置換群に翻弄された方程式の可解性―ガロア理論概論（第２版）

上野孝司

2017 年 1 月 5 日

置換群に翻弄された方程式の可解性―ガロア理論概論（第２版）
（第 1 版に対称群の定義とガロア拡大の説明のほか、命題 4 －(1) の証明を追加した）

筆者は別稿『響きあうガロアとガウス―正 17 角形の作図問題』で、ガロアの理論とガウスの考えた f 項周期（拡大体の基底）を基に正 17 角形が作図できることを示したが、本稿ではガロア理論を再考することによって代数方程式の可解性について概略を述べる。ガロア理論の中心的な定理――体と群の一対一対応――を概説して、それを方程式論に適用する。そして、何百年もの間、ひとびとを悩ませてきた一般代数方程式の可解性の帰趨が、極めて一般的で普遍的なガロアの基本定理の論理的枠組みに内包されつつも、最終的には対称群（置換群）$\mathfrak{S}_n$(定義は以下を参照）のテクニカルな性質の一端（擬人化すれば少々わがままな性格）に翻弄されたことは驚くべき事実である。その普遍性と個別性の大きな格差を見破ったガロアの慧眼に敬意を表しつつその舞台裏を明らかにする。

ここで、体論の用語を簡単に説明しておく。E を体とする。このとき、E の部分集合 K でそれ自体で体の構成要件を満たすとき、K を E の部分体という。逆に K からみたとき、E を K の拡大体という。さらに、体 K を固定してその拡大体を論じるとき、K を基礎体という言い方をすることがある。方程式論や円分体の議論では、有理数体 Q や Q（ζ）(Q に 1 の N 乗根 ζ を付加した体で円分体という）を基礎体とすることが多い。また、群ではその部分群の列を論じることが多いのに対して、体では拡大体の列を論じる場合が多い。

なお、**対称群**とは、集合 X からそれ自身への全単射（一対一対応）の集合をいう。これは、写像の合成を演算として群をなす。特に X が n 個の元から成る有限集合である場合には、この群を n 次対称群と呼び $\mathfrak{S}_n$ で表す。これは位数 $n!$ の有限群である。簡単にいえば対称群の元 σ は、順列 $(1, 2, \cdots, n)$ を順列 $(\sigma(1), \sigma(2), \cdots, \sigma(n))$ に移す一つの置き換えであるから、対称群はまた**置換群**とも呼ばれる。まったく動かさない場合でも自分自身に移す恒等写像と考えて置換群の元（単位元）とみなす。つまり、対称群 $\mathfrak{S}_n$ とは、置き換えという能動的な行為からなる群である。実は、置換群はラグランジュ（1736～1813）やガロア（1811～1832）が最初に取り扱ったものであり、群の発祥ともなった数学史上最も重要な群である。本稿の最後でこの対称群の性質が方程式の可解性に深く結び付いていることを示す。

$\forall \sigma \in \mathfrak{S}_n$ に対して、ひとつの置き換え

$$\sigma : (1, 2, \cdots, n) \text{――――} \succ (\sigma(1), \sigma(2), \cdots, \sigma(n))$$

$$(\sigma(i) \neq \sigma(j))$$

が対応する。

1．体の自己同型

E を体とするとき、E から E の全単射の写像で同型となるもの、すなわち、体の二つの演算、和と積を保存するもの、つまり、E の任意の元 a,b に対して、

$$\begin{cases} \sigma(a+b)=\sigma(a)+\sigma(b) \\ \sigma(ab)=\sigma(a)\sigma(b) \end{cases}$$

が成り立つ写像 σ を E の自己同型（写像）という。E の自己同型写像の集合は、写像の合成を演算として群を作ることは容易にわかり、これを E の自己同型群といい、$Aut(E)$ で表す。また、K を E の部分体とするとき、K の元を不動にするような E の自己同型の集合は $Aut(E)$ の部分群となり、これを、“E の K 上の自己同型群”といい、$G(E/K)$ で表す。特に E が K の**ガロア拡大（正規拡大ともいう）**という条件を満たすとき、自己同型群をガロア群と呼ぶ。また、$Aut(E)$ の部分群（部分集合でもよい）S に対して、すべての $\sigma\in S$ に対して、$\sigma(a)=a$ となるような $a\in E$ の全体からなる集合は E の部分体となり、これを S の固定体という。

2．ガロア理論の基本定理

基礎体 K とその拡大体 E があり、この拡大が**ガロア拡大（正規拡大）**という条件を満たすとき、K と E の中間体 M とガロア群（E の K 上の自己同型群）$G(E/K)$ の部分群 H には一対一対応が存在する（いわゆるガロア対応)。この体と群の対応という体と群を結びつける定理を**ガロア理論の基本定理**という。この定理で複雑な体の情報が、構造がわかりやすい群の情報に置きかわり、この群を分析すればよいことがわかる。基本定理は独立した定理で、方程式論や円分体の構造、正多角形の作図問題にも適用できる応用範囲の広い非常に重要な定理である。代数学で基本的で最も重要な定理であるといってもよい。

K がE のある有限自己同型群の固定体となっているとき、E をK のガロア拡大（正規拡大）という。これは、E が K の有限拡大であって、“E の K 上の自己同型群の固定体が K と一致している”ということに他ならない。ガロア拡大ではないとき、一般にH とM が一対一対応に一致するとは限らないが、ガロア拡大のときは対応することが保証される。ここにこの基本定理でガロア拡大の前提が必要となる所以がある。ガロア拡大はガロア理論の土台となる重要な概念だがその詳細は述べないが関連する以下の定理だけ述べておく（証明略)。読者はまずは、ガロア拡大の場合、体と群が一対一に対応するという点に着眼していただきたい。

【定理 1】G を体 E の位数 n の自己同型群とし、G の固定体を K とすれば、$(E:K)=n$ であり、E の K 上の自己同型群は G と一致する。

これは、ベクトル空間の次元と群の位数に関する美しい定理である。

【定理 2】K の有限拡大 E に関する以下の３つの条件は互いに同値である。

(1)E は K の正規拡大である。

(2)E は K の分離拡大で、E 内に根を持つ $K[x]$ の任意の既約多項式は E において分解する。

(3)E は $K[x]$ のある分離多項式の K 上の分解体である。

この定理は、正規拡大と分解体の関係についての命題であって、正規拡大の上述の定義より具体的で構成的な記述である。分離拡大、分離多項式については、以下を参照されたい。

分解体で相異なる１次多項式の積に分解される K 係数多項式を分離多項式という。分離多項式の根を K 上で分離的な元という。K の拡大体 E の任意の元が K 上分離的なとき、E を K の分離拡大という。より厳密に言えば、K 上の既約多項式 f が単根のみを持つとき f は分離的であるという。より一般に、定数でない多項式 $f \in K[x]$ は K におけるすべての規約因数が分離的であるとき、“K 上で”分離的であるという。K の標数が０ならば K 上の定数でない多項式はすべて K 上で分離的である。E を K の拡大体とし、$\alpha \in E$ を K 上で代数的な元とする。α の K 上の最小多項式が K 上で分離的であるかないかに応じて α は K 上で分離的あるいは非分離的であるという。E が K の代数拡大で、E のすべての元が K 上で分離的であるとき E を K の分離拡大という。

ガロア対応の体と群の対応規則は、
＊ $G\,(E/M) = H$(E の M 上の自己同型群）
＊ $M = E_H$(H の固定体）
で与えられる。（E が K の正規拡大のときは）E は M 上で正規であるが、M は K 上で正規であるとは限らない。正規であるための必要十分条件は 対応する H が G の正規部分群である ことである。つまり、正規部分群に正規拡大が対応する。ガロア拡大が正規拡大と言われる所以である。その場合、$G(M/K)$ は商群 G/H と同型である。

ガロアの基本定理－体と群の対応

$$
\begin{array}{ccccccc}
 & & E & === & e & & \\
 & & | & & | & & \\
E_H & = & M & === & H & = & G(E/M) \\
 & & | & & | & & \\
E_G & = & K & === & G & = & G(E/K)
\end{array}
$$

φ : 中間体の集合＜ーーーーーー＞部分群の集合

$$
\begin{array}{c}
M < \text{ーーーーーーーーーー} > H \\
\varphi(M) = G(E/M)(E \text{ の } M \text{ 上の自己同型群}) \\
\varphi^{-1}(H) = E_H(H \text{ の固定体})
\end{array}
$$

３．ガロア理論（方程式の可解性）の論点整理

ガロア理論は壮麗な交響楽のようで、その理論構成は見事としかいいようがないのだが、あまりの重層的な創りに見方を誤ると迷路から抜け出せないという危うさを常に孕んでいる。ガロア理論の解説書は多くみられるが、いずれも難解なものばかりで論点をまとめて提示するなど教育に配慮した書物は少ない。だから自分がいま、どこの山場の何合目にいるかという立ち位置がわからず、迷子になってしまうのである。体と群を結びつけるガロアの基本定理（いわゆるガロア対応）までは順調に進んだものの、特に『商群が巡回群となるような正規部分群の列を持つような群』を可解群とよび、これが５次以上の一般的な代数方程式には代数的な解法（解を係数の四則演算とべき根をとるという行為で表現する方法）がないことが結びつくというところでわか

らなくなってしまうひとが多いようである。なぜ、「商群が巡回群となる正規部分群の列」などというわかりにくいものを考える必要があるのだろうか？

そこで、方程式論の論点をまとめてみた。「方程式の可解性とガロア理論」の構成でわからなくなった場合、必ず下記の四つの山場のいずれかに迷い込んでいることは間違いない。この参考を自らの立ち位置を確認するものとして使っていただきたい。

(1) ガロアの基本定理：上記で述べたが再論すれば、基礎体 K とその拡大体 E があり、この拡大がガロア拡大という条件を満たすとき、K と E の中間体とガロア群（E の K 上の自己同型群）の部分群には、一対一対応が存在する――という体と群を結びつける美しい定理。ガロア拡大がこの基本定理の土台となっていることに留意されたい。複雑な体の情報が、構造がわかりやすい群の情報に置き換わり、この群を分析すればよいことがわかる。基本定理は代数学で独立した重要な定理で、方程式論や正多角形の作図問題にも応用できる重要な定理である。筆者はときどき、このガロアの基本定理を“代数学の基本定理”といい、通常の代数学の基本定理（実数係数の多項式は解を持つ）を“解析学の基本定理”と呼んだほうが妥当と思うことがあるが、そうなったら、代数学の基本定理を理解できるひとがほとんどいなくなってしまい、教育上好ましくないから、今のままでよいのだ、などと思っている。

(2) べき根拡大と巡回拡大の同値性：基礎体（1 の原始 N 乗根を含むとする）の拡大がべき根拡大（基礎体に正の定数 a の n 乗根 $\alpha = \sqrt[n]{a}$ を付加した体）であるならば、それは巡回拡大（自己同型群（ガロア群）が巡回群となるようなガロア拡大）である。逆も成り立つ。つまり、巡回拡大ならばべき根拡大となる――という定理が基本的かつ決定的に重要である。以下の（3）（可解群と方程式の可解性の関係）はイメージしにくいのだが、この（2）は数学的に美しく、納得性があるというか、イメージしやすい特徴があると筆者は思っている。ここに**可解群の原型（商群が巡回群の列）**をみることができるのである。

$$\begin{array}{ccccc} E(=K(\sqrt[n]{a})) & - & e & & \\ | & & | & & \text{（}E\text{ が }K\text{ のべき根拡大なら }G\text{ は巡回群）} \\ K & - & G & = & G(E/K) \end{array}$$

以下、べき根拡大ならば巡回拡大を示す（逆は省略）。

（証明）

べき根とは、$x^n = a$ の解のことをいい、$\alpha_0 = \sqrt[n]{a} = a^{\frac{1}{n}}$ をひとつの解とすると、

$$\omega_n = \cos(2\pi/n) + i\sin(2\pi/n)$$

とすると、$f(x) = x^n - a = 0$ のすべての解は、

$$\alpha_k = \omega_n^k \alpha_0 (k = 0, 1, \cdots, n-1)$$

で表される。E を基礎体 K にべき根 α_0 を付加した体（べき根拡大）$K(\alpha_0)$ とするとき、
自己同型は N 乗根を N 乗根に移すから、E の 2 個の自己同型を

$$s_k(\alpha_0) = \alpha_k = \omega_n^k \alpha_0, \quad s_h(\alpha_0) = \alpha_h = \omega_n^h \alpha_0$$

とすると、$k+h \equiv l(\mathrm{mod}\, n)$ として

$$s_h s_k(\alpha_0) = s_h(\alpha_k) = s_h(\omega_n^k \alpha_0) = \omega_n^k s_h(\alpha_0) = \omega_n^k \omega_n^h \alpha_o = \omega_n^{k+h}\alpha_0 = \omega_n^l \alpha_0 = s_l(\alpha_0)$$

となるから、

$$s_k \Leftrightarrow k(\mathrm{mod}\, n)$$

なる対応によって、べき根拡大の自己同型群 $G(E/K)$ は整数の加法群 $\mathbb{Z}_n$ の部分群に同型となる。一方、加法群 $\mathbb{Z}_n$ は位数 n の巡回群であるから、その部分群は位数が n の約数であるような巡回群に同型となる。■

(3) 代数方程が代数的に解けることと方程式のガロア群が可解群（商群が巡回群であるような正規部分群の列が存在する群）であることの同値性：これがガロア理論の最大の山場で難解にみえて、ここで迷い込んでしまうことが多いのだが、(1) からここに至るまでの橋渡しになるのが、(2) なのである。(3) は方程式論で最も重要なところでありこれを (1)、(2) を用いて証明することがポイントとなる。方程式が四則演算とべき根で解けるということは、「基礎体から分解体に至るまですべてがべき根拡大の列が存在する」と常識的に読みかえることができ、これにガロアの基本定理を適用すれば、“**それぞれのべき根拡大にひとつの（部分）群が対応するガロア対応**”を考えることができる。(2) によって「べき根拡大は巡回拡大」であるから、このガロア対応は、「商群が巡回群となるような正規部分群の列」となる、つまり可解群となることがわかる。以上より、

K(基礎体）$\subset F_i \cdots \subset E$ という拡大体の列と正規部分群の列 $G \supset H_i \cdots \supset e$ の対応が存在する（下図参照)。

体の列と部分群の対応（ガロア対応）

K(基礎体）	$\subset$	$\cdots\cdots$	$\subset$	F_i	$\subset$	F_{i+1}	$\subset$	$\cdots\cdots$	$\subset$	E(分解体）
$\vdots$				$\vdots$		$\vdots$				$\vdots$
G(ガロア群）	$\supset$	$\cdots\cdots$	$\supset$	H_i	$\supset$	H_{i+1}	$\supset$	$\cdots\cdots$	$\supset$	e
$\|\|$				$\|\|$		$\|\|$				
$G(E/K)$				$G(E/F_i)$		$G(E/F_{i+1})$				

H_{i+1}は H_iの正規部分群で、そのガロア群は H_i/H_{i+1}でしかも巡回群である。

（4）‐１ n 次の一般代数方程式のガロア群は、n 次対称群（置換群）$\mathfrak{S}_n$ である。

n 次の一般代数方程式とは、方程式 $a_0x^n + a_1x^{n-1} + \cdots\cdots + a_{n-1}x + a_n = 0 (a_0 \neq 0)$ のことである。これは n に制約がなく、すべての自然数 n について成り立つことに留意されたい。

（4）‐２ 対称群$\mathfrak{S}_n$ はn が４以下ならば可解群、５以上ならば非可解群となる。

(3) と (4) から、ガロアが見破った『５次以上の代数方程式には解の公式がない』、つまり、係数の四則演算とべき根では表現できない、という結論に到達する。現代のガロア理論では、(1) をガロアの基本定理（独立したひとつの定理）としたうえで、（1）～(4) を総称して (狭義の）ガロア理論と呼んでいるようだ。ここで、注意すべきは、(1)、(2)、(4) はそれぞれ独立した定理であることである（(4) ‐１と（4）‐２もそれぞれ独

立である)。また、群の可解性という言葉にも注意が必要だ。この可解群という表現は、方程式の可解性に結びつけて、後追いで定義された、とってつけたような表現になっていることがガロア理論をかえってわかりにくくしているようだ。以下では、(4) の証明の概略を述べる。

((4) - 1 の証明)

一般代数方程式を

$$f(x) = x^n - a_1 x^{n-1} + \cdots\cdots + (-1)^n a_n$$

とする。係数に $(-1)^n$ を付けたのは議論の便宜上のためである。

$f(x)$ の根を $b_1, b_2, \cdots, b_n$ とすると、

$$f(x) = \prod_{j=1}^{n} (x - b_j)$$

ここで、根と係数の関係、

$$\left.\begin{array}{c} a_1 = b_1 + b_2 + \cdots + b_n \\ a_k = \sum_{i(1)<i(2)<\cdots i(k)} b_{i(1)} b_{i(2)} \cdots b_{i(k)} \\ \cdots\cdots\cdots \\ a_n = b_1 b_2 \cdots b_n \end{array}\right\} \cdots (*)$$

が得られる。これらの右辺を、$b_1, b_2, \cdots, b_n$ の基本対称式という。

有理数体 Q に $a_1, a_2, \cdots, a_n$ を付加した体を K とする。

$$K = Q(a_1, a_2, \cdots, a_n)$$

このとき、$f(x)$ の K 上のガロア群が n 次対称群となる のである。

$f(x)$ の分解体は、$E = K(b_1, b_2, \cdots, b_n)$ である。

対称群 $\mathfrak{S}_n$ の元 s が $(1, 2, \cdots n)$ を順列 $(s(1), s(2), \cdots, s(n))$ に変換するとき、

$$s(b_j) = b_{s(j)}$$

で E の変換を定義すれば、これは E の同型で、(*) から、$a_1, a_2, \cdots, a_n$ **を不動にする**から、E の K 上の自己同型(ガロア群) $G = G(E/K)$ の元を定める。$\mathfrak{S}_n$ はしたがって、G の部分群で、

$$[E : K] = \#G \geqq \#S_n = n!$$

一方、体の拡大の列

$$K \subset K(b_1) \subset K(b_1, b_2) \subset \cdots \subset K(b_1, b_2, \cdots, b_n) = E$$

で拡大次数を考えると、

$$[K(b_1) : K] \leqq \deg f(x) = n$$

で、b_2 は $(n-1)$ 次多項式 $f(x)/(x-b_1)$ の根だから、

$$[K(b_1,b_2):K(b_1)] \leqq n-1 \cdots\cdots$$

であるから、

$[E:K] = [K(b_1):K]\cdots[E:K(b_1,b_2,\cdots,b_{n-1})]$

$\leqq n(n-1)\cdots 2\cdot 1 = n!$

より、上の不等式は等号で、$\#\ G = \#\ \mathfrak{S}_n = n!$ だから、$G = \mathfrak{S}_n$ となる。■

((4) - 2 の証明) 一般に群 G の正規部分群 N による商群 G/N が可換であれば、$xyN = xNyN = yNxN = yxN$

であるから、

$aba^{-1}b^{-1}N = aN\cdot bN\cdot a^{-1}N\cdot b^{-1}N = N$　　よって、$aba^{-1}b^{-1}\in N$

となる。$aba^{-1}b^{-1}$ の形の元を、a,b の“交換子”という。つまり、

G/N が可換であれば、N は任意の交換子を含む。$\cdots\cdots(*)$

いま、$(i,j,\cdots,k)$ で巡回置換 $(i\to j\to\cdots\to k\to i)$ を表す。ここで、以下の式が重要となる。i,j,k,l,m を 5 個の相異なる文字とする。

$(i,j,k)^{-1} = (k,j,i)$　　(1)

$(i,j)(k,l) = (i,j,k)(k,i,l)$　　(2)

$(i,j)(i,k) = (i,j,k)$　　(3)

$(i,j,k) = (i,l,k)(i,m,j)(k,l,i)(j,m,i)$　　(4)

$= (i,l,k)(i,m,j)(i,l,k)^{-1}(i,m,j)^{-1}$　　(5)

が成り立つ（積は左から読む)。

(2)、(3) は、交代群 $\mathfrak{A}_n$（偶置換からなる対称群 $\mathfrak{S}_n$ の部分群）が巡回置換から生成されることを示す。(5) は巡回置換 (i,j,k) が交換子であることを示す。n が 5 以上とすると、5 個の文字を含む上記の式はすべて成立する（逆に 4 以下なら成立しない)。したがって、交代群 $\mathfrak{A}_n$ の部分群 N で $\mathfrak{A}_n/N$ が巡回群であれば、これは可換群であるから、(*) より、N はすべての交換子を含み、その交換子は、すべての偶置換を生成する (i,j,k) を生成するから、実は $N=\mathfrak{A}_n$ であることを意味する。

もし、$\mathfrak{S}_n$ が可解群ならば、その正規部分群である $\mathfrak{A}_n$ も可解群となるが、上述より、商群が巡回群となる部分群の列は不可能となる。よって、$\mathfrak{S}_n$ は n が 5 以上ならば可解とならない。■

重要なことは上記は、5 個以上の文字があって初めて成り立つテクニカルな命題ということである。だから、n が 4 以下なら成立しない、逆にみればそもそも、2、3、4 次方程式が解の公式を持つ（四則演算とべき根で解ける）ことのほうが特殊であるという見方もできる。実際、$\mathfrak{S}_3,\mathfrak{S}_4$ それ自体は巡回群ではないが、商群が巡回群となる正規部分群の列が存在する ことが以下のように具体的に示される。

$\mathfrak{S}_3$ については、

$$\mathfrak{S}_3 \supset \mathfrak{A}_3 \supset \{e\}$$

が求めるものである。

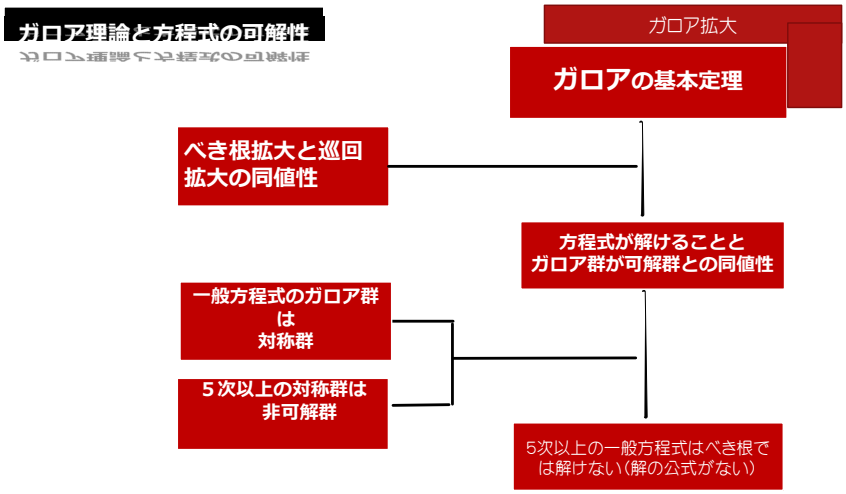
$\mathfrak{S}_4$ については、交代群 $\mathfrak{A}_4$ の部分群として、
$H = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$, $N = \{e, (1,2)(3,4)\}$ をとり、

$$\mathfrak{S}_4 \supset \mathfrak{A}_4 \supset H \supset N \supset \{e\}$$

が求めるものである。特に H が存在することが 4 次対称群の可解性にとっては重要である。

なお、5 次以上の一般代数方程式には解の公式がないが、方程式のガロア群が可解群ならば、5 次以上でも方程式は四則演算とべき根で解くことができることに留意されたい。実際、別稿で述べたように、$x^{17} - 1 = 0$ はべき根（しかも平方根号のみ）で解くことができ、さらに極論すれば、例えば、100 次方程式 $(x-1)^{100} = 0$ は $x = 1$ を 100 重根として解かれる。

果たして、ガロアはどのようにしてこれらを導いたのであろうか。現代の数学では、構造主義の影響をうけて理路整然と構成されているが、ガロアは (1) から (4) を順序付けて構築したのか、それとも死を前にした決闘前夜のガロアの情熱とともに渾然一体と感じながら総合的に導いたのか。たとえば、(4) は、(1)〜(3) がわからずとも理解できるひとつの定理（交換子群と巡回置換、偶置換の関連から導かれる）なのだが、(1)〜(3) があってはじめて存在意義があるものでもある。私個人的にはガロア群が巡回群であることと方程式の可解性の関係を感じとったのではないかと思う。その際、ガロア群として具体的な代数方程式の置換群 (対称群）を考えたのである。いや、代数方程式の解の置換（置き換える）という能動的な行為から群の概念が生み出されたのであり、それを構造的に構築しなおしたものが現代のガロア理論なのである。そして、これこそがガロアが後世に残した最大の遺産である。そもそも、群という概念は、ガロアの時代には一般論として存在せず、上述したように置換群という躍動的で原始的な群の概念がはじめにおこったと考えられる。このあたりは、現在、ガロアの原論文の邦訳が出ているので、興味ある方はそれを参照されたい。



＊本稿の執筆では、

『ガロアの理論』（ポストニコフ、東京図書）

『ガロワと方程式』（草場公邦、朝倉書店）

『代数系入門（松坂和夫、岩波書店)』

などを参考とした。

＊筆者経歴

東京大学理学部数学科を経て教育学部卒業。証券会社、外資系通信社で金融・資本市場の業務を経験。専門は、債券資本市場。主な著書・論文：『信用リスクを読む』（日本評論社)、『信用リスクとM＆A』（同)、『世界金融危機と信用リスク』（同)、『鎮めの文化と資本市場』（ブルームバーグ)、『金融派生商品』

メール：sakurasaku9286@willcom.com