5. モノイド・群

2022 秋期「哲学者のための数学」授業資料（大塚淳）

ver. 2022 年 11 月 25 日

1　モノイドとは何か，なぜそれを学ぶのか

前章で見た位相は，空間に関する幾何学的な概念であった．一方本章の主題となるモノイドや群は，本質的に代数的な「計算」にまつわる概念である．よって我々は，代数，幾何と来て我々は再び代数の世界に戻ってきた．

文系の学生にとって，「位相」という言葉は耳にしたことくらいはあっても，「モノイド」や「群」となると聞いたこともない，という人も多いかもしれない．しかし実のところ我々は皆，小学生のころからモノイドや群に親しんでいる．というのも，足し算や掛け算などはまさにこのモノイドや群の作用に他ならないからだ．モノイドや群は，そうした四則演算を始めとした「演算」一般の最もプリミティブな形を抜き出したものと言える．それ以外にも，モノイドは対象や系の変化・発展を表すために用いられるし，また群はモノの対称性（symmetry）の数学的な表現を与える．そしてこの対称性という考え方は，物理学における「法則性」という考えを裏から支えるものであり，また哲学的には客観性の概念と深い結び付きを持っている．こうしたことから，モノイドや群は非常に広範な科学的・哲学的含意を有している．

現代物理学を始め様々な科学で応用される群論は，極めて高度に発展しており，その全体像を掴むことを容易ではない．しかしその基本的な考え方はこれ以上ないくらいシンプルである．ここではその本質的な点のみに的を絞って紹介したい．そこから得られるモノイドや群は，数学者や物理学者からしたらおもちゃみたいに簡単なものでしかないかもしれないが，その哲学的含意を考えるには十分であろう．

2　モノイド

まずは例に倣い，集合をベースにモノイドを定義しよう．

定義 2.1（モノイド）　集合 M 上に，積と呼ばれる二項写像 $\circ : M \times M \to M$ が定義されており，以下の条件を満たすとき，組 $(M, \circ, i)$ を**モノイド** (monoid) という．

1. M の任意の元 x, y, z に対して，結合律 $(x \circ y) \circ z = x \circ (y \circ z)$ がなりたつ．
2. **単位元** (identity element) と呼ばれる元 $i \in M$ が存在して，M の任意の元 x に対して，

$i \circ x = x \circ i = x$ がなりたつ.

これだけである．モノイド演算 $\circ$ は，2 つの元 x, y をある元 $x \circ y$ に対応させる演算である．公理 1 は，この演算が結合律を満たすこと，そして公理 2 はこの演算において「何もしない」単位元が存在することを言っている．つまりモノイドとは，(1) 集合の元一つ一つが元を元に対応させる写像となっており（例えば $x \in M$ は $y \in M$ を $x \circ y \in M$ に移す），(2) その移し方は写像を適用する順番にはよらず（結合律），かつ (3) 「何もしない」写像 i を含んでいる，そんな集合である．しばしば演算記号は省略され，$x \circ y$ は xy のように書かれる．また誤解が生じないときは，演算や単位元を明示せずに単に M がモノイドである，というように言うこともある．

事例 2.1　ゼロを含む自然数 $\mathbb{N}$（つまり非負整数）は，二項演算 $+$ とモノイドをなす．ここでの単位元は 0 である．実際任意の自然数 x, y, z について，$(x + y) + z = x + (y + z)$ かつ $0 + x = x + 0 = x$. これはつまり，任意の自然数（例えば 5）は，他の自然数（例えば 7) を別の自然数（7+5=12）に移す写像である，ということを意味する．同様に，$\mathbb{N}$ が乗算 $\times$ についてもモノイドとなることを確認せよ（その単位元はなんだろうか).

事例 2.2　足し算についての上の議論は，自然数の代わりに有理数 $\mathbb{Q}$，実数 $\mathbb{R}$ のゼロ以上の部分を用いても成立する．例えば $\mathbb{R}^+ := \{x \in \mathbb{R} | x \geq 0\}$ と定義すると，$(\mathbb{R}^+, +, 0)$ はモノイドである．(負の部分はどうなるのか，と思うかもしれないが，これはあとで群を定義するときに見る.)

我々は今まで，(非負）実数 $\mathbb{R}$ を様々な数学的構造として見てきた．集合として見ると（2 章)，それは $\aleph_1$ の濃度を持つ不可算無限集合なのだった．3 章ではその要素の間に大小関係 $\leq, \geq$ を入れた全順序集合として見た．4 章では，実数が開区間 (a, b) からなる開集合を持つ位相空間であることを確認した．そしてここでは，二項演算 $+$ および $\times$ が定義されたモノイドとして定義した．このように，同じ「実数の集合」でも様々な顔を持ち，それらの顔はすでに見たような公理によって構成される．我々が普段何気なく使う実数は，実はこうした顔全てをあわせもつ存在なのである．

発展 2.1　もちろん，実数の特徴づけはこれで終わりなわけではない．まず引き算と割り算の導入がまだであるし（これは以下で群のところで見る)，またここで導入した足し算と掛け算が互いにどう関係し合うのか（例えば分配法則 $a(b + c) = ab + ac$ が満たされるか）などは，別個の公理によって定めなければならない．このためにはさらに**環** (ring)，**体** (field) といった概念を導入しなければならいのだが，本授業ではそこまでは扱わない.

3　モノイド作用

モノイドは，ある対象について作用を加えたときにどう変化するか，あるいは状態がどう変遷していくか，というダイナミックな過程をモデル化するためによく用いられる．その鍵になるのが，**モノイド作用** (monoid action) である.

定義 3.1　$(M, \circ, i)$ をモノイド，X を集合とする．モノイド M の集合 X への（左）M-**作用** *(M-act)* とは，写像

$$M \times X \to X, \quad (m, x) \mapsto mx$$

であり，以下を満たすものである：

1. 任意の $x \in X$ について，$ix = x$.
2. 任意の $m, n \in M$ と任意の $x \in X$ に対して，$m(nx) = (mn)x$.

M を X への作用とみなすということは，それぞれのモノイド元 $m \in M$ を，$X \to X$ の写像としてみなすということである．上の要件 1 は単位元 i が「何もしない」恒等写像 $i(x) = x$ であること，要件 2 はモノイド元の結合が写像の合成になっている（つまり x を n で飛ばしてから m で飛ばすのと，モノイド合成 mn したもので飛ばすものが等しい）ということを述べている．[*1]

モノイド作用をイメージするためには，X を何らかの対象が持つ状態の集合とし，モノイドの各元は各状態に対して働いてそれを変化させるもの，というように考えると良い．例えば次の例を考えてみよう．

事例 3.1　3 つの状態 $X := \{H(appy), C(alm), S(ad)\}$ をとり得るロボットを考える．このロボットに対する可能な入力として $M := \{$ ほめる, しかる, 放置 $\}$ の 3 つの選択肢があるとする．ロボットの状態は，その時の状態と入力に応じて，次のように変わる：

$$\begin{aligned}
&(H, \text{ほめる}) \mapsto C, \quad (H, \text{しかる}) \mapsto S, \quad (H, \text{放置}) \mapsto H, \\
&(C, \text{ほめる}) \mapsto H, \quad (C, \text{しかる}) \mapsto S, \quad (C, \text{放置}) \mapsto C, \\
&(S, \text{ほめる}) \mapsto C, \quad (S, \text{しかる}) \mapsto S, \quad (S, \text{放置}) \mapsto S.
\end{aligned}$$

このとき，入力 M はロボットの状態 X へのモノイド作用を与える．この演算は，図 XX のような**状態遷移図** (state transition diagram) によっても表すことができる．状態集合を持ち，その間の状態遷移関係が定まっているような機械を，**オートマトン** (automaton) という．オートマトンは，状態集合へのモノイド作用として考えることができる．

このように考えると，モノイド作用の射程は極めて広く，時間発展する系一般を記述することができる．それには例えばコンピュータのプログラムの動作や，物理系の時間発展などが考えられる．例えば古典力学の法則は，各質点の位置と運動量からなる**状態空間** (state space) に対するモノイド作用として考えることができる．こうした時間発展系を**力学系** (dynamic systems) という．

事例 3.2　あらゆるモノイドは，「自分自身への作用」として考えることができる．例えば上の自然数の足し算は，$(\mathbb{N}, +, 0)$ の $\mathbb{N}$ への作用：$\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ と考えられる．これは足し算を「与えられた数に作用して変えていく」という動的な仕方で捉えていることだといえる．この解釈では，それぞれのモノイド元（つまり自然数）m, n は，任意の与えられた数に m を足す，n を足す，という作用である．それらの作用は合成できて，$m + n$ は，「m を足してから n を足

[*1] 左作用についての注.

す」という一つの作用となる．また単位元 0 は「0 を足す」（つまり何も変えない）という作用である．

事例 3.3　脳に加えられる外的・内的刺激全体を M とすると，M は脳状態へ作用するモノイドと捉えられる．ここで $m, n \in M$ に対しその合成 mn は，「刺激 m を加えたあとに刺激 n を加える」こととする（ただし「何も刺激を与えないこと」を単位元と考えるのは良くないかもしれない．その問題点を考えてみよ）．

4　可換性

任意の 2 つのモノイド元 $m, n \in M$ の合成 $m \circ n$ および $n \circ m$ が常に等しくなるとき，つまり $\forall m, n \in M(m \circ n = n \circ m)$ がなりたつとき，M は**可換** (commutative) であるといわれる．そうならないものが一例でもあるときは，非可換 (noncommutative) であるという．

事例 4.1　足し算や掛け算は可換性が満たされる典型例である（任意の数につき $m + n = n + m, m \cdot n = n \cdot m$）．一方，$n \times n$ 行列の集合は行列積と単位行列 I によりモノイドをなすが，これは可換性を満たさない（2 つの行列 A, B について一般に $AB \neq BA$）．

足し算や掛け算に慣れ親しんだ身には，可換性は極めて一般的な性質に映るかもしれない．しかし上述の定義の通り，それは非常に強い性質である．モノイドとして表されるような現実世界の「作用」に目を向けると，多くの場面において可換性は必ずしも成立しない．非可換性を証明するためには，モノイド元のうち，$m \circ n \neq n \circ m$ であるようなものを一組でも見つければ良い．またモノイド作用の場合，$mn(x) \neq nm(x)$ となるようなモノイド元のペア (m, n) と状態 x を一つでも見つければ良い．

練習問題 4.1　事例 3.1 のロボットのモノイド作用は可換だろうか．そうでない場合反例をあげよ．

事例 4.2　ある人の心に生じる様々な心的刺激の集合 M を，その人の心的状態に作用するモノイドであると考えよう．例えば痛みや暖かさという感覚は，人の心的状態を快から苦あるいはその逆へと変化させる心的作用である．連続して与えられた刺激をモノイドの合成と考える．このとき，M は明らかに可換ではないだろう．というのも，痛みを感じてから暖かさを感じるときと，その逆では結果は異なるだろうからだ．

練習問題 4.2　数学以外の事例で，可換／非可換モノイドによってモデル化できそうな現象をそれぞれ一つ挙げよ．その場合の合成と単位元がそれぞれ何に相当するのかを明示すること．

5　準同型写像

我々は上で，モノイドの例として足し算と掛け算があることを見た．これは別の言い方をすれば，足し算と掛け算はモノイドとして見たら同じ構造を持つ，ということである．同じ構造を持つということは，両モノイドを橋渡しする関係性，つまり足し算を掛け算へとシステマティックに変換するルールがあるはずだ．その「ルール」を正確に表すのが，モノイド間の準同型写像である．

定義 5.1（準同型）　2 つのモノイド $(M, \circ, i), (M', \circ', i')$ が与えられているとき，写像 $f : M \to M'$ で，任意の $m, n \in M$ について次を満たすものを，M と M' の間の**準同型写像** (homomorphism) という：

$$f(m \circ n) = f(m) \circ' f(n)$$

位相空間の連続写像のところと同様，ここでの f はモノイドのもととなる集合 M, M' の間の写像である．しかし単なる集合上の写像ではなく，ここではモノイド M の構造を保つことが要請されており，それを示すのが上の等式である．この等式の左辺は，モノイド M 上の演算 $m \circ n$ を行ったものを，f で M' に飛ばしたものを表している．一方右辺は，M の元 m, n をそれぞれ f で飛ばした結果である $f(m), f(n) \in M'$ に，M' 上のモノイド演算 $\circ'$ を適用したものを表している．くどいようだが，$\circ$ は M の演算，$\circ'$ は M' の演算であるということをしっかり確認しよう．よってこの式全体は，M の演算 $\circ$ の結果を f で飛ばしたものと，先に f で飛ばしてから M' の演算 $\circ'$ を適用した結果が同じである，ということを表している．モノイドの構造はその演算のあり方によって決定されるのだから，このように作られた準同型写像はモノイドの構造をしっかり保っているといえる．

練習問題 5.1　$f : M \to M'$ がモノイド準同型のとき，$f(i) = i'$，つまり M の単位元は f によって M' の単位元に移されることを示せ．

ゼロ以上の実数 $\mathbb{R}^+ := \{x \in \mathbb{R} | x \geq 0\}$ 上の足し算と掛け算のモノイドの間の準同型写像はどのようなものがあるだろうか．つまり $M := (\mathbb{R}^+, +, 0), M' := (\mathbb{R}^+, \times, 1)$ としたときの準同型 $f : M \to M'$ を見つけたい．それは無数にあるのだが，一つの例として関数

$$2^{()} :: m \mapsto 2^m$$

を考えてみよう．まずこれは $m \in \mathbb{R}^+$ から $2^m \in \mathbb{R}^+$ への関数になっている．さらに

$$2^{m+n} = 2^m \cdot 2^n$$

なので，和を積へとしっかりと移している．これを「2 を底とする指数関数」という．2 に限らず，$a > 0$ を底とする指数関数はすべて足し算としての非負実数から掛け算としての非負実数への準同型を与える．特に底としてネイピア数 $e \approx 2.718$ をとるものを単に指数関数 (exponential function) とよび，exp() と表す．

事例 5.1　我々は上で，自然数 $\mathbb{N}$ 上の足し算と非負実数 $\mathbb{R}^+$ 上の足し算はともにモノイドであると述べた．これらの間にも準同型がある．いま埋め込み $i : \mathbb{N} \to \mathbb{R}^+$ を，$i(m) = m$ で

定義する．つまり i はある数 m をとって同じ数 m を返す．ただしここで入力される数 m は整数であるが（つまり $m \in \mathbb{N}$），出力される数 $i(m)$ は実数として解釈されている（つまり $i(m) \in \mathbb{R}^+$）点に注意しよう．当然 $i(m+n) = i(m) + i(n)$ となり，この関数は足し算を保存するので，準同型写像である．

練習問題 5.2　$(\mathbb{N}, +, 0)$ から $(\mathbb{R}^+, +, 0)$ への準同型写像には埋め込み以外にも沢山ある．その例を考えてみよう．

定義 5.2**（同型）**　モノイド M, N の間の準同型写像 $f : M \to N$ が全単射であるとき，f は**同型写像** (isomorphism)，M と N はモノイドとして**同型** (isomorphic) といわれる．このとき逆写像 $f^{-1} : N \to M$ は N から M への準同型写像になっている．

事例 5.2　$\exp() : \mathbb{R}^+ \to \mathbb{R}^+$ の逆写像は，（e を底とする）対数関数 $\log()$ である．$\log(x) = y$ とは，e を y 乗すると x になる，ということを意味する．よって任意の $x \in \mathbb{R}^+$ につき，$\log(\exp(x)) = x$ であり，$\exp(\log(x)) = x$. また

$$\log(x \cdot y) = \log(x) + \log(y)$$

かつ

$$\log(1) = 0$$

より，log は掛け算 $(\mathbb{R}^+, \times, 1)$ から足し算 $(\mathbb{R}^+, +, 0)$ への準同型写像になっている．

一方で，事例 4.1 と練習問題 4.2 で見たような $(\mathbb{N}, +, 0)$ と $(\mathbb{R}^+, +, 0)$ の間には，当然全単射は存在しない．よって両者は同型ではない．

事例 5.3　心の機能主義 (functionalism) によれば，心的状態は何らかの神経生理学的機能と同一視できる．この見方によれば「痛み」という質的な感じは，鋭い物理的刺激に対する神経生理学的反応の心的対応物に他ならない．これをモノイド準同型の観点からモデル化してみよう．いま，P を事例 2.3 で見たような脳状態モノイド，M を事例 3.2 で見た心的モノイドとする．このとき，機能主義とは準同型写像 $f : P \to M$ が存在する，という主張として捉えることができる．物理刺激から心的刺激へのマッピング f が単射である場合，複数の物理的刺激が同一の心的刺激（例えば「痛み」）を生み出すことがある．一方，これが全単射（つまり f が同型）である場合，両者は完全にパラレルであることになる．これを心脳同一説 (mind-brain identity theory) という．

練習問題 5.3　機能主義は，心的状態の物理的状態への付随説（2 章事例 7.1）と密接に関連する．ある（心的）状態の集合 S_M が（物的）状態の集合 S_P に付随 (supervene) するとは，2 つの心的状態 $s, s' \in S_M$ が異なるなら対応する物理状態 $f(s), f(s') \in S_P$ も異なる，つまる f が単射であるということであった．しかしこれは時間スライスごとの静的な対応を見ているだけで，本章で見たような時間発展を考慮していない．では通時的な心的・物的モノイド M, P を考えた場合，共時的に付随説が成立する条件はなんだろうか？

（この問題は様々な粒度で考えることができるが，しっかりと扱うためには，モノイド作用についての正式な定式化が必要になる．）

6 群

群 (group) は，以下のようにモノイドの特殊ケースとして定義される．

定義 6.1（群） モノイド $(M, \circ, i)$ が，モノイドの 2 要件に加え次を満たすとき，**群** (group) であるといわれる：

$$\forall m \in M, \exists m' \in M (m \circ m^{-1} = m^{-1} \circ m = i).$$

つまりすべての元 $m \in M$ に対して，それと掛け合わせると単位元になるような $m^{-1} \in M$ が存在する．このような m^{-1} を m の**逆元** (inverse element) という（逆元は，場合によって $-m$ などとも書かれる）．つまり群とは各元が逆元を持つモノイドである．

単位元 i は「何もしない」ことなので，$m \circ m^{-1} = i$ は元と逆元を合成すると結局「何もしない」ことと同じだといっている．このように，群のすべての元には，それをキャンセルする逆元が備わっている．

逆元については，次の性質が成り立つ．

1. 任意の元 $m \in M$ に対し，その逆元は一意的に定まる．
2. 逆元の逆元はもとに戻る：$(m^{-1})^{-1} = m$.
3. 任意の $m, n \in M$ に対し，$(mn)^{-1} = n^{-1}m^{-1}$.

証明は次の通り：

1. 仮に m の逆元として n, n' があるとしてみよう．すると $(n'm) = (mn) = i$ より，$n = in = (n'm)n = n'(mn) = n'i = n'$ となり，n と n' が等しいことが示される．
2. $m^{-1}m = i$ であるが，これは m^{-1} の逆元（すなわち $(m^{-1})^{-1}$）が m であると述べていることに等しい．
3. $n^{-1}m^{-1}$ を mn の左ないし右からかけると i になることで確かめられる．例として左からかけると $n^{-1}m^{-1}mn = n^{-1}in = n^{-1}n = i$.

事例 6.1 モノイドの事例として足し算の体系を見たが，足し算の「逆」は引き算であり，引き算とは負の数を足すことにほかならない．よって自然数に変えて（負の数を含む）整数 $\mathbb{Z}$ を考えると，$(\mathbb{Z}, +, 0)$ は二項演算 $+$ について群となる．ここで $m \in \mathbb{Z}$ の逆元は $-m$ であり，実際 $m + (-m) = 0$ がなりたつ．

練習問題 6.1 掛け算の場合の逆元はなんだろうか．$(\mathbb{Z}, \times, 1)$ は二項演算 $\times$ について群となるだろうか．有理数 $\mathbb{Q}$ や実数 $\mathbb{R}$ だったらどうだろうか．

しばしば，群は対象の**対称性** (symmetry) を示すものだといわれる．これはどういうことだろうか．下のような星型図形を考えよう．1