ガロア理論の基本定理を圏論で

—圏論の学習ノートより—

佐　藤　　創

まえがき

新田義彦教授とはこの数年，甘睡会と称する私的なセミナーで圏論を学ぶ苦楽を共にしている間柄から，新田教授の定年ご退職を記念してささやかな論考を寄稿させていただきます．

最初に圏論とその魅力の一端を簡単に紹介した後，以前から関心を抱いていたテーマ「ガロア理論の圏論による記述」に関して学び得た事柄を整理して記すことにします．

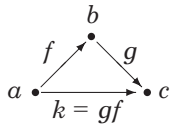
ガロア理論は代数方程式を解くアルゴリズムの存在条件を明らかにし，5 次以上の方程式に根の公式が存在しないことを導く理論として有名ですが，ガロア（Évariste Galois）はこの理論構築を 20 歳の若さで成し遂げた末，決闘で倒れた革命的天才としてさらに有名です．

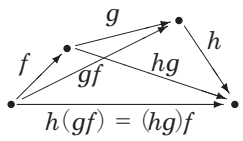
I　圏とは

圏論は 20 世紀の中頃，Eilenberg, Mac Lane, Freyd, Lawvere らによって創始され，発展してきた比較的新しい数学の潮流である．圏，函手，自然変換などの枠組みを用いて，数学を横断する概念の普遍性を明らかにし，さらに人間の論理的思考を普遍原理によって解明しようとしているように思われる．

1　矢の数学

一言で言えば，圏論は矢の数学である．圏論では射，函手，自然変換という 3 種類の矢が登場する．矢は有向線分であって始点と終点をもつ．ここでは「射」について述べる．射の始点，終点となるものは「対象」と呼ばれ，対象は射とともに圏を構成する．射 f の始点が対象 a，終点が対象 b のとき，これを $f : a \to b$ という形式で表現し，a から b への射という．さらに，b から c への射 $g : b \to c$ に関しては，常に結合された射 $g\,f : a \to c$ があるものと定め，これを f と g の合成射と呼ぶ．a から c への射 $k : a \to c$ が合成射 $g\,f$ と一致するとき，$k = g\,f$ という関係を図で表現すると下図左の 3 角図式となる．このように経路によらず射が一致することを示す図式を可換図式と呼ぶ．



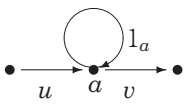


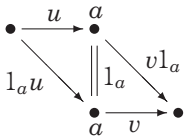
射の結合法則 $h(g\,f) = (h\,g)\,f$ の成立することは，上の図右の可換図式によって表現される．なお，一般に $g\,f$ と記したとき，この結合が可能な条件（f の終点 = g の始点）は断りなく前提とする．

各対象 a には恒等射 $1_a : a \to a$ が存在し，それぞれ a を終点，始点とする任意の射 u，v に対して，次の等式を満たす：

$$1_a\, u = u, \qquad v\, 1_a = v.$$

恒等射 1_a は，a から a に戻るループ，あるいは，対象 a を 2 度描きそれを結ぶ等号で表す．恒等射 1_a と対象 a を同一視すれば，射のみで圏を公理化することもできる．





このように図を多用し，概念を視覚化して表現するところが圏論の特徴である．

1 つの圏を名付けて圏 C と呼ぶとき，その対象全体も C で表し，a が圏 C の対象であることを $a \in C$ と記す．a から b への射全体を $C(a, b)$ で表し，a から b への「hom 集合[1)]」と呼ぶ．

すべての集合[2)] を対象とし，写像を射とする圏を **Set** で表す．同様に，すべての群と準同型の圏 **Grp**，すべての位相空間と連続写像の圏 **Top** など，壮大なスケールの枠組みが用意される．

2　集合の圏 Set ―写像における双対

具体的な例をあげて，圏論の魅力の一端を紹介する．

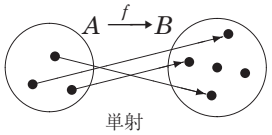
初等解析の「単射（1 対 1 写像）」と「全射（上への写像）」はよく知られているが，両者の関係は必ずしも明解ではない．集合 A, B 間の写像 $f : A \to B$ について，定義はこうであった：

- f が単射であるとは，任意の $x, y \in A$ に対して $x \neq y$ ならば $f(x) \neq f(y)$ であること．　(1)
- f が全射であるとは，任意の $z \in B$ に対して $f(x) = z$ となる $x \in A$ が存在すること．　(2)

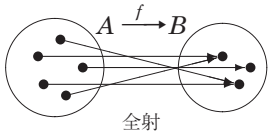
単射の定義(1)と全射の定義(2)は形式的な類似性に乏しく，その間に単純な関係があるようには見え

1)　hom は homo-morphism の略で，hom 集合 $C(a, b)$ は $\hom_C(a, b)$ とも記す．ちなみに，射は morphism である．

2)　集合論の逆理を避けるために，ユニバース $\mathcal{U}$ を想定し，集合はその要素に限定する．圏 **Grp**，**Top** などについても同様．



単射



全射

ない．一方，圏にはモニック射，エピ射という概念があり，次で定義される：

- f がモニック射であるとは，任意の射の対 u, v について $fu = fv$ ならば $u = v$ となること．　(3)
- f がエピ射であるとは，任意の射の対 u, v について $uf = vf$ ならば $u = v$ となること．　(4)

圏 Set において定義(3)，(4)を適用すると，単射はモニック射であり，全射はエピ射であることが容易に導かれる[3]．したがって，単射と全射の定義が集合の要素に言及せずに，射の性質のみで表現できた（これが素晴らしい）．図式ではモニック射とエピ射の性質は次のように描かれる：

モニック射	エピ射	参考図
$\bullet \underset{v}{\overset{u}{\rightrightarrows}} \bullet \xrightarrow{f} \bullet$	$\bullet \xrightarrow{f} \bullet \underset{v}{\overset{u}{\rightrightarrows}} \bullet$	$\bullet \underset{v^{\mathrm{op}}}{\overset{u^{\mathrm{op}}}{\leftleftarrows}} \bullet \xleftarrow{f^{\mathrm{op}}} \bullet$
$fu = fv \Rightarrow u = v$	$uf = vf \Rightarrow u = v$	$u^{\mathrm{op}} f^{\mathrm{op}} = v^{\mathrm{op}} f^{\mathrm{op}} \Rightarrow u^{\mathrm{op}} = v^{\mathrm{op}}$

左のモニック射の図式で矢の向きをすべて逆にする（肩付きの $^{\mathrm{op}}$ で表す．op は opposite の略）と右の参考図となり，これはエピ射の図式と一致する．射 $f^{\mathrm{op}} : y \to x$ を $f : x \to y$ の双対射といい，一般に，矢の向きを逆にした概念と元の概念は互いに「双対」をなすという．この意味で，「単射と全射は互いに双対である」という明解な結論を得る．

なお，圏 C のすべての射 f をすべてその双対射 f^{op} で置き換えると，対象は C と同一であるが新しい圏ができる．これを C の「逆圏」と呼び，C^{op} で表す．この考え方を次節で利用する．

射 $f : x \to y$ が同型射であるとは，f が左逆射 u（$uf = 1_x$）と右逆射 v（$fv = 1_y$）をもつことと定義される（このとき，$u = u(fv) = (uf)v = v$ である）．対象 x, y が「同型である」とはその間に同型射が存在することである．

Set では射がモニックかつエピならば同型射である[4]．集合 A, B の同型は $|A| = |B|$ を意味する．

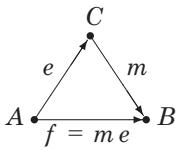
また Set では，任意の写像 $f : A \to B$ に対して，ある集合 C とエピ射 $e : A \to C$，およびモニック射 $m : C \to B$ が存在して，$f = me$ となる（$C = f(A)$, $e : a \mapsto f(a)$, $m : c \mapsto c$ とすればよい）．これを f

---

3) $f : A \to B$ を単射，また $u, v : C \to A$ について $fu = fv$，すなわち $\forall c \in C, f(u(c)) = f(v(c))$ とする．f の性質より $u(c) = v(c)$．ゆえに，$u = v$（f はモニック射）である．逆に，f をモニック射とする．1 点集合 $\{s\}$ から A への写像 $u : s \mapsto x, v : s \mapsto y$ に対して［$fu = fv$ ならば $u = v$］，すなわち［$f(x) = f(y)$ ならば $x = y$］（f は単射）である．全射とエピ射の同値性を示すには背理法を使う．

4) これは圏 Set の特殊性で，「全単射」が同型射の意味で使われるが，一般にはそうではない．一般に，左逆射をもてばモニック射，右逆射をもてばエピ射である．右逆射をもつモニック射，および，左逆射をもつエピ射は同型射になる．

のモニック･エピ分解という．エピ射 e は f の値により A の要素を「分類」し，モニック射 m は f の像となる B の部分を「限定」する．一般の圏ではモニック・エピ分解は必ずしも可能ではない．



Ⅱ　半順序の圏

ガロア理論を圏論で記述するためには，半順序の圏を用意する必要がある．一般に，順序とは反射律，反対称律，推移律を満たす関係をいう．半順序とは，２つの要素 x, y に順序 $x \preceq y$ の有無が設定されている集合である．すべての要素の間に順序のある全順序（線形順序）は半順序の特別な場合である．

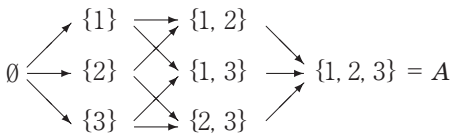
1　対象と射

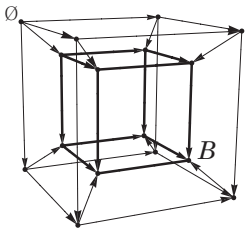
半順序集合 P の要素を対象とし，対象 x，y に対して，$x \preceq y$ のとき射 $x \to y$ が１つだけ存在し，そうでないときは存在しないものと定める．任意の $x \in P$ に対して反射律により恒等射 $1_x : x \to x$ が存在し，推移律により射の結合法則が成り立つ．したがって，P は圏とみなすことができる．

半順序の圏ではすべての射はモニックかつエピであるが，同型射とは限らない．反対称律により同型射は恒等射に限る．

例１　ある集合 A の部分集合全体 $\mathcal{P}(A)$は，集合の包含関係によって順序関係（$x \preceq y \Leftrightarrow x \subset y$）を定義すると半順序の圏となる．例えば，$A = \{1, 2, 3\}$ のとき，圏$\mathcal{P}(A)$における射は見慣れた次の可換図式になる（恒等射は省略）．射は写像ではなく，$\{1\}$ から $\{1, 2, 3\}$ への射は１つに限ることに注意．

$B = \{1, 2, 3, 4\}$ のときの半順序の圏 $\mathcal{P}(B)$の射は右の可換図式（４次元立方体）で表される．　□





2　順序保存関数とガロア接続

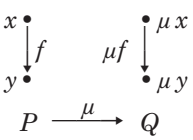
２つの半順序の圏 P, Q において，関数 $\mu : P \to Q$ が順序を保存するとき，すなわち

任意の対象 $x, y \in P$ に対して，$x \preceq y \Rightarrow \mu x \preceq \mu y$

であるとき，関数 μ は射に関して

P の射 $f : x \to y$　に対して，　Q の射 $\mu f : \mu x \to \mu y$

を対応させているものと考えれば，μ は「函手」の条件



$$\begin{cases} \text{任意の対象 } x \in P \text{ に対して，} \ \mu 1_x = 1_{\mu x}, & \text{（恒等射の保存）} \\ \text{任意の } P \text{ の射 } f, g \text{ に対して，} \ \mu(fg) = (\mu f)(\mu g) & \text{（射の合成の保存）} \end{cases}$$

を満たすので，$\mu : P \to Q$ を函手とみなす．函手は圏から圏への「矢」である．

順序を反転する関数 $\bar{\lambda} : P \to Q$ $(x \preceq y \Rightarrow \bar{\lambda} x \succeq \bar{\lambda} y)$ は，それを Q の逆圏 Q^{op} への関数 $\lambda : P \to Q^{\mathrm{op}}$ と考えれば，λ は順序を保存する．

さて，2つの順序保存関数 $\lambda : P \to Q^{\mathrm{op}}$, $\rho : Q^{\mathrm{op}} \to P$ について

$$\text{任意の対象 } p \in P, q \in Q \text{ に対して，} \quad \lambda p \preceq q \ (Q^{\mathrm{op}} \text{ 上で}) \Leftrightarrow p \preceq \rho q \ (P \text{ 上で}) \tag{5}$$

が成り立つとき，順序保存関数の組〈λ，ρ〉を P から Q への「**ガロア接続**」と呼ぶ．このとき，すべての対 p, q に対する hom 集合 $Q^{\mathrm{op}}(\lambda p, q)$，$P(p, \rho q)$ に関して同型射

$$\varphi = \varphi_{p,q} : Q^{\mathrm{op}}(\lambda p, q) \cong P(p, \rho q) \tag{6}$$

の存在は明らかである[5]．ガロア接続〈λ，ρ〉とφの組〈λ, ρ, φ〉が随伴となることをこの後に示す．

3　随伴

随伴というやや込み入った概念の定義を記す．これが本稿の中心概念である．

まず，自然変換を定義する．B, C を圏とし，2つの函手 $S, T : C \to B$ の間の変換 $\tau : S \to T$ を各対象 $c \in C$ 毎に B の射 τ_c を対応させる関数とする．C のすべての射 $f : c \to c'$ について次の4辺図式

$$\begin{array}{c} c \\ \downarrow f \\ c' \end{array} \quad (C \text{ において}) \qquad \begin{array}{ccc} Sc & \xrightarrow{\tau_c} & Tc \\ {\scriptstyle Sf}\downarrow & & \downarrow{\scriptstyle Tf} \\ Sc' & \xrightarrow{\tau_{c'}} & Tc' \end{array} \quad (B \text{ において})$$

を可換にするとき，変換 τは「自然である[6]」といい，射 τ_c を自然変換 τ の c- 成分と呼ぶ．自然変換は矢の上に点を添えて $\tau : S \dot{\longrightarrow} T$ と記す．自然変換は函手から函手への「矢」である．

hom 集合を函手とみなす発想がおもしろい．すなわち，圏 C の対象の組〈x, y〉に hom 集合 $C(x, y)$ を対応させる2変数関数〈x, y〉$\longmapsto C(x, y)$ は，函手 $C(-,-) : C^{\mathrm{op}} \times C \to \mathrm{Set}$ となる．なぜならば，第1変数を c に固定すると，C から Set への函手 $C(c,-)$ ができる．それは，y に集合 $C(c, y)$ を対応させ，C の射 $f : y \to y'$ には写像 $C(c, y) \to C(c, y')$ として $u \mapsto fu$ を対応させる函手である．同様に，第2変数を $d \in C$ に固定すると，C^{op} から Set への函手 $C(-, d)$ ができるからである．なお，$C^{\mathrm{op}} \times C$ は2つの圏 C^{op} と C の積と呼ばれる1つの圏である．

---

5)　hom 集合 $Q^{\mathrm{op}}(\lambda p, q)$，$P(p, \rho q)$ の要素の個数が，条件(5) により，ともに1または0となるからである．

6)　函手 S と T はすべての射 f に‘同じ効果を与える’という意味．自然性は普遍性を表現するキーワードである．

この発想を発展させる．圏 C と D との間の函手の組

$$C \underset{G}{\overset{F}{\rightleftarrows}} D$$

に関して，対象の組 $x \in C,\ y \in D$ に hom 集合 $D(Fx,\ y)$ を対応させる 2 変数関数は F と組み合せた函手 $D(F-,-) : C^{\mathrm{op}} \times D \ \to \ D^{\mathrm{op}} \times D \to \mathrm{Set}$ となり，hom 集合 $C(x,\ Gy)$ も函手 $C(-,\ G-) : C^{\mathrm{op}} \times D \to C^{\mathrm{op}} \times C \to \mathrm{Set}$ となるので，両者はともに函手 $C^{\mathrm{op}} \times D \to \mathrm{Set}$ である．したがって，その間の自然変換 $\varphi : D(F-,-) \dot{\longrightarrow} C(-,\ G-)$ を考えることができる．そして，φ のすべての成分 $\varphi_{x,\,y}$ が同型射となる自然変換（これを「自然同型」と呼ぶ）

$$\varphi \ = \ \varphi_{x,\,y} : D(Fx,\ y) \ \cong \ C(x,\ Gy)$$

が存在するとき，三つ組 $\langle F,\ G,\ \varphi \rangle$ を C から D への「随伴」と定義する．

随伴はなかなか捉えにくい概念であるが，“数学の至る所で起こっている”と書かれている [7]．詳細は省略するが，例えば，ある圏の 2 つの対象 $a,\ b$ の積 $a \times b$（集合の直積や群の積など）は，積をつくる函手 $F : C \times C \to C$ と対角函手 $\Delta : C \to C \times C$ の随伴として説明できる．また，ベクトル空間 $V,\ W$ の間の線形写像 $f : V \to W$ が V の基底 B 上の関数 $g : B \to W$ から一意に拡張されるという周知の性質も，ベクトル空間の圏 Vct と Set の間の函手の対 $\mathrm{Set} \underset{U}{\overset{G}{\rightleftarrows}} \mathrm{Vct}$（$U$ は忘却函手）を定義して，それが随伴をなすことと説明できる．いずれも，各概念の普遍性を示す．

4　ガロア接続は随伴である

2 つの半順序の圏 $P,\ Q$ について，順序保存関数 $\lambda : P \to Q^{\mathrm{op}},\ \rho : Q^{\mathrm{op}} \to P$ はそれぞれ函手とみなすことができた(II. 2 節)．ガロア接続と随伴の定義により，次の定理が得られる：

定理 1（文献 [1] 第 IV 章第 5 節）　半順序 $P,\ Q$ における順序保存関数 $\lambda : P \to Q^{\mathrm{op}},\ \rho : Q^{\mathrm{op}} \to P$ について，$\langle \lambda, \rho \rangle$ が P から Q へのガロア接続であることと，函手の組

$$P \underset{\rho}{\overset{\lambda}{\rightleftarrows}} Q^{\mathrm{op}}$$

と式 (6) の同型射 φ の三つ組 $\langle \lambda, \rho, \varphi \rangle$ が随伴となることとは，同値である．　□

Ⅲ　ガロア理論と圏論

1　ガロア理論の基本定理

有理数全体の集合を $\mathbb{Q}$ として，係数が有理数の多項式 $f(x) = x^n + c_1 x^{n-1} + \cdots + c_{n-1} x + c_n \in \mathbb{Q}[x]$

7)　例えば，文献［1］の序.

を考察の対象とする．方程式 $f(x)=0$ を解くとはその根をすべて求めることであり，その手段を四則演算とベキ根操作（γ から $\sqrt[k]{\gamma}$ を作る）の繰り返しに制限する．根の公式は根を求めるアルゴリズムを数式で表現したもので，例えば，3次方程式 $x^3+px+q=0$ の根 $\alpha_1,\ \alpha_2,\ \alpha_3$ は

$$\left.\begin{array}{l}\Delta=-4p^3-27q^2,\quad \omega=(-1+i\sqrt{3})/2\ (\omega^3=1),\\ z_1,z_2=\sqrt[3]{(-q\pm\sqrt{-\Delta/27})/2}\quad (z_1z_2=-p/3)\end{array}\right\}\ \text{とおけば,}\quad \begin{array}{c}\alpha_j=\omega^j z_1+\omega^{3-j}z_2\\ (j=1,2,3)\end{array}$$

と表される（カルダノの公式）．解法の過程は $\mathbb{Q}$ に次々とベキ根を添加して体を拡大することであり，方程式の可解性はすべての根 α_j を含むベキ根拡大体 $L=\mathbb{Q}(\sqrt[k_1]{\gamma_1},\sqrt[k_2]{\gamma_2},\cdots)$ の存在に帰着される．

一般に体 F の拡大をベキ根拡大に限定しないで，$f\in F[x]$ が $(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ と因数分解できる最小の拡大体を f の分解体と呼び，$K(f)$ で表す（$K(f)=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$ となる）．また，ある多項式 $f\in F[x]$ の分解体 $L=K(f)$ への拡大 $F\subset L$ をガロア拡大という．

体 L の演算を保存する同型射 $\sigma:L\to L$ のなす群を L の自己同型群と呼び，$\mathrm{Aut}(L)$ で表す．そして，体のガロア拡大 $F\subset L$ において，F を固定する L の自己同型群

$$G=\{\sigma\in \mathrm{Aut}(L)\,|\,x\in F\ \text{ならば}\ \sigma x=x\}$$

をこの拡大体の**ガロア群**と呼び，$\mathrm{Gal}(L/F)$ で表す．以下，群の単位元を1，自明な群を $\mathbf{1}$ で表す．

例2　$f(x)=x^3-2$ のガロア群．$\xi=\sqrt[3]{2}$ とおくと f の根は $\alpha_1=\xi\omega,\ \alpha_2=\xi\omega^2,\ \alpha_3=\xi$ であるから，f の分解体 $K(f)$ は $L=\mathbb{Q}(\alpha_1,\alpha_2,\alpha_3)=\mathbb{Q}(\xi,\omega)$ である．ガロア群 $\mathrm{Gal}(L/\mathbb{Q})$ の任意の元 σ に対して $f(\sigma(\alpha_j))=\sigma(f(\alpha_j))=\sigma(0)=0$，すなわち $\sigma(\alpha_j)$ は f の根であるから，σ は3根の置換であり，$\mathrm{Gal}(L/\mathbb{Q})$ は3次対称群 S_3 と同型となる．具体的には，$\eta(\xi\mapsto\xi\omega,\ \omega\mapsto\omega)$ と $\tau(\xi\mapsto\xi,\ \omega\mapsto\omega^2)$ がその生成元（$\eta^3=\tau^2=1,\ \eta\tau=\tau\eta^2$）で，$\mathrm{Gal}(L/\mathbb{Q})=\langle\eta,\tau\rangle$ である．対称群 S_3 との対応関係は以下の通り：$1\sim(1)$，$\eta\sim(123)$，$\eta^2\sim(132)$，$\tau\sim(23)$，$\tau\eta\sim(13)$，$\tau\eta^2\sim(12)$．　□

ガロア理論のハイライトは，ガロア拡大 $F\subset L$ とそのガロア群 $\mathrm{Gal}(L/\mathbb{Q})$ を対応させて，方程式の可解性を論ずるところにある．ガロア理論の基本定理を文献［4］第13章第10節から引用する．

定理2（ガロア理論の基本定理）$F\subset L$ をガロア拡大[8]とすれば，そのガロア群 $G=\mathrm{Gal}(L/F)$ の部分群 H と“中間体”M（$F\subset M\subset L$）の間に同型射が存在する．同型射 $\rho:H\mapsto M$ は G の各部分群 H に，H に属する自己同型により固定される L の要素全体

$$M=\rho H=\{s\in L|\ \text{すべての}\ \sigma\in H\ \text{に対して}\ \sigma s=s\}$$

を対応させる．ρ の逆射 $\lambda:M\mapsto H$ は各中間体 M に，M の要素を固定する L の自己同型全体

8)　文献［4］では $F\subset L$ は有限次の正規拡大となっているが，ここではそれより少し強いガロア拡大のもとで論ずる．

$$H = \lambda M = \{\sigma \in G \mid \text{すべての } s \in M \text{ に対して } \sigma s = s\}$$

を対応させる．すべての $M \subset L$ はガロア拡大であり，H はそのガロア群である．さらに，体拡大の次元と部分群の指数[9] とは次の関係にある：

$$[L : M] = [\lambda M : 1], \qquad [M, F] = [G : \lambda M].$$

同型射 ρ, λ は次の図で表すことができる（この対応は順序を反転する）：

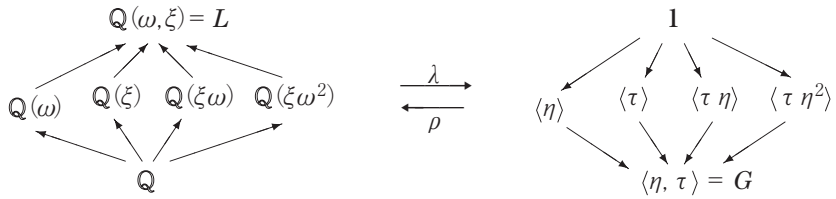
$$\begin{array}{rcl} & L \longmapsto \lambda L = 1 & \\ & \cup \qquad \cap & [L : M] = [H : 1] \\ \rho H = & M \longmapsto \lambda M = H & \\ & \cup \qquad \cap & [M : F] = [G : H] \\ & F \longmapsto \lambda F = G. & \end{array}$$

□

体の拡大列（左）の次元と部分群の列（右）の指数の対応に注目されたい．基本定理における同型対応 $M \longleftrightarrow H$ は「ガロア対応」と呼ばれている．

基本定理は，ガロア拡大 $\mathbb{Q} \subset L$ の中間体の集合とガロア群 $\mathrm{Gal}(L/\mathbb{Q})$ の部分群の集合が，（一方の順序を反転すれば）半順序として同型であることを表している．ガロア対応によって，複雑な世界の問題を比較的分かりやすい世界の問題に移行して，解決を導いたと言える．

例 3　例 2 の多項式 f に関するガロア対応（下図）．左右の同じ位置の体と群が対応する．例えば，部分群 $H = \langle \tau\eta^2 \rangle$ に対して，$(\tau\eta^2)s = s \Leftrightarrow s = a + b\,\xi\omega^2 + c(\xi\omega^2)^2$ $(a, b, c \in \mathbb{Q})$ であるから，$\rho H = \mathbb{Q}(\xi\omega^2)$ である．$\omega^2 = -\omega - 1$ であるから $\mathbb{Q} \subset \mathbb{Q}(\omega)$ は 2 次拡大，ξ，$\xi\omega$，$\xi\omega^2$ の添加はそれぞれ 3 次拡大，L は 6 次拡大である．一方，$\langle \eta \rangle$ は位数 3 で交代群 A_3 と同型，$\langle \tau \rangle$，$\langle \tau\eta \rangle$，$\langle \tau\eta^2 \rangle$ は位数 2，G は位数 6 である．等式 $[L : \mathbb{Q}(\omega)] = 3 = [\langle \eta \rangle : 1]$，$[\mathbb{Q}(\omega) : \mathbb{Q}] = 2 = [G : \langle \eta \rangle]$ などが成立する．□



2　基本定理の圏論による表現

基本定理を圏論で記述すると，定理 1 より次のようになる（次元・指数の関係を除く）．

9)　体拡大 $F \subset L$ の次元 $[L : F]$ とは F 上のベクトル空間 L の次元，部分群 $H \subset G$ の指数 $[G : H]$ とは各群の位数の比 $|G|/|H|$ のことである．

定理２’（圏論による基本定理）ガロア拡大 $F \subset L$ の中間体の集合とガロア群 G の部分群の集合

$$P = \{M \mid M \text{ は } F \subset L \text{ となる中間体}\}, \quad Q = \{H \mid H \text{ は } G = \mathrm{Gal}(L/F) \text{ の部分群}\}$$

はそれぞれ半順序の圏をなす．函手の組

$$P \underset{\mathcal{R}}{\overset{\mathcal{L}}{\rightleftarrows}} Q^{\mathrm{op}}$$

を

$$\begin{cases} \mathcal{L}M = \{\sigma \in G \mid \sigma s = s \ (\forall s \in M)\}, \\ \mathcal{L}g^{\mathrm{op}} : \mathcal{R}M' \to \mathcal{L}M \quad (g : M \to M' \text{ のとき}), \end{cases} \qquad \begin{cases} \mathcal{R}H = \{s \in L \mid \sigma s = s \ (\forall \sigma \in H)\}, \\ \mathcal{R}f : \mathcal{R}H \to \mathcal{R}H' \quad (f : H \to H' \text{ のとき}) \end{cases}$$

によって定義すれば，

$$(Q^{\mathrm{op}} \text{ において}) \ \mathcal{L}M \preceq H \iff (P \text{ において}) \ M \preceq \mathcal{R}H \tag{7}$$

が成り立つので，$\langle \mathcal{L}, \mathcal{R} \rangle$ は P から Q へのガロア接続となり，自然同型

$$\varphi : Q^{\mathrm{op}}(\mathcal{L}M, H) \cong P(M, \mathcal{R}H)$$

が存在する．したがって，三つ組 $\langle \mathcal{L}, \mathcal{R}, \varphi \rangle$ は随伴となる． □

圏論はガロア理論の定理の証明に直接的には何も寄与しない．基本定理を記述し直して，随伴という形式を見い出したにすぎないように見える．しかしこれは，「定理を生み出す発想」に普遍性があることを顕在化したことになっている．ここに圏論の特質が典型的に現れているように思われる．

３　代数方程式の可解性

ガロアの理論は基本定理のあと次のように続く．

体拡大 $\mathbb{Q} \subset L$ が可解であるとは，次のベキ根拡大の列が存在することである：

$$\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_{m-1} \subsetneq L \subset F_m \qquad (F_j = F_{j-1}(\sqrt[k_j]{\gamma_j}), \ \gamma_j \in F_{j-1}, 1 \leqq j \leqq m).$$

一方，有限群 G が可解であるとは，次の正規部分群の列（組成列と呼ぶ）が存在することである：

$$\mathrm{Gal}(L/\mathbb{Q}) = G_0 \supset G_1 \supset \cdots \supset G_{m-1} \supset G_m = 1 \qquad ([G_{j-1} : G_j] \text{ は素数}, 1 \leqq j \leqq m).$$

$\mathbb{Q}$ から L へのベキ根拡大の列 $\{F_j\}$ とガロア群 $\mathrm{Gal}(L/\mathbb{Q})$ の組成列 $\{G_j\}$ の間には，基本定理によりガロア対応 $F_j \leftrightarrow G_j$ $(1 \leqq j \leqq m)$ が存在する．

例４　例３に関する組成列は $\langle \eta, \tau \rangle \supset \langle \eta \rangle \supset 1$ に限られ，それにベキ根拡大の列 $\mathbb{Q} \subset \mathbb{Q}(\omega) \subset$

$\mathbb{Q}(\omega, \xi)$（$\omega = (-1+i\sqrt{3})/2$，$\xi = \sqrt[3]{2}$）が対応する．　□

そして，以下の定理群を得て一段落する．

定理 3　ガロア拡大 $\mathbb{Q} \subset L$ について，$\mathbb{Q} \subset L$ が可解拡大　$\Longleftrightarrow$　$\mathrm{Gal}(L/\mathbb{Q})$ が可解群．

定理 4　対称群 S_n（交代群 A_n）が可解　$\Longleftrightarrow$　$n \leqq 4$．

定理 5　n 次代数方程式の根の公式が存在する　$\Longleftrightarrow$　$n \leqq 4$．

あとがき

本稿は勉強会のテキストである文献［1］の第 IV 章第 5 節の内容を詳述したものにあたる．当初の熱い期待とは異なり，圏論でガロアの基本定理を記述してみてもとくに展望が開けたように感じられなかった．それは筆者の随伴に関する理解が未熟であることを意味する．このたび，ガロア接続が随伴という普遍性をもっていると認識できたことを新たな出発点と考えたい．

最後に，私達の勉強会を指導していただいている相沢輝昭先生（広島市立大学名誉教授）と，圏論の図的理解を促してくださる坂本實先生（専修大学名誉教授）に感謝する．

参考文献

［1］S. Mac Lane（1998）*Categories for the Working Mathematician,* Springer-Verlag New York.
三好博之，高木理訳（2007）『圏論の基礎』，シュプリンガー・ジャパン．
［2］P. Freyd（1964）*Abelian Categories,* Harper and Row.
［3］大熊正（1979）『圏論（カテゴリー）』，槙書店．
［4］S. Mac Lane & G. Birkhoff（1999）*Algebra,* AMS Chelsea.
［5］D. A. Cox（2004）*Galois Theory,* John Wiley & Sons, Inc.
梶原健訳（2008）『ガロワ理論（上，下）』，日本評論社．
［6］B. L. van der Waerden（1937）*Modern Algebra I,* Verlag von Julius Springer Berlin.
銀林浩訳（1978）『現代代数学』，東京図書．
［7］遠山啓（2011）『代数的構造』，ちくま学芸文庫，筑摩書房．