群とは何か

東京理科大学 理学部第二部 数学科 教授　佐藤（さとう）　隆夫（たかお）

1　群

数学で最も基本的な演算といえば，小学1年生で学ぶ整数の足し算（和）であろう．0の性質や交換法則，結合法則などを理解して，$1+0=1$ や $2+3=3+2$，$13+7=(10+3)+7=10+(3+7)=10+10=20$ などを授業参観でスラスラと解答している．小学校では $3-1$ などの引き算（差）も学ぶが，$1-3$ ができるようになるのは中学生になってからであろうか．ちなみに，$1-3$ は厳密には $1+(-3)$ のことであり，-2 に等しい．つまり，数学で引き算とはマイナス元を加えることを略記したもので，本質的には足し算である．実数の積は $2\times3=3\times2$ のように交換可能（可換）であるが，一般には可換でないような「積」もある．例えば，大学1年生の線型代数で学ぶ，正方行列たちの積は一般に可換ではない．非可換な積は珍しく感じるかもしれないが，数学で扱う様々な積は可換であることの方がむしろ珍しい．

端的に言えば，ある条件を満たす演算が与えられた集合を群という．G を集合とし，任意の $a,b\in G$ に対して，a と b の積と呼ばれる元 $a\cdot b\in G$（ab と略記する）が一意的に定まっており，以下を満たすとき G を**乗法群**という．

- （結合法則）任意の $a,b,c\in G$ に対して，$(ab)c=a(bc)$.
- （単位元の存在）ある $e\in G$ が存在して，任意の $a\in G$ に対して $ae=ea=a$.
- （逆元の存在）任意の $a\in G$ に対して，ある $a^{-1}\in G$ が存在して $aa^{-1}=a^{-1}a=e$.（a^{-1} を a の**逆元**という．）

加法群も同様に定義されるが，この場合 a と b の和は $a+b$，単位元は**零元**といい0，a の逆元は a の**マイナス元**といい $-a$ と，それぞれ表す．さらに，加法群では交換法則（任意の $a,b\in G$ に対して $a+b=b+a$）が成り立つものとする．

例えば，整数全体 $\mathbb{Z}$ は通常の和に関して加法群になり，零でない有理数全体 $\mathbb{Q}^\times$ は通常の積に関して乗法群になる．また，$n\geq1$ に対して1の複素 n 乗根全体

$$\left\{\cos\left(\frac{2k\pi}{n}\right)+i\sin\left(\frac{2k\pi}{n}\right)\,\middle|\,0\leq k\leq n-1\right\}$$

は複素数平面内の1を含む単位円周上の n 等分点の集合であり，通常の複素数の積に関して乗法群になる．

今日，群は純粋数学のみならず数理物理や分子の対称性などに幅広く応用されるなど大変奥が深いものであるが，本稿では，「**できないことを証明するための数学的道具**」という観点から群について簡単に眺めてみよう．

2　対称群

1から3までの番号が書かれた石 x_1,x_2,x_3 が一列に並んでおり，これらを並べ換えることを考える．どれか2つの石のみを入れ換える操作を**石の互換**と呼ぶことにする．例えば，x_1 と x_2 を入れ換える操作や，x_1 と x_3 を入れ換える操作は石の互換である．この石の互換を何回か（0回も含めて）繰り返してどのような列ができるかを考えると，石の並び換えすべての場合が現れ，全部で6通りある．

$$(x_1,x_2,x_3),(x_1,x_3,x_2),(x_2,x_1,x_3),$$
$$(x_2,x_3,x_1),(x_3,x_1,x_2),(x_3,x_2,x_1).$$

それでは，石の互換を一度に2回続けて行う操作（これを**石の重互換**と呼ぶことにする）を何回か繰り返してどのような列ができるかを考えてみよう．しばらく試行錯誤すると，$(x_1,x_2,x_3),(x_2,x_3,x_1),(x_3,x_1,x_2)$ は得られるが，$(x_2,x_1,x_3),(x_3,x_2,x_1),(x_1,x_3,x_2)$ は無理そうだという感じがしてくる．実際に不可能なのであるが，では，「**できない**」ということをどうやって証明したらよいだろうか．もちろん，場合の数が有限なのでしらみつぶしに考えても良い．では石の数を4個，5個，…と増やしていき，一般に n 個となったらどうだろうか．さすがに頭を使わないわけにはいかない．

n 個の文字 $1,2,\ldots,n$ の集合を $X=\{1,2,\ldots,n\}$ とおく．写像 $\sigma:X\to X$ が一対一対応のとき，すなわち，$\sigma(1),\sigma(2),\ldots,\sigma(n)$ が $1,2,\ldots,n$ を並べ換えたものであるとき，σ を X の**置換**という．X の置換は全部で $n!$

個ある．X の置換全体の集合を $\mathfrak{S}_n$ で表す．（$\mathfrak{S}$ はドイツ文字の S.）任意の $\sigma,\tau\in\mathfrak{S}_n$ に対して，合成写像 $\sigma\circ\tau : X\to X$ は X の置換であり，これを σ と τ の積 $\sigma\tau$ と定めると $\mathfrak{S}_n$ は乗法群になる．単位元はどの文字も動かさないような X 上の恒等写像であり，**恒等置換**と呼ばれる．この $\mathfrak{S}_n$ を n 次**対称群**という．$1\le i\ne j\le n$ に対して，i と j を入れ換えてそれ以外の文字を動かさない置換を (ij) と表す．$n\ge 3$ のとき，$(12)(13)\ne(13)(12)$ であるから $\mathfrak{S}_n$ は非可換群である．

X の文字のうち，ある 2 つの文字のみを入れ換えて，その他の文字は動かさないような置換を**互換**という．任意の置換はいくつかの互換の積として表せるが，表し方が一通りではない．例えば $\mathfrak{S}_4$ において，$(12)(23)(34)(12)(34)=(23)(12)(23)$ である．しかしながら，ある置換を互換で表すとき，どのように表しても互換の個数の偶奇は一定であることが知られている．置換 σ に対して σ が偶数（奇数）個の互換の積で書けるとき，$\mathrm{sgn}(\sigma)=1(-1)$ と定め，これを σ の**符号**という．(x_1,x_2,x_3) を (x_1,x_3,x_2) に変形する石の互換の符号は -1 であり，石の重互換の符号はすべて 1 であるから，石の重互換で (x_1,x_2,x_3) を (x_1,x_3,x_2) に変形**できない**ことが分かる．これは，石の数が増えても同様である．

似たような問題として，子どものおもちゃである「15 ゲーム」を考えよう．これは，1 から 15 までが正方形のマス目に上から下かつ左から右に順に並んでいて，最後の右下の一マスだけが空いており，マス目をスライドさせながら変形して遊ぶものである．少し遊んでみると，最初の状態から 14 と 15 が書かれた二つのマス目だけを入れ換えた状態には，通常の操作では絶対に変形**できない**ことが感覚的に分かる．これも対称群の性質を用いて示せることが参考文献 1)に紹介されている．

3　行列式

対称群の応用例の一つとして行列式を考える．実数係数連立一次方程式 $ax+by=u, cx+\mathrm{d}y=v$ がただ一つの解を持つための必要十分条件は，$ad-bc\ne 0$ である．では一般に，$n\ge 1$ に対して連立一次方程式

$$\begin{cases} a_{11}x_1+\cdots+a_{1n}x_n &= u_1,\\ \quad\vdots & = \ \vdots\\ a_{n1}x_1+\cdots+a_{nn}x_n &= u_n \end{cases}$$

の場合はどうだろうか．線型代数で学ぶように，$A=(a_{ij})$ とおくとこの場合の必要十分条件は $\det A\ne 0$ である．ここで，

$$\det A=\sum_{\sigma\in\mathfrak{S}_n}\mathrm{sgn}(\sigma)a_{1\sigma(1)}a_{2\sigma(2)}\cdots a_{n\sigma(n)}$$

は A の**行列式**と呼ばれる．

行列式は連立一次方程式の解を決定するものという意味でガウスが determinant（デテルミナント）と名付けた．邦訳は東京物理学校夜間部でも教鞭をとられた高木貞治氏によって「行列式」と命名された．群論的な観点から注目すべき行列式の性質は，n 次正方行列 A,B に対して，$\det AB=(\det A)(\det B)$ が成り立つことだろう．

いろいろな群を分類する際に，見かけ上は異なる群でも積の構造が同じようなものは同一視したい．そのために，群構造と両立するよう写像を考える．乗法群 G,H に対して，写像 $f : G\to H$ が任意の $a,b\in G$ に対して，$f(ab)=f(a)f(b)$ をみたすとき，f を**準同型写像**という．例えば，実数を成分とする n 次正則行列のなす群を $\mathrm{GL}(n,\mathbb{R})$，0 以外の実数全体のなす乗法群を $\mathbb{R}^\times$ とすれば，n 次正則行列にその行列式を対応させる写像 $\det : \mathrm{GL}(n,\mathbb{R})\to\mathbb{R}^\times$ は準同型写像である．

準同型写像 $f : G\to H$ が 1 対 1 対応のとき**同型写像**という．このとき，G と H は**同型**であるといい，群として同じものとみなす．例えば，実数全体のなす加法群 $\mathbb{R}$ と正の実数全体のなす乗法群 $\mathbb{R}_{>0}$ に対して，解析学の結果から指数函数 $\exp : \mathbb{R}\to\mathbb{R}_{>0}, x\mapsto e^x$ は同型写像である．ここで，e は自然対数の底を表わす．

4　代数方程式の可解性

群の起源の一つとして実数係数代数方程式の可解性に関するガロアの研究がある．2 次方程式の解の公式は有名であるが，3 次方程式 $ax^3+bx^2+cx+d=0\ (a\ne 0)$ はどうだろうか．実は，少し長いがカルダノの公式と呼ばれる解の公式が知られており，4 次についてもフェラーリの公式が知られている．ところが，5 次以上の代数方程式については，重複度も込めて次数の分だけ複素数解が存在することは比較的簡単に示せるものの，解の公式は存在しない．すなわち，$n\ge 5$ に対して，一般に代数方程式 $a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0=0(a_n\ne 0)$ のすべての解を，係数たちから四則演算と冪根（べきこん）を取る操作のみを用いて表わすことが**できない**．ここで，「一般に」というところが重要で，最初から因数分解された形で与えられた方程式 $(x-1)^5=0$

の解を求めることは造作もない．言い換えれば，$n\geq 5$ のとき，上記のような代数的演算で解けないような方程式がある．このような方程式は無数にあり，例えば，$x^5-3x+3=0$ はそのうちの一つである．（例えば，参考文献 2)の §3.12 を参照せよ．）

ガロアはこの「できない」ということを，方程式の解たちの置換がなす群の性質を調べることで証明した．当時はまだ群の概念がなく萌芽的なものであったが，より現代的な言葉で言えば，多項式 $f=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$ に f の**ガロア群**と呼ばれるある群を対応させる．このとき，方程式 $f=0$ が代数的に解けるための必要十分条件は，f のガロア群が**可解群**となることである．このような理論はガロア理論として整備され，今日，大学 3, 4 年次で学ぶ代数学のいわゆる花形の一つである．その応用として，1 cm の長さが測れる定規とコンパスだけでは $\sqrt[3]{2}$ cm の長さを作図**できない**ことや，3 等分**できない**角度があること，さらに作図**できない**正多角形があることなどが示される．これらはあくまで定規とコンパスのみを用いた場合で，それら以外の道具（例えば折り紙など）を用いて良ければ話は別であることが参考文献 3)の第 5 章に紹介されている．また，比較的最近得られた事実として以下のようなものもある．$n\geq 5$ に対して，円に内接する n 角形と各辺の長さが与えられているとする．このとき，その多角形の面積を各辺の長さたちから四則演算と冪根を取る操作のみを用いて表わすことが**できない**ことが，松本幸夫先生らによって 2007 年に初めて明文的に示され，参考文献 4)にその解説がある．

5　楕円曲線上の有理点

少し高度な代数学の話題を取り上げてみよう．有理数係数の 3 次多項式

$$f(x)=x^3+ax^2+bx+c$$

を考える．3 次多項式にも判別式というものがあり，$D(f):=-4a^3c+a^2b^2-4b^3-27c^2+18abc$ で与えられる．ただし，判別式といっても，2 次の場合のように方程式 $f(x)=0$ 解の存在範囲まで特定できるものではなく，$D(f)\neq 0$ のときに $f(x)=0$ が重解を持たないことが分かるのみである．

2 つの複素数の対 (x,y) 全体の集合を $\mathbb{C}^2$ と表す．$D(f)\neq 0$ である $f(x)$ に対して，$\mathbb{C}^2$ の部分集合 $E:=\{(x,y)\in\mathbb{C}^2\mid y^2=f(x)\}$ を有理数体上で定義された楕円曲線という．楕円曲線は元々，楕円の弧長を求める問題から，楕円積分の研究を経て考えられるようになった背景があり，現在では整数論と呼ばれる分野で活発に研究されている．E の点 (x,y) で x,y がともに有理数であるようなものを E の有理点という．E の有理点全体に無限遠点と呼ばれる点 $\mathcal{O}$ を付け加えたものが加法群になることが知られている．さらに，モーデルによって，この加法群は有限生成という非常に良い性質を持つことも知られている．

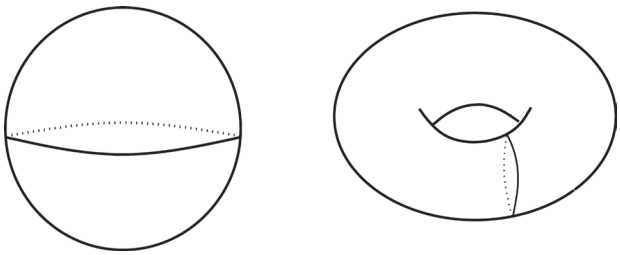
ここでは，具体的に $f(x)=x^3-x, D(f)=4$ について考えてみよう．この場合の楕円曲線の有理点たちのなす群は $\{\mathcal{O},(0,0),(\pm 1,0)\}$ である．この事実を認めると，3 辺の長さが有理数の直角三角形で，面積が 1 のものは**存在しない**ことが従う．実際，3 辺の長さが有理数 a,b,c の直角三角形（斜辺が c）で，$ab/2=1$ なるものが存在したとすると，$x:=c^2/4, y:=(a^2-b^2)c/8$ とおけば (x,y) は E 上の有理点であり，$y=0$ から $a^2=2$ となり矛盾である．

6　位相幾何学

ガロア理論や楕円曲線の有理点もそうであるが，群は純粋数学に限っても相当な応用がある．ここでは，群の位相幾何学への応用について考えてみよう．位相幾何学（トポロジーともいう．）は連続変形で不変な図形の性質を研究する学問である．厳密には，「図形」とは開集合系が定義された**位相空間**と呼ばれる集合のことで，ここでは弧状連結なものを考える．

ありふれた例であるが，自由自在にいくらでも伸縮可能なゴムでできたボールの表面（球面）を，切り貼りせずにどうにかして浮き輪の表面（トーラス）に変形できるだろうか．片方には「穴」が開いてるし，直感的には無理そうである．では，この「できない」をどうやって示せば良いだろうか．まさか無限通りの方法を試すわけにもいかない．やはり頭の使いどころである．

一般に，二つの図形 X,Y に対し，逆写像も含めて連続な 1 対 1 対応を与える写像（正確には同相写像という）$f: X\to Y$ が存在するとき，X と Y は**同相**であるといい，X と Y は図形として同じものとみなす．例えば，多角形の周は円と同相である．同様に，三角錐や正四面体の表面は球面と同相である．位相幾何学では図形の角度とか面積，体積などは一切気にしない．いささか乱暴に思えるかもしれないし，高校時代あれだけ苦労して積分を計算して面積や体積を求めたのは一体何だったのかと思うかもしれないが，まったく問



【図 1】球面とトーラス

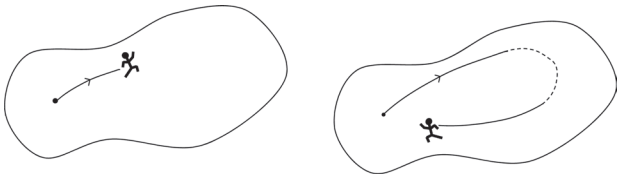
題ない．

位相幾何学では，与えられた 2 つの図形が同相かどうかを数学的に判定するために，**位相不変量**と呼ばれる，同相な図形の間で不変な量を構成する．これはオイラー数のような数である場合もあるが，群を用いて構成される不変量に大変重要なものがある．

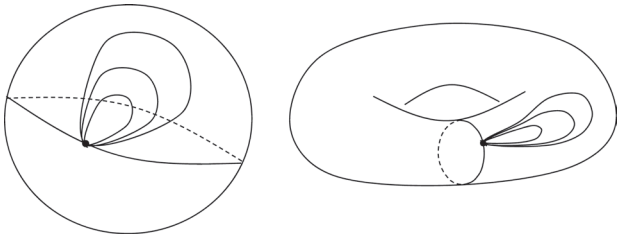
7　基本群

絵本の中に入り込むように，図形の中に自分が立っている世界を想像してみよう．図形の中に目印になるような基準を 1 点取って固定し，**基点**と呼ぶ．基点からいくらでも伸び縮みできるロープを持って出かけ，再び基点に戻ってくることを考える．すると，球面の場合はどのようなルートで歩いて帰ってきても球面上に沿ってロープを縮められるが，トーラスの場合は歩くルートによってはロープが引っ掛かってしまい，縮められないことが起こりそうである．球面とトーラスを区別する位相不変量を作りたければ，このようなことを数学的に定式化すれば良い．大雑把に言えば以下のようになる．X を図形，$p\in X$ を基点とする．閉区間 $[0,1]$ から X への連続写像 l で，$l(0)=l(1)=p$ となるものを p を基点とする X の**ループ**という．つまり，l は基点 p から出発して 1 秒間で戻ってくる X 内の閉じた道である．l,m を X のループとし，それぞれ 2 倍速で動かしてつなげればまたループになる．これを l と m の積といい $l\cdot m$ と表す．また，基点を固定したまま l を連続的に m に変形できるとき，l と m は**ホモトピック**であるといい，$l\simeq m$ と表す．ホモトピックなループは同じものとみなしたい．そこで，l とホモトピックなループ全体を一まとまりの集合と考えて $[l]$ と表し，l の**ホモトピー類**という．このようなホモトピー類すべての集合を $\pi_1(X,p)$ とおき，任意の $[l],[m]\in\pi_1(X,p)$ に対して，$[l]\cdot[m]:=[l\cdot m]$ と定めると，$\pi_1(X,p)$ はこの積に関して乗法群になる．これを p を基点とする X の**基本群**という．

基本群の一般論から，**2 つの図形が同相であればこれらの基本群は同型になる**という極めて重要な事実が成り立つ．対偶を取れば，基本群が同型でないような 2 つの図形は同相ではなく，連続的な 1 対 1 対応は作れないことが分かる．特に，球面の基本群はトーラスの基本群に同型でないことが知られており，言い換えれば，ボールの表面をどのように連続変形しても浮き輪の表面には**ならない**．



【図 2】基点からロープを持って出かけて戻る



【図 3】どんなロープも縮められる？

今日，ホモロジー群と並び代数的位相不変量の双璧をなす基本群は，閉曲面の分類のためにポワンカレが 1895 年の論文の中で導入したのが嚆矢とされている．1904 年にポワンカレは，$n\geq 2$ に対し，弧状連結で基本群が自明な n 次元閉多様体は n 次元球面に同相かという問題を提唱し，$n=3$ の場合だけが未解決問題として最後まで残されていた．この問題は 2006 年にペレルマンによって完全に解決されるまではポワンカレ予想とよばれ，1995 年に解決されたフェルマーの最終定理と並び世紀を跨ぐ大問題であった．

8　謝辞

このたび，本稿執筆の機会を与えていただいた先端的融合代数学研究部門長で創域理工学部教授の伊藤浩行先生，科学フォーラム編集委員長の渡辺一之先生，ならびに校正作業にご尽力いただきました本学広報課の皆様に心より深く感謝お礼申し上げます．

[参考文献]

1）芳澤光雄；置換群から学ぶ組合せ構造，日本評論社．
2）藤﨑源二郎；体とガロア理論，岩波基礎数学叢書．
3）西田吾郎；数，方程式とユークリッド幾何：ガロア理論から折り紙の数学まで，京都大学学術出版会．
4）のんびり数学研究会；ガロアに出会う：はじめてのガロア理論，数学書房．