§1 命題論理と述語論理

§§1.1 命題論理

定義1.1 (命題)

正しいか正しくないかを客観的に判断できる主張を命題という. $p, q, r, \ldots$ で表わされることが多い.

proposition の頭文字

例1.1

(1) p:「$1+1=2$」は命題

(2) q:「$1+1=3$」は命題

定義1.2 (真偽, 真理値)

命題が正しいことを真といい, 正しくないことを偽という. 真のときT, 偽のときFと略記し, 真理値という.

true　　false.

例1.2

例1.1で p の真理値はT, q の真理値はF.

定義1.3 (否定)

命題 p に対して「pでない」という命題を pの否定といい, $\neg p$ とかく.

例 1.3

例 1.1 の p・q について

$\neg p$: 「$1+1 \neq 2$」

$\neg q$: 「$1+1 \neq 3$」

定義 1.4 (真理表)

命題同士の真理値の対応関係を示した表を

真理表 という.

例 1.4

命題 p とその否定 $\neg p$ に関する真理表は次.

p	$\neg p$
T	F
F	T

定義 1.5 (論理和, 論理積)

命題 p・q に対し.

「p または q」を p と q の**論理和**といい "$p \vee q$" と書く.

「p かつ q」を p と q の**論理積**といい "$p \wedge q$" と書く.

注意 1.1

記号 $\vee$, $\wedge$ は別の意味で使うこともある.

例 1.5

真理表を書いてみる.

p	q	$\neg p$	$\neg q$	$p \vee q$	$\neg(p \vee q)$	$\neg p \wedge \neg q$
T	T	F	F	T	F	F
T	F	F	T	T	F	F
F	T	T	F	T	F	F
F	F	T	T	F	T	T

∴ $\neg(p \vee q)$ と $\neg p \wedge \neg q$ の真理値は同じ.

定義 1.6 (同値)

命題 p, q の真理値が等しいとき, p と q は

同値といい, "$p \Longleftrightarrow q$" とか "$p \underset{\text{同値}}{\Longleftrightarrow} q$" とかく.

定理 1.1 (de Morgan の法則)

命題 p, q に対し

(1) $\neg(p \vee q) \Longleftrightarrow \neg p \wedge \neg q$

(2) $\neg(p \wedge q) \Longleftrightarrow \neg p \vee \neg q$

定義 1.7 (含意, 条件命題)

命題 p, q に対し $\neg p \vee q$ を "$p \rightarrow q$" とかき.

「p ならば q」と読む. $p \rightarrow q$ が真のとき.

"$p \Rightarrow q$" と書き. p は q の十分条件, q は p の必要条件という.

例1.6

真理表を書いてみる

p	q	$\neg p$	$p \to q$ $(\neg p \vee q)$	$\neg(p \to q)$
T	T	F	T	F
T	F	F	F	T
F	T	T	T	F
F	F	T	T	F

◎「$p \to q$」の否定は「pが成り立ち、qが成り立たない」になる。

定理1.2

命題 p, q に対し、

「$p \Longleftrightarrow q$」 $\Longleftrightarrow$ 「$p \to q$」$\wedge$「$q \to p$」

($p \Rightarrow q$ と $q \Rightarrow p$ が成り立つ)

証明

真理表を書けばよい。

p	q	$p \Longleftrightarrow q$	$p \to q$	$q \to p$	「$p \to q$」$\wedge$「$q \to p$」
T	T	T	T	T	T
T	F	F	F	T	F
F	T	F	T	F	F
F	F	T	T	T	T

□

定義1.8 (逆, 対偶)

命題 p, q に対し「$q \to p$」を「$p \to q$」の**逆**

「$\neg q \to \neg p$」を「$p \to q$」の**対偶**という。

定理1.3

命題 p, q に対し

「$p \to q$」 $\underset{\text{同値}}{\Longleftrightarrow}$ 「$\neg q \to \neg p$」

証明

真理表を書いてみよ. □.

§1.2 述語論理

定義1.9 (命題関数)

$X_1, \cdots, X_n$ を集合とする. $x_1 \in X_1, \cdots, x_n \in X_n$ に対して

命題 $p(x_1, \cdots, x_n)$ が定まるとき. $p = p(x_1, \cdots, x_n)$

を命題関数という.

例1.7

次は命題関数である.

(1) $X =$ 数学科1年生全体. $x \in X$

$p(x)$: x は男子である.

(2) $X = \mathbb{R}$, $x \in X$, $q(x) : x + 3 = 1$

(3) $X = \mathbb{N}$, $Y = (0, \infty)$. $n \in X$, $\varepsilon \in Y$.

$r(n, \varepsilon) : \frac{1}{n} < \varepsilon$.

定義1.10 (全称命題)

命題関数 $p=p(x)$ $(x\in X)$ に対し.

"任意の $x\in X$ に対して $p(x)$ である"

を "$\forall x\in X\ \ p(x)$" とかき. 全称命題 という.

例1.8

(i) 例1.7の(1)で "$\forall x\in X.\ p(x)$" は偽 (女子もいる)

$Y=$ お茶大の大学生全体.

"$\forall y\in Y.\ \neg p(y)$" は真 (男子はいない)

(ii) 例1.7の(2)で

"$\forall x\in \mathbb{R}\ \ q(x)$" は偽 $\left(\begin{array}{l} x=-3 \text{のとき} \\ q(-3):\ -3+3=1 \end{array}\right)$

(iii) 例1.7の(3)で

"$\forall n\in X,\ \forall \varepsilon\in Y\ \ r(n,\varepsilon)$" は偽

($\varepsilon=1,\ n=1$ とすると $r(1,1):\ \frac{1}{1}<1$)

定理1.4

命題関数 $p=p(x,y)$ $(x\in X,\ y\in Y)$ に対し.

$$\forall x\in X,\ \forall y\in Y\ \ p(x,y) \underset{\text{同値}}{\Longleftrightarrow} \forall y\in Y,\ \forall x\in X\ \ p(x,y)$$

つまり $\forall x$, $\forall y$ の順序は入れかえてよい.

定義 1.11 (存在命題)

命題関数 $p=p(x)$ $(x\in X)$ に対し.

"ある $x\in X$ が存在して $p(x)$ である"

を"$\exists x\in X$ $p(x)$"とかき. 存在命題 という.

s.t. (such that) を書くことが多い

例 1.9

例1.7の(1) $\exists x\in X$ $p(x)$ は真.

例1.8の Y に対し $\exists x\in Y$ $p(x)$ は偽 (男子はいないはず)

例1.7の(2) $\exists x\in \mathbb{R}$ $q(x)$ は真 $\left(\begin{array}{l} x=-2 \text{ のとき} \\ q(-2):\ -2+3=1 \end{array}\right)$

例1.7の(3) $\exists n\in \mathbb{N}$. $\exists \varepsilon\in(0,\infty)$ $r(n,\varepsilon)$ は真

($\varepsilon=2$, $n=1$ ととると $r(1,2)$: $\frac{1}{1}<2$)

定理 1.5

命題関数 $p=p(x,y)$ $(x\in X,\ y\in Y)$ に対し

$$\exists x\in X,\ \exists y\in Y\ \ p(x,y) \underset{\text{同値}}{\Longleftrightarrow} \exists y\in Y.\ \exists x\in X\ \ p(x,y)$$

つまり $\exists x$, $\exists y$ の順序は入れかえてよい.

注意 1.2

定理1.4, 1.5 より

"$\forall x\in X$, $\forall y\in Y$" を "$\forall x\in X$, $y\in Y$"

"$\exists x\in X$, $\exists y\in Y$" を "$\exists x\in X$, $y\in Y$"

と略記することがある.

注意1.3（重要）

"$\forall x \in X, \exists y \in Y\ p(x,y)$" を "$\exists y \in Y, \forall x \in X\ p(x,y)$"

と交換してはいけない。$\exists$ と $\forall$ の交換は一般にできない。

定理1.6（de Morganの法則）

命題関数 $p = p(x)$ $(x \in X)$ に対して

(1) $\neg(\forall x \in X\ p(x)) \underset{\text{同値}}{\Longleftrightarrow} \exists x \in X\ \neg p(x)$

ここはかわらない

(2) $\neg(\exists x \in X\ p(x)) \underset{\text{同値}}{\Longleftrightarrow} \forall x \in X\ \neg p(x)$

ここはかわらない

〈否定のつくり方〉

$\forall \underset{\text{否定}}{\rightsquigarrow} \exists$, $\exists \rightsquigarrow \forall$, $p(x) \rightsquigarrow \neg p(x)$

例1.10（ε-N 論法）

$\{a_n\}_{n=1}^{\infty} \subset \mathbb{R}$：数列，$a \in \mathbb{R}$.

$\lim_{n\to\infty} a_n = a$

$\underset{\text{定義}}{\Longleftrightarrow}$ 任意の正数 ε に対して，ある自然数 N をとると，

任意の自然数 n に対して，

$n \geq N$ ならば $|a_n - a| < \varepsilon$.

（吹田．新保）

∀と∃を使ってかくと

$\forall \varepsilon \in (0,\infty),\ \exists N \in \mathbb{N},\ \forall n \in \mathbb{N}\quad p(\varepsilon, N, n)$

($\forall \varepsilon > 0$ ともかく)

ただし $p(\varepsilon, N, n)$: $n \geq N \Rightarrow |a_n - a| < \varepsilon$

$\lim_{n\to\infty} a_n = a$ でない

∈はかわらない

$\Longleftrightarrow\ \exists \varepsilon \in (0,\infty),\ \forall N \in \mathbb{N},\ \exists n \in \mathbb{N}\quad \neg p(\varepsilon, N, n)$

定理1.6

$\forall \to \exists$　$\exists \to \forall$　$\forall \to \exists$　否定をつけた.

または

$\neg p(\varepsilon, N, n) \Leftrightarrow \neg(\neg(n \geq N) \vee (|a_n - a| < \varepsilon))$

$\Leftrightarrow (n \geq N) \wedge \neg(|a_n - a| < \varepsilon)$

定理1.1　かつ

$\Leftrightarrow (n \geq N) \wedge (|a_n - a| \geq \varepsilon)$

$\therefore\ \lim_{n\to\infty} a_n = a$ でない

$\Longleftrightarrow\ \exists \varepsilon > 0.\ \forall n \in \mathbb{N},\ \exists n \in \mathbb{N}$ s.t.

$(n \geq N) \wedge (|a_n - a| \geq \varepsilon)$

§2 集合の濃度

§§2.1 集合の濃度

$A=\{a, b, c, d, e\}$, $B=\{\alpha, \beta, \gamma, \delta, \varepsilon\}$

AとBの元の個数はどちらも5個.

これを数学の言葉でどう表現するか?

〈アイデア〉

$C=\{1,2,3,4,5\}$　　5個あることはわかっていることにする.

$f: C \to A$を

$f(1)=a$, $f(2)=b$, $f(3)=c$, $f(4)=d$, $f(5)=e$

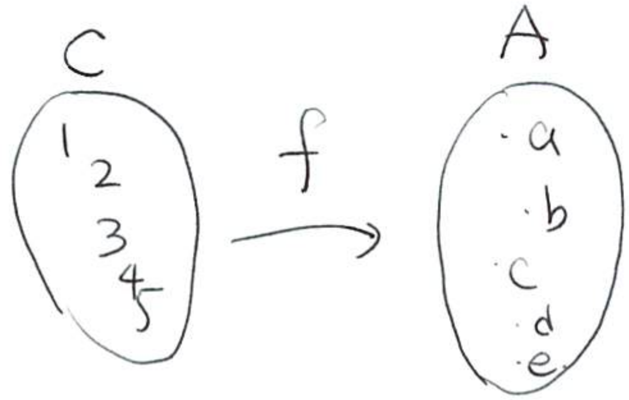
と定義すると, fは全単射.

単射: Aのどの2つの元も番号がちがう.

($\forall n, m \in \mathbb{N}$に対し, $n \neq m \Rightarrow f(n) \neq f(m)$)

全射: Aのどの元にも番号がついている

($\forall y \in A$に対し, $\exists n \in C$ s.t. $f(n)=y$)



定義 2.1（濃度）

X, Y：集合.

XとYの濃度が等しい

$\overset{\text{定義}}{\Longleftrightarrow}$ $\exists$ 全単射 $f : X \to Y$ が存在する.

記号

$X \sim Y$, $\#X = \#Y$ ：XとYの濃度が等しい.

縦が斜（でんわはこっち） → #　：番号記号. Number sign

横が斜 → ♯　：シャープ ｝音楽記号

ナチュラルの縦線をのばすとシャープ. → ♮　：ナチュラル ｝音楽記号

（cf.「番号記号」 wikipedia 日本語）

また 有限集合の場合.

$$\#A = \#C = \#\{1,2,3,4,5\} = 5$$

とかいたりする.

命題2.1 (同値関係)

集合 A, B, C に対し, 次が成り立つ.

(1) $A \sim A$

(2) $A \sim B \Rightarrow B \sim A$

(3) $A \sim B,\ B \sim C \Rightarrow A \sim C$

証明はレポートとする.

例2.1

$n \in \mathbb{N}$, $A = \{1, 2, \cdots, n\}$, $B = \{1, 2, \cdots, n, n+1\}$

とすると $\#A = n$, $\#B = n+1$. であり.

$\#A \neq \#B$. (全単射 $f: A \to B$ が存在するとの矛盾が示せる). 一般に有限集合 A, B に対し. $A \subset B$, $A \neq B$ ならば.

$\#A \neq \#B$. (実際 $\#A < \#B$)

無限集合についての濃度はそれほど自明ではない

例2.2

$A=\{2n : n\in\mathbb{N}\}$ とおくと

$\#A=\#\mathbb{N}$

証明

$f:\mathbb{N}\to A$ を $n\in\mathbb{N}$ に対し

$f(n):=2n$ とおくと f は全単射となる

ので $\#A=\#\mathbb{N}$

1. (f が単射になること)

$\forall n, m\in\mathbb{N}$ に対し $f(n)=f(m)$ ならば

$2n=2m$ より $n=m$.

2. (f が全射になること)

$\forall y\in A$ に対し、$\exists n\in\mathbb{N}$ が存在して $y=2n$

とかける. よって $f(n)=2n=y$ となる

$\square$.

例2.3

$$\#\mathbb{N} = \#\mathbb{Z}$$

理由

$f : \mathbb{N} \to \mathbb{Z}$ を $n \in \mathbb{N}$ に対し

$$f(n) := (-1)^n \left[\frac{n}{2}\right]$$

とおく。ここで $\left[\frac{n}{2}\right]$ は $\frac{n}{2}$ を超えない最大の整数
(Gauss記号)

このfは全単射になっている。実際、

$f(1) = (-1)^1\left[\frac{1}{2}\right] = 0$, $f(2) = (-1)^2\left[\frac{2}{2}\right] = 1$

$f(3) = (-1)^3\left[\frac{3}{2}\right] = -1$, $f(4) = (-1)^4\left[\frac{4}{2}\right] = 2$

$f(5) = (-1)^5\left[\frac{5}{2}\right] = -2$, $\cdots$

例2.4

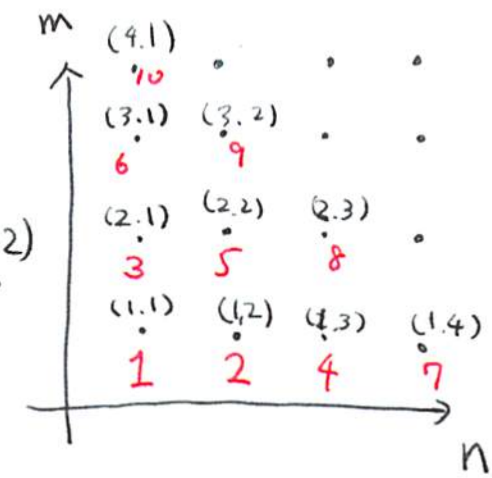
$$\#\mathbb{N} = \#(\mathbb{N} \times \mathbb{N})$$

理由

$f : \mathbb{N}\times\mathbb{N} \to \mathbb{N}$ を $(n, m) \in \mathbb{N}$ に対し

$$f(n, m) := m + \frac{(n+m-1)(n+m-2)}{2}$$

で定めると、fは全単射。



のつまり) $A \subset B$ であっても $\#A = \#B$ となることがある.

§§2.2 可算集合と非可算集合

$\#\mathbb{N} = \#\mathbb{Z} = \#(\mathbb{N}\times\mathbb{N})$ であった.

定義3.2 (可算集合)

$\#\mathbb{N} = \aleph_0$ (アレフゼロ) とかく.

$\#A = \aleph_0$ となる集合Aを **可算集合**という.

また, Aが有限集合か可算集合のとき,

たかだか可算集合 という.

例2.5

A:可算集合. $B \subset A$:無限集合.

$\Rightarrow$ Bは可算集合 i.e. $\#B = \aleph_0$.

たとえば $A = \mathbb{Z}$, $B = \{3n : n \in \mathbb{Z}\}$

いいかえると, 可算集合は(濃度において)

最小の無限集合

例2.6 (もう少し厳密な理由をあとでやる)

$\mathbb{Q}$は可算集合 i.e. $\#\mathbb{Q} = \aleph_0$.

(いいかげんな)理由 $\frac{p}{q} \in \mathbb{Q}$ を $(p, q) \in \mathbb{Z}\times\mathbb{Z}$ とみなすと

$\mathbb{Q} \subset \mathbb{Z}\times\mathbb{Z}$. $\mathbb{Q}$は無限集合で

$\#(\mathbb{Z}\times\mathbb{Z}) = \aleph_0$ より $\#\mathbb{Q} = \aleph_0$.

例2.7

$\#\mathbb{R} \neq \aleph_0$。

証明 （Cantorの対角線論法）

$\#\mathbb{R}$が可算集合ならば $(0,1] \subset \mathbb{R}$ も可算集合なので全単射 $a : \mathbb{N} \to (0,1]$ が存在する．そこで

$$a(n) = 0.a_{n1}a_{n2}a_{n3}\cdots$$

（a_{ni}は0から9までの整数）

と無限小数でかくことにする．ただし

$$1 = 0.\dot{9} = 0.999\cdots$$
$$0.2 = 0.1\dot{9} = 0.1999\cdots$$

とする．

$$a(1) = 0.\underline{a_{11}}\,a_{12}\,a_{13}\,a_{14}\cdots$$
$$a(2) = 0.a_{21}\,\underline{a_{22}}\,a_{23}\,a_{24}\cdots$$
$$a(3) = 0.a_{31}\,a_{32}\,\underline{a_{33}}\,a_{34}\cdots$$
$$a(4) = 0.a_{41}\,a_{42}\,a_{43}\,\underline{a_{44}}\cdots$$
$$\ddots$$

として．$n \in \mathbb{N}$に対し

$$b_n = \begin{cases} 1 & a_{nn} = 0,2,4,6,8 \text{ のとき} \\ 2 & a_{nn} = 1,3,5,7,9 \text{ のとき} \end{cases}$$

とおくと

$$b := 0.b_1b_2b_3\cdots \in (0,1]$$

が定まる．

$b = a(n)$ となる $n \in \mathbb{N}$ は存在しない

(∵ $\forall n \in \mathbb{N}$ に対して $a_{nn} \neq b_n$

よ) $a(n) \neq b$)

従って a が全単射であることに矛盾 □

※この証明に使った対角成分を選ぶ手法を

Cantorの対角線論法 という

定義 2.3 (非可算集合)

$\#\mathbb{R} = \aleph$ (アレフ)とかく. 集合Aがたかだか可算集合でないとき非可算集合という.

例2.8

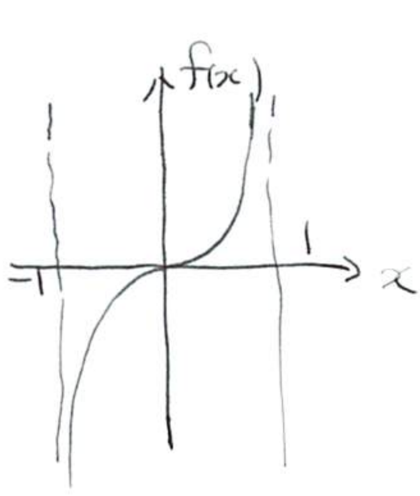
$\#(-1, 1) = \aleph$

理由

$f: (-1, 1) \to \mathbb{R}$ を $x \in (-1, 1)$ に対し

$$f(x) = \arctan\left(\frac{\pi}{2}x\right)$$

とおくと f は全単射



例2.9

$$\#\mathbb{R} = \#(\mathbb{R}\times\mathbb{R}) = \#(\mathbb{R}^2)$$

つまり) 濃度では次元を区別できない.

例2.10

$$\#\mathbb{R} \neq \# 2^{\mathbb{R}} = \#\{A \subset \mathbb{R}\}$$

一般に集合Xに対して. $\#X \neq \#2^X$

未解決問題 (連続体仮説)

例2.7により) $\aleph_0 \neq \aleph$ はわかっている.

では. 非可算集合 B で

$$\aleph_0 < \#B < \aleph$$

イミは未固

なるものはあるか? (「ない」が仮説)

結論 (1963, Cohen)

集合Bがあってもなくても困ることはない.

§§2.3 Bernsteinの定理

$A=\{a, b, c, d, e\}$. $B=\{1, 2, 3\}$

$f: B\to A$を

$f(1)=a$. $f(2)=b$, $f(3)=c$

とおくと. fは全射ではないが単射になる.

一般に有限集合 A, Bに対し

$\#A \leq \#B \Rightarrow {}^{\exists}$単射 $f: A\to B$が存在する.

<u>定義2.4</u>

X, Y: 集合

$\#X \leq \#Y \underset{\text{定義}}{\iff} {}^{\exists}$単射 $f: X\to Y$が存在する.

$\#X < \#Y \underset{\text{定義}}{\iff} \#X\leq\#Y$, $\#X \neq \#Y$.

$x, y, z\in\mathbb{R}$に対し.

$x\leq x$, 「$x\leq y, y\leq z \Rightarrow x\leq z$」

が成り立つ. これは濃度についても成り立つ.

命題2.2

X, Y, Zを集合とする

(1) $\#X \leq \#X$

(2) $\#X \leq \#Y,\ \#Y \leq \#Z \Rightarrow \#X \leq \#Z$.

証明

(1) $f: X \to X$を$x \in X$に対し$f(x) = x$で定めるとfは単射である.

(2) $\#X \leq \#Y,\ \#Y \leq \#Z$とすると

単射$f: X \to Y$. $g: Y \to Z$が存在する.

このとき$g \circ f: X \to Z$が単射となることを示せば$\#X \leq \#Y$がわかる.

$\forall x_1, x_2 \in X$に対し$g \circ f(x_1) = g \circ f(x_2)$ならば

$g(f(x_1)) = g(f(x_2))$よりgは単射だから

$f(x_1) = f(x_2)$. 次にfが単射より

$x_1 = x_2$も成り立つ. よって.

$g \circ f$は単射である

$\square$

④ $x, y \in \mathbb{R}$ に対し $x \leq y, y \leq x \Rightarrow x = y$ である.

これが濃度について成り立つかは自明ではない.

定理 2.1 (Bernstein の定理)

集合 X, Y に対し

$$\#X \leq \#Y, \ \#Y \leq \#X \Rightarrow \#X = \#Y$$

が成り立つ. つまり 単射 $f: X \to Y$ と $g: Y \to X$ が存在すれば 全単射 $F: X \to Y$ が存在する.

証明は難しい (内田 p.29)

命題 2.2 と定理 2.1 より

1. $\#X \leq \#X$ (X: 集合)
2. $\#X \leq \#Y, \#Y \leq \#X \Rightarrow \#X = \#Y$ (X, Y: 集合)
3. $\#X \leq \#Y, \#Y \leq \#Z \Rightarrow \#X \leq \#Z$ (X, Y, Z: 集合)

が成り立つ. この "$\leq$" を順序関係という

また $\mathcal{U}$ = 集合全体 (universe) として

$(\mathcal{U}, \leq)$ を半順序集合という.

実は$X, Y \in \mathfrak{U}$に対し

$$\#X \leq \#Y \quad \text{または} \quad \#Y \leq \#X \quad \text{—(*)}$$

のどちらかが成立する．半順序集合が(*)の性質を持つとき**全順序集合**という．

$(\mathbb{N}, \leq)$や$(\mathbb{R}, \leq)$は全順序集合である

例12.11

$\#\mathbb{Q} = \#\mathbb{N}$をBernsteinの定理を使って示す．

$f: \mathbb{N} \to \mathbb{Q}$を$f(n) = n \quad (n \in \mathbb{N})$により

定めればfは単射なので$\#\mathbb{N} \leq \#\mathbb{Q}$

次に$r \in \mathbb{Q}$を既約分数$r = \frac{p}{q}$とかき．

$g: \mathbb{Q} \to \mathbb{Z} \times \mathbb{Z}$を$g(r) := (p, q)$により

定義すると．これも単射になる（既約性より）

よって$\#\mathbb{Q} \leq \#(\mathbb{Z} \times \mathbb{Z})$だが

$$\#(\mathbb{Z} \times \mathbb{Z}) \underset{\#\mathbb{Z} = \#\mathbb{N}}{=} \#(\mathbb{N} \times \mathbb{N}) \underset{\text{例12.4}}{=} \#\mathbb{N}$$

より$\#\mathbb{Q} \leq \#\mathbb{N}$となる．

よってBernsteinの定理より$\#\mathbb{Q} = \#\mathbb{N}$である

□

§3 同値関係と商集合

$\triangle A$ と $\triangle B$ が合同 : $\triangle A \equiv \triangle B$.

この合同"$\equiv$"は次の性質をみたす.

(i) 同じ三角形は合同

$$\triangle A \equiv \triangle A \quad (\text{反射律})$$

(ii) $\triangle A$ と $\triangle B$ が合同なら $\triangle B$ と $\triangle A$ も合同

$$\triangle A \equiv \triangle B \implies \triangle B \equiv \triangle A \quad (\text{対称律})$$

(iii) $\triangle A$ と $\triangle B$ が合同, $\triangle B$ と $\triangle C$ が合同なら $\triangle A$ と $\triangle C$ も合同.

$$\triangle A \equiv \triangle B,\ \triangle B \equiv \triangle C \implies \triangle A \equiv \triangle C \quad (\text{推移律})$$

これにより. 三角形を分類できる. 物事を分類するには. 2つのものがみたすかみたさないかの規則を考えることが重要

§§3.1 同値関係

定義3.1 (同値関係)

X: 集合, $x, y \in X$ に対し.

$x \sim y$ か $x \not\sim y$ のどちらかがつねに成り立つ規則 "$\sim$" が与えられていて, 次をみたすとき. $\sim$ を同値関係という.

(1) 反射律 $x \sim x$ $(\forall x \in X)$

(2) 対称律 $x \sim y \Rightarrow y \sim x$ $(\forall x, y \in X)$

(3) 推移律 $x \sim y,\ y \sim z$

$\Rightarrow x \sim z$ $(\forall x, y, z \in X)$

例3.1

$\mathbb{R}$ 内の等号 "$=$" は 同値関係

不等号 "$\leqq$" は 同値関係でない

(対称律をみたさない)

例3.2

X を $\mathbb{R}^2$ 内の三角形全体 とする. このとき. 合同 "$\equiv$" や 相似 "$\backsim$" は 同値関係である.

例13.3

$p \in \mathbb{N}$ を素数とする. $x, y \in \mathbb{Z}$ に対し.

$$x \sim y \underset{\text{定義}}{\iff} {}^{\exists}k \in \mathbb{Z} \text{ s.t. } x - y = kp$$

$\iff$ $x-y$ が p でわりきれる.
(x, y を p でわったときの余りが同じ)

このとき. "$\sim$" は同値関係になる.

証明

(反射律) ${}^{\forall}x \in \mathbb{Z}$ に対し. $x - x = 0 = 0p$ より.
$x \sim x$ が成り立つ.

(対称律) ${}^{\forall}x, y \in \mathbb{Z}$ が $x \sim y$ をみたすならば
${}^{\exists}k \in \mathbb{Z}$ が存在して. $x - y = kp$. このとき.
$y - x = -kp = (-k)p$ であり $-k \in \mathbb{Z}$ より
$y \sim x$ が成り立つ.

(推移律) ${}^{\forall}x, y, z \in \mathbb{Z}$ が $x \sim y$, $y \sim z$ をみたす
ならば. ${}^{\exists}k_1, k_2 \in \mathbb{Z}$ が存在して

$$x - y = k_1 p, \quad y - z = k_2 p$$

となる. このとき.

$$x - z = (x - y) + (y - z) = k_1 p + k_2 p = (k_1 + k_2)p$$

であり. $k_1 + k_2 \in \mathbb{Z}$ だから. $x \sim z$ が成り立つ

□

この例3.3の同値関係は

$$x \equiv y \pmod p$$

でかくことが多い.

例3.4

$$\mathbb{R}[X] := \{a_0 + a_1X + \cdots + a_nX^n : n \in \mathbb{N}_0, a_0, \ldots, a_n \in \mathbb{R}\}$$

$$= \text{実数係数多項式全体}.$$

$f, g \in \mathbb{R}[X]$ に対し.

$$f \sim g \underset{\text{定義}}{\iff} \exists h \in \mathbb{R}[X] \text{ s.t. } f - g = (X^2+1)h$$

$$\iff f-g \text{ が } X^2+1 \text{ でわりきれる}.$$

とおく. このとき "$\sim$" は同値関係になる.

証明

推移律のみ示す. $f, g \in \mathbb{R}[X]$ が $f \sim g$ ならば. $\exists h \in \mathbb{R}[X]$ が存在して.

$f - g = (X^2+1)h$ をみたす. このとき.

$g - f = (X^2+1)(-h)$ となるが $-h \in \mathbb{R}[X]$

より $g \sim f$ が成り立つ $\square$.

§§3.2 同値類と代表元

$n, m \in \mathbb{Z}$ に対し

$n \equiv m \pmod 3 \iff n-m$ が 3 で割り切れる

$\iff n, m$ を 3 で割った余りは同じ.

よって

$$\cdots \equiv -8 \equiv -5 \equiv -2 \equiv 1 \equiv 4 \equiv 7 \equiv \cdots \pmod 3$$

これらをあつめて, 新しい集合を作る.

定義 3.2 (同値類, 代表元)

X: 集合, $\sim$: 同値関係, $x \in X$.

$$C(x) := \{y \in X : x \sim y\}$$

とおく. $C(x)$ を x の**同値類**, x を**代表元**という.

注意 3.1

記号 $C(x)$ は内田 (参考書) に従っている.

同値類に対する共通の記号はなさそう.

例3.5

$\mathbb{Z}$ 上の同値関係 $\equiv \pmod 3$ に対し

$$C(1) = \{n \in \mathbb{Z} : 1 \equiv n \pmod 3\}$$
$$= \{\cdots, -5, -2, 1, 4, 7, 10, \cdots\}$$
$$= \{3m+1 : m \in \mathbb{Z}\}$$

$$C(2) = \{n \in \mathbb{Z} : 2 \equiv n \pmod 3\}$$
$$= \{\cdots, -7, -4, -1, 2, 5, 8, \cdots\}$$
$$= \{3m+2 : m \in \mathbb{Z}\}$$

$$C(3) = \{n \in \mathbb{Z} : 3 \equiv n \pmod 3\}$$
$$= \{3m : m \in \mathbb{Z}\}$$

ところで $0 \equiv 3 \pmod 3$ より $0 \in C(3)$ だが.

$$C(0) = \{n \in \mathbb{Z} : 0 \equiv n \pmod 3\}$$
$$= \{n \in \mathbb{Z} : \exists k \in \mathbb{Z} \text{ s.t. } \underline{n-0 = 3k}\}$$
$$\Updownarrow$$
$$n-3 = 3(k-1)$$
$$= \{n \in \mathbb{Z} : 3 \equiv n \pmod 3\} = C(3)$$

また. $2 \not\equiv 1 \pmod 3$ より $2 \notin C(1)$ だが.

このとき. $C(1) \cap C(2) = \phi$ となる

∵ もし $n \in C(1) \cap C(2)$ ならば

$\exists k_1, k_2 \in \mathbb{Z}$ s.t. $n = 3k_1 + 1 = 3k_2 + 2$.

従って $3(k_1 - k_2) = 1$ となるが、左辺は3でわり切れ、右辺は3で割り切れないので矛盾 □.

より一般に次が成り立つ.

定理 3.1

X：集合、$\sim$：同値関係、$x, y \in X$.

(1) $x \sim y \Longrightarrow C(x) = C(y)$

(2) $x \nsim y \Longrightarrow C(x) \cap C(y) = \phi$.

証明

1. $x \sim y$ として $C(x) = C(y)$ を示す.

$\forall z \in C(x)$ に対し、$z \sim x$. 仮定より $x \sim y$ だから推移律と対称律により

$z \sim x \sim y$ i.e. $z \sim y$.

従って $z \in C(y)$ より $C(x) \subset C(y)$.

$C(y) \subset C(x)$ も同様.

2. $x \nsim y$ として $C(x) \cap C(y) = \phi$ を背理法で示す.

もし $z \in C(x) \cap C(y)$ が存在すると. $x \in C(x)$ かつ $x \in C(y)$ より $z \sim x$ かつ $z \sim y$ が成り立つ.
よって 推移律と対称律より

$$x \sim z \sim y \quad \text{i.e.} \quad x \sim y$$

となり $x \not\sim y$ に矛盾する $\square$.

※定理3.1の意味は次の節で説明する.

例3.6

$\mathbb{R}[X]$ に対し 例3.4 の同値関係 $\sim$ を考える.
$X^2+X+1 \in \mathbb{R}[X]$ に対し $X \sim X^2+X+1$ だから

$$C(X^2+X+1) = C(X).$$

$X^2+2 \in \mathbb{R}[X]$ に対し $X^2+2 \sim 1$ だから

$$C(X^2+2) = C(1)$$

一般に $f \in \mathbb{R}[X]$ に対し. ${}^{\exists}aX+b \in \mathbb{R}[X]$ が存在して.

$$f \sim aX+b$$

となることが知られている. (環論や単因子論 割り算と約数の話)

とくに. 定理3.1 から $f \in \mathbb{R}[X]$ の同値類 $C(f)$ の代表元として. 1次多項式 $aX+b \in \mathbb{R}[X]$ がとれて

$C(f) = C(aX+b)$ とできる.

§§3.3 商集合

$\mathbb{Z}$ 上の同値関係 $\equiv \pmod 3$ に対し

$$\mathbb{Z} = C(0) \cup C(1) \cup C(2) \qquad (*)$$

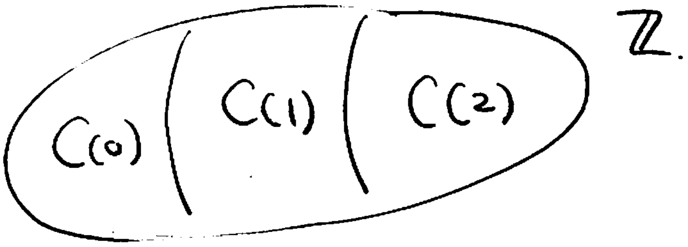
が成り立つ.

($\because$ 整数を3でわると. 余りは0か1か2)

さらに

$$C(n) \cap C(m) = \phi \quad \begin{pmatrix} n, m = 0, 1, 2 \\ n \neq m \end{pmatrix}$$

となるから $(*)$ の右辺は $\mathbb{Z}$ を3つにわけている



そこで

$$\mathbb{Z}_3 := \{ C(0), C(1), C(2) \}$$

と定める. 同値類を集合の元とみて.

新しい集合をつくることができる.

定義3.3（商集合）

X: 集合, $\sim$: 同値関係

$$X/\sim \; := \{ C(x) : x \in X \}$$

と定義する. $X/\sim$ を X の $\sim$ による**商集合**という.

$\mathbb{Z}_3 = \mathbb{Z}/_{\equiv (\mathrm{mod}\, 3)}$ である. 実際,

$$C(1) = C(4) = C(7) = \cdots$$

だったことに注意する.

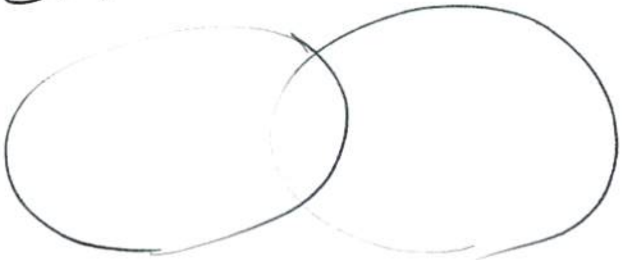
⑪ 定理3.1 の意味.

$$x \sim y \Rightarrow C(x) = C(y)$$
$$x \not\sim y \Rightarrow C(x) \cap C(y) = \phi$$

$\therefore$ $C(x) \neq C(y)$ かつ $C(x) \cap C(y) \neq \phi$

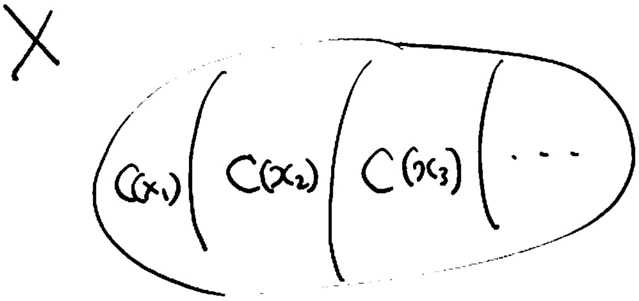
ということはない.

$C(x)$　　　　$C(y)$



こういうこと
はない.

よって $X/\sim$ は X を互いに交わらない部分集合に分割している



例3.7

$\mathbb{Z}$ 上の同値関係 $\equiv \pmod 5$ に対し、

$$\mathbb{Z}_5 = \mathbb{Z}/\equiv \pmod 5 = \{C(n) : n \in \mathbb{Z}\}$$
$$= \{C(0), C(1), C(2), C(3), C(4)\}$$
$$= \{C(5), C(6), C(7), C(8), C(9)\}$$
$$= \{C(0), \cdots, C(9), C(10)\}$$

↑ $C(0) = C(5) = C(10)$ なので、同じ元がいくつもある。

$\phi : \mathbb{Z} \to \mathbb{Z}_5$ を $n \in \mathbb{Z}$ に対し

$$\phi(n) = C(n)$$

とおくと、ϕ は全射になる。

$\because$ $C(n) \in \mathbb{Z}_5$ に対し、$\phi(n) = C(n)$ である ◻

定義3.4 (射影)

X: 集合, $\sim$: 同値関係

$$\begin{array}{rccc} \phi : & X & \longrightarrow & X/\sim \\ & \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ & x & \longmapsto & C(x) \end{array}$$

を X から $X/\sim$ への自然な射影という
(Canonical projection)

例3.8

$\mathbb{R}[X]$ に対し、例3.4の同値関係 $\sim$ を考える.

このとき.

$$\mathbb{R}[X]/\sim = \{ C(f) : f \in \mathbb{R}[X] \}$$
$$= \{ C(a+bX) : a, b \in \mathbb{R} \}$$

$f \sim a+bX$ となる $a, b \in \mathbb{R}$ がある.

この $\sim$ は X^2+1 での余りが等しいという〃

だったので $\mathbb{R}[X]/(X^2+1) := \mathbb{R}[X]/\sim$ とかく.

$\mathbb{R}[X]$ から $\mathbb{R}[X]/(X^2+1)$ への自然な射影 ϕ は.

$f \in \mathbb{R}[X]$ に対し

$$\phi(f) = C(f) = C(a+bX) \qquad (f \sim a+bX)$$

となる.

§§3.4. 同値類による計算と well-defined.

$\mathbb{Z}_3 = \{C(0), C(1), C(2)\}$ であった.

問い 3でわると1余る数をa. 2余る数をbとすると

$a+b$を3でわった余りは?

答 $\exists n, m \in \mathbb{N}$ s.t. $a = 3n+1$, $b = 3m+2$ と

できるから

$$a+b = (3n+1)+(3m+2) = 3n+3m+3$$
$$= 3(n+m+1)$$

より. $a+b$を3でわると余りは0 .

この計算の key point は $1+2=3$ が3でわりきれること

(余りだけを注意すればよい). だから

$$C(1)+C(2) := C(3) = C(0)$$

と定義すればよいのでは?

困ること

$C(1) = C(4)$, $C(2) = C(5)$.

$$C(1)+C(2) = C(1+2) = C(3)$$
$$C(4)+C(5) = C(4+5) = C(9)$$

このとき. $C(3) = C(9)$ か? 他の場合は?

つまり. 代表元をかえたときに. でてくる答えは

同じものか?

〈問題を整理する〉

$$\left.\begin{array}{l} a \equiv a' \pmod 3 \quad \text{i.e.} \quad C(a) = C(a') \\ b \equiv b' \pmod 3 \quad \text{i.e.} \quad C(b) = C(b') \\ \Longrightarrow a+b \equiv a'+b' \pmod 3 \\ \qquad \text{i.e.} \quad C(a+b) = C(a'+b') \end{array}\right\} \quad (*)$$

は成り立つか？

<u>証明</u>

$a \equiv a' \pmod 3$ より $\exists n \in \mathbb{N}$ s.t.

$a - a' = 3n$,

$b \equiv b' \pmod 3$ より $\exists m \in \mathbb{N}$ s.t.

$b - b' = 3m$ とできるから

$$(a+b) - (a'+b') = (a-a') + (b-b') = 3n + 3m = 3(n+m)$$

となる．よって $a+b \equiv a'+b' \pmod 3$ □．

このことから $C(a), C(b) \in \mathbb{Z}_3$ に対し

$$C(a) + C(b) := C(a+b) \qquad (**)$$

と定義できる．

このとき．(**)の定義は．(*)から a．b のとり方に依らずに定まる．このとき (**)の定義は well-defined であるという．

いい和訳はなさそう．

例3.7

$C(a), C(b) \in \mathbb{Z}_5$ に対し．$C(a)$と$C(b)$ のかけ算を．

$$C(a) \cdot C(b) = C(ab)$$

で定義したとき．well-defined であることを示す．

すなわち．

$$a \equiv a' \pmod 5, \quad b \equiv b' \pmod 5$$

$$\Longrightarrow \quad ab \equiv a'b' \pmod 5$$

を示す．

$a \equiv a', \ b \equiv b' \pmod 5$ より

$\exists n, m \in \mathbb{N}$ s.t.

$$a - a' = 5n \quad \text{i.e.} \quad a = a' + 5n$$

$$b - b' = 5m \quad \text{i.e.} \quad b = b' + 5m$$

とできる．従って

$$
\begin{aligned}
ab &= (a'+5n)(b'+5m) \\
&= a'b' + 5a'm + 5b'n + 25mn. \\
&= a'b' + 5(a'm + b'n + 5mn)
\end{aligned}
$$

i.e.

$$ab - a'b' = 5(a'm + b'n + 5mn)$$

より) $ab \equiv a'b' \pmod 5$ となる.

一般に素数 p と $C(a), C(b) \in \mathbb{Z}_p$ に対し

$$
\begin{aligned}
C(a) + C(b) &:= C(a+b) \\
C(a) \cdot C(b) &:= C(ab)
\end{aligned}
$$

とおくと. この定義は well-defined になる

(実は p は素数でなくてもよい). p が素数のとき.

$C(a) \neq C(0)$. $C(b) \neq C(0)$ ならば

$C(a) \cdot C(b) \neq C(0)$ がわかる. いいかえると

$C(a) \cdot C(b) = C(0) \Rightarrow C(a) = 0$ または $C(b) = 0$

となる. p が素数でないときは. この性質は成り立たない.

§§ 3.5 応用．$\mathbb{C}$ や $\mathbb{R}$ の構成

まとめ

(1) $\mathbb{R}[X]$ から $\mathbb{C}$ が作れる

(2) 有理 Cauchy 列から $\mathbb{R}$ が作れる．

〈$\mathbb{R}[X]$ から $\mathbb{C}$ を作る〉

$f \in \mathbb{R}[X]$ に対し．

$$\bar{f} := C(f) = \{h \in \mathbb{R}[X] : f-h \text{ は } (X^2+1) \text{ でわりきれる}\}$$

とおく．例3.4の同値関係 $\sim$ を考える．

1. $f, g \in \mathbb{R}[X]$ に対し．

$$\bar{f} + \bar{g} := \overline{f+g}$$

と定義すると．この定義は well-defined（レポート）

2. $f, g \in \mathbb{R}[X]$ に対し．

$$\bar{f} \cdot \bar{g} := \overline{fg}$$

と定義すると．この定義は well-defined（レポート）

3. $a, b, c, d \in \mathbb{R}$ に対し

$f(X) = a + bX$, $g(X) = c + dX$

とおく. このとき.

$$f(X) + g(X) = (a + bX) + (c + dX)$$
$$= (a+c) + (b+d)X$$

より

$$\overline{f} + \overline{g} = \overline{(a+c) + (b+d)X}$$

ところで. $i = \sqrt{-1}$ として $a+bi$, $c+di$ に対し

$$(a+bi) + (c+di) = (a+c) + (b+d)i$$

となるから. $\overline{f} + \overline{g}$ によくにている

($\overline{f} + \overline{g}$ で横線を消して $X = i$ としてみよ).

4. 3. と同じ記号の下で $\overline{f} \cdot \overline{g}$ を計算する.

$$f(X)g(X) = (a + bX)(c + dX)$$
$$= ac + (ad + bc)X + bdX^2$$
$$= (ac - bd) + (ad + bc)X$$
$$+ bd(X^2 + 1)$$

これを無理矢理出してみる.
((X^2+1) でわったと考えてもよい)

より

$$\overline{f} \cdot \overline{g} = \overline{(ac - bd) + (ad + bc)X}$$

ところで

$$(a+bi)(c+di) = ac + (ad+bd)i + bdi^2$$
$$= (ac-bd) + (ad+bd)i$$

より $\overline{f}\cdot\overline{g}$ によくにている

3. 4. の主張していることは

「$\mathbb{C}$ 上の計算(たし算, かけ算) と $\mathbb{R}[X]/(X^2+1)$ 上の計算
専門用語で演算という
(たし算, かけ算)は同じ」である

さらに写像

$$\begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{R}[X]/(X^2+1) \\ \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ a+bi & \longmapsto & \overline{a+bX} \end{array}$$

は全単射となる(各自) このことから

$\mathbb{C}$ と $\mathbb{R}[X]/(X^2+1)$ は同じものとみることができる

$\mathbb{R}[X]/(X^2+1)$ は $\mathbb{R}$ しか使っていないから

このことにより $\mathbb{R}$ から $\mathbb{C}$ が作れたことになる

これらの話題は代数学(群,環,体)を勉強すると,もっとすっきりした形で説明することができる.

〈$\mathbb{Q}$ から $\mathbb{R}$ を作る〉

$$X = \{ \{a_n\}_{n=1}^{\infty} : \text{Cauchy列},\ a_n \in \mathbb{Q}\ (^\forall n \in \mathbb{N}) \}.$$

とおく.つまり X は有理 Cauchy列全体

$\{a_n\}_{n=1}^{\infty}$ が Cauchy列

$$\underset{\text{定義}}{\iff}\ ^\forall \varepsilon > 0,\ ^\exists N \in \mathbb{N} \text{ s.t. } ^\forall n, m \in \mathbb{N}$$
$$n, m \geq N \Rightarrow |a_n - a_m| < \varepsilon$$

困ったこと

Cauchy列 $\Rightarrow$ 収束列

はどうやって示せばよいか?

例 $\mathbb{Q}$ では成立しない

$$\begin{array}{ccccccccc} 1, & 1.4, & 1.41, & 1.414, & \cdots, & \to & \sqrt{2} \\ \cap & \cap & \cap & \cap & & & \not\cap \\ \mathbb{Q} & \mathbb{Q} & \mathbb{Q} & \mathbb{Q} & & & \mathbb{Q} \end{array}$$

$\mathbb{Q}$ と $\mathbb{R}$ がどう違うかはっきりさせる必要がある.

$\{a_n\}_{n=1}^{\infty}, \{b_n\}_{n=1}^{\infty} \in X$ が $\{a_n\}_{n=1}^{\infty} \sim \{b_n\}_{n=1}^{\infty}$

$\overset{\text{定義}}{\iff} \lim_{n\to\infty}(a_n - b_n) = 0$ （これは $\mathbb{Q}$ の範囲で定義できる）

$\sim$ は同値関係となる（レポート）. このとき.

商集合 $X/\sim$ を $\mathbb{Q}$ の完備化という. そして.

$X/\sim$ を $\mathbb{R}$ と定義する

理由

$a_1 = 1,\ a_2 = 1.4,\ a_3 = 1.41,\ a_4 = 1.414,\ \cdots$

$\Longrightarrow \sqrt{2} = \lim_{n\to\infty} a_n$.

このとき. $\sqrt{2} = C(\{a_n\}_{n=1}^{\infty})$ (in $X/\sim$)

とみなす.

$b_1 = 1.\ b_2 = 1.41,\ b_3 = 1.4142,\ b_4 = 1.414213,\ \cdots$

としても $\sqrt{2} = \lim_{n\to\infty} b_n$ だから $\sqrt{2} = C(\{b_n\}_{n=1}^{\infty})$.

このとき.

$$\lim_{n\to\infty}(a_n - b_n) = \sqrt{2} - \sqrt{2} = 0$$

より $\{a_n\}_{n=1}^{\infty} \sim \{b_n\}_{n=1}^{\infty}$ だから

$$\sqrt{2} = C(\{a_n\}_{n=1}^{\infty}) = C(\{b_n\}_{n=1}^{\infty}).$$

定理

$\mathbb{R}$ 上の Cauchy 列は収束列となる.

§4 選択公理とその周辺

$\{A_\lambda\}_{\lambda\in\Lambda}$：集合族，$\Lambda$：添字集合

（わかりにくければ $\Lambda=\mathbb{N}$ としてよい）

$$\prod_{\lambda\in\Lambda} A_\lambda = \{f:\Lambda\to\bigcup_{\lambda\in\Lambda}A_\lambda,\ {}^\forall\lambda\in\Lambda \text{ に対し } f(\lambda)\in A_\lambda\}$$

（$\Lambda=\mathbb{N}$ のときは $a_1\in A_1$, $a_2\in A_2$, $a_3\in A_3$, … に対し
$(a_1, a_2, a_3, \dots)\in\prod_{n\in\mathbb{N}}A_n = A_1\times A_2\times A_3\times\cdots$ と思ってよい）

選択公理

$${}^\forall\lambda\in\Lambda \text{ に対し } A_\lambda\neq\phi \Rightarrow \prod_{\lambda\in\Lambda}A_\lambda\neq\phi$$

定理4.1

次は同値

(1) 選択公理が成り立つ

(2) 帰納的半順序集合は極大元を持つ（Zornの補題）

(3) すべての集合は，ある半順序を考えることで整列集合とできる（整列可能定理）

この節の目標

Zornの補題、整列可能定理の主張を理解する。

§§4.1 Zornの補題

〈順序関係〉

定義4.1 (半順序集合)

X：集合、$x, y \in X$ に対し、$x \leq y$ または $x \not\leq y$ のどちらかが成り立つ規則"$\leq$"が与えられていて、次をみたすとき"$\leq$"を**半順序**といい、$(X, \leq)$ を**半順序集合**という：

(1) (反射律) $x \leq x$ $(\forall x \in X)$

(2) (反対称律) $x \leq y \Rightarrow y \leq x$ $(\forall x, y \in X)$

(3) (推移律) $x \leq y,\ y \leq z \Rightarrow x \leq z$ $(\forall x, y, z \in X)$

例4.1

$(\mathbb{R}, \leq)$ は半順序集合。

例4.2

$\mathfrak{U}$ を集合全体としたとき、

$(\mathfrak{U}, \subset)$ は半順序集合

例4.3

$\leq$ を $\mathbb{R}$ の不等式としたとき、$(\mathbb{C}, \leq)$ は半順序集合ではない（$i \leq 1$ などの意味がない）

定義4.2（全順序集合）

$(X, \leq)$：半順序集合が**全順序集合**

$\underset{\text{定義}}{\Longleftrightarrow}$ $\forall x, y \in X$ に対し $x \leq y$ または $y \leq x$ のどちらかが成り立つ.

例4.4

$(\mathbb{R}, \leq)$ は全順序集合.

例4.5

$(\mathfrak{U}, \subset)$ は全順序集合ではない

（ $A=\{1,2,3\}$, $B=\{3,4\}$ とすると $A \not\subset B$ かつ $B \not\subset A$ ）

定義4.3（上界、下界、上限、下限）

$(X, \leq)$：半順序集合，$A \subset X$.

◎ $y \in X$ が A の**上界**（resp. **下界**）

$\underset{\text{定義}}{\Longleftrightarrow}$ $\forall a \in A$ に対し $a \leq y$ (resp. $y \leq a$)

◎ $y \in X$ が A の最大元 (resp. 最小元)

$\underset{\text{定義}}{\Longleftrightarrow}$ 「$y \in A$」かつ「$^\forall a \in A$ に対し $a \leq y$ (resp. $y \leq a$)」

このとき $y = \max A$ (resp. $y = \min A$) とかく.

◎ $y \in X$ が A の上限 (resp. 下限)

$\underset{\text{定義}}{\Longleftrightarrow}$ $y = {}^\exists \min \{x \in X : x$ は A の上界$\}$

(resp. $y = {}^\exists \max \{x \in X : x$ は A の下界$\}$)

例 4.6

$(\mathbb{R}, \leq)$, $[0,1) \subset \mathbb{R}$ に対し

$\{x \in \mathbb{R} : x$ は $[0,1)$ の上界$\} = \{x \in \mathbb{R} : {}^\forall y \in [0,1), y \leq x\}$

$= [1, \infty)$

$\{x \in \mathbb{R} : x$ は $[0,1)$ の下界$\} = \{x \in \mathbb{R} : {}^\forall y \in [0,1), x \leq y\}$

$= (-\infty, 0]$

よって

$\sup [0,1) = \min [1, \infty) = 1$

$\inf [0,1) = \max (-\infty, 0] = 0$

〈Zornの補題〉

定義4.4 (帰納的)

$(X, \leq)$：半順序集合が帰納的

$\underset{\text{定義}}{\Longleftrightarrow}$ $^\forall Y \subset X$ に対し

$(Y, \leq)$：全順序集合 $\Rightarrow$ Yは上界を持つ.

(1) 直観的には、どんな全順序部分集合の元よりも大きな元があるということ

定義4.5 (極大元)

$(X, \leq)$：半順序集合

$a \in X$が極大元

$\underset{\text{定義}}{\Longleftrightarrow}$ $^\nexists x \in X$ s.t. $a \leq x$ かつ $a \neq x$.

(1) 直観的には、$a < x$となる$x \in X$はないということ.

定理4.2 (Zornの補題)

$(X, \leq)$：帰納的半順序集合

$\Rightarrow$ $^\exists a \in X$ 極大元.

注意 4.1

Zornの補題は 存在を証明するときに使うことが多い.

§§4.2 整列可能定理

定義 4.6 (整列集合)

$(X, \leq)$:半順序集合 が **整列集合**

$\underset{\text{定義}}{\iff}$ $^{\forall}A \subset X$ に対し $^{\exists}\min A$.

① 直観的には $A \subset X$ が小さい順に並べられるということ

$a_1 = \min A$, $a_2 = \min(A \setminus \{a_1\})$, $a_3 = \min(A \setminus \{a_1, a_2\})$, …

とすれば $A = \{a_1, a_2, a_3, \cdots\}$ と小さい順に並べられる.

命題 4.1

$(X, \leq)$:整列集合 $\Longrightarrow$ $(X, \leq)$:全順序集合

証明

$^{\forall}x, y \in X$ に対し $A = \{x, y\} \subset X$ とすると. $(X, \leq)$は整列集合だから $\min A = \min\{x, y\}$ がある.

$x = \min A$ ならば $y \in A$に対し $x \leq y$.

$y = \min A$ ならば $x \in A$ に対し $y \leq x$

より, $x \leq y$ か $y \leq x$ のどちらかが成り立つから $(X, \leq)$は全順序集合である $\square$

よって命題4.1より

$(X, \leq)$：整列集合 $\Rightarrow$ $(X, \leq)$：全順序集合

$\Rightarrow$ $(X, \leq)$：半順序集合

例4.7

$(\mathbb{N}, \leq)$は整列集合（$\forall A \subset \mathbb{N}$に対し、最小元はある）

例4.8

$(\mathbb{Z}, \leq)$, $(\mathbb{Q}, \leq)$, $(\mathbb{R}, \leq)$は整列集合でない

（たとえば $(-\infty, 0] \subset \mathbb{R}$ に最小元は存在しない）

定理4.3（整列可能定理）

X：集合（なんでもよい）

$\Rightarrow$ あるX上の半順序"$\leq$"が存在して

$(X, \leq)$は整列集合にできる。

① たとえば、$\mathbb{C}$には$\mathbb{R}$の不等式による順序は定義できないが、別の整列集合となる順序"$\leq$"があることを定理4.3は主張している。ただし、その順序が役に立つかは別の問題である。