1　条件命題と真理集合

1.1　条件命題と真理集合

1.1.1　命題，条件命題，真理集合

判断を述べる文を**命題**（proposition）という。文には，等式や不等式のように数学記号で書かれたものも含まれる。

命題には，変数を含み，その変数に値を代入することができるものがある。そのような命題を特に**条件命題**，**述語**（predicate）などという。

例　「2x+3=4」,「$(x+1)^2 = x^2+2x+1$」,「n は素数である」

上の例の x や n のように自由に値を代入することのできる変数を**自由変数**という。

「$\int_1^a (x+2)dx = 4$」の x のように命題の内容を記述するために用いられて自由に値を代入することのできない変数を**束縛変数**という。この文が含む自由変数は a である。

問 1 次の文が含む変数のうち，自由変数はどれか。
(1) 2 次方程式 $ax^2+bx+c=0$ は実数解を持つ。
(2) $\displaystyle\sum_{k=1}^{n}(2k+1) = 20$

自由変数 x を含む条件命題を $P(x)$，$Q(x)$ などの記号で表す。このとき，x に a を代入してできる命題を $P(a)$ で表す。

自由変数 x,y を含む条件命題を $P(x,y)$ のように表す。このとき，x に a を代入してできる命題 $P(a,y)$ は y のみを自由変数として含む条件命題である。

自由変数を含む命題を**開いた文**と呼ぶ。それに対し，自由変数を含まない命題を**閉じた文**と呼ぶ。すべての自由変数に値を代入して得られる命題は閉じた文になる。閉じた文は，真偽を考える対象となる。

注意 2 閉じた文のみを**命題**と呼び，条件命題を命題に含めない流儀もある。高校の教科書はその流儀に従っていることが多い。この流儀に従うとき，条件命題を「命題関数」と呼ぶことがある。

注意 3 「2+3」とか,「$2x+3$」のように数学文の構成要素ではあるけれどもその一部に過ぎないものは命題ではない。命題は，数学文の文法上の‘文’である。少し詳しく述べると，自由変数として用いる文字の使用を許して，数学における文法に従って‘文’として構成されたものが命題である。等式や不等式もここでいう‘文’に含まれる。

条件命題 $P(x)$ に対し，集合 $\{x|P(x)\}$ をその**真理集合**という。真理集合の要素全体を条件命題の**外延**という。

例 4 条件命題「$x^2-3x+2=0$」の真理集合は $\{1,2\}$ で，外延は 1 と 2 である。

上の例のように，条件命題が方程式（あるいは不等式）であるとき，その真理集合は**解集合**と呼ばれ，外延は解のすべてのことである。

数学では，コンマで区切って並列的に書かれた式は同時に成り立つものとして扱うので，不等式 $(x-2)(x-3)<0$ の解集合は $\{x|x<2,3<x\}$ ではない。$\{x|x<2,3<x\}$ は $\{x|x<2\}\cap\{x|x>3\}(=\varnothing)$ を意味する。

問 5 方程式 $(x-2)(x-3)=0$ の解は $x=2,3$ なので，解集合は $x=\{2,3\}$。どこがおかしいか。また，解集合を $\{x|x=2,3\}$ と書いてよいか。

複数の自由変数を含む条件命題に対しても，たとえば，$P(x,y)$ に対して $\{(x,y)|P(x,y)\}$ をその真理集合という。

条件命題に含まれる自由変数の変域を**対象領域**という。条件命題 $P(x)$ に含まれる自由変数 x の対象領域が集合 U であるとき，$P(x)$ の真理集合を $\{x\in U|P(x)\}$ のように書く。また，真理集合からみたとき，対象領域 U を**全体集合**という。

1.1.2　数の集合

自然数全体の集合を $\mathbb{N}$，整数全体の集合を $\mathbb{Z}$，有理数全体の集合を $\mathbb{Q}$，実数全体の集合を $\mathbb{R}$，複素数全体の集合を $\mathbb{C}$ で表す。$\mathbb{N}$ は Natural number，$\mathbb{Z}$ は Zahlen（ドイツ語で数，整数は英語で Integer であるが I だと見ずらい），$\mathbb{Q}$ は Quotient（商を意味する英語，有理数は英語で Rational number だけれど R だと実数と被る），$\mathbb{R}$ は Real Number に由来する。

そして，正の整数全体を $\mathbb{Z}^+$，正の実数全体を $\mathbb{R}^+$ で表す。すなわち，

$\mathbb{Z}^+=\{1,2,3,\ldots\}$,　　$\mathbb{R}^+=\{x\in\mathbb{R}|x>0\}$

自然数にはモノの個数という意味があるので，自然数は 0 から始まるとしたほうが便利である。そのため，集合論では，$0,1,2,3,\ldots$ を**自然数**と呼ぶ。

すなわち，

$\mathbb{N}=\{0,1,2,3,\ldots\}$

そして，

$0=\{\}$, $1=\{0\}$, $2=\{0,1\}$, $\cdots\cdots$, $n=\{0,1,2,\ldots,n-1\}$

と考える。そうすると，自然数 n の要素の個数は n となる。

補足　$0,1,2,3,\ldots$ は，**非負整数**，**全数**などと呼ばれることがある。全数は，英語の“whole number”の訳。ただし，日本語の“全数”は，“全数調査”など別の意味で使われることが多いので，非負整数の意味で“全数”を用いると紛らわしい。

例 6 (1) 対象領域が実数全体であるとき，方程式 $x^2+1=0$ の真理集合 $\{x\in\mathbb{R}|x^2+1=0\}$ は $\varnothing$（空集合）である。
(2) 対象領域が複素数全体であるとき，方程式 $x^2+1=0$ の真理集合 $\{x\in\mathbb{C}|x^2+1=0\}$ は $\{i,-i\}$（i は虚数単位) である。

1.1.3　必要条件，十分条件，同値

$P(x)$，$Q(x)$ を条件命題とする。

$P(x)$ を満たす x は必ず $Q(x)$ を満たすことを，$P(x) \Rightarrow Q(x)$ と書いて，$P(x)$ は $Q(x)$ であるための**十分条件**である，あるいは，$Q(x)$ は $P(x)$ であるための**必要条件**であるなどという。また，$P(x) \Rightarrow Q(x)$ を順序を入れ替えて $Q(x) \Leftarrow P(x)$ とも書く。

$P(x) \Rightarrow Q(x)$ は，$\{x|P(x)\} \subset \{x|Q(x)\}$ を意味する。

$P(x)$ が $Q(x)$ であるための必要条件でも十分条件でもあるとき，$P(x)$ は $Q(x)$ であるための**必要十分条件**であるといって，$P(x) \Leftrightarrow Q(x)$ と書く。このとき，$P(x)$ と $Q(x)$ は**同値**である，あるいは，$P(x)$ は $Q(x)$ と**同値**であるという。

1.1.4　$P(x) \Rightarrow Q(x)$ の証明

$P(x) \Rightarrow Q(x)$ を証明するためには，対象領域の任意の要素を x として，$P(x)$ を仮定すると $Q(x)$ が成立することを示せばよい。

例題 7 対象領域を $\mathbb{Z}$ とするとき，次を示せ。
(1)　n は偶数 $\Rightarrow n^2$ は偶数
(2)　n は奇数 $\Rightarrow n^2$ は奇数

証明. (1) n を偶数とすると，$n = 2k$ となる整数 k が存在する。
$n^2 = 4k^2$ となり，k^2 は整数なので，n^2 は偶数。
(2) n を奇数とすると，$n = 2k + 1$ となる整数 k が存在する。
$n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ となり，$2k^2 + 2k$ は整数なので，n^2 は奇数 □

1.1.5　転換法

例題 8 対象領域を $\mathbb{Z}$ とするとき，次を示せ。
(1)　n は偶数 $\Leftrightarrow n^2$ は偶数
(2)　n は奇数 $\Leftrightarrow n^2$ は奇数

証明. (1) n^2 は偶数 $\Rightarrow n$ は偶数と　(2) n^2 は奇数 $\Rightarrow n$ は奇数　を示せばよい。
(1)　n^2 は偶数であるとする。
このとき，n が奇数であるとすると，上の例題 (2) より n^2 は奇数となり n^2 が偶数であることに反する。
だから，n は奇数ではない。奇数でない整数は偶数しかないから，n は偶数である。
(2)　n^2 は奇数であるとする。
このとき，n が偶数であるとすると，上の例題 (1) より n^2 は偶数となり n^2 が奇数であることに反する。
だから，n は偶数ではない。偶数でない整数は奇数しかないから，n は奇数である。 □

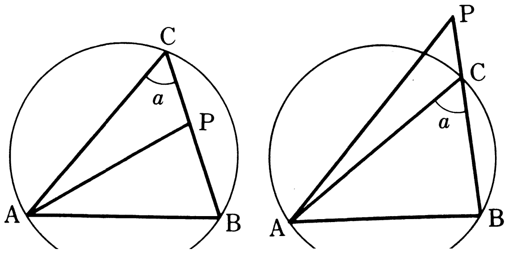
上の証明では，整数は偶数か奇数のいずれかであって，しかも，偶数でも奇数でもある整数はないことが使われている。

一般に，
$P_1(x) \Rightarrow Q_1(x)$
$P_2(x) \Rightarrow Q_2(x)$

が成立しているとき，
ｉ) どの x に対しても，$P_1(x)$ と $P_2(x)$ のうちどちらか少なくとも一方が成立する
ⅱ) どの x に対しても，$Q_1(x)$ と $Q_2(x)$ の双方が成立することはない
であれば，
　$P_1(x) \Leftrightarrow Q_1(x)$
　$P_2(x) \Leftrightarrow Q_2(x)$
がいえる。この証明法は**転換法**と呼ばれる。

練習 9 実数係数の 2 次方程式に対し次のことが知られている。
(1) $b^2 - 4ac > 0 \Rightarrow$2 次方程式 $ax^2 + bx + c = 0$ の解の個数は 2 個
(2) $b^2 - 4ac = 0 \Rightarrow$2 次方程式 $ax^2 + bx + c = 0$ の解の個数は 1 個
(3) $b^2 - 4ac < 0 \Rightarrow$2 次方程式 $ax^2 + bx + c = 0$ の解の個数は 0 個
上の (1)〜(3) から次の $(1)'$〜$(3)'$ を導け。ただし，a, b, c の変域は $\mathbb{R}$ とする。
$(1)'$ $b^2 - 4ac > 0 \Leftrightarrow$2 次方程式 $ax^2 + bx + c = 0$ の解の個数は 2 個
$(2)'$ $b^2 - 4ac = 0 \Leftrightarrow$2 次方程式 $ax^2 + bx + c = 0$ の解の個数は 1 個
$(3)'$ $b^2 - 4ac < 0 \Leftrightarrow$2 次方程式 $ax^2 + bx + c = 0$ の解の個数は 0 個

練習 10 平面上で，円 O が △ABC に外接し，直線 AB に対し点 C と同じ側に点 P があるとき，(1)(2) が成立すれば (3) が導かれることを示せ。ただし，点 P が中心 O，半径 r の円 O の内部（外部）の点であるとは，OP$<r$ (OP$>r$) となることとする。
(1) 点 P が円 O の内部にあるとき，$\angle$APB $>$ $\angle$ACB
(2) 点 P が円 O の外部にあるとき，$\angle$APB $<$ $\angle$ACB
(3) $\angle$APB $=$ $\angle$ACB ならば，点 P は円 O の周上にある。



1.1.6　対偶

　条件命題 $P(x)$ の否定を $\overline{P(x)}$ で表す。$P(x) \Rightarrow Q(x)$ に対して，$\overline{Q(x)} \Rightarrow \overline{P(x)}$ をその**対偶**という。
　$P(x) \Rightarrow Q(x)$ が成立しているとき，$\overline{Q(x)} \Rightarrow \overline{P(x)}$ も成立する。それは次のようにして分かる。
　x が $\overline{Q(x)}$ を満たすとき，$P(x)$ であるとすると $Q(x)$ となり $\overline{Q(x)}$ に反するから，$\overline{P(x)}$ が成立する。
　この証明では，次の 2 つの原理が使われている。ただし，p は命題を表す。
　ｉ) p かつ $\overline{p}$ から矛盾が生じる（矛盾律 ）
　ⅱ) p から矛盾が生じるとき，$\overline{p}$ が成立する

$P(x) \Rightarrow Q(x)$ を証明する代わりに対偶 $\overline{Q(x)} \Rightarrow \overline{P(x)}$ を証明することがある。その根拠は，対偶の対偶は元に戻ること。その際，次の原理が用いられている。

iii) $\overline{\overline{p}} \Leftrightarrow p$ （二重否定の法則)

1.1.7 練習問題

問 11 2 円 $x^2+y^2-2y-24=0, x^2+y^2-8x-6y+20=0$ の交点を求める。

$$x^2+y^2-2y-24=0 \tag{1}$$
$$x^2+y^2-8x-6y+20=0 \tag{2}$$

(1) − (2) より

$$8x+4y=44 \tag{3}$$

(3) を y について解いて，

$$y=11-2x \tag{4}$$

(1) を $x^2+(y-1)^2=25$ と変形し (4) を代入して

$$x^2+(10-2x)^2=25 \tag{5}$$

$x^2-8x+15=0$
$x=3$ または $x=5$

(4) より y を求めて，$(x,y)=(3,5),(5,1)$

この解において，$\left\{\begin{array}{l}(1)\\(2)\end{array}\right. \Leftrightarrow \left\{\begin{array}{l}(1)\\(3)\end{array}\right. \Leftrightarrow \left\{\begin{array}{l}(1)\\(4)\end{array}\right. \Leftrightarrow \left\{\begin{array}{l}(5)\\(4)\end{array}\right.$ であることを示せ。

それによって，$A=\{(x,y)|x^2+y^2-2y-24=0\}$,
$B=\{(x,y)|x^2+y^2-8x-6y+20=0\}$ に対して
$A\cap B=\{(3,5),(5,1)\}$ と結論できる。

$\mathbb{R}^+$ は正の数全体を表す。

練習 12 a,b の変域を $\mathbb{R}$ とするとき，$a>0$ かつ $b>0 \Leftrightarrow a+b>0$ かつ $ab>0$
[ヒント]$ab>0$ のとき，a,b は同符号。

練習 13 a,b の変域を $\mathbb{R}^+\cup\{0\}$ とするとき，$a<b \Leftrightarrow a^2<b^2$
[ヒント] $a^2-b^2=(a-b)(a+b)$

練習 14 a,b の変域を $\mathbb{R}^+\cup\{0\}$ とするとき，$a \leqq b \Leftrightarrow a^2 \leqq b^2$ [ヒント] 対偶

練習 15 x,y の連立方程式

$$\left\{\begin{array}{l}ax+by=1\\cx+dy=1\end{array}\right.$$

が解を持たないとき $ad-bc=0$ であることを示せ。

練習 16 n を整数とする。n^2-1 が 3 の倍数でないならば，n は 3 の倍数である。

1.2　全称命題と存在命題

1.2.1　全称命題

条件命題には真理集合が対象領域と一致するものがある。たとえば,
(1) x の変域を $\mathbb{R}$ とするとき,「$x^2 \geqq 0$」
(2) x の変域を $\mathbb{C}$ とするとき,「$(x+1)^2 = x^2+2x+1$」
それぞれ，真理集合は,
(1) $\{x \in \mathbb{R} | x^2 \geqq 0\} = \mathbb{R}$　　(2)$\{x \in \mathbb{C} | (x+1)^2 = x^2+2x+1\} = \mathbb{C}$
となっている。

$P(x)$ を自由変数 x を含む条件命題とする。すべての x に対して $P(x)$ が成立することを表す命題を $\forall x P(x)$ で表す。

対象領域が U であることを示す必要がある場合は，$\forall x \in U[P(x)]$ のように書く。たとえば,
(1) $\forall x \in \mathbb{R}[x^2 \geqq 0]$　　(2)$\forall x \in \mathbb{C}[(x+1)^2 = x^2+2x+1]$

論理記号 $\forall$ は**全称記号**と呼ばれる。英語の All の頭文字 A を逆さに印刷したのが始まり。

自由変数 x, y を含む条件命題 $P(x, y)$ に対し $\forall x[\forall y P(x, y)]$ を $\forall x \forall y P(x, y)$ と書く。順序を入れ替えた $\forall y \forall x P(x, y)$ と実質的な意味の違いは生じない。

数学における定理や公式の多くは任意の数について成り立つことを主張している。その場合，全称記号を省いて書かれるのが普通。たとえば，正弦の加法定理は，ていねいに書くと　$\forall \alpha \forall \beta\ [\sin(\alpha+\beta) = \sin\alpha\cos\beta + \cos\alpha\sin\beta]$　である。

$\forall x P(x)$ における変数 x に値を代入して新たな命題を作ることはできない。このことを x は**束縛**されているという。そして，束縛された変数のことを**束縛変数**という。

束縛変数は，他の文字に変えても意味は変わらない。すなわち，$P(x)$ が変数 y を含まなければ，$\forall y P(y)$ は $\forall x P(x)$ と同じ内容を表す。

複数の自由変数を含む条件命題のうちの一部の変数のみを束縛して新たな条件命題を作ることができる。

たとえば，4 個の自由変数を含む条件命題「$ax^2+bx+c>0$」のうち x を束縛して作られる「$\forall x \in \mathbb{R}[ax^2+bx+c>0]$」は，$a, b, c$ を自由変数として含む条件命題である。そして，a の変域を正の数全体，b, c の変域を実数全体とすると,

$$\forall x \in \mathbb{R}[ax^2+bx+c>0] \Leftrightarrow b^2-4ac<0$$

例 17 a, b, c の変域を実数全体とするとき，$\forall x \in \mathbb{R}[ax^2+bx+c=0] \Leftrightarrow a=b=c=0$

証明. $\Leftarrow$ は明らか。$\Rightarrow$ を示す。
$\forall x \in \mathbb{R}[ax^2+bx+c=0]$ が成立すると仮定する。
$x=0$ を代入して　　$c=0$
$x=1$ を代入して　　$a+b+c=0$
$x=-1$ を代入して　$a-b+c=0$
よって,　　　　　$a=b=c=0$ □

1.2.2 存在命題

平均値の定理　$a < b$ とする。関数 f が区間 $[a,b]$ で連続，(a,b) で微分可能であるとき，$\dfrac{f(b)-f(a)}{b-a} = f'(t)$ となる t が区間 (a,b) に存在する。

上述の平均値の定理のように，存在を主張する命題が数学には多く現れる。

$P(x)$ を自由変数 x を含む条件命題とする。$P(x)$ を満たす x が存在することを表す命題を $\exists x P(x)$ で表す。対象領域が U であることを示す必要がある場合は，$\exists x \in U[P(x)]$ のように書く。たとえば，

(1) $\exists x \in \mathbb{R}[x^2 \leqq 0]$　　(2)$\exists x \in \mathbb{C}[x^2+1=0]$

論理記号 $\exists$ は**存在記号**と呼ばれる。英語の Exist の頭文字 E を逆さに印刷したのが始まり。

$\exists x P(x)$ は，日本語で「ある x に対して $P(x)$」と読まれることがある。

$\exists x P(x)$ は，$P(x)$ の真理集合が空でないこと，すなわち，$\{x|P(x)\} \neq \varnothing$ を意味する。

$\exists x P(x)$ における変数 x に値を代入して新たな命題を作ることはできない。このことを x は**束縛**されているという。そして，束縛された変数のことを**束縛変数**という。

数学では多くの概念（述語）が存在命題の形で定義される。

$\overset{\text{def}}{\Longleftrightarrow}$ は左辺を右辺で定義することを表す。

例 18 n は偶数 $\overset{\text{def}}{\Longleftrightarrow}$ $\exists k \in \mathbb{Z}[n = 2k]$

a は b の約数 $\overset{\text{def}}{\Longleftrightarrow}$ $\exists k \in \mathbb{Z}[ak = b]$

例 19 P,A,B を平面上の点を表す変数とする。
点 P が直線 AB 上にある $\Leftrightarrow \exists k \in \mathbb{R}[\overrightarrow{\mathrm{AP}} = k\overrightarrow{\mathrm{AB}}]$

1.3 $\forall x \exists y P(x,y)$ と $\exists y \forall x P(x,y)$

1.3.1 悪文

(a) 任意の a に対し $ae = a$ となる e が存在する。

(b) 任意の a に対し $ax = e$ となる x が存在する。

(a),(b) どちらも述べたい内容をあらかじめ知っている人にはいいたいことを伝えることができるけれど，そうでなければ正しく意味を伝えることができない悪文である。

(a) は，乗法に関する単位元 $e = 1$ の存在を述べ，(b) は a の逆元 $x = a^{-1}$ の存在を主張している。日本語としては，どちらも　　　　任意の □ に対し △ となる ◇ が存在するという同じ構造をしているが，異なる読み方（解釈）が必要になる。

(a) は「(任意の a に対し $ae = a$）となる e が存在する」の意味で，
「任意の a に対し（$ae = a$ となる e が存在する)」と解釈すると誤読である。
一方，(b) を「(任意の a に対し $ax = e$）となる x が存在する」と解釈すると $e = 0, x = 0$ を想起させる文になるが，それは誤読で,「任意の a に対し（$ax = e$ となる x が存在する)」と読むのが正しい。

論理記号を用いて書くと (a)，(b) は，それぞれ，$\exists e[\forall a[ae = a]]$，$\forall a[\exists x[ax = e]]$ となる。そう書けば，それぞれ,「$\forall a[ae = a]$ となる e がある」,「任意の a に対し $\exists x[ax = e]$」を意味するから誤解は生じない。

(a),(b) を，英語の語順に合わせて，次のように書くこともある。日本語としては落ち着きが悪いが，注意深く読めば誤解を生じることがない。
(a)$'$ ある e が存在して，任意の a に対し $ae = a$ となる。
(b)$'$ 任意の a に対し，ある x が存在して $ax = e$ となる。

次の練習問題は異なる解釈で異なる答が出る。どう解釈するのが出題者の意図か，また，それを誤解なく伝えるにはどう書くのがよいかも考えよ。

練習 20 「すべての自然数 x に対して $x < y$ を満たす自然数 y が存在する」は真か偽か。

練習 21 $x > 0, y > 0$ を満たすすべての x, y について $x + ay \geqq 0$ が成り立つような a の値の範囲を求めよ。

練習 22 2 項演算 $\oplus$ を $a \oplus b = a + b - ab$ と定める。$(x \oplus e) = x$ となるような e の値を求めよ。

1.3.2 $\forall x \exists y P(x, y)$ と $\exists y \forall x P(x, y)$

$\forall x[\exists y P(x, y)]$，$\exists y[\forall x P(x, y)]$ は [　] を省いて $\forall x \exists y P(x, y)$，$\exists y \forall x P(x, y)$ のように書かれることが多い。けれども，$\forall x$ と $\exists y$ の順番を入れ替えると意味が変わることに注意。

2 論理と推論

2.1 命題論理

2.1.1 命題論理の記号

「ならば」,「かつ」,「または」,「でない」で表現可能な論理のことを**命題論理**という。命題論理では，以下の記号を用いて命題から新たな命題を作る。命題を p, q などの文字で表す。

$p \to q$	p ならば q
$p \wedge q$	p かつ q
$p \vee q$	p または q
$\overline{p}$	p でない
$\curlywedge$	矛盾

p の否定を $\neg p$ で表すこともある。矛盾は $\perp$ と書かれることもある。

結合の優先順位は，$\to$ より $\wedge, \vee$ が優先する。たとえば，$p \to q \wedge r$ は $p \to (q \wedge r)$ を意味する。
$\wedge$ と $\vee$ の間の優先順位は定めない。だから，$p \vee q \wedge r$ のような書き方はできない。必ず，$(p \vee q) \wedge r$ または $p \vee (q \wedge r)$ のように括弧を用いて意味不明にならないように書く。

2.1.2　メタ論理の記号 $\Rightarrow, \Leftrightarrow$

$\Rightarrow, \Leftrightarrow$ は条件命題をモノとして言及する記号で，合成命題を作る記号ではない。別のいい方をすると，$P(x) \Rightarrow Q(x)$ や $P(x) \Leftrightarrow Q(x)$ は，$\wedge$，$\vee$，$\rightarrow$，$\overline{\quad}$，$\forall$，$\exists$ で表される論理の世界を外から見た記述である。その意味で，$\Rightarrow, \Leftrightarrow$ をメタ論理の記号と呼ぶ。

$P(x) \Rightarrow Q(x)$ は，$P(x)$ を成立させるどの x に対しても $Q(x)$ が成立することを意味するから，同じ意味のことを表す命題は，$\forall x[P(x) \rightarrow Q(x)]$ である。

2.2　命題論理の推論規則

2.2.1　$p \rightarrow q$ の推論

$p \rightarrow q$ は，p と仮定すると q が導かれることを意味する。

$p \rightarrow q$ を導くためには，いったん p と仮定し，その仮定のもとで q が導かれることを示す。$p \rightarrow q$ が得られると，以後，p という仮定を残しておく必要がない。このことを次の推論図で表す。$\vdots$ は p を仮定して q を得る推論の過程，横線は推論の実行を表す。

$$\dfrac{\begin{array}{c}[p]\\ \vdots\\ q\end{array}}{p \rightarrow q}$$

p を囲う括弧 [ ] は，$p \rightarrow q$ を導いた後，仮定から除去されることを意味する。つまり，推論を始めるときは仮定として p を書き，$p \rightarrow q$ を導いた後に p を消す。実際に書くときは斜線などで消すことにしてもよい。

p と $p \rightarrow q$ が成立しているとき q は真である。このことを推論図で

$$\frac{p \quad p \rightarrow q}{q}$$

と書く。横線の上は p と $p \rightarrow q$ が書かれていれば，逆順に並んでいてもよい。

例 23 $p \rightarrow q$ と $q \rightarrow r$ を仮定するとき，$p \rightarrow r$ が成立する。

まず，仮定の 2 つを書く。

$$p \rightarrow q \quad q \rightarrow r$$

$p \rightarrow r$ を示したいので，p を仮定に追加する。

$$p \quad p \rightarrow q \quad q \rightarrow r$$

p と $p \rightarrow q$ とから q を導く。

$$\frac{p \quad p \rightarrow q}{q} \quad q \rightarrow r$$

q と $q \rightarrow$ r とから r を導く。

$$\dfrac{\dfrac{p \quad p \to q}{q} \quad q \to r}{r}$$

そして，最終的に $p \to r$ を導いたところで仮定の p を消す。

$$\dfrac{\dfrac{\dfrac{[p] \quad p \to q}{q} \quad q \to r}{r}}{p \to r}$$

このとき，最上段に消されずに残っている $p \to q$ と $q \to r$ がこの推論における仮定である。

Note.　推論図を書くとき，論拠が横線の上にうまく乗ってないとかっこ悪いが，論理的には関係ない。論理的な関係を誤らなければ，図の上で離れたところに書かれた命題から推論してよい。

注意 24 q が真であれば，p の真偽にかかわらず $p \to q$ は真である。すなわち，

$$\frac{q}{p \to q}$$

は正しい推論形式である。これは，1 番目の推論図の特別な場合とみなせる。

2.2.2　$\wedge$ の推論

$p \wedge q$ が得られるのは p と q が得られたときだから，それを推論規則として書くと，

$$\frac{p \quad q}{p \wedge q}$$

$p \wedge q$ が真であれば p も q も真だから，次の 2 つの推論規則が成立する。

$$\frac{p \wedge q}{p} \qquad \frac{p \wedge q}{q}$$

注意 25 推論規則の横棒の上に書く命題の順序（左右）は意味を持たない。だから，p と q が推論できたときには，$p \wedge q$ とともに $q \wedge p$ も得られる。一方，論理記号による結合は順序の違いを識別する（たとえば，$p \to q$ と $q \to p$ は意味が違う）。

2.2.3　$\vee$ の推論

p が真であれば $p \vee q$ は真であるし，q が真であっても $p \vee q$ は真だから次の 2 つの推論規則が成立する。

$$\frac{p}{p \vee q} \qquad \frac{q}{p \vee q}$$

$p \vee q$ は場合分けの証明で使われる。$p \vee q$ が正しくて，p のときも q のときも r が成立すれば，p, q の仮定を除去して r の成立がいえる。これを推論図で書くと，

$$\frac{p \vee q \quad p \to r \quad q \to r}{r}$$

例 26 n を正の整数とするとき，n^2 を 3 で割った余りは，0 または 1 である。

解. a を b で割った余りを $a \mod b$ で表す。
$n \mod 3$ は，0,1,2 のいずれかである。
$n \mod 3 = 0$ のとき，$n^2 \mod 3 = 0$ だから，$n^2 \mod 3$ は 0 または 1 である。
$n \mod 3 = 1$ のとき，$n^2 \mod 3 = 1$ だから，$n^2 \mod 3$ は 0 または 1 である。
$n \mod 3 = 2$ のとき，$n^2 \mod 3 = 1$ だから，$n^2 \mod 3$ は 0 または 1 である。
したがって，$n^2 \mod 3$ は，0 または 1 である。 □

注意 27 上の例のように証明を書く人は滅多にいない。$\vee$ の推論形式の 2 つを同時に適用して，次の形で使うことが多い。

$$\frac{p \vee q \quad p \to r \quad q \to s}{r \vee s}$$

2.2.4 否定の推論

「p でない」ことは，p だとすると矛盾することから推論できる。これを推論図で書くと，

$$\frac{p \to \curlywedge}{\overline{p}}$$

矛盾は，$p \wedge \overline{p}$ から導かれる。推論図で書くと，

$$\frac{p \wedge \overline{p}}{\curlywedge}$$

注意 28 上掲の推論規則から，$(p \to \curlywedge) \to \overline{p}$ と $p \wedge \overline{p} \to \curlywedge$ が得られる。逆にこれら 2 式を論理に関する公理と見なせば，上掲の推論が正しいことがいえる。

注意 29 $\dfrac{p \wedge \overline{p}}{\curlywedge}$ は，$\dfrac{p \quad \overline{p}}{\curlywedge}$ と書いても意味は変わらない。一般に，2 個以上の論理式を並べて書くのと $\wedge$ でつなげて書くのは同じ意味になる。

例題 30 $\sqrt{2}$ は有理数ではない。

解. まず，整数 m, n を用いて $\sqrt{2} = \dfrac{m}{n}$ と表すための必要条件を求める。
両辺を平方して分母を払うと $m^2 = 2n^2$ となるから m は偶数。
$m = 2k$（k は整数）とすると，$n^2 = 2k^2$ となるから n も偶数。
だから，$\sqrt{2}$ が分数で表せたら，分母子ともに偶数である。
ところが，分数は既約分数で表せるから，そのような分数は存在しない。 □

補足 1　分数は，その分母，分子をそれらの最大公約数で割れば既約分数になる。だから，少なくとも一方が 0 でない 2 つの整数に対してそれらの最大公約数が必ず存在することを証明したとき，上の証明が完結する。公約数全体の集合は有限集合なので，それはほぼ自明。

補足 2　素因数分解の一意性を用いて，$m^2 = 2n^2$ の両辺を素因数分解したときの 2 の指数が左辺で偶数，右辺で奇数となることから矛盾を導く証明もある。ただし，素因数分解の一意性の証明は，最大公約数の存在ほど簡単ではない。（注）素因数分解の一意性と

は，ある整数を素因数分解したとき，現れる素数とその指数が一通りに定まること。言い換えると，異なる手法で素因数分解しても答は同じだということ。もし素因数分解の一意性が成立しないとすると，平方数（m^2 や n^2）を素因数分解したときに含まれる素因数 2 の個数が偶数とは断定できないことになる。

補足 3　「$\sqrt{2}$ は無理数である」というためには，無理数の定義を明確にしておくことが必要。普通，有理数でない実数を無理数と呼ぶので，そのときは，$\sqrt{2}$ が実数であることを前提にすれば上の証明でよい。

練習 31 $p \wedge \overline{q}$ から $\overline{p \to q}$ が導かれることを示せ。(p が真で q が偽だったら $p \to q$ は偽だということ)　[ヒント] $p \to q$ と仮定して矛盾 ($\curlywedge$) を導く。

練習 32 $\overline{p \vee q}$ から $\overline{p} \wedge \overline{q}$ が導かれることを示せ。

[ヒント] $\overline{p \vee q}$ から $\overline{p}$ が導かれることと，$\overline{p \vee q}$ から $\overline{q}$ が導かれることを示す。$\overline{p}$ を示すためには p から矛盾 ($\curlywedge$) を導く。

練習 33 $\overline{p} \wedge \overline{q}$ から $\overline{p \vee q}$ が導かれることを示せ。

[ヒント]$p \to \curlywedge$ と $q \to \curlywedge$ を導くと $p \vee q \to \curlywedge$ が導かれる。

練習 34 $\overline{p} \vee \overline{q}$ から $\overline{p \wedge q}$ が導かれることを示せ。

[ヒント] $p \wedge q$ から $\overline{p} \to \curlywedge$ と $\overline{q} \to \curlywedge$ を導く。

2.2.5　二重否定

$p \to \overline{\overline{p}}$ はこれまでに述べた推論規則から導ける。

練習 35 p から $\overline{\overline{p}}$ を導く推論図を書け。[ヒント]　$\overline{p} \to \curlywedge$ を導けば $\overline{\overline{p}}$ が出る。

逆に $\overline{\overline{p}} \to p$ はこれまでに述べた推論規則からは導かれないので，次の推論規則 (**二重否定の法則** *(*正確には，**二重否定除去**の法則*)*) を追加する。

$$\frac{\overline{\overline{p}}}{p}$$

2.2.6　排中律　$p \vee \overline{p}$

$p \vee q$ を示すのに $\overline{p} \to q$ を示すことがある。その根拠として用いられるのが排中律である。

$p \vee \overline{p}$ を**排中律**という。通常，排中律は論理における公理として用いられ，推論中に排中律が現れてもそれを推論の仮定に算入しない。

排中律のように，常に真であって，証明に用いるとき仮定に算入する必要のない命題を**恒真式**(tautology) という。

$p \to p$ は自明な恒真式である。

排中律を用いると，$\overline{p} \to q$ から $p \vee q$ が導かれる (注意 27 参照)。p のとき p であり，$\overline{p}$ のとき $\overline{p} \to q$ から q が成立するから $p \vee \overline{p}$ から $p \vee q$ が導かれる。推論図の形に書くと

$$\frac{p \vee \overline{p} \quad p \to p \quad \overline{p} \to q}{p \vee q}$$

$p \vee \overline{p}$ と $p \to p$ は，恒真式だから，推論の仮定から省いてよい。すなわち，次の形式は正しい推論である。

$$\frac{\overline{p} \to q}{p \vee q}$$

次の例題は，$p \vee q$ を示す代わりに $\overline{p} \to q$ を示している。

例題 36 $x, y \in \mathbb{C}$ のとき，$xy = 0 \Rightarrow x = 0 \vee y = 0$

証明. $x \neq 0$ のとき，$\dfrac{1}{x}$ を $xy = 0$ の両辺にかけて，$y = 0$ □

練習 37 x に関する方程式 $ax^2 + 2x + c = 0$ が実数解を持つとき，$a = 0$ または $ac \leqq 1$。ただし，a, c は実数とする。

練習 38 $p \to q$ から $\overline{p} \vee q$ が導かれる。　[ヒント] $p \vee \overline{p}$

練習 39 $\overline{p \wedge q}$ から $\overline{p} \vee \overline{q}$ が導かれる。　[ヒント] $p \vee \overline{p}$

2.2.7　恒真式　$\curlywedge \to p$

証明の途中で矛盾が生じると，二重否定の法則を用いて，そこから任意の命題を導くことができる。

一般に，

$$\frac{\curlywedge}{p}$$

は正しい推論形式であり，その結果として，$\curlywedge \to p$ は恒真式である。なぜかというと，$\curlywedge$ を仮定すると，$\overline{p} \to \curlywedge$ が成立する (注意 24 参照) から $\overline{\overline{p}}$ となり，二重否定の法則から p が導かれる。推論図の形に書くと，

$$\cfrac{\cfrac{\cfrac{\curlywedge}{\overline{p} \to \curlywedge}}{\overline{\overline{p}}}}{p}$$

練習 40 $\overline{p}$ から $p \to q$ が導かれる。すなわち，p が偽のとき $p \to q$ は真である。

[ヒント] p と仮定すると $\overline{p}$ から矛盾が出る。そこで，恒真式 $\curlywedge \to q$ を用いる。

練習 41 $\overline{p} \vee q$ から $p \to q$ が導かれる。[ヒント] 注意 24

練習 42 $(p \vee q) \wedge \overline{p} \to q$　[ヒント] $\overline{p}$ を仮定すると，p のときも q のときも q となる。

2.2.8　背理法

背理法は，結論を否定して矛盾を導く証明法だと説明されることが多い。けれども，実際には，背理法には 2 パターンがある。

(1) $\overline{p}$ を示すために $\overline{\overline{p}}$ と仮定する。二重否定の法則を用いて $\overline{\overline{p}}$ から p が得られるので，p と仮定して矛盾を導いて $\overline{p}$ と結論する。

(2) p を示すために $\overline{p}$ と仮定する。$\overline{p}$ から矛盾が導かれると $\overline{\overline{p}}$ が結論できるから，二重否定の法則を用いて p と結論する。

(2) では二重否定の法則が本質的であるけれども，(1) のパターンの場合，$\overline{\overline{p}}$ と仮定する必要はなく，p と仮定するだけで $\overline{p}$ が得られる。

$\sqrt{2}$ が無理数であることの証明は (1) のパターンである。形式的には無理数であることを否定して証明を始めるけれども,「無理数でない」と仮定する代わりに，有理数であるという肯定形の仮定から始めれば二重否定の法則を用いずに証明が終わる。

次の定理の証明も,「無数に存在する」ことを「有限でない」ことと解釈すれば，(1) の型の推論である。

例 43 素数は無数に存在する。

証明. 素数の全体が $p_1, p_2, \dots, p_n$ の n 個であるとすると，$p = p_1 p_2 \cdots p_n + 1$ はどの p_k よりも大きい素数であるから，素数の総数が n 個であることに矛盾する。 □

まとめ 44　　背理法

背理法の本質は $(p \to \curlywedge) \to \overline{p}$ の型の推論である。
$\overline{p}$ 型の命題を示すときは，p から矛盾を導くのが常套手段
（事実上，それが否定の定義なのだから当然)。
p を示すために $\overline{p}$ から矛盾を導く手法が有効なこともある
（その場合，あわせて，二重否定の法則が用いられる)。

練習 45 m, n が奇数であれば，2 次方程式 $x^2 + mx + n = 0$ は整数の解を持たない。

練習 46 a, b が有理数のとき，$a + b\sqrt{2} = 0$ ならば $b = 0$ である。（$\sqrt{2}$ が有理数でないことを用いてよい)

2.2.9　鳩ノ巣原理（部屋割り論法）

練習 47 n 部屋しかないホテルに $n + 1$ 人の人が泊まると，少なくとも 1 室は 2 人以上の客がいる。（各部屋 1 人以下と仮定して矛盾を導く。この論法は，部屋割り論法，ディリクレの引き出し論法，鳩ノ巣原理などと呼ばれる。英語の pigeonhole には，整理棚の小区画という意味がある。ディリクレは 19 世紀ドイツの数学者。)

練習 48 $\dfrac{1}{7}$ を小数で表すと循環小数になる。（割り切れないとき，7 で割った余りは最大 6 通り)。一般に，有理数を小数で表すと，循環小数（整数，有限小数を含む）になる。（だから，無理数（有理数でない実数）を小数で表すと循環しない無限小数になる。)

2.2.10　排中律

排中律は命題の真偽値は真か偽のいずれかであって，その中間は存在しないという主張である。排中律を利用すると，次のような証明が可能になる。存在するものを具体的に示せない証明なので，この種の証明を**非構成的証明**という。

例 49 a^b が有理数となるような無理数 a, b が存在する。

証明. $(\sqrt{2})^{\sqrt{2}}$ が有理数であれば，$a = \sqrt{2}, b = \sqrt{2}$ とおく。
$(\sqrt{2})^{\sqrt{2}}$ が無理数であれば，$a = (\sqrt{2})^{\sqrt{2}}, b = \sqrt{2}$ とおくと，
$a^b = \{(\sqrt{2})^{\sqrt{2}}\}^{\sqrt{2}} = (\sqrt{2})^{\sqrt{2}\sqrt{2}} = (\sqrt{2})^2 = 2$ □

2.2.11 古典論理と直観主義論理

二重否定の法則と排中律の使用を認める論理を**古典論理**という。通常，数学では，古典論理が用いられる。

二重否定の法則を用いると，存在しないという仮定が否定されたとき，存在が導かれる。存在命題は，具体的に存在が示されたときにのみ証明されると考える立場だと，二重否定の法則は強すぎる。

人 $\to p$ は二重否定の法則から導かれるけれど逆はいえない。すなわち，人 $\to p$ は二重否定の法則より弱い推論規則である。そして，人 $\to p$ を前提とすると，排中律と二重否定の法則は一方を仮定すると他方が得られる関係にある (詳細は省く)。

人 $\to p$ のみを許し，二重否定の法則や排中律を認めない論理を**直観主義論理**という。直観主義は，非構成的証明を認めない論理である。

有限の数学であれば，論理法則として排中律を仮定しなくても，実質的に排中律に相当する命題が成立する。けれども，無限が絡むとそうはいかず，排中律なしでは実数論を展開するのも容易ではない。

2.3 古典論理の世界

2.3.1 $p \to q$ と $\overline{p} \vee q$

練習 38，練習 41 により，2 つの恒真式

$$(p \to q) \to (\overline{p} \vee q)$$
$$(\overline{p} \vee q) \to (p \to q)$$

が得られた。$(p \to q) \wedge (q \to p)$ を $p \rightleftarrows q$ と書く約束にすると，上記をまとめて，

$$(p \to q) \rightleftarrows (\overline{p} \vee q)$$

と書ける（排中律が仮定されていることに注意)。

練習 50 何枚かのカードがあって，どのカードも片面には整数が，もう一方の面には英字またはカタカナが書かれている。「英字の裏は偶数」という性質が成り立っているか，必要最小限のカードを裏返して調べるためにはどのカードをえらべばよいか。[ヒント] たとえば，$\boxed{\text{A}}$ $\boxed{5}$ $\boxed{\text{イ}}$ $\boxed{6}$

2.3.2 対偶

$(p \to q) \rightleftarrows (\overline{p} \vee q)$ なので，$(\overline{q} \to \overline{p}) \rightleftarrows (\overline{\overline{q}} \vee \overline{p})$
二重否定の法則から $(\overline{\overline{q}} \vee \overline{p}) \rightleftarrows (q \vee \overline{p})$
したがって，

$$(p \to q) \rightleftarrows (\overline{q} \to \overline{p})$$

2.3.3 $\wedge, \vee, \overline{\quad}$ の算術

排中律の成立を前提とするとき，$\wedge, \vee, \overline{\quad}$ によって表された論理式の計算公式を真理表を書いて確かめることができる。真 (true) を T，偽を F(false) で表す。

a	b	$a \wedge b$	$a \vee b$
T	T	T	T
T	F	F	T
F	T	F	T
F	F	F	F

a	$\overline{a}$
T	F
F	T

（注意） 排中律を前提にしないと，
すべての場合を尽くしたことにならない。

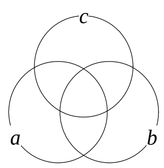
二重否定の法則	$\overline{\overline{a}} \rightleftarrows a$	
交換法則	$a \wedge b \rightleftarrows b \wedge a$	$a \vee b \rightleftarrows b \vee a$
結合法則	$(a \wedge b) \wedge c \rightleftarrows a \wedge (b \wedge c)$	$(a \vee b) \vee c \rightleftarrows a \vee (b \vee c)$
分配法則	$a \wedge (b \vee c) \rightleftarrows (a \wedge b) \vee (a \wedge c)$	$a \vee (b \wedge c) \rightleftarrows (a \vee b) \wedge (a \vee c)$
ド・モルガンの法則	$\overline{a \wedge b} \rightleftarrows \overline{a} \vee \overline{b}$	$\overline{a \vee b} \rightleftarrows \overline{a} \wedge \overline{b}$

練習 51 分配法則 $a \wedge (b \vee c) \rightleftarrows (a \wedge b) \vee (a \wedge c)$

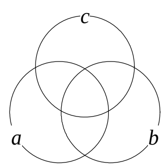
a	b	c	$b \vee c$	$a \wedge (b \vee c)$	$a \wedge b$	$a \wedge c$	$(a \wedge b) \vee (a \wedge c)$
T	T	T					
T	T	F					
T	F	T					
T	F	F					
F	T	T					
F	T	F					
F	F	T					
F	F	F					

(参考) ベン図を利用して場合分けを表現してもよい。円の内側が真，外側が偽。

$a \wedge (b \vee c)$



$(a \wedge b) \vee (a \wedge c)$



練習 52 正の整数 x, y, z が $x^2 + y^2 = z^2$ を満たすならば，x, y のうち少なくとも一方は偶数。

2.4 述語論理

$\forall$ や $\exists$ を含む命題を対象とする論理を**述語論理**という。(述語とは条件命題のこと)

述語論理は無限の可能性を扱うので，真理表を書いて真偽値を調べる手法が使えない。

2.4.1 $\forall x P(x)$ の証明

$\forall x P(x)$ を示すには，x を任意の要素として $P(x)$ を示せばよい。ただし，証明中，他の箇所で x が別の意味で使われていたら任意性が保証できない。他で使われていない変数 a に対し $P(a)$ を導いたとき $\forall x P(x)$ が結論できる。

$\forall x P(x)$ を導く正しい推論の型を推論図の形に書くと

$$\frac{P(a)}{\forall x P(x)}$$

である。ただし，変数 a の任意性を要求する。

2.4.2 $\exists x P(x)$ の証明

$\exists x P(x)$ を示すには，具体的に $P(t)$ となる t を示せばよい。その種の証明を**構成的証明**という。

例 53 $\exists x[x^3 = -8]$

証明. $(-2)^3 = -8$ より $\exists x[x^3 = -8]$ □

この型の推論を推論図で書くと，

$$\frac{P(t)}{\exists x P(x)}$$

である。$\forall x P(x)$ の証明と同じ形をしているが，t は変数である必要はなく，数式など，対象領域の要素であればよい。

一方，$\overline{\exists x P(x)}$ から矛盾を導いて二重否定の法則により成立を示すこともある。その種の証明を**非構成的証明**という。後に示す $\overline{\forall x P(x)} \to \exists x \overline{P(x)}$ を用いる証明は非構成的証明である。

2.4.3 $\forall x P(x)$ を用いる推論

$\forall x P(x)$ を用いる証明の形式は単純で，t を任意の要素として，$\forall x P(x)$ から $P(t)$ を結論してよい。

推論図の形に書くと，t を対象領域の任意の要素とするとき，

$$\frac{\forall x P(x)}{P(t)}$$

たとえば，$\forall x[x^2 > 0]$ が真だったら，x に 0 を代入して $0 > 0$ と結論してよい（推論としては正しい）。

練習 54 (1) 対象領域が空集合でなければ $\forall xP(x) \to \exists xP(x)$ が成立する。
(2) 対象領域が空集合のとき $\forall xP(x) \to \exists xP(x)$ は偽である。

注意 55 $\forall x \in S[P(x)]$ から $\exists x \in S[P(x)]$ を導く推論を行いがちなので注意。この推論が正しいのは $S \neq \varnothing$ のときにかぎり，$S = \varnothing$ のときには誤った結論を導く。たとえば，次の証明には不備がある。
$2 < x < 3$ のとき $x^2 - 5x + 6 < 0$ なので $\exists x[x^2 - 5x + 6 < 0]$
もしこの証明が正しければ，次の証明も正しい。
$2 < x < 2$ のとき $x^2 - 4x + 4 < 0$ なので $\exists x[x^2 - 4x + 4 < 0]$

2.4.4 $\exists xP(x)$ を用いる推論

関数 f が区間 $[a, b]$ で単調増加であるとは，
区間 $[a, b]$ 内の任意の 2 数 x_1, x_2 に対し，$x_1 < x_2$ ならば $f(x_1) < f(x_2)$
となることである。平均値の定理を用いると，
関数 f が区間 $[a, b]$ で連続，(a, b) で $f'(x) > 0$ ならば，f は区間 $[a, b]$ で単調増加することが示せる。

証明. 区間 $[a, b]$ 内の任意の 2 数 x_1, x_2 に対し，$x_1 < x_2$ とする。
平均値の定理から，$\dfrac{f(x_2) - f(x_1)}{x_2 - x_1} = f'(t)$ となる t が区間 (x_2, x_1) に存在する。
このとき，$f'(t) > 0$ だから，$x_1 < x_2$ より $f(x_1) < f(x_2)$。 □
この証明では，$f'(t) > 0$ から結論を導いているけれども，この t は結論には現れない。

一般に，$\exists xP(x)$ を前提とする次の推論は正しい推論形式である。

$$\frac{\exists xP(x) \quad \forall x[P(x) \to R]}{R}$$

練習 56 n が合成数であれば，$\sqrt{n}$ が整数であるか，または，$(n-1)!$ が n で割り切れるかのいずれかである。
[ヒント]n は合成数なので，$n = ab$ となる 1 より大きい整数 a, b がある。$n = ab$ から (a, b を含まない) 結論を導くと，$\exists a \exists b[n = ab]$ によって $n = ab$ を仮定から除去できる。排中律 $a = b \vee a \neq b$ を用いて分類する。

2.4.5 $\overline{\forall xP(x)}$ と $\overline{\exists xP(x)}$

対象領域が有限集合 $\{a_1, a_2, \ldots, a_n\}$ であれば，
$\forall xP(x) \rightleftarrows P(a_1) \wedge P(a_2) \wedge \ldots \wedge P(a_n)$,
$\exists xP(x) \rightleftarrows P(a_1) \vee P(a_2) \vee \ldots \vee P(a_n)$
なので，
ド・モルガンの法則から $\overline{\forall xP(x)} \rightleftarrows \overline{P(a_1)} \vee \overline{P(a_2)} \vee \ldots \vee \overline{P(a_n)}$,

$$\overline{\exists x P(x)} \rightleftarrows \overline{P(a_1)} \wedge \overline{P(a_2)} \wedge \ldots \wedge \overline{P(a_n)}$$ となって，

$\overline{\forall x P(x)} \rightleftarrows \exists x \overline{P(x)}$，$\overline{\exists x P(x)} \rightleftarrows \forall x \overline{P(x)}$ がいえる。

しかし，対象領域が無限集合になると場合分けの手法が使えないから,「同様」といって済ますわけにはいかない。

まず，結論が否定形である 2 つを示す。$\overline{p}$ を導くために p から矛盾を導く論法を使う。

2.4.6 $\forall x \overline{P(x)} \to \overline{\exists x P(x)}$

証明. $\forall x \overline{P(x)}$ と仮定する。
　$\exists x P(x)$ と仮定する。
　$P(c)$ となる c がある。
　$\forall x \overline{P(x)}$ より，$\overline{P(c)}$。これは矛盾。
　よって，$\overline{\exists x P(x)}$。 □

2.4.7 $\exists x \overline{P(x)} \to \overline{\forall x P(x)}$

反例が見つかれば $\forall x P(x)$ は偽だという意味だから，これは難しくない。

証明. $\exists x \overline{P(x)}$ という仮定のもとで，$\forall x P(x)$ と仮定して矛盾を導く。
$\exists x \overline{P(x)}$ から，対象領域の要素 c で $\overline{P(c)}$ となるものがある。
$\forall x P(x)$ より $P(c)$ だから，矛盾。 □

次に，否定形の仮定をもつ 2 つを示す。否定形の仮定 $\overline{p}$ を使うために，p を導いて矛盾 $\overline{p} \wedge p$ に導くのが常套手段。

2.4.8 $\overline{\exists x P(x)} \to \forall x \overline{P(x)}$

証明. $\overline{\exists x P(x)}$ と仮定する
　$\forall x \overline{P(x)}$ を示すために，a を任意の要素として $\overline{P(a)}$ を導く。
　　$P(a)$ と仮定すると，$\exists x P(x)$ が導かれるから $\overline{\exists x P(x)}$ に反する。
　よって，$\forall x \overline{P(x)}$ □

2.4.9 $\overline{\forall x P(x)} \to \exists x \overline{P(x)}$

証明. 対偶 $\overline{\exists x \overline{P(x)}} \to \forall x P(x)$ を示す。
直前に示した $\overline{\exists x P(x)} \to \forall x \overline{P(x)}$ の $P(x)$ の部分に $\overline{P(x)}$ を当てはめると
$\overline{\exists x \overline{P(x)}} \to \forall x \overline{\overline{P(x)}}$
二重否定の法則より $\overline{\overline{P(x)}} \rightleftarrows P(x)$ なので，$\overline{\exists x \overline{P(x)}} \to \forall x P(x)$ が得られる。 □

2.4.10　$\overline{\forall x P(x)}$ と $\overline{\exists x P(x)}$

以上の結果をまとめると，ド・モルガンの法則類似の次の法則が成立する。

$$\overline{\forall x P(x)} \rightleftarrows \exists x \overline{P(x)}$$
$$\overline{\exists x P(x)} \rightleftarrows \forall x \overline{P(x)}$$

2.5　等号

2.5.1　等しいことの意味

中学校 1 年で学ぶ等号の性質だけでは数学は成り立たない。

問 57 $x = 2$ のとき，$x^2 + 3x + 1 = 2^2 + 3 \times 2 + 1$ となる理由を中学校 1 年で学ぶ等号の性質を用いて説明しなさい。

問 58 $x = \pi$ のとき $\sin x = \sin \pi$ となるのはなぜか。

等号は数学の対象として同一であることを示すために用いられる。等しいものは等しいもので置き換えてよい。たとえば，関数 f に対し，$x = y$ であれば $f(x) = f(y)$ となるのは等号の基本性質と考えてよい。

2.5.2　一意性と存在の一意性

$\forall x \forall y [P(x) \wedge P(y) \to x = y]$ であるとき，$P(x)$ は x について**一意**であるという。$P(x)$ が x について一意であることを,「$P(x)$ を満たす x は高々 1 つ」ということもある。これは，$P(x)$ を満たす x の個数が 0 個または 1 個で，2 個以上存在することがないことを意味する。たとえば，平面幾何で,「異なる 2 直線の共有点は高々 1 つ」というとき，2 直線は共有点を持たないこともある。

$P(x)$ を満たす x が存在し，しかもそれが一意であるとき,「$P(x)$ となる x がただ一つ存在する」，あるいは,「$P(x)$ となる x が一意的に存在する」などといい，$\exists ! P(x)$ で表す。すなわち，

$$\exists ! x P(x) \Leftrightarrow \exists x P(x) \wedge \forall x \forall y [P(x) \wedge P(y) \to x = y]$$

だから，一意的に存在することを示すためには，存在と一意性を別々に示せばよい。

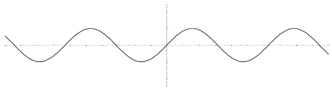
ただし，存在を示した後で，他に在ったとして同一を示すこともある。だから，

$$\exists ! x P(x) \Leftrightarrow \exists x [P(x) \wedge \forall y [P(y) \to x = y]]$$

と考えてもよい。

例 59 $P(x)$ を「x は 2 の正または 0 の平方根である（すなわち，$x \geqq 0$ かつ $x^2 = 2$)」とすると，
x の変域（対象領域）が $\mathbb{R}$ のとき，$P(x)$ となる x は高々一つしかない。
x の変域を $\mathbb{R} \cup \{0\}$ とすると，$P(x)$ となる x はただ一つ存在する。

存在が一意であるとき，それを関数記号で表すことができる。たとえば，正の数 x の平方根を $\sqrt{x}$ で表す。

例 60 平均値の定理において，$\dfrac{f(b)-f(a)}{b-a} = f'(t), a < t < b$ となる t は一意ではない。
たとえば，$f(x) = \sin x, a = -3\pi, b = 3\pi$ 

存在が一意でないとき，それを関数記号を用いて表すことは（普通は）しない。
たとえば，虚数 $a + bi$ の 2 つの平方根を $\pm\sqrt{a+bi}$ で表すが，単独の $\sqrt{a+bi}$ は意味を持たない。

3　集合と写像

3.1　集合

3.1.1　集合

集合は順序や重複を考えない，モノの集まりである。
集合を構成する個々のモノを**要素**または 元（げん） という。
$a_1, a_2, \ldots, a_n$ を要素として持つ集合を $\{a_1, a_2, \ldots, a_n\}$ で表す。これを集合の**外延的記法**という。
集合において，要素の順序は考えない。たとえば, {1,2,4,3} ={1,2,3,4} 。
書かれた要素の中に重複があっても，集合としては重複を無視して考える。たとえば，{1,2,5,2,3}={1,2,3,5}
x が集合 S の要素であることを $x \in S$ で表し，x は S に**属する**という。。
条件命題 $P(x)$ に対し，$P(x)$ を満たす x の全体からなる集合を $\{x|P(x)\}$ で表す。これを集合の**内包的記法**という。
x の変域が U であるとき，それを明示するために $\{x \in U|P(x)\}$ と書くこともある。
集合の内包的記法において，次が成立する。

$$a \in \{x|P(x)\} \Leftrightarrow P(a)$$

3.1.2　集合の包含関係

集合 A のいずれの要素も集合 B の要素であるとき，A は B の**部分集合**である，A は B に含まれる，B は A を**含む**などといい，$A \subset B$ で表す。

論理式を用いて書くと，$A \subset B$ の定義は，

$$A \subset B \overset{\text{def}}{\Leftrightarrow} \forall x[x \in A \to x \in B]$$

集合は要素を含むか含まないかの関係にのみ注目した概念なので，$A \subset B$ かつ $B \subset A$ のとき $A = B$ である。すなわち，

$$A = B \Leftrightarrow (A \subset B) \land (B \subset A)$$

$A \subset B$ かつ $A \neq B$ であるとき，A は B の**真部分集合**であるといい，$A \subsetneqq B$ で表す。

3.1.3 空集合

要素を一つも持たない集合を **空**(くう) **集合** といい，$\varnothing$ で表す。外延的記法で $\varnothing = \{\}$。

任意の集合 A に対し，$\varnothing \subset A$ である。なぜなら，$x \in \varnothing$ は偽なので $x \in \varnothing \to x \in A$ は真だから。

3.1.4 共通部分と和集合

集合 A, B のどちらにも属する要素全体の集合を A, B の**共通部分**(intersection) といい $A \cap B$ で表す。すなわち，

$$A \cap B \overset{\text{def}}{=} \{x | x \in A \land x \in B\}$$

集合 A, B の少なくともいずれかに属する要素全体の集合を A, B の**合併集合**(union)，または**和集合**といい $A \cup B$ で表す。すなわち，

$$A \cup B \overset{\text{def}}{=} \{x | x \in A \lor x \in B\}$$

例題 61 $A \cap B \subset A$

解. $x \in A \cap B$ とすると，$x \in A$ かつ $x \in B$ より $x \in A$。
次のように書くこともできる。
$x \in A \cap B \Leftrightarrow x \in A \land x \in B \Rightarrow x \in A$ □

練習 62 $A \subset A \cup B$

例題 63 $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

解.

$$\begin{aligned}
& x \in A \cup (B \cap C) \\
& \quad \Leftrightarrow x \in A \lor x \in B \cap C \\
& \quad \Leftrightarrow x \in A \lor (x \in B \land x \in C) \\
& \quad \Leftrightarrow (x \in A \lor x \in B) \land (x \in A \lor x \in C) \\
& \quad \Leftrightarrow x \in A \cup B \land x \in A \cup C \\
& \quad \Leftrightarrow x \in (A \cup B) \cap (A \cup C)
\end{aligned}$$

□

練習 64 $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

例題 65 $A = A \cap B \Leftrightarrow A \subset B$

解. $(\Rightarrow)$
$A = A \cap B$ とする。
（$A \subset B$ を示すために）$x \in A$ とすると，$x \in A = A \cap B \subset B$ より $x \in B$。
よって，$A \subset B$。
$(\Leftarrow)$
$A \subset B$ とする。
$A \supset A \cap B$ は明らか。
（$A \subset A \cap B$ を示すために）$x \in A$ とすると，$A \subset B$ から $x \in B$ となるので $x \in A \wedge x \in B$ より $x \in A \cap B$。
よって，$A = A \cap B$。 □

練習 66 $A = A \cup B \Leftrightarrow A \supset B$

3.1.5　補集合

全体集合 U の部分集合 A に対し，U の要素で A に属さないものの全体の集合を A の**補集合**といい，$\overline{A}$ で表す。

すなわち，$A \subset U$ に対し，$\overline{A} \overset{\mathrm{def}}{=} \{x | x \in U \wedge x \notin A\}$。

ただし，$x \notin A$ は $x \in A$ の否定を表す。

A の補集合を A^{c} で表すこともある（complement)。$\overline{A}$ を補集合と異なる意味に用いることがある。その場合，補集合を表すのに A^{c} を用いる。

例題 67 $A \cap \overline{A} = \varnothing$

解. $\supset$ は明らかなので， $A \cap \overline{A} \subset \varnothing$ を示す。
$x \in A \cap \overline{A}$ とすると，$x \in A$ であり，$x \in \overline{A}$ より $x \notin A$ だから矛盾。$\therefore x \in \varnothing$ □

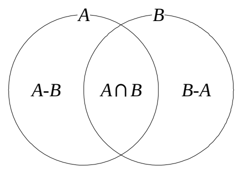
練習 68 (1) $A \cup \overline{A} = U$　　(2) $\overline{(\overline{A})} = A$
注意　証明においてどんな論理法則を用いたか明確に示すこと。

練習 69 (1) $\overline{(A \cup B)} = \overline{A} \cap \overline{B}$　　(2) $\overline{(A \cap B)} = \overline{A} \cup \overline{B}$
[ヒント]　論理に関するド・モルガンの法則を適用する。

3.1.6　差集合

２つの集合 A, B に対し，A の要素であって B の要素でないものの全体を A と B の**差集合**といって，$A - B$ で表す。すなわち，
$A - B = \{x | x \in A \ \wedge \ x \notin B\} = A \cap \overline{B}$ である。ただし，$x \notin B$ は x が B の要素でないことを表す。

差集合 $A-B$ を $A\setminus B$ で表すこともある。記号 $\setminus$ を後に述べる商集合と混同しないように注意。



3.1.7 集合の直積 $A\times B$

要素 a と要素 b を順序を考えに入れて組にしたものを**順序対**といい，記号で (a,b) で表す。

２つの順序対 (a,b)，(c,d) が等しいのは，$a=c$ かつ $b=d$ のときである。

２つの集合 A,B に対して，A の要素と b の要素から作られる順序対全体の集合 $\{(x,y)|x\in A\wedge y\in B\}$ を A と B の直積といい，$A\times B$ で表す。すなわち，

$$A\times B \overset{\text{def}}{=} \{(x,y)|x\in A\wedge y\in B\}$$

注意 70 コンマで区切って条件命題を並べて書いたとき，コンマは「かつ」を意味する。すなわち，$\{(x,y)|x\in A, y\in B\}=\{(x,y)|x\in A\wedge y\in B\}$

例 71 $A=\{1,2\}, B=\{3,4,5\}$ のとき，
$A\times B=\{(1,3),(1,4),(1,5),(2,3),(2,4),(2,5)\}$

A,B が $\mathbb{R}$ の部分集合であるとき，$A\times B$ は xy 平面の部分集合として図示できる。特に，$\mathbb{R}\times\mathbb{R}$ は xy 平面全体である。$\mathbb{R}\times\mathbb{R}$ を $\mathbb{R}^2$ で表す。

練習 72 任意の集合 A に対し　$\varnothing\times A=\varnothing$。
空集合の性質として　$\forall x[x\notin\varnothing]$　すなわち $\forall x[\neg(x\in\varnothing)]$ を用いてよい。$\neg(x\in\varnothing)$ は $x\in\varnothing\to\curlywedge$ と言い換えられることに注意。$\neg$ は否定，$\curlywedge$ は矛盾を表す。

練習 73 任意の集合 A,B,C に対し，
(1) $A\times(B\cap C)=(A\times B)\cap(A\times C)$
(2) $A\times(B\cup C)=(A\times B)\cup(A\times C)$
[ヒント] xy 平面で，x 軸上に区間 A，y 軸上に区間 B,C を置いて考えて見ると様子が解る。

練習 74 A,B,C,D を集合とするとき，
(1) $(A\times B)\cup(C\times D)\subset(A\cup C)\times(B\cup D)$ であることを示せ。
(2) $(A\times B)\cup(C\times D)\neq(A\cup C)\times(B\cup D)$ となる例を示せ。
[ヒント]　有限集合の範囲で反例を作れる。

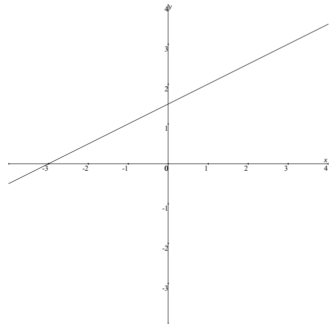
練習 75 A,B,C,D を集合とするとき，
$(A\times B)\cap(C\times D)=(A\cap C)\times(B\cap D)$
は正しいか？　正しければ証明し，正しくなければ反例を示せ。

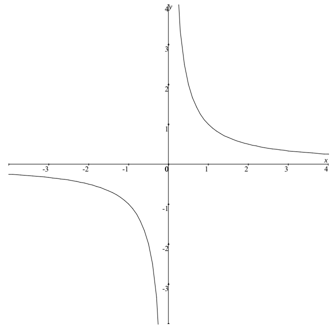
3.2 写像

3.2.1 対応 (Correspondence)

X, Y を集合，$R \subset X \times Y$ とする。
R は，X の要素 x と Y の要素 y の対応関係を定める。
$(x, y) \in R$ であるとき，x は y に**対応**するといい， $x \stackrel{R}{\longmapsto} y$ で表す。

例 76 $S_1 = \{(x, y) \in \mathbb{R} \times \mathbb{R} | x + 2y = 3\}$ $S_2 = \{(x, y) \in \mathbb{R} \times \mathbb{R} | xy = 1\}$

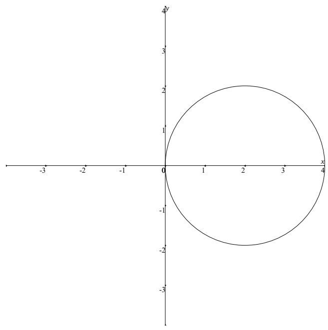




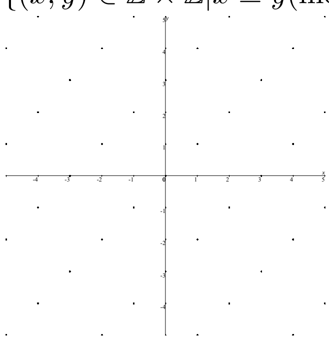
$-3 \stackrel{s_1}{\longmapsto} 0$ $-1 \stackrel{s_1}{\longmapsto} 1$ $-1 \stackrel{s_2}{\longmapsto} -1$ $1 \stackrel{s_2}{\longmapsto} 1$

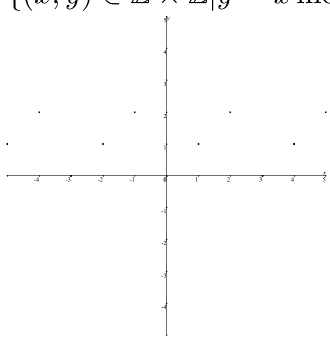
例 77 $S_3 = \{(x, y) \in \mathbb{R} \times \mathbb{R} | (x-2)^2 + y^2 = 2^2\}$

$2 \stackrel{s_3}{\longmapsto} 2$ $2 \stackrel{s_3}{\longmapsto} -2$



例 78 $x - y$ が a の整数倍と等しいことを $x \equiv y (\mathrm{mod}\, a)$ で表す。
x を a で割った余りを $x \bmod a$ で表す。
$S_4 = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} | x \equiv y (\mathrm{mod}\, 3)\}$ $S_5 = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} | y = x \bmod 3)\}$





3.2.2 写像 (Mapping) と関数 (Function)

対応関係には，X の要素 x に対応する Y の要素 y が高々一つしか存在しないものがある。たとえば，前項の S_1, S_2, S_5 が定める対応関係はそうなっている。

$X \times Y$ の部分集合 f が定められ，X のいずれの要素 x に対しても，$(x, y) \in f$ となる Y の要素 y が高々１つしか存在しないとき，f は X から Y への (**広義**) **写像**であるという。すなわち，f が X から Y への (**広義**) **写像**であるとは，
$f \subset X \times Y \quad \wedge \quad \forall x \in X[\ (x, y_1) \in f \ \wedge \ (x, y_2) \in f \ \rightarrow \ y_1 = y_2]$。
このとき，X を**始集合**，Y を**終集合**という。
f が X から Y への (広義) 写像であることを

$$f : X \longrightarrow Y$$

あるいは

$$X \xrightarrow{f} Y$$

で表す。X の要素 x に対応する Y の要素 y が存在するとき，それを $f(x)$ で表す。また，そのとき，f は x を y に**写す**という。
対応する Y の要素が存在する X の要素全体の集合を f の**定義域**という。また，対応する X の要素が存在するような Y の要素全体の集合を f の**値域**という。
定義域が始集合と一致する (広義) 写像を (**狭義**) **写像**，あるいは単に**写像**と呼ぶ。
関数は，(広義) 写像とほぼ同義であるが，本あるいは著者によって定義に微妙な差がある。
（広義）写像 f が関数と呼ばれるとき，$f(x)$ を x における f の **値**（あたい） と呼ぶ。
（広義）写像 $f : X \longrightarrow Y$ において $x \xmapsto{f} y$ であることを

$$\begin{aligned} f : X &\longrightarrow Y \\ x &\longmapsto y \end{aligned}$$

あるいは，

$$f : X \longrightarrow Y \ ; \ x \longmapsto y$$

で表す。

例 79 数列 $a_0, a_1, a_2, \ldots$ を $\{a_n\}_{n \in \mathsf{N}}$ で表す。$\{a_n\}_{n \in \mathsf{N}}$ は $\mathbb{N}$ から $\mathbb{R}$(または $\mathbb{C}$) への写像である。
（注意） 数列 $\{a_n\}_{n \in \mathsf{N}}$ と集合 $\{a_n | n \in \mathbb{N}\}$ を混同しないこと。$\{a_n | n \in \mathbb{N}\} = \{a_0, a_1, a_2, \ldots\}$ は数列 $\{a_n\}_{n \in \mathsf{N}}$ の値域である。集合との混同を避けるために，数列を $(a_n)_{n \in \mathsf{N}}$ のように書く流儀もある。

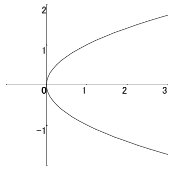
例 80 $x \longmapsto \frac{1}{x}$ で $\mathbb{R}$ から $\mathbb{R}$ への対応を定めると，この対応関係は定義域が $\mathbb{R} - \{0\}$ の (広義) 写像である。この (広義) 写像を (狭義) 写像と呼ぶためには，始集合を $\mathbb{R} - \{0\}$ と定めて定義し直さなければならない。

問 81 $\mathbb{R}$ から $\mathbb{R}$ への対応 $x \longmapsto y$ を以下のように定めるとき，この対応関係は (広義) 写像であるか。さらに (狭義) 写像でもあるか。(i.e. は英語で“すなわち”を意味する)
(1) $x \xmapsto{f} y \overset{\text{def}}{\Leftrightarrow} x = y^2$（$y$ は x の平方根） i.e. $f = \{(x, y) \in \mathbb{R} \times \mathbb{R} | x = y^2\}$
(2) $x \xmapsto{f} y \overset{\text{def}}{\Leftrightarrow} x = y^3$（$y$ は x の立方根） i.e. $f = \{(x, y) \in \mathbb{R} \times \mathbb{R} | x = y^3\}$

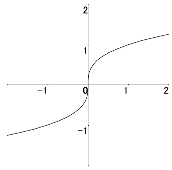
(3) $x \longmapsto \tan x$

(4) $x \longmapsto \begin{cases} 1(x \in \mathbb{Q} \text{ のとき}) \\ 0(x \notin \mathbb{Q} \text{ のとき}) \end{cases}$

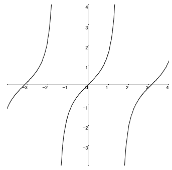
$y^2 = x$



$y^3 = x$



$y = \tan x$



注意 82 (広義) 写像は，**部分写像**(partial mapping) と呼ばれることがある。partial mapping は不完全な写像という意味で，写像の一部分という意味ではない。また，そのとき，始集合，終集合は，**始域**，**終域**と呼ばれる。

3.2.3 写像の相等

以後，(狭義) 写像のみを扱う。

写像の定義を確認しておく。

X, Y を集合とする。$f \subset X \times Y$ が写像 $X \longrightarrow Y$ であるとは，

$$\forall x \in X \ \exists! y \in Y \ [(x, y) \in f]$$

が成立することである。そして，この y を $f(x)$ で表す。

だから，写像 $f : X \longrightarrow Y$ に対し，$(x, y) \in f \Leftrightarrow y = f(x)$。

練習 83 同じ定義域を持つ 2 つの写像 $f : X \longrightarrow Y$，$g : X \longrightarrow Y'$ に対し，

$$\forall x[x \in X \to f(x) = g(x)] \Rightarrow f = g$$

注意 84 f が関数のとき，集合 $\{(x, y) \in X \times Y | y = f(x)\}$ は関数 $y = f(x)$ のグラフである。だから，2 つの関数が等しいとは，それらのグラフが一致することである。

3.2.4 写像の合成

写像 $f : X \longrightarrow Y$，$g : Y \longrightarrow Z$ に対して，f と g の合成写像 $g \circ f : X \longrightarrow Z$ を

$$x \overset{g \circ f}{\longmapsto} g(f(x))$$

で定義する。すなわち，$(g \circ f)(x) = g(f(x))$。

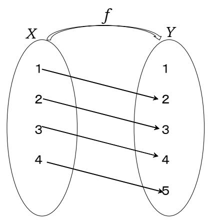
f と g の合成を $g \circ f$ と逆順に書くので注意。

写像の合成において，結合法則が成立する。すなわち，$f : X \longrightarrow Y$，$g : Y \longrightarrow Z$，$h : Z \longrightarrow W$ とするとき，$h \circ (g \circ f) = (h \circ g) \circ f$。

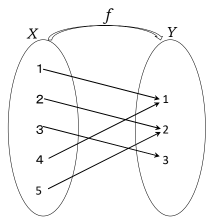
練習 85 $f(x) = x^2, g(x) = x + 1$ であるとき，$(g \circ f)(x)$ と $(f \circ g)(x)$ を求めよ。

問 86 1 次関数と 1 次関数の合成は何次関数か。2 次関数と 2 次関数の合成は何次関数か。一般に，m 次関数と n 次関数の合成は何次関数か。ただし，m, n は正の整数。

3.2.5 単射と全射



単射



全射

以後，$f : X \longrightarrow Y$ と書いたとき，写像概念に，始集合 X と終集合 Y が含まれるものとする。（写像 $f \subset X \times Y$ の始集合 X は f の定義域だから自動的に決まるが，Y は f からは定まらない。）

写像 $f : X \longrightarrow Y$ が**単射**であるとは，$\forall x_1 \in X\ \forall x_2 \in X[f(x_1) = f(x_2) \to x_1 = x_2]$ となること。言い換えると，単射となる条件は，任意の $y \in Y$ に対し，$y = f(x)$ となる $x \in X$ が（もし存在すれば）一意に定まることである。

例 87 $f(x) = x^3$ で定められる関数 $f : \mathbb{R} \longrightarrow \mathbb{R}$ は単射である。
$g(x) = x^2$ で定められる関数 $g : \mathbb{R} \longrightarrow \mathbb{R}$ は単射ではない。ただし，始集合を $\mathbb{R}^+ \cup \{0\}$ に制限すれば単射である。

写像 $f : X \longrightarrow Y$ が**全射**であるとは，$\forall y \in Y[\exists x \in X[y = f(x)]]$ となること。（終集合 Y の指定がないと全射は定義できないことに注意。）

例 88 $f(x) = x^3$ で定められる関数 $f : \mathbb{R} \longrightarrow \mathbb{R}$ は全射である。
$g(x) = x^2$ で定められる関数 $g : \mathbb{R} \longrightarrow \mathbb{R}$ は全射ではない。ただし，終集合を $\mathbb{R}^+ \cup \{0\}$ に制限すれば全射である。

全射であり単射でもある写像を**全単射**という。

例 89 $f(x) = x^3$ で定められる関数 $f : \mathbb{R} \longrightarrow \mathbb{R}$ は全単射である。
$g(x) = x^2$ で定められる関数 $g : \mathbb{R}^+ \cup \{0\} \longrightarrow \mathbb{R}^+ \cup \{0\}$ は全単射である。

練習 90 $f : X \longrightarrow Y$ を全単射とし，$y \in Y$ とする。このとき，$y = f(x)$ となる $x \in X$ がただ一つ存在する。

練習 91 $f : X \longrightarrow Y$，$g : Y \longrightarrow Z$ とする。
(1) $g \circ f$ が全射であれば，g は全射である。
(2) $g \circ f$ が単射であれば，f は単射である。

練習 92 $f : X \longrightarrow Y$，$g : Y \longrightarrow Z$ とする。
(1) $g \circ f$ が全射で g が単射ならば，f は全射である。
(2) $g \circ f$ が単射で f が全射ならば，g は単射である。

練習 93 $f : X \longrightarrow Y$，$g_1 : Y \longrightarrow Z$，$g_2 : Y \longrightarrow Z$ とする。f が全射で $g_1 \circ f = g_2 \circ f$ ならば $g_1 = g_2$ である。　[ヒント] $\forall y[y \in Y \to g_1(y) = g_2(y)]$ を示す。$y \in Y$ と仮定すると，$y = f(x)$ となる $x \in X$ がある。

練習 94 $f_1 : X \longrightarrow Y$, $f_2 : X \longrightarrow Y$，$g : Y \longrightarrow Z$ とする。g が単射で $g \circ f_1 = g \circ f_2$ ならば $f_1 = f_2$ である。　[ヒント] $\forall x[x \in X \to f_1(x) = f_2(x)]$ を示す。

3.2.6　有限集合

有限集合 X に対し，X に含まれる要素の個数を $|X|$ で表し，X の大きさという。たとえば，$X = \{0, 1, 2, 3\}$ のとき，$|X| = 4$

例題 95 S, T を $|S| = |T|$ の有限集合とする。$f : S \longrightarrow T$ が単射であるとき，f は全射でもある。

証明. 部屋割り論法 (鳩ノ巣原理) による。$S = \{x_1, x_2, \ldots, x_n\}$ とする。f が全射でないとすると集合 $\{f(x_1), f(x_2), \ldots, f(x_n)\}$ は $n - 1$ 個以下の要素を持つから $f(x_1), f(x_2)$ $, \ldots, f(x_n)$ のうち一致するものが存在する。これは，f が単射であることに反する。 □

練習 96 S, T を $|S| = |T|$ の有限集合とする。$f : S \longrightarrow T$ が全射であるとき，f は単射でもある。

例題 97 $A = \{1, 2, 3\}, B = \{1, 2, 3, 4, 5\}$ のとき，A から B への単射は全部でいくつあるか。

解. $f : A \longrightarrow B$ で単射を表す。
$f(1)$ の値によって単射を 5 グループに分けることができる。
$f(1) = 1$ である単射は，さらに $f(2)$ の値によって 4 グループに分けられる。
$f(1) = 1, f(2) = 2$ である単射は，$f(3) = 3, 4, 5$ の 3 つある。
同様に考えて，A から B への単射は全部で $5 \times 4 \times 3 (= {}_5\mathrm{P}_3)$ 個ある。 □

一般に，$|R| = r, |X| = n$ のとき，$n \geqq r$ であれば，R から X への単射は ${}_n\mathrm{P}_r$ 個ある。

これは，$r = 0,$ すなわち，$R = \varnothing$ のときも正しい。$\varnothing \times X$ の部分集合 $\varnothing$ は写像 $\varnothing \longrightarrow X$ の定義を満たし，単射の定義も満たすので，$\varnothing$ から X への単射は（少なくとも）1 つ存在する。$\varnothing \times X$ の部分集合は $\varnothing$ しかないから，$\varnothing$ から X への単射はちょうど 1 つだけある。

特に，X から X への全単射は $n! (= {}_n\mathrm{P}_n)$ 個ある。これは，$n = 0$，すなわち，$X = \varnothing$ のときも正しい。

$r \in \mathbb{Z}^+$ とする。集合 $R = \{1, 2, \ldots, r\}$ から有限集合 X への単射を**順列**，$X \longrightarrow X$ の全単射を**置換**という。

練習 98 $|A| = m, |B| = n$ のとき，A から B への写像は全部でいくつあるか。

練習 99 $\mathbb{Z}^+ \times \mathbb{Z}^+ \times \mathbb{Z}^+$ の部分集合 X, Y を

$$X = \{(a, b, c) | 1 \leqq a \leqq b \leqq c \leqq 10\},$$
$$Y = \{(a, b, c) | 1 \leqq a < b < c \leqq 12\}$$

と定めるとき，$|X| = |Y|$ であることを示せ。ただし，$\mathbb{Z}^+$ は正の整数全体の集合を表す。
[ヒント]　全単射 $X \longrightarrow Y$ を定義する。

3.2.7　逆写像（inverse mapping）

$f : X \longrightarrow Y$ が全単射であるとき，次式で $f^{-1} : Y \longrightarrow X$ を定める。

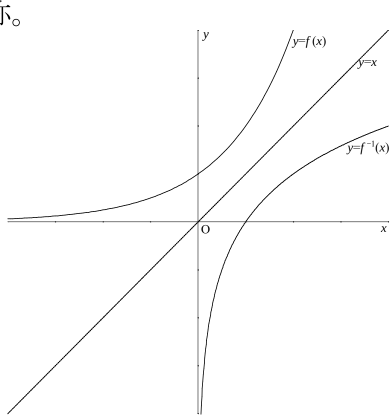
$$f^{-1} \stackrel{\text{def}}{=} \{(y, x) \in Y \times X | (x, y) \in f\}$$

練習 100 $f^{-1} : Y \longrightarrow X$ は写像である。すなわち，$\forall y \in Y\ \exists! x \in X\ [(y, x) \in f^{-1}]$

練習 101 $(x, y) \in f^{-1} \Leftrightarrow (y, x) \in f$，すなわち，$y = f^{-1}(x) \Leftrightarrow x = f(y)$

練習 102 $f^{-1} : Y \longrightarrow X$ は全単射である。

$f^{-1} : Y \longrightarrow X$ を $f : X \longrightarrow Y$ の**逆写像**という。(f^{-1} は f インバースと読む)。
$y = f^{-1}(x) \Leftrightarrow x = f(y)$ だから，$y = f^{-1}(x)$ のグラフは $y = f(x)$ のグラフと直線 $y = x$ について対称。



注意 103　f^{-1} を $x \longmapsto f(x)^{-1}$ で定められる関数と混同しないこと。混同を避けるために f の逆写像を $f^{\leftarrow}$ と書く流儀もある。

例 104 $f(x) = x^3$ であるとき，$f^{-1}(x) = \sqrt[3]{x}$ である。また，$g : \mathbb{R}^+ \cup \{0\} \longrightarrow \mathbb{R}^+ \cup \{0\}$ を $x \mapsto x^2$ で定めるとき，$g^{-1}(x) = \sqrt{x}$ である。

例 105　$a > 0, a \neq 1$ のとき，$f : \mathbb{R} \longrightarrow \mathbb{R}^+$; $x \mapsto a^x$ は逆関数を持ち，

$$f^{-1} : \mathbb{R}^+ \longrightarrow \mathbb{R}\ ;\ x \mapsto \log_a x$$

写像 $f : X \longrightarrow Y$ が逆写像を持つための必要十分条件は，$f : X \longrightarrow Y$ が全単射であることである。

練習 106 写像 $f : X \longrightarrow Y$ において，$g = \{(y, x) \in Y \times X | (x, y) \in f\}$ が写像 $Y \longrightarrow X$ であれば $f : X \longrightarrow Y$ は全単射である。

$\mathrm{id}_X : X \longrightarrow X$ は $x \mapsto x$ で定義され，X 上の**恒等写像**(identity mapping) と呼ばれる。

練習 107 $f : X \longrightarrow Y$ が全単射であるとき，$f^{-1} \circ f = \mathrm{id}_X$，$f \circ f^{-1} = \mathrm{id}_Y$。

例 108 $\qquad \log_a a^x = x \qquad a^{\log_a x} = x \qquad$（ただし，$a > 0, a \neq 1$）

練習 109 $f : X \longrightarrow Y$，$g : Y \longrightarrow X$ とする。$g \circ f = \mathrm{id}_X$，$f \circ g = \mathrm{id}_Y$ ならば f は全単射で，$g = f^{-1}$。　[ヒント]id_X，id_Y は全単射。

例 110 平面上で直線 l に関する線対称移動を σ_l で表す。$\sigma_l \circ \sigma_l = \mathrm{id}$ なので，$\sigma_l^{-1} = \sigma_l$。（σ は小文字のシグマ）

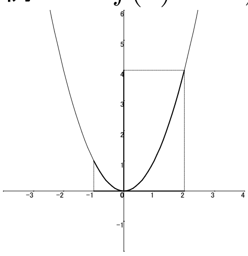
練習 111 $f : X \longrightarrow Y$，$g_1 : Y \longrightarrow X$，$g_2 : Y \longrightarrow X$ とする。$g_1 \circ f = \mathrm{id}_X$，$f \circ g_2 = \mathrm{id}_Y$ ならば f は全単射で，$g_1 = g_2 = f^{-1}$。

3.2.8 写像による集合の像

$f : X \longrightarrow Y$ を写像，$A \subset X$ とする。$x \in A$ に対する $f(x)$ 全体の集合を f による A の**像**(image) といい，$f(A)$ で表す。すなわち，$f(A) = \{f(x) | x \in A\}$。
(補足) f による X の像 $f(X)$ は f の値域。

例 112 $f(x) = x^2$,$A = \{-1, 0, 1, 2\}$ のとき，
$f(A) = \{f(-1), f(0), f(1), f(2)\} = \{1, 0, 1, 4\} = \{0, 1, 4\}$

例 113 $f(x) = x^2$,$A = \{x \in \mathbb{R} | -1 < x < 2\}$ のとき，$f(A) = \{y \in \mathbb{R} | 0 \leqq y < 4\}$



A が有限集合であれば $f(A) = \{f(x) | x \in A\}$ という定義は使いやすいが，A が無限集合だと逆に難しい。
$y \in f(A) \Leftrightarrow P(y)$ となる条件命題 $P(y)$ を求め，$f(A) = \{y | P(y)\}$ の形に書き換えたい。
$y \in f(A)$ とすると，A の要素 x を用いて $y = f(x)$ と書けるのだから，
$y \in f(A) \Leftrightarrow \exists x \in A[y = f(x)]$
すなわち，

$$f(A) \overset{\mathrm{def}}{=} \{y \in Y | \exists x \in A[y = f(x)]\}$$

以下，$f : X \longrightarrow Y$，$A \subset X, B \subset X$ とする。

例 114 $f(A \cap B) \subset f(A) \cap f(B)$

証明. $y \in f(A \cap B)$ とすると，$y = f(x)$ となる $x \in A \cap B$ がある。
$x \in A$ より $f(x) \in f(A)$。$x \in B$ より $f(x) \in f(A)$。$\therefore y \in f(A) \cap f(B)$ □

練習 115 上例で，$f(A \cap B) \neq f(A) \cap f(B)$ となる例を挙げよ。

練習 116 $A \subset B \Rightarrow f(A) \subset f(B)$

練習 117 $f(A \cup B) = f(A) \cup f(B)$
[ヒント]$f(A \cup B) \subset f(A) \cup f(B)$ と $f(A) \cup f(B) \subset f(A \cup B)$ を示せ。

練習 118 写像 $f : \mathbb{R} \longrightarrow \mathbb{R}^2$; $t \longmapsto \left(\dfrac{1-t^2}{1+t^2}, \dfrac{2t}{1+t^2}\right)$ の値域は
$\big\{(x,y)|x^2+y^2=1 \wedge x > -1\big\}$ である。
[ヒント]$\big\{(x,y)|x^2+y^2=1 \wedge x > -1\big\}$ の点に対し対応する t の存在を示すことが要点。

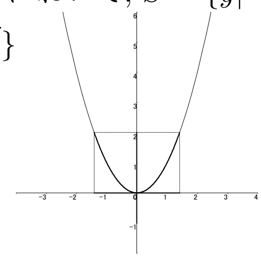
3.2.9 写像による集合の逆像

$f : X \longrightarrow Y$ を写像，$S \subset Y$ とする。$f(x) \in S$ となる $x \in X$ の集合を f による S の**逆像**(inverse image) といい，$f^{-1}(S)$ で表す。すなわち，

$$f^{-1}(S) \overset{\text{def}}{=} \{x \in X | f(x) \in S\}$$

例 119 $f : \mathbb{R} \longrightarrow \mathbb{R}$; $x \mapsto x^2$ において, $S = \{-1, 0, 1, 2\}$ のとき,
$f^{-1}(S) = \{0, 1, -1, \sqrt{2}, -\sqrt{2}\}$

例 120 $f : \mathbb{R} \longrightarrow \mathbb{R}$; $x \mapsto x^2$ において, $S = \{y| -1 < y < 2\}$ のとき,
$f^{-1}(S) = \{x| -\sqrt{2} < x < \sqrt{2}\}$



注意 121 集合の逆像 $f^{-1}(S)$ は，逆写像 f^{-1} が存在しない場合でも定義される。f が全単射であれば $f^{-1}(S) = \{f^{-1}(y)|y \in S\}$ であるが，一般にはそうでない。f が全単射でなければ，S の各要素に対し，対応する $f^{-1}(S)$ の要素は存在しないこともあるし，2 個以上存在することもある。

問 122 $f : \mathbb{R}^2 \longrightarrow \mathbb{R}$; $(x,y) \longmapsto x^2+y^2$ において $f^{-1}(\{-1\})$，$f^{-1}(\{0\})$，$f^{-1}(\{1\})$ を求めよ。

練習 123 $f : X \longrightarrow Y$ を写像，$A \subset X, S \subset Y, T \subset Y$ とする。
(1) $S \subset T \Rightarrow f^{-1}(S) \subset f^{-1}(T)$
(2) $f^{-1}(S \cup T) = f^{-1}(S) \cup f^{-1}(T)$
(3) $f^{-1}(S \cap T) = f^{-1}(S) \cap f^{-1}(T)$

(4) $A \subset f^{-1}(f(A))$
(5) $f(f^{-1}(S)) \subset S$

3.2.10　写像　まとめ

直積　$X \times Y \stackrel{\text{def}}{=} \{(x,y)|x \in X, y \in Y\}$
対応　$f \subset X \times Y$ において $x \stackrel{f}{\mapsto} y \stackrel{\text{def}}{\Leftrightarrow} (x,y) \in f$
(広義) 写像　$f : X \longrightarrow Y$ が (広義) 写像
$\stackrel{\text{def}}{\Leftrightarrow} f \subset X \times Y$ かつ $\forall x \in X\ [(x,y) \in f$ となる y が一意 $]$
定義域　(広義) 写像 $f : X \longrightarrow Y$ の定義域 $= \{x \in X|\exists y \in Y[(x,y) \in f]\}$
写像　$f : X \longrightarrow Y$ が写像 $\stackrel{\text{def}}{\Leftrightarrow} f \subset X \times Y$ かつ $\forall x \in X\ [\exists! y \in Y[(x,y) \in f]]$
値　$f : X \longrightarrow Y$ が (広義) 写像であるとき，$x \stackrel{f}{\mapsto} y$ となる y を $f(x)$ で表す。
写像の**合成**　$f : X \longrightarrow Y$，$g : Y \longrightarrow Z$ に対し，$g \circ f : X \longrightarrow Z$; $x \longmapsto g(f(x))$
単射　写像 $f : X \longrightarrow Y$ が単射　$\stackrel{\text{def}}{\Leftrightarrow} \forall y \in Y[y = f(x)$ となる $x \in X$ が一意 $]$
全射　写像 $f : X \longrightarrow Y$ が全射　$\stackrel{\text{def}}{\Leftrightarrow} \forall y \in Y\ \exists x \in X\ [y = f(x)]$
全単射　写像 $f : X \longrightarrow Y$ が全単射　$\stackrel{\text{def}}{\Leftrightarrow} \forall y \in Y\ \exists! x \in X\ [y = f(x)]$
逆写像　$f : X \longrightarrow Y$ が全単射であるとき，$f^{-1} \stackrel{\text{def}}{=} \{(y,x) \in Y \times X|(x,y) \in f\}$
恒等写像　$\mathrm{id}_X : X \longrightarrow X$; $x \mapsto x$
像　$f : X \longrightarrow Y$，$A \subset X$ に対し，$f(A) \stackrel{\text{def}}{=} \{y \in Y|\exists x \in A[y = f(x)]\}$
逆像　$f : X \longrightarrow Y$，$S \subset Y$ に対し，$f^{-1}(S) \stackrel{\text{def}}{=} \{x \in X|f(x) \in S\}$

3.3　べき集合と集合族

3.3.1　べき集合

集合 X の部分集合全体の作る集合を X のべき集合 (power set) といい $\mathcal{P}(X)$ で表す。すなわち，

$$\mathcal{P}(X) \stackrel{\text{def}}{=} \{S|S \subset X\}$$

例 124　$X = \{0,1,2\}$ のとき，$\mathcal{P}(X) = \{\varnothing, \{0\}, \{1\}, \{2\}, \{0,1\}, \{1,2\}, \{2,1\}, \{0,1,2\}\}$。

例 125　$\mathcal{P}(\varnothing) = \{\varnothing\}$。すなわち，$\varnothing$ のべき集合は，$\varnothing$ を要素として持つ集合 $\{\varnothing\}$ である。

練習 126　有限集合 X に対し，$|X| = n$ のとき，大きさ r の部分集合は ${}_n\mathrm{C}_r$ 個ある。
[ヒント] たとえば，$X = \{0,1,2\}$ のとき，
大きさ 0 の部分集合は，$\varnothing$　(1 個)
大きさ 1 の部分集合は，$\{0\}, \{1\}, \{2\}$　(3 個)
大きさ 2 の部分集合は，$\{0,1\}, \{1,2\}, \{2,0\}$ (3 個)
大きさ 3 の部分集合は，$\{0,1,2\}$　(1 個)

練習 127　有限集合 X に対し，$|\mathcal{P}(X)| = 2^{|X|}$。

3.3.2 集合族

集合 Ω に対し Ω の部分集合からなる集合を Ω 上の**集合族**という。すなわち，$\mathcal{A}$ が Ω 上の集合族であるとは，$\mathcal{A} \subset \mathcal{P}(\Omega)$ のことである。

Ω 上の集合族 $\mathcal{A}$ に対し，それらの**共通部分**，および**合併集合**を

$\bigcap \mathcal{A} \overset{\text{def}}{=} \{x \in \Omega \mid \forall S \in \mathcal{A}[x \in S]\}$，$\bigcup \mathcal{A} \overset{\text{def}}{=} \{x \in \Omega \mid \exists S \in \mathcal{A}[x \in S]\}$

で定める。

たとえば，$\mathcal{A} = \{A_1, A_2, A_3\}$ のとき，$\bigcap \mathcal{A} = A_1 \cap A_2 \cap A_3$，$\bigcup \mathcal{A} = A_1 \cup A_2 \cup A_3$。

$\bigcap \mathcal{A}$，$\bigcup \mathcal{A}$ は，それぞれ，$\bigcap_{S \in \mathcal{A}} S$，$\bigcup_{S \in \mathcal{A}} S$ と書かれることも多い。

練習 128 $\varnothing \neq \mathcal{A} \subset \mathcal{P}(\Omega)$，$\varnothing \neq \mathcal{B} \subset \mathcal{P}(\Omega)$ とする。このとき，

$$\bigcap_{S \in \mathcal{A} \cup \mathcal{B}} S = \left(\bigcap_{S \in \mathcal{A}} S\right) \cap \left(\bigcap_{S \in \mathcal{B}} S\right)$$

$$\bigcup_{S \in \mathcal{A} \cup \mathcal{B}} S = \left(\bigcup_{S \in \mathcal{A}} S\right) \cap \left(\bigcup_{S \in \mathcal{B}} S\right)$$

3.3.3 集合族上の関数

数学では，集合族上で定義された関数を考えることがある。

例 129 座標平面上の集合に対しその面積を対応させる (広義) 写像 $\mathcal{P}(\mathbb{R} \times \mathbb{R}) \longrightarrow \{0\} \cup \mathbb{R}^+ \cup \{\infty\}$。

面積を定義できない集合もある (正確には，その存在を否定できない)。この (広義) 写像の定義域に属する集合を**可測集合**という。可測集合に関する数学は測度論と呼ばれる。

例 130 確率論では，試行によって得られる結果全体の集合を**全事象**といい，全事象の部分集合を**事象**という。全事象が Ω であるとき，事象 $A \subset \Omega$ の確率を $\mathrm{Pr}(A)$ で表すと，Pr は (広義) 写像 : $\mathcal{P}(\Omega) \longrightarrow [0,1]$　である。($[0,1]$ は閉区間 $\{x \in \mathbb{R} | 0 \leqq x \leqq 1\}$ を表す)。

3.3.4 添字付き集合族

I と Ω を集合とする。I を添字集合とする **添字**(そえじ) **付き集合族**$\{A_i\}_{i \in I}$ とは，写像 $A : I \longrightarrow \mathcal{P}(\Omega)$; $i \longmapsto A_i$ のことである。各 A_i は添字付き集合と呼ばれる。添字付き集合族の共通部分および合併集合を次のように定義する。

$\bigcap_{i \in I} A_i \overset{\text{def}}{=} \{x | \forall i \in I[x \in A_i]\}$，$\bigcup_{i \in I} A_i \overset{\text{def}}{=} \{x | \exists i \in I[x \in A_i]\}$

添字集合が正の整数全体の集合 $\mathbb{Z}^+$ であれば，

$\bigcap_{i \in \mathsf{Z}^+} A_i = A_1 \cap A_2 \cap A_3 \cap \cdots$，$\bigcup_{i \in \mathsf{Z}^+} A_i = A_1 \cup A_2 \cup A_3 \cup \cdots$

である。数列 Σ にならって，

$\bigcap_{i=1}^{\infty} A_i = A_1 \cap A_2 \cap A_3 \cap \cdots$，$\bigcup_{i=1}^{\infty} A_i = A_1 \cup A_2 \cup A_3 \cup \cdots$

のように書くこともある。

例題 131 $A_k = \{x \in \mathbb{R} | \frac{1}{k} \leqq x\} (k \in \mathbb{Z}^+)$ とする。$\bigcup_{i \in \mathsf{Z}^+} A_i = \{x \in \mathbb{R} | 0 < x\}$ を示せ。

証明. $A_k \subset \{x \in \mathbb{R} | 0 < x\}$ だから $\bigcup_{i \in \mathsf{N}} A_i \subset \{x \in \mathbb{R} | 0 < x\}$ は明らか。
$\{x \in \mathbb{R} | 0 < x\} \subset \bigcup_{i \in \mathsf{Z}^+} A_i$ を示すために，$x \in \mathbb{R}, 0 < x$ とする。
$\frac{1}{x} \leqq k$ となる $k \in \mathbb{Z}^+$ を取ると，$\frac{1}{k} \leqq x$ より，$x \in A_k \subset \bigcup_{i \in \mathsf{Z}^+} A_i$ □
補足　$\forall x \in \mathbb{R} \exists n \in \mathbb{Z}^+ [x \leqq n]$ を実数のアルキメデス性といい，$\mathbb{R}$ の基本性質。
証明　$x \leqq 0$ のときは明らか。$x > 0$ のとき，x を小数で表すときの整数部分に 1 を加えた数を n とする。

練習 132 $B_n = \{x \in \mathbb{R} | x < \frac{1}{n}\} (n \in \mathbb{Z}^+)$ とする。$\bigcap_{k \in \mathsf{Z}^+} B_k = \{x \in \mathbb{R} | x \leqq 0\}$ を示せ。

3.3.5　ラッセルのパラドックス

べき集合という，集合の集合を定義した。それを発展させて，集合全体の集合を考察対象とすると困ったことが起こる。集合全体を，$X \in X$ となる集合と，$X \notin X$ となる集合とに分ける。そのうち，$X \notin X$ となる集合の全体を S とおく。すなわち，$S = \{X | X \notin X\}$。このとき，$S \in S$ であろうか，それとも $S \notin S$ であろうか。
(1) $S \in S$ とすると，S が S の要素であることから $S \notin S$ となって矛盾する。
(2) $S \notin S$ とすると，S は S を定義する条件を満たすから，$S \in S$ となり，矛盾。
だから，$S \in S$，$S \notin S$ のいずれでもないことになる。
(注)　$S = \{x | P(x)\}$ とすると $x \in S \Leftrightarrow P(x)$ であるが，(1) は $x \in S \Rightarrow P(x)$ を，(2) は $P(x) \Rightarrow x \in S$ を用いている。

現代の集合論では，新しい集合を作る操作を合併集合やべき集合などに限定することで，大きすぎる集合に言及するのを避けている。ただし，だからといって，それで安全だという確証はない。むしろ，自然数全体を考察対象に含めるかぎり，それ（確証を得ること）は不可能であることが証明されている（ゲーデルの不完全性定理)。

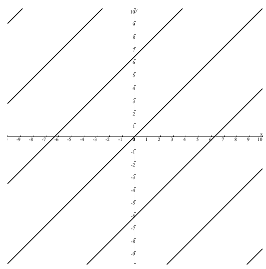
3.4　同値関係と商集合

3.4.1　同値関係

$R \subset X \times X$ のとき，R を集合 X 上の *2* **項関係**という。
集合 X 上の 2 項関係 R は，次の (1)〜(3) を満たすとき X 上の**同値関係**であるという。
(1) $\forall x [x \in X \to (x, x) \in R]$　（反射律）
(2) $\forall x \forall y [(x, y) \in R \to (y, x) \in R]$　（対称律）
(3) $\forall x \forall y \forall z [(x, y) \in R \wedge (y, z) \in R \to (x, z) \in R]$　（推移律）

例 133 $a \in \mathbb{R}^+$ とする。$x, y \in \mathbb{R}$ に対し,
$$x \equiv y \pmod{a} \overset{\mathrm{def}}{\Leftrightarrow} \exists k \in \mathbb{Z} [x - y = ka]$$
と定める（　$x \equiv y \pmod{a}$ は,「x, y は a を法として合同」と読む)。

たとえば，$\frac{5}{4}\pi - (-\frac{3}{4}\pi) = 2\pi$ なので $\frac{5}{4}\pi \equiv -\frac{3}{4}\pi \pmod{2\pi}$。
さらに，$\frac{5}{4}\pi \equiv \frac{13}{4}\pi \equiv \frac{21}{4}\pi \equiv \cdots \pmod{2\pi}$。
このとき，$\{(x,y) \in \mathbb{R} \times \mathbb{R} | x \equiv y (\operatorname{mod} a)\}$ は同値関係である。



$x \equiv y(\operatorname{mod} 2\pi)$

練習 134 上で定めた $x \equiv y \pmod{a}$ は同値関係であることを示せ。次の (1)〜(3) を示せばよい。
(1) $x \equiv x \pmod{a}$
(2) $x \equiv y \pmod{a}$ ならば $y \equiv x \pmod{a}$
(3) $x \equiv y \pmod{a}$ かつ $y \equiv z \pmod{a}$ ならば $x \equiv z \pmod{a}$

3.4.2 商集合

整数の集合 S_k を $S_k = \{n \in \mathbb{Z} | n \equiv k(\operatorname{mod} 3)\}$ で定めるとき，
$S_0 = \{\cdots, -3, 0, 3, \cdots\}$，$S_1 = \{\cdots, -2, 1, 4, \cdots\}$，$S_2 = \{\cdots, -1, 2, 5, \cdots\}$ で，
$S_0 \cap S_1 = \varnothing, S_0 \cap S_2 = \varnothing, S_1 \cap S_2 = \varnothing, S_0 \cup S_1 \cup S_2 = \varnothing$ となる。
また，$S_0 = S_3 = S_6 = \cdots$，$S_1 = S_4 = S_7 = \cdots$，$S_2 = S_5 = S_8 = \cdots$ でもある。

一般に，集合 X 上の同値関係 R があるとき，$(x,y) \in R$ を 2 項関係 $x \sim y$ の形に書くことが多い。($\sim$はチルダと読む)
2 項関係 $x \sim y$ が同値関係であることの条件を$\sim$について書くと，
$x \sim x$
$x \sim y \Rightarrow y \sim x$
$x \sim y \wedge y \sim z \Rightarrow x \sim z$
となる。
このとき，$[x] = \{y \in X | x \sim y\}$ を $\sim$ に関する x の**同値類**という。
このとき，添字付き集合族 $\{[x]\}_{x \in X}$ を考えると，次が成立する。
(1) $x \sim y \Leftrightarrow [x] = [y]$
(2) $\neg\,(x \sim y) \Leftrightarrow [x] \cap [y] = \varnothing$
$\neg\, p$ は p でないこと (p の否定) を表す。

練習 135 上の (1),(2) を示せ。

練習 136 $y \in [x]$ ならば $[x] = [y]$ であることを示せ。

そして，$\mathcal{A}=\{[x]|x\in X\}$ とおくと，
(1) $A,B\in\mathcal{A}$ で $A\neq B$ ならば $A\cap B=\varnothing$
(2) $\bigcup\mathcal{A}=X$

練習 137 上の (1)，(2) を示せ。

この $\mathcal{A}$ を X を $\sim$ で分割した**商集合**といい，$X/\sim$ で表す。
すなわち，$X/\sim\ \stackrel{\mathrm{def}}{=}\{[x]|x\in X\}$，ただし，$[x]=\{y\in X|x\sim y\}$

例 138 （幾何ベクトル）
平面上の有向線分 AB，CD について，それらが同一直線上にあって同じ向きで大きさが等しいか，または，四角形 ABDC が平行四辺形をなすとき，AB$\sim$CD と書くと，$\sim$は同値関係になる。このとき，有向線分 AB が属する同値類をベクトル AB といい，$\overrightarrow{\mathrm{AB}}$ で表す。

3.4.3 剰余類

実数 a に対して，a の倍数（整数倍）の集合 $\{x|\exists k\in\mathbb{Z}[x=ak]\}$ を $a\mathbb{Z}$ で表す。
さらに，$x-y\in a\mathbb{Z}$ で定まる同値関係による商集合を $\mathbb{R}/a\mathbb{Z}$（あるいは $\mathbb{Z}/a\mathbb{Z}$）で表す。
k を 1 より大きい整数とするとき $\mathbb{Z}/k\mathbb{Z}$ の要素は**剰余類**とも呼ばれる。

例 139 $\mathbb{Z}/3\mathbb{Z}=\{[0],[1],[2]\}$
ただし，$[0]=\{\cdots,-3,0,3,\cdots\},[1]=\{\cdots,-2,1,4,\cdots\},[2]=\{\cdots,-1,2,5,\cdots\}$

3.4.4 代表元と代表系

同値類 $[x]$ の要素を $[x]$ の**代表元**という。
たとえば，$\mathbb{Z}/3\mathbb{Z}$ において，$-1,2,5,8,\cdots$ は $[2]$ の代表元である。
写像 $I\longrightarrow X/\sim\ ;\ x\mapsto[x]$ が全単射となるように X の部分集合 I を定めるとき，I を X の $\sim$ に関する**代表系**という。代表系は，各同値類から 1 つだけ要素をとってきて作った集合である。
一般に代表系の取り方は一通りに定まらない。たとえば，{0,1,2} は $\mathbb{Z}/3\mathbb{Z}$ の代表系であるが，{1,2,3} も代表系である。そして，{1,2,4} や {1,2,3,4} は代表系ではない。

例 140 $[0,2\pi)=\{x|0\leqq x<2\pi\}$，$(-\pi,\pi]=\{x|-\pi<x\leqq\pi\}$ はいずれも $\mathbb{R}/2\pi\mathbb{Z}$ の代表系である。

練習 141 次のうち，$\mathbb{Z}/5\mathbb{Z}$ の代表系であるものはどれか（一つとはかぎらない）。
$\{0,1,2,3,4\},\{0,6,12,18,24\},\{0,-1,-2,-3,-4\},\{0,1,4,9,16\},\{0,1,8,27,64\}$

3.4.5 同値関係と商集合　まとめ

$R\subset X\times X$ とする。
同値関係　$(x,y)\in R$ を $x\sim y$ と書くとき，$x\sim y$ が同値関係であるとは

(1) $x \sim x$
(2) $x \sim y \Rightarrow y \sim x$
(3) $x \sim y \wedge y \sim z \Rightarrow x \sim z$
商集合　$X/\sim \overset{\text{def}}{=} \{[x] | x \in X\}$，ただし，$[x] = \{y \in X | x \sim y\}$
同値類　$[x] = \{y \in X | x \sim y\}$ を同値類という。
代表元　$y \in [x]$ のとき，y は $[x]$ の代表元。特に，x は $[x]$ の代表元。
代表系　$I \subset X$ が $\sim$ に関する**代表系**$\overset{\text{def}}{\Leftrightarrow}$ 写像 $I \longrightarrow X/\sim$; $x \mapsto [x]$ が全単射

3.5　補説

3.5.1　選択公理（選出公理）

商集合の代表系は必ず作れるのだろうか。商集合が有限集合であればそれは可能であるが，無限集合であるときは，そうとは言い切れない。

もっと，一般に，空でない集合からなる集合族があったときに，それぞれの集合から一つずつ要素を選び出して代表系を作ることができるという命題を**選択公理**（あるいは**選出公理**）という。詳しく書くと，

集合族 $\{A_i\}_{i \in I}$ において，$\forall i \in I[A_i \neq \emptyset]$ であれば，
写像 $f : I \longrightarrow \Omega$ で $\forall i \in I\ [f(i) \in A_i]$ となるものが存在する。

選択公理を含まない集合論から矛盾が生じないとすると，選択公理を付け加えた集合論と，選択公理の否定を付け加えた集合論のいずれからも矛盾が生じないことが証明されている。つまり，選択公理は証明することも反証することもできない命題である。

選択公理は不思議な結論を導きだす。

選択公理を用いると，球を 3 次元空間内で有限個の部分に分割し，それらを回転・平行移動の操作のみを使って組み替えることで，元の球と同じ半径の球を 2 つ作ることができる（バナッハ・タルスキーの定理，あるいは，バナッハ・タルスキーのパラドックス)。

参考　砂田利一（著）新版 バナッハ・タルスキーのパラドックス (岩波科学ライブラリー　2018/03)

4　数学的構造

4.1　順序集合

4.1.1　全順序と半順序

$R \subset X \times X$ のとき，R を集合 X 上の *2* **項関係**という。

$(x, y) \in R$ を $x \preceq y$ と書くとき，次の (1)〜(3) を満たす 2 項関係を**半順序**，(1)〜(4) を**全順序**または**線形順序**という。

(1) $\forall x[x \preceq x]$　　（反射律）
(2) $\forall x \forall y[(x \preceq y) \wedge (y \preceq x) \rightarrow x = y]$　　（反対称律）
(3) $\forall x \forall y \forall z[(x \preceq y) \wedge (y \preceq z) \rightarrow x \preceq z]$　　（推移律）

(4) $\forall x \forall y[(x \preceq y) \vee (y \preceq x)]$

例 142 集合の包含関係 $\subset$ は，べき集合 $\mathcal{P}(X)$ 上の半順序である。

例 143 大小関係 $\leqq$ は $\mathbb{R}$ 上の全順序である。

例 144 正の整数 a, b に対し，a が b を割り切ることを $a|b$ で表す。$|$ は $\mathbb{Z}^+$ 上の半順序である。特に，$S = \{1, 2, 4, 8, 16\}$ とするとき，$|$ は S 上の全順序である。

4.1.2 最大値・最小値

$\preceq$ を集合 X 上の半順序とし，$S \subset X$ とする。
$\forall x[x \in S \to x \preceq a]$ となる $a \in S$ を S の最大値という。
$\forall x[x \in S \to a \preceq x]$ となる $a \in S$ を S の最小値という。

練習 145 S の最大値，最小値は (もしあれば) ただ一通りに定まることを示せ。
[ヒント]a, b がともに S の最大値のとき $a = b$ であることを示す。

練習 146 $\mathbb{R}$ における順序を $\leqq$ で定めるとき，部分集合 $\{x|0 < x < 1\}$ は最大値を持たないことを示せ。　　[ヒント]m が最大値であるとして矛盾を導く。

4.1.3 整列集合

任意の空でない部分集合が必ず最小値を持つような全順序集合を**整列集合**という。

例 147 有限の全順序集合は整列集合である。

例 148 $\mathbb{N}$ は $\leqq$ について整列集合である。ただし，$\geqq$ で順序 $\preceq$ を定義すると整列集合ではない。

4.2 数学的帰納法

4.2.1 数学的帰納法の原理

$P(n)$ を自然数 n に関する条件命題とする。

$$P(0) \wedge \forall n[P(n) \to P(n+1)] \to \forall n P(n)$$

を数学的帰納法の原理という。

$\forall n[P(n) \to P(n+1)]$ は $P(n) \Rightarrow P(n+1)$ とも書けるから，数学的帰納法の原理を次のように言い換えることができる。

命題 149 数学的帰納法
次の [1]，[2] が成立するとき，$\forall n P(n)$ が成立する。
[1] $P(0)$
[2] $P(n) \Rightarrow P(n+1)$

数学的帰納法が正しいことは，将棋倒しになぞらえて，次のように説明できる。

a を任意の自然数とするとき，
$P(0)$ と [2] より得られる $P(0) \to P(1)$ とから $P(1)$
$P(1)$ と [2] より得られる $P(1) \to P(2)$ とから $P(2)$
$P(2)$ と [2] より得られる $P(2) \to P(3)$ とから $P(3)$
$\cdots\cdots\cdots\cdots$
$P(a-1)$ と [2] より得られる $P(a-1) \to P(a)$ とから $P(a)$

a として 100，1000 など具体的な数を指定すれば，将棋倒しの部分を $\cdots\cdots\cdots\cdots$ を用いずに書ける。しかし，$\forall n P(n)$ の証明は，a にどんな数が指定されてもよいように書かれなければならない。だから，a としてどの自然数が指定されるかわからないときは，将棋倒しの部分を無限個用意しておく必要がある。しかし，無限個の推論を含む証明は，証明として認められない。

すなわち，数学的帰納法の原理は数学における基本的な仮定（公理）であって，それ自身を証明することはできない。

練習 150 a, b を自然数とし，2 次方程式 $x^2 - ax + b = 0$ の 2 つの解を α, β とすると，任意の自然数 n に対し，$\alpha^n + \beta^n$ は整数である。[ヒント]
$\alpha^{k+1} + \beta^{k+1} = (\alpha^k + \beta^k)(\alpha + \beta) - \alpha^k\beta - \alpha\beta^k = (\alpha^k + \beta^k)(\alpha + \beta) - \alpha\beta(\alpha^{k-1} + \beta^{k-1})$
$\alpha^n + \beta^n$ が整数であることを $P(n)$，$P(n) \wedge P(n+1)$ を $Q(n)$ として，$Q(n)$ に帰納法を適用する。

練習 151 数列 $\{a_n\}$ において $a_0 = 0, a_1 = 1, a_n = a_{n-1} + a_{n-2}$ であるとき，
$a_n = \dfrac{1}{\sqrt{5}}\left\{\left(\dfrac{(1+\sqrt{5}}{2}\right)^n - \left(\dfrac{(1-\sqrt{5}}{2}\right)^n\right\}$

4.2.2 累積帰納法

$n > 1$ ならば n は素数の積に分解する（素因数分解できる）ことを数学的帰納法で証明しよう。

$P(n)$ を「n は素数の積に分解する」とすると，$P(2), P(3)$ は自明だけれど，$P(3)$ から $P(4)$ を導けない。

$P(n)$ を自然数 n に関する条件命題とする。

$$\forall n[\forall k[k < n \to P(k)] \to P(n)] \to \forall n P(n)$$

を**累積帰納法**と呼ぶことがある。

命題 152 累積帰納法
$P(n)$ を自然数 n に関する条件命題とする。
$P(0), P(1), P(2), \ldots, P(n-1) \Rightarrow P(n)$
であるとき，$\forall n P(n)$。

$n=0,1,2,3,\ldots$ について $\forall n[\forall k[k<n\to P(k)]\to P(n)]$ は次のように言い換えることができる。

$P(0)$
$P(0)\to P(1)$
$P(0)\wedge P(1)\to P(2)$
$P(1)\wedge P(1)\wedge P(2)\to P(3)$
$\cdots\cdots\cdots\cdots$

$\forall n[\forall k[k<n\to P(k)]\to P(n)]$ が成立していると，将棋倒しの原理で，
$P(0),P(1),P(2),P(3),\ldots\ldots$ の成立が順に示せる。
ただし，任意の n に対し $P(n)$ が成立するというためには $\ldots\ldots$ 部分の無限性を排除しなければならないことは，通常の数学帰納法と同じである。

数学的帰納法が正しければ累積帰納法も正しい。それは以下のようにして示すことができる。
$\forall n[\forall k[k<n\to P(k)]\to P(n)]\cdots$(*) とする。
$\forall k[k\leqq n\to P(k)]$ を $Q(n)$ として，$\forall nQ(n)$ を示す。
[1] $Q(0)$ は $P(0)$ を意味する。
$n=0$ のとき $\forall k[k<n\to P(k)]$ は形式的に真なので，(*) より $P(0)$ は真。
[2] $Q(n)$ とする。すなわち，$\forall k[k\leqq n\to P(k)]$ とする。
これは，$\forall k[k<n+1\to P(k)]$ と書くこともできる。
(*) より　$\forall k[k<n+1\to P(k)]\to P(n+1)$。
$\therefore P(n+1)$　　(**)
（$Q(n+1)$，すなわち $\forall k[k\leqq n+1\to P(k)]$ を示したいので）
$k\leqq n+1$ とする。
$k<n+1$ のとき，帰納法の仮定 $Q(n)$ より $P(k)$ がいえる。
$k=n+1$ のとき。(**) より $P(k)$
よって，$\forall k[k\leqq n+1\to P(k)]$，すなわち，$Q(n+1)$ が成立する。
[1],[2] より，$\forall nQ(n)$。
（次に $\forall nP(n)$ を示す）
m を任意の自然数とする。$\forall nQ(n)$ より $Q(m)$，すなわち，$\forall k[k\leqq m\to P(k)]$
ここで，$k=m$ のときを考えて $P(m)$
すなわち，$\forall nP(n)$。

例題 153 任意の自然数 $n>1$ は素数の積に分解する（素因数分解できる）。
（注意　素因数分解できることと，素因数分解の一意性とを混同しないように。）

証明. 「n は素数の積で表せる」を $P(n)$ とする。
$n>1$ とし，$P(2),P(3),\ldots,P(n-1)$ が成立するものとする。
n が素数のとき，$P(n)$ は成立する。
n が素数でないとき，$n=ab$ となる 1 より大きく n より小さい 2 数 a,b がある。

帰納法の仮定より a, b は素数の積に分解するので，n も素数の積に分解する。
数学的帰納法（累積帰納法）により，$n \geqq 2$ のとき $P(n)$ が成立する。 □

練習 154
正の数からなる数列 $\{a_n\}_{n\in\mathsf{Z}^+}$ が，任意の $n \in \mathbb{Z}^+$ に対して $\left(\sum_{k=1}^{n} a_k\right)^2 = \sum_{k=1}^{n} {a_k}^3$ となるとき，$a_n = n$ であることを示せ。
[ヒント] $\sum_{k=1}^{n} k^3 = \left\{\frac{1}{2}n(n+1)\right\}^2$

4.2.3 数学的帰納法の原理と整列原理

命題 155 整列原理
$\mathbb{N}$ の空でない部分集合は最小値を持つ。

数学的帰納法の原理と整列原理は同値な命題である。つまり，整列原理が正しければ数学帰納法は正しく，その逆もいえる。数学では，これら（どちらか一方または両方）を，自然数の集合のもつ基本性質として仮定する。

整列原理から数学的帰納法の原理を導いてみよう。
数学的帰納法の仮定の [1]，[2] が成立しているものとする。
$\neg\,\forall n P(n)$ と仮定して矛盾を導く。($\neg$ は否定を表す)
$\exists n \neg\, P(n)$ なので，$S = \{n | \neg\, P(n)\}$ とおくと，$S \neq \varnothing$。
整列原理から S は最小値 m を持つ。
$P(0)$ より $0 \notin S$ だから，$m > 0$ である。
このとき，$m-1 \notin S$，$m \in S$ から矛盾が生じる。
なぜなら，$m \in S$ より $\neg\, P(m)$。
$m-1 \notin S$ より $\neg\neg\, P(m-1)$，すなわち，$P(m-1)$。
[2] より，$P(m-1) \to P(m)$ なので $P(m)$。
$\neg\, P(m)$ と $P(m)$ が示せたので矛盾。

練習 156 数学的帰納法 (または累積帰納法) から整列原理を導く。 [ヒント]$S \subset \mathbb{N}$ に対し，S が最小値を持たないとき $S = \varnothing$ を示す。$S = \varnothing \Leftrightarrow \forall n \in \mathbb{N}[n \notin S]$ なので，$\forall n \in \mathbb{N}[n \notin S]$ を累積帰納法で示す。

練習 157 整列原理を用いて，任意の自然数 $n > 1$ は素数の積に分解することを示せ。[ヒント] 素数の積に分解しない 1 より大きい自然数の集合を考える。

4.2.4 数列の再帰的定義 (漸化式で定義される数列)

関数 $f : \mathbb{R} \longrightarrow \mathbb{R}$ を用いて，漸化式 $a_0 = a,\ a_{n+1} = f(a_n)$ で定義される数列について考える。

個別の自然数 n を指定すれば，$a_1, a_2, \ldots, a_n$ が定まることは確実だけれども，自然数全体を定義域とする写像として定義されるのだろうか。初期値 $a_0 = a \in \mathbb{R}$ としておく。

自然数全体を定義域とする数列の実体は，

$S \subset \mathbb{N} \times \mathbb{R}$，$\forall n \in \mathbb{N}\ \exists! x \in \mathbb{R}[(n, x) \in S]$

となる S である。だから，この条件を満たし，なお，かつ，

$(0, a) \in S,\ \forall n \in \mathbb{N}\ \forall x \in \mathbb{R}[(n, x) \in S \to (n+1, f(x)) \in S]$

をみたすものが定義できるかという問題になる。

$n+1 = \{0, 1, 2, \cdots n\}$ と考えることにして，有限数列 $a_0, a_1, \ldots, a_n$ を $\{a_i\}_{i \in n+1}$ で表すことにする。ここで，

$S = \{(n, x) \in \mathbb{N} \times \mathbb{R} | \exists \{a_i\}_{i \in n+1}[a_0 = a \wedge \forall k \in \mathbb{N}[k < n \to a_{k+1} = f(a_k)] \wedge a_n = x]\}$ とおく。

$(n, x) \in S$ となる条件は，わかりやすく書くと，

$a_0 = a, a_1 = f(a_0), a_2 = f(a_1), \ldots, a_n = f(a_{n-1}), a_n = x$　となる有限数列 $a_0, a_1, \ldots, a_n$ が存在する

ことである。このとき，

(1) $\forall n \in \mathbb{N}\ \exists! x \in \mathbb{R}[(n, x) \in S]$

(2) $(0, a) \in S,\ \forall n \in \mathbb{N}\ \forall x \in \mathbb{R}[(n, x) \in S \to (n+1, f(x)) \in S]$

の 2 つを示せばよい（実質，以下の 4 つ）。n に関する数学的帰納法を用いて示すことができる。

練習 158

(1) $\forall n \in \mathbb{N}\ \exists x \in \mathbb{R}[(n, x) \in S]$

(2) $\forall n \in \mathbb{N}\ [(n, x) \in S$ となる x は一意 $]$

(3) $(0, a) \in S$

(4) $\forall n \in \mathbb{N}\ \forall x \in \mathbb{R}[(n, x) \in S \to (n+1, f(x)) \in S]$

注意 159 上述で $\mathbb{R}$ の部分を他の集合に変えても議論はそのまま成立する。すなわち，
X を任意の集合，$f : X \longrightarrow X$ を写像，$a \in X$ とする。
このとき，次の (1)，(2) を満たす点列 $x : \mathbb{N} \longrightarrow X$ が存在する。
(1) $x_0 = a$
(2) $\forall n \in \mathbb{N}[x_{n+1} = f(x_n)]$
ただし，x_n は $x(n)$ を表す。

4.3 無限集合

4.3.1 集合の濃度

有限集合 X, Y の間に全単射が存在するとき，$|X| = |Y|$ である。この考えを無限集合にも適用して，集合 X, Y の間に全単射が存在するとき，X と Y は同じ**濃度**(cardinality) を持つといい，$X \sim Y$ で表す。（英語で cardinal number は，one, two, three のように，ものの個数を数えるときに用いる数をいう。）（$\sim$ が濃度が同じことを表すのは，濃度について議論しているときだけ。）

いずれかの自然数と同じ濃度を持つ集合を**有限集合**といい，そうでない集合を**無限集合**という。

集合 S について，$S\sim n$ であれば，$|S|=n$ である（ただし，$n\in\mathbb{N}$）。

4.3.2 可算集合

自然数全体の集合 $\mathbb{N}$ と同じ濃度を持つ集合を**可算集合**という。X が可算集合であれば，$X\times X$ も加算集合である（証明略）。

可算集合の特徴は，自身と同じ濃度を持つ真部分集合を含むことである。たとえば，$S=\{1,2,3,\ldots\}$ とすれば，$S\sim\mathbb{N}$ で $S\subsetneqq\mathbb{N}$ である。これは有限集合にはない特性である。

4.3.3 無限集合

自然数全体の集合との間に全単射を定義できないような無限集合を**非可算集合**という。$\mathbb{Z},\mathbb{Q}$ は可算集合であるが，$\mathbb{R}$ は非可算集合である（証明略）。

非可算集合についても，可算集合と同様に，自身と同じ濃度を持つ真部分集合を含むといえるだろうか。

まず，無限集合が加算集合を部分集合として含むかどうか考えてみよう。

X を無限集合とする。

$X\neq\varnothing$ だから，X の任意の要素をとり，それを a_0 とする。

$X-\{a_0\}\neq\varnothing$ だから，$X-\{a_0\}$ の任意の要素をとり，それを a_1 とする。

$X-\{a_0,a_1\}\neq\varnothing$ だから，$X-\{a_0,a_1\}$ の任意の要素をとり，それを a_2 とする。

$\cdots\cdots$

$X-\{a_0,a_1,\ldots,a_{n-1}\}\neq\varnothing$ だから，$X-\{a_0,a_1,\ldots,a_{n-1}\}$ の任意の要素をとり，それを a_n とする。

$\cdots\cdots$

このとき，$\{a_0,a_1,\ldots,a_n,\ldots\}$ は X の加算部分集合であるが，数列 $a_0,a_1,\ldots,a_n,\ldots$ の存在を示すのに，選択公理を用いる。

$\mathcal{A}=\mathcal{P}(X)-\{\varnothing\}$ とおくとき，集合族 $\{S\}_{S\in\mathcal{A}}$ に選択公理を適用すれば，写像 $f:\mathcal{A}\longrightarrow X$ で $\forall S\in\mathcal{A}[f(S)\in S]$ となるものの存在がいえる。

そして，4.2.4 と同様の手法を用いて，漸化式 $a_0=f(X),\quad a_n=f(X-\{a_0,a_1,\ldots,a_{n-1}\})$ で数列 $\{a_n\}_{n\in\mathsf{N}}$ を定義する。

命題 160 選択公理の下で，無限集合は加算集合を部分集合として含む。

証明. (概要) X を無限集合とする。$\mathcal{A}=\mathcal{P}(X)-\{\varnothing\}$ とおく。
$\mathcal{A}$ は空でない集合からなる集合族なので，選択公理により
写像 $f:\mathcal{A}\longrightarrow X$ で $\forall S\in\mathcal{A}[f(S)\in S]$ となるものが存在する。
$a_0=f(X),\quad a_n=f(X-\{a_0,a_1,\ldots,a_{n-1}\})$
とすると，$\{a_0,a_1,\ldots,a_n,\ldots\}$ は X の加算部分集合である。 □

命題 161 選択公理の下で，無限集合は自身と同じ濃度を持つ真部分集合を含む。

証明. X を無限集合とする。
前命題の証明における a_0,a_1,...,a_n,... を用いて，$S = \{a_0, a_1, \ldots, a_n, \ldots\}$ とおく。
$Y = X - \{a_0\}$ とおき，$f : X \longrightarrow Y$ を

$$f(x) = \begin{cases} x & (x \notin S \text{ のとき}) \\ a_{n+1} & (x = a_n \in S \text{ のとき}) \end{cases}$$

と定めれば，f は全単射である。 □

上記 2 命題で，選択公理の仮定は，より弱い公理に変えることはできるけれども，完全になくしてしまうことはできないことが知られている。それは,「どれでもよいから一つ選べ」と，無限回，指示するのは（各回での存在は保証されていても）,（選択公理を仮定しなければ）証明として許されないことを意味する。

4.3.4 参考　超実数と超準解析～選択公理がもたらすもの

選択公理を仮定すると，$\mathbb{R}$ に通常の代数操作の対象となるように無限小や無限大を付け加えて超実数とよばれる数の体系を作ることができる。無限小や無限大を含むから，超実数はアルキメデス性を持たない。超実数を用いる微積分学（超準解析）は初学者が微積分を学びやすくする体系として期待されていたが，旧来の解析学を置き換えるには至っていない。

参考　キースラー（著），齋藤正彦（訳）「無限小解析の基礎」（東京図書　1979/03）
　　　M. デービス (著)，難波完爾（訳）「超準解析」（培風館，1982/11）