可換代数への道標 集合論 ver 1.0

@Akari0koutya

March 12, 2022

Remark

- 数 1,A,2,B で学んだことは仮定する
  (沢山出てくるわけではないから安心して欲しい).
- シリーズの目標は可換代数まで.

Definition 1.1

有限集合 A に対し, A の元の個数を A の**濃度** (*cardinality*) といい, $|A|$ で表す.

無限集合に対しても写像の概念を用いて濃度の概念を与えることができ, その大小を比較することができるが, 喩え導入しなくても今後の章において実害を被ることは恐らくなく, また, 私はあまり詳しくないのでここでは省くことにする. 詳しくは適当な集合論の本を参照のこと.
興味を引くようなことを述べるとするなら, 自然数集合 $\mathbb{N}$ の濃度 $\aleph_0$ を基準に考えるとすると, $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ の濃度は等しく $\aleph_0$ となり **可算無限集合** (countably infinite set) という. 対して, $\mathbb{R}, \mathbb{C}$ の濃度は $2^{\aleph_0}(=\aleph_1)$ と表され, これは $\aleph_0$ より真に大きく, **非可算無限集合** という.

Remark

すべての集合の集合など, 大きすぎる集合は考えないこととする. 主に, カントールのパラドックスを回避し, ZF 公理系を満足させるためである. 詳しくは公理的集合論を勉強されたい.

Definition 1.1

有限集合 A に対し，A の元の個数を A の**濃度** (*cardinality*) といい，$|A|$ で表す．

無限集合に対しても写像の概念を用いて濃度の概念を与えることができ，その大小を比較することができるが，喩え導入しなくても今後の章において実害を被ることは恐らくなく，また，私はあまり詳しくないのでここでは省くことにする．詳しくは適当な集合論の本を参照のこと．

興味を引くようなことを述べるとするなら，自然数集合 $\mathbb{N}$ の濃度 $\aleph_0$ を基準に考えるとすると，$\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ の濃度は等しく $\aleph_0$ となり **可算無限集合** (countably infinite set) という．対して，$\mathbb{R}, \mathbb{C}$ の濃度は $2^{\aleph_0} (= \aleph_1)$ と表され，これは $\aleph_0$ より真に大きく，**非可算無限集合** という．

Remark

すべての集合の集合など，大きすぎる集合は考えないこととする．主に，カントールのパラドックスを回避し，ZF 公理系を満足させるためである．詳しくは公理的集合論を勉強されたい．

Definition 1.1

有限集合 A に対し, A の元の個数を A の**濃度** (*cardinality*) といい, $|A|$ で表す.

無限集合に対しても写像の概念を用いて濃度の概念を与えることができ, その大小を比較することができるが, 喩え導入しなくても今後の章において実害を被ることは恐らくなく, また, 私はあまり詳しくないのでここでは省くことにする. 詳しくは適当な集合論の本を参照のこと.
興味を引くようなことを述べるとするなら, 自然数集合 $\mathbb{N}$ の濃度 $\aleph_0$ を基準に考えるとすると, $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ の濃度は等しく $\aleph_0$ となり **可算無限集合** (countably infinite set) という. 対して, $\mathbb{R}, \mathbb{C}$ の濃度は $2^{\aleph_0} (= \aleph_1)$ と表され, これは $\aleph_0$ より真に大きく, **非可算無限集合** という.

Remark

すべての集合の集合など, 大きすぎる集合は考えないこととする. 主に, カントールのパラドックスを回避し, ZF 公理系を満足させるためである. 詳しくは公理的集合論を勉強されたい.

Definition 1.1

有限集合 A に対し, A の元の個数を A の**濃度** (*cardinality*) といい, $|A|$ で表す.

無限集合に対しても写像の概念を用いて濃度の概念を与えることができ, その大小を比較することができるが, 喩え導入しなくても今後の章において実害を被ることは恐らくなく, また, 私はあまり詳しくないのでここでは省くことにする. 詳しくは適当な集合論の本を参照のこと.
興味を引くようなことを述べるとするなら, 自然数集合 $\mathbb{N}$ の濃度 $\aleph_0$ を基準に考えるとすると, $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ の濃度は等しく $\aleph_0$ となり **可算無限集合** (countably infinite set) という. 対して, $\mathbb{R}, \mathbb{C}$ の濃度は $2^{\aleph_0}(=\aleph_1)$ と表され, これは $\aleph_0$ より真に大きく, **非可算無限集合** という.

Remark

すべての集合の集合など, 大きすぎる集合は考えないこととする. 主に, カントールのパラドックスを回避し, ZF 公理系を満足させるためである. 詳しくは公理的集合論を勉強されたい.

Definition 1.2 (直積)

有限個の集合，とくに n 個の $A_1, A_2, \ldots, A_n$ に対して，各 A_i の各元 a_i の組 $(a_1, a_2, \ldots, a_n)$ 全体の集合を集合 $A_1, A_2, \ldots, A_n$ の **直積** (*direct product*) という．すなわち，

$$\begin{aligned}\prod_i^n A_i &= A_1 \times A_2 \times \cdots \times A_n \\ &:= \{(a_1, a_2, \ldots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\}.\end{aligned}$$

また，n 個の直積 $\underbrace{A \times A \times \cdots \times A}_{n}$ は A^n で表し，$A^0 = \{()\}$ となる．

Example 1.3

日頃何気なく使うであろう座標での直線, 平面, 空間はすべて $\mathbb{R}$ の直積により記述可能である.

- 直線 : $\mathbb{R} = \{x \mid x \in \mathbb{R}\}$.
- 平面 : $\mathbb{R}^2 = \{(x, y) \mid x, y \in \mathbb{R}\}$.
- 空間 : $\mathbb{R}^3 = \{(x, y, z) \mid x, y, z \in \mathbb{R}\}$.

であり, 一般に n 次元空間 $\mathbb{R}^n$ を考えられる.

Example 1.4

複素 $\mathbb{C}$ は $\mathbb{R} \times \mathbb{R}$ からの関数として $\mathbb{R} \times \mathbb{R} \ni (x, y) \mapsto x + yi = \alpha \in \mathbb{C}$ のように記述することで, $\{1, i\}$ を基底に持つ平面上の点 α の集合と考えることができる. これを複素平面というのであった.

Example 1.3

日頃何気なく使うであろう座標での直線, 平面, 空間はすべて $\mathbb{R}$ の直積により記述可能である.

- 直線 : $\mathbb{R} = \{x \mid x \in \mathbb{R}\}$.
- 平面 : $\mathbb{R}^2 = \{(x, y) \mid x, y \in \mathbb{R}\}$.
- 空間 : $\mathbb{R}^3 = \{(x, y, z) \mid x, y, z \in \mathbb{R}\}$.

であり, 一般に n 次元空間 $\mathbb{R}^n$ を考えられる.

Example 1.4

複素 $\mathbb{C}$ は $\mathbb{R} \times \mathbb{R}$ からの関数として $\mathbb{R} \times \mathbb{R} \ni (x, y) \mapsto x + yi = \alpha \in \mathbb{C}$ のように記述することで, $\{1, i\}$ を基底に持つ平面上の点 α の集合と考えることができる. これを複素平面というのであった.

中学, 高校数学では, $f(x)=x^3-7$ であったり, $g(x)=e^x+x^3-5$, $h(x)=\frac{4x+1}{2(x+1)(x^2+3)}$, などなど, 多くの関数を扱ってきた. これらを見通しよく定義する.

Definition 2.1 (写像)

二つの集合 A, B に対し, A から B への**写像** (*map, function*) とは,A の各元に対して B のただ一つの元を定めるものをいう. そして, これを

$$f : A \to B$$

で表す. 元の対応を表す時,

$$f : a \mapsto f(a)$$

を用いる.

Definition 2.2

集合 A, B に対して,A から B への写像全体 (後述の圏においては射全体) の集合を $\mathrm{Hom}(A, B)$ で表す.

中学, 高校数学では, $f(x)=x^3-7$ であったり, $g(x)=e^x+x^3-5$, $h(x)=\frac{4x+1}{2(x+1)(x^2+3)}$, などなど, 多くの関数を扱ってきた. これらを見通しよく定義する.

Definition 2.1 (写像)

二つの集合 A, B に対し, A から B への**写像** (*map, function*) とは,A の各元に対して B のただ一つの元を定めるものをいう. そして, これを

$$f : A \to B$$

で表す. 元の対応を表す時,

$$f : a \mapsto f(a)$$

を用いる.

Definition 2.2

集合 A, B に対して,A から B への写像全体 (後述の圏においては射全体) の集合を $\mathrm{Hom}(A, B)$ で表す.

Definition 2.3 (写像の合成)

集合 A, B, C に対し，$f \in \mathrm{Hom}(A, B), g \in \mathrm{Hom}(B, C)$ をとる．このとき，二つの写像を続けて適用したもの $g \circ f : A \to C$ を f と g の **合成写像** という．

$$
\begin{array}{ccc}
\mathrm{Hom}(A, B) \times \mathrm{Hom}(B, C) & \longrightarrow & \mathrm{Hom}(A, C) \\
\rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\
(f, g) & \longmapsto & g \circ f
\end{array}
$$

Remark

$h \in \mathrm{Hom}(A, C)$ が $g \circ f$ と一致する時，これを絵で表すと下図のようになり，これを **図式** (diagram) という．特に，このように経路によらず写像が一致するとき，図式は**可換である** (commutative) といい，$\circlearrowright$ は絵が可換であることを示す．

$$
\begin{tikzcd}
A \arrow[r, "f"] \arrow[dr, "h"'] & B \arrow[d, "g"] \arrow[dl, phantom, "\circlearrowright"] \\
 & C
\end{tikzcd}
$$

Proposition 2.4 (結合律)

$f \in \mathrm{Hom}(A, B), g \in \mathrm{Hom}(B, C), h \in \mathrm{Hom}(C, D)$ に対して, 次が成り立つ.

$$h \circ (g \circ f) = (h \circ g) \circ f$$

Proof. $x \in A$ に対して,

$$\begin{aligned}(h \circ (g \circ f))(x) = h((g \circ f)(x)) &= h(g(f(x))) \\ &= (h \circ g)(f(x)) = ((h \circ g) \circ f)(x)\end{aligned}$$

が成り立つ. □

$$\begin{tikzcd}
A \arrow[rr, "h\circ(g\circ f)=(h\circ g)\circ f"] \arrow[d, "f"'] \arrow[drr, "g\circ f"] & & D \\
B \arrow[rr, "g"] \arrow[urr, "h\circ g"'] & & C \arrow[u, "h"']
\end{tikzcd}$$

Proposition 2.4 (結合律)

$f \in \mathrm{Hom}(A,B), g \in \mathrm{Hom}(B,C), h \in \mathrm{Hom}(C,D)$ に対して，次が成り立つ．

$$h \circ (g \circ f) = (h \circ g) \circ f$$

Proof. $x \in A$ に対して，

$$\begin{aligned}(h \circ (g \circ f))(x) &= h((g \circ f)(x)) = h(g(f(x))) \\ &= (h \circ g)(f(x)) = ((h \circ g) \circ f)(x)\end{aligned}$$

が成り立つ． □

$$\begin{tikzcd} A \arrow[r, "h\circ(g\circ f)=(h\circ g)\circ f"] \arrow[d, "f"'] \arrow[dr, "g\circ f"] & D \\ B \arrow[r, "g"] \arrow[ur, "h\circ g"'] & C \arrow[u, "h"'] \end{tikzcd}$$

Definition 2.5 (単射・全射・全単射)

集合 A から B への写像 $f : A \to B$ をとる.

1. **単射** (*injection*) : 任意の $a, b \in A$ に対して $f(a) = f(b)$ なら $a = b$ が成り立つことをいう.
2. **全射** (*surjection*) : 任意の $b \in B$ に対して $f(a) = b$ を満たす $a \in A$ が存在することをいう. また, 上への写像ともいう.
3. **全単射** (*bijection*) : 単射かつ全射であることをいう. また, 一対一対応ともいう.

Definition 2.5 (単射・全射・全単射)

集合 A から B への写像 $f : A \to B$ をとる.

1. **単射** (*injection*)：任意の $a, b \in A$ に対して $f(a) = f(b)$ なら $a = b$ が成り立つことをいう.
2. **全射** (*surjection*)：任意の $b \in B$ に対して $f(a) = b$ を満たす $a \in A$ が存在することをいう. また, 上への写像ともいう.
3. **全単射** (*bijection*)：単射かつ全射であることをいう. また, 一対一対応ともいう.

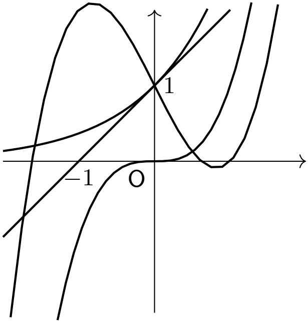
Definition 2.5 (単射・全射・全単射)

集合 A から B への写像 $f : A \to B$ をとる.

1. **単射** (*injection*) : 任意の $a, b \in A$ に対して $f(a) = f(b)$ なら $a = b$ が成り立つことをいう.
2. **全射** (*surjection*) : 任意の $b \in B$ に対して $f(a) = b$ を満たす $a \in A$ が存在することをいう．また, 上への写像ともいう.
3. **全単射** (*bijection*) : 単射かつ全射であることをいう．また, 一対一対応ともいう.

Example 2.6

$\mathbb{R}$ から $\mathbb{R}$ への写像 $x \mapsto x+1$ や $x \mapsto x^3$ は全単射である．しかし，$\mathbb{C}$ から $\mathbb{C}$ への写像 $x \mapsto x+1$ は全単射であるが $x \mapsto x^3$ は全単射ではない．特に，単射でない．また，$\mathbb{R}$ から $\mathbb{R}$ への写像 $x \mapsto e^x$ は単射であるが全射ではない．ただし，$\mathbb{R} \mapsto \mathbb{R}_{>0}$ と制限すると全単射となる．全射であるが単射でない例として $\mathbb{R}$ から $\mathbb{R}$ への写像 $x \mapsto x^3 - 2x + 1$ が挙げられる．



Definition 2.7 (恒等写像)

$f : A \to A$ において，すべての $a \in A$ に対して $f(a) = a$ となる f を **恒等写像** (*identity map*) といい，id_A と表す．図式で表すと次のようになる．

$$\begin{tikzcd} A \arrow[loop above, "\mathrm{id}_A"] \end{tikzcd}$$

Example 2.8

恒等写像は単位的に振る舞う．つまり，$f \in \mathrm{Hom}(A, B)$ に対して，

$$f \circ \mathrm{id}_A = f, \quad \mathrm{id}_B \circ f = f$$

が成り立つ．

Definition 2.7 (恒等写像)

$f : A \to A$ において，すべての $a \in A$ に対して $f(a) = a$ となる f を **恒等写像** (*identity map*) といい，id_A と表す．図式で表すと次のようになる．

$$\begin{tikzcd} A \arrow[loop above, "\mathrm{id}_A"] \end{tikzcd}$$

Example 2.8

恒等写像は単位的に振る舞う．つまり，$f \in \mathrm{Hom}(A, B)$ に対して，

$$f \circ \mathrm{id}_A = f, \quad \mathrm{id}_B \circ f = f$$

が成り立つ．

Definition 2.9 (像)

集合 A から B への写像 $f : A \to B$ をとる．元 $a \in A$ に対して，f による対応により $f(a) \in B$ となるものを **a の f による像** という．また，A の部分集合 A' に対して，B の部分集合

$$f(A') = \{f(a) \mid a \in A'\}$$

を A' の **像** (*image*) という．

Definition 2.10 (逆像)

集合 A から B への写像 $f : A \to B$ をとる．B の部分集合 B' に対して，A の部分集合

$$f^{-1}(B') = \{a \in A \mid f(a) \in B'\}$$

を B' の **逆像** (*inverse image*) という．

Remark

B の各元 b に対して $f^{-1}(b)$ を対応させるものは写像であるとは限らない．B' の元に対して複数の行き先が生じる可能性がある．

Definition 2.9 (像)

集合 A から B への写像 $f : A \to B$ をとる．元 $a \in A$ に対して，f による対応により $f(a) \in B$ となるものを **a の f による像** という．また，A の部分集合 A' に対して，B の部分集合

$$f(A') = \{f(a) \mid a \in A'\}$$

を A' の **像** (*image*) という．

Definition 2.10 (逆像)

集合 A から B への写像 $f : A \to B$ をとる．B の部分集合 B' に対して，A の部分集合

$$f^{-1}(B') = \{a \in A \mid f(a) \in B'\}$$

を B' の **逆像** (*inverse image*) という．

Remark

B の各元 b に対して $f^{-1}(b)$ を対応させるものは写像であるとは限らない．B' の元に対して複数の行き先が生じる可能性がある．

Definition 2.11 (逆写像)

集合 A から B への写像 $f : A \to B$ が $g : B \to A$ の **逆写像** (*inverse map*) であるとは,

$$g \circ f = \mathrm{id}_A, \quad f \circ g = \mathrm{id}_B$$

が成り立つことをいう. *Proposition 2.12* で示す通り g の逆写像は存在すれば一意的に定まるので, f を用いて f^{-1} と書く.

$$\begin{tikzcd} A \arrow[loop left, "\mathrm{id}_A"] \arrow[r, bend left, "f"] & B \arrow[loop right, "\mathrm{id}_B"] \arrow[l, bend left, "g=f^{-1}"] \end{tikzcd}$$

Proposition 2.12

集合 A から B への写像 $f : A \to B$ の逆写像 f^{-1} は, 存在すれば一意的である.

Proof. f の逆写像を g_1, g_2 とおくと,

$$g_1 = \mathrm{id}_A \circ g_1 = (g_2 \circ f) \circ g_1 = g_2 \circ (f \circ g_1) = g_2 \circ \mathrm{id}_B = g_2.$$

□

Definition 2.11 (逆写像)

集合 A から B への写像 $f : A \to B$ が $g : B \to A$ の **逆写像** (*inverse map*) であるとは,

$$g \circ f = \mathrm{id}_A, \quad f \circ g = \mathrm{id}_B$$

が成り立つことをいう. *Proposition 2.12* で示す通り g の逆写像は存在すれば一意的に定まるので, f を用いて f^{-1} と書く.

$$\begin{tikzcd}
A \arrow[loop left, "\mathrm{id}_A"] \arrow[r, bend left, "f"] & B \arrow[loop right, "\mathrm{id}_B"] \arrow[l, bend left, "g=f^{-1}"]
\end{tikzcd}$$

Proposition 2.12

集合 A から B への写像 $f : A \to B$ の逆写像 f^{-1} は, 存在すれば一意的である.

Proof. f の逆写像を g_1, g_2 とおくと,

$$g_1 = \mathrm{id}_A \circ g_1 = (g_2 \circ f) \circ g_1 = g_2 \circ (f \circ g_1) = g_2 \circ \mathrm{id}_B = g_2.$$

□

Definition 2.11 (逆写像)

集合 A から B への写像 $f : A \to B$ が $g : B \to A$ の **逆写像** (*inverse map*) であるとは,

$$g \circ f = \mathrm{id}_A, \quad f \circ g = \mathrm{id}_B$$

が成り立つことをいう. *Proposition* 2.12 で示す通り g の逆写像は存在すれば一意的に定まるので, f を用いて f^{-1} と書く.

$$\begin{tikzcd} A \arrow[loop left, "\mathrm{id}_A"] \arrow[r, bend left, "f"] & B \arrow[loop right, "\mathrm{id}_B"] \arrow[l, bend left, "g=f^{-1}"] \end{tikzcd}$$

Proposition 2.12

集合 A から B への写像 $f : A \to B$ の逆写像 f^{-1} は, 存在すれば一意的である.

Proof. f の逆写像を g_1, g_2 とおくと,

$$g_1 = \mathrm{id}_A \circ g_1 = (g_2 \circ f) \circ g_1 = g_2 \circ (f \circ g_1) = g_2 \circ \mathrm{id}_B = g_2.$$

□

Proposition 2.13

$f : A \to B$ が逆写像をもつ必要十分条件は, f が全単射であることである.

Proof. $(\Leftarrow)$: 一対一対応であるから, 逆像が写像となるため, これは逆写像となる.
$(\Rightarrow)$: $f \circ g = \mathrm{id}_B$ と仮定する. $b \in B$ に対し, $a = g(b)$ とおく. このとき,

$$f(a) = f(g(b)) = (f \circ g)(b) = \mathrm{id}_B(b) = b.$$

ゆえに, f は全射である.
次に, $g : B \to A$ に対し $g \circ f = 1_A$ であると仮定する. $a, a' \in A$ に対し $f(a) = f(a')$ とする, このとき,

$$a = \mathrm{id}_A(a) = (g \circ f)(a) = (g \circ f)(a') = a'$$

ゆえに, f は単射である. よって f は全単射となる. □

Proposition 2.13

$f : A \to B$ が逆写像をもつ必要十分条件は，f が全単射であることである．

Proof. ($\Leftarrow$)：一対一対応であるから，逆像が写像となるため，これは逆写像となる．

($\Rightarrow$)：$f \circ g = \mathrm{id}_B$ と仮定する．$b \in B$ に対し，$a = g(b)$ とおく．このとき，

$$f(a) = f(g(b)) = (f \circ g)(b) = \mathrm{id}_B(b) = b.$$

ゆえに，f は全射である．

次に，$g : B \to A$ に対し $g \circ f = 1_A$ であると仮定する．$a, a' \in A$ に対し $f(a) = f(a')$ とする，このとき，

$$a = \mathrm{id}_A(a) = (g \circ f)(a) = (g \circ f)(a') = a'$$

ゆえに，f は単射である．よって f は全単射となる．　□

Proposition 2.13

$f : A \to B$ が逆写像をもつ必要十分条件は, f が全単射であることである.

Proof. (⇐) : 一対一対応であるから, 逆像が写像となるため, これは逆写像となる.
(⇒) : $f \circ g = \mathrm{id}_B$ と仮定する. $b \in B$ に対し, $a = g(b)$ とおく. このとき,

$$f(a) = f(g(b)) = (f \circ g)(b) = \mathrm{id}_B(b) = b.$$

ゆえに, f は全射である.
次に, $g : B \to A$ に対し $g \circ f = 1_A$ であると仮定する. $a, a' \in A$ に対し $f(a) = f(a')$ とする, このとき,

$$a = \mathrm{id}_A(a) = (g \circ f)(a) = (g \circ f)(a') = a'$$

ゆえに, f は単射である. よって f は全単射となる. □

Proposition 2.13

$f : A \to B$ が逆写像をもつ必要十分条件は，f が全単射であることである．

Proof. $(\Leftarrow)$：一対一対応であるから，逆像が写像となるため，これは逆写像となる．
$(\Rightarrow)$：$f \circ g = \mathrm{id}_B$ と仮定する．$b \in B$ に対し，$a = g(b)$ とおく．このとき，

$$f(a) = f(g(b)) = (f \circ g)(b) = \mathrm{id}_B(b) = b.$$

ゆえに，f は全射である．
次に，$g : B \to A$ に対し $g \circ f = 1_A$ であると仮定する．$a, a' \in A$ に対し $f(a) = f(a')$ とする，このとき，

$$a = \mathrm{id}_A(a) = (g \circ f)(a) = (g \circ f)(a') = a'$$

ゆえに，f は単射である．よって f は全単射となる． □

Definition 3.1 (演算)

集合 A 上の**二項演算** (*binary operation*) とは,

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

となる写像のことである. そして, これは n 個の直積 $A^n \to A$ に対しても定義される.

Remark

二項演算が閉じているとは $a, a' \in A$ に対し, $\circ(a,a') \in A$ が成り立つことをいう.

簡易的に演算は $a \circ a'$ のようにあらわす. また, aa' のように混乱の恐れがないときには表記が省かれることも多い.

Definition 3.1 (演算)

集合 A 上の**二項演算** (*binary operation*) とは,

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

となる写像のことである．そして，これは n 個の直積 $A^n \to A$ に対しても定義される．

Remark

二項演算が閉じているとは $a, a' \in A$ に対し，$\circ(a,a') \in A$ が成り立つことをいう．

簡易的に演算は $a \circ a'$ のようにあらわす．また，aa' のように混乱の恐れがないときには表記が省かれることも多い．

Definition 3.1 (演算)

集合 A 上の**二項演算** (*binary operation*) とは,

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

となる写像のことである. そして, これは n 個の直積 $A^n \to A$ に対しても定義される.

Remark

二項演算が閉じているとは $a, a' \in A$ に対し, $\circ(a,a') \in A$ が成り立つことをいう.

簡易的に演算は $a \circ a'$ のようにあらわす. また, aa' のように混乱の恐れがないときには表記が省かれることも多い.

Example 3.2 (演算の例)

- $\mathbb{N}$ においての $+, \times$, 冪.
- 整数集合 $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{Q}$ においての $+, -, \times$.
- 二重数においての $+, -, \times$.
- $f \in \mathrm{Hom}(\mathbb{R}, \mathbb{R})$ に対する, 適当な写像.
- 母関数における微分.
- ベクトル空間 $\mathbb{R}^n$ においての内積.
- 四元数においての $+, \times$.
- クリフォード代数 Cl_n における 幾何積.
- 合成写像 $\mathrm{Hom}(A, B) \times \mathrm{Hom}(B, C) \to \mathrm{Hom}(A, C)$ $((f, g) \mapsto g \circ f)$.

Example 3.3 (演算でない例)

- 自然数集合 $\mathbb{N}$ においての $-, \div$
- 整数集合 $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ においての $\div$, 冪.
- 二重数においての $\div$, 冪.
- 四元数においての $\div$.
- 一般の合同式における $\div$.

Definition 3.4 (マグマ)

集合 A と A 上の二項演算 $\circ : A \times A \to A$ が定義されている時, 組 $(A, \circ)$ を **マグマ** (*magma*) という.

Definition 3.5 (部分マグマ)

マグマ $(A, \circ)$ に対して, 部分集合 $B \subseteq A$ に制限された二項演算 $\circ : B \times B \to A$ が定義され, B の二項演算が閉じ, これがマグマとなる時, $(B, \circ)$ を**部分マグマ** (*submagma*) という. $(B, \circ)$ は $(B, \circ|_B)$ とも表されることがある.

Example 3.6

$\mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}$ は **一次元トーラス** (*1-dimensional torus*) または **円周群** (*circle group*) といい $(\mathbb{T}, \times)$ は $(\mathbb{C}, \times)$ の部分マグマとなる.

Definition 4.1

集合 A に対する直積集合 $A \times A$ のすべての元 (a, b) に対して, ある関係 $\sim$ が与えられ, A 上比較ができる関係を **二項関係** (*binary relation*) という.

Example 4.2 (色々な律)

集合 A において, 二項関係 $\sim$ を考える.

- **反射律** (*reflexive*) : $a \sim a$ が成り立つ.
- **対称律** (*symmetric*) : $a \sim b$, $b \sim a$ が成り立つ.
- **推移律** (*transitive*) : $a \sim b$ かつ $b \sim c$ なら $a \sim c$ が成り立つ.
- **反対称律** (*antisymmetric*) : $a \sim b$ かつ $b \sim a$ なら $a = b$ が成り立つ.
- **完全律** (*total*) : $a \sim b$ または $b \sim a$ が成り立つ.

Definition 4.1

集合 A に対する直積集合 $A \times A$ のすべての元 (a,b) に対して, ある関係 $\sim$ が与えられ, A 上比較ができる関係を **二項関係** (*binary relation*) という.

Example 4.2 (色々な律)

集合 A において, 二項関係 $\sim$ を考える.

- **反射律** (*reflexive*) : $a \sim a$ が成り立つ.
- **対称律** (*symmetric*) : $a \sim b$, $b \sim a$ が成り立つ.
- **推移律** (*transitive*) : $a \sim b$ かつ $b \sim c$ なら $a \sim c$ が成り立つ.
- **反対称律** (*antisymmetric*) : $a \sim b$ かつ $b \sim a$ なら $a = b$ が成り立つ.
- **完全律** (*total*) : $a \sim b$ または $b \sim a$ が成り立つ.

Definition 4.3 (色々な関係)

集合 A において, 二項関係 $\sim$ を考える.

- **同値関係** (*equivalence relation*) : 反射律, 対称律, 推移律を満たすことをいう.
- **前順序** (*preorder*) : 反射律, 推移律を満たすこと. これを満たす組 $(A, \sim)$ を全順序集合という.
- **半順序** (*partial order*) : 全順序かつ反対象律を満たすこと. これを満たす組 $(A, \sim)$ を半順序集合という.
- **全順序** (*total order*) : 半順序かつ完全律を満たすこと. これを満たす組 $(A, \sim)$ を全順序集合という.

Example 4.4

$(\mathbb{N}, \leq), (\mathbb{Z}, \leq), (\mathbb{Q}, \leq), (\mathbb{R}, \leq)$ は通常の大小の関係において全順序である.

Definition 4.3 (色々な関係)

集合 A において，二項関係 $\sim$ を考える．

- **同値関係** (*equivalence relation*)：反射律，対称律，推移律を満たすことをいう．
- **前順序** (*preorder*)：反射律，推移律を満たすこと．これを満たす組 $(A, \sim)$ を全順序集合という．
- **半順序** (*partial order*)：全順序かつ反対象律を満たすこと．これを満たす組 $(A, \sim)$ を半順序集合という．
- **全順序** (*total order*)：半順序かつ完全律を満たすこと．これを満たす組 $(A, \sim)$ を全順序集合という．

Example 4.4

$(\mathbb{N}, \leq), (\mathbb{Z}, \leq), (\mathbb{Q}, \leq), (\mathbb{R}, \leq)$ は通常の大小の関係において全順序である．

Definition 4.5

半順序集合 $(A, \leq)$ において，A' を A の空でない部分集合とする．

- **最小元** (*minimum element*) (**resp.** **最大元** (*maximum* ;)) :
  $a \in A$ がすべての $b \in A'$ に対して $a \leq b$ (**resp.** $b \leq a$) が成り立つことをいい，$a = \min A'$ (**resp.** $a = \max A'$) で表す．
- **下界** (*lower bound*) (**resp.** **上界** (*upper* ;)) :
  $a \in A$ がすべての $b \in A'$ に対して $a \leq b$ (**resp.** $b \leq a$) が成り立つことをいう．
- **下限** (*infimum*) (**resp.** **上限** (*supremum*)) :
  $a \in A$ が A' の下界 (**resp.** 上界) 全体集合の最大元 (**resp.** 最小元) であることをいい，$\inf A'$ (**resp.** $\sup A'$) で表す．
- **極小元** (*minimal element*) (**resp.** **極大元** (*maximal* ;)) :
  $a \in A$ が $a' < a$ (**resp.** $a < a'$) を満たす $a' \in A$ を持たないことをいう．

Remark

最小元なら極小元であるが，逆は成り立たない．比較できないことがあるからである．同様のことが最大元，極大元に言える．

Definition 4.5

半順序集合 $(A,\leq)$ において, A' を A の空でない部分集合とする.

- **最小元** (*minimum element*) (**resp.** **最大元** (*maximum* ;)) :
  $a\in A$ がすべての $b\in A'$ に対して $a\leq b$ (**resp.** $b\leq a$) が成り立つことをいい, $a=\min A'$ (**resp.** $a=\max A'$) で表す.
- **下界** (*lower bound*) (**resp.** **上界** (*upper* ;)) :
  $a\in A$ がすべての $b\in A'$ に対して $a\leq b$ (**resp.** $b\leq a$) が成り立つことをいう.
- **下限** (*infimum*) (**resp.** **上限** (*supremum*)) :
  $a\in A$ が A' の下界 (**resp.** 上界) 全体集合の最大元 (**resp.** 最小元) であることをいい, $\inf A'$ (**resp.** $\sup A'$) で表す.
- **極小元** (*minimal element*) (**resp.** **極大元** (*maximal* ;)) :
  $a\in A$ が $a'<a$ (**resp.** $a<a'$) を満たす $a'\in A$ を持たないことをいう.

Remark

最小元なら極小元であるが, 逆は成り立たない. 比較できないことがあるからである. 同様のことが最大元, 極大元に言える.

Definition 4.5

半順序集合 $(A, \leq)$ において, A' を A の空でない部分集合とする.

- **最小元** (*minimum element*) (**resp.** **最大元** (*maximum* ;)) :
  $a \in A$ がすべての $b \in A'$ に対して $a \leq b$ (**resp.** $b \leq a$) が成り立つことをいい, $a = \min A'$ (**resp.** $a = \max A'$) で表す.
- **下界** (*lower bound*) (**resp.** **上界** (*upper* ;)) :
  $a \in A$ がすべての $b \in A'$ に対して $a \leq b$ (**resp.** $b \leq a$) が成り立つことをいう.
- **下限** (*infimum*) (**resp.** **上限** (*supremum*)) :
  $a \in A$ が A' の下界 (**resp.** 上界) 全体集合の最大元 (**resp.** 最小元) であることをいい, $\inf A'$ (**resp.** $\sup A'$) で表す.
- **極小元** (*minimal element*) (**resp.** **極大元** (*maximal* ;)) :
  $a \in A$ が $a' < a$ (**resp.** $a < a'$) を満たす $a' \in A$ を持たないことをいう.

Remark

最小元なら極小元であるが, 逆は成り立たない. 比較できないことがあるからである. 同様のことが最大元, 極大元に言える.

Definition 4.5

半順序集合 $(A, \leq)$ において, A' を A の空でない部分集合とする.

- **最小元** (*minimum element*) (**resp.** **最大元** (*maximum* ;)) :
  $a \in A$ がすべての $b \in A'$ に対して $a \leq b$ (**resp.** $b \leq a$) が成り立つことをいい, $a = \min A'$ (**resp.** $a = \max A'$) で表す.
- **下界** (*lower bound*) (**resp.** **上界** (*upper* ;)) :
  $a \in A$ がすべての $b \in A'$ に対して $a \leq b$ (**resp.** $b \leq a$) が成り立つことをいう.
- **下限** (*infimum*) (**resp.** **上限** (*supremum*)) :
  $a \in A$ が A' の下界 (**resp.** 上界) 全体集合の最大元 (**resp.** 最小元) であることをいい, $\inf A'$ (**resp.** $\sup A'$) で表す.
- **極小元** (*minimal element*) (**resp.** **極大元** (*maximal* ;)) :
  $a \in A$ が $a' < a$ (**resp.** $a < a'$) を満たす $a' \in A$ を持たないことをいう.

Remark

最小元なら極小元であるが, 逆は成り立たない. 比較できないことがあるからである. 同様のことが最大元, 極大元に言える.

Definition 4.6 (帰納的)

半順序集合 $(A, \leq)$ の全ての全順序部分集合が上界を持つ時, **帰納的** (*recursive*) であるという.

Theorem 4.7 (Zorn の補題)

帰納的半順序集合は少なくとも一つの極大元を持つ.

この Zorn の補題は証明が非常に長いためここでは証明無しに今後用いることにする.

Definition 4.6 (帰納的)

半順序集合 $(A, \leq)$ の全ての全順序部分集合が上界を持つ時, **帰納的** (*recursive*) であるという.

Theorem 4.7 (Zorn の補題)

帰納的半順序集合は少なくとも一つの極大元を持つ.

この Zorn の補題は証明が非常に長いためここでは証明無しに今後用いることにする.

Definition 4.6 (帰納的)

半順序集合 $(A, \leq)$ の全ての全順序部分集合が上界を持つ時, **帰納的** (*recursive*) であるという.

Theorem 4.7 (Zorn の補題)

帰納的半順序集合は少なくとも一つの極大元を持つ.

この Zorn の補題は証明が非常に長いためここでは証明無しに今後用いることにする.

参考文献 I

[内田 86] 内田 伏一. 集合と位相. 裳華房. 1986.

[AT69] M. F. Atiyah and I. G. MacDonald. Introduction to commutative algebra. Addison Wesley Publishing Company, 1969.

[松村 80] 松村 英之. 可換環論. 共立出版. 1980.

[雪江 10] 雪江 明彦. 代数学 2 環と体のガロア理論. 日本評論社. 2010.

[ポン 57] ポントリャーギン. 柴岡 泰光, 杉浦 光夫, 宮崎 功 (訳). 連続群論. 岩波書店. 1957.

[Rot12] J. Rotman. 関口次郎（訳). 改訂新版 ガロア理論. 丸善出版. 2012.

[加藤 12] 加塩 朋和. 代数学 II. 2021. https://www.rs.tus.ac.jp/a25594/2021_Galois_Theory.pdf.

[Mil21] J.S. Milne. Fields and Galois Theory (v5.00). 2021. https://www.jmilne.org/math/CourseNotes/FT.pdf.

参考文献 II

[Emi17] Emily Riehl. Category theory in context. Courier Dover Publications. 2017.

[Mac13] Mac Lane. Saunders. Categories for the working mathematician.. Springer. 2013.

[Mac12] Mac Lane. Saunders. Ieke Moerdijk. Sheaves in geometry and logic. Springer. 2012.

[Stacks] The Stacks project authors. The Stacks project. -2022. https://stacks.math.columbia.edu/.

[nLab] nLab authors. nLab. -2022. https://ncatlab.org/nlab/show/HomePage.

[MSE] Mathematics Stack Exchange. -2022.

[Wiki] Wikipedia. -2022.

[alg-d] alg-d. 壱大整域. http://alg-d.com/math/.

参考文献 III

[Yukari] Yukari. 群・環・体. 2021.