数学の基礎 II 講義ノート

安藤哲哉

はじめに

これは，千葉大学理学部数学・情報数理学科向け，1 年生後期の講義「数学の基礎 II」の講義ノートである．講義 13 回＋試験 1 回の授業構成を前提に書かれている．以前の，講義 14 回＋試験 1 回と，講義 15 回＋試験 1 回の構成の古いヴァージョンもあるので，ほしい人は直接安藤まで請求してほしい．

商業目的に利用しない限り (料金を徴収して配布したりしない限り)，誰が利用しても自由である．大学の講義用資料等として (無料) 配布してもよいが，著者名は残すこと．

数学の基礎 I と異なり，数学の基礎 II は非常に盛沢山の内容があり，しかも Zorn の補題など難解な話題が含まれている．内容としては，順序集合，濃度，数の集合の公理的構成，という 3 つの内容からなっていて，講義回数に比べて，ちょっと重いところがある．正直言って，Zorn の証明まできちんと理解することは 1 年生には困難かもしれない．ただ，Zorn の補題は数学のあらゆる場面で登場するので，徐々にその使い方に慣れていく必要がある．それが 1 年生の段階で無理でも，4 年生になるまでには，そうしたい．

有限集合における「元の個数」を無限集合にまで一般化した「濃度」の概念も，扱う主な対象が無限集合なので結構難しい．例えば平面上の点全体の集合 $\mathbb{R}^2$ と直線上の点全体の集合 $\mathbb{R}$ の間に全単射が存在する，というような定理も，それが発見され発表された直後には，多くの数学者がとまどった．直感に反することが濃度では起きるので，理解が難しいかもしれない．有限個の集合の直積だけでなく，無限個の集合の直積のような概念も，直感的に理解しにくいところがると思う．

数の集合の構成では，ペアノの公理よって自然数全体の集合 $\mathbb{N}$ (この講義では $\mathbb{N} \cup \{0\}$) を構成し，そこに和・積・順序を定義することから始めて，負の数を含む整数全体の集合 $\mathbb{Z}$ を構成し，整数の分数として有理数を構成する．そして，有理数のコーシー列の極限として実数を構成する．高校までに習ってきた数の話も，数学的に厳密に扱うと結構難しい．

第 I 部 順序集合

1. 順序集合の定義

しばらく，基本的な概念の定義が続き，定理はしばらく登場しない．まずは，しっかり用語を理解しよう．

定義 1.1.(半順序集合) A は空でない集合とする．直積集合 $A \times A$ から $\{0, 1\}$ への写像 $f\colon A \times A \longrightarrow \{0, 1\}$ が与えられているとき，f を A 上の**関係**という．この関係が，任意の元 $x, y, z \in A$ に対して次の (1), (2), (3) を満たすとする．
(1) $f(x, x) = 1$.
(2) $f(x, y) = 1$ かつ $f(y, x) = 1$ ならば $x = y$.
(3) $f(x, y) = 1$ かつ $f(y, z) = 1$ ならば $f(x, z) = 1$.
$f(x, y) = 1$ の場合に $x \leqq y$ と書くことにし，$\leqq$ は A 上の**半順序**であるという．このような半順序 $\leqq$ を 1 つ定めた集合 A を**半順序集合** (partially orderd set, poset) という．半順序 $\leqq$ を強調して，$(A, \leqq)$ は半順序集合である，と表記することもある．なお，上の (1), (2), (3) は下記のように表記されることが多い．
(1) (反射律) $x \leqq x$.
(2) (反対称律) $x \leqq y$ かつ $y \leqq x$ ならば $x = y$.
(3) (推移律) $x \leqq y$ かつ $y \leqq z$ ならば $x \leqq z$.
$(A, \leqq)$ は半順序集合とし，$x, y \in A$ とする．もし，$x \leqq y$ または $y \leqq x$ の少なくとも一方が成り立つとき，x と y は**比較可能**であるという．比較可能でないとき**比較不可能**であるという．
$x \leqq y$ を $y \geqq x$ とも書く．また，$x \leqq y$ かつ $x \neq y$ のとき $x < y$ と書き，$x \geqq y$ かつ $x \neq y$ のとき $x > y$ と書く．

例 1.2. (1) X は空でない集合とし，X の部分集合全体の集合を A とする．すなわち A は X の巾集合である．A の元 Y, Z に対し $Y \subset Z$ のときに $Y \leqq Z$ として $\leqq$ を定義すると $\leqq$ は定義 1.1 の (1), (2), (3) を満たす．この場合，包含関係 $\subset$ は A 上の半順序である，というような言い方をする．
Y と Z の間に包含関係がなければ，Y と Z は比較不可能である．

(2) 自然数全体の集合 $\mathbb{N}$ において，y が x の倍数 $(x, y \in \mathbb{N})$ のとき $x|y$ と書くことにする．すると，$|$ は $\mathbb{N}$ 上の半順序になる．

定義 1.3.(全順序集合) $(A, \leqq)$ は半順序集合であるとする．任意の $x, y \in A$ に対して，x と y が比較可能であるとき，$\leqq$ は A 上の**全順序**であるといい，$(A, \leqq)$ は**全順序集合** (totally orderd set) であるとか，**線形順序集合** (linearly orded set) であるという．
なお，**順序**とか**順序集合**という用語は，文献によって半順序のほうを指す場合と，全順序のほうを指す場合がある．しかし，中身を読んで意味を考えれば，どちらの意味で使っているかはすぐわかるのが普通である．この講義では「順序」といった場合には「半順序」のほうを表すことにしておく．

例 1.4. 実数全体の集合 $\mathbb{R}$ は通常の大小関係 $\leqq$ について全順序集合である．

問題 1.5. $(A, \leqq)$ は半順序集合であるとする．今，$x, y \in A$ に対し，$y \leqq x$ のとき $x \leqq' y$ として $\leqq'$ を定めると $(A, \leqq')$ も半順序集合であることを確かめよ．$\leqq'$ を $\leqq$ の**逆順序**とか**大小関係を反対にした順序**という．

命題 1.6. 空でない集合 A 上の関係 $<$ は次の (4), (5) を満たすとする．ただし，x, y, z は A の任意の元とする．
(4) (推移律) $x < y$ かつ $y < z$ ならば $x < z$.
(5) $x < y$ かつ $y < x$ となることはない．
このとき，$x, y \in A$ に対し $x < y$ または $x = y$ のとき $x \leqq y$ であるとして関係 $\leqq$ を定めると，$\leqq$ は A 上の半順序である．

証明はほとんど自明なので省略する．誤解の恐れがなければ，上の命題の意味で，$(A, <)$ は半順序集合である，ということもある．また，逆順序の意味で，$(A, \geqq)$ は半順序集合である，とか，$(A, >)$ は半

順序集合である，ということもある．不等号の向きと，等号が含まれるか否かを考えれば，混乱することはないであろう．

定義 1.7. $(A, \leqq)$ は半順序集合で，B は空でない A の部分集合とする．$x, y \in B$ に対し A 上で $x \leqq y$ であるとして B 上に半順序 $\leqq$ を定めるとき，A 上の半順序を B 上に制限して B 上に半順序を定めるという．この半順序について，B も半順序集合になる．このとき，B は A に**部分順序集合**であるという．(部分半順序集合であるという言い回しはあまりしない.)

定義 1.8. $(A, \leqq)$ と $(B, \leqq')$ は半順序集合で，$f\colon A \to B$ は写像とする．任意の $x, y \in A$ に対し，$x \leqq y$ ならば $f(x) \leqq' f(y)$ が成り立つとき，f は**単調**写像である，とか**順序を保つ**写像であるという．

$f\colon A \to B$ が全単射で単調写像であり，かつ逆写像 $f^{-1}\colon B \to A$ も単調写像であるとき，$f\colon A \to B$ は**順序同型**写像であるという．順序同型写像 $f\colon A \to B$ が存在するとき，A と B は**順序同型**であるという．このとき，$A \cong B$ とか $f\colon A \xrightarrow{\cong} B$ と書くことにする．(この記号 $\cong$ は群の同型，環の同型など，いろいろな場面で少し異なった意味で使われるので注意すること.)

定義 1.9.(辞書式順序) $(A, \leqq)$ は全順序集合，n は 2 以上の整数とし，$X = A^n = A \times A \times \cdots \times A$ (n 個) とする．X に次のように定めた順序を**辞書式順序** (lexicographic order) という．

$\mathbf{a} = (a_1, \ldots, a_n), \mathbf{b} = (b_1, \ldots, b_n) \in X$ を取る．ただし，$a_i, b_i \in A$ とする．$I := \{i \in \mathbb{N} \mid a_i \neq b_i\}$ とおく．もし，$I = \phi$ ならば $\mathbf{a} = \mathbf{b}$ である．以下，$I \neq \phi$ の場合を考える．$k := \min I$ (I 内の最小の元) とおく．$1 \leqq k \leqq n$ で $a_k \neq b_k$ である．もし，$a_k < b_k$ ならば $\mathbf{a} < \mathbf{b}$ と定め，$a_k > b_k$ ならば $\mathbf{a} > \mathbf{b}$ と定める．

つまり，辞書のように左端の元から順に大小を比較して定める順序である．

定義 1.10.(次数付き辞書式順序) 多変数多項式の項を次数によって並べるときなどに使われる順序である．$\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ とし，普通の順序で全順序集合と考える．$X := (\mathbb{N}_0)^n$ に以下のように定めた順序を**次数付き辞書式順序**という．

$\mathbf{a} = (a_1, \ldots, a_n) \in X$ に対し，$|\mathbf{a}| = a_1 + a_2 + \cdots + a_n$ と定める．

$\mathbf{a} = (a_1, \ldots, a_n), \mathbf{b} = (b_1, \ldots, b_n) \in X$ を取る．もし，$|\mathbf{a}| > \mathbf{b}|$ ならば $\mathbf{a} > \mathbf{b}$ と定め，$|\mathbf{a}| < |\mathbf{b}|$ ならば $\mathbf{a} < \mathbf{b}$ と定める．$|\mathbf{a}| = |\mathbf{b}|$ の場合には，辞書式順序で $\mathbf{a}$ と $\mathbf{b}$ の大小関係を定める．

問 1.11. $f(x, y) = x^4y^2 + x^3y^4 + x^5$ の項を，辞書式順序と，次数付き辞書式順序で，指数の高い項から順に並べて書け．

2. 最大・最小・極大・極小

定義 2.1. $(A, \leqq)$ は半順序集合とし，$a \in A$ とする．

(1) 任意の $x \in A$ に対し $x \leqq a$ が成り立つとき，a は A の**最大元** (maximum) であるといい，$a = \max A$ と書く．
(2) 任意の $x \in A$ に対し $a \leqq x$ が成り立つとき，a は A の**最小元** (minimum) であるといい，$a = \min A$ と書く．
(3) $x > a$ を満たす $x \in A$ が存在しないとき，a は A の**極大元** (maximal) であるという．
(4) $x < a$ を満たす $x \in A$ が存在しないとき，a は A の**極小元** (minimal) であるという．

一般に最大元，最小元，極大元，極小元は存在するとは限らないし，極大元，極小元は存在しても一意的とは限らない．

また，上の極大・極小は，実関数についての極大・極小 (local maximum, local minimum) とは別の概念である．

命題 2.2. $(A, \leqq)$ は半順序集合とする．

(1) A の最大元は存在すれば一意的 (高々1 個) である．
(2) A の最小元は存在すれば一意的 (高々1 個) である．
(3) a が A の最大元ならば a は A の極大元である．
(4) a が A の最小元ならば a は A の極小元である．

証明. (1) a と b が A の最大元であるとする．a は最大元だから $b \leqq a$ である．b は最大元だから $a \leqq b$ である．よって $a = b$ となる．(2) の証明も同様である．

(3) $a = \max A$, $x \in A$ とする．もし $x > a$ とすると a が最大元であることに矛盾する．よって，a は極大元である．(4) の証明も同様である． □

命題 2.3. $(A, \leqq)$ は半順序集合で，A は有限集合であるとする．すると，A には極大元と極小元が存在する (一意的とは限らない).

証明. 有限集合 A の元の個数を $\#A$ で表すことにし，$\#A$ に関する帰納法で，A に極大元が存在することを証明する．(極小元は逆順序で考えればよい.)

$\#A = 1$ ならば，$A = \{a\}$ として，a は A の最大元であり最小元である．よって，極大元であり極小元である．

$\#A \geqq 2$ の場合を考える．A の元 a を 1 つ選び，$B := A - \{a\}$ (a を取り除いた集合) とする．帰納法の仮定から，B には極大元 b が少なくとも 1 個存在する．

もし，a と b が比較不可能であるか，$a < b$ であれば，b は A の極大元である．$a > b$ の場合は，a が A の極大元である． □

命題 2.4. $(A, \leqq)$ は全順序集合で，a は A の極大元であるとする．すると，a は A の最大元である．(「大」を「小」に書き直した命題も成立する.)

証明. a は全順序集合 A の極大元であるとする．勝手な $x \in A$ を取る．定義から，$x > a$ となることはない．A は全順序集合だから，任意の $x \in A$ に対し $x \leqq a$ となり，a は A の最大元である． □

問 2.5. $a, b \in \mathbb{R}$ で $a < b$ とし，開区間 $A = (a, b)$ を考える．普通の順序について，A は全順序集合である．さて，A に最大元は存在しないことを示せ.

定義 2.6. $(A, \leqq)$ は半順序集合で，$a, b \in A$ で $a < b$ とする．もし，$a < x < b$ を満たす $x \in A$ が存在しないならば，b は a の**直後**の元であるといい，a は b の**直前**の元であるという.

命題 2.7. $(A, \leqq)$ は半順序集合で，A は有限集合であるとする．もし，$a \in A$ で，a が極大元でないならば，a には直後の元が存在する．また，a が極小でないならば，a には直前の元が存在する.

証明. a が極大元でないとする．$B := \{x \in A \mid a < x\}$ とする．a は極大元でないから，$B \neq \phi$ である．すると，B の極小元が a の直後の元である． □

問題 2.8. 平面上 π に有限個の相異なる点の集合 $A = \{P_1, \ldots, P_n\}$ が与えられていて，そのうちの何組かの 2 点は辺 (線分) で結ばれているとする．このような図形は**グラフ**と呼ばれる (ただし，もっと一般化されたグラフの概念もある)．平面 π 上では垂直に立てた紙面のように，上下の位置関係が定まっているとし，2 点を結ぶ辺の中に水平なものはないと仮定する．このグラフ上の相異なる 2 点 P, Q に対し，P と Q が辺で結ばれていて P が Q より下にあるとき $P \prec Q$ とか $Q \succ P$ と書くことにする．さらに，$P = Q$ であるか，ある 2 以上の自然数 n と点列 $P = P_1, P_2, \ldots, P_n = Q$ で各 $i = 1, 2, \ldots, n-1$ に対し $P_i \prec P_{i+1}$ が成り立つとき，$P \leqq Q$ であると定める，すると，この $\leqq$ は A 上の半順序であることを確かめよ.

命題 2.9. 今 $(A, \leqq)$ は半順序集合で，A は有限集合であるとする．すると，$(A, \leqq)$ と順序同型であるような問題 2.8 で述べたようなグラフが存在するこのような図形 (グラフ) を $(A, \leqq)$ の **Hass 図式** (ハッセ) という.

証明. $\#A$ に関する帰納法で証明する．$\#A = 1$ ならば，1 点のみからなるグラフが Hass 図式である．

$\#A \geqq 2$ の場合を考える．命題 2.3 より，A には極大元 a が存在する．$B = A - \{a\}$ とおくと，B と順序同型な Hass 図式 G_B が存在する．今，G_B のどの点より上に点 P_a を描く．A における a の直前の元全体を $b_1, \ldots, b_r$ とする．G_B において，各 b_i に対応する点と P_a を結んでできるグラフを G_A とする．G_A が A の Hass 図式である． □

定義 2.10.(上限・下限) $(X, \leqq)$ は半順序集合で，$A \subset X$ とする．A を X の部分順序集合と考える．

$$H := \{x \in X \mid \text{任意の } a \in A \text{ に対し } x \geqq a\}$$
$$L := \{x \in X \mid \text{任意の } a \in A \text{ に対し } x \leqq a\}$$

とおく．H の元，または H 自身を，X における A の**上界**という．また，L の元，または L 自身を，X における A の**下界**という．もし，$H \neq \phi$ ならば，A は X において**上に有界**であるという．$L \neq \phi$ ならば，A は X において**下に有界**であるという．A が上にも下にも有界であるとき，A は**有界** (bounded) であるという．

もし，$H \neq \phi$ で H に最小元 $\min H$ が存在するとき，$\sup A = \min H$ で $\sup A$ を定め，$\sup A$ を A の**上限** (supremum) という．$\sup A$ は X に依存するので，$\sup_X A$ と書くこともある．同様に，$\inf A = \max L$ を A の**下限** (infimum) という．$\inf A$ は $\inf_X A$ とも書く．

例 2.11. $X = \mathbb{R}$ とし開区間 $A = (a, b)$ (ただし $a, b \in \mathbb{R}$ で $a < b$) を考える．$\sup A = b$, $\inf A = a$ であるが，A に最大元，最小元は存在しない．

命題 2.12. $(X, \leqq)$ は半順序集合で，$A \subset X$ とする．もし，A に最大元が存在すれば $\sup A = \max A$ である．また，A に最小元が存在すれば $\inf A = \min A$ である．

証明. $m = \max A$ が存在すると仮定する．定義 2.10 の記号で，$m \in H$ なので $H \neq \phi$ である．勝手な $x \in H$ を取る．H の定義から $x \geqq m$ である．したがって，$m = \min H$ である．よって，$m = \sup A$ である．最小についても同様． □

問題 2.13. $X = \mathbb{Q}$, $A = \{x \in \mathbb{Q} \mid x^2 \leqq 2\}$ とおく．A は X で有界であるが，$\sup A$ も $\inf A$ も存在しないことを示せ．

問題 2.14. $(A, \leqq)$ は全順序集合とし，$a \in A$ とする．もし，a の直後の元が存在すれば，それは一意的 (ただ 1 つ) であることを証明せよ．(直前の元についても同様)

ここからは，順序集合の話ではなく，集合の一般論で，直和集合・直積集合の定義の話です．

定義 2.15.(合併集合と直和集合) 今，全体集合 Ω があるとする．それとは別に集合 Λ があり，各元 $\lambda \in \Lambda$ に対し，Ω の部分集合 A_λ が与えられているとする．A_λ 達の**合併集合** A は，

$$A = \bigcup_{\lambda \in \Lambda} A_\lambda := \{x \in \Omega \mid \text{ある } \lambda \in \Lambda \text{ に対して } x \in A_\lambda\}$$

として定義される．また，

$$B = \bigsqcup_{\lambda \in \Lambda} A_\lambda := \{(x, \lambda) \in A \times \Lambda \mid x \in A_\lambda \subset A\}$$

として，A_λ 達の**直和**集合 (disjoint union) を定義する．そして，$x \in A_\lambda$ と $(x, \lambda) \in B$ を同一視して，$A_\lambda \subset B$ と考える．このとき，B 内では $\lambda \neq \mu$ ならば，$A_\lambda \cap A_\mu = \phi$ が成り立つ．また，$A_\lambda \subset B$ と考えたとき，$B = \bigcup_{\lambda \in \Lambda} A_\lambda$ が成り立つ．

$\Lambda = \{1, 2, \ldots, n\}$ のときは，この直和集合 B を

$$A_1 \sqcup A_2 \sqcup \cdots \sqcup A_n$$

などとも書く．

Λ が非常に大きな無限集合で，A_λ 達がある全体集合の部分集合でない場合，直和集合 $B = \bigsqcup_{\lambda \in \Lambda} A_\lambda$ が存在することは証明できない．公理的集合論では，その存在を公理として仮定する．

公理 2.16.(直和集合の公理) Λ は集合で，各元 $\lambda \in \Lambda$ に対し集合 A_λ が与えられているとする．すると，次の条件 (1), (2), (3) を満たす集合 B が存在する．

(1) 任意の $\lambda \in \Lambda$ に対し $A_\lambda \subset B$.

(2) $B = \bigcup_{\lambda\in\Lambda} A_\lambda$.

(3) $\lambda, \mu \in \Lambda$, $\lambda \neq \mu$ ならば $A_\lambda \cap A_\mu = \phi$.

この B を $\bigsqcup_{\lambda\in\Lambda} A_\lambda$ と書き，A_λ $(\lambda \in \Lambda)$ の**直和集合**という．$B = \bigcup_{\lambda\in\Lambda} A_\lambda$ (直和) と表すこともある．

無限個の集合の直積集合は，直和集合を用いて定義される．

定義 2.17.(直積集合) Λ は集合で，各元 $\lambda \in \Lambda$ に対し集合 A_λ が与えられているとする．$B := \bigsqcup_{\lambda\in\Lambda} A_\lambda$ とおく．また，Λ から B への写像全体の集合を $\mathrm{Map}(\Lambda, B)$ と各ことにする．A_λ $(\lambda \in \Lambda)$ の**直積集合**を，

$$\prod_{\lambda\in\Lambda} A_\lambda := \left\{ f \in \mathrm{Map}(\Lambda, B) \;\middle|\; \text{任意の } \lambda \in \Lambda \text{ に対して } f(\lambda) \in A_\lambda \right\}$$

によって定義する．このとき，$f \in \prod_{\lambda\in\Lambda} A_\lambda$ に対し，$a_\lambda := f(\lambda) \in A_\lambda$ とおき，f を $(a_\lambda)_{\lambda\in\Lambda}$ とか，$(a_\lambda \,|\lambda \in \Lambda)$ とか，単に，(a_λ) などと書いて表すことが多い．

★ 補足説明

本来は「数学の基礎 I」で説明しておいてほしい内容であるが，ラッセルのパラドックスの話と，集合の定義の考え方を補足しておく．

ラッセルのパラドックス. すべての集合の集まりを X とする．もし，X が集合であるとすると，以下のような不都合が生じる．

今，X が集合であるとしよう．X はすべての集合の集合で，X も集合なので $X \in X$ (X は集合 X の元 (要素) である．$X \in X$ という奇妙な現象が間違いの始まりなのであるが，その話を見ていこう．いま，

$$Y := \left\{ A \in X \;\middle|\; A \in A \right\}$$
$$Z := \left\{ A \in X \;\middle|\; A \notin A \right\}$$

とおく．後で説明する分出公理から，Y と Z は X の部分集合である．また，集合 A は $A \in A$ か $A \notin A$ のいずれか一方のみを満たすので，$Y \cup Z = X, Y \cap Z = \phi$ である．ここで，ϕ は空集合 (後で説明する) である．$X \in X$ なので $X \in Y$ であり，$Y \neq \phi$ である．$Z \in X = Y \cup Z$ なので $Z \in Y$ または $Z \in Z$ のいずれか一方のみが起きる．

もし $Z \in Y$ ならば $Y \cap Z = \phi$ より $Z \notin Z$ である．すると Z の定義から $Z \in Z$ となって矛盾する．

もし $Z \in Z$ ならば Y の定義から $Z \in Y$ であり，$Z \notin Z$ となって矛盾する． □

このラッセルのパラドックスからわかるように，すべての集合の集まり X を集合として扱ってはいけないのである．つまり，すべての集合の集まりは集合ではない．

集合の定義をごまかして述べる場合には「ある明確な数学的思考対象の集まりを**集合**という」とか書くのであるが，本当は，これは全然集合の定義になっていない．

実際には，すべての集合の集まりが集合にならないように，集合の範囲を少し制限する必要がある．特に，無限集合については，それを構成する方法を限定して，すべての集合の集まりのようなものが集合に入ってこないようにしないといけない．

もう 1 つ注意するのは $x \in A$ という記号 $\in$ は A が集合でない場合に利用するのは危険であるということである．また，もし $A \in A$ が起きるとラッセルのパラドックスのような矛盾が発生するので，A が集合の場合は $A \notin A$ でないといけない．

★ 集合の定義の概略

この話は対面授業では話していないが，ついでなので書いておく．興味がなければ読まなくてよい．

BG-ZFC 公理系と呼ばれる集合の定義の大体の雰囲気を日本語で紹介しておく．まず，2 つの集合 A, B が等しい，ということを定義するための公理からスタートする．公理 1 の中で「集合」と書かれたものは，それ以降の公理で集合であると認定されたものである．なお，$x \in A$ という記号はアプリオリに存在するものとし，その否定命題が $x \notin A$ であるとする．

公理 1.(外延性公理) A, B が集合で「$x \in A \Longrightarrow x \in B$」が成り立つとき，$A \subset B$ とか $B \supset A$ と書き，A は B の**部分集合**であるという．A, B が集合で $A \subset B$ かつ $B \subset A$ ならば $A = B$ である．

上の外延性公理からわかるように，集合 A, B について $A = B$ が成り立つことを証明するには，$A \subset B$ と $B \subset A$ を証明することが基本になる．言い換えると,「$x \in A$ ならば $x \in B$」という命題と,「$x \in B$ ならば $x \in A$」という命題の 2 つを証明するのである．1 年生はこの原則を無視して，等式の変形だけで集合の等式を証明しようとする人が多いので，なかなか集合の等式が証明できない．

ここから先の公理は，空集合や有限集合から始めて，いろいろな集合を構成するための公理である．直和集合の公理は少し難しいと思うが，後の章で改めて説明する．

公理 2.(空集合の公理) 1 つも元を持たない空集合 ϕ が存在する．言い換えると，要素を持たない ϕ は集合である．なお，外延性公理の中の $\subset$ の定義により，任意の集合 A に対して $\phi \subset A$ が成り立つ．

公理 3(対の公理) 任意の a, b に対し $\{a, b\}$ は集合である．$a = b$ の場合は $\{a, b\} = \{a\}$ である．

公理 4.(直和集合の公理) X が集合で，X の各元 $x \in X$ に対して集合 A_x が与えられているとする．すると，以下の (1), (2), (3) を満たす集合 B がただ 1 つ存在する．
(1) 任意の $x \in X$ に対して $A_x \subset B$ である．
(2) $x, y \in X, x \neq y$ ならば B を全体集合として $A_x \cap A_y = \phi$ である．
(3) 任意の $b \in B$ に対し，ある $x \in X$ が存在して $b \in A_x$ となる．

この集合 B を $B = \displaystyle\bigsqcup_{x \in X} A_x$ と書き，$\{A_x \mid x \in X\}$ の**直和集合**という．なお，$X = \{1, 2, \ldots, n\}$ のときは，$B = A_1 \sqcup A_2 \sqcup \cdots \sqcup A_n$ とか $B = \displaystyle\bigsqcup_{x=1}^{n} A_x$ とも書く．

なお，直積集合のほうは，上に書いたように，直和集合から構成することができる．

公理 5.(無限公理) 次の条件 (1), (2) を満たす集合 A が存在する．
(1) $\phi \in A$.
(2) $x \in A$ ならば $x \cup \{x\} \in A$.

公理 3 から 1 個の元からなる集合 $\{a\}$ も，2 個の元からなる集合 $\{a, b\}$ も存在する．公理 4 を合わせると 3 個の元からなる集合 $\{a, b, c\}$ も存在することがわかり，1 個の元を付け加えることを繰り返すと $\{a_1, a_2, \ldots, a_n\}$ という n 個の元からなる集合が存在することがわかる．無限公理も分かりにくいとおもうが，ϕ を 0 と考え，$x \in A$ のとき $x \cup \{x\}$ を $x + 1$ と考える ($x + 1$ の定義だと考える) ことにすれば，A は 0 以上の整数をすべて含む集合である．無限集合 A が存在することを主張している公理であって，自然数全体の集合 $\mathbb{N}$ が存在することを保証する公理である．

公理 6.(巾集合の公理) A が集合のとき，A のすべての部分集合の集まり $\mathcal{P}(A)$ は集合である．なお，空集合 ϕ と A 自身も $\mathcal{P}(A)$ の元である．$\mathcal{P}(A)$ を A の巾集合 (べきしゅうごう) と言う．

$\mathcal{P}(\mathbb{N})$ が集合であることから，実数全体の集まり $\mathbb{R}$ も集合であることが導かれるが，この話も後日説明する．

公理 7.(分出公理) A が集合で $P(x)$ が $x \in A$ に対する命題のとき，

$$\{x \in A \mid P(x) \text{ は真}\} \qquad ①$$

は集合である．ここで，①は，集合 A の要素 x の中で，命題 $P(x)$ を満たすもの全体の集まりを表す記号である．

逆に，集合 A の任意の部分集合 B は上の①の形に表すことができる．実際，命題 $P(x)$ として「$x \in B$」という命題を採用すればよい．現在では「分出公理」を拡張した「置換公理」で置き換えた公理系が採用されているが，普通の代数・幾何・解析の議論をするのには分出公理で十分で，置換公理が使われることは基本的にない (私は使ったことがない)．確率論で特殊なボレル集合を構成するときには利用されるらしい．置換公理は非常に分かりにくい公理なので，分出公理のほうを説明しておいた．次の 2 つの公理の意味は理解しにくいと思う．選択公理は第 4 回の講義で登場する．

公理 8.(正則性公理. 基礎の公理) A が空集合でない集合のとき，ある $y \in A$ で，どんな $x \in A$ に対しても $x \in y$ とはならないものが存在する．

公理 9.(選択公理) X が集合で，X の各元 $x \in X$ に対して集合 A_x が与えられているとする．このとき，写像 (関数) $f\colon X \longrightarrow \bigsqcup_{x \in X} A_x$ で，任意の $y \in X$ に対して $f(y) \in A_y$ を満たすものが存在する．この f を**選択関数**という．言い換えると，すべての A_x から同時に 1 個づつの元 $a_x \in A_x$ を選ぶことができる．

正則性公理は A が集合のとき $A \in A$ が起きないことを保証している．最後の選択公理は深淵な公理で，Zorn の補題のところでまた説明する．

上の BG-ZFC 公理による集合の定義はよく理解できなくてもよいが，与えられた何個か (無限個でもよい) の集合の直和集合とか，後で説明する直積集合をとったり，巾集合をとることにより，より大きな集合を構成することができ，分出公理により構成された集合の部分集合を作ることも可能なのである．そういう積み上げ式の構成によらずに，例えば「すべての群の集まり」とか「すべての位相空間の集まり」のように,「ある一定の性質を満たすものすべての集まり」は集合になるかどうかわからない．実際,「すべての群の集まり」や「すべての位相空間の集まり」も集合にならないことが知られている．

$$\{x \mid P(x) \text{ は真}\}$$

が集合になることは保証されていないが，X が集合のとき

$$\{x \in X \mid P(x) \text{ は真}\}$$

は集合になる，という事実は大切なので覚えておいてほしい．

3. 整列集合

定義 3.1. $(A, \leqq)$ が全順序集合で，A の任意の空でない部分集合 B に対し $\min B$ が存在するとき，A は**整列集合** (well orderd set) であるという．

命題 3.2. $\mathbb{N}$ は整列集合である．

証明. $\phi \neq B \subset \mathbb{N}$ を取る．勝手な元 $b \in B$ を 1 つ取り，固定する．b に関する帰納法で $\min B$ が存在することを証明する．

$b = 1$ ならばこれが $\min B$ である．

$b \geqq 2$ と仮定する．もし，任意の $x \in B$ に対し $b \leqq x$ が成り立てば，$\min B = b$ である．そこで，$x < b$ を満たす $x \in B$ が存在すると仮定する．すると，帰納法の仮定により $\min B$ が存在する． □

問題 3.3. A が整列集合ならば，辞書式順序を定めた A^n も整列集合であることを証明せよ．

命題 3.4. A は整列集合で，$a \in A$ とする．このとき，以下が成り立つ．
(1) a が A の最大元でなければ，a の直後の元が存在する．
(2) B が A の空でない部分集合ならば，B も整列集合である．

証明. (1) a が A の最大元でなければ，$\{x \in A \mid x > a\}$ は空集合でなく，その最小元が a の直後の元である．

(2) は自明． □

なお，a が A の最小元でなくても，a の直前の元が存在するとは限らない．例えば $\mathbb{N}^2$ は辞書式順序で整列集合であるが，$(2, 1)$ の直前の元は存在しない．任意の $n \in \mathbb{N}$ に対して $(1, n) < (2, 1)$ であるが，$(1, n)$ という形の元全体の集合に中に最大限は存在しない．

一般に，集合 X, Y が全体集合 Ω の部分集合のとき，

$$X - Y := \{x \in X \mid x \notin Y\}$$

として，X から Y を除いた**差集合** $X - Y$ を定義する．

定理 3.5.(超限帰納法) A は整列集合で，$a \in A$ を変数とする命題 $P(a)$ があるとする．今，$P(a)$ が以下の (1), (2) を満たせば，任意の $a \in A$ に対して命題 $P(a)$ は真である．

(1) A の最小元 a_0 に対して $P(a_0)$ は真である．
(2) 任意の $a \in A$ をとるとき，$x < a$ を満たすすべての $x \in A$ に対して $P(x)$ が真ならば，$P(a)$ も真である．

証明. $B := \{x \in A \mid P(x) \text{ は真}\}$ とおく．$a_0 \in B$ なので $B \neq \phi$ である．$B \neq A$ と仮定して矛盾を導く．差集合 $A - B$ が空でないから $a_1 := \min(A - B)$ が存在する．仮定から $P(a_1)$ は偽である．$x \in A$, $x < a_1$ ならば $x \notin B$ だから，$P(x)$ は真である．条件 (2) から $P(a_1)$ は真となり矛盾する． □

補題 3.6. A が整列集合で，$f\colon A \to A$ が狭義単調増加単調写像 (つまり $x, y \in A$, $x < y$ ならば $f(x) < f(y)$) ならば，任意の $x \in A$ に対して $f(x) \geqq x$ が成り立つ．

証明. 結論を否定すると，$B := \{x \in A \mid f(x) < x\} \neq \phi$ となる．$b := \min B$ とおく．$b \in B$ だから $f(b) < b$ である．f は狭義単調増加だから $f(f(b)) < f(b)$ である．他方，$f(b) \notin B$ だから $f(f(b)) \geqq f(b)$ となり矛盾する． □

定理 3.7. A, B は整列集合で，$f\colon A \to B$ と $g\colon A \to B$ はともに順序同型写像であるとする．すると，$f = g$ である．

証明. $h := g^{-1} \circ f\colon A \to A$ も順序同型写像である．h は単調写像なので前補題より，$h(x) \geqq x$ $(\forall x \in A)$ が成り立つ．h^{-1} も単調写像なので，$h^{-1}(x) \geqq x$ $(\forall x \in A)$ である．h は単調だから $x = h(h^{-1}(x)) \geqq h(x)$ となり，$h(x) = x$ $(\forall x \in A)$ が得られる．
同様に，$f \circ g^{-1}\colon B \to B$ も恒等写像なので $f = g$ である． □

定義 3.8. 定まった記号はないが，A が整列集合で $a \in A$ のとき，

$$A_{<a} := \{x \in A \mid x < a\}$$

と書くことにする．$A_{<a}$ を a による A の**切片**ともいう．

補題 3.9. A は整列集合とし，$a, b \in A$ で $a \neq b$ とする．すると，A, $A_{<a}$, $A_{<b}$ はどの 2 つも順序同型ではない．

証明. (1) 順序同型写像 $f\colon A \to A_{<a}$ が存在したと仮定して矛盾を導く．$\iota\colon A_{<a} \xrightarrow{\subset} A$ を包含写像 (つまり $\iota(x) = x$) とし，$g := \iota \circ f : A \to A$ とする．g は単調写像だから，$g(a) \geqq a$ が成り立つ．つまり，$f(a) \geqq a$ で，$f(a) \notin A_{<a}$ となって矛盾する．
(2) $a < b$ と仮定しても一般性を失わない．順序同型写像 $f\colon A_{<b} \to A_{<a}$ が存在したと仮定する．$C := A_{<a}$, $c := f(b) \in C$ とすると，(1) より C と $C_{<c}$ は順序同型ではない．他方，$C_{<c}$ と $A_{<b}$ は順序同型だらか，$C = A_{<a}$ と $A_{<b}$ は順序同型でない． □

定理 3.10. A, B は整列集合とする．すると，以下の (1), (2), (3) のいずれか 1 つだけが成り立つ．
(1) $A \cong B$ (順序同型).
(2) ある $a \in A$ が存在して，$A_{<a} \cong B$.
(3) ある $b \in B$ が存在して，$A \cong B_{<b}$.

証明. (1), (2), (3) のうちの 2 つが同時に成り立つことがないことは，前の補題からすぐわかる．以下，(1), (2), (3) のいずれかが成り立つことを証明する．

$$\Gamma := \{(x, y) \in A \times B \mid A_{<x} \cong B_{<y}\}$$

とおく．$a_0 := \min A$, $b_0 := \min B$ とすれば $(a_0, b_0) \in \Gamma$ なので，$\Gamma \neq \phi$ である．$p_A\colon A \times B \longrightarrow A$, $p_B\colon A \times B \longrightarrow B$ を正射影として，$A_1 := p_A(\Gamma)$, $B_1 := p_B(\Gamma)$ とおく．$x \in A_1$ のとき，$A_{<x} \cong B_{<y}$ を満たす y は前補題より一意的だから，$x \in A_1$ に $A_{<x} \cong B_{<y}$ を満たす $y \in B_1$ を対応させることにより，写像 $g\colon A_1 \to B_1$ が定まる．$x \leqq x'$ $(x, x' \in A)$ ならば $A_{<x} \subset A_{<x'}$ である．$y = g(x)$, $y' = g(x')$ とおくと，$B_{<y} \subset B_{<y'}$ である．よって，$y \leqq y'$ であり，g が単調写像であることがわかる．$y \in B_1$ に $A_{<x} \cong B_{<y}$ を満たす $x \in A_1$ を対応する写像も存在するが，これは g^{-1} なので，$g\colon A_1 \to B_1$ は順序同型写像である．

今，$x \in A_1, x' \in A$ で $x' < x$ と仮定する．$y := g(x), y' := g(x')$ とおく．$g\colon A_{<x} \xrightarrow{\cong} B_{<y}$ を $(A_{<x})_{<x'}$ に制限すれば，順序同型写像 $(A_{<x})_{<x'} \xrightarrow{\cong} (B_{<y})_{<y'}$ が得られる．$(A_{<x})_{<x'} = A_{<x'}, (B_{<y})_{<y'} = B_{<y'}$ だから，$(x', y') \in \Gamma$ で，$x' \in A_1, y' \in B_1$ となる．よって，$x \in A_1$ ならば $A_{<x} \subset A_1$ である．同様に，$y \in B_1$ ならば $B_{<y} \subset B_1$ である．

もし，$A_1 = A$ かつ $B_1 = B$ ならば，(1) が成り立つ．そこで，$A_1 \neq A$ または $B_1 \neq B$ の場合を考察する．議論は対称だから，$A_1 \neq A$ と仮定しても一般性と失わない．

$a := \min(A - A_1)$ とおく．a の定義から $A_{<a} \subset A_1$ である．$x \in A_1$ かつ $x \geqq a$ であると仮定すると，$a \in A_{<x} \subset A_1$ となって矛盾するから，$x \in A_1$ ならば $x < a$ であり，$A_1 \subset A_{<a}$ となる．よって，$A_{<a} = A_1$ である．

ここで，もし $B_1 = B$ であれば，$A_{<a} \cong B$ となり，(2) が成り立つ．そこで，$B_1 \neq B$ の場合を考える．$b := \min(B - B_1)$ とおけば，上の議論と同様に，$B_{<b} = B_1$ となる．すると，$A_{<a} = A_1 \cong B_1 = B_{<b}$ だから $(a, b) \in \Gamma$ である．よって，$a = p_A(a, b) \in A_1$ であるが，これは $a = \min(A - A_1)$ と矛盾する．よって，$B_1 \neq B$ はありえない． □

補題 3.11. X, Λ は集合で，各 $\lambda \in \Lambda$ に対し X の空でない部分集合 A_λ が与えられていて，ある順序 $\leqq_\lambda$ に対し，$(A_\lambda, \leqq_\lambda)$ は整列集合になっていると仮定する．さらに，任意の $\lambda \neq \mu \in \Lambda$ に対し，
(a) ある $z \in A_\lambda$ が存在して $A_\mu = \left\{x \in A_\lambda \;\middle|\; x \leqq_\lambda z, x \neq z\right\}$, または，
(b) ある $z \in A_\mu$ が存在して $A_\lambda = \left\{x \in A_\mu \;\middle|\; x \leqq_\mu z, x \neq z\right\}$
のいずれかが成立すると仮定する．$B := \bigcup_{\lambda \in \Lambda} A_\lambda \subset X$ とおく．すると，任意の $x, y \in B$ に対し，$x, y \in A_\lambda$ を満たす $\lambda \in \Lambda$ が存在する．そこで，A_λ での x と y の大小関係によって B における x と y の大小関係を定義すると，これは $x, y \in A_\lambda$ を満たす λ の取り方に依存せずに矛盾なく定義できる．そして，B はこの順序について整列集合になる．また，各 A_λ は B の切片となるか $A_\lambda = B$ のいずれかである．

証明. (1) 勝手な $x, y \in B$ を取る．$x \in A_\lambda, y \in A_\mu$ を満たす $\lambda, \mu \in \Lambda$ が存在する．必要なら x と y を交換し，定理 3.10 より A_μ は A_λ の切片と同型であると仮定してよい．この場合 (b) は成立しないから，(a) が成り立つ．よって，$x, y \in A_\lambda$ である．定理 3.7 より，A_μ は A_λ の部分順序集合になる．よって，$x, y \in A_\mu$ であるとすると，$x \leqq_\lambda y$ と $x \leqq_\mu y$ は同値であるので，矛盾なく B において $x \leqq y$ が定義できる．B におけるこの $\leqq$ が順序の公理を満たし，全順序になることはすぐわかる．

(2) $x \in A_\lambda, y \in B$ で $y \leqq x$ ならば $y \in A_\lambda$ であることを証明する．

$y \notin A_\lambda$ と仮定してみる．$y \in A_\mu$ を満たす $\mu \in \Lambda$ が存在する．$A_\mu \not\subset A_\lambda$ だから，(b) が成り立つ．$x \in A_\mu$ だから $y \in (A_\mu)_{<z} = A_\lambda$ となり矛盾する．

(3) B が整列集合になることを証明する．

勝手な $\phi \neq C \subset B$ を取る．$\min C$ の存在を示せばよい．$C \cap A_\lambda \neq \phi$ となる $\lambda \in \Lambda$ が存在する．A_λ は整列集合だから，A_λ における $C \cap A_\lambda$ の最小元 c が存在する．今，$x < c$ を満たす $x \in C$ が存在すると仮定してみる．(2) より $x \in A_\lambda$ となり，$x < c = \min(C \cap A_\lambda)$ で矛盾する．よって，$c = \min C$ である．

(4) A_λ は B の切片であるか $A_\lambda = B$ のいずれかであることを証明する．

$A_\lambda \subset A_\mu$ のとき $\lambda \leqq \mu$ として Λ に順序を定めると，(a) または (b) が成立するから，Λ は全順序集合になる．

$A_\lambda \neq B$ と仮定する．$x \in B - A_\lambda$ を取ると，$x \in A_\mu$ を満たす $\mu \in \Lambda$ が存在し，$A_\lambda \subsetneqq A_\mu$ となる．よって，ある $z \in A_\mu$ が存在して，$A_\lambda = (A_\mu)_{<z}$ となる．$(A_\mu)_{<z} = B_{<z}$ だから，$A_\lambda = B_{<z}$ である． □

補題 3.12. $(A, \leqq)$ は半順序集合で，A の任意の空でない整列部分集合 B に対し $\sup_A B \in A$ が存在すると仮定する．また，$\varphi\colon A \to A$ は，任意の $a \in A$ に対して $\varphi(a) \geqq a$ を満たすと仮定する．すると，$\varphi(a) = a$ を満たす $a \in A$ が存在する．

証明. (I) $x_0 \in A$ を 1 つ固定する．X を以下の (1), (2), (3) を満たす A の部分順序集合 B 全体の集合とする．
(1) B は整列集合で $\min B = x_0$.
(2) $y \in B$ が B の中で直前の元 x を持つならば $y = \varphi(x)$.

(3) $y \in B$ が B の中で直前の元を持たない場合は，$\sup_A B_{<x} = x$ が成り立つ．
$\{x_0\} \in X$ なので，$X \neq \phi$ である．

(II) $B, C \in X$ を取る．定理 3.10 より，$B \cong C$, $B \cong C_{<c}$ $(\exists c \in C)$, $C \cong B_{<b}$ $(\exists b \in B)$ のいずれか 1 つが成立する．それぞれの場合，$B = C$, $B = C_{<c}$, $C = B_{<b}$ となることを証明する．
$f\colon B \xrightarrow{\cong} C_{<c}$ $(\exists c \in C)$ の場合を考える．$f(x) = x$ $(\forall x \in B)$ を超限帰納法で証明する．
$\min B = \min C_{<c} = x_0$ なので，$f(x_0) = x_0$ である．$x > x_0$ とし，任意の $y \in B_{<x}$ に対し $f(y) = y$ が成り立つと仮定する．
もし x が B 内に直前の元 y_1 を持てば，$f(x)$ の $C_{<c}$ 内での直前の元は $f(y_1) = y_1$ である．(2) より $x = \varphi(y_1) = \varphi(f(y_1)) = f(x)$ となる．
また，x が B 内に直前の元を持たない場合は，(3) より $\sup_A B_{<x} = x$ が成り立つ．$f(x)$ は C 内に直前の元を持たないから，(3) より，$\sup_A C_{<f(x)} = f(x)$ が成り立つ．
$B_{<x} = C_{<f(x)}$ であることを証明しよう．$y \in B_{<x}$ ならば $y = f(y) < f(x)$ となる．よって，$B_{<x} \subset C_{<f(x)}$ である．逆に，勝手な $z \in C_{<f(x)}$ を取る．$z = f(y)$ となる $y \in B$ が存在する．$f(y) = z < f(x)$ だから $y < x$ で，$z = f(y) = y \in B_{<x}$ である．よって，$B_{<x} = C_{<f(x)}$ である．よって，$f(x) = \sup_A C_{<f(x)} = \sup_A B_{<x} = x$ である．
$B \cong C$ ならば $B = C$ も同様に証明できる．
また，(II) より，X は包含関係を順序として，全順序集合になる．

(III) $A_1 := \bigcup_{B \in X} B$ とおく．補題 3.11 より A_1 は整列集合になる．また，$\min A_1 = x_0$ で，A_1 も B の条件 (2), (3) を満たす．よって，$A_1 \in X$ である．A_1 の定義から，$A_1 = \max X$ である．
A の仮定から $a := \sup_A A_1 \in A$ が存在する．もし $a \notin A_1$ ならば $A_1 \cup \{a\} \in X$ となり，$A_1 = \max X$ と矛盾するから，$a \in A_1$ である．

(IV) $\varphi(a) = a$ を証明する．
もし，$\varphi(a) \neq a$ ならば，$\varphi(a) > a$ である．すると，$A_1 \cup \{\varphi(a)\} \in X$ となり，$A_1 = \max X$ と矛盾する．よって，$\varphi(a) = a$ である． □

4. Zorn の補題

Zorn(ツォルン) の補題は，1 年生の学習内容としては，極めて難解な内容である．Zorn の補題の証明を理解すること困難なので要求しないが，4 年生になるまでには Zorn の補題を使えるようになってほしい．

公理 4.1.(選択公理) Λ は集合とし，各元 $\lambda \in \Lambda$ に対し，空でない集合 A_λ が与えられているとする．すると，A_λ の元 a_λ を 1 つずつ，同時に選ぶことができる．
もう少し厳密に言うと，写像 $f : \Lambda \longrightarrow \bigsqcup_{\lambda \in \Lambda} A_\lambda$ で，任意の $\lambda \in \Lambda$ に対し $f(\lambda) \in A_\lambda$ を満たすのが存在する．
これは**選択公理**とか**選出公理**と呼ばれ，数学 (集合論) ではこの選択公理は成立するものと仮定して議論を行う．$\Lambda = \mathbb{N}$ の場合には，上の性質は数学的帰納法の公理から証明でき，Λ が有限集合の場合には $\Lambda = \mathbb{N}$ の場合から証明できる．しかし，Λ が一般の無限集合の場合には，この公理は自明でない結果をいろいろ導く．

定理 4.2. A, B が集合で，全射 $f\colon A \to B$ が存在すれば，単射 $g\colon B \to A$ で，任意の $b \in B$ に対し $f(g(b)) = b$ を満たすものが存在する．

証明. 上の選択公理で $\Lambda := B$ とし，$b = \lambda \in \Lambda = B$ に対し，$A_b = A_\lambda := f^{-1}(b)$ とおく．$b \neq c \in B$ のとき $A_b \cap A_c = \phi$ で，$a \in A$ に対して $a \in A_{f(a)}$ だから $A = \bigsqcup_{\lambda \in \Lambda} A_\lambda$ である．$g : \Lambda \longrightarrow \bigsqcup_{\lambda \in \Lambda} A_\lambda$ で任意の $\lambda \in \Lambda$ に対し $g(\lambda) \in A_\lambda$ を満たすのが存在する．すると，$g(b) = g(\lambda) \in A_\lambda = f^{-1}(b)$ だから，$f(g(b)) = b$ となる．
なお，定理 4.2 は選択公理と同値な定理である． □

定理 4.3. $(A, \leqq)$ は半順序集合で，A の任意の空でない整列部分集合 B に対し $\sup_A B \in A$ が存在すると仮定する．すると，A には極大元が存在する．

証明. A には極大元が存在しないと仮定して矛盾を導く．A の空でない部分集合全体の集合を $\mathcal{P}$ とする．つまり，$\mathcal{P}$ は A の巾集合から ϕ を除いた集合である．選択公理から，各 $X \in \mathcal{P}$ に対し，その元 $a_X \in X$ を 1 つずつ同時に選ぶことができる．写像 $\psi\colon \mathcal{P} \to A$ を $\psi(X) = a_X$ $(X \in \mathcal{P})$ として定める．

次に，$a \in A$ に対し $X_a := \{y \in A \mid y > a\}$ とおく．A には極大元が存在しないから $X_a \neq \phi$ で，$X_a \in \mathcal{P}$ となる．$\varphi(a) = \psi(X_a) \in X_a$ で写像 $\varphi\colon A \to A$ を定めれば，$\varphi(a) > a$ $(\forall a \in A)$ が成り立つ．補題 3.12 より，$\varphi(a) = a$ を満たす $a \in A$ が存在する．これは矛盾である． □

定義 4.4. $(A, \leqq)$ は空でない半順序集合とする．A の任意の空でない全順序部分集合 B に対し $\sup_A B \in A$ が存在するとき，A は**帰納的順序集合** (inductive orderd set) であるという．

A が帰納的順序集合であれば，定理 4.3 の仮定「A の任意の空でない整列部分集合 B に対し $\sup_A B \in A$ が存在する」が満たされる．よって，次が成り立つ．

系 4.5.(Zorn の補題) A が帰納的順序集合ならば，A には極大元が存在する．

以下，Zorn の補題を使って証明する定理を 2 つ紹介します．証明は理解できなくていいです．1 つは Zermelo の整列定理で，この定理は後の濃度のところで使うので覚えておいて下さい．もう 1 つは「(無限次元) ベクトル空間には基底が存在する」です．Zorn の補題を使う証明には独特の難しさがあるので理解できないかもしれませんが，一応読んで雰囲気を知っておいて下さい．

定理 4.6.(Zermelo の整列定理) 任意の空でない集合 A は，そこに適当に順序を定めて整列集合になるようにできる．

証明. A の空でない部分集合 X と，X 上の全順序 $\leqq_X$ で $(X, \leqq_X)$ が整列集合になるようなもの全体の集合 Ω を考える．例えば $a \in A$ で，$X = \{a\}$ のとき，$a \leqq_X a$ で順序 $\leqq_X$ を定めると，これは整列集合になるので $\Omega \neq \phi$ である．

一般に，$(X, \leqq_X) \in \Omega$ と $(Y, \leqq_Y) \in \Omega$ に対し，$X \subset Y$ で $\leqq_X$ が $\leqq_Y$ の X 上への制限になっているときに $(X, \leqq_X) \leqq (Y, \leqq_Y)$ と定めると，$(\Omega, \leqq)$ は半順序集合になる．

(1) $(\Omega, \leqq)$ は帰納的順序集合であることを証明する．

Ω の勝手な全順序部分集合 $\mathcal{L}$ を取る．$\sup_\Omega \mathcal{L}$ が存在することを証明すればよい．$Z := \bigcup_{X \in \mathcal{L}} X$ とおく．Z 上に順序 $\leqq_Z$ を以下のように定める．勝手な $x, y \in Z$ を取る．$x \in X, y \in Y$ を満たす $X, Y \in \mathcal{L}$ が存在する．$\mathcal{L}$ は全順序集合だから $X \subset Y$ または $Y \subset X$ である．対称性から $Y \subset X$ と仮定してよい．すると $x, y \in X$ である．そこで，$x \leqq_X y$ のとき $x \leqq_Z y$ と定める．これが x, y を含む $X \in \mathcal{L}$ の選び方に依存しないことは，順序 $\leqq_Z$ の定義からすぐわかる．以上で，$(Z, \leqq_Z) \in \Omega$ が構成できた．

$(Z, \leqq_Z) = \sup_\Omega \mathcal{L}$ であることを証明する．構成法から，$(X, \leqq_X) \in \mathcal{L}$ ならば $(X, \leqq_X) \leqq (Z, \leqq_Z)$ である．

もし $(Y, \leqq_Y)$ が $\mathcal{L}$ の上界 $\overline{\mathcal{L}}$ の元ならば，任意の $(X, \leqq_X) \in \mathcal{L}$ に対し $X \subset Y$ を満たさないといけないから，$Z \subset Y$ となる．$\leqq_Z$ の定義から，$(Z, \leqq_Z) \leqq (Y, \leqq_Y)$ である．よって，$(Z, \leqq_Z) = \min \overline{\mathcal{L}}$ で，$(Z, \leqq_Z) = \sup_\Omega \mathcal{L}$ である．

(2) $(\Omega, \leqq)$ は帰納的順序集合であるから，Zorn の補題により極大元が存在する．その極大元の 1 つを改めて $(Z, \leqq_Z)$ と書くことにする．$Z = A$ であることが証明できれば，定理の証明が完了する．そこで，$Z \subsetneqq A$ と仮定して矛盾を導く．

$Z \subsetneqq A$ ならば，ある元 $a \in A - Z$ が存在する．$X := Z \cup \{a\}$ とおくと $Z \subsetneqq X$ である．X 上の順序 $\leqq_X$ を次のように定める．$x, y \in X$ を取る．もし $x, y \in Z$ ならば $x \leqq_Z y$ のとき $x \leqq_X y$ と定める．$x \in Z, y = a$ のときは $x <_X a$ と定める．すると $(X, \leqq_X)$ も整列集合になり，$(X, \leqq_X) \in \Omega$ で，$(Z, \leqq_Z) < (X, \leqq_X)$ となる．これは $(Z, \leqq_Z)$ が極大元であることに矛盾する． □

線形代数で実ベクトル空間や複素ベクトル空間と，有限次元ベクトル空間の基底の話は習ったと思う．ここでは，無限次元ベクトル空間の基底の話をする．$\mathbb{R}$ (実数全体の集合) を $\mathbb{Q}$ (有理数全体の集合) 上のベクトル空間と考える話が登場するので，ここでは，一般に体上のベクトル空間の定義から始める．

定義 4.7. (I) 集合 G 上に (2 項) 演算 $*$ が定められていて，また，$e \in G$ であるとする．
(0) (G は $*$ について閉じている) $x, y \in G$ ならば $x * y \in G$.
(1) (結合法則) $x, y, z \in G$ ならば $(x * y) * z = x * (y * z)$
(2) (e は単位元) $x \in G$ ならば $e * x = x$, $x * e = x$.
(3) (逆元の存在) $x \in G$ ならば，ある $y \in G$ が存在して，$x * y = e$, $y * x = e$.
を満たすとき，G は演算 $*$ について e を単位元とする**群** (group) であるという．(3) において，y を $*$ に関する x の**逆元**という．G が $*$ について群であって，
(4) (交換法則) $x, y \in G$ ならば $x * y = y * x$.
が成り立つとき，G は Abel 群であるという．

(II) 集合 K に和 $+$ と積 $\times$ ($x \times y$ は $x \cdot y$ とか xy とも書く) が与えられていて，
(1) K は加法 $+$ について 0 を単位元とする Abel 群である．
(2) $K^\times := \{x \in K \mid x \neq 0\}$ とおくとき，$K^\times$ は積について 1 を単位元とする Abel 群である．また，$0 \neq 1$ である．
(3) (分配法則) $x, y, z \in K$ ならば $(x + y)z = xz + yz$.
が成り立つとき，K は**体** (たい，field) であるという．

例えば，実数全体の集合 $\mathbb{R}$, 複素数全体の集合 $\mathbb{C}$, 有理数全体の集合 $\mathbb{Q}$ はいずれも体である．体の意味がよくわからない人は，ここでは $\mathbb{Q}$ と $\mathbb{R}$ と $\mathbb{C}$ が体であると思って聞いてもらっても構わない．

(III) K は体とし，V は加法 $+$ について 0 を単位元とするアーベル群とする．K の勝手な元 a と V の勝手な元 x の間に**スカラー倍**と呼ばれる演算 ax が定まっていて，$ax \in V$ が成り立つと仮定する．さらに，
(1) (分配法則) $a, b \in K$, $x, y \in V$ ならば，$(a + b)x = ax + bx$, $a(x + y) = ax + ay$.
(2) (結合法則) $a, b \in K$, $x \in V$ ならば，$(ab)x = a(bx)$.
(3) (1 の自明な作用) $x \in V$ ならば $1x = x$. ここで 1 は K の乗法の単位元である．
が成り立つと仮定する．このとき V は K-**ベクトル空間**であるという．$K = \mathbb{R}$ のとき**実ベクトル空間**, $K = \mathbb{C}$ のとき**複素ベクトル空間**, $K = \mathbb{Q}$ のとき**有理ベクトル空間**という．

例えば，$\mathbb{R}$ や $\mathbb{C}$ は $\mathbb{Q}$-ベクトル空間であある．

定義 4.8. K は体，V は K-ベクトル空間，$X \subset V$ は部分集合とする．
(1) X が K 上 1 **次独立** (または，**線形独立**) であるとは，X 内の相異なる 1 個以上の任意の有限個の元 $x_1, \ldots, x_n \in X$ が K 上 1 次独立 (つまり，$a_1, \ldots, a_n \in K$, $a_1x_1 + \cdots + a_nx_n = 0$ が成り立てば，$a_1 = \cdots = a_n = 0$) であることを言う．
(2) X が K 上の V の**生成系**であるとは，任意の $y \in V$ に対し，ある自然数 $n \in \mathbb{N}$ と，ある $a_1, \ldots, a_n \in K$ と，ある $x_1, \ldots, x_n \in X$ が存在して，$y = a_1x_1 + \cdots + a_nx_n$ が成り立つことをいう．
(3) X が K 上の V の**基底**であるとは，X が K 上 1 次独立で，X が K 上の V の生成系であることをいう．

上の定義において X が有限集合の場合には，線形代数で習うような通常の 1 次独立，生成系 (生成元)，基底の定義と一致する．

定理 4.9. K は体，V は K-ベクトル空間とする．すると，ある部分集合 $X \subset V$ で X が K 上の V の基底になるようなものが存在する．さらに，$A \subset V$ が K 上 1 次独立ならば，基底 X を $A \subset X$ となるように選ぶことができる．

証明. $V \neq \{0\}$ の場合の証明すれば十分である．A が与えられていないときは，$0 \neq x \in V$ を勝手に取り $A = \{x\}$ としておく．

$$\Omega := \{X \subset V \mid X \text{ は } K \text{ 上 1 次独立で } A \subset X\}$$

とおき，Ω を包含関係を順序として，半順序集合と考える．$A \in \Omega$ なので，$\Omega \neq \phi$ である．

(1) Ω が帰納的順序集合であることを証明する．

$\mathfrak{L} \subset \Omega$ を勝手な全順序部分集合とする．$\sup_\Omega \mathfrak{L} \in \Omega$ が存在することを示せばよい．$Y := \bigcup_{X \in \mathfrak{L}} X$ とおく．Y の勝手な有限部分集合 $\{x_1, \ldots, x_n\}$ をとるとき，$\{x_1, \ldots, x_n\} \subset X$ となるような $X \in \mathfrak{L}$ が存在

する．よって $x_1,\ldots,x_n$ は 1 次独立である．したがって，Y も 1 次独立であり，$Y \in \Omega$ となる．$X' \in \mathfrak{L}$ ならば $X' \subset Y$ である．また，$Z \in \Omega$ が任意の $X' \in \mathfrak{L}$ に対し $X' \subset Z$ を満たせば，Y の定義から $Y \subset Z$ である．よって，$Y = \sup_\Omega \mathfrak{L}$ である．

(2) Ω は帰納的順序集合なので，極大元 E が存在する．E が V の基底であることを証明する．

$E \in V$ なので E は 1 次独立である．あと，E が V の生成系であることを証明すればよい．E が V の生成系でないと仮定して矛盾を導く．すると，ある $y \in V$ が存在して，どのように自然数 $n \in \mathbb{N}$ と，$a_1,\ldots,a_n \in K$ と，$x_1,\ldots,x_n \in X$ を選んでも $y \neq a_1x_1 + \cdots + a_nx_n$ となる．つまり，$\{y, x_1,\ldots,x_n\}$ は 1 次独立である．そこで，$F := E \cup \{y\}$ とおくと，F も K 上 1 次独立となる．$E \subsetneqq F \in \Omega$ なので，E が Ω の極大元であることと矛盾する． □

$\mathbb{Q}$-ベクトル空間 $\mathbb{R}$ に基底が存在することは，次の例題に意外な解答を与える．

例題 4.10. 写像 $f\colon \mathbb{R} \to \mathbb{R}$ は次の (a) と (b) を満たすとする．
(a) 任意の $x, y \in \mathbb{R}$ に対し $f(x+y) = f(x) + f(y)$.
(b) $f(1) = 1$.
このとき，以下を示せ．
(1) 任意の $x \in \mathbb{Q}$ に対し $f(x) = x$ が成り立つ．
(2) (a), (b) を満たし，$f(\sqrt{2}) \neq \sqrt{2}$ となるような f が存在する．

解答. (1) $n \in \mathbb{N}$ に対し $f(n) = n$ であることは，n に関する帰納法ですぐ証明できる．$f(0) = f(0+0) = f(0) + f(0)$ より $f(0) = 0$ である．$f(n) + f(-n) = f(n + (-n)) = f(0) = 0$ なので，$f(-n) = -f(n) = -n$ $(n \in \mathbb{N})$ である．

$x \in \mathbb{Q}$ は $x = m/n$ $(m \in \mathbb{Z}, n \in \mathbb{N})$ と書ける．一般に，$n \in \mathbb{N}$ ならば $f(ny) = nf(y)$ であることは，n に関する帰納法ですぐ証明できる．よって，$m = f(m) = f(nx) = nf(x)$ となり，$f(x) = m/n = x$ である．

(2) 1 と $\sqrt{2}$ は $\mathbb{Q}$ 上 1 次独立なので，$\mathbb{Q}$-ベクトル空間 $\mathbb{R}$ の基底 E を $1, \sqrt{2} \in E$ となるように選ぶことができる．全単射 $g\colon E \to E$ で，$g(1) = 1$, $g(\sqrt{2}) \neq \sqrt{2}$ を満たすものが存在する．$0 \neq x \in \mathbb{R}$ に対し，自然数 n と，0 でない有理数 $a_1,\ldots,a_n$ と，相異なる $e_1,\ldots,e_n \in E$ で，$x = a_1e_1 + \cdots + a_ne_n$ となるものが一意的に存在する．そこで，$f(x) = a_1g(e_1) + \cdots + a_ng(e_n)$ として $f(x)$ を定めれば，f は (a), (b) を満たし，$f(1) = g(1) = 1$, $f(\sqrt{2}) = g(\sqrt{2}) \neq \sqrt{2}$ となる． □

第 II 部 濃度

5. 濃度の定義

今，自然数 n に対し，1 以上 n 以下の自然数全体の集合を $N_n := \{1, 2, \ldots, n\}$ と書くことにする．形式的に，$N_0 := \phi$ とおく．

A が n 個の元からなる有限集合である，ということを厳密に定義すると，全単射 $f\colon N_n \to A$ が存在すること，と言い替えられる．このとき，$\#A = n$ と書くことにする．$A = \phi$ のときは，$\#A = 0$ と約束しておく．$\#A$ は $|A|$ とか $n(A)$ などと書くことも多いが，この講義ノートでは $\#A$ という記号を採用する．$\#(A)$ と書くこともある．

問 5.1. A, B は有限集合とする．
(1) もし $\#A \neq \#B$ ならば，全単射 $f\colon A \to B$ は存在しないことを証明せよ．
(2) もし $\#A \leqq \#B$ ならば，単射 $f\colon A \to B$ が存在することを証明せよ．

(ヒント. 数学的帰納法を用いるとよい.)

無限集合の場合には元の個数を数えることはできないが，上の問題の精神を利用して以下のように「元の個数」を拡張した概念として「濃度」(cardinality) を定義する．食塩水の濃度 (concentration of saline solution) などとは全然異なる意味の用語である．(英語で食塩水の濃度の数学の問題を出題するときは，salt water とか saline water ではなく saline solution と食塩水を記述するのが普通である．例: How many liters of a 25% saline solution must be added to 3 liters of a 10% saline solution to obtain a 15% saline solution?)

定義 5.2. A, B は集合とする．
(1) 全単射 $f\colon A \to B$ が存在するとき $\#A = \#B$ と書くことにし，集合 A と B の**濃度は等しい**という．
(2) 単射 $f\colon A \to B$ が存在するとき $\#A \leqq \#B$ とか $\#B \geqq \#A$ と書くことにし，集合 A の濃度は集合 B の濃度以下であるとか，集合 B の濃度は集合 A の濃度以上であるという．

全射 $g\colon B \to A$ が存在すれば単射 $f\colon A \to B$ が存在することは定理 4.2 で証明した．

定理 5.3. A, B は集合とする．単射 $f\colon A \to B$ が存在すれば，全射 $g\colon B \to A$ で，任意の $x \in A$ に対し $g(f(x)) = x$ を満たすものが存在する．

したがって，$\#A \leqq \#B$ であることと，全射 $g\colon B \to A$ が存在することは同値である．

証明. $a_0 \in A$ を勝手に選んで 1 つ固定し，$b \in B - f(A)$ のときは $g(b) = a_0$ とする．f の値域を $f(A)$ に制限した写像 $f\colon A \to f(A)$ は全単射であるので，$b \in f(A)$ ならば $f(a) = b$ を満たす $a \in A$ を取って $g(b) = a$ と定める．すると写像 $g\colon B \to A$ ができる．作り方から $f(g(b)) = b$ $(\forall b \in B)$ が成り立ち，g は全射である． □

$f\colon A \to B$ と $g\colon B \to C$ が単射のとき，$g \circ f\colon A \to C$ も単射なので，$\#A \leqq \#B$ かつ $\#B \leqq \#C$ ならば $\#A \leqq \#C$ が成り立つ．しかし，濃度が全順序になることの証明は，結構難しい．以下，それを証明していく．

定理 5.4.(Bernstein の定理) A, B は集合で，$\#A \leqq \#B$ かつ $\#B \leqq \#A$ であると仮定する．すると $\#A = \#B$ が成り立つ．

証明. 単射 $f\colon A \to B$ と単射 $g\colon B \to A$ が存在するとき，全単射 $h\colon A \to B$ を構成すればよい．f か g が全射ならば $\#A = \#B$ であるから，f も g も全射でないと仮定する．

$B_0 := B - f(A)$ とおく．f は全射でないから $B_0 \neq \phi$. 以下帰納的に $A_n := g(B_{n-1})$, $B_n := f(A_n)$ $(n \in \mathbb{N})$ とおく．$i \neq j$ ならば $A_i \cap A_j = \phi$, $B_i \cap B_j = \phi$ であることは，帰納法ですぐ証明できる．そして，

$$X := \bigcup_{n=1}^{\infty} A_n, \quad Y := \bigcup_{n=0}^{\infty} B_n$$

とおく．$X = \bigsqcup_{n=1}^{\infty} A_n$, $Y = \bigsqcup_{n=0}^{\infty} B_n$ と書いてもよい．

$g|_Y : Y \to X$ は全単射であるので，その逆写像を $h_1 : X \to Y$ とおく．

(1) $f(A - X) = B - Y$ であることを証明する．

$f(X) = \bigsqcup_{n=1}^{\infty} B_n = Y - B_0$ である．他方 $B_0 = B - f(A)$ より $f(A) = B - B_0$ である．f は単射だから $f(A - X) = (B - B_0) - (Y - B_0) = B - Y$ となる．

(2) 上で示したことから $f|_{(A-X)} : (A - X) \longrightarrow (B - Y)$ は全単射であるが，この写像を $h_2 : (A - X) \to (B - Y)$ とおく．$x \in A$ に対し $x \in X$ ならば $h(x) = h_1(x)$, $x \in A - X$ ならば $h(x) = h_2(x)$ として $h : A \to B$ を定める．h_1 と h_2 は全単射だったので，h の全単射である． □

f は単射だから $f(A - X) = B - (Y - B_0) = (B - Y) \cup B_0$. $f(A_n) = B_n$ だから $f(X) \subset Y$ である．

定理 5.5.(濃度の比較定理) A, B は集合とする．すると $\#A \leqq \#B$ または $\#B \leqq \#A$ である．

証明. Zermelo の整列定理 (定理 4.6) を用いて，A, B に適当に順序を定めて整列集合にしておく．定理 3.10 より，(1) $A \cong B$, (2) $A_{<a} \cong B$ $(\exists a \in A)$, (3) $B_{<b} \cong A$ $(\exists b \in B)$ のいずれかが成立する．

(1) ならば順序同型 $f : A \to B$ が存在して，これは全単射であるので $\#A = \#B$ である．

(2) ならば順序同型 $f : A_{<a} \to B$ が存在する．その逆写像から単射 $B \xrightarrow{\cong} A_{<a} \xrightarrow{\subset} A$ が作れるので $\#B \leqq \#A$ である．(3) ならば同様に $\#A \leqq \#B$ である． □

以上で濃度の $\leqq$ は全順序の条件を満たすことが証明できた．そこで，$\#A \leqq \#B$ かつ $\#A \neq \#B$ のとき $\#A < \#B$ とか $\#B > \#A$ と書くことにする．

次に無限集合の定義を考える.「無限個の元を含む集合を無限集合という」という定義は,「無限個」の意味が不明瞭である．そこで，以下の定理から始める．

定理 5.6.(無限集合) A は集合で，空集合でも有限集合でもないとする．すると $\#\mathbb{N} \leqq \#A$ である．つまり，単射 $f : \mathbb{N} \to A$ が存在する．このとき，A は**無限集合**であるという．

証明. A は空集合でないとする．Zermelo の整列定理 (定理 4.6) を用いて，A に適当に順序を定めて整列集合にしておく．$\mathbb{N}$ は整列集合なので，定理 3.10 より，(1) $\mathbb{N} \cong A$, (2) $\mathbb{N}_{<n} \cong B$ $(\exists n \in \mathbb{N})$, (3) $A_{<a} \cong \mathbb{N}$ $(\exists a \in A)$ のいずれかが成立する．本章の最初の記号で $N_n = \mathbb{N}_{<n+1}$ である．よって，(2) が成り立てば $\#A = n - 1$ となり，有限集合である．(1), (3) の場合は単射 $f : \mathbb{N} \to A$ が存在する． □

なお，空集合も有限集合に含めるのが普通である．

定理 5.7. A の部分集合全体の集合を $\mathcal{P}(A)$ (巾集合) と書く．A が空集合でなければ，$\#\mathcal{P}(A) > \#A$ である．

証明. $x \in A$ に $\{x\} \in \mathcal{P}(A)$ を対応させる写像は単射なので，$\#\mathcal{P}(A) \geqq \#A$ である．$\#\mathcal{P}(A) \neq \#A$ を示そう．全単射 $f : A \to \mathcal{P}(A)$ が存在すると仮定して矛盾を導く．

$$B := \{x \in A \mid x \notin f(x)\}$$

とおく．$B \subset A$ なので $B \in \mathcal{P}(A)$ である．f は全単射なので $f(b) = B$ を満たす $b \in B$ が存在する．

もし $b \in B$ ならば B の定義から $b \notin f(B) = B$ となって矛盾する．もし $b \notin B = f(b)$ ならば B の定義から $b \in B$ となって矛盾する． □

6. 無限集合の濃度

定義 6.1. A が集合で $\#A = \#\mathbb{N}$ であるとき，A を**可算** (無限) 集合という．また，$\#A \leqq \#\mathbb{N}$ であるとき，A は**高々可算**であるという．$\#A = \#\mathbb{R}$ であるとき，A は**連続体濃度**であるという．

補題 6.2. n は自然数，$A_1, A_2, \ldots, A_n$ は可算集合で，B は有限集合であるとする．このとき，以下が成り立つ．
(1) $\#(A_1 \sqcup B) = \#\mathbb{N}$.
(2) $\#(A_1 \sqcup \cdots \sqcup A_n) = \#\mathbb{N}$.
(3) $\#(A_1 \times \cdots \times A_n) = \#\mathbb{N}$.

証明. $\#A_i = \#\mathbb{N}$ だから全単射 $f_i\colon \mathbb{N} \to A_i$ が存在する．そこで最初から，$A_1 = A_2 = \cdots = A_n = \mathbb{N}$ として証明すればよい．

(1) $B \neq \phi$ の場合に証明すれば十分である．$\#B = m$ とし，$B = \{b_1, \ldots, b_m\}$ とする．$n \in \mathbb{N}$ に対し，$n \leqq m$ ならば $g(n) = b_n$, $n > m$ ならば $g(n) = f_1(n-m)$ で写像 $g\colon \mathbb{N} \longrightarrow (A_1 \sqcup B)$ を定義する．g が全単射であることはすぐわかる．よって，$\#(A_1 \sqcup B) = \#\mathbb{N}$ である．

(2) $N_n = \{1, \ldots, n\}$ とおく．$A := A_1 \sqcup \cdots \sqcup A_n = \mathbb{N} \sqcup \cdots = \sqcup\mathbb{N}$ の元 x は，x が左から i 番目の $\mathbb{N}$ の元 $k \in \mathbb{N}$ であるとき，$x = (k, i)$ と書くことにすると，A の元 x と $(k, i) \in \mathbb{N} \times N_n$ $(k \in \mathbb{N}, i \in N_n)$ の対応が 1 対 1 だから，$\#A = \#(\mathbb{N} \times N_n)$ である．そこで，$\#(\mathbb{N} \times N_n) = \#\mathbb{N}$ を証明すればよい．

今，$x \in \mathbb{N}$ に対し，x を n で割った商を q, 余りを r とし，$g\colon \mathbb{N} \longrightarrow (\mathbb{N} \times N_n)$ を $g(x) = (q+1, r+1)$ で定める．逆に $h\colon (\mathbb{N} \times N_n) \longrightarrow \mathbb{N}$ を $h(k, i) = n(k-1) + i$ で定めると，h は g の逆写像になる．よって，g は全単射である．よって，$\#A = \#\mathbb{N}$ である．

(3) n に関する帰納法で証明すればよいから，$n = 2$ の場合に証明すれば十分である．$A_1 = A_2 = \mathbb{N}$ と仮定してよい．$(i, j) \in \mathbb{N}^2$ に対して $h(i, j) = \dfrac{(i+j-1)(i+j-2)}{2} + j$ で写像 $h\colon \mathbb{N}^2 \longrightarrow \mathbb{N}$ を定める．$h(1,1) = 1$, $h(2,1) = 2$, $h(1,2) = 3$, $h(3,1) = 4$, $h(2,2) = 5$, $h(1,3) = 6$, $h(4,1) = 7, \ldots$ である．

逆に $x \in \mathbb{N}$ に対し $g\colon \mathbb{N} \to \mathbb{N}^2$ を以下のように定める．$\dfrac{k(k-1)}{2} < x \leqq \dfrac{(k+1)k}{2}$ を満たす $k \in \mathbb{N}$ がただ 1 つ存在する．そこで，$j := x - \dfrac{k(k-1)}{2}$, $i := k - j + 1$ とおくと，$(i, j) \in \mathbb{N}^2$ で $h(i, j) = x$ を満たす．そこで，$g(x) = (i, j)$ で $g\colon \mathbb{N} \longrightarrow \mathbb{N}^2$ を定めると，g は h の逆写像になる．よって，g, h は全単射で，$\#\mathbb{N}^2 = \#\mathbb{N}$ がわかる． □

問題 6.3. $\#\mathbb{Z} = \#\mathbb{N}$, $\#\mathbb{Q} = \#\mathbb{N}$ であることを示せ．ここで，$\mathbb{Z}$ は整数全体の集合，$\mathbb{Q}$ は有理数全体の集合である．

(ヒント) $\#\mathbb{Z} = \#\mathbb{N}$ は前補題を使ってもいいし，直接全単射 $f\colon \mathbb{N} \to \mathbb{Z}$ を具体的に構成してもよい．$\mathbb{Q} = \left\{a/b \;\middle|\; a \in \mathbb{Z}, b \in \mathbb{N}\right\}$ であるので，$(a, b) \in \mathbb{Z} \times \mathbb{N}$ に $a/b \in \mathbb{Q}$ を対応させる全射 $g\colon (\mathbb{Z} \times \mathbb{N}) \longrightarrow \mathbb{Q}$ が存在する．これに，今まで習った定理・命題・補題を適用する．

定理 6.4.(カントールの対角線論法) $\#\mathbb{R} > \#\mathbb{N}$ である．また，$\#\mathbb{R} = \#\boldsymbol{\mathcal{P}}(\mathbb{N})$ である．

証明. $x \in (-\pi/2, \pi/2)$ に $\tan x \in \mathbb{R}$ を対応させる写像 $\tan : (\pi/2, \pi/2) \longrightarrow \mathbb{R}$ は全単射である．また，$f(x) = (x - 1/2)\pi$ とすると全単射 $f\colon (0, 1) \longrightarrow (-\pi/2, \pi/2)$ が定まる．よって，$\#\mathbb{R} = \#(0, 1)$ である．また，$(0, 1) \subset [0, 1] \subset \mathbb{R}$ だから，$\#\mathbb{R} = \#(0, 1) \leqq \#[0, 1] \leqq \#\mathbb{R}$ であり，$\#[0, 1] = \#\mathbb{R}$ である．同様に $\#[0, 1) = \#\mathbb{R}$ である．

さて，$x \in [0, 1]$ を取る．x を二進小数で表す．ここで，$\displaystyle\sum_{n=1}^{\infty} \frac{1}{2^n} = 1$ であるから，$0.1111\ldots$ で表わされる無限二進小数は 1 と等しい．同様に，$0.0111\cdots = 0.1$, $0.001111\cdots = 0.01$ など，有限二進小数で表せる実数は 2 通りの二進小数表示を持つ．

(1) $\#\mathbb{R} = \#\boldsymbol{\mathcal{P}}(\mathbb{N})$ を証明する．

今，$A \in \boldsymbol{\mathcal{P}}(\mathbb{N})$, つまり $A \subset \mathbb{N}$ に対し $n \in A$ ならば $a_n = 1$, $n \notin A$ ならば $a_n = 0$ とおき，$f(A) = \displaystyle\sum_{n \in A} \frac{a_n}{2^n}$ とすると $f(A) \in [0, 1]$ である．

逆に，$x \in [0, 1]$ に対し，$x = \displaystyle\sum_{n=1}^{\infty} \frac{a_n}{2^n} = 1$ $(a_n \in \{0, 1\})$ と表わし，$A = \left\{n \in \mathbb{N} \;\middle|\; a_n = 1\right\}$ とおけば，$f(A) = x$ である．$x = f(A)$ を満たす A は最大 2 個ある．いずれにせよ，$f\colon \boldsymbol{\mathcal{P}}(\mathbb{N}) \longrightarrow [0, 1]$ は全射である．よって，$\#\boldsymbol{\mathcal{P}}(\mathbb{N}) \geqq \#[0, 1] = \#\mathbb{R}$ である．

他方，$g\colon \mathcal{P}(\mathbb{N}) \longrightarrow \mathbb{R}$ を $g(A) = \displaystyle\sum_{n\in A} \frac{a_n}{3^n}$ で定める．ここで，$a_n \in \{0,\,1\}$ は上と同じように，$n \in A$ ならば $a_n = 1$, $n \notin A$ ならば $a_n = 0$ として定める．この g は単射である．よって，$\#\mathcal{P}(\mathbb{N}) \leqq \#\mathbb{R}$ である．したがって，$\#\mathcal{P}(\mathbb{N}) = \#\mathbb{R}$ である．

(2) $\#\mathbb{R} > \#\mathbb{N}$ を証明する．この証明方法が**カントールの対角線論法**と呼ばれる．

$\#\mathbb{N} < \#\mathcal{P}(\mathbb{N})$ だから，というとカントールの対角線論法の説明にならないので，古典的方法で直接的に証明する．

$\#[0,1) > \#\mathbb{N}$ を証明すればよい．全単射 $f\colon \mathbb{N} \to [0,1)$ が存在したと仮定して矛盾を導く．

$k \in \mathbb{N}$ に対し $f(k) = \displaystyle\sum_{n=1}^{\infty} \frac{a_{k,n}}{10^n}$ を満たす $a_{k,n} \in \{0,\ldots,\,9\}$ が存在する．(二進法以外なら何進法で表わしてもよい.) ただし，$0.5 = 0.49999\cdots$ のように 2 通りの表わし方がある場合は有限小数のほうで表すことと約束しておく．

$$b_k := \begin{cases} 1 & (a_{k,k} \neq 1 \text{ の場合}) \\ 0 & (a_{k,k} = 1 \text{ の場合}) \end{cases}$$

として b_k $(k \in \mathbb{N})$ を定め，$y = \displaystyle\sum_{b=1}^{\infty} \frac{b_n}{10^n}$ とおく．$y \in [0,\,1)$ である．$f(k) = y$ を満たす $k \in \mathbb{N}$ が存在する．$y = f(k) = \displaystyle\sum_{n=1}^{\infty} \frac{a_{k,n}}{10^n}$ なので，$b_k = a_{k,k}$ が成り立つ．しかし，b_k の定義から $b_k \neq a_{k,k}$ であり，矛盾する． □

補題 6.5. A は無限集合，B は空でない有限集合とする．すると 以下が成り立つ．
(1) $\#(A \sqcup B) = \#A$.
(2) $\#(A \times B) = \#A$.

証明. (1) A は無限集合なので単射 $f\colon \mathbb{N} \to A$ が存在する．$A_1 := f(\mathbb{N}) \subset A$, $A_2 := A - A_1$ とおく．$g_2\colon A_2 \longrightarrow A_2$ は恒等写像とする．$\#A = \mathbb{N}$ なので，補題 6.2 より全単射 $g_1\colon (A_1 \sqcup B) \longrightarrow A_1$ が存在する．そこで，写像 $g : (A \sqcup B) \longrightarrow A$ を，$x \in A_1 \sqcup B$ のとき $g(x) = g_1(x)$, $x \in A_2$ のとき $g(x) = g_2(x)$ として定めると，g は全単射である．

(2) $\Omega = \big\{(X,\,f) \;\big|\; X \subset A$ で全単射 $f\colon X \longrightarrow X \times B$ が存在する $\big\}$ とおく．$X \subset A$, $\#X = \mathbb{N}$ ならば，補題 6.2(2) より，全単射 $f\colon X \longrightarrow X \times B$ が存在する．よって，$(X,\,f) \in \Omega \neq \phi$ である．

$(X,\,f), (Y,\,g) \in \Omega$ に対して，$X \subset Y$ かつ $g|_X = f$ が成り立つとき $(X,\,f) \leqq (Y,\,g)$ として Ω 上に $\leqq$ を定めると，$(\Omega,\,\leqq)$ は半順序集合になる．

(2-1) $(\Omega,\,\leqq)$ は帰納的順序集合であることを証明する．

$\mathfrak{L}$ が Ω の全順序部分集合のとき $\sup_\Omega \mathfrak{L}$ が存在することを示せばよい．$Z := \displaystyle\bigcup_{X\in\mathfrak{L}} X$ とおく．$h : Z \longrightarrow Z \times B$ を以下のように定める．勝手な $x \in Z$ を取る．$x \in X$ を満たす $(X,\,f) \in \mathfrak{L}$ が存在する．自然に $X \times B \subset Z \subset B$ を考えて，$h(x) = f(x) \in X \times B \subset Z \subset B$ と定める．この定義は $x \in X$ を満たす $(X,\,f) \in \mathfrak{L}$ の選び方に依存しない．各 f が単射なので h も単射である．勝手な $(z,\,b) \in Z \times B$ に対し，$(z,\,b) \in X \times B$ となる $X \subset Z$ を選べば，ある $x \in X \subset Z$ が存在して $h(x) = f(x) = (z,\,b)$ となるので，h は全射である．よって，$(Z,\,h) \in \Omega$ である．

$(Z,\,h) = \sup_\Omega \mathfrak{L}$ であることを証明する．構成法から，$(X,\,f) \in \mathfrak{L}$ ならば $(X,\,f) \leqq (Z,\,h)$ である．

もし $(Y,\,g)$ が $\mathfrak{L}$ の上界の元ならば，任意の $(X,\,f) \in \mathfrak{L}$ に対し $X \subset Y$ を満たさないといけないから，$Z \subset Y$ となる．h の定義から，$(Z,\,h) \leqq (Y,\,g)$ である．よって，$(Z,\,h) = \sup_\Omega \mathfrak{L}$ である．

(2-2) $(\Omega,\,\leqq)$ は帰納的順序集合であるから，Zorn の補題により極大元が存在する．その極大元の 1 つを改めて $(Z,\,h)$ と書くことにする．

もし，$\#Z = \#A$ ならば，全単射 $f\colon A \to Z$ が存在する．f^{-1} から全単射 $g\colon (Z \times B) \longrightarrow (A \times B)$ が構成できる．全単射 $h\colon Z \to Z \times B$ を合成すると，全単射 $g \circ h \circ f : A \longrightarrow A \times B$ が得られ，(2) が成立する．

以下 $\#Z < \#A$ を仮定して矛盾を導けば証明が完了する．もし $A - Z$ が有限集合ならば，Z は無限集合だから補題 6.2(1) より，$\#A = \#\big(Z \cup (A - Z)\big) = \#Z < \#A$ となり矛盾する．よって，$A - Z$ は無限集合で，単射 $\iota\colon \mathbb{N} \to (A - Z) \subset A$ が存在する．$Y := \iota(\mathbb{N}) \subset A$ とする．$Y \cap Z = \phi$ である．補題

6.2(2) より，全単射 $g\colon Y \longrightarrow Y \times B$ が存在する．$X := Y \sqcup Z \subset A$ とおき，$f\colon X \to X \times B$ を，$x \in Y$ のとき $f(x) = g(x) \in Y \times B \subset X \times B$ と定め，$x \in Z$ のとき $f(x) = h(x) \in Z \times B \subset X \times B$ と定める．すると，f は全単射になり，$(X, f) \in \Omega$ となる．$(Z, f) < (X, f)$ なので，(Z, f) が Ω の極大元であることと矛盾する． □

定理 6.6. A は無限集合とすると，$\#A^2 = \#A$ が成り立つ．

証明. 方針は補題 6.5(2) の証明と似ている．

$$\Omega = \bigl\{(X, f) \bigm| X \subset A \text{ で全単射 } f\colon X \longrightarrow X^2 \text{ が存在する}\bigr\}$$

とおく．$X \subset A$, $\#X = \mathbb{N}$ ならば，補題 6.2(2) より，全単射 $f\colon X \longrightarrow X^2$ が存在する．よって，$(X, f) \in \Omega \neq \phi$ である．

$(X, f), (Y, g) \in \Omega$ に対して，$X \subset Y$ かつ $g|_X = f$ が成り立つとき $(X, f) \leqq (Y, g)$ として Ω 上に $\leqq$ を定めると，$(\Omega, \leqq)$ は半順序集合になる．

(1) $(\Omega, \leqq)$ は帰納的順序集合である．

この証明は，前補題の (2-1) の証明とまったく同じなので割愛する．

(2) $(\Omega, \leqq)$ は帰納的順序集合であるから，Zorn の補題により極大元が存在する．その極大元の 1 つを (Z, h) とする．

もし，$\#Z = \#A$ ならば，全単射 $f\colon A \to Z$ が存在する．f^{-1} から全単射 $g\colon Z^2 \longrightarrow A^2$ が構成できる．全単射 $h\colon Z \to Z^2$ を合成すると，全単射 $g \circ h \circ f : A \longrightarrow A^2$ が得られ，定理 (2) が成立する．

以下 $\#Z < \#A$ を仮定して矛盾を導けば証明が完了する．

(3) $\#(A - Z) = \#A$ を証明する．

$\#Z \leqq \#(A - Z)$ または $\#Z \geqq \#(A - Z)$ である．

$\#Z \leqq \#(A - Z)$ の場合を考える．前補題の証明の (2-2) のように $A - Z$ は無限集合である．よって，前補題から，$\#(A - Z) = \#\bigl((A - Z) \sqcup (A - Z)\bigr)$ である．単射 $Z \to A - Z$ から単射 $\bigl(Z \sqcup (A - Z)\bigr) \longrightarrow \bigl((A - Z) \sqcup (A - Z)\bigr)$ が作れるから，

$$\#A = \#\bigl(Z \sqcup (A - Z)\bigr) \leqq \#\bigl((A - Z) \sqcup (A - Z)\bigr) = \#(A - Z) \leqq \#A$$

となり，$\#(A - Z) = \#A$ が得られる．

$\#Z \geqq \#(A - Z)$ の場合を考える．Z は無限集合だから $\#(Z \sqcup Z) = \#Z$ である．よって，

$$\#A = \#\bigl(Z \sqcup (A - Z)\bigr) \leqq \#(Z \sqcup Z) = \#Z \leqq \#A$$

となり，$\#(A - Z) = \#A$ が得られる．

(4) (3) より単射 $\iota\colon Z \to (A - Z) \subset A$ が存在する．$Y := \iota(Z) \subset A$, $X := Y \sqcup Z$ とおく．$\#Y = \#Z$ であることに注意する．

全単射 $f\colon X \to X^2$ を構成したいが，その構成方法は前補題の (2) の証明とは変わってくる．

まず，$x \in Z$ のときは $f(x) = h(x) \in Z^2 \subset X^2$ とおく．$x \in Y$ のときは工夫を要する．

$$X^2 = Z^2 \sqcup Y^2 \sqcup (Y \times Z) \sqcup (Z \times Y)$$

と分解する．全単射 $Y \to Z$ から，全単射 $Y^2 \longrightarrow Y \times Z$ と全単射 $Y^2 \longrightarrow Z \times Y$ が作れる．よって，前補題より，全単射

$$Y^2 \longrightarrow \bigl(Y^2 \sqcup (Y \times Z) \sqcup (Z \times Y)\bigr)$$

が存在する．全単射 $h\colon Z \to Z^2$ と全単射 $Y \to Z$ と上の全単射を利用して，全単射

$$g : Y \longrightarrow \bigl(Y^2 \sqcup (Y \times Z) \sqcup (Z \times Y)\bigr)$$

を構成することができる．そこで，$x \in Y$ のときは $f(x) = g(y) \in X^2$ と定める．すると，$f\colon X \to X^2$ は全単射である．また，$f|_Z = h$ なので $(Z, h) < (X, f) \in \Omega$ となり，(Z, h) が Ω の極大元であることに矛盾する． □

系 6.7. n が自然数で，A が無限集合ならば $\#A^n = \#A$ である．つまり，全単射 $A^n \to A$ が存在する．

証明. $n = 1$ のときは自明で，$n = 2$ の場合は前定理である．$n \geqq 3$ とし，帰納法を使う．帰納法の仮定から全単射 $g\colon A \to A^{n-1}$ が存在する．$n = 2$ の場合から全単射 $h\colon A \to A^2$ が存在する．$f\colon A \to A^n$ を以

下のように構成する．$x \in A$ に対し $f(x) = (y,\, z) \in A^2$ $(y,\, y \in A)$ とする．$(y,\, g(z)) \in A \times A^{n-1} = A^n$ である．そこで，$f(x) = (y,\, g(z)) \in A^n$ と定める．この $f\colon A \to A^n$ は全単射である． □

上の系の特殊な場合として，n が自然数のとき $\#\mathbb{R}^n = \#\mathbb{R}$ がわかる．また，$a + b\sqrt{-1} \in \mathbb{C}$ $(a,\, b \in \mathbb{R})$ に $(a,\, b) \in \mathbb{R}^2$ を対応させる写像は全単射だから，

$$\#\mathbb{C} = \#\mathbb{R}^2 = \#\mathbb{R}$$

である．

7. 濃度の演算

定義 7.1. $A,\, B,\, C$ は集合とし，$\mathfrak{a} := \#A,\, \mathfrak{b} := \#B,\, \mathfrak{c} := \#C$ とおく．このとき，

$$\mathfrak{a} + \mathfrak{b} := \#(A \sqcup B), \quad \mathfrak{a}\mathfrak{b} = \#(A \times B)$$

として濃度の和と積を定義する．また，集合 B から A への写像全体の集合を $\mathrm{Map}(B,\, A)$ とし，

$$\mathfrak{a}^{\mathfrak{b}} := \#\,\mathrm{Map}(B,\, A)$$

として濃度の巾 (べき) を定義する．

なお $B = \{1,\ldots,\, n\}$ の場合，$(a_1,\ldots,\, a_n) \in A^n$ と $f(i) = a_i$ $(i \in B)$ で定まる写像 $f \in \mathrm{Map}(B,\, A)$ が 1 対 1 に対応するから $\#\,\mathrm{Map}(B,\, A) = \#A^n$ である．したがって，$\mathfrak{b} = n \in \mathbb{N}$ ならば $\mathfrak{a}^{\mathfrak{b}} = \underbrace{\mathfrak{a}\mathfrak{a}\cdots\mathfrak{a}}_{n\text{ 個}}$ である．

命題 7.2. 濃度 $\mathfrak{a},\, \mathfrak{b},\, \mathfrak{c},\, \mathfrak{a}',\, \mathfrak{b}'$ に対して以下が成り立つ．

(1) $\mathfrak{a} + \mathfrak{b} = \mathfrak{b} + \mathfrak{a}$.
(2) $(\mathfrak{a} + \mathfrak{b}) + \mathfrak{c} = \mathfrak{a} + (\mathfrak{b} + \mathfrak{c})$.
(3) $\mathfrak{a} + 0 = \mathfrak{a}$. ただし，$0 = \#\phi$.
(4) $\mathfrak{a} \leqq \mathfrak{b},\, \mathfrak{a}' \leqq \mathfrak{b}'$ ならば $\mathfrak{a} + \mathfrak{a}' \leqq \mathfrak{b} + \mathfrak{b}'$.
(5) $\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a}$.
(6) $(\mathfrak{a}\mathfrak{b})\mathfrak{c} = \mathfrak{a}(\mathfrak{b}\mathfrak{c})$.
(7) $(\mathfrak{a} + \mathfrak{b})\mathfrak{c} = \mathfrak{a}\mathfrak{c} + \mathfrak{b}\mathfrak{c}$.
(8) $0\mathfrak{a} = 0$.
(9) $1\mathfrak{a} = \mathfrak{a}$. ただし，$1 = \#\{1\}$.
(10) $\mathfrak{a} \leqq \mathfrak{b},\, \mathfrak{a}' \leqq \mathfrak{b}'$ ならば $\mathfrak{a}\mathfrak{a}' \leqq \mathfrak{b}\mathfrak{b}'$.

証明. 集合の性質から，簡単にわかる． □

定理 7.3. $\mathfrak{a},\, \mathfrak{b},\, \mathfrak{c}$ は濃度で 0 でないとする．すると以下が成り立つ．

(1) $\mathfrak{a}^{\mathfrak{b}}\mathfrak{a}^{\mathfrak{c}} = \mathfrak{a}^{\mathfrak{b}+\mathfrak{c}}$.
(2) $(\mathfrak{a}\mathfrak{b})^{\mathfrak{c}} = \mathfrak{a}^{\mathfrak{c}}\mathfrak{b}^{\mathfrak{c}}$.
(3) $(\mathfrak{a}^{\mathfrak{b}})^{\mathfrak{c}} = \mathfrak{a}^{\mathfrak{b}\mathfrak{c}}$.
(4) $\mathfrak{b} \geqq \#\mathbb{N}$ で $2 \leqq \mathfrak{a} \leqq \mathfrak{b}$ ならば $2^{\mathfrak{b}} = \mathfrak{a}^{\mathfrak{b}}$.

証明. $A,\, B,\, C$ は集合で，$\mathfrak{a} := \#A,\, \mathfrak{b} := \#B,\, \mathfrak{c} := \#C$ とする．

(1) $\mathfrak{a}^{\mathfrak{b}}\mathfrak{a}^{\mathfrak{c}} = \#\big(\mathrm{Map}(B,\, A) \times \mathrm{Map}(C,\, A)\big)$ であり，$\mathfrak{a}^{\mathfrak{b}+\mathfrak{c}} = \mathrm{Map}(B \sqcup C,\, A)$ である．$(f, g) \in \mathrm{Map}(B,\, A) \times \mathrm{Map}(C,\, A)$ を取る．ただし，$f\colon B \to A$. $g\colon C \to A$ である．$x \in B \sqcup C$ に対し，$x \in B$ ならば $h(x) = f(x)$, $x \in C$ ならば $h(x) = g(x)$ として $h \in \mathrm{Map}(B \sqcup C,\, A)$ を定め，$\varphi(f, g) = h$ で

$$\varphi : \big(\mathrm{Map}(B, A) \times \mathrm{Map}(C, A)\big) \longrightarrow \mathrm{Map}(B \sqcup C,\, A)$$

を定める．φ の逆写像は $\varphi^{-1}(h) = (h|_B,\, h|_C)$ で与えられ，φ は全単射である．

(2) $\varphi : \big(\mathrm{Map}(C, A) \times \mathrm{Map}(C, B)\big) \longrightarrow \mathrm{Map}(C,\, A \times B)$ を，$f \in \mathrm{Map}(C,\, A)$, $g \in \mathrm{Map}(C,\, B)$ に対して，$\varphi(f, g)(x) = \big(f(x),\, g(x)\big) \in A \times B$ $(x \in C)$ によって定める．また，$\pi_A\colon A \times B \longrightarrow A$, $\pi_B\colon A \times B \longrightarrow B$ を正射影とすると，φ の逆写像は，$\varphi^{-1}(h) = (\pi_A \circ h,\, \pi_B \circ h)$ によって与えられる．

(3) $\varphi : \mathrm{Map}\big(C, \mathrm{Map}(B, A)\big) \longrightarrow \mathrm{Map}(B \times C, A)$ を以下のように構成する．$f \in \mathrm{Map}\big(C, \mathrm{Map}(B, A)\big)$ を取る．$(b, c) \in B \times C$ を取るとき，$f(c)\colon B \to A$ なので，$(\varphi(f))(b, c) = (f(c))(b) \in A$ として $\varphi(f) \in\in \mathrm{Map}(B \times C, A)$ を定める．

逆に，$g \in \mathrm{Map}(B \times C, A)$ に対し，$\psi(g) : C \longrightarrow \mathrm{Map}(B, A)$ は，$c \in C, b \in B$ に対し，$\big((\psi(g))(c)\big)(b) = g(b, c) \in A$ によって $\psi : \mathrm{Map}(B \times C, A) \longrightarrow \mathrm{Map}\big(C, \mathrm{Map}(B, A)\big)$ を定義する．$\psi \circ \varphi$ と $\varphi \circ \psi$ が恒等写像であることはすぐわかるので，結論を得る．

(4) $2 \leqq \mathfrak{a}$ なので $C := \{1, 2\} \subset A$ と仮定してよい．$f \in \mathrm{Map}(B, C)$ は $\mathrm{Map}(B, A)$ の元とみなせるので，$\mathrm{Map}(B, C) \subset \mathrm{Map}(B, A)$ であり，$2^{\mathfrak{b}} \leqq \mathfrak{a}^{\mathfrak{b}}$ である．

以下 $2^{\mathfrak{b}} \geqq \mathfrak{a}^{\mathfrak{b}}$ を証明する．$\mathfrak{b} \geqq \#\mathbb{N}$, $1 \leqq \mathfrak{a} \leqq \mathfrak{b}$ なので，$\mathfrak{b} \leqq \mathfrak{a}\mathfrak{b} \leqq \mathfrak{b}^2 = \mathfrak{b}$ であり，$\mathfrak{a}\mathfrak{b} = \mathfrak{b}$ となる．$\mathfrak{a} \leqq 2^{\mathfrak{a}}$ と (3) より，

$$\mathfrak{a}^{\mathfrak{b}} \leqq \left(2^{\mathfrak{a}}\right)^{\mathfrak{b}} \leqq 2^{\mathfrak{a}\mathfrak{b}} = 2^{\mathfrak{b}}$$

となる．よって $2^{\mathfrak{b}} = \mathfrak{a}^{\mathfrak{b}}$ である． □

上定理の (4) より，$\#\,\mathrm{Map}(\mathbb{R}, \mathbb{R}) = \#\mathcal{P}(\mathbb{R})$ がわかる．しかし，通常扱う $\mathbb{R}$ 上の連続関数はそんなに沢山はない．

命題 7.4. $C^0(\mathbb{R}) := \big\{ f \in \mathrm{Map}(\mathbb{R}, \mathbb{R}) \;\big|\; f \text{ は連続} \big\}$ とおくと，$\mathbb{C}^0(\mathbb{R}) = \#\mathbb{R}$ である．

証明. $\varphi : C^0(\mathbb{R}) \longrightarrow \mathrm{Map}(\mathbb{Q}, \mathbb{R})$ を，$f \in C^0(\mathbb{R})$ に対し $\varphi(f) = f|_{\mathbb{Q}} \in \mathrm{Map}(\mathbb{Q}, \mathbb{R})$ で定める．任意の実数は，ある有理数列の極限として表せるから，2 つの連続関数が $\mathbb{Q}$ 上で一致すれば $\mathbb{R}$ 上でも一致する．$f, g \in C^0(\mathbb{R})$ に対し $\varphi(f) = \varphi(g)$ が成り立つとき．f と g は $\mathbb{Q}$ 上で一致するから $f = g$ である．よって φ は単射である．したがって，$\mathfrak{a} := \#\mathbb{N}$, $\mathfrak{c} := \#\mathbb{R}$ とおくとき，定理 6.4 より $\mathfrak{c} = 2^{\mathfrak{a}}$ であったから，

$$\#C^0(\mathbb{R}) \leqq \#\,\mathrm{Map}(\mathbb{Q}, \mathbb{R}) = \mathfrak{c}^{\mathfrak{a}} = \left(2^{\mathfrak{a}}\right)^{\mathfrak{a}} = 2^{\mathfrak{a}\mathfrak{a}} = 2^{\mathfrak{a}} = \mathfrak{c} = \#\mathbb{R}$$

となる． □

命題 7.5. Ω, B, Λ は集合で，各 $\lambda \in \Lambda$ に対して集合 $A_\lambda \subset \Omega$ が与えられているとする．

(1) 任意の $\lambda \in \Lambda$ に対して $\#A_\lambda \leqq \#B$ が成り立つと仮定すると，

$$\#\left(\bigcup_{\lambda \in \Lambda} A_\lambda\right) \leqq \#(\Lambda \times B)$$

が成り立つ．

(2) 任意の $\lambda \in \Lambda$ に対して $\#A_\lambda = \#B$ が成り立つと仮定すると，

$$\#\left(\bigsqcup_{\lambda \in \Lambda} A_\lambda\right) = \#(\Lambda \times B)$$

が成り立つ．

証明. (1) $\#A_\lambda \leqq \#B$ だから，単射 $f_\lambda\colon A_\lambda \longrightarrow B$ が存在する．$\displaystyle\bigcup_{\lambda \in \Lambda} A_\lambda$ の勝手な元 x を取る．ある $\lambda \in \Lambda$ が存在して $x \in A_\lambda$ となる．この λ を 1 つ選択する．そして $\varphi(x) = (\lambda, f_\lambda(x)) \in \Lambda \times B$ によって写像

$$\varphi : \left(\bigcup_{\lambda \in \Lambda} A_\lambda\right) \longrightarrow (\Lambda \times B)$$

を定める．これは単射である．

(2) の場合，f_λ が全単射である．さらに，$x \in A_\lambda$ を満たす $\lambda \in \Lambda$ は一意的である．よって，φ も全単射になる． □

複素数 $c \in \mathbb{C}$ に対して，ある自然数 $n \in \mathbb{N}$ と，ある有理数係数多項式 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ ($a_0, a_1, \ldots, a_n$ は有理数で $a_n \neq 0$) で $f(c) = 0$ を満たすものが存在するとき，c は ($\mathbb{Q}$ 上) **代数的**であるとか，単に**代数的数**であるという．$\mathbb{Q}$ 上代数的な元全体の集合を $\overline{\mathbb{Q}}$ と書くことにする．なお，$c \in \mathbb{Q}$ ならは $f(x) = x - c$ とおくと $f(c) = 0$ なので，c は $\mathbb{Q}$ 上代数的で $\mathbb{Q} \subset \overline{\mathbb{Q}}$ である．例えば，

$\sqrt[3]{2}$ は代数的数であるが，円周率 π や自然対数の底 e は代数的数でない (その証明は難しいので，ここでは述べない).

命題 7.6. $\#\overline{\mathbb{Q}} = \#\mathbb{N}$ である.

証明. $\mathbb{Q} \subset \overline{\mathbb{Q}}$ より $\#\overline{\mathbb{Q}} \geqq \#\mathbb{Q} = \#\mathbb{N}$ である．$\#\overline{\mathbb{Q}} \leqq \#\mathbb{N}$ を示せばよい.

有理数係数多項式全体の集合を $\mathbb{Q}[x]$ と書くことにする．$\mathbb{Q}[x]$ の中で n 次以下の多項式全体の集合を A_n とする．$\mathbb{Q}[x] = \bigcup_{n=1}^{\infty} A_n$ である．($m \leqq n$ のとき $A_m \subset A_n$ なので，これは直和ではない.) ところで $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in A_n$ に対して $(a_n, a_{n-1}, \ldots, a_1, a_0) \in \mathbb{Q}^{n+1}$ を対応させる写像は全単射なので，$\#A_n = \#\mathbb{Q}^{n+1} = (\#\mathbb{N})^{n+1} = \#\mathbb{N}$ である.

$c \in \overline{\mathbb{Q}}$ を取る．$f(c) = 0$ を満たす $f(x) \in \mathbb{Q}[x]$ を取る．$f(x)$ は $\mathbb{Q}$ 上既約 (有理数係数多項式の範囲でこれ以上因数分解できない) と仮定してよい．そういう $f(x)$ は定数倍を除いて一意的に定まる．$f(x)$ の次数が n のとき，$n = \deg c$ と書くことにする．$f(x)$ の x^n の係数が 1 の場合 $f(x)$ を $\mathbb{Q}$ 上の c の**最小多項式**という．この $f(x)$ は c から一意的に定まる．n 次方程式 $f(x) = 0$ は $\mathbb{C}$ 内で c を含めて全部で最大 n 個の解を持つ.

$$B_n := \left\{ c \in \overline{\mathbb{Q}} \;\middle|\; \deg c = n \right\}$$

とおけば，$\overline{\mathbb{Q}} = \bigsqcup_{n=1}^{\infty} B_n$ である．$c \in B_n$ に対して c の最小多項式 $f(x) \in A_n$ を対応させる写像を $\varphi_n \colon B_n \to A_n$ とおく．上で説明したように，$f(x) \in A_n$ に対し $\varphi_n(c) = f(x)$ となる $c \in B_n$ は高々 n 個しかない．$n \times \#B_n = \#B_n$ だから，$\#B_n \leqq \#A_n = \#\mathbb{N}$ である．B_n は無限集合だから，$\#B_n = \#\mathbb{N}$ である．$\overline{\mathbb{Q}} = \bigsqcup_{n=1}^{\infty} B_n$ と，命題 7.5(2) より，$\#\overline{\mathbb{Q}} = \#(\mathbb{N} \times \mathbb{N}) = \#\mathbb{N}$ が得られる. □

命題 7.7. $\mathbb{R}$ は $\mathbb{Q}$ 上のベクトル空間であるが，その基底の 1 つを B とする．すると $\#B = \#\mathbb{R}$ である.

証明. $0 \neq x \in \mathbb{R}$ を取ると，ある $n \in \mathbb{N}$ と，ある $E = \{e_1, \ldots, e_n\} \subset B$ と，ある $a_1, \ldots, a_n \in \mathbb{Q} - \{0\}$ が x に対して一意的に存在して，$x = a_1 e_1 + \cdots + a_n e_n$ と表すことができる．B の空でない有限部分集合全体の集合を $\mathcal{E}$ とし，$E \in \mathcal{E}$ に対して，

$$A_E := \left\{ \sum_{e \in E} a_e e \;\middle|\; a_e \in \mathbb{Q} - \{0\} \right\}$$

とおけば，$\mathbb{R} = \{0\} \sqcup \bigsqcup_{E \in \mathcal{E}} A_E$ が成り立つ．$\#E = n$ とおけば $\#A_E = \#(\mathbb{Q} - \{0\})^n = \#\mathbb{N}^n = \#\mathbb{N}$ である．よって，$\#\mathbb{R} = \#(\mathcal{E} \times \mathbb{N})$ が成り立つ．$\mathcal{E}$ は無限集合だから，

$$\#\mathcal{E} \leqq \#(\mathcal{E} \times \mathbb{N}) \leqq \#(\mathcal{E} \times \mathcal{E}) = \#\mathcal{E}$$

である．よって，$\#(\mathcal{E} \times \mathbb{N}) = \#\mathcal{E}$ であり，$\#\mathbb{R} = \#\mathcal{E}$ である．他方，各 $n \in \mathbb{N}$ に対して，

$$\mathcal{E}_n := \left\{ E \in \mathcal{E} \;\middle|\; \#E = n \right\}$$

とおく．$\mathcal{E} = \bigsqcup_{n \in \mathbb{N}} \mathcal{E}_n$ である．$\mathcal{E}_n \subset B^n$ で B は無限集合だから，$\#\mathcal{E}_n \leqq (\#B)^n = \#B$ が成り立つ．$x \in B$ に x を含む基底 $x \in E \in \mathcal{E}_n$ を対応させる単射 $B \to \mathcal{E}_n$ が存在するから，$\#\mathcal{E}_n = \#B$ がわかる.

命題 7.5(2) より，$\#\mathcal{E} = \#(\mathbb{N} \times B)$ である．$\#(\mathbb{N} \times B) = \#B$ なので，$\#B = \#\mathcal{E} = \#\mathbb{R}$ である. □

話題 7.8. $\#\mathbb{N} < \#A < \#\mathbb{R}$ を満たす集合 A は知られていない.「$\#\mathbb{N} < \#A < \#\mathbb{R}$ を満たす集合 A は存在しない」という命題を**連続体仮説**という．もっと一般に,「B が無限集合のとき，$\#B < \#A < \#\mathcal{P}(B)$ を満たす集合 A は存在しない」という命題を**一般連続体仮説**という．この命題は，普通の数学の諸定理と雰囲気が異なっていて，集合や命題の定義自体に大きく依存することが知られている.

話題 7.9. 濃度 $\mathfrak{a}, \mathfrak{b}$ が $2^{\mathfrak{a}} = 2^{\mathfrak{b}}$ を満たすとき $\mathfrak{a} = \mathfrak{b}$ である，という命題が成り立つかどうか，という問題は結構多くの人が思い付く．しかし，この問題は数学基礎論の問題で集合の定義に依存し，少なく

とも ZFC 公理系では証明できないことが知られている．また，この定理が成立しないような集合の定義が存在することが知られている．

第 III 部 数の定義と性質

8. 自然数とその上の和と積

伝統的には自然数全体の集合 $\mathbb{N}$ を定義し，そこに $+, \times, \leqq$ などを定義していくのであるが，記数法まで考えるときゼロ 0 がないと不便である．そこで，オリジナルのペアノの公理とは異なるが，$\mathbb{N}_0 := \mathbb{N} \sqcup \{0\}$ を定義するほうの公理から始めることにする．なお，以下の公理で写像 $\varphi\colon \mathbb{N}_0 \longrightarrow \mathbb{N}_0$ は $\varphi(x) = x + 1$ を念頭に考えている．なお，下記の公理を満たす集合が存在することは，集合論の中で無限集合が存在する公理を記述しておかないと証明できない.「無限個」の元からなる集合というのは，思考対象であって，現実世界の中に実在物として構成できるものではない.

公理 8.1.(ペアノの公理) $\mathbb{N}_0$ は集合で，
(1) $0 \in \mathbb{N}_0$. (0 という記号で書かれる元を $\mathbb{N}_0$ は含む.)
(2) 写像 $\varphi\colon \mathbb{N}_0 \to \mathbb{N}_0$ が与えられている.
(3) $0 \notin \varphi(\mathbb{N}_0)$.
(4) φ は単射である.
(5) $A \subset \mathbb{N}_0$ かつ $0 \in A$ かつ「$x \in A \Longrightarrow \varphi(x) \in A$」$\Longrightarrow A = \mathbb{N}_0$.
を満たすとする．また，$\mathbb{N} := \mathbb{N}_0 - \{0\}$ とおく．このとき，$\mathbb{N}$ は**自然数全体の集合**であるといい，$\mathbb{N}$ の元を**自然数**という．また，$1 := \varphi(0)$ とおく．(3) より $0 \neq 1$ である.

定理 8.2. X は集合，$\psi\colon X \to X$ は写像とし，1 つの元 $x_0 \in X$ が固定されているとする．このとき，写像 $f\colon \mathbb{N}_0 \to X$ で以下の (1), (2) を満たすものが一意的に存在する.
(1) $f(0) = x_0$.
(2) 任意の $n \in \mathbb{N}_0$ に対して $f(\varphi(n)) = \psi(f(n))$ が成り立つ.

証明. まず，$N_0 := \{0\}$ とし，写像 $f_0\colon N_0 \to X$ を $f_0(0) = x_0$ で定める．今 $n \in \mathbb{N}_0$ に対し $n \in N_n$ を満たす集合 N_n と，写像 $f_n\colon N_n \to X$ が与えられているとき，$N_{\varphi(n)} := N_n \cup \{\varphi(n)\}$ と定める.

(i) まず，任意の $n \in \mathbb{N}_0$ に対して $n \in N_n$ であることを示す.

$$A_1 := \{n \in \mathbb{N}_0 \mid n \in N_n\}$$

とおく．$0 \in N_0 = \{0\}$ なので，$0 \in A_1$ である．今，$n \in A_1$ とすると，$N_{\varphi(n)} := N_n \cup \{\varphi(n)\}$ なので，$\varphi(n) \in N_{\varphi(N)}$ である．よって，$\varphi(n) \in A_1$ である．ペアノの公理 (5) より，$A_1 = \mathbb{N}_0$ となる．よって，(i) がわかる.

(ii) $\varphi(n) \notin N_n$ であることを証明しておく.

$$A_2 := \{n \in \mathbb{N}_0 \mid \varphi(n) \notin N_n\}$$

とおく．ペアノの公理 (3) より，$\varphi(0) \neq 0$ だから，$\varphi(0) \notin N_0 = \{0\}$ で，$0 \in A_2$ である．$n \in A_2$ かつ $\varphi(n) \notin A_2$ とすると，$\varphi(\varphi(n)) \in N_{\varphi(n)}$ となる．もし $\varphi(\varphi(n)) = \varphi(n)$ だと，ペアノの公理 (4) より，$\varphi(n) = n \in N_n$ となって $\varphi(n) \notin A_2$ となり矛盾する．よって，$A_2 = \mathbb{N}_0$ であり，(ii) がわかる．(ii) より，上の f_n の定義に矛盾がないことが確認される.

(iii) 任意の $n \in \mathbb{N}_0$ に対して $f_n\colon N_n \to X$ が定義されていることを確認する.

$$A_3 := \{n \in \mathbb{N}_0 \mid f_n\colon N_n \to X \text{ が定義されている}\}$$

とおく．$f_0\colon N_0 \to X$ は定義されているから，$0 \in A_3$ である．また，$n \in A_3$ のとき，上のように $f_{\varphi(n)}\colon N_{\varphi(n)} \longrightarrow X$ 定義できるから $\varphi(n) \in A_3$ である．ペアノの公理 (5) より $A_3 = \mathbb{N}_0$ となる．よって，(iii) がわかる.

(iv) 写像 $f_{\varphi(n)}\colon N_{\varphi(n)} \longrightarrow X$ を以下のように定める．$k \in N_{\varphi(n)}$ をとる．もし，$k \neq \varphi(n)$ ならば $k \in N_n$ であるので，$f_{\varphi(n)}(k) = f_n(k)$ と定義する．$k = \varphi(n)$ の場合には，上の結果から $k \notin N_n$ なので，$f_{\varphi(n)}(\varphi(n)) = \psi(f_n(n))$ と矛盾なく定義できる.

(v) 以上より，$f\colon \mathbb{N}_0 \to X$ を $f(n) = f_n(n)$ $(n \in \mathbb{N}_0)$ として定義できる．$f(0) = f_0(0) = x_0$ であるから (1) が成り立つ．また，

$$f(\varphi(n)) = f_{\varphi(n)}(\varphi(n)) = \psi(f_n(n)) = \psi(f(n))$$

であるから，(2) も成り立つ．

(一意性) 写像 $g\colon \mathbb{N}_0 \to X$ が $g(0) = x_0$ かつ $g(\varphi(n)) = \psi(g(n))$ $(\forall n \in \mathbb{N}_0)$ を満たすとする．

$$A_4 := \{n \in \mathbb{N}_0 \mid \text{写像 } g(n) = f(n)\}$$

とおく．$g(0) = x_0 = f(0)$ より $0 \in A_4$ である．また，$n \in A_4$ ならば，$g(n) = f(n)$ だから，

$$g(\varphi(n)) = \psi(g(n)) = \psi(f(n)) = f(\varphi(n))$$

となる．よって，$\varphi(n) \in A_4$ で，ペアノの公理の (5) より $A_4 = \mathbb{N}_0$ となる． □

ペアノの公理で $\mathbb{N}_0$ と 0 と φ を定義したが，他にそういうものがないかどうかが問題になる．$\mathbb{N}_0$ が他にはない，ということは言えないが，いわゆる「同型」の概念がポイントで，他に存在しても，それは $\mathbb{N}_0$ と同型である，ということが言える．しかし，まだ「同型」を定義していないので，その定義も込めて書いたのが次の定理である．なお，ペアノの公理を満たす $\mathbb{N}_0$ と φ の存在は，集合の定義の段階で，それが存在するように集合を定義しておかないと証明できない．

定理 8.3. $\mathbb{N}_0'$ は集合で，
(1') $0' \in \mathbb{N}_0'$.
(2') 写像 $\varphi'\colon \mathbb{N}_0' \to \mathbb{N}_0'$ が与えられている．
(3') $0' \notin \varphi'(\mathbb{N}_0')$.
(4') $x, y \in \mathbb{N}_0'$, $\varphi'(x) = \varphi'(y) \Longrightarrow x = y$」
(5') $A \subset \mathbb{N}_0'$ かつ $0' \in A$ かつ「$x \in A \Longrightarrow \varphi'(x) \in A$」$\Longrightarrow A = \mathbb{N}_0'$.
を満たすとする，このとき，全単射 $\psi\colon \mathbb{N}_0 \to \mathbb{N}_0'$ が存在して，以下の (i), (ii) を満たす．
(i) $\psi(0) = 0'$.
(ii) 任意の $x \in \mathbb{N}_0$ に対して $\psi(\varphi(x)) = \varphi'(\psi(x))$.

証明. 定理 8.2 より，写像 $\psi\colon \mathbb{N}_0 \to \mathbb{N}_0'$ が存在して (i), (ii) を満たす．また，写像 $\psi'\colon \mathbb{N}_0' \to \mathbb{N}_0$ が存在して，(i') $\psi'(0') = 0$. (ii') 任意の $x \in \mathbb{N}_0'$ に対して $\psi'(\varphi'(x)) = \varphi(\psi'(x))$ を満たす．合成写像 $\psi' \circ \psi\colon \mathbb{N}_0 \to \mathbb{N}_0$ が恒等写像であることを証明する．

$$A := \{x \in \mathbb{N}_0 \mid \psi'(\psi(x)) = x\}$$

とおく．$\psi'(\psi(0)) = \psi'(0') = 0$ なので $0 \in A$ である．$x \in A$ のとき，

$$\psi'(\psi(\varphi(x))) = \psi'(\varphi'(\psi(x))) = \varphi(\psi'(\psi(x))) = \varphi(x)$$

であるので，$\varphi(x) \in A$ である．よって，ペアノの公理の (5) より $A = \mathbb{N}_0$ となる．すなわち，$\psi' \circ \psi\colon \mathbb{N}_0 \to \mathbb{N}_0$ は恒等写像である．

同様に，$\psi \circ \psi'\colon \mathbb{N}_0' \to \mathbb{N}_0'$ も恒等写像である．よって，ψ は逆写像 ψ' を持つので全単射である． □

次に足し算の定義をする．

定理&定義 8.4. 各 $x \in \mathbb{N}_0$ に対し，
(6) $f_x(0) = x$.
(7) 任意の $y \in \mathbb{N}_0$ に対し $f_x(\varphi(y)) = \varphi(f_x(y))$.
を満たす写像 $f_x\colon \mathbb{N}_0 \to \mathbb{N}_0$ が一意的に存在する．この $f_x\colon \mathbb{N}_0 \to \mathbb{N}_0$ を利用して，$x, y \in \mathbb{N}_0$ に対して $x + y := f_x(y)$ により，**加法** $x + y$ を定義する．このとき，$x + 0 = x$. $x + 1 = \varphi(x)$ $(\forall x \in \mathbb{N}_0)$ が成り立つ．

証明. 写像 $f_x\colon \mathbb{N}_0 \to \mathbb{N}_0$ が一意的に存在することは，定理 8.2 からわかる．(6) より $x + 0 = x$ である．(7) より $f_x(\varphi(0)) = \varphi(f_x(0))$ なので，$\varphi(0) = 1$ より $x + 1 = \varphi(x)$ である． □

(7) は $x + (y + 1) = (x + y) + 1$ $(\forall x, y \in \mathbb{N}_0)$ と書き換えられる．

定理 8.5. 任意の $x, y, z \in \mathbb{N}_0$ に対して，以下が成り立つ．
(8) (結合法則) $(x + y) + z = x + (y + z)$.
(9) (交換法則) $x + y = y + x$.

証明. (8) $A := \{z \in \mathbb{N}_0 \mid$ 任意の $x, y \in \mathbb{N}_0$ に対し $(x+y)+z = x+(y+z)\}$ とおく．$(x+y)+0 = x+y = x+(y+0)$ なので，$0 \in A$ である．

$z \in A$ ならば $z+1 \in A$ を証明する．$z \in A$ だから任意の $x, y \in \mathbb{N}_0$ に対し $(x+y)+z = x+(y+z)$ が成り立つ．(7) の $s+(t+1) = (s+t)+1$ を $(s, t) = (x+y, z), (x, y+z)$ として使うと，

$$(x+y)+(z+1) = ((x+y)+z)+1 = (x+(y+z))+1 = x+((y+z)+1) = x+(y+(z+1))$$

となり，$z+1 \in A$ がわかる．ペアノの公理の (5) より $A = \mathbb{N}_0$ となる．

(9) $B := \{x \in \mathbb{N}_0 \mid 0+x = x+0\}$ とおく．$0 \in B$ は自明．$x \in B$ とすると $0+x = x+0 = x$ だから，$0+(x+1) = (0+x)+1 = x+1 = (x+1)+0$ となり，$x+1 \in B$ となる．ペアノの公理の (5) より $B = \mathbb{N}_0$ となり，$0+x = x+0 = x$ $(\forall x \in \mathbb{N}_0)$ がわかる．

$$C := \{x \in \mathbb{N}_0 \mid 1+x = x+1\}$$

とおく．$0 \in C$ は自明．$x \in C$ とすると $1+x = x+1$ だから，$1+(x+1) = (1+x)+1 = (x+1)+1 = (x+1)+1$ となり，$x+1 \in C$ となる．ペアノの公理の (5) より $C = \mathbb{N}_0$ となる．

$$D := \{x \in \mathbb{N}_0 \mid \text{任意の } y \in \mathbb{N}_0 \text{ に対し } x+y = y+x\}$$

とおく．$0, 1 \in D$ は上で証明した．$x \in D$ とすると，$x+y = y+x$ より，

$$(x+1)+y = (1+x)+y = 1+(x+y) = 1+(y+x) = (1+y)+x = (y+1)+x = y+(1+x) = y+(x+1)$$

となり，$x+1 \in D$ がわかる．ペアノの公理の (5) より $D = \mathbb{N}_0$ となる． □

結合法則 $(x+y)+z = x+(y+z)$ のおかげで，これを単に $x+y+z$ と書くことが許される．4 個以上の有限個の和についても同様である．$\displaystyle\sum_{i=1}^{n} a_i$ のような記号も n に関する帰納法で自然に定義される．つまり，$\displaystyle\sum_{i=1}^{n+1} a_i := \left(\sum_{i=1}^{n} a_i\right) + a_{n+1}$.

問 8.6. 以下の性質を証明せよ．
(1) $x, y, z \in \mathbb{N}_0$, $x+z = y+z$ ならば $x = y$ である．
(2) $x, y \in \mathbb{N}_0$, $y \neq 0$ のとき $x+y \neq x$ が成り立つ．

自然数 2 〜 9 は，$\varphi(1) = 2$, $\varphi(2) = 3$, $\varphi(3) = 4$, $\varphi(4) = 5$, $\varphi(5) = 6$, $\varphi(6) = 7$, $\varphi(7) = 8$, $\varphi(8) = 9$ によって定義する．十進法でそれより大きい数を表すには，掛け算が必要になる．

問 8.7. 上の定義にもとづいて，$4+5 = 9$ であることを証明せよ．ここまでに証明された結果のみ用いてよい．

定理&定義 8.8. 各 $x \in \mathbb{N}_0$ に対し，次の 2 つの条件 (1), (2) を満たす写像 $g_x \colon \mathbb{N}_0 \to \mathbb{N}_0$ が一意的に存在する．
(1) $g_x(0) = 0$
(2) 任意の $y \in \mathbb{N}_0$ に対して，$g_x(y+1) = g_x(y)+x$ が成り立つ．

$x, y \in \mathbb{N}_0$ に対し，$xy = g_x(y)$ として乗法を定義する．xy を $x \times y$ とか $x \cdot y$ と書くこともある．$x \times 0 = 0$, $x(y+1) = xy+x$ $(\forall x, y \in \mathbb{N}_0)$ が成り立つ．

証明. 定理 8.2 からわかる． □

上の定義の (2) は，$x(y+1) = xy+x$ と書き直せる．

定理 8.9. 任意の $x, y, z \in \mathbb{N}_0$ に対して，以下が成り立つ．
(1) $0 \times x = x \times 0 = 0$
(2) $1 \times x = x \times 1 = x$
(3) (分配法則) $(x+y)z = xz+yz$
(4) (分配法則) $x(y+z) = xy+xz$
(5) (交換法則) $xy = yx$.

(6) (結合法則) $(xy)z = x(yz)$

証明. 以下の各 A_i について，ペアノの公理の (5) を用いて $A_i = \mathbb{N}_0$ を証明する．

$$A_1 := \{x \in \mathbb{N}_0 \mid 0 \times x = x \times 0 = 0\}$$
$$A_2 := \{x \in \mathbb{N}_0 \mid 1 \times x = x \times 1 = x\}$$
$$A_3 := \{z \in \mathbb{N}_0 \mid \text{任意の } x, y \in \mathbb{N}_0 \text{ に対して } (x+y)z = xz + yz\}$$
$$A_4 := \{z \in \mathbb{N}_0 \mid \text{任意の } x, y \in \mathbb{N}_0 \text{ に対して } x(y+z) = xy + xz\}$$
$$A_5 := \{x \in \mathbb{N}_0 \mid \text{任意の } y \in \mathbb{N}_0 \text{ に対して } xy = yx\}$$
$$A_6 := \{z \in \mathbb{N}_0 \mid \text{任意の } x, y \in \mathbb{N}_0 \text{ に対して } x(yz) = x(yz)\}$$

A_4 の $x(y+z) = xy + xz$ はどの変数について帰納法を使うかを間違えると，証明が困難になる．以上の A_i に対して $A_i = \mathbb{N}_0$ の証明は簡単なので，練習問題とする． □

9. 自然数の大小関係

補題 9.1. (1) $x \in \mathbb{N}_0$, $x \neq 0$ ならば $x = y + 1$ を満たす $y \in \mathbb{N}_0$ が一意的に存在する．
(2) $x, y \in \mathbb{N}_0$, $x + y = 0$ ならば $x = y = 0$ である．

証明. (1) $A := \{0\} \cup \{x \in \mathbb{N}_0 \mid x = y + 1\ (\exists y \in \mathbb{N}_0)\}$ とおく．$A = \mathbb{N}_0$ は簡単に証明できる．$x = y + 1 = z + 1$ のとき，ペアノの公理の (4) より $y = z$ となるので，一意性がわかる．

(2) $y \in \mathbb{N}$ に対し $A_y := \{x \in \mathbb{N}_0 \mid x + y \neq 0\}$ とおく．ペアノの公理の (3) より $A_1 = \mathbb{N}_0$ である．

$B := \{0\} \cup \{y \in \mathbb{N}_0 \mid A_y = \mathbb{N}_0\}$ とおく．$0, 1 \in B$ である．$y \in B$, $y \neq 0$ とする．$A_y = \mathbb{N}_0$ より $x + y \neq 0$ $(\forall x \in \mathbb{N}_0)$. ペアノの公理の (3) より $x + (y+1) = (x+y) + 1 \neq 0$ なので，$A_{y+1} = \mathbb{N}_0$ である．よって $B = \mathbb{N}_0$ である．

このことは，$x, y \in \mathbb{N}_0$ かつ $y \neq 0$ ならば $x + y \neq 0$ を意味する．$y + x = x + y$ より，$x, y \in \mathbb{N}_0$ かつ $x \neq 0$ ならば $x + y \neq 0$ も成り立つ．よって $x + y = 0$ ならば $x = y = 0$ である． □

定理&定義 9.2. $x, y \in \mathbb{N}_0$ のとき，次の (1), (2) のいずれかが成立する．
(1) $x = y + z$ を満たす $z \in \mathbb{N}_0$ が存在する．
(2) $y = x + z$ を満たす $z \in \mathbb{N}_0$ が存在する．

また，(1) と (2) が同時に成立するのは，$x = y$ かつ $z = 0$ の場合に限る．$x, y \in \mathbb{N}_0$ に対して，(1) が成立するとき $y \leqq x$, (2) が成立するとき $x \leqq y$ と定義する．すると，$\mathbb{N}_0$ はこの $\leqq$ に関して整列集合になる．$\geqq, <, >$ は一般の順序集合の場合と同様に定義する．

証明. (I) $A := \{x \in \mathbb{N}_0 \mid \text{任意の } y \in \mathbb{N}_0 \text{ に対して (1) または (2) が成立する}\}$ とおく．$x = 0$ のときは，$y = 0$ のとき (1) が，$y \neq 0$ のとき (2) が成り立つので，$0 \in A$ である．

$x \in A$ とする．$y \in \mathbb{N}$ が (1) を満たすとき，$x + 1 = (y + z) + 1 = y + (z + 1)$ なので (1) が成り立つ．y が (2) を満たす場合を考える．$x = y + 0$ の場合は $x + 1 = y + 1$ なので (1) が成り立つ．$z \neq 0$ のときは $z = w + 1$ $(\exists w \in \mathbb{N}_0)$ と書けるので，$y = (x+1) + w$ となり (2) が成り立つ．よって，$x + 1 \in A$ である．ペアノの公理 (5) より $A = \mathbb{N}_0$ であるから，任意の $x, y \in \mathbb{N}$ に対して (1) または (2) が成り立つ．

(II) (1) と (2) が成立すれば $x = y$ であることを示す．$x = y + z$, $y = x + z'$ $(\exists z, z' \in \mathbb{N}_0)$ と書ける．$x + 0 = x = (x + z') + z = x + (z' + z)$ である．問 8.6(1) より $0 = z' + z$ である．前補題の (2) から $z = z' = 0$ となる．よって $x = y$ である．

(III) $(\mathbb{N}_0, \leqq)$ が全順序集合であることを示す．(1) か (2) が成り立つから，任意の $x, y \in \mathbb{N}_0$ に対して，$y \leqq x$ または $x \leqq y$ が成り立つ．$x = x + 0$ だから 反射律 $x \leqq x$ が成り立つ．反対称律 $x \leqq y$ かつ $y \leqq x$ ならば $x = y$ は証明した．推移律 $x \leqq y$ かつ $y \leqq z$ ならば $x \leqq z$ を証明する，$x \leqq y$, $y \leqq z$ より $y = x + w_1$, $z = y + w_2$ $(\exists w_1, w_2 \in \mathbb{N}_0)$ である．よって，$z = x + (w_1 + w_2)$ であり，$x \leqq z$ である．

(IV) $(\mathbb{N}_0, \leqq)$ が整列集合であることは，整列集合の章で証明した通りである． □

定理 9.3. $x \in \mathbb{N}_0$ のとき，$x < y < x + 1$ を満たす $y \in \mathbb{N}_0$ は存在しない．

証明. $x < y < x+1$ ならば $y = x+z$, $x+1 = y+w$ ($\exists z, w \in \mathbb{N}_0$) と書ける．ここで，$z \neq 0$, $w \neq 0$ である．すると $x+(z+w) = x+1$ より $z+w = 1$ となる．$z \neq 0$, $w \neq 0$ だから $z = z'+1$, $w = w'+1$ ($\exists z', w' \in \mathbb{N}_0$) と書ける．すると，$(z'+w'+1)+1 = z+w = 1$ となるので $z'+(w'+1) = 0$ となる．すると，$z' = w'+1 = 0$ となる．$w'+1 = 0$ より $w' = 0$, $1 = 0$ となり矛盾する． □

ペアノの公理 (5)(数学的帰納法の公理) をもう少し使い易い形に書き直しておく．

定理 9.4. $c \in \mathbb{N}_0$ とし，$A := \{x \in \mathbb{N}_0 \mid x \geqq c\}$ とおく．$P(x)$ は $x \in A$ に関する命題とする．もし，$P(c)$ が真であり,「$x \in A$ に対して，$c \leqq y < x$ を満たす任意の $y \in A$ に対して $P(y)$ が真ならば $P(x)$ も真」が成り立つとすれば，任意の $x \in A$ に対して $P(x)$ は真である．

証明. A は $\mathbb{N}_0$ の部分集合なので整列集合である．超限帰納法 (定理 3.5) より，上の定理が成り立つ． □

定理 9.5. $a, b, c, d \in \mathbb{N}_0$ のとき，以下が成り立つ．
(1) $a < b$ ならば $a+c < b+c$.
(2) $a+c < b+c$ ならば $a < b$.
(3) $a \leqq b$, $c \leqq d$ ならば $a+c \leqq b+d$.
(4) $a \leqq b$ ならば $ac \leqq bc$.
(5) $ac < bc$ ならば $a < b$.
(6) $ac = bc$, $c \neq 0$ ならば $a = b$.

証明. 簡単なので練習問題とする． □

定義 9.6. $a \in \mathbb{N}$, $n \in \mathbb{N}_0$ に対し，$a^0 = 1$, $a^{n+1} = a \times a^n$ として，**累乗** a^n を帰納的に定義する．また，$n \in \mathbb{N}$ に対し $0^n = 0$ と定義する．0^0 は定義しない．

定義 9.7.(引き算) $a, b \in \mathbb{N}_0$, $a \geqq b$ とする．不等号の定義から，$a = b+c$ を満たす $c \in \mathbb{N}_0$ が一意的に存在する．そこで，$a-b = c$ として $\mathbb{N}_0$ における引き算を定義する．

$a < b$ の場合の引き算は，整数全体の集合 $\mathbb{Z}$ を定義した後の話である．割り算は以下のように「余り」のある割り算を考えないといけない．

定理&定義 9.8.(割り算) $n \in \mathbb{N}_0$, $m \in \mathbb{N}$ とすると，$n = mq+r$, $0 \leqq r < m$ を満たす $q, r \in \mathbb{N}_0$ が一意的に存在する．このとき，n を m で割った**商**は q, **余り**は r であるという．$r = 0$ のとき n は m の**倍数**であるといい，m は n の**約数**であるという．

証明. 先に一意性を証明しておく．$n = mq_1+r_1 = mq_2+r_2$, $0 \leqq r_1 < m$, $0 \leqq r_2 < m$，$q_1, q_2, r_1, r_2 \in \mathbb{N}_0$ とする．対称性から $r_2 \geqq r_1$ と仮定しても一般性を失わない．$r_2 = r_1+d$ を満たす $d \in \mathbb{N}_0$ が存在する．$0 \leqq d \leqq r_2 < m$ である．$mq_1+r_1 = mq_2+r_2 = (mq_2+d)+r_1$ より，$mq_1 = mq_2+d$ となる．もし $d \neq 0$ ならば $mq_1 > mq_2$ である．もし $q_1 \leqq q_2$ なら $mq_1 \leqq mq_2$ なので $q_1 > q_2$ である．$q_1 = q_2+c$ を満たす $c \in \mathbb{N}$ がある．$mq_2+mc = mq_1 = m_q2+d$ より $mc = d$ となる．すると $m \leqq mc = d < m$ となって矛盾する．よって，$r_1 = r_2$ である．$mq_1 = mq_2$ より $m_1 = m_2$ となる．
以下，m, r の存在を証明する．
$m = 1$ の場合は $q = n$, $r = 0$ とすればよいので，以下，$m \geqq 2$ の場合を考える．
$n = 0$ の場合は $q = r = 0$ とおけばよい．
$n > 0$ とする．$n'+1 = n$ となる $n' \in \mathbb{N}_0$ が存在する．帰納法の仮定から，$n' = mq'+r'$, $0 \leqq r' < m$ を満たす $q', r' \in \mathbb{N}_0$ が存在する．もし，$r'+1 < m$ ならば $q = q'$, $r = r'+1$ とおけば，$n = mq+r$, $0 \leqq r < m$ が成り立つ．$r'+1 = m$ のときは，$q = q'+1$, $r = 0$ とおけば，$n = mq+r$, $0 \leqq r < m$ が成り立つ． □

定理 9.9. p が 2 以上の整数，$x \in \mathbb{N}$ ならば $p^n > x$ となるような自然数 n が存在する．

証明. $x=1$ ならば $n=1$ とおけばよい．$x>1$ の場合は帰納法の仮定から，$p^m > x-1$ となるような自然数 m が存在する．そこで $n=m+1$ とおけば $p^n = p^m + (p-1)p^m > (x-1)+1 = x$ となる．
□

定理 9.10. p は 2 以上の整数とする．$x \in \mathbb{N}_0$ をとる．$x_0 = x$ とし，帰納的に x_n を p で割った商を x_{n+1}, 余りを a_n とする．このとき，ある非負整数 N に対して $x_{N+1}=0$ となる．また，

$$x = a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots + a_N p^N$$

$(a_N \neq 0)$ となる．

このとき $x = a_N a_{N-1} \cdots a_1 a_0$ と並べて書いて，これを x の p **進法表示**という．

証明. $x = px_1 + a_0$, $0 \leqq a_0 < p$ を満たす $x_1, a_0 \in \mathbb{N}_0$ が存在する．$x_1 = 0$ ならば，$N=0$ で終わり．ここから x に関する帰納法を始める．$x=1$ の場合は上で証明されている．さて，$x_1 \neq 0$ の場合を考える．$x_1 < x$ だから，帰納法の仮定から，次がわかる．

$y_0 = x_1$ とし，帰納的に y_n を p で割った商を y_{n+1}, 余りを b_n とする．このとき，ある非負整数 M に対して $y_{M+1}=0$ となる．また，

$$y_0 = b_0 + b_1 p + b_2 p^2 + b_3 p^3 + \cdots + b_M p^M$$

$(b_M \neq 0)$ となる．a_i, b_i は

$$x_i = px_{i+1} + a_i \quad (0 \leqq a_i < p)$$
$$y_i = py_{i+1} + b_i \quad (0 \leqq b_i < p)$$

で定義されている．定理&定義 9.8 を用いると，i に関する帰納法で，$x_{i+1} = y_i$, $a_{i+1} = b_i$ となることが容易に証明できる．よって，

$$x_1 = a_1 + a_2 p + a_3 p^2 + a_4 p^3 + \cdots + a_M p^M$$

となり，これを $x = px_1 + a_0$ に代入して整理すると，$N = M+1$ として，

$$x = a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots + a_N p^N$$

$(a_N \neq 0)$ が得られる．
□

10. 整数

整数全体の集合 $\mathbb{Z}$ を定義する方法としては，負の整数全体の集合 $(-\mathbb{N}) := \{-n \mid n \in \mathbb{N}\}$ を定義して，$\mathbb{Z} := \mathbb{N}_0 \sqcup (-\mathbb{N})$ とする素朴な方法もある．この場合，和や積を定義した後に，結合法則などの諸性質を証明するときに，場合分けが多くなって繁雑になる．そこで，その方法はやめて，$a-b$ $(a, b \in \mathbb{N}_0)$ という形の元全体の集合として $\mathbb{Z}$ を定義する．厳密には，以下の定義になる．

定義&命題 10.1. 直積集合 $A := \mathbb{N}_0 \times \mathbb{N}_0$ 上に関係 $\sim$ を，

$$(a, b) \sim (a', b') \iff a + b' = a' + b$$

として定義する．$\sim$ は同値関係である．

$\mathbb{Z} := (\mathbb{N}_0 \times \mathbb{N}_0)/\sim$ と定義し，$(a, b) \in \mathbb{N}_0 \times \mathbb{N}_0$ の $\sim$ による同値類を $[a, b]$ と表すことにする．「$[a, b] = [c, d] \Longrightarrow a + d = c + b$」である．$\mathbb{Z}$ 上で，$+, -, \times, <$ を定義したいが，$\mathbb{N}$ 上での $+, -, \times, <$ と混同しないように，しばらく慣れるまで，$\mathbb{Z}$ 上での $+, -, \times, <$ は，$\otimes, \ominus, \otimes, \prec$ と別の記号で書く．定義は以下の通りである．

(1) $[a, b] \oplus [c, d] = [a + c, b + d]$.
(2) $[a, b] \ominus [c, d] = [a + d, b + c]$.
(3) $[a, b] \otimes [c, d] = [ac + bd, ad + bc]$.
(4) $[a, b] \prec [c, d] \iff a + d < b + c$.

これは代表元の選び方に依存せずに，矛盾なく定義されている．また $x \times y$ は xy とか $x \cdot y$ とも書く．

証明. ($\sim$ が同値関係であること) 推移律を証明する．$(a_1, b_1) \sim (a_2, b_2)$ かつ $(a_2, b_2) \sim (a_3, b_3)$ とする．$a_1 + b_2 = a_2 + b_1$ かつ $a_2 + b_3 = a_3 + b_2$ だから，辺々加えて $(a_1 + b_3) + (a_2 + b_2) = (a_3 + b_1) + (a_2 + b_2)$ となり，これより $a_1 + b_3 = a_3 + b_1$ が導かれて $(a_1, b_1) \sim (a_3, b_3)$ となる．反射律と対称律は自明．

(代表元の選び方に依存せずに矛盾なく定義されていること)

(3) を証明する．$[a,b]=[a',b']$, $[c,d]=[c',d']$ のとき，$[ac+bd,\, ad+bc]=[a'c'+b'd',\, a'd'+b'c']$ が成り立つことを証明すればよい．つまり，$(ac+bd)+(a'd'+b'c')=(ad+bc)+(a'c'+b'd')$ —① を導く．仮定から $a+b'=a'+b$ —②，$c+d'=c'+d$ —③ である．② の両辺に c を掛けた式 $ac+b'c=bc+a'c$ —④，② の両辺を入れ替えた式に d を掛けた式 $bd+a'd=ad+b'd$ —⑤，③ の両辺に c を掛けた式 $a'c+a'd'=a'd+a'c'$ —⑥，② の両辺を入れ替えた式に b' を掛けた式 $b'd+b'c'=b'c+b'd'$ —⑦ を作って ④〜⑦ を辺々足すと

$$(ac+bd+a'd'+b'c')+(b'c+a'd+a'c+b'd)=(ad+bc+a'c'+b'd')+(a'c+b'd+a'd+b'c)$$

が得られる．後のカッコをキャンセルすると ① が得られる．

(1), (2), (4) は簡単なので省略する． □

定義&命題 10.2. $a\in\mathbb{N}_0$ に対し $\varphi(a)=[a,\,0]\in\mathbb{Z}$ として写像 $\varphi\colon\mathbb{N}_0\to\mathbb{Z}$ を定義する．すると φ は単射で，任意の $a,\,b\in\mathbb{N}_0$ に対して以下が成り立つ．

(1) $\varphi(a+b)=\varphi(a)\oplus\varphi(b)$. また $a\geqq b$ のとき $\varphi(a-b)=\varphi(a)\ominus\varphi(b)$.

(2) $\varphi(ab)=\varphi(a)\otimes\varphi(b)$.

(3) $a<b\iff\varphi(a)\prec\varphi(b)$.

そこで，$a\in\mathbb{N}_0$ と $\varphi(a)=[a,\,0]\in\mathbb{Z}$ を同じ元とみなして，$[a,\,0]$ を単に $a\in\mathbb{Z}$ と書くことにし，$\mathbb{N}_0\subset\mathbb{Z}$ と考える．

証明. $\varphi(a)=\varphi(b)$ ならば $[a,\,0]=[b,\,0]$ だから $a=a+0=b+0=b$ となり，φ は単射である．

(1), (2), (3) も簡単. □

$a\in\mathbb{N}$ に対し $[0,\,a]\in\mathbb{Z}$ を $-a$ と書くことにし，このような形の元を**負の整数**という．なお，負の整数 x ($x\in\mathbb{Z},\,x\prec 0$) に対しては，ある $a\in\mathbb{N}$ によって $x=[0,\,a]$ と書けるので，$-x=[a,\,0]\in\mathbb{Z}$ と定義する．$\mathbb{N}$ で考えれば $-x=a\in\mathbb{N}$ である．また，$-0=0$ と定義する．

$\mathbb{Z}$ 上の $\otimes,\,\ominus,\,\otimes,\,\prec$ と $\mathbb{N}$ 上の $+,\,-,\,\times,\,<$ を区別する必要がなくなったので，ここから先は，$\otimes,\,\ominus,\,\otimes,\,\prec$ を $+,\,-,\,\times,\,<$ という普通の記号で表す．$a,\,b\in\mathbb{N}_0$ に対し，

$$[a,b]=[a+0,\,0+b]=[a,0]\ominus[b,0]=a\ominus b=a-b$$

である．また，$0-a=[0,\,0]\ominus[a,\,0]=[0,\,a]=-a$ であり，$0-(-a)=[0,\,0]\ominus[0,\,a]=[a,\,0]=a$ である．両方あわせて，$-(-a)=a$ も得られる．

定理 10.3. $x,\,y,\,z\in\mathbb{Z}$ に対し以下が成り立つ．

(1) (結合法則) $(x+y)+z=x+(y+z)$, $(xy)z=x(yz)$.

(2) (交換法則) $y+x=x+y$, $yx=xy$.

(3) (単位元の存在) $x+0=x$, $1\times x=x$,

(4) (加法の逆元の存在) $x+(-x)=0$.

(5) (分配法則) $x(y+z)=xy+xz$.

(6) $x<y$ ならば $x+z<y+z$.

(7) $x<y$, $0<z$ ならば $xz<yz$.

(8) $xy=0$ ならば $x=0$ または $y=0$.

証明. $x=a-b$, $y=c-d$, $z=e-f$ ($a,\,b,\,c,\,d,\,e,\,f\in\mathbb{N}_0$) とする．

(1) の $(xy)z=x(yz)$ を示す．定義 10.1 の積の定義より，

$$\begin{aligned}(xy)z&=((a-b)(c-d))(e-f)=((ac+bd)-(ad+bc))(e-f)\\&=(ace+adf+bcf+bde)-(acf+ade+bcd+bdf)\\&=(a-b)((ce+df)-(cf+de))=(a-b)((c-d)(e-f))\\&=x(yz)\end{aligned}$$

である．(1) 〜 (5) の他の性質はもっと簡単に証明できる．

(7) を示す．$x < y$ ならば $<$ の定義から $a+d < b+c$ である．$0 < z$ ならば $z = e-0$ $(e \in \mathbb{N})$ と仮定してよい．よって，$ae+de < be+ce$ であるが，$xz = (a-b)(e-0) = ae-be$, $yz = (c-d)(e-0) = ce-de$ なので，これは $xz < yz$ を意味する．

(6) は (7) より簡単．

(8) を示す．(7) より，$x > 0, y > 0$ ならば $xy > 0$ であり，$x > 0, y < 0$ ならば $xy < 0$，$x < 0, y > 0$ ならば $xy < 0$，$x < 0, y < 0$ ならば $xy > 0$ が得られる．対偶をとると $xy = 0$ ならば $x = 0$ または $y = 0$ でなければならない． □

一般に集合 R に加法 $+$ と乗法 $\times$ が定義されていて，$0, 1 \in R$ で，任意の $x, y, z \in R$ に対して，上の定理の (1), (2), (3), (4), (5) が成り立つとき，R は**可換環**であるという．さらに (8) が成り立つとき，R は**整域**であるという．整域 R 上に全順序 $\leqq$ が定義されていて，$0 < 1$ であって，上の定理の (6), (7) を満たすとき，R は**順序整域**であるという．上の定理は $\mathbb{Z}$ は順序整域であることを意味している．

問 10.4. $x, y, z \in \mathbb{Z}$ とする．上で定義した減法は以下の性質を満たすことを証明せよ．

(1) $(x-y)-z = x-(y+z)$.

(2) $x-(y-z) = (x-y)+z = (x+z)-y$.

定理&定義 10.5. $n \in \mathbb{Z}, m \in \mathbb{N}$ とすると，$n = mq+r, 0 \leqq r < m$ を満たす $q, r \in \mathbb{Z}$ が一意的に存在する．このとき，n を m で割った**商**は q, **余り**は r であるという．$r = 0$ のとき n は m の**倍数**であるといい，m は n の**約数**であるという．

証明. $n \in \mathbb{N}_0$ の場合は定理&定義 9.8 で証明したから，$n < 0$ の場合に証明すればよい．$-n \in \mathbb{N}_0$ だから，$-n$ を m で割った商を q', 余りを r' とする．$-n = mq'+r'$ $(0 \leqq r' < m)$ である．

$r' > 0$ の場合は，$q = 1-q', r = m-r'$ とおくと，$n = mq+r$ $(0 \leqq r < m)$ が成り立つ．

$r' = 0$ の場合は $q = -q', r = 0$ とおけばよい． □

定義 10.6. $n_1,\ldots, n_r \in \mathbb{Z}$ に対し，$d \in \mathbb{N}$ がすべての $i = 1,\ldots, r$ に対して n_i の約数であるとき，d は $n_1,\ldots, n_r$ の**公約数**であるという．$n_1,\ldots, n_r$ の公約数の中で最大なものを，$n_1,\ldots, n_r$ の**最大公約数**といい，$\mathrm{GCD}(n_1,\ldots, n_r)$ で表す．$\mathrm{GCD}(n_1, n_2) = 1$ のとき，n_1 と n_2 は**互いに素**であるという．

$m \in \mathbb{Z}$ がすべての $i = 1,\ldots, r$ に対して n_i の倍数であるとき，m は $n_1,\ldots, n_r$ の**公倍数**であるという．$n_1,\ldots, n_r$ の正の公倍数の中で最小なものを，$n_1,\ldots, n_r$ の**最小公倍数**といい，$\mathrm{LCM}(n_1,\ldots, n_r)$ で表す．

p が 2 以上の自然数で，p の約数であるような自然数が 1 と p 以外に存在しないとき，p は**素数**であるという．

定義 10.7. 可換環 R の空でない部分集合 I が，以下の (1), (2) を満たすとき，R は I の**イデアル**であるという．

(1) $x, y \in I$ ならば $x+y \in I$.

(2) $a \in R, x \in I$ ならば $ax \in I$.

$x_1,\ldots, x_n \in R$ のとき，

$$Rx_1+\cdots+Rx_n := \left\{a_1x_1+\cdots+a_nx_n \in R \;\middle|\; a_1,\ldots, a_n \in R\right\}$$

とおくと，$Rx_1+\cdots+Rx_n$ は R のイデアルになる．これを $x_1,\ldots, x_n$ で**生成される** R のイデアルという．$Rx_1+\cdots+Rx_n$ は誤解の恐れがなければ $(x_1,\ldots, x_n)$ などとも書かれる．また，$x_1R+\cdots+x_nR$ とも書く．

定理 10.8. I が $\mathbb{Z}$ のイデアルならば，ある $x \in \mathbb{Z}$ が存在して，$I = \mathbb{Z}x$ となる．

証明. $I = \{0\}$ ならば $x = 0$ とすればよいので，$I \neq \{0\}, y \neq 0$ とする．$I \neq 0$ だから $y \in I$ を取る，(2) より $0y \in I$ だから $0 \in I$ である．$-1 \in \mathbb{Z}$ だから $-y = (-1)y \in I$ である．よって，$y > 0$ と仮定してよい．

I に含まれる自然数の中で，最小の正の数を d とする．$I \supset \mathbb{Z}d$ はすぐわかる．もし，$\exists x \in I-\mathbb{Z}d$ とすると x を d で割った余りが I に属し，d の最小性に矛盾する．よって，$I = \mathbb{Z}d$ である． □

定理 10.9. $a, b \in \mathbb{Z}$ で，$\mathrm{GCD}(a, b) = 1$ ならば，$ax + by = 1$ を満たす整数 $x, y \in \mathbb{Z}$ が存在する．

証明. $I = \mathbb{Z}a + \mathbb{Z}b$ は $\mathbb{Z}$ のイデアルである．前定理から，ある $d \in \mathbb{N}$ により $I = \mathbb{Z}d$ と書ける．$a, b \in \mathbb{Z}d$ であるから，a, b は d の倍数で，d は a, b の公約数である．よって $d = 1$ となる．I の定義から $ax + by = 1$ を満たす整数 x, y が存在する． □

定理 10.10. $a_1, \ldots, a_n \in \mathbb{Z}$ で $a_1 a_2 \cdots a_n$ が素数 p の倍数ならば，ある $1 \leqq i \leqq n$ に対して a_i は p の倍数である．

証明. $n = 2$ の場合に，$a, b \in \mathbb{Z}$ で ab が素数 p の倍数ならば，a か b は p の倍数であることを証明する．

a は p の倍数でないと仮定する．d は a と p の公約数とする．p の約数は 1 と p のみであって，p は a の約数でないから，$d = 1$ である．すると，$ax + py = 1$ を満たす整数 x, y が存在する．ab は p の倍数なので，$ab = pk$ $(\exists k \in \mathbb{Z})$ と書ける．$pkx = axb = (1 - py)b = b - pby$ なので，$b = pkx + pby = p(kx + by)$ とかけ，b は p の倍数である．

$n \geqq 3$ の場合は，n に関する帰納法で，$n = 2$ の場合の結果からすぐ証明できる． □

定理 10.11. $x \in \mathbb{N}$ で $x \geqq 2$ 以上の整数とする．すると，ある $r, e_1, e_2, \ldots, e_r \in \mathbb{N}$ と素数 $p_1, p_2, \ldots, p_r$ (ただし $p_1 < p_2 < \cdots < p_r$ とする) が存在して，

$$x = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$$

と表せる．さらに，自然数 $r, e_1, e_2, \ldots, e_r$ と素数 $p_1 < p_2 < \cdots < p_r$ は x に対して一意的に定まる．これを x の**素因数分解**という．

証明. (1) 素因数分解可能であることを証明する．

x に関する帰納法で証明する．x が素数 ($x = 2$ の場合を含む) なら，それが素因数分解である．x が素数でなければ，$x = ab$ (a, b は 2 以上の整数) と因数分解できる．$a < x, b < x$ だから，帰納法の仮定から，a, b は素数の積で表せる．よって，x の素数の積で表せる．

(2) 素因数分解の一意性を証明する．

$p_1 < p_2 < \cdots < p_r$ は素数，$q_1 < q_2 < \cdots < q_s$ も素数で，$e_i, f_i \in \mathbb{N}$ とし，

$$p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} = q_1^{f_1} q_2^{f_2} \cdots q_s^{f_s} \qquad ①$$

であったと仮定する．$e_1 + \cdots + e_r$ に関する帰納法で，$r = s, p_1 = q_1, \ldots, p_r = q_r; e_1 = f_1, \ldots, e_r = f_r$ であることを証明する．前定理より，ある $1 \leqq j \leqq s$ が存在して q_j は p_r の倍数である．q_j の 1 以外の約数は q_j しかないので $p_r = q_j$ である．同様に，$q_s = p_i$ となる $1 \leqq i \leqq r$ が存在するが，$p_r \geqq p_i = q_s \geqq q_j = p_r$ より，$i = r, j = s$ である．e_r に関する帰納法で $f_s = e_r$ はすぐ証明できる．① の両辺を $p_r = q_s$ で割ると，

$$p_1^{e_1} p_2^{e_2} \cdots p_{r-1}^{e_{r-1}} p_r^{e_r - 1} = q_1^{f_1} q_2^{f_2} \cdots q_s^{f_{s-1}} q_s^{f_s - 1} \qquad ②$$

となる．

$e_1 + \cdots + e_r = 1$ の場合は $r = 1, e_1 = 1$ だから，② の左辺が 1 になるから，$s = 1, f_s = f_1 = 1$ となる．$r \geqq 2$ の場合は，帰納法の仮定から $r = s, p_1 = q_1, \ldots, p_r = q_r; e_1 = f_1, \ldots, e_r = f_r$ が導かれる． □

11. 有理数

定義&命題 11.1. 直積集合 $A := \mathbb{Z} \times \mathbb{N}$ 上に関係 $\sim$ を，

$$(a, b) \sim (a', b') \iff ab' = a'b$$

として定義する．$\sim$ は同値関係である．

$\mathbb{Q} := (\mathbb{Z} \times \mathbb{N})/\sim$ と定義し，$(a, b) \in \mathbb{Z} \times \mathbb{N}$ の $\sim$ による同値類を $\dfrac{a}{b}$ とか a/b と表す．$\mathbb{Q}$ 上で，$+$, $-$, $\times$, $\leqq$ を以下のように定める．

(1) $\dfrac{a}{b} + \dfrac{c}{d} = \dfrac{ad + bc}{bd}$.

(2) $\dfrac{a}{b} - \dfrac{c}{d} = \dfrac{ad-bc}{bd}$.
(3) $\dfrac{a}{b} \times \dfrac{c}{d} = \dfrac{ac}{bd}$.
(4) $\dfrac{a}{b} < \dfrac{c}{d}$. $\Longleftrightarrow ad < bc$.
これは代表元の選び方に依存せずに，矛盾なく定義されている．また $x \times y$ は xy とか $x \cdot y$ とも書く．

証明. $\sim$ が同値関係であることの証明は $\mathbb{Z}$ の場合と同様である．
代表元の選び方に依存せずに矛盾なく定義されていることの証明も，中学からの勉強の通りである． □

定義&命題 11.2. $a \in \mathbb{Z}$ に対し $\varphi(a) = \dfrac{a}{1} \in \mathbb{Q}$ として写像 $\varphi\colon \mathbb{Z} \to \mathbb{Q}$ を定義する．すると φ は単射で，任意の $a, b \in \mathbb{Z}$ に対して以下が成り立つ．
(1) $\varphi(a+b) = \varphi(a) + \varphi(b)$.
(2) $\varphi(ab) = \varphi(a)\varphi(b)$.
(3) $a < b \Longleftrightarrow \varphi(a) < \varphi(b)$.
そこで，$a \in \mathbb{Z}$ と $\varphi(a) \in \mathbb{Q}$ を同じ元とみなして $\mathbb{Z} \subset \mathbb{Q}$ と考える．

証明. 簡単． □

定義 11.3. 一般に R が整域であって，$0 \neq 1$ であり，任意の $x \in R$, $x \neq 0$ に対しで $xy = 1$ を満たす $y \in R$ が存在するとき，R は**体**であるという．$xy = 1$ を満たす y を $y = x^{-1}$ とか $1/x$ とか $\dfrac{1}{x}$ と書く．R が体であって順序整域であるとき，**順序体**であるという．

定理 11.4. $\mathbb{Q}$ は順序体である．

証明. 通分して $\mathbb{Z}$ の性質に帰着するなどして，簡単に証明できる． □

定理 11.5. $x \in \mathbb{Q}$ に対し，$n \leqq x < n+1$ を満たすような整数 $n \in \mathbb{Z}$ が一意的に存在する．この n を $n = \lfloor x \rfloor$ を書く．昔は，$\lfloor x \rfloor$ を $[x]$ と書き，**ガウスの括弧**と読んでいたが，大括弧と区別しやすいので，最近は前者の記号が主流になっている．参考までに，$n-1 < x \leqq n$ を満たす整数 n を $\lceil x \rceil$ と書く．$\lfloor x \rfloor$ を **floor 関数**，$\lceil c \rceil$ を **ceil 関数**という．

証明. (存在) $x = \dfrac{b}{a}$ $(a \in \mathbb{N}, b \in \mathbb{Z})$ と表す．定理&定義 10.5 より $b = aq + r$ $(\exists q, r \in \mathbb{Z}, 0 \leqq r < a)$ と書ける．$0 \leqq r < a$ より，有理数の大小関係の定義にもどると，$0 \leqq \dfrac{r}{a} < 1$ がわかる．よって，$q \leqq q + \dfrac{r}{a} = \dfrac{b}{a} < q+1$ である．そこで，$n = q$ とおけばよい．
(一意性) $n \leqq x < n+1$, $m \leqq x < m+1$ $(m, n \in \mathbb{Z})$ ならば $m = n$ を示す．対称性から $m \leqq n$ と仮定してよい．もし $m \neq n$ ならば $m < n$ である．以前示したように，$m+1 \leqq n$ である．すると，$m+1 \leqq n \leqq x < m+1$ で，$m+1 < m+1$ となって矛盾する． □

定理 11.6. p は 2 以上の整数，x は $0 < x < 1$ を満たす有理数とする．$\lfloor p^n x \rfloor$ を p で割った余りを a_n とおく．もし，ある $N \in \mathbb{N}$ が存在して $n > N$ のとき $a_n = 0$ であるならば，

$$x = \frac{a_1}{p} + \frac{a_2}{p^2} + \cdots + \frac{a_N}{p^N}$$

が成り立つ．このとき，$x = 0.a_1 a_2 \cdots a_N$ と数字を並べて表わし，これを有理数 x の p 進小数表示という．

証明. (1) $\lfloor p^n x \rfloor$ を p で割った商を q_n とする．$\lfloor p^n x \rfloor = pq_n + a_n$ $(0 \leqq a_n < 1)$ である．$0 < p^1 x < p$ だから $q_1 := 0$ である．$n \geqq 2$ のとき

$$q_n = a_1 p^{n-2} + a_2 p^{n-3} + \cdots + a_{n-1} \qquad ①$$

が成り立つことを n に関する帰納法で証明する．$q_n = a_1p^{n-2} + a_2p^{n-3} + \cdots + a_{n-1}$ ($n \geqq 2$, ($n = 1$ の場合は $q_1 = 0$) を仮定する．$\lfloor p^n x \rfloor = pq_n + a_n$ なので，$pq_n + a_n \leqq p^n x < pq_n + a_n + 1$ である．書き換えると，

$$a_1p^{n-1} + a_2p^{n-2} + \cdots + a_{n-1}p + a_n \leqq p^n x < a_1p^{n-1} + a_2p^{n-2} + \cdots + a_{n-1}p + a_n + 1$$

である．$q'_{n+1} := pq_n + a_n = a_1p^{n-1} + a_2p^{n-2} + \cdots + a_n$ とおくと，$q'_{n+1} \leqq p^n x < q'_{n+1} + 1$ である．よって，$pq'_{n+1} \leqq p^{n+1}x < pq'_{n+1} + p$ である．

$\lfloor p^{n+1}x \rfloor = pq_{n+1} + a_{n+1}$ ($0 \leqq a_{n+1} < p$) であったので，$pq_{n+1} + a_{n+1} \leqq p^{n+1}x < pq_{n+1} + a_{n+1} + 1$ である．$k \leqq p^{n+1}x$ を満たす最大の整数 k は $k = pq_{n+1} + a_{n+1}$ で，pq'_{n+1} は整数で $pq'_{n+1} \leqq p^{n+1}x$ を満たすので，$pq'_{n+1} \leqq k = pq_{n+1} + a_{n+1}$ である．よって，$q_{n+1} \geqq q'_{n+1} - \dfrac{a_{n+1}}{p}$ である．特に，$q_{n+1} \geqq q'_{n+1}$ — ②である．

$l > p^{n+1}x$ を満たす最小の整数 l は $l = pq_{n+1} + a_{n+1} + 1$ で，$pq'_{n+1} + p$ は整数で $pq'_{n+1} + p > p^{n+1}x$ を満たすので，$pq'_{n+1} + p \geqq l = pq_{n+1} + a_{n+1} + 1$ である．よって，$q'_{n+1} + 1 \geqq q_{n+1} + \dfrac{a_{n+1}+1}{p}$ である．$0 \leqq 1 - \dfrac{a_{n+1}+1}{p} < 1$ なので，$q'_{n+1} \geqq q_{n+1}$ である．②とあわせて，$q'_{n+1} = q_{n+1}$ となる．

また，今の証明から $q_{n+1} \leqq p^n x < q_{n+1} + 1$ — ③が成り立つ．

(2) $x_n := \dfrac{q_{n+1}}{p^n} = \dfrac{a_1}{p} + \dfrac{a_2}{p^2} + \cdots + \dfrac{a_n}{p^n}$ とおく．$n > N$ ならば $a_n = 0$ なので，$x_{N+1} = x_{N+2} = x_{N+3} = \cdots$ である．そこで，$y = x_{N+1} \in \mathbb{Q}$ とおく．③より，$x_n \leqq x < x_n + \dfrac{1}{p^n}$ である．$n > N$ ならば $y \leqq x < y + \dfrac{1}{p^n}$ が成り立つ．もし $x \neq y$ ならば $y \leqq x$ だから $z := y - x > 0$ である．$z \in \mathbb{Q}$ だから $p^n > 1/z$ を満たす n が存在する．$n > N$ と仮定してよい．$\dfrac{1}{p^n} < z$ であるが，$x = y + z < y + \dfrac{1}{p^n}$ より $z < \dfrac{1}{p^n}$ であって，矛盾する．よって，$x = y$ である． □

無限小数の話は，次回扱う数列の極限の初歩的な部分を使わないと扱えないが，$0 < |x| < 1$ を満たす有理数 x (公式自体は x が実数や複素数でもよい) に対し，

$$\sum_{n=0}^{\infty} x^n = \lim_{k\to\infty} \sum_{n=0}^{k} x^n = \frac{1}{1-x}$$

が成り立つことを認めて，有限小数で表わせない有理数は循環小数になることを説明しておく．

定理 11.7. 前定理で，x が有限小数で表わせない場合を考える．すると，ある正の整数 l_0 と正の整数 r が存在して，$n \geqq l_0$ ならば $a_{n+r} = a_n$ が成り立つ．このような小数を周期 r の**循環小数**という．

証明. (1) まず，$x = \dfrac{c}{p^r - 1}$ ($c, r \in \mathbb{N}$) の場合に証明する．c を $p^r - 1$ で割った商を q, 余りを c_0 とすると，x の小数部分は $c_0/(p^r - 1)$ の小数部分に等しいので，c の代わりに c_0 を考えることにより，最初から $0 < c < p^r - 1$ と仮定してよい．

この講義ではまだ証明していない等式であるが，$\displaystyle\sum_{i=1}^{\infty} \frac{1}{p^{ir}} = \frac{1}{p^r - 1}$ であることを用いると，

$$x = \frac{c}{p^r - 1} = \sum_{i=1}^{\infty} \frac{c}{p^{ir}}$$

となる．これは，小数点以下を r 桁毎に区切ってみると，c を p 進法で展開した整数の列が繰り返し現れることを意味する．つまり，c は周期 r の循環小数で表せる．

(2) x が $0 < x < 1$ を満たす一般の有理数の場合に証明すれば十分である．$q_1 = 0$, $q_n = a_1p^{n-2} + a_2p^{n-3} + \cdots + a_{n-1}$ ($n \geqq 2$) とおくと，$\dfrac{q_{n+1}}{p^n} \leqq x < \dfrac{q_{n+1}}{p^n} + \dfrac{1}{p^n}$ であった．$x = \dfrac{b}{a}$ ($a, b \in \mathbb{N}$) とおく．

$0 < x < 1$ だから $0 < b < a$ である．$0 \leqq \dfrac{b}{a} - \dfrac{q_{n+1}}{p^n} < \dfrac{1}{p^n}$ で $\dfrac{b}{a} - \dfrac{q_{n+1}}{p^n} = \dfrac{bp^n - aq_{n+1}}{p^n a}$ なので，$0 \leqq bp^n - aq_{n+1} < a$ である $c_n := bp^n - aq_{n+1} < a$ とおく．もし $c_n = 0$ だと $\dfrac{b}{a} = \dfrac{q_{n+1}}{p^n} + \dfrac{c_n}{p^n a} = \dfrac{q_{n+1}}{p^n}$ は有限小数になり仮定に反するので，$1 \leqq c_n \leqq a - 1$ である．**鳩の巣原理**から $c_n = c_m$, $n < m$ を満たす $n, m \in \mathbb{N}$ が存在する．$r := m - n$ とおく．

$k \geqq n$ のとき，$a_{k+r} = a_k$ が成り立つことを証明する．$c_{k+r} = c_r$ なので，$bp^{k+r} - aq_{k+r+1} = bp^k - aq_{k+1}$ である．これより，

$$x = \frac{b}{a} = \frac{1}{p^k} \cdot \frac{q_{k+r+1} - q_{k+1}}{p^r - 1}$$

が成り立つ．(1) で示したことから，$\dfrac{q_{k+r+1} - q_{k+1}}{p^r - 1}$ の周期 r の循環小数で表せるので，x も周期 r の循環小数になる． □

問 11.8. $x = \dfrac{b}{a} \in \mathbb{Q}$ ($a \in \mathbb{N}$, $b \in \mathbb{Z}$ で $\mathrm{GCD}(a, b) = 1$) が十進小数で表したとき有限小数になるとする．すると，$a = 2^r \times 5^s$ ($r, s \in \mathbb{N}_0$) と表せることを証明せよ．

定義 11.9.(オーダー, 位数) $p \in \mathbb{N}$ は素数とする．$0 \neq n \in \mathbb{Z}$ に対し，素因数分解の存在とその一意性で証明したことから「n は p^e の倍数であり，かつ，n は p^{e+1} の倍数ではない」という性質を満たす $e \in \mathbb{N}_0$ が存在する．この e を $e = \mathrm{ord}_p\, n$ と書き，p に関する n の**オーダー**という．また，$\mathrm{ord}_p\, 0 = +\infty$ と約束しておく．ただし，$+\infty$ は $\mathbb{Q}$ 属さない元で，集合 $\mathbb{Q} \cup \{+\infty\}$ においては，任意の $x \in \mathbb{Q}$ に対し $x < +\infty$ であるとして順序を定める．また，任意の $x \in \mathbb{Q} \cup \{+\infty\}$ に対し $x + (+\infty) = +\infty$ であると約束しておく．

さらに，有理数 $x = \dfrac{a}{b}$ ($0 \neq a \in \mathbb{Z}$, $b \in \mathbb{N}$ に対し，$\mathrm{ord}_p\, x = \mathrm{ord}_p\, a - \mathrm{ord}_p\, b$ と定義する．

定理 11.10. 上の $\mathrm{ord}_p\, x = \mathrm{ord}_p\, a - \mathrm{ord}_p\, b$ の定義は，$x \in \mathbb{Q}$ の分数の表示法に依存しない．つまり，$\dfrac{a}{b} = \dfrac{c}{d}$ ($a, b, c, d \in \mathbb{Z}$) ならば，$\mathrm{ord}_p\, a - \mathrm{ord}_p\, b = \mathrm{ord}_p\, c - \mathrm{ord}_p\, d$ である．

証明. まず，$a, b \in \mathbb{Z}$ の場合に $\mathrm{ord}_p\, ab = \mathrm{ord}_p\, a + \mathrm{ord}_p\, b$ が成り立つことを証明する．

$a < 0$ のとき $\mathrm{ord}_p(-a) = \mathrm{ord}_p\, a$ だから，$a \geqq 0$, $b \geqq 0$ と仮定してよい．$\mathrm{ord}_p\, 0 = +\infty$ だから，$a = 0$ または $b = 0$ のときは，$+\infty + x = +\infty$ ($x \in \mathbb{N} \cup \{0, +\infty\}$) より $\mathrm{ord}_p\, ab = \mathrm{ord}_p\, a + \mathrm{ord}_p\, b$ が成り立つ．

以下，$a, b \in \mathbb{N}$ の場合を考える．相異なる素数 $p_1, \ldots, p_r$ により，$a = p_1^{e_1} \cdots p_r^{e_r}$, $b = p_1^{f_1} \cdots p_r^{f_r}$ と書ける．ここで，$e_1, \ldots, e_r$, $f_1, \ldots, f_r$ は非負整数である．もし，$p = p_i$ ならば $\mathrm{ord}_p\, a = e_i$, $\mathrm{ord}_p\, b = f_i$ である．$ab = p_1^{e_1+f_1} \cdots p_r^{e_r+f_r}$ だから，$\mathrm{ord}_p\, ab = e_i + f_i$ である．よって，$\mathrm{ord}_p\, ab = e_i + f_i = \mathrm{ord}_p\, a + \mathrm{ord}_p\, b$ である．

$p \notin \{p_1, \ldots, p_r\}$ のときは，$\mathrm{ord}_p\, a = 0$, $\mathrm{ord}_p\, b = 0$, $\mathrm{ord}_p\, ab = 0$ だから，$\mathrm{ord}_p\, ab = 0 = \mathrm{ord}_p\, a + \mathrm{ord}_p\, b$ である．

(2) 本題を証明する．$\dfrac{a}{b} = \dfrac{c}{d}$ ($a, c \in \mathbb{Z}$, $b, d \in \mathbb{Z}$) とする．$ad = bc$ であるので，$\mathrm{ord}_p\, ad = \mathrm{ord}_p\, bc$ である．(1) より，$\mathrm{ord}_p\, a + \mathrm{ord}_p\, d = \mathrm{ord}_p\, b + \mathrm{ord}_p\, c$ である．よって，$\mathrm{ord}_p\, a - \mathrm{ord}_p\, b = \mathrm{ord}_p\, c - \mathrm{ord}_p\, d$ である． □

定理 11.11. $x, y \in \mathbb{Q}$ のとき，以下が成り立つ．

(1) $\mathrm{ord}_p(xy) = \mathrm{ord}_p\, x + \mathrm{ord}_p\, y$, $\mathrm{ord}_p \dfrac{x}{y} = \mathrm{ord}_p\, x - \mathrm{ord}_p\, y$.

(2) $\mathrm{ord}_p\, x < \mathrm{ord}_p\, y$ ならば $\mathrm{ord}_p(x + y) = \mathrm{ord}_p\, x$

(3) $\mathrm{ord}_p(x + y) \geqq \min\{\mathrm{ord}_p\, x, \mathrm{ord}_p\, y\}$

証明. $x = \dfrac{a}{b}$, $y = \dfrac{c}{d}$, ($a, c \in \mathbb{Z}$, $b, d \in \mathbb{N}$) とおく．

(1) $\mathrm{ord}_p(xy) = \mathrm{ord}_p\, ac - \mathrm{ord}_p\, bd = (\mathrm{ord}_p\, a - \mathrm{ord}_p\, b) + (\mathrm{ord}_p\, c - \mathrm{ord}_p\, d) = \mathrm{ord}_p\, x + \mathrm{ord}_p\, y$.

$\mathrm{ord}_p \dfrac{x}{y} = \mathrm{ord}_p \dfrac{ad}{bc} = \mathrm{ord}_p\, ad - \mathrm{ord}_p\, bc = (\mathrm{ord}_p\, a - \mathrm{ord}_p\, b) + (\mathrm{ord}_p\, d - \mathrm{ord}_p\, c) = \mathrm{ord}_p\, x - \mathrm{ord}_p\, y$.

(2) (i) まず，$m, n \in \mathbb{N}$, $\mathrm{ord}_p\, m < \mathrm{ord}_p\, n$ ならば $\mathrm{ord}_p(m+n) = \mathrm{ord}_p\, m$ を示す．

$r = \mathrm{ord}_p\, m$, $s = \mathrm{ord}_p\, n$ とおくと，$m = p^r m'$, $n = p^s n'$ (m', n' は p の倍数でない自然数) と書ける．$r < s$ だから，$m + n = p^r(m' + p^{s-r}n')$ である．$p^{s-r}n'$ は p の倍数で m' は p の倍数でないから，$m' + p^{s-r}n'$ は p の倍数でない．よって，$\mathrm{ord}_p(m+n) = r = \mathrm{ord}_p\, m$ である．

(ii) $m, n \in \mathbb{Z}$ の場合も，$\mathrm{ord}_p(-m) = \mathrm{ord}_p\, m$, $\mathrm{ord}_p\, 0 = +\infty$ からすぐわかる．

(iii) 本題を証明する．$\mathrm{ord}_p\, x < \mathrm{ord}_p\, y$ ならば $\mathrm{ord}_p \dfrac{a}{b} < \mathrm{ord}_p \dfrac{c}{d}$ より，$\mathrm{ord}_p\, ad < \mathrm{ord}_p\, bc$ となる．(ii) より $\mathrm{ord}_p(ad+bc) = \mathrm{ord}_p\, ad$ だから，$\mathrm{ord}_p \dfrac{ad+bc}{bd} = \mathrm{ord}_p \dfrac{ad}{bd}$ である．よって，$\mathrm{ord}_p(x+y) = \mathrm{ord}_p\, x$ である．

(3) $\mathrm{ord}_p\, x < \mathrm{ord}_p\, y$ または $\mathrm{ord}_p\, x > \mathrm{ord}_p\, y$ の場合は，(2) より $\mathrm{ord}_p(x+y) = \min\{\mathrm{ord}_p\, x, \mathrm{ord}_p\, y\}$ である．

以下，$\mathrm{ord}_p\, x = \mathrm{ord}_p\, y$ の場合を考える．上と同様に考えると $\mathrm{ord}_p \dfrac{ad}{bd} = \mathrm{ord}_p \dfrac{bc}{bd}$ なので，$\mathrm{ord}_p\, ad = \mathrm{ord}_p\, bc$ となる．結局，$m, n \in \mathbb{N}$ で $\mathrm{ord}_p\, m = \mathrm{ord}_p\, n$ の場合に $\mathrm{ord}_p(m+n) = \min\{\mathrm{ord}_p\, m, \mathrm{ord}_p\, n\}$ を証明する問題に帰着される．

$r = \mathrm{ord}_p\, m = \mathrm{ord}_p\, n$ とおくと，$m = p^r m'$, $n = p^r n'$ (m', n' は p の倍数でない自然数) と書ける．すると，$m + n = p^r(m' + n')$ だから，$\mathrm{ord}_p(m+n) \geqq r = \min\{\mathrm{ord}_p\, m, \mathrm{ord}_p\, n\}$ である． □

12. $\mathbb{Q}$ の完備化

定義 12.1. 写像 $d\colon \mathbb{Q} \times \mathbb{Q} \longrightarrow \mathbb{Q}$ が次の 3 条件 (1), (2), (3) を満たすとき, d は $\mathbb{Q}$ 上の**距離** (関数) であるという．

(1) (対称性) $x, y \in \mathbb{Q}$ ならば $d(x, y) = d(y, x)$.

(2) (正定値性) $x, y \in \mathbb{Q}$ に対して $d(x, y) \geqq 0$ である．また,「$d(x, y) = 0 \Longleftrightarrow x = y$」が成り立つ．

(3) (三角不等式) $x, y, z \in \mathbb{Q}$ ならば $d(x, z) \leqq d(x, y) + d(y, z)$

定理 12.2. $x, y \in \mathbb{Q}$ とする．

(1) $d_0(x, y) = \bigl|x - y\bigr| \in \mathbb{Q}$ と定める．$d = d_0$ は距離である．

(2) p を素数とし，$d_p(x, y) = p^{-\mathrm{ord}_p(x-y)} \in \mathbb{Q}$ (ただし $x = y$ のときは $d_p(x, y) = 0$) と定める．$d_p(x+y, 0) \leqq \max\bigl\{d_p(x,0), d_p(y,0)\bigr\}$ が成り立つ．さらに，$d = d_p$ は距離である．

(3) $d = d_0$ も $d = d_p$ も，$d(x, y) = d(x - y, 0)$, $d(xy, 0) = d(x, 0)d(y, 0)$ を満たす．

証明. $d = d_0$ の場合は絶対値の性質としてよく知られているので，$d = d_p$ の場合のみ証明する．

(2) $d_p(x+y, 0) \leqq \max\bigl\{d_p(x,0), d_p(y,0)\bigr\}$ は書き換えると $p^{-\mathrm{ord}_p(x-y)} \leqq \max\bigl\{p^{-\mathrm{ord}_p x}, p^{-\mathrm{ord}_p y}\bigr\}$ と同値である．これは，$\mathrm{ord}_p(x-y) \geqq \min\bigl\{\mathrm{ord}_p\, x, \mathrm{ord}_p\, y\bigr\}$ と同値である．これは $\mathrm{ord}_p(-y) = \mathrm{ord}_p\, y$ と定理 11.11 から従う．

(3) $d_p(x, y) = p^{-\mathrm{ord}_p(x-y)} = d(x - y, 0)$, また,

$$d(xy, 0) = p^{-\mathrm{ord}_p(xy)} = p^{-\mathrm{ord}_p x - \mathrm{ord}_p y} = p^{-\mathrm{ord}_p x} p^{-\mathrm{ord}_p y} = d_p(x, 0)d(y, 0)$$

である． □

定義 12.3.(有理数列とその極限) 写像 $f\colon \mathbb{N} \to \mathbb{Q}$ を**有理数列**という．習慣上，$a_n = f(n)$ ($n \in \mathbb{N}$) とおいて，有理数列 f を $\bigl\{a_n\bigr\}$ とか $\bigl\{a_n\bigr\}_{n=1}^{\infty}$ などと書く．

d を $\mathbb{Q}$ 上の 1 つの距離関数とする．有理数列 $\{a_n\}$ が d に関する**基本列** (または**コーシー列**) であるとは，任意の正の有理数 ε に対し，ある自然数 $n(\varepsilon) \in \mathbb{N}$ が存在し，$k \geqq n(\varepsilon)$, $m \geqq n(\varepsilon)$ を満たす任意の自然数 k, m に対し $d(a_k, a_m) < \varepsilon$ が成り立つことをいう．以下，基本列であるような有理数列全体の集合を $\boldsymbol{\mathcal{A}}$ を書くことにする．

$\{a_n\} \in \boldsymbol{\mathcal{A}}$ に対し，ある有理数 a_∞ が存在し，任意の正の有理数 ε に対し，ある自然数 $n(\varepsilon) \in \mathbb{N}$ が存在し，$k \geqq n(\varepsilon)$ を満たす任意の自然数 k に対し $d(a_k, a_\infty) < \varepsilon$ が成り立つことき，$\{a_n\}$ は a_∞ に収束するといい，$\displaystyle\lim_{n\to\infty} a_n = a_\infty$ と書く．

いま，2 つの有理基本列 $\{a_n\}, \{b_n\} \in \boldsymbol{\mathcal{A}}$ に対し，$\{a_n\} \sim \{b_n\}$ であるとは，任意の正の有理数 ε に対し，ある自然数 $n(\varepsilon) \in \mathbb{N}$ が存在し，$k \geqq n(\varepsilon)$ を満たす任意の自然数 k に対し $d(a_k, b_k) < \varepsilon$ が成り立つことと定義する．

定理 12.4. $d = d_0$ または $d = d_p$ とし，$\{a_n\}, \{a'_n\}, \{b_n\}, \{b'_n\} \in \boldsymbol{\mathcal{A}}$ とする．

(1) 上で定義した $\sim$ は，集合 $\boldsymbol{\mathcal{A}}$ 上の同値関係である．

(2) $\{a_n + b_n\} \in \boldsymbol{\mathcal{A}}$ である．また，$\{a_n\} \sim \{a'_n\}$ かつ $\{b_n\} \sim \{b'_n\}$ ならば，$\{a_n + b_n\} \sim \{a'_n + b'_n\}$ である．

(3) $\{a_n b_n\} \in \boldsymbol{\mathcal{A}}$ である．また，$\{a_n\} \sim \{a'_n\}$ かつ $\{b_n\} \sim \{b'_n\}$ ならば $\{a_n b_n\} \sim \{a'_n b'_n\}$ である．

証明. (1), (2) は簡単なので (3) の後半のみ証明する．以下は $d = d_0$ でも $d = d_p$ でもよい．

まず，$\{a_n\} \in \boldsymbol{\mathcal{A}}$ ならば，ある $M \in \mathbb{Q}$ が存在して，任意の $n \in \mathbb{N}$ に対して $d(a_n, 0) \leqq M$ であることを証明する．

$\varepsilon = 1$ として $\{a_n\} \in \boldsymbol{\mathcal{A}}$ の定義を書くと，$n_1 \in \mathbb{N}$ が存在し，$k \geqq n_1$, $m \geqq n_1$ を満たす任意の k, $m \in \mathbb{N}$ に対し $d(a_k, a_m) < 1$ が成り立つ．$M_1 := \max\left\{d(a_i, 0) \;\middle|\; i = 1, 2, \ldots, n_1\right\}$ とおく．このとき任意の $k \in \mathbb{N}$ に対し

$$d(a_k, 0) \leqq d(a_{n_1}, 0) + d(a_k, a_{n_1}) \leqq M_1 + 1$$

だから，$M = M_1 + 1$ とおけばよい．

上の結果から，ある $M \in \mathbb{Q}$ が存在して，任意の $n \in \mathbb{N}$ に対して $d(a_n, 0) \leqq M$, $d(a'_n, 0) \leqq M$, $d(b_n, 0) \leqq M$, $d(b'_n, 0) \leqq M$ を満たす．

任意の正の有理数 ε を取る．$\varepsilon' := \dfrac{\varepsilon}{2M}$ とおく．

$\{a_n\} \sim \{a'_n\}$ かつ $\{b_n\} \sim \{b'_n\}$ だから，ある自然数 $n \in \mathbb{N}$ が存在し，$k \geqq n$ を満たす任意の自然数 k に対し $d(a_k, a'_k) < \varepsilon'$ かつ $d(b_k, b'_k) < \varepsilon'$ が成り立つ．$d(a_k - a'_k, 0) < \varepsilon'$ かつ $d(b_k - b'_k, 0) < \varepsilon'$ と書き換えられる．よって，

$$\begin{aligned}
d(a_k b_k, a'_k b'_k) &= d(a_k b_k - a'_k b'_k, 0) = d(a_k(b_k - b'_k) + b'_k(a_k - a'_k), 0) \\
&\leqq d(a_k(b_k - b'_k), 0) + d(b'_k(a_k - a'_k), 0) = d(a_k, 0)d(b_k - b'_k, 0) + d(b'_k, 0)d(a_k - a'_k, 0) \\
&\leqq \varepsilon' \cdot \big(d(a_k, 0) + d(b'_k, 0)\big) \leqq \varepsilon'(M + M) = 2\varepsilon' M = \varepsilon
\end{aligned}$$

である．よって，$\{a_n b_n\} \sim \{a'_n b'_n\}$ である． □

定義 12.5. 上の結果より，商集合 $\boldsymbol{\mathcal{A}}/\sim$ を定義することができる．$d = d_0$ の場合に $\boldsymbol{\mathcal{A}}/\sim$ を $\mathbb{R}$ と書き，$\mathbb{R}$ の元を**実数**という．$d = d_p$ の場合に $\boldsymbol{\mathcal{A}}/\sim$ を $\mathbb{Q}_p$ と書き，$\mathbb{Q}_p$ の元を p **進数**という．$\{a_n\} \in \boldsymbol{\mathcal{A}}$ の同値関係 $\sim$ による同値類を $\lim\limits_{n\to\infty} a_n$ と書く．

前定理より，$\boldsymbol{\mathcal{A}}/\sim$ 上で和 $+$ と積 $\times$ を以下のように定義することができる．$a = \lim\limits_{n\to\infty} a_n$, $b = \lim\limits_{n\to\infty} b_n \in \boldsymbol{\mathcal{A}}/\sim$ とする．このとき，

$$a + b := \lim_{n\to\infty}(a_n + b_n), \quad ab := \lim_{n\to\infty} a_n b_n$$

定義 12.6.($\mathbb{Q}$ の埋めこみ) 写像 $\iota\colon \mathbb{Q} \to \boldsymbol{\mathcal{A}}/\sim$ を以下のように構成する．$c \in \mathbb{Q}$ をとる．任意の $n \in \mathbb{N}$ に対し $a_n = c$ として有理数列 $\{a_n\}$ を定める (これを**定数数列**とか**定数列**という)．これは基本列である．そこで，$c \in \mathbb{Q}$ に対してこのように構成された定数数列 $\{a_n\}$ の $\sim$ に関する同値類を対応させる写像として $\iota\colon \mathbb{Q} \to \boldsymbol{\mathcal{A}}/\sim$ を定義する．容易にわかるように，ι は単射であり，$\iota(c + c') = \iota(c) + \iota(c')$, $\iota(cc') = \iota(c)\iota(c')$ が成り立つ．そこで，$c \in \mathbb{Q}$ と $\iota(c) \in \boldsymbol{\mathcal{A}}/\sim$ を同一視して $\mathbb{Q} \subset \boldsymbol{\mathcal{A}}/\sim$ と考える．

定理 12.7. 上のように構成された $\boldsymbol{\mathcal{A}}/\sim$ を $K = \boldsymbol{\mathcal{A}}/\sim$ とおく．すると K は体である．すなわち，a, b, $c \in K$ に対して以下が成り立つ．

(0) $a + b \in K$, $ab \in K$.

(1) (結合法則) $(a + b) + c = a + (b + c)$, $(ab)c = a(bc)$.

(2) (交換法則) $b + a = a + b$, $ba = ab$.

(3) (分配法則) $a(b + c) = ab + ac$.

(4) (0 と 1) $a + 0 = a$, $a \times 1 = a$, $0 \neq 1$.

(5) ($-a$ の存在) $a \in K$ に対し $-a = (-1) \times a$ とおけば $a + (-a) = 0$.

(6) (逆元の存在) $0 \neq a \in K$ ならば $ab = 1$ を満たす $b \in K$ が存在する．この b を $\dfrac{1}{a}$, $1/a$, a^{-1} などと書き a の**逆元**という．

証明. 有理数列 $\{a_n\}, \{b_n\}, \{c_n\}$ を $\lim_{n\to\infty} a_n = a$, $\lim_{n\to\infty} b_n = b$, $\lim_{n\to\infty} c_n = c$ となるようにとる．

(1) $(a+b)+c = \lim_{n\to\infty}((a_n+b_n)+c_n) = \lim_{n\to\infty}(a_n+(b_n+c_n)) = a+(b+c)$.

(2) 〜 (5) も (1) と同様にして証明できる．

(6) $\lim_{n\to\infty} a_n \neq 0$ だから，定数数列 $\{0\}$ と数列 $\{a_n\}$ を比較すると，ある正の有理数 ε を取ると，任意の自然数 $n \in \mathbb{N}$ に対し $k \geqq n$ を満たすある自然数 k が存在して $d(a_k, 0) \geqq \varepsilon$ となる．

$d(a_k, 0) \geqq \varepsilon$ を満たす自然数 k は無限個存在するから，そのような k を小さいほうから並べて数列 $\{k_n\}$ を作る．そして，$a'_n = a_{k_n}$ とおいて有理数列 $\{a_n\}$ の部分列 $\{a'_n\}$ を作る．$\lim_{n\to\infty} a'_n = \lim_{n\to\infty} a_n = 0$ である．そこで，数列 $\{a_n\}$ の代わりに $\{a'_n\}$ を考えることにより，任意の $n \in \mathbb{N}$ に対して $d(a_n, 0) \geqq \varepsilon$ であると仮定してよい．

$b_n = \dfrac{1}{a_n}$ として有理数列 $\{b_n\}$ を構成する．$\{b_n\}$ がコーシー列であれば，$b = \lim_{n\to\infty} b_n$ とおけば $ab = \lim_{n\to\infty} a_n b_n = 1$ である．そこで，$\{b_n\}$ がコーシー列であることを証明する．ε という有理数は上で固定されているので文字を変えて，任意の正の有理数 δ に対し，ある自然数 $n(\delta) \in \mathbb{N}$ が存在し，$k \geqq n(\delta)$, $m \geqq n(\delta)$ を満たす任意の自然数 k, m に対し $d(b_k, b_m) < \delta$ が成り立つことを証明すればよい．まず，任意の自然数 k, m に対し，

$$\begin{aligned} d(b_k, b_m) &= d(b_k - b_m, 0) = d\left(\frac{1}{a_k} - \frac{1}{a_m}, 0\right) = d\left(\frac{a_m - a_k}{a_k a_m}, 0\right) \\ &= \frac{d(a_m - a_k, 0)}{d(a_k, 0) d(a_m, 0)} \leqq \frac{d(a_k, a_m)}{\varepsilon^2} \end{aligned}$$

である．$\{a_n\}$ はコーシー列であったので，ある自然数 $n(\delta) \in \mathbb{N}$ が存在し，$k \geqq n(\delta)$, $m \geqq n(\delta)$ を満たす任意の自然数 k, m に対し $d(a_k, a_m) < \delta\varepsilon^2$ が存在する．したがって，$\{b_n\}$ はコーシー列である． □

定義&定理 12.8.(コーシー列) $K = \boldsymbol{\mathcal{A}}/\sim$ とおく．K の元の列 $\{a_n\}$ が**コーシー列**, あるいは**基本列**であるとは，任意の正の有理数 ε に対し，ある自然数 $n(\varepsilon) \in \mathbb{N}$ が存在し，$k \geqq n(\varepsilon)$, $m \geqq n(\varepsilon)$ を満たす任意の自然数 k, m に対し $d(a_k, a_m) < \varepsilon$ が成り立つことをいう．

K の元の列 $\{a_n\}$ がコーシー列ならば，ある $a \in K$ が存在して，任意の正の実数 ε に対し，ある自然数 $n \in \mathbb{N}$ が存在し，$k \geqq n$ を満たす任意の自然数 k に対し $|a_k - a| < \varepsilon$ が成り立つ．このとき，$\lim_{n\to\infty} a_n = a$ と書き，a を $\{a_n\}$ の**極限**という．

証明. $\lim_{n\to\infty} a_{k,n} = a_k$ を満たすコーシー有理数列 $\{a_{k,n}\}_{n=1}^{\infty}$ が存在する．このとき，有理数列 $\{a_{n,n}\}_{n=1}^{\infty}$ はコーシー列で，$\lim_{n\to\infty} a_{n,n} = a$ を満たす． □

定義 12.9.(実数の大小関係) $d = d_0$ とする．つまり，$x, y \in \mathbb{Q}$ に対して $d(x, y) = |x - y|$ とする．a, $b \in \mathbb{R} = \boldsymbol{\mathcal{A}}/\sim$ に対し，$a = \lim_{n\to\infty} a_n$, $b = \lim_{n\to\infty} b_n$ を満たすある有理数列 $\{a_n\}, \{b_n\} \in \boldsymbol{\mathcal{A}}$ で，任意の $n \geqq n_0$ $(n \in \mathbb{N})$ に対して $a_n \geqq b_n$ を満たすものが存在するとき，$a \geqq b$ と定義する．$b \leqq a$ とも書く．$a \geqq b$ で $a \neq b$ のとき $a > b$ とか $b < a$ と書く．

定理 12.10. $a, b, c \in \mathbb{R}$ とする．

(1) (反射率) $a \leqq a$ である．

(2) (反対称律) $a \leqq b$ かつ $b \leqq a$ ならば $a = b$.

(3) (推移律) $a \leqq b$ かつ $b \leqq c$ ならば $a \leqq c$.

(4) $a < b$ ならば $a + c < b + c$.

(5) $a < b$, $0 < c$ ならば $ac < bc$.

(6) $0 < 1$.

したがって，$\mathbb{R}$ は順序体である．

証明. 有理数列 $\{a_n\}, \{b_n\}, \{c_n\}$ を $\lim_{n\to\infty} a_n = a$, $\lim_{n\to\infty} b_n = b$, $\lim_{n\to\infty} c_n = c$ となるようにとる．$a \leqq b$ の場合には，任意の $n \in \mathbb{N}$ に対して $a_n \leqq b_n$ であると仮定しておく．

(1) は $a_n \leqq a_n$ から従う．

(2) $a \geqq b$ なので，$\lim_{n\to\infty} a'_n = a$ を満たす有理数列 $\{a'_n\}$ と，$\lim_{n\to\infty} b'_n = b$ を満たす有理数列 $\{b'_n\}$ で，任意の $n \in \mathbb{N}$ に対して $a'_n \geqq b'_n$ を満たすものが存在する．a'_n の代わりに $a''_n = a'_n + (b_n - b'_n)$ を考えれば，$\lim_{n\to\infty} a''_n = a$ で，$a_n \leqq b_n \leqq a''_n$ となる．$\lim_{n\to\infty} a''_n = \lim_{n\to\infty} a_n$ なので，任意の正の有理数 ε に対してある $m \in \mathbb{N}$ が存在し，$n \geqq m$ ならば $|a''_n - a_n| < \varepsilon$ となる．すると，$|b_n - a_n| = b_n - a_n \leqq |a''_n - a_n| < \varepsilon$ なので，$\lim_{n\to\infty} a_n = \lim_{n\to\infty} b_n$ が成り立つ．

(3) $b \leqq c$ なので，$\lim_{n\to\infty} b'_n = b$ を満たす有理数列 $\{b'_n\}$ で，任意の $n \in \mathbb{N}$ に対して $b'_n \leqq c_n$ を満たすものが存在する．$c'_n = c_n + (b_n - b'_n)$ とおけば，$\lim_{n\to\infty} c'_n = c$ で，任意の $n \in \mathbb{N}$ に対して $b_n \leqq c'_n$ が成り立つ．このとき，$a_n \leqq b_n \leqq c'_n$ なので $a \leqq c$ である．

(4) $a_n + c_n \leqq b_n + c_n$ なので $a + c \leqq b + c$ である．もし $a + c = b + c$ ならば両辺に $-c$ を足すと $a = b$ となってしまうので，$a + c \neq b + c$ で $a + c < b + c$ である．

(5) (4) より $a < b$ ならば $b - a > 0$ がわかる．また，$(b-a)c = bc - ac > 0$ ならば $ac < bc$ であることもわかる．よって，問題は $x > 0$ かつ $y > 0$ ならば $xy > 0$ であることを証明することに帰着される．

$x = \lim_{n\to\infty} a_n$ を満たすコーシー有理数列 $\{a_n\} \in \boldsymbol{\mathcal{A}}$ で，$n \geqq n_0$ のとき $a_n \geqq 0$ を満たすものが存在する．もし $1/N > x > 0$ であるとすると，ある $n_1(N) \in \mathbb{N}$ が存在して，$n \geqq n_1(N)$ のとき $1/N > a_n > 0$ となると仮定してよい．もし任意の $N \in \mathbb{N}$ に対して $1/N > x > 0$ であるとすると，$\lim_{n\to\infty} a_n = 0$ となり，$x = 0$ となってしまう．よって，十分大きい $N \in \mathbb{N}$ を取れば，$x \geqq 1/N$, $y \geqq 1/N$ となる．すると，$xy \geqq 1/N^2 > 0$ である． □

しかし，$d = d_p$ と $\mathbb{Q}_p$ の元 a, b に対して定義 12.9 のように $\leqq$ を定めても，上の定理の (2) は成立せず，順序にならない．例えば，$a = -1$, $b = 0$ とし，任意の $n \in \mathbb{N}$ に対して $a_n = -1$, $b_n = 0$ とする．また，$a'_n = p^n - 1$ とおく．$a_n \leqq b_n \leqq a'_n$ で，$d_p(a_n, a'_n) = 1/p^n$ であり，$\lim_{n\to\infty} a'_n = -1$ である．したがって，$-1 \leqq 0$ かつ $0 \leqq -1$ であるが，$0 \neq -1$ である．

補題 12.11. $x \in \mathbb{R}$ に対して，$n \leqq x < n+1$ を満たす整数 n が一意的に存在する．このとき，$n = \lfloor x \rfloor$ と書く．

証明. (存在) $\mathbb{R}$ の定義から，$|x - q| < 1$ を満たす $q \in \mathbb{Q}$ が存在する．定理 11.5 より $m \leqq q < m+1$ を満たす $m \in \mathbb{Z}$ が存在する．$q-1 < x < q+1$ なので，$m-1 < x < m+2$ である．もし，$m-1 < x < m$ なら $n = m-1$ とおけばよい．もし，$m \leqq x < m+1$ なら $n = m$ とおけばよい．もし，$m+1 \leqq x < m+2$ なら $n = m+1$ とおけばよい．

(一意性) $l \leqq x < l+1$, $n \leqq n < n+1$ $(l, n \in \mathbb{Z})$ とする．$l \leqq x < n+1$ より $n - l > -1$ であり，$n \leqq x < l+1$ より $n - l < 1$ である．$-1 < k < 1$ を満たす整数 k は $k = 0$ 以外に存在しないので，$n - l = 0$ である． □

定理 12.12. p は 2 以上の整数，$x \in \mathbb{R}$ で $0 < x < 1$ とする．$n \in \mathbb{Z}$ に対し $\lfloor p^n x \rfloor$ を p で割った余りを a_n とおく．$b_n = \sum_{k=1}^{n} \frac{a_k}{p^k} \in \mathbb{Q}$ とおく．このとき有理数列 $\{b_n\}$ は基本列で，$\lim_{n\to\infty} b_n = x$ が成り立つ．これを用いて，実数の p 進小数表示ができる．

証明. $\lfloor p^n x \rfloor$ を p で割った商を q_n とする．定理 11.6 の証明から，$n \geqq 2$ のとき

$$q_n = a_1 p^{n-2} + a_2 p^{n-3} + \cdots + a_{n-1}$$

と，$q_{n+1} \leqq p^n x < q_{n+1} + 1$ が成り立つ．よって，$b_n = \dfrac{q_{n+1}}{p^n}$ であり，$0 \leqq x - b_n < \dfrac{1}{p^n}$ が成り立つ．これは，$\lim_{n\to\infty} b_n = x$ を意味する． □

問 12.13.(アルキメデスの原理) $a, b \in \mathbb{R}$, $a > 0$, $b > 0$ ならば，$na > b$ を満たす自然数 $n \in \mathbb{N}$ が存在することを証明せよ．(上の定理を使えば，ほとんど自明.)

高木貞治「解析概論」では，p.3 の定理 1 で以下のデデキンドの切断が登場し，この定理から，$\mathbb{R}$ では任意のコーシー列が収束することを証明している.「解析概論」には定理 1 の証明は書いてないが，それは以下のように，実数全体の集合 $\mathbb{R}$ の定義に依存するものである．上のように，コーシー有理数列の極限として実数を定義すると，コーシー実数列の極限が $\mathbb{R}$ 内に存在することは簡単に証明でき，以下の定理が証明できるのである．

定理 12.14.(デデキンドの切断) A, B は空でない $\mathbb{R}$ の部分集合で，$A \cup B = \mathbb{R}$, かつ，$a \in A$, $b \in B$ ならば $a < b$ を満たすとする．すると，$\max A$ または $\min B$ のいずれか一方のみが存在する．

証明. $a \in A$, $b \in B$ ならば $a < b$ なので $A \cap B = \phi$ である．

$a_1 \in A \cap \mathbb{Q}$, $b_1 \in B \cap \mathbb{Q}$ を取っておく．今，$n \in \mathbb{N}$ に対し $a_n \in A$ と $b_n \in B$ が定まったとき，$c_{n+1} := \dfrac{a_n + b_n}{2}$ とおく．もし $c_{n+1} \in A$ ならば $a_{n+1} := c_{n+1}$, $b_{n+1} := b_n$ とおき，もし $c_{n+1} \in B$ ならば $a_{n+1} := a_n$, $b_{n+1} := c_{n+1}$ とおく．すると，$a_1 \leqq a_2 \leqq \cdots \leqq a_n < b_n \leqq \cdots \leqq b_1$ が成り立つ．他方 $b_n - a_n = \dfrac{b-a}{2^{n-1}}$ である．容易にわかるように $\{a_n\}$, $\{b_n\}$ はコーシー有理数列であるので，$a := \lim_{n\to\infty} a_n \in \mathbb{R}$ と $b := \lim_{n\to\infty} b_n \in \mathbb{R}$ が存在する．$\{a_n\} \sim \{b_n\}$ なので $a = b$ である．$a \in A$ ならば $a = \max A = \inf B$ で，$\min B$ は存在しない．$a \in B$ ならば $a = \sup A = \min B$ で，$\max A$ は存在しない． □

12-2. (付録) p 進数体 $\mathbb{Q}_p$

★ ここから先の第 12 章は，気が向いた人だけ呼んで下さい.

補題 12.15. p は素数とし，$x \in \mathbb{Q}$, $x \neq 0$ とする．$k \leqq \mathrm{ord}_p\, x$ のとき，ある $c_k \in \{0, 1, \ldots, p-1\}$ が一意的に存在して，$\mathrm{ord}_p(x - c_k p^k) > k$ となる．

証明. (存在) もし $k > \mathrm{ord}_p\, x$ ならば $c_k = 0$ とおけばよい．$k = \mathrm{ord}_p\, x$ の場合を考える．$y := p^{-k} x \in \mathbb{Q}$ とおくと，$\mathrm{ord}_p\, y = 0$ である．$y = \dfrac{a}{b}$ ($a, b \in \mathbb{Z}$ で $\mathrm{ord}_p\, a = \mathrm{ord}_p\, b = 0$) と書ける．$\mathrm{GCD}(b, p) = 1$ だから，$bc + pd = 1$ を満たす $c, d \in \mathbb{Z}$ が存在する．ac を p で割った余りを c_k とする．$\mathrm{ord}_p\, b = 0$ だから，$\mathrm{ord}_p(y - c_k) = \mathrm{ord}_p\, b + \mathrm{ord}_p(y - c_k) = \mathrm{ord}_p\, b(y - c_k) = \mathrm{ord}_p(a - bc_k)$ である．

$$a - bc_k \equiv a - bac \equiv a(1 - bc) \equiv a(pd) \equiv 0 \pmod{p}$$

なので，$\mathrm{ord}_p(y - c_k) = \mathrm{ord}_p(a - bc_k) > 0$ である．よって，$\mathrm{ord}_p(x - c_k p^k) > k$ である．

(一意性) $\mathrm{ord}_p(x - b_k p^k) > k$ と仮定し，$b_k = c_k$ を示す．$b_k \geqq c_k$ と仮定しても一般性を失わない．

$$\mathrm{ord}_p(b_k - c_k) p^k \geqq \min\left\{ \mathrm{ord}_p(x - c_k), \mathrm{ord}_p(x - b_k) \right\} > k$$

より，$\mathrm{ord}_p(b_k - c_k) \geqq 1$ で，$b_k - c_k$ は p の倍数である．$b_k - c_k \in \{0, 1, \ldots, p-1\}$ なので，$b_k - c_k = 0$ である． □

定義 12.16.(有理数の p 進表示) $x \in \mathbb{Q}$, $x \neq 0$ の p 進数表示を次のように構成する．まず，$r = \mathrm{ord}_p\, x$ とし，$k < r$ に対しては $c_k = 0$ と定める．そして，上のように $\mathrm{ord}_p(x - c_r p^r) > r$ となるような $c_r \in \{0, 1, \ldots, p-1\}$ をとる．次に，$x_1 = x - c_r p^r$ とおき，$\mathrm{ord}_p(x_1 - c_{r+1} p^{r+1}) > r+1$ となるような $c_{r+1} \in \{0, 1, \ldots, p-1\}$ をとり，$x_2 = x_1 - c_{r+1} p^{r+1}$ とおく．以下同様に x_n まで定まったとき，$\mathrm{ord}_p\, x_n \geqq r+n$ なので，$\mathrm{ord}_p(x_n - c_{r+n} p^{r+n}) > r+n$ となるような $c_{r+n} \in \{0, 1, \ldots, p-1\}$ をとり，$x_{n+1} = x_n - c_{r+n} p^{r+n}$ とおく．そして，

$$x = \sum_{n=r}^{\infty} c_n p^n$$

と表わし，これを $x \in \mathbb{Q}$ の p **進数表示**という．c_k を x の p^k の位という．

定理 12.17. 上の定義において，$a_n = \displaystyle\sum_{k=r}^{n+r} c_k p^k$ とおく．このとき，$\lim_{n\to\infty} d_p(a_n, x) = 0$ である．つまり，$d = d_p$ について $\lim_{n\to\infty} a_n = x$ である．

証明. $x_n - x_{n+1} = c_{r+n}p^{r+n}$ なので，$x - x_{n+1} = \sum_{k=0}^{n} c_{r+k}p^{r+k} = \sum_{k=r}^{n+r} c_k p^k = a_n$ である．よって，$x - a_{n-1} = x_n$ である．x_n の定義から，$\mathrm{ord}_p\, x_n \geqq r+n$ が成立している．よって，$d_p(x, a_{n-1}) = d_p(x_n, 0) \leqq p^{-r-n}$ である．これは $\lim_{n\to\infty} a_n = x$ を意味する． □

定義&定理 12.18.($\mathbb{Q}_p$ の元の ord_p) $x \in \mathbb{Q}_p$ が $x = \lim_{n\to\infty} a_n$ で定まるとき，$\mathrm{ord}_p\, x := \lim_{n\to\infty} \mathrm{ord}_p\, a_n$ として，$\mathrm{ord}_p\, x$ を定義すると，これは $\lim_{n\to\infty} a_n = x$ を満たす有理数列 $\{a_n\}$ の選び方に依存せずに矛盾なく定義できている．

証明. $x = \lim_{n\to\infty} b_n$, $\{b_n\} \in \mathcal{A}$ として，$\lim_{n\to\infty} \mathrm{ord}_p\, a_n = \lim_{n\to\infty} \mathrm{ord}_p\, b_n$ を証明すればよい．

$r := \lim_{n\to\infty} \mathrm{ord}_p\, a_n \neq +\infty$ の場合を考える．ある $n_1 \in \mathbb{N}$ が存在して，$n \geqq n_1$ ならば $\mathrm{ord}_p(a_n - a_{n_1}) > r$ となるから，$\mathrm{ord}_p\, a_n = \min\{\mathrm{ord}_p\, a_{n_1}, \mathrm{ord}_p(a_n - a_{n_1})\} = r$ である．

ある $n_2 \in \mathbb{N}$ が存在して，$n \geqq n_2$ ならば $\mathrm{ord}_p(b_n - a_n) > r$ となるから，$n \geqq \max\{n_1, n_2\}$ ならば，$\mathrm{ord}_p\, b_n = \min\{\mathrm{ord}_p(b_n - a_n), \mathrm{ord}_p\, a_n\} = r$ である．よって，$\lim_{n\to\infty} \mathrm{ord}_p\, b_n = r$ である．

$\lim_{n\to\infty} \mathrm{ord}_p\, a_n = +\infty$ の場合を考える．もし，$\lim_{n\to\infty} \mathrm{ord}_p\, b_n \neq +\infty$ ならば，上の証明から $\lim_{n\to\infty} \mathrm{ord}_p\, b_n = \lim_{n\to\infty} \mathrm{ord}_p\, a_n$ となって矛盾する．よって，$\lim_{n\to\infty} \mathrm{ord}_p\, b_n = r$ である． □

定理&定義 12.19.(p 進数の p 進表示) $x \in \mathbb{Q}_p$ が $x = \lim_{n\to\infty} a_n$ で定まるとき，任意の $k \in \mathbb{Z}$ に対し，ある $n(k) \in \mathbb{N}$ が存在して，$m \geq n(k)$ ならば $\mathrm{ord}_p(x - a_m) > k$ を満たす．したがって，$a_m = \sum_{n=r}^{\infty} c_{m,n}p^n$ と p 進数表示すると，$m \geqq n(k)$, $i \leqq k$ ならば $c_{m,i} = c_{n(k),i}$ が成り立つ．そこで，$c_i := c_{n(k),i}$ と定める．この c_i は $\lim_{n\to\infty} a_n = x$ を満たす有理数列 $\{a_n\}$ の選び方に依存せずに定まる．そこで，

$$x = \sum_{n=r}^{\infty} c_n p^n$$

と表わし，これを $x \in \mathbb{Q}_p$ の p **進数表示**という．

証明. 任意の $k \in \mathbb{Z}$ に対し，ある $n(k) \in \mathbb{N}$ が存在して，$m \geq n(k)$ ならば $\mathrm{ord}_p(x - a_m) > k$ を満たすことは，$\mathrm{ord}_p(x - a_m)$ の定義と $\lim_{n\to\infty}(x - a_n) = 0$ からわかる．

$\lim_{n\to\infty} b_n = x$, $b_m = \sum_{n=r}^{\infty} c'_{m,n}p^n$ のとき，各 n に対し m が十分大きければ $c'_{m,n} = c_{m,n}$ となることは，m が十分大きいとき $\mathrm{ord}_p(a_m - b_m) > n$ となることから従う． □

$x \in \mathbb{Q}$ の p 進表示は，x が自然数ならば中学・高校で習った (指導要領には含まれていないが) p 進法表示と一致するが，x が負の整数や (分母が 2 以上の) 分数の場合には p 進表示と p 進法表示は一致しない．

問 12.20. $p \geqq 3$ とする．すべての非負整数 n に対して $b_n = p - 1$ とおき，$x = \sum_{n=0}^{\infty} b_n p^n$ とおく．このとき，$x + 1 = 0$ であることを証明せよ．よって，$x = -1$ である．

このことから，$\mathbb{Q}$ における大小関係 $<$ を $\mathbb{Q}_p$ に拡張することはできないことがわかる．

定義 12.21. $\mathbb{Z}_p := \{x \in \mathbb{Q}_p \mid \mathrm{ord}_p\, x \geqq 0\}$ と書き，$\mathbb{Z}_p$ の元を p **進整数**という．$\mathbb{Z}_p$ を p **進整数環**という．$\mathbb{Z}_p$ の元 x は $x = \sum_{k=0}^{\infty} c_k p^k$ ($c_k \in \{0, 1, \ldots, p-1)$ と表すことができる．

問 12.22. $p=3$ の場合に，$1/2$ の p 進表示を計算する．$b_0=2$ とし，$n \geqq 1$ のとき $b_n=1$ とする．そして，$x=\sum_{n=0}^{\infty} b_n p^n$ とおく．このとき，$2x=1$ であることを証明せよ．つまり，$x=1/2$ であって，$1/2 \in \mathbb{Z}_3$ である．

定理 12.23. p は素数，$a \in \mathbb{Z}$ とする．もし a が p の倍数でなければ $1/a \in \mathbb{Z}_p$ である．もっと一般に，$a \in \mathbb{Z}_p$ が $\operatorname{ord}_p a=0$ を満たせば $1/a \in \mathbb{Z}_p$ である．

証明. $a \in \mathbb{Z}_p$ が $\operatorname{ord}_p a=0$ を満たすとき，$\operatorname{ord}_p 1/a=-\operatorname{ord}_p a=0$ なので，$1/a \in \mathbb{Z}_p$ である． □

13. 剰余系 $\mathbb{Z}/n\mathbb{Z}$

定義 13.1.(合同式) p を 2 以上の整数とする．m, n が整数で, m, n を p で割った余りが等しいとき, つまり, $m-n=px$ を満たす整数 x が存在するとき,

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

と表わし「m と n は p を**法として合同**である」とか,「m と n は **modulo** p で等しい」などという.

命題 13.2. $k, l, m, n \in \mathbb{Z}$, $k \equiv l \pmod{p}$ かつ $m \equiv n \pmod{p}$ ならば

$$\begin{aligned} k+m &\equiv l+n \pmod{p} \\ k-m &\equiv l-n \pmod{p} \\ km &\equiv ln \pmod{p} \end{aligned}$$

証明. 上の性質のうち，$km \equiv ln \pmod{p}$ だけ証明を書いておく (他はもっと易しい)．$k \equiv l \pmod{p}$, $m \equiv n \pmod{p}$ なので，ある整数 a, b により $l=k+ap$, $n=m+bp$ と書ける．すると，

$$ln-km=(k+ap)(m+bp)-km=(abp+am+bk)p$$

なので，$ln-km$ は p の倍数で，$km \equiv ln \pmod{p}$ である． □

問 13.3. $x^2+y^2=4z^2-1$ を満たす整数の組 (x, y, z) は存在しないことを証明せよ．

定義 13.4.(剰余系 $\mathbb{Z}/n\mathbb{Z}$) n は自然数とする．集合 $\mathbb{Z}$ 上に関係 $\sim$ を，$x, y \in \mathbb{Z}$ に対して,「$x \sim y \iff x \equiv y \pmod{n}$」で定義する．容易にわかるように，$\sim$ は $\mathbb{Z}$ 上の同値関係である．そこで，$\mathbb{Z}/n\mathbb{Z} := \mathbb{Z}/\sim$ によって $\mathbb{Z}/n\mathbb{Z}$ を定義する．いま (一時的に) $x \in \mathbb{Z}$ に対して x の $\sim$ による同値類を $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ と書くことにする．$x+n\mathbb{Z}$ とか $n\mathbb{Z}+x$ などと書くこともある．$\mathbb{Z}/n\mathbb{Z}$ 上に加法と乗法を，$\overline{x}, \overline{y} \in \mathbb{Z}/n\mathbb{Z}$ ($x, y \in \mathbb{Z}$) に対し，

$$\overline{x}+\overline{y} := \overline{x+y}, \quad \overline{x}\,\overline{y} := \overline{xy}$$

によって定義する．命題 13.2 により，これは矛盾のない定義である．また，$\mathbb{Z}/n\mathbb{Z}$ が可換環になることは容易に確認できる．このように和と積を定めた可換環 $\mathbb{Z}/n\mathbb{Z}$ を n を法とする**剰余系**という．差は $\overline{x}-\overline{y}=\overline{x-y}$ であるが，商については $\overline{y}\overline{z}:=\overline{x}$ を満たす $\overline{z} \in \mathbb{Z}/n\mathbb{Z}$ が一意的に存在する場合に限って，$\overline{z}:=\overline{x} \div \overline{y}=\overline{x}/\overline{y}=\dfrac{\overline{x}}{\overline{y}}$ を商として定義する．なお，慣れてきたら $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ を単に x とも書く．

定理 13.5. $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$ ($a, b \in \mathbb{Z}$) において，割り算 $\overline{a} \div \overline{b}$ が定義できるのは，b が n と互いに素な場合であり，また，その場合に限る．

証明. ます，$\mathrm{GCD}(b, n)=1$ のとき $\overline{a} \div \overline{b}$ が定義できることを証明する．b, n を整数と考えたとき，$\mathrm{GCD}(b, n)=1$ なので $bx+ny=1$ を満たす整数 x, y が存在する．$bx \equiv bx+ny \equiv 1 \pmod{n}$ なので $\overline{b}\overline{x}=\overline{1}$ である．$\overline{c}=\overline{a}\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ とおく．$\overline{b}\overline{c}=\overline{b}(\overline{a}\overline{x})=\overline{a}(\overline{b}\overline{x})=\overline{a} \times \overline{1}=\overline{a}$ である．

$\overline{b}\overline{z}=\overline{a}$ を満たす $\overline{z} \in \mathbb{Z}/n\mathbb{Z}$ は $\overline{z}=\overline{c}$ 以外に存在しないことを確認する．

$\overline{b}\overline{z}=\overline{a}$ ならば $\overline{0}=\overline{a}-\overline{a}=\overline{b}\overline{c}-\overline{b}\overline{z}=\overline{b}(\overline{c}-\overline{x})$ である．両辺に $\overline{x}$ を掛けると，$\overline{c}-\overline{z}=(\overline{x}\overline{b})(\overline{c}-\overline{z})=\overline{x}(\overline{b}(\overline{c}-\overline{z}))=\overline{x} \times \overline{0}=\overline{0}$ となる．よって $\overline{z}=\overline{c}$ である．

逆に, $\mathrm{GCD}(b,\, n) = d \neq 1$ のとき $\overline{a} \div \overline{b}$ は定義できないことを証明する．

$b,\, n$ は d の倍数なので $b = cd,\, n = md$ となる整数 $c,\, m$ が存在する．$\mathbb{Z}/n\mathbb{Z}$ において $\overline{c} \neq \overline{0},\, \overline{d} \neq \overline{0},\, \overline{m} \neq \overline{0}$ であるが，$bm = (cd)m = c(md)$ で md は n の倍数なので，$\overline{bm} = 0$ である．

$\overline{a} \div \overline{b} = \overline{q} \in \mathbb{Z}/n\mathbb{Z}$ が定義できたとすると，$\overline{bq} = \overline{a}$ である．$\overline{q} + \overline{m} \neq \overline{q} \in \mathbb{Z}/n\mathbb{Z}$ であるが，$\overline{b(q+m)q} = \overline{bq} + \overline{bm} = \overline{a} + \overline{c(dm)} = \overline{a} + \overline{cn} = \overline{a} \in \mathbb{Z}/n\mathbb{Z}$ であり，$\overline{q+m}$ も $\overline{a} \div \overline{b}$ の候補になり，$\overline{a} \div \overline{b}$ の値は一意的に定まらない．これは矛盾である． □

定義&系 13.6. p が素数のとき $\mathbb{Z}/p\mathbb{Z}$ は体になる．逆に，自然数 $n \in \mathbb{N}$ に対して $\mathbb{Z}/n\mathbb{Z}$ が体になれば n は素数である．p が素数のとき $\mathbb{Z}/p\mathbb{Z}$ を $\mathbb{F}_p$ とも書き，**標数 p の素体**という．

定義 13.7.(オイラーのファイ関数) 自然数 n に対し，$1, 2, 3.\ldots, n-1$ の中で　n と互いに素な整数の個数を $\varphi(n)$ で表し，$\varphi(n)$ を**オイラーのファイ関数**という．

定理 13.8. 自然数 n を $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ ($p_1,\ldots, p_r$ は相異なる素数) と素因数分解する．すると，

$$\varphi(n) = \prod_{i=1}^{r} p_i^{e_i - 1}(p_i - 1) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

である．

ここで，$\prod$ は総乗記号で $\displaystyle\prod_{i=1}^{r} a_1 = a_1 a_2 a_3 \cdots a_r$ である．

証明. n 未満の n と互いに素な自然数全体の集合を A とする．定義から $\varphi(n) = \#A$ である．($\#A$ は集合 A の要素の個数を表す.) 集合 B を

$$B := \left\{ (b_1, b_2, \ldots, b_r) \;\middle|\; \begin{array}{l} \text{各 } i = 1,\ldots, r \text{ に対し，} b_i \text{ は} \\ p_i \text{ と互いに素な } p_i^{e_i} \text{ 未満の自然数} \end{array} \right\}$$

とおく．$0 \leqq k < n$ に対し，k を $p_i^{e_i}$ で割った余りを k_i $(i = 1,\ldots, r)$ とし，$f(k) = (k_1,\, k_2,\ldots, k_r)$ とする．$f(k) \in B$ である．

逆に，$(b_1,\, b_2,\ldots,\, b_r) \in B$ を任意に選んだとき，中国剰余定理より，k を $p_i^{e_i}$ で割った余りが b_i $(i = 1,\ldots, r)$ となるような n 未満の自然数 $k \in A$ が存在する．よって，写像 $f\colon A \to B$ は全単射であり，$\#A = \#B$ となる．

ところで，p_i と互いに素な $p_i^{e_i}$ 未満の自然数の個数は $p_i^{e_i-1}(p_i - 1)$ である．よって，$\#B = \displaystyle\prod_{i=1}^{r} p_i^{e_i-1}(p_i - 1)$ である． □

群の定義はベクトル空間の定義のところで話たが，もう一度書いておく．

定義 13.9.(群) 集合 G があり，G 任意の元 $a,\, b$ に対し ($a = b$ の場合も含む) に対し二項演算 $a * b$ が定義されていて，$a * b$ は G の元になる，つまり $a * b \in G$ であるものとする (このことを，G は演算 $*$ について**閉じている**という．さらに以下の性質 (1), (2), (3) を満たすものとする．

(1) $a,\, b,\, c \in G$ ならば $(a * b) * c = a * (b * c) \in G$ が成り立つ．この性質を**結合法則**という．

(2) ある特別な元 $e \in G$ が存在して，任意の $a \in G$ に対して $a * e = a$ かつ $e * a = a$ を満たす．

(3) $a \in G$ ならば $a * b = e$ を満たす $b \in G$ がただ 1 つ存在する．

このとき G は演算 $*$ について**群**であるという．e を演算 $*$ についての**単位元**であるという．また，b を a の演算 a についての**逆元**であるという．

G が演算 $*$ について群であって，さらに**交換法則**

(4) $a * b = b * a$ が任意の $a,\, b \in G$ について成り立つ．

が成立するとき，G は**アーベル群**であるとか**可換群**であるという．

G は乗法 $\times$ について群であるとする．$a \times b$ は単に ab と書く．また，自然数 n に対し，

$$a^n = \underbrace{a \times a \times \cdots \times a}_{n \text{ 個}}$$

と書き，n が負の整数のときは $a^n = 1/a^{-n}$, $n = 0$ のときは $a^0 = 1$ (乗法の単位元) と約束する．

例えば，$\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ はいずれも演算 $+$ についてアーベル群であり，その単位元は 0 である．また a の $+$ についての逆元は $-a$ である．

$a-b=a+(-b)$ によって引き算が定義できることを注意する．

命題 13.10. 剰余系 $\mathbb{Z}/n\mathbb{Z}$ の中で，乗法についの逆元を持つような元全体の集合を $(\mathbb{Z}/n\mathbb{Z})^\times$ と書くと，$(\mathbb{Z}/n\mathbb{Z})^\times$ は乗法についてアーベル群になる．また，$\#(\mathbb{Z}/n\mathbb{Z})^\times=\varphi(n)$ (オイラーのファイ関数) である．

証明. $(\mathbb{Z}/n\mathbb{Z})^\times$ が群であるのは自明である．定理 13.5 より，

$$(\mathbb{Z}/n\mathbb{Z})^\times=\left\{\overline{x}\;\middle|\; x\in\mathbb{Z},\, 1\leqq x<n \text{ で } \mathrm{GCD}(x,\,n)=1\right\}$$

であるので，$\#(\mathbb{Z}/n\mathbb{Z})^\times=\varphi(n)$ である． □

定理 13.11. G は有限集合であって，乗法 $\times$ について群であるとする．$n=\#G$ とする．すると，任意の $a\in G$ に対して $a^n=1$ が成り立つ．

証明. G は有限集合なので, $a^k=a^l$ を満たす整数 $k<l$ が存在する．このとき, $a^{l-k}=1$ である．$a^e=1$ を満たす最小の自然数 e をとり, $H=\{1,\,a,\,a^2,\ldots,\,a^{e-1}\}\subset G$ とおく．ここで, 任意の整数 k に対し, $a^k\in H$ であることに注意する．

また, $x\in G$ に対し, $Hx=\{x,\,ax,\,a^2x,\ldots,\,a^{e-1}x\}\subset G$ とおく．$H=H1$ である．また, Hx も e 個の要素からなる集合である．

$x,\,y\in G$ に対し, $Hx=Hy$ または $Hx\cap Hy=\phi$ のいずれか一方のみが成り立つ．実際, もし, $Hx\cap Hy\neq\phi$ ならば, $z\in Hx\cap Hy$ をとるとき, $z=a^ex=a^fy$ ($e,\,f$ はある整数) と表せるので, $y=a^{e-f}x\in Hx$ となり, これより $Hx=Hy$ が得られる．

したがって, 適当に $x_1,\ldots,\,x_r\in G$ を選ぶと, $G=Hx_1\cup Hx_2\cup\cdots\cup Hx_r$, かつ, $1\leqq i<j\leqq r$ のとき $Hx_i\cap Hx_j=\phi$ と書ける．ゆえに, G の要素の個数は $m=er$ である．つまり, $a^m=a^{er}=(a^e)^r=1^r=1$ となる． □

上の定理を $G=(\mathbb{Z}/n\mathbb{Z})^\times$ に適応したものが次のオイラーの定理である．

定理 13.12.(オイラーの定理) n は 2 以上の整数とする．a が n と互いに素な整数のとき,

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

が成り立つ．ここで $\varphi(n)$ はオイラーのファイ関数である．

証明. $\#G=\varphi(n)$ で，G 乗法に関する群であったので，$\overline{a}^{\varphi(n)}=1$ が成り立つ．よって，$\mathbb{Z}$ で考えたとき $a^n\equiv 1 \pmod{n}$ である． □

上の定理で, n が素数の場合は $\varphi(n)=n-1$ であるので, 次の定理が成り立つ．

定理 13.13.(フェルマーの小定理) p が素数で, a が p の倍数でない整数とき

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

が成り立つ．

$\mathbb{Z}/n\mathbb{Z}$ についての重要な定理として，上記以外に，中国剰余定理とか，p が素数のとき $G=(\mathbb{Z}/p\mathbb{Z})^\times$ は巡回群になるというような話があります．これらは，代数学 II や代数学続論でもっと一般化された形で学習するので，ここでは割愛する．