alpha_q|<\iota(\eta)$ とする事が出来る。故に

$$\begin{aligned}&|\sigma(m_p)-\sigma(m_q)|=|\iota(\sigma(m_p))-\iota(\sigma(m_q))|\\&\leq|\iota(\sigma(m_p))-\alpha_p|+|\alpha_p-\alpha_q|+|\alpha_q-\iota(\sigma(m_q))|\\&\leq\iota(1/p)+\iota(\eta)+\iota(1/q)<3\iota(\eta)=\iota(3\eta)\end{aligned}$$

となるからである。

さて $\alpha=[\{\sigma(m_k)\}_{k\in\mathbb{N}}]$ と置く。$\{\alpha_k\}$ が α に収束する事を示そう。上の議論により任意の $\varepsilon\in\mathbb{R}_{>0}$ に対し $\delta\in\mathbb{Q}_{>0}$ 及び $N\in\mathbb{N}$ が存在して $k\geq N$ なる任意の $k\in\mathbb{N}$ に対し

$$|\iota(\sigma(m_k))-\alpha|<\iota(\delta)<\varepsilon$$

である事が従う。$N'\delta>1$ なる $N'\in\mathbb{N}$ を取り $N''=\max(N,N')$ と置く。
このとき $k\geq N''$ なる任意の $k\in\mathbb{N}$ に対し

$$\begin{aligned}|\alpha_k-\alpha|&\leq|\alpha_k-\iota(\sigma(m_k))|+|\iota(\sigma(m_k))-\alpha|\\&<\iota(1/k)+\iota(\delta)<2\varepsilon\end{aligned}$$

となる。これは $\lim_{k\to\infty}\alpha_k=\alpha$ を意味する。

定理２ (実数体の特徴付け)
実数体は全て同型である。即ち、二つの順序体 K と K' が共に実数の連続性の条件を満たしているとすると全単射 $f:K\to K'$ が存在し演算と順序を保つ。また $|f(k)|=|k|$ が任意の $k\in K$ に対して成立する。

(証明) 有理数体の特徴付けにより演算と順序を保つ単射 $\varphi:\mathbb{Q}\to K$ 及び $\varphi':\mathbb{Q}\to K'$ が存在する。K はアルキメデス的なので $\varphi(\mathbb{Q})$ は K で稠密である。よって任意の $k\in K$ に対し $\mathbb{Q}$ の列 $\{a_n\}$ が存在し $k=\lim_{n\to\infty}\varphi(a_n)$ となる。このとき $\{\varphi'(a_n)\}$ は K' でコーシー列を成す。実際 $m,n\to\infty$ なるとき

$$|\varphi'(a_m)-\varphi'(a_n)|=|\varphi'(a_m-a_n)|=|a_n-a_n|\to0$$

であるからである。K' の完備性により $k'\in K$ が存在し $k'=\lim_{n\to\infty}\varphi'(a_n)$ となる。以上より $K\ni k\mapsto k'\in K'$ が定まるので、この写像を f とする。$k\in\varphi(\mathbb{Q})$ に対しては $f(k)=(\varphi'\circ\varphi^{-1})(k)$ であるから f は $\varphi(\mathbb{Q})$ 上で演算と順序を保ち $|f(k)|=|(\varphi'(\varphi^{-1}(k))|=|\varphi^{-1}(k)|=|k|$ が成立つ。$\varphi(\mathbb{Q})$ は K で稠密であるから f は K 上で演算と順序と絶対値を

保つ。f の単射性は $|f(k)-f(\ell)|=|f(k-\ell)|=|k-\ell|$ より従い、全射性は $\varphi'(\mathbb{Q})$ の K' に於ける稠密性から従う。

7. 複素数

定理１ (複素数体の構成)　実数体 $\mathbb{R}$ の直積集合 $\mathbb{R}^2=\mathbb{R}\times\mathbb{R}$ に加法と乗法を

$$(a,b)+(c,d)=(a+c,b+d)$$
$$(a,b)\cdot(c,d)=(ac-bd,ad+bc)$$

で定める。加法及び乗法の単位元は夫々 $(0,0)$ 及び $(1,0)$ である。(a,b) の加法及び乗法（但し $(a,b)\neq(0,0)$）に関する逆元は夫々 $(-a,-b)$ 及び $(a/(a^2+b^2),-b/(a^2+b^2))$ で与えられる。$\mathbb{R}^2$ は可換体を成す。この可換体を $\mathbb{C}$ と表す。$a\in\mathbb{R}$ に対し $\iota(a)=(a,0)$ と置くと写像 $\iota:\mathbb{R}\to\mathbb{C}$ が定まる。ι は単射であり加法と乗法に関し準同型となる。$(a,b)\in\mathbb{C}$ に対し、その絶対値を

$$|(a,b)|=\sqrt{a^2+b^2}$$

で定めると

$$|(a,b)+(c,d)|\leq|(a,b)|+|(c,d)|$$
$$|(a,b)\cdot(c,d)|=|(a,b)||(c,d)|$$
$$|\iota(a)|=|a|$$

が成立つ。

（証明）　加法の可換則：

$$(a,b)+(c,d)=(a+c,b+d)=(c+a,d+b)=(c,d)+(a,b)$$

加法の結合則：

$$\begin{aligned}((a,b)+(c,d))+(e,f)&=(a+c,b+d)+(e,f)=((a+c)+e,(b+d)+f)\\&=(a+(c+e),b+(d+f))=(a,b)+(c+e,d+f)\\&=(a,b)+((c,d)+(e,f))\end{aligned}$$

乗法の可換則：

$$(a,b)\cdot(c,d)=(ac-bd,ad+bc)=(ca-db,da+cb)=(c,d)\cdot(a,b)$$

乗法の結合則：

$$\begin{aligned}((a,b)+(c,d))\cdot(e,f)&=(ac-bd,ad+bc)\cdot(e,f))\\&=((ac-bd)e-(ad+bc)f,(ac-bd)f+(ad+bc)e)\\&=(a(ce-df)-b(de+cf),a(cf+de)+b(-df+ce))\\&=(a,b)\cdot(ce-df,cf+de)=(a,b)\cdot((c,d)\cdot(e,f))\end{aligned}$$

加法に関する乗法の分配則：

$$\begin{aligned}
&(a,b)\cdot((c,d)+(e,f)) = (a,b)\cdot(c+e,d+f)\\
&= (a(c+e)-b(d+f), a(d+f)+b(c+e))\\
&= ((ac-bd)+(ae-bf),(ad+bc)+(af+be))\\
&= (ac-bd,ad+bc)+(ae-bf,af+be)\\
&= (a,b)\cdot(c,d)+(a,b)\cdot(e,f)
\end{aligned}$$

加法の単位元が $(0,0)$ **である事**：

$$(a,b)+(0,0) = (a+0,b+0) = (a,b)$$

乗法の単位元が $(1,0)$ **である事**：

$$(a,b)\cdot(1,0) = (a1-b0, a0+b1) = (a,b)$$

(a,b) **の加法に関する逆元**：

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

$(a,b)\neq(0,0)$ **の乗法に関する逆元**：

$$\begin{aligned}
&(a,b)\cdot(a/(a^2+b^2), -b/(a^2+b^2))\\
&= (a(a/(a^2+b^2))-b(-b/(a^2+b^2)), a(-b/(a^2+b^2))+b(a/(a^2+b^2)))\\
&= (a^2/(a^2+b^2)+b^2/(a^2+b^2), -ab/(a^2+b^2)+ba/(a^2+b^2))\\
&= ((a^2+b^2)/(a^2+b^2), (-ab+ba)/(a^2+b^2)) = (1,0)
\end{aligned}$$

絶対値に関する性質：

$$\begin{aligned}
&(|(a,b)|+|(c,d)|)^2 - |(a,b)+(c,d)|^2\\
&= |(a,b)|^2 + 2|(a,b)||(c,d)| + |(c,d)|^2 - |(a+c,b+d)|^2\\
&= (a^2+b^2) + 2\sqrt{a^2+b^2}\sqrt{c^2+d^2} + (c^2+d^2) - ((a+c)^2+(b+d)^2)\\
&= 2(\sqrt{a^2+b^2}\sqrt{c^2+d^2} - ac - bd) \geq 0,
\end{aligned}$$

$$\begin{aligned}
|(a,b)\cdot(c,d)|^2 &= |(ac-bd,ad+bc)|^2\\
&= (ac-bd)^2+(ad+bc)^2\\
&= a^2c^2 - 2acbd + b^2d^2 + a^2d^2 + 2adbc + b^2c^2\\
&= (a^2+b^2)(c^2+d^2) = |(a,b)|^2|(c,d)|^2,\\
|\iota(a)|^2 &= |(a,0)|^2 = a^2
\end{aligned}$$

$\iota : \mathbb{R} \to \mathbb{C}$ **に関する性質**：

$$\iota(a+b) = (a+b, 0) = (a, 0) + (b, 0) = \iota(a) + \iota(b)$$
$$\iota(ab) = (ab, 0) = (a, 0) \cdot (b, 0) = \iota(a) \cdot \iota(b)$$

ι の単射性は $\iota(a) = \iota(b) \Leftrightarrow (a, 0) = (b, 0) \Leftrightarrow a = b$ より従う。

定義　複素数体 $\mathbb{C}$ の元 $(0, 1)$ は虚数単位と謂い i で表す。

命題

(1) 任意の複素数 (a, b) は $(a, b) = \iota(a) + \iota(b) \cdot i$ と表される。

(2) $i^2 = i \cdot i = \iota(-1) = (-1, 0)$

(証明)

(1) $(a, b) = (a, 0) + (0, b) = (a, 0) + (b, 0) \cdot (0, 1) = \iota(a) + \iota(b) \cdot i$

(2) $i \cdot i = (0, 1) \cdot (0, 1) = (-1, 0) = \iota(-1)$

註　複素数 (a, b) を通常 z と表し、a を z の実部、b を z の虚部として
$a = \mathrm{Re}z,\ b = \mathrm{Im}z$ と表す。$(a, b) = \iota(a) + \iota(b) \cdot i$ は $z = a + bi, i^2 = (-1, 0)$ は $i^2 = -1$ と表す。

参考文献：

M. R. Dixon, L. A. Kurdachenko and I. Y. Subbotin, Algebra and Number Theory, Wiley 2010
M. E. Taylor, Numbers, www.math.unc.edu / Faculty/met
彌永昌吉，小平邦彦，現代数学概説，岩波書店
齋藤正彦，数学の基礎, 東京大学出版会
梶原壌二，解析学序説，森北出版