代　数　学　5 及び 6

2018 年度版

はじめに

「代数学 5」と「代数学 6」では Galois 理論を学ぶ. Abel や Galois 達によつて証明された 5 次以上の一般代数方程式には代数的な解の公式が存在しないといふ定理は Galois 理論を生み出す動機であつたが, Galois 理論自体はそれだけを目的にしたものではなく, もつと広い内容を持つてゐる. それを汲み取つていただくために, 「代数学 5」と「代数学 6」を学ぶに際しては,

(1) 体にはどの様なものがあるのか, また,

(2) 体から体への準同型[1] にはどの様なものがあるか

の 2 つを常に問題意識として持つておいていただきたい. これら講義の目標はこの問題に対する答を理解し, 多くの体を（別個にではなくて）自己同型写像のなす群を使つて統一的に捉へる感覚を養ふことに尽きる.

数学の書物を眺めてゐると, 数学を学ぶのには定義, 定理, 証明の連鎖を緻密に追跡し, そのあとで例を作つてみる, のが普通の様に思はれるであらう. しかし, 先に, 良い例に接したあとに, その例のどこが理論化されたのかを肉付けしていくといふ方向が最も学び易いのではないかと思ふ. そこで, できるだけ例に接しられる様な問題を入れておいた. また, 第 4 節で述べるいくつかの例が, この講義で述べる理論の流れを掴むのに有用であらうと信じる.

さらに, Android の Smart-phone をお持ちであれば, 是非 `paridroid` を install していただき, いろいろな例の計算を試して欲しい. iPhone をお持ちの場合は `SageMath` である程度代用できる.

この講義 note は, 主に [N] の第 4 章 体論 によつて構成されてをり, 節末問題やところどころの詳細な議論で [Iy] を参考にしてゐる. また, 第 1 節から 10 節が「代数学 5」の範囲で, 第 11 節以降が「代数学 6」の範囲である.

この講義 note の作成にあたり, 2017 年度の名城大学理工学部数学科の受講生には, 多くの誤りをご指摘していただいた. そのお陰で, かなり完成度の高いものになつたと思ふ. ここに深く感謝申し上げる次第である.

最後に方程式の可解性に関しての定式化について, 一言だけ触れておきたい. 第 16 節で学ぶ, 冪根による拡大については, [Iy] の定義を採用した. この定義は [N] のそれより精密であるが, 持ち上げや合成に関して保たれないため, 関連する種々の性質を導くのに手間が掛かる. しかし, [Iy] の定義を採用してゐる書物は少ないから, その事を解説する講義も恐らく少ないと思はれる. それゆゑ, 名城大学の数学科の講義で, きちんと取り上げておく意味はあるだらうと判断し採用した.

文 献

[N] 永尾 汎 著 : 代数学 (新数学講座 4), 1983, 朝倉書店

[Iy] 彌永 昌吉, 有馬 哲, 浅茅 陽 著 : 詳解 代数入門, 1990, 東京図書

[1] それは必然的に単射.

目 次

1. 環と体の概念, 環の準同型

はじめに, 環と体の概念を思ひ出しておく. 集合 R について, 加法と呼ばれる演算 $R\times R\to R$, $(a,b)\mapsto a+b$, 及び乗法と呼ばれる演算 $(a,b)\mapsto ab$ が与へられてゐて, 次の 4 つの条件がすべて満されるとき, R を 環 と呼ぶのであつた. 但し, a, b, c は R の任意の元である.

R1. R は加法に関して可換群である. (単位元は通常 0 で表す)

R2. 乗法の結合法則 : $(ab)c=a(bc)$.

R3. 左右の分配法則 : $a(b+c)=ab+ac,\ \ (b+c)a=ba+ca$.

R4. 乗法に関する単位元の存在 : 加法の単位元 0 とは異なるある元 $1\in R$ が存在して, R の任意の元 x に対して $1x=x1=x$ が満たされる.

環 R がさらに, 次の条件も満たすとき R は 可換環 と呼ばれるのであつた.

R5. 乗法の交換法則 : $ab=ba$

定義 1.1. 環は, その 0 以外のどの元も乗法に関する逆元を持つとき 斜体 といはれる. 可換環は, 零因子を持たないとき 整域 と呼ばれ, さらにそれが斜体のとき, 体 と呼ばれる. 従つて, 体は整域でもある.

定義 1.2. 環 R から環 T への写像 $\varphi : R\to T$ が 2 つの条件

H1. $\varphi(a+b)=\varphi(a)+\varphi(b)$

H2. $\varphi(ab)=\varphi(a)\varphi(b)$

を満たすとき φ は 環準同型 といはれる. 但し, a, b, c は R の任意の元である. **H2** より $\varphi(1)^2-\varphi(1)=0$ ($1=1_T$ は T の乗法に関する単位元)) ゆゑ, $\varphi(1)=1$ または 0 である.

定義 1.3. 可換環 R の空でない部分集合 $I\subset R$ は 2 つの条件

I1. $a\in I$, $b\in I$ ならば $a+b\in I$,

I2. $a\in I$, $x\in R$ ならば $xa\in I$

を共に満たすとき, R の ideal と呼ばれる. R の ideal P が,

P. 任意の a, $b\in R$ に対し, $ab\in P\iff a\in P$ または $b\in P$

を満たすとき P は 素 ideal といはれる. また, R の ideal M を含む R の ideal が M に限るとき, M は 極大 ideal であるといはれる.

問 1.4. 環準同型 $\varphi : R\to T$ の核 $\mathrm{Ker}(\varphi)=\{a\in R\,|\,\varphi(a)=0\}$ は R の ideal であることを示せ.

可換環 R と ideal I について, 加法に関する剰余類 R/I は自然な演算で, 可換環になることも既に学んだ. さらに

命題 1.5. 可換環 R の ideal I が素 ideal であるためには剰余環 R/I が整域であることが必要十分であり, I が極大 ideal であるためには剰余環 R/I が体であることが必要十分である.

証明 後半の証明. $a\in R$ に対し, a の属する R/I の類 $a+I$ を $\overline{a}$ と書くことにする.

$$\begin{aligned}\overline{a}\neq\overline{0} &\iff a\notin I \iff aR+I=R\ \ (\because I \text{ は極大 ideal だから})\\ &\iff af+g=1 \text{ となる } f\in R,\, g\in I \text{ が存在} \iff \overline{a}\,\overline{f}=\overline{1}\\ &\iff \overline{a} \text{ は乗法に関して逆元を持つ}\end{aligned}$$

となるからである. 前半は問 1.6 とする. □

問 1.6. 命題 1.5 の前半を証明せよ.

2. 部分体, 体の拡大

前節で定義した様に, この note 全体を通じて, 特に断らない限り 体の乗法は可換とする. もし, 非可換体に言及する場合は 非可換体 と明記し, 可換か非可換かが不明なときは 斜体 と呼び, 区別する. (環の場合も同様で, 単に環と呼ぶのは非可換の場合も含めてゐる)

体 L の部分集合 K が L の演算で体になつてゐるとき, K を L の 部分体 といふ. このとき, L の 0 と 1 は K の加法と乗法の単位元でもある.

問 2.1. K_1, K_2 を L の 2 つの部分体とすると, $K_1 \cap K_2$ も体である.

問 2.2. 体 L の部分体 M_1 と M_2 を共に含む L の最小の部分体が存在する. 一般に L の部分集合 S を含む最小の部分体が存在する. (Hint : 2.1 を使ふ.)

定義 2.3. K が L の部分体である場合 $L \supset K$ と表す. この関係を K から見たとき L を K の 拡大体 と呼ぶ. $L \supset M \supset K$ を満たす体 M を L と K の (あるいは拡大 L/K の) 中間体 といふ. 体 L が体 K の拡大体であることを, 以後簡単に拡大 L/K と称す. このとき, L は K 上の vector 空間[2] とみなせるが, その次元 $\dim_K L$ を L/K の拡大次数と呼び $[L : K]$ で表す. 特に体の拡大 L/K において, その拡大次数 $[L : K] < \infty$ であるとき, L/K は 有限次拡大 であるといはれる. $[L : K] = 1$, つまり $L = K$ のとき, L/K を 自明な拡大 といふ.

定義 2.4. $\alpha_i \in L$ $(i = 1, 2, 3, \cdots)$ とするとき, $\{\alpha_i \,|\, i = 1, 2, 3, \cdots\}$ を含む最小な体を $\{\alpha_i \,|\, i = 1, 2, \cdots\}$ で 生成された体 といふ. K を L の部分体とし, K のすべての元および $\{\alpha_i\}$ で生成された体を $K(\alpha_1, \alpha_2, \cdots)$ で表し, K に $\alpha_1, \alpha_2, \cdots$ を 添加 して得られる体と呼ぶ. 特に $L = K(\alpha_1, \alpha_2, \cdots, \alpha_n)$ の場合, L を K 上 有限生成 な体といふ. 同様に, K のすべての元および $\{\alpha_1, \cdots, \alpha_n\}$ を含む最小の環が存在する. これを K と $\{\alpha_1, \cdots, \alpha_n\}$ で生成された環と呼び, $K[\alpha_1, \alpha_2, \cdots, \alpha_n]$ で表す.

問 2.5. 元 α が K 上の既約多項式の根であるとき, $K(\alpha) = K[\alpha]$ となる.

一般には $K(\alpha) \supset K[\alpha]$ であり, 一致するとは限らない. また 1 つの元 α によつて $L = K(\alpha)$ となるとき, L を K の 単純拡大 (単拡大) といふ.

演 習 問 題

2.6. $\mathbb{R}(\sqrt{2}) = \mathbb{R}$, $\mathbb{R}(i) = \mathbb{C}$ であることを示せ.

2.7. $\mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(\sqrt{3}) = \mathbb{Q}$ であることを示せ.

2.8. $K(\alpha) \supsetneqq K[\alpha]$ となる例を 1 つ挙げよ.

2.9. 次の体の間の包含関係を理由を付して明示せよ. 但し i は虚数単位で $i^2 = -1$.
(1) $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{6})$, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.
(2) $\mathbb{Q}$, $\mathbb{Q}(\sqrt{3}\, i)$, $\mathbb{Q}(\frac{-1+\sqrt{3}i}{2})$, $\mathbb{Q}(\sqrt{3}, i)$.

2.10. $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\alpha)$ となる α を 1 つ求めよ.

[2] 線形代数学で学んだ理論は, 一般の体上で同様に展開できる.

3. 標 数

定義 3.1. K のいかなる部分体も単位元 1 で生成される体を含む. この体は構造の最も簡単な体である. これらと 同型[3] な体を 素体 といふ.

ここで, 素体の構造を見てみる. 1 を m 回加へて $m1 = 0$ となつたとし, m はその様な最小の正整数とする. このとき m は素数であり, さもなくば, 任意の整数 $m \neq 0$ について $m1 \neq 0$ である. 実際, その様な m が素数でないとする. $m = m_1 m_2$ と因数分解すれば, $m_1 1 \cdot m_2 1 = m1 = 0$ より $m_1 1 = 0$ または $m_2 1 = 0$ となつて m の最小性に矛盾する. ゆゑに m は素数である. この様に, 素数 p について $p1 = 0$ となる場合, 体 K の 標数 は p であるといひ, $m1 = 0 \implies m = 0$ となる場合, 体 K の 標数 は 0 であるといふ. 一般に, 体 K の標数を $\operatorname{char} K$ と書く. 標数 p の素体は p 元体 $\mathbb{Z}/p\mathbb{Z}$ と同型である. また標数 0 の素体は 整域[4] $\{m1 | m \in \mathbb{Z}\}$ の 商体[5] に他ならず, それは有理数体 $\mathbb{Q}$ と同型である. どんな体も素体を含むから, 任意の体 K に対し K の部分体の共通部分が K に含まれる唯一の素体に他ならない. 以上を次の定理にまとめておく.

定理 3.2. (1) どんな素体も, 有理数体 $\mathbb{Q}$ または p 元体 $\mathbb{Z}/p\mathbb{Z}$ (p は素数) に同型である.
(2) 任意の体は素体を唯一つ含む.
(3) 標数 $p > 0$ の体は素体 $\mathbb{Z}/p\mathbb{Z}$ を含み, 標数 0 の体は素体 $\mathbb{Q}$ を含む.

問 3.3. K を体とし $\operatorname{char} K = p > 0$ とする. $a, b \in K$ について次を示せ.
(1) $pa = 0$.
(2) $n \in \mathbb{Z}$ に対し, $a \neq 0$ かつ $na = 0 \implies p | n$.
(3) N を非負整数とするとき $(a+b)^{p^N} = a^{p^N} + b^{p^N}$.
(4) N を非負整数とするとき $a_1, \cdots, a_t \in K$ について $\left(\sum_{i=1}^{t} a_i \right)^{p^N} = \sum_{i=1}^{t} {a_i}^{p^N}$.

演 習 問 題

3.4. 3 元体 $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$ 上の次の多項式は既約であることを示せ.
(1) $x^2 + 1$ (2) $x^4 + x + 2$

3.5. 剰余環 $\mathbb{F}_3[x]/(x^2+1)$ は体であることを示せ. また, これは素体ではないことを示せ.

3.6. 標数 5 の素体でない体の例を 1 つ挙げよ.

---

[3] この体からの全単射な環準同型の像となり得る体のこと.
[4] 零因子を持たない可換環のこと.
[5] その整域を含む最小の体のこと. 一般に整域 R の商体の厳密な定義は以下の通り. 記号 $\frac{a}{b}$ ($a \in R$, $0 \neq b \in R$) の全体 S に関係 $\frac{a}{b} \sim \frac{a'}{b'}$ を $ab' - a'b = 0$ で定めるとこれは同値関係になり, これによる分類で得られる集合 $S/\sim$ は和 $\frac{a}{b} + \frac{a'}{b'} = \frac{ab'+a'b}{bb'}$, 積 $\frac{a}{b}\frac{a'}{b'} = \frac{aa'}{bb'}$ に関して体をなし, $\frac{a}{1}$ と $a \in R$ を同一視することで R は $S/\sim$ の部分環になる. $S/\sim$ を R の 商体 と呼ぶ

4. いくつかの例

理論を展開する前に, 感覚を整へるための例を述べるが, その前に最低限の準備をする.

命題 4.1. 体 K から別の体 L への $1 \mapsto 1$ なる準同型は単射である.

証明 この準同型の核を考へる (1.4 参照). 体の ideal は $\{0\}$ であるか, さもなくばその体全体であるから, この準同型の核は $\{0\}$ でなければならない. □

命題 4.2. 体の有限次拡大 L/K があり, 環の準同型 $\varphi : L \to L$ で, どの $a \in K$ についても $\varphi(a) = a$ となるものは, 4.1 により必然的に同型である. これを L の K 上の自己同型と呼ぶ（第 9 節を参照）.

証明 φ は 4.1 により必然的に単射であるが, L は K 上の有限次元 vector 空間なので, 線形代数学で学んだ様に, それは全射でもある. □

$L = K(\alpha)$ のとき, L の K 上の自己同型 φ は α の写る元 $\varphi(\alpha)$ だけで定まる. 例へば a, $b \in K$ のとき $\varphi(a + b\alpha) = \varphi(a) + \varphi(b)\varphi(\alpha) = a + b\varphi(\alpha)$, $\varphi(\alpha^2) = \varphi(\alpha)^2$ 等となるし, 一般に, 任意の $K(\alpha)$ の元は K の元を係数とする α の 多項式で表され, それを $f(\alpha)$ と書けば

$$\varphi\big(f(\alpha)\big) = f\big(\varphi(\alpha)\big)$$

であるからである. 以降でこの様な自己同型の, いくつかの例を述べる.

例 4.3. 拡大 $\mathbb{C}/\mathbb{R}$ に関して, $\mathbb{C}$ の $\mathbb{R}$ 上の自己同型, 即ち,
環準同型 $\varphi : \mathbb{C} \to \mathbb{C}$ で $\varphi|_{\mathbb{R}}$ が恒等写像であるものをすべて求めてみる. $-1 = \varphi(-1) = \varphi(i^2) = \varphi(i)^2$ であるから, $\varphi(i) = \pm i$, $\varphi(a + bi) = a \pm bi$.

例 4.4. $\mathbb{Q}(i)/\mathbb{Q}$. $\varphi : \mathbb{Q}(i) \to \mathbb{C}$ を環準同型で $1 \mapsto 1$ なるものとせよ. このとき $\varphi(n) = \varphi(1+1+\cdots+1) = n\varphi(1) = n$ で, $0 = \varphi(0) = \varphi(1+(-1)) = 1+\varphi(-1)$ より, $\varphi(-1) = -1$. このとき $\varphi(i)^2 = \varphi(-1) = -1$ より $\varphi(i) = \pm i$.

例 4.5. $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. これも $\varphi(\sqrt{2})^2 = 2$ であるから $\varphi(a + b\sqrt{2}) = a \pm b\sqrt{2}$ の 2 つだけ.

例 4.6. $\mathbb{Q}(\sqrt[3]{2}, \omega) \,/\, \mathbb{Q}$, 但し $\omega = \frac{-1+\sqrt{-3}}{2}$.
$\varphi\big((\sqrt[3]{2})\big)^3 = \big(\varphi(\sqrt[3]{2})^3\big) = \varphi(2) = 2$ であるから, $\varphi(\sqrt[3]{2})$ は $x^3 = 2$ の解である. 同様に $\varphi(\omega)$ は $x^2 + x + 1 = 0$ の解である. よつて

(1) $\varphi(\sqrt[3]{2}\,) = \sqrt[3]{2}$, $\varphi(\omega) = \omega$
(2) $\varphi(\sqrt[3]{2}\,) = \sqrt[3]{2}$, $\varphi(\omega) = \omega^2$
(3) $\varphi(\sqrt[3]{2}\,) = \sqrt[3]{2}\,\omega$, $\varphi(\omega) = \omega$
(4) $\varphi(\sqrt[3]{2}\,) = \sqrt[3]{2}\,\omega$, $\varphi(\omega) = \omega^2$
(5) $\varphi(\sqrt[3]{2}\,) = \sqrt[3]{2}\,\omega^2$, $\varphi(\omega) = \omega$
(6) $\varphi(\sqrt[3]{2}\,) = \sqrt[3]{2}\,\omega^2$, $\varphi(\omega) = \omega^2$

の 6 通りに限られるが, これらすべてが実際に自己同型になつてゐることが確かめられる (最終的には 12.14 (4) で示される). ここで $[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = 6$ であることに注意せよ.

例 4.7. $\mathbb{Q}(\sqrt[3]{2}\,)/\mathbb{Q}$.
上の 4.6 から, 自己同型は恒等写像以外には有り得ない. ここで $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ であることに注意せよ.

例 4.8. いま $\alpha = \sqrt{6+3\sqrt{2}+2\sqrt{3}+2\sqrt{6}}$ とおき (根号内は正), 体

$$K = \mathbb{Q}(\alpha)$$

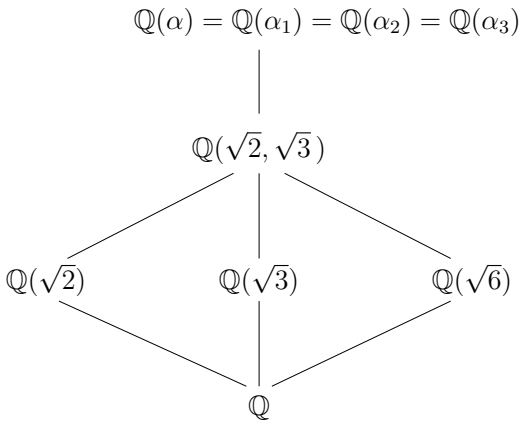
を考へる. これは有理数体 $\mathbb{Q}$ と α を含む $\mathbb{C}$ の部分体のうち最小なもののことである. つまり, α と任意の有理数について, 可能な限りの四則演算を行なひ得られた元を集めたものである. K の要素をいくつか挙げてみる. 例へば

$$K \ni \alpha^2 = 6+3\sqrt{2}+2\sqrt{3}+2\sqrt{6}$$

であるし, $\beta = \alpha^2 - 6$ とおくとき,

$$\begin{aligned}
\frac{\beta^2-54}{12} &= 2\sqrt{2}+2\sqrt{3}+\sqrt{6} \in K,\\
\gamma = \beta - \frac{\beta^2-54}{12} &= \sqrt{2}+\sqrt{6} \in K,\\
\left(\beta - \frac{\beta^2-54}{12}\right)^2 &= 8+4\sqrt{3} \in K,\\
\frac{(\beta - \frac{\beta^2-54}{12})^2 - 8}{4} &= \sqrt{3} \in K,\\
\frac{\gamma(\sqrt{3}-1)}{2} &= \sqrt{2} \in K.
\end{aligned}$$

以上から $K \supset \mathbb{Q}(\sqrt{2},\sqrt{3})$ がわかる. ここで $\mathbb{Q}(\sqrt{2},\sqrt{3})$ は $\sqrt{2}$ と $\sqrt{3}$ を含む最小の ($\mathbb{C}$ の) 部分体である. 体 K, $\mathbb{Q}(\sqrt{2},\sqrt{3})$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}$ の間には次の図の様な包含関係がある. 図においては, 線分で結ばれた体について,
より上の方にある体ががより下の体を含む.



いま,

$$\begin{aligned}
\alpha_0 &= \alpha,\\
\alpha_1 &= \sqrt{6-3\sqrt{2}+2\sqrt{3}-2\sqrt{6}},\\
\alpha_2 &= \sqrt{6+3\sqrt{2}-2\sqrt{3}-2\sqrt{6}},\\
\alpha_3 &= \sqrt{6-3\sqrt{2}-2\sqrt{3}+2\sqrt{6}}
\end{aligned}$$

とおくとき (これらすべての根号内は正),
8 つの写像

$$\begin{aligned}
\sigma_i^{\pm} : K &\longrightarrow K\\
f(\alpha) &\longmapsto f(\pm\alpha_i)
\end{aligned}$$

はどれも自己同型である. ここに $f(x)$ は x の有理数係数の任意の有理式を表す. $\pm\alpha_i$ はどれも α の有理式で表はされる. 実際, $\alpha\,\alpha_1 = \sqrt{6}$, $\alpha\,\alpha_2 = (1+\sqrt{2})\sqrt{6}$, $\alpha\,\alpha_3 = 3\sqrt{2}+2\sqrt{3}$ であるが, $\sqrt{2}$, $\sqrt{3}$, $\sqrt{6}$ は α の有理式であるからである.

問 4.9. 上の記号の下で, $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha_1) = \mathbb{Q}(\alpha_2) = \mathbb{Q}(\alpha_3)$ であることを示せ.

問 4.10. 上の $\{\,\pm\alpha_i \,|\, i = 0,\cdots,3\,\}$ は方程式 $f(x) = x^8 - 24x^6 + 108x^4 - 144x^2 + 36 = 0$ の根であることを示せ. また, 拡大次数 $[\,\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2},\sqrt{3}\,)\,] = 2$ を証明せよ.

(Hint : `paridroid` を使ひ $f(x)$ を調べよ. 但し, 最後は手でできる証明に落し込むこと.)

例 4.11. 2 つ目の例は有限体についてのもの. $\mathbb{Z}/5\mathbb{Z}$ を $\mathbb{F}_5$ と略記する. いま $\alpha^3+\alpha+1=0$ なる α を考へる. この式を満たす数 α は $\mathbb{F}_5$ の中には存在しない（確かめよ）からこの α を新しい数として, α の $\mathbb{F}_5$ 上の多項式の全体

$$\mathbb{F}_5[\alpha]=\{\,a+b\,\alpha+c\,\alpha^2\,|\,a,\ b,\ c\in\mathbb{F}_5\,\}$$

を考察する[6) 7)]. これは, 自然に除法も備へてゐて, 有理式の全体 $\mathbb{F}_5(\alpha)$ と一致する, つまり

$$\mathbb{F}_5[\alpha]=\mathbb{F}_5(\alpha)$$

であることが次の様にしてわかる. 例へば

$$\begin{aligned}\frac{2+3\alpha}{1+2\alpha+3\alpha^2}&=\frac{(2+3\alpha)(1+2\alpha^5+3\alpha^{10})(1+2\alpha^{25}+3\alpha^{50})}{(1+2\alpha+3\alpha^2)(1+2\alpha^5+3\alpha^{10})(1+2\alpha^{25}+3\alpha^{50})}\\&=\frac{2\alpha^2+3}{2}=\alpha^2+4.\end{aligned}$$

ここで $a+bi$ の共役は $a-bi$（の 1 つだけ）である様に, $1+2\alpha+3\alpha^2$ の共役[8)] が $1+2\alpha^5+3\alpha^{10}$ と $1+2\alpha^{25}+3\alpha^{50}$ である. これは, $\mathbb{F}_5(\alpha)$ の自己同型

$$\mathbb{F}_5(\alpha)\longrightarrow\mathbb{F}_5(\alpha)$$

は 3 つあつて, それぞれ,

$$\alpha\longmapsto\alpha,\quad\alpha\longmapsto\alpha^5,\quad\alpha\longmapsto\alpha^{25}$$

から定まり, これ以外にはないからである.

上の計算は次の様にしてもできる. x^3+x+1 と $1+2x+3x^2$ に対して $\mathbb{F}_5$ 上の多項式の互除法を行ふと, $4(x^3+x+1)+(2x+2)(1+2x+3x^2)=1$ が得られる. ゆゑに $(2\alpha+2)(1+2\alpha+3\alpha^2)=1$ であり,

$$\frac{2+3\alpha}{1+2\alpha+3\alpha^2}=(2+3\alpha)(2\alpha+2)=6\alpha^2+10\alpha+4=\alpha^2+4.$$

注意 4.12. 以上, 様々な例を見てきたが, どの例についても自己同型全体が写像の合成を演算として, 群をなす ことが見て取れる[9)]. このことを銘記しておいて欲しい.

演 習 問 題

4.13. 上の最後の互除法による計算の細部を再現せよ.

4.14. 本文で取り上げた体 $\mathbb{F}_5(\alpha)$ について $\alpha\mapsto\alpha^5$ により定まる写像は自己同型であり, 各 $f(\alpha)\in\mathbb{F}_5(\alpha)$ を $f(\alpha)^5$ に写す写像であることを示せ.

4.15. `paridroid` で次の様な入力を試してみよ. 何がわかるか.

```
? a=Mod(a,a^3+a+1)
? Mod(a^125,5)
```

---

6) ここで, 高校で虚数単位を導入したときを思ひ出して欲しい. 「$i^2=-1$ となる数 i は実数の中には存在しない. そこでこの様な性質をもつ 新しい数 を考へて, $a+bi$ $(a,\,b\in\mathbb{R})$ なる形の数の全体を複素数と呼ぶ. 複素数についての四則演算は $i^2=-1$ 以外は極く自然に定義する」の様に導入される. ただ, その様な「新しい数」といふのが何なのかが気に掛かる. 実際, 複素数を導入した Gauss は非常に慎重にそれを導入してゐる. しかし, ここでは高校でのやり方で α を導入する.

7) なぜ, $a+b\alpha$ $(a,\,b\in\mathbb{F}_5)$ の全体でないのか理解できるか.

8) 一般に代数的拡大 L/K と $\alpha\in L$ について, α と同じ既約多項式の根を α の共役であるといふ. 9.3 参照.

9) 次節の 5.4(2) で $\alpha^{125}=\alpha$ を示す.

5. 代数的拡大

定義 5.1. 拡大 L/K において $L \ni \alpha$ が K 上のある多項式 $f(x) \neq 0$ の根であるとき, α は K 上 代数的 であるといはれ, さうでないときは 超越的 であるといはれる. また L の任意の元が K 上代数的であるとき, L/K は 代数的拡大 であるといはれる. K の元は $x - a$ の根であるから, もちろん K 上代数的である.

問 5.2. M は L/K の中間体とする. M/K, L/M はともに有限次拡大とし, $\{\alpha_1, \cdots, \alpha_m\}$ を M の K 上の基底, $\{\beta_1, \cdots, \beta_l\}$ を L の M 上の基底とする. このとき $\{\alpha_i\beta_j \,|\, 1 \leq i \leq m,\ 1 \leq j \leq l\}$ は L の K 上の基底である. 特に L/K も有限次拡大であり,

$$[L : K] = [L : M][M : K] \tag{5.3}$$

が成り立つ. これらのことを示せ.

例 5.4. (1) $[\mathbb{Q}(\sqrt[3]{2}, i) : \mathbb{Q}(\sqrt[3]{2})] = 2$, $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, $[\mathbb{Q}(\sqrt[3]{2}, i) : \mathbb{Q}] = 6$.
(2) 有限体の有限次拡大について. 有限個の元からなる体を 有限体 と呼ぶ. K を $\operatorname{char} K = p$ なる有限体とする. ここで, $[K : \mathbb{F}_p] = n$ とすれば, $|K| = p^n$ である [10]. 「代数学 1」 (系 13.6) で学んだ様に, 0 以外の元のなす乗法群 $K^\times$ は位数 $p^n - 1$ の巡回群である. 従つて $0 \neq a \in K$ ならば $a^{p^n-1} = 1$ である. このことから K の任意の元は $a^{p^n} = a$ を満たす. 従つて $K/\mathbb{F}_p$ は代数的拡大である.

一般に, 拡大 L/K, $\alpha \in L$, および不定元 x について写像

$$\varphi : K[x] \longrightarrow L \quad f(x) \mapsto f(\alpha)$$

を考へる. これは 環準同型 である. また $\operatorname{Ker}\varphi \neq \{0\}$ のときは α は代数的であり, $\operatorname{Ker}\varphi = \{0\}$ のときは α は超越的である. このいづれの状況においても, 2.4 の記号を使へば

$$\begin{aligned} K[\alpha] &= \operatorname{Im}\varphi = \{f(\alpha) \,|\, f(x) \in K[x]\}, \\ K(\alpha) &= \{f(\alpha)/g(\alpha) \,|\, f(x),\ g(x) \in K[x],\ g(\alpha) \neq 0\} \end{aligned} \tag{5.5}$$

となる. $K(\alpha)$ は $K[\alpha]$ の商体 [11] である. $\operatorname{Im}\varphi = K[\alpha]$ は整域であるから (体の部分環), $\operatorname{Ker}\varphi$ は素 ideal であるが, $K[x]$ は単項 ideal 整域 [12] なので, (0) 以外の素 ideal は極大 ideal である. それゆゑ $\operatorname{Ker}\varphi = \{0\}$ または既約多項式 $p(x) \in K[x]$ によつて $\operatorname{Ker}\varphi = (p(x))$ (ideal の記法) となつてゐる. まとめると
(1) $\operatorname{Ker}\varphi = \{0\}$ のとき, $K[\alpha] \simeq K[x]$, $K(\alpha) \simeq K(x)$ である.[13]
(2) $\operatorname{Ker}\varphi = (p(x)) \neq \{0\}$ のとき, $K[\alpha] \simeq K[x]/(p(x))$ で, $(p(x))$ は極大 ideal である.

問 5.6. α を K 上代数的な元として, α を根とする K 上の最高次係数が 1 である多項式 [14] で既約なものを $p(x)$ とする. 次を示せ.
(1) $p(x)$ は一意的に定まる.
(2) $f(x) \in K[x]$, $f(\alpha) = 0 \implies p(x) | f(x)$.

---

[10] 基底 $\{v_1, \cdots, v_n\}$ を 1 つとれば, K の元は一意的に $a_1v_1 + \cdots + a_nv_n$ (a_1, $\cdots$, $a_n \in \mathbb{F}_p$) と書けるから.
[11] 整域 $K[\alpha]$ を含む最小の体のこと.
[12] すべての ideal が単項 ideal である様な整域の事.
[13] 記号 $\simeq$ は両者が環として同型であることを意味する.
[14] 最高次係数が 1 である多項式を monic と称す.

定義 5.7. 5.6 の多項式を $\mathrm{irr}\,(\alpha, K, x)$ で表し, α の K 上の 最小多項式 と呼ぶ.

定理 5.8. 拡大 L/K と $\alpha \in L$ について次が成り立つ.
(1) α が K 上代数的 $\iff$ $K(\alpha) = K[\alpha]$.
(2) α が K 上代数的で $\deg \mathrm{irr}\,(\alpha, K, x) = n$ $\iff$ $[K(\alpha) : K] = n$. さらに, この両辺が成立してゐるとき, $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ は $K(\alpha)$ の K 上の基底である.
(3) α が K 上代数的 $\iff$ $K(\alpha)/K$ は代数拡大.

証明 (1) の $(\Rightarrow)$ 任意の $f(x) \in K[x]$ について, $f(\alpha) \neq 0$ のとき $1/f(\alpha) \in K[\alpha]$ を示せばよい. $\mathrm{irr}\,(\alpha, K, x) = p(x)$ と書き, $\deg p(x) = n$ とせよ. $f(\alpha) \neq 0$ ならば, $p(x)$ の既約性により, $f(x)\,g(x) + h(x)\,p(x) = 1$, $g(x)$, $h(x) \in K[x]$ となる $g(x)$, $h(x)$ が存在する. このとき $f(\alpha)g(\alpha) = 1$ となる. (1) の $(\Leftarrow)$ $\alpha \in K$ なら明かなので $\alpha \notin K$ とする. このとき $1/\alpha = f(\alpha)$ $(f(x) \in K[x])$ と書かれるが, $\alpha\,f(\alpha) - 1 = 0$, $xf(x) - 1 \in K[x]$ であり α は代数的である.
(2) の $(\Rightarrow)$ もし $\{1, \alpha, \cdots, \alpha^{n-1}\}$ の間に K 上の線形関係が存在すれば α は $n-1$ 次以下の多項式の根となるから, 仮定に反する. 一方, 任意の多項式 $g(\alpha) \in K[\alpha]$ について, $g(x)$ の $\mathrm{irr}\,(\alpha, K, x)$ による剰余は $n-1$ 次式であるから, $g(\alpha)$ は $\{1, \alpha, \cdots, \alpha^{n-1}\}$ の 1 次結合で書ける. よつて, $\{1, \alpha, \cdots, \alpha^{n-1}\}$ は $K(\alpha)$ の K 上の基底をなし, $[K(\alpha) : K] = n$ である. (2) の $(\Leftarrow)$ $\{1, \alpha, \cdots, \alpha^{n-1}\}$ が $K(\alpha)$ の K 上の基底をなす. 実際, $n+1$ 個の集合 $\{1, \alpha, \cdots, \alpha^{n}\}$ は 1 次従属であるから, α は n 次以下の多項式の根である. その最小次数で monic な多項式が $\mathrm{irr}\,(\alpha, K, x)$ に他ならないし, 上と同じ議論で他の任意の $g(\alpha) \in K(\alpha)$ は $\{1, \alpha, \cdots, \alpha^{d-1}\}$ $(d = \deg \mathrm{irr}\,(\alpha, K, x))$ の K 上の 1 次結合で書けるからである. このとき $[K(\alpha) : K] = d$ となるから, $d = n$ でなければならない.
(3) の $(\Leftarrow)$ 明らか. (3) の $(\Rightarrow)$ α が K 上代数的で, $\deg \mathrm{irr}\,(\alpha, K, x) = n$ ならば, $[K(\alpha) : K] = n$ である. よつて, 任意の $\beta \in K(\alpha)$ について, 1, β, $\cdots$, β^n は K 上 1 次従属である. よつて β は K 上の多項式の根であつて代数的である. □

上の考察から容易に次の定理が得られる.

定理 5.9. $f(x) \in K[x]$, $\deg f(x) > 0$ とすれば, $f(x) = 0$ の根を少なくとも 1 つ含む K の拡大体が存在する.

証明 $p(x)$ を $f(x)$ の 1 つの既約因子とすれば, $L = K[x]/(p(x))$ は体である. $K \ni a$ とそれを含む剰余類 $a + (p(x))$ を同一視して $K \subset L$ と考へてよい. $\alpha = x + (p(x))$ とおけば $p(\alpha) = 0$, 従つて $f(\alpha) = 0$ である. □

例 5.10. 多項式 $x^3 - 2 \in \mathbb{Q}[x]$ は既約であり, 対応 $x + (x^3 - 2)\mathbb{Q}[x] \mapsto \sqrt[3]{2}$ により

$$\mathbb{Q}[x]/(x^3 - 2) \simeq \mathbb{Q}(\sqrt[3]{2}\,).$$

同様に $\mathbb{Q}(\sqrt[3]{2}\omega\,)$ と対応 $x + (x^3 - 2)\mathbb{Q}[x] \mapsto \sqrt[3]{2}\omega$ により

$$\mathbb{Q}[x]/(x^3 - 2) \simeq \mathbb{Q}(\sqrt[3]{2}\omega\,).$$

$\mathbb{Q}(\sqrt[3]{2}\omega^2\,)$ についても同じ. しかし, もちろん $\mathbb{Q}(\sqrt[3]{2}\,) \neq \mathbb{Q}(\sqrt[3]{2}\omega\,)$ 等である.

例題 5.11. 有限次拡大は代数的拡大である.

証明 L/K は有限次拡大とし, $[L:K]=n$ とせよ. このとき $\alpha\in L$ に対して, $n+1$ 個の元 $\{1,\alpha,\alpha^2,\cdots,\alpha^n\}$ は K 上 1 次従属である. このことは次数が高々 n の多項式 $f(x)$ があつて $f(\alpha)=0$ であることに他ならない. 従つて L の元はすべて K 上代数的である. □

K の拡大体 L の元 $\alpha_1,\cdots,\alpha_n$ に対して

$$K[\alpha_1,\cdots,\alpha_n]=\{f(\alpha_1,\cdots,\alpha_n)\,|\,f(x_1,\cdots,x_n)\in K[x_1,\cdots,x_n]\}$$

であり, その商体を $K(\alpha_1,\cdots,\alpha_n)$ と書くのであつた. これは L 内の $\alpha_1,\cdots,\alpha_n$ を含む最小の K の拡大体である.

問 5.12. $\alpha_1,\cdots,\alpha_n$ がすべて K 上代数的ならば $K[\alpha_1,\cdots,\alpha_n]=K(\alpha_1,\cdots,\alpha_n)$ となることを示せ.

定理 5.13. 拡大 L/K について次の 2 つは同値である.
(1) L/K は有限次拡大である.
(2) $L=K(\alpha_1,\cdots,\alpha_n)$ と書けて, 各 $\alpha_i\in L$ は K 上代数的である.

証明 (1)⇒(2). いま, $\alpha_1,\cdots,\alpha_n$ を K 上の vector 空間としての L の基底とせよ. このとき $L=K(\alpha_1,\cdots,\alpha_n)$ でなければならない. ゆゑに, 各 α_i は 5.11 より K 上代数的である.
(2)⇒(1). 各 α_i は K 上代数的であるから, もちろん $K(\alpha_1,\cdots,\alpha_{i-1})$ 上代数的で, $[K(\alpha_1,\cdots,\alpha_i):K(\alpha_1,\cdots,\alpha_{i-1})]<\infty$ である. $K\subset K(\alpha_1)\subset\cdots\subset K(\alpha_1,\cdots,\alpha_{n-1})\subset L$ なる体の列を考へれば, 5.2 より

$$[\,L:K\,]=[K(\alpha_1,\cdots,\alpha_n):K(\alpha_1,\cdots,\alpha_{n-1})]\cdots[K(\alpha_1,\alpha_2):K(\alpha_1)][K(\alpha_1):K]<\infty$$

となる. □

5.13 から容易に次のことがわかる.

例題 5.14. 体の列 $K\subset M\subset L$ において L/M, M/K が共に代数的拡大であれば L/K も代数的拡大である.

証明 $\alpha\in L$ とすれば, $\alpha^n+a_1\alpha^{n-1}+\cdots+a_n=0$ となる $a_i\in M$ がある. このとき α は $N=K(a_1,\cdots,a_n)$ 上代数的で, また各 a_i は K 上代数的であるから $[N:K]<\infty$ である. 従つて $[N(\alpha):K]=[N(\alpha):N][N:K]<\infty$ となり, α は K 上代数的である. □

例題 5.15. 拡大 L/K において K 上代数的な L の元の全体を M とすれば, M は体である. 従つて K 上代数的な 2 元の和, 差, 積, 商はまた K 上代数的である.

証明 $\alpha,\beta\in M$ とすれば, 5.13 より $K(\alpha,\beta)$ は代数的, 従つて $\alpha\pm\beta$, $\alpha\beta\in M$, また $\beta\neq0$ なら $\alpha\beta^{-1}\in M$ となる. □

上の M を K の L <u>における代数的閉包</u> と呼ぶ.

演 習 問 題

5.16. 5.15 の記号のもとで, L の元で M 上の代数的な元は M の元に限ることを示せ.
(Hint : $\alpha \in L$ は M 上代数的とせよ. $\mathrm{irr}\,(\alpha, M, x)$ の係数を K に添加した体について, 5.14 を利用せよ.)

5.17. $\mathbb{F}_p$ を標数 p の素体とせよ. 多項式 $x^2+1 \in \mathbb{F}_p[x]$ が既約であるためには $p \equiv 3 \bmod 4$ であることが必要十分である.

5.18. 次の拡大次数を求めよ.
(1) $[\,\mathbb{C} : \mathbb{R}\,]$
(2) $[\,\mathbb{Q}(\sqrt{5}) : \mathbb{Q}\,]$
(3) $[\,\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}\,]$
(4) $[\,\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}\,]$

5.19. 体の拡大 L/K があり, M をその中間体とせよ. $\alpha \in L$ が K 上代数的であるとせよ. このとき $[\,M(\alpha) : M\,] \leq [\,K(\alpha) : K\,]$ であることを示せ.

5.20. 体の拡大 L/K と中間体 M_1, M_2 があつて $[\,M_1 : K\,] = m_1$, $[\,M_2 : K\,] = m_2$, $\gcd(m_1, m_2) = 1$ とせよ. このとき $M_1 \cap M_2 = K$ であることを示せ.

5.21. 体の拡大 L/K があり, α, $\beta \in L$ とせよ. $[\,K(\alpha) : K\,] = m$, $[\,K(\beta) : K\,] = n$, $\gcd(m, n) = 1$ ならば, $[\,K(\alpha, \beta) : K\,] = mn$ であることを示せ.

5.22. 体の有限次拡大 L/K があり R は $L \supset R \supset K$ を満たし, L の演算に関して環であるとせよ. このとき R は体であることを示せ. (Hint : (5.11 と 5.8(1)) を用ゐよ.)

6. 超越次数

拡大 L/K があり, $\alpha_1, \cdots, \alpha_n \in L$ とする. 0 でない任意の $f(x_1, \cdots, x_n) \in K[x_1, \cdots, x_n]$ に対して $f(\alpha_1, \cdots, \alpha_n) \neq 0$ であるとき, $\alpha_1, \cdots, \alpha_n$ は K 上代数的に独立であるといひ, さうでないとき代数的に従属であるといふ. $n = 1$ のとき, α が K 上代数的に独立といふことは, K 上超越的であることと同じである. また $\alpha_1, \cdots, \alpha_n$ が K 上代数的に独立であることは, 写像

$$\varphi : K[x_1, \cdots, x_n] \longrightarrow K[\alpha_1, \cdots, \alpha_n] \quad f(x_1, \cdots, x_n) \longmapsto f(\alpha_1, \cdots, \alpha_n)$$

が環同型であることと同値である. このとき $K(\alpha_1, \cdots, \alpha_n)$ は有理函数体 $K(x_1, \cdots, x_n)$ に同型である.

L の部分集合 S に対して, その任意の有限部分集合が K 上代数的に独立であるとき, S は K 上代数的に独立であるといはれる. S が代数的に独立な部分集合のうち極大なものであるとき, S は L/K の超越基であるといはれる.

問 6.1. 拡大 L/K において, $\alpha_1, \cdots, \alpha_n$ が K 上代数的に独立であるとき, 次のことを示せ.
(1) $\alpha_1, \cdots, \alpha_n, \beta$ が K 上代数的に従属 $\iff$ $K(\alpha_1, \cdots, \alpha_n, \beta)/K(\alpha_1, \cdots, \alpha_n)$ が代数的.
(2) $\{\alpha_1, \cdots, \alpha_n\}$ が L/K の超越基 $\iff$ $L/K(\alpha_1, \cdots, \alpha_n)$ が代数的.

Vector 空間における基底と同様に, 超越基について次の定理が成り立つ.

定理 6.2. 拡大 L/K が有限生成ならば, L/K は有限個の元からなる超越基を持ち, その元の個数は超越基の選び方によらず一定である. この個数を L/K の超越次数と呼び, $\mathrm{trans.deg}_K L$ で表す.

証明 $L = K(\alpha_1, \cdots, \alpha_n)$ とし, $\{\alpha_1, \cdots, \alpha_n\}$ の部分集合で K 上代数的に独立なもののうち, 元の個数が最大なものを (必要ならばその番号を付け替へて) $\{\alpha_1, \cdots, \alpha_r\}$ とせよ. $M = K(\alpha_1, \cdots, \alpha_r)$ とおけば, 6.1 (1) より任意の α_i は M 上代数的で $L = K(\alpha_{r+1}, \cdots, \alpha_n)$ であるから, L/K は代数的である. 従つて $\{\alpha_1, \cdots, \alpha_r\}$ は超越基であり, L/K は有限個の元からなる超越基を持つことがわかつた.

さて, $\{\beta_1, \cdots, \beta_s\}$ を L/K の任意の超越基とする. このとき $\gamma_1, \cdots, \gamma_t \in L$ が K 上代数的に独立ならば, $\{\beta_j\}$ の番号を適当につけかへて, $\{\gamma_1, \cdots, \gamma_t, \beta_{t+1}, \cdots, \beta_s\}$ が L/K の超越基になること, 特に $t \leq s$ であることを t に関する帰納法で示さう. これが示されれば $\{\alpha_i \,|\, 1 \leq i \leq r\}$ と $\{\beta_j\}$ について $r \leq s$ かつ $s \leq r$ がわかり, $r = s$ を得る.

簡単のため $M_i = K[\gamma_1, \cdots, \gamma_i, \beta_{i+1}, \cdots, \beta_s]$ とおき, その商体を L_i とおく. $t = 0$ のときは明らかであるから $t > 0$ とし, $\gamma_1, \cdots, \gamma_{t-1}, \beta_t, \cdots, \beta_s$ は K 上代数的に独立で L/L_{t-1} は代数的であると仮定する. $\gamma_t \in L$ は L_{t-1} 上代数的であるから, 既約多項式 $f(x) \in L_{t-1}[x]$ で $f(\gamma_t) = 0$ となるものがある. 係数の分母を払つて $f(x) = c_0 x^m + c_1 x^{m-1} + \cdots + c_m = 0$, $c_i \in M_{t-1}$ としてよい. また M_{t-1} を多項式環とみて, $c_0, c_1, \cdots, c_m$ は互ひに素であるとしてよい. このとき, $\gamma_1, \cdots, \gamma_t$ の代数的独立性から, ある β_j $(t \leq j \leq s)$ が少なくとも 1 つの c_i に実際に現はれる. この β_j を更めて β_t と記すと, $0 \neq g(x) \in M_{t-1}[x]$, $g(\gamma_t) = 0$ ならば $f(x) | g(x)$ となるから, $g(x)$ のある係数に β_t が必ず現はれる.

以上のことから $\gamma_1, \cdots, \gamma_t, \beta_{t+1}, \cdots, \beta_s$ は K 上代数的に独立である. 実際, もしこれら

が代数的に従属であれば

$$K(\gamma_1,\cdots,\gamma_{t-1},\gamma_t,\beta_t,\beta_{t+1},\cdots,\beta_s) \supset K(\gamma_1,\cdots,\gamma_{t-1},\gamma_t,\beta_{t+1},\cdots,\beta_s)$$
$$\supset K(\gamma_1,\cdots,\gamma_{t-1},\beta_{t+1},\cdots,\beta_s)$$

は代数的な拡大であるが

$$K(\gamma_1,\cdots,\gamma_{t-1},\gamma_t,\beta_t,\beta_{t+1},\cdots,\beta_s) \supset K(\gamma_1,\cdots,\gamma_{t-1},\beta_t,\beta_{t+1},\cdots,\beta_s)$$
$$\supset K(\gamma_1,\cdots,\gamma_{t-1},\beta_{t+1},\cdots,\beta_s)$$

なる拡大列の後半は超越拡大であるから, 矛盾である. また等式 $f(\gamma_t)=0$ を β_t の方程式とみれば β_t が L_t 上代数的であることがわかる. L は $L_t(\beta_t)$ 上代数的であるから L/L_t も代数的である. □

例題 6.3. 体の列 $K\subset M\subset L$ において L/M が代数的拡大ならば
$\mathrm{trans.deg}_K L=\mathrm{trans.deg}_K M$ が成り立つ. 但し, M/K は有限生成とする.

証明 $\{\alpha_1,\cdots,\alpha_n\}$ を M/K の超越基とし, $N=K(\alpha_1,\cdots,\alpha_n)$ とすれば, M/N は代数的拡大である (6.1(2)). よつて L/N は代数的拡大で, 6.1(2) より $\{\alpha_1,\cdots,\alpha_n\}$ は L/K の超越基である. □

6.2 の証明から, 次のことがわかる.

例題 6.4. $L=K(\alpha_1,\cdots,\alpha_n)$ で $\mathrm{trans.deg}_K L=n$ ならば $\{\alpha_1,\cdots,\alpha_n\}$ は K 上代数的に独立で, それゆゑ L/K の超越基である.

証明 6.2 の証明の最初に示した様に, $\{\alpha_1,\cdots,\alpha_n\}$ の部分集合で K 上代数的独立なものがある. このうち, 元の個数が最大なものを (番号を付け替へて) $\{\alpha_1,\cdots,\alpha_r\}$ とすれば, これは L/K の超越基である. よつて仮定により $r=n$ となる. □

演 習 問 題

6.5. ξ が K 上超越的であれば, 任意の整数 $n>0$ に対し $[\,K(\xi):K(\xi^n)\,]=n$ であることを示せ.

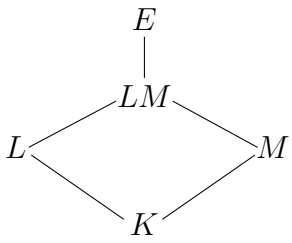
6.6. 体 k と不定元 t について, $K=k(t^5)$, $L=k(t)$ とせよ.
(1) $[L:K]$ はいくつか.
(2) $\alpha=t^2+t+1$ とおく. $K(\alpha)=L$ であることを示せ.
(3) t を t^5 と α の有理式で具体的に書け.
(Hint : t が $\beta=\alpha-1$ と t^5 で表せればよい. $t\beta$, β^2, β^3, t^5 の間のうまい 1 次関係を考へよ.)

6.7. 円周率 π は $\mathbb{Q}$ 上超越的であることが知られてゐる. $\mathrm{trans.deg}_{\mathbb{Q}}\mathbb{Q}(\pi+\sqrt{\pi})$ はいくつか.

6.8. K を 環 $\mathbb{Q}[x,y]/(x^2+y^2-1)$ の商体とする. $\mathrm{trans.deg}_{\mathbb{Q}}K$ はいくつか. また, 拡大 $K/\mathbb{Q}$ の超越基を 1 組求めよ.

7. 合成体

拡大体 E/K において, L をその中間体, S を E の部分集合とするとき, L の元を係数とし S の有限個の元の有理式の形で表される元の全体は E/L の中間体である. これを $L(S)$ で表す. $L(S)$ は L と S を含む E の最小の部分体である. 特に M が E/K の中間体のときは $L(M) = M(L)$ となる. これを L と M の 合成体 と呼んで LM または ML で表す. また拡大 ML/M を拡大 L/K の M への (または, M/K による) 持ち上げ と呼ぶ.



任意の拡大 L/K とその任意の持ち上げ LM/M に関し, 拡大に関する性質 $\boldsymbol{P}$ が L/K で満たされてゐれば, LM/M でも成り立つとき, 性質 $\boldsymbol{P}$ は持ち上げによつて 保たれる といふ. この様な性質として次の様なものがある.

例題 7.1. 体の拡大に関する次の性質は持ち上げによつて保たれる.
(i) 代数的拡大, (ii) 有限生成, (iii) 有限次拡大, (iv) 単純拡大.

証明 拡大 L/K の持ち上げ ML/M を考へる.
(i) L/K が代数的であるとせよ. $\alpha \in ML = M(L)$ は

$$\alpha = \frac{f(\gamma_1, \cdots, \gamma_n)}{g(\gamma_1, \cdots, \gamma_n)}, \quad f,\ g \in M[x_1, \cdots, x_n],\ \ \gamma_i \in L$$

と表されてゐる. このとき $\alpha \in M(\gamma_1, \cdots, \gamma_n)$ であるが, 各 γ_i は K 上代数的であるから M 上でも代数的, 従つて $M(\gamma_1, \cdots, \gamma_n)/M$ は代数的であり, 5.13 により, α は M 上代数的である.
(ii) L/K が有限生成, つまり $L = K(\alpha_1, \cdots, \alpha_n)$ と書けてゐるとせよ. このとき $ML = M(L) = M(\alpha_1, \cdots, \alpha_n)$ であるから ML/M も有限生成.
(iii) L/K が有限次拡大であれば, 5.11 により代数的拡大でもある. より強く, 5.13 から K 上代数的な α_j $(1 \le j \le n)$ によつて $L = K(\alpha_1, \cdots, \alpha_n)$ と書けてゐる. このとき (ii) と同様に $ML = M(\alpha_1, \cdots, \alpha_n)$ と書けて, 各 α_j は M 上でも代数的であるから, 再び 5.13 により ML/M は有限次拡大である.
(iv) (ii) の証明で $n = 1$ の場合を考へれば, 直ちにわかる. □

演 習 問 題

7.2. 次に挙げる 2 つの体の合成体を求めよ. また, その合成体の $\mathbb{Q}$ 上の基底と $\mathbb{Q}$ 上の拡大次数を求めよ.
(1) $\mathbb{Q}(\sqrt{2})$ と $\mathbb{Q}(\sqrt{3})$ (2) $\mathbb{Q}(\sqrt[3]{2})$ と $\mathbb{Q}(\sqrt{3})$
(3) $\mathbb{Q}(\sqrt[3]{2})$ と $\mathbb{Q}(\sqrt[3]{2}i)$ (4) $\mathbb{Q}(\sqrt{2})$ と $\mathbb{Q}(\sqrt{2}+\sqrt{3})$

7.3. 体の拡大 L/K があり, $\alpha_1, \cdots, \alpha_m, \beta_1, \cdots, \beta_n \in L$ であるとする. $K(\alpha_1, \cdots, \alpha_m)$ と $K(\beta_1, \cdots, \beta_m)$ の合成体は $K(\alpha_1, \cdots, \alpha_m, \beta_1, \cdots, \beta_m)$ であることを説明せよ.

7.4. 代数的拡大 L/K の 2 つの部分体 M_1, M_2 で $[\,M_1M_2 : M_1\,] < [\,M_2 : K\,]$ であり, $[\,M_1M_2 : M_1\,] = [\,M_2 : M_1 \cap M_2\,]$ となる例を挙げよ. また $[\,M_1M_2 : M_1\,] < [\,M_2 : M_1 \cap M_2\,]$ となる例を挙げよ. (Hint : 後半は $M_1M_2 = \mathbb{Q}(\sqrt[3]{2}, \omega)$ となる M_1, M_2 を考へよ.) (16.5 (1) も参照.)

8. 代数的閉包

この節では, いくつもの体に関する種々の考察をするのに便利な代数的閉包と呼ばれる体の存在を証明する.

例題 8.1. 体 Ω について, 次の条件は互ひに同値である.
(1) $f(x) \in \Omega[x]$, $\deg f > 0$ ならば, Ω は $f(x)$ の根を少くとも 1 つ含む.
(2) $f(x) \in \Omega[x]$, $\deg f > 0$ ならば, $f(x)$ は $\Omega[x]$ で 1 次式の積に分解する.
(3) $\Omega[x]$ の既約多項式はすべて 1 次式または定数である.
(4) Ω の代数的拡大は Ω 以外には存在しない.

証明 (1)⇒(2). $\deg f$ に関する帰納法で容易に証明される.
(2)⇒(3). 自明.
(3)⇒(4). L/Ω を代数的拡大とせよ. $\alpha \in L$ とすれば $\mathrm{irr}\,(\alpha, \Omega, x)$ は 1 次式である. 従つて $\alpha \in \Omega$ であり, $L = \Omega$ である.
(4)⇒(1). 5.9 より $f(x)$ の根 α を含む拡大が存在する. その 1 つを L/Ω すれば $L \supset \Omega(\alpha)$. ゆゑに $\Omega(\alpha)/\Omega$ も代数的拡大であるが, 仮定より $\alpha \in \Omega(\alpha) = \Omega$ となる. □

定義 8.2. 体 Ω が 8.1 の条件を満たすならば, Ω は 代数的閉体 であるといはれる.

例 8.3. (1) 複素数体 $\mathbb{C}$ は代数的閉体である (代数学の基本定理).
(2) $\overline{\mathbb{Q}} = \{\, \alpha \in \mathbb{C} \,|\, \alpha \text{ は } \mathbb{Q} \text{ 上代数的} \,\} (\subset \mathbb{C})$ は代数的閉体である (5.14 を使ふ).
円周率 $\pi = 3.14159265\cdots$ や Napier の数 $e = 2.7182818284590\cdots$ などは $\overline{\mathbb{Q}}$ に属さないことが知られてをり, $\overline{\mathbb{Q}} \subsetneqq \mathbb{C}$ である (8.10 も参照されたい).

定義 8.4. 拡大 Ω/K が条件
(1) Ω/K は代数的拡大,
(2) Ω は代数的閉体
をともに満たすとき, Ω は K の 代数的閉包 であるとはれる.

問 8.5. L/K が代数的ならば L の代数的閉包は K の代数的閉包であることを示せ.

以下では代数的閉包の存在と, ある意味での一意性を示す.

定理 8.6. (E. Steinitz) 任意の体 K に対し K の代数的閉包が存在する.

これは K 上のあらゆる多項式の根を添加してできあがる最大の体が存在するといふことであるが, 当面, これを認めて証明を飛ばし先に進んでもよい. この定理の証明のためにまづ, 次のことを示す.

補題 8.7. 多項式環 $K[x]$ において, 次数が 1 以上の多項式の全体を $K[x]^*$ と表す. K の代数的拡大で, 任意の $f(x) \in K[x]^*$ がそこで少くとも 1 つ根を持つ様なものが存在する.

証明 各 $f(x) \in K[x]^*$ ごとに文字 X_f を用意し, それらの文字の全体を S とする : $S = \{\, X_f \,|\, f(x) \in K[x]^* \,\}$. また S の有限個の元に関する K 上の多項式の全体を $K[S]$ と書く. $K[S]$ はもちろん可換環である. $K[S]$ において $\{\, f(X_f) \,|\, f \in K[x]^* \,\}$ で生成される ideal を

I とする. $K[S] \supsetneqq I$ となることが次の様にして示される. いま $K[S] = I$ であるとすれば, $f_1(x), \cdots, f_n(x) \in K[x]^*$ と $g_1, \cdots, g_n \in K[S]$ が存在して

$$1 = g_1 \cdot f_1(X_{f_1}) + \cdots + g_n \cdot f_n(X_{f_n}) \tag{8.8}$$

が成り立つ. $g_1, \cdots, g_n$ に現れる変数の個数は有限であるから, ある $N \in \mathbb{N}$ について, これらはすべて $K[X_{f_1}, \cdots, X_{f_n}, \cdots, X_{f_N}]$ の元としてよい. さて, 5.9 より $f_1(x)$ の根の 1 つ α_1 を含む拡大 L_1/K が存在する. さらに $f_2(x)$ の根の 1 つ α_2 を含む拡大 L_2/L_1 がある. 以下同様にして体の拡大列 $K \subset L_1 \subset L_2 \subset \cdots \subset L_n = L$ を考へる. このとき L はこれら $\{f_1(x), \cdots, f_n(x)\}$ の根の全体 $\{\alpha_1, \cdots, \alpha_n\}$ を含む. そこで (8.8) に

$$X_{f_1} = \alpha_1, \ \cdots, \ X_{f_n} = \alpha_n, \ X_{f_{n+1}} = \cdots = X_{f_N} = 0$$

なる代入をすれば $1 = 0$ となり矛盾である. よつて $K[S] \supsetneqq I$ である. これにより I を含む $K[S]$ の極大 ideal が存在する. その 1 つを J とせよ. $E_K = K[S]/J$ は体であり, 自然に $K \subset E_K$ と見做せる. X_f を含む剰余類 $X_f + J$ を $\overline{X_f}$ で表す. I の定義から, 任意の $f \in K[x]^*$ に対して $f(\overline{X_f}) = 0$ となるから, E_K は所望の条件を満たす. □

証明 (8.6 の) 上で示した様に $K[S] \supsetneqq I$ であるから, I を含む $K[S]$ の極大 ideal J がある. $E_S = K[S]/J$ は体で, $E_K \supset K$ と考へてよい. いま X_f を含む剰余類 $X_f + J$ を $\overline{X_f}$ と表せば, I の定義から任意の $f \in K[x]^*$ に対して $f(\overline{X_f}) = 0$ となり, E_K/K は (8.7) に叶ふ拡大である. $K_0 = K$ とし, (8.7) の様な E_K を 1 つ取つて $E_K = K_1$ とおく. K に対して行つた手続きを K_1 に対して行ひ, E_{K_1} を得るが, それを E_2 とおく. 以下同様に手続きを行ひ $K_{i+1} = E_{K_i}$ と記せば, 体の列

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots$$

が得られる. この作り方から K_{i+1}/K_i は代数的拡大であり, 任意の $h(x) \in K_i[x]^*$ は K_{i+1} で少くとも 1 つの根を持つ. $\Omega = \cup_{i=0}^{\infty} K_i$ は K の拡大で, $\alpha \in \Omega$ はある K_i に含まれ, K_i/K は代数的拡大であるから Ω/K は代数的拡大である. また $h(x) = c_0x^r + c_1x^{r-1} + \cdots + c_r \in \Omega[x]$ が次数 1 以上であれば, ある m について, K_m は, すべての c_i $(0 \leq i \leq r)$ を含む. $h(x) \in K_m[x]^*$ であるから $h(x)$ は K_{m+1} 内に, つまり Ω 内に, 少くとも 1 つ根を持つ. これで Ω は代数的閉体であることがわかつた. つまり Ω は K の代数的閉包である. □

例 8.9. Ω は体 K を含む代数的閉体とし, $\overline{K}$ を K の Ω における代数的な元全体の集合とすれば, $\overline{K}$ は K の代数的閉包である.

演 習 問 題

8.10. $\overline{\mathbb{Q}}$ は集合として可算濃度であることを示せ. (Hint : 各多項式 $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \in \mathbb{Z}[x]$ $(a_0 \geq 1)$ に対し $n + a_0 + |a_1| + \cdots + |a_n|$ を考へて, これをもとに $\overline{\mathbb{Q}}$ の元を数へればよい.)

8.11. $\mathbb{C}$ は非可算集合であることを示し, $\overline{\mathbb{Q}} \subsetneqq \mathbb{C}$ を示せ.

8.12. $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$ であることを示せ. (Hint : Eisenstein の既約性判定定理を使ひ, いくらでも次数の高い既約多項式があることを示せ.)

9. 部分体の上の同型

体 K から体 L への環準同型 $\sigma : K \to L,\ a \mapsto a^\sigma$ について, その核 $\mathrm{Ker}\,\sigma$ は K の極大 ideal であるから K 自身であるか $\{0\}$ である. 前者の場合, つまり像が $\{0\}$ のとき, σ は 自明 であるといはれる. 後者の場合, つまり σ が自明でないとき, $\mathrm{Ker}\,\sigma = \{0\}$ であり, σ は単射である. よつて K は部分体 $\mathrm{Im}\,\sigma \subset L$ に同型である. この準同型の像は通常

$$K^\sigma = \{\, a^\sigma \,|\, a \in K \,\}$$

と書かれる. このとき σ を K から L の 中への同型 といふ. 特に $\mathrm{Im}\,\sigma = L$ のときは $\sigma : K \tilde{\to} L$ と書いて, K から L への上への 同型 といふ.

体 K の 2 つの拡大 L/K と L'/K の間の同型 $\sigma : L \tilde{\to} L'$ が K の各元を不変にするとき, 即ち $\mathrm{id}_K : K \tilde{\to} K$ の拡張になつてゐるとき, σ は K 上の同型 であるといふ. 中への K 上の同型 も同様に定義される.

体 L から自身への同型 $\sigma : L \tilde{\to} L$ を L の 自己同型 といふ. また拡大 L/K に対して K 上の同型 $\sigma : L \tilde{\to} L$ を L の K 上の自己同型 といふ. これらは写像の合成を演算として群をなす. それぞれを

$$\mathrm{Aut}\, L, \qquad \mathrm{Aut}\, L/K$$

と書いて, それぞれ L の 自己同型群, K 上の自己同型群 と呼ぶ.

体の同型 $\sigma : K \tilde{\to} K'$ は自然に多項式の間の同型

$$K[x] \tilde{\to} K'[x] \qquad \sum_{i=0}^{n} a_i\, x^i \mapsto \sum_{i=0}^{n} {a_i}^\sigma x^i$$

に拡張される. これを同じ記号 σ で表して $f(x) \in K[x]$ の像を $f^\sigma(x)$ で表す. 明らかに, $p(x)$ が $K[x]$ の既約多項式ならば, $p^\sigma(x)$ は $K'[x]$ の既約多項式であり, この逆も成り立つ.

問 9.1. 次の問に答へよ.

(1) $\mathrm{char}\, F = p > 0$ とせよ. $\mathbb{Q}$ から F への (または F から $\mathbb{Q}$ への) 環準同型写像は, すべての元を $0 \in F$ (または $0 \in \mathbb{Q}$) に写すものだけであることを示せ.

(2) $\mathbb{Q}(\sqrt{2}\,)$ の自己同型写像は 2 つだけ存在する. それらを記述せよ.

(3) $\mathbb{Q}(\sqrt[3]{2}\,)$ の自己同型写像は恒等写像しかないことを示せ.

(4) $\mathbb{Q}(\sqrt[3]{2}\,)$ から $\mathbb{C}$ の中への同型写像は 3 つだけ存在する. それらを記述せよ.

例題 9.2. $\sigma : K \tilde{\to} K'$ を体の同型とせよ. いま $L = K(\alpha)$ は $K[x]$ の既約多項式 $p(x)$ の根 α を K に添加した体とし, $L' = K'(\alpha')$ は $p^\sigma(x)$ の根 α' を K' に添加した体とする. このとき σ の拡張 $\overline{\sigma} : L \tilde{\to} L'$ で α を α' に写すものが存在する.

証明 $\sigma : K[x] \tilde{\to} K'[x]$ から自然に環準同型 $\overline{\sigma} : K[x]/(p(x)) \tilde{\to} K'[x]/(p^\sigma(x))$ が得られる. これは $\sigma : K \tilde{\to} K'$ の拡張で $x + (p(x)) \mapsto x + (p^\sigma(x))$
となつてゐる. 一方,

$$\tau : K[x]/(p(x)) \tilde{\to} K(\alpha),\ x + (p(x)) \mapsto \alpha\ ;$$
$$\tau' : K'[x]/(p^\sigma(x)) \tilde{\to} K'(\alpha'),\ x + (p^\sigma(x)) \mapsto \alpha'$$

はそれぞれ K 上の同型, K' 上の同型である.

$$\begin{array}{ccc} K[x]/(p(x)) & \xrightarrow{\overline{\sigma}} & K'[x]/(p^\sigma(x)) \\ \downarrow{\scriptstyle \tau} & & \downarrow{\scriptstyle \tau'} \\ K(\alpha) & \xrightarrow{\rho} & K'(\alpha') \end{array}$$

このとき $\rho = \tau' \overline{\sigma} \tau^{-1} : K(\alpha) \mapsto K'(\alpha')$ は求めるものである □

問 9.3. 体 K 上代数的な 2 元 α, α' に対して, 次の 2 つの条件は同値である.
(1) $\mathrm{irr}\,(\alpha, K, x) = \mathrm{irr}\,(\alpha', K, x)$.
(2) K 上の同型 $\sigma : K(\alpha) \xrightarrow{\sim} K(\alpha')$ で $\alpha^\sigma = \alpha'$ となるものがある.

9.3 の様な性質をもつ 2 元 α, α' は K 上で共役であるといはれる. さて, 代数的閉包の一意性は次の定理の様に述べられる.

定理 9.4. $\overline{K}$, $\overline{K'}$ をそれぞれ体 K, K' の代数的閉包とし, $\sigma : K \xrightarrow{\sim} K'$ は体の同型であるとせよ. このとき σ は同型 $\overline{\sigma} : \overline{K} \xrightarrow{\sim} \overline{K'}$ に拡張される. 特に K の 2 つの代数的閉包は互ひに K 上同型である.

証明 $\overline{K}/K$ の中間体 L と, L から $\overline{K'}$ の中への同型 $\rho : L \to \overline{K'}$ であつて, σ の拡張であるものの組 (L, ρ) の全体を $\mathscr{L}$ で表す. $\mathscr{L}$ に順序を次の様に入れる :

$$(L_1, \rho_1) \leq (L_2, \rho_2) \iff L_1 \subset L_2 \text{ かつ } \rho_2 \text{ は } \rho_1 \text{ の拡張.}$$

このとき, $\mathscr{L}$ は半順序集合で, また帰納的であることが次の様にして示される.
いま $\{(L_\lambda, \rho_\lambda) \,|\, \lambda \in \Lambda\}$ を $\mathscr{L}$ の全順序部分集合とするとき, $L = \bigcup_\lambda L_\lambda$ とおく. $\alpha \in L$ はある L_λ に属し, $\alpha^{\rho_\lambda} \in \overline{K'}$ がきまるが, 順序の定義と全順序性からこれは $\alpha \in L_\lambda$ である限り λ の選び方に依らないことが容易にわかる. そこで α に α^{ρ_λ} を対応させて, L から $\overline{K'}$ の中への同型 $\rho : L \to \overline{K'}$ が得られる. ここで $(L, \rho) \in \mathscr{L}$ かつ $(L_\lambda, \rho_\lambda) \leq (L, \rho)$ $(\forall \lambda \in \Lambda)$ となることは作り方から明らかである. 以上から Zorn の補題によつて, $\mathscr{L}$ は極大元 (L_0, ρ_0) を持つ. このとき $L_0 = \overline{K}$ で, $\mathrm{Im}\,\rho_0 = \overline{K'}$ となることを示せばよい. いま $\overline{K} \supsetneqq L_0$ とし, $\alpha \in \overline{K} - L_0$ とする. 9.2 により $\rho_0 : L_0 \to \overline{K'}$ は $\rho_1 : L_0(\alpha) \to \overline{K'}$ に拡張できる. このとき $(L_0, \rho_0) < (L_0(\alpha), \rho_1)$ となつて (L_0, ρ) の極大性に矛盾する. よつて $L_0 = \overline{K}$ である. また $\mathrm{Im}\,\rho_0 = {L_0}'$ とおけば, $\overline{K} \simeq {L_0}'$ より ${L_0}'$ は代数的閉体である. なぜなら, 任意の $f(x) \in {L_0}'[x]$ の ρ_0 による逆像 $f^{\rho^{-1}}(x)$ は $\overline{K}$ 上 1 次式だけの積に分解するから, $f(x)$ 自身はそれらの 1 次式の ρ_0 による像の積に分解するからである. 一方, $\overline{K'}/K'$ は代数的で ${L_0}' \supset K'$ であるから $\overline{K'}/{L_0}'$ も代数的で, それゆゑ ${L_0}' = \overline{K'}$ である. □

上の定理の応用として, 次のことが示される.

例題 9.5. $\sigma : K \to \Omega$ を体 K から代数的閉体 Ω の中への同型とし, L/K を任意の代数的拡大とせよ. このとき σ は L から Ω の中への同型 $\rho : L \to \Omega$ に拡張できる.

証明 $\overline{K^\sigma}$ を K^σ の Ω における代数的閉包とせよ. 8.5 により, L の任意の代数的閉包は K の代数的閉包でもあるから, それを $\overline{K}$ と書く. 9.4 により $\sigma : K \xrightarrow{\sim} K^\sigma$ は $\overline{\sigma} : \overline{K} \xrightarrow{\sim} \overline{K^\sigma}$ に拡張できる. $\overline{\sigma}$ の L への制限 $\overline{\sigma}|_L$ を L から Ω の中への写像と見做せば, これが求める ρ である. □

定義 9.6. 以後, 任意の体に対して $\overline{K}$ は K の 1 つの代数的閉包を示すものとする.

補題 9.7. (重要, 12.11 と関連) $L = K(\alpha)$ を K の単純な代数的拡大とし, $p(x) = \mathrm{irr}\,(\alpha, K, x)$ とおく. このとき, L から K の代数的閉包 $\overline{K}$ の中への K 上の同型の個数は $p(x)$ の異なる根の個数に一致する.

証明 $p(x)$ は $\overline{K}[x]$ で 1 次式の積に分解される. その異る根を $\alpha_1, \cdots, \alpha_r$ とする. いま $\sigma : L \to \overline{K}$ が K 上の同型であれば, $p(\alpha^\sigma) = p(\alpha)^\sigma = 0^\sigma = 0$ であるから, α の像は $\alpha_1, \cdots, \alpha_r$ のどれかでなければならない. 一方, $\alpha \mapsto \alpha_i$ により L から $\overline{K}$ の中への r 個の K 上の同型 $\sigma_i : L \to \overline{K}$ が定まる. このとき, 9.4 から, L から $\overline{K}$ の中への K 上の同型はこれらの中のどれかと一致することがわかる. □

演 習 問 題

9.8. K を体, α, β を K 上代数的な元とする. 次を示せ.

(1) $\mathrm{irr}\,(\alpha, K, x) = \mathrm{irr}\,(\alpha, K(\beta), x) \iff \mathrm{irr}\,(\beta, K, x) = \mathrm{irr}\,(\beta, K(\alpha), x)$

(2) α' を α の K 上の共役元, β' を β の K 上の共役元とせよ. $\mathrm{irr}\,(\alpha, K, x) = \mathrm{irr}\,(\alpha, K(\beta), x)$ であれば, $\sigma(\alpha) = \alpha'$, $\sigma(\beta) = \beta'$ となる K 上の同型写像 $\sigma : K(\alpha, \beta) \to K(\alpha', \beta')$ が存在する.

10. 最小分解体

多項式の最小分解体とそれらの間の同型写像が関連する種々の問題を解く鍵となる.

定義 10.1. K を体, $f(x) \in K[x]$ とする. K の拡大体 L において $f(x)$ が 1 式のみによる積に分解されるとき L を $f(x)$ の 分解体 といふ. また L が $f(x)$ の分解体であり, かつ, K を含む L のいかなる真の部分体も $f(x)$ の分解体にならないとき, L を $f(x)$ の 最小分解体 といふ.

最小分解体は常に存在する. 実際, $\overline{K}$ は $f(x) \in K[x]$ の分解体であるが, $\overline{K}$ に含まれる $f(x)$ のすべての根を K に添加した体 $K(\alpha_1, \cdots, \alpha_n)$ は $f(x)$ の最小分解体である.

定理 10.2. 体の同型写像 $\sigma : K \longrightarrow K'$ があり, $f(x) \in K[x]$ とする. また L, L' はそれぞれ $f(x)$, $f^\sigma(x)$ の K 上, および K' 上の最小分解体とする. このとき, σ は同型 $\tilde{\sigma} : L \longrightarrow L'$ に拡張できる. 特に K 上の最小分解体は全て互いに K 上同型である.

証明 $\overline{K}$, $\overline{K'}$ をそれぞれ L, L' を含む K, K' の代数的閉包とし, 体の同型 $\bar{\sigma} : \overline{K} \xrightarrow{\sim} \overline{K'}$ を σ の拡張とする. いま $f(x) = c_0x^n + c_1x^{n-1} + \cdots + c_n$ $(c_i \in K)$ が $\overline{K}[x]$ において $f(x) = c_0(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ と分解されたとすれば, $L = K(\alpha_1, \cdots, \alpha_n)$ である. また $f^\sigma(x) = c_0{}^{\bar{\sigma}}(x-\alpha_1{}^{\bar{\sigma}})(x-\alpha_2{}^{\bar{\sigma}})\cdots(x-\alpha_n{}^{\bar{\sigma}})$ であるから $L' = K'(\alpha_1{}^{\bar{\sigma}}, \cdots, \alpha_n{}^{\bar{\sigma}}) = L^{\bar{\sigma}}$ である. よつて $\bar{\sigma}$ の L への制限は同型 $\rho : L \xrightarrow{\sim} L'$ を与へ, これは σ の拡張である. □

定義 10.3. 一般に $\{f_\lambda(x) \,|\, \lambda \in \Lambda\} \subset K[x]$ に対し, 1 つの拡大体 L/K が全ての $\lambda \in \Lambda$ について $f_\lambda(x)$ の分解体であるとき, L はこの多項式の集合の 分解体 であるといひ, L における根の集合を $S = \{\alpha \,|\, \exists\lambda \in \Lambda \;\; f_\lambda(\alpha) = 0\}$ として $L = K(S)$ となつてゐるとき, L はこの集合 $\{f_\lambda(x) \,|\, \lambda \in \Lambda\}$ の K 上の 最小分解体 であるといはれる.

演 習 問 題

10.4. $[\,K : \mathbb{F}_p\,] = [\,K' : \mathbb{F}_p\,]$ のとき $K \simeq K'$ であることを示せ.
(Hint : 17.1 を参照されたい.)

10.5. 次の各多項式の $\mathbb{Q}$ 上の因数分解と最小分解体, およびそれぞれの $\mathbb{Q}$ 上の拡大次数を求めよ.
(1) $x^3 - 1$ (2) $x^3 - 2$ (3) $x^4 + 5x^2 + 6$ (4) $x^6 - 8$

10.6. 多項式 $x^5 - 4x + 2$ は $\mathbb{Q}$ 上既約であるか. また $x^5 - 4x - 4$ はどうか. 理由をつけて答へよ.

10.7. 拡大 L/K の 2 元 α, β は K 上代数的であるとせよ. $f(x) = \mathrm{irr}\,(\alpha, K, x)$, $g(x) = \mathrm{irr}\,(\beta, K, x)$ とおく. このとき $f(x)$ が $K(\beta)$ 上可約ならば $g(x)$ は $K(\alpha)$ 上可約であることを示せ. (Hint : $[\,K(\alpha,\beta) : K\,]$ を考へよ.)

11. 正規拡大

例題 11.1. 体 K とその代数的閉包 $\overline{K}$ を固定する. 中間体 $K \subset L \subset \overline{K}$ について次の (1) 〜 (4) は同値である.

(1) L から $\overline{K}$ の中への K 上の任意の同型 $\sigma : L \longrightarrow \overline{K}$ に対して, $L^\sigma = L$ である.

(2) 任意の $\sigma \in \mathrm{Aut}\overline{K}/K$ に対して $L^\sigma = L$ である.

(3) $K[x]$ の既約多項式 $p(x)$ が L で少くとも 1 つの根を持てば, $p(x)$ は $L[x]$ で 1 次式の積に分解する.

(4) L はある $\{f_\lambda(x) \,|\, \lambda \in \Lambda\} \subset K[x]$ の最小分解体である.

証明 (1)⇒(2). $\sigma \in \mathrm{Aut}\overline{K}/K$ の L への制限 $\sigma|_L : L \to \overline{K}$ について, $L = L^{\sigma|_L} = L^\sigma$ となる.
(2)⇒(3). $\overline{K}[x]$ で $p(x) = c(x-\alpha_1)\cdots(x-\alpha_n)$ と分解されるとし, また $\alpha_1 \in L$ とする. このとき各 α_i に対して 9.2 を使ふと, $\alpha_1 \mapsto \alpha_i$ によつて K 上の同型 $\sigma : K(\alpha_1) \xrightarrow{\sim} K(\alpha_i)$ が定まる. $K(\alpha_1), K(\alpha_i) \subset \overline{K}$ であるから, これは, 9.4 により K 上の同型 $\overline{\sigma} : \overline{K} \to \overline{K}$ に拡張される. このとき $\overline{\sigma} \in \mathrm{Aut}\overline{K}/K$ で, $\alpha_i = {\alpha_1}^{\overline{\sigma}} \in L^{\overline{\sigma}} = L$ となり, $p(x)$ は $L[x]$ で 1 次式の積に分解される.
(3)⇒(4). L の各元 α に対し, $p_\alpha(x) = \mathrm{irr}\,(\alpha, K, x)$ とおけば, 明らかに L は $\{\, p_\alpha(x) \,|\, \alpha \in L \,\}$ の最小分解体である.
(4)⇒(1). $f_\lambda(x)$ $(\lambda \in \Lambda)$ の $\overline{K}$ における根の全体を S とすると, $L = K(S)$ である. L から $\overline{K}$ の中への同型 $\sigma : L \to \overline{K}$ に対して ${f_\lambda}^\sigma(x) = f_\lambda(x)$ であるから, σ は $f_\lambda(x)$ の根の集合を不変にし, 従つて $S^\sigma = S$ である. よつて $L^\sigma = K(S^\sigma) = K(S) = L$ となる. □

注意 11.2. 10.2 と 11.1(1) から $f(x) \in K[x]$ の K 上の最小分解体は $\overline{K}$ の中に唯 1 つだけ存在する. いま $\{\alpha_1, \cdots, \alpha_n\}$ を $f(x)$ の全ての根の集合とすると, K 上の最小分解体は $K(\alpha_1, \cdots, \alpha_n)$ に他ならない.

定義 11.3. 代数的拡大 L/K が 11.1 の条件を満たすとき, L/K は 正規拡大 (normal extension) と呼ばれる. 特に, K 上の多項式のある集合の K 上の最小分解体と K 上の正規拡大は同じ概念である.

命題 11.4. 正規拡大性について次が成り立つ.

(1) $K \subset M \subset L$ を体の列とし, L/K が正規拡大なら, L/M も正規拡大である.

(2) L_1, L_2 を $\overline{K}/K$ の中間体とする. L_1/K と L_2/K がともに正規拡大であるとすれば L_1L_2/K も正規拡大である.

(3) M と M' を L/K の中間体とせよ. M'/K が正規拡大ならば MM'/M も正規拡大である. (つまり, 正規拡大性は持ち上げにより保たれる.)

証明 (1) L/K は代数的であるから, L を含む K の代数的閉包 $\overline{K}$ がある. $\overline{K} = \overline{L}$ としてよい. このとき $\mathrm{Aut}\overline{K}/K \supset \mathrm{Aut}\overline{M}/M$ であるから, $\sigma \in \mathrm{Aut}\overline{M}/M$ に対し $L^\sigma = L$. よつて 11.1(2) が成り立つのであるから L/M は正規拡大である.
(2) ${L_i}^\sigma = L_i$ $(i = 1, 2)$ であるから $(L_1L_2)^\sigma = {L_1}^\sigma {L_2}^\sigma = L_1L_2$ となる.

(3) $K[x]$ の部分集合 $\{f_\lambda(x) \mid \lambda \in \Lambda\}$ があつて, 各 $f_\lambda(x)$ は M' で 1 次式の積に分解され, S をその L における根の全体とすれば $M' = K(S)$ となつてゐる. このとき $f_\lambda(x) \in M[x]$, $MM' = MK(S) = M(S)$ であるから, MM'/M は正規拡大である. □

問 11.5. 拡大次数が 2 である拡大を 2 次拡大といふ. 次の事を示せ.

(1) 2 次拡大は正規拡大である.

(2) 有理数体 $\mathbb{Q}$ の拡大列 $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$ において, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ はともに正規拡大であるが, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ は正規拡大ではない.

注意 11.6. 11.5 (2) より, 一般に, 体の列 $K \subset M \subset L$ において, $K \subset M$, $M \subset L$ がともに正規拡大であつても $K \subset L$ は正規拡大とは限らない. 例へば, $K = \mathbb{Q}$, $M = \mathbb{Q}(\sqrt[3]{2})$, $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$.

演 習 問 題

11.7. 次の代数的拡大は正規であるか否かを理由を付して答へよ. 但し $\omega = \frac{-1+\sqrt{-3}}{2}$ で, t は不定元とする.

(1) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$

(2) $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$

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

(4) $\mathbb{Q}(\omega)/\mathbb{Q}$

(5) $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$

(6) $\mathbb{F}_5(t)/\mathbb{F}_5(t^3)$

(7) $\mathbb{F}_5(t)/\mathbb{F}_5(t^4)$

(8) $\mathbb{F}_5(t)/\mathbb{F}_5(t^5)$

12. 分離性

$\mathbb{Q}$ 上のいかなる既約多項式 $f(x) \in \mathbb{Q}[x]$ も重根を持たない. 同様に p を素数とするとき, $\mathbb{F}_p$ 上のいかなる既約多項式 $f(x) \in \mathbb{F}_p[x]$ も重根を持たない. しかし, 不定元 t について, 多項式 $x^p - t \in \mathbb{F}_p(t)[x]$ は $\mathbb{F}_p(t)$ の代数的閉包の中に根を持つが, それを α とすれば ($\alpha^p = t$), $x^p - t$ は既約であるにも拘らず, $x^p - t = (x - \alpha)^p$ と因数分解されるので, 重根を持つ. つまり既約多項式であつても重根を持つ場合がある. その様な場合についてまとめて考察しておかう, といふのがこの節の目的である.

但し, Galois 理論の様子を一通り掴むためには, 標数が 0 の場合を主にして学習するといふ道筋もあるので, 余り深入りはしないでおく.

多項式 $f(x) \in K[x]$ が $\overline{K}$ 上で, 異る 1 次式の冪積

$$f(x) = c(x - \alpha_1)^{m_1}(x - \alpha_2)^{m_2} \cdots (x - \alpha_r)^{m_r}$$

に分解されるとき, 各 α_i は $f(x)$ の m_i 重根 であるといひ, $m_i > 1$ のとき α_i は $f(x)$ の 重根 であるといはれる.

例へば $\operatorname{char} K = p > 0$ のとき, $a \in K$, $e \in \mathbb{N}$ に対して α を $x^{p^e} - a$ の 1 つの根とすれば, $(x - \alpha)^{p^e} = x^{p^e} - \alpha^{p^e} = x^{p^e} - a$ となり, α は $x^{p^e} - a$ の p^e 乗根である.

一般に $x^n - a$ の根を a の n 乗根 と呼ぶ. 上のことから次のことがわかる.

命題 12.1. $\operatorname{char} K = p > 0$ ならば, K の元 a の p^e 乗根は $\overline{K}$ で唯 1 つだけ存在する. (これを $\sqrt[p^e]{a}$ または a^{1/p^e} と書く.)

多項式 $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ を形式的に微分した多項式を $f'(x) = na_0x^{n-1} + (n-1)a_1x^{n-2} + \cdots + a_{n-1}$ を $f'(x)$ または $(f(x))'$ と書き, $f(x)$ の 導函数 と呼ぶ. このとき 2 つの多項式に関して $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$ が成り立つことが容易に確かめられる (確かめよ).

例題 12.2. $f(x) \in K[x]$, $\alpha \in \overline{K}$ とせよ. 次が成り立つ.
(1) α が $f(x)$ の重根 $\iff$ $f(\alpha) = f'(\alpha) = 0$.
(2) $f(x)$ が既約で $f(\alpha) = 0$ のとき :
α が $f(x)$ の重根 $\iff$ $f'(x) = 0$ (多項式として)

証明 (1) ($\Rightarrow$) $f(x) = (x - \alpha)^2 g(x)$ とすれば, $f'(x) = 2(x - \alpha)g(x) + (x - \alpha)^2 g'(x) = (x - \alpha)(2g(x) + (x - \alpha)g'(x))$ となり, α は $f'(x) = 0$ の根でもある.
($\Leftarrow$) α が重根でないとすれば, $f(x) = (x - \alpha)h(x)$, $h(\alpha) \neq 0$ となる. このとき $f'(x) = h(x) + (x - \alpha)h'(x)$ となり, $f'(\alpha) = h(\alpha) \neq 0$ である.
(2) α が重根ならば $f'(\alpha) = 0$, よつて $f(x) | f'(x)$ となる. $\deg f' < \deg f$ であるから, $f'(x) = 0$ である. 逆に $f'(x) = 0$ ならば当然 $f'(\alpha) = 0$ であり, α は $f(x)$ の重根である. □

注意 12.3. 12.2 (2) は $\operatorname{char} K = p > 0$ のときに意味を持つ主張である. 実際, このとき, もし $\overline{K} \ni b^{\frac{1}{p}} \notin K$ かつ $b \in K$ なる元があれば $x^p - b$ は $K[x]$ においては既約で, $\alpha = b^{\frac{1}{p}}$ は $f(x)$ の p 重根であり, $f'(x) = px^{p-1} = 0$ であることに注意せよ.

定義 12.4. $f(x) \in K[x]$ が $\overline{K}$ で重根を持たないとき, $f(x)$ は 分離的 であるといはれる. また, $\alpha \in \overline{K}$ に対して, $\mathrm{irr}(\alpha, K, x)$ が重根を持たないとき, α は K 上(じょう) 分離的 であるといはれる.
代数的拡大 L/K において, L のすべての元が K 上分離的であるとき, L/K は 分離的拡大 である, 或いは単に 分離的 であるといはれる. 体 K の元や部分集合についても, それらが K 上に生成する拡大が分離的なとき 分離的 といふ. 分離的でない状況を 非分離的 といふ.

問 12.5. 体の列 $K \subset M \subset L$ において, L/K が分離的であれば, L/M も M/K も分離的である. これを示せ.

問 12.6. t を不定元とし, $L = \mathbb{F}_5(t)$ の部分体 $K = \mathbb{F}_5(t^5)$ を考へる. このとき, 多項式 $x^5 + t^5$, $x^{25} + t^5 \in K[x]$ はともに既約で, 非分離的であることを示せ.

注意 12.7. $\mathrm{char}\, K = 0$ ならば, 任意の $f(x) \in K[x]$, $\deg f(x) \geq 1$ に対して $f'(x) \neq 0$ となるから, 12.2 (2) により, あらゆる $\alpha \in \overline{K}$ は K 上分離的である. 従つてこの場合は, 拡大体が分離的であるかどうかを気にしなくてよい.

定義 12.8. 体 K のあらゆる代数的拡大が分離的であるとき, K は 完全体 といはれる.

標数が 0 の体はどれも完全体である. したがつて $\mathrm{char}\, K = p > 0$ の場合を問題にする.

例題 12.9. $\mathrm{char}\, K = p > 0$, $\alpha \in \overline{K}$, $f(x) = \mathrm{irr}\,(\alpha, K, x)$ とする. 次が成り立つ.
(1) 分離的かつ既約な $q(x) \in K[x]$ と整数 $e \geq 0$ が存在して, $f(x) = q(x^{p^e})$ と表せる.
(2) 上の q, e に関し, $\overline{K}$ において α に K 上共役な元の個数は $\deg q$ に等しい. また α は $f(x)$ の p^e 重根で α^{p^e} は K 上分離的である.

証明 (1) $f(x)$ が分離的ならば $e = 0$, $q(x) = f(x)$ とすればよい. $f(x)$ が非分離的ならば, 12.2(2) より $f'(x) = 0$ となる. いま $f(x) = a_0 + a_1 x + \cdots + x^n$ とすれば $f'(x) = a_1 + \cdots + i a_i x^{i-1} + \cdots + n x^{n-1} = 0$ であることから $i a_i = 0$ である. 従つて $a_i \neq 0$ ならば $p|i$ でなければならないので, $f(x) = a_0 + a_p x^p + a_{2p} x^{2p} + \cdots$ となる. $q_1(x) = a_0 + a_p x + a_{2p} x^2 + \cdots$ とおけば $f(x) = q_1(x^p)$ で $f(x)$ の既約性から $q_1(x)$ も既約である. $q_1(x)$ が非分離的ならば, 同様にして $q_1(x) = q_2(x^p)$ となる $q_2(x)$ があり, $f(x) = q_2(x^{p^2})$ となる. これを続けてゆけば, 最後は $f(x) = q_e(x^{p^e})$ で $q_e(x)$ は分離的かつ既約となる.
(2) $\overline{K}$ 上で $q(x) = (x - \beta_1) \cdots (x - \beta_r)$ とすれば $f(x) = q(x^{p^e}) = (x^{p^e} - \beta_1) \cdots (x^{p^e} - \beta_r) = (x - {\beta_1}^{1/p^e})^{p^e} \cdots (x - {\beta_r}^{1/p^e})^{p^e}$ となり, その異なる根の個数は r で, 各根は p^e 重根である. また α^{p^e} は分離的な多項式 $q(x)$ の根であるから K 上分離的である. □

定義 12.10. 上の 12.9 で $r = \deg q$ を $f(x)$ の 被約次数 と呼び, p^e を $f(x)$ の 非分離次数 と呼ぶ. それらの積 rp^e は $n = \deg f$ に一致する. 一般に代数的拡大 L/K に対して, L から $\overline{K}$ の中への K 上の同型の個数を 分離次数 と呼び, $[\,L : K\,]_s$ で表す [15].

[15] 添字の s は separable (分離的) の最初の文字である.

単純拡大については, 次のことがわかる.

例題 12.11. 12.9 の仮定のもとで, $\mathrm{irr}\,(\alpha, K, x)$ の被約次数を r, 非分離次数を p^e とすれば, $r = [K(\alpha) : K]_s$ で

$$[\,K(\alpha) : K\,] = [\,K(\alpha) : K\,]_s\, p^e$$

が成り立つ. 特に α が K 上分離的であるためには $[\,K(\alpha) : K\,] = [\,K(\alpha) : K\,]_s$ が成り立つことが必要十分である. $\mathrm{char}\, K = 0$ のとき $e = 0$ であるが, $0^0 = 1$ と考へれば, 上の等式はそのときも成り立つ.

証明 12.9 の記号を用ゐ, 順に 5.8(2), 12.9, 9.7 と使つて

$$[K(\alpha) : K] = \deg\, f = \deg\, q \cdot p^e = [K(\alpha) : K]_s\, p^e$$

となつて正しい. □

例題 12.12. L/K は代数的拡大で Ω は代数的閉体であるとせよ. また $\sigma : K \to \Omega$ は中への同型とする. このとき, L から Ω の中への同型 $\rho : L \to \Omega$ で σ の拡張であるものの個数は $[\,L : K\,]_s$ に等しいことを示せ.

証明 9.5 により, $\sigma : K \to \Omega$ の $\overline{K}$ 上への拡張が存在する. その 1 つを固定し $\overline{\sigma} : \overline{K} \to \Omega$ とおく. また $[L : K]_s = r$ とおき $\{\,\sigma_i \,|\, i = 1, \cdots, r\,\}$ を L から $\overline{K}$ への中への同型の全体とせよ. このとき $\{\,\overline{\sigma}\sigma_i \,|\, i = 1, \cdots, r\,\}$ が σ の L 上への拡張 $L \to \Omega$ の全てである [16]. 実際, これらは互ひに異る写像であり, σ の任意の拡張 $\tau : L \to \Omega$ に対して $L^\tau \subset \overline{K}^{\sigma} = \overline{K}^{\overline{\sigma}}$ であることに注意すれば, $\overline{\sigma}\sigma_i = \tau$ となる σ_i が $(\overline{\sigma}|_{\overline{K}^\sigma})^{-1}\tau$ として存在するからである. よつて, L から Ω の中への同型 $\rho : L \to \Omega$ で σ の拡張であるものの個数も r である. □

例題 12.13. (1) 代数的拡大 L/K とその中間体 M に対して, 次が成り立つ :

$$[\,L : K\,]_s = [\,L : M\,]_s [\,M : K\,]_s$$

(2) L/K が有限次拡大ならば

$$[\,L : K\,] = [\,L : K\,]_s\, p^e$$

となる. 但し $p = \mathrm{char}\, K$ で e は非負整数である.

証明 (1) $\{\,\sigma_i : M \to \overline{K} \,|\, i \in I\,\}$ を M から $\overline{K}$ の中への K 上の同型の全体とせよ. このとき $|I| = [\,M : K\,]_s$ である. 各 σ_i に対し $\{\,\rho_{ij} : L \to \overline{K} \,|\, j \in J_i\,\}$ をその L への拡張の全体とすれば, 12.12 から $|J_i| = [\,L : M\,]_s$ となる. $\{\,\rho_{ij} \,|\, i \in I,\, j \in J\,\}$ は L から $\overline{K}$ の中への K 上の同型の全体と一致するから (1) の等式が成り立つ.

(2) $L = K(\alpha_1, \cdots, \alpha_n)$ で, 各 α_i は K 上代数的であるとしてよい. いま, $L_0 = K$, $L_i = K(\alpha_1, \cdots, \alpha_i)$ とおき, 体の列 $K = L_0 \subset L_1 \subset \cdots \subset L_n = L$ を考へて, (5.3) を繰り返し用ゐてから 12.11 を使ひ, さらに (1) を繰り返し使へば,

$$[\,L : K\,] = \prod_{i=1}^{n} [\,L_i : L_{i-1}\,] = \prod_{i=1}^{n} [\,L_i : L_{i-1}\,]_s\, p^{e_i} = \left(\prod_{i=1}^{n} [\,L_i : L_{i-1}\,]_s \right) \cdot p^{\sum_i e_i} = [\,L : K\,]_s\, p^e$$

を得る. ここに $e = \sum_i e_i$. □

[16] この教科書では 2 つの写像 σ と τ の合成写像 $\tau \circ \sigma$ を $\tau\sigma$ と書くことにする.

有限次拡大 L/M に対して, $[\,L:K\,]/[\,L:K\,]_s$ を $[\,L:K\,]_i$ と書いて[17], これを L/K の非分離次数 と呼ぶ. 従つて

$$[L:K]=[L:K]_s\,[L:K]_i$$

である. 上の例題から $[\,L:K\,]_i$ は K の標数 p の冪である. また $K\subset M\subset L$ のとき, $[\,L:K\,]_i=[\,L:M\,]_i[\,M:K\,]_i$ が成り立つ.

有限次拡大の分離性について, 次の定理が成り立つ.

定理 12.14. $L=K(\alpha_1,\ldots,\alpha_n)$ を K の有限次拡大とせよ. 次の 4 つは同値である.
(1) L/K は分離的拡大である.
(2) α_i $(1\le i\le n)$ はすべて K 上分離的である.
(3) 各 α_i は $K(\alpha_1,\cdots,\alpha_{i-1})$ 上分離的である.
(4) $[\,L:K\,]=[\,L:K\,]_s$.

証明 (1)⇒(2). 分離的拡大の定義より明らかである. (2)⇒(3). 12.5 より明かである. (3)⇒(4). 12.13(2) の証明において, 各 $e_i=0$ となるから $e=0$ となる. (4)⇒(1). 対偶を証明する. L は K 上非分離的な元 α を含むと仮定する. 体の列 $K\subset K(\alpha)\subset L$ において

$$[K(\alpha):K]>[K(\alpha):K]_s,\quad [L:K(\alpha)]\ge[L:K(\alpha)]_s$$

となるから, $[L:K]>[L:K]_s$ を得る. □

例題 12.15. 体の列 $K\subset M\subset L$ において, M/K, L/M がともに分離的拡大ならば L/K も分離的拡大である. また, この逆も成り立つ.

証明 逆は 12.5 に他ならない. そこで, M/K, L/M はともに分離的であるとする. $\alpha\in L$ に対して $\mathrm{irr}\,(\alpha,M,x)=x^n+\alpha_1x^{n-1}+\cdots+\alpha_n$ $(\alpha_i\in M)$ とすれば, これは重根を持たない. よつて $K(\alpha_1,\cdots,\alpha_n,\alpha)$ は 12.14(3) の条件をみたし, K 上分離的である. 特に α は K 上分離的で, L/K は分離的である. □

問 12.16. M, M' が代数的拡大 L/K の中間体であるとき, 次のことを示せ.
(1) M/K が分離的ならば, MM'/M' も分離的. (即ち, 拡大の分離性は持ち上げによつて保たれる.)
(2) M/K, M'/K がともに分離的ならば, MM'/K も分離的である.

自明でない代数的拡大 L/K において, K 上分離的な L の元の全体を L_s で表す. ここで 12.14 (2)⇒(1) により, α, $\beta\in L_s$ ならば $K(\alpha,\beta)$ は K 上分離的で, 従つて $\alpha\pm\beta$, $\alpha\beta\in L_s$ で $\alpha\beta^{-1}\in L_s$ $(\beta\neq0)$ となり, L_s は L の部分体である. 実際 L_s は K 上分離的な L/K の中間体のうち最大なもので, これを K の L における 分離閉包 といふ. また $L_s=K$ となるとき, 拡大 L/K を 純非分離的拡大 であるといふ.

例題 12.17. $\mathrm{char}\,K=p>0$ とする. 自明でない代数的拡大 L/K について, 次の 3 つは同値である.
(1) L/K は純非分離的拡大である.
(2) 任意の $\alpha\in L$ に対し, $\alpha^{p^e}\in K$ となる $e\ge0$ がある.
(3) $[L:K]_s=1$.

[17] i は inseparable (非分離的) の頭文字

証明 (1)⇒(2). 12.9 (2) より, ある $e \geq 0$ に対し α^{p^e} は K 上分離的ゆえ, $\alpha^{p^e} \in K$ となる.
(2)⇒(3). L を含む K の代数的閉包を $\overline{K}$ とし, $\sigma : L \to \overline{K}$ を中への K 上の同型とする. $\alpha \in L$ に対して $\alpha^{p^e} \in K$ とすれば $(\alpha^{p^e})^\sigma = \alpha^{p^e}$ ゆえ, $(\alpha^\sigma - \alpha)^{p^e} = (\alpha^\sigma)^{p^e} - \alpha^{p^e} = (\alpha^{p^e})^\sigma - \alpha^{p^e} = 0$ となり, $\alpha^\sigma = \alpha$. 従つて σ は L の各元をそれ自身に写す. よつて $[L : K]_s = 1$ となる.
(3)⇒(1). L_s/K は分離的であるから 12.14(4) および 9.5 より, $[L_s : K] = [L_s : K]_s \leq [L : K]_s = 1$ ゆえ $L_s = K$ である. □

例題 12.18. L/K を代数的拡大, L_s を L における K の分離閉包とするとき,
(1) $L = L_s$ であるか, または L/L_s は純非分離的拡大である. 特に, $(L_s)_s = L_s$ である.
(2) L/K が有限次拡大ならば, 次の等式が成り立つ :

$$[L : K]_s = [L_s : K], \quad [L : K]_i = [L : L_s].$$

証明 (1) L_s 上分離的な L の元は K 上分離的であるから, 明らかである.
(2) $[L : K]_s = [L : L_s]_s [L_s : K]_s$ において, (1) と 12.17 より $[L : L_s]_s = 1$. また L_s/K は分離的であるから $[L_s : K]_s = [L_s : K]$ となり, $[L : K]_s = [L_s : K]$ である. $[L : K]_i$ については明らかである. □

演 習 問 題

12.19. ($[L : K]$ と $[L : K]_s$ が異なる例) t は不定元とし, $K = \mathbb{F}_5(t^{25})$,

$$f(x) = x^{75} + t^{25}x^{50} + 2\,t^{50}x^{25} - t^{75}$$

とおく. 体 $L = \mathbb{F}_{25}(t)$ は $f(x)$ の K 上の最小分解体であること示せ. また $[L : K]_s$, $[L : K]_i$, $[L : K]$ はそれぞれいくつか.

12.20. $\mathbb{F}_5(t)$ の部分体 $K = \mathbb{F}_5(t^5)$ を考へる. 多項式 $f(x) = \mathrm{irr}\,(t+1, K, x)$, $g(x) = \mathrm{irr}\,(t^2+t+1, K, x)$ を求めよ. $g(x) = 0$ の 1 つの根を α とし, $L = K(\alpha)$ とおく. $[L, K]_s$ はいくらか. (Hint : 6.6)

12.21. 3 つの体 $L \supset M \supset K$ について, L/M は正規拡大, M/K は純非分離的拡大である. このとき, L/K は正規拡大であることを示せ.

13. 分離的拡大の単純性

有限次の分離的拡大は単純拡大である. もつと一般に次の定理が成り立つ.

定理 13.1. 体 K の有限次拡大 $L = K(\alpha_1, \cdots, \alpha_{n-1}, \alpha_n)$ において α_1, ..., α_{n-1} がすべて K 上分離的ならば, $L = K(\theta)$ となる $\theta \in L$ がある.

証明 K が有限体ならば L も有限体で, その乗法群 $L^\times = L - \{0\}$ は,「代数学 1」の系 13.6 より, 巡回群である. $L^\times = \langle\theta\rangle$ とすれば, 明らかに $L = K(\theta)$ である.

また, 主張は $n = 2$ のときに示されれば, 一般の場合は n に関する帰納法で示される. 実際, $K(\alpha_1, \cdots, \alpha_{n-2}, \alpha_n) = K(\beta)$ となれば, $L = K(\alpha_{n-1}, \beta)$ となるから, $n = 2$ の場合に帰着する.

よつて以下では K を無限体とし, $L = K(\alpha, \beta) \subset \overline{K}$, α は K 上分離的であると仮定する. $[L : K]_s = m$ とし, $\sigma_i : L \to \overline{K}$ $(1 \le i \le m)$ を中への異なる K 上の同型とする. このとき $i \neq j$ ならば $\alpha^{\sigma_i} \neq \alpha^{\sigma_j}$ か $\beta^{\sigma_i} \neq \beta^{\sigma_j}$ となるから, x についての多項式

$$f(x) := \prod_{i \neq j} \big((\alpha^{\sigma_i} - \alpha^{\sigma_j}) + (\beta^{\sigma_i} - \beta^{\sigma_j})x\big)$$

は [18] 0 と異なる. $f(x) = 0$ の根は有限個であるが, $|K| = \infty$ であるから, $f(c) \neq 0$, $c \neq 0$ なる元 $c \in K$ がある. このとき $i \neq j$ ならば

$$0 \neq (\alpha^{\sigma_i} - \alpha^{\sigma_j}) + (\beta^{\sigma_i} - \beta^{\sigma_j})c = (\alpha + c\beta)^{\sigma_i} - (\alpha + c\beta)^{\sigma_j}.$$

よつて $\theta = \alpha + c\beta$ とおけば

$$i \neq j \Rightarrow \theta^{\sigma_i} \neq \theta^{\sigma_j}$$

となり, θ は少なくとも m 個の K 上共役な元を持つ. 従つて $m \le [K(\theta) : K]_s \le [L : K]_s = m$ となり, $[K(\theta) : K]_s = [L : K]_s$ を得る. いま L_s, $K(\theta)_s$ をそれぞれ L, $K(\theta)$ における K の分離閉包とすれば, $K(\theta)_s \subset L_s$ であるが, 上の等式と 12.18(2) より $\alpha \in L_s = K(\theta)_s \subset K(\theta)$ である. また $\beta = c^{-1}(\theta - \alpha) \in K(\theta)$ となるから $K(\alpha, \beta) \subset K(\theta)$ を得る. □

演 習 問 題

13.2. 次のそれぞれの拡大について, 単純拡大として生成する元を 1 つ求めよ.
(1) $\mathbb{Q}(\sqrt{2}, \sqrt{5})/\mathbb{Q}$
(2) $\mathbb{Q}(\sqrt{2}, \sqrt{3}, i)/\mathbb{Q}$

[18] $f(x) \in K(\beta)_s[x]$ となるが, ここではそれは必要ない.

14. 完全体

前に 12.7 で述べた様に, 標数 0 の体はすべて完全体であるから, この節では $\operatorname{char} K = p > 0$ なる体 K についてのみ考へる. $\overline{K}$ を K の代数的閉包とする. また

$$K^p = \{\, a^p \mid a \in K \,\}, \quad K^{1/p} = \{\, a^{1/p} \in \overline{K} \mid a \in K \,\} = \{\, \alpha \in \overline{K} \mid \alpha^p \in K \,\}$$

と記すことにすると, これらは体であつて, $K^p \subset K \subset K^{1/p}$ となつてゐる.

定理 14.1. 次の 3 つの条件は同値である.

(1) K は完全体である.

(2) $K^{1/p} = K$.

(3) $K^p = K$.

証明 (1)⇒(2). K が完全体ゆゑ $K^{1/p}/K$ 純非分離的拡大ではあり得ず, 12.17 より $K^{1/p} = K$ となる.

(2)⇒(3). $a \in K$ を任意にとれば $a = (a^{1/p})^p$. ここで $K = K^{1/p}$ ならば $a^{1/p} \in K$ ゆゑ, $a \in K^p$ となる.

(3)⇒(1). $\alpha \in \overline{K}$ が K 上非分離的であれば,

$$f(x) := \operatorname{irr}(\alpha, K, x) = (x^p)^m + a_1(x^p)^{m-1} + \cdots + a_m \quad (\, a_i \in K \,)$$

となる. ここで各 a_i に対し ${b_i}^p = a_i$ なる $b_i \in K$ があるから

$$f(x) = (x^m + b_1 x^{m-1} + \cdots + b_m)^p$$

となり, $f(x)$ の既約性に矛盾する. よつて $\overline{K}/K$ は分離的である. □

例題 14.2. 有限体は完全体である.

証明 K 有限体とし, その標数 $p > 0$ とせよ. このとき $\sigma : K \to K$ $(a \mapsto a^p)$ は単射であるが, $|K| < \infty$ により全射となる. よつて K は 14.1 の条件を満たす. □

演 習 問 題

14.3. p を素数, t を不定元とせよ. 体 $\mathbb{F}_p(t)$ の上の非分離的拡大体を 1 つ挙げ, この体が完全体でないことを示せ.

14.4. p を素数, t を不定元とせよ. $L = \bigcup_{n=1}^{\infty} \mathbb{F}_p(t^{1/p^n})$ は完全体であることを示せ.

15. Artin の定理

ここでは次節に述べる Galois の基本定理の証明の核心部分となる事柄を述べる.

定義 15.1. 代数的拡大 L/K (有限次とは限らない) が分離的かつ正規であるとき, これを Galois 拡大 と呼び, $\mathrm{Aut}\, L/K$ をその Galois 群 と呼んで $\mathrm{Gal}\,(L/K)$ で表す.

命題 15.2. M, M' を拡大 L/K の中間体とせよ. M'/K が Galois 拡大ならば MM'/M も Galois 拡大である. さらに M/K も Galois 拡大ならば MM'/K は Galois 拡大.

証明 前半は, 正規性も分離性も拡大に関する持ち上げによつて保たれる (11.4 (3) と 12.16 (1)) からである. 後半は 11.4(2) と 12.16(2) からわかる. □

定義 15.3. 一般に拡大 L/K に対して, $G = \mathrm{Aut}\, L/K$ とおく.
(1) G の部分群 H をとり固定する. このとき, 体 L^H を次の様に定める :

$$L^H = \{\, \alpha \in L \mid \alpha^\sigma = \alpha \ \ (\forall \sigma \in H) \,\}.$$

これを L における H の 不変体 と呼ぶ.
(2) 逆に, 拡大 L/K の中間体 M に対して, G の部分集合 G^M を次の様に定める :

$$G^M = \{\, \sigma \in G \mid \alpha^\sigma = \alpha \ \ (\forall \alpha \in M) \,\}.$$

これは G の部分群であり, G における M の 不変群 と呼ばれる. 特に $G^K = G$.

問 15.4. 上の集合 L^H が体であり, G^M が G の部分群であることを示せ.

例題 15.5. L/K は Galois 拡大, M をその中間体とすれば, L/M はまた Galois 拡大で,

$$\mathrm{Gal}\,(L/M) = \mathrm{Gal}\,(L/K)^M$$

となることを示せ.

証明 15.2 により $L/M = ML/M$ は Galois 拡大であり, $\mathrm{Gal}\,(L/M) \subset \mathrm{Gal}\,(L/K) = G$ であるが, $\sigma \in G$ に対し $\sigma \in \mathrm{Gal}\,(L/M) \iff \alpha^\sigma = \alpha\ (\forall \alpha \in M) \iff \sigma \in G^M$ となる. □

命題 15.6. L/K を有限次 Galois 拡大, $G = \mathrm{Gal}\,(L/K)$ とする. 次が成り立つ.
(1) $[L : K] = [L : K]_s = |G|$.
(2) $L^G = K$. より一般的に L/K の中間体 M について $\boxed{L^{G^M} = M}$.

証明 (1) 分離性より $[L : K] = [L : K]_s$. また L を含む K の代数的閉包を $\overline{K}$ とし, $\sigma : L \to \overline{K}$ を $\overline{K}$ の中への K 上の同型とすれば, 正規性により $L^\sigma = L$ となる. よつて σ の値域を L に制限して $\sigma : L \xrightarrow{\sim} L$ なる $\mathrm{Gal}\,(L/K)$ の元が得られる. 逆に $\mathrm{Gal}\,(L/K) \ni \rho : L \xrightarrow{\sim} L$ の値域を $\overline{K}$ に拡張すれば中への K 上の同型 $\rho : L \to \overline{K}$ が得られる. 従つて $|\mathrm{Gal}\,(L/K)| = [L : K]_s$ である.
(2) $K \subset L^G \subset L$ で, 15.5 により L/L^G は Galois 拡大で, $\mathrm{Gal}\,(L/L^G) = G^{L^G} = G$ (G は L^G ($\supset K$) の元を動かさないから) であり, (1) より $[L : L^G] = |\mathrm{Gal}(L/L^G)| = |G| = [L : K]$ ゆゑ, $L^G = K$ である. 15.5 より $G^M = \mathrm{Gal}(L/M)$. G を G^M に取り換へて同じ議論を行へば後半を得る. □

定理 15.7. （E. Artin） L を体, G を $\mathrm{Aut}\, L$ の有限部分群とし, $K = L^G$ とおく. 次が成り立つ.
(1) L/K は有限次 Galois 拡大である.
(2) $\mathrm{Gal}\,(L/K) = G$.
(3) $[L : K] = |G|$.

注意 15.8. $|G| = \infty$ のときは, 15.7 の (1), (2), (3) は必ずしも成立しない.

この定理を示すために次の補題を用意する.

補題 15.9. 代数的拡大 L/K は分離的とし, n を固定された自然数とする. このとき, すべての $\alpha \in L$ に対して $[K(\alpha) : K] \leq n$ が成り立つならば, $[L : K] \leq n$ である.

証明 13.1 より, ある $\gamma \in L$ によつて $L = K(\gamma)$ と書けるから. □

これを用ゐて 15.7 の証明を行なふ.

証明 任意に $\alpha \in L$ とる. α を含む G 軌道を $\alpha^G = \{\alpha = \alpha_1, \alpha_2, \cdots, \alpha_r\}$ とし, $f(x) = \prod_{i=1}^{r}(x - \alpha_i) = x^r + c_1 x^{r-1} + \cdots + c_r$ とおく. このとき, $r \leq |G|$ で, 任意の $\sigma \in G$ に対して $f^\sigma(x) = \prod_{i=1}^{r}(x - \alpha_i{}^\sigma) = f(x)$ となるから, 各 $c_i \in L^G = K$ となり, $f(x) \in K[x]$ である. $f(\alpha) = 0$ であるから, $\mathrm{irr}\,(\alpha, K, x) | f(x)$ である. ここで $f(x)$ は重根を持たないから α は K 上分離的で, したがつて L/K は分離的拡大である. また $\mathrm{irr}\,(\alpha, K, x)$ は L 上で 1 次式の積に分解でき, α は L の任意の元であつたから, 11.1(2), 11.3 により L/K は正規拡大, よつて Galois 拡大である. 上の議論から $[K(\alpha) : K] = \deg \mathrm{irr}\,(\alpha, K, x) \leq r \leq |G|$ $(\forall \alpha \in L)$ となるから, 15.9 により, $[L : K] \leq |G|$ となる. 一方 $G \subset \mathrm{Gal}(L/K)$ で, 15.6(1) より $[L : K] = |\mathrm{Gal}(L/K)|$ であるから $G = \mathrm{Gal}(L/K)$ で $[L : K] = |G|$ でなくてはならない. □

演 習 問 題

15.10. 体 K の拡大体の元 α と $\alpha+1$ が K 上共役であれば, $\operatorname{char} K \neq 0$ であることを示せ.

15.11. (Artin-Schreier の拡大) p を素数, $f(x)=x^p-x-1\in\mathbb{F}_p[x]$ とする.

(1) $f(x)=0$ の 1 つの根を α とせよ. このとき, $\operatorname{Aut}\mathbb{F}_p(\alpha)/\mathbb{F}_p$ は $\alpha\mapsto\alpha+r$ ($r=0, 1, \cdots, p-1$) で尽されることを示せ.

(2) 多項式 $f(x)$ は $\mathbb{F}_p$ 上既約であること, および $\mathbb{F}_p(\alpha)/\mathbb{F}_p$ が Galois 拡大であることを示せ. (16.7 の特殊な場合)

15.12. 体 $L=\mathbb{Q}(\sqrt{2},\sqrt{3})$ を考へる. 次の問に答へよ.

(1) 拡大 $L/\mathbb{Q}$ が Galois 拡大であることを示せ, さらに, 任意の a, b, $c\in\mathbb{Q}$ に対して,

$$\sigma: a+b\sqrt{2}+c\sqrt{3}\mapsto a-b\sqrt{2}+c\sqrt{3},\quad \tau: a+b\sqrt{2}+c\sqrt{3}\mapsto a+b\sqrt{2}-c\sqrt{3}$$

は L の $\mathbb{Q}$ 上の自己準同型であり, $\operatorname{Gal}(L/\mathbb{Q})=\{\,\mathrm{id},\sigma,\tau,\sigma\tau\,\}$ であることを示せ.

(2) $\operatorname{Gal}(L/\mathbb{Q})$ の部分群を全て求めよ.

(3) (2) の各部分群について, その不変体を求めよ.

15.13. $\alpha=\exp(2\pi i/7)+\exp(-2\pi i/7)$ とおくとき,

(1) $\operatorname{irr}(\alpha,\mathbb{Q},x)=x^3+x^2-2x-1$ であることを示せ.

(2) $\exp(2\pi i/7)\mapsto\exp(4\pi i/7)$ は $\mathbb{Q}(\alpha)$ の $\mathbb{Q}$ 上の自己同型を与へることを示せ.

(3) 上の自己同型を σ とおく. α^σ を α の有理式で書け. それを $\varphi(\alpha)$ とするとき, $\alpha^{\sigma^2}=\varphi(\varphi(\alpha))$, $\sigma^3=\mathrm{id}$ であることを示せ.

(4) 拡大 $\mathbb{Q}(\alpha)/\mathbb{Q}$ が Galois 拡大であり, $\operatorname{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ は位数 3 の巡回群であることを示せ.

15.14. $\mathbb{Q}$ に係数を持つ既約多項式 $f(x)$ の $\mathbb{Q}$ 上の最小分解体を K とするとき, Galois 群 $\operatorname{Gal}(K/\mathbb{Q})$ は `paridroid` で簡単に求められる. 以下の入力を試してみよ.

(1) `? polgalois(x^4-4*x-1)`

(2) `? polgalois(x^4+x^3+x^2+x+1)`

(3) `? polgalois(x^5-2*x^4+x^3+x^2-x+1)`

(4) `? polgalois(x^5-2)`

16. Galois の基本定理

拡大 L/K の中間体の全体を $\mathscr{F}(L/K)$ で表し, 群 G の部分群の全体を $\mathscr{G}(G)$ で表す[19]. このとき, 次の定理が我々が目標としてきたものである.

定理 16.1. (Galois の基本定理 1) L/K を有限次 Galois 拡大とし, $G = \mathrm{Gal}\,(L/K)$ とする. このとき, G の部分群にその不変体を対応させる写像

$$\varphi : \mathscr{G}(G) \longrightarrow \mathscr{F}(L/K), \qquad H \longmapsto L^H$$

は全単射で, $H \in \mathscr{G}(G)$, $M \in \mathscr{F}(L/K)$ に対して

(1) $\mathrm{Gal}\,(L/L^H) = H$. 特に $[L : L^H] = |H|$ である.

(2) $\varphi^{-1}(M) = G^M$. 従つて $H = G^{L^H}$, $M = L^{G^M}$ が成り立つ.

注意 16.2. (1) $\{1\} < H_1 < H_2 < G$ ならば $L^{H_1} \supset L^{H_2}$ であるから, 上の φ は包含関係を逆転させる全単射である.

(2) 全射性は比較的易しいが, 単射性はやや面倒 (Artin の定理が必要) である.

証明 $M \in \mathscr{F}(L/K)$ に対し, 15.5 より, L/M は Galois 拡大で $\mathrm{Gal}(L/M) = G^M$ であるから, $M = L^{G^M} = \varphi(G^M)$ (15.6(2) による). よつて φ は全射である.

次に 15.7 (Artin の定理) により, $H \in \mathscr{G}(G)$ に対し, L/L^H は Galois 拡大で, $\mathrm{Gal}(L/L^H) = H$, $[L : L^H] = |H|$ となる. 一方 15.5 により, L/K の中間体 M に対し $\mathrm{Gal}(L/M) = G^M$ である. よつて $H \in \mathscr{G}(G)$ に対して $\boxed{H = \mathrm{Gal}(L/L^H) = G^{L^H}}$ となる. 特に H_1, $H_2 \in \mathscr{G}(G)$ で $L^{H_1} = L^{H_2}$ ならば, $H_1 = G^{L^{H_1}} = G^{L^{H_2}} = H_2$ となつて φ は単射である. □

定理 16.3. (Galois の基本定理 2) 有限次 Galois 拡大 L/K とその中間体 M について次が成り立つ.

(1) $\tau \in \mathrm{Gal}\,(L/K)$ に対し, $\tau\,\mathrm{Gal}\,(L/M)\tau^{-1} = \mathrm{Gal}\,(L/M^\tau)$.

(2) M は K の Galois 拡大 $\iff$ $\mathrm{Gal}\,(L/M) \lhd \mathrm{Gal}\,(L/K)$.

(3) (2) の両側が成り立つとき, $\mathrm{Gal}\,(M/K) \simeq \mathrm{Gal}\,(L/K)\,/\,\mathrm{Gal}\,(L/M)$ (群としての同型).

証明 (1) 一般に $M \in \mathscr{F}(L/K)$, $\tau \in G = \mathrm{Gal}(L/K)$ に対して

$$\begin{aligned} G^{M^\tau} &= \{\,\sigma \in G \,|\, \alpha^\sigma = \alpha \ (\forall \alpha \in M^\tau)\,\} = \{\,\sigma \in G \,|\, (\beta^\tau)^\sigma = \beta^\tau \ (\forall \beta \in M)\,\} \\ &= \{\,\sigma \in G \,|\, \beta^{\tau^{-1}\sigma\tau} = \beta \ (\forall \beta \in M)\,\} = \{\,\tau\rho\tau^{-1} \in G \,|\, \beta^\rho = \beta \ (\forall \beta \in M)\,\} = \tau\, G^M\, \tau^{-1} \end{aligned}$$

である. ($\tau\rho\tau^{-1} \in G \iff \rho \in \tau^{-1}G\tau = G$ に注意)

(2) の ($\Rightarrow$). M/K は正規拡大であるから, すべての $\tau \in G$ に対して $M^\tau = M$ となる. よつて $\tau G^M \tau^{-1} = G^{M^\tau} = G^M$ となり, $G^M \lhd G$ である.

(2) の ($\Leftarrow$). 任意の $\tau \in G$ に対して $G^M = \tau\, G^M \tau^{-1} = G^{M^\tau}$ ゆゑ 16.1(2) から $M^\tau = M$.

(3) G の元の M への制限の全体を $G' = \{\,\sigma|_M \,|\, \sigma \in G\}$ とする. ここで $\sigma \mapsto \sigma|_M$ により定義される写像 $G \to G'$ は全射で, その核は G^M に他ならない. よつて $G/G^M \simeq G'$ (群として同型) である. また, $M^{G'} = K$ であるから 15.7(1), (2) により M/K は Galois 拡大で, $\mathrm{Gal}(M/K) = G' \simeq G/G^M$ となる. □

[19] $\mathscr{F}$ は F の, $\mathscr{G}$ は G の script 体.

定義 16.4. Galois 拡大 L/K に対し, $\mathrm{Gal}\,(L/K)$ が Abel 群であるとき, L/K は Abel 拡大 であるといはれる. また, $\mathrm{Gal}\,(L/K)$ が巡回群であるとき, L/K は 巡回拡大 であるといはれる.

命題 16.5. 体 M, M' は拡大 L/K の中間体であるとする. 次が成り立つ :

(1) M'/K が Galois 拡大であれば MM'/M も Galois 拡大であり,

$$\mathrm{Gal}\,(MM'/M) \simeq \mathrm{Gal}\,(M/M\cap M').$$

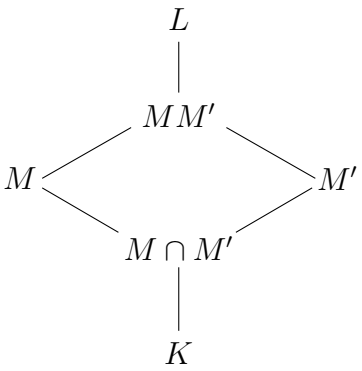
この時, 特に $[\,MM' : M\,] = [\,M : M\cap M'\,]$ である.

(2) M, M' がともに K の Abel 拡大ならば, MM'/K も Abel 拡大である.

証明 (1) 15.2 により, MM'/M は Galois 拡大である. $\sigma \in \mathrm{Gal}\,(MM'/M)$ とすれば, その M' への制限 $\sigma|_{M'}$ は $\mathrm{Gal}\,(M'/M\cap M')$ の元で, 写像

$$f \ :\ \mathrm{Gal}\,(MM'/M) \to \mathrm{Gal}\,(M'/M\cap M')$$
$$\sigma \ \mapsto\ \sigma|_{M'}$$

は群の準同型である. $\mathrm{Gal}\,(MM'/M)$ の元 σ は M' の元の像で決まるから, f は単射である. また $H = \mathrm{Im}\, f$ の不変体は,



$$M'^{H} = \{\alpha \in M' \,|\, \alpha^{\sigma} = \alpha \ (\,\forall\sigma \in \mathrm{Gal}\,(MM'/M)\,)\,\}$$

である. また

$$M = \{\alpha \in MM' \,|\, \alpha^{\sigma} = \alpha \ (\,\forall\sigma \in \mathrm{Gal}\,(MM'/M)\,)\,\}$$

であるから $M'^{H} = M\cap M'$. よつて 16.1(1) より, $H = \mathrm{Gal}\,(M'/M\cap M')$ であり, f は全射である.

(2) 15.2 の後半より MM'/K は Galois 拡大である. $\mathrm{Gal}\,(MM'/K) = G$ とおくと $G^{M'} \lhd G$, $G^{M} \lhd G$ である. また, $G/G^{M'} \simeq \mathrm{Gal}\,(M'/K)$, $G/G^{M} \simeq \mathrm{Gal}\,(M/K)$ で, これらは仮定から Abel 群である. それゆゑ, 交換子群について $[G,G] \subset G^{M}\cap G^{M'} = G^{MM'} = \{1\}$ であることがわかり, G は Abel 群である. □

例 16.6. 体 K 上の n 次の多項式 $f(x)$ は重根を持たないとし, α_1, $\cdots$, α_n を $f(x)$ の $\overline{K}$ における根の全体とする : $f(x) = c(x-\alpha_1)\cdots(x-\alpha_n)$. このとき $f(x)$ の最小分解体 $L = K(\alpha_1,\cdots,\alpha_n)$ は K の Galois 拡大である. Galois 群 $G = \mathrm{Gal}\,(L/K)$ を多項式 $f(x)$ の K 上の Galois 群 と呼ぶ. $\sigma \in G$ は K 同型であるから $f^{\sigma}(x) = f(x)$ となり, σ は n 個の元からなる集合 $\{\alpha_1,\cdots,\alpha_n\}$ に置換 $\sigma' = \begin{pmatrix} \alpha_1 & \cdots & \alpha_n \\ {\alpha_1}^{\sigma} & \cdots & {\alpha_n}^{\sigma} \end{pmatrix} \in S_n$ として作用[20] するので, 単射 $\varphi : G \longrightarrow S_n$ が定まる. ゆゑに G は S_n の部分集合と同型である. 特に $[L:K] = |G| \le n!$ である.

[20] 26.1 を見よ.

演 習 問 題

16.7. $f(x) \in K[x]$ は分離的であるとする. G を $f(x)$ の K 上の Galois 群とする. また, $\{\alpha_1, \cdots, \alpha_n\}$ を $f(x)$ の $\overline{K}$ における根の全体とする. このとき, 次を示せ :

$f(x)$ が既約多項式 $\iff$ G が $\{\alpha_1, \cdots, \alpha_n\}$ 上に可移的[21] に作用する.

16.8. 有限次分離的拡大 L/K に対し L を含む K の有限次 Galois 拡大が存在することを示せ.

16.9. 次の $\zeta \in \mathbb{C}$ について $\mathrm{Gal}\,(\mathbb{Q}(\zeta)/\mathbb{Q})$ とその部分群, および, それらに対応する $\mathbb{Q}(\zeta)$ の部分体を求めよ.

(1) $\zeta = \exp\dfrac{2\pi i}{8}$ (2) $\zeta = \exp\dfrac{2\pi i}{5}$ (3) $\zeta = \exp\dfrac{2\pi i}{15}$

16.10. $\alpha = \sqrt{6+3\sqrt{2}+2\sqrt{3}+2\sqrt{6}}$ とおく. 4.8 の拡大 $\mathbb{Q}(\alpha)/\mathbb{Q}$ は Galois 拡大である. その理由を述べよ. そこでの記号で ${\sigma_1}^+ = \sigma$, ${\sigma_2}^+ = \tau$ とおき, $G = \mathrm{Gal}\left(\mathbb{Q}(\alpha)/\mathbb{Q}\right)$ を σ, τ で記述せよ. また, この拡大に関し, Galois の基本定理により G の交換子群 $D(G) = [G, G]$ に対応する中間体を求めよ. さらに, G のすべての部分群に対応する中間体を求めよ.

16.11. K を体とし, $a \in K$ について $b = 1 + a^2 \in K$ が K の元の平方ではないとする. このとき $\mathrm{char}\,K \neq 2$ で $\mathrm{Gal}\left(K(\sqrt{b+\sqrt{b}}\,)/K\right)$ は 4 次の巡回群であることを示せ.

(Hint : $\beta = \sqrt{b+\sqrt{b}}$ とおく. $[K(\beta) : K] = 4$ が確かめられれば, $\beta^\sigma = -\sqrt{b-\sqrt{b}}$ なる $\mathrm{Gal}\left(K(\beta)/K\right)$ の元 σ が存在する. このとき β^{σ^2}, β^{σ^3} を調べよ.)

16.12. 多項式 $f(x) = x^3 - 6x + 2$ について問に答へよ.

(1) $f(x) = 0$ の解を $\omega = \frac{-1+\sqrt{3}i}{2}$ と平方根号 $\sqrt{\ }$, $\sqrt[3]{\ }$ および四則演算だけで表せ.
(Hint : 恒等式 $x^3 + y^3 + z^3 - 3xyz = (x + y + z)(x + \omega y + \omega^2 z)(x + \omega^2 y + \omega z)$ を利用する.)

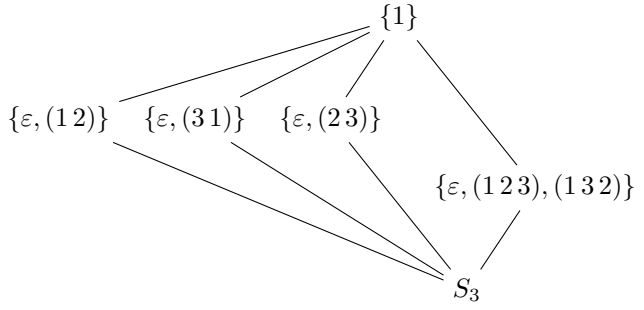
(2) $f(x)$ の最小分解体を L とし, $K = \mathbb{Q}(\omega)$ とする. $\mathrm{Gal}\,(L/K)$ が $\{1, 2, 3\}$ に関する 3 次対称群 S_3 と次の対応で同型であることを示せ. 即ち, $f(x) = 0$ の 3 つの解を t_1, t_2, t_3 とするとき, $\sigma \in S_3$ を ${t_i}^\sigma = t_{\sigma(i)}$ で $\mathrm{Gal}\,(L/K)$ の元と見做して, $S_3 \simeq \mathrm{Gal}\,(L/K)$.
(Hint : $\Delta = (t_1 - t_2)(t_2 - t_3)(t_3 - t_1)$ を求め, $K(\Delta)$ に対応する $\mathrm{Gal}\,(L/K)$ の部分群を考察せよ.)

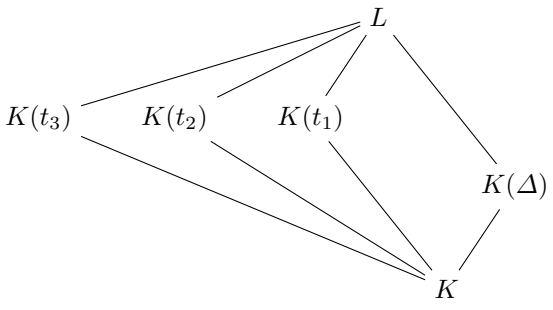
(3) $H = \{\varepsilon, (1\,2)\} < S_3$ に対応する体 M を求めよ. $\tau = (1\,3)$ のとき

$$(\ \tau\,\mathrm{Gal}\,(L/M)\tau^{-1} = \ )\ \ \tau H \tau^{-1} = \mathrm{Gal}\,(L/M^\tau)$$

であることを確かめよ.

参考のために, 以上の内容を図示しておく.





[21] 26.1 を見よ.

17. 有限体

有限体についてまとめておく.

命題 17.1. p を任意の素数とし, n を任意の自然数とする. このとき $|F| = p^n$ なる有限体 F が存在する. この様な F は素体 $\mathbb{Z}/p\mathbb{Z}$ 上の, 多項式 $x^{p^n} - x$ の最小分解体に同型である. 従つて, その様な体 F は同型を度外視して一意的に存在する.

証明 $\overline{\mathbb{F}_p}$ を $\mathbb{F}_p$ の代数的閉包とし, $F = \{\, \alpha \in \overline{\mathbb{F}_p} \,|\, \alpha^{p^n} = \alpha \,\}$ とおけば, F が体になることは容易に確かめられる. F は多項式 $f(x) = x^{p^n} - x$ の根の全体で, $f'(x) = -1$ と $f(x)$ の共通根は存在しないから $f(x)$ は重根を持たず, $|F| = p^n$ となる. 一方 K を元の個数が p^n の任意の有限体とせよ. 5.4(2) により K は $x^{p^n} - x$ の $\mathbb{F}_p$ の最小分解体で $K \simeq F$ となる. □

上の 17.1 で得られた体 F を $\mathbb{F}_{p^n}$ で表す. 特に $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ である. 以後, 素体 $\mathbb{F}_p$ の代数的閉包 $\overline{\mathbb{F}_p}$ を 1 つ決めて固定し, あらゆる $\mathbb{F}_{p^n}$ $(n \in \mathbb{N})$ は $\overline{\mathbb{F}_p}$ の部分体であるものとする :

$$\mathbb{F}_{p^n} = \{\, \alpha \in \overline{\mathbb{F}_p} \,|\, \alpha^{p^n} = \alpha \,\}.$$

例題 17.2. 次を示せ. $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m} \iff n|m$.

証明 $(\Rightarrow)$ $[\mathbb{F}_{p^m} : \mathbb{F}_{p^n}] = d$ とすれば, $|\mathbb{F}_{p^m}| = |\mathbb{F}_{p^n}|^d = p^{nd}$ であるから $m = nd$ となる.
$(\Leftarrow)$ $m = nd$ $(d \in \mathbb{N})$ とし, $q = p^n$ とおけば $p^m = q^d$ である. $\alpha \in \mathbb{F}_q$ とすれば $\alpha^q = \alpha$. よつて $\alpha^{q^d} = \alpha$ となり $\alpha \in \mathbb{F}_{q^d}$ を得る. □

有限体についての基本的性質は次の定理の様にまとめられる.

定理 17.3. $q = p^n$ (p は素数, $n \in \mathbb{N}$) とせよ. 次が成り立つ.
(1) $\mathbb{F}_q$ の乗法群 $\mathbb{F}_q{}^\times = \mathbb{F}_q - \{0\}$ は位数 $q-1$ の巡回群である.
(2) $\mathbb{F}_q$ は完全体である.
(3) $\mathbb{F}_{q^d}/\mathbb{F}_q$ は Galois 拡大であり, $\mathrm{Gal}\,(\mathbb{F}_{q^d}/\mathbb{F}_q)$ は巡回群で

$$\sigma : \mathbb{F}_{q^d} \longrightarrow \mathbb{F}_{q^d}, \quad \alpha \longmapsto \alpha^q$$

とおくと $\mathrm{Gal}\,(\mathbb{F}_{q^d}/\mathbb{F}_q) = \langle \sigma \rangle$.

上の 17.3 (1) で $\mathbb{F}_q{}^\times = \langle \gamma \rangle$ と書いたとき, γ を有限体 $\mathbb{F}_q$ の 原始根 と呼ぶ. 17.3 で $n = 1$ の場合は, 「代数学 1」で学んだ原始根の概念に一致する. また, $\mathbb{F}_q$ は $\mathbb{F}_p$ に γ を添加して得られる : $\mathbb{F}_q = \mathbb{F}_p(\gamma)$.

演 習 問 題

17.4. p を素数, $n = 2^2 \cdot 3^3 \cdot 5$ とする. $G = \mathrm{Gal}\,(\mathbb{F}_{p^n}/\mathbb{F}_p)$ を求め, その構造を記せ. G の部分群とそれらに対応する拡大 $\mathbb{F}_{p^n}/\mathbb{F}_p$ の中間体を求めよ.

17.5. p を素数とせよ. K を $\mathbb{F}_p$ の m 次拡大体, L を K の n 次拡大体とせよ.

(1) 乗法群 $L^\times$ の生成元を g とする. $K^\times$ の生成元の 1 つを g で表せ.

(2) L の $\mathbb{F}_p$ 上の自己同型 σ は $\sigma(g) = g^\nu$ となる $\nu \in \mathbb{Z}$ によつて定まる. L の $\mathbb{F}_p$ 上の互ひに異るすべての自己同型を ν の値を示して記述せよ. そのうち, L の K 上の自己同型であるものを ν の値を示して記述せよ.

17.6. $\mathbb{F}_q = \mathbb{F}_p(\gamma)$ のとき γ は必ず ${\mathbb{F}_q}^\times$ の原始根であるか.

18. Hilbert の定理 90

定義 18.1. L/K は n 次の分離的拡大とし, L を含む K の代数的閉包を $\overline{K}$ とする. いま L から $\overline{K}$ の中への K 上の同型の全体を $\sigma_i : L \to \overline{K}$ $(i = 1, \cdots, n)$ とするとき, $\alpha \in L$ に対して

$$\mathrm{N}_{L/K}(\alpha) = \prod_{i=1}^{n} \alpha^{\sigma_i}, \quad \mathrm{Tr}_{L/K}(\alpha) = \sum_{i=1}^{n} \alpha^{\sigma_i},$$

と定義し, それぞれ拡大 L/K の norm, trace と呼ぶ.

問 18.2. $\gamma \in \overline{K}$ が K 上分離的で, 任意の $\sigma \in \mathrm{Aut}\overline{K}/K$ に対して $\gamma^\sigma = \gamma$ となれば $\gamma \in K$ であることを示せ.

例題 18.3. L/K は n 次の分離的拡大とする.

(1) $\mathrm{N}_{L_K} : L^\times \to K^\times$ $(\alpha \mapsto \mathrm{N}_{L/K}(\alpha))$ は乗法群の準同型で,
$\mathrm{Tr}_{L_K} : L \to K$ $(\alpha \mapsto \mathrm{Tr}_{L/K}(\alpha))$ は K 加群としての準同型である.

(2) M を L/K の中間体とすれば,

$$\mathrm{N}_{L/K} = \mathrm{N}_{M/K}\mathrm{N}_{L/M}, \quad \mathrm{Tr}_{L/K} = \mathrm{Tr}_{M/K}\mathrm{Tr}_{L/M}.$$

(3) $\alpha \in L$, $\mathrm{irr}\,(\alpha, K, x) = x^m + a_1 x^{m-1} + \cdots + a_m$ とすれば, 拡大 $K(\alpha)/K$ について

$$\mathrm{N}_{K(\alpha)/K}(\alpha) = (-1)^m a_m, \quad \mathrm{Tr}_{K(\alpha)/K}(\alpha) = -a_1.$$

証明 18.1 にある σ_i を用意する.

(1) 任意の $\sigma \in \mathrm{Aut}\overline{K}/K$ に対して $\{\sigma\sigma_1, \cdots, \sigma\sigma_n\} = \{\sigma_1, \cdots, \sigma_n\}$ となるから, $\alpha \in L$ に対して $\mathrm{N}_{L/K}(\alpha)$, $\mathrm{Tr}_{L/K}(\alpha)$ はともに σ で不変であり, K 上分離的である. 従つて共に K の元である. また $\mathrm{N}_{L/K}$, $\mathrm{Tr}_{L/K}$ がそれぞれ乗法, 加法を保つことは明らかである. さらに定義から $a \in K$ について $\mathrm{Tr}_{L/K}(a\alpha) = a\mathrm{Tr}_{L/K}$ となるから Tr は K 加群の間の準同型である.

(2) $[L : K] = r$, $[M : K] = s$ とし, $\rho_j : L \to \overline{K}$ $(j = 1, \cdots, r)$ を中への M 上の同型, $\tau_k : M \to \overline{K}$ $(k = 1, \cdots, s)$ を $\overline{K}$ の中への K 上の同型とせよ. 各 τ_j は K 上の同型 $\overline{\tau_j} : \overline{K} \xrightarrow{\sim} \overline{K}$ に拡張できるが, このとき $\overline{\tau_k}\rho_j : L \to \overline{K}$ は K 上の異なる同型で, $\{\sigma_i\} = \{\overline{\tau_k}\rho_j\}$ となる. よつて $\alpha \in L$ に対して, $\mathrm{N}_{L/K}(\alpha) = \prod_k (\prod_j \alpha^{\rho_j})^{\overline{\tau_k}} = \mathrm{N}_{M/K}(\mathrm{N}_{L/M}(\alpha))$ となる. Trace についても同様である.

(3) $\mathrm{irr}\,(\alpha, K, x) = (x - \alpha_1)\cdots(x - \alpha_m)$ とすると, m 個の K 上の同型 $\rho_i : K(\alpha) \to \overline{K}$ $(\alpha \mapsto \alpha_i)$ があり,

$$\mathrm{N}_{K(\alpha)/K}(\alpha) = \prod_{i=1}^{m} \alpha_i = (-1)^m a_m, \quad \mathrm{Tr}_{K(\alpha)/K}(\alpha) = \sum_{i=1}^{m} \alpha_i = -a_1$$

となる. □

補題 18.4. (Artin の定理) $\sigma_i : L \to \Omega$ $(i = 1,\cdots,n)$ は体 L から体 Ω の中への異る同型写像とする. このとき $\alpha_1, \cdots, \alpha_n \in \Omega$ に対し

$$\alpha_1\,\theta^{\sigma_1} + \cdots + \alpha_n\,\theta^{\sigma_n} = 0\ (\forall\theta \in L\,) \implies \alpha_1 = \cdots = \alpha_n = 0.$$

この性質を, $\{\sigma_i\}$ は L 上1次独立である, と称する.

証明 ある $(\alpha_1, \cdots, \alpha_n) \neq (0, \cdots, 0)$ に対して, 上の左側の関係式が成り立つとして, その様な関係式の内で $\alpha_i \neq 0$ なる i の個数が最小なものを更めて (必要ならば番号を付け変へて)

$$\alpha_1\,\theta^{\sigma_1} + \alpha_2\,\theta^{\sigma_2} + \cdots + \alpha_r\,\theta^{\sigma_r} = 0\ (\forall\theta \in L\,), \quad \alpha_i \neq 0\ \ (1 \leq i \leq r\,) \tag{18.5}$$

とする. このときもちろん $r \geq 2$ で, 仮定により $\sigma_1 \neq \sigma_2$ ゆゑ, $\gamma^{\sigma_1} \neq \gamma^{\sigma_2}$ となる $\gamma \in L$ がある. (18.5) から

$$\alpha_1\,\gamma^{\sigma_1}\theta^{\sigma_1} + \alpha_2\,\gamma^{\sigma_2}\theta^{\sigma_2} + \cdots + \alpha_r\,\gamma^{\sigma_r}\theta^{\sigma_r} = 0\ (\forall\theta \in L\,) \tag{18.6}$$

を得る. (18.5) を γ^{σ_1} 倍して (18.6) を差し引けば

$$\alpha_2\,(\gamma^{\sigma_1} - \gamma^{\sigma_2})\theta^{\sigma_2} + \cdots + \alpha_r\,(\gamma^{\sigma_1} - \gamma^{\sigma_r})\theta^{\sigma_r} = 0\ (\forall\theta \in L\,)$$

となるが, $\alpha_2(\gamma^{\sigma_1} - \gamma^{\sigma_2}) \neq 0$ であるから, これは (18.5) の項数 r の最小性に反する. □

問 18.7. L/K を有限次分離的拡大とすれば, $\mathrm{Tr}_{L/K}(\theta) \neq 0$ となる $\theta \in L$ がある. 従つて $\mathrm{Tr}_{L/K}(L) = K$ となることを示せ.

さて, 次がこの節で目標とした定理である.

定理 18.8. (Hilbert の定理 90) L/K は巡回拡大で $\mathrm{Gal}\,(L/K) = \langle\sigma\rangle$ とせよ.
(1) $\mathrm{N}_{L/K}(\alpha) = 1 \iff \alpha = \beta^{1-\sigma}(= \beta(\beta^{\sigma})^{-1})$ となる $\beta \in L$ が存在する.
(2) $\mathrm{Tr}_{L/K}(\alpha) = 0 \iff \alpha = \beta - \beta^{\sigma}$ となる $\beta \in L$ が存在する.

注意 18.9. "定理 90" といふ名称は, Hilbert が前世紀までの数論の成果を集大成して著した Zahlbericht (1897) における定理の番号に由来する.

証明 $[L : K] = n$ とする. (1) ($\Leftarrow$) $\mathrm{N}_{L/K}(\alpha) = \alpha^{1+\sigma+\cdots+\sigma^{n-1}} = \beta^{(1-\sigma)(1+\sigma+\cdots+\sigma^{n-1})} = \beta^{1-\sigma^n} = 1$ となり正しい. ($\Rightarrow$) 18.4 を $1 = \mathrm{id}_L$, σ, $\cdots$, σ^{n-1} に適用して, ある $\theta \in L$ について

$$\theta + \alpha\theta^{\sigma} + \alpha^{1+\sigma}\theta^{\sigma^2} + \cdots + \alpha^{1+\sigma+\cdots+\sigma^{n-2}}\theta^{\sigma^{n-1}} \neq 0 \tag{18.10}$$

となる. 上の左辺を β とおけば, $\mathrm{N}_{L/K}(\alpha) = 1$ ゆゑ $\alpha\beta^{\sigma} = \beta$, 従つて $\alpha = \beta^{1-\sigma}$ を得る.
(2) 一般に $\mathrm{Tr}_{L/K}(\theta) = \theta + \theta^{\sigma} + \cdots + \theta^{\sigma^{n-1}}$ である.
($\Leftarrow$) $\mathrm{Tr}_{L/K}(\beta - \beta^{\sigma}) = (\beta + \beta^{\sigma} + \cdots + \beta^{\sigma^{n-1}}) - (\beta^{\sigma} + \beta^{\sigma^2} + \cdots + \beta^{\sigma^n}) = 0.$
($\Rightarrow$) 18.7 により $\mathrm{Tr}_{L/K}(\theta) \neq 0$ となる $\theta \in L$ がある. これを使ひ,

$$\beta = \{\alpha\theta^{\sigma} + (\alpha + \alpha^{\sigma})\theta^{\sigma^2} + \cdots + (\alpha + \alpha^{\sigma} + \cdots + \alpha^{\sigma^{n-2}})\theta^{\sigma^{n-1}}\}\,\mathrm{Tr}_{L/K}(\theta)^{-1}$$

とおく. このとき $\theta^{\sigma^n} = \theta$, および仮定 $0 = \mathrm{Tr}_{L/K}(\alpha) = \alpha + \alpha^{\sigma} + \cdots + \alpha^{\sigma^{n-1}}$ より

$$\alpha + \beta^{\sigma} = \{\alpha\mathrm{Tr}_{L/K}(\theta) + \alpha^{\sigma}\theta^{\sigma^2} + \cdots + (\alpha^{\sigma} + \alpha^{\sigma^2} + \cdots + \alpha^{\sigma^{n-1}})\theta^{\sigma^n}\}\,\mathrm{Tr}_{L/K}(\theta)^{-1} = \beta$$

となる. □

注意 18.11. α と θ に関する (18.10) の左辺の式を Lagrange の分解式と呼ぶ.

演 習 問 題

18.12. p を素数, $x^p - x - 1 = 0$ の根の 1 つ $\alpha \in \overline{\mathbb{F}_p}$ をとり, $K = \mathbb{F}_p(\alpha)$ とおく [22].

(1) このとき拡大 $K/\mathbb{F}_p$ は $\sigma : \beta \mapsto \beta + 1$ で定まる自己同型が生成する p 次巡回拡大となることを示し, $\mathrm{irr}\,(\alpha, \mathbb{F}_p, x) = x^p - x - 1$ および $\mathrm{N}_{K/\mathbb{F}_p}(\alpha) = 1$ を示せ.

(2) $p = 2, 5, 7$ のときに, (1) の σ について $\alpha = y^{1-\sigma}$ となる $y \in K$ を求めよ.

18.13. 有限次拡大 L/K について, L/K は分離的 $\iff \exists \alpha \in L,\ \mathrm{Tr}_{L/K}(\alpha) \neq 0,$ である. これを証明せよ.

[22] 15.11 と一部重複.

19. Kummer 拡大

18.8 を用ゐて次の定理が得られる.

定理 19.1. (単純 Kummer 拡大) 体 K は 1 の原始 n 乗根 ζ を含むとせよ [23]. このとき次が成り立つ.

(1) L/K が n 次の巡回拡大ならば, $\beta \in K$ が存在して $L = K(\beta)$ かつ $\mathrm{irr}\,(\beta, K, x) = x^n - a$ $(a \in K)$ となる.

(2) 逆に $a \in K$ に対して, 多項式 $x^n - a$ の 1 つの根 $\sqrt[n]{a}$ を取つて $L = K(\sqrt[n]{a}\,)$ とおけば, L/K は d 次の巡回拡大である. ここで d は $d|n$, $(\sqrt[n]{a}\,)^d \in K$ を満たすある自然数.

証明 (1) $G = \mathrm{Gal}\,(L/K) = \langle\sigma\rangle$ とする. $\mathrm{N}_{L/K}(\zeta^{-1}) = \zeta^{-n} = 1$ であるから, 18.8(1) より $\zeta^{-1} = \beta^{1-\sigma}$, 即ち $\beta^\sigma = \beta\zeta$ となる $\beta \in L$ が存在する. このとき, 仮定により 1 の n 乗根 $1, \zeta, \cdots, \zeta^{n-1}$ はすべて異なるから, $\beta, \beta^\sigma = \beta\zeta, \beta^{\sigma^2} = \beta\zeta^2, \cdots, \beta^{\sigma^{n-1}} = \beta\zeta^{n-1}$ はすべて異なり, 従つて $n \le [K(\beta) : K]_s \le [K(\beta) : K]$ となる. 一方 $L \supset K(\beta)$, $[L : K] = n$ であるから $L = K(\beta)$ となる. また $(\beta^n)^\sigma = \beta^n\zeta^n = \beta^n$ であるから, $\beta^n \in L^G = K$. $a = \beta^n$ と書けば $\beta = \sqrt[n]{a}$ $(a \in K)$ である. また, 5.8(2) から $\mathrm{irr}\,(\sqrt[n]{a}, K, x) = x^n - a$ も示された.
(2) $\gamma = \sqrt[n]{a}$ とおく. このとき $\gamma, \gamma\zeta, \cdots, \gamma\zeta^{n-1}$ はすべて, 互ひに異なり, かつ $x^n - a$ の根であるから $x^n - a = \prod_{i=0}^{n-1}(x - \gamma\zeta^i)$ となり, これは分離的である. $\mathrm{irr}\,(\gamma, K, x)|x^n - a$ であるから γ は K 上分離的で, γ の K 上の共役はすべて $\gamma\zeta^i$ の形の元であるから, それらは $L = K(\gamma)$ に含まれる. 従つて L/K は Galois 拡大である. その Galois 群を $G = \mathrm{Gal}\,(L/K)$ とする. $\sigma \in G$ について $\gamma^\sigma = \gamma\zeta^{i(\sigma)}$ $(\,i(\sigma) \in \{0, 1, \cdots, n-1\}\,)$ の形に書ける. σ は γ の像 γ^σ によつて定まるから写像 $G \to \langle\zeta\rangle$ $(\sigma \mapsto \zeta^{i(\sigma)})$ は単射準同型である. よつて G は位数 n の巡回群 $\langle\zeta\rangle$ の部分群と同型であり, それ自身も巡回群である. ゆゑに $|G| = d$ とすれば $d|n$ である. ここで更めて G の生成元を σ と書いて $G = \langle\sigma\rangle$ とすれば, $(\zeta^{i(\sigma)})^d = 1$ であるから, $(\gamma^d)^\sigma = (\gamma^\sigma)^d = \gamma^d(\zeta^{i(\sigma)})^d = \gamma^d$. よつて $\gamma^d \in L^G = K$ である. □

注意 19.2. 体 K は 1 の原始 n 乗根を含むとする. K 上のいくつかの多項式 $f_j(x) = x^n - a_j$ $(1 \le j \le r)$ を考へる [24]. これらの根を K に添加してできる拡大 $K(\sqrt[n]{a_1}, \cdots, \sqrt[n]{a_r}\,)/K$ を Kummer 拡大 と呼ぶ. 19.1 で述べた拡大は $r = 1$ の場合なので, ここでは 単純 Kummer 拡大と呼ぶこととした.

[23] 従つて $\gcd(\mathrm{char}\,K, n) = 1$ である
[24] これらは K 上分離的である.

20. 円分体

体 K の代数的閉包 $\overline{K}$ を 1 つ決めて固定する. $\overline{K}$ 内の 1 の n 乗根の全体を U_n で表す. U_n は多項式 x^n-1 の根の全体であり, 一般に位数 n 以下の巡回群である (代数学 1, 系 13.6).

命題 20.1. 1 の n 乗根の個数について次のことが成り立つ.
(1) $\operatorname{char} K = 0$ のとき $|U_n| = n$.
(2) $\operatorname{char} K = p > 0$ のとき, $n = p^r m$, $\gcd(p, m) = 1$ とすれば, $U_n = U_m$ で $|U_n| = m$.
(3) 1 の n 乗根は K 上分離的である.

証明 $f(x) = x^n - 1$ とすれば $f'(x) = nx^{n-1}$. 従つて $\operatorname{char} K = p$, $n|p$ なる場合を除けば, $f(x)$ は重根を持たず, $|U_n| = n$ となる. また, (2) の場合は $x^n - 1 = (x^m - 1)^{p^r}$ となり, $x^m - 1$ は重根を持たないから $U_n = U_m$, $|U_n| = m$ である. さらに 1 の n 乗根はどれも, 分離的多項式 $x^m - 1$ の根であるから K 上分離的である. □

定義 20.2. 体 K に対し, 位数 n の元 $\zeta \in K^\times$ を 1 の <u>原始</u> n <u>乗根</u> と呼ぶ.

このとき $U_n = \langle \zeta \rangle$ で $\gcd(i, n) = 1$ ならば ζ^i もまた 1 の原始 n 乗根である. $L = K(U_n)$ は多項式 $x^n - 1$ の最小分解体であり, K の正規拡大である. このとき ζ は K 上分離的であるから, L/K は分離的である. 従つて L/K は Galois 拡大である.

定義 20.3. 体 M がある $K(U_n)/K$ の中間体であるとき, M を K 上の <u>円分体</u> といふ.

命題 20.4. 体 K 上の円分体は K の Abel 拡大である.

証明 Abel 群の部分群はすべて正規であり, それにより剰余類群も Abel 群なので, Galois の基本定理 16.3 により, $L = K(U_n)$ が K 上の Abel 拡大であることを示せばよい. 20.1 を踏まへれば $|U_n| = n$ としてよい. $U_n = \langle \zeta \rangle$, $G = \operatorname{Gal}(L/K)$ とおく. $\sigma \in G$ について $\zeta^\sigma = \zeta^{i(\sigma)}$ なる $i(\sigma) \in (\mathbb{Z}/n\mathbb{Z})^\times$ が定まるが, これにより G は $(\mathbb{Z}/n\mathbb{Z})^\times$ の部分群と同型であることがわかる. ゆゑに G は Abel 群である. 次に M を L/K の中間体とし, $H = G^M$ (M による不変群) とする. このとき G が Abel 群ゆゑ, $H \lhd G$ であるから M/K は 16.3 (2) より Galois 拡大で, 16.3 (3) より $\operatorname{Gal}(M/K) \simeq G/H$ である. G が Abel 群だから, これは Abel 群である. □

注意 20.5. 後に, 25.6 において, $\operatorname{Gal}(\mathbb{Q}(U_n)/\mathbb{Q})$ と $(\mathbb{Z}/n\mathbb{Z})^\times$ が同型であることが示される.

21. 代数的に解ける方程式

この節では, 特に断らない限り, 体はすべて標数 0 であるとする. 従つて常に $\mathbb{Q}$ を含む. また 19.1 と同様に $\sqrt[n]{a}$ は $x^n - a$ の根の 1 つを表すものとする.

定義 21.1. 有限次拡大 E/K に対して, その中間体の列

$$K = E_0 \subset E_1 \subset \cdots \subset E_r = E \tag{21.2}$$

があつて, $0 \le i \le r-1$ なる各 i に対して $\operatorname{irr}(\sqrt[n_i]{a_i}, E_i, x) = x^{n_i} - a_i$ であつて

$$E_{i+1} = E_i(\sqrt[n_i]{a_i}) \quad (a_i \in E_i)$$

となつてゐるとき, E/K は 冪根による拡大 であるといふ. また, この様な拡大体の元は K 上で 根号表示できる といふ.

注意 21.3. 冪乗根号の定義によれば $\frac{-1+\sqrt{-3}}{2} = \sqrt[3]{1}$ と書けるが, 左辺の方がより根源的な記述である. 一般の原始 n 乗根が $\sqrt[n]{1}$ 以外のより根源的な記述を持つか否かは自明ではない. この定義中の条件 $\operatorname{irr}(\sqrt[n_i]{a_i}, K, x) = x^{n_i} - a_i$ は, その様なより根源的な記述を前提とするために入れてある. 我々は, この既約性に拘(こだは)るがゆゑに, 最終的な到達点 21.15 までの議論がかなり複雑になる. 文献 [N] では, この条件を入れない議論しかされてゐない.

定義 21.4. 体 K 上の多項式 $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ に対して, その根がすべて $\mathbb{Q}(a_0, a_1, \cdots, a_n)$ 上で根号表示できるとき, 方程式 $f(x) = 0$ は 代数的に解ける といはれる.

このことは, 方程式 $f(x) = 0$ の解がすべて $f(x)$ の係数 a_0, a_1, $\cdots$, a_n に四則演算 ($+$, $-$, $\times$, $\div$) と冪根を取るといふ操作 $\sqrt[r]{\ }$) を有限回行つて得られることを意味してゐる. さらにこのことはまた, $f(x)$ の $K' = \mathbb{Q}(a_0, a_1, \cdots, a_n)$ 上の最小分解体が, K' のある冪根による拡大体に含まれることに他ならない.

問 21.5. 次のことを示せ.

(1) 体の列 $K \subset M \subset L$ において, M/K, L/M がともに冪根による拡大ならば L/K も冪根による拡大である.

(2) L/K を冪根による拡大とし, $\overline{K}$ を L を含む K の代数的閉包とする. K 上の中への同型 $\sigma : L \to \overline{K}$ に対し, L^σ/K も冪根による拡大である.

(3) 拡大 L/K で, L は K 上の冪根拡大体 E に含まれるが (つまり L の元はすべて K 上で根号表示できるにも拘らず), L/K 自体は冪根による拡大ではない様な例を挙げよ.
(Hint : 第 23 節の最後を参照.)

(4) L, M が拡大 $\overline{K}/K$ の中間体で, L/K が冪根による拡大であるにも拘らず ML/M が冪根による拡大にならない例を挙げよ. また, L/K と M/K が共に冪根による拡大であるにも拘らず, LM/K が冪根による拡大にはならない例を挙げよ.

注意 21.6. $n \in \mathbb{N}$ に対し, $\mathbb{Q}$ の代数的閉包 $\overline{\mathbb{Q}}$ 内の 1 の n 乗根の全体を U_n で表す. $\mathbb{Q}(U_n)/\mathbb{Q}$ は常にある冪根による拡大に含まれるが, それ自体が冪根による拡大になるとは限らない ($n = 7$ の場合が反例. 21.19 参照. 1 の原始 7 乗根を表すのに $\sqrt{-3}$ つまり 1 の原始 3 乗根が必要であるが $U_7 \not\supset U_3$.). しかし, 後の 21.8 の様に, ある $n \in \mathbb{N}$ に対し, N を $1, 2, \cdots, n$ の最大公倍数とすれば, $\mathbb{Q}(U_N)/\mathbb{Q}$ は冪根による拡大になる. 21.8 は 21.15 の証明に必要である.

定義 21.7. 有限群 G の部分群 G_i からなる列で

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{1\}$$

となるものを 正規列 と呼ぶ.

補題 21.8. K を体とする. 自然数 n に対し, 1 の原始 m 乗根 ($m = 1, 2, \cdots, n$) の全てからなる集合を Γ_n ($\subset \overline{K}$) とすれば, $K(\Gamma_n)/K$ は冪根による拡大である.

証明 n に関する帰納法で示す. $K_n = K(\Gamma_n)$ とおく. $K = K_1 = K_2$, $K_3 = K(\sqrt{-3})$, $K_4 = K(\sqrt{-3}, \sqrt{-1})$ については主張は正しい. $n \geq 5$ とし $n-1$ まで主張が成り立つてゐるとせよ. ζ_n を 1 の原始 n 乗根の 1 つとする. このとき $K_n = K_{n-1}(\zeta_n)$ であるから, K_n は K_{n-1} の Abel 拡大であつて, $[K_n : K_{n-1}] \leq \varphi(n) < n$ である (20.4 より). Abel 群 $G_0 := \mathrm{Gal}\,(K_n/K_{n-1})$ は有限巡回群の直積 $H_1 \times H_2 \times \cdots \times H_r$ と表される (有限 Abel 群の構造定理). ここで

$$G_i = \{1\} \times \cdots \times \{1\} \times H_{i+1} \times \cdots \times H_r \ (< G_0) \quad (0 \leq i \leq r)$$

とおけば, G_0 の正規列 $G_0 \rhd G_1 \rhd \cdots \rhd G_{r-1} \rhd G_r = \{1\}$ が得られて, $G_{i-1}/G_i \cong H_i$ となつてゐる. 各 $1 \leq i \leq r$ について, K_n と K_{n-1} の中間体で, G_i に対応するものを L_i とする. 特に $L_0 = K_{n-1}$, $L_r = K_n$. G_0 は Abel 群だから $G_i \lhd G_0$ で, L_i は L_0 の Galois 拡大, $\mathrm{Gal}\,(L_i/L_0) \cong G_0/G_i$ であり, L_{i-1} が L_i と L_0 の中間体で部分群 $G_{i-1}/G_i < G_0/G_i$ に対応するものである. 即ち, $\mathrm{Gal}\,(L_i/L_{i-1}) \cong G_{i-1}/G_i \cong H_i$ で L_i は L_{i-1} の巡回拡大である (16.1, 16.3 参照). $|H_i| = m_i$ と記すと $m_i = [L_i : L_{i-1}] \leq [K_n : K_{n-1}] < n$ であるから, K_{n-1} は (従つて L_{i-1} は) 1 の原始 m_i 乗根を含み, $L_i = L_{i-1}(\alpha_i)$, $\mathrm{irr}\,(\alpha_i, L_{i-1}) = x^{m_i} - a_i$ ($a_i \in L_{i-1}$) の形に表される (19.1 より). これで K_n が K_{n-1} の冪根による拡大であることが示された. K_{n-1} に関する帰納法の仮定より K_n が K の冪根による拡大であることがわかり, 帰納法の証明が完了する. □

以下では方程式の代数的可解性と Galois 群の可解性の関係を考へる.

定義 21.9. 有限群 G が 可解群 であるとは, 正規列 $G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{1\}$ が存在して, G_i/G_{i+1} ($0 \leq i \leq n-1$) が Abel 群になることをいふ. もちろん Abel 群は可解群である.

問 21.10. S_2, S_3, S_4 が可解群であることを示せ. (以下 21.14 まで, [N] の 16.1 節, [Iy] の §1.11)

問 21.11. 可解群の部分群は可解群であることを示せ.

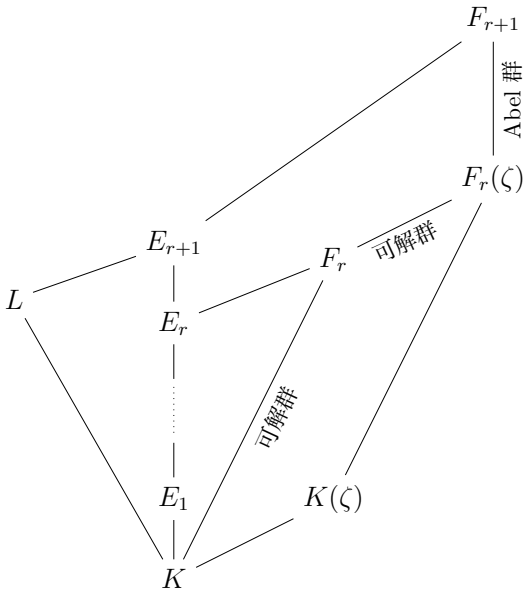
問 21.12. 可解群から別の群への準同型の像は可解群であることを示せ.

問 21.13. 可解群 G に対し, 正規列 $G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{1\}$ で全ての G_i/G_{i+1} ($0 \leq i \leq n-1$) が素数位数の巡回群となるものが存在することを示せ.

問 21.14. 群 G と $N \lhd G$ に対し, N と G/N がともに可解群ならば, G も可解群であることを示せ. (このことから, L/K が Galois 拡大であり, 中間体 M についても M/K が Galois 拡大のとき, $\mathrm{Gal}\,(L/M)$ と $\mathrm{Gal}\,(M/K)$ が可解群であれば $\mathrm{Gal}\,(L/K)$ も可解群であることが帰結される.)

定理 21.15. L/K が有限次拡大のとき, 次の 2 つは同値である.
(1) L を含む冪根による拡大 E/K がある.
(2) L を含む有限次 Galois 拡大 F/K で $\mathrm{Gal}\,(F/K)$ が可解群となるものがある.

証明 (1)⇒(2). 冪根による拡大 E/K を与へる体の列の長さ r による数学的帰納法で, (2) の様な拡大 F/K が存在することを示す.



Step 1 まづ, $r = 0$ のときは $L = E$ であり, $F = E$ とすれば $\mathrm{Gal}\,(F/K) = \{1\}$ となる. ゆゑに, この場合は (1)⇒(2) が成り立つ.

Step 2 $r \geq 0$ とし, 冪根による拡大 E/K を与へる体の列の長さが r までは (1)⇒(2) が正しいと仮定する. いま体の列

$$K = E_0 \subset E_1 \subset \cdots \subset E_r \subset E_{r+1} = E,$$
$$E_{i+1} = E_i(\sqrt[n_i]{a_i}) \quad (\exists\, a_i \in E_i)$$

があつて $L \subset E$ となつてゐる. 一方, 主張 (1) の E/K として, この体の列の部分

$$K = E_0 \subset E_1 \subset \cdots \subset E_r$$

を考へ, L として E_r 自身を考へれば, 帰納法の仮定より E_r を含む K の Galois 拡大 F_r があつて, $\mathrm{Gal}\,(F_r/K)$ が可解群になつてゐる.

Step 3 ζ を 1 の原始 n_r 乗根とする. $K(\zeta)/K$ も F_r/K も Galois 拡大なので, 15.2 の後半より, $F_r(\zeta)/K$ は Galois 拡大. F_r/K は Galois 拡大ゆゑ 16.3(2) と (3) から, $\mathrm{Gal}\,(F_r(\zeta)/K) \triangleright \mathrm{Gal}\,(F_r(\zeta)/F_r)$ で, この 2 群の剰余類群は可解群 $\mathrm{Gal}\,(F_r/K)$ と同型であり, 20.4 から $\mathrm{Gal}\,(F_r(\zeta)/F_r)$ は Abel 群, 従つて可解群だから, $\mathrm{Gal}\,(F_r(\zeta)/K)$ も可解群である (21.14).

Step 4 さて, $a_r \in E_r \subset F_r$ で, 各 $\sigma \in \mathrm{Gal}\,(F_r/K)$ について,

$$x^{n_r} - {a_r}^{\sigma} = \prod_{\nu=0}^{n_r-1} \left(x - \sqrt[n_r]{{a_r}^{\sigma}}\,\zeta^{\nu}\right)$$

である. ここで $\mathrm{Gal}\,(F_r/K) = \{\sigma_1, \cdots, \sigma_N\}$ と記すこととし, 次の体を考へる :

$$F_{r+1} = F_r\big(\zeta, \sqrt[n_r]{{a_r}^{\sigma_1}}, \cdots, \sqrt[n_r]{{a_r}^{\sigma_N}}\big).$$

Step 5 拡大 F_{r+1}/K が所望の Galois 拡大体 F/K の 1 つである. それを示さう. まづ, $F_{r+1}/F_r(\zeta)$ は Abel 拡大 $F_r(\zeta, \sqrt[n_r]{{a_r}^{\sigma_i}})/F_r(\zeta)$ 達の合成体ゆゑ, 16.5(2) より, Abel 拡大, 従つて $\mathrm{Gal}\,(F_{r+1}/F_r(\zeta))$ は可解群である. また F_{r+1} は多項式

$$\prod_{\sigma \in \mathrm{Gal}\,(F_r/K)} \left(x^{n_r} - {a_r}^{\sigma}\right) \in K[x]$$

の最小分解体であるから F_{r+1}/K は Galois 拡大であり, 明らかに $E_{r+1} = E_r\big(\sqrt[n_r]{a_r}\big) \subset F_r\big(\sqrt[n_r]{a_r}\big) \subset F_{r+1}$ である. Step 3 より拡大 $F_r(\zeta)/K$ は Galois であり, それゆゑ $\mathrm{Gal}\,(F_{r+1}/K) \triangleright \mathrm{Gal}\,(F_{r+1}/F_r(\zeta))$ である (16.3(2)). この 2 群の剰余類群は可解群 $\mathrm{Gal}\,(F_r(\zeta)/K)$ に同型で, $\mathrm{Gal}\,(F_{r+1}/K)$ も可解群 (21.14). 従つて, 体の列の長さが $r+1$ でも (1)⇒(2) は正しい.

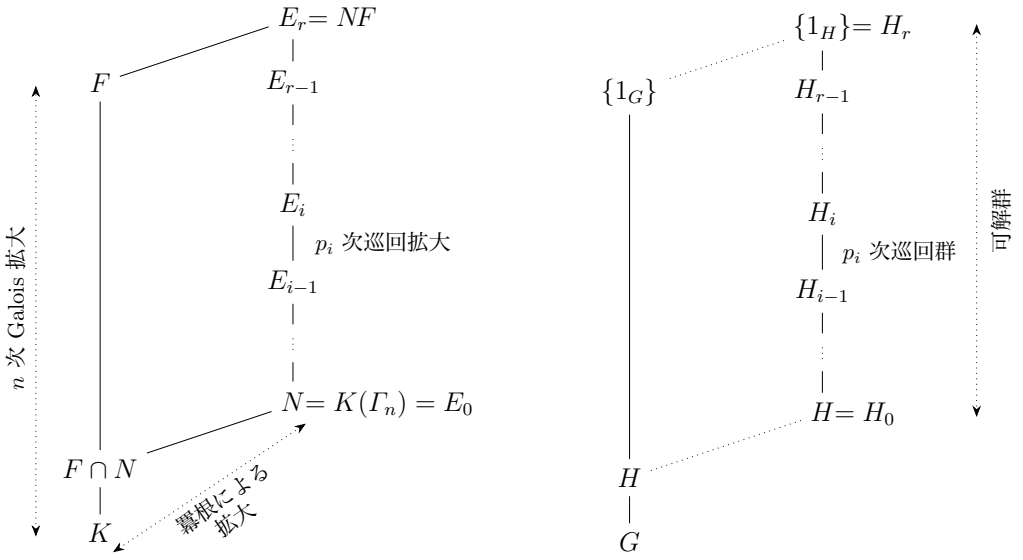
(2)⇒(1). 仮定の F を含む K の代数的閉包を $\overline{K}$ とする. また $G=\mathrm{Gal}\,(F/K)$, $|G|=n$ とし, $\overline{K}$ において 21.8 の記号で Γ_n による拡大を $N=K(\Gamma_n)$ とおく. このとき Galois 拡大 F/K の N による持ち上げ NF/N も Galois 拡大で, その Galois 群 $H=\mathrm{Gal}\,(NF/N)$ は G のある部分群と同型である (16.5(1)). よつて H は可解群 (21.11) で, 正規列

$$H=H_0\rhd H_1\rhd\cdots\rhd H_r=\{1\},\quad (\,H_i/H_{i+1}\text{ は位数が素数の巡回群 (}\ p_i\text{ 次とする)})$$

が存在する (21.13). $E_i=(NF)^{H_i}$ とおけば, 上の正規列に対応して NF/N の中間体の列

$$K\subset N=E_0\subset E_1\cdots\subset E_r=NF$$

を得る. E_{i+1}/E_i は p_i 次の巡回拡大で, $p_i=[E_{i+1}:E_i]\,\big|\,[NF:N]\,\big|\,n$ であるから 1 の原始 p_i 乗根は N に, 従つて E_i に含まれ, 19.1 より, $E_{i+1}=E_i(\sqrt[p_i]{a_i}\,)$ となる $a_i\in E_i$ が存在する.



このとき $\deg\mathrm{irr}\,(\sqrt[p_i]{a_i},E_i,x)=[E_{i+1}:E_i]=p_i$ ゆゑ, $\mathrm{irr}\,(\sqrt[p_i]{a_i},E_i,x)=x^{p_i}-a_i$ でなければならない. 一方 21.8 によれば, N/K は冪根による拡大であるから, 21.5 (2) より $E=NF$ は求める拡大体である. □

注意 21.16. 我々の冪根による拡大の定義は [N] の本のそれと異るため, 冪根による拡大の持ち上げが冪根による拡大になるとは限らないし, いくつかの冪根による拡大の合成体が再び冪根による拡大になるとも限らない (21.5 (1), (2)). これが原因で 21.15 の証明が複雑になつてしまふ. この証明は [Iy] に書かれてゐるものである.

上の定理から容易に次の定理が得られる.

定理 21.17. 体 K は元 $a_0,\cdots,a_n$ により $K=\mathbb{Q}(a_0,a_1,\cdots,a_n)$ となつてゐるとする. $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n$ の K 上の最小分解体を L とする. 次の 2 つは同値.
(1) 方程式 $f(x)=0$ は代数的に解ける.
(2) Galois 群 $\mathrm{Gal}\,(L/K)$ は可解群である.

証明 (1)⇒(2). 定義から (1) の主張は, K の冪根による拡大 E で L を含むものがあることと同値である. 21.15 より, このとき L を含む K の Galois 拡大 F/K で $\mathrm{Gal}\,(F/K)$ が可解群となるものがある. 21.12 により $\mathrm{Gal}\,(L/K)$ も可解群. (2)⇒(1) は 21.15 より明らか. □

演 習 問 題

21.18. 方程式 $x^6+x^5+x^4+x^3+x^2+x+1=0$ の根は四則演算, 平方根号, 3 乗根号によつて書けることを示せ. 具体的な表示は要求しない.

21.19. $\alpha=\exp(2\pi i/7)+\exp(-2\pi i/7)$ とおくとき,

(1) $\mathrm{irr}\,(\alpha,\mathbb{Q},x)=x^3+x^2-2x-1$ であることを示せ.

(2) $\exp(2\pi i/7)\mapsto\exp(6\pi i/7)$ は $\mathbb{Q}(\alpha)$ の $\mathbb{Q}$ 上の同型を与へることを示せ.

(3) 上の自己同型を σ とおく. α^σ を α の有理式で書け. それを $\varphi(\alpha)$ (但し $\varphi(x)\in\mathbb{Q}(x)$) とするとき, $\alpha^{\sigma^2}=\varphi(\varphi(\alpha))$ であることを確かめよ.

(4) $\mathbb{Q}(\alpha)/\mathbb{Q}$ は Galois 拡大で, $\mathrm{Gal}\,(\mathbb{Q}(\alpha)/\mathbb{Q})$ は位数 3 の巡回群であることを示せ.

(5) α を四則演算と根号 $\sqrt{\ },\sqrt[3]{\ }$ だけで表せ. $\Big($ 答 : $\alpha=\frac{1}{3}\Big(-\sqrt[3]{\frac{-7+21\sqrt{-3}}{2}}-\sqrt[3]{\frac{-7-21\sqrt{-3}}{2}}-1\Big)$. $\Big)$

21.20. 方程式 $x^5-2=0$ の $\mathbb{Q}$ 上の最小分解体を K とする. $\mathrm{Gal}\,(K/\mathbb{Q})$ はどの様な群か. (Hint : $\zeta=\exp(2\pi i/5)$ とおく. σ,τ を $\sqrt[5]{2}^{\,\sigma}=\sqrt[5]{2}\,\zeta$, $\zeta^\sigma=\zeta$, $\sqrt[5]{2}^{\,\tau}=\sqrt[5]{2}$, $\zeta^\tau=\zeta^2$ で定めると $\sigma,\tau\in\mathrm{Gal}\,(K/\mathbb{Q})$ であり, $\mathrm{Gal}\,(K/\mathbb{Q})=\langle\sigma,\tau\rangle$.)

21.21. 1 の原始 11 乗根について考へる.[25] $\zeta=\exp(2\pi i/11)$, $\rho=\exp(2\pi i/5)$ とおく. 以下, すべての数は複素数体 $\mathbb{C}$ の元であるとする. まづ

$$V_1=\sqrt[5]{\tfrac{11}{4}\big(89+25\sqrt{5}-5\sqrt{-5-2\sqrt{5}}+45\sqrt{-5+2\sqrt{5}}\,\big)}=3.31568\cdots+i\,0.07884\cdots,$$
$$V_2=\sqrt[5]{\tfrac{11}{4}\big(89+25\sqrt{5}+5\sqrt{-5-2\sqrt{5}}-45\sqrt{-5+2\sqrt{5}}\,\big)}=3.31568\cdots-i\,0.07884\cdots,$$
$$V_3=\sqrt[5]{\tfrac{11}{4}\big(89-25\sqrt{5}-5\sqrt{-5+2\sqrt{5}}-45\sqrt{-5-2\sqrt{5}}\,\big)}=3.19787\cdots-i\,0.87953\cdots,$$
$$V_4=\sqrt[5]{\tfrac{11}{4}\big(89-25\sqrt{5}+5\sqrt{-5+2\sqrt{5}}+45\sqrt{-5-2\sqrt{5}}\,\big)}=3.19787\cdots+i\,0.87953\cdots$$

とおく. ここで 5 乗根は 5 つづつ存在するが, 明確にするため, 上の様に虚数部分の絶対値が最も小さいものを選ぶことにした. 但し $\sqrt{-5+2\sqrt{5}}$ と $\sqrt{-5-2\sqrt{5}}$ の虚数部分はともに正にとつてゐる. 以下の問に答へよ.

(1) $V_1V_2=V_3V_4=11$ であることを示せ.

(2) $y=\zeta+\zeta^{-1}$ とおくと y は
$$y^5+y^4-4y^3-3y^2+3y+1=0$$
を満足することを示せ.

(3) (2) の y は
$$y=-\tfrac{1}{5}(1+V_1\,\rho^3+V_2\,\rho^2+V_3\,\rho^2+V_4\,\rho^3)\quad(=2\cos(\tfrac{2\pi}{11})=1.68250\cdots)$$
と書けることを示せ.

以上より $\zeta^2-y\zeta+1=0$ を解いて ζ の冪根表示が得られる.[26]

---

[25] この話題について Ian Stewart : Galois theory §21.1 に記述があるが, (4th ed. までの全てに) 多くの誤りを含む. Olaf Neumann : *Cyclotomy: From Euler through Vandermonde to Gauss*, Leonhard Euler: Life, Work and Legacy, Robert E. Bradley and C. Edward Sandifer (Editors), pp. 323-362 に正確な記述がある.

[26] この状況で $\mathbb{Q}(\zeta)/\mathbb{Q}$ が冪根による拡大 $\mathbb{Q}(V_1,V_2,V_3,V_4,\rho)/\mathbb{Q}$ の中間体であることがわかるが, この拡大 $\mathbb{Q}(\zeta)/\mathbb{Q}$ は冪根による拡大になつてゐるであらうか.

22. 一般代数方程式

$a_1, a_2, \cdots, a_n$ は体 K 上で代数的に独立であるとする. このとき, これらを係数とする多項式 $g(x) = x^n + a_1x^{n-1} + \cdots + a_n$ を体 K 上の n 次一般多項式 と呼び, 方程式 $g(x) = 0$ を n 次一般方程式 といふ. 2 次の一般方程式 $x^2 + a_1x + a_2 = 0$ は代数的に解けて, 解の公式

$$x = \frac{-a_1 \pm \sqrt{{a_1}^2 - 4a_2}}{2}$$

が知られてゐる. 3 次や 4 次の一般方程式も代数的に解けてその解の公式も与へられてゐる. しかるに 5 次以上の一般方程式は代数的には解けず, その様な解の公式は存在しない. これを最初に証明したのは N.H. Abel である. 以下, 21.17 を用ゐて一般方程式の可解性を調べる.

いま $t_1, t_2, \cdots, t_n$ は体 K 上代数的に独立であるとし, $L = K(t_1, \cdots, t_n)$ とおく. L は変数 $t_1, \cdots, t_n$ に関する有理函数体と呼ばれるものである. $\{1, 2, \cdots, n\}$ 上の対称群を S_n とすれば S_n の元 σ は ${t_i}^\sigma = t_{\sigma(i)}$ とおいて $\{t_1, \cdots, t_n\}$ の置換を引き起す. さて, K の各元を不変にして, それ以外の元には置換 σ を施すことによつて L/K の自己同型が得られる. それも σ で表すこととし $S_n < \mathrm{Aut}\, L/K$ とみなす. L における S_n の不変体を

$$F = L^{S_n} = K(t_1, \cdots, t_n)^{S_n}$$

と書けば, 15.7 により L/F は S_n を Galois 群とする Galois 拡大に他ならない. F に属する多項式は $t_1, \cdots, t_n$ の対称式と呼ばれ, そのうち次の形の式を 基本対称式 と呼ぶ :

$$s_1 = t_1 + t_2 + \cdots + t_n, \quad s_2 = \sum_{i<j} t_it_j, \quad \cdots, \ s_n = t_1t_2 \cdots t_n.$$

明らかに $K(s_1, s_2, \cdots, s_n) \subset F \subset L$ で, 15.7(3) により $[L : F] = |S_n| = n!$ であるが, 次のことが成り立つ.

例題 22.1. 上の記号の元で
(1) $K(s_1, \cdots, s_n) = F$.
(2) $s_1, \cdots, s_n$ は K 上代数的に独立である.

証明 (1) $[L : K(s_1, \cdots, s_n)] \leq n!$ となることを示せばよい. n に関する帰納法で証明する. $n = 1$ のときは明らかである. $M = K(s_1, \cdots, s_n)$ とし

$$f(x) = \prod_{i=1}^{n}(x - t_i) = x^n - s_1x^{n-1} + \cdots + (-1)^n s_n$$

とおけば $f(x) \in M[x]$, $f(t_n) = 0$ ゆゑ $[M(t_n) : M] \leq n$. 一方 $N = K(t_n)$ とおけば, $L = N(t_1, \cdots, t_{n-1})$ である. いま $t_1, \cdots, t_{n-1}$ に関する基本対称式を ${s_1}', \cdots, {s_{n-1}}'$ とすれば

$$s_1 = {s_1}' + t_n, \quad s_j = t_n{s_{j-1}}' + {s_j}' \quad (2 \leq j \leq n-1), \quad s_n = {s_n}'t_n$$

となるから, $K(s_1, \cdots, s_n, t_n) = K({s_1}', \cdots, {s_{n-1}}', t_n)$ となり, $M(t_n) = N({s_1}', \cdots, {s_{n-1}}')$ を得る. 帰納法の仮定により $[L : M(t_n)] \leq [L : K({s_1}', \cdots, {s_{n-1}}')] \leq (n-1)!$ である. よつて $[L : M] = [L : M(t_n)][M(t_n) : M] \leq (n-1)!\, n = n!$ となる.
(2) L/F は代数的であるから, 6.3 により $\mathrm{trans.deg}_K F = \mathrm{trans.deg}_K L = n$ となる. このとき (1) から, n 個の元 $s_1, \cdots, s_n$ は K 上代数的に独立でなければならない. □

22.1 から次の定理が得られる.

定理 22.2. $g(x) = x^n + a_1x^{n-1} + \cdots + a_n$ を体 K の一般多項式 (従つて $a_1, \cdots, a_n$ は K 上代数的独立) とし, E を $N = K(a_1, \cdots, a_n)$ 上の $g(x)$ の最小分解体とする. このとき E/N は n 次対称群 S_n と同型な Galois 群をもつ Galois 拡大である.

証明 22.1 で示した様に, $t_1, \cdots, t_n$ は K 上代数的に独立とし, これらに関する基本対称式を $s_1, \cdots, s_n$ とするとき, $L = K(t_1, \cdots, t_n)$ は $F = K(s_1, \cdots, s_n)$ 上の Galois 拡大で $\mathrm{Gal}\,(L/F) = S_n$, また $s_1, \cdots, s_n$ は K 上代数的に独立である. 従つて K 上の同型 $\sigma : N \xrightarrow{\sim} F$ $(a_i \mapsto (-1)^i s_i)$ があり, この写像で一般多項式 $g(x)$ は

$$g^\sigma(x) = x^n - s_1x^{n-1} + \cdots + (-1)^n s_n = \prod_{i=1}^{n}(x - t_i)$$

に写される. L は $g^\sigma(x)$ の F 上の最小分解体であるから, σ は $\overline{\sigma} : E \xrightarrow{\sim} L$ に拡張される (10.2 による). このとき $\varphi : \mathrm{Gal}\,(E/N) \to \mathrm{Gal}\,(L/F)$ $(\rho \mapsto \overline{\sigma}\rho\overline{\sigma}^{-1})$ は同型写像である. よつて $\mathrm{Gal}\,(E/N) \simeq S_n$ である. □

22.2 と 21.17 から次の定理が得られる.

定理 22.3. (Galois の定理) 体 K 上の n 次の一般方程式 $x^n + a_1x^{n-1} + \cdots + a_n = 0$ は $n \leq 4$ のとき, しかもそのときに限つて代数的に解ける.

証明 対称群 S_n は $n \leq 4$ のときは可解群であるが, $n \geq 5$ ならば非可解群であつた (22.6 で示される [27]). $x^n + a_1x^{n-1} + \cdots + a_n$ は素体 $\mathbb{Q}$ 上の一般多項式でもある. よつて 22.2 で $K = \mathbb{Q}$ とおけば, 21.17 から主張が導かれる. □

演 習 問 題

$n \geq 5$ のとき n 次対称群 S_n が可解群でないことを以下に従つて示せ.

22.4. $S_n = \langle (1\ 2), (1\ 3), \cdots, (1\ n) \rangle$ であることを示せ.
(Hint : $(i\ j) = (1\ i)(1\ j)(1\ i)$ であることと, S_n が互換の全体で生成されることを使ふ.)

22.5. $n \geq 3$ のとき, $A_n = \langle (1\ 2\ 3), (1\ 2\ 4), \cdots, (1\ 2\ n) \rangle$ であることを示せ.
(Hint : A_n が 2 個の互換の積の全体から生成されること, 22.4, および $(1\ 2)(1\ j) = (1\ 2\ j)^2$, $(1\ i)(1\ j) = (1\ 2\ i)(1\ 2\ j)^2$ $(3 \leq i, 3 \leq j)$ であることを使ふ.)

22.6. $n \geq 5$ とする. H は A_n の正規部分群で, A_n/H は Abel 群であるとせよ. 次の問に答へよ. 但し, i, j, k はどれも 1 でも 2 でもなく, 互ひに異る任意の数字の組である.
(1) $(1\ 2\ k) = (1\ i\ k)(k\ 2\ j)(1\ i\ k)^{-1}(k\ 2\ j)^{-1}$ を確かめよ.
(2) $(1\ 2\ k) \in H$ であることを示せ. (Hint : 仮定より $H \supset [A_n : A_n]$.)
(3) $H = A_n$ を示し, A_n が可解群でないことを確認せよ.

22.7. $n \geq 5$ とする. S_n は可解群でないことを示せ (Hint : 21.11).

[27] 代数学 3 で既習かも知れない.

23. 3 次の一般方程式の解法

a, b, c を不定元として, 3 次の一般方程式

$$f(x) = x^3 + ax^2 + bx + c = 0 \tag{23.1}$$

の解の公式を求めてみる. (23.1) の 3 つの解を t_1, t_2, t_3 とおく. 以下, $\omega = \frac{-1+\sqrt{-3}}{2}$, $K = \mathbb{Q}(a,b,c)$, $L = K(t_1,t_2,t_3)$ とする. 以下, 第 22 節の記号に従ふ. 22.3 が得られたといつても, そこから直ちに解の公式を書き下せるわけではなく, 別途, 作業が必要である. まづ, $S_3 = \mathrm{Gal}\,(L/K)$ とその部分群 $A_3 = \{\varepsilon,\ (1\ 2\ 3),\ (1\ 3\ 2)\}$ について, の正規列

$$S_3 \rhd A_3 \rhd \{1\}$$

において S_3/A_3 も A_3 も Abel 群であるから, 確かに S_3 は可解群である. このとき, $\Delta = (t_1-t_2)(t_2-t_3)(t_3-t_1)$ を不変にする元の全体が A_3 に一致する. もちろん $\Delta^2 \in K$ の筈であるが, 少し計算すれば $\Delta^2 = -4a^3c + a^2b^2 - 18abc + 4b^3 - 27c^2$ を得る. 上の正規列に対応して, 体の拡大列 $L \supset K(\Delta) \supset K$ ($[K(\Delta):K] = 2$) があるが, 21.17 により, L/K は冪根による拡大に含まれる筈である. 実際に, その様な冪根拡大を構成してみる. その際,

$$\beta = t_1 + \omega t_2 + \omega^2 t_3, \quad \gamma = t_1 + \omega^2 t_2 + \omega t_3$$

を考へることが鍵となる. $-a = t_1 + t_2 + t_3 \in K$ であるから, $K(\beta,\gamma,\omega) \supset L$ がわかるが, 体 $L(\omega) = K(\beta,\gamma,\omega)$ は K 上の冪根による拡大として記述できるのである. これは 12 次拡大である. 少し計算すれば $\beta\gamma = a^2 + 3b$, $\beta^3 + \gamma^3 = 2a^3 + 9ab + 27c$ を得,

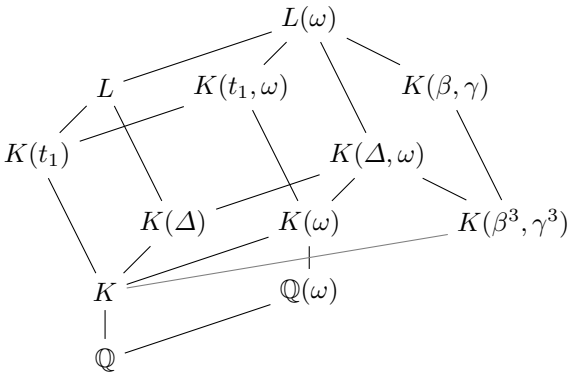
$$K(\beta,\gamma,\omega) = K(\beta,\omega) = K(\gamma,\omega)$$

がわかる. また β^3 と γ^3 は 2 次方程式

$$x^2 - (2a^3 + 9ab + 27c)x + (a^2 + 3b)^3 = 0$$

の 2 根である. また $f'(t_1) = 3{t_1}^2 + 2at_1 + b = (t_1-t_2)(t_1-t_3)$ で $t_2 - t_3 = -\Delta/f'(t_1) \in K(\Delta,t_1)$, $t_2 + t_3 = -a - t_1 \in K(t_1)$ だから $t_2, t_3 \in K(\Delta,t_1)$ がわかり $L = K(\Delta,t_1)$ である.

もちろん $f(t_1) = {t_1}^3 + a{t_1}^2 + bt_1 + c = 0$ であるから, $[L : K(\Delta)] = 3$ であり, L は $K(\Delta)$ 上の vector 空間としての基底 $\{1, t_1, {t_1}^2\}$ を持つ. ここで, $\omega \notin L = \mathbb{Q}(t_1,t_2,t_3)$ であることに注意されたい. つまり L は K 上の冪根による拡大に含まれるのであるが, L 自身は冪根による拡大にはならない.



演 習 問 題

23.2. 本文での説明と 16.12 を参考に, 3 次方程式 $x^3 + x + 1 = 0$ の解を四則演算と冪根のみで表せ.

23.3. 一般に 3 次の monic な既約多項式 $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Q}[x]$ について, その Galois 群は A_3 (3 次巡回群, $\lhd S_3$) または S_3 と同型になり, そのことは上記の Δ が $\mathbb{Q}$ 内の平方元であるか否かで, 判定できる. このことを示せ.

24. 4 次の一般方程式の解法

4 次一般方程式の解法を述べる. a, b, c, d を不定元として $K = \mathbb{Q}(a, b, c, d)$ とおき, K 上の 4 次多項式 $f(x) = x^4 + ax^3 + bx^2 + cx + d$ を考へる. t_1, t_2, t_3, t_4 を $f(x) = 0$ の根として, $L = K(t_1, t_2, t_3, t_4)$ とおく. 以下, 第 22 節の記号を踏襲してゐる. 4 次対称群 S_4 の正規列

$$S_4 \rhd A_4 \rhd V \rhd H \rhd \{1\}$$

を考へる. 但し, $V = \{\varepsilon, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$, $H = \{\varepsilon, (1\ 2)(3\ 4)\}$ である. (V が存在してゐるのは幸運.) ここで S_4/A_4, A_4/V, V/H, H はどれも Abel 群である. いま

$$\Delta = (t_1 - t_2)(t_1 - t_3)(t_1 - t_4)(t_2 - t_3)(t_2 - t_4)(t_3 - t_4) \quad (f(x) \text{ の } \underline{\text{判別式}} \text{ と呼ぶ})$$

とおくと, $\Delta^2 \in K$ である. $\mathrm{Gal}\,(L/K) = S_4$ とみて, 上の正規列に対応する体の拡大列は

$$K \subset K(\Delta) \subset K(t_1t_2 + t_3t_4, t_1t_3 + t_2t_4, t_1t_4 + t_2t_3) \subset K(t_1t_2 + t_3t_4) \subset K(t_1, t_2, t_3, t_4)$$

である (★). ここで $\alpha = t_1t_2 + t_3t_4$, $\beta = t_1t_3 + t_2t_4$, $\gamma = t_1t_4 + t_2t_3$ とおく. これらの基本対称式は a, b, c, d の $\mathbb{Q}$ 上の多項式の筈であるが,

$$\alpha + \beta + \gamma = b, \quad \alpha\beta + \beta\gamma + \gamma\delta = ac - 4d, \quad \alpha\beta\gamma = a^2d - 4bd + c^2$$

が, いくらかの計算ののち得られる. それゆゑ α, β, γ は K 上の 3 次方程式

$$g(y) = y^3 + by^2 - (ac - 4d)y + (a^2d - 4bd + c^2) = 0$$

の根として得られる. この方程式は, 第 23 節の方法で解ける. ここで, 容易に確かめられる

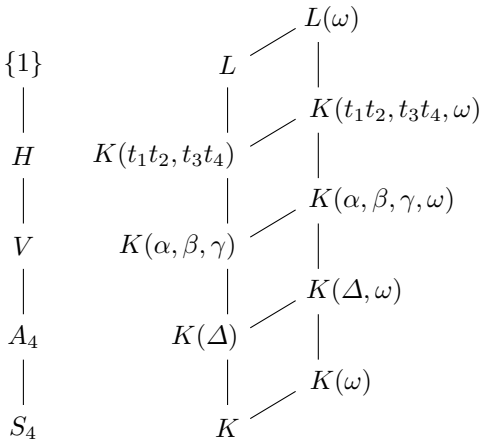
$$(\alpha - \beta)(\beta - \gamma)(\gamma - \alpha) = -\Delta$$

に注意せよ. さらに $t_1t_2 + t_3t_4 = \alpha$, $(t_1t_2)(t_3t_4) = d$ より t_1t_2 と t_3t_4 が 2 次方程式 $z^2 - \alpha z + d = 0$ の解として得られる. $(t_1 + t_2)t_3t_4 + (t_3 + t_4)t_1t_2 = -c$ と $t_1 + t_2 + t_3 + t_4 = -a$ から $t_1 + t_2$, $t_3 + t_4 \in K(t_1t_2, t_3t_4)$ がわかる :

$$K(t_1t_2, t_3t_4, t_1 + t_2, t_3 + t_4) = K(t_1t_2, t_3t_4).$$

$t_1 + t_2$ と t_1t_2 の値から 2 次方程式を解いて t_1 と t_2 が得られる. また, $t_3 + t_4$ と t_3t_4 の値から t_3 と t_4 が得られるが, これは $t_1t_2t_3 + \cdots + t_2t_3t_4 = -c$ と $t_1, t_2, t_3 + t_4, t_3t_4$ の値から 1 次方程式を解いても得られるから, 体の拡大は生じない.

ここで 1 つ注意をしておく. 3 次一般方程式の解法では, 1 の原始 3 乗根 ω を添加する必要があつた. しかし, この解法では, 正規列に 4 次巡回群が含まれないから, $i = \sqrt{-1}$ を添加する必要がない. 以上を図にまとめておく.



演 習 問 題

24.1. 本文中の (★) が正しいことを示せ.

24.2. 本文で説明した方法に沿つて, 4 次方程式 $x^4 + x + 1 = 0$ を解き, 解を四則演算と冪根のみで表せ.

25. 円分多項式

以下, 本節では有理数体 $\mathbb{Q}$ 上の円分体を考察する. 1 の原始 n 乗根 ζ を 1 つ固定し,

$$\Phi_n(x) = \prod_{\substack{0<r<n \\ \gcd(r,n)=1}} (x - \zeta^r)$$

とおく. これは 1 のすべての原始 n 乗根を根とする多項式で, n 次 円分多項式 と呼ばれる.

例 25.1. 円分多項式 $\Phi_n(x)$ の例を挙げておく. 素数 p については

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$$

である. その他を少し計算してみれば

$$\Phi_1(x) = x - 1, \quad \Phi_4(x) = x^2 + 1, \quad \Phi_6(x) = x^2 - x + 1, \quad \Phi_8(x) = x^4 + 1,$$
$$\Phi_9(x) = x^6 + x^3 + 1, \quad \Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1, \quad \Phi_{12}(x) = x^4 - x^2 + 1,$$
$$\Phi_{14}(x) = x^6 - x^5 + x^4 - x^3 + x^2 - x + 1, \quad \Phi_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1,$$
$$\Phi_{16}(x) = x^8 + 1, \quad \Phi_{18}(x) = x^6 - x^3 + 1, \quad \Phi_{18}(x) = x^8 - x^6 + x^4 - x^2 + 1, \quad \cdots\cdots$$

と, 係数が ± 1 のみになる様に見えるが, 反例がある :

$$\begin{aligned}\Phi_{105}(x) = {} & x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - \boxed{2}x^{41} - x^{40} - x^{39} + x^{36} + x^{35} + x^{34} \\ & + x^{33} + x^{32} + x^{31} - x^{28} - x^{26} - x^{24} - x^{22} - x^{20} + x^{17} + x^{16} + x^{15} \\ & + x^{14} + x^{13} + x^{12} - x^9 - x^8 - \boxed{2}x^7 - x^6 - x^5 + x^2 + x + 1.\end{aligned}$$

命題 25.2. 円分多項式について次が成り立つ
(1) $\deg \Phi_n(x) = \varphi(n)$ (Euler の函数).
(2) $x^n - 1 = \prod_{d|n} \Phi_d(x)$.
(3) $\Phi_n(x) \in \mathbb{Z}[x]$.

証明 (1) は明かである. また 1 の n 乗根の任意の 1 つを取れば, それは, 唯 1 つのある約数 $d|n$ に対して 1 の原始 d 乗根であるから, (2) が成り立つ. (3) を n の帰納法で示す. いま

$$x^n - 1 = \Phi_n(x)\, f(x), \quad f(x) = \prod_{d|n,\, d<n} \Phi_d(x) \tag{25.3}$$

とすれば, 帰納法の仮定により $f(x) \in \mathbb{Z}[x]$. また $f(x)$ の最高次の係数は 1 であるから, それは 原始多項式[28] である. (25.3) を利用しての, n に関する数学的帰納法から $\Phi_n(x) \in \mathbb{Q}[x]$ となることが示されるから, 下記の 25.4 により $\Phi_n(x) \in \mathbb{Z}[x]$ がわかる. □

問 25.4. R を一意分解環[29] (UFD) とし, K をその商体とせよ. $f(x),\ g(x) \in R[x]$ で $g(x) \in R[x]$ は原始多項式であるとせよ. $K[x]$ において $f(x) = g(x)\, h(x)$ $(h(x) \in K[x])$ と分解されれば, $h(x) \in R[x]$ である.

---

[28] $g(x) = a_0 x^n + a_{n-1} x^{n-1} + \cdots + a_n$ の係数の最大公約数が 1, $\gcd(a_0, \cdots, a_n) = 1$, であること.
[29] 可換環 R は, その零元と単元以外のあらゆる元が既約元の積に (単元の積を無視して) 一意的に分解できるとき , 一意分解環 (UFD) と呼ばれる.

定理 25.5. $\Phi_n(x)$ は $\mathbb{Q}[x]$ において既約な多項式である. 即ち $\Phi_n(x) = \mathrm{irr}\,(\zeta, \mathbb{Q}, x)$.

証明 ζ を 1 の原始 n 乗根とし, $f(x)$ を ζ を根とする既約かつ原始的な $\mathbb{Z}$ 上の多項式とする. このとき $f(x)\,|\,x^n - 1$ で, 25.4 から $x^n - 1 = f(x)g(x)$ となる $g(x) \in \mathbb{Z}[x]$ がある. いま p を n と互ひに素な任意の素数とすれば, $f(\zeta^p) = 0$ となることが次の様にして示される. これの否定 $f(\zeta^p) \neq 0$ を仮定する. このとき $g(\zeta^p) = 0$ でなくてはならない. $g(x^p)$ は ζ を根にもつから $g(x^p) = f(x)h(x)$ となる $h(x) \in \mathbb{Z}[x]$ が存在する. いま任意の元 $a \in \mathbb{Z}$ に対し, 対応する剰余類を $\overline{a} \in \mathbb{F}_p$ と記し, 任意の多項式 $\varphi(x) \in \mathbb{Z}[x]$ に対し, その係数を対応する剰余類に置き替へたものを $\overline{\varphi}(x)$ と書くことにする. このとき $\overline{a}^{\,p} = \overline{a}$ に注意すれば,

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

であるから, $\overline{f}(x)$ と $\overline{g}(x)$ は共通根を持つ. 従つて $\mathbb{F}_p$ 上で $x^n - 1 = \overline{f}(x)\overline{g}(x)$ は重根を持ち, これは仮定 $\gcd(p, n) = 1$ に矛盾する. 上のことを用ゐて, 一般に $\gcd(r, n) = 1$ ならば ζ^r は $f(x)$ の根になることが, r の素因数の個数に関する帰納法で示される. 従つて $\Phi_n(x)|f(x)$ となるが, $f(x)$ は既約であるから $f(x) = c\Phi_n(x)$ $(c \in \mathbb{Q}^\times)$ となつて $\Phi_n(x)$ も既約である. □

系 25.6. 1 の n 乗根全体のなす群を $U_n \subset \overline{\mathbb{Q}}$ とおく. $\mathrm{Gal}\,(\mathbb{Q}(U_n)/\mathbb{Q})$ は $(\mathbb{Z}/n\mathbb{Z})^\times$ と同型である.

証明 20.4 の証明の前半で述べた通り $\mathrm{Gal}\,(\mathbb{Q}(U_n)/\mathbb{Q})$ は $(\mathbb{Z}/n\mathbb{Z})^\times$ の部分群と同型である. しかるに, $\mathbb{Q}(U_n)$ は $\Phi_n(x)$ の最小分解体であるから, 25.5 と 25.2 (1) により, $\mathrm{Gal}\,(\mathbb{Q}(U_n)/\mathbb{Q})$ の位数は $\varphi(n)$ であり, これは $(\mathbb{Z}/n\mathbb{Z})^\times$ の位数に他ならない. ゆゑに, この 2 群は同型でなければならない. □

問 25.7. ζ を 1 の原始 n 乗根とする. $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$ を示せ.

演 習 問 題

25.8. 任意の $n \in \mathbb{N}$ をとれ. このとき $p \equiv 1 \mod n$ なる素数 p が無数に存在することを次の方針で示せ. $\{p_1, p_2, \cdots, p_k\}$ をその様な素数の任意の集合とせよ (空集合でも良い). $a = np_1p_2\cdots p_k$ とおいて $\Phi_n(a)$ を考察する. 次の問に答へよ.

(1) $\Phi_n(a)$ は $1, -1$ ではないことを示せ.

(Hint : 複素数平面における絶対値と $\Phi_n(x)$ の定義.)

(2) $q > 1$ を $\Phi_n(a)$ の 1 つの素因子とせよ. このとき $q \equiv 1 \mod n$ であることを示せ.

(Hint : m を $a \in (\mathbb{Z}/q\mathbb{Z})^\times$ とみたときの位数とせよ. $\Phi_n(a)|a^n - 1$ であるから $a^n \equiv 1 \mod q$. ゆゑに $m|n$. ここで $m < n$ と仮定する. 一方 $a^m - 1 = \prod_{d|m}\Phi_d(a) \equiv 0 \mod q$ であるからある $d|m$ について $\Phi_d(a) \equiv 0 \mod q$. しかも $\Phi_n(a) \equiv 0 \mod q$ であるから, 結局 a は $x^n - 1 = \prod_{d|n}\Phi_d(a) \in \mathbb{F}_q[x]$ の重根である. 12.2(1) によれば $na^{n-1} \equiv 0 \mod q$ でなければならない. しかるに $q \nmid a$, $n|a$ より $q \nmid n$ でなければならないので, 矛盾が生ずる. よつて $m = n$. Fermat の小定理から $m = n$ は $q - 1$ の約数でなければならず, $q - 1 \equiv 0 \mod n$.)

(3) 上の q は集合 $\{p_1, p_2, \cdots, p_k\}$ に含まれないことを示せ. (Hint : $q|\Phi_n(a) \equiv \pm 1 \mod a$.)

以上から, 限りなく $p \equiv 1 \mod n$ なる素数 p を見出すことができるから, その様な素数は無限に存在する.

26. 群の作用

定義 26.1. 群 G と集合 X, および写像 $X \times G \to X$, $(\alpha, a) \mapsto \alpha^a$ が与へられてゐて, 任意の $a, b \in G$, $\alpha \in X$ について
A1. $\alpha^1 = \alpha$,
A2. $\alpha^{ab} = (\alpha^b)^a$
の 2 つが共に成り立つとき, G は X に 作用 するといふ. さらに, 任意の $\alpha, \beta \in X$ に対し $\alpha^a = \beta$ となる元 $a \in G$ が存在するとき, G は X に 可移的 に作用するといふ.

例 26.2. 作用の例とさうでない例を記す.
(1) 加法を演算とする群 $G = \mathbb{Z}$ と $X = \mathbb{Z}$ について

$$\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (m, n) \mapsto m + n$$

は作用である. これは可移的である.
(2) 乗法を演算とする群 $G = \mathbb{Q}^\times$ と $X = \mathbb{Q}$ について

$$\mathbb{Q} \times \mathbb{Q}^\times \to \mathbb{Q}, \quad (x, y) \mapsto x + y$$

は作用ではない.
(3) Galois 拡大 L/K とその Galois 群 $\mathrm{Gal}(L/K)$ について,

$$L \times \mathrm{Gal}(L/K) \to L, \quad (\alpha, \sigma) \mapsto \alpha^\sigma$$

は作用である. これは可移的ではない.
(4) K を体とし, これの代数的閉包 $\overline{K}$ を 1 つ固定する. α の $\overline{K}$ 内の K 上の共役元のすべてからなる集合を $S = \{\alpha_1, \cdots, \alpha_n\}$ とし, $L = K(\alpha_1, \cdots, \alpha_n)$ とせよ. このとき

$$S \times \mathrm{Gal}(L/K) \to S, \quad (\alpha_i, \sigma) \mapsto {\alpha_i}^\sigma$$

は作用である. これは可移的である.

作用を利用すると, 新しく群を見出すこともできる. 例へば p 元体 $\mathbb{F}_p$ を $\mathbb{F}_p$ 自身の上の 1 次元 vector 空間として, vector $a \in \mathbb{F}_p$ による “a 移動”

$$\mathbb{F}_p \ \to \ \mathbb{F}_p, \quad v \mapsto v + a$$

および $b \in {\mathbb{F}_p}^\times$ による “b 倍”

$$\mathbb{F}_p \ \to \ \mathbb{F}_p, \quad v \mapsto bv$$

を考へると, これら写像の全体とそれらの合成は $\mathbb{F}_p$ と ${\mathbb{F}_p}^\times$ の元の組からなるある群を成してゐて, それが $\mathbb{F}_p$ に作用してゐると見做せる. 例へば $p = 5$ とすれば ${\mathbb{F}_5}^\times$ の原始根として 2 が取れる. いま 5 元集合 $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$ に関する対称群 S_5 を使へば, 元 (0 1 2 3 4) と (2 4 3 1) がそれぞれ “1 移動” と “2 倍” を表してゐて,

$$(0\ 1\ 2\ 3\ 4) : \ \mathbb{F}_p \ \to \ \mathbb{F}_p, \quad v \mapsto v + 1$$
$$(2\ 4\ 3\ 1) : \ \mathbb{F}_p \ \to \ \mathbb{F}_p, \quad v \mapsto 2v$$

であり, これらの生成する群 $H < S_5$ が見付かつた.

問 26.3. 上の群 H の元を全て書き上げよ. 位数はいくつか. また, H が 21.20 の $\mathrm{Gal}\,(K/\mathbb{Q})$ と同型であることを示せ.

索 引