環・体論 II — GALOIS 理論

高山　幸秀

Contents

Date: ２０１１年9月１６日版.

記号上の約束。

- $\mathbb{N} = \{0, 1, 2, \ldots\}$ とする。
- 集合の包含関係 $S \subset T$ は、特に断りの無い限り、$S = T$ の場合も含むものとする。

はじめに

$\mathbb{Q}$ (有理数全体の集合), $\mathbb{R}$ (実数全体の集合), $\mathbb{C}$ (複素数全体の集合) のように四則演算 $(+, -, \times, /)$ が自由に行える集合を体とよぶ。体論は代数方程式の研究に伴って発展・整備されてきたと考えられる。

代数方程式の研究とは、つまるところ方程式の係数と解の関係を調べることである。方程式の係数を含むじゅうぶん小さな体 K と方程式の解と係数を同時に含む十分小さな体 L を考えると、代数方程式の研究は、「係数と解の関係」といった素朴な視点から、「体 K とそれを含むより大きな体 L の関係」を調べることと捉え直される。この新たな視点で代数方程式を眺めることによって、初めて、代数方程式が「代数的に解ける」ことの意味が明確に理解され、さらには、5次以上の代数方程式には（2，3、4次方程式の場合とは違って）「解の公式」が存在し得ない本質的理由が明らかになる。

本講座のテーマは、包含関係にある2つの体 $K \subset L$ – これを拡大体という– の関係を詳細に研究することである。ここでの最大のアイディアは、フランスの数学者 Evariste Galois (1811–1832) によって発見された、体と群の対応関係（Galois 対応) である。これによって、拡大体の構造を群論を使って調べることが可能となる。

Galois のアイディアは、方程式論や代数学にとどまらず、現代数学の広い範囲に影響を与えている。また、ガロア理論そのものも、整数論や代数幾何学といった分野を中心に、現代でも盛んに研究が続けられている。

1. 有限次代数拡大

1.1. **体とその拡大体.** 体 L を研究する際、構造がよく知られているより単純な体 K がその一部に含まれていると議論がしやすくなることがある。つまり、$K \subset L$ となっている場合、K と L を比較し、L は K に比べてどれぐらい、あるいは、どのように複雑になっているかを調べるわけである。

定義 1 (拡大体)**.** *2*つの体 K, L が、$K \subset L$ のような包含関係にあって、

(1) K の積演算、加法演算は L のものが流用されている。
(2) 従って特に、K の 0 *(*加法の単位元*)*, 1 *(*乗法の単位元*)* は L の 0, 1 と同じもの、

であるとき、「L は K の**拡大体**」、「K は L の**部分体**」、「L/K は**拡大 (体)**」、「K は L の**部分体**」という。

例 2. $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ を考える。

(1) $\mathbb{C}$ は $\mathbb{R}$ に $\sqrt{-1}$ を「付け加えて」得られる拡大体。
(2) $\mathbb{R}$ は $\mathbb{Q}$ に、全ての無理数を「つけ加えて」得られる拡大体。

「付け加える」の正確な意味については、後に触れるであろう。

定義 3 (1 変数の多項式環)**.** K を体（または可換環）とし、不定元（変数）x を使って

$$K[x] = \left\{ \sum_{i=0}^{n} a_i x^n \mid a_i \in K,\ \mathbb{Z} \ni n \geq 0 \right\}$$

と定義される集合を K 上の**多項式環**と呼ぶ。これは K の要素を係数とする変数 x についての多項式全体の集合に他ならず、多項式同士の掛け算、加法、減法により、$k[x]$ は可換環になる。

例 4 (有理関数体)**.** K を体とし、不定元 *(*変数*)* x を使って L を以下のように定義する：

$$L = K(x) := \left\{ \frac{f(x)}{g(x)} \ :\ f(x), g(x) \in K[x],\ g(x) \neq 0 \right\}$$

とする。L は K に不定元 x を付け加えて得られる拡大体である。$K(x)$ を**有理関数体**と呼び、以下に述べる純超越拡大の典型例である。

定義 5 (代数的元と超越元)**.** 拡大体 L/K を考える。

(1) $a \in L$ が K 上**代数的**であるとは、適当な $f(x) \in K[x]$ が存在して、a が f の**零点**になっている、すなわち、$f(a) = 0$ になっている場合をいう。
(2) $a \in L$ が K 上代数的でないとき、a は K 上**超越的**であるという。
(3) L/K が**代数拡大**であるとは、L の全ての元が K 上代数的であることをいう。
(4) L の中に超越的な元が含まれている場合（$L - K$ の中に代数的元が含まれていてもよい)、L/K は**超越拡大**であるという。
(5) $K - K$ の元が全て超越的であるとき、L/K は**純超越拡大**であるという。

例 6 (代数的数)**.** 拡大体 $\mathbb{C}/\mathbb{Q}$ を考える。$\mathbb{Q}$ 上代数的な $\mathbb{C}$ の元は**代数的数**と呼ばれる。

- $a = \sqrt{-3} \in \mathbb{C}$ は $\mathbb{Q}$ 上代数的である。実際、a は $f = x^2 + 3 \in \mathbb{Q}[x]$ の零点である。

- $\zeta = \dfrac{-1+\sqrt{-3}}{2}$ は $\mathbb{Q}$ 上代数的である。実際、ζ は $f = x^2 + x + 1 \in \mathbb{Q}[x]$ の零点、つまり 1 の原始 3 乗根である。
- $a \in \mathbb{Q}$ ならば、a は $\mathbb{Q}$ 上代数的である。実際、a は $f = x - a \in \mathbb{Q}[x]$ の零点である。
- π (円周率) や、e (自然対数底) は、$\mathbb{Q}$ 上超越的である。このことの証明は難しい。一般にある複素数が $\mathbb{Q}$ 上超越的であることを証明するのは難しい。
- $\mathbb{C}$ には $\sqrt{-3}$ や 1 の原始 3 乗根など、$\mathbb{Q}$ 上代数的な元が沢山含まれているが、同時に π や e などの超越的な元も含まれている。従って、$\mathbb{C}/\mathbb{Q}$ は超越拡大であるが、純超越拡大ではない。

例 7 (純超越拡大体)**.** 有理関数体 $L = \mathbb{Q}(x)$ によって、拡大体 $L/\mathbb{Q}$ を考える。任意の元 $a \in L - \mathbb{Q}$ は、定数でない x についての有理関数。これは $\mathbb{Q}$ 上超越的である。実際、どんな $f \in \mathbb{Q}[x]$ を持ってきても、$f(a)$ は変数 x を含んだ有理式であることにかわりなく、決して $f(a) = 0$ にはならないからである。例えば、$a = \frac{x}{x^2+3}$, $f = 2x^3 + x - 1 \in \mathbb{Q}[x]$ とすると

$$f(a) = 2 \cdot \left(\frac{x}{x^2+3}\right)^3 + \frac{x}{x^2+3} - 1 \neq 0.$$

従って、$\mathbb{Q}(x)/\mathbb{Q}$ は純超越的である。ここで、右辺の $\neq 0$ は「x の式として 0 ではない」という意味であって、「x にどんな値を代入しても 0 にならない」という意味では**ない**ことに注意。

1.2. **拡大次数.** 拡大体 L/K について、K と L を比較する際、もっとも素朴な疑問のひとつは「L は K の何倍の大きさか？」であろう。それを測る尺度が拡大次数であり、それは拡大体が線形空間になっているという性質を使って定義される。

命題 8. 拡大体 L/K が与えられた時、L は K-線形空間である。

Proof. 線形空間の公理をチェックすればよい。すなわち、

加法群としての公理: $a, b \in L$ に対して、$a + b \in L$ なる加法演算が定義されていて、

(1) $(a + b) + c = a + (b + c)$
(2) $a + b = b + a$
(3) 任意の $a \in L$ に対して $a + 0 = 0 + a = a$ となる元 $0 \in L$ が存在する。
(4) 任意の $a \in L$ に対して、$-a \in L$ なる元が存在して、$a + (-a) = 0$.

スカラー倍についての公理: $\lambda, \mu \in K$, $a, b \in L$ とすると、

(1) $(\lambda\mu)a = \lambda(\mu a)$
(2) $1a = a$
(3) $\lambda(a + b) = \lambda a + \lambda b$
(4) $(\lambda + \mu)a = \lambda a + \mu a$

加法群としての公理は、L が体だから当然満たされる。また、スカラー倍についての公理も、L が K 拡大体だから、当然成り立つ。 □

定義 9 (中間体)**.** E/K, L/K が拡大（体）、すなわち $K \subset E \subset L$ のとき、E を拡大体 L/K の**中間体**と呼ぶ。

定義 10 (拡大次数)**.** 拡大体 L/K に対し、$[L:K] := \dim_K L$ と書き、L/K の **(拡大) 次数**と呼ぶ。$[L:K] < \infty$ *(*または、$= \infty$*)* のとき、L/K は**有限 (次) 拡大** *(*または、**無限 (次) 拡大***)* と呼ぶ、

例 11. 有理関数体による拡大 $\mathbb{Q}(x)/\mathbb{Q}$ に対して、$[\mathbb{Q}(x):\mathbb{Q}] = \infty$ である。実際、$\mathbb{Q}(x) \supset \mathbb{Q}[x] \supset \mathbb{Q}$ であるが、$\mathbb{Q}[x]$ は $\mathbb{Q}$ 上の無限次元ベクトル空間である（$\mathbb{Q}$ 上の $\mathbb{Q}[x]$ の線形基底は無限集合 $\{1, x, x^2, x^3, \dots, \}$ だから)。よって $\mathbb{Q}(x)$ もやはり $\mathbb{Q}$ 上の無限次元ベクトル空間。

命題 12. $[L:K] < \infty$ なる拡大体 L/K は、代数拡大である。

Proof. 実際、L に K 上超越的な元 $t \in L$ が含まれていれば、t はどんな多項式 $f \in K[x]$ の零点にもなっていないのだから、t は変数のように考えてもよい。つまり、

$$K[t] = \{f(t) \mid f(x) \in K[x]\}$$

は多項式環 $K[x]$ と同一視できる。そこで、

$$L \supset K[t] \supset K$$

より $[L:K] \geq \dim_K K[t] = \infty$ だから、$[L:K] = \infty$. □

命題 *12* の別証明. $[L:K] = n < \infty$ とし、任意の元 $\xi \in L$ をとる。すると、すくなくとも $\xi^0, \xi^1, \dots, \xi^n$ は K-線形従属のはずである。よって適合な元 $c_i \in K$ が存在して

$$c_0 + c_1\xi + \cdots + c_m\xi^m = 0 \quad (m \leq n, c_m \neq 0)$$

となる。従って、ξ は

$$f(x) = c_m x^m + c_{m-1}x^{m-1} + \cdots + c_0 \in K[x]$$

によって $f(\xi) = 0$ となるから、k 上代数的である。 □

注意 13 (無限次数代数拡大)**.** $[L:K] = \infty$ であっても、L/K は超越的であるとは限らず、無限次代数拡大というものが存在するが、本講ではそれいついては触れない。

命題 14. 拡大 $K \subset E \subset L$ に対して $[L:K] = [L:E] \cdot [E:K]$.

Proof. 有限次拡大の場合、L の E-線形基底を $\mathbf{a}_1, \dots, \mathbf{a}_m$, E の K-線形基底を $\mathbf{b}_1, \dots, \mathbf{b}_n$ とおくと、$\mathbf{a}_i\mathbf{b}_j$ $(1 \leq i \leq m, 1 \leq j \leq n)$ が L の K-線形基底になり、その個数は $m \cdot n$ となる。それを確かめるためには、以下のことを示せばよい。

(1) 任意の $a \in L$ が $a = \sum_{i,j} \alpha_{i,j}\mathbf{a}_i\mathbf{b}_j$, $\alpha_{ij} \in K$ の形に書き表せること。
(2) $0 = \sum_{i,j} \alpha_{i,j}\mathbf{a}_i\mathbf{b}_j$, $\alpha_{ij} \in K$, ならば全ての $\alpha_{ij} = 0$ であること。

(1) **の証明:** a を E 線形空間 L の要素と見ると、$a = \sum_{i=1}^m c_i\mathbf{a}_i$, $(\exists c_i \in E)$ と書き表せる。また、各 c_i は K 線形空間 E の要素だから、$c_i = \sum_{j=1}^n \alpha_{ij}\mathbf{b}_j$, $(\exists \alpha_{ij} \in K)$ と書き表せる。これらを纏めると、

$$a = \sum_{i=1}^m c_i\mathbf{a}_i = \sum_{i=1}^m (\sum_{j=1}^n \alpha_{ij}\mathbf{b}_j)\mathbf{a}_i = \sum_{i,j} \alpha_{ij}\mathbf{a}_i\mathbf{b}_j$$

(2) **の証明:** 上の式で $a=0$ とおいてみると、$\mathbf{a}_i$, $(i=1,\dots,m)$, が E 上一次独立だから、$\sum_j \alpha_{ij}\mathbf{b}_j = 0$, $(i=1,\dots,m)$, である。さらに。$\mathbf{b}_j$, $(j=1,\dots,n)$, が K 線形独立だから、$\alpha_{ij}=0$, $(i=1,\dots,m, j=1,\dots,n)$, となる。

L/E, L/K, E/K のいずれかが無限次拡大の場合、上の m, n のいずれかが ∞ の場合は、基底 $\mathbf{a}_i\mathbf{b}_j$ も無限個になるので、明らかに $[L:K]=[L:E]\cdot[E:K](=\infty)$ が成り立つ。また、$[L:K]=\infty$ のとき、$[L:E],[E:K]<\infty$ ならば、上の証明により $[L:K]<\infty$ となり矛盾。よって $[L,E]=\infty$ または $[E:K]=\infty$ でなければならず、この場合も $[L:K]=[L:E]\cdot[E:K](=\infty)$ が成り立つ。 □

1.3. **単純代数拡大.** ここでは、拡大体を構成するための基本的な方法 (Kronecker の方法) を示す。これは 1 変数の多項式環 $K[x]$ の極大イデアルによる剰余環という形で体を構成するものだが、後に出てくる、より複雑な拡大体の構成法やそれにまつわる考察の基礎となる重要なテクニックである。

1.3.1. 単純拡大.

定義 15 (単純拡大)**.** 体 K と K に含まれない元 a が与えられた時、集合 $K\cup\{a\}$ を含む最小の体を $K(a)$ と書き表す。すなわち、$K\cup\{a\}\subset L$ なる任意の体 L に対して、$K\subset K(a)\subset L$ となるような体が $K(a)$ である。これを K に a を付け加えて得られる**単純拡大（体）**と呼ぶ。

注意 16. 厳密に言えば、上の定義で「元 a」は一体どこから持ってきたのかを明示しないと意味をなさない。実際、単純代数拡大の場合は、a は後述する K の代数的閉包 $\overline{K}$ から取ってくる。しかしここでは、この問題をあまり気にしないことにする。

例 17 (単純超越拡大)**.** 任意の体 K に不定元（変数）x を付け加えて得られる単純拡大体は、（1 変数の）有理関数体 $K(x)$ にほかならない。

例 18 (単純代数拡大)**.** 有理数体 $\mathbb{Q}$ に $\sqrt{-2}\in\mathbb{C}$ を付け加えた単純拡大体 $\mathbb{Q}(\sqrt{-2})$ を求めてみよう。まず、$\mathbb{Q}(\sqrt{-2})$ は「$\mathbb{Q}$ と $\sqrt{-2}$ だけを使ってありとあらゆる四則演算を行った結果を全て集めたもの」にほかならないことに注意しよう。つまり、$a:=\sqrt{-2}$ としたとき、

$$(1)\quad \frac{c_0+c_1a+c_2a^2+\cdots+c_ma^m}{d_0+d_1a+d_2a^2+\cdots+c_na^n} \qquad (n,m\in\mathbb{N}, c_i,d_j\in K, 0\le i\le m,\ 0\le j\le n)$$

の形の元を全て集めたものが $\mathbb{Q}(\sqrt{-2})$ となる。ところが、

$$(\sqrt{-2})^2=-2\in\mathbb{Q}$$

だから、$0\le n,m\le 1$ でよいことがわかるので、(1) の式は、実は

$$\begin{aligned}\frac{c_0+c_1\sqrt{-2}}{d_0+d_1\sqrt{-2}} &= \frac{(c_0+c_1\sqrt{-2})(d_0-d_1\sqrt{-2})}{(d_0+d_1\sqrt{-2})(d_0-d_1\sqrt{-2})}\\ &= \frac{(c_0d_0+2c_1d_1)}{d_0^2+2d_1^2}+\frac{c_1d_0-c_0d_1}{d_0^2+2d_1^2}\cdot\sqrt{-2}\end{aligned}$$

で良いことがわかる。しかも、この表し方は一意的である（つまり $\alpha+\beta\sqrt{-2}=\gamma+\delta\sqrt{-2}$ ならば、$\alpha=\gamma$ かつ $\beta=\delta$ が成り立つ）。よって、$\mathbb{Q}(\sqrt{-2})$ の任意の元は $\alpha+\beta\sqrt{-2}$, *(*但し $\alpha,\beta\in\mathbb{Q}$*)* の形をしている。従って、

$$\mathbb{Q}(\sqrt{-2})=\mathbb{Q}\cdot 1\oplus\mathbb{Q}\cdot\sqrt{-2}=\{\alpha+\beta\sqrt{-2}\mid\alpha,\beta\in\mathbb{Q}\}$$

すなわち、$\mathbb{Q}$ は $\{1, \sqrt{-2}\}$ を基底とする 2 次元の $\mathbb{Q}$ 線形空間であることがわかり、$[\mathbb{Q}(\sqrt{-2}) : \mathbb{Q}] = 2$. 従って、命題 *12* より、$\mathbb{Q}(\sqrt{-2})/\mathbb{Q}$ は代数拡大である。

ここで、以下のことに注意したい。$a = \sqrt{-2}$ は $x^2 + 2 \in \mathbb{Q}[x]$ の零点だから、$\mathbb{Q}$ 上代数的数である。$\mathbb{Q}$ に代数的数 a を付け加えた単純拡大 $\mathbb{Q}(a)$ が代数的であることを示すには、$\mathbb{Q}(a)$ に含まれる $\mathbb{Q}$ や a 以外の元、つまり $\mathbb{Q}(a) - \mathbb{Q} \cup \{a\}$ に含まれる全ての元もやはり $\mathbb{Q}$ 代数的になることを保証しなければならない。これは決して自明な事実ではなく、命題 *12* のような議論を経てわかることなのである。

1.3.2. *Kronecker* の方法. ここでは、$\mathbb{Q}(\sqrt{-2})/\mathbb{Q}$ のような単純代数拡大の一般的な構成法を与えよう。ある拡大体 L/K が与えらていて、K 上に代数的な元 $a \in L$ があったとする。この時、K の代数的単純拡大体 $K(a)$ を構成しよう[1]。

Step 1: a は K 上代数的だから、適当な多項式 $f \in K[x]$ の零点になっている。しかし $x = a$ を零点にもつ多項式は沢山ある（例えば、上の f と任意の別の多項式 $g \in K[x]$ を掛けた $h := fg$ も当然 $x = a$ を零点にもつ。）そこで、$x = a$ を零点にもつ多項式全体の集合

$$\mathcal{I} = \{h \in K[x] \mid h(a) = 0\} \ (\subset K[x])$$

を考える。

Step 2: $\mathcal{I}$ に含まれている多項式の中で、もっとも次数の小さいものをとり、他の任意の多項式 $h \in \mathcal{I}$ に対して、f による割り算を考える：

$$h = q \cdot f + r \quad (\exists q, \exists r \in K[x])$$

ここで、r は余りだから、$\deg r < \deg f$. ここで $r \neq 0$ だとすると、$r = h - q \cdot f$ は $x = a$ を零点にもつ f より次数の小さい $\mathcal{I}$ の元になってしまい、f を次数最小にとったことに矛盾する。従って、$r = 0$ でなければならない。つまり、$\mathcal{I}$ の元は f の倍元[2]に他ならない。以上により、

$$\mathcal{I} = \{gf \mid g \in K[x]\}$$

であることがわかった。

注意 19. 上のことを環・体論 I で習った言葉で言えば、「$\mathcal{I}$ は単項イデアル整域 *(PID)*$K[x]$ の単項イデアルで、その生成元は f」. このことを記号で $\mathcal{I} = (f)$ と書き表す。

ここで、f については、$x = a$ を零点にもつかどうかだけに関心があるので、最高次数の係数を払って 1 としておいてもよい。

定義 20 (最小多項式)**.** 上のような f すなわち、$f(a) = 0$ となる最小次数の $K[x]$ の元で、x についての最高次数の係数が 1 のものを、a の K 上の**最小多項式**と呼ぶ。*(*一般に最高次数の係数が 1 である多項式のことを、**モニック**な多項式と呼ぶ。）

Step 3: ここで、以下のような可換環 $K[a]$ を考える

$$K[a] := \{c_n a^n + c_{n-1} a^{n-1} + \cdots + c_1 a + c_0 \mid n \in \mathbb{N},\ c_n, \ldots, c_n \in K\}$$

[1] この L としては、標準的には後に述べる K の代数的閉包 $\overline{K}$ を考える

[2] 多項式は「数」ではないので、倍数と呼ぶのは変なので、倍元と呼ぶ。

さらに可換環の準同型

$$\begin{array}{rccc} \varphi: & K[x] & \longrightarrow & K[a] \\ & x & \mapsto & a \end{array}$$

を考える。これは簡単な書き方をしているが、次のことを表している：可換環の準同型の定義により、$\varphi(f+g)=\varphi(f)+\varphi(g)$, $\varphi(f\cdot g)=\varphi(f)\cdot\varphi(g)$, $\varphi(1)=1$ が成り立つことから、

$$\begin{aligned} &\varphi(c_nx^n+c_{n-1}x^{n-1}+\cdots+x_1a+c_0) \\ &\quad = \quad c_na^n+c_{n-1}a^{n-1}+\cdots+c_1a+c_0 \quad (n\in\mathbb{N}, c_i\in K, i=0,\ldots,n). \end{aligned}$$

このことから、φ が全射であることは明らかである。

Step 4: さて、φ の核 $\operatorname{Ker}\varphi := \{h\in K[x] \mid \varphi(h)=0\}$ は $\mathcal{I}$ にほかならないこと ($h(a)=\varphi(h)=0$ だから) に注意すると、可換環の準同型定理[3]により

$$K[a]\cong K[x]/\operatorname{Ker}\varphi = K[x]/(f).$$

となる。剰余環 $K[x]/(f)$ の意味は次のように考えればよいであろう：「多項式全体の集合 $K[x]$ に対し、『f という式が現れたら、それらを全部 0 に置き換える』という新たなルールを導入した集合」。

例 21. $\mathbb{R}[x]/(x^2+1)$ なる剰余環は、実数係数の 1 変数多項式全体の集合 $\mathbb{R}[x]$ において、変数 x に対する関係式 "$x^2+1=0(\Leftrightarrow x^2=-1)$ をを付け加えた集合である。$x^2=-1$ ということは、要するに x を純虚数 $\sqrt{-1}$ と同じものとみなすということだから、結局 $\mathbb{R}[x]/(x^2+1)$ は複素数体 $\mathbb{C}$ を表している。それにしても、なぜ剰余「環」$\mathbb{R}[x]/(x^2+1)$ が、いつの間にか複素数「体」になってしまうのだろうか？それについては以下に一般原理を説明するが、要するに (x^2+1) が $\mathbb{R}[x]$ の極大イデアルだからである。

Step 5: Step 4 で得られた剰余環が、実は単なる可換環ではなく、体になっていることを示そう。それを示すことによって、

$$K(a)=K[a]\cong K[x]/(f)$$

であることが言えるわけである。さて、任意の $\ell\in K[x]$ に対し、f による割り算を行うと

$$\ell = q\cdot f+r \quad (q,r\in K[x],\ \deg r<\deg f)$$

となる。ここで、$r\neq 0$ だと仮定すると、$(r,f)=1$, すなわち r,f は共通因子を持たないことに注意しよう。

$(r,f)=1$ であることの証明: もし共通因子が $g=(r,f)\neq 1$ ならば、$f=hg$, $(h,g\in K[x]\ \deg h,\deg g<\deg f)$ の形に因数分解されてしまい、$f(a)=0$ だったから、$h(a)=0$ または $g(a)=0$ となってしまう。ところが、f は $f(a)=0$ となる最低次数の多項式だったから、これは矛盾する。したがって $(r,f)=1$ でなければならない。 □

[3]「可換環の全射準同型写像 $\varphi: A\longrightarrow B$ に対し、$B\cong A/\operatorname{Ker}\varphi$」を可換環の準同型定理とよぶ。

そこでユークリッドの互除法により

$$p \cdot r + q \cdot f = 1$$

となる $p, q \in K[x]$ が存在する。$K[x]/(f)$ の中では $f = 0$ と考えてよいことから、このことは $K[x]/(f)$ の中では

$$p \cdot r = 1 \quad (\text{if } \ell \neq 0)$$

となっていることを意味する ($K[x]/(f)$ の中では、$\ell = q \cdot f + r = q \cdot 0 + r = r$ となるから、$\ell \neq 0$ は $r \neq 0$ という仮定と同値であることに注意)。すなわち、$K[x]/(f)$ の中の 0 でない任意の元 ℓ に対して、その乗法逆元 ℓ^{-1} が $K[x]/(f)$ の中に存在する。言い換えれば、$K[x]/(f)$ が体ということである。

以上の結果をまとめておこう。

定理 22 (Kronecker の方法)**.** 拡大 L/K において、K 上代数的な任意の元 $a \in L$ が存在したとする。このとき、

(*i*) a の K 上の最小多項式を $f \in K[x]$ とすると、

$$K(a) \cong K[x]/(f)$$

(*ii*) 最小多項式 f は $\mathcal{I} = \{h \in K[x] \mid h(a) = 0\}$ となる $K[x]$ の部分集合の中で、最も次数が低い多項式の最高次数係数を払ってモニックにしたものに等しく、K 上既約な多項式である。

以下の結果は、さまざまな拡大体の拡大次数を計算する際の基礎である。

定理 23. 拡大 L/K において、K 上代数的な元 $a \in L$ が存在したとする。このとき、

$$[K(a) : K] = \deg f$$

ただし、f は a の K 上の最小多項式。従って、特に $K(a)/K$ は有限次拡大である。

Proof. $K(a)$ は a に関する K 係数の有理式

$$\frac{g(a)}{h(a)} \qquad \text{ただし} \quad g(x), h(x) \in K[x].$$

全体の集合である。f が既約であることから、$(f, h) = 1$ となり、ユークリッドの互除法により、$p \cdot f + q \cdot h = 1$ となる $p, q \in K[x]$ が存在するが、$f(a) = 0$ だから、$x = a$ を代入すると、$q(a) \cdot h(a) = 1$ となる。すなわち、$q(a) = \frac{1}{h(a)}$. さらに、

$$f(a) = a^n + c_1 a^{n-1} + \cdots c_n = 0 \quad (c_i \in K)$$

の形をしているので、a^m $(m \geq n)$ の形の式は、全て da^m $(m < n, d \in K)$ の形の式の和におきかえることができる。従って、$K(\alpha)$ の任意の元は

$$c_0 + c_1 a + \cdots + c_{n-1} a^{n-1} \quad (c_i \in K)$$

の形である。また、この表現の一意性も $n = \deg f$ であることからわかる。よって、$1, a, \ldots, a^{n-1}$ が $K(a)$ の K-線形基底であり、従って $[K(a) : K] = n = \deg f$ である。 □

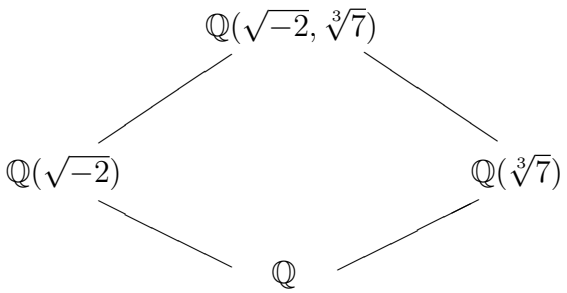
1.3.3. 一般の拡大体. 一般の拡大体は単純拡大を繰り返して構成される。すなわち、拡大体 $K(a_1,\dots,a_n)/K$ は、たとえば単純拡大の列

$$\begin{aligned} K(a_1) & \\ K(a_1,a_2) &:= L_1(a_2) \quad (\text{但し } L_1 := K(a_1)) \\ & \cdots \\ K(a_1,\dots,a_{n-1},a_n) &:= L_{n-1}(a_n) \quad (\text{但し } L_{n-1} = K(a_1,\dots,a_{n-1})) \end{aligned}$$

によって構成される。

また、K に無限個の元 $a_1,\dots,a_n,\dots$ を付け加えた拡大体 $K(a_1,\dots,a_n,\dots)$ も考えることができて、これも単純拡大を無限回繰り返して得られるものと定義される。

例 24. $\mathbb{Q}(\sqrt{-2},\sqrt[3]{7})/\mathbb{Q}$ は以下の図示するように 2 通りの方法で構成できる：



ここで、$\mathbb{Q}(\sqrt{-2})$ 上 $\sqrt[3]{7}$ の最小多項式は $x^3-7 \in \mathbb{Q}(\sqrt{-2})[x]$ であり、従って定理 *23* より $[\mathbb{Q}(\sqrt{-2},\sqrt[3]{7}):\mathbb{Q}(\sqrt{-2})] = \deg(x^3-7) = 3$ である。また、$\mathbb{Q}(\sqrt[3]{7})$ 上 $\sqrt{-2}$ の最小多項式は $x^2+2 \in \mathbb{Q}(\sqrt[3]{7})[x]$ であり、ふたたび定理 *23* より $[\mathbb{Q}(\sqrt{-2}),\sqrt[3]{7}] = \deg(x^2+2) = 2$ である。そこで、命題 *14* より

$$\begin{aligned} [\mathbb{Q}(\sqrt{-2},\sqrt[3]{7}):\mathbb{Q}] &= [\mathbb{Q}(\sqrt{-2},\sqrt[3]{7}):\mathbb{Q}(\sqrt{-2})]\cdot[\mathbb{Q}(\sqrt{-2}):\mathbb{Q}] = 3\cdot 2 \\ \text{あるいは} & \\ &= [\mathbb{Q}(\sqrt{-2},\sqrt[3]{7}):\mathbb{Q}(\sqrt[3]{7})]\cdot[\mathbb{Q}(\sqrt[3]{7}):\mathbb{Q}] = 2\cdot 3 \\ &= 6. \end{aligned}$$

命題 12 と定理 23 により、K に (K 上) 代数的な元 a を付け加えた単純拡大 $K(a)/K$ は代数拡大である。すなわち、$K(a)$ の a 以外の元も全て K 上代数的である。ここでは、このことの拡張として、以下の事実を証明する。

定理 25. 拡大体 L/K, $L := K(a_1,\dots,a_n,\dots)$, において、$a_1,\dots,a_n,\dots$ (無限個でもよい) が全て K 上に代数的ならば、L/K は代数拡大である。

この定理の意味するところは、$a_1,\dots,a_n,\dots$ が K 上代数的ならば、それらと K の要素をつかった四則演算の結果得られる要素もまた K 上代数的だということである。

Proof. まずは有限生成拡大、つまり $L = K(a_1, \ldots, a_n)$ で、全ての a_i が K 上代数的な場合について、L/K が有限次代数拡大になることを n に関する数学的帰納法で証明する。$n = 1$ の場合は上で述べたとおりである。次に、単純拡大 $L = M(a_n)/M$, $M := K(a_1, \ldots, a_{n-1})$, を考える。$a_n$ は K 上で代数的だから、勿論 K の拡大体である M 上でも代数的である。従って $n = 1$ の場合を使って L/M は有限次代数拡大であることがわかり、さらに $a_n \in L$ の M 上の最小多項式を $g \in M[x]$ とすると、$[L : M] = \deg g < \infty$ である（定理 23)。また、帰納法の仮定により、M/K も有限次代数拡大である: $[M : K] < \infty$。従って命題 14 より $[L : K] = [L : M][M : K] < \infty$ となるから、命題 12 より L/K は有限次代数拡大とわかる。

次に無限生成の拡大体 $L = K(a_1, \ldots, a_n, \ldots)$ を考えよう。これは K の有限生成代数拡大体の無限和

$$L = \bigcup_{n=1}^{\infty} K(a_1, \ldots, a_n)$$

であるから、任意の要素 $a \in L$ に対して、適当な $n \in \mathbb{N}$ を選べば $a \in K(a_1, \ldots, a_n)$ となっており、従って a は K 上に代数的。つまり L の任意の要素が K 上代数的だから、L/K は代数拡大である。 □

最後に、代数拡大を繰り返せば、元の体の代数拡大になることを示そう。

命題 26. 拡大体の列 $K \subset L \subset M$ を考える。M/L, L/K が代数拡大ならば、M/K もまた代数拡大である。

Proof. 命題の仮定のもとで、任意の元 $a \in M$ が K 上代数的であることを示せばよい。$a \in M$ は L 上代数的だから、その最小多項式 $f = X^m + a_1 X^{m-1} + \cdots a_{m-1} X + a_m \in L[X]$ が存在する。そこで、$L' := K(a_1, \ldots, a_m)$ を考えると、L/K が代数拡大ゆえ $a_1, \ldots, a_m$ は K 上代数的だから、L'/K は有限代数拡大である。また単純拡大 $L'(a)/L'$ を考えると、これもまた有限代数拡大。よって $[L'(a) : K] = [L'(a) : L'][L' : K]$ は有限で、結局 $L'(a)/K$ は有限次拡大 (命題 12)。よって特に代数拡大。そして $a \in L'(a)$ だから、a は K 上代数的になる。 □

まとめ

- 拡大体（代数拡大、超越拡大）
- 拡大体は線形空間である。
- 最小多項式
- 拡大次数
- Kronecker の方法による単純代数拡大の構成

2. 体の標数と有限体

体を特徴づける重要な数値として「標数」を定義する。これは 0 または正の整数（実は素数）で、正標数の体は素数の深い性質とかかわる興味深い研究対象である。

2.1. 体の標数.

定義 27 (標数)**.** 体 K に対して、

$$\underbrace{1+\cdots+1}_{n}=0$$

となるような $n\in\mathbb{N}$ が存在するならば、$\mathrm{char}(K):=\min\{n\in\mathbb{N}\mid \underbrace{1+\cdots+1}_{n}=0\}$,

そのような $n\in\mathbb{N}$ が存在しない（つまり 1 を何回加えても決して 0 にならない）場合は、$\mathrm{char}(K)=0$ と定義し、$\mathrm{char}(K)(\geq 0)$ を体 K の**標数**と呼ぶ。

命題 28. $\mathrm{char}(K)>0$ ならば $\mathrm{char}(K)$ は素数である。

Proof. $\mathrm{char}(K)=n>0$ が合成数だと仮定して、$n=s\cdot t$ $(s,t\geq 2)$ とおく。すると

$$\underbrace{(1+\cdots+1)}_{s}\cdot\underbrace{(1+\cdots+1)}_{t}=\underbrace{1+\cdots+1}_{s\cdot t}=0.$$

ここで $s=\underbrace{(1+\cdots+1)}_{s}$ も $t=\underbrace{(1+\cdots+1)}_{t}$ も K の要素で、体は整域[4]だから、s か t のいずれかが 0 でなければならない。仮に $s=0$ だとして、s が合成数だとすれば、因数分解 $s=q\cdot r$ をして同様に考えていくと、結局標数は素数でなければならないことがわかる。 □

例 29. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ は全て標数 0 の体である。

例 30. 体 $\mathbb{F}_p:=\mathbb{Z}/p\mathbb{Z}=\{\overline{0},\overline{1},\ldots,\overline{p-1}\}$ の和と積は

$$\overline{x}+\overline{y}=\overline{x+y},\qquad \overline{x}\cdot\overline{y}=\overline{x\cdot y}$$

と定義される。ここで $\overline{x}=\overline{y}$ であることは、$x-y$ が p の倍数であることと同値。$\mathbb{F}_p$ は上のように定義された和と積によって可換環となるが、さらに体となるのは以下の理由による。すなわち、任意の $\overline{x}(\neq\overline{0})$ に対し、$(x,p)=1$　すなわち、p と x は互いに素だから、ユークリッドの互除法定理により $sx+tp=(x,p)=1$ となるような $s,y\in\mathbb{Z}$ が存在する。すると、

$$\overline{1}=\overline{sx+tp}=\overline{sx}+\overline{tp}=\overline{s}\cdot\overline{x}.$$

よって、$\overline{s}$ は $\mathbb{F}_p$ における $\overline{x}$ の乗法逆元。$\overline{0}$ 以外の任意の元が逆元を持つのだから、$\mathbb{F}_p$ は体である。また特に、

$$\underbrace{\overline{1}+\cdots+\overline{1}}_{p}=\overline{\underbrace{1+\cdots+1}_{p}}=\overline{p}=\overline{0}$$

となるから、$\mathbb{Z}/p\mathbb{Z}$ の標数は p となる。

[4]可換環 R が**整域**であるとは、任意の $a,b\in R$ に対して、「$a\cdot b=0$ ならば $a=0$ または $b=0$」が成り立つ場合をいう。体は可換環の特殊な場合であり、しかも整域になっていることに注意。

定義 31 (素体)**.** $p \in \mathbb{N}$ を 0 または素数であるとするとき、$\mathrm{char}(K) = p$ となるもっとも小さい体 K のことを、標数 p の**素体**と呼ぶ。

命題 32. 標数 0 の素体は有理数体 $\mathbb{Q}$ である。また、標数 $p(>0)$ の素体は $\mathbb{F}_p$ である。

Proof. 任意の体 K を考える。体は必ず 0 と 1 を含むので、$\mathrm{char}(K) = 0$ の場合は $\mathbb{Z}$ とその乗法逆元は必ず含まれる。つまり $\mathbb{Q} \subset K$ である。だから $\mathbb{Q}$ が最も小さい体である。

同様に考えて、$\mathrm{char}(K) = p$ (素数) の場合、K は少なくとも

$$0,\ 1,\ 2(=1+1),\ 3(=1+1+1), \ldots,\ p-1(=\underbrace{1+\cdots+1}_{p-1})$$

を含む。これらは乗法逆元も既に含んでいる。つまり、$\mathbb{Z}/p\mathbb{Z} \subset K$ である。だから、$\mathbb{Z}/p\mathbb{Z}$ が標数 p のもっとも小さい体である。 □

2.2. **有限体.** $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ などは、無限個の要素を持つため、**無限体**と呼ばれることがあるが、要素の数が有限個の体は、とくに**有限体**と呼ばれる。有限体の代表例は素体 $\mathbb{F}_p$ (p は素数) だが、それ以外の有限体がどのようなものかを考えよう。まず、以下の事実に注意する。

命題 33. 有限体の標数は素数である。

Proof. 素体を考える。もし $\mathrm{char}(K) = 0$ ならば、$\mathbb{Q} \subset K$ となるはずで、K は無限体になってしまう。これは矛盾。 □

定理 34. 任意の有限体 K に対して、

$$\sharp(K) = p^n \qquad (\exists n \geq 1)$$

ただし、$\mathrm{char}(K) = p > 0$ とする。

Proof. K は素体 $\mathbb{F}_p$ を部分体として持つ。従って命題 8 より、K は $\mathbb{F}_p$ 線形空間。とくに $\sharp(K) < 0$ だから $n := \dim_{\mathbb{F}_p} K = [K : \mathbb{F}_p] < \infty$:

$$K = \underbrace{\mathbb{F}_p \oplus \cdots \oplus \mathbb{F}_p}_{n}$$

つまり、K の各要素は $(x_1, \ldots, x_n)$, $x_i \in \mathbb{F}_p$ $(i = 1, \ldots, n)$ なる形に一意的に書き表され、また、逆にこのような形で書き表せるものは全て K の要素である。よって、$\sharp(K) = \sharp(\mathbb{F}_p)^n = p^n$ となる。 □

2.3. **Frobenius 写像.** 正標数の体に特徴的な現象として Frobenius 写像が重要である。体 K と素数 p に対して写像

$$\begin{array}{rccc} F: & K & \longrightarrow & K \\ & x & \longmapsto & x^p \end{array}$$

を考える。すると

$$F(x \cdot y) = (x \cdot y)^p = x^p \cdot y^p = F(x) \cdot F(y)$$

だから、F は積を保存する写像である。ところが和については、二項定理により、

$$\begin{aligned} F(x+y) &= (x+y)^p = \sum_{k=0}^{p} \binom{p}{i} x^{p-i} y^y \\ &= x^p + p \cdot x^{p-1} y + \cdots + p \cdot x \cdot y^{p-1} + y^p \\ &= F(x) + \underline{p \cdot x^{p-1} y + \cdots + p \cdot x \cdot y^{p-1}} + F(y) \end{aligned}$$

となる。つまり、一般に F は和を保存しない。ところがもし $\mathrm{char}(K) = p > 0$ ならば、上の下線の部分が 0 になって $F(x+y) = F(x) + F(y)$ となる。これは次章で述べる用語を使えば、「F は $\mathrm{char}(K) = 0$ の時に限って、体の準同型」になるということである。このような写像 F を **Frobenius 写像**と呼ぶ。本講座では今後 Frobenius 写像を使うことはないが、正標数の体を扱う際に以下の計算は暗黙のうちに頻繁に用いる：

命題 35. $\mathrm{char}(K) = p > 0$ なる体の任意の元 $a, b \in K$ に対し、$(a+b)^p = a^p + b^p$.

有限体の構造については、9 章でさらに詳しく述べることにする。

まとめ

- 体の標数は 0 または素数
- 素体は $\mathbb{Q}$ または $\mathbb{F}_p$ (p は素数)
- 有限体の標数は素数 p で、要素の数は p のべき。
- 正標数の体の Frobenius 写像

3. 代数閉体と代数的閉包

例えば単純代数拡大 $K(a)/K$ を作りには、まず K 上代数的な元 a を持ってきて、それを K に付け加える。では、元 a は一体どこから持ってくるのだろうか？その答えは K の代数的閉包 $\overline{K}$ である。自分自身が既に代数的閉包になっている体のことを代数閉体と呼ぶ。代数学の基本定理により、複素数体は代数閉体の典型例だが、それ以外にも任意の体の代数的閉包は代数閉体である。

3.1. 代数閉体とその特徴づけ.

定義 36 (代数閉体)**.** 体 K が**代数閉体**であるとは、定数でない任意の多項式 $f \in K[X]$ に対して、f の零点（方程式 $f = 0$ の解）のひとつが K の中に存在する場合をいう。

方程式の解の存在性の観点から、代数閉体は以下のように特徴づけることができる。つまり、任意の多項式 $f \in K[X]$ の「1つ」の零点が K に含まれることと、f の「すべて」の零点が K に含まれることは、同じことだというわけである。

命題 37. 体 K にたいして、以下は同値。
- (i) K は代数閉体
- (ii) 任意の多項式 $f \in K[X]$ は、$f = c(X-\alpha_1)\cdots(X-\alpha_n)$, $c, \alpha_1, \ldots, \alpha_n \in K$, のように、一次式の積に分解される。

命題 37 を証明するために、以下に示す因数定理を準備する。

定理 38 (因数定理)**.** 体 K 上の多項式 $f \in K[X]$ を考える。ある $\alpha \in K$ に対して $f(\alpha) = 0$ ならば、適当な $g \in K[X]$ によって $f = (X-\alpha)g$ と因数分解する。

Proof. f を $X-\alpha$ で割った商を g, 余りを r とする：

$$f = g(X-\alpha) + r$$

ここで $\deg r < \deg(X-\alpha) = 1$ だから $r \in K$. 仮定より $f(\alpha) = 0$ だから、上の割り算の式に $X = \alpha$ を代入すると $0 = f(\alpha) = g(\alpha)(\alpha-\alpha) + r$. 従って、$f = g(X-\alpha)$ を得る。 □

命題 *37* の証明. $(i) \Rightarrow (ii)$: f の零点のひとつが $a \in K$ だとすると、因数定理 38 により $f = (X-a)g$ となる $g \in K[X]$ が存在する。もし、g が定数でなければ、$g \in K[X]$ に K が代数閉体であることを適用すれば、g も K の中にすくなくとも1つ零点をもつことになる。同様の議論を繰り返せば、K が代数閉体であれば、$f = c(X-a_1)(X-a_2)\cdots(X-a_n)$ $a_1, \ldots, a_n \in K$ の形に分解することがわかる。
$(ii) \Rightarrow (i)$ は明らか。 □

拡大体の観点から見れば、代数閉体は以下のようにも特徴づけることができる。つまり、代数閉体とは、もうこれ以上代数拡大ができない体と考えてよい。

命題 39. 体 K が代数閉体であることの必要十分条件は、任意の代数拡大 L/K に対して $L = K$ となることである。

Proof. K が代数閉体と仮定して、任意の代数拡大 L/K を考える。任意の $a \in L$ とその K 上の最小多項式 $f \in K[X]$ を考える。K が代数閉体だから命題 37 より、$f = c(X - a_1) \cdots (X - a_n)$ $c, a_1, \ldots, a_n \in K$ のように $K[X]$ の一次式に分解する。f の零点 a は $a_1, \ldots, a_n$ のうちのいずれかだから、$a \in K$ となり、結局 $K = L$ である。

逆に、K が真に大きい代数拡大体を持たないと仮定する。$f \in K[X], \deg f \geq 1$ を任意に選び、クロネッカーの方法により、必要なら f を既約因子に取り変えて、K の代数拡大体 $L = K[X]/(f)$ を作ると、$L \cong K(a), (f(a) = 0\ \exists a \in L)$ となるから、L の中に f の零点がすくなくとも 1 個存在する。ところが仮定より、$K = L$ だから、その零点は K からとれることになる。従って、K は代数閉体である。 □

3.2. **代数的閉包の存在.** 以下の定理は、任意の体 K が与えられた時、その代数拡大をどんどんとって行けば、最後には必ず代数閉体が得られると主張している。証明は Kronecker の方法を無限回適用して行われるが、やや難しく、この証明を読み飛ばしても、以後の内容の理解には差し支えない。

定理 40. 任意の体 K に対して、適当な代数閉体 $\overline{K}$ が存在して、$\overline{K}/K$ が代数拡大になっている。

Proof. 証明のアイディアは以下の通り：体 K の拡大体は、K 上の多項式環 $R = K[X_1, X_2, \ldots]$ の極大イデアル $\mathfrak{m}$ を選んで剰余環 $R/\mathfrak{m}$ を作ることによって得られる [クロネッカーの方法]。このとき、$\mathfrak{m}$ は極大イデアルだから $L := R/\mathfrak{m}$ は（K を含む）体になることに注意。ここで多項式環は無限変数でも構わない。この方法を（無限回）繰り返すことにより、代数閉体がつくれる。

Step 1: 定数でない K 上の多項式全体の（無限）集合

$$S_+ = \{f \in K[X] | \deg f \geq 1\} (= K[X] - K)$$

を考える。各 $f(X) \in S_+$ の根のひとつ、つまり K 上代数的な元 $X = \alpha_f$, s.t. $f(\alpha) = 0$ を選び、$\{\alpha_f\}_{f \in I}$ を全て K に付け加えた体 $K(\{\alpha_f\}_{f \in I})$ をクロネッカーの方法によって構成しよう。そのための便宜上、各 $f(X) \in S_+$ の変数は他の S_+ の元で使われている変数とは別のものとして扱うために、X を X_f という変数に取り変え、そうやってして得られた新しい多項式 $f(X_f)$ を無限変数の多項式環 $K[\mathfrak{X}], \mathfrak{X} = (X_f)_{f \in I}$ の要素だと考える。[5]

Step 2: 変数名を取り変えたあとの S_+ を $\mathcal{S}_+$ と書くことにする。

$$\mathcal{S}_+ = \{f(X_f) \in K[\mathfrak{X}] \mid f \in S_+\}$$

この $\mathcal{S}_+$ 生成された $K[\mathfrak{X}]$ のイデアルを I とおく：

$$I = (f(X_f) \mid f \in \mathcal{S}_+) \quad (\subset K[\mathfrak{X}]).$$

[5] このテキストでは多項式は"$f \in K[X]$" のように標記して、$f(X)$ のような書き方はしないが、今はどの変数で考えるかを強調するために、$f(X)$ とか $f(X_f)$ といった標記を使っている。

この時、$I \neq K[\mathfrak{X}]$ となることを示そう。実際、もし $I = K[\mathfrak{X}]$ ならば

$$\sum_{i=1}^{n} g_i \cdot f_i(X_{f_i}) = 1$$

となるような $f_1(X_{f_1}), \ldots, f_n(X_{f_n}) \in \mathcal{S}_+$, $g_1, \ldots, g_n \in K[\mathcal{X}]$ が存在する。ここで各 $f_j(X_{f_j})$ には変数 X_{f_j} しか現れないが、g_j にはそういう制約はない。しかし、ここで出てくる各 $f_i \in \mathcal{S}_+$ に対し、クロネッカーの方法を使えば (必要なら f_i をその既約因子にとりかえて)、K の拡大体 $K_i := K[X_f]/(f_i(X_f))$ の中に $f_i(\alpha_i) = 0$ となるような $\alpha_i \in K_f$ が存在する。そこで、$X_{f_i} = \alpha_i$, $(i = 1, \ldots, n)$ といっせいに代入してやれば、上式左辺は (拡大体 $K(\alpha_1, \ldots, \alpha_n)$ の中で)0 になってしまう。したがって上式のような恒等式はなりたたない。従って、$I \neq K[\mathfrak{X}]$ でなければならないとわかる。

Step 3: Step 2 の結果より、$I \neq K[\mathfrak{X}]$ だから、極大イデアルの一般論により、

$$I \subset \mathfrak{m} \subset K[\mathfrak{X}]$$

となる極大イデアル $\mathfrak{m}$ が存在する。そこで、その剰余環として得られる K の拡大体を L_1 とする：

$$K \subset L_1 = K[\mathfrak{X}]/\mathfrak{m}.$$

こうやって得られた L_1 は $\mathcal{S}_+$ に含まれる全ての多項式 $f(X_f)$ に対して、その零点のひとつを含んでいる。それは何故かというと、$\mathcal{S}_+ \subset I \subset \mathfrak{m}$ だから、自然準同型

$$\psi : K[\mathfrak{X}] \longrightarrow L_1 = K[\mathfrak{X}]/\mathfrak{m}$$

による任意の $K[\mathfrak{X}] \supset \mathcal{S}_+ \ni f(X_f)$ の像は 0 となるので、

$$f(\psi(X_f)) = \psi(f(X_f)) = 0$$

となり、従って $K[\mathfrak{X}] \ni X_f$ の像を $\alpha_f \in L_1$ と書くと、L_1 は $f(X_f)$ の零点のひとつである α_f を含んでいることになる。そして、

$$L_1 = K[\mathfrak{X}]/\mathfrak{m} = K[\{\alpha_f\}_{f \in \mathcal{S}_+}]$$

と書けることから、結局 L_1 は S_+ に含まれる全ての多項式 $f(X)$ からその零点の 1 つを選びだし、それらを全部付け加えて得られる拡大体であることがわかる。

Step 4: Step 1, 2, 3 の構成を K のかわりに L_1 に対して行うことにより、拡大体 L_2/L_1 を得る。同様の操作を繰り返せば、拡大体の列

$$K = L_0 \subset L_1 \subset L_2 \subset \cdots$$

で、各 $f \in L_n[X]$, $\deg f \geq 1$, は L_{n+1} の中に少なくとも 1 個の零点を持つようなものが得られる。この列は無限列かもしれない。そこで

$$L = \bigcup_{n=0}^{\infty} L_n$$

と置く。

Step 5: L が代数閉体であることを示そう。任意の $f(X) \in L[X]$, $\deg f \geq 1$, を選ぶ。$f(X)$ に現れる係数は高々有限個だから、増加列 $\{L_n\}_{n\in\mathbb{N}}$ の中のいずれかの L_n に全て含まれている。つまり、$f(X) \in L_n[X]$ である。従って、L_{n+1} の中に、従って L の中に、少なくとも 1 つは $f(X)$ の零点が存在する。よって L は代数閉体である。

Step 6: 最後に、L/K が代数拡大であることを示そう。任意の $\alpha \in L$ に対して、適当な $n \in \mathbb{N}$ に対して $\alpha \in L_n$. 各 L_{i+1}/L_i は代数拡大だから、それを有限回繰り返した L_n/K もまた代数拡大である。従って、α は K 上代数的。よって L は K 上代数的である。

□

定義 41 (代数的閉包)**.** 任意の体 K にたいして、定理 *40* のような $\overline{K}$ を K の代数的閉包という。

3.3. **代数的閉包の一意性.** 体 K の代数的閉包 $\overline{K}$ は複数存在しうるが、それらは全て K 同型と呼ばれる写像で結ばれる。その意味で（つまり「K 同型なものは同一視する」とい立場で）代数的閉包が一意的であることを示すのが、ここでの目標である。

まずは K 同型の定義から始める。

定義 42 (体の準同型)**.** 2 つの体 K, L の間の写像 $\varphi : K \longrightarrow L$ が**準同型**とは、環としての準同型をいう。すなわち、任意の $a, b \in K$ に対して

(1) $\varphi(a+b) = \varphi(a) + \varphi(b)$ [和の保存]
(2) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ [積の保存]
(3) $\varphi(1_K) = 1_L$ [乗法単位元の保存]

を満たすものをいう。和の保存性から、加法単位元の保存も従うことに注意（実際 $f(0) = f(0+0) = f(0) + f(0)$ だから）。

命題 43. 体の間の準同型写像はつねに単射である。

Proof. $\varphi : K \longrightarrow L$ が体の準同型だとすると、$\operatorname{Ker}\varphi (= \{x \in K \mid \varphi(x) = 0\}) \subset K$ はイデアルだから、$\operatorname{Ker}\varphi = \{0\}$ または K [6]. もし $\operatorname{Ker}\varphi = K$ ならば、$1_L = \varphi(1_K) = 0$ となり、矛盾。 □

定義 44 (K 同型)**.** 体 K の 2 つの拡大体 L_1, L_2 の間の準同型写像 $\varphi : L_1 \longrightarrow L_2$ が K **準同型**であるとは、任意の $a \in K$ に対して $\varphi(a) = a$ となることを言う。従って特に、$\varphi(\sum_{i=1}^n c_i x_i) = \sum_{i=1}^n \varphi(c_i)\varphi(x_i) = \sum_{i=1}^n c_i \varphi(x_i)$ *($c_i \in K$, $x_i \in L_1$, $i = 1, \ldots, n$)*, すなわち、φ は K 線形写像であることに注意。また、φ が K **同型**であるとは、φ が全射である場合をいう。命題 *43* により K 同型は全単射であることに注意。

次の概念は後に Galois 群を考える際に重要になる。

定義 45 (K 自己同型)**.** 拡大体 L/K に対し、K 同型 $\sigma : L \longrightarrow L$ のことを L **の** K **上の自己同型** *(*または L の K 自己同型）と呼ぶ。また、記号として以下のものを定義しておく：

$$\operatorname{Aut}_K(L) := \{\sigma; \mid \sigma : L \longrightarrow L \ K \text{ 自己同型 }\}$$

[6]「体のイデアルは 0 または全体になる」は、環論の簡単な演習問題。

定義 46 (記号 f^σ)**.** 体の準同型 $\sigma : K \longrightarrow L$ と多項式 $f = \sum_{i=0}^{n} a_i X^i \in K[X]$ に対して、$f^\sigma = \sum_{i=0}^{n} \sigma(a_i) X^i \in L[X]$ と書き表すことにする。

代数拡大 K'/K を研究する際、K をまず適当な代数閉体 L に埋め込む写像 $\sigma : K \to L$ を考え、σ を $L \to \overline{K}$ まで拡張することをよく考える。

例 47. 拡大体 $\mathbb{C}/\mathbb{Q}$ において、$a = \sqrt[3]{-2} \in \mathbb{C}$ を使って $\mathbb{Q}$ の単純拡大体 $\mathbb{Q}(a)/\mathbb{Q}$ を考える。a の $\mathbb{Q}$ 上の最小多項式は $f = X^3 + 2 \in \mathbb{Q}[X]$. 従って、*Kronecker* の方法 *(*定理 *22)* によって

$$\begin{aligned}
&\mathbb{Q}[X]/(X^3+2)\\
&= \{c_0 + c_1 x + c_2 x^2 \mid c_1, c_2, c_3 \in \mathbb{Q}\}\\
&\quad \text{ただし } x \text{ は自然準同型 } \mathbb{Q}[X] \to \mathbb{Q}[X]/(X^3+2) \text{ による } X \in \mathbb{Q}[X] \text{ の像}\\
&\cong \{c_0 + c_1 a + c_2 a^2 \mid c_1, c_2, c_3 \in \mathbb{Q}\}\\
&\quad \text{同型} \cong \text{は } x \leftrightarrow a \text{ の対応による。}\\
&= \{c_0 + c_1 \sqrt[3]{-2} + c_2 (\sqrt[3]{-2})^2 \mid c_1, c_2, c_3 \in \mathbb{Q}\} = \mathbb{Q}(a)
\end{aligned}$$

特に、$[\mathbb{Q}(a) : \mathbb{Q}] = \deg f = 3$ で *(*定理 *23)*、その $\mathbb{Q}$ 線形基底は $1, \sqrt[3]{-2}, (\sqrt[3]{-2})^2$ である。さて、最小多項式を $\mathbb{C}[X]$ の中で因数分解すると

$$f = X^3 + 2 = (X - \sqrt[3]{-2})(X - \zeta\sqrt[3]{-2})(X - \zeta^2\sqrt[3]{-2}) \qquad \left(\text{但し} \quad \zeta = \frac{-1+\sqrt{-3}}{2}\right)$$

となる。$\zeta\sqrt[3]{-2}$ も $\zeta^2\sqrt[3]{-2}$ も $\sqrt{-3}$ を含んでいるため、$c_0 + c_1\sqrt[3]{-2} + c_2(\sqrt[3]{-2})^2$ *(*$c_1, c_2, c_3 \in \mathbb{Q}$*)* の形には表せない。すなわち、$\mathbb{Q}(a)$ は f の $a = \sqrt[3]{-2}$ 以外の零点は含まない。しかし、$L := \mathbb{Q}(a, \sqrt{-3})$ とすると、f は $L[X]$ の中で上のように一次式の積に因数分解する。そこで $M := \mathbb{Q}(a)$ とおくと、命題 *14* より

$$[L : \mathbb{Q}] = [M(\sqrt{-3}) : M][M : \mathbb{Q}] = 2 \cdot 3 = 6$$

となり、$L/\mathbb{Q}$ は 6 次の代数拡大である。この L は「f の最小分解体」と呼ばれるもので、次章で詳しく述べる。

例 48. 拡大体 $\mathbb{Q}(\sqrt[3]{-2})/\mathbb{Q}$（例 *47* 参照）を考え、埋め込み写像 $\mathbb{Q} \hookrightarrow \mathbb{C}$ を σ とし、これを $\mathbb{Q}(\sqrt[3]{-2}) \to \mathbb{C}$ なる写像 σ' に拡張 *(*すなわち、$\sigma'|_{\mathbb{Q}} = \sigma$ なる写像 σ' を構成*)* しよう。

$$\begin{array}{ccc}
\mathbb{Q}(\sqrt[3]{-2}) & \xrightarrow[\sigma']{} & \mathbb{C}\\
\uparrow & & \| \\
\mathbb{Q} & \xrightarrow[\sigma]{} & \mathbb{C}
\end{array}$$

σ' は好き勝手な写像がとれるわけではなく、体の準同型という条件によって、その有り様がかなり決まってしまう。このことを確かめよう。まず、例 *47* で見たように、$\mathbb{Q}(\sqrt[3]{-2})$ の任意の要素は $c_1 + c_2\sqrt[3]{-2} + c_3(\sqrt[3]{-2})^2$ *(*$c_1, c_2, c_3 \in \mathbb{Q}$*)* の形をしているか

ら、σ' を作用させると次のようになる：

$$\begin{aligned}
&\sigma'(c_1 + c_2\sqrt[3]{-2} + c_3(\sqrt[3]{-2})^2) \\
&= \sigma'(c_1) + \sigma'(c_2)\sigma'(\sqrt[3]{-2}) + \sigma'(c_3)\sigma'(\sqrt[3]{-2})^2 \\
&= \sigma(c_1) + \sigma(c_2)\sigma'(\sqrt[3]{-2}) + \sigma(c_3)\sigma'(\sqrt[3]{-2})^2 \qquad (\sigma'|_{\mathbb{Q}} = \sigma \text{ による}) \\
&= c_1 + c_2\sigma'(\sqrt[3]{-2}) + c_3\sigma'(\sqrt[3]{-2})^2 \qquad (\sigma \text{ は埋め込み写像だから})
\end{aligned}$$

このことから、σ' は $\sigma'(\sqrt[3]{-2}) \in \mathbb{C}$ の値さえ決まれば、完全に決まってしまうことがわかる[7]。では、$\sigma'(\sqrt[3]{-2})$ の値は好き勝手なものを選ぶことができるのかというと、そうではない。実際、$\sqrt[3]{-2}$ の最小多項式 $f = X^3 + 2$ を考えると、

$$0 = f(\sqrt[3]{-2}) = (\sqrt[3]{-2})^2 + 2$$

だから、この式の両辺に σ' を作用させると、準同型だから $\sigma'(0) = 0$ となることに注意して

$$0 = f(\sigma'(\sqrt[3]{-2})) = (\sigma'\sqrt[3]{-2})^2 + 2$$

となる。すなわち、$\sigma'(\sqrt[3]{-2})$ は f の零点でなければならない。よって

$$\sigma'(\sqrt[3]{-2}) = \sqrt[3]{-2},\ \zeta\sqrt[3]{-2},\ \text{または}\ \zeta^2\sqrt[3]{-2} \qquad (\text{ただし} \quad \zeta = \frac{-1+\sqrt{-3}}{2})$$

と決まってしまう。$\sigma'(\sqrt[3]{-2})$ の 3 つの値によって決まる σ' をそれぞれ $\sigma'_1,\ \sigma'_2,\ \sigma'_3$ とおくと、これらの写像による $\mathbb{Q}(\sqrt[3]{-2})$ の像は

$$\sigma_1(\mathbb{Q}(\sqrt[3]{-2}) = \mathbb{Q}(\sqrt[3]{-2}), \quad \sigma_2(\mathbb{Q}(\sqrt[3]{-2}) = \mathbb{Q}(\zeta\sqrt[3]{-2}), \quad \sigma_3(\mathbb{Q}(\sqrt[3]{-2}) = \mathbb{Q}(\zeta\sqrt[3]{-2})$$

となり、$\mathbb{C}$ の中に $\mathbb{Q}$ の拡大体が 3 つ（うちひとつは例 *47* のものと同じ）できる。注意したいことは、$\sqrt[3]{-2},\ \zeta\sqrt[3]{-2},\ \zeta^2\sqrt[3]{-2}$ の $\mathbb{Q}$ 上の最小多項式はいずれも $f = X^2 + 2$ で、*Kronecker* の方法 *(*定理 *22)* で単純拡大体を構成すると、上の σ_i *(*$i = 1, 2, 3$*)* による $\mathbb{Q}(\sqrt[3]{-2})$ の像はいずれも $\mathbb{Q}[X]/(X^3 + 2)$ と同型である。

例 48 のアイディアを一般化したものが、次の補題 49 で、これは今後のさまざまな考察で使われる重要な結果である。

補題 49. K を体とし、その単純代数拡大 $K' = K(a)$ を考える。ここで a の最小多項式を $f \in K[X]$ とする。さらに、体の準同型 $\sigma : K \longrightarrow L$ が与えられたとする。このとき

(*i*) $\sigma' : K' \longrightarrow L$ が σ の拡張、すなわち $\sigma = \sigma'|_K$ であるとすると、$\sigma'(a)$ は f^σ の零点である。

(*ii*) 逆に、$f^\sigma \in L[X]$ の各零点 $b \in L$ に対して、σ の拡張 $\sigma' : K' \longrightarrow L$ で $\sigma'(a) = b$ となるものが一意的に決まる。

以上のことから、特に、σ の拡張 σ' の個数は、f^σ の相異なる零点の個数に等しく、従ってとくに $\leq \deg f$ である。

[7] ある写像を決定するには、任意の要素がどこに写像されるかを決めればよいから。

Proof. (i) **の証明：** $f(a)=0$ だから、$f=\sum_{i=0}^{n} c_iX^i$ と書くと、準同型 $\sigma : K \longrightarrow L$ の任意の拡大 $\sigma' : K' \longrightarrow L$ に対して、

$$f^{\sigma}(\sigma'(a)) = \sum_{i=0}^{n} \sigma(c_i)\sigma'(a)^i = \sum_{i=0}^{n} \sigma'(c_i)\sigma'(a)^i = \sigma'(f(a)) = 0.$$

よって $\sigma'(a)$ は f^{σ} の零点である。

(ii) **の証明:** $K'=K(a)=K[a]$ だから、K' の任意の元 $c \in K'$ は $\sum_{i=0}^{m} d_ia^i$ $(d_i \in K)$ の形をしており、従って σ' による像は

$$\sigma'(c) = \sigma'(\sum_{i=0}^{m} d_ia^i) = \sum_{i=0}^{m} \sigma'(d_i)\sigma'(a^i) = \sum_{i=0}^{m} \sigma(d_i)\sigma'(a)^i$$

となる。$\sigma'(a)$ の値によって σ' は完全に決まってしまう。

さて、$f^{\sigma} \in L[X]$ の L における零点 $b \in L$ を（もし存在すれば）任意にとる（L は代数閉体とは限らないので、このような b が存在しない可能性もある）。すると以下の 2 つの短完全列[8] が存在する。ここで ψ は全射とは限らないことに注意。

$$\begin{array}{ccccccccc} & & & & (X & \mapsto & a) & & \\ 0 & \longrightarrow & (f) & \longrightarrow & K[X] & \xrightarrow{\varphi} & K[a] & \longrightarrow & 0 \\ & & \cap & & \| & & & & \\ 0 & \longrightarrow & \operatorname{Ker}\psi & \longrightarrow & K[X] & \xrightarrow{\psi} & L & & \\ & & & & (g & \mapsto & g^{\sigma}(b)) & & \end{array}$$

ここで $f^{\sigma}(b)=0$ だから $(f) \subset \operatorname{Ker}\psi$ であることに注意。ここで、自然全射準同型 $K[X] \to K[X]/(f)$ による X の像を x と書くことにすると、最初の完全列より同型写像 $\overline{\varphi} : K[X]/(f) \longrightarrow K[a]$ が $\overline{\varphi}(x) := \varphi(X) = a$ として誘導され (準同型定理)、また、$\operatorname{Ker}\psi \supset (f)$ であることから、

$$\begin{array}{rccc} \overline{\psi} : & K[X]/(f) & \longrightarrow & L \\ & x & \mapsto & b \end{array}$$

が誘導される。そこで、合成写像

$$\begin{array}{ccccc} K'=K[a] & \xrightarrow{\overline{\varphi}^{-1}} & K[X]/(f) & \xrightarrow{\overline{\psi}} & L \\ a & \mapsto & x & \mapsto & b \end{array}$$

を $\sigma' : K' \longrightarrow L$ とおけば、$\sigma'(a)=b$ となる。そして、最初に示したことより、このような $\sigma' : K' \longrightarrow L$ は $\sigma'(a)=b$ と決めれば一意的に決まる。 □

命題 50. K'/K を代数拡大とし、ある代数閉体 L への準同型 $\sigma : K \to L$ が与えられているとする。このとき、σ は K' 上に拡張される。すなわち、$\sigma' : K' \longrightarrow L$ $s.t.$ $\sigma = \sigma'|_K$ なる σ' が存在する。さらに、K' が代数閉体で、$L/\sigma(K)$ が代数拡大ならば、σ' は同型である。

[8] 可換環 A, B, C に対して、短完全列

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

とは、f が単射、g が全射、$A=\operatorname{Ker} g(=\{x \in B \mid g(x)=0\})$ である場合をいう。特に準同型定理により $C \cong B/A$

Proof. 集合 M を

$$M := \{(F,\tau) \mid K \subset F \subset K' \text{ (中間体)}, \ \tau : F \to L \text{ は } \sigma \text{ の拡張 }\}$$

と定義し、M の要素の間の部分順序 $\preceq$ を

$$(F,\tau) \preceq (F',\tau') \quad \overset{def}{\Leftrightarrow} F \subset F' \text{ かつ } \tau'|_F = \tau$$

と定義すると、

Claim 1: M は帰納的集合[9]である。

Claim 1 の証明. 実際、$(K,\sigma) \in M$ ゆえ $M \neq \emptyset$ であり、また、任意の全順序部分集合 $H \subset M$ に対して $\tilde{F} := \bigcup_{(F,\tau)\in H} F$ を考え、$\tilde{\tau} : \tilde{F} \longrightarrow L$ を $\tilde{\tau}(x) = \tau(x)$ for $(F,\tau) \in H$ s.t. $x \in \tilde{F}$, と定義すれば、$(\tilde{F},\tilde{\tau}) \in M$ であり、かつ、これが H の上界になる。 □

そこで Zorn の補題より M の極大元 (F,τ) が存在する。このとき、

Claim 2: $F = K'$

Claim 2 の証明. $F \subset K'$, $F \neq K'$ と仮定して、矛盾を導く。仮定から $\alpha \in K' - F$ なる元が存在する。さらに命題の仮定より K'/K は代数拡大だから、α は $F\ (\supset K)$ 上にも代数的である。そこで、$\tau : F \longrightarrow L$ と単純代数拡大体 $F(\alpha)$, そして仮定より L は代数閉体だから、α の F 上の最小多項式 $f \in F[X]$ に対して $f^\sigma \in L[X]$ の零点 γ が少なくとも 1 個はとれる。そこで補題 $49(ii)$ を適用すると、τ の拡張 $\tau' : F(\alpha) \to L$ で $\tau'(\beta) = \gamma$ となるものが作れる。しかしこれは (F,τ) の極大性に反する。 □

従って、σ の拡張 $\sigma' : K' \longrightarrow L$ が構成できた。それは結局 $\tau : F \longrightarrow L$ と同じものである。

さらに、K' が代数閉体だとすると、$\sigma(K')$ もまた代数閉体である[10]。さらに L が $\sigma(K)$ 上に代数的であるとすると、$\sigma(K')(\supset \sigma(K)$ 上にも代数的である。したがって $\sigma'(K') = L$ (命題 39) でなければならない。よって K' と L は同型になる (命題 43 参照)。 □

代数的閉包の一意性は、命題 50 より直ちに従う。すなわち、

系 51. 体 K の 2 つ代数的閉包 $\overline{K_1}$ と $\overline{K_2}$ が与えられたとき、K 同型 $\varphi : K_1 \longrightarrow K_2$ が存在する。

以後我々は代数拡大を考える際には、代数的閉包 (またはそれを含む代数閉体) の 1 つを固定して、そこから代数的元を集めてきて拡大体をつくる。どの代数的閉包を使ったか区別しなければならない場合もあれば、それらは K 同型で代数的性質は

[9]空でない集合 M が帰納的集合であるとは、$(M,\leq)$ が部分順序集合であり、任意の全順序部分集合 $H \subset M$ が上限を持つ、すなわち、$x \in M$ で任意の $y \in H$ に対し $y \leq x$ なるものが存在する場合をいう。Zorn の補題とは、任意の帰納的集合には極大元が存在することを主張するものであった。

[10]体の準同型写像は単射 (命題 43) だから、K' の代数的な性質はすべて $\sigma(K')$ に写される。従って、K' が代数閉体ならば、$\sigma(K')$ もそうなる。詳細は各自の演習。

同じだから、あえて区別しない場合もある。それぞれの議論で、どちらの考え方で行っているか、注意する必要がある。

例 52. 実数体 $\mathbb{R}$ の代数的閉包（のひとつ）は $\mathbb{C}$ で、これは *1* 回の代数拡大だけで得られる：$\mathbb{C} = \mathbb{R}(\sqrt{-1}) \cong \mathbb{R}[X]/(X^2+1)$. $\mathbb{C}$ が確かに代数閉体であることは、まさに「代数学の基本定理」の主張そのものであることに注意。

例 53. 有理数体 $\mathbb{Q}$ の代数的閉包は通常複素数体 $\mathbb{C}$ の中で考えることが多い。$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \ : \ \alpha \text{は} \mathbb{Q} \text{上代数的}\}$. これは $\mathbb{C}$ とは一致しない。実際、$\mathbb{C}$ には π *(*円周率*)* や e *(*自然対数底*)* が含まれいていて、これらは $\mathbb{Q}$ 上代数的でない *(*例 *6)* から $\overline{\mathbb{Q}}$ には含まれない。

例 54. 有限体 $\mathbb{F}_q$ の代数的閉包 $\overline{\mathbb{F}}_q$ は $\mathbb{C}$ とは別のもので、包含関係もない。実際、もしこれらに包含関係があれば、標数は一致するはずである。ところが、$\mathrm{char}\,\mathbb{F}_q > 0$ だが、$\mathrm{char}\,\mathbb{C} = 0$ である。

まとめ

- 任意の体 K い大して代数的閉包 $\overline{K}$ は K 同型を除いて一意的に存在する。
- 代数的閉包は代数閉体である。
- 代数拡大を考えるときは、適当な代数的閉包の中で考える。
- 代数拡大 K'/K と体の準同型 $\sigma : K \longrightarrow L$ に対して、その拡張 $\sigma' : K' \longrightarrow L$ s.t. $\sigma'|_K = \sigma$ を考えること。

4. 分解体と正規拡大

4.1. 分解体.

例 55 (例 47 再出). $f = X^3 + 2 \in \mathbb{Q}[X]$ は、拡大体 $L = \mathbb{Q}(\sqrt[3]{-2}, \sqrt{-3})$ をととって $f \in L[X]$ と考えれば、

$$f = (X - \sqrt[3]{-2})(X - \xi\sqrt[3]{-2})(X - \xi^2\sqrt[3]{-2}) \qquad \xi = \frac{-1+\sqrt{-3}}{2}$$

と 1 次式だけの積に分解する。このとき L は f の分解体であるという。

演習問題 1. $\sqrt{-3} \notin \mathbb{Q}(\sqrt[3]{-2})$ であることを示せ。

演習問題 2. $\mathbb{Q}(\sqrt[3]{-2}, \zeta\sqrt[3]{-2}, \zeta^2\sqrt[3]{-2}) = \mathbb{Q}(\sqrt[3]{-2}, \sqrt{-3})$ であることを示せ。

代数学の基本定理により $\mathbb{C}$ は代数閉体なので、例えば $\mathbb{Q}$ 係数の任意の多項式 $f \in \mathbb{Q}[X]$ は $\mathbb{C}$ 係数の中で考えればいつでも 1 次式だけの積に分解する。しかし、$\mathbb{C}$ よりももっと小さな体で考えても 1 次式に分解しないのだろうか？そのような体のうち、もっとも小さいなものを考えよう。それが以下に定義する最小分解体である。

定義 56 (分解体). 定数でない多項式の族 $\mathfrak{F} = \{f_i\}_{i\in I},\ f_i \in K[X]$ を考える。こに時、拡大体 L/K が $\mathfrak{F}$ の（最小）分解体であるとは、

(*i*) 任意の $i \in I$ に対して $f_i = c_i(X - a_1)\dots(X - a_{n_i})\ c_i \in K,\ a_1, \dots, a_{n_i} \in L$ の形に因数分解でき、L はそのような体のうちもっとも小さいもの[11]である場合をいう。

(*ii*) 拡大 L/K は、全ての多項式 f_i の全ての零点を K に付け加えることによって生成される。

命題 57. 任意の族 $\mathfrak{F}(\subset K[X])$ に対して、その分解体 L は常に存在する。

Proof. 実際、K の代数的閉包 $\overline{K}$ を考えると、各多項式 $f_i \in \mathfrak{F}$ の零点は $\overline{K}$ の中でとれる。それらを全て K に付け加えてえられる拡大体 L が $\mathfrak{F}$ に分解体である。 □

4.2. 分解体の一意性.

分解体の一意性の考え方は、代数的閉包の一意性と同じ考え方である。

命題 58 (分解体の一意性). $L_1,\ L_2$ がいずれも定数でない多項式の族 $\mathfrak{F}(\subset K[X])$ の分解体であるとする。この時、L_2 の代数的閉包 $\overline{L}_2$ への任意の K-準同型写像

$$\overline{\sigma} : L_1 \longrightarrow \overline{L}_2$$

の像は L_2 となり、同型 $L_1 \cong L_2$ を与える。

Proof. 命題 50 より、包含写像 $K \hookrightarrow \overline{L}_2$ の拡張 $\overline{\sigma} : L_1 \longrightarrow \overline{L}_2$ がとれる。ここで $\overline{\sigma}$ は K の元を動かさないので、K 準同型になっていることに注意。このとき、$\overline{\sigma}$ が同型 $L_1 \cong L_2$ を与えていることを示そう。

[11] すなわち、任意の拡大 F/K に対して、f が $F[X]$ の中で一次式だけの積に分解すれば、$L \subset F$ となることをいう。

まず、$\mathfrak{F}=\{f\}$, f はモニック多項式、の場合を考える。f の L_1 における零点を $a_1,\dots,a_n$, L_2 における零点を $b_1,\dots,b_n$ とする。すると

$$f^\sigma=\prod(X-\overline{\sigma}(a_i))=\prod(X-b_i).$$

$K[X]$ が一意分解整域だから $\{\sigma(a_1),\dots,\sigma(a_n)\}=\{b_1,\dots,b_n\}$ である。従って、

$$L_2=K(b_1,\dots,b_n)=K(\sigma(a_1),\dots,\sigma(a_n))=\overline{\sigma}(L_1).$$

つまり $\overline{\sigma}$ は同型 $L_1\cong L_2$ を誘導している。

次に $\mathfrak{F}$ が一般の場合を考える。$\sharp\mathfrak{F}<\infty$ の場合は、$\mathfrak{F}$ に現れる多項式全ての積を f とすれば、$\mathfrak{F}$ の分解体と $\{f\}$ の分解体は同じものなので、上の証明に帰着される。また、$\sharp\mathfrak{F}=\infty$ の場合、その分解体は $\mathfrak{F}$ の有限部分集合列

$$\mathfrak{F}_0\subset\mathfrak{F}_1\subset\cdots\subset\mathfrak{F}_n\subset\cdots\subset\mathfrak{F}=\bigcup_{n\geq 0}\mathfrak{F}_n$$

を考えて、各 $\mathfrak{F}_n$ の分解体を $L_1^{(n)}$, $L_2^{(n)}$ として、$L_1=\bigcup_{n\geq 0}L_1^{(n)}$, $L_2=\bigcup_{n\geq 0}L_2^{(n)}$ と書き表せるから、$L_1^{(n)}\cong L_2^{(n)}$, $n\in\mathbb{N}$, から $L_1\cong L_2$ も従う。 □

系 59. 定数でない K 上の多項式の族 $\mathfrak{A}\subset K[x]$ の分解体は、互いに K 同型である。

4.3. **正規拡大.** K の代数拡大体 L が、適当な多項式集合 $F\subset K[X]$ の分解体になっている時、L/K は正規拡大であるという。正規拡大を、K 準同型の観点から特徴づけることが、この節の目標である。この考え方は、後に Galois 群の概念に繋がっていく重要なものである。

定義 60 ($\mathrm{Hom}_K(L,M)$)**.** 2つの拡大体 L/K と M/K を考える。このとき、

$$\mathrm{Hom}_K(L,M):=\{\varphi\mid\sigma:L\to M\ \text{は}\ K\ \text{準同型}\}$$

と定義する。

例 61. 例 *47* で考えた $f=X^3+2$ の $\mathbb{Q}$ 上の最小分解体 $L:=\mathbb{Q}(\sqrt[3]{-2},\sqrt{-3})$ を考えよう。L の代数的閉包 $\overline{L}$ への $\mathbb{Q}$ 準同型 $\varphi\in\mathrm{Hom}_{\mathbb{Q}}(L,\overline{L})$ がどんなものかを調べよう。

Step 1: $L/\mathbb{Q}(\sqrt[3]{-2})$ と $\mathbb{Q}(\sqrt[3]{-2})/\mathbb{Q}$ の二つの単純拡大の基底がそれぞれ $1,\ \sqrt{-3}$ *(*$\mathbb{Q}(\sqrt[3]{-2})$-線形空間としての基底*)* および $1,\sqrt[3]{-2},(\sqrt[3]{-2})^2$ *(*$\mathbb{Q}$-線形空間としての基底*)* だから、命題 *14* の証明みたように、拡大 $L/\mathbb{Q}$ の $\mathbb{Q}$ 基底はこれらの基底をかけ合わせて得られる

$$1,\ \sqrt{-3},\ \sqrt[3]{-2},\ (\sqrt[3]{-2})^2,\ \sqrt{-3}\sqrt[3]{-2},\ \sqrt{-3}(\sqrt[3]{-2})^2$$

の 6 個である。

Step 2: 任意の $\varphi\in\mathrm{Hom}_{\mathbb{Q}}(L,\overline{L})$ をとる。まず、φ は $\mathbb{Q}$ 線形写像だから、基底の像

$$\varphi(1),\ \varphi(\sqrt{-3}),\ \varphi(\sqrt[3]{-2}),\ \varphi((\sqrt[3]{-2})^2),\ \varphi(\sqrt{-3}\sqrt[3]{-2}),\ \varphi(\sqrt{-3}(\sqrt[3]{-2})^2)$$

さえ決まれば、φ そのものが決まる。さらに φ は体の準同型だから、上の像は

$$\begin{aligned}
\varphi(1) &= 1,\\
\varphi(\sqrt{-3}) &= ?,\\
\varphi(\sqrt[3]{-2}) &= ?,\\
\varphi((\sqrt[3]{-2})^2) &= \varphi(\sqrt[3]{-2})^2,\\
\varphi(\sqrt{-3}\sqrt[3]{-2}) &= \varphi(\sqrt{-3})\varphi(\sqrt[3]{-2})\\
\varphi(\sqrt{-3}(\sqrt[3]{-2})^2) &= \varphi(\sqrt{-3})\varphi(\sqrt[3]{-2})^2
\end{aligned}$$

となる。結局、$\varphi(\sqrt{-3})$ と $\varphi(\sqrt[3]{-2})$ が決まれば、残りのものも全部決まるわけである。

Step 3: では $\varphi(\sqrt{-3})$ と $\varphi(\sqrt[3]{-2})$ は $\overline{L}$ の中の好き勝手な値を取れるのかというと、そうではない。$\sqrt{-3}$ は $X^2+3 \in \mathbb{Q}[X]$ の零点だから、$0 = x^2+3$ *(*ただし、$x := \sqrt{-3}$ とする）の両辺に φ を適用すると、

$$0 = \varphi(0) = \varphi(x^2+3) = \varphi(x)^2 + 3$$

となるから、$\varphi(\sqrt{-3})$ は X^2+3 の零点でなければならない。すなわち、

$$\varphi(\sqrt{-3}) = \sqrt{-3} \quad \text{または} \quad \varphi(\sqrt{-3}) = -\sqrt{-3}.$$

同様に $\sqrt[3]{-2}$ は $X^3+2 \in \mathbb{Q}[X]$ の零点のひとつで、それ以外の零点としては $\zeta\sqrt[3]{-2}$ と $\zeta^2\sqrt[3]{-2}$ がある。ただし、ここで $\zeta = \frac{-1+\sqrt{-3}}{2}$, $\zeta^2 = \frac{-1-\sqrt{-3}}{2}$ である。従って、

$$\varphi(\sqrt[3]{-2}) = \sqrt[3]{-2},\ \zeta\sqrt[3]{-2},\ \text{または}\ \zeta^2\sqrt[3]{-2}.$$

Step 4: Step 3 で得られた $\varphi(\sqrt{-3})$ と $\varphi(\sqrt[3]{-2})$ の値はいずれも $L = \mathbb{Q}(\sqrt{-3}, \sqrt[3]{-2})$ に含まれていることに注意する。従って **Step 2** の φ による $L/\mathbb{Q}$ の $\mathbb{Q}$ 基底の像も、やはり L に含まれている。任意の $a \in L$ に対して、

$$\begin{aligned}
a &= c_0\cdot 1 + c_1\cdot\sqrt{-3} + c_2\cdot\sqrt[3]{-2} + c_3\cdot(\sqrt[3]{-2})^2\\
&\quad + c_4\cdot\sqrt{-3}\sqrt[3]{-2} + c_5\cdot\sqrt{-3}(\sqrt[3]{-2})^2\\
&\quad (\exists c_0, \ldots, \exists c_5 \in \mathbb{Q})
\end{aligned}$$

と書けるから、K 準同型 φ を適用すると

$$\begin{aligned}
\varphi(a) &= c_0\varphi(1) + c_1\varphi(\sqrt{-3}) + c_2\varphi(\sqrt[3]{-2}) + c_3\varphi((\sqrt[3]{-2})^2)\\
&\quad + c_4\varphi(\sqrt{-3}\sqrt[3]{-2}) + c_5\varphi(\sqrt{-3}(\sqrt[3]{-2})^2)\\
&= c_0\varphi(1) + c_1\varphi(\sqrt{-3}) + c_2\varphi(\sqrt[3]{-2}) + c_3\varphi((\sqrt[3]{-2}))^2\\
&\quad + c_4\varphi(\sqrt{-3})\varphi(\sqrt[3]{-2}) + c_5\varphi(\sqrt{-3})\varphi(\sqrt[3]{-2}))^2
\end{aligned}$$

となり、結局 φ による L の像は L に含まれていることがわかる。さらに φ は（$\mathbb{Q}$ 線形写像として）全射であることもわかり、$\varphi \in \mathrm{Aut}_{\mathbb{Q}}(L)$ となる。

すなわち、

$$\mathrm{Hom}_{\mathbb{Q}}(L, \overline{L}) = \mathrm{Aut}_{\mathbb{Q}}(L)$$

となっている。また、上の考察から $\mathbb{Q}(\sqrt[3]{-2}, \sqrt{-3})$ は多項式の集合

$$F := \{X^3+2,\ X^2+3\} \in \mathbb{Q}[X]$$

の $\mathbb{Q}$ 上の分解体なっている。

例 61 の考察は、以下のように一般化される。

定理 62. 代数拡大 L/K に対し、以下は同値：

(i) 任意の $\sigma \in \mathrm{Hom}_K(L, \overline{L})$ に対し、$\sigma \in \mathrm{Aut}_K(L)$.

(ii) L は適当な多項式集合 $\mathfrak{F} \subset K[X]$ の分解体である。

(iii) 任意の多項式 $f \in K[X]$ に対して、もし f の零点が 1 つでも L に存在すれば、$f = c(X-a)(X-a_1)\cdots(X-a_n)$, $c \in K$, $a_1, \ldots, a_n \in L$ の形に因数分解する（すなわち f の他のすべての零点も L の中に存在する）。

Proof. $(i) \Rightarrow (iii)$ の証明：$f \in K[X]$ を $\deg f \geq 2$ なる既約多項式とし、$a \in L$ をその零点のひとつとする。f のそれ以外の任意の零点を $b \in (\overline{K} \subset)\overline{L}$ とする。この時、補題 49 を、埋め込み写像 $\sigma : K \hookrightarrow \overline{K}$, $(\sigma(x) = x, \forall x \in K)$, $K' = K(a)$, $f^\sigma = f$ の零点 b に適用すると、体の準同型

$$\sigma' : K(a) \longrightarrow \overline{L}$$

で $\sigma'|_K = \sigma$ （すなわち K-準同型）かつ $\sigma'(a) = b$ となるものが存在する。さらに、拡大体 $L/K(a)$ と σ' に対して命題 50 を適用すると、K-準同型

$$\sigma'' : L \longrightarrow \overline{L} \quad s.t \quad \sigma''|_{K(a)} = \sigma',\ \sigma''(a) = \sigma'(a) = b$$

が作れる。そこで仮定 (i) を $\sigma'' \in \mathrm{Hom}_K(L, \overline{L})$ に適用すると、$\sigma''(L) = L$, 従ってとくに $b \in L$. よって f の任意の零点は全て L に含まれることになり、(iii) が言える。

$(iii) \Rightarrow (ii)$ の証明: $(a_i)_{i \in I}$ が L の K 上の生成元の族とする：$L = K(a_i : i \in I)$. L/K は代数拡大だから各 a_i は K 上代数的。そこで $f_i \in K[X]$ をその最小多項式とする。仮定 (iii) より、$f_i = c(X-a_i)(X-\beta_2)\cdots(X=\beta_n)$, $c \in K$, $\beta_2, \ldots, \beta_n \in L$ の形に分解するので、L は族 $\mathfrak{F} = \{f_i\}_{i \in I}$ の分解体である。すなわち (ii) が成り立つ。

$(ii) \Rightarrow (i)$ の証明：(ii) を仮定して、L が多項式集合 $\mathfrak{F} \subset K[X]$ の分解体であるとする。$\sigma \in \mathrm{Hom}_K(L, \overline{L})$ を任意にとる。すると $\sigma(L)$ は多項式の族 $(f^\sigma : f \in \mathfrak{F}) \subset \sigma(K)[X] = K[X]$ の分解体である。ここで σ は K-準同型なので、$(f^\sigma : f \in \mathfrak{F}) = \mathfrak{F}$ だから、$\sigma(L)$ も L も $\mathfrak{F}$ の分解体である。しかも $\sigma \in \mathrm{Hom}_K(L, \overline{L})$ だから包含写像

$$\sigma(L) \hookrightarrow \overline{L}$$

が存在する。すると命題 58 より、この包含写像の像は L そのものとなる。つまり $\sigma(L) = L$ となる。すなわち $\sigma \in \mathrm{Aut}_K(L)$. □

定義 63 (正規拡大)**.** 代数拡大 L/K が正規であるとは、定理 *62* の条件を満たす場合をいう。

4.4. **正規閉包.** 拡大体 L/K が正規拡大でない場合、L を少し大きく取り直して拡大体 L'/L を適当にとることにより、L'/K を正規拡大にすることができる。ここでは、そのような L' の構成方法を考える。

定義 64. L/K を代数拡大とするとき、$L \subset L'$ なる正規拡大体 L'/K の最小のもの、すなわち、L' の任意の真の部分体 $L \subset E \subset L'$, $E \neq L'$, に対して E/K が正規拡大にならないものを、L の**正規閉包** と呼ぶ。

命題 65. L/K を（有限とは限らない）代数拡大とする。このとき

(i) L の正規閉包 L'/K が同型を除いて一意的に存在する。

(ii) L/K が有限拡大なら、L'/K も有限拡大である。

(iii) M/L が正規拡大だとする。この時、L/K の正規閉包 L' を $K \subset L \subset L' \subset M$ となるようにとることができ、それは M の部分体として一意的に決まる。ここで $\{\sigma_i\}_{i\in I} = \mathrm{Hom}_K(L, M)$ とすると

$$L' = K(\sigma_i(L) : i \in I)$$

と構成される。

Proof. (i) の前半の証明 (正規閉包の存在) :L/K は代数拡大だから、K 上代数的な元の集合 $\mathfrak{A} = (a_j)_{j\in J} \subset L$ によって、$L = K(\mathfrak{A})$ と書けるが、各 $a_j \in L$ の K 上の最小多項式を $f_j \in K[X]$ とおく。また、M/L を正規拡大とする（例えば $M = \overline{L}$ (代数的閉包) ととればよい)。すると、f_j は ($L[X]$ の元とみなせば)、定理 62(iii) により、$M[X]$ の中で 1 次式の積に分解する。そこで L' を $\{f_j\}_{j\in J}$ の M の中での分解体とする：$L \subset L' \subset M$. このとき、L' が L/K の正規閉包であることは定理 62 より明らかである。逆に、L/K の正規閉包 L'/K は、必然的に $\{f_j\}_{j\in J}$ の分解体を含み、また正規閉包の最小性から $\{f_j\}_{j\in J}$ の分解体そのものになる。

(ii) の証明：この構成から, L/K が有限拡大なら、$\mathfrak{A}$, 従って $\{f_j\}_{j\in J}$ は有限集合であり、L'/K も有限拡大になる。

(i),(iii) における L' の一意性証明 :L'_1/K と $L'_2.K$ がいずれも L/K の正規閉包だとすれば、L'_1, L'_2 ともに $\{f_j\}_{j\in J}$ の K 上の分解体。したがって、L 上の分解体でもある。すると系 59 により L 同型 $\sigma : L'_1 \longrightarrow L'_2$ が存在する, i.e., $\sigma(L'_1) = L'_2$. これが (i) の意味の一意性である。また、(iii) のように、L'_1, L'_2 が正規拡大 M/L の中で構成されたとすると、上で見たように $\sigma(L'_1) = L'_2$ だが、$M \subset \overline{L'_1}$ だから $\sigma \in \mathrm{Hom}_L(L'_1, \overline{L'_1})$ とみなすことができる。すると包含写像

$$\sigma(L'_1) = L'_2 \hookrightarrow \overline{L'_1}$$

が作れるが、定理 62(i) より、この像は L'_1 そのものになる。すなわち $L'_1 = L'_2$. これは (iii) の意味での同型、すなわち、M の部分体としては L' は完全に 1 つに決まることを意味する。

(iii) の証明 :K 準同型の集合 $\{\sigma_i\}_{i\in I} = \mathrm{Hom}_K(L, M)$ を考える。補題 49 と $f_j^{\sigma_j} = f_j$ より、σ_i は f_j の零点を別の零点に移すことがわかる。ただ、σ を $\mathrm{Hom}_K(L, \overline{L})$ の中から取っているわけではないので、$M \supset \overline{L}$ に注意すると、上の σ_i の像だけで f_j らの零点をすべて尽くせるかどうかはわからない。したがって、L の各元は K 上代数的だから、$\sigma_i(L), i \in I$, は σ_i の像として得られる別の代数的元の集合であるが、そのようなもの全部を尽くしているかどうかはわからない。いっぽう、上に述べた構成法により、L' は f_j たちの零点をすべて K に付け加えて得られる拡大体だから、上の考察により

$$K(\sigma_i(L) : i \in I) \subset L'.$$

を得る。逆に f_j の任意の零点 $a \in L'$ に対し、補題 49 より

$$K(a_i) \longrightarrow L' \qquad a_i \longmapsto a$$

なる K 準同型を定義できる。これを $\overline{L'}$ への写像と考えて、さらには $\overline{L'}/K(a_i)$ が代数拡大であることに注意すると、命題 50 より、上の K 準同型は $\overline{L'}$ の K-自己同型

$$\overline{L}' \longrightarrow \overline{L}'$$

に拡張できる。L'/K は正規だから、この写像を L' に制限すれば、その像は L' である。勿論さらに小さい L に制限しても、その像は L' に含まれる。したがって、上の写像を K-準同型

$$\sigma : L \longrightarrow L' \qquad s.t. \quad \sigma(a_i) = a$$

に制限できる。$L' \subset M$ だから、$\sigma \in \mathrm{Hom}_K(L, M)$ とみなせる。よって $a \in K(\sigma_i(L) \mid i \in I)$ となり、$L' = K(\sigma_i(L) \mid i \in I)$ が得られる。 □

たとえば、代数拡大 L/K が正規でないとする。定理 62(i) より直ちにわかるように、$\overline{L}/L$ は正規拡大だから、命題 65(iii) より、正規閉包 L' は

$$L' = K(\sigma(L) \mid \sigma \in \mathrm{Hom}_K(L, \overline{L}))$$

と構成される。

まとめ

- （最小）分解体の存在と一意性
- 正規拡大 L/K を $\mathrm{Hom}_K(L, \overline{L}) = \mathrm{Aut}_K(L)$ として特徴づけること。
- 正規閉包とその構成

5. 分離拡大

最小多項式が重根を持たないような代数的元で生成された拡大体を分離拡大と呼ぶ。これは正規拡大と並び、Galois 理論で最も重要な概念のひとつである。

定義 66 (分離的多項式)**.** 定数でない多項式 $f \in K[X]$ が**分離的**であるとは、f の代数的閉包 $\overline{K}$ における零点（方程式の解）が全て重根でない場合をいう。

定義 67 (分離拡大)**.** 代数拡大 L/K を考える。$a \in L$ が K 上**分離的**であるとは、a の最小多項式が分離的である場合をいう。また、全ての $a \in L$ が分離的であるとき、**拡大 L/K は分離的である**という。

定義 68 (完全体)**.** 体 K の任意の代数拡大が分離的になるとき、K は**完全体**であるという。

定理 69. $\mathrm{char}(K) = 0$ なる任意の体 K は完全体である。

Proof. 任意の代数拡大 L/K をとり、任意の $a \in L$ に対する最小多項式が分離的であることを示せばよい。もし f が分離的でないならば、

$$f = (X-\alpha)^r g \quad r \geq 2,\ \alpha \in \overline{K}, g \in \overline{K}[X]$$

の形になっている ($a = \alpha$ とは限らない)。従って、

$$f'\left(= \frac{df}{dX}\right) = (X-\alpha)^{r-1}(r \cdot g + (X-\alpha)g')$$

となり、$\deg f > \deg f'$, $f' \in K[X]$, $f'(\alpha) = f(\alpha) = 0$ だから、α の K 上の最小多項式 h の次数は $\deg f$ よりも真に小さく、かつ、f の因子になっている。すなわち $f = h\ell$ となる $\ell \in K[X]$ が存在することになり、f の既約性に反する。よって f は分離的でなくてはならず、$a \in L$ は分離的、すなわち L/K は分離拡大。 □

注意 70. 定理 125 で、有限体も完全体であることを示す。

注意 71. 定理 69 の証明より、$f \in K[X]$ が分離多項式であるための必要十分条件は、X による導関数 f' と f が $\overline{K}$ の中で共通零点を持たないこと、だとわかる。

5.1. 分離次数.

ここでは、分離拡大を研究するために必要な、分離次数の概念を導入する。多項式の相異なる零点の個数というのが元々のアイディアだが、それが拡大体の代数的閉包への準同型の個数とも考えられる点が重要である。

定義 72 (分離次数)**.** 代数拡大 L/K に対して、K の代数的閉包 $\overline{K}$ への K-代数準同型 $\sigma : L \to \overline{K}$ の個数を、分離次数 $[L:K]_s$ と呼ぶ：

$$[L:K]_s = \sharp \mathrm{Hom}_K(L, \overline{K}).$$

単純代数拡大 $K(a)/K$ の場合、$\mathrm{Hom}_K(K(a), \overline{K})$ の要素は結局 a の最小多項式 f の全ての零点 $\{a_1(:=a), a_2, \ldots, a_n\}$, $n = \deg f$, の並べ替えであった。以下は、このことの言い換えである。

命題 73. $L = K(a)/K$ なる単純代数拡大を考え、$f \in K[X]$ を $a \in L$ の K 上の最小多項式とする。このとき、$[L:K]_s$ は f の相異なる零点の数に等しい。

Proof. 補題 49 より $\mathrm{id}_K : K \longrightarrow K \subset \overline{K}$ の拡張 $\sigma : K(a) \longrightarrow \overline{K}$, すなわち $\mathrm{Hom}_K(L, \overline{K})$ の元の個数は最小多項式 f の相異なる零点の個数である。従ってそれは分離次数 $[L : K]_s$ である。 □

例 74. 例 *61*で考えた $K = \mathbb{Q}$ の正規拡大体 $L = \mathbb{Q}(\sqrt[3]{-2}, \sqrt{-3})$ について、$\mathrm{Aut}_K(L) = \mathrm{Hom}_K(L, \overline{L})$ であった。ここで L/K は代数拡大だから、$L \subset \overline{K}$ であり、従って $\overline{L} = \overline{K}$ である。よって

$$[L : K]_s = \sharp \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{-2}, \sqrt{-3})) = 6.$$

$\mathrm{Aut}_K(L)$ の元は、L/K の *6* つの K 線形基底の φ による像を決めることによって決まった。例 *61* の計算により、$\mathrm{Aut}_K(L) = \{\varphi_i \mid i = 0, \ldots, 5\}$ は具体的には次のよういいなっていることがわかる。以下の表は各 φ_i が 6 つの基底をどこに写像するかを示している。

基底	φ_0の像	φ_1の像	φ_2の像	φ_3の像	φ_4の像	φ_5の像
1	1	1	1	1	1	1
$a = \sqrt{-3}$	a	a	a	$-a$	$-a$	$-a$
$b = \sqrt[3]{-2}$	b	ζb	$\zeta^2 b$	b	ζb	$\zeta^2 b$
b^2	b^2	$\zeta^2 b^2$	ζb^2	b^2	$\zeta^2 b^2$	ζb^2
ab	ab	ζab	$\zeta^2 ab$	$-ab$	$-\zeta ab$	$-\zeta^2 ab$
ab^2	ab^2	$\zeta^2 ab^2$	ζab^2	$-ab^2$	$-\zeta^2 ab^2$	$-\zeta ab^2$

ここで、

$$\zeta = \frac{-1 + \sqrt{-3}}{2} = -\frac{1}{2} + \frac{1}{2}a, \quad \zeta^2 = \frac{-1 - \sqrt{-3}}{2} = -\frac{1}{2} - \frac{1}{2}a$$

だから、例えば

$$\zeta ab^2 = -\frac{1}{2}ab^2 + \frac{1}{2}a^2b^2 = -\frac{1}{2}ab^2 - \frac{3}{2}b^2$$

となり、φ_i による基底の像は、ちゃんと基底の $\mathbb{Q}$ 上の線形和として表せることに注意。

この例の状況は以下のように一般化される。

命題 75. *L/K が正規拡大のとき、$[L : K]_S = \sharp \mathrm{Aut}_K(L)$.*

Proof. L/K は代数拡大だから、$\overline{K} = \overline{L}$. 従って $\mathrm{Hom}_K(L, \overline{K}) = \mathrm{Hom}_K(L, \overline{L})$. そこで、もし L/K が正規拡大ならば、定理 62 より $\mathrm{Hom}_K(L, \overline{L}) = \mathrm{Aut}_K(L)$ である。 □

以下の結果は、命題 14 と形は良く似ているが、命題 14 では線形空間の次元、以下の定理では体の間の写像の個数を考えているので、内容的にはかなり異なることに注意。

命題 76. *$K \subset L \subset M$ を代数拡大とするとき、$[M : K]_s = [M : L]_s [L : K]_s$*

Proof. M の代数的閉包 $\overline{K}$ をひとつ固定しておく。$M/L/K$ は代数拡大だから、$\overline{K} = \overline{L} = \overline{M}$ であることに注意。そこで

$$\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_i \mid i \in I\}, \quad \mathrm{Hom}_L(M, \overline{L}) = \mathrm{Hom}_L(M, \overline{K}) = \{\tau_j \mid j \in J\}$$

とおくと、定義より $[L:K]_s = \sharp \mathrm{Hom}_K(L, \overline{K})$ かつ $[M:K]_s = \sharp \mathrm{Hom}_K(M, \overline{K})$ である。さらに、命題 50 により、各 $\sigma_i : L \to \overline{K}$ は体 $\overline{K}(= \overline{L})$ の自己同型 $\overline{\sigma}_i : \overline{K} \to \overline{K}$ に拡張できる。そこで、次のことが言えれば $[M:K]_s = [M:L]_s \cdot [L:K]_s$ が示せたことになる：

Claim 1: $\overline{\sigma}_i \circ \tau_j : M \longrightarrow \overline{K}$, $i \in I$, $j \in J$ は互いに異なる。(従って、その個数は $[H:L]_s \cdot [L:K]_s$ と等しい。)

Claim 2: $\mathrm{Hom}_K(M, \overline{K}) = \{\overline{\sigma}_i \circ \tau_j \mid i \in I, j \in J\}$
(cf. $\sharp \mathrm{Hom}_K(M, \overline{K}) = [M, K]_s$).

Claim 1 の証明. $\overline{\sigma}_i \circ \tau_j = \overline{\sigma}_{i'} \circ \tau_{j'}$ とすると、$\tau_j|_L = \tau_{J'}| = \mathrm{id}_L$ であり、σ_i, $\sigma_{i'}$ が L 上の準同型であることから、

$$\sigma_i = \overline{\sigma}_i|_L = (\overline{\sigma}_i \circ \tau_j)|_L = (\overline{\sigma}_{i'} \circ \tau_{j'})|_L = \overline{\sigma}_{i'}|_L = \sigma_{i'}.$$

これよりさらに、$\tau_j = \tau_{j'}$ も従う。 □

Claim 2 の証明 . $\tau \in \mathrm{Hom}_K(M, \overline{K})$ を任意にとる。$\tau|_L \in \mathrm{Hom}_K(L, \overline{K})$ だから、$\tau|_L = \sigma_i$ なる $i \in I$ がとれる。すると、

$$(\overline{\sigma}_i^{-1} \circ \tau)|_L = \overline{\sigma}_i^{-1} \circ \sigma_i = \mathrm{id}_L$$

となるから、$\overline{\sigma}_i^{-1} \circ \tau \in \mathrm{Hom}_L(M, \overline{K})$ となる。従って、$\overline{\sigma}_i^{-1} \circ \tau = \tau_j$ となる $j \in J$ がとれる。よって $\tau = \overline{\sigma}_i \circ \tau_j$ となる。 □

□

例 77. 多項式

$$f = X^{2p^2} + X^{p^2} + 1 \in \mathbb{F}_p[X]$$

を考える。ここで、$x := X^{p^2}$ とおくと $f = x^2 + x + 1$ と書ける. そこで

$$g = X^2 + X + 1 \in \mathbb{F}_p[X]$$

とすれば、$f = g(X^{p^2})$ となる。ここで $f' = 2p^2 X^{2p^2-1} + p^2 X^{p^2-1} = 0$ だから、注意 *71* により、f は分離多項式ではない[12]。

g の分離性を調べよう。まず、$g' = 2X + 1$. 今、$p = 2$ とすれば $g' = 1 \neq 0$, すなわち g と g' は $\overline{\mathbb{F}_2}$ の中で共通零点を持たないから、g は分離多項式である。また、$p \geq 3$ の場合、2 は $\mathbb{F}_p$ の中で可逆元だから、g と g' の共通零点の候補としては、g' の零点である $a = -2^{-1} \in \mathbb{F}_p$ が考えられる。 ところが

$$g(a) = 2^{-2} - 2^{-1} + 1 = 2^{-2}(1 - 2 + 2^2) = 2^{-1} \cdot 3$$

だから、$g(a) = 0$ となるのは $p = 3$ の場合のみ。そこで $p \neq 3$ の場合は、g と g' は共通零点を持たず、g は分離多項式となる。$p = 3$ の場合、$a = -2^{-1} = 1$ であり $g = (x-1)^2 (= x^2 - 2x + 1 = x^2 + x + 1)$ と分解されるので、g は既約でも分離的でもない。

[12]有限体が完全体であることを使うと、f の非分離性から、f が既約でないことがわかる。

例 77 での考察を一般的に扱ったのが、以下の結果である。

命題 78. 有限次代数拡大 L/K について、$\mathrm{char}(K) = p > 0$ とすると、以下が成り立つ。

(i) 任意の $a \in L$ に対する K 上の最小多項式を f とすると、K 上の分離多項式 g と $r \in \mathbb{N}$ が存在して $f = g(X^{p^r})$ となる。

(ii) $[L : K] = p^r[L : K]_s$ となる $r \in \mathbb{N}$ が存在する。従って特に、$[L : K] \geq [L : K]_s \geq 1$ で、$[L : K]_s$ は $[L : K]$ の約数である。

Proof. (i) の証明: $a \in L$ の K 上の最小多項式を f とし、適当な多項式 $g \in K[X]$ によって $f = g(X^{p^r})$ と書けるような $r \in \mathbb{N}$ の最大値をとる。すると f が既約だから、g も既約でなければならない。さらに、$g(X)$ は分離多項式になる。実際、

- まず、$g' \neq 0$ である。

  Proof. $g = \sum_{i=0}^{n} c_i X^i$ とおくと $g' = \sum_{i=1}^{n} i c_i X^{i-1}$. すると $g' \equiv 0$ は $ic_i = 0$ $(i = 1, \ldots, n)$ と同値であり、$\mathrm{char}(K) = p > 0$ だから、それは各 i に対して、$p|i$ か $c_i = 0$ であることと同値である。従って、適当な $h \in K[X]$ によって $g(X) = h(X^p)$ となることと同値である。従って、$f(X) = h(X^{p^{r+1}})$ となってしまい、$r \in \mathbb{N}$ の最大性に反する。よって $g' \neq 0$ でなければならない。 □

- すると、もし g が非分離的であれば、定理 69 の証明と同様ににして $g = hk$ となる $h, k \in K[X]$ が存在することがわかる。よって $f = h(X^{p^r})k(X^{p^r})$ となって、f の既約性に反する。

(ii) の証明: L/K は有限次代数拡大だから、$L = K(a_1, \ldots, a_k)$ の形に書ける。$a_1 \in L$ とその最小多項式 $f_1 \in K[X]$ に補題 73 と (i) を適用すれば、$[K(a_1) : K] = p^{r_1}[K(a_1) : K]$ なる $r_1 \in \mathbb{N}$ が存在することが分かる。次に $a_1 \in L$ の最小多項式 $f_1 \in K(a_1)[X]$ に同様の考察を行って $[K(a_1, a_2) : K(a_1)] = p^{r_2}[K(a_1, a_2) : K(a_1)]_s$ なる $r_2 \in \mathbb{N}$ の存在がわかる。同様にして、

$$
\begin{aligned}
&[K(a_1, \ldots, a_k) : K] \\
&= [K(a_1, \ldots, a_k) : K(a_1, \ldots, a_{k-1})][K(a_1, \ldots, a_{k-1}) : K(a_1, \ldots, a_{k-2})] \\
&\quad \cdots [K(a_1, a_2) : K(a_2)][K(a_1) : K] \quad \text{命題 14 より} \\
&= p^{r_k}[K(a_1, \ldots, a_k) : K(a_1, \ldots, a_{k-1})]p^{r_{k-1}}[K(a_1, \ldots, a_{k-1}) : K(a_1, \ldots, a_{k-2})] \\
&\quad \cdots p^{r_2}[K(a_1, a_2) : K(a_2)]p^{r_1}[K(a_1) : K]_s \\
&= p^r[K(a_1, \ldots, a_k) : K]_s \qquad (r = r_1 + \cdots + r_k) \quad \text{命題 76 より}
\end{aligned}
$$

を得る。 □

さて、K 上代数的な元 $a_1, \ldots, a_n$ による拡大体 $K(a_1, \ldots, a_n)$ が代数拡大であることを定理 25 で示したが、K 上分離代数的な $a_1, \ldots, a_n$ による拡大体 $K(a_1, \ldots, a_n)$ は果たして分離的であろうか？次の結果は、このことを示している。証明のポイントは、$[L : K]$ は線形空間としての次数、$[L : K]_s$ は体の間の写像の個数を表しているが、両者が分離的拡大の時に一致することである。

定理 79. L/K が有限次拡大とするとき、以下は同値：
(i) L/K は分離拡大
(ii) K 上分離的な適当な要素 $a_1, \ldots, a_n \in L$ によって、$L = K(a_1, \ldots, a_n)$ となる。
(iii) $[L : K]_s = [L : K]$

Proof. $(i) \Rightarrow (ii)$: L/K が有限次拡大だから、$L = K(a_1, \ldots, a_n)$ の形に書けるが、(i) より分離拡大だから $a_1, \ldots, a_n \in L$ は全て K 上分離的でなければならない。
$(ii) \Rightarrow (iii)$: (ii) より $L = K(a_1, \ldots, a_n)$ だとして、$L_i = K(a_i, \ldots, a_n), i = 1, \ldots, n$ とおく。すると L_i/L_{i+1} $(i = 1, \ldots, n-1)$, および L_n/K は単純拡大であり、命題 14 より

$$[L : K] = [L_1 : L_2][L_2 : L_3] \cdots [L_{n-1} : L_n][L_n : K]$$

また命題 76 より

$$[L : K]_s = [L_1 : L_2]_s[L_2 : L_3]_s \cdots [L_{n-1} : L_n]_s[L_n : K]_s$$

となるから、結局 L が単純拡大の場合 $L = K(a)$ について (iii) を証明すれば十分である。そこで a の K 上の最小多項式を $f \in K[X]$ とおき、$\deg f = n$ とすると、$[L : K] = n$. いっぽう、a は K 上分離的だから、f は相異なる n 個の零点を持つ。従って補題 49(ii) より、$\sigma : L = K(a) \longrightarrow \overline{K}$ なる K-準同型写像は f の相異なる零点ごとに 1 つずつ決まるから、$n = \sharp \mathrm{Hom}_K(L, \overline{K}) = [L : K]_S$ となり、結局 $[L : K] = [L : K]_S$ となる。
$(iii) \Rightarrow (i)$: 定理 69 より $\mathrm{char}(K) = 0$ の場合は、L/K はいつでも分離拡大だから、$\mathrm{char}(K) = p > 0$ の場合についてだけ証明すればよい。すなわち、任意 $a \in L$ に対して、これが K 上分離的であることを示せばよい。a の K 上の最小多項式を f とする。このとき、命題 78 より分離多項式 $g \in K[X]$ と適当な $r \in \mathbb{N}$ に対して

$$f = g(X^{p^r})$$

となる。従って $\deg f = p^r \deg g$ であるから、

$$[K(a) : K] = p^r[K(a) : K]_s$$

そこで

$$\begin{aligned}
[L : K] &= [L : K(a)][K(a) : K] \\
&\geq [L : K(a)]_s \cdot p^r[K(a) : K]_s \\
&\qquad (\text{命題 78 より } [L : K(a)] \geq [L : K(a)]_s) \\
&= p^r[L : K]_s \quad (\text{命題 76}). \\
&= p^r[L : K] \quad (iii).
\end{aligned}$$

よって $[L : K] = p^r[L : K]$ となり、$r = 0$, 従って $f = g$ で f は元々分離的。すなわち a は K 上分離的である。 □

以下の結果は、命題 26 の分離拡大版である。

系 80. 拡大体の列 $K \subset L \subset M$ を考える。M/L, L/K が分離拡大ならば、M/K もまた分離拡大である。

Proof. $a \in M$ の L 上の最小多項式 $f \in L[x]$ をとる。M/L は分離的だから, f は分離多項式である。f の係数を K に付け加えた有限拡大 L'/K をとる：$L \supset L' \supset K$. このとき a の L' 上の最小多項式はやはり f だから、$L'(a)/L'$ は分離的である。また、L/K は分離的だから、L'/K も分離的有限拡大。そこで

$$[L'(a) : K]_s = [L'(a) : L']_s[L' : K]_s = [L'(a) : L'][L' : K] = [L'(a) : K]$$

となるから、$L'(a)/K$ は分離的。従って特に $a \in L$ は K 上分離的となる。 □

5.2. **原始元定理.**

例 81. $K = \mathbb{Q}$ の拡大体 $L = \mathbb{Q}(\sqrt[3]{-2}, \sqrt{-3})/\mathbb{Q}$ を考える。$\mathrm{char}(\mathbb{Q}) = 0$ だから定理 *69* により、これは $\mathbb{Q}$ に 2 つの代数的元を付け加えて得られる分離的代数拡大である。これを単純拡大として書き直せないだろうか？今 $t = \sqrt[3]{-2} + a\sqrt{-3}$, $a \in \mathbb{Q}$, とおいてみると、$t \in L$ だから、$K(t) \subset L$ である。ここで t の $\mathbb{Q}$ 上の最小多項式 $f \in \mathbb{Q}[x]$ が $\deg f = 6$ ならば、$[L : K] = [K(t) : K] = 6$ だから $L = k(t)$ となる。そこで

$$t - a\sqrt{-3} = \sqrt[3]{-2}$$

の両辺を *3* 乗することにより

$$t^3 - 9a^2t + 2 = 3a(t^2 - a^2)\sqrt{-3}$$

を得るので、この両辺をさらに *2* 乗すれば

$$t^6 + 9a^2t^4 + 4t^3 + 27a^4t^2 - 36a^2t + 27a^6 + 4 = 0$$

となる。従って、

$$f = x^6 + 9a^2x^4 + 4x^3 + 27a^4x^2 - 36a^2x + 27a^6 + 4 \in \mathbb{Q}[x]$$

が既約になるように $a \in \mathbb{Q}$ を選ぶことができればよい。$f(t) = 0$ の式の両辺に任意の $\varphi \in \mathrm{Aut}_K(L) = \{\varphi_0, \ldots, \varphi_5\}$ *(*例 *61* 参照*)* を作用させると、$f(\varphi(t)) = 0$ となるから、$\varphi(t)$ はこの多項式の零点になっているはずである。とくに、$\varphi_i(t)$, $i = 0, \ldots, 5$ が全て異なっていれば、

$$f = (x - \varphi_0(t))(x - \varphi_1(t))(x - \varphi_2(t))(x - \varphi_3(t))(x - \varphi_4(t))(x - \varphi_5(t))$$

となり、f は分離的で、これが t の $K = \mathbb{Q}$ 上の最小多項式になり、$\deg f = 6$ が言える。

$\varphi_i(t)$, $i = 0, \ldots, 5$ を全て下記下すと以下のようになる。

$$\begin{aligned}
\varphi_0(t) &= \sqrt[3]{-2} + a\sqrt{-3} \\
\varphi_1(t) &= \zeta\sqrt[3]{-2} + a\sqrt{-3} \\
\varphi_2(t) &= \zeta^2\sqrt[3]{-2} + a\sqrt{-3} \\
\varphi_3(t) &= \sqrt[3]{-2} - a\sqrt{-3} \\
\varphi_4(t) &= \zeta\sqrt[3]{-2} - a\sqrt{-3} \\
\varphi_5(t) &= \zeta^2\sqrt[3]{-2} - a\sqrt{-3}
\end{aligned}$$

つまり、$\mathbb{Q} \ni a \neq 0$ であれば何でもよいことがわかる。$a = 0$ ならば、$f = (x^3 + 2)^2$ となることに注意。

例 74 の考察を一般化して、以下の結果を得る。

命題 82 (原始元定理)**.** L/K が有限次分離拡大ならば、適当な元 $a \in L$ によって、$L = K(a)$ と単純拡大になっている。

Proof. まず K が有限体の場合を考える。すると L/K は有限次拡大なので、L もまた有限体である。すると乗法部分群 $L^* := L - \{0\}$ は有限巡回群である（命題 123)。L^* の巡回群としての生成元 $a \in L$ は、勿論 K 上の拡大体としての L の生成元でもある。

次に K が無限体の場合を考える。L/K が有限次拡大だから、$L = K(a_1, \ldots, a_n)$ の形で書けるが、$L = E(a_1, a_2),\ E := K(a_3, \ldots, a_n)$ と考えると、L/E が分離拡大である。そこで、もし $L = E(a)$ となる $a \in L$ が選べることがわかれば、次は $L = E'(a, a_3),\ E' := K(a_4, \ldots, a_n)$ に同様の議論を行って $L = E'(a')$ となる $a' \in L$ を見つける。同様の議論を繰り返せば、結局 $L = K(a'')$ なる $a'' \in L$ がみつかることになる。従って $n = 2$ の場合、すなわち $L = K(a, b)$ の場合だけ証明できればよい。

L/K の分離指数 $[L : K]_s = n$ とし、互いに相異なる。

$$\sigma_1, \ldots, \sigma_n \in \mathrm{Hom}_K(L, \overline{K})$$

をとる。そこで多項式

$$P = \prod_{i \neq j} [(\sigma_i(a) - \sigma_j(a)) + (\sigma_i(b) - \sigma_j(b))X] \in \overline{K}[X]$$

を考える。これは 0 多項式にはならない。実際、$P \equiv 0$ ならば、$\sigma_i(a) = \sigma_j(a)$ かつ $\sigma_i(b) = \sigma_j(b)$ となる $i \neq j$ が存在するはず。しかし、$L = K(a, b)$ だから、これは $\sigma_i = \sigma_j$ となってしまい、$\sigma_i,\ i = 1, \ldots, n$ のとりかたに反する。さて、$P \not\equiv 0$ ゆえ P の K における零点は高々有限個。ところが K は無限体だから、$P(c) \neq 0$ となるような $c \in K$ が存在する。P の定義式に $X = c$ を代入することにより、$i \neq j$ なる全ての i, j に対して

$$0 \neq\ \sigma_i(a) + c\sigma_i(b) - (\sigma_j(a) + c\sigma_j(b)) \in \overline{K}$$

を得る。すなわち、

$$\sigma_i(a) + c\sigma_i(b) = \sigma_i(a + cb) \in \overline{K}$$

は $i = 1, \ldots, n$ に対して全て相異なる。そこで $a + cb \in L$ の K 上の最小多項式を $f \in K[X]$ とすると、$\sigma_i(a+cb),\ i = 1, \ldots, n$ は $f(X)$ の零点である。よって $\deg f \geq n$. よって

$$[L : K]_s = n \leq \deg f = [K(a + cb) : K] \leq [L : K]$$

となる。ところが L/K は分離拡大だから $[L : K]_s = [L : K]$ となり、従って $[K(a + cb) : K] = [L : K]$. よって $L = K(a + cb)$ である。 □

まとめ

- 分離多項式、分離拡大、完全体

- 標数 0 の体は完全体
- 分離次数
- 分離次数と拡大次数が等しい場合が分離拡大
- 正規拡大の分離次数は自己同型群の位数
- 分離的元で生成された代数拡大は分離拡大
- 分離拡大の分離拡大は、また分離拡大
- 有限次分離拡大は単純拡大にできる（原始元定理）

6. Galois 拡大と Galois の基本定理

代数拡大 L/K が正規拡大かつ分離拡大の時、Galois 拡大と呼ぶ。定理 62 より $\mathrm{Hom}_K(L,\overline{L}) = \mathrm{Aut}_K(L)$ となり、この自己同型群の位数は命題 75 により分離指数 $[L:K]_s$ に等しい。さらに分離拡大だから、定理 79 より、この値は拡大次数 $[L:K]$ に等しい。この群は Galois 群と呼ばれ、L/K の性質を調べるための強力な道具となる。

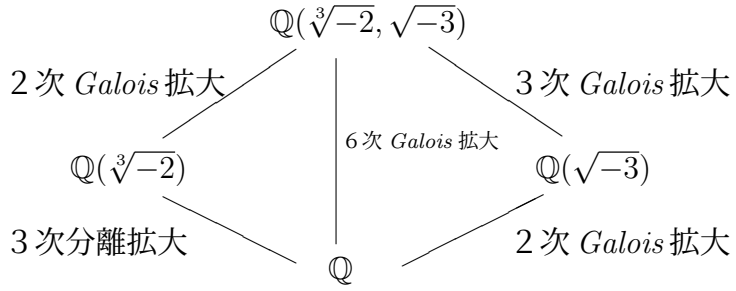
6.1. Galois 拡大.

定義 83 (Galois 拡大)**.** 代数拡大 L/K が、正規かつ分離的であるとき、**Galois 拡大** *(ガロア拡大)* と呼ぶ。このとき、$\mathrm{Gal}\,(L/K) := \mathrm{Aut}_K(L)$ のことを *Galois* 拡大 L/K の *Galois* 群と呼ぶ。

例 84. 定理 *69* より $\mathbb{Q}$ の代数拡大は全て分離的であり、例 *61* によりさらに正規性も言えているから、$\mathbb{Q}(\sqrt[3]{-2},\sqrt{-3})$ は $\mathbb{Q}$ の *6* 次のガロア拡大である。また、$\mathbb{Q}(\sqrt{-3})$ の *3* 次の *Galois* 拡大にもなっている。何故ならば、$\mathbb{Q}(\sqrt[3]{-2},\sqrt{-3})$ は $\mathbb{Q}(\sqrt{-3})$ に $\sqrt[3]{-2}$ を付け加えた単純拡大であるが、最小多項式は $g = X^3+2 \in \mathbb{Q}(\sqrt{-3})[X]$ となり、$\zeta = \frac{-1+\sqrt{-3}}{2} \in \mathbb{Q}(\sqrt{-3})$ に注意すると $\mathbb{Q}(\sqrt[3]{-2},\sqrt{-3})$ は

$$g = (x-\sqrt[3]{-2})(x-\zeta\sqrt[3]{-2})(x-\zeta\sqrt[3]{-2})$$

の分解体、すなわち正規拡大になっているからである。同様に考えて、$\mathbb{Q}(\sqrt[3]{-2})$ の 2 次のガロア拡大でもある。また、$\mathbb{Q}(\sqrt{-3})$ は $\mathbb{Q}$ の 2 次のガロア拡大。しかし $\mathbb{Q}(\sqrt[3]{-2})/\mathbb{Q}$ は $\mathrm{char}(\mathbb{Q}) = 0$ だから分離拡大ではあるが、正規拡大ではなく *(*例 *47* 参照*)*、従って *Galois* 拡大ではない。



命題 85. L/K を *Galois* 拡大とし、$a \in L$ の K 上の最小多項式を $f \in K[X]$ とする。この時、$b \in \overline{K}$ を f の a 以外の零点とすると、$\sigma \in \mathrm{Gal}\,(L/K)$ で $\sigma(a) = b$ となるものが存在する。

Proof. ここで L/K が正規拡大だから $b \in L$ である。さて、埋め込み準同型 $K(\alpha) \hookrightarrow L$ に補題 $49(ii)$ を適用することにより、K 準同型 $\sigma : K(\alpha) \longrightarrow L$ で $\sigma(a) = b$ となるものを得る。$L/K(a)$ は代数拡大だから、この σ は命題 50 により $\sigma : L \longrightarrow L$ なる K-準同型に拡張できる。すなわち、$\sigma \in \mathrm{Gal}\,(L/K)$, s.t. $\sigma(a) = b$ が得られた。 □

注意 86. 命題 85 の証明では、L/K が分離拡大であることは使っていない。従って L/K を正規拡大としても成り立つ。

定理 87. L/K を有限次 *Galois* 拡大とすると、$[L:K] = \sharp\mathrm{Gal}\,(L/K)$.

Proof. 命題 75 と定理 79 から直ちに従う。 □

6.2. **Galois の基本定理.** L/K を有限次 Galois 拡大とし、その Galois 群を $G := \mathrm{Gal}\,(L/K)$ とする。ここで述べる Galois の基本定理は、拡大体 L/K の中間体と群 G の部分群の対応関係 (Galois 対応) を与えるものである。そこで

$$\begin{aligned}\mathcal{G} &:= \{S \,:\, S \subseteq G \text{ 部分群}\}\\ \mathcal{K} &:= \{E \,:\, L \supseteq E \supseteq K \text{ 中間体}\}\end{aligned}$$

なる 2 つの集合を考える。ここで次のことに注意する。

命題 88. *Galois* 拡大 L/K の任意の中間体 E に対し、L/E もまた *Galois* 拡大。

Proof. L の任意の元 $a \in L$ は K 上分離的だから、その最小多項式 $f \in K[X]$ は分離的である。さらに $f \in E[X]$ と考えると、$f = f_1 f_2$ $f_1, f_2 \in E[X]$ と分解するかもしれないが、このとき f_1 か f_2 のいずれか一方が ($\overline{K}[X]$ の中で因数分解したときに) $X - a$ という因子を含むはずだから、(必要ならば f_i の添え字を付け替えて) f_1 が $X - a$ を因子として含む既約多項式と思ってよい。すると f_1 これが a の E 上の最小多項式になる。f が分離的だから、f_1 も分離的である。よって L/E は分離的。

次に、$\sigma \in \mathrm{Hom}_E(L, \overline{L})(\subset \mathrm{Hom}_K(L, \overline{L}))$ を任意にとると、L/K が正規拡大だから、定理 62 により $\sigma \in \mathrm{Aut}_K(L)$. しかも σ は E を固定するから、$\sigma \in \mathrm{Aut}_E(L)$ と考えることができ、再び定理 62 より L/E は正規拡大である。

よって L/K は分離的かつ正規拡大だから Galois 拡大である。 □

注意 89. 拡大体 $L \supset E \supset K$ にて、L/K が Galois 拡大なら L/E も Galois 拡大になるというのが命題 88 の主張だが、では E/K はどうかというと、これは必ずしも Galois 拡大にはならない。実際、例 84 で見たように、$L = \mathbb{Q}(\sqrt[3]{-2}, \sqrt{-3})/\mathbb{Q}$ は Galois 拡大だが、$\mathbb{Q}(\sqrt[3]{-2})/\mathbb{Q}$ は分離拡大であって正規拡大にはならない。では、E/K が Galois 拡大になるのはどういう場合かというと、その答は定理 91(ii) で与えられる。

以下の結果は、今後頻繁に使われる。

命題 90. L/K を *Galois* 拡大とし、中間体 $K \subset E \subset L$ を考える。もし E/K もまた正規拡大ならば、$\mathrm{Gal}\,(E/K)$ の元は以下のような群としての全射準同型写像によって得られる：

$$\mathrm{Gal}\,(L/K) \ni \sigma \longmapsto \sigma|_E \in \mathrm{Gal}\,(E/K).$$

Proof. 任意の $\sigma \in \mathrm{Gal}\,(L/K) \subset \mathrm{Hom}_K(L, \overline{L})$ を E に制限すれば、$\sigma|_E \in \mathrm{Hom}_K(E, \overline{L}) = \mathrm{Hom}_K(E, \overline{E})$ となる。ここで L/E が代数拡大だから、$\overline{L} = \overline{E}$ となることに注意。さ

れに、定理 62 より $\mathrm{Hom}_K(E,\overline{E}) = \mathrm{Aut}_K(E) = \mathrm{Gal}\ (E/K)$ だから、結局 $\sigma|_E \in \mathrm{Gal}\ (E/K)$ となる。よって制限写像

$$\rho : \mathrm{Gal}\ (L/K) \longrightarrow \mathrm{Gal}\ (E/K) \quad \rho(\sigma) = \sigma|_E$$

が得られる。また、任意の K 同型 $\sigma' : E \longrightarrow E \subset \overline{L}$, i.e., $\sigma' \in \mathrm{Gal}\ (E/K)$, に対し、$L/E$ が代数拡大であることから命題 50 により K 同型 $\sigma : L \longrightarrow \overline{L}$ が存在して、$\sigma|_E = \sigma'$ となる。ここで L/K が正規拡大だから、$\sigma \in \mathrm{Aut}_K(L) = \mathrm{Gal}\ (L/K)$ となる。すなわち、$\rho(\sigma) = \sigma'$ となって、制限写像 ρ は全射とわかる。 □

$\mathcal{G}$ と $\mathcal{K}$ の間の写像 (Galois 対応) を以下のように定義する。

- 部分群を中間体に対応させる：

$$\begin{aligned} \Phi : \ \mathcal{G} \ &\longrightarrow \mathcal{K} \\ H \ &\mapsto L^H := \{x \in L \ : \ \sigma(x) = x \ \forall \sigma \in H\} \end{aligned}$$

演習問題 3. Φ が *well-defined* であること、すなわち、L^H が確かに L/K の中間体になることを、次の順序で証明せよ。
(1) $L \supset L^H$ であることは、定義より明らか。
(2) 任意の $a \in K$ は任意の $\sigma \in H$ によって $\sigma(a) = a$ となることを確かめることにより、$K \subset L^H$ を示す。
(3) L^H が体であることを示す。そのために任意の $a, b \in L^H$ に対して、$a + b$, $-a$, $a \cdot b$, a^{-1} (これらは L の元としての演算を考える）が全て L^H に含まれていることを示す。

- 中間体を部分群に対応させる：

$$\begin{aligned} \Psi : \ \mathcal{K} \ &\longrightarrow \mathcal{G} \\ E \ &\mapsto \mathrm{Gal}\ (L/E)\ (\subseteq \mathrm{Gal}\ (L/K) = G) \end{aligned}$$

Ψ が well-defined であること、すなわち、$\mathrm{Gal}\ (L/E)$ が存在することは命題 88 より従う。

このとき、以下が成り立つ：

定理 91 (Galois の基本定理)**.** 有限次 *Galois* 拡大 L/K と、上で定義した *Galois* 対応 Φ ,Ψ に対し、以下が成り立つ。
(i) $\Psi \circ \Phi = Id_{\mathcal{G}}$ かつ $\Phi \circ \Psi = Id_{\mathcal{K}}$. すなわち、$\Phi$, Ψ は全単射で、互いに他の逆写像になっている。
(ii) L^H/K が *Galois* 拡大 $\Leftrightarrow$ $H \lhd G$ (正規部分群)
(iii) (ii) が成り立っているとき、$\mathrm{Gal}\ (L^H/K) \cong G/H$.

とくに定理 91(i) は以下のような対応関係が成立することを主張している：

中間体		Galois 群
L	$\leftrightarrow$	$\mathrm{Gal}\,(L/L) = 1$
$\cup$		$\cap$
E_1	$\leftrightarrow$	$\mathrm{Gal}\,(L/E_1)$
$\cup$		$\cap$
E_2	$\leftrightarrow$	$\mathrm{Gal}\,(L/E_2)$
$\cup$		$\cap$
$\vdots$		$\vdots$
$\cup$		$\cap$
E_k	$\leftrightarrow$	$\mathrm{Gal}\,(L/E_k)$
$\cup$		$\cap$
K	$\leftrightarrow$	$\mathrm{Gal}\,(L/K)$

上の中間体の例と部分群の列とで、包含関係が逆転しているところにも注意。この理由については、以下の演習問題を参照せよ。

演習問題 4. 群 G が集合 X に作用しているとする。このとき、任意の部分群 $H \subset G$ に対し、$X^G \subset X^H$ であることを示せ。ただし、$X^G := \{x \in X |\ \sigma(x) = x\ \forall \sigma G\}$ と定義され、X^H も同様に定義されるものとする。

例 92. 例 *84* で考えた、$K = \mathbb{Q}$ の *Galois* 拡大 $L = \mathbb{Q}(\sqrt[3]{-2}, \sqrt{-3})$ やその部分体と *Galois* 群の対応関係をみてみよう。まず *Galois* 群は例 *74* でみたように

$$\mathrm{Gal}\,(L/K) = \{\varphi_0, \ldots, \varphi_5\}$$

で、つぎの関係式が成り立つことがわかる：

$$\begin{aligned}
\mathrm{id}_L &= \varphi_0 = \varphi_1 \circ \varphi_1 \circ \varphi_1 = \varphi_3 \circ \varphi_3 = \varphi_4 \circ \varphi_4 = \varphi_5 \circ \varphi_5 \\
\varphi_2 &= \varphi_1 \circ \varphi_1, \\
\varphi_4 &= \varphi_1 \circ \varphi_3, \\
\varphi_5 &= \varphi_1 \circ \varphi_1 \circ \varphi_3 = \varphi_3 \circ \varphi_1
\end{aligned}$$

そこで、$a = \varphi_1$, $b = \varphi_3$ とおけば、

$$\mathrm{Gal}\,(L/K) = \langle a, b \mid a^3 = b^2 = 1, a^2 b = ba \rangle = \{1, a, a^2, b, ab, a^2 b\}$$

と書き表すことができる。$a^2 = \varphi_2$, $ab = \varphi_4$, $a^2 b = \varphi_5$ である。これは 3 次対称群 $\mathfrak{G}_3$ と同型な群であることに注意しよう。従って、集合 $\mathcal{G}$ は、次のような部分群の集合である：

(1) $\langle a \rangle$ 位数 3 の巡回正規部分群
(2) $\langle b \rangle$, $\langle ab \rangle$, $\langle a^2 b \rangle$ 位数 2 の巡回部分群
(3) 1 (単位群), $\mathrm{Gal}\,(L/K)$

そこで、これらに対応する中間体を計算すると、

$$\begin{aligned}
\Phi(\langle a\rangle) &= \{x\in L \mid \varphi_1(x)=x\} = \mathbb{Q}(\sqrt{-3})\\
\Phi(\langle b\rangle) &= \{x\in L \mid \varphi_3(x)=x\} = \mathbb{Q}(\sqrt[3]{-2})\\
\Phi(\langle ab\rangle) &= \{x\in L \mid \varphi_4(x)=x\} = \mathbb{Q}(\sqrt[3]{-2}(1+\sqrt{-3}))\\
\Phi(\langle a^2b\rangle) &= \{x\in L \mid \varphi_5(x)=x\} = \mathbb{Q}(\sqrt[3]{-2}(1-\sqrt{-3}))\\
\Phi(1) &= \{x\in L \mid \varphi_1(x)=x\} = L = \mathbb{Q}(\sqrt[3]{-2},\sqrt{-3})\\
\Phi(\mathrm{Gal}\,(L/K)) &= \{x\in L \mid \varphi_i(x)=x,; i=0,1,2,3,4,5\} = K = \mathbb{Q}
\end{aligned}$$

Galois の基本定理 *(*定理 *91)* は、これらが L/K の中間体のすべてであり、また、$\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$ は *Galois* 拡大で、その *Galois* 群 $\mathrm{Gal}\,(\sqrt{-3}/\mathbb{Q})$ は剰余群 $\langle a,b\rangle/\langle a\rangle \cong \langle b\rangle$、すなわち

$$\mathrm{Gal}\,(\mathbb{Q}(\sqrt{-3})/\mathbb{Q}) = \{\mathrm{id},\ \sigma : \sqrt{-3}\mapsto -\sqrt{-3}\}$$

であることを主張している。$\mathbb{Q}(\sqrt[3]{-2})/\mathbb{Q}$ が *Galois* 拡大でないことは、例 *47* の考察によって正規拡大でないことからわかる。また、$\mathbb{Q}(\sqrt[3]{-2}(1+\sqrt{-3}))$ が $\mathbb{Q}$ の *Galois* 拡大でないことは、次のようにしてわかる。$\sqrt[3]{-2}(1+\sqrt{-3})$ の $\mathbb{Q}$ 上の最小多項式は $X^3-16\in\mathbb{Q}[X]$ であり、それは $\sqrt[3]{-2}(1+\sqrt{-3}) = -2\zeta^2\sqrt[3]{-2}$ となることに注意すると

$$X^3-16 = (X+2\zeta\sqrt[3]{-2})(X+2\zeta^2\sqrt[3]{-2})(X+2\sqrt[3]{-2})$$

と因数分解することがわかる。そして

$$-2\zeta\sqrt[3]{-2} = \sqrt[3]{-2}(1-\sqrt{-3}) = -\frac{1}{2}(\sqrt[3]{-2}(1+\sqrt{-3}))^2 \in \mathbb{Q}(\sqrt[3]{-2}(1+\sqrt{-3}))$$

であるが、$2\sqrt[3]{-2}\notin\mathbb{Q}(\sqrt[3]{-2}(1+\sqrt{-3}))$ だから[13]、$\mathbb{Q}(\sqrt[3]{-2}(1+\sqrt{-3}))$ は X^3-16 の分解体ではなく、従って正規でない。つまり *Galois* 拡大でもない。同様にして 3 次拡大 $\mathbb{Q}(\sqrt[3]{-2}(1-\sqrt{-3}))/\mathbb{Q}$ も *Galois* 拡大でないことがわかる。

6.3. **Galois の基本定理の証明.** 有限次 Galois 拡大 L/K が与えられたとする。

6.3.1. $\Phi\circ\Psi = \mathrm{id}$ の証明. 任意の中間体 E, $K\subseteq E\subseteq L$, を考える。このとき命題 88 より L/E も Galois 拡大であから、その Galois 群 $H = \mathrm{Gal}\,(L/E)$ を考えることができるが、

Claim 1: H は $\mathrm{Gal}\,(L/K)$ の部分群である。

Claim 1 の証明. 任意の元 $\sigma\in\mathrm{Gal}\,(L/E) = \{\sigma\in\mathrm{Aut}(L)\ :\ \sigma(x)=x\ \forall x\in E\}$ をとると、$K\subseteq E$ ゆえ、$\sigma\in\mathrm{Gal}\,(L/K) = \{\sigma\in\mathrm{Aut}(L)\ :\ \sigma(x)=x\ \forall x\in K\}$) だから、集合としての包含関係 $\mathrm{Gal}\,(L/E)\subset\mathrm{Gal}\,(L/K)$ が成り立つ。また $\mathrm{Gal}\,(L/E)$ 自身は群であり、その演算も $\mathrm{Aut}(L)$ の元として $\mathrm{Gal}\,(L/K)$ のものと同じなので、$\mathrm{Gal}\,(L/K)$ の部分群になっている。 □

Claim 2: $E = L^H$. すなわち $\Phi\circ\Psi = id$

[13]このことは、$\mathbb{Q}(\sqrt[3]{-2}(1+\sqrt{-3})) = \mathbb{Q}\cdot 1\oplus\mathbb{Q}\cdot\sqrt[3]{-2}(1+\sqrt{-3})\oplus\mathbb{Q}\cdot(\sqrt[3]{-2}(1+\sqrt{-3}))^2 = \mathbb{Q}\cdot1\oplus\mathbb{Q}\cdot\sqrt[3]{-2}(1+\sqrt{-3})\oplus\mathbb{Q}\cdot\sqrt[3]{4}(1-\sqrt{-3})$ だから、$2\sqrt[3]{-2} = a\cdot1\oplus b\cdot\sqrt[3]{-2}(1+\sqrt{-3})\oplus c\cdot\sqrt[3]{4}(1-\sqrt{-3})$ となるような $a,b,c\in\mathbb{Q}$ が存在しないことを確かめればわかる。

*Claim 2*の証明. 定義により $L^H = \{\alpha \in L \,:\, \sigma(\alpha) = \alpha\ \forall \sigma \in H\}$ であるが、任意の元 $\sigma \in H = \mathrm{Gal}\,(L/E)$ は E の元を固定する。従って

$$E \subseteq L^H.$$

ここで、$E \neq L^H$ であると仮定すると、$\alpha \in L^H - E$ なる元が存在する。そこで α の E 上の最小多項式を $f \in E[X]$ とおくと、L/E が Galois 拡大だから、

$$f = (X-\alpha)(X-\alpha_1)\cdots(X-\alpha_n)$$

$\alpha, \alpha_1, \ldots, \alpha_n \in L$ で (L/E が正規拡大だから)、これらはすべて相異なる元のはず（L/E は分離拡大だから）。もし $n \geq 1$ ならば、$\tau : \alpha \mapsto \alpha_1$ となるような $\tau \in \mathrm{Gal}\,(L/E) = H$ が存在するはずだが (命題 85)、$\alpha \in L^H$ だから、任意の $\tau \in \mathrm{Gal}\,(L/E)$ に対して $\tau(\alpha) = \alpha$ となって矛盾。したがって $n = 0$ すなわち、$\alpha \in L^H$ の E 上の最小多項式は 1 次式。これは $\alpha \in E$ であることを意味し、α のとりかたに反する。従って $E \neq L^H$ ではあり得ず、結局 $E = L^H$ でなければならないことになる。 □

注意 93. 以上の証明では、L/K が Galois 拡大であることは使っているが、それが有限次拡大であることは使っていない。すなわち、上の部分は無限次 Galois 拡大でも成り立つ。

6.3.2. $\Psi \circ \Phi = \mathrm{id}$ の証明. 任意の部分群 $H \subset G$ に対して、中間体 $\Phi(H) = L^H =: E$ をとると、$\Psi \circ \Phi(H) = \mathrm{Gal}\,(L/E)$. そこで $H = \mathrm{Gal}\,(L/E)$ を示せばよい。

特に L/K が有限次分離代数拡大だから、L/E もそうである。そこで命題 82 より適当な元 $a \in L$(原始元) をとれば $L = E(a)$ となる。また、G は有限群だから、H も有限群なので $\sharp H = n(< \infty)$ と置く。このとき、

Claim: $[L : E] \leq n$

Claim の証明. $\sigma_1, \ldots, \sigma_r \in H$ を $\sigma_1(a), \ldots, \sigma_r(a)(\in L)$ が相異なるようなもので極大なもの、すなわち、それ以外のどの $\sigma \in H$ に対しても $\sigma(a)$ がいずれかの $\sigma_i(a)$ に等しくなってしまうものを選ぶ（H は有限群なので、当然 r も有限である)。ここで、任意の $\sigma \in H$ に対して、

$$S := \{\sigma_1(a), \ldots, \sigma_r(a)\} = \{\sigma(\sigma_1(a)), \ldots, \sigma(\sigma_r(a))\} = \sigma(S)$$

となる。実際、$\sigma(\sigma_i(a)) \notin S$ ならば、$\sigma_{r+1} = \sigma \circ \sigma_i$ とすれば、上の列は $\sigma_1, \ldots, \sigma_r, \sigma_{r+1}$ まで拡大できることになり、極大性に反する。また、σ は L の同型写像だから、$\sigma(\sigma_1(a)), \ldots, \sigma(\sigma_r(a))$ は全て異なる元である。従って、上の 2 つの集合は一致し、H の任意の元 σ は S の r 個の元の並べ替えとして作用する。すると、$\sigma_1(a), \ldots, \sigma_r(a)$ でつくられた基本対称式[14]は、H によって固定されるから、$E = L^H$ の元になる。従って多項式

$$f = \prod_{i=1}^{r}(X - \sigma_i(a)) \in E[X]$$

[14]式 $f_1, \ldots, f_m$ の i 次基本対称式とは、$\prod_{j=1}^{m}(X - f_j)$ を展開したときの X^{m-i} の係数（かその符号を変えたもの）であり、添え字 j を入れ替えても式全体としては変わらないという性質をもつ。例えば $m = 3$ の時は、$f_1 + f_2 + f_3$, $f_1f_2 + f_2f_3 + f_1f_3$, $f_1f_2f_3$ が基本対称式である。

を得る。これは $a \in L$ の E 上の最小多項式（を因数に含む）分離多項式である。従って、$[L:E] = [E(a):E] \leq \deg f = r \leq n$ となる。 □

すると、定理 87 を使って

$$n = \sharp H \leq \sharp \mathrm{Gal}\,(L/E) = [L:E] \leq n$$

より $\sharp H = \sharp \mathrm{Gal}\,(L/E)$ となり、従って $H = \mathrm{Gal}\,(L/E)$ を得る。

6.3.3. L^H/K が *Galois* 拡大ならば、$H \triangleleft G$, $\mathrm{Gal}\,(L^H/K) \cong G/H$ となることの証明. L^H/K が Galois 拡大だから、分離拡大かつ正規拡大である。L/K が分離拡大だから、L/K は常に分離拡大になる。従って、ここで特に意味をもつのは、L^H/K が正規拡大であるということで、以下の証明でも正規拡大であることだけを使う。

L^H/K が正規拡大だから、命題 90 より群の全射準同型写像

$$\begin{array}{rccc} \varphi: & G := \mathrm{Gal}\,(L/K) & \longrightarrow & \mathrm{Gal}\,(L^H/K) \\ & \sigma & \longmapsto & \sigma|_{L^H} \end{array}$$

が存在する。

$$\mathrm{Ker}\,\varphi = \{\sigma \in \mathrm{Gal}\,(L/K) \mid \sigma(x) = x,\ \forall x \in L^H\} = \mathrm{Gal}\,(L/L^H) = H$$

となるが、準同型写像の核は正規部分群[15]だから、$H \triangleleft G$ となる。さらに群の準同型定理[16]により $\mathrm{Gal}\,(L^H/K) \cong G/H$ を得る。

6.3.4. $H \triangleleft G$ に対し、L^H/K が *Galois* 拡大であることの証明. L/K が Galois 拡大だから、分離拡大であり、従って L^H/K も分離拡大である。従って L^H/K が正規拡大であることを示せば、Galois 拡大であることが示せたことになる。そこで L の代数的閉包 $\overline{L}$ を 1 つとって固定すると、$\overline{K} \subset \overline{L^H} = \overline{L}$ と考えてよい。ここで $\mathrm{Hom}_K(L^H, \overline{L^H}) = \mathrm{Hom}_K(L^H, \overline{L})$ が $\mathrm{Aut}_K(L^H)$ と一致すること、すなわち任意の $\sigma \in \mathrm{Hom}_K(L^H, \overline{L})$ に対して $\sigma(L^H) = L^H$ であることが示せれば、L^H/K の正規性が示せたことになる。

まず、L/L^H が代数拡大なので、命題 50 により $\sigma : L^H \longrightarrow \overline{L}$ は $\sigma' : L \longrightarrow \overline{L}$ に拡張される（$\sigma'|_{L^H} = \sigma$）. ところが、L/K が正規拡大だから $\mathrm{Hom}_K(L, \overline{L}) = \mathrm{Aut}_K(L)$. よって $\sigma' \in \mathrm{Aut}_K(L)$ と考えられる。よって σ は L への K 準同型と考えられる：$\sigma \in \mathrm{Hom}_K(L^H, L)$. そこで任意の $b \in \sigma(L^H)$ をとる: $L \ni b = \sigma(a), \exists a \in L^H$. ここで $b \in L^H$ であることが示せればよい。すなわち b は H の作用によって固定されることを示せばよい。そこで任意の $\tau \in H$ をとる、$H \triangleleft G$ で $\sigma' \in G$ だから $H\sigma' = \sigma' H$ であり、ここでの群演算が写像の合成であることに注意すると、従って $\tau \circ \sigma' = \sigma \circ \tau'$ となる $\tau' \in H$ が存在する。すると

$$\begin{array}{rcll} \tau(b) & = & \tau \circ \sigma'(a) (= \tau \circ \sigma(a)) & (\sigma'|_L^H = \sigma,\ a \in L^H \text{ だから}) \\ & = & \sigma' \circ \tau'(a) = \sigma'(a) & (\tau' \in H,\ a \in L^H \text{ だから}) \\ & = & \sigma(a) = b & \end{array}$$

となり、$b \in L^H$. よって $\sigma(L^H) \subset L^H$. 最後に逆の包含関係 $\sigma(L^H) \supset L^H$ を示そう。L/K が代数拡大だから、$L \supset L^H \supset \sigma(L^H) \supset K$ なる拡大 $L^H/\sigma(L^H)$ もまた代数拡大である。そこで $\sigma^{-1} : \sigma(L^H) \longrightarrow L^H$ は命題 50 より $\rho : L^H \longrightarrow \overline{L}$ に拡

[15]群の準同型 $\varphi : G \longrightarrow G'$ に対し、$g^{-1}(\mathrm{Ker}\,\varphi)g \subset \mathrm{Ker}\,\varphi$ $(\forall g \in G)$ となる。実際、$\forall x \in \mathrm{Ker}\,\varphi$ に対し、$\varphi(g^{-1}xg) = \varphi(g)^{-1}\varphi(x)\varphi(g) = \varphi(g)^{-1}\varphi(g) = 1_{G'}$ となるからである。

[16]群の全射準同型 $\varphi : G \longrightarrow G'$ に対し、$G' \cong G/\mathrm{Ker}\,\varphi$ を主張するのが、準同型定理であった。

張される ($\rho|_{L-H} = \sigma^{-1}$). すると、$\sigma : L^H \longrightarrow \overline{L}$ に対して行った上の議論を繰り返すことによって、$\rho(L^H) = \sigma^{-1}(L^H) \subset L^H$, すなわち $L^H \subset \sigma(L^H)$ が得られ、結局 $\sigma(L^H) = L^H$ を得る。

まとめ

- 正規かつ分離的な代数拡大が Galois 拡大
- L/K が Galois 拡大なら、中間体 E に対して L/E も Galois 拡大。しかし E/K はそうとは限らない。
- L/K が Galois 拡大で、中間外 E に対しても E/K が Galois 拡大ならば、全射制限写像 Gal $(L/K) \longrightarrow$ Gal (E/K) が存在し、さらに、Gal $(E/K) \triangleleft$ Gal (L/K).
- L/K が有限次 Galois 拡大ならば、$[L : K] =$ Gal (L/K)
- L/K が有限次 Galois 拡大ならば、中間体と Galois 群の部分群との間に Galois 対応がある。

7. 円分拡大

Galois の基本定理により、Galois 拡大と群の対応関係が明らかになった。そこで次の問題は、さまざまな Galois 拡大の構造を群論をつかって詳しく調べることである。アーベル群に対応する Galois 拡大の構造はよく分かっているが、非アーベル群に対応するものについては、未知の問題も多く、現在も盛んに研究されている。

ここではアーベル群に対応する Galois 拡大の重要な例として、円分拡大を考える。

7.1. **1 の原始 n 乗根.** $\overline{K} = \mathbb{C}$ の場合は代数学序論 I で学んだが、ここではより一般の場合を考える。体 K とその代数的閉包 $\overline{K}$ を考える。$n \in \mathbb{N} - \{0\}$ に対して $X^n - 1$ の $\overline{K}$ における零点を 1 **の** n **乗根**と呼び、それら全体の集合 $U_n \subset \overline{K}^* := \overline{K} - \{0\}$ は乗法に関して群をなす。実際、$\alpha, \beta \in U_n$ ならば、$\alpha^n = \beta^n = 1$ であり、従って $(\alpha\beta)^n = 1$ となるから、$\alpha\beta \in U_n$. また $1 \in U_n$ は単位元であり、$\alpha \in U_n$ の逆元は α^{n-1} である。

(1) $\mathrm{char}(K) = 0$ **の場合:** $\frac{d}{dx}(X^n - 1) = nX^{n-1}$ と $X^n - 1$ は共通零点を持たないから、$X^n - 1$ は分離多項式であり、従って $\sharp U_n = n$ となる。

(2) $\mathrm{char}(K) = p > 0$ **の場合:** $n = p^r m$, $(r \in \mathbb{N},\ p \not| m)$ とすると、

$$X^n - 1 = X^{p^r m} - 1 = (X^m - 1)^{p^r}$$

となるから、$U_n = U_m$、$\sharp U_m = m$ となる。つまり 1 の n 乗根は 1 の m 乗根、$p \not| m$, の場合に帰着されてしまう。そこで以後、$\mathrm{char}(K) = p > 0$ の場合に 1 の n 乗根を考えるときは、$p \not| n$ なる条件をつけて考えることにする。

命題 94. $n \in \mathbb{N} - \{0\}$, $\mathrm{char}(K) \not| n$ に対して、U_n は位数 n の巡回群である。

Proof. U_k は $\overline{K}^*$ の有限乗法部分群だが、それは後述する命題 123 により、巡回群になる。 □

定義 95. U_n の巡回群としての生成元のことを 1 **の原始** n **乗根**と呼ぶ。

7.2. **Euler 関数.** 1 の原始 n 乗根の個数を数えるには、以下の Euler 関数の概念が必要である。

定義 96 (Euler 関数)**.** $n \in \mathbb{N} - \{0\}$ に対し

$$\varphi(n) = \sharp(\mathbb{Z}/n\mathbb{Z})^*$$

とおく。但し、$(\mathbb{Z}/n\mathbb{Z})^*$ は剰余環としての $\mathbb{Z}/n\mathbb{Z}$ の可逆元集合であり、したがって乗法群であることに注意する。この関数 $\varphi : \mathbb{N} - \{0\} \longrightarrow \mathbb{N}$ を **Euler 関数**と呼ぶ。

$a \in \mathbb{Z}$ の $\mathbb{Z}/n\mathbb{Z}$ における像 $\bar{a}$ が可逆元ということは、$xa + yn = 1$ となる $x, y \in \mathbb{Z}$ が存在することと同値だから、Euclid の互除法定理により $(a, n) = 1$ であることと同値である。従って、

命題 97. $\varphi(n) = \sharp\{a \mid 1 \leq a \leq n-1, (a, n) = 1\}$

Euler 関数の計算には、次の結果が便利である。

命題 98. $m, n \in \mathbb{N} - \{0\}$ に対して、もし $(m, n) = 1$ ならば $\varphi(mn) = \varphi(m)\varphi(n)$. また、$n = p_1^{n_1} \cdots p_r^{n_r}$ と因数分解したとき、

$$\varphi(n) = \prod_{i=1}^{r} p_i^{n_i - 1}(p_i - 1)$$

Proof. 中国人剰余定理[17] により

$$\psi : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \qquad a + mn\mathbb{Z} \longmapsto (a + m\mathbb{Z}, a + n\mathbb{Z})$$

は同型であるが、この同型がさらに、可逆元のなす乗法部分群の同型

$$(\mathbb{Z}/mn\mathbb{Z})^* \longrightarrow (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^* \tag{2}$$

を誘導することを示そう。

Claim 1: ψ を $(\mathbb{Z}/mm\mathbb{Z})^*$ に制限すれば、$(\mathbb{Z}/mn\mathbb{Z})^* \longrightarrow (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$ なる写像が得られる。

Claim 1 の証明. $(\mathbb{Z}/mn\mathbb{Z})^* \ni \overline{a} = a + mm\mathbb{Z} \in \mathbb{Z}/mn\mathbb{Z}$ を任意にとる。その逆元を $\overline{b} = b + mm\mathbb{Z}$ とすると、$ab = 1 + mn\ell$ $(\exists \ell \in \mathbb{Z})$ となっている。すると $ab = 1 + m(n\ell) \in 1 + m\mathbb{Z}$ と見れば $ab + m\mathbb{Z} = 1 + m\mathbb{Z}$ となり、また、$ab = 1 + n(m\ell) \in 1 + n\mathbb{Z}$ と見れば $ab + n\mathbb{Z} = 1 + n\mathbb{Z}$ である。すなわち、$\psi(\overline{a}) \in (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$ となる。 □

Claim 2: 制限写像 $\psi|_{(\mathbb{Z}/mn\mathbb{Z})^*} : (\mathbb{Z}/mn\mathbb{Z})^* \longrightarrow (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$ ψ が同型だから単射だが、さらに全射でもある (従って、全単射)。

Claim 2 の証明. $(\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$ の元 $(s + m\mathbb{Z}, t + n\mathbb{Z})$ とその逆元 $(\hat{s} + m\mathbb{Z}, \hat{t} + n\mathbb{Z})$ をとる。すると、Euclid の互除法定理により、

$$\hat{s}s + \hat{y}m = 1, \quad \hat{x}n + \hat{t}t = 1 \qquad (\exists \hat{x}, \hat{y} \in \mathbb{Z}).$$

また、$(m.n) = 1$ だから、再び Euclid の互除法定理により、$xm + yn = 1$ なる $x, y \in \mathbb{Z}$ が存在する。そこで、$a := xmt + yns$ とおけば、

$$a + m\mathbb{Z} = yns + m\mathbb{Z} = yns + xms + m\mathbb{Z} = (yn + xm)s + m\mathbb{Z} = s + m\mathbb{Z}$$

かつ

$$a + n\mathbb{Z} = xmt + n\mathbb{Z} = xmt + ynt + n\mathbb{Z} = (xm + yn)t + n\mathbb{Z} = t + n\mathbb{Z}$$

[17] イデアル版の一般的な中国人剰余定理もあるが、ここで使っているのは、次のもの。「正整数の因数分解を考える: $\mathbb{N} \ni a = p_1^{n_1} \cdots p_r^{n_r}$, ($p_i$ は互いに相異なる素数、$\mathbb{Z} \ni n_i \geq 1$). このとき、可換環としての同型 $\mathbb{Z}/(a) \cong \mathbb{Z}/(p_1^{n_1}) \times \cdots \times \mathbb{Z}/(p_r^{n_r})$ が成り立つ。」

となり、$\mathbb{Z}/mn\mathbb{Z} \ni a + mm\mathbb{Z} = \psi^{-1}((s + m\mathbb{Z}, t + n\mathbb{Z}))$ とわかる。同様に $\psi^{-1}((\hat{s} + m\mathbb{Z}, \hat{t} + n\mathbb{Z}) = \hat{a} := xm\hat{t} + yn\hat{s}$ を得る。そこで、

$$\begin{aligned} a\hat{a} &= (xmt + yns)(xm\hat{t} + yn\hat{s}) \\ &= x^2m^2t\hat{t} + y^2n^2s\hat{s} + mn(xys\hat{t} + xy\hat{s}t) \\ &= x^2m^2(1 - \hat{x}n) + y^2n^2(1 - \hat{y}m) + mn(xys\hat{t} + xy\hat{s}t) \\ &= (xm + yn)^2 + mn(-2xy + x^2m\hat{x} + y^2n\hat{y} + xys\hat{t} + xy\hat{s}t) \\ &= 1 + mn(\cdots) \end{aligned}$$

だから、$\hat{a}+mm\mathbb{Z}$ は $a+mm\mathbb{Z}$ の逆元である。つまり $\psi^{-1}(s+m\mathbb{Z}, t+n\mathbb{Z}) \in (\mathbb{Z}/mn\mathbb{Z})^*$ となる。 □

以上により、(2) が得られたが、これより直ちに $\varphi(mn) = \varphi(m)\varphi(n)$ を得る。
この結果を使うと、$n = p_1^{n_1} \cdots p_r^{n_r}$ と因数分解されたとき

$$\varphi(n) = \prod_{i=1}^{r} \varphi(p_i^{n_i})$$

を得る。従って、命題の後半を得るためには

$$\varphi(p^n) = p^{n-1}(p - 1)$$

を示せばよい。ところが、$\ell \cdot p$, $(\ell = 0, \ldots, p^{n-1} - 1)$ のは $0 \leq d < p^n$ なる d で $(d, p^n) > 1$ なるもの全てを尽くしていることに注意すると、

$$\begin{aligned} \varphi(p^n) &= \sharp\{a \in \mathbb{N} \mid 0 \leq a < p^n, (a, p^n) = 1\} \\ &= p^n - \sharp\{0, 1, \ldots, p^{n-1} - 1\} = p^n - p^{n-1} \\ &= p^{n-1}(p - 1) \end{aligned}$$

となる。 □

7.3. **円分拡大.** $K = \mathbb{Q}$ に 1 の原始 n 乗根 ζ を付け加えた拡大体を**円分拡大**と呼ぶが、ここではより一般の K について拡大 $K(\zeta)/K$ の構造を考える。

命題 99. 体 K と $\mathrm{char}(K) \not| n$ なる $n \in \mathbb{N}$ に対し、1 の原始 n 乗根 $\zeta \in \overline{K}$ を考える。このとき、

- (i) $K(\zeta)/K$ は有限 *Galois* 拡大で $\mathrm{Gal}\,(K(\zeta)/K)$ はアーベル群。そして $[K(\zeta) : K] \leq \varphi(n)$
- (ii) 任意の $\sigma \in \mathrm{Gal}\,(K(\zeta)/K)$ に対し、$r(\sigma) \in \mathbb{N}$ が対応して、以下の性質をもつ：
  - (a) $\sigma(\zeta) = \zeta^{r(\sigma)}$
  - (b) $r(\sigma)$ の $\mathbb{Z}/n\mathbb{Z}$ における像 $\overline{r(\sigma)}$ は、その乗法部分群 $(\mathbb{Z}/n\mathbb{Z})^*$ に入っていて、この像は ζ の取り方によらず一意的に決まる。
  - (c) $\psi : \mathrm{Gal}\,(K(\zeta)/K) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^* \qquad \sigma \longmapsto \overline{r(\sigma)}$ は単射準同型で、$K = \mathbb{Q}$ の場合はさらに同型になる。

Proof. (i) の証明：$\mathrm{char}(K) \not| n$ だから、$X^n-1 \in K[X]$ は分離多項式であり[18]、X^n-1 の全ての零点は ζ^s $(s=1,,2\ldots,n)$ によって得られるから、$K(\zeta)$ は X^n-1 の分解体として正規拡大でもある。従って $K(\zeta)/K$ は Galois 拡大。また、$\varphi(n)=\sharp((\mathbb{Z}/n\mathbb{Z})^*)$ だから、$[K(\zeta):K] \leq \varphi(n)$ であることは (ii) より直ちに得られる。

(ii) の証明：$X^n-1=0$ の $\overline{K}$ における解集合 $U_n \cong \mathbb{Z}/n\mathbb{Z}$ は、1 の原始 n 乗根 ζ によって生成される巡回群である。そして $\mathrm{Gal}\,(K(\zeta)/K)$ の元 σ は X^n-1 の零点たちの置換として作用する。従って、$r(\sigma)$ は $\bmod n$ では一意的に決まる。さらに任意の $s \in \mathbb{Z}$ に対し

$$\sigma(\zeta^s)=\sigma(\zeta)^s=(\zeta^{r(\sigma)})^s=(\zeta^s)^{r(\sigma)}$$

だから、$\overline{r(\sigma)} \in \mathbb{Z}/n\mathbb{Z}$ は ζ の選び方によらず一意的に決まる。また、$\sigma(\zeta)$ が 1 の原始 n 乗根でない X^n-1 の零点だとすると、$1=\sigma(\zeta)^k=\sigma(\zeta^k)$ なる $1<k<n$ が存在することになるが、$\zeta^k \neq 1$ であり、$\sigma \in \mathrm{Gal}\,(K(\zeta)/K)$ は体の自己同型で、特に単射だから、これは矛盾である。従って、$\sigma(\zeta)$ もまた 1 の原始 n 乗根でなければならない。よって

$$\psi : \mathrm{Gal}\,(K(\zeta)/K) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^* \qquad \sigma \longmapsto \overline{r(\sigma)}$$

は well-defined (つまり像がちゃんと $(\mathbb{Z}/n\mathbb{Z})^*$ に入っている）な群準同型になる。また、上で示したように $r(\sigma)$ は σ によって一意的に決まるから ψ は単射である。すると

$$\sharp\mathrm{Gal}\,(K(\zeta)/K) \leq \sharp(\mathbb{Z}/n\mathbb{Z})^*=\varphi(n).$$

また、$K=\mathbb{Q}$ の場合、さらに上式の等号が成り立つが、それは次の命題 101 による。 □

例 100 ($\sharp\mathrm{Gal}\,(K(\zeta)/K)<\varphi(n)$ となる例)**.** K を標数 2 の素体 $\mathbb{F}_2$ に 1 の原始 3 乗根 $a,\,b$ を付け加えた拡大体とする。すなわち $K \cong \mathbb{F}_2[X]/(X^2+X+1)$, $X^2+X+1=(X-a)(X-b)$. この時、$n=5$ とすると、$\mathrm{char}(K) \not| n$ 条件は満たされ、$\varphi(5)=4$ である。さて、$\zeta \in \overline{K}$ を 1 の原始 5 乗根とすると、ζ は X^5-1 の零点であるが、

$$\begin{aligned} X^5-1 &= (X-1)(X^4+X^3+X^2+X+1) \\ &= (X-1)(X^2+aX+1)(X^2+bX+1) \end{aligned}$$

と因数分解できる。実際、

$$(X^2+aX+1)(X^2+bX+1)=X^4+(a+b)X^3+(ab+2)X^2+(a+b)X+1$$

だが、$\mathrm{char}(K)=2$ ゆえ $ab+2=ab$ となり、また、a,b は X^2+X+1 の零点だから、2 次方程式の解と係数の関係により $a+b=-1=1$ ($\mathrm{char}(K)=2$ だから $-1=1$ となることに注意）かつ $ab=1$. よって $(X^2+aX+1)(X^2+bX+1)=X^4+X^3+X^2+X+1$ を得る。すると、ζ の最小多項式は X^2+aX+1 か X^2+bX+1 となり、結局

$$\begin{aligned} \sharp\mathrm{Gal}\,(K(\zeta)/K) &= [K(\zeta):K]=\deg(X^2+aX+1)(\text{または}=\deg(X^2+bX+1)) \\ &= 2<4=\varphi(n) \end{aligned}$$

となる。

[18]注意 71 参照。n が $\mathrm{char}(K)$ の倍数でないから、X^n-1 の導関数 nX^{n-1} は恒等的には 0 にならず、従って X^n-1 と共通零点をもたないことに注意。

上の定理の特殊な場合として、以下の円分拡大の構造定理が得られる。

命題 101. 任意の 1 の原始 n 乗根 $\zeta \in \mathbb{C}$ に対して、$\mathbb{Q}(\zeta)/\mathbb{Q}$ は *Galois* 拡大で、

$$\mathrm{Gal}\,(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$$

が成り立つ。

Proof. 1 の原始 n 乗根 ζ の $\mathbb{Q}$ 上の最小多項式を $f \in \mathbb{Q}[X]$ とする。その時、他の全ての原始 n 乗根もやはり f の零点であることが示せれば、1 の原始 n 乗根の個数が $\varphi(n)$ であることから、$\varphi(n) \leq \deg f$. そして逆の不等号が命題 99 で示されているので、結局 $\varphi(n) = \deg f$ となる。よって $\sharp\mathrm{Gal}\,(\mathbb{Q}(\zeta)/\mathbb{Q}) = \sharp(\mathbb{Z}/n\mathbb{Z})^*$ とあり、命題 99 で示されている単射は実は全射にもなっていることがわかる。そこで以下では、ζ 以外の 1 の原始 n 乗根も f の零点であることを示す。

Step 1: f は $X^n - 1$ の因子だから、

$$X^n - 1 = fh \qquad (\exists h \in \mathbb{Q}[X])$$

と分解できるが、実は $f, h \in \mathbb{Z}[X]$ として良いことをまず示そう。まず、$X^n - 1$ も f もモニックだから、係数比較すれば h もモニックだとわかる。次に、$\mathbb{Q}$ の任意の元 a は $a = \pm\prod_{i=1}^{r} p_1^{n_1} \cdots p_r^{n_r}$ （p_i は素数、$n_i \in \mathbb{Z}$）の形に一意的に書けるので、$\nu_{p_i}(a) := n_i$ として、さらに任意の $g = \sum_j a_j X^j \in \mathbb{Q}[X]$ に対して

$$\nu_p(g) := \min_j \nu_p(a_j)$$

と定義する。つまり、$\nu_p(-)$ とは、与えられた式なり有理数なりを、$p^n \times (\cdots)$ のように素数 p をくくり出して書き表した時の n のうち、絶対値が一番大きい物を表している。この時、以下のことが成り立つ

補題 102 (Gauß)**.** $(0 \neq) f, g \in \mathbb{Q}[X]$ と任意の素数 p に対して、$\nu_p(fg) = \nu_p(f) + \nu_p(g)$

補題 *102* の証明. $f \in \mathbb{Q}$ または $g \in \mathbb{Q}$ の場合は明白。それ以外の場合、f, g の係数の分母を全てかけ合わせたものを、それぞれ $a, b \in \mathbb{Z}$ とすると、$af, bg \in \mathbb{Z}[X]$. さらにこれらの係数 (整数）の最大公約数をそれぞれ $c, d \in \mathbb{Z}$ とし、$F := af/c,\ G := bg/d \in \mathbb{Z}[X]$ とおく。すると $F = \sum_i a_i X^i$ としたとき、$\gcd(\{a_i\}_i) = 1$ だから、どんな素数 p に対しても、かならず $\nu_p(a_i) = 0$ となるような i が存在する。このことから、任意の素数 p に対して $\nu_p(F) = 0$ であることがわかる。同様にして $\nu_p(G) = 0$. そこで、自然準同型 $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ を使って、全射準同型

$$\psi : \mathbb{Z}[X] \longrightarrow \mathbb{F}_p[X] \qquad \sum_i a_i X^i \mapsto \sum_i \overline{a}_i X^i$$

を考えると、

$$\mathrm{Ker}\,\psi = \{f \in \mathbb{Z}[X] \mid \nu_v(f) > 0\}$$

とわかる。従って、$\psi(F), \psi(G) \neq 0$ である。$\mathbb{F}_p[X]$ は整域だから、$\psi(FG) = \psi(F)\psi(G) \neq 0$. つまり $FG \notin \mathrm{Ker}\,\psi$ だから、$\nu_p(FG) = 0$ となり、結局

$$\nu_p(FG) = \nu_P(F) + \nu_p(G)$$

が言えた。そこで

$$\begin{aligned}
\nu_p(fg) &= \nu_P(\frac{c}{a}F \cdot \frac{d}{b}G) = \nu_P(\frac{cd}{ab}F \cdot G) \\
&= \nu_p(\frac{cd}{ab}) + \nu_p(FG) \\
&\qquad f, g \text{ の一方が } \mathbb{Q} \text{ の場合の結果による} \\
&= \nu_p(\frac{cd}{ab}) + \nu_p(F) + \nu_p(G) \\
&= \nu_p(\frac{c}{a}) + \nu_p(\frac{d}{b}) + \nu_p(F) + \nu_p(G) \\
&\qquad f, g \text{ の両方が } \mathbb{Q} \text{ の場合の結果による} \\
&= \nu_p(\frac{c}{a}F) + \nu_p(\frac{d}{b}G) \\
&\qquad f, g \text{ の一方が } \mathbb{Q} \text{ の場合の結果による} \\
&= \nu_p(f) + \nu_p(g)
\end{aligned}$$

を得る。 □

Gaußの補題 102 により、任意の素数 p に対して

$$0 = \nu_p(X^n - 1) = \nu_p(fh) = \nu_p(f) + \nu_p(h)$$

となり、また、f, h はモニックだから、$\nu_p(f), \nu_p(h) \leq 0$ である。よって結局、任意の素数 p に対して $\nu_p(f) = \nu_p(h) = 0$ である、これは $f, h \in \mathbb{Z}[X]$ であることを意味する。

Step 2: $p \not| n$ なる任意の素数 p に対して、ζ^p も 1 の原始 n 乗根になる[19]。このとき、ζ^p もまた f の零点であることを示そう。もしそうでないとすると、$f(\zeta^p) \neq 0$ となるが、その一方

$$0 = (\zeta^p)^n - 1 = f(\zeta^p)h(\zeta^p)$$

だから、$h(\zeta^p) = 0$, つまり ζ は $h(X^p) \in \mathbb{Z}[X]$ の零点である。従って最小多項式 f で割り切れる。すなわち、$h(X^p) = fg$ となる $g \in \mathbb{Q}[X]$ が存在するが、Step 1 と同様の議論により、$g \in \mathbb{Z}[X]$ でモニックと考えてよい。そこで自然全射 $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ を使って次のような全射 ψ を考える:

$$\psi : \mathbb{Z}[X] \longrightarrow (\mathbb{Z}/p\mathbb{Z})[X] = \mathbb{F}_p[X] \qquad \sum_i c_i X^i \longmapsto \sum_i \overline{c}_i X^i.$$

すると

$$\overline{h}^p = \overline{h}(X^p) = \overline{f}\,\overline{g}$$

となる[20]。$\mathbb{F}_p[X]$ が UFD であることに注意すると、これより $\overline{h}$ と $\overline{f}$ が $\mathbb{F}_p[x]$ で共通因子をもつことがわかる。すると $X^n - \overline{1} = \overline{fh}$ は（$\mathbb{F}_p$ の代数的閉包の中で）重根を持つことになり、$p \not| n$ 条件より $X^n - 1$ が $\mathbb{F}_p[X]$ の中でも分

[19]証明：実際、$(\zeta^p)^m = 1$, $m < n$ だとすると、$n|pm$ となるはずで、p が素数で、$p \not| n$ から $n|m$ とならねばならないが、$m < n$ だからそれはあり得ない

[20]命題 35 の Frobenius 写像の原理を使っていることに注意.

離多項式であることに矛盾する。よって $f(\zeta^p) = 0$ でなければならないとわかる。

Step 3: 次に、任意の 1 の原始 n 乗根 ζ' を考える。$\zeta' \in U_n = \langle\zeta\rangle$ だから、$\zeta' = \zeta^m$ なる $m \in \mathbb{N} - \{0\}$ が存在する。ζ' が原始 n 乗根だから、$(m, n) = 1$ も成り立つ。すると

$$m = p_1^{n_1} \cdots p_r^{n_r} \qquad (p_i \not| n, i = 1, \ldots, r)$$

の形に素因数分解される。すると ζ' は ζ を何回か素数べき乗して得られ、その素数は Step 2 で考えた $p \not| n$ 条件を満たす。すなわち、何回素数べきしても必ず f の零点になっているような 1 の原始 n 乗根が得られる。よって ζ' もまた f の零点になっている。

□

まとめ

- ζ を 1 の原始 n 乗根とすると、$\mathbb{Q}(\zeta)/\mathbb{Q}$ は円分拡大と呼ばれる Galois 拡大であり、$\mathrm{Gal}\,(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$.
- $\varphi(n) := \sharp(\mathbb{Z}/n\mathbb{Z})^*$ は Euler 関数と呼ばれ、$\varphi(n) = \sharp\{k \mid 1 \leq k < n, (k, n) = 1\}$ となる。
- $\varphi(p^n) = p^{n-1}(p-1)$
- $(m, n) = 1$ ならば $\varphi(mn) = \varphi(m)\varphi(n)$

8. 巡回拡大

ここでは、Galois 拡大の特殊な場合として、巡回拡大を考える。

定義 103 (巡回拡大)**.** 有限次 *Galois* 拡大 L/K で、*Galois* 群 $\mathrm{Gal}\,(L/K)$ が有限巡回群になるものを、**巡回拡大**と呼ぶ。

8.1. **Hilbert の定理９０.** 巡回拡大の構造を考えるにあたって、重要な役割を果たすのが Hilbert の定理９０と呼ばれるものだが、この定理を示すためには有限拡大体のノルムとトレースの概念を準備しておく必要がある。ノルムとトレースは、いずれも線形代数の概念を、線形空間としての拡大体に応用したものである。

8.1.1. 有限拡大体のノルム. 有限拡大体 L/K を考える。すなわち L は有限次元 K ベクトル空間だが、$a \in L$ に対して

$$\varphi_a : L \longrightarrow L, \quad x \mapsto ax,$$

なる写像を考えると K 線形写像になる。実際、$c \in K, x, y \in L$ に対して

$$\begin{aligned} \varphi_a(x+y) &= a(x+y) = ax + ay = \varphi_a(x) + \varphi_a(y) \\ \varphi_a(cx) &= a(cx) = c(ax) = c\varphi_a(x) \end{aligned}$$

となるからである。K 線形写像だから、L の K 線形基底を適当に決めれば、φ_a は K 上の $n \times n$ 行列（但し、$n = [L:K] = \dim_K L$）で表現できる。記号の節約のため、この行列も φ_a と表すことにする。

定義 104. L/K を有限次拡大とし、$a \in L$ に対して $\varphi_a(x) = ax$ なる K 線形写像 $L \to L$ を考える。このとき、$N_{L/K}(a) := \det \varphi_a$ を L/K の**ノルム**と呼ぶ。

注意 105. 線形代数の理論により、ノルムは L の K 基底の取り方には依存しないことに注意しよう。実際、基底のとりかえは適当な n 次正則行列 $A \in \mathrm{GL}_n(K)$ によって表され、とり換えられた基底での表現行列は $A^{-1}\varphi_a A$ となる。従って、そのノルムは $\det(A^{-1}\varphi_a A) = \det(A)^{-1} \det \varphi_a \det(A) = \det \varphi_a$ となり、基底変換前のものと同じになる。

注意 106. 行列 φ_a がどんなものかを見ておこう。$n = [L:K]$ とし、L の K 基底を $\mathbf{x}_1, \ldots, \mathbf{x}_n$ とすると、$a = \sum_{i=1} a_i \mathbf{x}_i$ $(a_i \in K)$ と表せて、さらに適当な $\alpha_{ij} \in K$ によって

$$\varphi_a(\mathbf{x}_j) = \sum_{i=1}^{n} \alpha_{ij} \mathbf{x}_i$$

と書けるが、線形写像の行列表現の一般論により、$\varphi_a = (\alpha_{ij})$ となる。そこでこの α_{ij} を求めればよい。特に $a = \mathbf{x}_k$ の場合、

$$\varphi_a(\mathbf{x}_j) = a\mathbf{x}_j = \mathbf{x}_k \mathbf{x}_j = \sum_{i=1}^{n} c_i^{kj} \mathbf{x}_i \qquad (j = 1, \ldots, n)$$

なる $c_i^{kj} \in K$ が存在する。つまり

$$\varphi_{\mathbf{x}_k} = (c_i^{kj})_{ij} = \begin{pmatrix} c_1^{k1} & c_1^{k2} & \cdots & c_1^{kn} \\ c_2^{k2} & c_2^{k2} & \cdots & c_2^{kn} \\ \vdots & \vdots & & \vdots \\ c_n^{kn} & c_n^{kn} & \cdots & c_n^{kn} \end{pmatrix}$$

$\varphi_{\mathbf{x}_j}(\mathbf{x}_i) = \varphi_{\mathbf{x}_i}(\mathbf{x}_j)$ だから、$c_i^{kj} = c_i^{jk}$ $(\forall i, j, k)$ であることに注意する。すると、a が一般の場合、

$$\varphi_a(\mathbf{x}_j) \quad = \quad a\mathbf{x}_j = (\sum_{k=1}^{n} a_k \mathbf{x}_k)\mathbf{x}_j = \sum_{k=1}^{n} a_k (\sum_{i=1}^{n} c_i^{kj} \mathbf{x}_i) = \sum_i (\sum_k a_k c_i^{kj})\mathbf{x}_i$$

となるから、

$$\alpha_{ij} = a_1 c_i^{1j} + a_2 c_i^{2j} + \cdots + a_n c_i^{nj}$$

となる。これは結局

$$\varphi_a = \varphi_{\sum_i a_i \mathbf{x}_i} = \sum_{k=1}^{n} a_k \varphi_{\mathbf{x}_k} = \sum_{k=1}^{n} a_k \begin{pmatrix} c_1^{k1} & c_1^{k2} & \cdots & c_1^{kn} \\ c_2^{k2} & c_2^{k2} & \cdots & c_2^{kn} \\ \vdots & \vdots & & \vdots \\ c_n^{kn} & c_n^{kn} & \cdots & c_n^{kn} \end{pmatrix}$$

ということに他ならない。特に、$a \in K$ の時は、$a = a\mathbf{x}_1$　(実際、このとき $\mathbf{x}_1 = 1$ である）と思って良いので、

$$\varphi_a(\mathbf{x}_j) = a\mathbf{x}_j = \sum_{i=1}^{n} \alpha_{ij} \mathbf{x}_i$$

よって $\alpha_{ij} = a\delta_{ij}$ である。但し、δ_{ij} はクロネッカーのデルタ。すなわち、$a \in K$ の場合、φ_a は aE_n (E_n は n 次単位行列）で表現される。

補題 107. $[L : K] = n$ のとき、$a \in K$ ならば $N_{L/K}(a) = a^n$ である。

Proof. 注意 106 の最後の考察により、$a \in K$ ならば φ_a は aE_n で表される（E_n は n 次単位行列)。従って $N_{L/K}(a) = \det(aE_n) = a^n$ となる。 □

命題 108. 有限次拡大 L/K に対して、$n = [L : K] = qr,\ r = [L : K]_s := \sharp \mathrm{Hom}_K(L, \overline{K})$ であるとし *(*命題 *78* 参照*)*、$\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_1, \ldots, \sigma_r\}$ とおく。このとき、

$$N_{L/K}(a) = \left(\prod_{i=1}^{n} \sigma_i(a) \right)^q$$

である。特に L/K が *Galois* 拡大の場合は $N_{L/K}(a) = \prod_{\sigma \in \mathrm{Gal}\,(L/K)} \sigma(a)$ となる。

Proof. 後半の L/K が Galois 拡大の場合の主張は、定理 79(iii) より $q = 1$ が、そして 定理 62(i) より $\mathrm{Hom}_K(L, \overline{K}) = \mathrm{Gal}\,(L/K)$ が従うので、前半から直ちに得られる。以下前半を示そう。$n = [L : K]$ とし、$a \in L$ についての場合分けで考える。

(1) $a \in K$ **の場合:** 補題 107 より $N_{L/K}(a) = a^n$ であり、また、任意の $\sigma \in \mathrm{Hom}_K(L, \overline{K})$ に対して $\sigma(a) = a$ であるから。$(\prod_{i=1}^{r} \sigma_i(a))^q = (\prod_{i=1}^{r} a)^q = a^{rq} = a^r = N_{L/K}(a)$ となる。

(2) $L = K(a)$ **の場合:** $a \in L$ の最小多項式を

$$f = X^n + c_1 X^{n-1} + \cdots + c_n \in K[X]$$

とおく。これは

$$\varphi_a : L \longrightarrow L \qquad t \longmapsto at \quad (t \in L)$$

の最小多項式にもなっていることに注意する。実際、

$$\begin{aligned} f(\varphi_a)(t) &= ((\varphi_a)^n + c_1(\varphi_a)^{n-1} + \cdots + c_n E_n)(t) \\ &= (a^n + c_1 a^{n-1} + \cdots c_n)(t) = 0 \qquad (\forall t \in L) \end{aligned}$$

だから、$f(\varphi_a) = O_n$ (n 次零行列）となる。すると線形代数の一般論より $N_{L/K}(a) = \det \varphi_a = (-1)^n c_n$ である。ところが $n = qr$, $r = [L : K]_s$ だから、

$$f = \left(\prod_{i=1}^{r} (X - \sigma_i(a)) \right)^q$$

と因数分解する。何故ならば、命題 73 により、f の相異なる解は $\sigma_i(a)$, $i = 1, \ldots, r$, だと分かり、正標数の場合は $q > 1$ となるが、命題 78(i) より f の全ての解は同じ重複度をもつからである。従って、$(-1)^n c_n = (\prod_{i=1}^{r} \sigma_i(a))^q$ である。よって、$N_{L/K}(a) = \left(\prod_{i=1}^{r} \sigma_(a)\right)^q$ となる。

(3) **それ以外の場合:** $a \in L$ として、拡大体の列 $K \subset K(a) \subset L$ を考える。$K(a)$ の K 線形基底 $\mathbf{x}_1, \ldots, \mathbf{x}_s$ と L の $K(a)$ 線形基底 $\mathbf{y}_1, \ldots, \mathbf{y}_t$ をとる ($s = [K(a) : K]$, $t = [L : K(a)]$). すると $\{\mathbf{x}_i \mathbf{y}_j\}_{ij}$ は L の K 線形基底になる。従って、$a\mathbf{x}_i \in K(a)$ を $\mathbf{x}_1, \ldots, \mathbf{x}_s$ の K 線形結合で表すことにより、$\varphi_a|_{K(a)}$ の表現行列 A を K 上の s 次正方行列としてとることができる。すると、φ_a は

$$\varphi_a = \begin{pmatrix} A & & 0 \\ & \ddots & \\ 0 & & A \end{pmatrix}$$

の形の K 上の st 次の正方行列で表すことができる[21]。すると

$$N_{L/K}(a) = (\det A)^t = (N_{K(a)/K}(a))^{[L:K(a)]} = N_{K(a)/K}(a^{[L:K(a)]})$$

---

[21]まず、行列 φ_a の $1 \sim s$ 列目の縦ベクトルは、$\varphi_a(\mathbf{x}_k \mathbf{y}_1)$ $k = 1, \ldots, s$ の像の $\{\mathbf{x}_i \mathbf{y}_j\}_{ij}$ による線形結合であり、$s+1 \sim 2s$ 行目の縦ベクトルは $\varphi_a(\mathbf{x}_k \mathbf{y}_2)$ $k = 1, \ldots, s$ の像の $\{\mathbf{x}_i \mathbf{y}_j\}_{ij}$ による線形結合 etc. となっていることに注意しよう。すると例えば、φ_a 行列の 1 列目の縦ベクトル $\begin{bmatrix} a_{1,1} \\ \vdots \\ a_{st,1} \end{bmatrix}$ は $\varphi_a(\mathbf{x}_1 \mathbf{y}_1) = \sum_{k=1}^{s} a_{k,1} \mathbf{x}_k \mathbf{y}_1$ によって定義されている。$\varphi_a(\mathbf{x}_1 \mathbf{y}_1) = \varphi_a(\mathbf{x}_1)\mathbf{y}_1$ だから、結局 $\varphi_a(\mathbf{x}_1) = \sum_{k=1}^{s} a_{k,1} \mathbf{x}_k$. すなわち、$\varphi_s$ 行列の 1 列目は、上から s 行目までは A の 1 列目と一致し、それより下は全て 0 となる。同様に、φ_a 行列の $s+1$ 列目の縦ベクトル $\begin{bmatrix} a_{1,s+1} \\ \vdots \\ a_{st,s+1} \end{bmatrix}$ は $\varphi_a(\mathbf{x}_1 \mathbf{y}_2) = \sum_{k=1}^{s} a_{k,1} \mathbf{x}_k \mathbf{y}_2$ によって定義されており、上から $s+1$ 行目から $2s$ 行目までが A の 1 列目と一致して、それ以外はすべて 0 となる。

となる。ただし、最後の等式は $N_{L/K}$ の定義から従う[22]。また、補題 107 より $N_{L/K(a)}(a) = a^{[L:K(a)]}$ だから、結局

$$\begin{aligned}
&N_{L/K}(a)\\
&= N_{K(a)/K}(N_{L/K(a)}(a))\\
&= N_{K(a)/K}\left(\prod_{\tau\in\mathrm{Hom}_{K(a)}(L,\overline{K})}\tau(a)\right)^{q_1}\\
&\qquad (1)\text{ の場合の結果による。ただし、}[L:K(a)] = q_1[L:K(a)]_s\\
&= \left(\prod_{\sigma\in\mathrm{Hom}_K(K(a),\overline{K})}\sigma\left(\prod_{\tau\in\mathrm{Hom}_{K(a)}(L,\overline{K})}\tau(a)\right)^{q_1}\right)^{q_2}\\
&\qquad (2)\text{ の場合の結果による。ただし、}[K(a):K] = q_2[K(a):K]_s.
\end{aligned}$$

さて、$(\prod_{\tau\in\mathrm{Hom}_{K(a)}(L,\overline{K})}\tau(a))^{q_1} = N_{L/K(a)}(a) \in K(a)$ であるから、定理 50 を使って $\sigma \in \mathrm{Hom}_K(K(a),\overline{K})$ を $\mathrm{Hom}_K(\overline{K},\overline{K})$ の元 σ' に拡張しても計算結果は変わらない。すると、

$$N_{L/K}(a) = \left(\prod_{\sigma'\in\mathrm{Hom}_K(\overline{K},\overline{K})}\prod_{\tau\in\mathrm{Hom}_{K(a)}(L,\overline{K})}(\sigma'\circ\tau)(a))\right)^{q_1q_2}$$

あとは、$q_1q_2 = q$, $\{\sigma'\circ\tau \mid \sigma \in \mathrm{Hom}_K(K(a),\overline{K}), \tau \in \mathrm{Hom}_{K(a)}(L,\overline{L})\} = \mathrm{Hom}_K(L,\overline{K})$ となることを言えばよい。$[L:K(a)] = q_1[L:K(a)]_s$, $[K(a):K] = q_2[K(a):K]_s$ だから、命題 76 と命題 14 より

$$\begin{aligned}
[L:K] &= [L:K(a)][K(a):K] = q_1q_2[L:K(a)]_s[K(a):K]_s\\
&= q_1q_2[L:K]_s.
\end{aligned}$$

よって $q = q_1q_2$. また、$\sigma'\circ\tau$ はそれぞれ相異なる写像（実際 τ は $K(a)$ の元を固定し、σ' は $K(a)$ の元を動かす相異なる準同型を動くから）ゆえ、その個数は上の計算結果を使って

$$\begin{aligned}
&\sharp\mathrm{Hom}_K(K(a),\overline{K}) \times \sharp\mathrm{Hom}_{K(a)}(L,\overline{K})\\
&= [K(a):K]_s \times [L:K(a)]_s = [L:K]/q = [L:K]_s
\end{aligned}$$

となる。従って $\{\sigma'\circ\tau \mid \cdots\}$ の元だけで $\mathrm{Hom}_K(L,\overline{K})$ の元を全て尽くしている。

□

以下の結果は、ノルムは Galois 群の作用で保存されることを主張する。

系 109. *L/K が有限次 Galois 拡大の時、任意の $a \in L$ と $\sigma \in \mathrm{Gal}\,(L/K)$ に対して $N_{L/K}(a) = N_{L/K}(\sigma(a))$.*

[22]つまり、$\det(A^n) = (\det A)^n$ という行列式の性質を使っている。

Proof. 命題 108 より $N_{L/K}(a) = \prod_{\tau\in\mathrm{Gal}\,(L/K)} \tau(a)$, また $N_{L/K}(\sigma(a)) = \prod_{\tau\in\mathrm{Gal}\,(L/K)} \tau(\sigma(a))$. ここで、$\sigma \in \mathrm{Gal}\,(L/K)$ を固定して $\tau \in \mathrm{Gal}\,(L/K)$ を動かすと、$\tau\circ\sigma$ は $\mathrm{Gal}\,(L/K)$ の元全てを動くことに注意すると、$N_{L/K}(a) = N_{L/K}(\sigma(a))$ とわかる。 □

8.2. **指標の独立性.**

定義 110 (指標)**.** 任意の群 G と体 K に対して、群の準同型写像 $\chi : G \longrightarrow K^*(:= K - \{0\})$ のことを G の K に値を持つ**指標**と呼ぶ。

Hilbert の定理 90 の証明のために、以下の「指標の独立性定理」を示す。

命題 111. $\chi_i : G \longrightarrow K^*$ $(i = 1, \ldots, n)$ を群 G から体 K の乗法部分群 K^* への相異なる群の準同型とし、$c_1, \ldots, c_n \in K$ に対して写像

$$\varphi_{c_1,\ldots,c_n} := \sum_{i=1} c_i\chi_i : G \to K \qquad g \longmapsto \sum_{i=1} c_i\chi_i(g)$$

を考える。このとき、$\varphi_{c_1,\ldots,c_n} = 0$ となるための必要十分条件は、$c_1 = \cdots = c_n = 0$ となることである。

Proof. 線形代数の用語を流用すれば、証明すべき結論は「$\chi_1, \ldots, \chi_n$ は K 上一次独立」である。結論が成り立たないと仮定すると、$\varphi_{c_1,\ldots,c_n} = 0$ であるが、$c_i \neq 0$ となるような i が存在することになる。これも線形代数の用語を流用して、「$\chi_1, \ldots, \chi_n$ の間に非自明な線形関係式が成り立つ」と呼ぶことにしよう。

今、$c_j = 0$ なる部分は除外して、$c_i \neq 0$, $i = 1, \ldots, m$, $(m \leq n)$ と仮定してよい。また、m は非自明な線形関係式成立する最小値であるようにとっておく。

さて、$\chi_1 \neq \chi_2$ だから、適当な $g \in G$ を選べば $\chi_1(g) \neq \chi_2(g)$ となる。また、

$$0 = \varphi_{a_1,\ldots,a_n}(gh) = \sum_{i=1}^{m} c_i\chi_i(gh) = \sum_{i=1}^{m} c_i\chi_i(g)\chi_i(h) \qquad (\forall h \in G)$$

だから、$\varphi^g_{c_1,\ldots,c_n} := \sum_{i=1}^m c_i\chi_i(g)\chi_i : G \longrightarrow K$ はゼロ写像になる。そこで

$$\begin{aligned} 0 &= \chi_1(g)\varphi_{c_1,\ldots,c_n} - \varphi^g_{c_1,\ldots,c_n} \\ &= \sum_{i=1}^{m} a_i\chi_1(g)\chi_i - \sum_{i=1}^{n} a_i\chi_i(g)\chi_i \\ &= \sum_{i=2}^{m} c_i(\chi_1(g) - \chi_i(g))\chi_i \end{aligned}$$

を得るが、$\chi_1(g) \neq \chi_2(g)$, $c_2 \neq 0$ だから、結局長さ $m-1$ よりも短い非自明な線形関係式が作れたことになり、m の最小性に矛盾する。よって、$\chi_1, \ldots, \chi_n$ はやはり K 上一次独立でなければならない。 □

8.3. **Hilbert の定理９０（乗法版）.** 以下は Hilbert 定理９０の乗法版と呼ばれるものであり、n 次巡回拡大 L/K で n と $\mathrm{char}(K)$ が互いに素な場合の構造に深く関係する。

定理 112 (Hilbert 90 (乗法版))**.** L/K が巡回拡大とし、$\sigma \in \mathrm{Gal}\,(L/K)$ を生成元とする：$\langle\sigma\rangle = \mathrm{Gal}\,(L/K)$. このとき、$b \in L$ に対して以下は同値

(i) $N_{L/K}(b) = 1$

(ii) 適当な元 $a \in L^*$ が存在して、$b = a \cdot \sigma(a)^{-1}$ となる。

Proof. $\underline{(ii) \Rightarrow (i) \text{ の証明：}}b = a \cdot \sigma(a)^{-1}$ だとする。この時、

$$(N_{L/K})|_{L^*} : L^* \longrightarrow K^* \qquad a \mapsto N_{L/K}(a)$$

は乗法群 L^* と K^* の間の準同型である。実際、$c, d \in L^*$ に対し、$N_{L/K}(c \cdot d) = \det \varphi_{c\cdot d} = \det(\varphi_c \circ \varphi_d) = \det \varphi_c \cdot \det \varphi_d = N_{L/K}(c) \cdot N_{L/K}(d)$ となるからである。このことを使うと、

$$\begin{aligned} N_{L/K}(b) &= N_{L/K}(a \cdot \sigma(a)^{-1}) = N_{L/K}(a) \cdot N_{L/K}(\sigma(a))^{-1} \\ &= N_{L/K}(a) \cdot N_{L/K}(a)^{-1} \quad \text{系 109 より} \\ &= 1 \end{aligned}$$

より (i) を得る。

$\underline{(i) \Rightarrow (ii) \text{ の証明：}}N_{L/K}(b) = 1$ なる $b \in L$ が存在すると仮定し、$n = [L : K]$ とおく。

$$\varphi := \sigma^0 + b \cdot \sigma^1 + b \cdot \sigma(b) \cdot \sigma^2 + \cdots + b \cdot \sigma(b) \cdot \cdots \cdot \sigma^{n-2}(b) \cdot \sigma^{n-1}$$

とおくと、$\varphi : L^* \longrightarrow L$ なる写像と考えられるが、$\sigma^0 = 1, \sigma, \sigma 2, \ldots, \sigma^{n-1}$ は全て相異なる $L^* \to L^*$ なる準同型写像であり、σ^0 の係数は 1、つまり 0 でないから、命題 111 により φ は零写像ではなく、従って $c \in L^*$ で $a := \varphi(c) \neq 0$ なるものが存在する。すると

$$\begin{aligned} b \cdot \sigma(a) &= b \cdot \sigma(\varphi(c)) \\ &= b \cdot (\sigma^1(c) + \sigma(b) \cdot \sigma^2(c) + \sigma(b) \cdot \sigma^2(b) \cdot \sigma^3(c) \\ &\quad + \cdots + \sigma(b) \cdot \sigma^2(b) \cdot \cdots \cdot \sigma^{n-2}(b) \cdot \sigma^{n-1}(c) \\ &\quad + \sigma(b) \cdot \sigma^2(b) \cdot \cdots \cdot \sigma^{n-1}(b) \cdot \sigma^n(c)) \\ &= b \cdot \sigma(c) + b \cdot \sigma(b) \cdot \sigma^2(c) + b \cdot \sigma(b) \cdot \sigma^2(b) \cdot \sigma^3(c) \\ &\quad + \cdots + b \cdot \sigma(b) \cdot \sigma^2(b) \cdot \cdots \cdot \sigma^{n-2}(b) \cdot \sigma^{n-1}(c) \\ &\quad + \underline{b \cdot \sigma(b) \cdot \sigma^2(b) \cdot \cdots \cdot \sigma^{n-1}(b) \cdot \sigma^n(c)}. \end{aligned}$$

ここで、上式下線部にあたる

$$b \cdot \sigma(b) \cdot \sigma^2(b) \cdot \cdots \cdot \sigma^{n-1}(b) \cdot \sigma^n(c) = c \tag{3}$$

であることが言えれば、上の式は $= a$ となり、$b = a \cdot \sigma(a)^{-1}$ を得る。まず、σ が巡回群 $\mathrm{Gal}\,(L/K)$ の生成元で $n = [L : K] = \sharp\mathrm{Gal}\,(L/K)$ だから、$\sigma^n(c) = c$ である。また、命題 108 より

$$b \cdot \sigma(b) \cdot \sigma^2(b) \cdot \cdots \cdot \sigma^{n-1}(b) = N_{L/K}(b)$$

であり、これは仮定により $= 1$ である。よって (3) が成り立つ。 □

8.4. **Hilbert の定理９０（加法版）.** 乗法版の Hilbert の定理９０では扱えない巡回拡大、すなわち巡回次数 n が標数 $\mathrm{char}(K) = p > 0$ の倍数である場合は Hilbert の定理９０の加法版によって扱うことができる。乗法版の Hilbert の定理９０ではノルム関数 $N_{L/K} : L \longrightarrow K$ が重要な役割を果たしたが、加法版では以下に述べるトレース関数 $\mathrm{Tr}_{L/K} : L \longrightarrow K$ がノルムに代わって使われる。以下では Hilbert の定理９０と同様の方法で理論を構成してゆく。

定義 113 (トレース)**.** 有限次拡大 L/K を考える。任意の $a \in L$ に対して、写像

$$\varphi_a : L \longrightarrow L, \qquad x \longmapsto ax,$$

を K ベクトル空間としての L の間の線形写像としてとらえる。このとき、φ_a の行列表現を $(a_{ij})_{ij}$ とする。このとき、$\mathrm{Tr}_{L/K}(a) := \mathrm{Tr}\varphi_a = \sum_i a_{ii}$ を a の**トレース**と呼ぶ。

補題 114. L/K を有限次拡大体とし $n = [L : K]$ とおく。このとき、$a \in K$ に対して $\mathrm{Tr}_{L/K}(a) = na$ である。

Proof. $a \in K$ ならば、φ_a を行列表現すれば、$\varphi_a = aE_n$ (E_n は n 次単位行列）となるから、そのトレースは na となる。 □

補題 115. $\mathrm{char}(K) = p > 0$ とし、$L = K(\alpha)/K$ が分離拡大でないとする。このとき、適当な $\mathbb{Z} \ni r > 0$ が存在して、α が K 上の最小多項式の p^r 重根となり、$[L : K] = p^r[L : K]_s$.

Proof. $f \in K[X]$ を α の最小多項式とし、$r > 0$ を $f = g(X^{p^r})$ となるような $g \in K[X]$ が存在する最大の整数とする。f が K 上既約と仮定しているから、g もまた K 上既約。従って g は分離的多項式である。なぜならば、もし $g = 0$ が $\overline{K}$ の中で重根を持つならば、それは $g = 0$ と $g' = 0$ の共通根だが、g が既約だから g はその重根の最小多項式なので、より次数の低い $g' = 0$ の根ではありえないからである。このことから、$f(\alpha) = g(\alpha^{p^r}) = 0$ ならば、それは $f = 0$ の p^r 重根であり、$\mathrm{Hom}_K(L, \overline{K})$ は補題 73 により $g = 0$ の根の個数となる。よって $[L : K] = \deg f = \deg g^{p^r} = p^r \cdot \deg g = p^r \cdot \sharp\mathrm{Hom}_X(L, \overline{K}) = p^r \cdot [L : K]_s$ を得る。 □

命題 116. 有限次拡大 L/K に対して、$n = [L : K] = qr,\ r = [L : K]_s := \sharp\mathrm{Hom}_K(L, \overline{K})$ であるとし、$\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_1, \ldots, \sigma_r\}$ とおく。このとき、$a \in L$ に対して

$$\mathrm{Tr}_{L/K}(a) = q \sum_{i=1}^{r} \sigma_i(a).$$

また、L/K が正標数 $p > 0$ の体であり、分離拡大でなければ、$q = p^r\ (r > 0)$ の形になり、従って $\mathrm{Tr}_{L/K}$ は零関数となる。

Proof. 最後の主張、つまり q が p の冪になることは、$L = K(a_1, \ldots, a_k)$、$a_1, \ldots, a_k$ は非分離的元、として補題 115 を繰り返し適用し、命題 14 と命題 76 を使えば得ら

れる。以下は前半の証明を行うが、そこでは命題 108 と同様の議論を行う。$a \in L$ についての場合分けで考える。

(1) $a \in K$ **の場合:** 補題 114 より $\mathrm{Tr}_{L/K}(a) = na$ であり、また、任意の $\sigma \in \mathrm{Hom}_K(L, \overline{K})$ に対して $\sigma(a) = a$ であるから。$q\sum_{i=1}^{r}\sigma_i(a) = qra = na = \mathrm{Tr}_{L/K}(a)$ を得る。

(2) $L = K(a)$ **の場合:** $a \in L$ の最小多項式を

$$f = X^n + c_1X^{n-1} + \cdots + c_n \in K[X]$$

とおく。これは

$$\varphi_a : L \longrightarrow L \qquad t \longmapsto at \quad (t \in L)$$

の最小多項式にもなっていることに注意する。すると線形代数の一般論より $\mathrm{Tr}_{L/K}(a) := \mathrm{Tr}\varphi_a = -c_1$ (解と係数の関係による) である。ところが $n = qr$, $r = [L : K]_s$ であることより、

$$f = \left(\prod_{i=1}^{r}(X - \sigma_i(a))\right)^q$$

と因数分解する。これより $-c_1 = q\sum_{i=1}^{r}\sigma_i(a)$ を得て、$\mathrm{Tr}_{L/K}(a) = q\sum_{i=1}^{r}\sigma_i(a)$ を得る。

(3) **それ以外の場合:** $a \in L$ として、拡大体の列 $K \subset K(a) \subset L$ を考える。$K(a)$ の K 線形基底 $\mathbf{x}_1, \ldots, \mathbf{x}_s$ と L の $K(a)$ 線形基底 $\mathbf{y}_1, \ldots, \mathbf{y}_t$ をとる ($s = [K(a) : K]$, $t = [L : K(a)]$). すると $\{\mathbf{x}_i\mathbf{y}_j\}_{ij}$ は L の K 線形基底になる。従って、$a\mathbf{x}_i$ を $\mathbf{x}_1, \ldots, \mathbf{x}_s$ の K 線形結合で表すことにより、$(\varphi_a)|_{K(a)}$ の表現行列 A を K 上の s 次正方行列としてとることができる。すると、φ_a は

$$\varphi_a = \begin{pmatrix} A & & 0 \\ & \ddots & \\ 0 & & A \end{pmatrix}$$

の形の K 上の st 次の正方行列で表すことができる。すると、$t = [L : K(a)]$ として

$$\mathrm{Tr}_{L/K}(a) = t \cdot \mathrm{Tr}(A) = t \cdot \mathrm{Tr}_{K(a)/K}(a) = \mathrm{Tr}_{K(a)/K}(ta)$$

となる。ただし、最後の等式は $\mathrm{Tr}_{L/K}$ の定義から従う。また、補題 114 より $\mathrm{Tr}_{L/K(a)}(a) = t \cdot a$ だから、結局

$$\begin{aligned}
&\mathrm{Tr}_{L/K}(a) \\
&= \mathrm{Tr}_{K(a)/K}(\mathrm{Tr}_{L/K(a)}(a)) \\
&= \mathrm{Tr}_{K(a)/K}\left(q_1 \sum_{\tau \in \mathrm{Hom}_{K(a)}(L,\overline{K})} \tau(a)\right) \\
&\qquad (1) \text{ の場合の結果による。ただし、} [L : K(a)] = q_1 [L : K(a)]_s \\
&= q_2 \sum_{\sigma \in \mathrm{Hom}_K(K(a),\overline{K})} \sigma\left(q_1 \sum_{\tau \in \mathrm{Hom}_{K(a)}(L,\overline{K})} \tau(a)\right) \\
&\qquad (2) \text{ の場合の結果による。ただし、} [K(a) : K] = q_2 [K(a) : K]_s.
\end{aligned}$$

さて、$q_q \sum_{\tau \in \mathrm{Hom}_{K(a)}(L,\overline{K})} \tau(a) = \mathrm{Tr}_{L/K(a)}(a) \in K(a)$ であるから、定理 50 を使って $\sigma \in \mathrm{Hom}_K(K(a), \overline{K})$ を $\mathrm{Hom}_K(\overline{K}, \overline{K})$ の元 σ' に拡張してもよい。すると、

$$\mathrm{Tr}_{L/K}(a) = q_1 q_2 \sum_{\sigma', \tau \in \mathrm{Hom}_{K(a)}(L,\overline{K})} (\sigma \circ \tau)(a)$$

あとは、$q_1 q_2 = q$, $\{\sigma' \circ \tau \mid \sigma \in \mathrm{Hom}_K(K(a), \overline{K}), \tau \in \mathrm{Hom}_{K(a)}(L, \overline{L})\} = \mathrm{Hom}_K(L, \overline{K})$ となることを言えばよい。これは、命題 108 の証明と全く同じである。

□

系 117. *L/K を有限次 Galois 拡大とすると、任意の $a \in L$, $\sigma \in \mathrm{Gal}\,(L/K)$ に対して $\mathrm{Tr}_{L/K}(a) = \mathrm{Tr}_{L/K}(\sigma(a))$.*

Proof. L/K が Galois 拡大であることに注意すると、命題 116 より $\mathrm{Tr}_{L/K}(a) = \sum_{\tau \in \mathrm{Gal}\,(L/K)} \tau(a)$. 同様に $\mathrm{Tr}_{L/K}(\sigma(a)) = \sum_{\tau \in \mathrm{Gal}\,(L/K)} \tau(\sigma(a))$ であるが、$\sigma \in \mathrm{Gal}\,(L/K)$ だから $\sigma\mathrm{Gal}\,(L/K) = \mathrm{Gal}\,(L/K)$、すなわち、$\tau$ が $\mathrm{Gal}\,(L/K)$ 全体を動くと、$\tau \circ \sigma$ もまた $\mathrm{Gal}\,(L/K)$ の元の全てを動く。従って、

$$\mathrm{Tr}_{L/K}(a) = \sum_{\tau \in \mathrm{Gal}\,(L/K)} \tau(\sigma(a)) = \sum_{\tau \in \mathrm{Gal}\,(L/K)} \tau(a) = \mathrm{Tr}_{L/K}(\sigma(a))$$

を得る。 □

命題 118. *有限代数拡大 L/K が分離拡大であるための必要十分条件は、トレース関数 $\mathrm{Tr}_{K/L} : L \longrightarrow K$ が零関数ではなく、従って全射であることである。*

Proof. L/K が分離拡大だとし、$\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_1, \ldots, \sigma_r\}$ とおくと、命題 116 より

$$\mathrm{Tr}_{L/K} = \sigma_1 + \cdots + \sigma_r$$

と書けるが、命題 111(指標の独立性) を $G = L^*$, $n = r$, $c_i = 1$, $\chi_i = \sigma_i$ の場合に適用すると、$\mathrm{Tr}_{L/K}$ は零関数ではないことがわかる。

逆に $\mathrm{Tr}_{L/K}$ が零関数でないとすると、L/K は分離拡大でなければならない。なぜならば、もし分理拡大でないとすると、標数零の体は完全体だから、L/K は正標数の体である。このとき、命題 116 より $\mathrm{Tr}_{L/K}$ は零写像になってしまい、仮定に反する。

尚、$\mathrm{Tr}_{L/K}$ が零関数でなければ、補題 114 より $\mathrm{Tr}_{L/K}(a) = na(\neq 0)$ $(a \in K - \{0\})$ である。従って、$n^{-1} \in K - \{0\}$ である。そこで、$\mathrm{Tr}_{L/K}(n^{-1}a) = a$ とすれば、$\mathrm{Tr}_{L/K}$ が全射であることがわかる。 □

以下は Hilbert 定理９０の加法版と呼ばれるものであり、p 次巡回拡大 L/K で $p = \mathrm{char}(K) > 0$ の構造に深く関係する。

定理 119 (Hilbert 90 (加法版))**.** L/K を有限次元巡回拡大とし、Gal (L/K) の生成元を σ とする。この時、$b \in L$ に対して、以下は同値。

(i) $\mathrm{Tr}_{L/K}(b) = 0$

(ii) 適当な $a \in L$ によって $b = a - \sigma(a)$.

Proof. $(ii) \Rightarrow (i)$ の証明：$b = a - \sigma(a)$ だとすると、

$$\begin{aligned}
&\mathrm{Tr}_{L/K}(b) \\
&= \mathrm{Tr}_{L/K}(a - \sigma(a)) \\
&= \mathrm{Tr}_{L/K}(a) - \mathrm{Tr}_{L/K}(\sigma(a)) \\
&\quad (\text{行列のトレース } tr \text{ において } tr(A+B) = tr(A) + tr(B) \text{ が成り立つから}) \\
&= \mathrm{Tr}_{L/K}(a) - \mathrm{Tr}_{L/K}(a) \quad (\text{系 } 117 \text{ による}) \\
&= 0.
\end{aligned}$$

$(i) \Rightarrow (ii)$ の証明：$b \in L$ に対して $\mathrm{Tr}_{L/K}(b) = 0$ であるとし、$n = [L : K]$ とおく。L/K は Galois 拡大だから分離拡大になっていて、従って命題 118 よりトレース関数 $\mathrm{Tr}_{L/K} : L \longrightarrow K$ は零関数ではない。よって $\mathrm{Tr}_{L/K}(c) \neq 0$ となるような $c \in L$ が存在する。さて、$a \in L$ を以下のように定義する (両辺を $\mathrm{Tr}_{L/K}(c)(\neq 0)$ で割れば a が得られることに注意)。

$$\begin{aligned}
&a \cdot \mathrm{Tr}_{L/K}(c) \\
&= b \cdot \sigma(c) + (b + \sigma(b)) \cdot \sigma^2(c) + \cdots + (b + \sigma(b) + \cdots + \sigma^{n-2}(b)) \cdot \sigma^{n-1}(c).
\end{aligned}$$

この $a \in L$ によって、$b = a - \sigma(a)$ となる。実際、上式両辺に σ を適用して、

$$\begin{aligned}
\sigma(a) \cdot \mathrm{Tr}_{L/K}(c) &= \sigma(b) \cdot \sigma^2(c) + (\sigma(b) + \sigma^2(b)) \cdot \sigma^3(c) + \\
&\quad \cdots + (\sigma(b) + \sigma^2(b) + \cdots + \sigma^{n-1}(b)) \cdot \sigma^n(c).
\end{aligned}$$

ここで、$\mathrm{Tr}_{L/K}(c) \in K$ だから、$\sigma(\mathrm{Tr}_{L/K}(c)) = \mathrm{Tr}_{L/K}(c)$ となることに注意。従って、

$$\begin{aligned}
&(a-\sigma(a))\cdot \mathrm{Tr}_{L/K}(c)\\
&= \left(\begin{array}{l} b\cdot\sigma(c)+(b+\sigma(b))\cdot\sigma^2(c)+(b+\sigma(b)+\sigma^2(b))\cdot\sigma^3(c)+\\ \cdots+(b+\sigma(b)+\cdots+\sigma^{n-2}(b))\cdot\sigma^{n-1}(c)\end{array}\right)\\
&\quad -\left(\begin{array}{l} \sigma(b)\cdot\sigma^2(c)+(\sigma(b)+\sigma^2(b))\cdot\sigma^3(c)+\\ \cdots+(\sigma(b)+\sigma^2(b)+\cdots+\sigma^{n-2}(b))\cdot\sigma^{n-1}(c)\\ +(\sigma(b)+\sigma^2(b)+\cdots+\sigma^{n-1}(b))\cdot\sigma^n(c).\end{array}\right)\\
&= b\cdot(\sigma(c)+\sigma^2(c)+\sigma^3(c)+\cdots+\sigma^{n-1}(c))\\
&\quad -(\sigma(b)+\sigma^2(b)+\cdots+\sigma^{n-1}(b))\cdot\sigma^n(c).
\end{aligned}$$

となるが、さらに、仮定 (i) と命題 116 より

$$(0=)\mathrm{Tr}_{L/K}(b) = b+\sigma(b)+\cdots+\sigma^{n-1}(b)$$

さらに

$$\mathrm{Tr}_{L/K}(c) = c+\sigma(c)+\cdots+\sigma^{n-1}(c)$$

を使うと、

$$\begin{aligned}
&(a-\sigma(a))\cdot \mathrm{Tr}_{L/K}(c)\\
&= b\cdot(\mathrm{Tr}_{L/K}(c)-c)+b\cdot\sigma^n(c)\\
&= b\cdot \mathrm{Tr}_{L/K}(c) \qquad (\mathrm{Gal}\,(L/K)=\langle\sigma\rangle \text{ は } n \text{ 次巡回群だから } \sigma^n=1)
\end{aligned}$$

を得る。ここで $\mathrm{Tr}_{L/K}(c)\neq 0$ だから、$b = a-\sigma(a)$ となる。 □

8.5. n **次巡回拡大の構成 (**$\mathrm{char}(K)\not| n$ **の場合).** 体 K が 1 の原始 n 乗根を含む場合、n 次の巡回拡大は次のように構成される。

命題 120. 拡大体 L/K と $n\in\mathbb{N}-\{0\}$ で $\mathrm{char}(K)\not| n$ なるものを考える。このとき、L/K が n 次の巡回拡大ならば、$L=K(a)$ で、$a\in L$ の K 上の最小多項式は $X^n-c\in K[X]$ の形をしている。

Proof. $(n,\mathrm{char}(K))=1$ だから、1 の原始 n 乗根 $\zeta\in K$ が存在する。L/K を n 次の巡回拡大だとすると、補題 107 により $N_{L/K}(\zeta^{-1})=\zeta^{-n}=1$ となるから、Hilbert の定理９０により適当な元 $a\in L^*$ が存在して $\sigma(a)=\zeta a$ となる。ここで $\langle\sigma\rangle=\mathrm{Gal}\,(L/K)$ とする。そこで

$$\sigma^i(a)=\zeta^i a,\quad (i=0,\ldots,n-1)$$

となり、これらは互いに相異なる。$a\in L$ の K 上の最小多項式 f を考えると、$\mathrm{Gal}\,(L/K)$ の元は一般に a を f の a 以外の元に移すのだから、このことは f の根が少なくとも n 個は存在することを意味する。従って、

$$[K(a):K]\geq n.$$

また、$K(a) \subset L$, $[L:K] = n$ だから、$n = [L:K] \geq [K(a):K] \geq n$ より、結局 $L = K(a)$ で、上の $\sigma^i(a)$, $i = 0, \ldots, n-1$ が、a の最小多項式の解の全てである。ここで

$$\sigma(a^n) = \sigma(a)^n = \zeta^n a^n = a^n$$

となって、a^n は $\mathrm{Gal}\,(L/K)$ によって固定されるから、$a^n \in K$. 従って、$f = X^n - c$, $c := a^n$ となる。 □

注意 121. 命題 *120* の逆、すなわち「1 の原始 n 乗根を含む体 K に対し、$X^n - c \in K[X]$ が既約多項式ならば、その零点 $a \in \overline{K}$ による拡大 $L := K(a)/K$ は n 次巡回拡大である」も成立するが、証明は省略。

8.6. **巡回拡大の構成 (Artin-Schreier 拡大).** 以下の定理は正標数の拡大体において基本的である。

定理 122 (Artin-Schreier)**.** $\mathrm{char}\, K = p > 0$ とし、L/K を拡大体とする。このとき

(*i*) L/K が p 次巡回拡大ならば、適当な $c \in K$ による $X^p - X - c \in K[X]$ を最小多項式とする $a \in L$ によって $L = K(a)$ となる。

(*ii*) 逆に、$X^p - X - c \in K[X]$ の零点 $a \in L$ によって $L = K(a)$ となっているならば、L/K は巡回拡大であり、特に $X^p - X - c$ が $K[X]$ の中で既約ならば p 次巡回拡大であるが、既約でなければ 1 次式の積の分解し、$L = K$ となる。

Proof. (*i*) の証明: L/K が次数 p の巡回拡大とし、$\mathrm{Gal}\,(L/K) = \langle\sigma\rangle$ とする。補題 114 より、任意の $c \in K$ に対して $\mathrm{Tr}_{L/K}(c) = pc = 0$. 特に $c = -1$ をとれば、Hilbert の定理 90 の加法版 (定理 119) より、$\sigma(a) - a = 1$ となるような $a \in L$ が存在する。すると

$$\sigma^i(a) = a + i, \qquad i = 0, \ldots, p-1$$

となる。$\sigma^0(a) = a$, $\sigma^1(a) = a+1, \ldots, \sigma^{p-1}(a) = a + p - 1$ は互いに相異なるから、a の K 上の最小多項式は少なくとも p 次以上である。すなわち、$[K(a):K] \geq p$. 従って

$$p = [L:K] = [L:K(a)][K(a):K] \geq p$$

より、$L = K(a)$ でなければならないことがわかる。さらに、

$$\sigma(a^p - a) = \sigma(a)^p - \sigma(a) = (a+1)^p - (a+1) = a^p - a$$

だから、$c := a^p - a \in K$ であり、a は $X^p - X - c$ の零点である。$a \in L$ の K 上の最小多項式は p 次以上だったから、$X^p - X - c$ が実は a の最小多項式になっている。

(*ii*) の証明 :$L = K(a)$ かつ、$a \in L$ は $f = X^p - X - c \in K[X]$ の零点であるとする。ここで

$$a, a+1, \ldots, a+p-1 \in L$$

が f の全ての零点であること、すなわち $a+i$, $(i = 0, \ldots, p-1)$, が f の零点であることを i に関する数学的帰納法で示そう。$i = 0$ の場合は仮定により成り立つ。$i > 0$ の場合は、

$$\begin{aligned} f(a+i+1) &= (a+i+1)^p - (a+i+1) - c \\ &= (a+i)^p - (a+i) - c + 1^p - 1 = f(a+i) \\ &= 0 \quad (\text{帰納法の仮定により } f(a+i) = 0 \text{ だから}) \end{aligned}$$

となる。ここで f の零点の１つでも K に含まれていれば、それ以外の元との差は $\mathbb{N}$ の要素分でしかないから、それらも全て K に含まれてしまう。したがって f は K 上の１次式の積の形に完全に分解されるかのどちらかである。また、以上の議論により、f は分離多項式であり、L は f の分解体で K 上の Galois 拡大であることもわかる。特に f が１次式に完全に分解されるので $L = K$ であり、これは自明な巡回拡大（１次の巡回拡大）である。次に、f のいずれの零点も K に含まれない場合を考える。このとき、f が K 上既約になることを示そう。もしそうでないとすると、$a + i$ $(i = 0, \ldots, p-1)$ が f の零点であることから、

$$f = \prod_{i=0}^{p-1}(X - a - i) = gh \qquad (g, h \in K[X] - K)$$

の形に分解する。ここで $\deg g = d(> 0)$ だとする。すると、g は $X - a - i$, $(0 \leq i \leq p-1)$ の一次因子のうちのいずれかの d 個の積になっているから、g における X^{d-1} の係数は、

$$-da + j \qquad (0 \leq j \leq p-1)$$

の形をしている。特に j の範囲を上のように考えて良いのは、標数が p であるからである。$0 < d < p = \deg f$ だから $p \not| d$ となり、d は（標数 p の体である）K の中で零にはならない。従って、$-da + j \in K$ より $a \in K$ が従い、$a + i$, $(0 \leq i \leq p-1)$ のいずれも K に含まれないという仮定に反する。よって f は K 上既約でなければならないことが分かった。この場合もやはり、L は既約な分離多項式 f の分解体になっているから、L/K は $p(= \deg f)$ 次の Galois 拡大であることがわかる。そこで補題 49 により $\sigma \in \mathrm{Gal}\,(L/K)$ として $\sigma(a) = a + 1$ なるものを選ぶことができるが、σ の位数は p なので、σ で生成される巡回部分群だけで $\mathrm{Gal}\,(L/K)$ 全体を占めている。つまり L/K は p 次巡回拡大である。 □

まとめ

- $\mathrm{char}(K) = p$, $(n, p) = 1$ の場合、K の n 次巡回拡大 L/K は $X^n - c \in K[X]$ の形の最小多項式を持つ $a \in \overline{K}$ による単純拡大 $L = K(a)$ に限られる。
- $\mathrm{char}(K) = p > 0$ の時、K の p 次巡回拡大 L/K は $X^n - X - c \in K[X]$ の最小多項式を持つ $a \in \overline{K}$ による単純拡大 $L = K(a)$ に限られる。

9. 有限体とその代数拡大

体 K には乗法が定義されているが、だからと言って K は乗法群ではない。実際、$0 \in K$ は乗法単位元 (つまり 1) ではないにもかかわらず、逆元 $1/0$ が存在しないからである。しかし、K から 0 を除いた集合 $K - \{0\}$ は一般に乗法群になる。この乗法群のことを K^* と書く（文献によっては $K^\times$ と書くことも少なくない)。

命題 123. K を体とし、K^* の任意の有限乗法群 $H \subset K$ は巡回群である。特に K が有限体ならば、K^* は巡回群である。

Proof. $\sharp H < \infty$ ゆえ、位数 (order) が最大の元 $a \in H$ をとることができる。その元の位数を $m := \mathrm{ord}(a)$ として、$H_m := \{b \in H \mid \mathrm{ord}(b) \text{ は } m \text{ の約数 }\}$ とする。このとき

Claim 1: これは H の部分群である

Claim 1 の証明. K は可換体だから、乗法群 K^* はアーベル群であることに注意する。さて、$a, b \in H_m$ とし、$\ell := \mathrm{lcm}(\mathrm{ord}(a), \mathrm{ord}(b))$ とすると $\ell = \ell_1 \cdot \mathrm{ord}(a) = \ell_2 \cdot \mathrm{ord}(b)$ なる $\ell_1, \ell_2 \in \mathbb{N}$ が存在して、$(a \cdot b)^\ell = a^\ell \cdot b^\ell = (a^{\mathrm{ord}(a)})^{\ell_1} \cdot (b^{\mathrm{ord}(b)})^{\ell_2} = 1$ となるから、$\mathrm{ord}(a \cdot b)$ は ℓ の約数[23]. また、m は $\mathrm{ord}(a)$, $\mathrm{ord}(b)$ の公倍数だから、(それらの最初公倍数である)ℓ の倍数。よって $\mathrm{ord}(a \cdot b)$ は m の約数となり、$a \cdot b \in H_m$ を得る。また $1 = b^{\mathrm{ord}(b)} = b \cdot b^{\mathrm{ord}(b)-1} = b^{\mathrm{ord}(b)-1} \cdot b$ だから $b^{-1} = b^{\mathrm{ord}(b)-1}$ であるが、$(b^{-1})^{\mathrm{ord}(b)} = (b^{\mathrm{ord}(b)})^{\mathrm{ord}(b)-1} = 1$ だから、$\mathrm{ord}(b^{-1})$ は $\mathrm{ord}(b)$ の約数。よって m の約数となるから、$b^{-1} \in H_m$ となる。以上により、$a, b \in H_m$ に対して $a \cdot b^{-1} \in H_m$ を得るから、H_m は H の部分群である。 □

H_m の要素は全て $X^m - 1$ の零点だから、$\sharp(H_m) \leq m$ である。いっぽう、Claim 1 より H_m は群だから、$a \in H$ のべきは全て H に含まれる。すなわち、a で生成される巡回部分群が $\langle a \rangle \subset H_m$ となる。そして $m = \mathrm{ord}(a)$ だから $\sharp\langle a \rangle = m$ となる。つまり不等式

$$m = \sharp\langle a \rangle \leq \sharp(H_m) \leq m$$

が成り立つから、結局 $H_m = \langle a \rangle$ でなければならない。さらに以下の Claim 2 によって H は巡回群であることがわかる。

Claim 2: $H = H_m$ である。

Claim 2 の証明. 実際、$H \ni b \notin H_m$ なる b が存在したとすると、$n := \mathrm{ord}(b) \not| m$. すると $\mathrm{ord}(a \cdot b) = \mathrm{lcm}(n, m) > m$ となってしまい[24]、$m = \mathrm{ord}(a)$ を最大にとったことに矛盾する。よって、上のような $b \in H$ は存在せず、$H = H_m$ となる。 □

[23] ここで $\ell = \mathrm{ord}(a \cdot b)$ となるとは限らない。例えば、$\mathrm{ord}(c) = 12$ だとし、$a := c^2$, $b := c^4$ とすると、$\mathrm{ord}(a) = 6$, $\mathrm{ord}(b) = 3$ で $\ell = 6$ である。しかるに $a \cdot b = c^6$ だから $\mathrm{ord}(a \cdot b) = 2$ となる。

[24] $\mathrm{ord}(a \cdot b)$ は $\mathrm{lcm}(n, m)$ の約数であるが、もし $k := \mathrm{ord}(a \cdot b) < \mathrm{lcm}(n, m)$ となるとすれば、それは a^k と b^k が互いに逆元になっている場合である。すなわち、ある $c \in K$ があって、それによって $a = c^s$, $b = c^t$, $k(s + t) = \mathrm{ord}(c)$, $\mathbb{N} \ni s, t < m$ となっている場合に限られる。今 a が最大位数の元と仮定しているから、$\gcd(s, m) = 1$ かつ $\mathrm{ord}(c) = \mathrm{ord}(a) = m$ でなければならない（$\gcd(s, m) > 1$ ならば、$\mathrm{ord}(a) < \mathrm{ord}(c)$ となってしまう)。よって $\mathrm{ord}(b) = \mathrm{ord}(c^t) = \frac{\mathrm{ord}(c)}{\gcd(t, \mathrm{ord}(c))}$, すなわち m の約

□

有限体の構造については、次の定理が基本的である。

定理 124. 任意の素数 p と $n \in \mathbb{N} - \{0\}$ に対し、拡大体 $\mathbb{F}_q/\mathbb{F}_p$, $\sharp\mathbb{F}_q = q = p^n$ が存在し、$X^q - X = 0$ の $\mathbb{F}_p$ 上の分解体として同型を除いて一意的である。また、$\mathrm{char}(K) = p > 0$ なる任意の有限体 K は、いずれかの $\mathbb{F}_q$ に同型である。

Proof. $f = X^q - X$ とおく。$\frac{df}{dX} = p^n X^{p^n-1} - 1 = -1$ だから、f は分離的多項式。したがって f は適当な代数的閉包 $\overline{\mathbb{F}_p}$ の中でちょうど q 個の（重複のない）零点をもつ。ここで $a, b \in \overline{\mathbb{F}_q}$ を f の相異なる 2 つの零点とすると、命題 35 より

$$(a \pm b)^q = a^q \pm b^q = a \pm b$$

だから、$a \pm b$ もまた f の零点である。さらに $b \neq 0$ だとすると

$$(ab^{-1})^q = a^q (b^q)^{-1} = ab^{-1}$$

だから、結局 f の $\overline{\mathbb{F}_q}$ における零点集合は、体になっている。特に、これは $X^q - X$ の分解体である。よって $\mathbb{F}_q$ の存在と分解体としての一意性は言えた。

次に、K が $\mathrm{char}(K) = p > 0$ なる任意の有限体だとすると、K は $\mathbb{F}_p$ 上の有限次元ベクトル空間だから、

$$K \cong \underbrace{(\mathbb{F}_p \oplus \cdots \oplus \mathbb{F}_p)}_{\dim_{\mathbb{F}_p} K}$$

となる。従って $\sharp K = p^n =: q$, $(n := \dim_{\mathbb{F}_p} K)$. 命題 123 より K^* は位数 $q-1$ の巡回群であり、$X^{q-1} - 1$ の零点集合。従って、K は $X^q - X = 0$ の零点集合である。つまり、K は $\mathbb{F}_p$ 上 $X^q - X = 0$ の分解体で $\sharp(K) = q = p^n$ である。

□

標数 0 の体は完全体だったが (定理 69)、正標数の体も有限体の場合は完全体となる。

定理 125. 有限体の有限次代数拡大は *Galois* 拡大である。特に有限体は完全体である。

Proof. $\mathbb{F}$ を有限体とし、$K/\mathbb{F}$ を任意の有限次代数拡大とする。K は $\mathbb{F}$ 上の有限次元ベクトル空間だから、有限体である。よって $K = \mathbb{F}_q$, $q = p^n$, の形に書けるので、K は分離多項式 $X^q - X = 0$ の分解体に他ならない。従って $K/\mathbb{F}$ は Galois 拡大になる。 □

命題 126. 有限体の有限次代数拡大は巡回拡大である。

数となり、$b \in H_m$ となってしまう。これは b のとりかたに反する。よって $\mathrm{ord}(a \cdot b) = \mathrm{lcm}(n, m)$ でなければならない。

Proof. 有限体 $K := \mathbb{F}_q$ の有限次拡大 $L := \mathbb{F}_{q'}$ を考え、$[\mathbb{F}_{q'} : \mathbb{F}_q] = n$ とする。このとき、定理 125 より L/K はガロア拡大であり、$\sharp\mathrm{Gal}\,(\mathbb{F}_{q'}/\mathbb{F}_q) = n$ である。また、$q = p^r$ とおけば、$q' = q^n = p^{rn}$ となる。ただし、$\mathrm{char}(K) = \mathrm{char}(L) = p > 0$ とする。

さて、ここで Frobenius 写像

$$\sigma : L \longrightarrow L, \qquad a \longmapsto a^p$$

を考える。K^* は位数 $q - 1 = p^r - 1$ の巡回群（命題 123)、すなわち任意の $a \in K^*$ に対して $a^{p^r-1} = 1$. よって特に任意の $a \in K$ に対して

$$\sigma^r(a) = a^{p^r} = a \qquad (\text{ただし、} \sigma^r = \underbrace{\sigma \circ \cdots \circ \sigma}_{r})$$

が成り立つ。すなわち、σ^r は K の元を固定するので、$\sigma^r \in \mathrm{Gal}\,(L/K)$ となる。また、有限体 $L = \mathbb{F}_{p^{nr}}$ は $X^{p^{nr}} - X = 0$ の根だから、任意の $a \in L$ に対して $a^{p^{nr}} = a$, すなわち、$\sigma^{nr} = 1$ である。したがって σ^r の位数は $\leq n$ となる。ここでもし、$\mathrm{ord}(\sigma^r) < n$ だとすると、$e := \mathrm{ord}(\sigma) < rn$ となり、全ての $a \in L$ が $\sigma^e(a) = a$, すなわち $X^{p^e} - X = 0$ の根となってしまう。つまり、$\sharp L = p^e < p^{nr} = q' = \sharp L$. これは矛盾である。よって、$\mathrm{ord}(\sigma^r) = n$ でなければならない。すると $\langle\sigma\rangle \subset \mathrm{Gal}\,(L/K)$ で $n = \sharp\langle\sigma\rangle \leq \sharp\mathrm{Gal}\,(L/K) = n$ だから、結局 $\mathrm{Gal}\,(L/K) = \langle\sigma\rangle$ でなければならない。つまり L/K は巡回拡大。 □

まとめ

- 有限体 K に対して K^* は巡回群。
- 任意の有限体 K は $X^q - X$, $(q = p^n,\, n \in \mathbb{N} = \{0\}, \mathrm{char}(K) = p > 0)$ の分解体であり、$q = p^n$ 個の要素を持つ。
- 有限体の有限次代数拡大はすべて巡回拡大で、その Galois 群は Frobenius 写像で生成される。特に、有限体は完全体である。

10. 代数方程式論への応用

この章で示す結果は、正標数でも同様のことが示せるが、議論を簡単にするために、下では体は全て標数 0 であると仮定する。従って、ここで考える任意の体 K は、素体として $\mathbb{Q}$ を含み（$\mathbb{Q} \subset K$）、代数拡大は全て分離拡大になることに注意。

10.1. **方程式の可解性.** 4 次以下の代数方程式に「根の公式」が存在するということは、それらの方程式が以下に定義する意味で「代数的に解ける」ということである。

定義 127 (代数的に解ける)**.** 代数方程式

$$X^n + a_1 X^{n-1} + \cdots + a_{n-1} X + a_n = 0 \quad (a_i \in \mathbb{C})$$

が**代数的に解ける**とは、方程式の根が、係数 $a_1, \ldots, a_n$ と有理数を使った四則演算とべき根 $(\sqrt[m]{-},\ m \geq 2)$ 演算を使って表せることを言う。

このことを代数拡大の理論から見れば、次の概念でとらえることができる。

定義 128 (べき根による拡大)**.** 有限次代数拡大 L/K が、**べき根による拡大**であるとは、体の列

$$K = K_0 \subset K_1 \subset \cdots \subset K_r = E$$

で各 K_i $(i \geq 1)$ は $K_{i-1}(\sqrt[n_i]{a_i})$ の形で得られるものが存在し、$L \subset E$ となっている場合をいう。特別な場合として $E = L$ となる場合も当然含む。ただし、$a_i \in K_{i-1}$ で、$X^{n_i} - a_i \in K_{i-1}[X]$ は既約であるとする。

2 つの定義を見比べれば、以下のことが直ちに従う。

命題 129. 代数方程式

$$f := X^n + a_1 X^{n-1} + \cdots + a_{n-1} X + a_n = 0 \quad (a_i \in \mathbb{C})$$

の根を $x_1, \ldots, x_n \in \mathbb{C}$ とし、拡大体 $K := \mathbb{Q}(a_1, \ldots, a_n) \subset L := K(x_1, \ldots, x_n)$ を考える。このとき、以下は同値：

(1) $f = 0$ が代数的に解ける。
(2) L/K はべき根による拡大。

例 130. 2 次方程式

$$X^2 + aX + b = 0 \quad (a, b \in \mathbb{C})$$

を考えると、その根は $K := \mathbb{Q}(a, b)$ のべき根による拡大体

$$L = K\left(\frac{-a + \sqrt{a^2 - 4b}}{2}, \frac{-a - \sqrt{a^2 - 4b}}{2}\right) = K(\sqrt{a^2 - 4b})$$

に含まれる。

例 131. 3 次方程式

$$X^3 + pX + q = 0 \quad (p, q \in \mathbb{C})$$

を考えると、その根は $K := \mathbb{Q}(p,q)$ のべき根による拡大体

$$\begin{aligned} K &\subset K_1 := K(\zeta) = K(\sqrt{-3}) \\ &\subset K_2 := K_1\left(\sqrt{\frac{p^3}{27}+\frac{q^2}{4}}\right) \\ &\subset K_3 := K_2\left(\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{p^3}{27}+\frac{q^2}{4}}}\right) \\ &\subset K_4 := K_3\left(\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{p^3}{27}+\frac{q^2}{4}}}\right) \end{aligned}$$

に含まれる。ここで $\zeta = \frac{-1+\sqrt{-3}}{2}$ は 1 の原始 *3* 乗根。実際、解 x_1, x_2, x_3 は

$$\begin{aligned} x_1 &= \sqrt[3]{-\frac{q}{2}+\sqrt{\frac{p^3}{27}+\frac{q^2}{4}}}+\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{p^3}{27}+\frac{q^2}{4}}} \\ x_2 &= \zeta^2\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{p^3}{27}+\frac{q^2}{4}}}+\zeta\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{p^3}{27}+\frac{q^2}{4}}} \\ x_3 &= \zeta\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{p^3}{27}+\frac{q^2}{4}}}+\zeta^2\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{p^3}{27}+\frac{q^2}{4}}} \end{aligned}$$

であることが知られている。

例 132. *4* 次方程式

$$X^4 + pX^2 + qX + r = 0 \quad (p,q,r \in \mathbb{C})$$

の解は、まずは 3 次方程式

$$Z^3 - 2pZ^2 + (p^2 - 4r)Z + q^2 = 0$$

の解を含むような $K := \mathbb{Q}(p,q,r)$ のべき根による拡大

$$K \subset \cdots \subset K_4$$

を考え（例 *131* 参照）、$z_1, z_2, z_3 \in K_4$ を上の 3 次方程式の解とすると、

$$K \subset \cdots \subset K_3 \subset K_4 := K_3(\sqrt{-z_1}) \subset K_5 := K_4(\sqrt{-z_2}) \subset K_6 := K_5(\sqrt{-z_3})$$

の中に４次方程式の解 x_1, x_2, x_3, x_4 が含まれる。実際、

$$\begin{aligned} x_1 &= \frac{1}{2}(\sqrt{-z_1} + \sqrt{-z_2} + \sqrt{-z_3}) \\ x_2 &= \frac{1}{2}(\sqrt{-z_1} - \sqrt{-z_2} - \sqrt{-z_3}) \\ x_3 &= \frac{1}{2}(-\sqrt{-z_1} + \sqrt{-z_2} - \sqrt{-z_3}) \\ x_4 &= \frac{1}{2}(-\sqrt{-z_1} - \sqrt{-z_2} + \sqrt{-z_3}) \end{aligned}$$

であることが知られている。

10.2. **５次以上の代数方程式の非可解性.** 前節では代数方程式が代数的に解けることを、べき根による代数拡大として特徴づけた。ここでは、べき根による代数拡大を群論的に特徴づける。これによって、５次以上の代数方程式に「解の公式」が存在しないことを、群論を使って証明することができるようになる。

定義 133. 群 G が**可解群**であるとは、

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\}$$

なる部分群の列で、$G_{i+1} \triangleleft G_i$ $(i = 0, \ldots, n-1)$ かつ、剰余群 G_{i+1}/G_i がアーベル群である場合をいう。

定義 134 (可解拡大)**.** 有限次拡大 L/K が**可解拡大**であるとは、適当な有限次 *Galois* 拡大 E/K が存在して、$E \supset L$ かつガロア群 $\mathrm{Gal}\,(E/K)$ が可解群となる場合をいう。

定理 135. 有限次拡大 L/K がべき根による拡大であることと、可解拡大であることは、同値である。

この定理の証明は次節以降に回し、まずは重要な応用を述べよう。

系 136. *5*次以上の代数方程式の解の公式は存在しない。すなわち、方程式の解を、係数（と有理数）の四則演算とべき根演算で書き表す一般的な公式は作れない。

Proof. n 次方程式

$$f = X^n + a_1 X^{n-1} + \cdots + a_{n-1} X + a_n = 0 \quad (a_i \in \mathbb{C})$$

の解は代数学の基本定理により、重根も含めて n 個ある。それを $x_1, \ldots, x_n \in \mathbb{C}$ と置き、拡大体 $K := \mathbb{Q}(a_1, \ldots, a_n) \subset L := K(x_1, \ldots, x_n)$ を考える。

今、f が $K[X]$ の元として既約としてよい（そうでなければ因数分解して、より低次の方程式に帰着されてしまう）。すると $\mathrm{char}(K) = 0$ だから f は分離多項式で、$x_1, \ldots, x_n$ はすべて相異なる。すると L/K は有限次 Galois 拡大である。

そこでガロア群 $\mathrm{Gal}\,(L/K)$ は $x_1, \ldots, x_n$ の置換だから n 次対称群 $\mathfrak{S}_n$ の部分群（に同型）である。ありとあらゆる n 次方程式を考えると、ちょうど $\mathrm{Gal}\,(L/K) = \mathfrak{S}_n$ となるような方程式も存在する（次の命題 137 参照））。

方程式の解の公式をつくろうと思えば、このような方程式にも対応できなければならない。しかるに、$\mathfrak{S}_n$ $(n \geq 5)$ は可解群にならないことが群論で知られている。よって定理 135 により、そのような方程式は代数的には解けない。したがって、方程式を代数的に解くための一般的な公式は存在しえない。 □

以下は、一般多項式と呼ばれるものの存在を示している。

命題 137. 任意の $n \in \mathbb{N} - \{0\}$ に対して、適当な拡大体 $K/\mathbb{Q}$ と既約分離 n 次多項式 $f \in K[X]$ が存在して、その $\overline{K}$ における解を $x_1, \ldots, x_n$ として $L := K(x_1, \ldots, x_n)$ をすると、L/K は *Galois* 拡大になり、$\mathrm{Gal}\,(L/K) \cong \mathfrak{S}_n$ となる。

Proof. まず、$x_1, \ldots, x_n \in \mathbb{C}$ で、任意の零でない $\mathbb{Q}$ 係数の多項式 $h(X_1, \ldots, X_n)$ に対して、$h(x_1, \ldots, x_n) \neq 0$ となるようなものが存在する[25]。これは次のように示される：$\mathbb{Q}$ 上代数的な $\mathbb{C}$ の中の元に、その最小多項式の係数を対応させると、代数的な元の個数は高々$\sharp\mathbb{Q}$ の可算無限倍だから、結局、可算無限個しかない。しかるに $\sharp\mathbb{C}$ は可算無限個よりも大きいから、$\mathbb{Q}$ 上代数的でない元は無限個存在する。その 1 つを $x_1 \in \mathbb{C}$ とする。$\mathbb{Q}(x_1)/\mathbb{Q}$ は純超越拡大だから、$\mathbb{Q}(x_1)$ の元は x_1 を変数とみなした時の $\mathbb{Q}[x_1]$ の元の分数の形。ここで $\sharp\mathbb{Q}[x_1]$ は可算無限個だから、$\sharp\mathbb{Q}(x_1)$ も可無限個。次に $\mathbb{Q}(x_1)$ 上代数的な元を考えると、それは上と同じ議論により高々可算無限個だから、やはり $\mathbb{Q}(x_1)$ 上超越的な元 $x_2 \in \mathbb{C}$ がとれる。同様にして、x_i を $\mathbb{Q}(x_1, \ldots, x_{i-1})$ 上超越的な元として選んでいけば、上の条件を満たすような $x_1, \ldots, x_n \in \mathbb{C}$ が選べる。

そこで X についての多項式

$$\begin{aligned} f &= (X - x_1)(X - x_2)\cdots(X - x_n) \\ &= X^n - s_1 X^{n-1} + \cdots + (-1)^k s_k X^{n-k} + \cdots + (-1)^n s_n \end{aligned}$$

を考える。ここで s_k は k 次基本対称式と呼ばれるもので、

$$\begin{aligned} s_1 &= x_1 + \cdots + x_n \\ &\vdots \\ s_k &= \prod_{i_1 < \ldots < i_k} x_{i_1} \cdots x_{i_k} \\ &\vdots \\ s_n &= x_1 \cdots x_n \end{aligned}$$

である。$x_1, \ldots, x_n$ の選び方から、これらは相異なる変数と考えてよいから、s_k は変数 $x_1, \ldots, x_n$ に関する k 次の単項式と思ってよい。さて、$K := \mathbb{Q}(s_1, \ldots, s_n) \subset L := K(x_1, \ldots, x_n)$ なる拡大体を考える。すると $f \in K[X]$ で、L は分離多項式 f の K 上の分解体になっているから、Galois 拡大である。また、f は K 上既約多項式である。何故なら、もし既約でなければ、$f = gh$, なる 1 次以上の多項式 $g, h \in K[X]$ が存在することになるが、この時、必要ならば x_i の添え字を付け替えて $g = (X - x_1)(X - -x_2)\cdots(X - x_k)$ $(k < n)$ としてよい。しかし、このとき $g = X^k - (x_1 + \cdots + x_k)X^{k-1} + \cdots + (-1)^k x_1 \cdots x_k$ で、例えば $s_1' := x_1 + \cdots + x_k \in K = \mathbb{Q}(x_1 + \cdots + x_n, s_2, \cdots s_n)$

[25] これを $x_1, \ldots, x_n$ は $\mathbb{Q}$ 上**代数的独立**であると言う。

でなければならない。しかし s_1' は $\{x_i\}$ に関する 1 次式で、K の中に $\{x_i\}$ の 1 次式は $x_1+\cdots+x_k+\cdots+x_n$ しかない。そして $\{x_i\}$ の取り方から、次数の高い s_j $(j\geq 2)$ と $\mathbb{Q}$ をいくら組み合わせても $x_1+\cdots+x_k$ を表すことはできないからである。よって $f\in K[X]$ は既約と分かった。

すると任意の $1\leq i<j\leq n$ に対して、$\sigma(x_i)=x_j$ となる $\sigma\in \mathrm{Gal}\,(L/K)$ が存在するから、結局 $\mathrm{Gal}\,(L/K)$ は $x_1,\ldots,x_n$ の並べ替え操作の全てを含んでいる。つまり $\mathfrak{S}_n\subset \mathrm{Gal}\,(L/K)$ と考えることができる。また、一般に $\mathrm{Gal}\,(L/K)\subset \mathfrak{S}_n$ だから、結局 $\mathrm{Gal}\,(L/K)=\mathfrak{S}_n$ となる。 □

注意 138. 5 次以上の代数方程式には、「(代数的にとくための) 一般的解の公式がつくれない」のであって、「5 次以上の全ての代数方程式は代数的には解けない」わけでは**ない**。実際、特殊な方程式については代数的に解くことができる。たとえば、$X^6-1=(X-1)(X^5+X^4+X^3+X^2+X+1)$ に注意すると、5 次方程式

$$X^5+X^4+X^3+X^2+X+1=0$$

の根は、原始 6 乗根 $\zeta=\frac{1+\sqrt{-3}}{2}$ で生成された巡回群から $\zeta^6=1$ を除いたものである。つまり、根はべき根による拡大

$$\mathbb{Q}\subset \mathbb{Q}(\zeta)=\mathbb{Q}(\sqrt{-3})$$

の元になっていし、方程式の係数に四則演算とべき演算をほどこしたもので書き表すことができる。

10.3. **群論からの準備.** この節では、定理 135 を証明するために、特に可解群の扱いについて、いくつかの群論の結果を準備しておく。

命題 139. G を有限可解群とする。このとき、部分群列

$$G=G_0\supset G_1\supset\cdots\supset G_n=\{1\}$$

で、$i=0,\ldots,n-1$ に対して $G_i\triangleright G_{i+1}$ かつ G_i/G_{i+1} は素数位数の巡回群 となるものが存在する。

Proof. まず、G が可解群であることから、

$$G=G_0\supset G_1\supset\cdots\supset G_n=\{1\}$$

で、$i=0,\ldots,n-1$ に対して $G_i\triangleright G_{i+1}$ かつ G_i/G_{i+1} がアーベル群であるような部分群列が存在する。ここで G は有限群だから、各 G_i/G_{i+1} は有限アーベル群。これがもし素数位数の巡回群でなければ、単位元ではない任意の元 $\overline{a}\in G_i/G_{i+1}$ をとり、適当な $\ell\in\mathbb{N}$ によって $\overline{b}:=\overline{a}^{\ell}$ をとれば、$\overline{b}$ は素数位数になる (例えば、$\mathrm{ord}(\overline{a})=pq$, p は素数, とすれば、$\ell=q$ とすればよい)。そこで巡回部分群 $\langle\overline{b}\rangle\subset G_i/G_{i+1}$ の、自然準同型

$$\varphi: G_i\longrightarrow G_i/G_{i+1}$$

による逆像を H とすれば

$$G_i\supset H\supset G_{i+1},\quad (G_i\neq H\neq G_{i+1})$$

となる。ここで $G_i \triangleright H$ である。実際、G_i/G_{i+1} はアーベル群だから、$G_i/G_{i+1} \triangleright \langle \bar{b} \rangle$ であり、その φ による逆像である H も (G_i/G_{i+1} の逆像である)G_i の正規部分群であり、短完全列

$$1 \to \mathrm{Ker}\,\varphi \longrightarrow H \xrightarrow{\varphi|_H} \langle \bar{b} \rangle \to 1$$

にて、$\mathrm{Ker}\,\varphi = H \cap G_{i+1} = G_{i+1}$ だから、群の準同型定理により

$$H/G_{i+1} \cong \langle \bar{b} \rangle$$

が成り立つ。つまり H/G_{i+1} は巡回群である。さらに、$G_i \triangleright G_{i+1}$ で、$G_i \supset H$ だから、$H \triangleright G_{i+1}$ が成り立つ。また、

$$G_i/G_{i+1} \longrightarrow G_i/H$$

なる自然全射が存在し、G_i/G_{i+1} がアーベル群だから、G_i/H もまたアーベル群でなければならない。以上のことから、

$$G = G_0 \supset G_1 \supset \cdots \supset G_i \supset H \supset G_{i+1} \supset \cdots \supset G_n = \{1\}$$

を新しい部分群列とできる。ここで H/G_{i+1} が素数位数の巡回群に代わっていることに注意。同様の操作をして、$G_i \supset G_{i+1}$ を

$$G_i \supset H_0 \supset H_1 \supset \cdots \supset H_k \supset G_{i+}1$$

なる部分群列に細分化して、$G_i \triangleright H_0,\ H_j \triangleright H_{i+1},\ (i = 0, \ldots, k-1),\ H_k \triangleright G_{i+1},$ $G_i/H_0, H_j/H_{j+1}, (j = 0, \ldots, k-1), H_k/G_{i+1}$ が全て素数位数の巡回群となるようにできる。この操作を繰り返せば、所期の部分群列を構成することができる。 □

可解群を扱う際には、次の概念が便利である。

定義 140 (交換子と交換子群)**.** 群 G と $a, b \in G$ に対して $[a, b] := aba^{-1}b^{-1}$ を a, b の**交換子**と呼び、

$$[G, G] = \langle [a, b] \mid a, b \in G \rangle \quad \textit{(}\text{交換子全体で生成された群}\textit{)}$$

を G の**交換子群**と呼ぶ。

注意 141. ここで、$[G, G] = \{[a, b] \mid a, b \in G\}$ (交換子の集合）ではないことに注意する。実際、一般に 2 つの交換子の積が再び交換子になるとは限らない。つまり、任意の $a, b, c, d \in G$ に対して、上手に $e, f \in G$ を選べば、

$$\begin{aligned} [a, b] \cdot [c, d] &= aba^{-1}b^{-1}cdc^{-1}d^{-1} \\ &= efe^{-1}f^{-1} \end{aligned}$$

とすることができるかというと、必ずしもそうではない。

交換子群はアーベル群とは限らない群からアーベル群をつくるための便利なツールである。以下の結果の証明で鍵となるのは、次の単純な事実である：

$$[a, b] = 1 \Longleftrightarrow ab = ba.$$

つまり、交換子は 2 つの要素の（非）可換性を測る尺度の役割を果たす。

命題 142. 群 G に対して、$[G,G] \triangleleft G$ であり、剰余群 $G/[G,G]$ はアーベル群である。さらに、任意の正規部分群 $H \triangleleft G$ に対して G/H がアーベル群ならば、$[G,G] \subset H$ である。

Proof. $[G,G]$ は、その定義からそもそも G の部分群であるから、$[G,G] \triangleleft G$ を示すためには、任意の $g \in G$ に対して $g^{-1}[G,G]g \subset [G,G]$ であること、すなわち、任意の $a,b,g \in G$ に対して、$g^{-1}[a,b]g \in [G,G]$ であることを示せばよい。実際、

$$\begin{aligned} g^{-1}[a,b]g &= g^{-1}aba^{-1}b^{-1}g \\ &= (g^{-1}ag)(g^{-1}ag)(g^{-1}bg)(g^{-1}a^{-1}g)(g^{-1}b^{-1}g) \\ &= [g^{-1}ag, g^{-1}bg] \end{aligned}$$

となっているから、それは成り立つ。次に $G/[G,G]$ がアーベル群であることを示そう。自然全射準同型

$$\pi : G \longrightarrow G/[G,G] \qquad (g \longmapsto \overline{g} := \pi(g))$$

を考えると、$G/[G,G]$ の任意の 2 つの元は $\overline{g}, \overline{h}$ $(g,h \in G)$ の形に掛けるが、その交換子をとると

$$\begin{aligned} [\overline{g},\overline{h}] &= \overline{g}\overline{h}\overline{g}^{-1}\overline{h}^{-1} \\ &= \pi(g)\pi(h)\pi(g)^{-1}\pi(h)^{-1} \\ &= \pi(ghg^{-1}h^{-1}) \quad (\pi \text{ は準同型写像だから}) \\ &= \overline{1} \qquad (\pi \text{ の核 } \mathrm{Ker}\,\pi = [G,G] \text{ だから}) \end{aligned}$$

これより、直ちに $\overline{g}\overline{h} = \overline{h}\overline{g}$ となり、任意の 2 つの要素の積が可換であるとわかる。よって $G/[G,G]$ はアーベル群。

最後に、正規部分群 $H \triangleleft G$ に対して G/H がアーベル群であるとする。この時、上と同様に自然全射準同型 $G \longrightarrow G/H,\ g \mapsto \overline{g}$ を考えると、任意の $g,h \in G$ に対して $\overline{g}\overline{h} = \overline{h}\overline{g}$、すなわち $[\overline{g},\overline{h}] = \overline{1}$. 従って、$[g,h] \subset H$ である。よって $[G,G] \subset H$ となる。 □

交換子群の構成を繰り返し適用することによって、高次交換子群が得られる。

定義 143 (高次交換子群)**.** 群 G に対して、i 次**交換子群** D^iG *(*$i = 0,1,\ldots$*)* を以下のように定義する：

$$D^0G := G, \quad D^{i+1}G = [D^iG, D^iG]$$

命題 144. 群 G が可解群であることの必要十分条件は、$D^nG = \{1\}$ となるような $n \in \mathbb{N}$ が存在することである。

Proof. G が可解群だとすると、

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\}$$

なる部分群の列で、$i = 0,1,\ldots,n-1$ に対して、$G_{i+1} \triangleleft G_i$ かつ、G_i/G_{i+1} がアーベル群であるものが存在する。このとき、

$$D^iG \subset G_i \qquad (i = 0,\ldots,n) \tag{4}$$

であることが示せれば、特に $i = n$ とすれば $D^nG = \{1\}$ が従う。そこで (4) を $i \in \mathbb{N}$ に関する数学的帰納法で示そう。まず、$i = 0$ の場合は $D^0G = G \subset G$ だから $D^iG \subset G_i$ は成り立っている。また、$i < n$ なるある i に対して (4) が成り立っていたとすると、仮定より G_i/G_{i+1} がアーベル群だから、命題 142 より

$$\{1\} = [G_i/G_{i+1}, G_i/G_{i+1}] \ (= [G_i, G_i]/G_{i+1})$$

となるから、$[G_i, G_i] \subset G_{i+1}$ を得る。従って

$$D^{i+1}G := [D^iG, D^iG] \subset [G_i, G_i] \subset G_{i+1}$$

が成り立つ。よって帰納法により、全ての i について $D^iG \supset G_i$ であることが示せた。

逆に、適当な $n \in \mathbb{N}$ に対して $D^nG = \{1\}$ であると仮定して、G が可解群であることを示そう。部分群の列

$$G = D^0G \supset D^1G \supset \cdots \supset D^nG = \{1\}$$

を考える。命題 142 より、これが G が可解群であることを示す部分群列になっている。よって G は可解群である。 □

可解群という性質が部分群や剰余群にどう反映するかを示すのが、以下の結果である。

命題 145. 群とその部分群 $H \subset G$ を考える。このとき、G が可解群ならば、H もまた可解群である。また、$H \triangleleft G$ のとき、G が可解であることと、H と G/H が可解であることは同値である。

Proof. 部分群 $H \subset G$ に対して、$D^iH \subset D^iG$ だから、命題 144 より G が可解ならば H も可解になることは、直ちにわかる。[26]

次に $H \triangleleft G$ であるとする。このとき、剰余群 G/N への自然全射準同型

$$\pi : G \longrightarrow G/H$$

を考える。今、H と G/H がともに可解群だと仮定すると、命題 144 より $D^kH = D^j(G/H) = \{1\}$ となるような $i, j \in \mathbb{N}$ が存在するが、一般に $D^mG = \{1\}$ ならば、$D^nG = \{1\}$ $(n \geq m)$ だから、$n = \max\{i, j\}$ として

$$D^nH = D^n(G/H) = \{1\}$$

[26] より直接的には以下のようにも示せる。G が可解群ならば、

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\}$$

なる部分群列が存在し、全ての i に対して $G_{i+1} \triangleleft G_i$ かつ G_i/G_{i+1} がアーベル群である。そこで部分群 $H \subset G$ との交わりをとると

$$H = H \cap G = H \cap G_0 \supset H \cap G_1 \supset \cdots \supset H \cap G_n = \{1\}$$

なる部分群列が作れるが、これが全ての i に対し、$H \cap G_{i+1} \triangleleft H \cap G_i$ かつ $H \cap G_i/H \cap G_{i+1}$ がアーベル群であればよい。これには、次のことを示せば十分である：N, K, H がある群の部分群だとする。このとき、

(1) $N \triangleleft K$ ならば、$H \cap N \triangleleft N \cap K$

(2) K/N がアーベル群なら、$(H \cap K)/(H \cap N)$ もアーベル群である。

しかし、これは容易に証明できる。

と考えてよい。すると

Claim: $\pi(D^nG) = D^n(G/H) = \{1\}$

Claim の証明. D^nG の生成元は $[a,b]$, $(a,b \in D^{n-1}(G))$ の形である。すると π による像は

$$\begin{aligned}\pi([a,b]) &= \pi(aba^{-1}b^{-1}) \\ &= \pi(a)\pi(b)\pi(a)^{-1}\pi(b)^{-1} = [\pi(a),\pi(b)] \\ &\in [D^{n-1}(G)/H, D^{n-1}(G)/H] = [D^{n-1}(G/H), D^{n-1}(G/H)] \\ &= D^n(G/H).\end{aligned}$$

となり、これは上の結果により $= \{1\}$. □

従って、$D^nG \subset \operatorname{Ker}\pi = H$. これを使ってさらに交換子をつくると $D^n(D^nG) \subset D^nH = \{1\}$ となり、$D^n(D^nG) = D^{2n}G$ である。よって

$$D^{2n}G = \{1\}$$

とわかり、命題 144 より、G は可解である。 □

10.4. **定理 135 の証明.** まず、証明の鍵となる次の補題を示す。

補題 146. L/K を有限次拡大とし、F/K を任意の拡大とする。$\overline{F}$ の中に適当な K 準同型をつかって L を埋め込んでおく、このとき、L/K が可解ならば、FL/F も可解である。

ここで FL は F に L の元すべてを付け加えてえられる拡大体を表す。$FL = F(L) = L(F)$ と書いてもよい。

Proof. L/K が可解とする。このとき L を拡大して L/K が有限時 Galois 拡大と思ってよい。ここで $L = K(a_1,\ldots,a_n)$ の形で書けるから、$F \supset K$ に注意すれば $FL = F(a_1,\ldots,a_n)$ となり、これは F の有限次 Galois 拡大になる。そこで任意の $\sigma \in \mathrm{Gal}\,(FL/F)$ を考えると、これ F の元を固定するから勿論 $K(\subset F)$ の元も固定する。よって $\sigma|_L \in \mathrm{Hom}_K(L,\overline{K})$ となるが、L/K は正規拡大だから、$\sigma|_L \in \mathrm{Aut}_K(L) = \mathrm{Gal}\,(L/K)$ となる。すなわち制限写像

$$\mathrm{Gal}\,(FL/F) \longrightarrow \mathrm{Gal}\,(L/K)$$

が得られるが、これは単射である。なぜなら、$\sigma \in \mathrm{Gal}\,(FL/F)$ に対して $\sigma|_L = 1$ だとすると、$\sigma|_L$ は L の元を全て固定する。また σ は元々 F の元を全て固定したのだから、結局 σ は FL の元全てを固定する。すなわち $\sigma = 1$ となるからである。よって $\mathrm{Gal}\,(FL/F) \subset \mathrm{Gal}\,(L/K)$ となるが、$\mathrm{Gal}\,(L/K)$ は可解群だから、命題 145 より $\mathrm{Gal}\,(FL/F)$ も可解群となる。 □

以下の結果は、可解拡大やべき根による拡大を繰り返せば、再び可解拡大やべき根による拡大が得られることを主張する。

補題 147. 拡大体 $K \subset L \subset M$ において、L/K, M/L がいずれもべき根による有限次拡大 *(or* 可解拡大*)* ならば、M/K もべき根による有限次拡大 *(or* 可解拡大*)* である。

Proof. べき根による有限次拡大の場合は定義より明らかであり、例 132 の考察でも既に使っていることに注意する。そこで以下では可解拡大の場合を示す。L/K, M/L がいずれも可解拡大の場合、まず、

Claim 1: L/K, M/L がいずれも Galois 拡大だと仮定してもよい

Claim 1 の証明. L/K が可解拡大だから、定義により、L の有限次拡大体 L' で L'/K が可解な Galois 拡大になるものが存在する。すると、M/L が可解拡大であることから、補題 146 より ML'/L' も可解である。従って ML' の $\overline{M}$ における有限次拡大 M'/ML' で M'/L' が可解な Galois 拡大になっているものがとれる。このとき、M'/K が可解であることが示せれば、M/K の可解性がわかる。L' にとりかえて、最初から M/L, L/K が Galois 可解拡大であると思ってよい。 □

さて、系 80 より M/K は分離的である。しかし正規とは限らないので、正規閉包 M' をとる。それは

$$M' := \prod_{\sigma \in \mathrm{Hom}_K(M, \overline{M})} \sigma(M)$$

として得られる[27]。ここで M/K は有限拡大なので、M'/K も有限拡大である（命題 65)。$\mathrm{char}(K) = 0$ なので、M'/K は分離的。従って M'/K は有限次 Galois 拡大になる。いま L/K は Galois 拡大と仮定していたので、$\sigma(L) = L, \forall \sigma \in \mathrm{Hom}_K(M, \overline{M})$. よって $\sigma(M)/L$ は M/L と同型な Galois 拡大である。そこで

Claim 2: $\mathrm{Gal}\,(M'/K)$ は可解である

が言えれば、M/K の可解性が言えたことになる。

Claim 2 の証明. 次のような完全列を考える：

$$0 \longrightarrow \mathrm{Gal}\,(M'/L) \longrightarrow \mathrm{Gal}\,(M'/K) \xrightarrow{\varphi} \mathrm{Gal}\,(L/K) \longrightarrow 0$$

ここで φ は制限写像である。仮定より $\mathrm{Gal}\,(L/K)$ は可解。さらに $\mathrm{Gal}\,(M'/L)$ も可解であることが言えれば、命題 145 より $\mathrm{Gal}\,(M'/K)$ も可解とわかる。ところが $M' = \prod_\sigma \sigma(M)$ だったから、制限写像 $\mathrm{Gal}\,(M'/L) \ni \xi \mapsto \xi|_{\sigma(M)} \ni \mathrm{Gal}\,(\sigma(M)/L)$ を使って

$$\mathrm{Gal}\,(M'/L) \xrightarrow{\Psi} \prod_{\sigma \in \mathrm{Hom}_K(M, \overline{M})} \mathrm{Gal}\,(\sigma(M)/L)$$

なる写像を考える。$\mathrm{Gal}\,(\sigma(M)/L) \cong \mathrm{Gal}\,(\sigma(M)/\sigma(L)) \cong \mathrm{Gal}\,(M/L)$ は可解ゆえ、その直積である $\prod_\sigma \mathrm{Gal}\,(\sigma(M)/L)$ もまた可解。そこで、もし Ψ が単射であ

[27]ただし、ここで $\prod_i K_i$, (ただし K_i は体)、は、直積ではなく、体の合成 $K_1 \cdot K_2 \cdots$ の意味である。$\{K_i\}$ が 2 つの要素だけの場合は $K_1 \times K_2 = K_1 \cdot K_2 = K_1(K_2)$ のことである。

ることが示せれば、可解群の部分群ということで $\mathrm{Gal}\,(M'/L)$ も可解とわかる（命題 145）。実際、$\mathrm{Ker}\,\Psi$ は $\sigma(M)$ のいずれに制限しても自明な自己同型写像になる。従って $M' = \prod_\sigma \sigma(M)$ の上でも自明である。すなわち $\mathrm{Ker}\,\Psi$ は自明となり、Ψ は単射である。 □

□

さて、定理 135 の証明に移ろう。

- L/K が可解拡大なら L/K がべき根による拡大になる

  Proof. $[L : K]$ を因数分解したときに現れる素数をすべてかけ合わせたものを m とし、F を K に 1 の原始 m 乗根 ζ を付け加えた単純拡大とする: $F = K(\zeta)$. 勿論 F/K はべき根による拡大である、さらに

  $$K \subset F \subset FL := L(\zeta)$$

  という拡大の列もできる。ここでもし FL/F もべき根による拡大であることが示せれば、補題 147 により $L(\zeta)/K$ がべき根による拡大になり、従って L/K もべき根による拡大になる。そこで、FL/F がべき根による拡大であることを示そう。

  今、仮定より L/K が可解拡大だから、FL/F, すなわち $L(\zeta)/K(\zeta)$ もまた可解拡大である。実際、

  $$\begin{array}{ccccc} \varphi & \mathrm{Gal}\,(L(\zeta)/K(\zeta)) & \longrightarrow & \mathrm{Gal}\,(L/K) \\ & \sigma & \mapsto & \sigma|_L \end{array}$$

  なる制限写像を考えると、これは群の準同型であり、さらに単射でもある。実際、$\sigma|_L = \mathrm{id}$ であることは $\sigma(x) = x$ $(\forall x \in L)$ を意味し、さらに $\sigma \in \mathrm{Gal}\,(L(\zeta)/K(\zeta))$ だから $\sigma(\zeta) = \zeta$. 従って $\sigma(x) = x$ $(\forall x \in L(\zeta))$ となって、結局 $\sigma = \mathrm{id}$. 以上のことから、$\mathrm{Ker}\,\varphi = \{1\}$ となり、φ は単射である。すると、この単射により $\mathrm{Gal}\,(L(\zeta)/K(\zeta)) \subset \mathrm{Gal}\,(L/K)$ と考えることができ、$\mathrm{Gal}\,(L/K)$ は仮定より可解群だから、命題 145 より $\mathrm{Gal}\,(L(\zeta)/K(\zeta))$ も可解となる。

  そこで次のような部分群の列が存在する。

  $$\mathrm{Gal}\,(FL/F) = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\}$$

  $G_{i+1} \lhd G_i$, G_i/G_{i+1} はアーベル群 $(i = 0, \ldots, n-1)$. さらに、命題 139 より G_i/G_{i+1} は全て素数位数の巡回群と考えることができる。すると、Galois の基本定理 91 により、上の部分群列に対応する中間体の列

  $$F = F_0 \subset F_1 \subset \cdots \subset F_n = FL$$

  で、F_{i+1}/F_i $(i = 0, \ldots, n-1)$ が素数次の巡回拡大になっているものが存在する。そこで、$[F_{i+1} : F_i] = p_i$ とおく。命題 120 より、F_{i+1} は F_i に適当な $X^{p_i} - a \in F_i[X]$ $(a \in F_i)$ の根を付け加えたものである[28]。したがって、FL/F はべき根による拡大で、$L \subset LF$ だから L/K もまたべき根による拡大となる。 □

- L/K がべき根による拡大なら L/K が可解拡大になる

[28] ここで巡回拡大を作るために必要な 1 の原始 p_i 乗根は、最初に選んだ ζ のべきとして得られることに注意。

Proof. L/K がべき根による拡大だとすると、拡大体の列

$$K = K_0 \subset K_1 \subset \cdots \subset K_n$$

で、$L \subset K_n$, かつ、$i = 0, \ldots, n-1$ に対して $K_{i+1} = K_i(a_i)$, ただし、a_i は $X^{n_i} - c_i \in K_i[X]$ なる形の式の零点 ($a_i = 1$ の場合、つまり 1 の原始根の場合も含む）なるものが存在する。可解拡大の定義から、$K_n = L$ と仮定して証明しても差し支えない。また、各 K_{i+1}/K_i が可解であることが示せれば、補題 147 により K_n/K も可解とわかるから、結局、次のことを証明すれば十分である：

主張：「$L = K(a)$, $a \in L$ は $X^n - c \in K[X]$ の零点、とする。このとき L/K は可解拡大である」

$c = 1$ の場合、すなわち円分拡大の場合、命題 99 により L/K は Galois 拡大で Galois 群 Gal (L/K) はアーベル群、したがって可解群だから、L/K は可解拡大とわかる。そこで以下では $c \neq 1$ の場合を考える。K が 1 の原始 n 乗根を含んでいれば、命題 120 により L/K は巡回拡大になり、従って L/K は可解拡大になる。もし K が 1 の原始 n 乗根 ζ を含んでいなければ、それを K に添加した拡大体 $F = K(\zeta)/K$ をつくり、拡大体の列

$$K \subset F = K(\zeta) \subset FL = F(a)$$

を考える。このとき、FL/F は命題 120 により巡回拡大。また、F/K は命題 99 によりアーベル群を Galois 群に持つ Galois 拡大である。すなわち、いずれも可解拡大であり、従って FL/K は可解拡大、特に L/K も可解となる。
□

この資料を作成するにあたっては、以下の書籍を参考にした。

References

[1] S. Bosch, *Algebra, 4.Auflage*, Springer, 2001

Yukihide Takayama, Department of Mathematical Sciences, Ritsumeikan University, 1-1-1 Nojihigashi, Kusatsu, Shiga 525-8577, Japan
E-mail address: takayama@se.ritsumei.ac.jp