

代数方程式の根の公式とガロア理論入門 (その2)

2026.7.11 鈴木 実

8 冪根拡大体列と可解列

本節では、まず二項方程式 (10) の最小分解体である拡大体が、連続して単拡大された 2 つの単純拡大体と等価であること、および、それぞれがガロア拡大であることを示す。次に、それぞれに対応するガロア群が巡回群になることを示す。さらに、それが 2 つの巡回群の直積になることを示す。このことは、代数方程式が代数的に解けるための必要十分条件を明らかにすることと密接に関係する。すなわち、本節では最終的にガロア群が巡回群の直積になることが代数方程式が可解であることと等価であることが示される。

前節 7.7 において、二項拡大体のガロア群 G において、その正規部分群 H と H に関する剰余群 G/H が巡回群であることを示した。多項式の根が冪根と四則演算で表されることと、二項拡大体に根が含まれることは必要十分の関係にある。したがって、二項拡大体のガロア群が巡回群であることが、多項式の根が冪根と四則演算で表されることと同等であることが示されれば、ガロア群が可解性と密接な関係を有することがわかる。このように、ガロア群が巡回群になるか否かということは極めて重要な可解性の判断条件になるのである。しかし、この関係を明解にするには、二項拡大体から冪根拡大体に視点を変える必要があることを示す。以下では、まず二項拡大体のガロア群が巡回群になることから見てみよう。

8.1 二項拡大体のガロア群とその部分群

二項拡大体がガロア拡大であり、そのガロア群と正規部分群を見てきた。ここでは、二項拡大体のガロア群全体をもう一度詳しく調べる。これは、この後述べる冪根拡大体がより重要になることを明らかにするために必要である。

8.1.1 二項拡大体のガロア群は巡回群か

二項拡大体のガロア群 G の正規部分群 H と剰余群 G/H が巡回群であることは前節で示した。一方、もとの群 G が巡回群であるか否かは明らかではない。先に結果を言えば、 G は巡回群ではない。もし、巡回群であれば以下で述べるような細かい検討を省略してそのまま可解性の問題に取り組むことができるが、そのようにはならない。

まず、群 G が巡回群にならないことを示そう。 G の元を一般に $[a, b]$ とすると、式 (44) により、

$$\begin{aligned} [a, b]^2 &= [a^2, b(1+a)] \\ [a, b]^3 &= [a^3, b(1+a+a^2)] \\ &\vdots \\ [a, b]^i &= [a^i, b(1+a+a^2+\cdots+a^{i-1})] \end{aligned} \tag{65}$$

となる。 n が素数で法 n のもとで、 a が n と互いに素で乗法群 $Z_n^\times$ (n を法とする整数の剰余類から 0 を除いた乗法群) の原始元であるとする。そのとき、 $a^{n-1} = 1$ である。整数 i を 2 つの整数変数 m と l で表すことにし、

$i = m(n-1) + l$ とおき, $m = 0, \dots, n-1, l = 1, \dots, n-1$ とすると, $i = 1, \dots, n(n-1)$ となる. $a^{n-1} = 1$ に注意すると, 式 (65) は

$$\begin{aligned}
[a, b]^i &= [a^{m(n-1)}, b(1 + a + \dots + a^{m(n-1)-1})] \\
&= [a^{m(n-1)+l}, b\{(1 + a + \dots + a^{n-2}) + a^{n-1}(1 + a + \dots + a^{n-2}) \\
&\quad + a^{2(n-1)}(1 + a + \dots + a^{n-2}) \dots + a^{(m-1)(n-1)}(1 + a + \dots + a^{n-2}) \\
&\quad + a^{m(n-1)}(1 + a + \dots + a^{l-1})\}] \\
&= [a^l, b\{m(1 + a + \dots + a^{n-2}) + (1 + a + \dots + a^{l-1})\}] \\
&= [a^l, b(ms + r)]
\end{aligned} \tag{66}$$

となる. ここで,

$$1 + a + \dots + a^{n-2} = s, \tag{67}$$

$$1 + a + \dots + a^{l-1} = r \tag{68}$$

とおいた. s と r は整数定数である.

$a \neq 1$ のとき, $s = (1 - a^{n-1})/(1 - a)$ であるから, $a^{n-1} = 1$ より $s = 0$ である. したがって, $a \neq 1$ のとき式 (66) は,

$$[a, b]^i = [a^l, -br] \tag{69}$$

となる. 右辺の式は変数 l の値で決定されるから, いかなる a または b の値にかかわらず, 異なる値の種類は l を超えないことがわかる. すなわち, $[a, b]$ の位数は G の位数 $n(n-1)$ より小さい. したがって, いかなる a または b に対しても $[a, b]$ は原始根にはならない.

一方, $a = 1$ のときは, $s = n - 1 = -1 \pmod{n}$ および $r = l$ であるから, 式 (66) は,

$$[a, b]^i = [1, b(-m + l)] \tag{70}$$

となる. この式の右辺の異なる値は法 n のもとで $n - 1$ 種類を超えない. したがって, $[a, b]$ の位数は G の位数 $n(n-1)$ より小さいから, 上と同様に G の原始根にはならない. ゆえに, G には原始根が存在しないから巡回群ではない.

8.1.2 二項拡大体のガロア群の部分群は巡回群か

第 7.2 節と第 7.3 節で, ガロア群 G の部分群には $[1, b]$ を元とする部分群 H があることを示した. また, H は正規部分群であることも示した. H の位数は n である.

G の部分群には H 以外に $[a, 0]$ を元とする部分群がある. これは,

$$\begin{aligned}
[a, 0][b, 0] &= [ab, 0] \\
([a, 0])^{-1} &= [\bar{a}, 0]
\end{aligned} \tag{71}$$

となることから示される. この部分群を F とする. G の任意の元を $[a, b]$, F の任意の元を $[c, 0]$ とすると,

$$\begin{aligned}
[a, b][c, 0]([a, b])^{-1} &= [a, b][c, 0][\bar{a}, -\bar{a}b] = [a, b][[c\bar{a}, -\bar{a}bc]] \\
&= [c, -bc + b]
\end{aligned}$$

となり, これは F に含まれないから F は正規部分群ではない.

さて、部分群 H と F は巡回群であるだろうか．まず、 H から調べてみよう． H の位数は、 b のとり得る値 $(0, 1, \dots, n-1)$ の個数 n と一致する． H の任意の元 $\xi = [1, b]$ ($0 \leq b \leq n-1$) を取り上げる． $i = 1, \dots, n$ とすると、明らかに、

$$\xi^i = ([1, b])^i = [1, ib] \quad (72)$$

であるから、たとえば、 $b = 1$ なら $i = n$ で $\xi^n = [1, 0]$ となり、 ξ の位数が n となり、 H の位数 n と等しいので $[1, 1]$ は原始根である．したがって、 H は巡回群であることがわかる． n が素数であるとしているので、 $b = 1, \dots, n-1$ の場合にも同様に原始根となる．なお、 H は n を法とする整数の剰余類 Z_n の加群と同型である．

F の場合を考えてみよう． F の元を $\eta = [a, 0]$, ($a = 1, \dots, n-1$) とすると、明らかに、

$$\eta^i = [a^i, 0] \quad (73)$$

である．これは、この部分群 F が n を法とする整数の剰余群 $Z_n^\times$ あるいは $(Z/nZ)^\times$ と同型であることを示す． $(Z/nZ)^\times$ は位数 $n-1$ の巡回群である． F の位数も a のとり得る値の個数から $n-1$ である．したがって、 F は巡回群である． a を F の生成元とすると、 a^k が F の生成元になるのは、 k と $n-1$ が互いに素な場合である．なぜなら、 $i = 2, \dots, n-1$ のすべての i に対して、 $(a^k)^i$ が a^k と異なるのは k と $n-1$ が互いに素な場合に限られるからである．すなわち、位数 $n-1$ の巡回群では、 $\varphi(m)$ を m 以下の m と互いに素な正の整数の個数を表すオイラーの関数とすると、 $\varphi(n-1)$ 個の原始根をもつ．たとえば、 $n = 13$ とすると、 $\varphi(12) = 4$ で $2, 5, 7, 11$ が原始根である．

巡回群 F では、位数 $n-1$ の約数の個数だけ部分群をもつ (ラグランジュの定理の逆が成り立つ)．なぜなら、 d を $n-1$ の約数、 $dd' = n-1$ として、生成元 a に対して、 $a^{d'}$ は位数 d の巡回群 $\langle a^{d'} \rangle$ になるからである．

以上のように、群 G の部分群 H と F はいずれも巡回群となることがわかった．しかしながら、もとの G は巡回群ではない．これは二項拡大体のガロア群の 2 つの自己準同型 $[1, b]$ と $[a, 0]$ が始域と終域において $\theta\gamma^i$ を共有し互いに干渉するからである．また、 $[1, b]$ と $[a, 0]$ が可換ではないということにも関係がある．しかし、このことがガロア拡大あるいはガロア群と可解性に関係付ける特徴を見出す上で最も邪魔になるのである．このことは連続して二項拡大を施したときに起こることによってここに問題がある．そのことについて次節以降で明らかにする．

以上が二項拡大体のガロア群の構造であるが、可解性を定義する明確な特徴をここから引き出すためにはまだ少し複雑である．以下の節ではもう少し簡単な構造にする手法について述べる．

8.2 二項拡大体と冪根拡大体

本節では代数的生成拡大体で表される二項拡大体 $P(\theta, \gamma)$ を代数的組成拡大体 $P(\theta)(\gamma)$ または $P(\gamma)(\theta)$ として段階的に拡大した場合を考えてみる．

8.2.1 二項拡大体の組成拡大体化

二項拡大体 G が持つ 2 つの部分群 F (元は $[a, 0]$) と H (元は $[1, b]$) が群 G の任意の元 $[a, b]$ に対して相補的であるように見えてところから、群 G がこの 2 つの部分群の直積になるように思われる．しかし、実際には群 G はこのような直積では表されない．実際、 G の元 $[a, b]$ と $[c, d]$ の間の演算が式 (44) の $[a, b][c, d] = [ac, ad + b]$ という関係式で表されるように、 a と c または b と d の間で閉じていないからである．閉じていないのは、二項方程式の根が式 (24) の $\theta\gamma^i$ で表され、二項拡大体が 6.3.1 節のように $P(\theta, \gamma)$ であるところから来ている．もし、これが

$$P(\theta, \gamma) = P(\theta)(\gamma) = P(\gamma)(\theta) \quad (74)$$

という関係に着目すれば、2つの連続した単純拡大と等価であるから、ガロア群 G がそれぞれの単純拡大のガロア群の直積として表されるようにならないのだろうか、と考えるのが興味深い方向であろう。これを以下にみてみよう。

基礎体 P に γ を追加して得られる拡大体 $P(\gamma)$ を K_1 、同様に、 K_1 に θ を追加して得られる拡大体 $K_1(\theta) = P(\gamma)(\theta)$ を L_1 とする。すなわち、

$$\begin{aligned} K_1 &= P(\gamma) \\ L_1 &= K_1(\theta) = P(\gamma)(\theta) = P(\theta, \gamma) \end{aligned}$$

である。二項方程式 $x^n - 1 = 0$ の 1 とは異なる根を γ とする。他の根であっても構わないことは、 n が素数であることを前提としていることから導かれる。 γ を P に追加すれば γ の冪乗はすべて $K_1 = P(\gamma)$ に含まれることになるので、 $x^n - 1$ の根 $1, \gamma, \gamma^2, \dots, \gamma^{n-1}$ はすべて K_1 に含まれる。 $x^n - 1 = (x - 1)(x^{n-1} + \dots + x + 1)$ であるから、 $x^{n-1} + \dots + x + 1$ が γ の最小多項式であり、重根はなく、その根がすべて K_1 に含まれるから K_1 は P のガロア拡大である。

P の元を不変にする K_1 から K_1 への自己同型（環準同型全単射）は $1, \gamma, \gamma^2, \dots, \gamma^{n-1}$ から同じ集合への単射に含まれる。その中で準同型を満たす単射 σ は第 6.3 節の式 (29), (30) で表される同型写像で、それ以外の全単射は準同型条件を満足しない ($[1, b]$ という全単射は $1, \gamma, \dots, \gamma^{n-1}$ に対しては単なる恒等写像である)。すなわち、式 (29), (30) の $\sigma[a]$ を二項拡大体の場合と同様な $[a, 0]$ という表し方をすると、

$$\sigma[a]\gamma_i = [a, 0]\gamma_i = [a, 0]\gamma^i = \gamma^{ai} \quad (75)$$

と表される。ここで、 $a = 1, 2, \dots, n-1$ である。この $\sigma[a]$ の集合は位数 $n-1$ の群を形成する。この群はガロア拡大に対応するガロア群である。上の式は $\sigma[a]$ と $[a, 0]$ が 1 対 1 対応しており、このガロア群は群 G の部分群 F ($[a, 0] \in F$) と同型であることがわかる。また、群 G の正規部分群 H に関する剰余群 G/H は、 a で指定される類 $\{[a, i]\}$ ($i = 0, 1, \dots, n-1$) であるから、このガロア群は剰余群 G/H と同型であることがわかる。

次に、体 K_1 に θ を追加して L を生成する単純拡大について考えてみよう。 θ の最小多項式は $x^n - \alpha$ であり、その根は $\theta, \theta\gamma, \theta\gamma^2, \dots, \theta\gamma^{n-1}$ である。 γ^i ($i = 1, \dots, n-1$) はすでに体 K_1 に含まれているので、 L には θ の最小多項式の根がすべて含まれている。さらに、これらの根は重根ではない。したがって、 L は K_1 の上のガロア拡大体である。

次に、 K_1 を不変体とする L の自己準同型写像を考える。 K_1 から L への拡大の生成元は θ であるから、その自己準同型は、 $x^n - \alpha$ の根の間の置換に含まれ、その中で準同型条件を満たす全単射は式 (31), (32) の $\tau[b]$ であり、 $[1, b]$ という表し方をして、

$$\tau[b]\theta\gamma^i = [1, b]\theta\gamma^i = \theta\gamma^b\gamma^i \quad (76)$$

となる関係のみである。ここで、 $b = 0, 1, \dots, n-1$ である。この $\tau[b]$ の集合は位数 n の群を形成し、 K_1 の上のガロア拡大体 K に対応するガロア群である。この式の演算関係から、このガロア群は群 G の正規部分群 H と同型であることは明らかである。したがって、このガロア群は巡回群である。ここで、巡回群であることを強調しておこう。これが、この後で述べるように、可解性と密接に関係するようにできる。

P の上の単純拡大体として考えられるもう一つの拡大体は $P(\theta)$ である。この拡大体は $x^n - \alpha$ の分解体にはなっていない。なぜなら、 γ が P に含まれていないので、 $x^n - \alpha$ の根のうち $P(\theta)$ には $\theta\gamma^0$ しか含まれていないからである。したがって、 $P(\theta)$ はガロア拡大ではない。この点が $P(\gamma)$ の上の拡大と異なる点である。

これまでは二項拡大を 1 回操作した場合を述べてきた。しかし、多項式の根を冪根と有理演算操作で表すためには、この二項拡大を複数回操作する必要がある。そこで、以下ではそのような場合のガロア拡大とガロア群について述べる。

8.2.2 二項拡大体の上の二項拡大体と冪根拡大体

上で述べた基礎体 P の上の二項拡大体を L とした． L は P の上の代数的組成拡大体 $P(\gamma)(\theta)$ でもある．以下では， L_1 の上の同様な二項拡大体について考えてみよう．その二項拡大を L_2 とする．2 つの二項拡大体の生成元を区別するために P の上の K の生成元を θ_1 と γ_1 ， L_1 の上の L の生成元を θ_2 と γ_2 とする．この L_2 を代数的組成拡大体 $L_1(\theta_2, \gamma_2) = L_1(\gamma_2)(\theta_2)$ とするとき， L_1 の上の代数的単純拡大体 $L_1(\gamma_2)$ を K_2 とする．すなわち，

$$K_1 = P(\gamma_1) \quad (77)$$

$$L_1 = K_1(\theta_1) = P(\gamma_1)(\theta_1) = P(\theta_1, \gamma_1) \quad (78)$$

$$K_2 = L_1(\gamma_2) \quad (79)$$

$$L_2 = K_2(\theta_2) = L_1(\gamma_2)(\theta_2) = L_1(\theta_2, \gamma_2) \quad (80)$$

である．前節と同様の理由によって， K_2 は L_1 のガロア拡大， L_2 は K_2 のガロア拡大であり，かつ， L_1 のガロア拡大である．したがって，それぞれのガロア拡大体の自己準同型はガロア群を形成する．これを次のように表す．ただし， $H = \text{Gal}(L/K)$ はガロア拡大体 L/K において K を固定体 (不変体) とする L の自己準同型のガロア群を H とするという意味である．すなわち，上のガロア拡大体について，

$$H_1 = \text{Gal}(L_1/P) \quad (81)$$

$$F_1 = \text{Gal}(K_1/P) \quad (82)$$

$$E_1 = \text{Gal}(L_1/K_1) \quad (83)$$

$$H_2 = \text{Gal}(L_2/L_1) \quad (84)$$

$$F_2 = \text{Gal}(K_2/L_1) \quad (85)$$

$$E_2 = \text{Gal}(L_2/K_2) \quad (86)$$

のように中間体によりこれだけのガロア群が存在する． E_1 と F_1 は H_1 の部分群であり， E_2 と F_2 は H_2 の部分群である．前者は， $L_1 \supset K_1$ および， $K_1 \supset P$ から明らかである．後者についても， $L_2 \supset K_2$ および， $K_2 \supset L_1$ から明らかである．

F_1 はガロア群であり，前節で述べた $[a, 0]$ を元とする部分群 F と同型であり，かつ巡回群である．一方， H_1 は前節のガロア群 G と同じであり， $[a, b]$ の群と同型で，非巡回群である． E_1 は前節の K_1 を不変体とする L の自己同型群と同一であって， $[1, b]$ の群と同型であり，巡回群である．

同じく，群 F_2 ， H_2 ， E_2 に関しても，上の場合と同様で， L_1 ， L_2 ， K_2 を P ， L_1 ， K_1 に置き換えた場合に等しく， F_2 ， E_2 は H_2 の部分群であり， H_2 は非巡回群であり， F_2 と E_2 は巡回群である．ただし，ここでは $\gamma_1 \neq \gamma_2$ および $\theta_1 \neq \theta_2$ であるとした．

基礎体 P から連続した二項拡大体 L_1 と L_2 において，それぞれのガロア拡大に対応するガロア群は巡回群にはならない．連続した二項拡大体の列が多項式の根を含むか否かの判断をする上で，そのガロア群が何かの特徴を持つことが望ましい．しかし，このままでは特別な特徴は見いだせない．一方，二項拡大体を代数的組成拡大体にすればガロア群の部分群が巡回群になる．この点に着目すれば一つの解決策が得られることになる．それが明確に現れるのが 2 つの二項拡大体における二項方程式の次数が同じ場合である．以下にそれを見てみよう．

二項拡大体 L_1/P の二項方程式が $x^2 - \alpha_1 = 0$ とし，二項拡大体 L_2/L_1 の二項方程式が $x^2 - \alpha_2 = 0$ であって，2 つの方程式の次数が等しく n である場合を考える．このとき，ガロア拡大の L_1/P ， K_1/P ，および L_1/K_1 はそのまま変わらない．一方， L_1 からの二項拡大においては， $\gamma_2 = \gamma_1$ はすでに L_1 に含まれているので， $L_2 = L_1(\theta_2)$ となり， L_2 は単なる L_1 の冪根拡大体になる．これは， $\gamma_1 \neq \gamma_2$ のときの K_2 から L_2 へのガ

ロア拡大と同型であり、そのガロア群は E_2 であった．しかも、 E_2 は巡回群である．つまり、二項拡大を冪根拡大にすることにより、ガロア群は巡回群になるということである．それは、原始 n 乗根を拡大される体に予め含めればできるということである．

連続した二項拡大における生成元の θ_i ($i = 1, 2$)、は拡大する直前の体の元の関数になる可能性があるが、同じ生成元である γ_i ($i = 1, 2$) は拡大される体の元には関係なく、もともとの基礎体に含まれる整数にのみに依存して得られる原始 n 乗根であるから、もともとの基礎体 P に含めておくことが可能である．むしろ、そうすることにより、ガロア拡大としての体の構造とガロア群の構造が単純になり、かつ巡回群としての特徴が一律に備わることがわかる．つまり、有限の大きさの整数 n について、原始 n 乗根を基礎体に含め、連続して冪根拡大の系列を生成することにより、連続した二項拡大と同じ体の系列を生成することができるのである．しかも、その系列のガロア拡大のガロア群は巡回群になるという重要な特徴も得られることになる．つまり、ガロア拡大は巡回拡大になり、巡回拡大の系列を作成して、それが多項式の根を含むか否かの判断の基準にすればよいということになるのである．

多項式の根が代数的に表されるということは、有理数体に二項拡大を連鎖的に続けて施した拡大体とその根を含んでいることと等価であるが、このときの二項拡大は上で述べたように、冪根拡大と原始冪乗根による拡大に分解することができる．何回目かの二項拡大において、原始冪乗根による拡大のところで、すでにその冪乗根がそれまでの拡大体に含まれている場合もあり得る．そのときの二項拡大体は実質上単なる冪根拡大体に他ならない．しかも、そのときの冪根の字数は素数 n であって、二項拡大によって生成される元ではなく、基礎体 P にもともと含まれている元である．このようなことを考えれば、十分大きな整数 n までの整数のすべての原始冪根を基礎体 P に含めておけばこれまで着目していた二項拡大の連鎖は単純に冪根拡大の連鎖に置き換えることができる．つまり、拡大体の連鎖はすべて冪根拡大になり、そのガロア群は位数 n のガロア群となる．このように原始冪乗根を基礎体に含めることにより、二項拡大の連鎖の意味は変わることなく冪根拡大の連鎖に置き換えることができるようになる．

このように、原始 n 乗根 γ が基礎体 P に含まれている場合の n 次冪根拡大体を扱うことにより、冪根拡大体の系列の各ガロア拡大に対応するガロア群の構造が単純になり、かつこのガロア群は巡回群となる．冪根拡大体の系列を含む拡大体が多項式の根を含めば、その根もいずれかの冪根拡大体に含まれることになり、その冪根拡大体に対応するガロア群が巡回群となることがわかる．すなわち、多項式の根よりなるガロア拡大体のガロア群が巡回群に含まれることが重要な基準になることがわかる．

以上のように、二項拡大の列を取り扱うよりも冪根拡大の列を扱うほうがより直接的であり重要であることがわかった．次節以降では、拡大体の系列を冪根拡大体に移して多項式の根の解法を取り扱う．

8.2.3 冪根拡大体のガロア群が巡回群の直積になること

前節では、二項拡大を連続して施した 2 つの二項拡大体を取り上げた．その上で、二項拡大体の生成元の中から n 次原始根を基礎体 P に含めることで、2 つの連続した冪根拡大体の列となり、対応するガロア群が巡回群になるという特徴的な構造をもつことが明らかになった．以下では、これをさらに多くの冪根拡大体の系列について考えてみよう．

基礎体 P を L_0 とし、その上の冪根拡大を L_1 とし、以下 $i = 1, \dots, l$ として、 L_{i-1} の上の冪根拡大体を L_i とし、最後の冪根拡大体を $L_l = K$ とする．そうすると、

$$P = L_0 \subset L_1 \subset L_2 \subset \dots \subset L_{i-1} \subset L_i \subset \dots \subset L_l = K \quad (87)$$

である．各ガロア拡大 L_i/L_{i-1} に対応するガロア群を $H_i = \text{Gal}(L_i/L_{i-1})$ とする． H_i は巡回群であり、 H_i の間に包含関係はない．

ここで、 $P(=L_0)$ を不変体 (固定体) とする L_1 から L_1 への P の上の自己同型写像を考えてみよう．これらの写像の始域と終域は本来 L_1 であるが、 P の元はこれらの写像に関して不変であるから、これらの写像の始域と終域を、 L_1 から P の元を差し引いた集合 (差集合) に制限しても、これらの写像は P を除いてこの差集合の中に閉じているので、個々の写像はこの制限によって変わらない．また L_1 以外の他の同型写像に対しても独立である．したがって、このような不変体の上の自己同型写像に関しては差集合に制限された写像ともとの写像は、もともと不変体の領域が始域から除かれたのみで、同一の写像とみなすことができる．以下では、式 (87) の拡大体の系列において、このような自己同型写像の差集合への制限を考える．なぜこのような始域の制限を考えるのかというと、この後で述べるガロア群の直積に関して、その定義を明確にするためである． L_1 から P を差し引いた差集合を $L_1 \setminus P$ と表すことにする．他の場合も同様とする．

ガロア拡大 L_i/L_{i-1} において、 L_{i-1} を不変体とする L_i の自己同型写像において、その写像の始域を差集合 $L_i \setminus L_{i-1}$ に制限した写像を考える．この写像は、 $x^{n_i} - \alpha_i$ の共役根の集合である

$$Q = \{\theta_i, \theta_i \gamma_i, \theta_i \gamma_i^2, \dots, \theta_i \gamma_i^{n_i-1}\} \quad (88)$$

の元を $[1, b]\theta_i = \theta_i \gamma_i^b$ という変換により、同じ集合 Q の別の元に変換する全単射である．ただし、 n_i を整数とし、 θ_i は α_i の n_i 次冪根、 γ_i は n_i 次原始根とする．この変換は $\theta_i \gamma_i^j$ を $\theta_i \gamma_i^{j+b}$ に移す変換であり、 $b = 0$ の $[1, 0]$ は恒等変換である． $[1, -b]\theta_i = \theta_i \gamma_i^{-b}$ で表される逆変換も可能であるから、写像は単射であり、自己同型の数は変換の種類と一致する．このことから、この写像によって生成元の集合は全体として変わらず、この変換によって決まる写像の終域は拡大体の生成元と不変体の元の間のあらゆる四則演算の結果と同じになるから、始域と同じ $L_i \setminus L_{i-1}$ である．

この変換で定義される写像を ϕ とすると、この ϕ において、差集合 $L_i \setminus L_{i-1}$ 以外の L_i の元は変化しない．さらに、 $L_i \setminus L_{i-1}$ の元を p とすると、 $q = \phi(p)$ は $L_i \setminus L_{i-1}$ に含まれなければならない．なぜなら、 ϕ は準同型写像であるから、もし、最小多項式の根 $\theta_i \gamma_i^j$ が $L_i \setminus L_{i-1}$ の中の式 88 以外の元になれば最小多項式の根ではなくなるからである．別の表現をすれば、 ϕ は最小多項式の根の間の置換であるから、写像の終域は最小多項式の根が含まれている $L_i \setminus L_{i-1}$ に含まれるからである．このように、 L_{i-1} の上の L_i の自己同型は、始域を $L_i \setminus L_{i-1}$ に制限されることにより、 $L_i \setminus L_{i-1}$ に閉じており、他の L_j ($j \neq i$) の元とは独立である．つまり、 $\phi(L_i \setminus L_{i-1}) = L_i \setminus L_{i-1}$ である．

このように、始域を $L_i \setminus L_{i-1}$ に制限した自己同型が $L_i \setminus L_{i-1}$ のみに閉じているということは $L_l \setminus P$ のすべての範囲における他の L_j についても成り立つ．この制限された自己同型は明らかに L_{i-1} の上の L_i の自己同型、すなわち、ガロア群 $H_i = \text{Gal}(L_i/L_{i-1})$ と始域が $L_i \setminus L_{i-1}$ に制限されたことを除いて同一である． H_i の定義域のうち L_{i-1} の部分に関しては H_i の自己同型は恒等写像である．そこで、以下の直積に関する議論においては、 H_i の定義域を $L_i \setminus L_{i-1}$ に制限することにする．そうすると、 L_i の自己同型が他の L_j ($j \neq i$) と独立であることから、 $L_l = K$ を P の上のガロア拡大としたとき、ガロア群 $G = \text{Gal}(L_l/P) = \text{Gal}(K/P)$ は次のように H_i ($i = 1, \dots, l$) の直積として表すことができるのである．

$$G = H_1 \times H_2 \times \dots \times H_i \times \dots \times H_{l-1} \times H_l \quad (89)$$

これを G の部分群と次のように対応させることができる． G の部分群の中で G に次いで大きな部分群 G_1 は L_1 を不変体とするガロア群であるが、それは式 (89) の直積の中で H_1 を H_1 の単位元 e_1 に固定すればよい．すなわち

$$G_1 = e_1 \times H_2 \times \dots \times H_i \times \dots \times H_{l-1} \times H_l \quad (90)$$

となる．同じく G の部分群である、 L_1 を不変体とするガロア群 G_2 についても同様で、

$$G_2 = e_1 \times e_2 \times H_3 \times \dots \times H_i \times \dots \times H_{l-1} \times H_l \quad (91)$$

となる．ここで， e_2 は H_2 の単位元である．以下同様に， e_i は H_i の単位元とすると，

$$G_{i-1} = e_1 \times e_2 \times \cdots \times e_{i-1} \times H_i \times H_{i+1} \times \cdots \times H_{l-1} \times H_l \quad (92)$$

$$G_i = e_1 \times e_2 \times \cdots \times e_{i-1} \times e_i \times H_{i+1} \times \cdots \times H_{l-1} \times H_l \quad (93)$$

となり，最後は，

$$G_{l-1} = e_1 \times e_2 \times \cdots \times e_i \times \cdots \times e_{l-1} \times H_l$$

および，

$$G_l = e_1 \times e_2 \times \cdots \times e_i \times \cdots \times e_{l-1} \times e_l \quad (94)$$

となる．したがって， $G_l = \{e\}$ である． K 自身も K の拡大とみなすことができるので，このガロア群は $L_l = K$ の上の拡大 K の場合である．このように，冪根拡大体の列からガロア群の列を作れば，全体のガロア群とその部分群は冪根拡大体のガロア群列の直積として表されることがわかる．以上の式から明らかに，

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_{i-1} \supset G_i \supset \cdots \supset G_l = \{e\} \quad (95)$$

という包含関係が成り立つことがわかる．

8.2.4 ガロア群の剰余群が冪根拡大体のガロア群の直積成分と同値であること

7.6 節，7.7 節で，ガロア群と部分群の間で，剰余群が定義されることをすでに述べた．ここでは，ガロア群の部分群の系列の中で隣り合う G_{i-1} と G_i の間の剰余群が同様に定義されることを示す． $G_{i-1} \supset G_i$ であるから，剰余群は G_{i-1} の G_i に関する剰余群 G_{i-1}/G_i になる．これを式 (92)，(93) の直積表現でみると，

$$G_{i-1}/G_i \cong e_1 \times e_2 \times \cdots \times e_{i-1} \times H_i \times e_{i+1} \times \cdots \times e_{l-1} \times e_l$$

となることがわかる．明らかに，式 (93) の G_i は G_{i-1} の類を表しており，異なる類の個数はガロア群 H_i の位数である．より直接的に表せば，

$$G_{i-1}/G_i \cong H_i$$

となる．すなわち，冪根拡大体の列におけるガロア群は巡回群であり，ガロア部分群の剰余群と同値である．

8.2.5 冪根拡大体のガロア群の任意の部分群が正規部分群であること

式 (89) のガロア群 G の部分群は H_i の任意の組み合わせを取り上げ，残りを単位元 e_j にすることで表すことができる．正規部分群となる理由は，複数の H_i からなる部分群においても同様であるから，ここでは 1 個の H_i が正規部分群になる場合を示す．部分群 G_i が次のように表されることは明らかである．

$$G_i = e_1 \times e_2 \times \cdots \times e_{i-1} \times H_i \times e_{i+1} \times \cdots \times e_l$$

ここで， G_i と G のそれぞれの任意の元 a と c を次のように表す．

$$a = e_1 \times e_2 \times \cdots \times e_{i-1} \times a_i \times e_{i+1} \times \cdots \times e_l$$

$$c = c_1 \times c_2 \times \cdots \times c_{i-1} \times c_i \times c_{i+1} \times \cdots \times c_l$$

$$c^{-1} = c_1^{-1} \times c_2^{-1} \times \cdots \times c_{i-1}^{-1} \times c_i^{-1} \times c_{i+1}^{-1} \times \cdots \times c_l^{-1}$$

そうすると，

$$\begin{aligned} c^{-1}ac &= c_1^{-1}e_1c_1 \times c_2^{-1}e_2c_2 \times \cdots \times c_{i-1}^{-1}e_{i-1}c_{i-1} \times c_i^{-1}a_ic_i \times c_{i+1}^{-1}e_{i+1}c_{i+1} \times \cdots \times c_l^{-1}e_lc_l \\ &= e_1 \times e_2 \times \cdots \times e_{i-1} \times c_i^{-1}a_ic_i \times e_{i+1} \times \cdots \times e_l \end{aligned}$$

となる． $c_i^{-1}a_i c_i$ は H_i の元であるから， $c^{-1}ac$ は G_i の元である．すなわち， G_i は正規部分群である．これから明らかに， H_i のどのような組み合わせの部分群であっても，同様にして正規部分群であることを示すことができる．

8.2.6 可解群であることの代数的な定義

以上のガロア拡大およびガロア群の包含関係を基礎として多項式の根が有理演算で解くことができること，すなわち，可解性について重要な結論を導くことができる．これを以下に示す．

多項式の根が冪根拡大体列の中に含まれているとしよう．そのとき，多項式の最小分解体はガロア拡大体で，その拡大体が冪根拡大体列に含まれることになる．この最小分解体のガロア群は，上の冪根拡大体列とガロア群部分群列の関係から，いずれかのガロア群部分群に含まれていなければならない．すなわち，多項式の根が冪根と有理演算で解けるなら，その根をもつ多項式の最小分解体のガロア群が冪根拡大体列のガロア群の部分群でなければならない．これから多項式が可解であるということは，その最小分解体であるガロア拡大体が冪根拡大体列の中に含まれるということである．これをガロア群の面から見ると，多項式の最小分解体のガロア群が冪根拡大体列のガロア群の部分群列の中に含まれるということになる．冪根拡大体列のガロア群部分群列の特徴は，各部分群の包含関係で隣り合う部分群に関する剰余群が巡回群であることである．これは，式 (89) における H_i が巡回群あることから明らかである．したがって，多項式の根が可解であるということは，多項式の最小分解体に関するガロア群の部分群列において，包含関係で隣り合う部分群が巡回群であるということになる．これが可解であるということの代数的な定義になる．

8.2.7 ガロア群の剰余群が巡回群なら冪根拡大体に対応すること / ヒルベルトの定理 90

多項式の根が可解であるということは，根が冪根拡大体列の中に含まれていることであり，その多項式を最小分解体とするガロア群の部分群の系列における剰余群が巡回群であることであり，そして，このような特徴をもつガロア群は可解であるという．すなわちガロア群が可解であることが意義付けされた．では，ガロア群における剰余群の部分群が巡回群なら，それに対応する中間体が冪根拡大体になっているのだろうか．これを示すことができれば，ガロア群が可解であることが，多項式の根が冪根拡大体列に含まれることの必要十分条件であることになる．それを示さなければならない．これは，次のヒルベルトの定理 90 を用いて証明することができる．

ヒルベルトの定理 90

K/P を n 次巡回拡大とする． $G = \text{Gal}(K/P)$ は巡回群で，その生成元を σ とすると，

$$G = \langle \sigma \rangle = \{1, \sigma, \sigma^2, \dots, \sigma^{n-1}\} \quad (96)$$

となる． K の元を α とし，ノルム $N(\alpha)$ を次のように定義する．¹

$$N(\alpha) = \alpha \cdot \sigma(\alpha) \cdot \sigma^2(\alpha) \cdots \sigma^{n-1}(\alpha) \quad (97)$$

ここで， α を 0 と異なる K の元とする．このとき， $N(\alpha) = 1$ であることは，ある K の元 β があって $\alpha = \beta/\sigma(\beta)$ となることの必要十分条件である．

¹ ノルムの一般的な定義は，分離拡大 K/P において， P の元を係数とする K の間の線形写像を， x と a を K の元として， x から ax であると定義するとき，その表現行列の行列式をノルムという． a の最小多項式を $g(x)$ とすれば， a の共役な元 $a_1, a_2, \dots, a_n$ は $g(x)$ の相異なる根であり，表現行列の固有値である．したがって，ノルムは $a_1 a_2 \cdots a_n$ である．巡回拡大の場合は， $a, \sigma(a), \sigma^2(a), \dots, \sigma^{n-1}(a)$ が共役な元であり，ノルムは $a\sigma(a)\sigma^2(a) \cdots \sigma^{n-1}(a)$ である．

[必要であることの証明] ($\alpha = \beta/\sigma(\beta)$ なら $N(\alpha) = 1$)

K から 0 元を除いた差集合 $K^\times = K \setminus \{0\}$ は乗法群である．同様に， P から 0 元を除いた集合 $P^\times = P \setminus \{0\}$ も乗法群である．また， $N(\alpha)$ は σ に対して不変である．なぜなら， G は巡回群であるから $\sigma^n = 1$ となるので，

$$\begin{aligned}\sigma(N(\alpha)) &= \sigma(\alpha \cdot \sigma(\alpha) \cdot \sigma^2(\alpha) \cdots \sigma^{n-1}(\alpha)) \\ &= \sigma(\alpha) \cdot \sigma^2(\alpha) \cdot \sigma^3(\alpha) \cdots \sigma^n(\alpha) \\ &= \sigma(\alpha) \cdot \sigma^2(\alpha) \cdot \sigma^3(\alpha) \cdots \sigma^{n-1}(\alpha) \cdot \alpha \\ &= N(\alpha)\end{aligned}\tag{98}$$

となるからである．すなわち， $\sigma(N(\alpha)) = N(\alpha)$ である．したがって， $N(\alpha) \in P$ である．これから， $N(\alpha)$ は $\alpha \in K$ から $N(\alpha) \in P$ への写像であり，この写像は乗法群の準同型写像になる．準同型であることは， σ が準同型であることから，

$$\begin{aligned}N(\alpha\beta) &= (\alpha\beta) \cdot \sigma(\alpha\beta) \cdot \sigma^2(\alpha\beta) \cdots \sigma^{n-1}(\alpha\beta) \\ &= (\alpha\beta) \cdot \sigma(\alpha)\sigma(\beta) \cdot \sigma^2(\alpha)\sigma^2(\beta) \cdots \sigma^{n-1}(\alpha)\sigma^{n-1}(\beta) \\ &= \alpha \cdot \sigma(\alpha) \cdot \sigma^2(\alpha) \cdots \sigma^{n-1}(\alpha) \cdot \beta \cdot \sigma(\beta) \cdot \sigma^2(\beta) \cdots \sigma^{n-1}(\beta) \\ &= N(\alpha)N(\beta)\end{aligned}$$

となるからである．いま， $\alpha = \beta/\sigma(\beta)$ の関係が与えられているから，この式の両辺のノルムをとると，準同型であるから，

$$N(\alpha) = N(\beta/\sigma(\beta)) = N(\beta)/N(\sigma(\beta)) = N(\beta)/\sigma(N(\beta)) = N(\beta)/N(\beta) = 1\tag{99}$$

となる．なお，途中で，

$$\begin{aligned}N(\sigma(\beta)) &= \sigma(\beta) \cdot \sigma(\sigma(\beta)) \cdot \sigma^2(\sigma(\beta)) \cdots \sigma^{n-1}(\sigma(\beta)) \\ &= \sigma(\beta \cdot \sigma(\beta) \cdot \sigma(\sigma(\beta)) \cdots \sigma^{n-2}(\sigma(\beta))) \\ &= \sigma(\beta \cdot \sigma(\beta) \cdot \sigma^2(\beta) \cdots \sigma^{n-1}(\beta)) \\ &= \sigma(N(\beta))\end{aligned}$$

という関係を用いた．以上で題意が示された．

[十分であることの証明] ($N(\alpha) = 1$ なら $\alpha = \beta/\sigma(\beta)$)

$K^\times$ の元 q に対する G の元， $1, \sigma, \sigma^2, \dots, \sigma^{n-1}$ による写像の線形結合の値 β を考える．すなわち，

$$\beta = a_0q + a_1\sigma(q) + a_2\sigma^2(q) + \cdots + a_{n-1}\sigma^{n-1}(q)\tag{100}$$

とする． $a_i (i = 0, 1, \dots, n-1)$ は係数で 0 でないとする．このとき， $\beta \neq 0$ となるような q は必ず存在する．もし，すべての $q \in K$ に対して β が 0 になれば， K の自己準同型写像である $1, \sigma, \sigma^2, \dots, \sigma^{n-1}$ は一次独立であるから（デデキントの補題，後述）， $a_0 = a_1 = \cdots = a_{n-1} = 0$ でなければならないが，これは矛盾するからである．

ここで，係数 a_i を次の漸化式によって定義する．

$$\begin{aligned}a_0 &= 1, \\ a_r &= \sigma(a_{r-1})\alpha, \quad (r = 1, \dots, n-1)\end{aligned}\tag{101}$$

式 (100) に σ を施すと、準同型に注意して、

$$\sigma(\beta) = \sigma(a_0)\sigma(q) + \sigma(a_1)\sigma^2(q) + \sigma(a_2)\sigma^3(q) + \cdots + \sigma(a_{n-1})\sigma^n(q) \quad (102)$$

となる。ここで、係数である $\sigma(a_0)$ から $\sigma(a_{n-2})$ までは漸化式を使って次のように変形できる。

$$\sigma(a_0) = a_1\alpha^{-1}, \quad \sigma(a_1) = a_2\alpha^{-1}, \quad \sigma(a_2) = a_3\alpha^{-1}, \quad \cdots, \quad \sigma(a_{n-2}) = a_{n-1}\alpha^{-1} \quad (103)$$

一方、 $\sigma(a_{n-1})$ については、次のように変形する。

$$\begin{aligned} \sigma(a_{n-1}) &= \sigma(\sigma(a_{n-2})\alpha) = \sigma^2(a_{n-2})\sigma(\alpha) \\ &= \sigma^2(\sigma(a_{n-3})\alpha) = \sigma^3(a_{n-3})\sigma^2(\alpha)\sigma(\alpha) \\ &= \sigma^3(\sigma(a_{n-4})\alpha)\sigma^2(\alpha)\sigma(\alpha) = \sigma^4(a_{n-4})\sigma^3(\alpha)\sigma^2(\alpha)\sigma(\alpha) \\ &\vdots \\ &= \sigma^n(a_0)\sigma^{n-1}(\alpha)\sigma^{n-2}(\alpha)\sigma^{n-3}(\alpha)\cdots\sigma^2(\alpha)\sigma(\alpha) \end{aligned} \quad (104)$$

ここで、 $\sigma^n = 1$ であるから、 $\sigma^n(a_0) = 1 = \alpha\alpha^{-1}$ として、ノルムの式を当てはめると

$$\sigma(a_{n-1}) = \sigma^{n-1}(\alpha)\sigma^{n-2}(\alpha)\sigma^{n-3}(\alpha)\cdots\sigma^2(\alpha)\sigma(\alpha)\alpha\alpha^{-1} = N(\alpha)\alpha^{-1} \quad (105)$$

となる。さらに、前提となる条件 $N(\alpha) = 1$ を用いると、

$$\sigma(a_{n-1}) = \alpha^{-1} = \alpha^{-1}a_0 \quad (106)$$

となる。この式 (106) と式 (103) を式 (102) に代入すると、

$$\begin{aligned} \sigma(\beta) &= a_1\alpha^{-1}\sigma(q) + a_2\alpha^{-1}\sigma^2(q) + a_3\alpha^{-1}\sigma^3(q) + \cdots + a_{n-1}\alpha^{-1}\sigma^{n-1}(q) + \alpha^{-1}a_0q \\ &= [a_0q + a_1\sigma(q) + a_2\sigma^2(q) + a_3\sigma^3(q) + \cdots + a_{n-1}\sigma^{n-1}(q)]\alpha^{-1} \\ &= \beta\alpha^{-1} \end{aligned} \quad (107)$$

となる。これから、

$$\alpha = \beta/\sigma(\beta) \quad (108)$$

が得られる【証明終】

長い証明であったが、以上でヒルベルトの定理 90 は示された。次節では、このヒルベルトの定理 90 を用いて、ガロア群の剰余群が巡回群ならそれに対応する中間体が冪根拡大であることを示す。これによって、ガロア群が可解であることを示すことができれば、実際の拡大体に多項式のどのような根が含まれているのかを具体的に把握しないでも、根が冪根と四則演算のみで表すことができるか否かが明らかになるのである。

8.3 巡回拡大と冪根拡大

8.3.1 ガロア群の剰余群が巡回群なら体列は冪根拡大であること

それでは、ガロア群が巡回群であればそのもととなる拡大体は冪根拡大であることを示す。ガロア群が巡回群になる場合の拡大を巡回拡大という。これまで、冪根拡大体のガロア群は巡回群になることはすでに述べた。逆に、ガロア群が巡回群であれば、そのもとの拡大体は冪根拡大になることを示すことができれば、多項式の根を有理演算と冪根で解くことができること、すなわち可解であることを示すことができることになるので、

非常に重要である．すなわち，ガロア群が巡回群であることと体が冪根拡大であることは必要十分の関係にある．したがって，ガロア群が巡回群の列になることと多項式の根が可解であることが同値になり，このようなガロア群を可解ということができるのである．したがって，この巡回拡大と冪根拡大が同値であることを示すことは非常に重要なのである．以下に残された半分の証明を示す．

証明すべきことは以下のことである．

γ を n 次原始根とし， γ は基礎体 P に含まれているとする．そのとき， K/P のガロア群 G が n 次巡回群であることは， K が P の上の n 次冪根拡大体であることの必要十分条件である．

[証明]

[十分であることの証明 (ガロア群 G が n 次巡回群ならガロア拡大 K/P は n 次冪根拡大)]

巡回群 G の 1 つの生成元を σ とする． γ は σ の不変体 P に含まれるから，

$$\sigma(\gamma) = \gamma, \sigma^2(\gamma) = \gamma, \dots, \sigma^{n-1}(\gamma) = \gamma$$

である．これから，

$$\begin{aligned} N(\gamma) &= \gamma \cdot \sigma(\gamma) \cdot \sigma^2(\gamma) \cdots \sigma^{n-1}(\gamma) \\ &= \gamma \cdot \gamma \cdot \gamma \cdots \gamma = \gamma^n = 1 \end{aligned}$$

となるので，ヒルベルトの定理 90 により，

$$\gamma = \beta / \sigma(\beta)$$

となる K の元 β が存在する．すなわち，

$$\sigma(\beta) = \beta \gamma^{-1} \quad (109)$$

となる．このとき，

$$\sigma(\beta^n) = (\sigma(\beta))^n = (\beta \gamma^{-1})^n = \beta^n \gamma^{-n} = \beta^n \quad (110)$$

となり， β^n は σ に対して不変である．したがって， β^n は P の元である．これから， β を生成元とする P の上の拡大体 $P(\beta)$ において， $\{1, \beta, \beta^2, \dots, \beta^{n-1}\}$ は基底になることがわかる．これから， $P(\beta)$ の次元は n であることがわかる．すなわち，

$$[P(\beta) : P] = n \quad (111)$$

である．一方，群 G の位数を $|G|$ のように表すことにすると，

$$|\text{Gal}(K/P)| = [K : P] \quad (112)$$

が成り立つ (証明は後述する)．したがって，巡回群であるガロア群の位数 $|\text{Gal}(K/P)| = n$ であるから， $[K : P] = n$ である．これから，

$$P(\beta) = K \quad (113)$$

である．

一方， K における β と共役な元は

$$\beta, \sigma(\beta), \sigma^2(\beta), \dots, \sigma^{n-1}(\beta)$$

である．この共役元は式 (109) を用いて，

$$\beta, \beta \gamma^{-1}, \beta \gamma^{-2}, \dots, \beta \gamma^{-n+1}$$

と表される．これら n 個の元はすべて異なり， $x^n - \beta^n$ の根である． β^n は P の元であるから，これを a と表すと， β の最小多項式は $x^n - a$ である．これから， $x^n - a$ は K の P の上の最小分解体である．すなわち， K/P は n の冪根拡大体である．

[必要であることの証明 (K/P は n 次冪根拡大なら G が n 次巡回群)]

$x^n - a$ の n 次冪根を β とする．そうすると，この二項多項式は

$$x^n - a = (x - \beta)(x - \beta\gamma)(x - \beta\gamma^2) \cdots (x - \beta\gamma^{n-1}) \quad (114)$$

と表される．したがって，ガロア群 G は $\beta\gamma^i$ ($i = 0, 1, \dots, n-1$) の間の置換になるが，準同型写像になるのは， $\sigma(\beta) = \beta\gamma^b$ であり， b と n が素数の場合に $\sigma(\beta)$ は巡回群の生成元になる．したがって， G は n 次巡回群である．[証明終]

8.4 多項式の根の可解性

以上により，冪根拡大のガロア群は巡回群になり，かつガロア群が巡回群になる体の拡大は冪根拡大になることが示された．これにより，代数的に根の解法が得られること，すなわち可解性の条件が代数的に明確に定義できるようになった．可解ということは，冪根と四則演算の組み合わせであるから，多項式の根が連続した体の拡大の列の中に含まれることになるから，これを代数的により具体的に定義すれば，次のようになる．

多項式が可解であることの定義には次の冪根拡大体の有限列が基礎になる．基礎体 P が n 次原始根を含むとき，冪根拡大体の有限列

$$P = L_0 \subset L_1 \subset L_2 \subset \cdots \subset L_l = K \quad (115)$$

において，

$$L_{i+1} = L_i(\sqrt[p_i]{a_i}) \quad (i = 0, 1, 2, \dots, l-1) \quad (116)$$

が満たされ， a_i は体 L_i の元で， $p_0, p_1, \dots, p_l$ は素数とする． p_i の中に同一のものがあってもよい．

多項式が可解であるとは上の冪根拡大体の列の中に多項式の根が含まれているということである．しかしながら．根が含まれているか否かは根が明らかになっていなければならないので，これが可解性の判断の条件にはならない．根が明らかではないときに，可解性を判断するには，上の可解性の定義と同値な条件を考える必要がある．そのため，この冪根拡大体列に付随する式 (89) のガロア群列を考えよう．

$$H_1, H_2, \dots, H_l \quad (117)$$

このガロア群 H_i は巡回群であるが， L_i の列と同じように，冪根拡大の次数や冪根を知ることなしに判断することはできない．一方，このガロア群 H_i の直積から定義づけられるガロア群 G_i に関して，その系列は

$$G = G_0 \subset G_1 \subset G_2 \subset \cdots \subset G_l = \{e\} \quad (118)$$

であり，その剰余群 (G_{i-1}/G_i) ($i = 0, 1, \dots, l-1$) は H_i と同型である (8.2.4 節) ．

このガロア群の系列は，元のガロア群 G の部分群として定義されるのみで，ガロア群 G は多項式で十分定義づけられるので，冪根拡大の次数や冪根を知らなくてもガロア群 G のみで H_i が巡回群になるか否かを知ることができる．つまり，ガロア群 G の部分群の系列における剰余群 (H_i と同型) が巡回群になるか否かを知ることだけで，その部分群に対応する拡大体が冪根拡大体であること，さらにその拡大体が多項式の根を含むことまで知ることができるということを意味するのである．つまり，多項式のガロア群の部分群の系列を知ることにより，その剰余群が巡回群であれば，その多項式は可解であるということができるのである．このようなガロア群を可解とよぶのである．

まとめると、次のようになる。多項式が可解であるということは、根が冪根拡大の列の中に含まれていることであり、このことはガロア群が可解であることと等価である。

これで多項式の根の可解性が明らかになったように思われるが、まだ、上の命題の根拠としての中間体の存在の証明が残っている。すなわち、ガロア群があれば、そのすべての部分群に対応する拡大体と中間体が必ず存在することを示さないといけない。これを示すことによって、ガロア群が可解であることが、多項式の根の公式が存在することの必要十分条件になるのである。これを次節で述べる。

8.5 中間体とガロア部分群の対応—ガロア対応

本節では、ガロア拡大における拡大体と基礎体との間の中間体には必ず一つのガロア部分群が対応し、かつ、ガロア群の部分群には必ず一つの中間体に対応することを示す。この対応関係はガロア対応とよばれる。

8.5.1 一つの中間体に必ず一つのガロア部分群が対応すること

P を基礎体、 K を P の上のガロア拡大とする。すなわち、 K/P はガロア拡大である。 L を P と K の中間体とする。 $G = \text{Gal}(K/P)$ をガロア群、 H をその部分群とする。 K/P はガロア拡大であるから、 K は P の上のある多項式の最小分解体である。これを $f(x)$ とする。 $L \supset P$ であるから、 $f(x)$ は L の上の多項式でもあり、したがって、 K は L の上の多項式 $f(x)$ の最小分解体である。ゆえに、 K/L はガロア拡大である。なお、 $f(x)$ は P の上でも必ずしも既約ではない。その場合は最小多項式の積になる。 $f(x)$ の根が差集合 $L \setminus P$ の中に含まれている場合には、これを β とすると $(x - \beta)$ は $f(x)$ の因子になるので、それで割り切った多項式の最小分解体が K になる。 K/L はガロア拡大であることに変わりはない。

K は L のガロア拡大であるから、そのガロア群を $H = \text{Gal}(K/L)$ とする。 H の元は L の上の K の自己同型である。これを σ とする。 H の元は L の元を不変に保つ。 $L \supset P$ であるから、 P の元も不変に保つ。したがって、 $\sigma \in G$ である。これから、 $H \subset G$ であることがわかる。すなわち、 H は G の部分群であることがわかる。このことは、ガロア拡大体の中間体には必ず一つのガロア群が対応することを意味している。

次に、ガロア群 G の一つの部分群 H を取り上げる。 H の元 σ は K に関する自己同型写像である。 H のすべての σ に対して不変な K の元の全体は体を形成する。なぜなら、この集合の任意の 2 つの元を a と b とした場合、以下のようにして体の規則が満たされるからである。 σ の準同型規則により、 $\sigma(a+b) = \sigma(a) + \sigma(b) = a+b$ であるから $a+b$ はこの集合に含まれる。ここで、 $b = -a$ とおくと、 $\sigma(0) = \sigma(a) + \sigma(-a) = a - a = 0$ より $\sigma(-a) = -a$ となり、加法の逆元が含まれる。同じ式から零元もこの集合に含まれることがわかる。

乗法に関しても、 $\sigma(ab) = \sigma(a)\sigma(b) = ab$ であるから ab もこの集合に含まれる。上と同様にして、 $b = a^{-1}$ と置くことにより、 $\sigma(e) = e$ 、 $\sigma(aa^{-1}) = \sigma(a)\sigma(a^{-1}) = a\sigma(a^{-1}) = e$ より $\sigma(a^{-1}) = a^{-1}$ が成り立ち、逆元と単位元が含まれることがわかる。このように、この集合は体を形成することがわかる。この体を H の作用に不変な K の元ということで慣用的に用いられる K^H と表すことにする。 P の元を a とする。 σ は H の元であるから G の元でもある。したがって、 $\sigma(a) = a$ であるから、 $a \in K^H$ でもある。 a は σ に対して不変であるから $\sigma(a) = a$ である。これから、 K^H は K と P の中間体である。以上により、ガロア群 G の一つの部分群はガロア拡大体 K と基礎体 P の間の一つの中間体に対応することがわかる。

$L = K$ の場合は $K^H = \{e\}$ である。

2 つの中間体 L_1 と L_2 があり、 $L_1 \supset L_2$ であるとする。 L_1 と L_2 に対応するガロア部分群を H_1 と H_2 とする。 H_1 の元は L_1 を不変に保つから、 L_2 も不変に保つ。したがって、 H_2 の元でもある。これから、 $H_1 \subset H_2$ である。

もし、 $H_1 \supset H_2$ なら、 L_2 は H_2 の元に対して不変である。 H_2 の元は H_1 の元でもあるから、 H_1 に対しても不変である。したがって、 L_2 は H_1 に対しても不変な L_1 の中に含まれる。すなわち、 $L_2 \supset L_1$ という関係がある。

これで、ガロア群の部分群には必ず一つの間体に対応し、それが、可解である場合は中間体も可解となる。以上により、多項式の根が冪根と四則演算で表されることが示されたことになる。

8.6 主な定理の証明

本節までで、一般の多項式の可解性はガロア群の可解性の有無から明らかになることが示された。この後は、一般の多項式のガロア群を具体的に議論して、多項式が可解か非可解を明らかにする。本節の残りの部分では、これまで証明なしに述べられてきた定理や補題の証明をまとめて示す。

8.6.1 デデキントの補題

K_1, K_2 を任意の体で $K_1 \subset K_2$ とし、 $\sigma_1, \sigma_2, \dots, \sigma_h$ を K_1 から K_2 への相異なる準同型写像とする。また、 $b_1, \dots, b_h$ を K_2 の元、 a を K_1 の任意の元とする。このとき、

$$b_1\sigma_1(a) + b_2\sigma_2(a) + \dots + b_h\sigma_h(a) = 0 \quad (119)$$

が成り立つなら、 $b_1 = b_2 = \dots = b_h$ である。この補題は、相異なる準同型写像は 1 次独立であることを意味する。

[証明]

帰納法で証明する。 $h = 1$ のとき、 $b_1\sigma_1(a) = 0$ である。 $a = 1$ とすると、 $\sigma(1) = 1$ であるから、 $b_1 = 0$ となる。したがって、 $h = 1$ のときに成り立つ。

$h - 1$ のときに、

$$b_1\sigma_1(a) + b_2\sigma_2(a) + \dots + b_{h-1}\sigma_{h-1}(a) = 0 \quad (120)$$

なら、 $b_1 = b_2 = \dots = b_{h-1}$ が成り立つと仮定する。いま、 $\sigma_1 \neq \sigma_h$ であるから、 $\sigma_1(a_0) \neq \sigma_h(a_0)$ となる K_1 の元 a_0 が存在する。式 (119) の a は任意の K_1 の元であるから、これに aa_0 を代入すると、準同型であるから、 $\sigma_i(aa_0) = \sigma_i(a)\sigma_i(a_0)$ であることに注意すると、

$$b_1\sigma_1(a)\sigma_1(a_0) + b_2\sigma_2(a)\sigma_2(a_0) + \dots + b_h\sigma_h(a)\sigma_h(a_0) = 0 \quad (121)$$

となる。一方、式 (119) に $\sigma_1(a_0)$ をかけると、

$$b_1\sigma_1(a)\sigma_1(a_0) + b_2\sigma_2(a)\sigma_1(a_0) + \dots + b_h\sigma_h(a)\sigma_1(a_0) = 0 \quad (122)$$

となる。式 (121) から式 (122) を引くと、左辺第 1 項が打ち消しあって、

$$b_2\sigma_2(a)[\sigma_2(a_0) - \sigma_1(a_0)] + \dots + b_h\sigma_h(a)[\sigma_h(a_0) - \sigma_1(a_0)] = 0 \quad (123)$$

となる。帰納法の仮定により、式 (123) の $\sigma_i(a)$ は $h - 1$ 項であるのでその係数はすべて 0 に等しい。したがって、左辺の第 $h - 1$ 項の係数は

$$b_h[\sigma_h(a_0) - \sigma_1(a_0)] = 0$$

となる。一方、 a_0 を $\sigma_1(a_0) \neq \sigma_h(a_0)$ となるようにとっているので、 $b_h = 0$ でなければならない。これを式 (119) に代入すると、式 (120) になり、この式からは帰納法で $b_1 = b_2 = \dots = b_{h-1}$ が成り立つことが仮定されているので、結局、 $b_1 = b_2 = \dots = b_h$ が成り立つ。 [証明終]

8.6.2 デデキントの補題 2

$L/K/P$ を代数的拡大, $\text{Hom}_P(K, L)$ を体 P の上の体 K から L への準同型写像の全体がなす集合とすると, 次の式が成り立つ.

$$|\text{Hom}_P(K, L)| \leq [K : P] \quad (124)$$

ここで, $|\text{Hom}_P(K, L)|$ は $\text{Hom}_P(K, L)$ の位数, $[K : P]$ は P の上の K の次元である.

[証明]

$[K : P] = n$ とする. そのとき, P の上の K の基底を $\{u_1, u_2, \dots, u_n\}$ とする. 背理法で示す. 式 (109) が成り立たないとする. その場合, $|\text{Hom}_P(K, L)| > n$ であるから, $|\text{Hom}_P(K, L)| = n + 1$ としてよい. そのとき, $\text{Hom}_P(K, L)$ の $n + 1$ 個の異なる元を $\sigma_1, \sigma_2, \dots, \sigma_n, \sigma_{n+1}$ とする. $\sigma_i(u_1), \sigma_i(u_2), \dots, \sigma_i(u_n)$, を n 個の成分とする n 次元のベクトルを用いて, 次の x_i を係数とする線形結合を考える.

$$x_1 \begin{pmatrix} \sigma_1(u_1) \\ \sigma_1(u_2) \\ \vdots \\ \sigma_1(u_n) \end{pmatrix} + x_2 \begin{pmatrix} \sigma_2(u_1) \\ \sigma_2(u_2) \\ \vdots \\ \sigma_2(u_n) \end{pmatrix} + \dots + x_{n+1} \begin{pmatrix} \sigma_{n+1}(u_1) \\ \sigma_{n+1}(u_2) \\ \vdots \\ \sigma_{n+1}(u_n) \end{pmatrix} = 0 \quad (125)$$

この式において, n 次元ベクトルが $n + 1$ 個あるから左辺は線形従属である. したがって,

$$(x_1, x_2, \dots, x_{n+1}) \neq (0, 0, \dots, 0) \quad (126)$$

となる x_i が存在する. ここで, a を K_1 の任意の元とすると, 基底 u_i を用いて,

$$a = c_1 u_1 + c_2 u_2 + \dots + c_n u_n \quad (127)$$

と表すことができる.

式 (125) の第 1 行に c_1 をかけ, 第 2 行に c_2 をかけ, 以下同様にして, 第 n 行に c_n をかけると, 準同型により,

$$x_1 \sigma_1(c_1 u_1 + \dots + c_n u_n) + x_2 \sigma_2(c_1 u_1 + \dots + c_n u_n) + \dots + x_n \sigma_n(c_1 u_1 + \dots + c_n u_n) = 0$$

となる. すなわち,

$$x_1 \sigma_1(a) + x_2 \sigma_2(a) + \dots + x_n \sigma_n(a) = 0 \quad (128)$$

である. a は K_1 の任意の元であるから, デデキントの補題により, $x_1 = x_2 = \dots = x_{n+1} = 0$ でなければならない. しかし, これは最初の仮定である $|\text{Hom}_P(K, L)| > n$ と矛盾する. したがって, 背理法により,

$$|\text{Hom}_P(K, L)| \leq [K : P]$$

でなければならない. [証明終]

8.6.3 アルティンの補題

G を自己同型群 $\text{Aut}(K)$ の部分群とする. $P = K^G$ なら K/P はガロア拡大であり,

$$[K : P] \leq |G| \quad (129)$$

である.

[証明]

G の元を $\sigma_1, \sigma_2, \dots, \sigma_n$ とする. P の上の K の基底を $\omega_1, \omega_2, \dots, \omega_k$ とする. すなわち, $|G| = n, [K : P] = k$ である.

背理法で証明する. そのため, $k > n$ と仮定しよう. K を P の上の k 次元線形空間と考えると, 相異なる準同型写像 $\sigma_1, \dots, \sigma_n$ 1 次独立であるから (デデキントの補題), これをベクトルの n 個の成分として扱い, 次の k 個のベクトルを考える.

$$\begin{pmatrix} \sigma_1(\omega_1) \\ \vdots \\ \sigma_n(\omega_1) \end{pmatrix}, \begin{pmatrix} \sigma_1(\omega_2) \\ \vdots \\ \sigma_n(\omega_2) \end{pmatrix}, \dots, \begin{pmatrix} \sigma_1(\omega_k) \\ \vdots \\ \sigma_n(\omega_k) \end{pmatrix} \quad (130)$$

ここで, $k > n$ であるから, この k 個のベクトルは 1 次従属であり,

$$c_1 \begin{pmatrix} \sigma_1(\omega_1) \\ \vdots \\ \sigma_n(\omega_1) \end{pmatrix} + c_2 \begin{pmatrix} \sigma_1(\omega_2) \\ \vdots \\ \sigma_n(\omega_2) \end{pmatrix} + \dots + c_k \begin{pmatrix} \sigma_1(\omega_k) \\ \vdots \\ \sigma_n(\omega_k) \end{pmatrix} = 0 \quad (131)$$

を満たす K の元 $c_1, \dots, c_k$ で $(c_1, \dots, c_k) = (0, \dots, 0)$, すなわち全てが 0 ではないものが存在する. $k > n$ と仮定しているから, $k = n + 1$ を取り上げてみよう. この c_i ($i = 1, \dots, n + 1$) のうち, 1 個以上の c_i において, 任意の σ_j に対し $\sigma_j(c_i) = c_i$ が成り立つものとする. すなわち, $c_i \in P$ であるとする. 式 (131) に σ_l を作用させると,

$$\sigma_l(c_1) \begin{pmatrix} \sigma_l \sigma_1(\omega_1) \\ \vdots \\ \sigma_l \sigma_n(\omega_1) \end{pmatrix} + \sigma_l(c_2) \begin{pmatrix} \sigma_l \sigma_1(\omega_2) \\ \vdots \\ \sigma_l \sigma_n(\omega_2) \end{pmatrix} + \dots + \sigma_l(c_k) \begin{pmatrix} \sigma_l \sigma_1(\omega_k) \\ \vdots \\ \sigma_l \sigma_n(\omega_k) \end{pmatrix} = 0 \quad (132)$$

となる. ここで, $\sigma_l \sigma_i$ ($i = 1, \dots, n + 1$) において, σ_l は固定されており, $\sigma_l \sigma_i$ は $n + 1$ 個の相異なる σ_i を与えるので, $\sigma_l \sigma_i = \sigma_j$ ($j = 1, \dots, n + 1$) としても構わないから, 行を j の順に入れ替えると,

$$\sigma_l(c_1) \begin{pmatrix} \sigma_1(\omega_1) \\ \vdots \\ \sigma_n(\omega_1) \end{pmatrix} + \sigma_l(c_2) \begin{pmatrix} \sigma_1(\omega_2) \\ \vdots \\ \sigma_n(\omega_2) \end{pmatrix} + \dots + \sigma_l(c_k) \begin{pmatrix} \sigma_1(\omega_k) \\ \vdots \\ \sigma_n(\omega_k) \end{pmatrix} = 0 \quad (133)$$

となる. 左辺のベクトルを入れ替えても和は変わらないから $c_i \in P$ となる項を最後に移動して $k' + 1$ 項から k 項までとしても一般性は失われない. そのとき, 式 (131) でも同じようにベクトルを入れ替えておくことにする. そうして, 式 (131) から式 (133) を差し引くと, $k' + 1$ 項から k 項までは $c_j \sigma_l(c_j) = c_j$ となるから, 相殺して消える. 残った項は k' 項で, $k' < k = n + 1$ であるから, 1 次独立であり, その係数はすべて 0 となり, 結局,

$$\sigma_l(c_1) = c_1, \sigma_l(c_2) = c_2, \dots, \sigma_l(c_{k'}) = c_{k'}$$

となる. すなわち, すべての c_i は P に含まれることになる.

次に, すべての c_i が P に含まれない場合を考える. $c_1 \neq 0$ であるから, 式 (131) を c_1 で割ると, 第 1 項の係数は 1 となり, P に含まれることになる. したがって, 1 個以上の c_i が P に含まれる場合に該当するから, 上の場合と同様に係数はすべて P に含まれなければならない.

結局, 式 (131) の係数 c_i はすべて P に属し, $\sigma_l(c_i) = c_i$ となるから, これが第 j 行で $\sigma_j(c_i)$ となるので, 準同型規則により次の式になる.

$$\begin{pmatrix} \sigma_1(c_1 \omega_1) \\ \vdots \\ \sigma_n(c_1 \omega_1) \end{pmatrix} + \begin{pmatrix} \sigma_1(c_2 \omega_2) \\ \vdots \\ \sigma_n(c_2 \omega_2) \end{pmatrix} + \dots + \begin{pmatrix} \sigma_1(c_k \omega_k) \\ \vdots \\ \sigma_n(c_k \omega_k) \end{pmatrix} = 0 \quad (134)$$

各項を成分ごとに加えて準同型規則を用いると各行は $\sigma_i(c_1\omega_1 + \cdots + c_k\omega_k)$ となるので、すべての行を加えると、

$$\sum_{i=1}^k \sigma_i(c_1\omega_1 + \cdots + c_k\omega_k) = 0 \quad (135)$$

となる。 σ_i は相異なる準同型写像であり、係数はすべて 1 であるから、これが成り立つためには、

$$c_1\omega_1 + \cdots + c_k\omega_k = 0 \quad (136)$$

でなければならない。 $\omega_1, \dots, \omega_k$ は K の基底であるから、この式は 1 次独立であり、 $c_1 = c_2 = \cdots = c_k = 0$ でなければならない。しかし、これは $k > n$ と仮定して $(c_1, \dots, c_k) \neq (0, \dots, 0)$ としたことに矛盾する。したがって、背理法により、 $k \leq n$ でなければならない。すなわち、

$$[K : P] \leq |G| \quad (137)$$

が成り立つ。

デデキントの補題 2 は一般的に成り立ち、一方、ガロア拡大ではアルティンの補題が成り立つ。したがって、ガロア拡大では両方が満足されるので、

$$[K : P] = |G| \quad (138)$$

が成り立つ。

8.7 ガロア拡大の異なる定義

前節でガロア拡大とは、二項式の根がすべて体拡大の生成元となる場合であると述べた。あるいは、多項式の根がすべて拡大生成元となる場合と言ってもよい。一般には、正規拡大かつ分離拡大であることと述べた。標数が 0 の体では、すなわち、複素数体のような場合には分離拡大であることが明らかであるので分離拡大であることを条件として強調することがなかった。ここでは、より一般的なガロア拡大の定義とそれと異なる同等な定義として次のガロア拡大の定義を述べ、その同等性を示す。以下、体 K を体 P の上の代数的有限拡大体とする。

- (1) K が正規拡大かつ分離拡大のとき、 K/P はガロア拡大である。

これは前節で示した定義である。 K の任意の元に対し、その最小多項式が K で 1 次式の積に分解されれば正規拡大であり、 K のすべての元に対し、その最小多項式が重根をもたなければ分離拡大である。標数 0 の体ではすべての元が分離的である。実数体や複素数体は分離的である。

- (2) K が P の上のある関数 $f(x)$ の最小分解体になっているとき、 K/P はガロア拡大である。

$f(x)$ が 1 次式の積に分解できる体を分解体といい、その最小の体が最小分解体である。

- (3) G が K の自己同型群で、 $K^G = P$ とするとき、 K/P はガロア拡大である。

これはアルティンの定理と呼ばれる。

- (4) P の上の K の自己同型群を $\text{Aut}(K/P)$ 、その位数を $|\text{Aut}(K/P)|$ 、 $[K : P]$ を拡大の次数とすると、

$$|\text{Aut}(K/P)| = [K : P] \quad (139)$$

なら、 K/P はガロア拡大である。

8.7.1 (1) $\Rightarrow$ (2) の証明 [正規拡大, 分離拡大なら最小分解体]

K/P が有限拡大であるので, $K = P(\alpha_1, \dots, \alpha_n)$ と表すことができる. α_1 の最小多項式を f_1 とする. K/P の正規性から α_1 と共役なすべて K に含まれるが, それが生成元 $\alpha_1, \dots, \alpha_n$ を網羅しない場合, 残った α_i の中から一つ選んでその最小多項式 f_2 を作る. f_1 と f_2 の共役元に含まれない生成元があれば同様に最小多項式を作り, その結果, $f_1, f_2, \dots, f_m$ の有限個の最小多項式の共役元で生成元を網羅できたとする. この操作は, 有限拡大であるから必ず有限回で終わる. そうすると, $F = f_1 f_2 \cdots f_m$ の最小分解体 U は K を含む. すなわち, $U \supset K$ である.

最小多項式 f_i の根は共役も含めて $\alpha_1, \dots, \alpha_n$ の中にある. したがって, F の根とその共役元も $\alpha_1, \dots, \alpha_n$ の中にあるので, $U \subset P(\alpha_1, \dots, \alpha_n) = K$ である. すなわち, ガロア拡大体 K は F の最小分解体である. [証明終]

8.7.2 (2) $\Rightarrow$ (1) の証明 [最小分解体なら正規拡大, 分離拡大]

K が多項式 F の最小分解体であるとする. F を既約多項式 f_i の積に分解すると,

$$F = \prod_{i=1}^m f_i$$

となる. F の最小分解体を U とすると, $U = P(\alpha_1, \dots, \alpha_n)$ は P の元を係数とする代数的生成拡大体である. ここで, $\alpha_1, \dots, \alpha_n$ は $f_1, f_2, \dots, f_m$ の根の集合である. U の任意の元 α は P の元と $\alpha_1, \dots, \alpha_n$ の有理関数である. これを $g(\alpha_1, \dots, \alpha_n)$ と表す. $\alpha_1, \dots, \alpha_n$ に P の上の K の自己同型写像 σ_i ($i = 1, \dots, m$) を施すと, それぞれ $\sigma_i(\alpha_1), \dots, \sigma_i(\alpha_n)$ に変換される. ここで $\sigma_i(\alpha_1), \dots, \sigma_i(\alpha_n)$ は $\alpha_1, \dots, \alpha_n$ の置換である. 詳しく述べると, この置換は, m 個の f_i について, その根の置換がそれぞれあり, その m 個の置換の直積である. σ_i ($i = 1, \dots, m$) を $\alpha = g(\alpha_1, \dots, \alpha_n)$ に施すと, 準同型により, $\sigma_i(\alpha) = g(\sigma_i(\alpha_1), \dots, \sigma_i(\alpha_n))$ となるが, 変化しない場合を除いて l 個相異なる $\sigma_i(\alpha)$ が l 個あったとする. 相異なる場合の添字 i を 1 から l まで書き換えると, σ_i は f_k の根の置換の直積であるから, $\sigma_i(\alpha_j)$ は $\alpha_1, \dots, \alpha_n$ のいずれかであり, $g(\sigma_i(\alpha_1), \dots, \sigma_i(\alpha_n))$ は U に含まれる. したがって, α の最小多項式は

$$(x - \alpha)[x - g(\sigma_1(\alpha_1), \dots, \sigma_1(\alpha_n))] \cdots [x - g(\sigma_l(\alpha_1), \dots, \sigma_l(\alpha_n))]$$

と 1 次式の積に分解される. したがって, K/P は正規拡大である. また, 相異なる 1 次式の積であるから重根はなく, 分離的である. したがって, K/P はガロア拡大である. [証明終]

8.7.3 (1) $\Rightarrow$ (3) の証明 [正規拡大, 分離拡大なら $K^G = P$]

P の有限次代数拡大を K とする. P に含まれない K の元 α_1 の最小多項式を $f_1(x)$ とし, K は正規拡大であるから, $f_1(x)$ は K の上で次のように 1 次式の積に分解される.

$$f_1(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

f_1 の根の間の置換, すなわち, $\alpha_1, \dots, \alpha_n$ の間の置換は K から K への写像 ϕ となる. かつ, この写像は準同型規則を満たす. なぜなら, その写像の一つを ϕ とすると, ϕ は α_i の置換であるから,

$$\phi(\alpha_i \alpha_j) = \phi(\alpha_i) \phi(\alpha_j), \quad \phi(\alpha_i + \alpha_j) = \phi(\alpha_i) + \phi(\alpha_j)$$

となり, さらに,

$$\phi(f_1(\alpha_1)) = f_1(\phi(\alpha_1)) = 0$$

となるからである．根の置換以外の写像は準同型規則が満たされない．

P 中の任意の元 β の最小多項式は単一の 1 次式 $x - \beta$ であり，根は一つで，根の間の写像は恒等写像のみである．

f_1 の根 $\alpha_1, \dots, \alpha_n$ を含まず， P 中にも含まれない元 K の中から任意の元 γ_1 を選びその最小多項式を $f_2(x)$ とする． K/P は正規拡大であるから，共役な元 $\gamma_1, \gamma_2, \dots, \gamma_m$ を用いて，

$$f_2(x) = (x - \gamma_1)(x - \gamma_2) \cdots (x - \gamma_m)$$

と表される． f_1 の場合と同様に，共役な根 γ_i の間の準同型写像を定義することができる．このように， K 中に f_1 の共役元も f_1 の共役元を含まず， P の元でもない元があればその最小多項式を作り，その根の間の準同型写像を定義していけば， K は有限次拡大体であるから最後には P の元でもなく共役元も含まない元はなくなる．

各最小多項式の共役根の間の置換からなる準同型写像を一つの類として，そのような類が複数ある．この類の直積を作ると，その元は最小多項式 $f_1, f_2, \dots$ で定義されたそれぞれの共役根をすべて合わせた集合の間の置換という K の自己準同型写像が定義される．この準同型写像は以下のように群を構成することがわかる．

まず，明らかに恒等写像が存在する．2 つの連続した置換はもう一つの置換であるから，置換の直積も置換となり，写像の演算はこの集合の中で閉じている．さらに，この置換の写像は 1 対 1 写像であるから，単射であり，逆元が存在する．したがって，この準同型写像の集合は群を形成する．これを G と表す．

群 G の成り立ちから明らかなように， P の元に関しては，恒等写像しか存在しない．したがって，すべて類の直積である G の元は P の元を不変に保つ． P 以外の元に対しては， G はすべての共役元の間のすべての置換となる写像を含むことがわかる．以上から， G は自己同型群 $\text{Aut}(K)$ の部分群であり， G に関して不変となる K の元全体の集合を K^G と表せば，

$$K^G = P$$

となる．[証明終]

8.7.4 (3) $\Rightarrow$ (1) の証明 $[K^G = P$ なら 正規拡大，分離拡大]

K/P を有限次代数拡大とする． G を K の自己同型群 $\text{Aut}(K)$ の部分群で，その位数を n とする． K の任意の元 α を取り上げ，これに G の元をすべて作用させたとき， $\alpha_1 = \alpha$ として， $\alpha_1, \alpha_2, \dots, \alpha_r$ に変換されるとする．ここで， $r \leq n$ である．このとき， G のすべての元の作用は $\alpha_1, \alpha_2, \dots, \alpha_r$ の置換のみに閉じている．なぜなら， G の任意の元 σ と $\alpha_1, \dots, \alpha_r$ の任意の元 α_i に対し， $\sigma(\alpha_i) = \beta$ になったとする．一方， $\alpha_i = \tau(\alpha_1)$ となる G の元 τ が必ずあるので， $\beta = \sigma(\alpha_i) = \sigma\tau(\alpha_1)$ となり， $\sigma\tau$ は群 G の元であるから， β は $\alpha_1, \dots, \alpha_r$ 含まれてしまうからである．

また， G の元が $\alpha_1, \alpha_2, \dots, \alpha_r$ のすべての置換を尽くしているわけではない．さらに， G の相異なる元が $\alpha_1, \alpha_2, \dots, \alpha_r$ の一つの置換に重複して変換する場合もあることもある．重要なことは， G の元が $\alpha_1, \alpha_2, \dots, \alpha_r$ の置換のみを起こすということである．

ここで，

$$f_1(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_r)$$

とすると， $f_1(x)$ の各係数は $\alpha_1, \dots, \alpha_r$ の対称式である．つまり，すべての係数は， G の元による $\alpha_1, \dots, \alpha_r$ の置換に対し不変であり， P の元であることがわかる．すなわち， $f_1(x)$ は P の上の多項式であるから， $f_1(x)$ は $\alpha = \alpha_1$ の最小多項式となる．したがって， K/P は正規拡大である．また， $f_1(x)$ は重根を含んでいないのが明らかである．したがって， K/P は分離拡大でもある．[証明終]

8.7.5 (1) $\Rightarrow$ (4) の証明 [正規拡大, 分離拡大なら $|\text{Aut}(K/P)| = [K : P]$]

$L/K/P$ を有限次代数拡大とする. $\text{Hom}_P(K, L)$ は体 P の上の拡大体 K から同 L への準同型写像の集合である. L は K の任意の元の共役元をすべて含む程度に十分大きいとする.

以下では, 分離拡大の場合は

$$|\text{Hom}_P(K, L)| = [K : P]$$

が成り立ち, 正規拡大の場合には,

$$|\text{Hom}_P(K, L)| = \text{Aut}(K/P)$$

が成り立つことを示す. 両方が満たされるとき, $|\text{Aut}(K/P)| = [K : P]$ が成り立つ.

分離拡大の場合は $|\text{Hom}_P(K, L)| = [K : P]$ が成り立つことをまず示す.

K が P の上の単拡大の場合を考え, これを α を生成元として $P(\alpha)$ とする. α の最小方程式 $f(x)$ の根を $\alpha_1, \alpha_2, \dots, \alpha_n$ とする. このうち, $P(\alpha)$ には $\alpha = \alpha_1$ しか含まれていない. 一方, L にはすべての共役元が含まれている. 準同型写像は最小多項式の根の間の置換であり, それ以外の写像は準同型規則を満足しない. したがって, $P(\alpha)$ から L への準同型は, $\alpha_1 \rightarrow \alpha_1, \alpha_1 \rightarrow \alpha_2, \dots, \alpha_1 \rightarrow \alpha_n$ の n 種類となる. したがって, 準同型写像の数は $f(x)$ の根の数に等しい. すなわち, $|\text{Hom}_P(P(\alpha), L)|$ は根の数に等しい.

一方, $P(\alpha)$ の基底は最小多項式 $f(x)$ の次元で決定し, $f(x)$ の最大次数が n ならば, $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ が基底になる. α^{n-1} より大きい次数の項は $f(x) = 0$ の関係より $n-1$ 次の多項式に変換される. したがって, $P(\alpha)/P$ の次元は $f(x)$ の次元の n である. すなわち,

$$[P(\alpha)/P] = \dim f = n \quad (140)$$

である.

一般の場合, K は代数的組成拡大体となり, $K = P(\alpha_1, \dots, \alpha_n)$ とすることができる. この場合を数学的帰納法で証明する.

$n = 1$ の場合はすでに示した.

$n - 1$ の場合, $\alpha_1, \dots, \alpha_{n-1}$ が P 上で分離的なら, $M = P(\alpha_1, \dots, \alpha_{n-1})$ として,

$$|\text{Hom}_P(M, L)| = [M : P]$$

が成り立つと仮定する. ここで, $\alpha_n \in K$ を取り上げ, P 上分離的とすると, M 上でも分離的で, $n = 1$ の場合と同様にして,

$$|\text{Hom}_M(M(\alpha_n), L)| = [M(\alpha_n) : M]$$

が成り立つ. 書き換えると,,

$$\text{Hom}_M((K, L) = [K : M]$$

である. この式と仮定の式から, $L/K/M/P$ という体拡大の関係の中で,

$$\text{Hom}_P((M, L) = [M : P]$$

$$\text{Hom}_M((K, L) = [K : M]$$

が成り立ち, この式の辺々を掛けて,

$$\text{Hom}_P(M, L)\text{Hom}_M((K, L) = [K : M][M : P]$$

となる．これから，

$$\text{Hom}_P(L, M) = [L : P]$$

となる． $K = M(\alpha_n) = P(\alpha_1, \dots, \alpha_{n-1}, \alpha_n)$ であるから，

$$\text{Hom}_P(P(\alpha_1, \dots, \alpha_n), L) = [P(\alpha_1, \dots, \alpha_n) : P]$$

が成り立つ．すなわち， K/P が分離拡大なら

$$\text{Hom}_P(K, L) = [K : P] \quad (141)$$

が成り立つ．

次に，正規拡大の場合について示す．

K/P が有限次代数拡大であるから，

$$\text{Aut}(K/P) \subset \text{Hom}_P(K, L)$$

が成り立つ．なぜなら， ϕ を $\text{Aut}(K/P)$ の元とすると， ϕ は K から K への写像で， $K \subset L$ であるので， K から L への写像の中に含まれるからである．

一方，正規拡大であれば， K の任意の元 α の共役な元がすべて K に含まれるので， K から L への準同型写像は共役な根の間の置換となり，根を含まない元は不変であるから，写像先はすべて K に含まれる．つまり， ψ を $\text{Hom}_P(K, L)$ の任意の元とすると， ψ は全単射であり， $\psi(K) = K$ となる．したがって， $\psi \in \text{Aut}(K/P)$ となり，

$$\text{Hom}_P(K, L) \subset \text{Aut}(K/P)$$

でなければならない．以上から，正規拡大の場合には，

$$\text{Hom}_P(K, L) = \text{Aut}(K/P) \quad (142)$$

が成り立つ．

式 (141)(142) から，

$$\text{Aut}(K/P) = [K : P] \quad (143)$$

が成り立つ．[証明終]

8.7.6 (4) $\Rightarrow$ (1) の証明 $|\text{Aut}(K/P)| = [K : P]$ なら正規拡大，分離拡大

一般に，デデキントの補題 2 より

$$|\text{Hom}_P(K, L)| \leq [K : P]$$

が成り立つ．また，上で述べたように， K/P が有限次代数拡大であるから，

$$\text{Aut}(K/P) \subset \text{Hom}_P(K, L)$$

が成り立つ，したがって，

$$|\text{Aut}(K/P)| \leq |\text{Hom}_P(K, L)| \leq [K : P]$$

となる．この関係式と与えられた関係式 $|\text{Aut}(K/P)| = [K : P]$ から $|\text{Aut}(K/P)| = |\text{Hom}_P(K, L)|$ および $|\text{Hom}_P(K, L)| = [K : P]$ となり，前の照明により，それぞれ，正規拡大および分離拡大であることを示す．[証明終]

8.7.7 (2) $\Rightarrow$ (3) の証明 [最小分解体なら $K^G = P$]

K を P の上の $F(x)$ の最小分解体とする． $F(x)$ は単一または複数の最小分解体 $f_i(x)$ の積である． $F(x)$ の一つの根を α とすると，これはある $f_i(x)$ の根であり， K から K への自己同型 $\text{Aut}(K)$ の元は， $f_i(x)$ の共役な根の間の置換および他の最小多項式の共役な根の間の置換の直積である．(1) から (3) への証明で詳しく述べたように，このような自己同型写像の全体の集合は群 G を形成する． G の元は共役な根の間の置換であるから， P の元を不変にする．したがって， $K^G = P$ である．[証明終]

8.7.8 (3) $\Rightarrow$ (2) の証明 [$K^G = P$ なら最小分解体]

K/P は有限次代数拡大である．(3) から (1) への証明と同様にして， K の一つ元 α の最小多項式 $f_1(x)$ を得ることができる．次に， K の中に， $f_1(x)$ の元と P の元を含まない元 β があれば，これに G の元をすべて作用させて得られる元の集合から β の最小多項式 $f_2(x)$ を得ることができる．さらに，残った K の元の中から， f_1 と f_2 の共役元および P の元 γ を選び，最小多項式 $f_3(x)$ を得ることができる． K は有限であるから，この操作はある回数 m で終わり， f_1 から f_m の最小多項式が得られる．そこで，

$$F(x) = \prod_{i=1}^m f_i(x)$$

とし， $F(x)$ の最小分解体を U とする． U の元は， K の元とその最小多項式に関する共役元および体 P の元との間の有理演算結果であるから， K に含まれる．すなわち， $U \subset K$ である．一方， K の任意の元は， $F(x)$ の生成の仕方から，いずれか，あるいはいくつかの $f_i(x)$ の根を含んでいる．したがって， α はこれらの根の関数である．すなわち， α は体 U の元でもある．これから， $K \subset U$ が成り立つ．両方を合わせると， $K = U$ が成り立ち， K は最小分解体であることが示された．[証明終]

(つづく)

参考文献

- [1] エム・ポストニコフ「ガロアの理論」日野寛三訳 (東京図書, 1964) .
- [2] エミール・アルティン「ガロア理論入門」寺田文行訳 (ちくま学芸文庫) (筑摩書房, 2010) .
- [3] 彌永 昌吉「ガロアの時代 ガロアの数学 第二部 数学篇」(シュプリンガー数学クラブ) (シュプリンガー・フェアラーク, 2002) .
- [4] 中島 匠一「代数方程式とガロア理論」(共立叢書現代数学の潮流,) (共立出版, 2006) .
- [5] 雪江 明彦「代数学 2 環と体とガロア理論 第 2 版」(日本評論社, 2023) .