「ガロア理論」と高校数学

～2 次方程式を用いてガロア理論を読み解く～

千葉商業高等学校　藤田 有加　島上 直人

1　はじめに

数学の理論の中でも難解と言われるガロア [1] 理論は，2000 年来のギリシャ三大作図問題を解決し，自然科学を中心に様々な分野で応用されている。フェドロフ [2](1891) が証明した，アラビア芸術に見られる繰返し文様が 17 種類であること（2 次結晶群），ワイルズ [3](1995) の証明したフェルマー [4] の最終定理 [5] の証明にも利用され，ペレルマン [6](2002) の証明した「ポアンカレ [7] 予想 [8]」の題材を提供し，ガロア理論からなる抽象代数は現代の IT 社会の基盤となる「情報の誤り補正技術」にも応用されているなど，例は枚挙に遑がない。20 歳で逝った天才が，近代から現代に至る数学を根底から変革したといっても過言ではなかろう。

その難解性もあり高校の数学においてガロア理論を扱うことはない。数学科に進学し代数学を専攻しない限りはなかなか接することはない。しかしながら，ガロア理論の中核をなす「群論」,「拡大体」や「自己同型写像」の考え方が高校数学の中に見え隠れしていると常日頃から感じていた。新教育課程になりさらに鮮明になってきた。加えて，難解と言われる「ガロア理論」の入門書がここ数年にわたって数多く出版されてきていて，ガロアブームである。ガロア理論の入門書をあげてみる。どの本も，最終的なガロア理論に至るには表現しきれていない所もあるが，ガロアが考えたことは垣間みることができる良書である。

- リリアン・リーバー (浜稲雄), ガロアと群論, みすず書房, 1979
  ガロア理論の概略を散文調・イラスト付きで簡潔に紹介
- 加藤文元, ガロア, 中央公論新書, 2010
  ガロア理論の説明ではなく，ガロアの生い立ちの話
- 小島寛之, 天才ガロアの発想力, 技術評論社, 2010
  著者が 13 歳のときにこんな本があったら良かったと思って書いた
- 金　重明, 13 歳の娘に語る ガロアの数学, 岩波書店, 2011
  ガロア理論の導入を 13 歳の娘と対話形式で書いてある

[1] Évariste Galois 1811-1832　フランスの数学者，革命家
[2] Evgraf Stepanovich Fedorov 1853-1919) ロシアの結晶学者。1885 年に菱形 20 面体も発見している。
[3] Andrew John Wiles, 1953-　イギリスの数学者
[4] Pierre de Fermat，1607-1665
[5] $n \geq 3, n \in \boldsymbol{N}$ について，$x^n + y^n = z^n$ となる 0 でない自然数 (x, y, z) の組が存在しない
[6] Grigory Yakovlevich Perelman, 1966-　ロシアの数学者
[7] Jules-Henri Poincaré，1854-1912　フランスの数学者
[8]「単連結な 3 次元閉多様体は 3 次元球面 S^3 に同相である」

- 結城　浩, 数学ガール／ガロア理論, ソフトバンククリエイティブ, 2012
  ガロア理論を理解するための前段階が中心
- 藤田岳彦, 解いてわかるガロア理論, 東京図書, 2013
  高校からの数学の問題を解きならがガロア理論に発展していく
- 石井俊全, ガロア理論の頂を踏む, ベレ出版, 2014
  かなり初歩からガロア理論の核心まで詳細に述べられている。
- 木村俊一, 数学のかんどころ 14 ガロア理論, 共立出版, 2013
  数学科の学生向け，ギリシャ3 大作図問題や正 17 角形の作図にもふれている

「数学 I」と「数学 II」の双方ともに 2 次方程式の解法についてふれているが,「数学 I」の 2 次方程式は古代バビロニア数学[9] がらアルフワリズミ[10] の数学であり,「数学 II」の 2 次方程式はガロアの数学である。「無理数の分母の有理化」「対称式」「2 次方程式の解法」「2 次関数の判別式」「解と係数の関係」「剰余の定理」「因数定理」「高次方程式」「複素数」「指数関数」などは「ガロア理論」においては欠かせない内容である。

今回は授業中に使用した演習・教材をもとに,「無理数の分母の有理化」「対称式」「2 次方程式の解法」「2 次関数の判別式」「解と係数の関係」について触れ，高校数学（特に 2 次方程式の解法）とガロア理論の関連をまとめてみた。

2　解の公式について

ガロアが証明したことは,

> 5 次以上の代数方程式には解の公式が存在しない

である。つまり,「2 次，3 次，4 次方程式は加減乗除（四則演算）と平方根（2 乗根），立方根（3 乗根）などのベキ根をとる操作で解を求めることはできるが，5 次以上の方程式ではそのような操作で解を得ることはできない。」ということである。[11]

2 次方程式の公式はアルフワリズミ，3 次方程式の解の公式（カルダノ[12] の公式[13]）はフォンタナ[14]，4 次方程式の解の公式はフェラーリ[15] がそれぞれ証明したとされている。そもそも解の公式が存在するということは,

> 4 次以下の方程式は，有理数を加減乗除（四則演算）と平方根（2 乗根），立方根（3 乗根）などのベキ根をとる操作で，かならず解を表現することができる

ということである。ガロア理論（ガロア群が可解群にならない）により有理数の四則演算とベキ

[9] B.C.3000?-B.C,1000?　現在のメソポタミア地域
[10] Alkwarizmi,780?-850?　アラビアの数学者　アルゴリズムの語源とされている
[11] Niels Henrik Abel，1802-1829　ノルウェイの数学者もほぼ同時期に証明している。
[12] Gerolamo Cardano 1501-1576
[13] 3 次方程式の解の公式は公表したのがカルダノであったため「カルダノの公式といわれる」
[14] Niccolò Fontana 1499?-1557　イタリアの数学者　別名 [Tartaglia] タルタリア
[15] Ludovico Ferrari, 1522-1565　イタリアの数学者　カルダノの弟子

根をとる操作では解を表現することができないことが証明できる 5 次方程式 $x^5-6x+3=0$ の 3 個の実数解もニュートン法を用いれば極めて正確な値を得ることができる。逆に $x^5=2$ の解 $x=\sqrt[5]{2}$ は，有理数 2 の 5 乗根で表現できる。また，5 次方程式 $x^5+x^4-4x^3+3x^2-3x+1=0$ の解はガロア理論（ガロア群が可解群になる）により有理数の四則演算とベキ根で表すことができるのだ。つまり，四則演算とベキ根を利用するというルールによって表現することが可能か不可能かをガロア理論により判定できるということなのだ。

2.1 解の公式の意味すること

2 次方程式の解の公式を例にとって解の公式が存在するとはどういうことなのかを考えてみる。$a(\neq 0), b, c \in \mathbb{Q}$ において，2 次方程式 $ax^2+bx+c=0$ の解の公式は，

$$x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$$

である。このことが意味していることは，どんな 2 次方程式を与えられようとも，その係数からはじまり，四則演算とベキ乗根をとる計算によって，すべての解にたどり着くということである。

(1) 方程式の係数 a, b, c より，b^2-4ac を得る。（四則演算）
(2) b^2-4ac の平方根 $\sqrt{b^2-4ac}$ を得る。（ベキ乗根）
(3) $-b$ に，$\sqrt{b^2-4ac}$ を加える，または引く。（四則演算）
(4) $-b\pm\sqrt{b^2-4ac}$ を $2a$ で割る。（四則演算）

このような決まった手続きによって解を得ることができるということなのだ。3 次方程式，4 次方程式もこのように，その係数からはじまり，四則演算とベキ乗根をとる計算によって，すべての解にたどり着くことができるが，5 次以上の方程式ではそのような操作で解を得ることは必ずしもできるとは限らないのだ。

3 2 次方程式が四則演算とベキ乗根で解けることを確認する

ここからは，2 次方程式が四則演算とベキ乗根で解けるかを解の公式を使わずに探っていく。2 次方程式の解の公式を使えばいとも簡単に進む話も，やたら専門的な概念が出てきて回りくどいことになるが，この手法が 3 次以上の方程式にも適用できるのだ。つまり，3 次や 4 次の方程式の解の公式を知らなくても，四則演算とベキ乗で解を表現することが可能であることを示すことができるということである。

3.1 「体」の概念

解の公式の存在につながる理論的な背景を順次見ていく。

まず，集合が演算に「閉じている」という状態を定義する。ある集合 G の任意の要素同士をある演算を実行したときのその演算 $\circ$ した値もその集合の要素となっていることを「閉じている」という。すなわち，

$$\forall x, y \in G \Rightarrow x \circ y \in G$$

が成り立つとき,「集合 G は演算 $\circ$ について閉じている」と言う。

演習 1 i を虚数単位とするとき $\dfrac{1+2i}{2+i}$ を計算せよ。

この問題は「数学 II」における「複素数と方程式」「複素数」で扱う。複素数は四則演算に閉じている（複素数体）ことを意味している。（解答略）

「数学 I」においても，

> 2 つの有理数の和, 差, 積, 商は有理数である
> 2 つの実数の和, 差, 積, 商は実数である

の記述がある。（数研出版「数学 I」（平成 26 年度）$pp25$）

演習 2 [16]

下の表において，それぞれの数の範囲で四則演算を考えるとき，計算がその範囲で常にできる場合には○を，常にできるとは限らない場合には×をつけよ。ただし，除法では 0 で割ることは考えない。

数の範囲	加法	減法	乗法	除法
整数				
有理数				
実数				

この問題は「数学 I」における「数と式」「実数」においてのべられている。「体」の定義は高校では学習しないが，これはまさしく「体」にほかならない。（解答略）

演習 3 ここで「体」を「四則演算について閉じている集合」とする。このとき,「体」となる集合は上の演習 2 の集合のどれか。

[16] 数研出版「数学 I」（平成 26 年度）pp25

3.2 拡大体

演習 4 $\dfrac{2+3\sqrt{2}}{-1+2\sqrt{2}}$ を計算せよ。

この問題は「数学 I」における「数と式」「根号を含む式の計算」で述べられている。$a+b\sqrt{2}$ の形をした式に四則演算をした結果は $a+b\sqrt{2}$ の形になる，すなわち有理数体 $\mathbb{Q}$ に無理数 $\sqrt{2}$ を加えた集合も「体」となることを意味している。（解答略）

ここで，ある「体 $\boldsymbol{F}$」にある数値 α を加えても「体」となるとき，体 F の α による**拡大体**といい

$$F(\alpha)$$

と表す。

演習 5 有理数体に $\sqrt{3}$ を加えた集合が拡大体 $\mathbb{Q}\left(\sqrt{3}\right)$ となることを示せ。

$a+b\sqrt{3}$ の形をした式どうしに四則演算をした結果は $a+b\sqrt{3}$ の形になることを示せばよい。この問題も前問と同様に，有理数体 $\mathbb{Q}$ に無理数 $\sqrt{3}$ を加えた集合も閉じていて「体」となることを示している。（解答略）

3.3 自己同形写像

ガロアの天才的なアイディアと言われる自己同形写像とは「四則演算を保存する全単射」のことである。

(1) f は「一対一対応（単射）」である。2 つの異なる数が同じ数に対応することはない。
つまり，$\forall x, y \in K, x \neq y \Rightarrow f(x) \neq f(y)$
(2) f は「全射」である。どの y にもそれに対応する x が存在する。
つまり，$\forall y \in K, \exists x, y = f(x)$
(3) 演算 $\circ$ において，$\forall x, y \in K$ において，$f(x \circ y) = f(x) \circ f(y)$

上の定義 (3) においては，四則演算に適用されるので，

- $\forall x, y \in K$ において，
  $f(x+y) = f(x) + f(y)$
- $\forall x, y \in K$ において，
  $f(x-y) = f(x) - f(y)$
- $\forall x, y \in K$ において，
  $f(x \cdot y) = f(x) \cdot f(y)$
- $\forall x, y \in K$ において，
  $f(x \div y) = f(x) \div f(y)$

演習 6 拡大体 $\mathbb{Q}\left(\sqrt{2}\right)$ において，次の問いに答えよ，

(1) 恒等写像 $\forall p,q\in\mathbb{Q}$ において，$f\left(p+q\sqrt{2}\right)=p+q\sqrt{2}$ が自己同形写像になることを示せ。
(2) 共役写像 $\forall p,q\in\mathbb{Q}$ において，$f\left(p+q\sqrt{2}\right)=p-q\sqrt{2}$ が自己同形写像になることを示せ。

この問題は「数学 II」における「複素数と方程式」「複素数」で「共役な複素数」としても扱っている。$p+q\sqrt{2}$ の共役な無理数は $p-q\sqrt{2}$，$p+qi$ の共役な複素数は $p-qi$ となることである。（解答略）

演習 7 有理数の拡大体 $\mathbb{Q}\left(\sqrt{2}\right)$ の任意の自己同形写像 f において，次の問いに答えよ，

(1) $f(0)=0$ を示せ。
(2) $f(1)=1$ を示せ。
(3) $\forall n\in\mathbb{N}, f(n)=n$ を示せ。
(4) $\forall m\in\mathbb{Z}, f(m)=m$ を示せ。
(5) $\forall q\in\mathbb{Q}, f(q)=q$ を示せ。

これにより，拡大体 $\mathbb{Q}\left(\sqrt{2}\right)$ の自己同型写像においては，有理数は自分自身に対応するということが示された。つまり，有理数 p の共役な無理数は自分自身 p となるということ。
（解答）

(1) $x-x=0$ より $f(x-x)=f(0)$ これは $f(x)-f(x)=f(0)$ ゆえに，$f(0)=0$
(2) $x\neq 0$ とする。$x\cdot 1=x$ より $f(x\cdot 1)=f(x)$ これは $f(x)\cdot f(1)=f(x)$ 変形すると $f(x)(f(1)-1)=0$ となるが $f(x)\neq 0$ より
$f(1)=1$
(3) $f(n)=f(1+1+\cdots+1)=f(1)+f(1)+\cdots+f(1)=1+1+\cdots+1=n$
(4) $m=-n$ とすると $f(m)=f(-n)=-f(n)-n=m$
(5) $m\in\mathbb{Z}, n\in\mathbb{N}$ とする。$q=\dfrac{m}{n}$ とすると，$f(q)=f\left(\dfrac{m}{n}\right)=\dfrac{f(m)}{f(n)}=\dfrac{m}{n}=q$

（解答終）

演習 8 $x^2=2$ の解が $x=\pm\sqrt{2}$ であることを利用して，拡大体 $\mathbb{Q}\left(\sqrt{2}\right)$ の自己同型写像は恒等写像と共役写像の 2 通りのみであることを証明せよ。

2 次方程式に関しての自己同型写像は 2 個しかないから，この先の話は単純に進んでいくことができる。3 次方程式における自己同型写像は $3!=6$，4 次方程式における自己同型写像は $4!=24$ となり，簡単には話が進まない。そこで「群」の概念が必要となってくる。
（解答）$f\left(x^2\right)=f(2)$ より $\{f(x)\}^2=2$ ゆえに $f(x)=\pm\sqrt{2}$ これは $f\left(\sqrt{2}\right)=\pm\sqrt{2}$
ここで，$p,q\in\mathbb{Q}$ とすると $f\left(p+q\sqrt{2}\right)=f(p)+f(q)\,f\left(\sqrt{2}\right)=p\pm q\sqrt{2}$（解答終）

3.4 解と係数の関係

「数学 II」における「複素数と方程式」「解と係数の関係」の内容である。

演習 9

$a, b \in \mathbb{Q}$ とする。2 次方程式 $x^2 + ax + b = 0$ の解を α, β とするとき，

$$\alpha + \beta = -a$$

を，$\alpha^2 + a\alpha + b = 0$ となることを利用して証明せよ。

（方針）解と係数の関係は，解の具体的な値がわからなくても，2 次方程式の二つの解を加えたら，有理数 $-a$ となることがわかった。このことから，2 次方程式の一方の解が無理数ならば，もう一方の解も無理数となることがわかる。

（解答）

$$\begin{aligned} x^2 + ax + b &= x^2 + ax + b - 0 \\ &= x^2 + ax + b - \left(\alpha^2 + a\alpha + b\right) \\ &= x^2 - \alpha^2 + ax - a\alpha + b - b \\ &= (x - \alpha)(x + \alpha) + a(x - \alpha) \\ &= (x - \alpha)(x + a + \alpha) \end{aligned}$$

ゆえに $\beta = -a - \alpha$，よって $\alpha + \beta = -a$（解答終）

演習 10 $a, b \in \mathbb{Q}$ とする。2 次方程式 $x^2 + ax + b = 0$ の 2 つの解は一方が無理数なら他方も無理数であることを証明せよ。

（解答）背理法を用いる。α が無理数のとき β を有理数と仮定すると，$\alpha = -\beta - a$ であるから α が有理数となり矛盾する。ゆえに β は無理数である。（解答終）

演習 11 2 次方程式の一つの解 α が無理数であったとする。有理数体 $\mathbb{Q}$ に α を加えた集合が $\mathbb{Q}$ の拡大体，すなわち $\mathbb{Q}(\alpha)$ になることを証明せよ。

2 次方程式の一つの解 α が無理数であったとする。有理数体 $\mathbb{Q}$ に α を加えた集合が $\mathbb{Q}$ の拡大体，すなわち $\mathbb{Q}(\alpha)$ になることを確認すればよい。つまり，$p_1, q_1, p_2, q_2 \in \mathbb{Q}$ としたとき，ふたつの数 $p_1 + q_1\alpha$, $p_2 + q_2\alpha$ が四則演算で閉じていることを示せばよいのだ。加法，減法は簡単だ。乗法も $\alpha^2 = -a\alpha - b$ を利用すれば難なく解決する。除法は少してこずるが，ヒントは，

$$(p + q\alpha)\left(a - \frac{p}{q} + \alpha\right)$$

を展開してみるとよい。

（解答）
和，差は自明であり，積は $\alpha^2+a\alpha+b=0$ から $\alpha^2=-a\alpha-b$ を利用すれば $p+q\alpha$ の形に変形できる。商については，

$$\begin{aligned}&(p+q\alpha)\left(a-\frac{p}{q}+\alpha\right)\\&=pa-\frac{p^2}{q}+qa\alpha+q\alpha^2\\&=q\left(\alpha^2+a\alpha\right)+pa-\frac{p^2}{q}\\&=-qb+pq-\frac{p^2}{q}\end{aligned}$$

の計算のように分母を有理化できる。　（解答終）

3.5　2 次体

2 次方程式の解を有理数に付加した体を総称して，**2 次体**という。

演習 12 $a,b\in\mathbb{Q}$ とする。2 次方程式 $x^2+ax+b=0$ の一つの解 α において，2 次体 $\mathbb{Q}(\alpha)$ はもう一つの解 β を必ず含んでいることを証明せよ。

（解答） $\beta=-a-\alpha\in\mathbb{Q}(\alpha)$　（解答終）

ここで，2 次体 $\mathbb{Q}(\alpha)$ における自己同型写像を考える。手法は拡大体 $\mathbb{Q}\left(\sqrt{2}\right)$ のときと同じで，結論も恒等写像と共役写像の 2 通りとなる。それを示す。それには，自己同型では有理数は自分自身に対応するということを利用する。

$f(x)$ が体 $\mathbb{Q}(\alpha)$ の自己同型ならば，すべての有理数 x を不変にする。すなわち，

$$\text{写像 } f:\mathbb{Q}(\alpha)\to\mathbb{Q}(\alpha)\text{ が自己同型 }\Rightarrow\ \forall x\in\mathbb{Q},f(x)=x$$

を念頭に置く。さらに，写像 $f:\mathbb{Q}(\alpha)\to\mathbb{Q}(\alpha)$ が自己同型のとき，$f(0)=0$ となることに留意して，

演習 13 2 次体 $\mathbb{Q}(\alpha)$ における自己同型写像 $f:\mathbb{Q}(\alpha)\to\mathbb{Q}(\alpha)$ は，恒等写像と共役写像の 2 通りのみとなることを証明せよ。

（証明）$p+q\alpha\in\mathbb{Q}(\alpha)$ に対して，自己同型写像 f の像 $f(p+q\alpha)$ は，

$$\begin{aligned}f(p+q\alpha)&=f(p)+f(q)f(\alpha)\\&=p+qf(\alpha)\end{aligned}$$

このことは，$\mathbb{Q}(\alpha)$ の元が自己同型 f によって何に対応するかを知るためには，α が f によって何に対応するかを考えれば良い。つまり，$f(\alpha)$ がどのような値をとるのか考えていく。そこで，$\alpha^2+a\alpha+b=0$ に対して，両辺に自己同型 f を操作すると，

$$\begin{aligned}f\left(\alpha^2+a\alpha+b\right)&=f(0)\\f(\alpha)^2+af(\alpha)+b&=0\end{aligned}$$

ここで，2 次方程式

$$f(\alpha)^2 + af(\alpha) + b = 0$$

の解は 2 次方程式 $x^2 + ax + b = 0$ と同じ解であるから。

$$f(\alpha) = \alpha \text{ または，} f(\alpha) = \beta$$

ゆえに，

$$f(p + q\alpha) = p + q\alpha \text{ または，} f(p + q\alpha) = p + q\beta$$

このことは，2 次体の自己同型写像は恒等写像または共役写像であることを示している。（証明終）

3.6 自己同型の有理数保存則

演習 14 2 次体の自己同型写像のうち共役写像 f について，$\forall p, q \in \mathbb{Q}, \alpha, \beta$ を 2 次方程式 $x^2 + ax + b = 0$ の無理数解とすると，以下のことが成り立つことを証明せよ。

- $f(\alpha) = \beta, f(\beta) = \alpha$
- $\forall x \in \mathbb{Q}(\alpha), f(f(x)) = x$

（証明）解と係数に関係により，$\alpha + \beta = -a$

この両辺に，2 次体の自己同型写像のうち共役写像を施すと，

$$f(\alpha + \beta) = f(-a) \quad \text{よって，} f(\alpha) + f(\beta) = -a$$

つまり，$f(\alpha) = \beta$ ならば，$f(\beta) = -a - f(\alpha) = -a - \beta = a$ となる。（証明終）

以上より，「自己同型の有理数保存則」が成り立つ。ここではその逆の，「自己同型で不変になるものは有理数のみである」ことを示す。

演習 15 $\mathbb{Q}(\alpha)$ の自己同型写像のうち共役写像 f において，$f(x) = x$ となる x は有理数のみであることを証明せよ。

（証明）$\forall p, q \in \mathbb{Q}, \alpha, \beta$ は 2 次方程式 $x^2 + ax + b = 0$ の無理数解とすると，共役写像 f は，

$$f(p + q\alpha) = p + q\beta$$

であるから，$p + q\alpha = p + q\beta$，これは $q(\alpha - \beta) = 0$ となる。ここで，解と係数の関係より，$\alpha + \beta = -a$ であるが，$\alpha = \beta$ とすると，$\alpha = \beta = -\dfrac{a}{2}$ となり，解 α が有理数となって，無理数である仮定に反する。よって，$q = 0$ である。ゆえに $x = p$ となり，x は有理数となる。（証明終）

4 2次方程式は四則演算とベキ根で解ける

演習 16 2次方程式は，係数に関する平方根と四則演算をとる操作だけによってすべての解を求めることができることを証明せよ。

（方針）共役写像 f において，$f\left((\alpha-\beta)^2\right)$ を計算することにより，$(\alpha-\beta)^2$ が有理数であることを示す。$\alpha-\beta$ は有理数の平方根であり，この $\alpha-\beta$ と，解と係数の関係 $\alpha+\beta=-a$ によって，α が有理数の平方根と四則演算から求められることを示せば良い

（証明）共役写像 f において，

$$\begin{aligned} f\left((\alpha-\beta)^2\right) &= f\left((\alpha-\beta)(\alpha-\beta)\right) \\ &= f(\alpha-\beta)\,f(\alpha-\beta) \\ &= (f(\alpha)-f(\beta))\,(f(\alpha)-f(\beta)) \\ &= (\beta-\alpha)(\beta-\alpha) \\ &= (\alpha-\beta)^2 \end{aligned}$$

ゆえに，$(\alpha-\beta)^2\in\mathbb{Q}$ となる。ここでは $D=(\alpha-\beta)^2$ とおくと，

$$\alpha-\beta=\pm\sqrt{D}$$

これと，解と係数の関係 $\alpha+\beta=-a$ によって，α が有理数の平方と有理数との四則演算から求められることがわかる。（証明終）

ここでは自己同型写像により $(\alpha-\beta)^2$ が有理数となることがポイントであった。ここで，$(\alpha-\beta)^2$ を対称式[17]という観点からみてみよう。

「数学 II」における「複素数と方程式」「解と係数の関係」では，2次方程式 $ax^2+bx+c=0$ の解と係数の関係の基本対称式 $\alpha+\beta=-\dfrac{b}{a},\alpha\cdot\beta=\dfrac{c}{a}$ により，α と β の対称式の値[18]を求めている。ところが対称式だけでは2次方程式は解けない。解の一方に代入すると2次方程式の解の公式が必要になってくるからだ。ここでは2次方程式の解の公式は使ってはならない。そこで登場してきたのが $\alpha-\beta$ である。これは対称式ではない。すなわち α と β を入れ替えると別の式になる。ところが2乗すると $(\alpha-\beta)^2$ は対称式となるのだ。そして平方根を利用するのだ。つまり平方根に課せられた任務は四則演算だけでは対称性を保ち続けている状態をぶち壊わすことにある。対称式 $(\alpha-\beta)^2$ を計算した後に平方根をとれば，$\alpha+\beta$ と $\alpha-\beta$ により解を得ることができる。すなわち，四則演算と平方根で2次方程式の解は表現できるということになる。

演習 17 [19]

2次方程式 $x^2-3x-1=0$ の二つの解を α,β とするとき，次の式の値を求めよ。

(1) $\alpha^2+\beta^2$　　(2) $\dfrac{\beta}{\alpha}+\dfrac{\alpha}{\beta}$　　(3) $(\alpha-\beta)^2$

[17] 2次の対称式は，お互いを入れ替えても式がかわらない式のことをいう。
[18] 任意の対称式は，基本対称式の四則演算で値を求めることができる。（証明略）
[19] 数研出版「数学 II」（平成 26 年度）pp46

基本対称式から，対称式の値を求める問題である。まさにここで述べた事柄である。

5 まとめ

ここでは 2 次方程式の解の公式を使わずに話を進めてきたため，専門的な概念を用いた非常に回りくどい内容となってしまったが，この方法が 3 次以上では効果を発揮するのだ。

2 次方程式の解の公式の存在の証明では，2 次体 $\mathbb{Q}(\alpha)$ の自己同型で不変となるものが有理数であることが重要であった。それから，実際に自己同型で不変になる式 $\alpha-\beta$ と解と係数の関係 $\alpha+\beta=-a$ を使った。3 次以上も基本的にはこの方法論で話は進む。3 次方程式においては対称式 $\{(\alpha-\beta)(\beta-\gamma)(\gamma-\alpha)\}^2$ を利用して平方根により対称性を崩している。さらには，この考え方を発展させて，5 次以上の方程式には解の公式が存在しないことを明確に与えることができるのだ。

2 次方程式においては，2 次体の自己同型は 2 種類しかなく，とても単純な構造である。しかし，3 次以上となるともっと複雑となり，それを解決するには「群」という概念を用いなくてはならない。ガロア理論は最終的には「5 次交代群は単純群 (単位元と自分自身以外に正規部分群がない) である。」に帰結する。加えて方程式の解から作る「体」を記述するためには「複素数」の導入も必要となる。複素数における「1 のベキ根」をも考えなければならない。線形代数の知識も不可欠である。数学の基礎を積み重ねたその先に，ガロアの定理が見えてくるのだ。今後はガロア理論の応用としてギリシャ三大作図問題の解決や正 17 角形の作図 [20] も教材として探っていきたい。

なお，平易と思われる演習の解答は紙面の都合上，割愛した。ご容赦頂きたい。

参考文献

1. 冒頭の 8 冊
2. Artin,E., (寺田文行), ガロア理論入門, ちくま学芸文庫, 2010
3. 志賀浩二, 群論への 30 講, 朝倉書店, 1996
4. 草場公邦, ガロワと方程式, 朝倉書店, 1989
5. 渡辺敬一, 代数の世界 改訂版, 朝倉出版, 2012
6. 上野健爾, 「ガロアの考えたこと」, 現代思想, vol39-4, pp38-58, April, 2011

[20] ガウス (1796 年)Carolus Fridericus Gauss,1777-1855 によって証明された。そののち，$p=2^{2^e}-1$ が素数ならば，正 p 角形が作図可能でありことがガロア理論によって示される。