HANDOUTS
Basic Concepts in Mathematics I
数学通論 I: 集合と代数系

Hiroshi SUZUKI*
International Christian University

平成 20 年 7 月 25 日

目 次

*E-mail:hsuzuki@icu.ac.jp

1 集合と論理

1.1 Sets：集合

集合 (Set)： 「もの」の集まり。ただし、ある「もの」が、その集まりの中にあるかないかがはっきりと定まっているようなものでなければならない。

元、要素 (Element)： 集合 A のなかに入っている個々の「もの」を A の元、要素といい、a が集合 A の元であることを、記号で $a \in A$ または $A \ni a$ と書く。その否定を $a \notin A$ または $A \not\ni a$ と書く。

1.2 Logic：論理

命題 (Proposition)： 正しい (真 True) か正しくない (偽 False) が明確に区別できる文を命題という。

真理値 (Truth Value)： 命題が真であることを「T」、偽であることを「F」で表す。これを命題の真理値という。

否定・論理和・論理積・含意： $\sim P$、$P \wedge Q$、$P \vee Q$、$P \Rightarrow Q$、$P \Leftrightarrow Q$

P	$\sim P$
T	F
F	T

P	Q	$P \wedge Q$	$P \vee Q$	$P \Rightarrow Q$	$P \Leftrightarrow Q$
T	T	T	T	T	T
T	F	F	T	F	F
F	T	F	T	T	F
F	F	F	F	T	T

数学語では、'and' 「かつ」は 'logical and' 「論理積」を、'or' 「または」は 'logical or' 「論理和」をあらわす。

このようにおのおのの論理式に対して、真理値関数が一つずつ決まる。$(\sim P) \vee Q$ の真理値と $P \Rightarrow Q$ の真理値は P, Q の真理値に関わらず等しい。二つの論理式が同一の真理値関数を決める時、この二つの論理式は互いに論理的に同値 (logically equivalent) であるという。このことを $\equiv$ で表す。(e.g. $(P \Rightarrow Q) \wedge (Q \Rightarrow P) \equiv P \Leftrightarrow Q$、$(\sim P) \vee Q \equiv P \Rightarrow Q$。) $P \vee \sim P$ の真理値は常に真である。このような命題をトートロジー (tautology) という。$P \Leftrightarrow Q$ がトートロジーであれば $P \equiv Q$ である。$P \wedge \sim P$ の真理値は常に偽である。このような命題を矛盾 (contradiction) という。

命題 1.1 (基本性質) 次が成立する。

(1) $P \wedge P \equiv P \equiv P \vee P.$

(2) $\sim(\sim P) \equiv P.$

(3) $P \wedge Q \equiv Q \wedge P$, $P \vee Q \equiv Q \vee P.$ [交換法則]

(4) $(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R)$, $(P \vee Q) \vee R \equiv P \vee (Q \vee R).$ [結合法則]

(5) $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$, $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R).$ [分配法則]

(6) $\sim(P \vee Q) \equiv (\sim P) \wedge (\sim Q)$, $\sim(P \wedge Q) \equiv (\sim P) \vee (\sim Q).$ [ド・モルガンの法則]

(7) $P \Rightarrow Q \equiv (\sim P) \vee Q.$

全称命題 (Universal Proposition)： 「任意の（すべての）X について命題 $P(X)$ が成り立つ」を全称命題といい $\forall X\ P(X)$ と書く。

存在命題 (Existential Proposition)： 「ある X について命題 $P(X)$ が成り立つ」を存在命題といい $\exists X\ P(X)$ と書く。

1.3 集合演算

部分集合 (Subset)： 集合 A、B において A のすべての元が、B の元であるとき、A は B の部分集合であると言い、$A \subseteq B$ または $B \supseteq A$ と書く。すなわち、

$$A \subseteq B \Leftrightarrow (x \in A) \Rightarrow (x \in B) \text{ がつねに真} \Leftrightarrow (\forall x \in A)[x \in B]$$

集合の相等 (Equality of Sets)： 二つの集合 A, B において、$A \subseteq B$ かつ $B \subseteq A$ が成り立つ時 A と B は相等であると言い $A = B$ と書く。

共通部分 (Intersection)： 二つの集合 A, B において、A と B の両方に共通な元全体の集合を A と B との共通部分といい $A \cap B$ と書く。すなわち、

$$A \cap B = \{x \mid (x \in A) \wedge (x \in B)\} = \{x \mid x \in A \text{ かつ } x \in B\} = \{x \mid x \in A, x \in B\}.$$

和集合 (Union)： 二つの集合 A, B において、A の元と B の元とを全部寄せ集めて得られる集合を A と B との和集合といい $A \cup B$ と書く。すなわち、

$$A \cup B = \{x \mid (x \in A) \vee (x \in B)\} = \{x \mid x \in A \text{ または } x \in B\}$$

空集合 (Empty Set)： 元を全く含まない集合を空集合といい $\emptyset$ で表す。

差集合 (Difference)： 二つの集合 A, B において、A の元で B の元ではない元全体の集合を A と B との差集合といい、$A-B$ または $A-B$ と書く。すなわち、

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

補集合 (Complement)： 全体集合 (X, U または Ω が良く使われる：(Universal Set)) を一つ定めた時その部分集合 A に対し、A に含まれない要素全体を $\overline{A}$ または A^c で表し、A の補集合と言う。 定義から $A \cap \overline{A} = \emptyset$ かつ、$A \cup \overline{A} = U$。差集合も $A-B = A \cap \overline{B}$ と表すことができる。

対称差（Symmetric Difference)： $A \triangle B = (A \cup B)-(A \cap B)$ を A と B の対称差という。$A \triangle B = (A-B) \cup (B-A)$ となっている。

$\lambda \in A$ に対して、$C_\lambda \subseteq X$ とする。

$$\begin{aligned} \bigcap_{\lambda \in A} C_\lambda &= \{x \mid (\forall \lambda \in A)[x \in C_\lambda]\}, \\ \bigcup_{\lambda \in A} C_\lambda &= \{x \mid (\exists \lambda \in A)[x \in C_\lambda]\}. \end{aligned}$$

$A_1, A_2, \ldots, A_n$ を集合とするとき、$(a_1, a_2, \ldots, a_n)$, $a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n$ となる長さ n の列全体を

$$A_1 \times A_2 \times \cdots \times A_n = \prod_{i=1}^{n} A_i = \{(a_1, a_2, \ldots, a_n) \mid (\forall i \in \{1, 2, \ldots, n\})[a_i \in A_i]\}$$

と書き、$A_1, A_2, \ldots, A_n$ の直積という。A を集合とした時、$A \times A$ は、A の元の対の全体で、例えば、A が整数全体の集合 $\boldsymbol{Z}$ であるとき、$(1,2), (1,1)$ などを含む。$(1,2) \neq (2,1)$。

2　証明

2.1　直接証明・対偶・背理法・反例

真理表により、または命題 1.1 を用いることにより簡単に次の論理同値が確かめられる。

$$P \Rightarrow Q \equiv\sim P \vee Q \equiv\sim Q \Rightarrow\sim P \equiv\sim (P\wedge \sim Q).$$

$\sim Q \Rightarrow\sim P$ を、命題 $P \Rightarrow Q$ の対偶 (contraposition) という。また、$P \Rightarrow Q$ をそのまま証明することを直接証明 (direct proof)、$\sim Q \Rightarrow\sim P$ を証明することを対偶による証明 (proof by contrapositive) という。$\sim (P\wedge \sim Q)$ が真でることを示すのは、P が真であって Q が偽であることは無いことを示すことなので、背理法 (proof by contradiction) と呼ばれる。

証明の例として集合に関する二つの命題を証明する。以下においては、集合 X, Y, Z において一般に $X \subseteq X \cup Y$、$X \cap Y \subseteq Y$ であり、$X \subseteq Z$ かつ $Y \subseteq Z$ ならば $X \cup Y \subseteq Z$、$X \subseteq Y$ かつ $X \subseteq Z$ ならば $X \subseteq Y \cap Z$、また、$X \subseteq Y$ かつ $Y \subseteq Z$ ならば $X \subseteq Z$ であることを暗黙のうちに用いている。これらが正しいことを $\cup, \cap, \subseteq$ の定義に現れる、$\vee, \wedge, \Rightarrow$ の真理値にもどって確かめ、かつそれぞれの性質がどこで用いられているか、また仮定が何で、それはどこで用いられているか確認しながら読み進むこと。

例 2.1 A, B を集合とする。このとき、

$$A \cup B = A \Leftrightarrow B \subseteq A.$$

証明　$A \cup B = A$ とする。$B \subseteq A \cup B = A$ だから $B \subseteq A$。$B \subseteq A$ とする。一般に、$A \subseteq A \cup B$。また、仮定より $B \subseteq A$ だから $A \cup B \subseteq A \cup A = A$。したがって、$A \cup B = A$。 ■

上の証明を考えてみましょう。まず、P を $A \cup B = A$ という命題。Q を $B \subseteq A$ という命題とします。上は、$P \Leftrightarrow Q$ が真であることを示せということです。この命題が真となるのは、P、Q の真理値がそれぞれ T, T か F, F の時ですから、P が T のときはいつでも Q は T。Q が T のときはいつでも P が T であることを示せば良いことになります。他の表現をすると、$P \Leftrightarrow Q$ と $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$ は論理同値でしたから、$P \Rightarrow Q$ が真でかつ $Q \Rightarrow P$ が真であることを示す事になります。たとえば $P \Rightarrow Q$ が真であることを示すのは、P が真ならば Q が真を示せば良いからです（P が偽のときは、$P \Rightarrow Q$ はいつでも真ので)。従って、上の証明は二つの部分に分かれ、$A \cup B = A$ を仮定して、$B \subseteq A$ を示す部分と、$B \subseteq A$ を仮定して、$A \cup B = A$ を示す部分に分かれています。

例 2.2 A, B, C を集合とする。このとき、

$$A \cup (B \cap C) = (A \cup B) \cap C \Leftrightarrow A \subseteq C.$$

証明　まず $A \cup (B \cap C) = (A \cup B) \cap C$ を仮定する。

$$A \subseteq A \cup (B \cap C) = (A \cup B) \cap C \subseteq C.$$

$A \subseteq C$ と仮定する。このとき、

$$A \subseteq A \cup B \text{ かつ } A \subseteq C \text{ だから } A \subseteq (A \cup B) \cap C.$$

また $B \subseteq A \cup B$ だから $B \cap C \subseteq (A \cup B) \cap C$ したがって、$A \cup (B \cap C) \subseteq (A \cup B) \cap C$ — (1)。また、$x \in (A \cup B) \cap C$ とする。すると、$x \in C$ でありかつ、$x \in A \cup B$ だから $x \in A$ または $x \in B$。$x \in A$ とすると、$x \in A \cup (B \cap C)$。一方、$x \in B$ とすると $x \in C$ だったから $x \in B \cap C$ したがって、いずれの場合も $x \in A \cup (B \cap C)$ である。これは、$(A \cup B) \cap C \subseteq A \cup (B \cap C)$ — (2) を意味する。(1) と (2) から $A \cup (B \cap C) = (A \cup B) \cap C$ が示された。 ■

2.2 練習問題 3.23

以下の結果の証明を評価せよ。

結果. $a, b \in \boldsymbol{Z}$ とする。このとき、$a-b$ が偶数であることの必要十分条件 a と b が同じパリティを持つことである。

証明 2つの場合を考える。

場合 1. a と b は同じパリティを持つとする。私たちはここで2つの部分集合を考察する。(以下略)

場合 2. a と b は逆のパリティを持つとする。ふたたび2つの部分場合がある。(以下略)

証明のどこが悪いのか判然としないというコメントが多かったので、以下に私の評価を書いてみます。

証明すべき命題は、$a, b \in \mathbb{Z}$ としたとき

$$2 \mid a-b \Leftrightarrow ((2 \mid a) \wedge (2 \mid b)) \vee ((2 \nmid a) \wedge (2 \nmid b)).$$

表現は異なっていますが、同じパリティを持つ (教科書 3.4) など (教科書 4.2) の定義を参照して下さい。

3.23 の証明、場合 1 は $\Leftarrow$ の証明が書かれています。これは問題ないと思います。

場合 2 は $((2 \mid a) \wedge (2 \nmid b)) \vee ((2 \nmid a) \wedge (2 \mid b))$ を仮定して $2 \nmid a-b$ を証明しています。証明自体は問題ないと思います。

場合1が $\Leftarrow$ の証明ですから、残りは $\Rightarrow$ の証明であるべきです。場合2は、$2 \nmid a-b$ を証明していますから、対偶を証明していると思われます。$((2 \mid a) \wedge (2 \mid b)) \vee ((2 \nmid a) \wedge (2 \nmid b))$ の否定が仮定となりますからそれを考えると、

$$\begin{aligned} \sim (((2 \mid a) \wedge (2 \mid b)) \vee ((2 \nmid a) \wedge (2 \nmid b))) &= \sim ((2 \mid a) \wedge (2 \mid b)) \wedge \sim ((2 \nmid a) \wedge (2 \nmid b)) \\ &= ((2 \nmid a) \vee (2 \nmid b)) \wedge ((2 \mid a) \vee (2 \mid b)) \\ &= ((2 \nmid a) \wedge (2 \mid b)) \vee ((2 \mid a) \wedge (2 \nmid b)) \end{aligned}$$

これは、場合2で扱っている場合となります。そこで、場合2は $\Leftarrow$ の対偶を証明している、と考えれば、全体の証明としては問題無いことになります。

しかし、これは、証明の基本の勉強ですから、皆さんは頭の中で考えて、後半は対偶と思われるのだと思いますが、そこは対偶を示していることを、論理的に明確にすべきだと言うことだと思います。即ち、

「$\Rightarrow$ の対偶を考える。$((2 \mid a) \wedge (2 \mid b)) \vee ((2 \nmid a) \wedge (2 \nmid b))$ の否定は、$((2 \nmid a) \wedge (2 \mid b)) \vee ((2 \mid a) \wedge (2 \nmid b))$ だから、この仮定のもとで、$a-b$ が奇数であることを示せばよい。」

と書いてあれば、良いということです。

もう一点は、さらに本質的ですが、$a, b \in \mathbb{Z}$ に対しては、それぞれが偶数、奇数を考えれば、4 通りしかあり得ません。そのなかで $a-b$ が偶数になるか、奇数になるかをすべて決定すれば、上記の同値関係も確定するということです。おそらく殆どの方は、こちらを考えたのではないかと思います。これも正しい考え方です。繰り返しになりますが、これは、証明の基本の勉強ですから、もしそのように考えるのであれば、それを最初に明確にしないといけないと言うことです。

「a, b は奇数か、偶数からのいずれかであるから、a, b の組みについては、偶奇性に関して、全部で4通りの可能性がある。また $a-b$ は偶数か奇数かのいずれであるから、命題を証明するには、パリティーが同じであれば、$a-b$ は偶数、パリティが異なれば、$a-b$ が奇数であることを示せばよい。」

と書いてあれば、良いと言うことです。納得しましたか。

by hs, April 26, 2007

3 関係

3.1 順序関係・同値関係

A を集合とし、$a, b \in A$ について、aRb または $\sim(aRb)$ のいずれかが定まっている時、R を A における関係 (relation) という。

次のようにも定義することができる。$R \subseteq A \times A = \{(a, b) \mid a, b \in A\}$ とした時、$a, b \in A$ に対して、

$$aRb \Leftrightarrow (a, b) \in R$$

と定義する。$a, b \in A$ のとき、$(a, b) \in R$ すなわち、aRb、または、$(a, b) \notin R$ すなわち $\sim(aRb)$ のいずれかが成り立つから、最初に定義した関係になっている。R を最初に定義した関係とした時、

$$\{(a, b) \mid (a, b \in A) \wedge (aRb)\} \subseteq A \times A$$

だから、どちらで定義しても本質的には同じであることがわかる。今後も、この両方の意味で「関係」ということばを使う。

R を集合 A における関係であるとき、以下の性質について考える。

(R) $(\forall a \in A)[aRa]$ (反射律, reflexive law).

(S) $(\forall a \in A)(\forall b \in A)[aRb \Rightarrow bRa]$ (対称律, symmetric law)

(A) $(\forall a \in A)(\forall b \in A)[(aRb \wedge bRa) \Rightarrow a = b]$ (半対称律, antisymmetric law)

(T) $(\forall a \in A)(\forall b \in A)(\forall c \in A)[(aRb \wedge bRc) \Rightarrow aRc]$ (推移律, transitive law)

例 3.1 以下のそれぞれは関係であることを確かめ、上のどの性質を満たすかを定めよ。

1. $(\boldsymbol{Z}, \leq)$ または、$R_{\leq} = \{(a, b) \mid \boldsymbol{Z} \times \boldsymbol{Z} \mid a \leq b\}$ によって定めた関係。'$\leq$' は通常の大小関係。
2. X を集合、$(P(X), \subseteq)$。ここで、$P(X)$ $(= 2^X)$ は X のベキ集合を表す。

このように (R), (A), (T) を満たす関係を順序関係または、半順序といい、半順序の定義された集合を半順序集合 (partially ordered set, poset) という。$(\boldsymbol{Z}, <)$ は順序ではない。順序関係は、'大小関係' を数学的に定義し直したものと考えて良い。ただし、$(\boldsymbol{Z}, \geq)$ も順序関係になることに注意。

1. A を集合とし、$(A, =)$ とする。これは、上のすべての条件を満たす。
2. A をこの教室の学生の集合とし、

   $$R_{\sim} = \{(a, b) \in A \times A \mid a, b \text{ の誕生日は同じ月 }\}$$

   によって定義した関係。
3. $(\boldsymbol{Z}, \equiv_3)$。ここで、$a, b \in \boldsymbol{Z}$ のとき $a \equiv_3 b$ は $a - b$ が 3 で割り切れるという条件とする。

これらは、すべて (R), (S), (T) を満たす。このように、(R), (S), (T) を満たす関係を同値関係 (equivalence relation) という。同値関係は、'ある意味で等しい' という関係を数学的に定義したものと考えられる。ただし、A を集合とし、$(A, \sim)$ を同値関係としたとき、$a \sim b$ だからといって、$a = b$ とは限らない。

$(A, \sim)$ を同値関係とする。このとき、$a \in A$ によって定まる A の部分集合

$$[a] = [a]_{\sim} = \{x \mid (x \in A) \wedge (x \sim a)\}$$

を、a を含む同値類 (the equivalence class of a) という。

命題 3.1 集合 A に定義された関係 $\sim$ が同値関係であるとする。$[a]_\sim$ を $[a]$ であらわす。この時以下が成立する。

(i) $(\forall a \in A)[a \in [a]]$.

(ii) $(\forall a \in A)(\forall b \in A)[b \in [a] \Rightarrow [a] = [b]]$.

(iii) $(\forall a \in A)(\forall b \in A)[[a] \cap [b] \neq \emptyset \Rightarrow [a] = [b]]$.　(iii') $(\forall a \in A)(\forall b \in A)[[a] \neq [b] \Rightarrow [a] \cap [b] = \emptyset]$.

(iv) $A = \bigcup_{a \in A} [a]$.

証明

(i): $a \in [a]$。

反射律より、$a \sim a$ だから $a \in [a]$ が成立する。

(ii): $b \in [a]$ ならば $[b] = [a]$。

まず、$b \in [a] \Rightarrow [b] \subseteq [a]$ を示す。$b \in [a] = \{x \mid (x \in A) \wedge (x \sim a)\}$ より $b \sim a$。$x \in [b]$ とすると、$[b]$ の定義より $x \sim b$。$b \sim a$ と推移律より $x \sim a$。したがって $x \in [a]$。$(x \in [b]) \Rightarrow (x \in [a])$ が常に言えたから $[b] \subseteq [a]$。$b \sim a$ に対称律を用いると $a \sim b$。したがって $[b]$ の定義より $a \in [b]$。最初に示したことから (a と b の役割と取り替えると) $[a] \subseteq [b]$ 。従って、先に示したこととあわせて $[a] = [b]$ である。

(iii): $[a] \cap [b] \neq \emptyset$ ならば $[a] = [b]$。

$[a] \cap [b] \neq \emptyset$ だから $\exists c \in [a] \cap [b]$。従って、$(c \in [a]) \wedge (c \in [b])$。$c \in [a]$ だから (a) より $[c] = [a]$。また、$c \in [b]$ だから (a) より $[c] = [b]$。集合における $=$ は同値関係だから $[c] = [a]$ かつ $[c] = [b]$ より集合の等号に関する対称律と推移律を用いて $[a] = [b]$ を得る。

(iv): $A = \bigcup_{a \in A} [a]$.

定義より $[a] \subseteq A$。したがって、$A \supseteq \bigcup_{a \in A}[a]$。$x \in A$ とすると (i) より $x \in [x]$ だから $x \in \bigcup_{a \in A}[a]$ である。したがって、$A \subseteq \bigcup_{a \in A}[a]$。これで等号が証明された。 ■

例 3.2 $(\boldsymbol{Z}, \equiv_3)$ においては、$[0] = [3] = [6] = [-3]$, $[1] = [4] = [-2]$ などとなり、$\boldsymbol{Z} = [0] \cup [1] \cup [2]$ となる。

3.2 証明について：第 7 章の問題から

7.5 $R = \{(a,a),(a,b),(a,c)\}$ を集合 $S = \{a,b,c\}$ 上の関係とするとき R は反射的・対照的・推移的であるか判定せよ。

解. $b \in S$ であるが、$(b,b) \notin S$ であるので反射的ではない。

$(a,b) \in S$ であるが、$(b,a) \notin R$ であるので対称的ではない。

$x,y,z \in S$ において $(x,y),(y,z) \in S$ とする。すると、$R = \{(a,a),(a,b),(a,c)\}$ だから $x = y = a$。特に、$(x,z) = (y,z) \in R$ が成立する。すなわち、推移的である。 ■

すべての $x \in S$ について $(x,x) \in R$ が成立するのが R が反射的であった。したがって反射的でないことを示すには、この条件を満たさないものを一つ与えれば十分である。この問題の場合確かに c についても同じように、$c \in S$ かつ $(c,c) \notin R$ だが、一つ反例があれば十分。対称的ではないことの証明も同じ。

推移的であることの証明は一般的には簡単ではなく、しらみつぶしで調べないといけない場合が多いが、この問題では、上記の様にすれば、証明を書くことができる。

7.29 R を $\boldsymbol{Z}$ 上で $a + b \equiv 0 \pmod 3$ と定義したとき、R は同値関係ではないことを証明せよ。

解. $1 \in \boldsymbol{Z}$ であるが、$1+1 = 2 \not\equiv 0 \pmod 3$ だから、$(1,1) \notin R$ となり、R は反射的ではないので、同値関係ではない。 ■

同値関係であるためには、反射的で、対照的で、推移的でなければいけなかった。したがって、同値関係でないことをしめすには、これらの条件の一つでも満たされないことを示せば良い。上では、反射的ではないことを示している。反射的ではないことを示すには、$a \in \boldsymbol{Z}$ でかつ、$(a,a) \notin R$ であるものを一つ与えればよい。上の証明では、1 を与えてある。これを満たさないものはたくさんあるが、具体的に、一つ示すことが大切である。$(\forall x)[P(x)]$ 型の命題の否定は $(\exists x)[\sim P(x)]$ で、一つでも成り立たない例があれば十分であることとともに、本当にそのような条件を満たすものが存在するのかどうかは、単純ではないこともあるからである。

7.41 $\boldsymbol{Z}_{11}$ において、$[r]$, ただし $0 \le r < 11$ によって和と積を述べよ。

解.

(a) $[7] + [5] = [12] = [1]$.

(b) $[7][5] = [35] = [2]$.

(c) $[-82] + [207] = [-8 \cdot 11 + 6] + [18 * 11 + 9] = [6] + [9] = [15] = [4]$.

(d) $[-82][207] = [6][9] = [54] = [10]$.

以上で使っているものは、以下の性質と、通常の整数の演算の性質だけである。(c), (d) も $-82+207$ や $(-82)(207)$ を計算してもよいが大きな数になるので、まずは、以下の性質 2, 3, 4 を用いている。

1. $[a]$ の定義：$[a] = \{x \in \boldsymbol{Z} \mid x \equiv a \pmod{11}\}$.
2. $[a] = [b] \Leftrightarrow a \equiv b \pmod{11} \Leftrightarrow 11 \mid b - a$.
3. $[a] = [a']$ かつ $[b] = [b']$ ならば $[a+b] = [a'+b']$. この性質から $[a] + [b] = [a+b]$ と定義する。
4. $[a] = [a']$ かつ $[b] = [b']$ ならば $[ab] = [a'b']$. この性質から $[a][b] = [ab]$ と定義する。

良問 7.9, 11, 13, 17, 19, Extra-Problem BCMMI 2007 3.1.6, 3.1.7 はよい問題だと思います。

4 写像

4.1 全射・単射・原像

定義 4.1 X, Y を集合とし、X の各元ごとに、Y の唯一つの元を割り当てる法則が与えられた時、この法則を、X から Y への写像 (mapping)[1]という。X をこの写像の定義域 (domain)、Y を終域 (codomain) という。X の元 x に割り当てられた Y の元 y を $f(x)$ と表す。$f(x)$ を x の f による像、f は x を $f(x)$ に写すなどという。また、f が集合 X から Y への写像であることを $f : X \longrightarrow Y$ とか、$X \xrightarrow{f} Y$ と書く。対応も明示するときは、$f : X \longrightarrow Y$ $(x \mapsto f(x))$ とも書く。

二つの写像 $f : X \longrightarrow Y$, $g : A \longrightarrow B$ が等しい ($f = g$ と書く) とは、$X = A$, $Y = B$ でかつ、$(\forall x \in X)[f(x) = g(x)]$ が成り立つことをいう。

Y^X: 集合 X から集合 Y への写像全体の集合を Y^X と書くことがある。

全射: 写像 $f : X \longrightarrow Y$ が次の条件を満たす時、f を全射 (surjection, epimorphism, onto mapping) であるという。

$$(\forall y \in Y)(\exists x \in X)[f(x) = y]^2.$$

単射: 写像 $f : X \longrightarrow Y$ が次の条件を満たす時、f を単射 (injection, monomorphism, one-to-one mapping[3]) であるという。

$$(\forall a \in X)(\forall b \in X)[(f(a) = f(b)) \Rightarrow (a = b)]^4.$$

全単射: 写像が全射かつ単射であるとき、全単射または双射 (bijection, one-to-one onto mapping) であるという。

像: $f : X \longrightarrow Y$ を写像、$A \subseteq X$ とするとき、$f(a)$ $(a \in A)$ 全体からなる Y の部分集合を $f(A)$ と書き、A の f による像 (the image of A) という。$f(X)$ を f の像 (the image of f) といい、$\mathrm{Im}f$ と書く[5]。

$$f(X) = \mathrm{Im}f = \{f(x) \mid x \in X\} = \{y \mid (y \in Y) \wedge (\exists x \in X)[f(x) = y]\} \subseteq Y.$$

原像: $f : X \longrightarrow Y$ を写像、$B \subseteq X$ とするとき、次の集合を $f^{-1}(B)$ と書き、B の f による原像または逆像 (the inverse image (or preimage) of B by f) という。$B = \{b\}$ のときは、$f^{-1}(B)$ を $f^{-1}(b)$ とも書く。

$$f^{-1}(B) = \{x \mid (x \in X)[f(x) \in B]\}.$$

$f^{-1}(B) \subseteq X$, また $b \in B$ とするとき、$f^{-1}(b) \subseteq X$ であることに注意する[6]。

合成: $f : X \longrightarrow Y$, $g : Y \longrightarrow Z$ を写像とする時、X の元 x の $g(f(x))$ への対応を h とすると、h は X から Z への写像を定義する。この写像を $h = g \circ f$ と書き、写像 f と g の合成 (composition) という。

恒等写像: 集合 X から X 自身への写像で、各 $x \in X$ をそれ自身に写す写像を X 上の恒等写像 (identity mapping) といい、id_X と書く。$(\forall x \in X)[id_X(x) = x]$。

---

[1] 関数または函数 (function) ともいうが、X, Y などは一般の集合であるので、数の集合と区別する意味で授業では「写像」を中心的に使うことにする。教科書では Function の和訳として「関数」を用いている。Function には「数」が入っていないので誤解の恐れはないのだが。

[2] 注：$(\forall x \in X)(\exists y \in Y)[f(x) = y]$ との違いは何か。

[3] one-to-one mapping は次の全単射を表すこともあるので注意。

[4] 注：$(\forall a \in X)(\forall b \in X)[f(a) = f(b) \Rightarrow (f(a) = f(b))]$ との違いは何か。

[5] この記号を用いると、f が全射であるということと $\mathrm{Im}f = Y$ であることとは同値である。

[6] $f^{-1}(B) = \emptyset$ の場合もある。ただし $f^{-1}(Y) = X$ が常に成立する。

逆写像: 写像 $f : X \longrightarrow Y$, $g : Y \longrightarrow X$ が $g \circ f = id_X$, $f \circ g = id_Y$ を満たす時、写像 g は、写像 f の逆写像 (inverse mapping) であるという。このとき、写像 f は、写像 g の逆写像である。(注：g が f の逆写像であるとき、$g = f^{-1}$ と書くこともある。このときは、$f^{-1}(y)$ は X の元をあらわし、X の部分集合ではない。f^{-1} を f の逆写像とすると明言して使う必要がある。)

制限: $f : X \longrightarrow Y$ を写像とし、$A \subseteq X$ とする。このとき、$f_{|A} : A \longrightarrow Y$ を $a \in A$ について $f_{|A}(a) = f(a)$ と定めたものを、f の A への制限 (restriction) という。

射影: $p_X : X \times Y \longrightarrow X$ $((x, y) \mapsto x)$, $p_Y : X \times Y \longrightarrow Y$ $((x, y) \mapsto y)$ をそれぞれ X への射影 (projection)、Y への射影という。

例 4.1 $f : \boldsymbol{R} \to [-1, 1] = \{x \mid (x \in \boldsymbol{R}) \wedge (-1 \leq x \leq 1)\}$ $(x \mapsto \sin x)$ とすると、f は全射であるが、単射ではない。$f^{-1}(0) = \{m\pi \mid m \in \boldsymbol{Z}\}$, $f^{-1}(-1/2) = \{m\pi - (-1)^m \frac{\pi}{6} \mid m \in \boldsymbol{Z}\}$ となる。$A = [-\pi, \pi]$ とすれば、$f_{|A} : A \to [-1, 1]$ は全単射で、逆写像 $\arcsin(x) = \sin^{-1}(x)$ を持つことになる。

4.2 写像の性質

$f : X \longrightarrow Y$ が写像であるとき、

$$G(f) = \{(x, y) \in X \times Y \mid f(x) = y\}$$

とする。$G(f)$ を f のグラフという[7]。$G(f)$ は次の条件を満たす。

(i) $(\forall x \in X)(\exists y \in Y)[(x, y) \in G(f)]$.

(ii) $(\forall x \in X)(\forall y \in Y)(\forall y' \in Y)[((x, y) \in G(f)) \wedge ((x, y') \in G(f))) \Rightarrow (y = y')]$.

命題 4.1 X, Y を集合とし、$f : X \longrightarrow Y$ および $g : Y \longrightarrow X$ を写像とする。$g \circ f = id_X$ であれば、f は単射、g は全射である。

証明 $x, x' \in X$ に対して、$f(x) = f(x') \Rightarrow x = x'$ を示せば良い。$f(x) = f(x')$ とすると、

$$x = id_X(x) = (g \circ f)(x) = g(f(x)) = g(f(x')) = (g \circ f)(x') = id_X(x') = x'$$

だから f は単射である。

g の定義域は Y で、値域は X だから、$x \in X$ に対して、$g(y) = x$ となる $y \in Y$ が存在することを示せば良い。$y = f(x)$ とすると、

$$g(y) = g(f(x)) = id_X(x) = x$$

だから、g は全射である。 ■

例 4.2 写像 f を次のように定義する。

$$f : \boldsymbol{R} \longrightarrow \boldsymbol{R} \left(f(0) = 1,\ x \neq 0 \text{ ならば } f(x) = \frac{1}{x} + 1 \right)$$

この写像は全単射である。これを示すために

$$g : \boldsymbol{R} \longrightarrow \boldsymbol{R} \left(g(1) = 0,\ x \neq 1 \text{ ならば } g(x) = \frac{1}{x - 1} \right)$$

とすると、これは確かに $\boldsymbol{R}$ から $\boldsymbol{R}$ への写像で、$g(f(x)) = x$, $f(g(x)) = x$ が成り立っていることが分かる。上の命題を用いると、f も g も全単射であることが分かる。

[7]教科書では $G(f)$ を関数と呼んでいるが一般的ではない。しかし $G(f) \subseteq X \times X$ で (i), (ii) を満たすものが与えられれば、$f : X \to Y$ を定義できるので、本質的には同じ概念です。$f(x)$ はどのように定義しますか。条件 (i), (ii) をひとまとめに、$(\forall x \in X)(\exists_1 y \in Y)[(x, y) \in G(f)]$ と書くこともある。$\exists_1$ または $\exists!$ は一意的に（ただ一つ）存在する意。

5　数学的帰納法

5.1　整列集合と数学的帰納法の原理

定義 5.1 $(A, \leq)$ を半順序集合とする[8]。$a, b \in A$ に対して、$a \leq b$ または $b \leq a$ が成立する時 $\leq$ を全順序、A を全順序集合 (totally ordered set) という。

A が全順序集合で、A の空でない部分集合がつねに、最小元をもつとき、A は整列集合 (well-ordered set) である (または well-ordering law を満たす) という。$S \subseteq A$ において、s が S の最小元であるとは、$s \in S$ かつ $x \in S$ ならば $s \leq x$ が成立することをいう。$s = \min S$ とも書く。

The Well-Ordering Law (WO):　m を整数とするとき、$\boldsymbol{N}_m = \{x \mid (x \in \boldsymbol{Z}) \wedge (x \geq m)\}$ とおく[9]。このとき $\boldsymbol{N}_m$ の空でない部分集合は、最小元をもつ。すなわち、$(\boldsymbol{N}_m, \leq)$ は整列集合である。$(\boldsymbol{Z}, \leq)$ は全順序集合であるが、整列集合ではない。

定理 5.1 (Mathematical Induction) $m \in \boldsymbol{Z}$ とし、$P(n)$ は、整数 $n \geq m$ に関するある命題を表すものとする。命題 $P(n)$ は以下の条件を満たすと仮定する。

(I) $P(m)$ は真。

(II) $k \geq m$ なる各 k について、$P(k)$ が真であるとの仮定のもとでは、$P(k+1)$ は真である。

すると、命題 $P(n)$ はすべての $n \geq m$ なる整数に対して真である。

証明　$\boldsymbol{N}_m = \{x \mid (x \in \boldsymbol{Z}) \wedge (x \geq m)\}$ とする。ここで

$$S = \{x \mid (x \in \boldsymbol{N}_m) \wedge \sim P(x)\}$$

とおく。$S \neq \emptyset$ とする。**WO** により $s = \min S$ が存在する。$s \in S$ だから $\sim P(s)$ が真である。(I) より $P(m)$ は真だから $s \neq m$。$k = s-1$ とすると、$k \in \boldsymbol{N}_m$ でかつ、$P(k)$ は真である。したがって、(II) により $P(k+1) = P(s)$ は真。これは、$\sim P(s)$ に反する。したがって、$S = \emptyset$。これは、$(\forall x)[(x \in \boldsymbol{N}_m) \Rightarrow P(x)]$ を意味するから、命題 $P(n)$ はすべての $n \geq m$ なる整数に対して真である。 ■

これは次のようにも表現できる。

$$(P(m) \wedge (\forall k)[(k \geq m) \wedge P(k) \Rightarrow P(k+1)]) \Rightarrow (\forall n)[(n \geq m) \Rightarrow P(k)].$$

上の定理で、(I), (II) を次のようにしても結論が成立する。証明を試みよ。

(O) $k \geq m$ なる各 k について、$m \leq x < k$ のとき[10] $P(x)$ が真であるとの仮定のもとで、$P(k)$ は真である。

さらに、整列集合に拡張することもできる。整列集合上の数学帰納法を超限帰納法ともいう。

定理 5.2 (Transfinite Induction) W を整列集合、$P(x)$ は、$x \in W$ に関するある命題を表すものとする。命題 $P(x)$ は以下の条件を満たすと仮定する。

W の任意の元 a について、$x < a$ なるすべての x について、$P(x)$ が真であるとの仮定のもとでは、$P(a)$ は真である。

このとき、命題 $P(x)$ はすべての $x \in W$ に対して真である。

---

[8] すなわち、$\leq$ は、A 上に定義された関係で、半対称律 : $(a \leq b) \wedge (b \leq a) \Rightarrow a = b$ および、推移律 : $(a \leq b) \wedge (b \leq c) \Rightarrow a \leq c$ が成り立つ。また、$a \leq b$ かつ $a \neq b$ であるとき $a < b$ と書く。

[9] $\boldsymbol{N}_1$ を $\boldsymbol{N}$ と書き、また $\boldsymbol{N}_0$ を $\boldsymbol{Z}^+$ とも書く。

[10] $k = m$ のときには、$m \leq x < k$ なる x は存在しないから、$P(m)$ は結局真でなければならず (I) を暗黙のうちに仮定している。しかし、実際には、(I) は別に示さず、(O) の形で証明できることもあるので、この形で記す。教科書の p.19 にある The Principle of Mathematical Induction – Alternate From 参照。

5.2 数学的帰納法または整列可能性を用いた証明

例 5.1 任意の自然数 n について次の等式が成り立つ。

$$1^3 + 2^3 + 3^3 + \cdots + n^3 = \left(\frac{n(n+1)}{2}\right)^2.$$

証明 $n = 1$ とおくと両辺は 1 であるから等式が成り立つ。

$n = k$ の時に、等式が成立するとする。$n = k + 1$ のとき

$$\begin{aligned} & 1^3 + 2^3 + 3^3 + \cdots + k^3 + (k+1)^3 \\ = \ & \left(1^3 + 2^3 + 3^3 + \cdots + k^3\right) + (k+1)^3 \qquad \text{（帰納法の仮定を用いると[11]）} \\ = \ & \left(\frac{k(k+1)}{2}\right)^2 + (k+1)^3 = \frac{(k+1)^2}{4}(k^2 + 4(k+1)) = \frac{(k+1)^2}{4}(k+2)^2 \\ = \ & \left(\frac{(k+1)(k+2)}{2}\right)^2. \end{aligned}$$

最後の式は証明すべき等式の右辺の n に $k+1$ を代入した式だから、$n = k$ の時に等式が成立すると仮定して、$n = k + 1$ の時に等式が成立することが示されたから、数学的帰納法によってすべての自然数 n について、等式は成り立つ。 ■

例 5.2 2 以上の自然数は、素数[12]の積に書くことができる。

証明 n を 2 以上の自然数とする。n が素数の時は良いから、素数ではないとする。すると、1 と n 以外の正の約数 m_1 を持つから、$n = m_1 \cdot m_2$ と書くことができ、$2 \leq m_1, m_2 < n$ である。したがって帰納法の仮定から、m_1 も m_2 も素数の積に書くことができる。n は m_1 と m_2 の積だから、n 自身素数の積に書くことができる。2 以上 n 未満の自然数について、素数の積に書けることを仮定して n 自身が素数の積に書くことができることが証明できたから、数学的帰納法によって、2 以上のすべての自然数は素数の積に書くとができることが証明された。 ■

例 5.3 $a, b \in \boldsymbol{Z}$ としたとき、次の三つの条件を満たす数 d がただ一つ存在する。これを、a, b の最大公約数とよび $d = \gcd\{a, b\}$ と書く。このとき、$d = ax + by$ となる $x, y \in \boldsymbol{Z}$ が存在する。

$$\text{(i) } d \geq 0, \quad \text{(ii) } d \mid a \text{ かつ } d \mid b, \quad \text{(iii) } c \mid a \text{ かつ } c \mid b \text{ ならば } c \mid d.$$

証明 $d = ax + by$ $(x, y \in \boldsymbol{Z})$ と書ける整数の中で、(i), (ii), (iii) を満たすものが存在することを示す。$a = b = 0$ のときは、$d = 0$, $x = y = 0$ とすればよいから、$a \neq 0$ または $b \neq 0$ とする。

$$S = \{ax + by > 0 \mid x \in \boldsymbol{Z},\ y \in \boldsymbol{Z}\} \subseteq \boldsymbol{N}$$

とする。$a \neq 0$ または $b \neq 0$ だから、$x = a$, $y = b$ とすれば $ax + by = a^2 + b^2 > 0$ だから、$S \neq \emptyset$ である。$\boldsymbol{N}$ は整列集合だから S は最小元を持つ。それを d とする。$d > 0$ だから (i) を満たす。また S の定義より $d = ax + by$ となる $x, y \in \boldsymbol{Z}$ が存在する。$c \mid a$ かつ $c \mid b$ とすると、$d = ax + by$ だから $c \mid d$ であり (iii) を満たす。$d \nmid a$ とする。すると、$a = dq + r$, $0 < r < d$ と書くことができる。すると $r = a - dq = a - (ax + by)q = a(1 - qx) + b(-qy)$ だから S の定義より $r \in S$ ところが $r < d$ だったから d の最小性に反する。したがって、$d \mid a$ である。同様に、$d \mid b$ である。よって d は (ii) を満たし、d は求める性質を持つことがわかった。

d' も条件を満たすと、d' が (ii) を満たし、d が (iii) を満たすことから $d' \mid d$。同様にして $d \mid d'$ を得る。(i) より $d = d'$ となる。したがって (i), (ii), (iii) を満たすものは、ただ一つである。 ■

[12] 素数は 2 以上の自然数で 1 とその数自身以外に、正の約数を持たないものを言う。また、素数自身も素数の一つの積と考える。

6　代数系

6.1　整数の整除

$a, b \in \boldsymbol{Z}$ に対して、$b = ac$ となる整数 c が存在するとき、a は b を整除する (a divides b) といい $a \mid b$ と書く。b は a で割り切れる (b is divisible by a) などとも言うが、定義はあくまでも、

$$(\forall a \in \boldsymbol{Z})(\forall b \in \boldsymbol{Z})[a \mid b \Leftrightarrow (\exists c \in \boldsymbol{Z})[b = ac]].$$

命題 6.1 (4.1, 4.3, Ex.4.2) $a, b, c \in \boldsymbol{Z}$ とする。

(i) 常に $1 \mid a$, $a \mid 0$ でありかつ $0 \mid a \Leftrightarrow a = 0$.

(ii) $(a \mid b) \wedge (b \mid c) \Rightarrow a \mid c$。

(iii) $(a \mid b) \wedge (b \mid a) \Leftrightarrow a = \pm b$.

(iv) $(a \mid b) \wedge (a \mid c) \Leftrightarrow a \mid bx + cy$ *for all* $x, y \in \boldsymbol{Z}$.

命題 6.2 $a, b \in \boldsymbol{Z}$ とする。$b \neq 0$ ならば $a = qb + r$ $(0 \leq r < |b|)$ を満足する $q, r \in \boldsymbol{Z}$ がただ一組に限って存在する。すなわち、

$$(\forall a \in \boldsymbol{Z})(\forall b \in \boldsymbol{Z})[(b \neq 0) \Rightarrow (\exists! q \in \boldsymbol{Z})(\exists! r \in \boldsymbol{Z})[(a = bq + r) \wedge (0 \leq r < |b|)].$$

最大公約数・素因数分解

定義 6.1 $a, b \in \boldsymbol{Z}$ とする。次の性質を満たす $d \in \boldsymbol{Z}$ を a, b の最大公約数 (the greatest common divisor) といい $d = \gcd\{a, b\}$ と書く。$\gcd\{a, b\} = 1$ であるとき a, b は互いに素である (relatively prime) という。

(i) $d \geq 0$.

(ii) $d \mid a$, $d \mid b$.

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

定理 6.3 $a, b \in \boldsymbol{Z}$ としたとき、最大公約数 $d = \gcd\{a, b\}$ がただ一つ存在する。このとき、$d = ax + by$ となる $x, y \in \boldsymbol{Z}$ が存在する[13]。

証明　d と d' が共に、$\gcd\{a, b\}$ の条件を満たすとする。すると、d が (ii) を、d' が (iii) を満たすことより、$d \mid d'$。同様にして、$d' \mid d$。(i) の条件と、命題 6.1 (iii) より $d = d'$ となる。従って、一意性は成立する。

$a, b \in \boldsymbol{Z}$ の最大公約数の存在を $|b|$ に関する帰納法で示す。$|b| = 0$ とすると、$b = 0$ で $d = |a|$ は、定義 6.1 の条件を満たす。(2.2.2) を用いると、

$$(\exists q \in \boldsymbol{Z})(\exists r \in \boldsymbol{Z})[(a = bq + r) \wedge (0 \leq r < |b|)]$$

である。帰納法の仮定により、$d = \gcd\{b, r\}$ は存在する。d が $\gcd\{a, b\}$ の条件を満たすことを示す。(i) は明らか。$a = bq + r$ だから (ii) も満たす。$c \mid a$, $c \mid b$ とすると、$r = a \cdot 1 - b \cdot q$ だから (2.2.1) より $c \mid r$ したがって、$d = \gcd\{b, r\}$ であることより $c \mid d$。したがって、$d = \gcd\{a, b\}$ であり、定理の前半が証明された。

[13] 例 5.2 参照

$d = ax+by$ となる $x, y \in \boldsymbol{Z}$ が存在することも、$|b|$ に関する帰納法で示す。$|b| = 0$ のときは、$\gcd\{a, b\} = |a|$ だったから、$a = 0$ のときは、$x = y = 0$ とし、$a \neq 0$ のときは、$x = a/|a|$, $y = 0$ とすればよい。$|b| > 0$ とすると、帰納法の仮定から 上と同じく $a = bq + r$ とすると、$d = x'b + y'r$ となる整数 x', y' が存在する。したがって、$d = x'b + y'(a - bq) = y'a + (x' - qy')b$ と書ける。そこで $x = y'$, $y = x' - qy$ とすればよい。 ■

上の証明は、実際に $d = \gcd\{a, b\}$ を求めたり $d = xa + yb$ となる $x, y \in \boldsymbol{Z}$ を求める方法（算法またはアルゴリズムとよぶ）も与えている。このアルゴリズムは特にユークリッド算法 (Euclidean Algorithm) と呼ばれる[14]。

さらに、$\langle a, b\rangle = \{ax + by \mid x, y \in \boldsymbol{Z}\}$ とすると、$\langle a, b\rangle = \{zd \mid z \in \boldsymbol{Z}\}$ であることがわかる。まず定理より $d \in \langle a, b\rangle$ だから $\langle a, b\rangle = \{ax + by \mid x, y \in \boldsymbol{Z}\} \supseteq \{zd \mid z \in \boldsymbol{Z}\}$ である。また、$a, b \in \{zd \mid z \in \boldsymbol{Z}\}$ だから $\langle a, b\rangle \subseteq \{zd \mid z \in \boldsymbol{Z}\}$ である。

例えば、ここで、$a = 132$, $b = -36$ としてみる。

$$132 = (-36)(-3) + 24,\ -36 = 24(-2) + 12,\ 24 = 12 \cdot 2 + 0$$

であるから、最後の 0 でない剰余 12 が 132 と -36 の最大公約数である。実際、上の考察から

$$\gcd\{a, b\} = \gcd\{132, -36\} = \gcd\{-36, 24\} = \gcd\{24, 12\} = \gcd\{12, 0\} = 12.$$

さらに 12 が $-36x + 24y$ の形に書けるはずであるが、それは、$-36 = 24(-2) + 12$ から $x = 1$, $y = 2$ とすれば良い。また、$12 = \gcd\{132, -36\}$ であるが、$132 = (-36)(-3) + 24$ で $24 = 132 + (-36)3$ と書けているから、$12 = -36 + 24 \cdot 2$ を用いれば、次のようになる。

$$12 = -36 + 24 \cdot 2 = -36 + (132 + (-36)3) \cdot 2 = 132 \cdot 2 + (-36)7.$$

次の補題は、a, b の最大公倍数 d が $d = ax + by$ の形に表せることを利用したものであるが、素因数分解の一意性を証明する鍵となるものである。

補題 6.4 $a, b, m \in \boldsymbol{Z}$ とする。このとき

$$(m \mid a \cdot b) \wedge (\gcd\{m, a\} = 1) \Rightarrow m \mid b.$$

証明 $x, y \in \boldsymbol{Z}$ で $1 = \gcd\{m, a\} = mx + ay$ となるものが存在する。両辺に b をかけると $b = mbx + aby$ となる。仮定より $m \mid ab$ だから (2.2.1) より $m \mid b$ である。 ■

素数は 2 以上の整数で 1 とその数自身以外に正の約数を持たない数である。すなわち p が素数であるとは

$$(p \in \boldsymbol{Z}) \wedge (p \geq 2) \wedge (\forall m \in \boldsymbol{Z})[(m \mid p) \wedge (m > 0) \Rightarrow (m = p) \vee (m = 1)].$$

2 以上の数で素数ではないものを合成数 (a composite number) という。

定理 6.5 2 以上の整数は素数の積として表すことができる。さらに積の順序を度外視するとこの表し方は一意的である。

[14] 純粋理論としての抽象代数では例 5.2 の様に存在型の定理で十分とされる面もあるが、実際に求めることが重要な場合には、アルゴリズムは不可欠である。コンピュータの発達とその様々な技術の応用がされはじめ、素数判定問題などとも関連して、このアルゴリズムも重要な位置を占めるようになった。一見このユークリッド算法で十分に見えるが、a, b の最大公約数を a, b の一次結合で書くことなどを考えると、係数膨張という現象が起こり、様々な改善が必要になる。計算量などの問題とも関連して、情報科学において重要な課題である。

6.2 m を法とした合同

m を正の整数とする。$a, b \in \boldsymbol{Z}$ が m を法として合同 (congruent modulo m) を $a \equiv b \pmod{m}$ と書き、次のように定義する。

$$a \equiv b \pmod{m} \Leftrightarrow m \mid a - b.$$

$a \equiv b \pmod{m}$ は $\boldsymbol{Z}$ に同値条件を定義する。すなわち、

(i) $a \equiv a \pmod{m}$.

(ii) $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$.

(iii) $(a \equiv b \pmod{m}) \wedge (b \equiv c \pmod{m}) \Rightarrow a \equiv c \pmod{m}$.

a の属する同値類を $[a]$ または $[a]_m$ と書く。

$$[a]_m = \{x \in \boldsymbol{Z} \mid x \equiv a \pmod{m}\} = \{x \mid (\exists q \in \boldsymbol{Z})[x = mq + a]\}.$$

(2.2.2) を用いて $a = mq + r$, $0 \leq r < m$ と書くと、$a \equiv r \pmod{m}$ だから、m を法とした合同に関する同値類は $[0], [1], [2], \ldots, [m-1]$ の m 個であることがわかる。全ての同値類からなる集合を $\boldsymbol{Z}_m$ と書く。すなわち、$\boldsymbol{Z}_m = \{[0], [1], \ldots, [m-1]\}$.

$\boldsymbol{Z}_m$ に和と積とよばれる演算を定義する。

$$[a] + [b] = [a + b], \quad [a] \cdot [b] = [ab].$$

$[a] = [a']$, $[b] = [b']$ ならば $[a + b] = [a' + b']$、$[ab] = [a'b']$ が成り立ち、これらの演算は Well-defined （すなわち、$[a]$, $[b]$ に対して、$[a + b]$ および $[ab]$ が一意的に決まり、演算が定義される）である。

命題 6.6 (4.9, 4.10, Ex.7.43) m を正の整数。$[a]$, $[b]$, $[c] \in \boldsymbol{Z}_m$ とする。このとき、

(i) $[a] + [b] = [b] + [a]$ かつ $[a] \cdot [b] = [b] \cdot [a]$。 *(交換律, commutativity law)*

(ii) $([a] + [b]) + [c] = [a] + ([b] + [c])$ かつ $([a] \cdot [b]) \cdot [c] = [a] \cdot ([b] \cdot [c])$。 *(結合律, associativity law)*

(iii) $([a] + [b]) \cdot [c] = [a] \cdot [c] + [b] \cdot [c]$。 *(分配律, distributive law)*

(iv) $[0] + [a] = [a]$ かつ $[1] \cdot [a] = [a]$。 *(単位元の存在, existence of identity elements)*

(v) $[a] + [-a] = [0]$。 *(加法に関する逆元の存在, existence of an inverse in addition)*

$m = 0$ の場合は考えていないが、$a \equiv b \pmod{0} \Leftrightarrow 0 \mid a - b$ とすれば、$a \equiv b \pmod{0} \Leftrightarrow a = b$ で、$[a] = \{a\}$ となるので、議論は、まったく同じように進めることができる。ただし、$\boldsymbol{Z}_0$ は $[a]$ を a 自身と見ることにより $\boldsymbol{Z}$ と何らかわらない。こう考えると (2.3.2) は $\boldsymbol{Z}$ の加法と乗法に関する、基本的な性質であり、その基本的な性質が $\boldsymbol{Z}_m$ においても成り立つことを主張していることもわかる。

[0] は 0 と同じように、[1] は 1 と同じような働きをするので、[0] を加法の単位元または零元といい 0 であらわし、[1] を乗法の単位元または単に単位元とよび 1 で表すこともある。しかし、$[2]_6 \cdot [3]_6 = [0]_6$ からもわかるように、$a, b \in \boldsymbol{Z}_m$ において $ab = 0 \Rightarrow (a = 0) \vee (b = 0)$ が得られるわけではないので注意を要する。その意味で、次の命題は重要である。

命題 6.7 m を正の整数、$a \in \boldsymbol{Z}$ とするとき $\boldsymbol{Z}_m$ において

$$(\exists x \in \boldsymbol{Z})[[a][x] = [1]] \Leftrightarrow \gcd\{a, m\} = 1.$$

6.3 演算とその性質

定義 6.2 集合 A に（二項）演算 $\circ$ が定義されているとは、次で定義される f が写像であることをいう。

$$f : A \times A \to A \ ((a, b) \mapsto a \circ b)$$

どの順序に演算をするかを表すため括弧を用いる。$\circ$ が写像 f によって決まる演算であるとき、$(a \circ b) \circ c = f(f(a, b), c)$ であり、$a \circ (b \circ c) = f(a, f(b, c))$ を表す。

定義 6.3 (1) 集合 A に演算 $\circ$ が定義されているとする。

結合法則 $(\forall a \in A)(\forall b \in A)(\forall c \in A)[(a \circ b) \circ c = a \circ (b \circ c)]$.

単位元の存在 $(\exists e \in A)(\forall a \in A)[a \circ e = e \circ a = a]$. この e を単位元という。

逆元の存在 単位元 e は存在するとする。このとき $a \in A$ に対し
$a \circ a' = a' \circ a = e$ を満たす $a' \in A$ を a の逆元という。

交換法則 $(\forall a \in A)(\forall b \in A)[a \circ b = b \circ a]$.

(2) 集合 A に演算 $\circ$ および $*$ が定義されているとする。

$*$ に関する左分配法則 $(\forall a \in A)(\forall b \in A)(\forall c \in A)[a * (b \circ c) = a * b \circ a * c]$.

$*$ に関する右分配法則 $(\forall a \in A)(\forall b \in A)(\forall c \in A)[(a \circ b) * c = a * c \circ b * c]$.

6.4 いろいろな代数系

定義 6.4 (1) 集合 A に演算 $\circ$ が定義されているとする。

1. 結合法則が成り立つとき、$(A, \circ)$ を半群 (semi-group) という。
2. 半群にさらに単位元がそんざいするとき、$(A, \circ)$ をモノイド (monoid) という。
3. 各元に対し逆元が存在するモノイド $(A, \circ)$ を群 (group) という。
4. 半群、モノイド、群がそれぞれ交換法則をみたすとき、可換半群、可換モノイド、可換群という。

(2) 集合 A に演算 $\circ$ および $*$ が定義されているとする。

1. $\circ$ に関して可換群になり、$*$ に関して半群であり、かつ $*$ に関して、右および左分配法則をもつとき、$(A, \circ, *)$ を環 (ring) という。
2. 環 $(A, \circ, *)$ において、$*$ に関してもモノイドであり、$\circ$ と $*$ に関する単位元がことなるとき単位元を持つ環 (unital ring) という。
3. 単位元を持つ環 $(A, \circ, *)$ がさらに、$\circ$ に関する単位元以外の元について逆元をもつとき、斜体 (skew field) であるという。
4. $*$ に関して交換法則をみたす環を可換環、単位元をもつ環を単位元をもつ可換環、斜体を体という。

例 6.1 1. $(\boldsymbol{N}, +)$ は可換半群。$(\boldsymbol{Z}, \cdot)$ 可換モノイド。$(\boldsymbol{Z}, +), (\boldsymbol{Z}_m, +)$ は可換群。$(\mathrm{GL}_n(\boldsymbol{R}), \cdot)$ は、非可換群。ここで、$\mathrm{GL}_n(\boldsymbol{R})$ は n 次正則行列全体で、演算は、行列のかけ算。

2. $(\boldsymbol{Z}, +, \cdot)$, $(\boldsymbol{Z}_m, +, \cdot)$ は可換環。$(\mathrm{Mat}_n(\boldsymbol{R}), +, \cdot)$ は非可換環。$(\boldsymbol{Q}, +, \cdot)$, $(\boldsymbol{R}, +, \cdot)$ は可換体。

7　集合の濃度（基数）

7.1　集合の対等・可算集合

$\boldsymbol{N}$ は自然数全体の集合、 A から 集合 B への写像全体からなる集合を B^A または $\mathrm{Map}(A,B)$ と書く。

定義 7.1　1. 集合 X から集合 Y への全単射（双射）が存在する時、X は Y と対等（equinumerous, equipollent）または個数同値 (numerically equivalent) であるといい $X \sim Y$ と書く。集合における関係 $\sim$ は同値関係である。

2. 互いに対等な集合の同値類のおのおのに一つの記号を対応させて、これを集合の濃度（または基数, cardinal）という。集合 X の濃度を $|X|$（または $\sharp X$）であらわす。

3. n を自然数としたとき、集合 $I(n) = \{1, 2, \ldots, n\}$ と対等な集合の濃度を n で表す。$|\emptyset| = 0$ とする。集合 X の濃度が n であるとは、X が n 個の要素をもつことである。

4. 濃度が 0 またはある自然数である集合を有限集合という。

5. 自然数の集合と対等である集合を可算無限集合という。その濃度を $\aleph_0$（アレフ・ゼロ）で表す。

6. 可算無限集合と、有限集合をあわせて、可算 (countable) 集合または可付番集合という。これを高々可算ともいう。

命題 7.1 自然数 n、m について、濃度が n の集合と、濃度が m の集合が対等ならば $n = m$ である。すなわち、$I(m) \sim I(n) \Leftrightarrow m = n$。

上の命題は、有限集合においては、集合の濃度が通常の元の個数と対応していることを示している。無論、明らかではないのは、$\Rightarrow$ である。対偶を帰納法で証明するなどして示してみて下さい。次の例は、無限集合のときには、有限の時とは少し違うことが起こることを示しています。

例 7.1　1. $2\boldsymbol{Z} = \{2n \mid n \in \boldsymbol{Z}\}$ で偶数全体の集合を表すとする。$g : \boldsymbol{Z} \to 2\boldsymbol{Z}\ (n \mapsto 2n)$ は全単射である。したがって $\boldsymbol{Z} \sim 2\boldsymbol{Z}$。

$1 + 2\boldsymbol{Z} = \{2n+1 \mid n \in \boldsymbol{Z}\}$ で奇数全体の集合を表すとする。$g : \boldsymbol{Z} \to 1 + 2\boldsymbol{Z}\ (n \mapsto 2n+1)$ は全単射である。したがって $\boldsymbol{Z} \sim 1 + 2\boldsymbol{Z}$。

$2\boldsymbol{Z} \cap 1 + 2\boldsymbol{Z} = \emptyset$、$\boldsymbol{Z} = 2\boldsymbol{Z} \cup 1 + 2\boldsymbol{Z}$ であるが、$|\boldsymbol{Z}| = |2\boldsymbol{Z}| = |1 + 2\boldsymbol{Z}|$ となっている。

2. $f : \boldsymbol{N} \to \boldsymbol{Z}\ \left(n \mapsto \dfrac{1 + (-1)^n(2n-1)}{4}\right)$ とすると[15]、f は全単射であるから、$\boldsymbol{N} \sim \boldsymbol{Z}$ である。

3. 以上のことから $\aleph_0 = |\boldsymbol{N}| = |\boldsymbol{Z}| = |2\boldsymbol{Z}| = |1 + 2\boldsymbol{Z}|$。

命題 7.2　(1) 集合 S に対して、単射 $f : S \to \boldsymbol{N}$ が存在すれば、S は可算集合である[16]。

(2) 集合 S に対して、全射 $f : \boldsymbol{N} \to S$ が存在すれば、S は可算集合である。

(3) $\boldsymbol{N} \times \boldsymbol{N} \sim \boldsymbol{N}$ すなわち、$|\boldsymbol{N} \times \boldsymbol{N}| = \aleph_0$。

(4) 集合族 $\{X_i\}_{i \in \boldsymbol{N}}$ において、どの X_i も高々可算ならば、$U = \bigcup_{i=1}^{\infty} X_i$ も高々可算である。

---

[15] $f(2m-1) = -m+1$, $f(2m) = m$ となっている事に注意。

[16] これから「集合 S から可算集合 A への単射 $f : S \to A$ が存在すれば S は可算集合である」こと特に「可算集合の任意の部分集合は可算集合である」ことが簡単に導き出される。

証明　(1) 一般的に、$f : X \to Y$ を単射とすると、$X \sim f(X)$ である。f は X から $f(X) = \mathrm{Im}f = \mathrm{ran}f$ への全単射とも見ることができるからである。 S を無限集合とする。f は単射で、$f(S) \subseteq \boldsymbol{N}$ だから、$f(S) = \{i_1, i_2, i_3, \ldots, i_n, \ldots\}$, $i_1 < i_2 < i_3 < \cdots < i_n < \cdots$ とすると、$g : \boldsymbol{N} \to f(S)\ (n \mapsto i_n)$ は全単射である。従って、$S \sim f(S) \sim \boldsymbol{N}$。 ■

(2) $g : S \to \boldsymbol{N}\ (s \mapsto \min f^{-1}(s))$ とする。$f^{-1}(s) = \{n \in \boldsymbol{N} midf(n) = s\} \subseteq \boldsymbol{N}$ で、f は全射だから $f^{-1}(s) \neq \emptyset$ かつ $\boldsymbol{N}$ は整列集合だったから $\min f^{-1}(s)$ は必ず存在し、かつただ一つの元を定める。したがって g は写像となる。$g(s) = m$ ならば $m = \min f^{-1}(s)$ だから $f(m) = s$。したがって $f(g(s)) = s$ すなわち、$f \circ g = id_S$。これより、g は単射である。(1) より S は可算集合である。 ■

(3) $h : \boldsymbol{N} \times \boldsymbol{N} \to \boldsymbol{N}((m, n) \mapsto 2^{m-1}(2n-1))$ とする。$2^{m-1}(2n-1) = 2^{m'-1}(2n'-1)$ とすると、素因数分解の一位性から $m = m'$。したがって、$n = n'$。すなわち、h は単射である。任意の自然数は、$2^{m-1}(2n-1)$ $(m, n) \in \boldsymbol{N} \times \boldsymbol{N}$ の形に書けるから、h は全射でもある。したがって h は全単射である。 ■

(4) X_i はたかだか可算だから、$\emptyset, I(n)$ または $\boldsymbol{N}$ と対等である。そこで、必要なら番号を付け替えて $X_i \neq \emptyset$ とし、各 i について $f_i : X_i \to \boldsymbol{N}$ を単射とする。$x_i \in X_i$ とし、$g_i : \boldsymbol{N} \to X_i$ を $f_i(x) = n$ となっているときは、$g_i(n) = x$、$x \notin f_i(X_i)$ のときは $g_i(x) = x_i$ とすると、g_i は全射。$g : \boldsymbol{N} \times \boldsymbol{N} \to U\ ((i, n) \mapsto g_i(n))$ とすると g は全射である。$g \circ h$ は、$\boldsymbol{N}$ から S への全射だから (2) より U は可算。(X_i 達に共通部分がなければ、$f : U \to \boldsymbol{N} \times \boldsymbol{N}$ に単射を簡単に作ることができます。$u \in X_i$ のとき 上の f_i を用いて $f(u) = (i, f_i(u))$ とすれば良いからです。) ■

命題 7.3 *A, B, C, D を $A \sim C$、$B \sim D$ なる集合とする。*

(1) *$A \cap B = \emptyset = C \cap D$ ならば $A \cup B \sim C \cup D$ である。*

(2) *$A \times B \sim C \times D$ である。*

(3) *$P(A) \sim P(C)$ である。*

(4) *$B^A \sim D^C$ すなわち $\mathrm{Map}(A, B) \sim \mathrm{Map}(C, D)$ である。*

7.2　無限集合

定理 7.4 *任意の無限集合は可算な無限部分集合を含む。*

証明　S を無限集合とする。$x_1 \in S$, $x_2 \in S - \{x_1\}$, とし、x_n まで選んだとき、$S_n = S - \{x_1, x_2, \ldots, x_n\}$ は空集合ではないから $x_{n+1} \in S_n$ を取ることができる。したがって、$\{x_1, x_2, \ldots\}$ は可算な無限部分集合である。 ■

命題 7.5 *X が無限集合、A が X の高々可算な部分集合で、$X - A$ が無限集合ならば、$X - A$ と X は対等である。*

証明　定理 7.4 によって、$X - A$ の部分集合 B で $B \sim \boldsymbol{N}$ となるものが存在する。$A \cup B$ が可算無限集合であることは簡単にわかるから、$A \cup B \sim B$。そこで、$f : A \cup B \to B$ を全単射とし、$g : X \to X - A$ を $A \cup B$ 上では f、$X - (A \cup B)$ 上では恒等写像とすると、g は全単射であり、$X - A$ と X は対等である。■

注　上の命題では、$f : N \to S$ を全射とするとき、単射 $g : S \to \boldsymbol{N}$ で $f \circ g = id_S$ となるものを構成しました。これは、一般の集合で可能でしょうか。すなわち、$f : X \to Y$ を全射とする。この時、単射 $g : Y \to X$ で $g \circ f = id_Y$ となるものが存在するでしょうか。これが常に存在することを保証するのが「選択公理」と言われるもので、他の公理と独立である（すなわち、これを認めても、認めなくてもそれぞれの数学のモデルが構成できる）ということが知られています。通常は選択公理を認めて数学の理論を構築することが普通です。しかし、単射 $g : Y \to X$ が与えられているとき 全射 $f : X \to Y$ で $f \circ g = id_Y$ となるものはいつでも存在します。証明できますが。

8 濃度の比較

8.1 Cantor–Bernstein の定理

定義 8.1 集合 X から集合 Y への単射が存在するとき $|X| \leq |Y|$ と書き、X の濃度は Y の濃度を越えないという。また、$|X| \leq |Y|$ かつ $|X| \neq |Y|$ のとき $|X| < |Y|$ と書く。

定理 8.1 (1.4.2 (Cantor–Bernstein)) 集合 X、Y に対し、$|X| \leq |Y|$ かつ $|Y| \leq |X|$ ならば $|X| = |Y|$ である。

証明　$f : X \to Y$、$g : Y \to X$ を単射とする。f および g は全射ではないとして良い。$X - g(Y)$、$Y - f(X)$ の元を原始元と呼び、$f(x) = y$ のとき、y を x の子、x を y の親と呼ぶことにする。g についても同様。

第一種 有限回の親をとる操作で X の原始元にたどりつく。

第二種 有限回の親をとる操作で Y の原始元にたどりつく。

第三種 親を取る操作が無限に操作が続く。

ここで、X_i を X の第 i 種の元の集合 $(i = 1, 2, 3)$、Y_j を Y の第 j 種の元の集合 $(j = 1, 2, 3)$ とする。この時、以下が成立する。

1. $X = X_1 \cup X_2 \cup X_3$ (disjoint)、$Y = Y_1 \cup Y_2 \cup Y_3$ (disjoint)。
2. 第 i 種の元の子は第 i 種である。第 i 種の元に親があれば（すなわち原始元でなければ）その親も第 i 種である。
3. $f(X_1) = Y_1$。（注：Y_1 の元は原始元ではない。）
4. $g(Y_2 \cup Y_3) = X_2 \cup X_3$。（注：$X_2$ の元および X_3 の元は原始限ではない。）

$h : X \to Y$ $(h(x) = f(x)$ if $x \in X_1, g^{-1}(x)$ (if $x \in X_2 \cup X_3 = g(Y_2 \cup Y_3))$、と定義すると、$h$ は全単射である。 ■

8.2 非可算集合

X および Y を集合とする。$|X| \leq |Y|$ かつ $|X| \neq |Y|$ であるとき、$|X| < |Y|$ と書くことにする。

定理 8.2 (1.4.5) 任意の集合 X に対して、そのべき集合 $P(X)$ の濃度は X の濃度より大きい。すなわち、$|X| < |P(X)|$。

証明　$|X| \leq |P(X)|$ は明らか。$(\psi : X \to P(X)\ (x \mapsto \{x\})$ を考えよ。$)$

φ を X から $P(X)$ への写像とする。各 $x \in X$ に対して、 $\varphi(x) \subseteq X$ である。ここで、$B = \{x \mid (x \in X) \wedge (x \notin \varphi(x))\}$ とおく。$B \subseteq X$ である。$z \in X$ とすると、$z \in \varphi(z)$ であるか $z \in B$ であるかのいずれかである。$\varphi(z) = B$ と仮定する。$z \in \varphi(z)$ とすると、B の定義より $z \notin B$ となり、$\varphi(z) = B$ に矛盾する。一方、$z \notin \varphi(z)$ とすると、B の定義より $z \in B$ であるが、これも、$\varphi(z) = B$ に矛盾する。したがって、$\varphi(z) \neq B$、 すなわち、$\varphi(z) = B$ となる $z \in X$ は存在しない。特に、X から $P(X)$ への全射は存在しない。したがって $|X| < |P(X)|$ である。 ■

上の定理より、$n \in \boldsymbol{N}$ としたとき、$X = \{1, 2, \ldots, n\}$ とすると、$|X| = n$ で、$|P(X)| = 2^n$ となる。これより、初等的にも証明できる不等式 $2^n > n$ を得る。これが濃度の定義のもとで、無限の濃度の場合にも成立する。

$a \in \boldsymbol{N} \cup \{0\}$, p を 2 以上の自然数とする。このとき、$p^{m-1} \leq a < p^m$ なる m を取ることにより、

$$a = \sum_{i=0}^{m-1} a_i p^i,\ 0 \leq a_i < p,\ i = 0, 1, \ldots m-1$$

と書くことができることはよく知られている。これを p 進表示という。たとえば通常の記述で、164 とあれば、これは 10 進表示で、$164 = 4 + 6 \cdot 10 + 1 \cdot 10^2$ の意味である。a が非負の実数のときには、a を越えない最大の整数を $[a]$ で表すと[17]、$0 \leq a - [a] < 1$ である。$a = [a]$ のときは、上のような p 進表示を持つから、a が $0 < a < 1$ なる実数のときを考える。p をやはり 2 以上の自然数とするとき、

$$a = \sum_{i=1}^{\infty} a_i p^{-i} = \sum_{i=1}^{\infty} \frac{a_i}{p^i},\ 0 \leq a_i < p,\ i = 0, 1, \ldots m-1$$

と書くことができる。

復習から。まず等比級数を考えると、公比が $1/p$、初項が q とすると、

$$q + q\frac{1}{p} + q\frac{1}{p^2} + \cdots = q\sum_{i=0}^{\infty} \frac{1}{p} = \frac{q}{1-(1/p)} = \frac{qp}{p-1}$$

したがって、特に、

$$(p-1)\frac{1}{p^{j+1}} + (p-1)\frac{1}{p^{j+2}} + (p-1)\frac{1}{p^{j+3}} + \cdots = \sum_{i=j+1}^{\infty} \frac{p-1}{p^i} = \frac{1}{p^j}$$

すなわち、同じ数に二つの表示がある。つまり、あるところからさき、ずっと、$p-1$ が係数に続くものと、そこからすべて係数が 0 となる表示である。10 進の場合には、たとえば、$0.164 = 0.1639999\cdots$

$$a = \sum_{i=1}^{\infty} \frac{a_i}{p^i} \leq \sum_{i=1}^{\infty} \frac{p-1}{p^i} = (p-1)\sum_{i=1}^{\infty} \frac{1}{p^i} = (p-1)\frac{1/p}{1-(1/p)} = 1$$

だから、このように表示されたものは、$0 \leq a \leq 1$ で、0 となるのは、a_i がすべて 0 のとき、1 となるのは、a_i がすべて $p-1$ となるときに限ることもわかる。両辺に p^i をかけると

$$[p^i a] = \sum_{j=0}^{i-1} a_j p^{i-j-1}$$

または、これに 1 を足した物でそうなるのは、$a_h = p-1,\ h = i+1, i+2, \ldots$ となる場合であることもわかる。すなわち、ある番号から先すべて $p-1$ であるか すべて 0 であるかのいずれかに決めれば、この表示は一通りである。以下では、$p = 3$ と $p = 2$ の場合を使っている。

定理 8.3 $|\boldsymbol{R}| = |P(\boldsymbol{N})|$ である[18]。特に、$|\boldsymbol{R}| > |\boldsymbol{N}|$。

証明　$|\boldsymbol{R}| = |(0,1)|$ だから、$P(\boldsymbol{N})$ から $(0,1)$ と $(0,1)$ から $P(\boldsymbol{N})$ への単射を定義する。

$$\varphi : P(\boldsymbol{N}) \to (0,1)\ (S \mapsto \frac{1}{3} + \sum_{s \in S} \frac{1}{3^{s+1}}).$$

また、$0 < a < 1$ のとき a の無限 2 進表示を $(a)_2$ とすると、

$$\psi : (0,1) \to P(\boldsymbol{N})\ ((a)_2 = (a_0, a_1, \ldots) \mapsto \{i \mid a_i \neq 0\})$$

は単射である。したがって、Cantor–Bernstein の定理により $|(0,1)| = |P(\boldsymbol{N})|$。 ■

$|\boldsymbol{R}| > |\boldsymbol{N}|$ の別証明を記す。$|(0,1)| \neq |\boldsymbol{N}|$ を示せば十分。$(0,1)$ の元を無限 10 進数として表す。$(a) = 0.a_1 a_2 \ldots$ とする。これらに $\boldsymbol{N}$ から $(0,1)$ に全単射があったとし、$i \mapsto \varphi(i)$ とする。ここで (a) を次のように決定する。$\varphi(i)_i \neq 1$ なら $a_i = 1$。$\varphi(i)_i = 1$ なら $a_i = 2$。すると、$\varphi(j) = a$ となる j は存在しない。

[17] $[a]$ をガウス記号という。$[2] = 2$, $[1.2] = [1]$, $[\pi] = [3]$, $[-\pi] = -4$ 等となる。
[18] この濃度を $\aleph$ で表す。ドイツ文字の小文字の c を用いることもある。