平成26年度教員免許状更新講習テキスト

「数の体系」

講師：牧野　哲　（山口大学工学部教授）
makino@yamaguchi-u.ac.jp

2014年6月22日/山口大学常盤キャンパス

長年にわたって教育現場で日々の実践経験を積み重ねてこられた先生方を前にして，数学の基礎を講習するなど，はなはだ僭越ではある。しかし，自然数から順を追って論理的に厳密に複素数まで，数の概念を拡張する過程としてどのようなものがあるか，多忙な先生方のなかでじっくり吟味した経験をおもちの方はそんなに多くないのではなかろうか。この講習がその機会となれば，少しは意義があろう。

むろん，そのような論理的に厳密な数の体系の構築の過程を生のままで初等中等教育の現場にもちこむことが愚の骨頂であることは明らかである。しかし，生徒が計算規則の根拠について疑問を起こして質問してきたようなばあい,「昔からそうすることになっている」と頭ごなしにおしつけるのではなく，余裕をもって説得的に対応できるためには，先生方が自分でこの過程を一度は辿ってみて，その論理構造を血肉化していることが望ましいと思われるのである。そういう点で，この講習が先生方の教育実践のお役にたてば，さいわいである。

1　自然数

数の体系を構築していく出発点として，自然数系をペアノの公理で規定することから始めよう。論理的な完全を期するためには，この公理系を満たすものが存在することを，そのひとつを（公理的）集合論のみか

ら構成することによって証明しなければならないだろう。しかし，それはしないでおく。というのは，それは限りなく循環論法に近くなりがちで，議論の過程でこっそり自然数の概念を前提として引き込むことを避けようとすると，いたずらに神経を使わねばならないからである。

なお，このテキストでは，叙述を簡潔にするため，以下の記号を用いる：

- P, Q が命題のとき，「P ならば Q」という命題を $P \Rightarrow Q$ あるいは $Q \Leftarrow P$ と記す。「$P \Rightarrow Q$ かつ $Q \Rightarrow P$」であることを $P \Leftrightarrow Q$ と記す。
- E が集合であり，$P(x)$ が文字 x を含む命題であるとき，「E の任意の要素 x にたいして $P(x)$ がなりたつ」を $\forall x \in E[P(x)]$ と記し，「$P(x)$ がなりたつような E の要素 x が少なくともひとつ存在する」を $\exists x \in E[P(x)]$ と記す。
- E が集合であり，$P(x)$ が文字 x を含む命題であるとき，$P(x)$ をみたす E の要素 x 全体のなす集合を $\{x \in E | P(x)\}$ と記す。

1.1 ペアノの公理

集合 N，N の特定の要素 $\mathfrak{o}$，N から N への写像 s が次の性質をもつとき，この組 $(N, \mathfrak{o}, s)$ ないし N を自然数系とよぶ：

1）s は 1 対 1 である；すなわち $s(x) = s(y) \Rightarrow x = y$；

2）$s(x) = \mathfrak{o}$ となる $x \in N$ は存在しない；

3）（数学的帰納法）　N の部分集合 A にたいして

$$\mathfrak{o} \in A \qquad \text{かつ} \qquad [x \in A \Rightarrow s(x) \in A]$$

がなりたつとき，$A = N$ である。

1.2

$(N, \mathfrak{o}, s)$ は自然数系であるとする。N の要素 x が $x \neq \mathfrak{o}$ ならば，x は $\mathfrak{o}$ に s を有限回ほどこしてえられる。

証明：

$$A = \{x | x = \mathfrak{o} \text{ あるいは,} x \text{ は } \mathfrak{o} \text{ に有限回の } s \text{ をほどこしてえられる } \}$$

は数学的帰納法の仮定をみたすので，$A = N$ である。QED

この表し方は一意的である。ここで,「有限回」とは何か，定義してみろ，といいだすと，また循環論法に陥る危険がある。（自然数を使わず，ある操作を有限回ほどこすということを定義することができるかどうか，試みられたい。）したがって，これには深入りしないことにしよう。

1.3 自然数系の（本質的）一意性

$(N, \mathfrak{o}, s), (N', \mathfrak{o}', s')$ が自然数系であれば，これらは次の意味で同型である：

N から N' の上への 1 対 1 写像 Φ であって，

$$\Phi(\mathfrak{o}) = \mathfrak{o}' \qquad \Phi(s(x)) = s'(\Phi(x))$$

となるものが存在する。

証明：1.2 より条件じしんが Φ を一意的かつ完璧に定義している。Φ が N' の上への写像であることは，Φ の像 $A = \Phi(N)$ が数学的帰納法の仮定をみたすことで確かめられる。QED

したがって，以下，通常の

$$0, \quad 1, \quad 2, \quad 3, \quad \cdots$$

を自然数系の標準的な代表として用いることにして，これを $\mathbb{N}$ と記す。つまり，少なくともひとつ自然数系 $(N, \mathfrak{o}, s)$ が存在することを承認した上で，

$$0 := \mathfrak{o}, \quad 1 := s(0), \quad 2 := s(1), \quad 3 := s(2), \quad \cdots$$

等々と定義するわけである。十進法の位取り記法もむろん定義に含まれる。すると，他の自然数系はみな，$\mathbb{N}$ に同型である。

もちろん，そうしたければ，標準的な自然数系として，

$$壱, \quad 弐, \quad 参, \quad \cdots$$

とか，

$$0, \quad 1, \quad 10, \quad 11, \quad 100, \quad \cdots$$

とか，

$$0, \quad 2, \quad 4, \quad 6, \quad \cdots$$

とか，

$$1, \quad \frac{1}{2}, \quad \frac{1}{4}, \quad \frac{1}{8}, \quad \cdots$$

とかを採用するのは自由である。しかし，このように，標準的な自然数系としてどのような図式の系列をとるかにおいて恣意性があるからといって，ペアノの公理が自然数系を的確に規定していないという批判は的外れである。

なお，集合論から自然数系を構成する方法としては，von Neumann の方法が知られている。これは，

$$0 := \emptyset(\text{空集合}), 1 := \{\emptyset\}, 2 := \{\emptyset, \{\emptyset\}\}, \cdots, s(n) := \{0, 1, 2, \cdots, n\}, \cdots$$

とする。また，Zermero の方法は，

$$0 := \emptyset, 1 := \{\emptyset\}, 2 := \{\{\emptyset\}\}, \cdots, s(n) = \{n\}, \cdots$$

とする。前者では，たとえば，$3 \in 5$ であるが，後者では $3 \notin 5$ となり，同じではないが，どちらが優れているとも云いがたい。

1.4 加法の定義

$\mathbb{N}$ 上に加法とよばれる演算 $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ を次のように定義する：
$x, y \in \mathbb{N}$ にたいして

$$\begin{aligned} & f(x, 0) = x, \qquad f(x, 1) = s(x), \\ & \cdots \\ & f(x, s(y)) = s(f(x, y)), \\ & \cdots \end{aligned}$$

と定める。

これで f は一意的かつ完璧に定義される。以下，$f(x, y)$ を $x+y$ と記す。

1.5 加法の性質

1）$x + 0 = x$
2）$x + y = y + x$
3）$x + (y + z) = (x + y) + z$
証明： 1）は定義である。2）を証明しよう。

まず，

$$P(y): \quad \forall x[f(x,s(y)) = f(s(x),y)]$$

を証明する。$P(0)$ については，左辺$= x+1 = s(x)$ で，右辺$= s(x)+0 = s(x)$ だから，なりたっている。$P(y)$ を仮定すると，

$$f(x,s(s(y))) = s((f(x,s(y))) = s(f(s(x),y)) = f(s(x),s(y))$$

であり，やはり $P(s(y))$ がなりたつ。ゆえに，数学的帰納法により，$P(y)$ はつねになりたつ。いっぽう，

$$Q(x): \qquad f(x,0)(=x) = f(0,x)$$

を示そう。$Q(0)$ はむろん正しい。$Q(x)$ を仮定すると，

$$f(s(x),0) = s(x), \qquad f(0,s(x)) = s(f(0,x)) = s(f(x,0)) = s(x)$$

となり，$Q(s(x))$ がなりたつ。ゆえに，数学的帰納法により，$Q(x)$ がつねになりたつ。そこで，これらを用いて，y を止めて，$g(x) := f(x,y)$ と $h(x) := f(y,x)$ がつねに等しいことを証明しよう。$Q(y)$ より，$g(0) = h(0)$ である。$g(x) = h(x)$ を仮定すると，$P(y)$ を用いて，

$$\begin{aligned} g(s(x)) &= f(s(x),y) = f(x,s(y)) = s(f(x,y)) = \\ &= s(f(y,x)) = f(y,s(x)) = h(s(x)) \end{aligned}$$

となる。ゆえに数学的帰納法により，つねに $g(x) = h(x)$ である。これが証明すべきことであった。

次に３）を証明しよう。x, y を止めて，

$$G(z) := f(x,f(y,z)), \qquad H(z) := f(f(x,y),z)$$

を考える。$G(0) = H(0) = f(x,y)$ は明らかである。$G(z) = H(z)$ を仮定すると，

$$\begin{aligned} G(s(z)) &= f(x,f(y,s(z))) = f(x,s(f(y,z))) = \\ &= s(f(x,f(y,z))) = s(f(f(x,y),z)) = f(f(x,y),s(z)) = \\ &= H(s(z)) \end{aligned}$$

となるから，数学的帰納法により，つねに $G(z) = H(z)$ がなりたつ。これが証明すべきことであった。QED

1.6　消去

$x, y, a \in \mathbb{N}$ について，$x + a = y + a$ ならば，$x = y$ である。
（このことを以下,「両辺から a を消去する」という。）
証明：命題

$$P(a): \qquad \forall x \forall y [x + a = y + a \Rightarrow x = y]$$

を考える。$P(0)$ はむろん正しい。$P(a)$ を仮定し，$x + s(a) = y + s(a)$ とすると，$s(x + a) = s(y + a)$ となり，公理から $x + a = y + a$ となって，$P(a)$ から $x = y$ が出る。すなわち，$P(s(a))$ がなりたつ。ゆえに，数学的帰納法により，つねに $P(a)$ がなりたつ。QED

1.7　順序の定義

$x, y \in \mathbb{N}$ にたいして，$y = x + z$ となる $z \in \mathbb{N}$ が存在するとき，$x \leq y$ であると定義する。$x \leq y$ かつ $x \neq y$ のとき $x < y$ と記す。

1.8　順序の性質

1）$[x \leq y$ かつ $y \leq x] \Leftrightarrow x = y$
2）$[x \leq y$ かつ $y \leq z] \Rightarrow x \leq z$
3）$x \leq y$ か $y \leq x$ かのいずれかはなりたつ
4）$0 \leq x$
5）$x \leq y \Leftrightarrow x + a \leq y + a$
（いっぱんに 1），2），3）がなりたつ二項関係を全順序とよぶ。）
証明：1）については，$\Rightarrow$ を示せばよい。$x \leq y$ より，$y = x + u$ となり，$y \leq x$ より，$x = y + v$ となる。ゆえに，$y = y + u + v$ となり，両辺から y を消去すると，$0 = u + v$ となる。これから，Peano の公理 2）を用いると，$u = v = 0$ が容易に証明できる。2）は明らかである。3）を証明しよう。x を止めて，

$$A = \{y | x \leq y \text{ あるいは } y \leq x\}$$

を考える。4）は明らかであり，したがって，$0 \in A$ である。$y \in A$ を仮定する。$x \leq y$ か $y \leq x$ がなりたつのであるから，今 $x \leq y$ であったとしよう。$y = x + z$ となる z があり，$s(y) = x + s(z)$ だから，$x \leq s(y)$ となり，

$s(y) \in A$ である。$y \leq x$ のときは，$x = y + z$ となる z がある。もし $z = 0$ なら，$x = y$ であり，$s(y) = s(x) \geq x$ だから，$s(y) \in A$ である。もし $z \neq 0$ なら，$z = s(u) = u + 1$ となる u があり，$x = y + u + 1 = s(y) + u \geq s(y)$ となって，$s(y) \in A$ である。ゆえに数学的帰納法により $A = \mathbb{N}$ である。４）は明らかであり，５）は消去によって容易に証明できる。QED

1.9　乗法の定義

$\mathbb{N}$ 上に乗法 $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ を次のように定義する：
$x, y \in \mathbb{N}$ にたいして

$$
\begin{aligned}
& g(x,0) = 0, \qquad g(x,1) = x, \\
& \cdots, \\
& g(x, s(y)) = g(x,y) + x, \\
& \cdots
\end{aligned}
$$

これで g は一意的かつ完璧に定義される。以下，$g(x,y)$ を xy と記す。

1.10　乗法の性質

１）$x0 = 0, \qquad x1 = x$
２）$xy = yx$
３）$x(yz) = (xy)z$
４）$x(y+z) = xy + xz$
証明： １）は定義である。２）を証明しよう。まず，

$$P(y) : \qquad g(s(x), y) = g(x,y) + y$$

を証明しよう。あきらかに，$P(0)$ は正しい。$P(y)$ を仮定すると，

$$
\begin{aligned}
g(s(x), s(y)) &= g(s(x), y) + s(x) = g(x,y) + y + s(x) = \\
&= g(x,y) + s(y) + x = g(x,y) + x + s(y) = \\
&= g(x, s(y)) + s(y)
\end{aligned}
$$

だから，$P(s(y))$ がなりたつ。ゆえに数学的帰納法により，$P(y)$ はつねになりたつ。そこで，

$$G(x) := g(x,y), \quad H(x) := g(y,x)$$

について考える。容易に証明できるように，$g(0,y)=0$ であるから，$G(0)=H(0)=0$ である。$G(x)=H(x)$ を仮定すると，$P(y)$ より，

$$\begin{aligned} G(s(x)) &= g(s(x),y)=g(x,y)+y= \\ &= g(y,x)+y=g(y,s(x))=H(s(x)) \end{aligned}$$

がなりたつ。ゆえに，数学的帰納法により，つねに $G(x)=H(x)$ がなりたつ。これが証明すべきことであった。

つごうにより，３）の証明はあとまわしにして，先に４）を証明しよう。命題

$$Q(z): \qquad \forall x \forall y[x(y+z)=xy+xz]$$

を考える。$Q(0)$ はむろん正しい。$Q(z)$ を仮定すると，

$$\begin{aligned} x(y+s(z)) &= x(s(y)+z)=xs(y)+xz= \\ &= xy+x+xz=xy+xz+x=xy+xs(z) \end{aligned}$$

となり，$Q(s(z))$ がなりたつ。ゆえに数学的帰納法により，つねに $Q(z)$ がなりたつ。これが証明すべきことであった。

最後に３）を証明しよう。

$$R(z): \qquad x(yz)=(xy)z$$

について，$R(0)$ はむろん正しい。$R(z)$ を仮定すると，４）を用いて，

$$\begin{aligned} x(ys(z)) &= x(yz+y)=x(yz)+xy= \\ &= (xy)z+xy=xys(z) \end{aligned}$$

となり，$R(s(z))$ がなりたつ。ゆえに数学的帰納法により，$R(z)$ はつねに正しい。QED

1.11

$xy=0$ ならば，$x=0$ か $y=0$ かのどちらかはなりたつ。

証明：もし $y\neq 0$ ならば，$y=s(u)$ であり，

$$xy=xs(u)=xu+x\geq x$$

である。ゆえに $xy=0$ から $x\leq 0$ となり，$x=0$ が出る。QED

1.12

$a \neq 0$ にたいして $xa = ya$ ならば $x = y$ である。

証明：$x < y$ ならば，$y = x + z, z \neq 0$ であるから，$ya = xa + za$ であり，1.11 より $za \neq 0$ となり，$ya > xa$ となる。ゆえに $xa = ya$ ではありえない。同様に $x > y$ でもありえない。QED

1.13

$a \neq 0$ のとき，$x \leq y \Leftrightarrow xa \leq ya.$

証明：$\Rightarrow$ は明らかである。逆を証明する。$xa \leq ya$ とする。もし，$x \leq y$ でないとすると，$y < x$ である。すなわち，$x = y + z$ となる $z \neq 0$ が存在する。すると，$a \neq 0$ の大前提より，$za \neq 0$ となり，したがって $xa = ya + za > ya$ である。これは仮定に反する。QED

2　同値関係と商集合

これから自然数系を拡張していくのであるが，そのさい，「同値関係によって商集合をつくる」という操作を何回か繰り返すので，このことを一般的に取り出して説明しておきたい。

E は集合とする。E の要素 x, y の対 (x, y) の全体のなす集合を $E \times E$ と記す。E 上の二項関係というのは，$E \times E$ の部分集合のことである。そこで，E 上の二項関係 R が与えられたとき，$E \times E$ の要素 (x, y) が R に属することを $R(x, y)$ と記すことにし，x は y と関係 R をみたすという。また，このとき xRy と記すこともある。

E 上の二項関係 R が次の 3 つの性質をもつとき，R は同値関係であるという：

1）（反射的）：すべての $x \in E$ にたいしてつねに $R(x, x)$ がなりたつ；

2）（対称的）：任意の $x, y \in E$ にたいして $R(x, y) \Leftrightarrow R(y, x)$ がなりたつ；

3）（推移的）：任意の $x, y, z \in E$ にたいして，$[R(x, y)$ かつ $R(y, z)] \Rightarrow R(x, z)$ がなりたつ。

いま，E 上の同値関係 R がひとつ与えられたとする。このとき，$a \in E$ を止めるごとに E の部分集合 $\{x | R(x, a)\}$ がきまるから，これを $R[a]$ と記して，a の同値類とよぶ。逆に a を同値類 $R[a]$ の代表元とよぶ。

同値関係の性質１）により，少なくとも $a \in R[a]$ であるから，どの同値類も空集合ではないし，全ての同値類の合併は全集合となる。また異なる同値類はたがいに交わらない。じっさい，もし，$c \in R[a]$ かつ $c \in R[b]$ ならば，$R(c,a)$ かつ $R(c,b)$ だから，同値類の性質２），３）により，$R(a,b)$ となり，$R[a] = R[b]$ が従う。こうして，E は異なる同値類に類別される。

そこで，E の同値関係 R にかんする同値類全体のなす集合が考えられるので，これを E/R と記し，E を R で割ってえられる商集合とよぶ。

3　整数

$a, b \in \mathbb{N}$ が与えられたとき，方程式 $a + x = b$ が解をもつ条件は，$a \leq b$ である。$2 + x = 1$ のように $a > b$ のときは，解は存在しない。そのばあいも解をもつように $\mathbb{N}$ を拡張する。

3.1　整数の定義

$X = (a,b), Y = (c,d) \in E := \mathbb{N} \times \mathbb{N}$ にたいして，関係 R を次にように定義する：

$$R(X,Y) \Leftrightarrow b + c = d + a.$$

このとき，関係 R は同値関係になる。念のため，

$$[R(X,Y) \text{ かつ } R(Y,Z)] \Rightarrow R(X,Z)$$

を証明しておこう。

$$X = (a,b), \quad Y = (c,d), \quad Z = (e,f)$$

とすると，仮定は

$$b + c = d + a, \qquad d + e = f + c$$

である。すると，

$$b + c + d + e = d + a + f + c$$

であり，両辺から $d + c$ を消去すると，$b + e = f + a$ すなわち，$R(X,Z)$ を得る。QED

そこで，$\mathbb{N}\times\mathbb{N}$ をこの同値関係 R で割って得られる商集合を $\mathbb{Z}$ とし，その要素を整数とよぶ。

- さて，

$$R((a,b),(a',b')) \Leftrightarrow b+a'=b'+a$$

と定義した。いま，$b\leq b'$ であるとして，$b'=b+m$ としよう。すると，$b+a'=b+m+a$ であるから，両辺から b を消去すると，$a'=a+m$ となる。$b'\leq b$ のばあいも同様である。けっきょく，次のことがいえる：

$R((a,b),(a',b'))$ ということは，$a'=a+m, b'=b+m$ となる $m\in\mathbb{N}$ が存在するか，$a=a'+n, b=b'+n$ となる $n\in\mathbb{N}$ が存在するということに他ならない。

3.2 $\mathbb{N}$ の $\mathbb{Z}$ への埋め込み

$n\in\mathbb{N}$ にたいして，$R[(0,n)]$ を n と同一視して，$\mathbb{N}\subset\mathbb{Z}$ とみなす。じっさい，$R((0,n),(0,n'))$ ならば，$n=n'$ となるから，この同一視をしてよい。

$a,b\in\mathbb{N}$ にたいして，もし $a\leq b$ ならば，$b=a+n$ であり，

$$R((a,b),(0,n)), \qquad R[(a,b)]=n\in\mathbb{N}$$

となる。$a>b$ ならば，$a=b+m$ であり，

$$R((a,b),(m,0))$$

となる。そこで，

$$R[(m,0)]=-m$$

と記す。いいかえると，$x\in\mathbb{Z}$ にたいして，$x\in\mathbb{N}$ であるか，さもなくば，$x=-m$ となる $m\in\mathbb{N},\neq 0$ が存在する。前者の場合で $x\neq 0$ のとき，x は正であるといい，後者の場合，x は負であるという。

3.3 加法の定義

$\mathbb{Z}$ 上に加法 $f:\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$ を次のように定義する：

$$f(R[(a,b)],R[(c,d)])=R[(a+c,b+d)].$$

これが定義になっているためには，それが定義のなかの代表元のとりかたに依存しないことが確かめられていなければならない。すなわち，$R((a,b),(a',b'))$ かつ $R((c,d),(c',d'))$ ならば，$R((a+c,b+d),(a'+c',b'+d'))$ であることが確かめられねばならない。しかし，これはだいじょうぶである。じっさい，このとき，

$$b+a'=b'+a, \qquad d+c'=d'+c$$

であるから，

$$b+d+a'+c'=b'+d'+a+c$$

であり，

$$R((a+c,b+d),(a'+c',b'+d'))$$

が確かになりたつ。

以下，$f(x,y)=x+y$ と記す。これが正当であるのは，$m,n\in\mathbb{N}$ のとき，

$$f(m,n)=f(R[(0,m)],R[(0,n)])=R[(0,m+n)]=m+n$$

だから，f が $\mathbb{N}$ 上のすでに定義されている加法 $+$ の拡張になっているからである。

3.4 加法の性質

1）$0+x=x$
2）$x+y=y+x$
3）$x+(y+z)=(x+y)+z$
証明：証明は受講者の練習問題とする。

3.5 加法にかんする逆元の存在

$a,b\in\mathbb{Z}$ にたいして $a+x=b$ となる $x\in\mathbb{Z}$ がただひとつ存在する。

[**注**]：そもそも整数という概念は，$a,b\in\mathbb{N}$ のときの方程式 $a+x=b$ につねに解をもたせるために，方程式じしんを数とみなして構成したものである。したがって，$a,b\in\mathbb{N}$ のときはこの方程式が解をもつのは，いわば論理的にあたりまえである。しかし，a,b じしんがこうして拡張した整数のときにもまた解があるかどうかは論理的には自明でない。そのば

あいにも解があるためには，さらに拡張する必要はもうないというのが，この主張である。だから，自明なことではなく，証明が必要である。

証明：$a = R[(A, B)], b = R[(C, D)]$ とする。$x = R[(C + B, D + A)]$ とおくと，

$$a + x = R[(A + C + B, B + D + A)] = R[(C, D)] = b$$

がなりたつから，これは解である。また，$x' = R[(U, V)]$ も解ならば，

$$R[(A + U, B + V)] = R[(C, D)]$$

より，

$$B + V + C = D + A + U$$

がなりたち，$x = x'$ となる。QED

3.6　可換群あるいはアーベル群

いっぱんに空でない集合 E の上に演算 $(x, y) \mapsto x + y$ が与えられて次の性質をもっているとき，E はこの演算で可換群ないしアーベル群になっているという：

1）$x + y = y + x$

2）$x + (y + z) = (x + y) + z$

3）任意の $a, b \in E$ にたいして $a + x = b$ となる $x \in E$ がただひとつ存在する（以下，この x を $b - a$ と記す）

- このとき，ただひとつ

$$\forall x \quad [x + O = x]$$

となる要素 O が存在する。これは単位元とよばれる。じっさい，$a + x = a$ の解 $a - a$ をさしあたり O_a と記すとすると，これは実は a に依存しない。じっさい，任意の a' にたいして，

$$a' + O_a + a = a' + a$$

がなりたつので，$O_a = O_{a+a'}$ である。ところが，任意の b にたいして，$a + a' = b$ となる a' が存在するというのであるから，$O_a = O_b$ である。つまり，O_a は a に依存しないので，O と記してよく，任意の a にたいして $a + O = a$ である。

- とくに，$O-a$ を $-a$ と記す。すなわち，$x+(-x)=O$ である。
- 逆に，１）と２）と以下の４），５）がなりたてば，３）が出てくるので，１），２），４），５）を可換群の公理としてもよい：

４）ただひとつの $O \in E$ があって，すべての $x \in E$ にたいして

$$x+O=x$$

である

５）すべての $x \in E$ にたいしておのおの

$$x+x'=O$$

となる $x' \in E$ が存在する。

- いずれにせよ，$\mathbb{Z}$ は定義した加法で可換群となっているわけである。

3.7 乗法の定義

$\mathbb{Z}$ 上の乗法 g は

$$g(R[(a,b)],R[(c,d)])=R[(bc+ad,ac+bd)]$$

と定義する。これが定義となるためには，

(1) $$b+a'=b'+a$$

かつ

(2) $$d+c'=d'+c$$

のとき，

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

とならねばならない。これを確かめよう。(1) × (2) を計算して，

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

であり，

$$\begin{aligned}
\text{左辺} &= bd + bc' + a'd + a'c' \\
&= bd + bc' + a'(d + c') \\
&= bd + bc' + a'(c + d') \\
&= bd + bc' + a'c + a'd', \\
\text{右辺} &= b'd' + b'c + ad' + ac \\
&= b'd' + b'c + a(d' + c) \\
&= b'd' + b'c + a(d + c') \\
&= b'd' + b'c + ad + ac'
\end{aligned}$$

である。ゆえに両辺に $ac+b'c'$ を加え，右辺を (1)(2) を用いて変形すると，

$$\begin{aligned}
\text{左辺} &= bd + ac + b'c' + a'd' + bc' + a'c, \\
\text{右辺} &= b'd' + ad + b'c + ac' + ac + b'c' \\
&= b'd' + ad + (b' + a)c + (a + b')c' \\
&= b'd' + ad + (b + a')c + (a' + b)c' \\
&= b'd' + ad + bc + a'c + a'c' + bc'
\end{aligned}$$

となり，両辺から $a'c + bc'$ を消去して (3) を得る。

$x, y \in \mathbb{N}$ ならば，

$$g(x, y) = R[(0, xy)] = xy$$

となるから，g は $\mathbb{N}$ 上の乗法の $\mathbb{Z}$ 上への拡張になっているので，以下，$g(x, y)$ を xy と記す。

3.8 乗法の性質

1）$x0 = 0, \qquad x1 = x$

2）$xy = yx$

3）$x(yz) = (xy)z$

4）$x(y + z) = xy + xz$

証明：証明は受講者にゆだねる。

3.9　可換環

いっぱんに加法と乗法が定義されていて加法について可換群をなし，乗法が3.8の性質１）～４）をもつとき，可換環であるという。乗法の性質２）を仮定しないときは，たんに環になっているという。

- 次のことに注意しよう。上にすでに定義した加法とともに，すでに定義した乗法と同じかどうか知らない乗法 $*$ があって，とにかく $+$ と $*$ とで環になっているとしよう。すなわち，

$$\begin{aligned} x*(y*z) &= (x*y)*z, \\ x*(y+z) &= x*y+x*z, \\ (x+y)*z &= x*z+y*z \end{aligned}$$

はなりたっているとする。しかも，この乗法 $*$ は $\mathbb{N}$ 上のわれわれの乗法を拡張したものではあるとしよう。このとき，$*$ はわれわれの乗法にほかならない。証明しよう。以下 $m,n\in\mathbb{N}$ とする。

$x=m*n$ は仮定によって mn に等しい。

$x=(-m)*n$ にたいしては，

$$m*n+x=(m+(-m))*n=0*n=0n=0$$

がなりたつから，

$$x=-(m*n)=-(mn)=(-m)n$$

である。ゆえに $(-m)*n=(-m)n$ がなりたつ。

$x=m*(-n)$ にたいしては，

$$m*n+x=m*(n+(-n))=m*0=m0=0$$

がなりたつから，

$$x=-(m*n)=-(mn)=m(-n)$$

である。ゆえに $m*(-n)=m(-n)$ がなりたつ。

また，同様にして，

$$\begin{aligned} (-m)*(-n) &= -(m*(-n))=-(-(m*n))= \\ &= -(-mn)=mn=(-m)(-n) \end{aligned}$$

が確かめられ，$(-m)*(-n)=(-m)(-n)$ である。これですべての場合を尽くした。QED

- このことから，負の数と負の数をかけると正の数になるのは，環になるように乗法を拡張することからくる必然であることがわかる。

3.10

$a, x, y \in \mathbb{Z}$ について，$a \neq 0$ かつ $ax = ay$ ならば $x = y$ である。

証明：$z = x - y$ とおくと，$az = 0$ である。一般性をそこなわず，$a \in \mathbb{N}$ としてよい。ところが，$z \in \mathbb{N}$ ならば，1.11 により $z = 0$ である。$z = -m, m \in \mathbb{N}, m \neq 0$ としても矛盾するので，やはり $z = 0$ である。QED

3.11　順序の定義

$x, y \in \mathbb{Z}$ は，$y - x \in \mathbb{N}$ のとき，$x \leq y$ であると定義する。あきらかにこれは $\mathbb{N}$ 上の順序の拡張になっている。

3.12　順序の性質

1）$x = y \Leftrightarrow [x \leq y$ かつ $y \leq x]$
2）$[x \leq y$ かつ $y \leq z] \Rightarrow x \leq z$
3）$x \leq y$ か $y \leq x$ のいずれかはなりたつ
4）$x \leq y \Leftrightarrow x + a \leq y + a$
5）$a > 0$ ならば，$x \leq y \Leftrightarrow ax \leq ay$

4　有理数

$a, b \in \mathbb{Z}$ にたいして，$a \neq 0$ であっても，方程式 $ax = b$ は解をもつとはかぎらない。たとえば，$2x = 1$ は解をもたない。このような方程式がつねに解をもつように数を拡張する。

4.1　有理数の定義

$E = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} | a \neq 0\}$ とおく。$X = (a, b), Y = (c, d) \in E$ にたいして関係 R を次のように定義する：

$$R(X, Y) \Leftrightarrow bc = ad$$

このとき，R が同値関係であることが 3.1 と同様に確かめられる。「消去」に対応する操作は 3.10 を用いる。そこで，E をこの同値関係 R で割ってえられる商集合 E/R を $\mathbb{Q}$ とし，その要素（同値類）を有理数とよぶ。

- $b \in \mathbb{Z}$ にたいして $R[(1,b)]$ を b と同一視することによって，$\mathbb{Z} \subset \mathbb{Q}$ とみなすことにする。じっさい，$R((1,b),(1,b'))$ ならば，$b = b'$ であるから，こうみなしてさしつかえない。

4.2 加法の定義

$\mathbb{Q}$ 上に加法 f を次のように定義する：

$$f(R[(a,b)], R[(c,d)]) = R[(ac, bc+ad)]$$

これが定義になっているためには，

$$ba' = ab', \qquad dc' = d'c$$

から

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

が導かれねばならないが，じっさい，

$$\begin{aligned}(bc+ad)a'c' &= a'bcc' + ad'dc' \\ &= ab'cc' + aa'd'c \\ &= ac(b'c'+a'd')\end{aligned}$$

である。また，$a \neq 0, c \neq 0$ ならば $ac \neq 0$ であることにも留意しておこう。

$f(R[(1,b)], R[(1,d)]) = R[(1,b+d)]$ だから，f は $\mathbb{Z}$ 上の加法 $+$ の拡張になっているので，以下，$f(x,y)$ を $x+y$ と記す。

4.3 加法の性質

1）$0 + x = x$
2）$x + y = y + x$
3）$x + (y + z) = (x + y) + z$

4.4 加法についての逆元の存在

$a, b \in \mathbb{Q}$ にたいして，$a + x = b$ は $\mathbb{Q}$ のなかにただひとつの解 x をもつ。

証明：$a = R[(A,B)], b = R[(C,D)]$ ならば，$x = R[(AC, AD - BC)]$ が解である。また，$x' = R[(U,V)]$ も解ならば，

$$R[(AU, BU + AV)] = R[(C,D])$$

より

$$AUD = (BU + AV)C$$

となり，

$$(AD - BC)U = ACV$$

だから，$x' = x$ となる。QED

4.5 乗法の定義

$\mathbb{Q}$ 上の乗法 g を次のように定義する：

$$g(R[(a,b)], R[(c,d)]) = R[(ac, bd)]$$

じっさい，$ad' = a'd, cd' = c'd$ のとき，$acb'd' = a'c'bd$ であるから，これは定義になっている。

$$g(R[(1,b)], R[1,d]) = R[(1,cd)]$$

から g は $\mathbb{Z}$ 上の乗法の拡張になっているので，以下 $g(x,y)$ を xy と記す。

4.6 乗法の性質

1）$0x = 0, \qquad 1x = x$
2）$xy = yx$
3）$x(yz) = (xy)z$
4）$x(y+z) = xy + xz$

4.7 乗法についての逆元の存在

$a, b \in \mathbb{Q}, a \neq 0$ のとき，$ax = b$ となる $x \in \mathbb{Q}$ がただひとつ存在する。

証明：$a = R[(A,B)] \neq 0, b = R[(C,D)]$ ならば，明らかに $B \neq 0$ であり，$x = R[(BC,AD)]$ が解である。また，$x' = R[(U,V)]$ も解ならば，

$$R[(AU,BV)] = R[(C,D)]$$

となり，$BVC = AUD$ であるから，$x = x'$ となる。QED

- とくに，$ax = 1$ の解を a^{-1} と記し，a の逆数とよぶ。むろん，$a = R[(A,B)]$ ならば，$a \neq 0$ より，$B \neq 0$ であり，$a^{-1} = R[(B,A)]$ である。

4.8 体

いっぱんに集合 E の上に加法と乗法が定義されて環になっており，しかも，加法の単位元を O とするとき，E から O を除いたものが乗法にかんして可換群になっているとき，E は体になっているという。したがって，$\mathbb{Q}$ は体である。

4.9 順序の定義

$x \in \mathbb{Q}$ について，$x = R[(a,b)]$ となる $a > 0, b \geq 0$ があるとき，$x \geq 0$ と定義する。$x, y \in \mathbb{Q}$ は，$y - x \geq 0$ のとき，$x \leq y$ と定義する。

4.10 順序の性質

$\mathbb{Q}$ は次の性質をもつという意味で全順序体である：

1）$x = y \Leftrightarrow [x \leq y$ かつ $y \leq x]$

2）$[x \leq y$ かつ　$y \leq x] \Rightarrow x \leq z$

3）$x \leq y$ か $y \leq x$ かのいずれかがなりたつ

4）$x \leq y \Leftrightarrow x + a \leq y + a$

5）$a > 0$ ならば，$x \leq y \Leftrightarrow ax \leq ay$

5 実数

よく知られているように，方程式 $x^2 = 2$ は $\mathbb{Q}$ のなかに解をもたない。$\mathbb{Q}$ を実数体 $\mathbb{R}$ に拡張すると，この方程式は $\mathbb{R}$ のなかに解をもつようになる。しかし，$\mathbb{Q}$ から $\mathbb{R}$ への拡張は，$\mathbb{N}$ から $\mathbb{Z}$ への，$\mathbb{Z}$ から $\mathbb{Q}$ への拡張が

そうであったように，このような代数方程式に解をもたせるだけの代数的な拡張ではなく，いわば超越的である。古くからある「連続性とは何か」という問いに正面から答えることによって，この拡張はなされる。その拡張の方法には同値なものがいくつかあるが，この章ではデーデキントの方法に基づくことにする。

5.1 実数の定義

$\mathbb{Q}$ の部分集合 A は，次の性質をもつとき，実数であるという：

1）$A \neq \emptyset, \quad A \neq \mathbb{Q}$

2）$\forall p \in A[p \leq q] \Leftrightarrow q \notin A$

実数すべてのつくる集合を $\mathbb{R}$ と記す。

- $r \in \mathbb{Q}$ にたいして，

$$A =] \leftarrow, r[:= \{p \in \mathbb{Q} | p < r\}$$

を考えると，A は実数である。

じっさい，$A \neq \emptyset, A \neq \mathbb{Q}$ であるし，もし $\forall p[p \leq q]$ ならば，それは $p < r \Rightarrow p \leq q$ であるということなので，$q \in A$ すなわち $q < r$ ではありえない（もしそうなら，$p = \frac{1}{2}(r+q)$ は $q < p < r$ となって矛盾）。逆に $q \notin A$ ならば，$r \leq q$ だから，$\forall p \in A[p \leq q]$ は確かである。ゆえに A は条件 2）をみたして，実数であるといってよい。

そこで，$A =] \leftarrow, r[$ を r と同一視して，以下 $\mathbb{Q} \subset \mathbb{R}$ とみなす。$r \neq r'$ ならば $] \leftarrow, r[\neq] \leftarrow, r'[$ だから，こうみなしてよい。このとき，もちろん，$p, q \in \mathbb{Q}$ について，

$$p \in q \Leftrightarrow p < q$$

である。

とはいえ，以下でこの同一視によって議論が混乱しそうなときは，$r \in \mathbb{Q}$ にたいして $r^* :=] \leftarrow, r[$ と記して，これを $\mathbb{R}$ の要素とみなしていることを強調することにしよう。

- さて，$x \in \mathbb{R}, p \in \mathbb{Q}, p \in x$ ならば，$r < p$ をみたす $r \in \mathbb{Q}$ は $r \in x$ となる。（じっさい，もし $r \notin x$ ならば，$\forall p \in x[p \leq r]$ のはずである。）したがって，$p \in x$ ならば，

$$] \leftarrow, p] := \{r \in \mathbb{Q} | r \leq p\} \subset x$$

であり，したがって，

$$x = \bigcup_{p \in x}]\leftarrow, p]$$

といえる。

- $\mathbb{Q}$ の部分集合 A が実数であるためには，１）と次の３），４）がなりたつことが必要充分である：

３）$[p \in A$ かつ $r < p] \Rightarrow r \in A$

４）$\forall p \in A[p \leq q] \Rightarrow q \notin A$　（言い換えると A には最大元がない）

証明：$2) \Rightarrow 3), 4)$ はいま観察したとおりである。$3), 4) \Rightarrow 2)$ を確かめるには，

$$q \notin A \Rightarrow \forall p \in A[p \leq q]$$

を示せばよい。しかし，もしそうでないとすると，$q \notin A$ と $q < p$ となる $p \in A$ とがあるわけだが，すると $q < p \in A$ から３）より $q \in A$ のはずであり，矛盾である。QED

- デーデキントの元の論文（「連続性と無理数」1872）では実数は次のように定義されている。

> いま $\mathbb{Q}$ の部分集合 A, B の対 (A, B) は次の条件をみたすとき，「切断」とよぶ：
>
> $$A \neq \emptyset, \quad B \neq \emptyset, \quad [p \in A, q \in B] \Rightarrow p < q$$
>
> ただし，切断 (A, B) において，A に最大 r があるばあいと，B に最小 r があるばあいは，区別せず，このとき (A, B) は有理数 r じしんと同一視する。実数（すなわち有理数でなければ無理数）とは，切断に他ならない。

この定義はわれわれのものと同じである。じっさい，(A, B) が切断で，A には最大がないとすると，A はわれわれの意味で実数である。なんとならば，$p < q \in A$ であれば $p \in A$ である。（さもなくば，$p \notin A$ だから，$p \in B$ となり，$q < p$ でなければならない。）また，$\forall p \in A[p \leq q]$ であるとすると，$q \notin A$ である。（さもなくば，$q \in A$ であり，これは A の最大元となり，仮定に反する。）ゆえに A はわれわれの意味で実数である。逆に，$A \subset \mathbb{Q}$ がわれわれの意味で実数であるとすると，$\mathbb{Q}$ における A の補集合を B とすると，(A, B) は切断である。なんとなれば，$p \in A, q \in B$ なら，$p \in A, q \notin A$ だから，実数の定義の条件２）により，$p \leq q$ であり，$p \neq q$ より $p < q$ である。

5.2　順序の定義

$x, y \in \mathbb{R}$ にたいして，$x \subset y$ のとき，$x \leq y$ と定義する。これはあきらかに $\mathbb{Q}$ 上の順序の拡張になっている。

5.3　順序の性質

1）$x = y \Leftrightarrow [x \leq y$ かつ $y \leq x]$
2）$[x \leq y$ かつ $y \leq z] \Rightarrow x \leq z$
3）$x \leq y$ か $y \leq x$ かのいずれかはなりたつ
証明：1），2）はあきらかなので，3）を証明しよう。もし，$x \leq y$ でなかったとすると，$p_1 \in x, p_1 \notin y$ となる $p_1 \in \mathbb{Q}$ があるはずである。$p_1 \notin y$ だから，$\forall p \in y[p \leq p_1]$ となる。$p_1 \in x$ から $] \leftarrow, p_1] \subset x$ だから，これは $y \subset x$ を導く。すなわち，$y \leq x$ である。QED

5.4

$p \in \mathbb{Q}, x \in \mathbb{R}$ にたいして，

$$p \in x \Leftrightarrow p < x$$

がなりたつ。
証明：議論の混乱を避けるため，$p \in \mathbb{Q}$ にたいして，これを $\mathbb{R}$ の要素とみなすときは，$p^* =] \leftarrow, p[$ と記して区別することにしよう。すると，示すべきことは，「$p \in x \Leftrightarrow p^* < x$」である。
まず $\Rightarrow$ を示そう。すなわち，$x \in \mathbb{R}, p \in \mathbb{Q}$ について，$p \in x$ ならば，$p^* < x$ である。なぜなら，$p \in x$ なら，5.1 で注意したように，$] \leftarrow, p] \subset x$ であるから，$p^* \leq x$ であり，$p \notin p^* =] \leftarrow, p[$ であるから，$p^* = x$ ではありえない。ゆえに $p^* < x$ である。
つぎに $\Leftarrow$ を示そう。$p \in \mathbb{Q}, x \in \mathbb{R}$ について，もし $p \notin x$ ならば，$x \leq p^*$ である。じっさい，実数の定義から，$p \notin x$ から $\forall q \in x[q \leq p]$ であるから，$x \subset] \leftarrow, p]$ となる。$p \notin x$ より，$x \subset] \leftarrow, p[$ となり，$x \leq p^*$ が出る。したがって，$p^* < x \Rightarrow p \in x$ がいえる。QED

5.5 $\mathbb{Q}$ の稠密性

$x, y \in \mathbb{R}$ が $x < y$ をみたすと，$x < p < y$ となる $p \in \mathbb{Q}$ が存在する。

証明：この証明でも，混乱を避けるため，$p \in \mathbb{Q}$ にたいして $p^* =]\leftarrow, p[$ と記す。すると示すべきことは，$x < p^* < y$ となる $p \in \mathbb{Q}$ の存在である。

さて，$x < y$ とは，$x \subset y$ かつ $x \neq y$ であるということであるから，$p_1 \notin x, p_1 \in y$ となる $p_1 \in \mathbb{Q}$ がある。このとき，上のことから，$x \leq p_1^* < y$ である。さらに，$x < p^* < y$ となる $p \in \mathbb{Q}$ が存在する。なんとならば，$x < p_1^*$ ならばいいから，p_1 が $p_1^* = x$ をみたす場合を考えよう。そのときは，$x \in \mathbb{Q}$ で，$x = p_1^* =]\leftarrow, p_1[$ である。$p_1 < p$ となる $p \in y$ が存在しなければ，$p \in y \Rightarrow p \leq p_1$ となるので，これから $p_1 \notin y$ である。したがって，5.4 から，$y \leq p_1^*$ となって矛盾である。ゆえに，$p_1 < p \in y$ となる p が存在し，$x = p_1 < p^* < y$ である。QED

- このことからまた，

$$x = \bigcup_{p \in x}]\leftarrow, p[$$

である。じっさい，

$$x = \bigcup_{p \in x}]\leftarrow, p]$$

であったので，

$$\bigcup_{p \in x}]\leftarrow, p[\subset x$$

であるし，逆に $q \in x$ ならば，$q^* < x$ であるので，$q^* < p_1^* < x$ となる $p_1 \in \mathbb{Q}$ があり，$p_1 \in x$ である。$q \in]\leftarrow, p_1[$ だから，

$$q \in \bigcup_{p_1 \in x}]\leftarrow, p_1[$$

といえる。すなわち

$$x \subset \bigcup_{p \in x}]\leftarrow, p[$$

である。

5.6 上限

$\mathbb{R}$ の部分集合 A が空でなく，しかも次の意味で上に有界とする：$\forall x \in A[x \leq M]$ となる $M \in \mathbb{Q}$ が存在する。このとき，次のふたつの性質をも

つ $\alpha \in \mathbb{R}$ がただひとつ存在するので，これを $\sup A$ と記し，A の上限とよぶ：

1）$\forall x \in A[x \leq \alpha]$

2）$\forall x \in A[x \leq \mu] \Rightarrow \alpha \leq \mu$

証明：

$$\alpha = \{p \in \mathbb{Q} | \exists x \in A[p < x]\}$$

とおく。これは実数である。じっさい，A は空でないと仮定してあるから，α は空でないし，A は上に有界だから，α が $\mathbb{Q}$ 全体に一致することもない。$p' < p \in \alpha \Rightarrow p' \in \alpha$ はあきらかである。$q \in \mathbb{Q}$ が $\forall p \in \alpha[p \leq q]$ をみたすとすると，$\forall x \in A[x \leq q]$ である。（じっさい，$q < x_0 \in A$ とすると，5.5 から $q < p < x_0$ となる $p \in \mathbb{Q}$ が存在し，α の定義より $p \in \alpha$ となる一方，$q < p$ は $\forall p \in \alpha[p \leq q]$ と矛盾する。）ゆえに，$q \notin \alpha$ である。以上より α は実数である。

しかも，$x \in A$ ならば，$x \leq \alpha$ である。（じっさい，さもなくば，$\alpha < x$ となり，$\alpha < p < x$ となる $p \in \mathbb{Q}$ をとると，$p < x \in A$ から $p \in \alpha$ が出て，5.4 より $p < \alpha$ となり，矛盾。）

また，$\forall x \in A[x \leq \mu]$ であるとすると，$\alpha \leq \mu$ である。（じっさい，さもなくば，$\mu < \alpha$ となり，5.5 より $\mu < p < \alpha$ となる $p \in \mathbb{Q}$ が存在する。このとき，$p \in \alpha$ より $p < x_0$ となる $x_0 \in A$ が存在する。一方，$\mu < p$ であるから，$\mu < x_0$ となり，これは仮定に反する。）QED

5.7　下限

$\mathbb{R}$ の部分集合 A は空でなく，しかも次の意味で下に有界とする：$\forall x \in A[N \leq x]$ となる $N \in \mathbb{Q}$ が存在する。このとき，次のふたつの性質をもつ $\beta \in \mathbb{R}$ がただひとつ存在するので，これを $\inf A$ と記し，A の下限とよぶ。

1）$\forall x \in A[\beta \leq x]$

2）$\forall x \in A[\nu \leq x] \Rightarrow \nu \leq \beta$

証明：いま

$$B = \{p \in \mathbb{Q} | \forall x \in A[p < x]\}$$

とおく。次のふたつのばあいがありうる：

甲）$\forall p \in B[p \leq q] \Rightarrow q \notin B$

乙）$\exists q \in B \forall p \in B[p \leq q]$

甲）のばあいは，B が実数となるので，$\beta = B$ とおく。乙）のばあいは，条件をみたす q はただひとつであるので，それを $q = Q$ として，$\beta = B - \{Q\}$ とおく。すると，β は実数となる。いずれのばあいも，β が下限であることを示そう。

まず，1）を確かめる。もし，$x_0 < \beta$ となる $x_0 \in A$ が存在すれば，$x_0 < p_0 < \beta$ となる $p_0 \in \mathbb{Q}$ が存在する。すると，$p_0 \in \beta \subset B$ だから，$\forall x \in A[p_0 < x]$ のはずであり，矛盾である。したがって，$\forall x \in A[\beta \leq x]$ はよい。

次に2）を確かめる。$\forall x \in A[\nu \leq x]$ とする。$\nu \leq \beta$ を示すため，$\beta < \nu$ と仮定して矛盾を導こう。もし，$\beta < \nu$ ならば，$\beta < p_0 < \nu$ となる $p_0 \in \mathbb{Q}$ がある。このとき，$\forall x \in A[\nu \leq x]$ と $p_0 < \nu$ とから $\forall x \in A[p_0 < x]$ となり，$p_0 \in B$ である。甲）のばあいは，$B = \beta$ だから，$p_0 \in \beta$ となり，これは $\beta < p_0$ すなわち $p_0 \notin \beta$ と矛盾する。乙）のばあいは，$p_0 \in B, p_0 \notin \beta$ だから，$p_0 = Q$ であって，$\forall p \in B[p \leq Q]$ である。いいかえると，

$$(*) \qquad \forall x \in A[p < x] \Rightarrow p \leq p_0$$

である。しかし，$p_0 < \nu$ であったから，$p_0 < p_1 < \nu$ となる $p_1 \in \mathbb{Q}$ がある。すると，$\forall x \in A[\nu \leq x]$ の仮定から $\forall x \in A[p_1 < x]$ となるから，$(*)$ より $p_1 \leq p_0$ が出てきて，$p_0 < p_1$ と矛盾する。したがって，いずれにせよ，$\nu \leq \beta$ である。QED

5.8 連続の公理

$\mathbb{R}$ の部分集合 A, B がいずれも空でなく，$A \cup B = \mathbb{R}$ をみたし，かつ

$$a \in A, \quad b \in B \quad \Rightarrow \quad a < b$$

ならば，

$$a \in A \Rightarrow a \leq c, \quad b \in B \Rightarrow c \leq b$$

となる $c \in \mathbb{R}$ が存在する。

証明：$c = \sup A$ でよい。

[**注**]：この定理について，ある哲学者は2010年に発表した論文で次のように書いている：

ともあれ著作 [デーデキント 1872] は実数体 R が上記の定義に従って，連続であるという証明において頂点に達する。このことが意味するのは，R 上に任意の切断が与えられると，それを産出する，有理数，無理数はいずれにせよ，唯一つの数が存在するということである。その証明は至って簡単である。というのは，有理数体 Q 上の切断（それは R 上の切断に含まれる）によって定義された実数を考えれば十分だからである。

そうだろうか。私にはこの哲学者は事態の本質を把握しそこなっているとしか思えない。たしかに，実数体は有理数体のあらゆる切断が数を定めるように，切断自体を数とみなして構成されている。しかし，そうして拡張された実数体において，切断を考えると，もはやその産出する数をそれ以上付け加える必要はない，というのがデーデキントのアイデアであり，この定理の主張である。これはちょうど，自然数系から整数環へと数を拡張したときに 3.5 で注意したのと同じ事態であり，証明抜きに見方を変えるだけで自明なことであるとはけして云えない。このテキストの流れでは上限の存在を先に証明してあるので，証明が 1 行で済んでいるが，デーデキント 1872 の元の証明は，次のようになっている。

一般性を損なわず，A には最大元がないとして，$c = A \cap \mathbb{Q}$ とおけばよい，というのである。

まず，何はともあれ，$A \cap \mathbb{Q}$ が実数であることを確かめねばならない。

$p < r \in A \cap \mathbb{Q}, p \in \mathbb{Q}$ ならば，$p \in A$ である。（さもなくは，$p \in B$ となり，$r \in A$ だから，$r \leq p$ のはずである。）さらに，いま $\forall p \in A \cap \mathbb{Q}[p \leq q], q \in \mathbb{Q}$ ならば，$q \notin A$ である。さもなくは，$q \in A \cap \mathbb{Q}$ は $A \cap \mathbb{Q}$ の最大元である。それは A の最大元となる。（じっさい，$x \in A$ ならば，$x \leq q$ でなければならない。さもなくは，$q < x$ となり，$q < r < x$ となる $r \in \mathbb{Q}$ があり，$r < x \in A$ から $r \in A$ でもあり，けっきょく $r \in A \cap \mathbb{Q}$ であるから，q が $A \cap \mathbb{Q}$ の最大元であることに反する。）A には最大元はないと前提してあるので，$q \notin A$ である。これにより，$A \cap \mathbb{Q}$ は確かに実数である。

いま $a \in A$ とすると，$a \leq c$ である。さもなくは，$c < a$ であり，$c < r < a$ となる $r \in \mathbb{Q}$ があって，$r < a \in A$ から $r \in A \cap \mathbb{Q} = c$ となる。これから 5.4 によって $r < c$ のはずであり，$c < r$ と矛盾する。

また $b \in B$ とすると，$c \leq b$ である。さもなくは，$b < r < c$ となる $r \in \mathbb{Q}$ があり，$r < c = A \cap \mathbb{Q}$ から，$r \in c = A \cap \mathbb{Q}$ となる。すると，仮定から $r \leq b$ のはずであり，$b < r$ と矛盾する。QED

以上の証明をもって,「自明である」,「至って簡単である」という感覚で

臨むならば，それは，デーデキントの仕事ぜんたいが「自明である」「至って簡単である」というに等しいのではないか。しかしこれは，数学において創造的な仕事をした経験が全くない人の感覚である。数学をやるときは，この哲学者のようにレトリックに頼って問題が解決したかのように早合点すべきではない。

5.9 加法の定義

$\mathbb{R}$ 上の加法を次のように定義する：

$$f(x,y) = \{p+q | p \in x, q \in y\}$$

ここで，右辺 $A := \{p+q|p \in x, q \in y\}$ が実数であることを確かめよう。

いま，$\forall r \in A[r \leq t]$ であるとする。このとき，もし $t \in A$ ならば，

$$t = p_0 + q_0, \quad p_0 \in x, \quad q_0 \in y$$

であり，しかも

$$\forall p \in x \forall q \in y[p+q \leq p_0 + q_0]$$

となる。とくに $q = q_0$ ととると，

$$\forall p \in x[p \leq p_0]$$

となり，$p_0 \notin x$ でなければならず，矛盾である。ゆえに $t \notin A$ である。

逆に，$\exists r \in A[t < r]$ としよう。すると，

$$t < p_1 + q_1, \quad p_1 \in x, \quad q_1 \in y$$

となる p_1, q_1 がある。$s := p_1 + q_1 - t \ \in \mathbb{Q}$ は $s > 0$ をみたすので，

$$t = (p_1 - \frac{s}{2}) + (q_1 - \frac{s}{2}), \quad p_1 - \frac{s}{2} \in x, \quad q_1 - \frac{s}{2} \in y$$

となり，$t \in A$ が出る。以上のことから，A は実数である。

さらに，$x, y \in \mathbb{Q}$ ならば，

$$A = \{r | r < x + y\} =] \leftarrow, x + y[$$

はあきらかであり，これは $x+y$ と同一視されている。ゆえに f は $\mathbb{Q}$ 上の加法の拡張となっており，以下 $f(x,y)$ を $x+y$ と記す。

5.10　加法の性質

1）$0+x=x$
2）$x+y=y+x$
3）$x+(y+z)=(x+y)+z$
証明： 1）を証明しよう。すなわち

$$\{p+q|p\in 0, q\in x\}=x$$

を示す。$p\in 0, q\in x$ ならば，$p<0$ より $p+q<q\in x$ だから，$p+q\in x$ である。逆に，$r\in x$ ならば，$r<q\in x$ となる $q\in\mathbb{Q}$ が存在し，

$$r=(r-q)+q$$

であり，$p:=r-q<0$ より，$p\in 0, q\in x$ だから，

$$r\in\{p+q|p\in 0, q\in x\}$$

となる。
2），3）はあきらかである。

5.11

あきらかに，任意の $x, y, a\in\mathbb{R}$ にたいして

$$x\leq y\Rightarrow x+a\leq y+a$$

がなりたつ。じつは逆もなりたつのだが，いまは証明しない。減法を確立してから証明する。

5.12　加法にかんする逆元の存在

$a, b\in\mathbb{R}$ にたいして，$a+x=b$ となる $x\in\mathbb{R}$ がただひとつ存在する。
証明：

$$\begin{aligned} x &= \{q-p|q\in b, \quad p\notin a\} \\ &= \{q-p|q\in b, \forall r\in a[r\leq p]\} \end{aligned}$$

とおく。

x は実数である。じっさい，$s' < s = q - p \in x, q \in b, p \notin a$ ならば，$s' = q - (p + s - s') \in x$ はあきらかであろう。もし $\forall s \in x[s \leq t]$ であれば，$t \notin x$ である。（さもなくは，

$$t = q_0 - p_0, \quad q_0 \in b, \quad p_0 \notin a$$

となる q_0, p_0 があり，一方，仮定 $\forall s \in x[s \leq t]$ は

$$q \in b, p \notin a \quad \Rightarrow \quad q + p \leq q_0 + p_0$$

ということである。ここで $p = p_0$ ととると，

$$q \in b \Rightarrow q \leq q_0$$

となる。これから，b は実数だから，$q_0 \notin b$ となり，矛盾。）かくて，x は実数である。

$a + x = b$ を示そう。

まず $a + x \leq b$ を示すために，$r \in a, s \in x$ とする。$r + s \in b$ を示さねばならない。$s \in x$ より

$$s = q - p, \quad q \in b, \quad \forall t \in a[t \leq p]$$

である。したがって，

$$r + s = r + q - p \leq r + q - r = q \in b$$

となっているので，たしかに $r + s \in b$ である。

次に $a + x < b$ と仮定して矛盾をみちびくことにする。もしそうなら，$a + x < q_0 < b$ となる $q_0 \in \mathbb{Q}$ が存在する。むろん $q_0 \in b$ である。$q_0 \notin a + x$ であるから，$\forall u \in a + x[u \leq q_0]$ である。すなわち，

$$r \in a, q \in b, p \notin a \qquad \Rightarrow \qquad r + q - p \leq q_0$$

である。$q_0 < b$ より，$q_1 = q_0 + e < b$ となる $e > 0, e \in \mathbb{Q}$ がある。すると，上の条件で $q = q_1$ ととると，

$$r \in a, p \notin a \qquad \Rightarrow \qquad r + e - p \leq 0$$

となる。ところが，$a < p_0 < a + e$ をみたす $p_0 \in \mathbb{Q}$ があり，この p_0 は $p_0 \notin a$ をみたすので，この条件から，

$$r \in a \qquad \Rightarrow \qquad r + e \leq p_0$$

である。しかし，$p_0 < a + e$ より $p_0 < r_1 + e < a + e$ となる $r_1 \in \mathbb{Q}$ が存在し，このとき $r_1 < a$ だから $r_1 \in a$ である。すると，上の条件より，$r_1 + e \leq p_0$ でなければならず，$p_0 < r_1 + e$ と矛盾する。

解の一意性を示そう。すなわち，

$$a + x = a + y \quad \Rightarrow \quad x = y$$

を確かめる。このためには，とにかく $a + z = 0$ の解 z は少なくとも一つは存在したから，それを用いて，

$$\begin{aligned} x + a = y + a \quad &\Rightarrow \quad x + a + z = y + a + z \\ &\Rightarrow \quad x + 0 = y + 0 \\ &\Rightarrow \quad x = y \end{aligned}$$

といえる。QED

これで，$\mathbb{R}$ は加法にかんして可換群となった。

5.13 順序と加法の両立

1）$x \leq y \quad \Rightarrow \quad y - x \leq 0$

2）$x \leq y \quad \Leftrightarrow \quad x + a \leq y + a$

証明：1）を示そう。$z = y - x$ とおくと，$y = x + z$ である。まず，$x \leq y \Rightarrow z \geq 0$ を示す。もし，$x < y$ であり，$z < 0$ であれば，$z < s_0 < 0$ となる $s_0 \in \mathbb{Q}$ があり，$\forall q \in z[q < s_0 < 0]$ となる。$p + q \in y, p \in x, q \in z$ をとると，$p + q < p + s_0 < p$ より，$p + q \in x$ となる。ゆえに $y \leq x$ となって仮定 $x < y$ に反する。次に，$z \geq 0 \Rightarrow x \leq y$ を示そう。もし，$z > 0$ であれば，$p \in x$ にたいして，$0 \in z$ だから，$p = p + 0 \in y$ となる。すなわち，$x \subset y, x \leq y$ である。もし $z = 0$ ならば，$y = x$ である。いずれにせよ，$z \geq 0$ ならば，$x \leq y$ である。

すでに減法は可能になっているので，2）は1）からただちに出る。QED

5.14 以下の議論の方針

ほんらいなら，続けて，加法と同じように乗法を集合論的に定義し，その性質を調べて，$\mathbb{R}$ が全順序体であることを確かめる，というように議

論を運ぶべきところである。しかし，このようにすると，議論はきわめて煩瑣になるだろう。したがって，ここで議論の方向をいったん転じて，いわば位相構造を導入し，議論を軽くすることにする。このトリックはデーデキントの提起による。

5.15　絶対値

$x \in \mathbb{R}$ にたいして

$$|x| = \begin{cases} x & \text{if } 0 \leq x \\ -x & \text{if } x < 0 \end{cases}$$

と定義し，x の絶対値とよぶ。次のことは容易に確かめられよう：

1）$0 \leq |x|, \qquad |x| = 0 \Leftrightarrow x = 0$

2）$|x + y| \leq |x| + |y|$

5.16　数列の収束

$\mathbb{N}$ から $\mathbb{R}$ への写像 $n \mapsto a_n$ を $\mathbb{R}$ のなかの数列とよび，$(a_n)_{n=0,1,2,\cdots}$ と記す。これが $a \in \mathbb{R}$ に収束するとは

$$\forall K \in \mathbb{N} \exists N \in \mathbb{N} \forall n \in \mathbb{N} [n \geq N \Rightarrow |a_n - a| \leq \frac{1}{K}]$$

となることをいう。このとき，

$$a_n \to a \qquad (n \to \infty)$$

と表す。

a はこの数列の極限とよばれるが，これは存在してもただひとつである。なんとならば，$a < a'$ なら，じゅうぶん大きな K について

$$a + \frac{1}{K} < a' - \frac{1}{K}$$

となるから，a, a' どちらも極限となるということはない。

5.17　有界単調列の収束

数列 $(a_n)_n$ が上に有界で，かつ単調非減少，すなわち，

$$\forall n [a_n \leq a_{n+1}]$$

ならば，a_n が $a = \sup\{a_n | n \in \mathbb{N}\}$ に収束することは容易に確かめられる。

5.18　コーシーの判定条件

数列 $(a_n)_n$ が収束するためには，これが次の意味でコーシー列ないし基本列であることが必要充分である：

$$\forall K \in \mathbb{N} \exists N \in \mathbb{N} \forall m, n \in \mathbb{N} [m, n \geq N \Rightarrow |a_m - a_n| \leq \frac{1}{K}].$$

証明：　$a_n \to a$ と仮定し，K が与えられたとする。ある N があって，$n \geq N$ ならば，$|a_n - a| \leq \frac{1}{2K}$ となる。すると，$m, n \geq N$ にたいして，

$$\begin{aligned} |a_m - a_n| &= |(a_m - a) + (a - a_n)| \\ &\leq |a_m - a| + |a - a_n| \\ &\leq \frac{1}{2K} + \frac{1}{2K} = \frac{1}{K} \end{aligned}$$

となる。

逆に $(a_n)_n$ がコーシー列であるとしよう。すると，これはあきらかに有界であるから，

$$A_n = \inf\{a_m | m \geq n\}$$

がきまり，$(A_n)_n$ も有界であり，しかも単調非減少であるので，上限 a に収束する。$a_n \to a$ を示そう。任意の K にたいして，N をじゅうぶん大きくとると，

$$n \geq N \Rightarrow a - \frac{1}{K} \leq A_n \leq a$$

となる。一方，必要なら N を大きくとりなおすと，

$$m, n \geq N \Rightarrow |a_m - a_n| \leq \frac{1}{K}$$

となる。このとき，

$$N \leq n \leq m \Rightarrow a_n - \frac{1}{K} \leq a_m \leq a_n + \frac{1}{K}$$

となり，

$$N \leq n \Rightarrow a_n - \frac{1}{K} \leq A_n \leq a_n + \frac{1}{K}$$

がなりたつ。すると，$n \geq N$ にたいして

$$a - \frac{2}{K} \leq A_n - \frac{1}{K} \leq a_n \leq A_n + \frac{1}{K} \leq a + \frac{1}{K}$$

となる。QED

5.19　加法の連続性

$a_n \to a, b_n \to b$ ならば，$a_n + b_n \to a + b$ である。
証明：

$$|(a_n + b_n) - (a + b)| \leq |a_n - a| + |b_n - b|$$

よりあきらか。QED

5.20　有理数近似

実数 x にたいして，有理数数列 $(r_n)_n$ を適当にとると，$r_n \to x$ となる。
証明：各 $n \in \mathbb{N}$ にたいして，

$$x - \frac{1}{n} < r_n < x + \frac{1}{n}$$

となる $r_n \in \mathbb{Q}$ は存在する。QED

5.21　乗法の定義

$\mathbb{R}$ 上の乗法 g を次のように定義する：$(r_n)_n, (s_n)_n$ が x, y をそれぞれ近似する有理数数列のとき，$(r_n s_n)_n$ がコーシー列となることは，

$$|r_m s_m - r_n s_n| \leq |r_m - r_n||s_m| + |s_m - s_n||r_n|$$

に注意すれば容易にわかる。したがって，それは極限をもつので，その極限を $g(x, y)$ と定義する。じっさい，この極限は近似列のとりかたに依存しないことも容易に確認できる。これがまた，$\mathbb{Q}$ 上の乗法の拡張であることもわかるので，$g(x, y)$ を xy と記す。

5.22　乗法の性質その他

加法と乗法をこのように定義すれば，$\mathbb{R}$ が体となることは，近似列からの極限移行によって，容易に証明できる。また，乗法の連続性，すなわち，$a_n \to a, b_n \to b$ ならば $a_n b_n \to ab$ となることも容易に証明できる。さらに順序の連続性も確かめられる。また，順序が加法，乗法と両立することも，極限移行により，確認できよう。

5.23　実数体の本質的一意性

かくして，$\mathbb{R}$ は演算と両立する全順序を備えた体である。

一方，F が演算と両立する全順序を備えた体であるとし，さらに

（１）$\mathbb{Q} \subset F$ であって，F の順序と演算は $\mathbb{Q}$ のそれの拡張であり，

（２）$x, y \in F$ にたいして $x < y$ ならば $x < r < y$ となる $r \in \mathbb{Q}$ が存在し（F における $\mathbb{Q}$ の稠密性），

（３）F は連続の公理をみたす

ならば，F においても 5.15 以下の議論は平行して妥当する。（$\mathbb{Q}$ の稠密性と連続の公理のみから上限と下限の存在を導く証明については，後の 6.8 をみられたい。）そして，写像 $\Phi : \mathbb{R} \to F$ を次のように定義すると，これは $\mathbb{R}$ から F への順序体同型となる：$x \in \mathbb{Q}$ については，$\Phi(x) = x$ とし，$x \notin \mathbb{Q}$ にたいしては，x に収束する有理数数列をとって，それがコーシー列であることを用い，その F での極限を以って $\Phi(x)$ と定義する。これは近似列のとりかたに依存しない。性質（２）により，この写像 Φ は F の上への写像である。

この意味で，有理数体の実数体への拡張は本質的に一意的である。次の章で実数体の別の構成法を紹介するが，結果はむろん，ここで構成した実数体と同型である。

5.24　$\sqrt{2}$ の存在

念のため，方程式 $x^2 = 2$ の解 $\sqrt{2}$ の存在を証明しておこう。

いま，$A := \{x \in \mathbb{R} | x \leq 0 \text{ あるいは } x^2 < 2\}$ は $x \in A \Rightarrow x \leq 2$ をみたすから，上に有界である。そこで，$a := \sup A$ を考える。むろん，$1 \leq a \leq 2$ である。

$a^2 = 2$ を示そう。A 内の数列 $(x_n)_n$ で a に収束するものをとってくる。$x_n^2 < 2$ だから，乗法の連続性により，$a^2 \leq 2$ である。いま，$a^2 < 2$ と仮定する。$a^2 + e = 2, 0 < e \leq 1$ としよう。$t = e/6$ のとき，

$$(a+t)^2 = a^2 + 2at + t^2 \leq 2 - e + 5t = 2 - \frac{e}{6} < 2$$

である。すると，$a + t \in A$ となって，上限の定義に反する。ゆえに $a^2 = 2$ である。

- じつは，

$$a = \{p \in \mathbb{Q} | p \leq 0 \text{ あるいは } p^2 < 2\}$$

がなりたつ。これを確かめておこう。

右辺

$$\alpha = \{p \in \mathbb{Q} | p \leq 0 \text{ あるいは } p^2 < 2\}$$

は実数である。じっさい，$p < p_1 \in \alpha$ とすると，$p \leq 0$ ならば $p \in \alpha$ だし，$0 < p < p_1$ とすると，$p^2 < p_1^2 < 2$ より $p \in \alpha$ となる。また，$\forall p \in \alpha[p \leq q]$ ならば，$q \notin \alpha$ である。なんとならば，もし $\forall p \in \alpha[p \leq q]$ で $q \in \alpha$ だったとすると，$1 \leq q < 2$ であり，$q^2 < 2$ より $q^2 = 2 - e, 0 < e \leq 1$ である。すると，$t = e/6$ について，

$$(q+t)^2 = q^2 + 2tq + t^2 \leq 2 - e + 5t = 2 - \frac{e}{6} < 2$$

がなりたつから，$q + t \in \alpha$ となり，$\forall p \in \alpha[p \leq q]$ に反する。以上のことから，α は実数である。

$\alpha \subset A$ であるから，$\alpha \leq a = \sup A$ である。もし $\alpha < a$ ならば $\alpha < p < a$ となる $p \in \mathbb{Q}$ があり，$p \notin \alpha$ で，$p > 1$ であるから，$p^2 \geq 2$ である。すると，$2 \leq p^2 < a^2$ となり，$a^2 = 2$ と矛盾する。ゆえに $\alpha = a$ である。

[注]： ある哲学者は次のように書いている：

> デデキントの議論を導く発想法を調べてみると，そこにはすでにひとつの問題点が存していたことがわかる。デデキントの切断には，直線上の全ての点を二組に分け，第一組のどんな点も第二組のどんな点よりも左にあるようにするとき，こうした組み分けを引き起こす点は一つ，そしてただ一つだけ存在するという考えが前提されている。ところがこの種の組み分けについては，ただそれが「何らかの仕方で」可能だというだけで，それの可否については全く検討されていない。直線上の「すべての」点，すなわち「すべての」有理点を現実に算えあげることに難点があるばかりでなく，果たして切断に対応する点，無理点が存在するかどうかはあらかじめ決定できない問題であろう。「すべての」有理点を算えあげたのであれば，切断に対応する点が有理点でない，という消極的な予想が立つが，それが果たして無理点であるかどうかは未定のことであるし，またそこに何らかの点が存在するかどうかも実は未定だといわなければならない。それにもかかわらず，とにかくそれを存在するものとして前提し，証明にとりかか

> るのがデデキントのやり方なのである。もちろんデデキントは，切断を定義することによってはじめて無理数を創造するのであるから，形式的には何ら無理数の概念を前提しているわけではないが，しかし実質的には，すでに無理数（無理点）の存在を前提としているとしなければならないのである。そうでなければ，事実上，有理数全体の上述のような組み分けといった発想そのものが不可能であろう。ここに，一つの予断がある。

これはデーデキントの仕事にたいする全く酷い誹謗中傷である。

デーデキントの議論は，この哲学者が下司のかんぐりをたくましくしているように，無理数を構成するために予め無理数の存在を仮定するというような，誤った循環論法をまったく含んでいないし，有理数体の切断を考えるときに,「すべての有理数を算えあげて，どちらの組に属するかふりわける」というような，およそ不可能なことが要求されているわけではない。たとえば，

$$\begin{aligned} A &:= \{r \in \mathbb{Q} | r \leq 0 \text{ あるいは } r^2 < 2\} \\ B &:= \{r \in \mathbb{Q} | r > 0 \text{ かつ } r^2 \geq 2\} \end{aligned}$$

とすれば，(A, B) は切断であり，無理数 $\sqrt{2}$ はこの切断 (A, B) に他ならないが，A に属するすべての有理数を算えあげるというようなことは不可能であるし，必要でもない。しかし，具体的な有理数がひとつ与えれたとき，A に属するか B に属するか振り分けるには単に分母，分子の 2 乗を計算して一方の 2 倍と他方を比較するだけだから，確定した有限の操作で可能である。誰が「存在するかどうか未定なものを，とにかく前提して証明にとりかかる」というような食言をしているというのか。この哲学者の妄想である。

それでは，なぜこのような妄想，誹謗中傷が出てくるのであろうか。それは，デーデキントが本論に入る前に，人々が予めもっている直線の直観を利用して切断という概念をどのように思いついたかという楽屋話を親切で説明しているためである。本論はそういう直観に全く依存しないのであるが，この哲学者は本論の数学が理解できないので，その親切のための説明だけをひねくりまわして，デーデキントは「実質的にはすでに無理数の存在を前提にして議論している」という妄想を組み立てたのである。しかし，そもそも幾何学的直観に訴えるようなやりかたで解析学の基礎を導入するのでは学問的なやりかたとはいえず，純粋に算術的

で全く厳密な論理によって基礎を確立しようというのが，デーデキントのそもそもの動機であった。このような哲学者の妄想は，まさしく「燕雀いずくんぞ鴻鵠の志を知らんや」である。

6　実数体のもうひとつの構成法

この章では，ふたたび有理数体まで構成した時点にもどって，実数体を構成するもうひとつの方法を紹介する。これはカントールがデーデキントと同年（1872 年）に公表した方法である。

この章で構成する実数体を前章で構成したものと区別するため F と表示するが，もちろん前章で構成したと同型なので，$\mathbb{R}$ と記してもよいわけである。

6.1　零列

$\mathbb{Q}$ 内の有理数数列 $(a_n)_n$ が零列であるとは，次の条件をみたすことである：

$$\forall K \in \mathbb{N} \exists N \in \mathbb{N} \forall n \in \mathbb{N} [n \geq N \Rightarrow |a_n| \leq \frac{1}{K}]$$

このことを $a_n \to 0 (n \to \infty)$ と記す。（絶対値 $|\cdot|$ の定義と基本的な性質はくりかえさない。）

6.2　縮小区間列

有理数区間 $I_n = [a_n, a'_n] (:= \{r \in \mathbb{Q} | a_n \leq r \leq a'_n\})$ の列 $(I_n)_n$ は次の条件をみたすとき，縮小区間列とよぶ：

$$a_n \leq a_{n+1} \leq a'_{n+1} \leq a'_n, \qquad a'_n - a_n \to 0 (n \to \infty)$$

縮小区間列全体のなす集合を E とする。

E のなかに次の関係 R を定義する：$I_n = [a_n, a'_n], J_n = [b_n, b'_n]$ のとき，

$$R((I_n)_n, (J_n)_n) \Leftrightarrow \forall n [a_n \leq b'_n, b_n \leq a'_n]$$

このとき，R は E 上の同値関係となる。

じっさい，

$$R((I_n)_n, (I_n)_n)$$

および

$$R((I_n)_n,(J_n)_n) \quad \Leftrightarrow \quad R((J_n)_n,(I_n)_n)$$

はあきらかである。いま，

$$I_n=[a_n,a'_n], \quad J_n=[b_n,b'_n], \quad K_n=[c_n,c'_n]$$

として，$R((I_n)_n,(J_n)_n)$ かつ $R((J_n)_n,(K_n)_n)$ であると仮定する。このとき，$R((I_n)_n,(K_n)_n)$ であること，すなわち，

$$\forall n: \quad a_n \le c'_n, \quad c_n \le a'_n$$

を示そう。もしそうでないとして，かりに，$a_N > c'_N$ となる N があると仮定しよう。すると，

$$\forall n \ge N : a_n - c'_n \ge a_N - c'_N > 0$$

であり，一方，仮定から

$$\forall n: \quad b'_n \ge a_n, \quad b_n \le c'_n$$

であるから，

$$\forall n \ge N : b'_n - b_n \ge a_n - c'_n \ge a_N - c'_N > 0$$

となって，$b'_n - b_n \to 0 (n \to \infty)$ に反する。したがって，$\forall n[a_n \le c'_n]$ である。同様に $\forall n[c_n \le a'_n]$ もわかる。

そこで，E をこの同値関係 R で割って得られる商集合 E/R を F とし，その要素を実数とよぶ。

$r \in \mathbb{Q}$ については，$I_n = [r,r]$ は縮小区間列であるから，その同値類 $R[(I_n)_n]$ を r と同一視して，$\mathbb{Q} \subset F$ とみなす。

- なお，$(I_n)_n,(J_n)_n \in E, I_n=[a_n,a'_n], J_n=[b_n,b'_n]$ について，$R((I_n)_n,(J_n)_n)$ となるには $a_n - b_n \to 0 (n \to \infty)$ が必要充分であることが容易に確かめられる。受講者自ら証明を書き下されたい。

6.3 順序の定義

$x,y \in F$ とする。

$$(I_n)_n \in x, \quad (J_n)_n \in y, \quad I_n=[a_n,a'_n], \quad J_n=[b_n,b'_n]$$

のとき，

$$\forall n[a_n \leq b'_n]$$

であることを $x \leq y$ とする。

これが定義となっているためには，

$$(K_n)_n \in x, \quad (L_n)_n \in y, \quad K_n = [c_n, c'_n], \quad L_n = [d_n, d'_n]$$

にたいして

$$\forall n[a_n \leq b'_n] \quad \Rightarrow \quad \forall n[c_n \leq d'_n]$$

を示さねばならない。

もし $c_N > d'_N$ となったとすると，

$$\forall n \geq N \quad : \quad c_n - d'_n \geq c_N - d'_N > 0$$

である。一方，$R((I_n)_n, (K_n)_n)$ と $R((J_n)_n, (L_n)_n)$ とより，

$$\forall n \quad : \quad c_n \leq a'_n, \quad b_n \leq d'_n$$

だから，

$$\forall n \geq N : a'_n - b_n \geq c_n - d'_n \geq c_N - d'_N \geq \frac{1}{K} > 0$$

となる。しかし，$a'_n - a_n \to 0, b'_n - b_n \to 0 (n \to \infty)$ より，じゅうぶん大きな n について，

$$a_n \geq a'_n - \frac{1}{4K}, \quad b'_n \leq b_n + \frac{1}{4K}$$

としてよい。すると，必要なら N を大きくとりなおして，

$$\forall n \geq N \quad : \quad a_n - b'_n \geq -\frac{1}{4K} - \frac{1}{4K} + \frac{1}{K} = \frac{1}{2K}$$

となり，仮定に反する。ゆえに，$\forall n[c_n \leq d'_n]$ である。これで，定義の正当性が確立する。

この関係 $\leq$ が $\mathbb{Q}$ の順序の拡張になっていることはあきらかである。

6.4　順序の性質

1）$[x \leq y$ かつ $y \leq x] \Leftrightarrow x = y$
2）$[x \leq y$ かつ $y \leq z] \Rightarrow x \leq z$
3）$x \leq y$ か $y \leq x$ かのいずれかはなりたつ
証明： 1）は定義からあきらかである。
2）を証明しよう。

$$(I_n)_n \in x, (J_n)_n \in y, (K_n)_n \in z, I_n = [a_n, a'_n], J_n = [b_n, b'_n], K_n = [c_n, c'_n]$$

とする。

$$\forall n \quad : \quad a_n \leq b'_n, \quad b_n \leq c'_n$$

から $\forall n[a_n \leq c'_n]$ を導かねばならない。もし，$a_N > c'_N$ となったとすると，

$$\forall n \geq N : a_n - c'_n \geq a_N - c'_N \geq \frac{1}{K} > 0$$

となる。すると，

$$\forall n \geq N : b'_n - b_n \geq a_n - c'_n \geq \frac{1}{K}$$

となり，$b'_n - b_n \to 0 (n \to \infty)$ に反する。
次に 3）を証明しよう。

$$(I_n)_n \in x, \quad (J_n)_n \in y, \quad I_n = [a_n, a'_n], \quad J_n = [b_n, b'_n]$$

とする。$x \leq y$ でないならば，$b'_N < a_N$ となる N が存在する。すると，$n \geq N$ にたいして，

$$b_n \leq b'_n \leq b'_N < a_N \leq a'_N \leq a'_n$$

となる。$n < N$ については，

$$b_n \leq b_N \leq b'_N < a_N \leq a'_N \leq a'_n$$

である。したがって $\forall n[b_n < a'_n]$ となり，$y \leq x$ が従う。QED

6.5

$x \in F$ にたいして，$(I_n)_n \in x, I_n = [a_n, a'_n]$ とすると，$\forall n[a_n \leq x \leq a'_n]$ である。

6.6 $\mathbb{Q}$ の稠密性

$x, y \in F, x < y$ ならば，$x < r < y$ となる $r \in \mathbb{Q}$ が存在する。
証明：

$$(I_n)_n \in x, \quad (J_n)_n \in y, \quad I_n = [a_n, a'_n], \quad J_n = [b_n, b'_n]$$

とする。$x \leq y$ であるから，$\forall n[a_n \leq b'_n]$ である。$x \neq y$ であるから，$b_N > a'_N$ となる N が存在する。このとき，$a'_N < r < b_N$ となる $r \in \mathbb{Q}$ をとる（たとえば，$r = \frac{1}{2}(a'_N + b_N)$）。すると，あきらかに $x \leq r \leq y$ であり，$x \neq r, y \neq r$ となって，$x < r < y$ である。QED

6.7 連続の公理

$A, B \subset F, A \neq \emptyset, B \neq \emptyset, A \cup B = F$ で，

$$a \in A \quad b \in B \quad \Rightarrow \quad a < b$$

ならば，

$$a \in A \Rightarrow a \leq c, \qquad b \in B \Rightarrow c \leq b$$

となる $c \in F$ が存在する。
証明： $c_0 = \max\{n \in \mathbb{Z} | n \in A\}$ とする。$c_0 \in A, c_0 + 1 \in B$ である。縮小区間列 $K_n = [c_n, c'_n]$ を次のようにつくることができる：

$$c'_n - c_n = \frac{1}{2^n}, \quad c_n \in A, \quad c'_n \in B$$

そこで，$c = R[(K_n)_n]$ とおく。$a \in A$ であるとし，$(I_n)_n \in a, I_n = [a_n, a'_n]$ としよう。すると，$\forall n[a_n \in A]$ である。じっさい，もし $a_N \notin A$ ならば，$a_N \in B$ となり，$\forall n \geq N[a_N \leq a_n \leq a'_n]$ により，$\forall n \geq N[a_n \in B]$ となる。すると，$a \in A$ より，$\forall n \geq N[a < a_N \leq a_n]$ となり，6.5 より矛盾である。したがって，$\forall n[a_n \in A]$ であり，$\forall n[a_n < c'_n]$ である。すなわち，$a \leq c$ がなりたつ。$b \in B \Rightarrow c \leq b$ も同様に証明できる。QED

6.8 上限と下限の存在

いま F の部分集合 A が空でなく，上に有界であるとしよう。このとき，

$$C = \{\xi \in F | \exists x \in A[\xi < x]\}$$

とおく。A は空でないから，C は空でない。C の補集合を D とする。すなわち，

$$D = \{\eta \in F | \forall x \in A[x \leq \eta]\}$$

である。A は上に有界であるから，D は空でなく，$F = C \cup D$ であり，

$$\xi \in C, \eta \in D \quad \Rightarrow \quad \xi < \eta$$

はあきらかである。ゆえに連続の公理から

$$\xi \in C \Rightarrow \xi \leq c, \qquad \eta \in D \Rightarrow c \leq \eta$$

となる $c \in F$ が存在する。c が A の上限であることを確かめるには，$c \in D$ を示せばじゅうぶんである。もし，$c \notin D$ ならば，$c \in C$ であり，$c < x_0$ となる $x_0 \in A$ が存在する。$c < \xi_0 < x_0$ となる ξ_0 をとると，定義から $\xi_0 \in C$ であり，$\xi_0 \leq c$ でなければならない。これは $c < \xi_0$ と矛盾する。ゆえに c は A の上限である。

下限についても，議論はまったく同様である。

6.9 加法の定義

$x, y \in F$ にたいして，

$$(I_n)_n \in x, \quad (J_n)_n \in y, \quad I_n = [a_n, a'_n], \quad J_n = [b_n, b'_n]$$

とする。このとき，$K_n = [a_n + b_n, a'_n + b'_n]$ はまた縮小区間列であり，$R[(K_n)_n]$ は x, y の代表元 $(I_n)_n, (J_n)_n$ のとりかたに依存しない。そこで，$R[(K_n)_n]$ を $x+y$ と定義する。これは $\mathbb{Q}$ 上の加法の拡張になっており，この加法は，F を可換群とし，順序 $\leq$ と両立する。

6.10

以下，F に乗法を定義したり，F が全順序体であることを確認したりなどの議論は前章のくりかえしになるから，受講者に任そう。

7　複素数

方程式 $x^2+1=0$ は $\mathbb{R}$ のなかに解をもたない。このような方程式が解をもつように実数体を複素数体に拡張する。この拡張はふたたび純粋に代数的に遂行される。

しばしば次のようにして複素数が導入されることがある：

> 実数の 2 乗は 0 または正の数で，負の数になることはないから，2 次方程式 $x^2=-1$ は，実数の範囲で解をもたない。そこで，このような方程式も解をもつように，数の範囲を広げることを考えよう。2 乗すると -1 になる新しい数を 1 つ考えて，これを文字 i で表し，虚数単位という。すなわち，$i^2=-1$ とする。更に，$3+2i$ のように，2 つの実数 a,b を用いて $a+bi$ の形に表される数を考え，これを複素数という。

しかし，これで数の拡張ができているとはいえない。なぜならば，もしこの論理が正当なら，次の論理も認めざるをえないだろう：

> 実数に 0 を乗じると 0 であり，正の数になることはないから，方程式 $0x=1$ は，実数の範囲で解をもたない。そこで，このような方程式も解をもつように，数の範囲を広げることを考えよう。0 を乗じると 1 になる新しい数を 1 つ考えて，これを文字 j で表し，無限大という。すなわち，$0j=1$ とする。

ところが，これで数の拡張ができているとすると，

$$2=2\cdot 1=2\cdot(0\cdot j)=(2\cdot 0)\cdot j=0j=1$$

となって，$2=1$ という矛盾が証明できてしまう。だから，さきのような複素数の導入の論理はそのままでは承認するわけにはいかない。複素数の導入は別の論理で行う必要がある。以下，その一つを提示する。

積集合 $\mathbb{R}\times\mathbb{R}$ を $\mathbb{C}$ とし，このなかに次のように加法と乗法を定義する：

$$\begin{aligned}(a,b)+(c,d) &= (a+b,c+d)\\ (a,b)(c,d) &= (ac-bd,bc+ad)\end{aligned}$$

$a\in\mathbb{R}$ は $(a,0)$ と同一視して，$\mathbb{R}\subset\mathbb{C}$ とみなす。すると，上で定義した加法，乗法は $\mathbb{R}$ 上の加法，乗法の拡張になっていることはあきらかである。

$\mathbb{C}$ の要素を複素数とよぶ。

これらの演算によって $\mathbb{C}$ は体となる。すなわち，以下がなりたつ。(z, w などは任意の複素数を表す。)

1) $z + 0 = z$

2) $z + w = w + z$

3) $z_1 + (z_2 + z_3) = (z_1 + z_2) + z_3$

4) $\alpha = (a, b), \beta = (c, d)$ にたいして，$z = (c - a, d - b)$ は $\alpha + z = \beta$ のただ一つの解である

5) $1z = 0 \qquad 0z = 0$

6) $zw = wz$

7) $z_1(z_2 z_3) = (z_1 z_2)z_3$

8) $\alpha = (a, b), \beta = (c, d)$ にたいして，$\alpha \neq 0$ ならば，

$$z = \left(\frac{ac + bd}{a^2 + b^2}, \frac{ad - bc}{a^2 + b^2}\right)$$

は $\alpha z = \beta$ のただひとつの解である

9) $z(w_1 + w_2) = zw_1 + zw_2$

以上は定義に基づいて容易に確かめられる。

ただし，順序はふつう定義しない。

あきらかに，$z = (0, 1), (0, -1)$ は方程式 $z^2 + 1 = 0$ をみたす。

いっぱんに複素数を係数とする代数方程式はかならず複素数体のなかに解をもつ（代数学の基本定理）のであるが，そのことの手軽で純粋に代数的な証明は知られていないようであり，その証明には複素函数の解析を利用するのがふつうであるので，この講習の範囲外となる。

****

これで講習を終わります。ご清聴ありがとうございました。