可換代数への道標

ver 1.2

@akari0kouty

2022 年 3 月 30 日

概要

YouTube, niconico(ニコニコ) に投稿しているであろう動画の資料にあたるものです. 以下のような構成を考えており、この PDF はその一つ目のものとなっています。
(1) 集合論
(2) 群論
(3) 環論と体論の入門
(4) ガロア理論 (古典的なものではないかもしれない)
(5) 可換環論
動画と違い, 埋め込まれているリンクにより定義間の参照がしやすくなっています. 誤植などあれば, Twitter の DM, ホームページ記載のメールアドレスまでお願いします. 尚, 数学的質問に関して, DM, メールアドレスに送っていただいたとしてもお答えすることはできません.

目次

(**Remark**. 目次に*がついているものは読み飛ばしても差し支えのないものである.)

表記.

- $\mathbb{N}$ = $\{0\}$ を含む正整数.
- $\mathbb{Z}$ = 整数環.
- $\mathbb{R}$ = 実数体.
- $\mathbb{C}$ = 複素数体.
- $\mathbb{F}_{p^n}$ = 素数 p の冪 p^n を位数にもつ有限体 .
- $\mathrm{Hom}(M, N)$ = M から N への写像, または準同型写像全体.
- 環 (**resp**. 体) といえば可換環 (**resp**. 可換体) のことをいう.
- 自分自身を含む集合は $\subset$ で表し, 真部分集合は $\subsetneq$ で表す.

第 I 部
幾らかの準備

数 1,A,2,B で学んだことは仮定する. 数 2,B,3 で扱うものもあるが, 適当に読み飛ばしてほしい.

1 写像と集合と演算と

Definition 1.0.1

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[*1] 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, $\mathbb{R}, \mathbb{C}$ などの集合の濃度は $\aleph_0$ より真に大きく, 一般に可算無限集合でない無限集合のことを**非可算無限集合** という.

Remark 1.0.2

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.

1.1 直積

Definition 1.1.1 : 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

[*1] 特別, 代数に詳しいというわけでもない.

合を集合 $A_1, A_2, \dots, A_n$ の **直積** (direct product) という．すなわち,

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

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

Example 1.1.2

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．直線は $\mathbb{R}$, 平面は $\mathbb{R}^2 = \{(x, y) \mid x, y \in \mathbb{R}\}$, 空間は $\mathbb{R}^3 = \{(x, y, z) \mid x, y, z \in \mathbb{R}\}$ であり, 一般に n 次元空間 $\mathbb{R}^n$ を考えられる．

Example 1.1.3

複素数 $\mathbb{C}$ は $\mathbb{R} \times \mathbb{R}$ からの写像として $\mathbb{R} \times \mathbb{R} \ni (x, y) \mapsto x + yi = \alpha \in \mathbb{C}$ 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．

1.2　写像

Definition 1.2.1 : 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 $f : A \to B$ であらわす．元の対応を表す時, $f : a \mapsto f(a)$ であらわす．

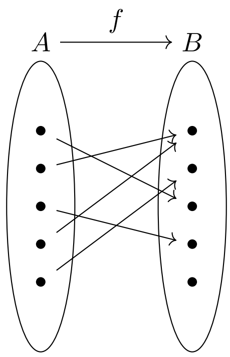

図 1.1　写像の例

Definition 1.2.2

集合 A, B に対して, A から B への写像全体 (Definition 2.1.1においては射全体) の集合を $\mathrm{Hom}(A, B)$ であらわす．

Example 1.2.3

高校数学において, 関数というものには馴染み深いと思う．$f(x) = x^3 - 7$ 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ているはずだ．これらは, 明示されてはいないが暗黙の了解として $\mathbb{R} \to \mathbb{R}$ や、定義域をより小さい部分集合に制限したものを扱っている そしてこれらは

$f, g, h \in \mathrm{Hom}(\mathbb{R}, \mathbb{R})$ となっている.

Definition 1.2.4 : 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 (下図参照).

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

また, $h \in \mathrm{Hom}(A, C)$ 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.

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[dr, "h"'] \arrow[dr, phantom, bend left=20, "\circlearrowright"] & B \arrow[d, "g"] \\ & C \end{tikzcd}$$

図 1.2　可換図式

Proposition 1.2.5 : 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,

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

が成り立つ. □

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

Definition 1.2.6 : 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.

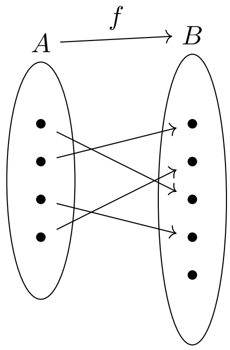

図 1.3　単射のイメージ

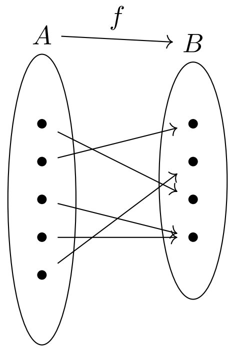

図 1.4　全射のイメージ

Example 1.2.7

$\mathbb{R}$ 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.

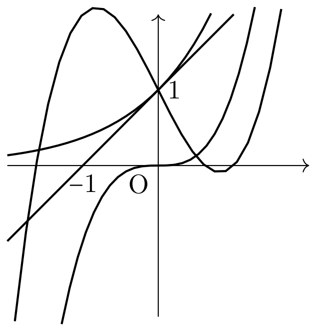

図 1.5　関数の例

Definition 1.2.8 : 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 とあらわす.

$$A \circlearrowleft^{\mathrm{id}_A}$$

図 1.6　恒等写像の図式

Example 1.2.9

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 1.2.10 : 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 1.2.11 : 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．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．

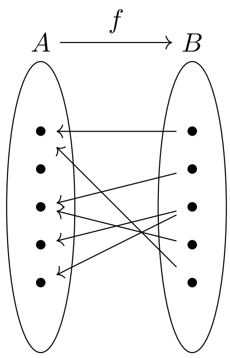

図 1.7　逆像の例

Definition 1.2.12 : 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 1.2.15 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．

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

図 1.8　逆写像

Exercise 1.2.13

写像 $f : A \to B$ に対して次の主張は同値である.

(1) f は単射である.

(2) ある写像 $g : B \to A$ が存在し, $g \circ f = \mathrm{id}_A$ が成り立つ.

Exercise 1.2.14

写像 $f : A \to B$ に対して次の主張は同値である.

(1) f は全射である.

(2) ある写像 $g : B \to A$ が存在し, $f \circ g = \mathrm{id}_B$ が成り立つ.

Proposition 1.2.15

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 1.2.16

$f : A \to B$ 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. $(\Leftarrow)$: f は全射であるから, $B \ni y = f(x)$ を満たす $x \in A$ が存在する. また, f は単射であるから $y = f(x)$ を満たすような x は一意的である. そのため, $g : B \ni y \mapsto x \in A$ のように定めると, $(g \circ f)(x) = x$, $(f \circ g)(y) = y$ が成り立つため, g は f の逆写像となる.

$(\Rightarrow)$: $f \circ g = \mathrm{id}_B$, $g \circ f = \mathrm{id}_A$ 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. $a, a' \in A$ 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. □

Exercise 1.2.17

写像 $f : A \to B, g : B \to C$ に対して, 次が成り立つ.

(1) $g \circ f$ が単射ならば f は単射である.

(2) $g \circ f$ が全射ならば g は全射である.

1.3 演算

Definition 1.3.1 : 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 1.3.2

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.

大凡, 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.

多くの代数系において, 演算は複数定義される.

Example 1.3.3 : 演算の例

(1) $\mathbb{N}$ においての $+, \times$, 冪.

(2) 整数集合 $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{Q}$ においての $+, -, \times$.

(3) 二重数においての $+, -, \times$.

(4) $f \in \mathrm{Hom}(\mathbb{R}, \mathbb{R})$ に対する, 適当な写像.

(5) 母関数における微分.

(6) ベクトル空間 $\mathbb{R}^n$ においての内積.

(7) 四元数においての $+, \times$.

(8) クリフォード代数 Cl_n における 幾何積.

(9) 合成写像 $\mathrm{Hom}(A,B) \times \mathrm{Hom}(B,C) \to \mathrm{Hom}(A,C)$ $((f,g) \mapsto g \circ f)$.

[*2]

Example 1.3.4 : 演算でない例

(1) 自然数集合 $\mathbb{N}$ においての $-, \div$

(2) 整数集合 $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ においての $\div$, 冪.

(3) 二重数においての $\div$, 冪.

(4) 四元数においての $\div$.

(5) 一般の合同式における $\div$.

Definition 1.3.5 : 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.

[*2] **二重数** (dual number) とは, $\varepsilon^2 = 0$ となる $\varepsilon \neq 0$ を実数集合 $\mathbb{R}$ に添加し, $x, y \in \mathbb{R}$ を用いて $x + y\varepsilon$ と表される数全体のことであり, 可換環である. これは剰余環 $\mathbb{R}[X]/(X^2)$ と同型となる.

Definition 1.3.6 : 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 1.3.7

$\mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}$ 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.

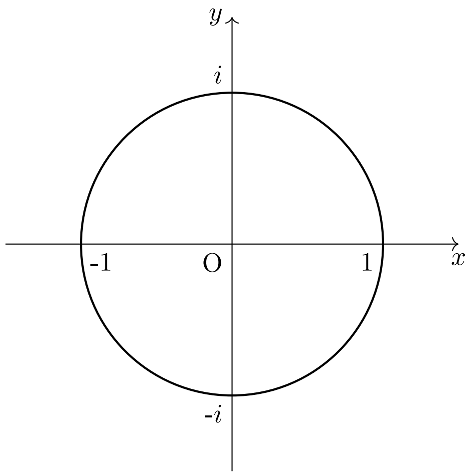

図 1.9　一次元トーラス

1.4　関係

Definition 1.4.1

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 1.4.2 : 色々な律

集合 A において, 二項関係 $\sim$ を考える.

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

Definition 1.4.3 : 色々な関係

集合 A において, 二項関係 $\sim$ を考える.

(1) **同値関係** (equivalence relation) : 反射律, 対称律, 推移律を満たすことをいう.

(2) **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.
(3) **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.
(4) **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 1.4.4

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

Definition 1.4.5

$(A,\leq),(A',\leq')$ を半順序集合とする. このとき, 写像 $f: A\to B$ が $a\leq b$ ならば $f(a)\leq' f(b)$ を保存するとき, f は **順序を保つ写像** という. また, 写像 f が全単射であり, f の順像及び逆写像が順序を保つとき $(A,\leq),(A',\leq')$ は **順序同型** (order isomorphic) であるという.

Definition 1.4.6

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.

(1) **最小元** (minimum element)(**resp**. **最大元** (maximum element)) :
$a\in A$ 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. これを $a=\min A'$ (**resp**. $a=\max A'$) であらわす.
(2) **下界** (lower bound) (**resp**. **上界** (upper bound)) :
$a\in A$ 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.
(3) **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.
(4) **極小元** (minimal element) (**resp**. **極大元** (maximal element)) :
$a\in A$ が $a'<a$ (**resp**. $a<a'$) を満たす $a'\in A$ を持たないことをいう.

Remark 1.4.7

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.

Example 1.4.8

$\mathbb{Z},\mathbb{Q},\mathbb{R}$ は通常の大小の関係において最小元, 最大元を持たない. $\mathbb{N}$ の最小元は 0 であり, 最大元は持たない.

Definition 1.4.9 : 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 1.4.10 : 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.

Proof. [内田 86] を参照. □

1.5　直積再論

??において有限個の積で直積を考えた．そのとき, 正整数 i に対して集合 A_i が与えられていた．これを 正整数集合から集合への写像 $i \mapsto A_i$ であると考えることでより広い視点を持ち, 集合を扱うことができる．

Definition 1.5.1 : 集合族

一般に有限とは限らない集合 Λ から添字をもつ集合の集まり X への写像 $A : \Lambda \to X$ を Λ の **集合族** (family of sets) (集合系とも呼ばれる) といい

$$(A_i \mid i \in \Lambda), \quad \{A_i\}_{i\in\Lambda}, \quad (A_i)_{i\in\Lambda}$$

で表される. そしてこの Λ を **添字集合** という.

Example 1.5.2

$A = \{1, 2, 4\}$ としたとき, $\mathfrak{P}(A) = \{\varnothing, \{1\}, \{2\}, \{4\}, \{1, 2\}, \{2, 4\}, \{4, 1\}, \{1, 2, 4\}\}$ とする．これは集合族である．一般に集合 A に対して, A のすべての部分集合を含む集合 $\mathfrak{P}(A)$ を A の**冪集合** という．

Definition 1.5.3 : 直積

集合族 $(A_i)_{i\in\Lambda}$ から, すべての A_i の和集合すなわち $\bigcup_{i\in\Lambda} A_i$ への写像 f において, すべての Λ の元に対して $f(i) \in \bigcup_{i\in\Lambda} A_i$ となるもの全体の集合を

$$\prod_{i\in\Lambda} A_i := \left\{ f : \Lambda \to \bigcup_{i\in\Lambda} A_i \;\middle|\; \forall i \in \Lambda; f(i) \in \bigcup_{i\in\Lambda} A_i \right\}$$

で表し, 集合族 $(A_i)_{i\in\Lambda}$ の **直積** という．また, この A_i を **直積因子** (direct factor) という．

このとき, $\Lambda = \{1, 2, \ldots, n\}$ とすると確かに Definition 1.1.1 で定義したものと一致する．

2　蛇足と不足*

2.1　圏

読まなくてもいい記述, 後の議論において知らなくても議論の主には差し支えのないものである．圏について学ぶのであれば, 日本語の文献であれば [alg-d] を, 英語であれば [Mac13] や [Emi17] がポピュラーなものとなっている．ここで登場する圏や関手の例は非常に多く, さらに必要とするなら, [alg-d] を読むとその多様さがわかるだろう．適時読者で自ら補ってほしい.

数学において数学対象 (例えばこれから扱っていく群や環であったり, 集合や関数でさえも) が ”同じ振る舞い” をすると何かとうれしい (都合が良い) ことがある．A. Grothendieck によると,

”The introduction of the digit 0 or the group concept was general nonsense too, and mathematics was more or less stagnating for thousands of years because nobody was around to take such childish steps...”

ということなので, この直訳を真に受けるのであれば圏という言語の導入は, 数学の議論を ”nonsense” なものから ”sense” あるものへと足らしめるもであり, 広い視野を持つ, 集合論に囚われているとできないような抽象的な議論が可能であるということだ.

学問の中でも特に数学という型を扱う分野であるからして, 何かしらの例というものが思考を彩度を高めるものであるが, 今までここに記してきた数学的対象対象たちだけでは面白いことをあまり述べることができな

いため, 今後の議論において新たに登場してき次第蛇足という形で例など, その他の発展 (?) を扱っていく. そして, ここでは圏の定義を導入し単射と全射の概念を圏の言葉で書き直し, 矢印の論理の面白さを堪能できるようにしていくことにする.

Definition 2.1.1 : 圏

クラス $\mathcal{C}$ が**圏** (category) であるとは, **対象** (object) の集まり $\mathrm{Ob}(\mathcal{C})$ と 対象 $A, B \in \mathrm{Ob}(\mathcal{C})$ に対し, **始点** (domain) A から **終点** (codomain) B への **射** (morphism) の集まり $\mathrm{Hom}_{\mathcal{C}}(A,B)$ で $\mathcal{C}$ が構成され, $A,B,C \in \mathrm{Ob}(\mathcal{C})$ に対して $\mathrm{Hom}_{\mathcal{C}}(A,B) \times \mathrm{Hom}_{\mathcal{C}}(B,C)$ から $\mathrm{Hom}_{\mathcal{C}}(A,C)$ への合成射を持ち, 次の条件を満たすことをいう.

(C1) 結合律 : 対象 $A,B,C,D \in \mathrm{Ob}(\mathcal{C})$ と 射 $f \in \mathrm{Hom}_{\mathcal{C}}(A,B), g \in \mathrm{Hom}_{\mathcal{C}}(B,C), h \in \mathrm{Hom}_{\mathcal{C}}(C,D)$ に対して, $f \circ (g \circ h) = (f \circ g) \circ h$ が成り立つ.

(C2) 恒等射が存在し, 射 $f \in \mathrm{Hom}(A,B)$ に対し $f = f \circ 1_A = 1_B \circ f$ が成り立つ.

結合律に関しては Proposition 1.2.5 を思い出そう.

Remark 2.1.2

圏 $\mathcal{C}$ の $\mathrm{Ob}(\mathcal{C})$ は多くの場合で大きすぎるがゆえ, 集合となり得ない. Remark 1.0.2 を思い出そう. ここで, $\mathrm{Ob}(\mathcal{C})$ が集合となるような圏を **小さい** (small) といい, また, 対象 $A, B \in \mathcal{C}$ に対して $\mathrm{Hom}_{\mathcal{C}}(A,B)$ が集合となるような圏を **locally small** という. このようなことのため, 今後考える圏はすべて locally small であるとする.

Example 2.1.3 : 集合の圏

対象を集合, 射を写像とする. これは圏となり, **Set** で表す. このとき, $\mathrm{Ob}(\mathbf{Set})$ は全ての集合で構成されている.

Example 2.1.4

前順序集合 $(A, \leq)$ に対して, 対象を集合 A, 射を A の元 a, b に対し, $a \leq b$ なら 1 個. そうでないなら, 0 個と定める. これは圏となる.

Definition 2.1.5 : 関手

圏 $\mathcal{C}$ から $\mathcal{D}$ への **関手** (functor) $F : \mathcal{C} \to \mathcal{D}$ とは, $A \in \mathcal{C}$ に $F(A) \in \mathcal{D}$ を, $f \in \mathrm{Hom}_{\mathcal{C}}(A,B)$ に $F(A) \in \mathrm{Hom}_{\mathcal{C}}(F(A), F(B))$ を対応させる関数であって, 次の条件を満たすことをいう.

(1) $A \in \mathcal{C}$ に対し, $F(\mathrm{id}_{\mathcal{C}}) = \mathrm{id}_{F(\mathcal{C})}$ が成り立つ.

(2) $f \in \mathrm{Hom}_{\mathcal{C}}(A,B), g \in \mathrm{Hom}_{\mathcal{C}}(B,C)$ に対し, $F(g \circ f) = F(g) \circ F(f)$ が成り立つ.

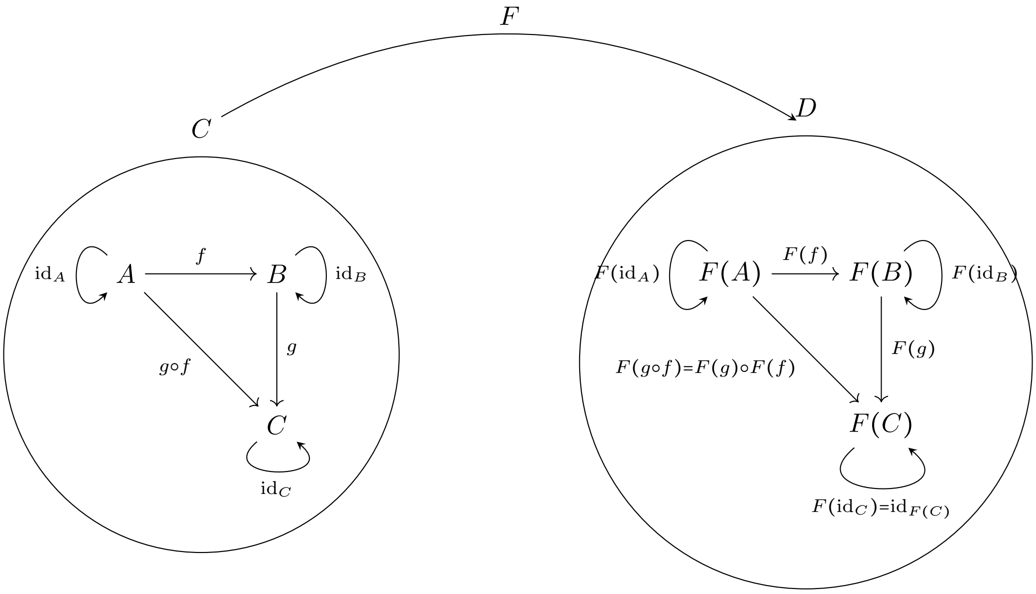

図 2.1　関手

Example 2.1.6

対象を圏, 射を関手とする. これは圏となり, **Cat** で表す.

Definition 2.1.7 : 双対圏

] 圏 $\mathcal{C}$ に対し, その**双対圏** (dual category) $\mathcal{C}^{\mathrm{op}}$ を 対象 $\mathrm{Ob}(\mathcal{C}^{\mathrm{op}}) = \mathrm{Ob}(\mathcal{C})$ と 射の集まり $\mathrm{Hom}(A,B)^{\mathrm{op}}_{\mathcal{C}} = \mathrm{Hom}_{\mathcal{C}}(B,A)$ で定義する.

2.2　単射・全射再論

前に定義した単射・全射は一般的なものであるが, この二つの概念を万人が自然であると納得できるとは思えない. そこで, 矢印による記述により見通しをよくしよう.

Definition 2.2.1 : モノ射・エピ射

対象 A から B への射 $f: A \to B$ をとる.

(1) **モノ射** (monomorphism) : 任意の $g, h \in \mathrm{Hom}(C,A)$ について $f \circ g = f \circ h$ ならば $g = h$ が成り立つことをいう.

(2) **エピ射** (epimorhism) : 任意の $g, h \in \mathrm{Hom}(B,C)$ について $g \circ f = h \circ f$ ならば $g = h$ が成り立つことをいう.

$$\begin{tikzcd} C \arrow[r, shift left, "g"] \arrow[r, shift right, "h"'] & A \arrow[r, "f"] & B \end{tikzcd}$$

図 2.2　モノ射

$$\begin{tikzcd} A \arrow[r, "f"] & B \arrow[r, shift left, "g"] \arrow[r, shift right, "h"'] & C \end{tikzcd}$$

図 2.3　エピ射

Proposition 2.2.2

集合 A から B への写像 $f: A \to B$ をモノ射とする. このとき, f は単射である.

Proof. 単集合 $\mathbf{1}(:=\{*\})$ から A への任意の二つの写像 g,h をとる.

$$\mathbf{1} \underset{h}{\overset{g}{\rightrightarrows}} A \xrightarrow{f} B.$$

このとき, もし, $(f\circ g)(*) = f(g) = f(h) = (f\circ h)(*)$ なら f がモノ射であることから明らかに $g = h$ が成り立つ. □

Exercise 2.2.3

集合間の写像において写像が単射であることとモノ射であることは同値である.

Proposition 2.2.4

集合 A から B への写像 $f: A \to B$ をエピ射とする. このとき, f は全射である.

Proof. 任意の二つの写像 $g,h \in \mathrm{Hom}(B,C)$ をとる.

$$A \xrightarrow{f} B \underset{h}{\overset{g}{\rightrightarrows}} C.$$

$g\circ f = h\circ f$ であるから $g\circ f(A) = h\circ f(A)$ において $f(A)$ の終点と g,h の始点に対応するものが存在する. よって $f(A)$ は B を埋め尽くすことから f は全射であることがわかる. □

Exercise 2.2.5

集合間の写像において写像が全射であることとエピ射であることは同値である.

一般の圏でモノ射・エピ射は単射・全射が成り立つことはないが, **Set** でモノ射・エピ射を考えると, これは単射・全射と等しくなる.

ここで, $\mathrm{Hom}(A,B)^{\mathrm{op}}$ が $\mathrm{Hom}(B,A)$ と等しくなるよう, そして $f\circ g$ (**resp.** $f\circ h$) が $g\circ f$ (**resp.** $h\circ f$) と等しくなるよう **図 2.2** の写像や集合を全て反対にしてみる.

$$C^{\mathrm{op}} \underset{h^{\mathrm{op}}}{\overset{g^{\mathrm{op}}}{\leftleftarrows}} A^{\mathrm{op}} \xleftarrow{f^{\mathrm{op}}} B^{\mathrm{op}}$$

図 2.4　エピ射の双対

するとは**図 2.3** の絵と一致することがわかる. よって, モノ射, エピ射は互いに対をなしており単射, 全射が自然なものであるように感じられる.

第 II 部

誤植と修正

誤植 1 (ver 1.0. p.2)**.** 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．

修正 1. 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，$\mathbb{R}, \mathbb{C}$ などの集合の濃度は $\aleph_1$ と表され，これは $\aleph_0$ より真に大きく，一般に可算無限集合でない無限集合のことを**非可算無限集合** という．

誤植 2 (ver 1.0. p.2)**.** 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，$\mathbb{R}, \mathbb{C}$ などの集合の濃度は $\aleph_1$ と表され，これは $\aleph_0$ より真に大きく，一般に可算無限集合でない無限集合のことを**非可算無限集合** という．

修正 2. 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，$\mathbb{R}, \mathbb{C}$ などの集合の濃度は $\aleph_0$ より真に大きく，一般に可算無限集合でない無限集合のことを**非可算無限集合** という．

誤植 3 (Definition 1.1.1 ver 1.0. p.2)**.** 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，

$$\prod_{i}^{n} A_i = A_1 \times A_2 \times \cdots \times A_n := \{(a_1, a_2, \ldots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\}.$$

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．

修正 3. 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，

$$\prod_{i}^{n} A_i = A_1 \times A_2 \times \cdots \times A_n := \{(a_1, a_2, \ldots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\}.$$

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

誤植 4 (Example 1.1.3 ver 1.0. p.2)**.** 複素 $\mathbb{C}$ は $\mathbb{R} \times \mathbb{R}$ からの写像として $\mathbb{R} \times \mathbb{R} \ni (x, y) \mapsto x + yi = \alpha \in \mathbb{C}$ 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．

修正 4. 複素数 $\mathbb{C}$ は $\mathbb{R} \times \mathbb{R}$ からの写像として $\mathbb{R} \times \mathbb{R} \ni (x, y) \mapsto x + yi = \alpha \in \mathbb{C}$ 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．

誤植 5 (Proposition 1.2.16 ver1.0 p.7)**. 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. □

修正 5. Proof. (⇐)： f は全射であるから, $B \ni y = f(x)$ を満たす $x \in A$ が存在する. また, f は単射であるから $y = f(x)$ を満たすような x は一意的である. そのため, $g : B \ni y \mapsto x \in A$ のように定めると, $(g \circ f)(x) = x$, $(f \circ g)(y) = y$ が成り立つため, g は f の逆写像となる.
(⇒)： $f \circ g = \mathrm{id}_B$, $g \circ f = \mathrm{id}_A$ 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. $a, a' \in A$ 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. □

参考文献

[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.

[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/.

[Yukari] Yukari. 群・環・体. 2021.