

現代数学のめざすもの — ガロア理論, 整数論とその周辺から —

吉田 輝義*

概要

数学は文学に似ています。小学校では、国語と算数が対になっています。アメリカ型の大学では、法・医・工・経営・教育などの学部は大学院なので、本来の大学の学問は理学と人文学だけです。大ざっぱには、ものごとのしくみを考えるのが理学で、ひとのいとなみを考えるのが人文学ですが、そのうち数学と文学は、人類の脳が際限なく紡ぎだす、何らかの意味を持った記号・言葉の羅列です。どちらも膨大な文献の集積がありますが、その他の学問でいう意味での知識の蓄積・進歩はなく（だから数学と文学は古代のものから全て勉強せざるを得ません）、その他の学問に応用される考え方・方法を提示することはあっても、それ自身は無目的な活動なのかもしれません。

ガロア理論は、一般の 5 次方程式に解の公式が存在しないことを示しただけでなく、代数学の主要な対象は方程式ではなく代数系（群・環・体）であることを示しました。フェルマー予想は 350 年の後に証明されましたが、それはフェルマーの方程式について何ら新しい知見や重要性をもたらさず、むしろその特定の方程式の徹底的な無意味さを示すような証明でした。数学の歴史は、人間が数・図形・関数、ひいては論理・知識・思考に関する見方を絶えず破壊・再創造してきた歴史のようです。人間の脳にはそういう衝動があるのだと思います（言語表現を続ける衝動と同様に）。大学の学部レベル（数学科）で学ぶ、20 世紀に起きた数・図形・関数の概念の変革を概観しつつ、現代数学について考えてみたいと思います。

A 数学の目的・応用

「数学、あるいは数学の学習・研究は何の役に立つのでしょうか？」という問いに対する可能な答えを考え、以下の 4 つに分類してみました。

(1) 数学を勉強すると受験に役に立つ。訓練すると競争に有利である、という個人にとっての有用性。そのような状況が作られている理由は、社会が、人間のある種の能力を客観的に測り競争させ選別するという用途に数学を使っているということでしょう。どんな能力でもよいから、人間を選別するために、統計的に大きなばらつきが現れてしかも客観的に安定した能力差を測定できるような題材を選べ、と言われたら、最も便利な題材として数学の能力が選ばれるかもしれません（数学の能力が実際に有用かどうかとは全くかわりなく）。正誤の判定・点数の評価も明確で、しかも最も易しい数学から非常に難しい数学まで、統計的分布のかなり端の方まで競争させ順位をつけ選別することができます。しかも、ここで測られた「数学の能力」が社会にとって有用なその他の能力と何らかの相関性があり、したがって高い社会的地位を与えられる人材を選別するのに適した指標になる、というように一般的に（選別される当事者も含めて）感じられている、というおまけもついてきます。人間を序列化し選別するという非常に困難な課題のための、現代社会にとって便利な道具として数学が使われています。

*University of Cambridge, Department of Pure Mathematics and Mathematical Statistics

(2) 科学技術への応用．工学・経済学のための問題意識に直接応える応用数学（例えば確率論・統計学）があります．また物理学，例えば応用数学では流体力学や航空工学，純粋数学では量子力学（素粒子・物性理論）に応用される数学があります．物理学の学問的関心に応える他に，社会全体へのインパクトとしては，前者は軍事・宇宙工学，後者は半導体・核兵器・原子力発電などへ応用されます．とくに後者は現代数学なしには現れなかったものですが，逆に，半導体と核技術を除けば人類は本質的には18世紀までに創り出された数学しか使っていないと言うこともできます．より偶然的な純粋数学の応用として，整数論や代数幾何学の暗号理論への応用があり，これはインターネット全体，例えばオンラインショッピングなどを支える重要な技術です．ただし暗号理論への数学の応用も，もとは軍事利用のために発展したものです．これらすべてについて，数学の「進歩」は広い意味で近現代の資本主義社会の商業・軍事システムに牽引されてきた面があります（現在のアカデミアでの数学研究の究極的な資金源についても同様です）

(3) 論理的思考力そのものの重要性．実生活においても数学的 数理的 論理的な物の考え方が役に立つと言われています．実生活に「役に立つ」かどうかを別にしても，数学を学ぶことで思考力が訓練されるとされ，思考を用いることは人間として日常的にも（数独などの「頭の体操」）実存的にも（Cogito, ergo sum / roseau pensant）重要なことであると思われています．もう少し高尚な文脈では，狭義の学問（理学・人文学）の基礎として数学が重要な意味を持っているとされています．基礎学問の構造にはあとでまた触れますが，学問をするための基礎的思考力，とくに「ものごとのしくみ」を考える（理学）のための言語・方法を数学が提供していると考えられています．より直接的に，自然科学の理解のために数学が必要である，とも言われますが，物理学を除く自然科学においては，小学校で学ぶ算数以上の数学が本質的に活躍する場面は少ないかもしれません．人文系でも，古代ギリシャの幾何学・ヒルベルトの公理主義・ゲーデルの定理などの数学基礎論が哲学・文学に直接与えてきた影響は大きなものです．

(4) 数学は美しい．数学は芸術である．あるいは，数学はおもしろい！「数学をする」という行為は自己目的化されることがあります．これは，仮に「何の役にも立たなく」ても数学に意義を認めるという意味で，問いそのものを無化しているとも言えますが，美しい・おもしろいという言葉は，数学が人間に審美的快感あるいは愉悦を与えるということですから，より直接的に「役に立つ」ことを主張しているとも言えます．

事前に以上の4つのカテゴリーを考えておきましたが，実際に講義で生徒さんたちに質問してみたとき出てきた答えは，すべていずれかのカテゴリーにあてはまるものでした．ただし，真っ先に出てくると思った(1)を挙げる生徒さんがいなかったのは意外でした．これらのカテゴリーに便宜的に次のような名前をつけてみます：

- (1) 現実主義 realism
- (2) 実用主義 pragmatism
- (3) 教養主義 academism
- (4) 耽美主義 aestheticism

数学は，ほとんど身体的といってもいいような人間の脳の基本的な機能を用いる営為ですから，数学の「目的」として上の4つのカテゴリーのどれを思い浮かべるかによって，その人の基本的な性向・世界観がうかがえるのではないのでしょうか？（例えば将来どんな職業につくかをこれで

占えるかもしれません。)

また、数学(算数)と対をなす文学(国語)について同じ問い(「文学(国語)は何の役に立つのでしょうか?」)を考えた場合、その答えはやはり上の4つのカテゴリーを生むように見えます。(1) 国語力は何より試験に役立ちます。あらゆる資格試験は国語力の試験だといっても過言ではないでしょう。(2) 実生活(「コミュニケーション」)にも役に立ちます。良いラブレターを書けるという実用的な意味でも、あるいは法律・政治・ビジネスその他各種の人間の社会生活、すなわち人間の支配と力の行使にも。(3) また文学は狭義の学問(哲学・歴史学・社会学)の基礎でもあります。(4) そして詩歌・演劇・小説などが芸術の大きな部分をなしていることも言うまでもありません。

数理能力と言語能力は、表面的には、本質的に「実用的な」能力であるように見えますが、その「目的」は全く異なる4つの方向に拡がっているようです。これらの能力は、もともとは生物としては「役に立たない・目的のない」脳の機能であったものを、ヒトだけが偶然的に爆発的に発展させてしまった能力なのかもしれません。

私は大学教員という職業を選んだ人間なので、数学の目的としては上の分類では(3)にあたる立場をいちばん気持ちよく考えることができます。私は10年前にアメリカの大学院に留学して、今はイギリスの大学で教えているのですが、日本で考えていた「学問」の概念とは違う形の学問の構造を向こうで学んだので、ここでそれを紹介します。上の分類の(2),(3)の違いは、私は「広義の学問」と「狭義の学問」の違いと考えています。狭義の学問とは理学と人文学を指します。これはアメリカ型の総合大学では Arts and Sciences つまり教養学科と呼ばれているもので、大学の4年間はこの狭義の学問だけを学び、広義の学問はそのあとの大学院(Graduate School または Professional School)で学びます。つまり、日本の大学でいう医学部・法学部・工学部・農学部・薬学部・教育学部・経済/経営学部、つまり理学部・文学部以外のすべての学部で教わる「学問」は、アメリカでは大学院で学ぶこと、つまり職業訓練であって、大学院に進む前に誰もが理学か人文学を学ぶという建前になります。この「狭義の学問」の概念は古代ギリシャから中世を通じて続いた西洋のアカデミアの伝統に基づくものですが、日本の大学システムにはあまりはっきりと現れていないので、簡単に説明しておきます。

大まかには、理学は「ものごとのしくみ」を考える学問で、人文学は「ひとのいとなみ」を考える学問です。理学は数学(論理学)・物理学・化学・生物学・地球科学など、人文学は文学(言語学)・哲学・歴史学などからなり、後者には社会学・心理学を含めることもあります。これらの学問分野のあいだには大まかな階層構造があり、例えば化学に全く触れずに数学を学ぶことはできますが、化学に全く触れずに生物学を学ぶことはできません。その意味で、数学の方が化学より基礎的であり、生物学よりも化学は基礎的であるということが出来ます。しかし、基礎的な学問を修めないと応用的な学問はわからない、ということではありません。専門家になる人を除けば、むしろ学問全体の構造を知っておくことが大事です。現代においてはこのような伝統的な学問分野の分類などは無意味であると考える人もいますが、それは知識・情報を蓄積するシステムの変化、あるいはアカデミアという組織の運営の変化の話であって、人間がものごとを考える筋道が大きく変わるわけではありません。数理能力と言語能力が理学と人文学の根底にある「基礎的な」脳の機能であることは、このような狭義の学問の構造にも現れています。インターネットの普及以後の学問のあり方については後にまた触れます。

B ガロア理論と群

それでは、数学をするということがどういうことなのか、少しやってみることにします、ここではまず、ガロア理論の説明をします。ガロア理論とは(1変数の)高次方程式の解法の理論で、例えば5次以上の方程式には係数から四則演算と根号によって解を求める「解の公式」が存在しないことを主張します。逆に、2次・3次・4次の方程式の「解の公式」がどのように得られるかという仕組みが理解できれば、どうして5次以上の方程式ではそれができないのかがわかるのですから、ここではそれを見ていくことにします。

(1) 2次方程式 $x^2 + b = 0$. この解は $x = \pm\sqrt{-b}$ です。

「ルート」の意味はこの方程式の解であるということであり、それは定義すなわち同語反復です。ここでしていることはほとんど、特別な形をした2次方程式の解に「名前をつける」ことでしかありません。しかし一つだけ数学的な事実が解明・主張されていて、それは、一つの解に $\sqrt{-b}$ という名前をつけると $-\sqrt{-b}$ がもう一つの解であり、この2つ以外に解はない、ということです。 $-b$ が平方数ではない場合、もし $-\sqrt{-b}$ の方に $\sqrt{-b}$ という名前をつけたとすると、 $\sqrt{-b}$ は $-\sqrt{-b}$ であったことになりやはり同じ答えになります。このことが表しているのは2つの解の間の対称性です。名前をつけるためにはこの対称性をいったん崩す必要があることに注意しましょう。

(2) 2次方程式 $x^2 - ax + b = (x - \alpha)(x - \beta) = 0$. これを解くのは「2次方程式の解の公式」ですが、その方針は、特別な場合(1)、つまり $a = 0$ の場合に帰着するというものです。展開すると「解と係数の関係」

$$a = \alpha + \beta, \quad b = \alpha\beta$$

を得ますが、この a を0にするために、

$$\alpha' = \alpha - \frac{a}{2}, \quad \beta' = \beta - \frac{a}{2}$$

とおけば、

$$\begin{aligned}\alpha' + \beta' &= 0 \\ \alpha'\beta' &= \alpha\beta - \frac{a}{2}(\alpha + \beta) + \frac{a^2}{4} \\ &= b - \frac{a^2}{2} + \frac{a^2}{4} = b - \frac{a^2}{4}\end{aligned}$$

ですから、(1) より α', β' は $x^2 + \left(b - \frac{a^2}{4}\right) = 0$ の解すなわち $\pm\sqrt{\frac{a^2}{4} - b}$ です。したがって $\alpha, \beta = \frac{a}{2} \pm \sqrt{\frac{a^2}{4} - b}$ を得ます(2次方程式の解の公式)。

この(2)から(1)への帰着は、四則演算 $+, -, \times, \div$ だけで行われていて、新たに根号を開く必要はなかった、つまり新たに対称性が現れたりそれを崩したりする必要がなかったことに注意しましょう。解の公式の導出ではこの帰着の部分は複雑に見えますが、一見簡単に見える(1)の部分に比べると、この部分は数学の本質としては単純な一本道にすぎないのです。

(3) 3次方程式 $x^3 - c = 0$. まず特別な場合 ($c = 1$) の $x^3 - 1 = 0$ を解きます. $x = 1$ は解です. から因数分解して $(x-1)(x^2+x+1) = 0$ となり, $x^2+x+1 = 0$ の解は (2) より $x = -\frac{1}{2} \pm \frac{\sqrt{-3}}{2}$ です (すなわち 1 の 3乗根は $x = 1, -\frac{1}{2} \pm \frac{\sqrt{-3}}{2}$ の 3つです). そのうち一方を ζ と書くと ζ^2 も 1 の 3乗根でしかも $\zeta^2 \neq 1$ ですから, この 2つは ζ, ζ^2 と書けます. ζ^2 の方を ζ と書くと $\zeta = (\zeta^2)^2$ は ζ^2 になることに注意しましょう (2次方程式の対称性).

さてこの $1, \zeta, \zeta^2$ を用いると, $x^3 - c = 0$ の解は $x = \sqrt[3]{c}, \sqrt[3]{c}\zeta, \sqrt[3]{c}\zeta^2$ となります. これは 3乗根と平方根 (ζ を表すのに用いた) によって書けているので「解けた」ことにはなりますが, ここでは $\sqrt[3]{c}$ はただの記号ですから, 3つの解のうちどれを表してもよいはずですが, つまりここでも名前をつけるために対称性を崩しています. もし $\sqrt[3]{c}\zeta$ を $\sqrt[3]{c}$ と書いていれば, $\sqrt[3]{c}, \sqrt[3]{c}\zeta, \sqrt[3]{c}\zeta^2$ はそれぞれ $\sqrt[3]{c}\zeta^2, \sqrt[3]{c}, \sqrt[3]{c}\zeta$ と名前が変わりますから, 3つの解をくるくると回す形になります. ここで新たに現れた対称性は, 平面上で正三角形を回転させる時と同じ対称性です.

(4) 3次方程式 $x^3 + bx - c = (x - \alpha)(x - \beta)(x - \gamma) = 0$. これも特別な場合 (3), つまり $b = 0$ の場合に帰着して解くことを試みます. 展開すると「解と係数の関係」

$$0 = \alpha + \beta + \gamma, \quad b = \alpha\beta + \beta\gamma + \gamma\alpha, \quad c = \alpha\beta\gamma$$

を得ますが, ここでラグランジュの分解式 $p = \alpha + \beta\zeta + \gamma\zeta^2, \quad q = \alpha + \beta\zeta^2 + \gamma\zeta$ を導入すると,

$$\begin{aligned} p &= \alpha + \beta\zeta + \gamma\zeta^2, & p\zeta &= \alpha\zeta + \beta\zeta^2 + \gamma, & p\zeta^2 &= \alpha\zeta^2 + \beta + \gamma\zeta \\ q &= \alpha + \beta\zeta^2 + \gamma\zeta, & q\zeta &= \alpha\zeta + \beta + \gamma\zeta^2, & q\zeta^2 &= \alpha\zeta^2 + \beta\zeta + \gamma \end{aligned}$$

となり, また $\zeta^2 + \zeta + 1 = 0$ と $\alpha + \beta + \gamma = 0$ を用いると, 上の式から

$$p + q = 3\alpha, \quad p\zeta^2 + q\zeta = 3\beta, \quad p\zeta + q\zeta^2 = 3\gamma$$

を得ますから, $p, p\zeta, p\zeta^2, q, q\zeta, q\zeta^2$ から,

$$(\alpha, \beta, \gamma) = \left(\frac{p+q}{3}, \frac{p\zeta^2+q\zeta}{3}, \frac{p\zeta+q\zeta^2}{3} \right)$$

として α, β, γ が復元できます. ところが (3) によって $p, p\zeta, p\zeta^2$ は $x^3 - p^3 = 0$ の, $q, q\zeta, q\zeta^2$ は $x^3 - q^3 = 0$ の 3つの解であり, その解き方はわかっていますから, あとは p^3, q^3 を求めればよいこととなります. そのためには:

$$\begin{aligned} pq &= \alpha^2 + \beta^2 + \gamma^2 - \alpha\beta - \beta\gamma - \gamma\alpha \\ &= (\alpha + \beta + \gamma)^2 - 3b = -3b \\ p^3q^3 &= -27b^3 \\ p^3 + q^3 &= (p+q)(p+q\zeta)(p+q\zeta^2) \\ &= (p+q)(p\zeta + q\zeta^2)(p\zeta^2 + q\zeta) = 3\alpha \cdot 3\beta \cdot 3\gamma = 27c \end{aligned}$$

と計算すると, p^3, q^3 は $x^2 - 27cx - 27b^3 = 0$ の 2つの解ですから (2) によって求められます. また p^3 の 3乗根である p の選び方は 3通りありますが, p を選ぶと $pq = -3b$ によって q が定まり, それぞれの選び方が α, β, γ を与えます. これで (4) は解けました.

(5) 3次方程式 $x^3 - ax^2 + bx - c = (x - \alpha)(x - \beta)(x - \gamma) = 0$. これは(2)を(1)に帰着した時と同様にして(4), つまり $a = 0$ の場合に帰着します. すなわち「解と係数の関係」

$$a = \alpha + \beta + \gamma, \quad b = \alpha\beta + \beta\gamma + \gamma\alpha, \quad c = \alpha\beta\gamma$$

における a を 0 にするために,

$$\alpha' = \alpha - \frac{a}{3}, \quad \beta' = \beta - \frac{a}{3}, \quad \gamma' = \gamma - \frac{a}{3}$$

とにおいて, これらを解にもつ3次方程式を計算します. 詳細は省略しますが, α', β', γ' は

$$x^3 + \left(b - \frac{a^2}{3}\right)x - \left(\frac{2}{27}a^3 - \frac{ab}{3} + c\right) = 0$$

の解となり, これは(4)で解けますから, それに $\frac{a}{3}$ を足せば(5)も解けました.

この部分の計算は少々面倒ですが, 係数の四則演算のみでできますから, (2)を(1)に帰着した時と同様に数学的には一本道を進んだだけで, 新たな現象は現れていません. 全く同様にして,

(6) 4次方程式 $x^4 - ax^3 + bx^2 - cx + d = (x - \alpha)(x - \beta)(x - \gamma)(x - \delta) = 0$ も, $a = 0$ の場合に帰着することができるので, その計算は省略して, $a = \alpha + \beta + \gamma + \delta = 0$ の場合を考えましょう. 今度は4次方程式を3次方程式(5)に帰着するために,

$$p = \alpha + \beta = -(\gamma + \delta), \quad q = \alpha + \gamma = -(\beta + \delta), \quad r = \alpha + \delta = -(\beta + \gamma)$$

とおきます. もし p, q, r が求めれば,

$$(\alpha, \beta, \gamma, \delta) = \left(\frac{p+q+r}{2}, \frac{p-q-r}{2}, \frac{-p+q-r}{2}, \frac{-p-q+r}{2}\right)$$

として $\alpha, \beta, \gamma, \delta$ が求まります. まずは

$$\begin{aligned} pqr &= (\alpha + \beta)(\alpha + \gamma)(\alpha + \delta) \\ &= \alpha^3 + (\beta + \gamma + \delta)\alpha^2 + (\beta\gamma + \gamma\delta + \delta\beta)\alpha + \beta\gamma\delta \\ &= (\alpha + \beta + \gamma + \delta)\alpha^2 + (\beta\gamma\alpha + \gamma\delta\alpha + \delta\beta\alpha + \beta\gamma\delta) = c \end{aligned}$$

によって $p^2q^2r^2 = c^2$ です. 次に

$$p^2 = -(\alpha + \beta)(\gamma + \delta), \quad q^2 = -(\alpha + \gamma)(\beta + \delta), \quad r^2 = -(\alpha + \delta)(\beta + \gamma)$$

ですから,

$$\begin{aligned} p^2 + q^2 + r^2 &= -2(\alpha\beta + \alpha\gamma + \alpha\delta + \beta\gamma + \gamma\delta + \gamma\delta) = -2b \\ p^2q^2 + q^2r^2 + r^2p^2 &= b^2 - 4d \end{aligned}$$

(最後の式は練習問題)となるので, p^2, q^2, r^2 は分解3次方程式

$$x^3 + 2bx^2 + (b^2 - 4d)x - c^2 = 0$$

の3つの解であることがわかりました。これは(5)で解けていますから、その解の平方根を取って(つまり(1)を用いて) p, q, r が求まります。平方根の符号の選び方は $2 \times 2 \times 2 = 8$ 通りありますが、 p, q を選ぶと $pqr = c$ によって r が定まりますから、許される選び方は4通りで、それらが上の p, q, r から $\alpha, \beta, \gamma, \delta$ を求める公式に現れています。これで4次方程式も解けました。

これらの解の公式をよく見つめたガロアの洞察は、(2)→(1)、(5)→(4)などの帰着のように四則演算だけでできる部分は、どんなに複雑に見えても数学的には重要なことは起きていないから捨象できるということ、新しい現象が起きているのは、新たな対称性が現れそれを崩して名前をつける、すなわち根号を開くときだけである、ということでした。これらの対称性は、解たちに名前をつける仕方の自由度、いいかえれば「名前をつけかえる」ときに生じる解の置換のなす集合—それらのなす群—によって表されます。2つの解の間の置換(1)および3つの解をくるくる回す置換(3)については説明しました。(4)に現れている対称性は、 α, β, γ をくるくる回すことと同等な、 $p, p\zeta, p\zeta^2$ を回すこと($pq = -3b$ ですからそれに伴って $q, q\zeta, q\zeta^2$ も逆向きに回ります)に加えて、 p^3 と q^3 は2次方程式の2解ですから、ルートの中身が平方数ではない場合は入れ替えることができ、 p と q の入れ替えは β と γ の入れ替え、つまり α, β, γ のなす正三角形を「裏返す」操作を与え、結局 α, β, γ の順序の変更は6通りすべてが現れることになります(3次対称群)。(6)で現れるのは、最大の場合 $\alpha, \beta, \gamma, \delta$ という4つの解の24通りの置換のなす4次対称群ですが、各々の置換は p^2, q^2, r^2 という3つの数の置換(6通り)を導き、これらの3つの数をいっさい動かさないような $\alpha, \beta, \gamma, \delta$ の置換は4通り(全く動かさない、 $(\alpha \leftrightarrow \beta, \gamma \leftrightarrow \delta)$ 、 $(\alpha \leftrightarrow \gamma, \beta \leftrightarrow \delta)$ 、 $(\alpha \leftrightarrow \delta, \beta \leftrightarrow \gamma)$ の4つ)あります。これは例えば立方体の回転によって4つの対角線が置換され、それに伴って3つの直交座標軸が置換される様子と全く同じです。3次・4次方程式の「解の公式」の導出に使われていた式は、これらの対称性をうまく表したものになっています。

ガロア理論の主張は、「方程式」の本質は、上で見たようにその解たちのもつ対称性を表す群(置換群)にあるということです。5次方程式にもし解の公式があるとすると、 n 乗根を開くという根号によってできる「正 n 角形をくるくる回す」という形の対称性を積み上げることで5次対称群(5個のものの置換120通りのなす群)が記述できなくてははいけません。それは不可能であることが5次対称群を分析することで証明できるのです。ガロア理論は従来探し求められていた意味での「解の公式」の不可能を示しましたが、逆に言えば「根号」による解法にそれほどの重要性を与える意味はないことを示したとも言えます。実際、ガロア以後の数学者により、「根号」とは別の特殊な操作(根号=指数関数とは異なるが、よく性質のわかる解析関数を用いるなど)によって解ける方程式を考察するなどの新たな、より豊かな研究が開始されました。

C 群と幾何学

ここで、対称性を表す群というものの説明のために、幾何学からとても基本的な問題「円とは何か？」をとりあげることにします。この問いに対して、ここでは3通りの答えを紹介します。

(A) 紀元前3世紀、ユークリッド(古代ギリシャ)式の定義。円とは平面上のある一点P(中心)からある一定の距離 r (半径)にある(その平面上の)点全体のなす図形である。

(B) 17世紀、デカルト式の定義。円とは xy 平面上で $x^2 + y^2 = r^2$ をみたす点 (x, y) 全体のなす集合である。この場合、円の中心は原点P(0,0)、半径は r である。

これらの定義はいずれも厳密で正確なものですが、私たちが直観的に図形を捉える方法と一致しているとは言えません。親戚のおうちで3歳のこどもに「円ってなあに」とたずねられたとき、これらの定義が役に立つでしょうか？円を見ても、ふつう中心は見えません。ましてや (x, y) 座標が2次式をみたしているかどうかなど皆目わかりません。私たちにとっては、ユークリッド式の定義はコンパスで円を作図するための定義、デカルト式の定義はコンピュータで画面に円を(近似的に)描画させるための定義と考えたほうが自然です。3歳のこどもに「円とは何か」を伝えるには、「まるい」とはどういうことかを伝えることが早道であり、「まるい」とはどういうことかを伝えるには、まるいものをくるくる回してみせるのが簡単です。「まるいものをくるくる回す」ことに最も近い定義を与えるのが、群の考え方をういた現代数学の定義です。

(C) 19世紀、ガロア・リー式の定義。円とは、その形を変えないまま、各実数 θ に対する操作 T_θ (角 θ 度の回転) であって次の性質をみたすものを行うことができる対象である：

- (i) T_0 は「何もしない」操作である。
- (ii) $T_\theta \circ T_{\theta'} = T_{\theta+\theta'}$ (左辺の \circ は操作の合成、つまり操作を続けて行うということ。)
- (iii) $T_\theta = T_{\theta'}$ となるのは、 $\theta - \theta'$ が360の倍数のときであり、そのときに限る。

「まるい」というのは円という図形のもつ対称性を表す言葉です。対称性とは、他のものならば変形されてしまうような操作(例えば回転・反転)を加えても形が変わらないということです。その図形を変えないような操作全体のなす集合が、その図形の対称性を表す群であり、この場合は回転群という形を取ります。これは「抽象的」つまり対象の具体的な形(例えば平面上の図形であること)にこだわらない考え方なので、円以外の「まるい」もの(例えば円柱、円錐)の「まるさ」もとらえることができます。また、群の概念そのものは図形であることも超えて、例えば方程式の解たちの中の置換群として、数たちの中の対称性を表すこともできます。解たちを適当に置換しても、それらを解にもつ方程式は不変に保たれるということです。図形の「形」の本質が対称性であり、方程式(その解たち)も対称性をもつのであれば、方程式にも「形」があると考えるのが自然です。ガロア理論は、方程式のもっている「形」、その本来の姿を人類史上初めて「見た」理論だったといえることができます。

再び円の定義に戻ると、同じ円という図形を(A),(B),(C)という三通りの仕方でとらえることができるということは、それらに関係があるはずですが、その関係をとらえるために、学校で学ぶ数学の技術が活躍します。まず(A)と(B)を結ぶのは、原点 $P(0,0)$ と点 (x, y) の間の距離を r とすると $x^2 + y^2 = r^2$ という式がみたされること、つまりピタゴラスの定理です。(B)と(C)を結ぶには、角 θ の回転を (x, y) 座標の上で表すことが必要です。これは、三角関数を使って次のように表されます：

$$T_\theta(x, y) = (x \cos \theta - y \sin \theta, x \sin \theta + y \cos \theta)$$

これは行列を使って

$$T_\theta \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

と表すのが便利です。このとき、点 (x, y) が円にのっている、つまり $x^2 + y^2 = r^2$ をみたしているとき、角 θ 回転した点 $(x \cos \theta - y \sin \theta, x \sin \theta + y \cos \theta)$ もまた同じ円にのっていることは、

$$(x \cos \theta - y \sin \theta)^2 + (x \sin \theta + y \cos \theta)^2 = x^2 + y^2 = r^2$$

という計算からわかりますが、この計算は $\cos^2 \theta + \sin^2 \theta = 1$ という関係を使っています。また、(C) の条件 (ii) を (B) の言葉で表すのは三角関数の加法定理に他なりません：

$$\begin{pmatrix} \cos(\theta + \theta') & -\sin(\theta + \theta') \\ \sin(\theta + \theta') & \cos(\theta + \theta') \end{pmatrix} = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \begin{pmatrix} \cos \theta' & -\sin \theta' \\ \sin \theta' & \cos \theta' \end{pmatrix}$$

このように、(C) が成り立っていることを (B) の言葉で確かめていく過程でわかることは、(B) の式 (方程式) $x^2 + y^2 = r^2$ が、行列 $\begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$ の表す 1 次変換という「対称性」をもっているということです。これは、円という図形を表しているのだから当たり前なのですが、方程式だけを見てそれが隠し持つ対称性を見抜くのは容易なことではありません。

ガロアの洞察も、1 変数の方程式ですがこれに似たものです。 $x^2 - 3x - 5 = 0$ という方程式は、 x を $3 - x$ で置き換えるという操作で不変です ($(3 - x)^2 - 3(3 - x) - 5 = x^2 - 3x - 5$) が、それは一目見てわかるというわけにはいきません。しかも $3 - (3 - x) = x$ ですから、この操作は x と $3 - x$ を互いに置換する操作になっていて、2 度合成すると元に戻るわけです。同様に、4 次方程式 $x^4 + 52x^3 - 26x^2 - 12x + 1 = 0$ は x を $-\frac{4x}{(1-x)^2}, \frac{1-x}{1+3x}, \frac{(1-x)(1+3x)}{-4x^2}$ で置き換えるという操作で不変になります (ガウス 19 歳の日記より) が、それを見抜くのはさらに困難です。しかし、前節で見たガロアの一般的な洞察は、これらの「隠れた置換」たちの合成のなすパターン、すなわち置換群が方程式を「解く」操作を支配しているのだ、というものでした。

上では、円に対する 3 つのアプローチを比較することで三角関数が必要になることを見ましたが、高校数学に現れるベクトルの概念も、「平面」「空間」という「図形」の「形」を群論的にとらえることで自然に現れます。円の「形」が「まるい」であるように、平面の「形」は「たいら」であることです (正確には、平らであって無限にのびている)。「たいら」であるという「対称性」を表す操作は、平行移動です。つまり、平行移動を行ってもその形が変わらない、それが平面という形の本質です。この平行移動という「操作」を表しているのが平面ベクトルであり、この操作の合成はベクトルの足し算です。3 次元空間は、私たちの世界がその中に入っている容器物ですからその「形」は見えにくいのですが、やはりその「形」の本質は「たいら」であることです。これを表しているのが空間ベクトルとその合成であるということになります (平面・空間には拡大縮小という操作による対称性もありますが、その操作はベクトルでは表されません。ただし、その操作は、ベクトル全体のなす集合における拡大縮小 (実数倍) に反映されています)。

本節で説明したことを一言でまとめると、現代数学での考え方によれば「形」とは「対称性」であり、「対称性」を表す言葉が「群」であるということです。19 世紀になって、群という考え方をを用いることで初めて、私たちが直観的に「形」を考えたときに用いる考え方を直接に厳密に取り扱うことができるようになりました。

D 20 世紀の数・図形・関数—数学とは何か？

さて、前二節で見た数学の内容を踏まえて、「数学とは何か」という問いに戻りたいと思います。この問いへの答え方として、真正面から数学を定義することは難しいとしても、数学を分類してそれぞれの部分について説明するという方法があります (百科事典的な答え方)。伝統的には、数学には次の 3 つの分野があることになっています：

- (a) 代数学：数・式，すなわち「四則演算を施せるもの」を扱う．
- (b) 幾何学：図形，すなわち「部分と全体」，「形」をもつものを扱う．
- (c) 解析学：関数，すなわち量と量と間の「関係」を扱う．

しかし，数学には，代数幾何学，解析幾何学，さらには代数解析学といった分野がありますから，このように数学を対象によって分類するのは見当はずれにも見えます．古典的な数学では，

- 代数学 解析学：多項式を関数と考える．
- 解析学 幾何学：関数のグラフを考える．
- 幾何学 代数学：図形を表す方程式を考える（座標平面・空間）．

という形での関連づけが起きていました．さらに，前節で見たように，方程式にもその群があり，したがって「形」をもつ，というのは，数を図形と考えることで代数学を幾何学的に考えていることになります．このように，とくに 20 世紀の現代数学では，上の矢印とは反対向きの関連づけが活躍しました：

- 代数学 幾何学：方程式・代数系にも「形」がある（ガロア理論・スキーム理論）．
- 幾何学 解析学：図形もその上の関数たちを用いてとらえるべきである（多様体論）．さらには図形そのものもある種の関数（圏のあいだの関手）と考えられる．
- 解析学 代数学：関数とその微分積分の理論にも線型代数（関数空間）・作用素環などの四則演算的方法が有効である．

こうなってくると，やはり伝統的な三分類は無意味なものなのだとということなのではないでしょうか？

ここからは私見になりますが，この三分類は数学の分類・数学の対象の分類としてはあまり意味のないものですが，上のように相互浸透が起きても，やはり依然としてこれら 3 つの考え方のあいだに関係がつくという形をとっていることは興味深いことです．つまり，全く新たな形の数学が現れてすべてを同時に説明するというようなことは起きていません．私は，この 3 つの分類は数学の対象あるいは方法の分類と言うよりは，ヒトの脳の数理能力の分類，より具体的には人間の脳がものごとを論理的に「理解する」ということの 3 つの形なのではないか，と考えています．数学を「理解する」というのはどういうことなのかというのは微妙な問いで，突き詰めて考えれば考えるほどよくわからなくなります．それに対する答えとして，例えば「代数的な理解」というものがあるのではないのでしょうか．これは，四則演算のように，対象に次々と操作を施していき，その操作が従うルールや操作を実現するアルゴリズムを知る（見る）と，人間の脳は何かを「理解した」と感じるのではないかということです．例えば知らない街に行って，そこでバスや地下鉄に乗るためのアルゴリズム，手続きを知る（特定の操作を特定の順序で遂行すると特定の結果が現れる，ということを確認する）と，その街に少し近づいたような，その街について何らかの「理解」を得たような気持ちになります．その「理解」にとっては，どのような仕組みと動力で自動券売機が機能するかとか，交通システムをどのような行政機構が運営しているかといったことの「理解」は関係がないのです．数学において「数・式とは何か」と問う場合，その答えは「四則演算を施せるもの」に他ならないのですが，その四則演算とは，結合法則・分

配法則・交換法則などの「ルールに従う操作」でしかありません。しかも、数や式そのものに意味づけをする以前に「ルールと操作ありき」なのです。例えば、累乗の式

$$a^b = c$$

は、 b が正の整数であれば、 a を b 回かけると c になるという意味ですが、 b が負であったりさらに一般の有理数や実数の場合は意味づけが難しい式です。しかし人間はこの式がいつでも意味をもつように数学を拡張していきました（そのためには、幾何学や解析学が必要でした）。さらに、

$$a = \sqrt[b]{c}, \quad b = \log_a c, \quad c = a^b$$

が同じ意味をもつという「ルール」を決めた上で、これら累乗根・対数・指数が整合的な「意味」をもつように、数学を（数の概念そのものも含め）拡張しました。これらの記号で表される操作にとっては、上の3つの式の等価性や指数法則といった「ルールをみたく」ということが至上命題で、そのためには例えば $\log_a c$ の値が一つに定まらない（多価関数）といった面倒な状況も受け入れてしまいました。それは、人間の脳がどういう状況を「理解できる状況」ととらえるか、ということについて強力な示唆を与えています。ここで「理解」されている「ルールに従う操作の列」といったものが「記号化」されていることも重要です。 $x^2 + 2 = 0$ という方程式の解のうち的一方に $\sqrt{-2}$ という記号を与えたのは数学の進歩にとって便利なものではありませんでしたが、それはやはり任意な記号の選択だったのであって、 $\sqrt{-2}$ でなく「あ」であっても構わなかったわけです（ちなみに、私たちは英字やギリシャ文字で数学をするのが当たり前と思っていますが、これは西洋人にとってはひらがなで数学をしているようなもので、面積を「め」で表す、などと言っているようなものです。ひらがなや漢字を数学の記号として使おうとすると西洋人は面白がりません。）そしていったん「あ」が数を表す記号であり一定のルールに従う操作を許すと考えれば、「 $3 + \text{あ}$ 」も意味をもつこととなります（だから $3 + \sqrt{-2}$ も数になるわけです）。ルールに従う操作を許す対象、というのが数学における「記号」の意味です。このような状況を「理解した」と感じる人間の脳の状態を、ここでは「代数的な理解」と呼ぶことにします。

ここでは立ち入りませんが、同様に、部分と全体をもつ対象の「形」ととらえるという「幾何学的な理解」、2つの対象の「関係」を記述するという「解析学的な理解」というものもあるように見えます。これらの「理解の原型」があらゆるタイプの数学・数理、ひいてはあらゆるタイプの論理的思考にも認められるのではないのでしょうか？数学は「ものごとのしくみ」を考える学問である「理学」の基礎をなすと考えられている、と言いました。数学の3つの分野の真の意味は、人間がものごとのしくみをとらえる能力、論理的に「理解する」脳機能の3つの形であるということなのではないのでしょうか？そのようなことが何らかの脳科学の知見によって裏付けられる可能性はないのでしょうか？また、そうだとすれば、「数学を使って」自然科学が記述され理解される、ということは驚くべきことでも何でもなく、むしろ人間が自然について何かを「理解した」と考えられるとき、それはここで説明したような意味で数学的（「代数的・幾何学的・解析学的」）に記述されたものでしかありえない、という人間の脳機能の限界の表れにすぎないのではないのでしょうか？そうだとすれば、最初のA節で述べた数学の目的・応用のうち、(3) はほとんどトートロジーであり、(2) も直ちに従う帰結となり、(1) および (4) も人間の脳の特性の帰結として説明されることとなります。これと同様のことを国語・文学・言語学について考えること（とくに言語を生得の脳機能と考える生成文法などの立場から）も興味深いかもしれません。

E スタディガイド

私が中高生だったのはほんの15~20年前ですが、インターネットの登場によって学問へのアクセスは様変わりしました。ブルーバックスや「数学セミナー」などの啓蒙書を読んでガロア理論やスキーム理論に憧れても、その内容を学ぶにはまずは文献の題名を知り、大書店や神田の古書店（明倫館書店など）に通ってそれを探し、それでも見当たらなければ、結局大学に入学して数学科の図書館に入れる時が来るのを待つしかないのだ、と溜息をついて諦めるほかはありませんでした（本郷にあった東大数学科は果てしなく遠い場所でした）。大学に入学してまずしたことは数学科の図書館からグロタンディークのEGA（「あまつさえ美しい青表紙」の…）を借りだしてひたすらコピーを取ることでした。

今は、単純に「ガロア理論」「スキーム理論」とGoogleに入力して、現れるウィキペディアの記事を順々に読んでいくだけで、本物の数学そのもの（例えば群の定義、ガロア群の定義、など）をかなりの部分「知る」ことができます（数学だけでなく、「roseau pensant」でも「生成法」でも同様です。）ガロア理論そのものを記述した講義録も、グロタンディークのEGAもネットからすぐに手に入ります。それは、学問そのものが身近になり学ぶことが易くなったことを意味するのでしょうか？

知識、より正確には「情報」を独占するギルドとしてのアカデミアの役割が崩れつつある以上、単なる情報の整理・貯蔵・処理（インターネットがやってくれること、コンピュータにできること）を除いた部分が学問的営為として生き残っていくことになるでしょう。そこで残るのはまさに、前節で考察した「理解する」という脳機能ではないでしょうか？

「学問」-「情報」=「理解」

ここで「情報」とは「ウィキペディアに書いてあること」で、「理解」は脳がやること、ヒトの脳にしかできないことということになります。より応用的な学問では情報へのアクセスを制限する動きもありますが、数学の論文はほとんどすべて無料でネットから手に入りますから、極論すれば大学の数学科に入学しなくても数学の研究をすることはできます（もちろんそれは、その時点でのアカデミアで要求されるようなスタイルの「研究」ではないかもしれませんが）。

「コンピュータにはできず、ヒトの脳にしかできないこと」をするのは、動物種の中ではヒトのみが持っていると考えられている脳機能、つまり数理能力・言語能力そのものであると考えるのは自然でしょう。また、コンピュータは「役に立つこと」、つまり外部から与えられた目的のために必要な処理をすることは得意なのですから、コンピュータにはできないことを可能にするのは、まさに「役に立たない」ような脳機能であるべきです。数理能力や言語能力は本来「役に立たない」機能であるからこそ、このように人間のあらゆる活動（「役に立つ」ものそうでないものも含め）の基盤として働くのでしょうか。これからの学問は、20世紀の学問が行った以上に、ヒトの脳が何を「理解」しているのかに鋭く迫っていくことが求められるかもしれません。

（本稿は、講演の内容をほぼそのまま記録したものです。2012年1月15日記）