ガロア理論の初等的解題

１．ガロア理論の基本定理

エヴァリスト・ガロア[1]という，わずか20歳で夭逝した数学者の遺した一篇の論文が，数百年に及ぶ数学史上の難問を根底から解決し，後の数学界に革命をもたらしたという一大ロマンは，専門の研究者ばかりでなく，数学にあまり関心のない人々にとっても興味のある出来事であろう．しかもこの論文は死後の発表当時はだれにも理解されず，何十年も後にやっと「解読」されるに至ったのである．もちろん当時の数学者たちが愚かだったわけではなく，ガロアがあまりにも卓越しすぎていたのである．

幸い，かつ当然なことに，後世の数学者たちの尽力によって，彼の思想は数学全般の中でもひときわ美しい体系を持つガロア理論として仕上げられ，今も発展を遂げている．そんな魅力的な理論をエッセンスだけでも賞味しようとは誰しも思うのではないか，精緻な証明を抜きにしてでも天才のひらめきがもたらす威力を味わってみたいものだと．それは簡単なことではないが不可能ではないであろう．

この小論の冒頭から「ガロア理論の基本定理」と呼ばれるものを掲げることは一見無謀に思えるが，それには小論であるがゆえに始めに目標を掲げ，目指す峰を常に視野に入れておこうという目論見がある．一つ一つの用語が理解され，定理全体の意味がつかめたときには，その峰からの眺望に思わず感嘆を洩らすことになろう．「幾何学に王道なし」とはユークリッドの言葉ではあるが，我々は先人のおかげでこの王道をゆっくり楽しみながら登ることが可能である．

これを読む人の数学のレベルとしては高校数学II～IIIの特に代数･複素数くらいを想定するが，随時必要な定義や用語をなるべく平易な形で取り入れていくことにする．

というわけで，まず，天下り的に「ガロア理論の基本定理」を述べる．

【定理１】(基本定理)　K を k の正則拡大体，G をそのガロア群とする．K の中間体と G の部分群は１対１に対応し，相対応する中間体の次数と部分群の位数は等しい．

この定理がなぜ「代数方程式の不可解性」や「作図不可能問題」などという難解極まりない問題に対して威力を発揮するのかというと，これらの問題は，体（タイ）と呼ばれるある集合の性質の問題に帰着され，さらにその体の性質を群（グン）と呼ばれる別の集合に反映させることによって解決できるからである．基本定理のなかに体とか群という語が出てくるのがそれである．

実際，ガロアに先行する夭折の天才数学者アーベル[2] は体の思想を駆使して五次方程式の代数的不可解性を証明したのであった．その証明の中には群の性質も取り入れられてはいたものの，その強力な一般的原理を確立するにはガロアの功績を待たなければならなかったのである．

以下において，まずは基本定理の意味するところを理解するために，体や群などの用語を順次説明し，その威力を十分知った上で，その証明を試みることにする．

---

[1] GALOIS，Èvariste (1811/10/25~1832/5/31)　岩波数学辞典第２版を参照した．

[2] ABEL，Niels Henrik（1802/8/5~1829/4/6）ガロアと同時代のノルウエーの数学者．26歳で逝去（同上）．

２．体とその次数

まず，体について．なお，以下の用語の説明は平易を旨とし，必ずしも厳密ではないことをことわっておく．正確な数学的概念としては数学辞典等を参照されることを望むものである．

体とは，数の集合で**四則**（加減乗除）において閉じているものをいう．

一般に，ものの集まりを**集合**といい，それに含まれている一つ一つのものを**元**（または**要素**）というが，体は四則計算がいつでも行なえてその答えが同じ集合に属しているような集合をいうのである．もちろん0（ゼロ）で割ることは除いて考える．体は加減乗除について閉じていることを要求するため，対象は主に数の集合に限られる．方程式の（代数的）解法とは，その係数などに対する四則や累乗根等の計算によってその解を求めようとするのであるから，体という考えに到るのは自然であるといえよう．

例えば，分数全体の集合を考えたとき，普通これを**有理数の集合**という．分数±分数，分数×分数，分数÷分数などはいずれも答えがまた分数になる．これを**有理数体**といい，数における体のなかでもっとも「小さい」ものである．この小論において重要な脇役の一人で，Q で表わされる．

同様に実数の集合，複素数の集合なども体である．それぞれを**実数体** R，**複素数体** C と呼ぶ．

こう考えると体はもうこれ以外にはないように思われるが，これらのいわば「自然」な体に対して人為的に構成される体を考えることができるのである．

それは、有理数でない数を１つまたは数個、有理数体 Q に「付け加えて」やることで実現できる．

例えば，$\sqrt{2}$ という有理数でない数[3]と有理数とを加減乗除してできるすべての数から成る集合，

$$\{a+b\sqrt{2} \mid a,b\in Q\}$$

を考えると，この集合は体になる．実際に計算して確かめてみよう．

加減法：$(a+b\sqrt{2})\pm(c+d\sqrt{2})=(a\pm c)+(b\pm d)\sqrt{2}=A+B\sqrt{2}$ ，

乗法　：$(a+b\sqrt{2})(c+d\sqrt{2})=(ac+2\mathrm{bd})+(ad+bc)\sqrt{2}=C+D\sqrt{2}$ ，

除法：$\dfrac{a+b\sqrt{2}}{c+d\sqrt{2}}=\dfrac{(a+b\sqrt{2})(c-d\sqrt{2})}{(c+d\sqrt{2})(c-d\sqrt{2})}=\dfrac{(ac-2bd)+(ad-bc\sqrt{2})}{c^2-2d^2}=\dfrac{ac-2bd}{c^2-2d^2}+\dfrac{ad-bc}{c^2-2d^2}\sqrt{2}=E+F\sqrt{2}$ ．

ここで A,B,C,D,E,F はいずれも有理数(分数)であり，この集合は四則に閉じていることがわかる．要するに，有理数と $\sqrt{2}$ を何度加減乗除しても有理数でない数は $\sqrt{2}$ 以外には出てこない．この体を，「有理数体 Q に $\sqrt{2}$ を付け加えて作った体」という意味で Q の**拡大体**といい，$Q(\sqrt{2})$ と表わす．

体 $Q(\sqrt{2})$ の任意の元は，すべて $a+b\sqrt{2}$ の形で表わすことができる．いいかえると，1と $\sqrt{2}$ にそれぞれ任意の有理数を掛けて足せばどんな元でも表わせる．このときの1と $\sqrt{2}$ の組 {1，$\sqrt{2}$ } のことを体 $Q(\sqrt{2})$ のひとつの**底**（テイ）（または**基底**）という．「ひとつの」というのは，一般に a，b を有理数とすれば，a と $b\sqrt{2}$ を底とすることができるからである．従って底はいくつにも取れるが，その個数は決まっている．その個数２を体 $Q(\sqrt{2})$ の Q に対する**次数**といい，[$Q(\sqrt{2})$:Q]= 2 と表わされる．$Q(\sqrt{2})$ は Q に対して**2次の体**であるともいう．体の次数は，その拡大の程度を表わすものと見ることができる．「基本定理」にも出ているように非常に重要な概念である．

さて，この１つの例で類推できるように，体はいくらでも存在する．容易に $Q(\sqrt{3})$ とか $Q(\sqrt{5})$ などが作られるのがわかるだろう．Q のある数からその平方根を作り，それを Q に追加することで簡単に新たな体を作ることができるのである．ただし，追加する数は有理数でないものでなければならない．$\sqrt{9}$ では=3なので，$Q(\sqrt{9})$ =Q となり，新たな拡大体を作ることはできない．このようにある既存の体に対してその体には属さないある数を追加して拡大体を作るとき，追加する数をその体の**超数**[4]という．

---

3) $\sqrt{2}$ が有理数でないことは，次のように説明できる．$\sqrt{2}$ = p/q (p : 整数, q: 自然数)とおき，既に約分されているとする．分母を払って２乗すると，$2q^2=p^2$ となって p が偶数になるので，$p=2p'$ とおいて代入すれば，$q^2=2p'^2$ となって今度は q が偶数になり，結局 p/q が既に約分されているというのに反する．

4) 著者による造語．

有理数体Qに追加できるのは累乗根だけとは限らない．有理数でない数なら何を追加しても新たな体を作ることができる．虚数単位のiやπなどでも可能である．さらには追加する個数も何個でもかまわない．

しかし，この小論では体に追加する数は有限個とし，さらに次の条件を設定する．それは<u>追加する数（超数）はある代数方程式の解になる数のみとする</u>のである．これに関して次の重要な定理が成り立つ．

【定理2】．Qを有理数体とする．$f(x)$をQの元を係数に持つn次既約代数方程式，αをその一つの解とするとき，体$Q(\alpha)$の元はすべて $a+b\alpha+c\alpha^2+...+m\alpha^{n-1}$ の形に一通りに書き表される．ただし， $a,b,c,...m$ はQの元である．

この定理の意味は，αがn次方程式の解ならば，体 $Q(\alpha)$ のどんな元もαのn-1次式で表されるということである．これは方程式の解から作られた拡大体の持つ著しい性質である．

この定理を証明するのに必要な用語をいくつか述べる．

まず一般的に，代数方程式を，有理数体Qにこの方程式の係数を追加した拡大体を基礎にして考えることにする．この体を方程式の**基礎体**という．方程式の係数がすべて有理数なら基礎体はQのままである．また，もし係数の中に $\sqrt{2}$ が入っていたら基礎体は $Q(\sqrt{2})$ ということになる．

【定理2】の中で**既約方程式**といっているのは，基礎体の中に解をひとつも持たない方程式のことで，その方程式を**基礎体上で既約**という． $x^2+x+1=0$ や $x^3-2=0$ は基礎体Q上で既約である．一方，$x^2+x-2=0$ や $x^3-1=0$ は有理数の解を持つので，Q上既約ではない（既約でない場合を可約という）．

では，方程式 $x^3-2=0$ に即して上の定理を証明してみよう．

この方程式の解のひとつは $\sqrt[3]{2}$ である（これは2の3乗根のうちの実数であるものとする．およそ1.2599...で，もちろん無理数）．これをQに追加して体 $Q(\sqrt[3]{2})$ を作る． $Q(\sqrt[3]{2})$ の元は有理数と $\sqrt[3]{2}$ との四則計算によって得られるすべての数から作られる集合であるから，その一般形は取りあえず次のような分数式で表わされる．以下， $\sqrt[3]{2}$ の係数はすべて有理数である．

$$\frac{a_1+a_2\sqrt[3]{2}+a_3(\sqrt[3]{2})^2+...}{b_1+b_2\sqrt[3]{2}+b_3(\sqrt[3]{2})^2+...} \quad .$$

【定理２】は，これがすべて $a+b\sqrt[3]{2}+c(\sqrt[3]{2})^2$ の形に表わされるといっているのである．これを証明してみよう．まず思い付くことは，問題は分母の有理化の可能性に限定されるということである．これを踏まえ，また見やすくするために $\sqrt[3]{2}$ をαで置き換えて，

$$\frac{a_1+a_2\alpha+a_3\alpha^2+...}{b_1+b_2\alpha+b_3\alpha^2+...}=\frac{f(\alpha)}{g(\alpha)} \qquad [1]$$

とする．いま，$g(\alpha)$のαをxに置き換えて$g(x)$というxの整式を作り，$g(x)$と x^3-2 との最大公約数を考える．x^3-2 はQ上既約なので，最大公約数は１である．

次に，一般に整式に関する一定理として「**整式$F(x)$，$G(x)$の最大公約数を$d(x)$とするとき，ある整式$p(x)$，$q(x)$が存在して，**

$$p(x)F(x)+q(x)G(x)=d(x)$$

が成り立つ」というのがある（この証明は付録１で行なっている）．今これを，$g(x)$と x^3-2 に応用すれば，ある多項式$p(x)$，$q(x)$がが存在し，

$$p(x)g(x)+q(x)(x^3-2)=1 \quad .$$

が成り立つ．これに$x=\alpha$を代入すると， $\alpha^3-2=0$ より $p(\alpha)g(\alpha)=1 \quad \therefore g(\alpha)=\frac{1}{p(\alpha)}$ となる．これを式[1]に代入すると，

$$\frac{f(\alpha)}{g(\alpha)}=f(\alpha)\,p(\alpha)$$

となって，分母が有理化された．

次はこの式がαの2次以下の式になることを示す．またαの替わりに x を使って $c(x)=f(x)p(x)$ とし，$c(x)$ を x^3-2 で割ったときの商を $a(x)$，余りを $r(x)$ とすると，

$$c(x)=\ a(x)(x^3-2)+r(x)$$

となって $r(x)$ は余りだから2次以下の多項式となる．ここでまた $x=\alpha$ を代入すると，$\alpha^3-2=0$ により $c(\alpha)=r(\alpha)$ となって $c(\alpha)$ は2次以下のαの多項式となる．（【定理2】の証明終わり[5]）

以上の結果，$Q(\sqrt[3]{2})$ の底の一組は $\{1,\ \sqrt[3]{2}\ ,\ (\sqrt[3]{2})^2\ \}$ であり，次数は3である．

$$[\ Q(\sqrt[3]{2})\ :\ Q\ ]=3\ .$$

さて，拡大体 $Q(\sqrt[3]{2})$ と Q を集合の包含関係式で表わせば，

$$Q\subset Q(\sqrt[3]{2})$$

となり，Q は $Q(\sqrt[3]{2})$ の部分集合になる．部分集合であって体なので，Q を $Q(\sqrt[3]{2})$ の部分体という．拡大体と部分体の関係を表わす記号が $Q(\sqrt[3]{2})\ /Q$ である．「$Q(\sqrt[3]{2})$ は Q の拡大体」という意味でもある．

拡大体のなかで特に重要なものが，基本定理にも出ている正則拡大体である．

Q上のある既約代数方程式の解がすべて拡大体K/Qに含まれているとき，Kを正則拡大体という．特に n 次既約代数方程式の n 個の解を $\alpha_1,\alpha_2,...,\alpha_n$ とするとき，拡大体 $Q(\alpha_1,\alpha_2,..,\alpha_n)$ を ***n*** 次の正則拡大体という．正則拡大体は，ガロア理論においてガロア群とともに主役を成す用語である．ガロア拡大体とも，単にガロア体ともいう．

一般に n 次方程式は（重複も含めて）n 個の解を持つ[6]．これらを互いに共役な解と呼ぶ．前述の体 $Q(\sqrt{2})$ は，Q に $\sqrt{2}$ だけを追加したのであるが，既約方程式 $x^2-2=0$ の共役な解 $x=\pm\sqrt{2}$ を両方とも含んでいるので，正則拡大体である．

また例えば，方程式 $x^2+1=0$ の場合は，解は虚数 $x=\pm i$ になるが，この場合も拡大体 $Q(i)$ は正則拡大体になる．一般に2次体はすべて正則である．

しかし，3次の体になるとすべてそうとはいかない．例えば前述の $Q(\sqrt[3]{2})$ は方程式 $x^3-2=0$ のひとつの解 $\sqrt[3]{2}$ を追加した3次の体であるが，これは正則ではない．$Q(\sqrt[3]{2})$ はこの方程式の他の解を含まないのである．一般に，

$$x^n-a=0\quad (a\text{は複素数}) \qquad [2]$$

の形の方程式を二項方程式という．この方程式の解は次のようにして形式的に求められる．例えば n=3 の場合，$x^3-2=0$ の $\sqrt[3]{2}$ 以外の他の解を求めるためには，まず1の虚数立方根を導入する．

方程式 $x^3-1=0$ は Q 上既約ではないので，これを因数分解すると，

$$x^3-1=(x-1)(x^2+x+1)=0\ .$$

ここから x = 1 以外の1の3乗根が求められる．$x^2+x+1=0$ の解は，2次方程式の解の公式から，

$$x=\frac{-1\pm\sqrt{-3}}{2}$$

となるが，この2つの複素数を1の虚数立方根といい，どちらか一方を ω（オメガ，ギリシャ文字）で表わす習慣がある．一方を ω とすると，もう一方は ω^2 で表わされるという強い性質がある．よってどちらかを ω と特

---

[5] 【定理2】をここでは $x^3-2=0$ を例として説明したが，同じ論法で一般の方程式についても証明できる．

[6] これを通常「代数学の基本定理」という．簡単な証明を付録2に載せた．

定しないことになっている．このことは方程式の解が強い対称性を持っていることの現れでもある．

$\omega=\dfrac{-1\pm\sqrt{-3}}{2}$ ならば， $\omega^2=\left(\dfrac{-1\pm\sqrt{-3}}{2}\right)^2=\dfrac{1\mp2\sqrt{-3}-3}{4}=\dfrac{-1\mp\sqrt{-3}}{2}$ （複号同順）

従って方程式 $x^3-1=0$ の３つの解は，1，ω，ω^2 ということになる． $\omega^2+\omega+1=0$ というのも重要な性質である．

$x^3-2=0$ の３つの解を表すには，２の３乗根 $\sqrt[3]{2}$ に１の３乗根を各々かけて $\sqrt[3]{2}$ ， $\sqrt[3]{2}\omega$ ， $\sqrt[3]{2}\omega^2$ とするのである（どれでも３乗すれば２になることを確かめよ）．さらには通常 $\sqrt[3]{2}$ の意味は２の３乗根のうちの実数を表わすとするのであるが，ここまで来るとそれは意味を持たなくなる．すなわち $\sqrt[3]{2}$ とは $\sqrt[3]{2}$ ， $\sqrt[3]{2}\omega$ ， $\sqrt[3]{2}\omega^2$ のうちのどれかであると決めればよい．ひとたび決めれば，他の２つのものはやはり $\sqrt[3]{2}\omega$ ， $\sqrt[3]{2}\omega^2$ で表わされるのである．２の３乗根とは常に $\sqrt[3]{2}$ ， $\sqrt[3]{2}\omega$ ， $\sqrt[3]{2}\omega^2$ であって，互いに全く平等である．

さて一般の場合には，「１の n 乗根」というのをド･モアブルの定理を用いて，

$$\lambda_k=\cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n}\quad(k=0,\ 1,\ 2,\ \ldots\ ,\ n-1)\quad(\lambda:\ \text{ラムダ，ギリシア文字})$$

で表わし，これを使って一般の二項方程式 $x^n-a=0$ （a は複素数）の解を表わす． $x=\sqrt[n]{a}$ をそのひとつの解とし，１の n 乗根を 1，λ，λ^2，…，λ^{n-1} とすると，

$$x\ =\ \sqrt[n]{a},\ \lambda\sqrt[n]{a},\ \lambda^2\sqrt[n]{a},\ \ldots\ ,\ \lambda^{n-1}\sqrt[n]{a} \qquad [3]$$

がすべての解である[7]．

さて，話を体 $Q(\sqrt[3]{2})$ に戻そう．Q に解のひとつ $\sqrt[3]{2}$ を追加して拡大体を作っても，その体の中には $\sqrt[3]{2}\omega$ や $\sqrt[3]{2}\omega^2$ は含まれてこない．なぜならもし $\sqrt[3]{2}$ を実数と決めてあれば，有理数と $\sqrt[3]{2}$ を加減乗除しても $\sqrt[3]{2}\omega$ や $\sqrt[3]{2}\omega^2$ という虚数を作り出すことはできないからだ．同様に Q に $\sqrt[3]{2}\omega$ か $\sqrt[3]{2}\omega^2$ のどちらかを追加して作った拡大体には，今度は実数 $\sqrt[3]{2}$ が含まれてこない．だからこの方程式の解をすべて含む正則拡大体を作ろうと思えば，Q に二つの数，ω と $\sqrt[3]{2}$ を「別々に」追加しなくてはならないのである．こういうときは， $Q(\omega,\sqrt[3]{2})$ と表わす．

一般に，有理数体 Q の元 $a_1,a_2,\ldots,a_{n-1},a_n$ を係数とする n 次方程式

$$x^n+a_1x^{n-1}+a_2x^{n-2}+\ldots+a_{n-1}x+a_n=0\ . \qquad [4]$$

の解を $x_1,x_2,\ldots,x_n$ とするとき，体 $Q(x_1,x_2,\ldots,x_n)$ を，この方程式の分解体という（既約･可約を問わない）．そして Q が $x_1,x_2,\ldots,x_n$ をひとつも含まないときに体 $Q(x_1,x_2,\ldots,x_n)$ は正則拡大体となる．

$x^3-2=0$ の場合，求める正則拡大体は $Q(\sqrt[3]{2},\ \omega\sqrt[3]{2},\ \omega^2\sqrt[3]{2})$ であるが，一方 $Q(\omega,\sqrt[3]{2})$ には３つの解が含まれているのは明らかである．よって， $Q(\sqrt[3]{2},\ \omega\sqrt[3]{2},\ \omega^2\sqrt[3]{2})\subseteq Q(\omega,\sqrt[3]{2})$ ，他方， $Q(\omega,\sqrt[3]{2})$ の ω は $Q(\sqrt[3]{2},\ \omega\sqrt[3]{2},\ \omega^2\sqrt[3]{2})$ の $\sqrt[3]{2}$ と $\sqrt[3]{2}\omega$ の商によって作り出せるから，$\omega\in Q(\sqrt[3]{2},\ \omega\sqrt[3]{2},\ \omega^2\sqrt[3]{2})$ ，従って， $Q(\omega,\sqrt[3]{2})\subseteq Q(\sqrt[3]{2},\ \omega\sqrt[3]{2},\ \omega^2\sqrt[3]{2})$ ，ゆえに $Q(\omega,\sqrt[3]{2})=Q(\sqrt[3]{2},\ \omega\sqrt[3]{2},\ \omega^2\sqrt[3]{2})$ が成り立つ[8]．

$Q(\omega,\sqrt[3]{2})$ の元の一般形はどんな形になるだろうか．

まず Q に ω を追加して $Q(\omega)$ を作ろう．これを Q' とすると Q' の一般形は $a+b\omega$ となる．なぜなら ω は $\omega^2+\omega+1=0$ を満たす，すなわち $\omega^2=-\omega-1$ となって２次の項は１次の項に解消されるため，ω は１次の項しか出てこないのである．従って，Q' の Q に体する底（のひとつ）は{1，ω}であり，次数は$[Q':Q]=2$ である．

---

[7] １の n 乗根は代数的にも解かれるが，普通は以上のようにして表現される．

[8] 一般に２つの集合 A，B について，A⊆B かつ A⊇B ならば，A=B が成り立つ．

次に，このQ'にさらに $\sqrt[3]{2}$ を追加して $Q'(\sqrt[3]{2})$ すなわち $Q(\omega,\sqrt[3]{2})$ を作るのであるが，ここでも式の見通しをよくするために $\sqrt[3]{2}$ をTで表わすことにしよう．

$Q'(\sqrt[3]{2})$ すなわち $Q'(T)$ とQ'とQの，３つの集合としての包含関係は， $Q\subset Q'\subset Q'(T)$ ということになる．

Q'の元を a',b',c' 等で表わせば，それに追加するTとの四則によってつくられる数は，【定理2】の Q をQ'に読み替えてやることによって，

$$a'+b'T+c'T^2 \qquad (\ a',b',c'\in Q'\ ) \tag{5}$$

となる．これが $Q'(T)$ の元の一般形である．つまり底として {1，T，T^2} を取ることができる．

$Q'(T)$ のQ'に対する次数は，[$Q'(T):Q'$]= 3 である．そしてさらに a',b',c' はQ'= $Q(\omega)$ の元であるから， $a'=a_1+a_2\omega$， $b'=b_1+b_2\omega$， $c'=c_1+c_2\omega$ （ $a_1,a_2,b_1,b_2,c_1,c_2\in Q$ ）とおける．ゆえに，

$$(a_1+a_2\omega)+(b_1+b_2\omega)T+(c_1+c_2)T^2 \tag{6}$$

となる．さらにこの式のカッコを外せば，

$$a_1+a_2\omega+b_1T+b_2\omega T+c_1T^2+c_2\omega T^2 \tag{7}$$

となるので， $Q'(T)$ のQに対する底を $\{1,\omega,T,\omega T,T^2,\omega T^2\}$ とすることができ，従って $Q'(T)$ のQに対する次数は，[$Q'(T):Q$]= 6 となる．

いうなれば， $Q'(T)$ は２次の体Q'= $Q(\omega)$ の上に３次の体 $Q(T)$ を積み上げて６次の体を作っているのである．よって，

$$\underset{6}{[Q'(T):Q]}=\underset{3}{[Q'(T):Q']}\cdot\ \underset{2}{[Q':Q]}$$

という式が成り立つ．

一般に， $k\subset L\subset K$ の関係にある体の次数について，

$$[K:k]=[K:L][L:k] \tag{8}$$

という式が成り立つ[9]．

では，Qに一度にひとつだけの数を追加して $Q(\omega,\sqrt[3]{2})$ と同じ体を作ることはできないだろうか．実はできるのである．その一例として $\omega+\sqrt[3]{2}$ という数がある．すなわち，

$$Q(\omega,\sqrt[3]{2})\ =\ Q(\omega+\sqrt[3]{2}) \tag{9}$$

が成り立つのである．注 8)で述べた二つの集合の等しいことを示す方法で簡単な証明を述べておく．

まず明らかに，

$$Q(\omega,\sqrt[3]{2})\ \subset\ Q(\omega+\sqrt[3]{2}) \tag{10}$$

が成り立つ（ωと $\sqrt[3]{2}$ があれば $\omega+\sqrt[3]{2}$ が作られるから）．

これとは反対に $Q(\omega,\sqrt[3]{2})\supset Q(\omega+\sqrt[3]{2})$ も成り立つことを示そう．そのためにはωと $\sqrt[3]{2}$ が $Q(\omega+\sqrt[3]{2})$ に含まれていること，つまり $\omega\in Q(\omega+\sqrt[3]{2})$， $\sqrt[3]{2}\in Q(\omega+\sqrt[3]{2})$ であることを示せばよい．そこでまず，$\theta=\omega+\sqrt[3]{2}$ とおく． $Q(\omega+\sqrt[3]{2})\ =\ Q(\theta)$ である．

$\theta=\omega+\sqrt[3]{2}$ から $\sqrt[3]{2}=\theta-\omega$ とすれば， $(\sqrt[3]{2})^3-2=0$ であるから，

$$(\theta-\omega)^3-2=0\ .$$

これを展開し，ω^3= 1 も使って，

[9] ここでは証明はしないが，体の元の一般項の項の数を見て何となく納得できるのではないだろうか．

$$\theta^3-3\theta^2\omega+3\theta\omega^2-3=0 \qquad [11]$$

ここで $\omega^2=-\omega-1$ であるから，式[11]に代入すれば，

$$\theta^3-3\theta^2\omega+3\theta(-\omega-1)-3=0$$
$$\therefore\ \theta^3-3\theta^2\omega-3\theta\omega-3\theta-3=0$$
$$\therefore\ \omega=\frac{\theta^3-3\theta-3}{3\theta^2+3\theta}$$

となって，ω は Q の元と θ で表わされる．すなわち $\omega \in Q(\theta)$ ．また $T=\theta-\omega$ であるから，$T \in Q(\theta)$ となる．よって $\omega \in Q(\omega+\sqrt[3]{2})$ ，$T \in Q(\omega+\sqrt[3]{2})$ が示された．ゆえに $Q(\omega,\sqrt[3]{2}) \supset Q(\omega+T)$ ．従って，目的の $Q(\omega,\sqrt[3]{2}) = Q(\omega+T)$ が得られる．

一般に，ただ一つの数を追加してできる拡大体を単純拡大体という．さらに，Q に既約方程式の解を何個か追加して正則拡大体を作るときに，それを上記のようにただひとつの数を追加して同じ拡大体を作ることが可能であるが，ここでは一般的な証明は略す．大略は上記の方法と変わらない．

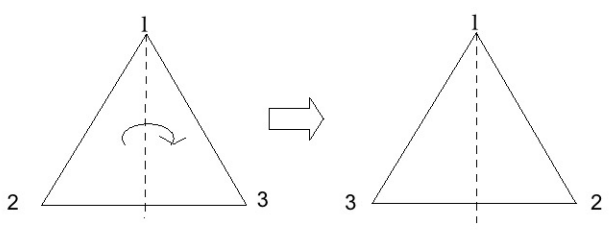
このことを逆にいうと，既約方程式の解を（いくつか）追加してできる任意の拡大体は，ある正則拡大体の部分体であるということになる．

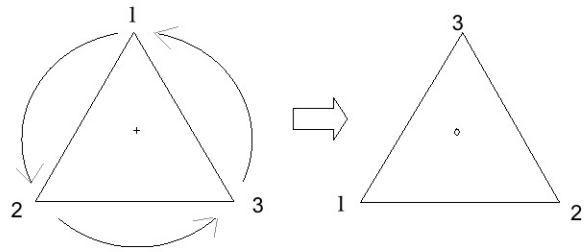
これで，ガロア理論の基本定理のうち，「K を k の正則拡大体」というところの説明が終わった．次はガロア群について説明するのであるが，そのためにまず群についての一般論を述べる．

３．群および置換群

群とは，ガロアが初めて使い出した数学用語で，数ではないもの（数でもよいが）の集合がある演算を満たしているとき，それを群と呼ぶ．今では群にもいろいろあるが，ガロア理論で群といえば置換群のことといってよい．

置換とはものの位置を置き換えることである．例えば正三角形を動かしてまたそれ自身にぴったり重ねるとき，これを正三角形の置換ということにする．正三角形の各頂点を 1，2，3 とするとき，頂点 1 から対辺に垂線を引いて，この垂線を軸にして対称移動させた時，正三角形はまた自分にぴったり重なるのでこの対称移動は置換である．（下図左）





また正三角形の重心を中心として 120°回転させることでも置換できる．（上図右）

この置換の中に，正三角形をまったく「動かさない置換」も含むことにすると（これを恒等置換という），これらの置換には全部で 6 通りある（線対称による置換 3 つと重心を中心とした正 120°の回転と正 240°の回転，そして恒等置換）．

この 6 つの置換を記号で表現してみよう．正三角形の置換は頂点を表わす 1,2,3 という 3 つの文字を置き換えていると見ることもできる．よってこの 6 つの置換を正三角形という言葉を使わずに単に 3 つの文字 123 がこの順序から 132 に，あるいは 312 等々に換わることと表現しても同じことである．

実際の置換:: 123→123，123→132，123→231，123→213，123→321，123→312.

置換の表現: $\begin{pmatrix}123\\123\end{pmatrix}$, $\begin{pmatrix}123\\132\end{pmatrix}$, $\begin{pmatrix}123\\231\end{pmatrix}$, $\begin{pmatrix}123\\213\end{pmatrix}$, $\begin{pmatrix}123\\321\end{pmatrix}$, $\begin{pmatrix}123\\312\end{pmatrix}$.

置換の名前: σ_1, σ_2, σ_3, σ_4, σ_5, σ_6.

(σ はシグマと読む).

この表現では括弧の中の上の文字列を下の文字列に並べ替えて（置き換えて）いる．

この 6 つの置換の集合に G_3 という名前を付ける．

$$G_3=\{\sigma_1,\ \sigma_2,\ \sigma_3,\ \sigma_4,\ \sigma_5,\ \sigma_6\}\quad(\sigma_1\text{は恒等置換}).$$

置換が 6 つあるのに G_3 と名付けるのは 3 個のものの置換という意味である．文字列は数字でなくても ABC でもアイウでもよい．3 つのものの置き換えや並べ替えを表現するのにこの G_3 が使える．

さて，この σ_1，…，σ_6 を使って，例えば $\sigma_2\sigma_3$ という「掛け算」を定義してみよう．

$\sigma_2\sigma_3$ とは，文字列 123 に対して，まず $\sigma_2=\begin{pmatrix}123\\132\end{pmatrix}$ を行ない，続けて $\sigma_3=\begin{pmatrix}123\\231\end{pmatrix}$ を行なうことを意味するものとするのである．すると，1 は σ_2 によって 1 のままだが，σ_3 によって 2 に置き換わっているから結局 1 は 2 に換わる．同様に 2 はまず σ_2 で 3 に，その 3 は次の σ_3 で 1 に換わっているから結局 2 は 1 に換わっている．最後に 3 は σ_2 で 2 に，その 2 は σ_3 で 3 に換わっている．よって 1→2，2→1，3→3 と置換されたからこれは上の $\sigma_4=\begin{pmatrix}123\\213\end{pmatrix}$ に当たる．よって，$\sigma_2\sigma_3=\sigma_4$ となる．

これらの置換を関数の一種と考えることもできる．例えば，定義域 {1，2，3} から値域 {1，2，3} への対応 σ_2 を，$\sigma_2(1)=1$，$\sigma_2(2)=3$，$\sigma_2(3)=2$ によって定義すれば，σ_2 は関数になる．また，1 に対して σ_2 を行ない，次に σ_3 を行なうことを $\sigma_2\sigma_3(1)$ と表わそう．これを使って置換の「掛け算」を言い換えてみると，

$\sigma_2(1)=1$，$\sigma_3(1)=2$　よって　$\sigma_2\sigma_3(1)=2$，
$\sigma_2(2)=3$，$\sigma_3(3)=1$　よって　$\sigma_2\sigma_3(2)=1$，
$\sigma_2(3)=2$，$\sigma_3(2)=3$　よって　$\sigma_2\sigma_3(3)=3$

となる．以上から $\sigma_2\sigma_3=\sigma_4$．

この置換の「掛け算」を先ほどの正三角形の移動に当てはめてみると，$\sigma_2\sigma_3$ とは，頂点 1 からの垂線による対称移動のあと，重心を中心とした正 120°の回転移動を行なうことを表わすから，1 の頂点は 2 へ，2 は 1 へ，3 はもとの位置に戻るから，結局頂点 3 からの垂線による対称移動を行なった結果と同じになるので σ_4 を 1 回行なったことになる．

こうして置換に「掛け算」を導入することができた．この演算によって G_3 に群を定義することができる．

群の定義とは次のような簡単なものである．

一般に，集合 **G** の元のあいだに，あるひとつの演算が定義されていて，次の３つの条件，

A：演算の成立とその一意性

B：演算の結合法則

C：逆演算が可能

が満たされるとき，**G** を群と呼ぶ．

（参考：「群論入門」稲葉榮次著より　培風館「新数学シリーズ 7」昭和 47 年）．

ガロア理論の持つ体系的な美しさにおいて，この群の持つ見た目の単純性と奥深さはその根拠となるものである．

この定義でいう「演算」とは今の場合でいえば置換の掛け算のことをいうのであるが，一般には「集合内の 2 つのものに同じ集合内の一つのものを対応させる決められた操作のこと」である．決められた操作に対して対応するものがあれば演算が成り立ち，ないときは成り立たないとする．いわゆる四則計算も実は 2 つの元の間に加法と乗法という二つの演算が定義されていて，減法･除法はそれぞれの「逆演算」と考えることができる群のように定義する演算をひとつにすることで，置換の集合などのように数以外の集合も対象とすることができるようになる．

群をなす集合の元の個数を群の位数という．位数が有限の群を有限群，無数の群を無限群という．有限群の例はこれから詳述する置換群を上げることができるが，無限群の身近な例としては，整数全体の集合 Z に加法を演算として定義したとき，Z は無限群になる．演算の一意性も結合法則も，逆演算も（もちろん減法）成り立つ．

G_3 が群の定義にあてはまることを確かめるには，置換 σ_1～σ_6 の積の「九九表」を作るのが便利である．いま示した置換の積 $\sigma_2\sigma_3=\sigma_4$ のような演算を σ_1 から σ_6 まですべてで行ない，その結果を表にする．

G_3	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_1	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_2	σ_2	σ_1	σ_4	σ_3	σ_6	σ_5
σ_3	σ_3	σ_5	σ_6	σ_2	σ_4	σ_1
σ_4	σ_4	σ_6	σ_5	σ_1	σ_3	σ_2
σ_5	σ_5	σ_3	σ_2	σ_6	σ_1	σ_4
σ_6	σ_6	σ_4	σ_1	σ_5	σ_2	σ_3

先に行なう置換 σ_2 を左端の列から選び，あとに行なう σ_3 を最上行から取って，その結果が置換 σ_4 を行な

ったのと同じであることを示している．表の他の部分も同じ意味を表わす．

この表から群の定義を考えてみよう．

まず，表で著しいのは σ_1 である．数の 1 のようにどの元に掛けてもその元を変えない．置換の場合には恒等置換を表わしていたが，一般の群では単位元と呼ばれる．任意の元 σ_n に対して，

$$\sigma_n\sigma_1 = \sigma_1\sigma_n = \sigma_n$$

が成り立つ．

次に，σ_1～σ_6 のどれとどれを掛けても積は σ_1～σ_6 のいずれかである．これが群の定義の「A：演算の成立」を示している．言い換えると演算が閉じている，そしてどの欄にも 1 個の答えしか入ってない．これが一意性である．ゆえにどの行または列にも σ_1～σ_6 が必ず 1 個ずつ現れている．同じ行または列に同じものが 2 個以上出てくることはない．

次に，群の定義　「C：逆演算が可能』というのを表から考えてみよう．

逆演算とは，例えば整数の掛け算で考えるとき，その逆演算は割り算ということになる．6 ÷ 2 は，3 という解が存在するので，この場合は逆演算が可能であるといえる．しかし，6 ÷ 4 だと整数としての解がないので，この場合は逆演算が可能ではない．つまり，逆演算がいつでも可能ではないので，整数の集合は掛け算の逆演算が可能ではないことになる．

しかし，この G_3 の積の表では，$\sigma_x\sigma_m=\sigma_n$ というとき，m や n が 1～6 のどれであっても表から σ_x が求められる．例えば，m=2，n=3 のときは $\sigma_x\sigma_2=\sigma_3$ となるから，群表で最上行の σ_2 を下へ降りて行くと σ_3 があるのでそこを左端までたどれば σ_5 すなわち σ_x が得られる．すなわち G_3 は置換の積について逆演算がいつでも可能である．

群における逆演算には特記すべき事柄がある．それは逆元である．群の任意の元 σ_n には，

$$\sigma_n\sigma_x=\sigma_1 \text{（=単位元）}$$

となる元 σ_x が必ずある．この σ_x を σ_n の逆元といい，σ_n^{-1} で表わす．

掛け算の結果が単位元になるとき，一方を他方の逆元といってもよい．それぞれの元の逆元を表から見てみよう．

$$\sigma_1^{-1}=\sigma_1,\quad \sigma_2^{-1}=\sigma_2,\quad ,\quad \sigma_6^{-1}=\sigma_3,\quad \sigma_4^{-1}=\sigma_4,\quad ,\quad \sigma_5^{-1}=\sigma_5,\quad ,\quad \sigma_3^{-1}=\sigma_6.$$

逆元を正三角形の置換で考えるとき，例えば σ_2 の逆元が σ_2 なのは，σ_2 は線対称移動を表しており、もう一度同じ線対称移動を行なうと正三角形が元に戻る，つまり恒等置換と同じになるからである．また σ_6 の逆元が σ_3 なのは σ_6 が 120°の回転を表わすのに対して，それを元に戻す（恒等置換にする）移動は 240°の回転（=σ_3）だからである．

群の定義の最後は，「B：演算の結合法則」であるが，これは次のことを表わしている．

$$(\sigma_l\sigma_m)\sigma_n=\sigma_l(\sigma_m\sigma_n)$$

この式の左辺は，まず σ_l と σ_m を掛け，その結果に σ_n を掛けている．そして右辺は，先に $\sigma_m\sigma_n$ を行なっておいて，それから σ_l とさっきの結果を掛けた結果を示している．それが同じになるというのが結合法則である．要するに，三つの置換の積を表わすときには，$\sigma_l\sigma_m\sigma_n$ のように括弧がいらないということである．もちろん σ_1～σ_6 のすべてにおいて三つ以上の場合にも成り立たなければならない．

ただ，置換の掛け算では注意すべきこととして，交換法則が（一般には）成り立たないということがある．例えば $\sigma_2\sigma_3$ と $\sigma_3\sigma_2$ とでは結果が異なる．

$$\sigma_2\sigma_3=\sigma_4,\quad \sigma_3\sigma_2=\sigma_5.$$

こうして，G_3 は「群」であることが確かめられた．上の群の九九表のことを群表という．

σ_1～σ_6 からなる集合 G_3 に置換の「掛け算」を定義した群をとくに **3 次対称群**という．この群の元は 6 個あるので，位数は 6 である．位数にはとくに記号はないが，一般に集合 A の元の個数を表わすのに，

$|A|$

という記号があるので，$|G_3|$=6 と表わすことがある．

群 G_3 の元で，σ_2= $\begin{pmatrix}123\\132\end{pmatrix}$ のように，1 は 1 のままで，2 と 3 だけが入れ換わっているときには単に(23)と表わすことにすると，σ_2=(23)．また，σ_4=(12)，σ_5=(13)となる．このように 2 つのものだけが入れ替わっている置換を特に互換という．

そして，σ_3= $\begin{pmatrix}123\\231\end{pmatrix}$ のように，1 は 2 に，2 は 3 に，そして 3 は 1 に戻る，というように一巡して入れ替わっているときには，σ_3=(123)と表わすことにする．σ_6= $\begin{pmatrix}123\\312\end{pmatrix}$ は，1→3→2→1 と巡回しているので σ_6 =(132)．このような置換を巡回置換と（循環置換とも）いう．括弧の中のものの個数を巡回置換の長さという．(132) は長さ 3 の巡回置換である．互換は長さ 2 のもっとも短い巡回置換である．巡回置換はどこから始めても同じなので，σ_3=(123)=(231)=(312)であるが，見極めやすいように小さい数から書くことにする．

この表現を使うと置換の積が求めやすくなる場合がある．例えば，

$\sigma_2\sigma_3$=(23)(123)

の場合には，1 は始めの置換では変わらない（かつこの中にないものは変わらない），次の置換では 2 になっているので，2 に，次の 2 は始めの置換で 3 に，次の置換で 1 に変わっているので，2 に続けて 1 と書き，21，　残っているのは 3 だけなので，213 となる．これは $\begin{pmatrix}123\\213\end{pmatrix}$ のことであるから，積は σ_4 =(12)となる．

別の例で，

$\sigma_3\,\sigma_4$=(123)(12)→132→(23)=σ_2

というような計算表記ができる．（注意：途中の 132 は(132)のことではなく，$\begin{pmatrix}123\\132\end{pmatrix}$ の上の行を省略して下の行のだけを書いたもの．）

また，σ_1 のような恒等置換は，誤解のない場合は $\mathbf{1}$ で表わすことがある．

G_3 を巡回置換の集合として表わすと，G_3={1,(12),(13),(23),(123),(132)}となる．

ガロア理論で最低限必要な群の知識としては対称群，部分群，共役部分群，正規部分群，交代群，巡回群，正規列，剰余群，そして可解群などである．これらはおのおの個別の群というよりは，ひとつの群の性質，あるいは群と群の関連を示すものといってよい．群はそれぞれ部分群を持ち，その部分群には互いに共役なものがある．また部分群のなかには正規部分群と呼ばれるものがある．それを用いて正規列が作られ，その剰余群を調べることで可解群となるものがある，…　そしてこの可解群こそがガロア理論の最初の精華である代数方程式の可解性の根拠となるのである．以下，順次説明しよう．

ある群の部分集合がまた群になっているとき，それを部分群という．例えば G_3 には群表からもわかる通り，

H_1= {σ_1，σ_2}

という部分群がある．なぜなら σ_1 と σ_2 だけで演算の閉じた群表が出来るからである．

H_1	σ_1	σ_2
σ_1	σ_1	σ_2
σ_2	σ_2	σ_1

同様に，

$$H_2=\{\sigma_1,\ \sigma_4\}\ ,\qquad H_3=\{\sigma_1,\ \sigma_5\}$$

も部分群である．これらは互いに兄弟のような部分群なので共役部分群という．しかし，σ_1とそれ以外の元1個からなるものがみなG_3の部分群というわけではない．例えば$\{\sigma_1,\ \sigma_3\}$は部分群ではない$\sigma_3\sigma_3=\sigma_6$となるので演算が閉じていない．$\{\sigma_1,\ \sigma_6\}$も同様に部分群ではない．

このことを，正三角形の置換で考えてみると，部分群$H_1=\{\sigma_1\sigma_2\}$のσ_2とは，(23)のことであったから，正三角形の頂点1から底辺23に引いた垂線を軸とする対称移動である．この移動は，もう一度行なうと元に戻る（$\sigma_2\sigma_2=\sigma_1$）．だから部分群になるのである．しかし$\sigma_3$=(123)は反時計回りの120°の回転移動であるから同じ移動をもう一度行っても240°の回転（=σ_6）になって元通りにはならないのである．

しかし，$\{\sigma_1,\ \sigma_3\}$にσ_6を加えれば部分群になる．これをA_3で表わそう．

$$A_3=\{\sigma_1,\ \sigma_3,\ \sigma_6\}$$

群表にすれは次のとおり．これらはこの3個の置換で演算が閉じている．

σ_1	σ_1	σ_3	σ_6
σ_1	σ_1	σ_3	σ_6
σ_3	σ_3	σ_6	σ_1
σ_6	σ_6	σ_1	σ_3

さらにこのA_3には他の部分群にはない大きな特徴がある．それは共役部分群がない，いいかえれば$\boldsymbol{A_3}$の共役部分群は$\boldsymbol{A_3}$だけ，ということである．そういう部分群をとくに正規部分群という．

他に，恒等置換（単位元）σ_1だけからなる群$\boldsymbol{E}=\{\sigma_1\}$や$G_3$自身も，$G_3$の部分群であるだけでなく，正規部分群でもある．$\boldsymbol{E}$や$G_3$を，あって当たり前という意味で自明な（正規）部分群という（$\boldsymbol{E}$は特に単位群ともいう）．

これらG_3の部分群の元の個数が，1個，2個，3個，6個というようにG_3の位数6の約数になっていることも大きな特徴である（これをラグランジュの定理という）．元の個数が4個や5個の部分群はG_3にはないのである．

もうひとつ，これら$H_1\sim H_3$とA_3の中では置換の積について交換法則が（たまたま）成り立っている．このように積の交換法則の成り立つ群をアーベル群（または可換群．「可解群」と混同しないように）と呼ぶ．G_3はアーベル群ではないが，その正規部分群A_3はアーベル群である．位数が2である群はもちろんすべてアーベル群である．

4．群と体

では，いよいよ体に群を適用することを考えよう．

体 Q や $Q(\sqrt{2})$ に群を適用するといっても，体の演算である四則のどれかを群の演算と看做そうというのではない．それはそれで興味のあることではあるが，われわれが扱う群は置換群である．それは体の置換である．

前に $Q(\sqrt{2})$ が正則拡大体であることを述べたが，これはこの体が２次方程式；

$$x^2-2=0 \qquad [12]$$

の２つの解 $x=\pm\sqrt{2}$ をともに含んでいるという意味であった．このことをもう少し詳しく述べる．

$Q(\sqrt{2})$ は Q に $\sqrt{2}$ を追加して作ったが，ここで Q に $-\sqrt{2}$ を追加して $Q(-\sqrt{2})$ を作ってみよう．これも体になることは容易にわかるが，集合としても， $Q(\sqrt{2})$ と同じものになるのだ．

$$Q(\sqrt{2}) \;=\; Q(-\sqrt{2}) \;.$$

このことを示す方法として， $Q(\sqrt{2})$ の各元 $a+b\sqrt{2}$ に対して， $Q(-\sqrt{2})$ の $a+b(-\sqrt{2})=a-b\sqrt{2}$ を対応させると，お互いのすべての元が１対１に対応するというのがある．どちらの任意の元にも相手側にただひとつ対応する元があるので，集合として同じものだといえるのだ．Q の元 $a,\,b$ はそれぞれまったく同じものに対応させているので，この対応を Q-同型対応という．

体における Q-同型対応が四則も対応しているときには「体の Q-同型対応」という．

前に $Q(\sqrt{2})$ が体であることを示した四則計算で， $a+b\sqrt{2}$ ， $c+d\sqrt{2}$ をそれぞれ $a-b\sqrt{2}$ ， $c-d\sqrt{2}$ に置き換えて計算してみれば，その結果は右辺の $A+B\sqrt{2}$ 等々の $\sqrt{2}$ を $-\sqrt{2}$ に替えただけのものになるのである．

こうして $Q(\sqrt{2})$ と $Q(-\sqrt{2})$ は，集合としてはまったく同じものであり，体としても元 $a+b\sqrt{2}$ に $a-b\sqrt{2}$ を対応させることにより，体としてもまったく同じ型をしていることがわかる．体における Q-同型対応が Q の元をまったく動かさずに，単に $\sqrt{2}$ に $-\sqrt{2}$ を対応させることで実現できることから，このことを Q に関して同値ということもある．

さらにこの２つの体は正則拡大体としての $Q(\sqrt{2})$ の部分体として考えることもできる（すべての Q の拡大体は自分自身と Q を部分体として持つ）ことから，こういう部分体を互いに共役体という．これは $\sqrt{2}$ と $-\sqrt{2}$ がどちらも同じ方程式[12]の解（共役な解）であるであることに拠っている．

同様に $Q(\sqrt{3})$ から $Q(-\sqrt{3})$ への Q-同型対応などが考えられる．しかし $Q(\sqrt{2})$ から $Q(\sqrt{3})$ への Q-同型対応はない．なぜならこの対応は和と差は対応するが，積･商が対応しないからである．積の場合では，以下のように Q-同型対応にはならない．

$$(a+b\sqrt{2})(c+d\sqrt{2})=(ac+2\mathrm{bd})+(ad+bc)\sqrt{2}$$
$$(a+b\sqrt{3})(c+d\sqrt{3})=(ac+3\mathrm{bd})+(ad+bc)\sqrt{3}\,.$$

Q-同型対応は，和には和，積には積が対応し，和と積が対応すれば，差や商も対応する．

さて，これから体に対して行なおうとする置換とは，正則拡大体の Q-自己同型対応のことである．$Q(\sqrt{2})$ と $Q(-\sqrt{2})$ をどちらも正則拡大体 $Q(\sqrt{2})$ の部分体として考えたとき，部分体 $Q(\sqrt{2})$ から部分体 $Q(-\sqrt{2})$ への Q-同型対応は，結局は正則拡大体 $Q(\sqrt{2})$ の自分自身の中の体の置換であり，<u>自分自身の中で</u> $Q(\sqrt{2})$ を $Q(-\sqrt{2})$ に対応させているのである．この対応を Q-自己同型対応という．これを正則拡大体における部分体の置換として表現するためには， $Q(\sqrt{2})$ と $Q(-\sqrt{2})$ を入れ替えると考えることにすればよい．同様の意味でもう一つ Q-自己同型対応がある．それは恒等置換で， $Q(\sqrt{2})$ には $Q(\sqrt{2})$ を， $Q(-\sqrt{2})$ には $Q(-\sqrt{2})$ を対応させる．恒等置換を σ_1， $Q(\sqrt{2})$ と $Q(-\sqrt{2})$ を入れ替える方を σ_2 とすれば，