数学入門公開講座

（昭和52年8月2日～11日）

講師：松浦重武
荒木不二洋
西尾英之助
一松 信

京都大学数理解析研究所

講師及び内容

1. 数と代数の話（6時間）　　京都大学数理解析研究所教授　松浦重武

社会を無視すると個々の人間の意味が怪しくなるように，数の場合も数全体の集団としての構造を離れては，個々の数の意味はわからない。

このような立場から，整数および有理数から出発して，実数および複素数を説明する。また，それに必要な代数の話をつけ加える。

(1) 数の演算と順序

(2) 同型とは何か？

(3) 実数の話

(4) 複素数の話

2. 複素数と物理学（6時間）　　京都大学数理解析研究所教授　荒木不二洋

方程式を解くときの便宜上仮の数として考案された虚数が，ガウス，コーシーなどの大数学者の手をへて，数学の表舞台に登場したのは19世紀のことである。その結果，物理学においても計算や記述の便宜上複素数が使用されるようになったが，今世紀の物理学上の革命のひとつである量子力学において，複素数は物理学上本質的役割を獲得するに到った。このような虚から本質への移り変りを，量子力学における複素数の役割に重点をおいて解説する。

3. 記号列の数理（6時間）　　京都大学理学部助教授　西尾英之助

情報科学の一つの特徴は様々な対象を記号の列として表現することである。また，記号列を作り出したり，書換えたり，区別したりすることは情報処理の基本的な操作である。このような概念を扱うための数学的方法とそれらの生物学などへの応用について述べる。

(1) 記号列とオートマトン

(2) 記号の二次元配列

(3) 生物の発生の記号列モデル

4. 和算の話（6時間）　　京都大学数理解析研究所教授　一松　信

徳川時代に和算とよばれる日本独特の数学が発展した。その背景や，その内容の意味するところ，明治初年の日本の数学に及ぼした影響などに重点をおいて，和算の解説をする。また和算家達の計算法を電卓によって追試し，彼らの発見的方法を今日の数学教育に活用することを試みる。

時　間　割

時間＼日	2日(火)	3日(水)	4日(木)	5日(金)	6日(土)	7日(日)	8日(月)	9日(火)	10日(水)	11日(木)
13:30～15:00	数と代数の話　(松浦)						記号列の数理　(西尾)			
15:00～15:15	休　憩						休　憩			
15:15～16:45	複素数と物理学(荒木)						和算の話　(一松)			

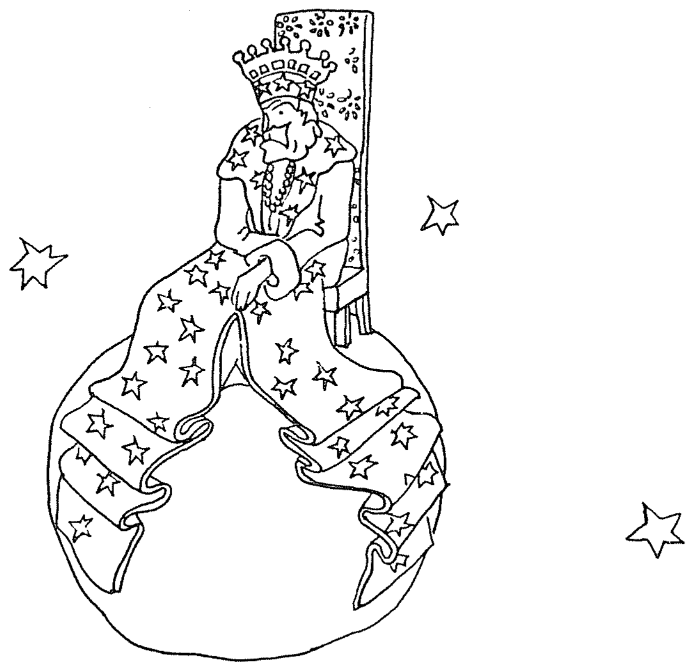
数と代数の話

講師： 松浦重武

期間： 昭和52年8月2日～5日

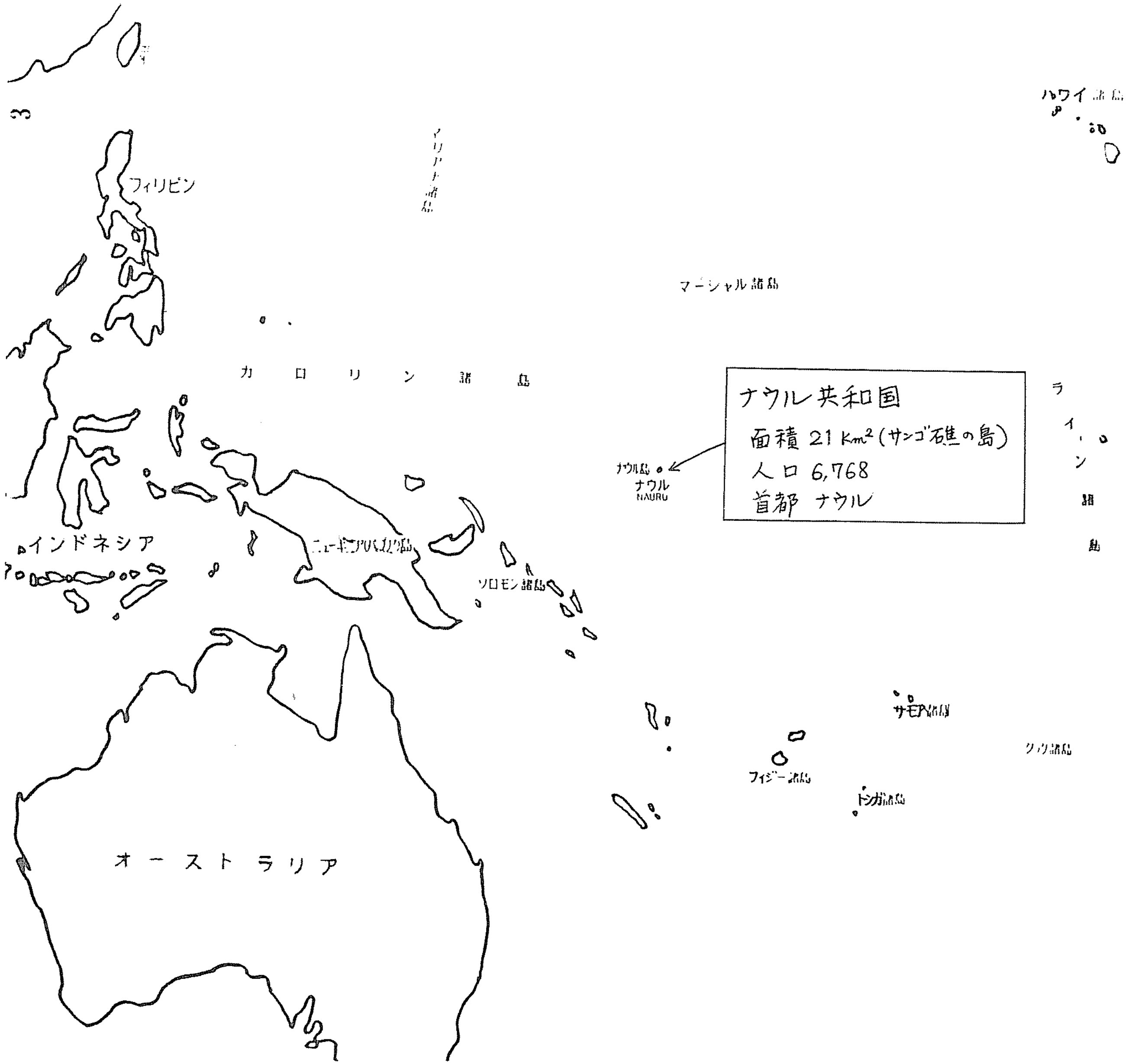
時間： 13:30 ～ 15:00

LE PETIT PRINCE



La première était habitée par un roi.

The first planet was inhabited by a king.



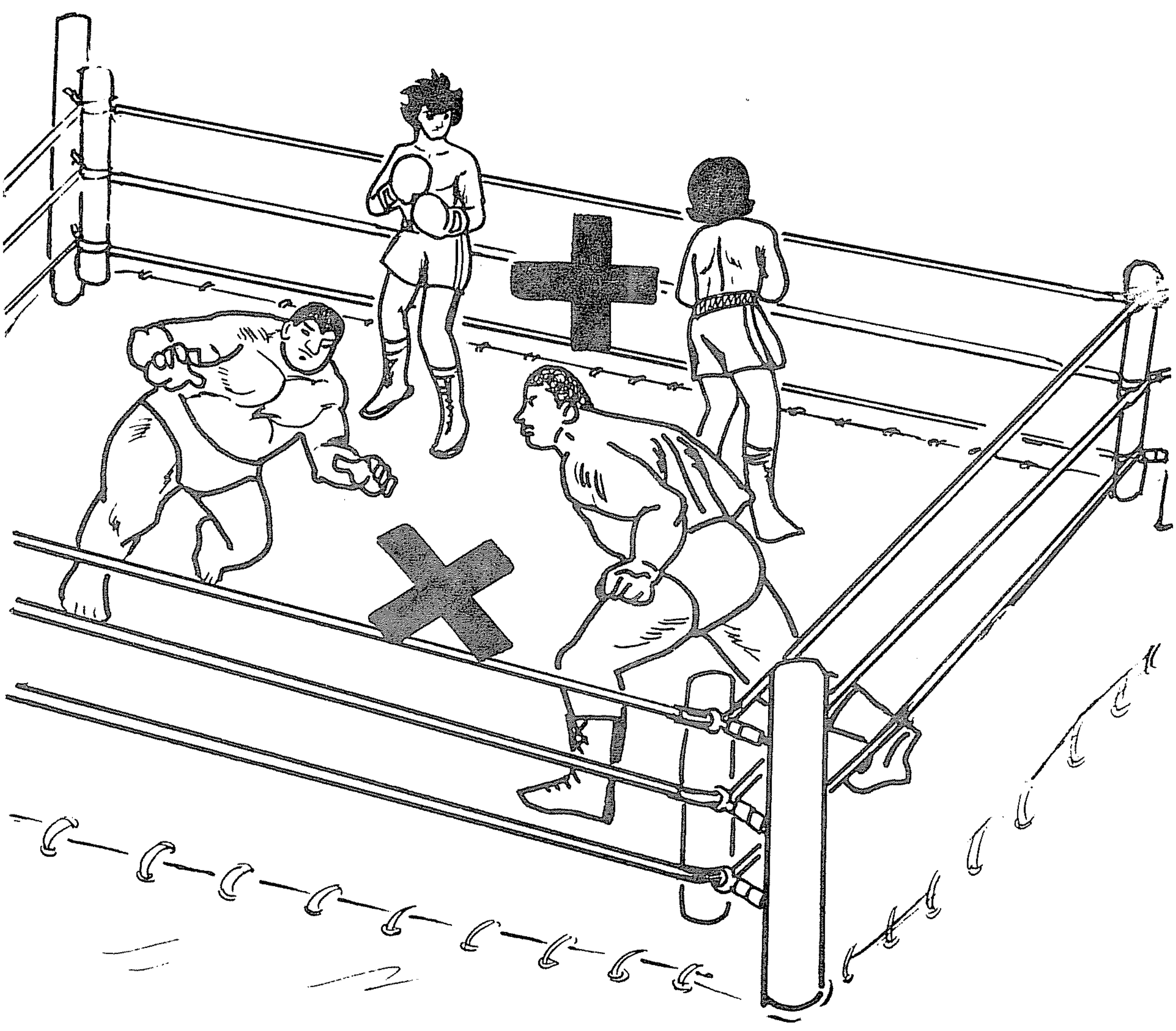
ナウル共和国
面積 21 km^2 (サンゴ礁の島)
人口 6,768
首都 ナウル

政体：議会政治
元首：デ・ロバート大統領
(立法院で選出)
首相と外相を兼ねる
産業：リン鉱石の輸出
一人当りの年所得：
31,000ドル
(世界1)
交通：鹿児島との間に
定期航空路

4

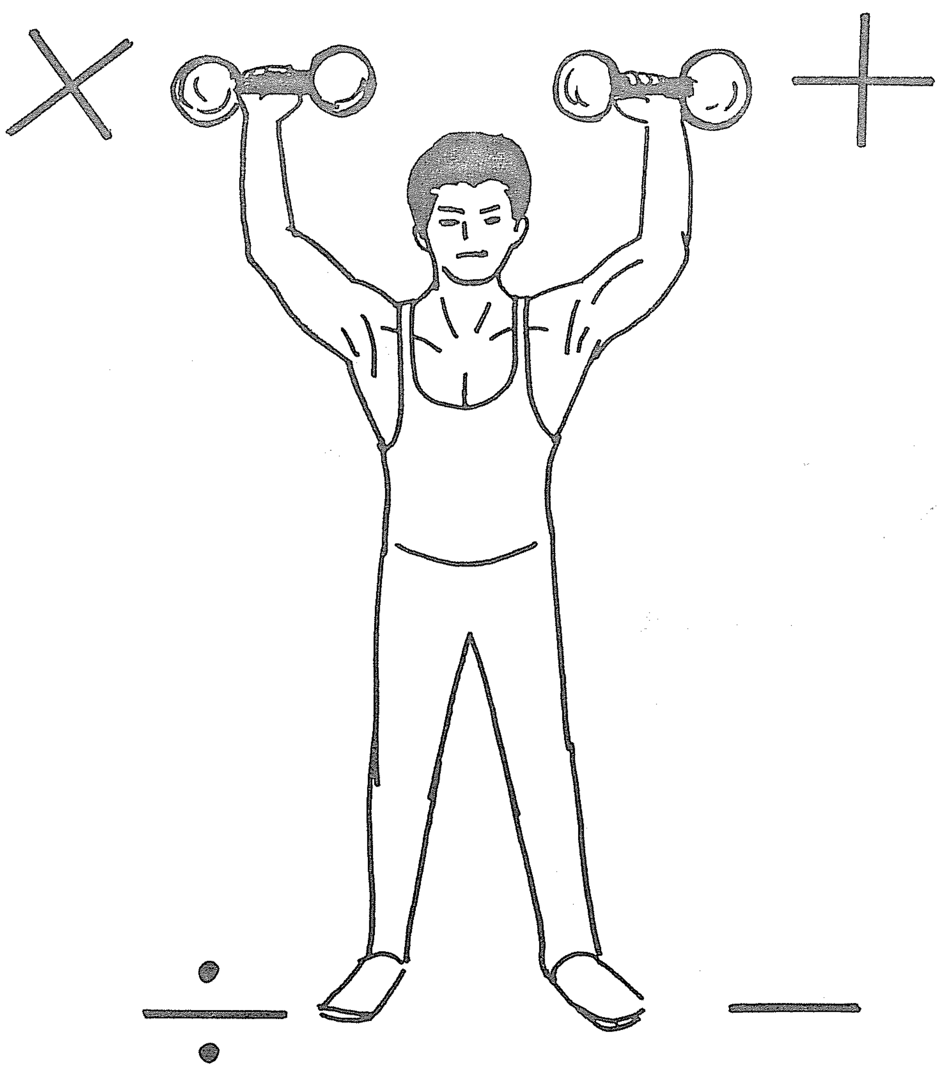
環（リング）

RING



FIELD KÖRPER

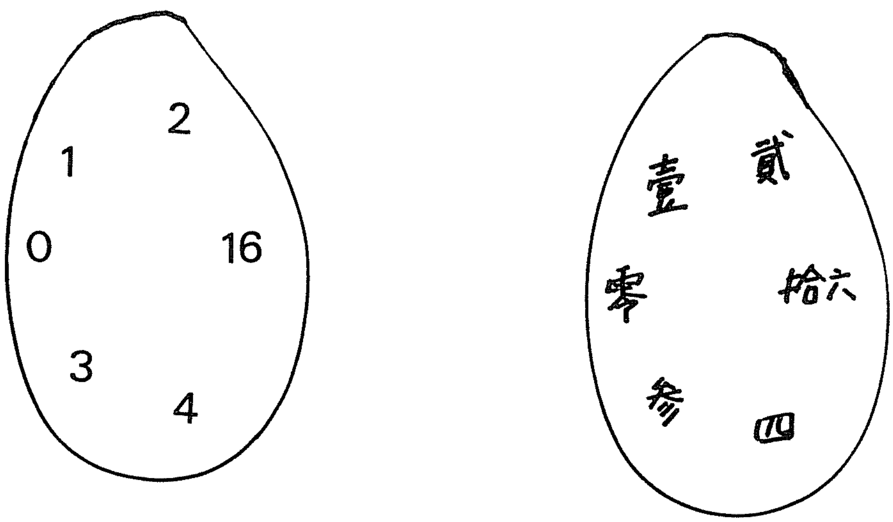
体（フィールド，ケルペル）



同型

$$R_1 \xrightarrow{\quad f \quad} R_2$$

R_1	R_2
加法 $+$	加法 足ス
乗法 $\times$	乗法 掛ル



f(0) = 零 , f(1) = 壹

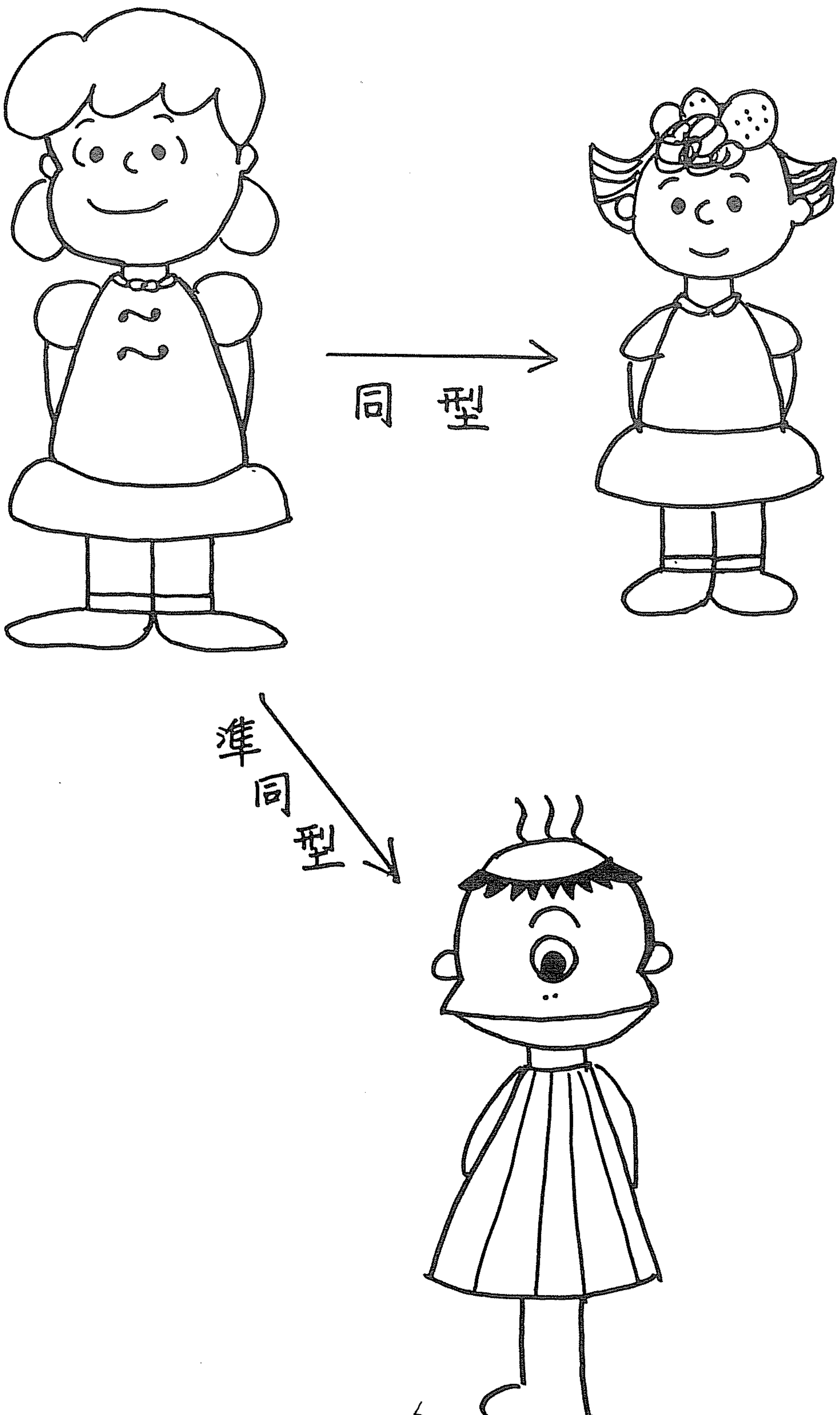
f(2) = 貳 , f(3) = 参

$2 + 2 = 4$　　f(2) 足ス f(2) = f(4)

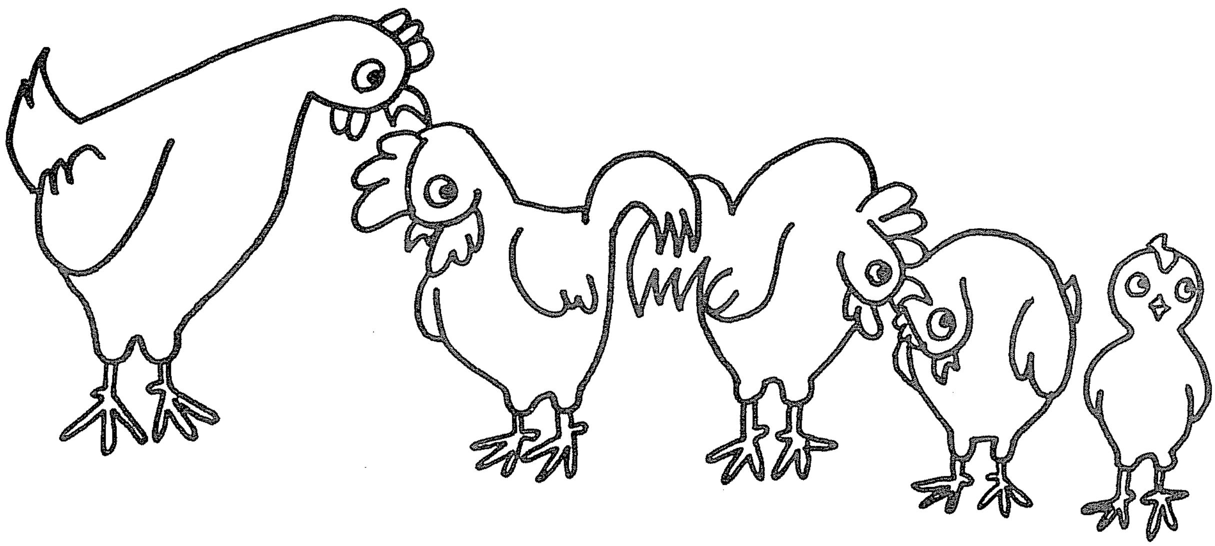
貳 足ス 貳 = 四

$3 \times 4 = 12$　　f(3) 掛ル f(4) = f(12)

参 掛ル 四 = 拾貳

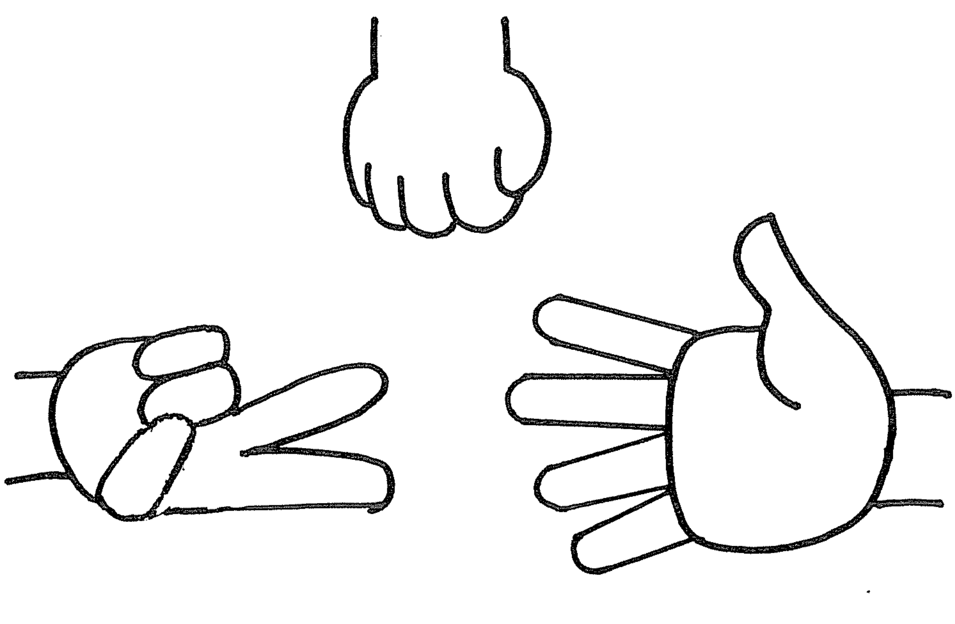

同型
準同型

Peckingの順序

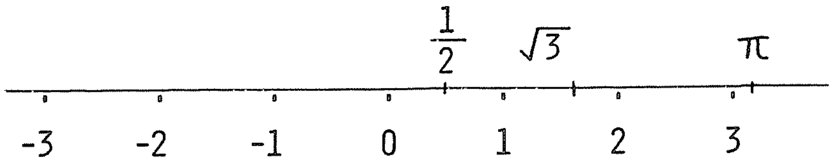


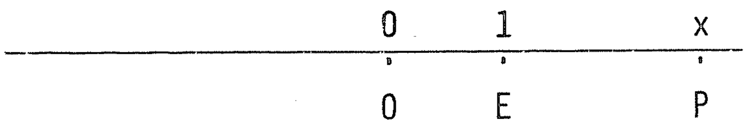
****

じゃんけん（順序ではない）



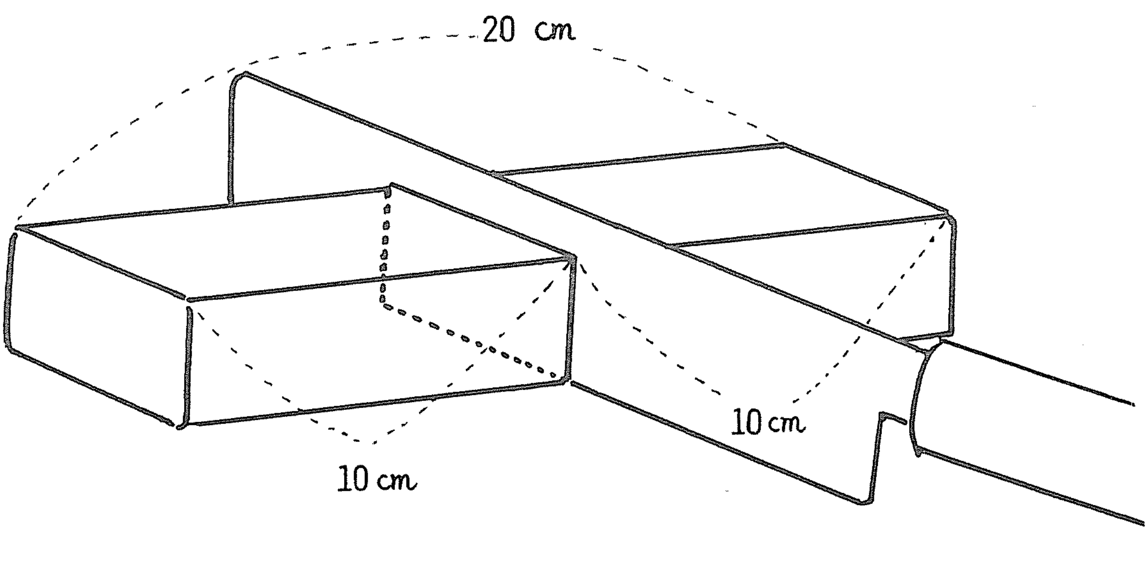
数 直 線





包丁で羊羹を切る

実数の連続性



数と代数の話

松浦重武

このノートは，お話したいと思っていることの「メモ」にすぎない．実際には，しばしば脱線することもあるし，時間の都合で省略することも起るかもしれない．このメモは単に定義や記号を並べただけになるが，話が終ってから見るならば，備忘録の一部として役立つかも知れない．

—— ◦ ——

数の集りを示す記号

$\mathbb{N}$　自然数の集合 $=\{1, 2, 3, \cdots\}$，数 = **N**umber

$\mathbb{Z}$　整数の集合 $=\{0, \pm 1, \pm 2, \cdots\}$，数 = **Z**ahl (ドイツ語)

$\mathbb{Q}$　有理数 (分数) の集合 $=\left\{\dfrac{m}{n} ; m, n \text{ 整数}, n \neq 0\right\}$.

$\dfrac{m}{n}$ は m を n で割った商，商 = **q**uotient

$\mathbb{R}$　実数の集合，実数 = **r**eal number

$\mathbb{C}$　複素数の集合，複素数 = **c**omplex number

($\mathbb{H}$　四元数の集合，四元数はハミルトン (**H**amilton) の発明である．

この他にも種々あるが，それは大学で学ぶこと．)

—— ・ ——

<u>集合に関する記号</u>　$\in$,　$\subseteq$,　$\{x\,;\,\cdots\cdots\}$,

集合＝「モノ」の集り．個々のモノのことをその集合の元(ゲン)という．x が集合 S の一つの元であることを

$x \in S$　(又は $S \ni x$)　と書く．記号の読み方は，「x は S に属する」(「S は x を元として含む」)など．

集合 A が集合 B の部分集合であることを $A \subseteq B$ (又は $B \supseteq A$) と書く．読み方は，「A は B に含まれる」(「B は A を含む」)など．集合を具体的に表わすには，

$$\{1,2,3\}\ ,\ \{x\,;\,x\text{は実数}\}$$

というように書く．$\{x\,;\,x \neq x\}$ は空集合 (記号 $\emptyset$)．

(a と $\{a\}$ は同じものではない．例えば $\emptyset \neq \{\emptyset\}$)

$$\begin{cases} \text{共通部分 (交わり)} & A \cap B = \{x\,;\,x \in A \text{ かつ } x \in B\} \\ \text{合併 (結び)} & A \cup B = \{x\,;\,x \in A \text{ 又は } x \in B\} \\ \text{差} & A \setminus B = \{x\,;\,x \in A \text{ かつ } x \notin B\} \end{cases}$$

―――― ∘ ――――

<u>論理記号</u>　$\Rightarrow$,　$\forall$,　$\exists$

二つの命題 p, q があるとき，「p が成立するならば q が成立する」(即ち「p ならば q」)を表わすのに

$p \Rightarrow q$　(又は $q \Leftarrow p$)　と書く．

(命題 p から命題 q が出る)

$\forall$ すべての（all Aの逆立ち）

（用い方） $\forall x \in \mathbb{R}$, $x^2+1 \neq 0$

$\exists$ 存在（exist Eの逆立ち）

（用い方） $\exists x \in \mathbb{C}$, $x^2+1=0$

――――― ◦ ―――――

（二項）演算　　演算＝オペレーション＝操作

集合 S の二つの元に対して，それらから S の別の元を作り出す規則を S 上の二項演算という．「二変数の関数（写像）」と同義語である．

$\mathbb{R}$ における演算の例

二項演算

$$\begin{cases} x, y \longmapsto x+y & \text{加法} \\ x, y \longmapsto x-y & \text{減法} \\ x, y \longmapsto x \times y & \text{乗法} \\ \text{など} \end{cases}$$

一項演算　$x \longmapsto -x$

三項演算　$x, y, z \longmapsto \dfrac{\sin(x+y)+\cos(y+z)}{2}$

など．

断わらない限り，演算とは二項演算を指すことにする

一つの集合の上で，幾種類もの演算を考えることが出来る．　S が有限集合で，元の個数が n ならば，二項演算は全部で　$n^{n^2}=n^{(n^2)}$　だけある．　しかし，

勝手に考えた演算がすべて興味あるわけではない.

環(カン) (= ring)

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ などに共通の性質は, それが環になることである. ring リングと言っても, 指輪を考えるのではない. ボクシングやレスリングの仕合が行われるリングに相当する

環の定義

集合 R 上に 2 種類の二項演算を考え(それらを便宜上 $+$ と $\times$ で表わす)たものが環であるとは, それらの演算が次の諸条件を満たすことを言う.
($+$ と $\times$ を採用するのに他意はない. 普通の数の演算記号に合しただけである. □ と ○ にしても構わない)

(1) 加法($+$ と書いた方の演算)について

可換律 $a+b=b+a$

結合律 $(a+b)+c=a+(b+c)$

中性元の存在 $\exists\,\theta\in R\ \ \forall a\in R\ \ a+\theta=a$

(このような θ を R の零元とよぶ)

逆元の存在 $\forall a\ \exists a'\ \ a+a'=\theta$

(2) 乗法($\times$ と書いた方の演算)について

[略記法 $a\times b=a\cdot b=ab$]

可換律　$ab = ba$

結合律　$(ab)c = a(bc)$

中性元の存在　$\exists e \in R \ \forall a \in R \quad ae = a$

（このような元 e を R の単位元とよぶ）

（3）加法と乗法について

分配律　$a(b+c) = ab + ac$

注意

1）零元の一意性　$0, 0'$ を共に零元とすると

$0 = 0 + 0' = 0' + 0 = 0'$. R の零元を 0_R と書くことにする。誤解のおそれがなければ、単に 0 と書く。

2）逆元の一意性　$a \in R$ とし、a の逆元が二つあったとして、それを a_1, a_2 とする。$a + a_1 = 0$

$a + a_2 = 0$. $\therefore a_1 = a_1 + 0 = a_1 + (a + a_2) =$

$= (a_1 + a) + a_2 = 0 + a_2 = a_2$. a の逆元を $-a$ と書く。$a + (-a) = 0$, $-(-a) = a$

$a + (-b)$ を $a - b$ と略記する。

3）方程式 $x + a = b$ は唯一つの解 $b - a$ を持つ。

4）単位元の一意性　e, e' を共に単位元とすると

$e = ee' = e'e = e'$. R の単位元を 1_R と書く。誤解のおそれがないときには、単に 1 と書く。

5) $\forall a \in R,\ a0 = 0$. $a0 = a(0+0) = a0 + a0$
両辺から $a0$ をひくと $a0 = 0$.

6) $(-a)(-b) = ab$. まず, $-ab = a(-b) = (-a)b$
$= (-1_R)ab$ であることに注意する どれも ab の
逆元だから等しい. $\therefore\ (-a)(-b) = -(a)b = -(-(ab))$
$= ab$. とくに $(-1_R)^2 = 1_R$ である.

注意 環 R において $0_R = 1_R$ が成立したとすると
任意の $a \in R$ に対して $a = a \cdot 1_R = a \cdot 0_R = 0_R$
即ち $R = \{0_R\}$ となる. この場合を除けば

$$(4) \qquad 1_R \neq 0_R$$

となる. 今後 (4) はつねに仮定する.

環の例 $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ はすべて環
この他に関数環の例はいくらでもつくれる.
R を環としたとき, R 上の多項式環 $R[X]$ を
作ることが出来る $f \in R[X]$ とは

$$f = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$$

の形のものである. 加法, 乗法は $\mathbb{R}[X]$ のときの
ようにやればよい.

部分環，イデアル

部分環の定義　R を環，S をその部分集合で

$a, b \in S \Rightarrow a \pm b \in S,\ ab \in S,\ 1_R \in S$

となるものを R の部分環という。

イデアルの定義　R を環，J をその部分集合で

$$\begin{cases} a, b \in S \Rightarrow a \pm b \in S \\ a \in S,\ b \in R \Rightarrow ab \in S \end{cases}$$

となるものを R のイデアル (ideal) という

(ideal は 理想数 ideal number から来る 後者は(観念数)用いない)

部分環の例　$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ はすべて $\mathbb{R}$ の部分環

R を環とすれば，R は $R[X]$ の部分環と思える。

イデアルの例

R を環，$a \in R$ とするとき

$Ra = \{xa ;\ x \in R\}$ は R のイデアル

(これは単項イデアルと呼ばれる。)

イデアルであって，環全体とは一致しないとき，真のイデアルとよぶ。(これは 1_R を含まないことと同等)

真のイデアルは部分環ではない。($\because$ 1_R を含まぬから)

剰余環　R を環，J をその真のイデアルとする．
R の元の間の同値関係 $\sim$ を次のように定義する．

$$a \sim b \iff a - b \in J$$

このとき，次のことが成立する

$$\begin{cases} 1) & a \sim a & & (\text{反射律}) \\ 2) & a \sim b,\ b \sim c & \Rightarrow a \sim c & (\text{推移律}) \\ 3) & a \sim b & \Rightarrow b \sim a & (\text{対称律}) \end{cases}$$

1) 2) 3) から R の「クラス分け」（類別）が出来る．

$C(a) = \{ x \,;\, x \in R,\ x \sim a \}$ は a の入るクラス

$C(a) = C(b) \iff a \sim b$

このようにして出来るクラス全体からなる集合を R/J で表わす．加法と乗法を

$$\begin{cases} C(a) + C(b) = C(a+b) \\ C(a) \times C(b) = C(ab) \end{cases}$$

で定義することによって R/J は環となる．とくに

$$0_{R/J} = C(0_R),\quad 1_{R/J} = C(1_R)$$

となる．

例　$\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$

これは有限個の元からなる環である（元の個数 $= m$）

$m = 2$ のとき

$\mathbb{Z}_2 = \{0, 1\}$　最も小さい環

環の同型と準同型

R_1, R_2 二つの環, $f : R_1 \longrightarrow R_2$, $x \longmapsto y = f(x)$

が1対1, 上への写像であって

$$\begin{cases} f(x+y) = f(x) + f(y) \\ f(xy) = f(x)f(y) \end{cases}$$

が成り立つとき, f は同型写像という. 同型写像が存在するとき, R_1 と R_2 は同型であるという. 同型な環は環としての構造が同じであると考えられる.

(とくに $f(0_{R_1}) = 0_{R_2}$, $f(1_{R_1}) = 1_{R_2}$)

R_1, R_2 二つの環, $f : R_1 \longrightarrow R_2$ 写像

$$\begin{cases} f(x+y) = f(x) + f(y) \\ f(xy) = f(x)f(y) \\ f(1_{R_1}) = 1_{R_2} \end{cases}$$

となるとき, f は R_1 から R_2 への準同型写像という

このとき f による像 $f(R_1) = \{ f(x) \; ; \; x \in R_1 \}$ は R_2 の部分環である. f が上への準同型写像であるとき R_2 は R_1 に準同型であるという. 準同型な環はもとの環と比べて, 構造的には模型のようなものと考えられる.

<u>定理</u>　R_1, R_2 二つの環，$f: R_1 \to R_2$ 準同型写像とすれば，$f(R_1)$ は R_2 の部分環であり，$f^{-1}(0_{R_2}) = \{x;\ x \in R_1,\ f(x) = 0_{R_2}\}$ は R_1 の真のイデアルである．
このとき $R_1/f^{-1}(0_{R_2})$ は $f(R_1)$ に同型である．

（証明）　$J = f^{-1}(0_{R_2})$ とおけば J が R_1 のイデアルになることはすぐわかる．$f(1_{R_1}) = 1_{R_2}$ だから J は真のイデアルとなる．R_1/J に属するクラス $C(a)$ に対して

$$g(C(a)) = f(a)$$

とおくと　$g: R_1/J \longrightarrow f(R_1)$ が同型写像になることは容易にわかる（証終）

<u>環の標数，素環</u>

R を環，$a \in R$ とする．今 $m \in \mathbb{Z}$ に対して ma を次のように定義する

$$\begin{cases} m > 0 \text{ のとき} & ma = \underbrace{a + \cdots + a}_{m\text{個}} \\ m = 0 \text{ のとき} & 0a = 0_R \\ m < 0 \text{ のとき} & ma = -(-m)a \end{cases}$$

こうすると
$$\begin{cases} (m+n)a = ma + na \\ m(a+b) = ma + mb \\ m(ab) = (ma)b = a(mb) \end{cases}$$
は容易に分る．

いま　$f : \mathbb{Z} \longrightarrow R$　を　$f(m) = m1_R$　と定義すると，$f(m+n) = f(m) + f(n)$，$f(mn) = f(m)f(n)$，$f(1) = 1_R$　となることは直ちにわかる．即ち f は準同型写像である　$f(\mathbb{Z}) = \{ m1_R \ ; \ m \in \mathbb{Z} \}$ は R の部分環であるが，これを R に含まれる　素環と呼ぶことにしよう．前出の定理によって，$f(\mathbb{Z})$ は $\mathbb{Z}/J$ に同型である．ただし，$J = f^{-1}(0_R)$．

<u>定理</u>　$J \subseteq \mathbb{Z}$，J イデアルとすれば，$\exists q$ 整数 ≥ 0

$$J = \{ nq \ ; \ n \in \mathbb{Z} \} = q\mathbb{Z}$$

(証)　$J = \{0\}$ なら明らか．$J \neq \{0\}$ とする．$m \in J$ なら $-m \in J$ だから，J には正整数がある．その最小のものを q とする　いま，任意の $m \in J$ に対して

$$m = kq + h \qquad k \in \mathbb{Z}, \quad 0 \leq h \leq q-1$$

となる k，h が定まるが

$$h = m - kq \in J$$

より　$h = 0$　故に　$J = \{ kq \ ; \ k \in \mathbb{Z} \}$　(証終)

<u>注意</u>　上の定理から，$\mathbb{Z}$ は単項イデアル環である．

(<u>応用</u>　a, b 自然数，その最大公約数を d とすれば
$\exists m, n \in \mathbb{Z}$　　$d = ma + nb$
これから自然数の素因数分解の一意性が出る)

もとに戻って考えると．任意の環 R を考えたとき，その素環は $\mathbb{Z}/q\mathbb{Z} = \mathbb{Z}_q$ に同型となる．この q を R の標数と呼ぶことにする（$q>0$ のとき）．$q=0$ ならその素環は $\mathbb{Z}$ に同型である．これで素環の構造は全部わかったことになる．

———— ◦ ————

体（タイ）

$\mathbb{Q}$，$\mathbb{R}$，$\mathbb{C}$ などは単なる環ではなく，体（field，Körper（ドイツ語））である．人体には手足が4本あるように，体（タイ）とは4則演算（加減乗除）が円滑に行われる場（フィールド）である．

体の定義

集合 F 上に2種類の演算（加法＋，乗法×）が定義されていて，次の性質をみたしているとき，F は体であるという．

(1) F は環である．

(2) 0_F と異なる F の元には，乗法に関する逆元が存在する．即ち，$a \neq 0_F$，$a \in F \Longrightarrow \exists\, b \in F \quad ab = 1_F$

（注意　零元 0_F には逆元はない．それは，どんな $a \in F$ に対しても $0_F a = 0_F \neq 1_F$ だからである．）

注意　逆元の一意性　$a \in F$　$a \neq 0$　として，aに逆元が二つあったとして，それを b_1, b_2 とすると，

$$b_1 = 1_F b_1 = a b_2 b_1 = b_2 (a b_1) = b_2 1_F = b_2 .$$

今後 aの逆元を a^{-1} 又は $\frac{1}{a}$ で表わす．

また $\frac{a}{b} = a \cdot \frac{1}{b}$ とする　$(b \neq 0)$．

問題（練習）　$q > 0$ として，$\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ が体になるのは，qが素数のときである．これを示せ．

順序関係

$\mathbb{Z}$，$\mathbb{Q}$，$\mathbb{R}$ は環であるだけでなく，その元の間には順序関係（大小関係）がある．順序は大小関係だけでなく，鳥の群における pecking 順序のようなものもある．

順序集合の定義　集合 S 上に一つの関係（それを $\leqq$ で示す）が定義されていて，それが次の諸条件をみたすとする（$x \leqq y$ のことを $y \geqq x$ とも書く）

$$\begin{cases} (1) & x \leqq x \\ (2) & x \leqq y,\ y \leqq x \Rightarrow x = y \\ (3) & x \leqq y,\ y \leqq z \Rightarrow x \leqq z \end{cases}$$

このとき, $\leqq$ は一つの順序(関係)であるという. 順序が定義されている集合を順序集合という

$x \leqq y$ かつ $x \neq y$ のとき $x < y$ と書く

そうすれば $x \leqq y \iff x = y$ 又は $x < y$ となる

注意 S の任意の2元 $\underbrace{\ }_{x\ y}$ の間に $x \leqq y$ 又は $x \geqq y$ のどちらか一方が成立するとき, その順序は全順序(又は線型順序)であるという このとき x y の間には

$$x < y \ , \quad x = y \ , \quad x > y$$

のどれか一つが成立することになる(一つだけ).

問題 S を有限集合として, その元の個数を n とすれば, S に線型順序を入れる仕方は $n!$ 通りある. これを示せ.

今後は, 順序としては, 線型順序だけを考えてよい.

有界性, 上界(下界), 上限(下限), 最大(最小)

S を順序集合とする. $A \subseteq S$ としたとき, A が上に有界であるとは, 適当な $u \in S$ に対して $a \leqq u$ がすべての $a \in A$ について成立することを云う. 上の式を簡単に $A \leqq u$ と表わすこともある このような u を A の一つの上界という u が上界ならば, u より大きい元はすべて A の上界となる したがって, A の上界

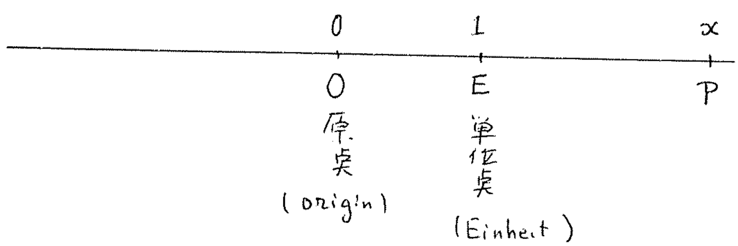
は一般には多数ある。このことから，なるべく小さい上界に興味があることになる。$A \subseteq S$ に対して，c が A の最大元であるとは，$c \in A$ であって，$\forall a \in A \quad a \leq c$ となる元のことを言う。A に最大元があるとすれば，それは唯一つである（その証明は練習問題）。それを $\max A$ と書く。$\max A$ が存在すれば，それは一番小さい上界である

不等号を向きを反対にして考えて，下に有界，下界，最小元などを定義する。A の最小元は $\min A$ で示す。

$\max A$，$\min A$ という考えの欠点は，それが存在しない場合の多いことである。A の最小上界のことを A の上限という。記号 $\sup A$。（同様に A の最大下界を A の下限と言って $\inf A$ で表わす。）$\sup A$ が $\max A$ よりも便利な点は，$\max A$ が存在すれば $\max A = \sup A$ となり，しかも $\max A$ が存在しないときでも $\sup A$ の存在する場合が多いのである

実数の連続性，順序集合の完備性

直観にうったえるために，おなじみの数直線を導入する。



このようにすれば，実数体 $\mathbb{R}$ の元 x と直線上の点 P とは，一対一に対応して過不足がなく，実数の大小関係は直線上の点の位置関係（右にある方が大きい）になるというのがその考えである．

これを承認すれば，実数の連続性とは，「数直線を二つに切るには断点が必要である」ということである．

［ヨーカンを切る；1日には始めと終りがあるか］

<u>完備性の定義</u>　順序集合 S が完備であるとは，S の空でない部分集合 A が上に（下に）有界ならば sup A（inf A）が存在することを言う．

<u>切断の定義</u>　順序集合 S の空でない部分集合の対 (A, B) が S の切断であるとは

(1)　$A \leq B$　（即ち $\forall a \in A, \forall b \in B \quad a \leq b$）

(2)　$A \cup B = S$

(3)　$A \cap B = \emptyset$

(A, B) を一つの S の切断としたとき，論理的には次の四つの場合が考えられる

(i)　max A，min B が両方共に存在する

(ii)　max A は存在するが，min B は存在しない

(iii) max A は存在しないが, min B は存在する

(iv) max A も min B も存在しない.

連続性の定義　順序集合 S が連続であるとは, その任意の切断 (A, B) が (ii) 又は (iii) の場合になることをいう.

自己稠密性の定義　順序集合 S が自己稠密であるとは, $a, b \in S$, $a < b$ ならば $\exists c \in S$　$a < c < b$ となることを言う.

定理　順序集合が連続であるためには, 自己稠密かつ完備であることが必要十分である

(証明) やさしい. 練習問題としよう.

例　$\mathbb{Z}$ は完備であるが自己稠密ではない (明らか)

$\mathbb{Q}$ は自己稠密ではあるが完備でない

$\mathbb{R}$ は連続である.

$\mathbb{R}$ の連続性を考察しよう. その自己稠密なことは明らかである ($a < b$ なら $c = \frac{a+b}{2}$ を考えると $a < c < b$) したがって, 完備性を示せばよい.

そこで A, B $\mathbb{R}$ の部分集合(空でない)として,

$$(*)\begin{cases} A \leqq B \quad (\text{即ち } \forall a \in A,\ \forall b \in B \quad a < b) \quad \text{とする} \\ \text{このとき} \quad \exists c \in \mathbb{R} \\ \qquad A \leqq c \leqq B \end{cases}$$

となることを承認しよう(直線の直観から)

これから $\mathbb{R}$ の完備性は直ちに出る.

(証明) A を上に有界な(空でない)部分集合とする. U を A の上界の全体とすれば $A \leqq U$. よって $(*)$ から $\exists c \in \mathbb{R}$ $A \leqq c \leqq U$ この不等式から $c = \sup A$ であることは明らか, 下に有界なときも同様 (証終).

———— ∘ ————

順序環, 順序体

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ は環であると同時に順序集合でもある. しかも, その環としての構造と順序の構造の間に整合性がある.

順序環の定義　集合 R が順序環であるとは,

(1) R は環である.

(2) R は順序集合である.

(3) 整合性.
- (i) $x \geqq y \iff x - y \geqq 0$
- (ii) $x > 0,\ y > 0 \Rightarrow x + y > 0,\ xy > 0$
- (iii) $\forall x \in R$ に対して $x > 0$ 又は $x = 0$ 又は $-x > 0$ のどれか一つ, 一つだけが成り立つ

注意　順序環には零因子がない．即ち

$$x \neq 0,\ y \neq 0 \Rightarrow xy \neq 0$$

$$\left(\begin{array}{llll} x > 0, & y > 0 & \text{なら} & xy > 0 \\ x > 0 & -y > 0 & \text{なら} & xy = -(x(-y)) < 0 \\ x < 0 & y < 0 & \text{なら} & xy = (-x)(-y) > 0 \end{array}\right)$$

また，順序環の標数は 0 である

零因子のない環を整域という

順序体の定義　順序環 R であって，その環が体であるものを順序体という

標数 0 の　環 R に対して

$$\begin{array}{rccc} f: & \mathbb{Z} & \longrightarrow & R \\ & \rotatebox{90}{$\in$} & & \\ & n & \longmapsto & n1_R \end{array}$$

は R の素環の上への同型写像であった．

いま R を標数 0 の体であるとすれば，上の同型写像を拡張して

$$g: \mathbb{Q} \longrightarrow R$$

なる「中への」同型写像を作ることが出来る．その作り方：

$\alpha \in \mathbb{Q}$ を $\alpha = \dfrac{m}{n}$　$m, n \in \mathbb{Z}$, $n \neq 0$ とする

$n1_R \neq 0$ だから，その(乗法に関する)逆元を a と

とする（ $a=(n1_R)^{-1}$ ）．このとき　$g(\alpha)=ma$　と定義する。もっ　$\frac{m}{n}=\frac{p}{q}$　ならば　$mq=np$　だから

$$mq1_R=np1_R$$

これから　$m(n1_R)^{-1}=p(q1_R)^{-1}$　となり，定義は有効である　$m(n1_R)^{-1}=(m1_R)(n1_R)^{-1}$　だから　これは　f の拡張になっている　f が同型写像になることも　容易にわかる。

<u>定理</u>　上の対応は，R が順序体のとき，順序を保つ．

（証明）　$1_R=1_R^2>0$　である

$\mathbb{Z}\ni n>0$ のとき　$\underbrace{(n1_R)^{-1}+\cdots+(n1_R)^{-1}}_{n\text{個}}=1_R>0$

だから　$(n1_R)^{-1}>0$　よって　$m,n>0$ なら　$\alpha 1_R\overset{\text{定義}}{=}g(\alpha)=m(n1_R)^{-1}>0$　（証終）

<u>完備な順序体の構造</u>

F を完備な順序体とする．F は標数 0 であり，その素体　$\{\alpha 1_F\ ;\ \alpha\in\mathbb{Q}\}$　は　$\mathbb{Q}$ と（順序もこめて）同型である．最終的には，F は $\mathbb{R}$ と（順序もこめて）同型となることが分る．しかもその同型写像は一意的に定まる．このことから，完備な順序体は $\mathbb{R}$ に他なら

ないと言ってよい。

定理（アルキメデス）F を完備な順序体として，
$a, b \in F$，$a > 0$，$b > 0$ とすれば，$\exists n \in \mathbb{N}$，$na > b$.

（証明）結論を否定すると $\exists a, \exists b \in F$，$a > 0$，$b > 0$
$\forall n \in \mathbb{N}$　$b \geqq na$ となる。$A = \{na ; n \in \mathbb{N}\}$ は
上に有界となるから，$\sup A$ が存在する。$c = \sup A$ と
すると，$\forall n \in \mathbb{N}$ に対して　$c \geqq (n+1)a$　$\therefore c - a \geqq na$
n は任意だから　$c - a$ が A の上界となり $\inf A = c$
に反する（証終）

定理（有理数の稠密性）F を完備な順序体，
$a, b \in F$，$a < b$ とすれば，$\exists \frac{m}{n} \in \mathbb{Q}$

$$a < \frac{m}{n} 1_F < b$$

（証明）

$b - a > 0$ だから，$\exists n \in \mathbb{N}$　$n(b-a) > 1_F$
即ち　$\frac{1}{n} 1_F < b - a$　そこで $m \in \mathbb{Z}$ を $m 1_F > na$
となる最小の整数とする。すると　$\frac{m-1}{n} 1_F \leqq a$
ゆえに

$$\frac{m}{n} 1_F = \frac{(m-1)}{n} 1_F + \frac{1}{n} 1_F < a + (b-a) = b$$

また $\frac{m}{n} 1_F > a$ だから　$a < \frac{m}{n} 1_F < b$　（証終）

系　F を完備な順序体とすれば，その任意の元は，
有理数（$\frac{m}{n} 1_F$ の形の数）の集合の $\sup$ および $\inf$
となる。

定理　F を完備な順序体とすれば，F は $\mathbb{R}$ に（順序もこめて）同型である．

（証明）

$$\mathbb{Q}_F = \left\{ \frac{n}{m} 1_F \;;\; \frac{n}{m} \in \mathbb{Q} \right\}$$ とおく

$f : \mathbb{Q} \longrightarrow \mathbb{Q}_F$ を同型対応 $\alpha \longmapsto \alpha 1_F$ とする

これは順序を保つ　このとき $g : \mathbb{R} \longrightarrow F$ を次のように定義する．$x \in R$ に対して

$$g(x) = \inf \{ f(\alpha) \;;\; \alpha \in \mathbb{Q} \,,\, \alpha \geqq x \}$$

$x \in \mathbb{Q}$ ならば $g(x) = f(x)$ となることは明らか．

次にこれが同型写像になることを見る

$$g(x+y) = g(x) + g(y)$$

は容易にわかる

$$g(xy) = g(x) g(y)$$

となることは $x > 0$, $y > 0$ のとき容易．他の場合は加法と $(-a)b = -ab$，$(-a)(-b) = ab$ 等を用いてわかる．上への写像であることは前定理より出る　一対一であることは，$g^{-1}(0)$ がイデアルであり，$\mathbb{R}$ が体であることから $= \{0\}$ を得る（証終）

注意　同型対応の一意性は，次のようにしてわかる．

$g : \mathbb{R} \longrightarrow F$ を一つの同型対応とすると $g(1) = 1_F$ より $g\left(\frac{m}{n}\right) = \frac{m}{n} 1_F$ が出る．あとは，前定理を

考慮すれば，g が順序を保つことを言うとよい．
いま $x \in \mathbb{R}$ $x > 0$ とすれば，$\exists y \in \mathbb{R}$，$x = y^2$
ゆえに $g(x) = g(y)^2 > 0$ よって順序を保つ．

複素数体 $\mathbb{C}$ と多項式環 $\mathbb{R}[X]$

$\mathbb{R}[X]$ を $\mathbb{R}$ 上の多項式環，そのイデアル $J = (X^2 + 1)\mathbb{R}[X]$ を考えれば 商環 $\mathbb{R}[X]/J$ が複素数体 $\mathbb{C}$ になる．

$\mathbb{C}$ は $\mathbb{R}$ や $\mathbb{Q}$ と違って，恒等変換でない自己同型 $\mathbb{C} \ni z \longmapsto \bar{z} \in \mathbb{C}$ をもつこと；したがって $i = \sqrt{-1}$ と $-i$ とは区別し難いことを説明する．